EXPRESSCLUSTER X 4.2 for Linux
Reference Guide

Release 2

NEC Corporation

Jul 10, 2020

TABLE OF CONTENTS:

1 Preface **1**
- 1.1 Who Should Use This Guide . . . 1
- 1.2 How This Guide is Organized . . . 1
- 1.3 EXPRESSCLUSTER Documentation Set . . . 1
- 1.4 Conventions . . . 2
- 1.5 Contacting NEC . . . 3

2 Parameter details **5**
- 2.1 Parameter settings . . . 5
- 2.2 Cluster properties . . . 5
- 2.3 Server Common Properties . . . 57
- 2.4 Server properties . . . 59
- 2.5 Group Properties . . . 65
- 2.6 Group Resource Properties . . . 66
- 2.7 Monitor Resource Properties . . . 66
- 2.8 Parameters list . . . 66
- 2.9 Upper limits of registration . . . 113

3 Group resource details **115**
- 3.1 Group resources and supported EXPRESSCLUSTER versions . . . 116
- 3.2 Attributes common to group resources . . . 117
- 3.3 Group common properties . . . 144
- 3.4 Group properties . . . 146
- 3.5 Resource Properties . . . 155
- 3.6 Understanding EXEC resources . . . 164
- 3.7 Understanding Disk resource . . . 190
- 3.8 Understanding Floating IP resource . . . 198
- 3.9 Understanding Virtual IP resources . . . 208
- 3.10 Understanding Mirror disk resources . . . 219
- 3.11 Understanding Hybrid disk resources . . . 251
- 3.12 Understanding NAS resource . . . 261
- 3.13 Understanding Volume manager resources . . . 265
- 3.14 Understanding VM resources . . . 274
- 3.15 Understanding Dynamic DNS resources . . . 279
- 3.16 Understanding AWS Elastic IP resources . . . 285
- 3.17 Understanding AWS Virtual IP resources . . . 288
- 3.18 Understanding AWS DNS resources . . . 293
- 3.19 Understanding Azure probe port resources . . . 296
- 3.20 Understanding Azure DNS resources . . . 299
- 3.21 Understanding Google Cloud Virtual IP resources . . . 302

3.22 Understanding Oracle Cloud Virtual IP resources . . . 304

4 Monitor resource details **307**
4.1 Monitor resource . . . 309
4.2 Monitor resource properties . . . 363
4.3 Understanding the disk monitor resources . . . 371
4.4 Understanding IP monitor resources . . . 377
4.5 Understanding floating IP monitor resources . . . 379
4.6 Understanding NIC Link Up/Down monitor resources . . . 380
4.7 Understanding mirror disk connect monitor resources . . . 382
4.8 Understanding mirror disk monitor resources . . . 383
4.9 Understanding hybrid disk connect monitor resources . . . 383
4.10 Understanding hybrid disk monitor resources . . . 384
4.11 Understanding PID monitor resources . . . 384
4.12 Understanding User mode monitor resources . . . 385
4.13 Understanding multi target monitor resources . . . 392
4.14 Understanding virtual IP monitor resources . . . 395
4.15 Understanding ARP monitor resources . . . 396
4.16 Understanding custom monitor resources . . . 397
4.17 Understanding volume manager monitor resources . . . 399
4.18 Understanding message receive monitor resources . . . 401
4.19 Understanding VM monitor resources . . . 405
4.20 Understanding Dynamic DNS monitor resources . . . 406
4.21 Understanding process name monitor resources . . . 407
4.22 Understanding BMC monitor resources . . . 408
4.23 Understanding DB2 monitor resources . . . 409
4.24 Understanding FTP monitor resources . . . 412
4.25 Understanding HTTP monitor resources . . . 413
4.26 Understanding IMAP4 monitor resources . . . 415
4.27 Understanding MySQL monitor resources . . . 417
4.28 Understanding NFS monitor resources . . . 420
4.29 Understanding ODBC monitor resources . . . 422
4.30 Understanding Oracle monitor resources . . . 425
4.31 Understanding Oracle Clusterware Synchronization Management monitor resources . . . 431
4.32 Understanding POP3 monitor resources . . . 431
4.33 Understanding PostgreSQL monitor resources . . . 433
4.34 Understanding Samba monitor resources . . . 436
4.35 Understanding SMTP monitor resources . . . 438
4.36 Understanding SQL Server monitor resources . . . 439
4.37 Understanding Sybase monitor resources . . . 443
4.38 Understanding Tuxedo monitor resources . . . 446
4.39 Understanding Weblogic monitor resources . . . 447
4.40 Understanding Websphere monitor resources . . . 450
4.41 Understanding WebOTX monitor resources . . . 451
4.42 Understanding JVM monitor resources . . . 453
4.43 Understanding System monitor resources . . . 502
4.44 Understanding Process resource monitor resources . . . 510
4.45 Understanding AWS Elastic IP monitor resources . . . 514
4.46 Understanding AWS Virtual IP monitor resources . . . 515
4.47 Understanding AWS AZ monitor resources . . . 516
4.48 Understanding AWS DNS monitor resources . . . 517
4.49 Understanding Azure probe port monitor resources . . . 519
4.50 Understanding Azure load balance monitor resources . . . 519
4.51 Understanding Azure DNS monitor resources . . . 520

4.52 Understanding Google Cloud Virtual IP monitor resources . . . 521
4.53 Understanding Google Cloud load balance monitor resources . . . 522
4.54 Understanding Oracle Cloud Virtual IP monitor resources . . . 522
4.55 Understanding Oracle Cloud load balance monitor resources . . . 523

5 Heartbeat resources details 525
5.1 What are heartbeat resources? . . . 525
5.2 Understanding LAN heartbeat resources . . . 527
5.3 Understanding kernel mode LAN heartbeat resources . . . 527
5.4 Understanding disk heartbeat resources . . . 528
5.5 Understanding COM heartbeat resources . . . 530
5.6 Understanding BMC heartbeat resources . . . 530
5.7 Understanding Witness heartbeat resources . . . 531

6 Network partition resolution resources details 533
6.1 Network partitions . . . 533
6.2 Understanding the network partition resolution resources . . . 533
6.3 Understanding network partition resolution by PING method . . . 534
6.4 Understanding network partition resolution by HTTP method . . . 535
6.5 Not resolving network partition . . . 536

7 Information on other settings 537
7.1 Shutdown monitoring . . . 537
7.2 Bonding . . . 540
7.3 Forced stop . . . 544
7.4 Script for forced stop . . . 547
7.5 Chassis Identify . . . 549
7.6 Alert Service . . . 552
7.7 SNMP linkage . . . 554
7.8 Cluster service automatic startup prohibition after improper stop . . . 559
7.9 Grace period dependence at the automatic failover between server groups . . . 560
7.10 Witness server service . . . 561

8 EXPRESSCLUSTER command reference 565
8.1 Operating the cluster from the command line . . . 566
8.2 EXPRESSCLUSTER commands . . . 567
8.3 Displaying the cluster status (clpstat command) . . . 569
8.4 Operating the cluster (clpcl command) . . . 587
8.5 Shutting down a specified server (clpdown command) . . . 591
8.6 Shutting down the entire cluster (clpstdn command) . . . 592
8.7 Operating groups (clpgrp command) . . . 593
8.8 Collecting logs (clplogcc command) . . . 598
8.9 Changing, backing up, and checking cluster configuration data (clpcfctrl command) . . . 607
8.10 Adjusting time-out temporarily (clptoratio command) . . . 626
8.11 Modifying the log level and size (clplogcf command) . . . 628
8.12 Managing licenses (clplcnsc command) . . . 638
8.13 Locking disk I/O (clproset command) . . . 644
8.14 Mirror-related commands . . . 645
8.15 Hybrid-disk-related commands . . . 678
8.16 Outputting messages (clplogcmd command) . . . 707
8.17 Controlling monitor resources (clpmonctrl command) . . . 709
8.18 Controlling group resources (clprsc command) . . . 714
8.19 Controlling reboot count (clpregctrl command) . . . 718
8.20 Turning off warning light (clplamp command) . . . 720
8.21 Controlling CPU frequency (clpcpufreq command) . . . 720

8.22 Controlling chassis identify lamp (clpledctrl command) . . . 723
8.23 Processing inter-cluster linkage (clptrnreq command) . . . 725
8.24 Requesting processing to cluster servers (clprexec command) . . . 727
8.25 Changing BMC information (clpbmccnf command) . . . 730
8.26 Controlling cluster activation synchronization wait processing (clpbwctrl command) . . . 731
8.27 Estimating the amount of resource usage (clpprer command) . . . 732
8.28 Checking the process health (clphealthchk command) . . . 737
8.29 Controlling the rest point of DB2 (clpdb2still command) . . . 739
8.30 Controlling the rest point of MySQL (clpmysqlstill command) . . . 741
8.31 Controlling the rest point of Oracle (clporclstill command) . . . 743
8.32 Controlling the rest point of PostgreSQL (clppsqlstill command) . . . 745
8.33 Controlling the rest point of SQL Server (clpmssqlstill command) . . . 747
8.34 Controlling the rest point of Sybase (clpsybasestill command) . . . 749
8.35 Displaying the cluster statistics information (clpperfc command) . . . 751
8.36 Checking the cluster configuration information (clpcfchk command) . . . 753

9 Troubleshooting **755**
9.1 Troubleshooting . . . 755
9.2 Troubleshooting problems with VERITAS volume manager . . . 786
9.3 To confirm the progress of the fsck / xfs_repair command . . . 789

10 Error messages **791**
10.1 Messages . . . 791
10.2 Messages reported by syslog, alert, mail, and SNMP trap . . . 791
10.3 Driver syslog messages . . . 899
10.4 Detailed information in activating and deactivating group resources . . . 935
10.5 Detailed info of monitor resource errors . . . 951
10.6 JVM monitor resource log output messages . . . 983

11 Glossary **1009**

12 Legal Notice **1011**
12.1 Disclaimer . . . 1011
12.2 Trademark Information . . . 1011

13 Revision History **1013**

CHAPTER

ONE

PREFACE

1.1 Who Should Use This Guide

The *EXPRESSCLUSTER X Reference Guide* is intended for system administrators. Detailed information for setting up a cluster system, function of the product, and how to troubleshoot the problems are covered in this guide. The guide provides supplemental information to the *Installation and Configuration Guide*.

1.2 How This Guide is Organized

- 2. *Parameter details*: Provides information on parameters configured in EXPRESSCLUSTER.
- 3. *Group resource details*: Provides information on group resource which configures a failover group.
- 4. *Monitor resource details*: Provides information on monitor resource which works as a monitoring unit in EXPRESSCLUSTER.
- 5. *Heartbeat resources details*: Provides information on heartbeat resource.
- 6. *Network partition resolution resources details*: Provides information on the network partition resolution resource.
- 7. *Information on other settings*: Provides information on other configurations.
- 8. *EXPRESSCLUSTER command reference*: Provides information on commands available to use in EXPRESSCLUSTER.
- 9. *Troubleshooting*: Provides instruction on how to troubleshoot the problem.
- 10. *Error messages*: Provides explanation on error messages displayed during EXPRESSCLUSTER operation.
- 11. *Glossary*

1.3 EXPRESSCLUSTER Documentation Set

The EXPRESSCLUSTER manuals consist of the following four guides. The title and purpose of each guide is described below.

EXPRESSCLUSTER X Getting Started Guide

> This guide is intended for all users. The guide covers topics such as product overview, system requirements, and known problems.

EXPRESSCLUSTER X Installation and Configuration Guide

This guide is intended for system engineers and administrators who want to build, operate, and maintain a cluster system. Instructions for designing, installing, and configuring a cluster system with EXPRESSCLUSTER are covered in this guide.

EXPRESSCLUSTER X Reference Guide

This guide is intended for system administrators. The guide covers topics such as how to operate EXPRESSCLUSTER, function of each module and troubleshooting. The guide is complement to the *Installation and Configuration Guide*.

EXPRESSCLUSTER X Maintenance Guide

This guide is intended for administrators and for system administrators who want to build, operate, and maintain EXPRESSCLUSTER-based cluster systems. The guide describes maintenance-related topics for EXPRESSCLUSTER.

EXPRESSCLUSTER X Hardware Feature Guide

This guide is intended for administrators and for system engineers who want to build EXPRESSCLUSTER-based cluster systems. The guide describes features to work with specific hardware, serving as a supplement to the Installation and Configuration Guide.

EXPRESSCLUSTER X Legacy Feature Guide

This guide is intended for administrators and for system engineers who want to build EXPRESSCLUSTER-based cluster systems. The guide describes EXPRESSCLUSTER X 4.0 WebManager, Builder, and EXPRESSCLUSTER Ver 8.0 compatible commands.

1.4 Conventions

In this guide, **Note**, **Important**, **Related Information** are used as follows:

Note: Used when the information given is important, but not related to the data loss and damage to the system and machine.

Important: Used when the information given is necessary to avoid the data loss and damage to the system and machine.

See also:

Used to describe the location of the information given at the reference destination.

The following conventions are used in this guide.

Convention	Usage	Example
Bold	Indicates graphical objects, such as fields, list boxes, menu selections, buttons, labels, icons, etc.	In **User Name**, type your name. On the **File** menu, click **Open Database**.
Angled bracket within the command line	Indicates that the value specified inside of the angled bracket can be omitted.	`clpstat -s [-h host_name ]`

Continued on next page

Table 1.1 – continued from previous page

Convention	Usage	Example
Monospace (courier)	Indicates path names, commands, system output (message, prompt, etc.), directory, file names, functions and parameters.	`c:\Program files\ EXPRESSCLUSTER`
Monospace bold (courier)	Indicates the value that a user actually enters from a command line.	Enter the following: **clpcl -s -a**
Monospace italic (courier)	Indicates that users should replace italicized part with values that they are actually working with.	`clpstat -s [-h` *`host_name`*`]`

1.5 Contacting NEC

For the latest product information, visit our website below:

https://www.nec.com/global/prod/expresscluster/

CHAPTER

TWO

PARAMETER DETAILS

This chapter describes the details of the parameters configured in EXPRESSCLUSTER.

This chapter covers:

- 2.1. *Parameter settings*
- 2.2. *Cluster properties*
- 2.3. *Server Common Properties*
- 2.4. *Server properties*
- 2.5. *Group Properties*
- 2.6. *Group Resource Properties*
- 2.7. *Monitor Resource Properties*
- 2.8. *Parameters list*
- 2.9. *Upper limits of registration*

2.1 Parameter settings

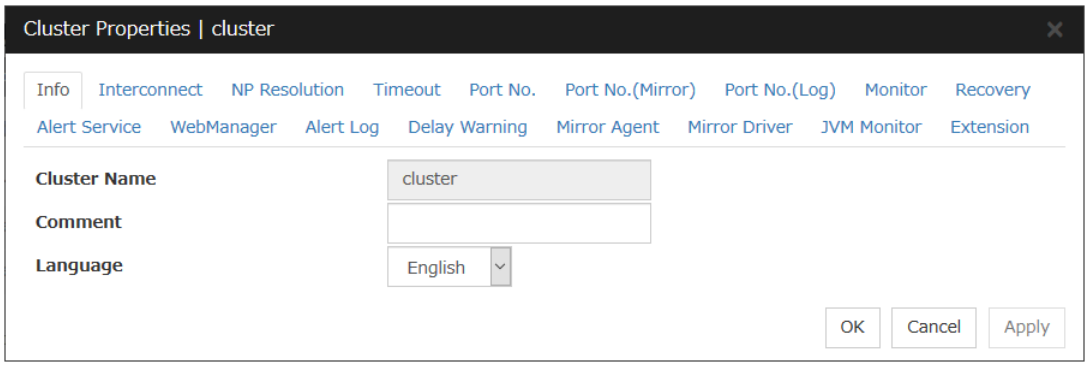
This section describes the details of the parameters configured in EXPRESSCLUSTER.
Use Cluster WebUI to configure the parameters.
For more information of Cluster WebUI, refer to the online manual of Cluster WebUI.

2.2 Cluster properties

In **Cluster Properties**, you can view and change the cluster's settings.

2.2.1 Info tab

You can view the cluster name, and enter or change a comment for this cluster.



Cluster Name

The cluster name is displayed. You cannot change the name here.

Comment (Within 127 bytes)

You can enter a comment for the cluster. Only alphanumeric characters are allowed.

Language

Select a language for cluster from the following. Set the language (locale) of OS on which the Cluster WebUI runs.

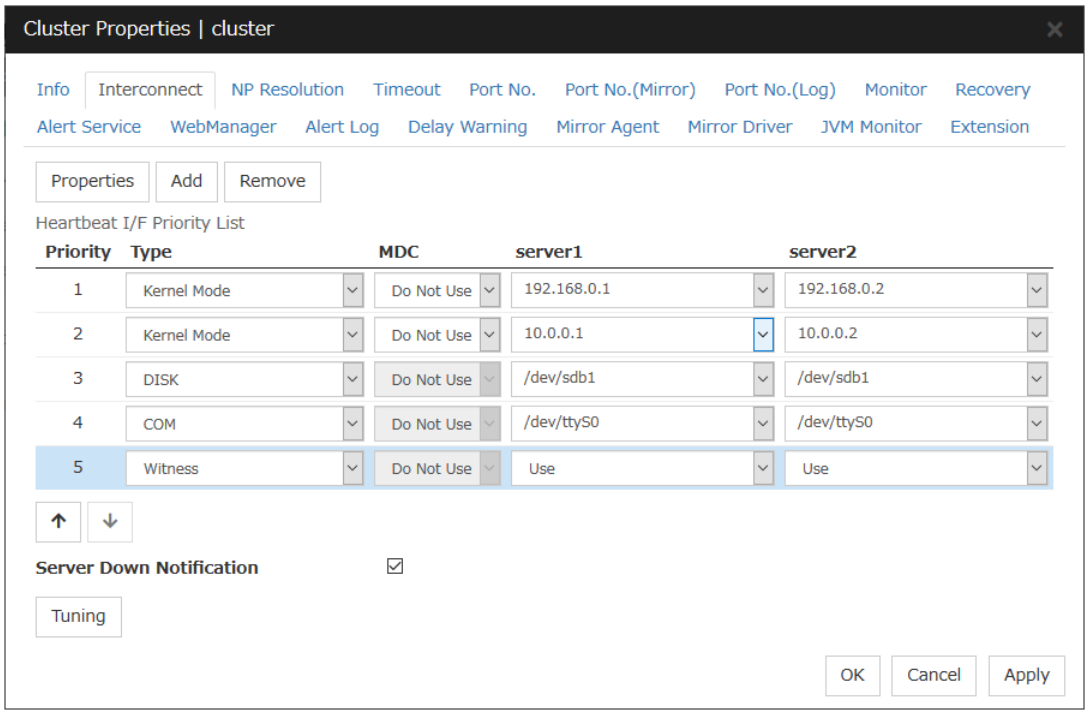
- English
- Japanese
- Chinese

Cluster WebUI and the results of clpstat command are displayed in the language set in the **Language** settings on the cluster properties.

Note: Run the clpstat command in the environment where the font of the specified language can be displayed. On the console which is connected to a server directly, setting a frame buffer is required. When logging on to the server remotely using ssh, a terminal emulator which can display the specified language may be needed.

2.2.2 Interconnect tab

This tab allows you to set up network communication paths between cluster servers.



The **Communication paths between servers list** displays network communication paths between servers in the cluster.

Add

Adds a communication path. To specify the IP address of the communication path for each server, click a cell in each server's column, and then select or enter the address. If some servers are not connected on the communication path, leave the cells for all the unconnected servers empty.

Remove

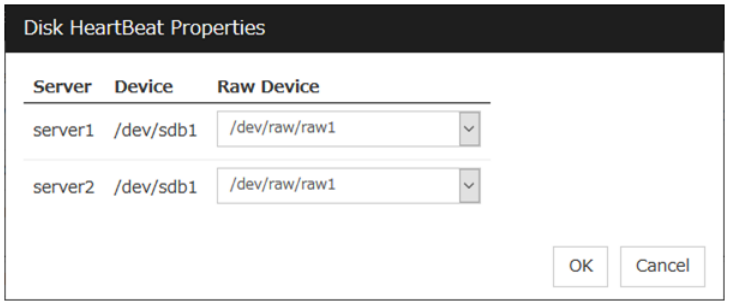
Removes a communication path. Select the column of the communication path to remove, and then click **Remove** to remove the selected path.

Properties

Displays heartbeat properties window. This is only available only when the type is DISK or Witness.

DISK HeartBeat Properties

Displays DISK heartbeat properties.



Server

Displays server list.

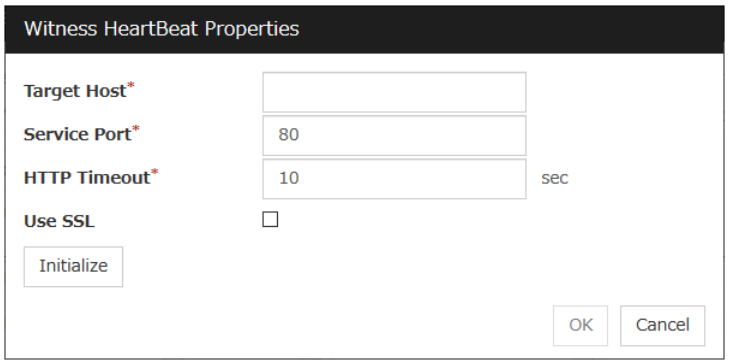
Device

Displays the device configured in the previous window.

Raw Device

When using RAW device, set RAW device by selecting or entering directly.
When not using RAW device, set blank.

Witness heartbeat properties



Target host

Sets the host address of the Witness server to be connected.

Service port

Sets the port number of the Witness server to be connected.

Use SSL

Configures whether or not to use SSL for communicating with the Witness server. When the checkbox is selected, SSL is used, and when the checkbox is not selected, it is not used.

Use OpenSSL 1.0/1.1 for SSL. By default, the following libraries are used:

- libssl.so.10 (if you installed the rpm package of EXPRESSCLUSTER)
- libssl.so.1.0.0 (if you installed the deb package of EXPRESSCLUSTER)

To use other libraries, go to the **Encryption** tab and set **SSL Library** and **Crypto Library**.

Use Proxy

Configures whether or not to use a proxy for communicating with the Witness server. When the checkbox is selected, the settings of the **Proxy** tab in the server properties become effective. When the checkbox is not selected, any proxy setting is not used even if the proxy is set in the server properties.

HTTP Timeout

Sets the timeout of receiving HTTP response.

Initialize

Resets the Witness heartbeat properties settings to default values.

Priority

When multiple interconnects are configured, the communication path with the smallest number in the **Priority** column is used preferentially for the internal communication among cluster servers. To change the priority, change the order of selected rows with the arrows.

It is recommended to specify a higher priority for the interconnect communication path than any other paths.

Note: **Priority** is used to decide on the priority of communication routes used for internal communication between the servers in the cluster. Heartbeat between the servers in the cluster is implemented on all communication routes that are set up for heartbeat, regardless of **Priority**.

Type

Select the path to be used for heartbeat from **Kernel Mode**, **User Mode**, **DISK**, **COM, BMC, Witness**, or **Mirror Communication Only**

- **Kernel mode** performs alive monitoring by using kernel mode LAN heartbeat resources.
- **User Mode** performs alive monitoring by using LAN heartbeat resources.
- **DISK** performs alive monitoring by using disk heartbeat resources.
- **COM** performs alive monitoring by using COM heartbeat resources.
- **BMC** performs alive monitoring by using BMC heartbeat resources.
- **Witness** performs alive monitoring by using Witness heartbeat resources.

For details about the heartbeat resources, see "5. *Heartbeat resources details*"in this guide.

MDC

To use a communication path as the mirror disk connect, click **MDC** and then select **Mirror Connect Disk**.

The contents to be entered differ by type.

- **Kernel Mode, User Mode, Mirror Communication Only**
  Select **Mirror Disk Connect** from the combo box.
  When the mirror disk connect is not used, select **Do Not Use**.

Note: A combination of IPv4 and IPv6 is not allowed for the IP addresses that are used for mirror disk connects. Specify IP addresses in either IPv4 only or IPv6 only for all mirror disk connects.

- **DISK, COM, BMC, Witness**
  The mirror disk connect cannot be used.
  MDC automatically changes to **Do Not Use** and can no longer be edited.

Server column

Entry differs depending on the type.

- **Kernel Mode, User Mode, Mirror Communication Only**
  Enter IP address. Set blank to the not used communication path.
- **DISK**
  Enter disk device. Set blank when not using DISK device.
- **COM**
  Enter COM device. Set blank when not using COM device.
- **BMC**
  Enter the IP address of the BMC. Set blank when not using the BMC.

- **Witness**
  Select **Use** or **Do Not Use**.

Note:

More than one IP addresses which belong to the same network address cannot exist in a single server. And also, inclusive relation cannot exist like the following relation.
IP address:10.1.1.10, subnet mask:255.255.0.0
IP address:10.1.2.10, subnet mask:255.255.255.0

Server down notification

When a server stops successfully (including a shutdown or reboot), the server is reported to be down to other servers in the cluster. You can perform failovers faster by reporting this in advance.

When there is a failure to deactivate groups when a server stops (including a shutdown or reboot), or when other abnormalities occur, other servers are not notified of the server that went down regardless of the server down notification settings.

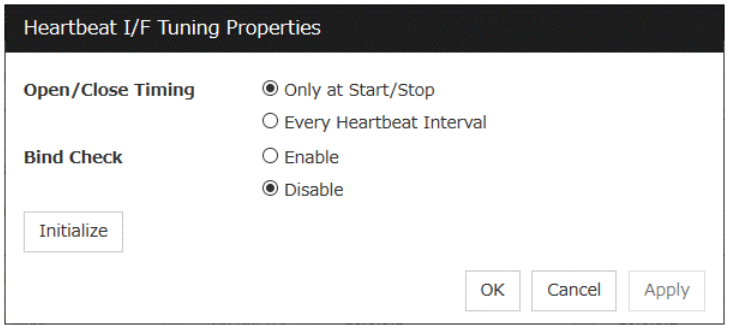
- When Follow the default dependence is selected:
  A server going down is reported.
- When Follow the default dependence is not selected:
  A server going down is not reported.

Note: Do not use server down notification when using a hybrid disk resource.

Tuning

Displays heartbeat I/F tuning property window.

Heartbeat I/F Tuning Properties



- **Open/Close Timing**
  - Only at Start/Stop
    Opens raw device when a cluster starts and close it when a cluster stops. Performs only reads and writes of raw device at each heartbeat interval.
  - Every Heartbeat Interval
    Opens raw device when a cluster starts, and closes it when a cluster stops. Performs open, reads, writes and close of raw device at each heartbeat interval.
- **Bind Check**
  - Enable

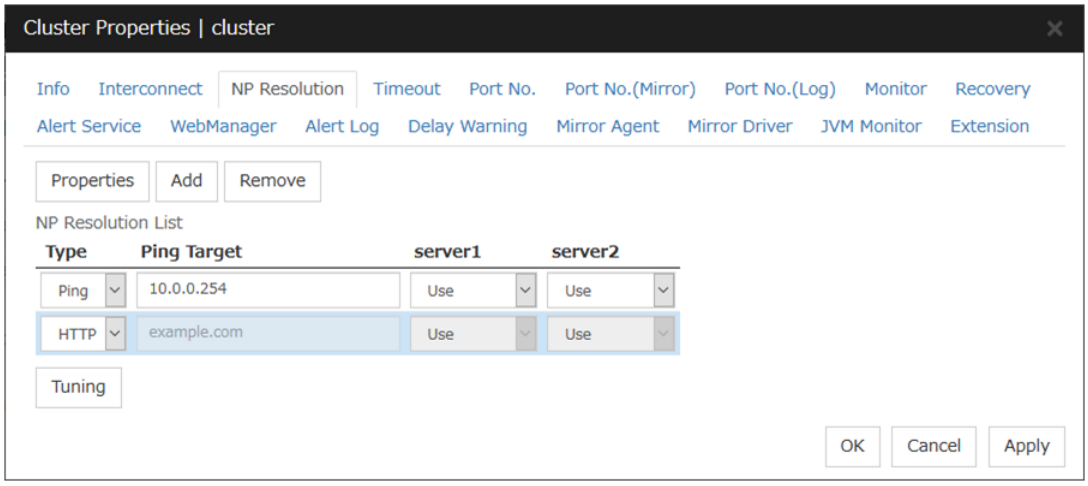
Checks if raw device for disk heartbeat is not bound to the actual device other than for disk heartbeat. Binding raw device is not performed if it is bound to the actual device other than for disk heartbeat. When binding a disk is not performed, the status of disk heartbeat resource becomes offline.

– Disable

Does not check if raw device for disk heartbeat is not bound to the actual device other than for disk heartbeat. If raw device is bound to the actual device other than for disk heartbeat, the bind is canceled and raw device is bound to the actual device for disk heartbeat.

2.2.3 NP Resolution tab

Change the setting of the network partition interface. The network partition resolution interface used for EXPRESSCLUSTER is displayed on the **NP**.



Add

Add network partition resolution I/F. Click the **Type** column cell and select the type of NP resolution (**Ping** or **HTTP**). If you select **Ping**, click the **Ping target** column cell and set the IP address. Click the cell of each server and set **Use** or **Do Not Use**.

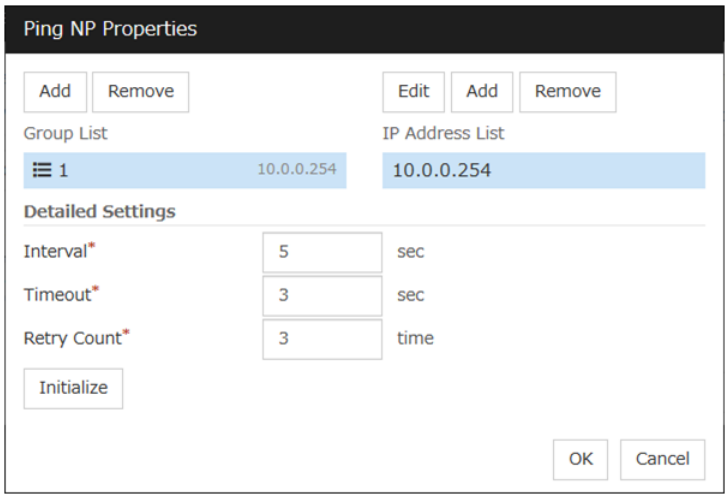
Remove

Remove network partition resolution I/F. Select network partition resolution I/F to be removed and click **Remove**, then the selected network partition resolution I/F is removed.

Properties

Display the **Ping NP Properties** or the **HTTP NP Properties** window.

Ping NP Properties

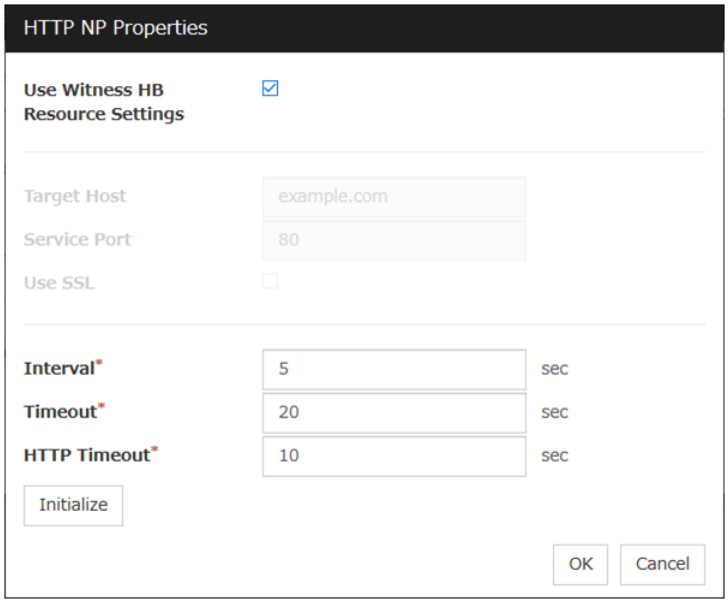


- Add Group List
  - Add group.
  - The maximum number of registered group is 16.
  - If multiple IP addresses are registered in one group, and if the state in which no response to the Ping command is returned from all the IP addresses is maintained, NP resolution processing cannot be performed (if there is even one IP address responding to the Ping command, NP resolution processing can be performed). Also, if multiple groups are registered, and if the state in which no response to the Ping command is returned from any one group is maintained, NP resolution processing cannot be performed (if all groups respond to the Ping command, NP resolution processing can be done).
- Remove Group List
  - Remove the selected group.
- Add IP Address List
  - Add IP address to the selected group.
  - The maximum number of registered IP address is 16.
  - Maximum 256 IP addresses are able to be registered to a single Ping NP, and 16 kinds of IP addresses can be registered. (The same IP addresses can be used.)
- Remove IP Address List
  - Remove the selected IP address from the list.
- Edit
  - Edit the selected IP address.
- Interval
  - Set the Ping interval.
- Timeout
  - Set the Ping timeout.
- Retry Count
  - Set the retry count.
- Initialize

– Set the interval, timeout and retry count to the default values. Note that, when an interval and retry count are specified, the following conditional expression must be satisfied.
If not satisfied, NP resolution processing cannot be performed normally.

Conditional expression) Heartbeat timeout
> (Ping NP Interval *Ping NP Retry Count) + Ping NP Timeout

HTTP NP Properties



- Use Witness HB Resource Settings
  Use the same target host and service port as those of Witness HB which has already been configured.
- Target Host
  Sets the host address of the Web server to be connected.
- Service Port
  Sets the port number of the Web server to be connected.
- Use SSL
  Configures whether or not to use SSL for communicating the Web server. When the checkbox is selected, SSL is used, and when the checkbox is not selected, it is not used.

  Use OpenSSL 1.0/1.1 for SSL. By default, the following libraries are used:

  – libssl.so.10 (if you installed the rpm package of EXPRESSCLUSTER)
  – libssl.so.1.0.0 (if you installed the deb package of EXPRESSCLUSTER)

  To use other libraries, go to the **Encryption** tab and set **SSL Library** and **Crypto Library**.

- Interval
  Sets the interval for sending HTTP requests.
- Timeout
  Sets the timeout time from receiving an HTTP response to receiving the subsequent HTTP response.
- HTTP timeout
  Sets the timeout time from sending an HTTP request to receiving an HTTP response.
- Initialize
  Resets the settings of HTTP NP Properties to default values.

Type

Set the type of network partition resolution I/F. **Ping** or **HTTP** is selectable.

Target

Enter the information depending on the type you chose.

- **Ping**
  Enter the IP address of the device where you send a ping.
- **HTTP**
  Enter the DNS name or IP address of the Web server where you send an HTTP request.

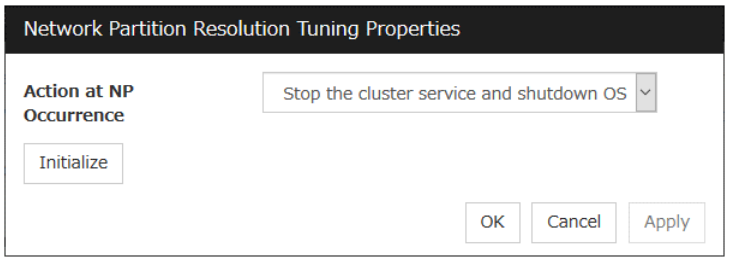
Server name

Select either **Use** or **Do Not Use**.

Tuning

Network Partition Resolution Tuning Properties window is displayed.

Network Partition Resolution Tuning Properties



- Action at NP Occurrence
  - Stop the cluster service
    Stop the cluster service of the server in network partition.
  - Stop the cluster service and shutdown OS
    Stops the cluster service of the server in network partition, and then shuts down the OS.
  - Stop the cluster service and reboot OS
    Stops the cluster service of the server in network partition, and then reboots the OS.
  - Sysrq Panic
    Performs a sysrq panic on the server in network partition.
  - Keepalive Reset
    Use this on the server in network partition to perform an OS reset by using the clpkhb and clpka drivers.
  - Keepalive Panic

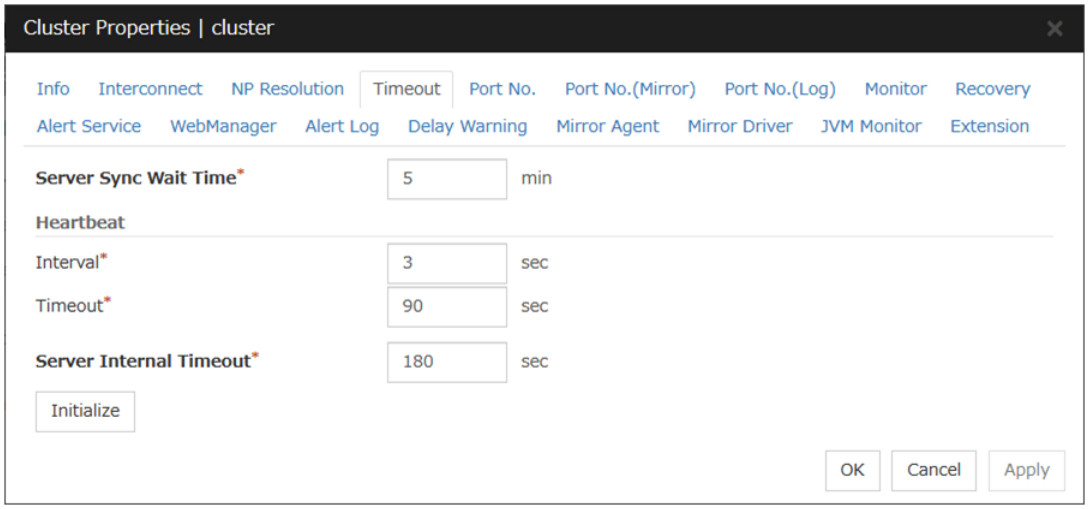
Use this on the server in network partition to perform an OS panic by using the clpkhb and clpka drivers.

- BMC Reset
  Use this on the server in network partition to perform a hardware reset of the server by using the ipmi command.
- BMC Power- Off
  Use this on the server in network partition to power off the server by using the ipmi command. The OS may be shut down depending on how the ACPI of OS is configured.
- BMC Power Cycle
  Use this on the server in network partition to perform the Power Cycle (powering on/off) by using the ipmi command. The OS may be shut down depending on how the ACPI of OS is configured.
- BMC NMI
  Use this on the server in network partition to generate NMI in the server by using the ipmi command. The behavior after the generation of NMI depends on the OS setting.
- I/O Fencing(High-End Server Option)
  It can't be used.

- Initialize
  - Set the actions at NP occurrence to the default settings.

2.2.4 Timeout tab

Specify values such as time-out on this tab.



Server Sync Wait Time (0 to 99)

For the time specified here, the server will wait at startup until other servers are started.

Heartbeat

Heartbeat interval and heartbeat time-out.

- **Interval** (1 to 99)
  Interval of heartbeats
- **Timeout** (2 to 9999)
  A failed server is determined if there is no response for the time specified here.

- This time-out should be longer than the interval.
- To perform the shutdown monitoring (see *Monitor tab*), this time-out should be longer than the time it takes to shut down applications and the operating system.
- When a hybrid disk resource is used, the time-out value must be longer than the value specified at the cluster partition I/O time-out in the **mirror agent** tab.

Server Internal Timeout (1 to 9999)

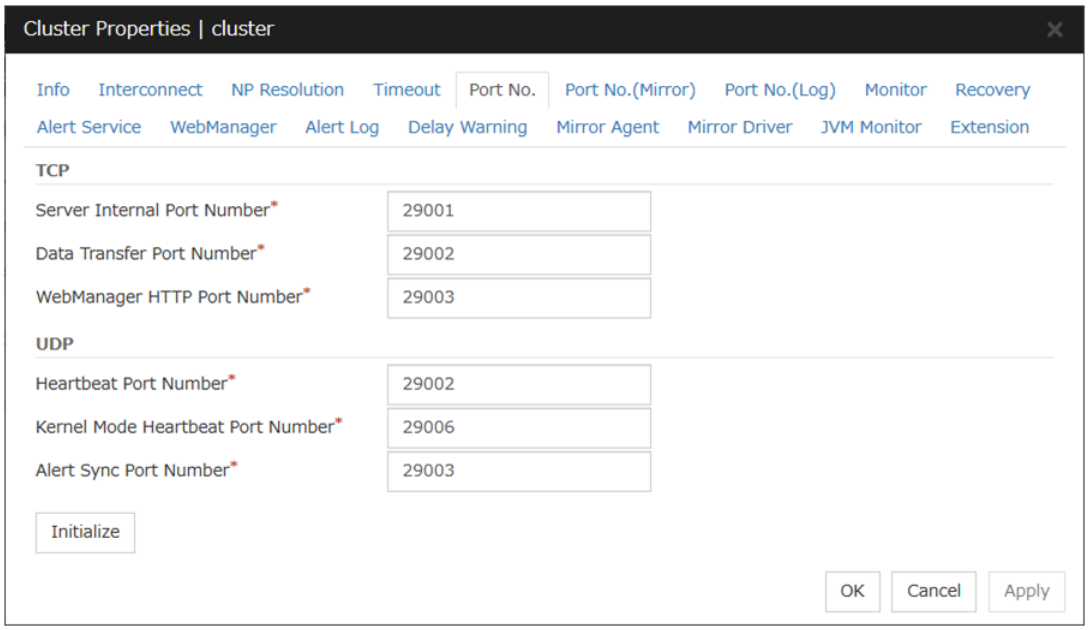
The timeout to be used in the EXPRESSCLUSTER Server internal communications that are performed while an EXPRESSCLUSTER command is executed, or an operation is performed or a screen is displayed by Cluster WebUI.

Initialize

Used for initializing the value to the default value. Click **Initialize** to initialize all the items to their default values.

2.2.5 Port No. tab

Specify TCP port numbers and UDP port numbers.



TCP

No TCP port numbers can be overlapped. When the Replicator is used, TCP port numbers on the **Port No.(Mirror)** tab and any mirror data port number of any mirror disk resources/hybrid disk resources cannot be overlapped.

- **Server Internal Port Number** (1 to 65535[1])
  This port number is used for internal communication.
- **Information Base Port Number** (1 to 65535[1])
  This port number is used for cluster information management.
- **Data Transfer Port Number** (1 to 65535[1])

[1] It is strongly recommended not to use well-known ports, especially reserved ports from 1 to 1023.

This port number is used for transactions such as applying and backing up the cluster configuration data, sending and receiving the license data and running commands.

- **WebManager HTTP Port Number** (1 to 65535[1])
  This port number is used for a browser to communicate with the EXPRESSCLUSTER Server.
- **API HTTP Port Number** (1 to 65535[1])
  This port number is used when a Restful API client communicates with the EXPRESSCLUSTER Server.
- **API Server Internal Port Number** (1 to 65535[1])
  This port number is used for internal communication of Restful API.

UDP

No UDP port numbers can be overlapped. When the communication method for internal logs is UDP on the **Port No.(Log)** tab, UDP port numbers cannot be overlapped with the port numbers.

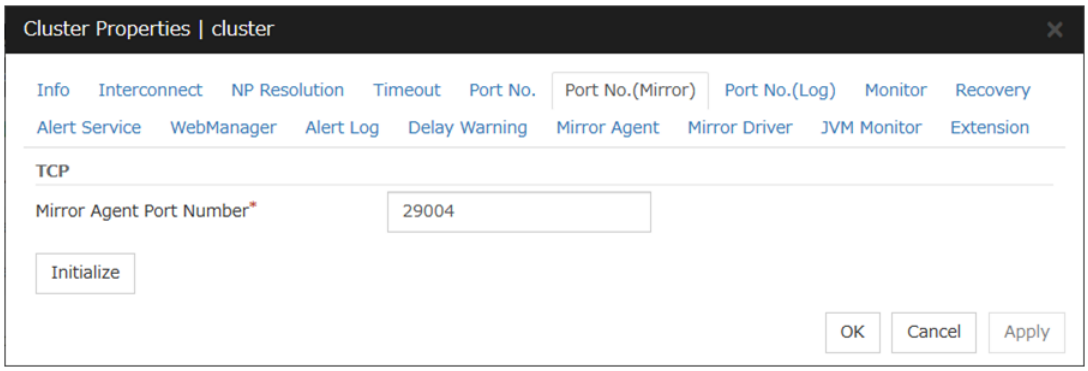
- **Heartbeat Port Number** (1 to 65535[1])
  This port number is used for heartbeat.
- **Kernel Mode Heartbeat Port Number** (1 to 65535[1])
  This port number is used for kernel mode heartbeat.
- **Alert Sync Port Number** (1 to 65535[1])
  This port number is used for synchronizing alert messages among servers.

Initialize

This is used for initializing the value to the default value. Click **Initialize** to initialize all items to their default values.

2.2.6 Port No. (Mirror) tab ~ For the Replicator/Replicator DR ~

Specify TCP port numbers.



TCP

No TCP port numbers can be overlapped. TCP port numbers on the **Port No.** tab and any mirror data port number of any mirror disk resources/hybrid disk resources cannot be overlapped.

Note: Port numbers are not used when mirror disk resource/hybrid disk resource is not used.

- Mirror Agent Port Number (1 to 65535[2])

[2] It is strongly recommended not to use well-known ports, especially reserved ports from 1 to 1023.

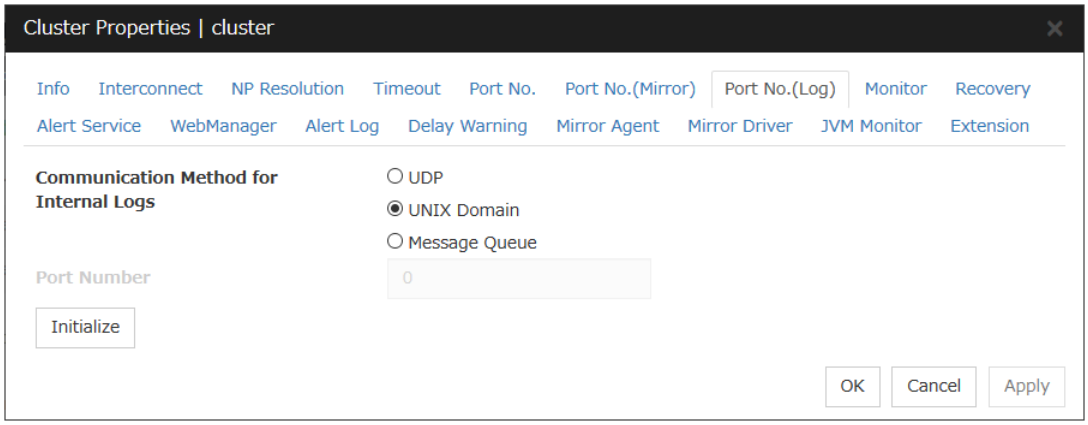
Mirror agent is a user mode module for controlling mirror disk resource/hybrid disk resource. The Mirror Agent uses this port number to communicate with servers.

Initialize

Used for initializing the value to the default value. Click **Initialize** to initialize all the items to their default values.

2.2.7 Port No. (Log) tab

Specify the communication method for internal logs.



Communication Method for Internal Logs

- UDP
  Use UDP for the communication method for internal logs.
- UNIX Domain
  Use UNIX Domain for the communication method for internal logs.
- Message Queue
  Use Message Queue for the communication method for internal logs.

Port No. (1 to 65535)

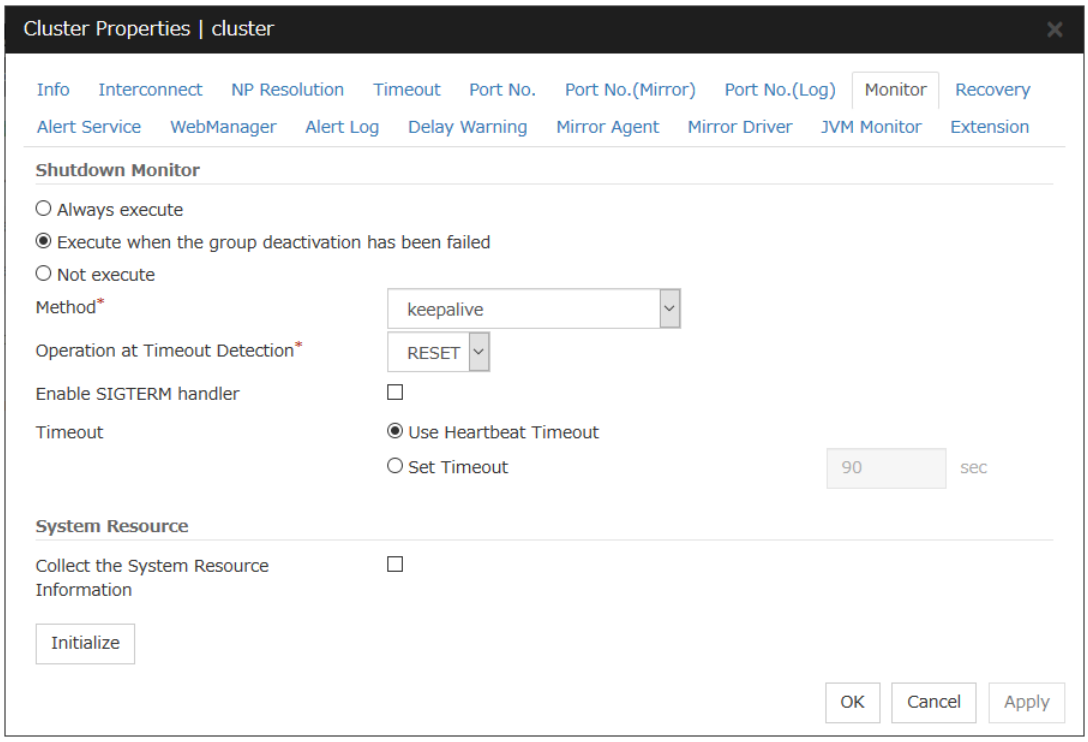
This is the port number used when UDP is selected for the communication method for internal logs.

Initialize

Used for initializing the value to the default value. Click **Initialize** to initialize all the items to their default values.

2.2.8 Monitor tab

Configure the settings for monitoring. For details about the shutdown monitor and reboot limit, see "4. *Monitor resource details*" in this guide.



Shutdown Monitor

Monitors whether or not the operating system is stalling when an EXPRESSCLUSTER command to shut down the cluster or servers is run.

The cluster service forcibly resets the operating system or performs a panic of the operating system if it determines the OS stall. Server panic can be set when the monitoring method is keepalive.

- **Always execute:**
  If selected, the shutdown monitor is performed. For the heartbeat time-out, specify a longer time than the time required to shut down every application and the operating system (see "*Timeout tab*").
- **Execute when the group deactivation has been failed:**
  The shutdown monitor is applied only when a group cannot be deactivated. For the heartbeat time-out, specify a longer time than the time required to shut down every application and the operating system (see "*Timeout tab*"). If you use shared disks or mirror disks, it is recommended to select **Execute when the group deactivation has been failed**.
- **Not execute:**
  If selected, the shutdown monitor is not performed.
  - **Method**

    Select the shutdown monitor method from:

    * softdog
    * ipmi
    * ipmi (High-End Server Option)
    * keepalive

    For details about the shutdown monitoring method, see "*Shutdown monitoring* " in "*Shutdown monitoring method*" in "*7. Information on other settings*" in this guide.

– **Operation at Timeout Detection**

Selects the operation performed when the operating system is determined to be stalled. This can be set only when the monitoring method is keepalive.

* RESET
  Resets the server.
* PANIC
  Performs a panic of the server.

– **Enable SIGTERM handler**

Select this to enable SIGTERM handler when performing the shutdown monitor.
For details about the SIGTERM settings, see "*Shutdown monitoring*" in " *Setting of SIGTERM* " in "7. *Information on other settings*" in this guide.

Note: If you select ipmi in **Method** and set **Enable SIGTERM handler** to **Off**, this may be reset even if the operating system is successfully shut down.

– **Use Heartbeat Timeout**

Select this for heartbeat time-out to work in conjunction with shutdown monitoring time-out.

– **Timeout (2 to 9999)**

Specify a time-out when the heartbeat time-out value is not used as shutdown monitoring time-out.
A value equal to or smaller than the heartbeat timeout value must be specified to prevent both systems from activating when a failover occurs upon detection of a server down.

System Resource

Select whether to collect system resource information.

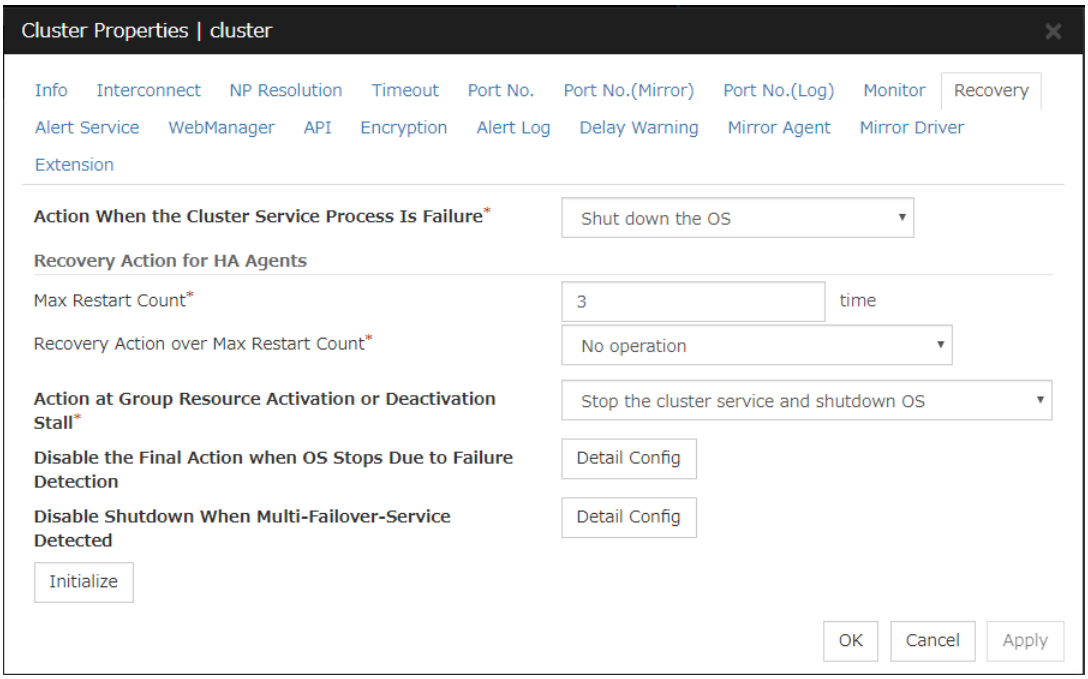
System resource information is collected regularly so as to improve system operability. System resource information is useful for investigating the operation status of EXPRESSCLUSTER, and makes it easy to determine the cause of a failure attributable to a shortage of system resources.

- When the check box is selected:
  System resource information related to the CPU, memory, processes, and others is collected regularly while the cluster is running.
  The collected system resource information are collected as a log by the clplogcc command or Cluster WebUI.
  Specify type 1 to collect the log by the clplogcc command; specify Pattern 1 to collect the log by the Cluster WebUI. For details about log collection, see "*Collecting logs (clplogcc command)*" in "8. *EXPRESSCLUSTER command reference*" in this guide, and the online manual.
  A disk area of 450 MB or more is required to store the resource information, depending on the system operating conditions such as the number of processes that are running.
  To use this feature, a zip (unzip) package tool is required on each server.
- When the check box is cleared:

No system resource information is collected.

2.2.9 Recovery tab

Configure the settings for cluster recovery.



Action When the Cluster Service Process Is Failure

Specify the action when a cluster service process error occurs.

- Shut down the OS
  Shut down the OS.
- Reboot the OS
  Reboot the OS.
- Sysrq Panic
  Performs a sysrq panic on the server in network partition..
- Keepalive Reset
  Use this on the server in network partition to perform an OS reset by using the clpkhb and clpka drivers.
- Keepalive Panic
  Use this on the server in network partition to perform an OS panic by using the clpkhb and clpka drivers.
- BMC Reset
  Use this on the server in network partition to perform a hardware reset of the server by using the ipmi command.
- BMC Power Off
  Use this on the server in network partition to power off the server by using the ipmi command. The OS may be shut down depending on how the ACPI of OS is configured.

- BMC Power Cycle
  Use this on the server in network partition to perform the Power Cycle (powering on/off) by using the ipmi command. The OS may be shut down depending on how the ACPI of OS is co
- BMC NMI
  Use this on the server in network partition to generate NMI in the server by using the ipmi command. The behavior after the generation of NMI depends on the OS setting.
- I/O Fencing(High-End Server Option)
  It can't be used.

Recovery Action for HA Agents

- Max Restart Count (0 to 99)
  Specify the max restart count when an HA Agent error has occurred.
- Recovery Action over Max Restart Count
  Specify the action when an HA Agent error has occurred.
  - No operation
  - Stop the cluster service
    Stops the cluster service of the server that detected an error.
  - Stop the cluster service and shutdown OS
    Stops the cluster service of the server that detected an error, and then shuts down the OS.
  - Stop the cluster service and reboot OS
    Stops the cluster service of the server that detected an error, and then reboots the OS.

Note: The HA process is used with the system monitor resources, process resource monitor resource, JVM monitor resources, and the system resource information collection function.

Action at Group Resource Activation or Deactivation Stall

Specify the action to apply in the event of an activation/deactivation stall of a group resource.

- Stop cluster service and shutdown OS
  Stops the cluster service of the server that stalled, and then shuts down the OS.
- Stop cluster service and reboot OS
  Stops the cluster service of the server that stalled, and then restarts the OS.
- Sysrq Panic
  Performs a sysrq panic on the server that stalled.
- Keepalive Reset
  Use this on the server that stalled to perform an OS reset by using the clpkhb and clpka drivers.
- Keepalive Panic
  Use this on the server that stalled to perform an OS panic by using the clpkhb and clpka drivers.
- BMC Reset
  Use this on the server that stalled to perform a hardware reset of the server by using the ipmi command.
- BMC Power- Off
  Use this on the server that stalled to power off the server by using the ipmi command. The OS may be shut down depending on how the ACPI of OS is configured.

- BMC Power Cycle
  Use this on the server that stalled to perform the Power Cycle (powering on/off) by using the ipmi command. The OS may be shut down depending on how the ACPI of OS is configured.
- BMC NMI
  Use this on the server that stalled to generate NMI in the server by using the ipmi command. The behavior after the generation of NMI depends on the OS setting.
- I/O Fencing(High-End Server Option)
  It can't be used.
- No Operation (Operates as an activity or deactivity failure)
  Use this to perform recovery upon the detection of an activation/deactivation failure of a group resource. For details on the recovery operation, see "*Recovery Operation tab*" in "*Resource Properties*" in "*3. Group resource details*" in this guide.

Note: If a stall occurs with "Nothing (handle a stall as an activation/deactivation failure)" specified, the effect on the group resources is undefined, so we do not recommend changing the setting to "Nothing (handle a stall as an activation/deactivation failure).".

If you do specify "Nothing (handle a stall as an activation/deactivation failure)", set the recovery operation upon the detection of an activation/deactivation failure of a group resource as described below.

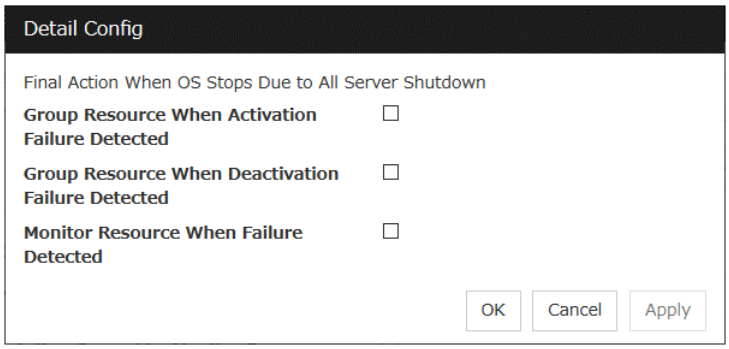
Activation/Deactivation Retry Threshold: 0

Failover Threshold: 0

Final Action: Action that accompanies the OS stop

Disable the Final Action when OS Stops Due to Failure Detection

Click **Detail Config** to set suppression of the final action which accompanies the OS stop caused by error detection.



- **Group Resource When Activation Failure Detected**
  If the final action caused by an activation error detection in a group resource accompanies the OS stop, the final action is suppressed if all other servers are stopped.
- **Group Resource When Deactivation Failure Detected**
  If the final action caused by a deactivation error detection in a group resource accompanies the OS stop, the final action is suppressed if all other servers are stopped.
- **Monitor Resource When Failure Detected**

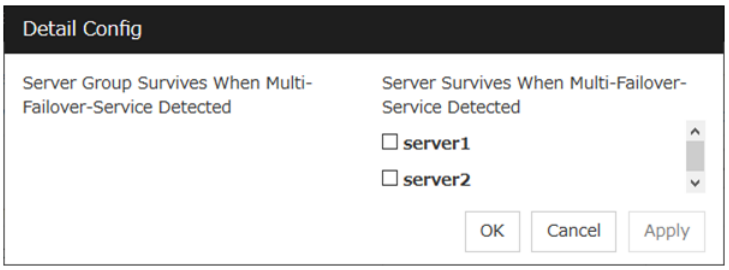
If the final action caused by an error detection in a monitor resource accompanies the OS stop, the final action is suppressed if all other servers are stopped.

Note:

- If errors were detected on multiple servers almost at the same time, and the final action was taken for those servers, the final action which accompanies the OS stop may be taken for all the servers even if the final action caused by an error detection in a monitor resource is set to be suppressed.
- The message receive monitor resource does not become the target for which the final action caused by error detection is suppressed.
- The following situations lead to an OS stop during the final action when an activation/deactivation error is detected in a group resource and during the final action when a monitor resource error is detected.
  - Cluster service stop and OS shutdown
  - Cluster service stop and OS restart
  - sysrq panic
  - keepalive reset
  - keepalive panic
  - BMC reset
  - BMC power off
  - BMC power cycle
  - BMC NMI

Disable Shutdown When Multi-Failover-Service Detected

Click **Detail Config** to suppress the shutdown of all servers upon detection of both-system activation.



Server Group Survives When Multi-Failover-Service Detected

Select one server group. The shutdown of the server, which belongs to the server group selected when the both-system activation of the failover group was detected, is suppressed. When the both-system activation is detected among servers in the selected server group, both of the servers will be shut down. If you want to suppress the shutdown in this case, make the settings to disable shutdown when the following double activation is detected.

Server Survives When Multi-Failover-Service Detected

Select one server. The shutdown of the server, selected when the both-system activation of the failover group was detected, is suppressed.

If a server group to which shutdown is not executed when Multi-Failover is detected is set, it is possible to select only a server belonging to the set server group. If no server group is set, all the servers can be selected.

Note: When the both-system activation is detected, the group statuses will be inconsistent among the servers, and failover and failback operations will be able to fail.

If a group status mismatch occurs, the following alert log is output:

Type: Warning
Module name: rc
Event ID: 503
Message: A mismatch in the group %1 status occurs between the servers. A mismatch in the group %1 status occurs between the servers.

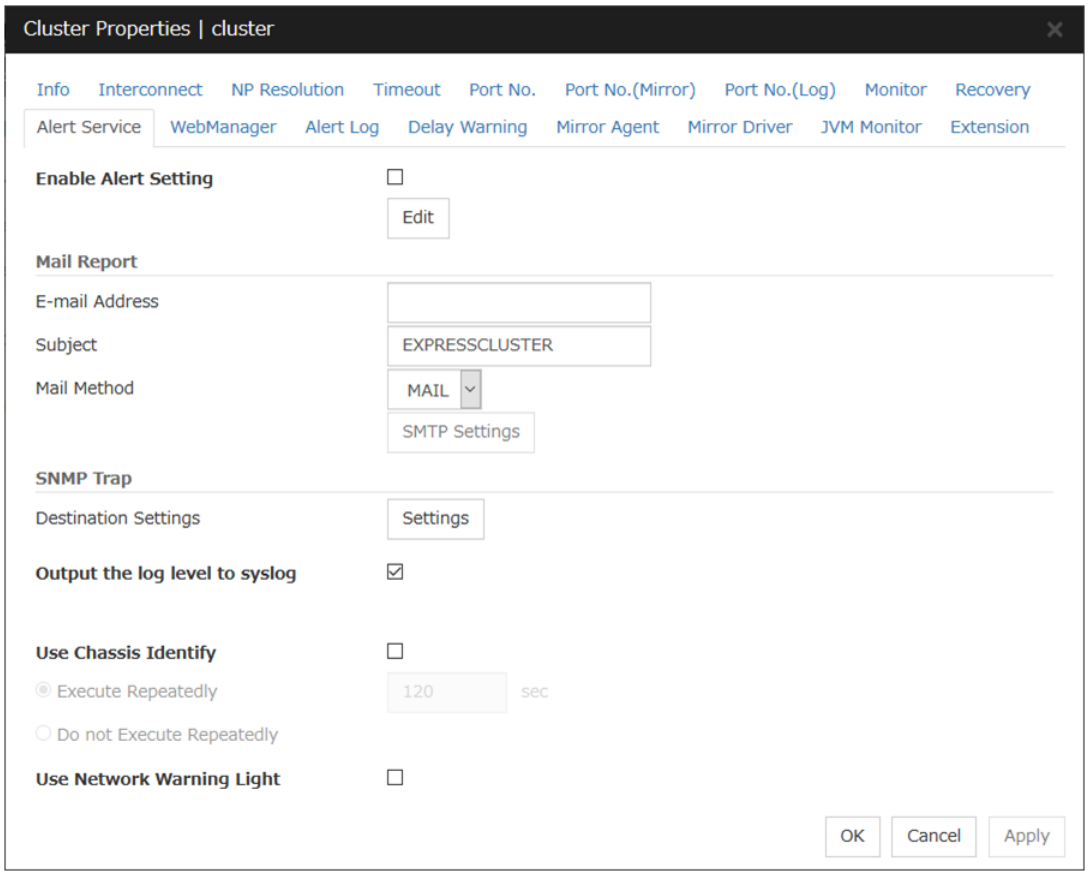
2.2.10 Alert Service tab

Configure the settings for the mail report function, the network warning light, alert report destination, and SNMP trap transmission.

To use the mail report function, register the Alert Service license.

To use the network warning light, register the Alert Service license.

Note: To use the mail report function and the network warning light, purchase the EXPRESSCLUSTER X Alert Service 4.2 for Linux.



Enable Alert Setting

Configure whether to modify the alert destination from the default value. To modify the alert report destination, click **Edit** to configure the address.

By canceling **Enable Alert Setting,** the modified destination turns to the default value temporarily.

For details about the default alert destination, see "*Messages reported by syslog, alert, mail, and SNMP trap*" in "10. *Error messages*" in this guide.

E-mail Address (Within 255 bytes)

Enter the e-mail address to which the report is sent. If more than two e-mail addresses are set, delimit the address by semicolon.

Subject (Within 127 bytes)

Enter the subject title for the e-mail message.

Mail Method

Configure the methods to send mail.

- MAIL
  This method uses the mail command. Check that a mail is sent to the mail address by using the mail command in advance.
- SMTP
  This method allows for sending mail by directly communicating with the P server.

Destination Settings

Configure the SNMP trap transmission function. Click **Setting** to configure the SNMP trap transmission destination.

Output Log Level to syslog

Add Log Level to the syslog messages which EXPRESSCLUSTER put out while it is in operation.

Use Chassis Identify

Configure whether or not to enable **Use Chassis Identify.**

Execute Repeatedly

Repeat Chassis Identify Command.

- Interval (1 to 999)

  Set the interval of Chassis Identify Command.

Do not Excute Repeatedly

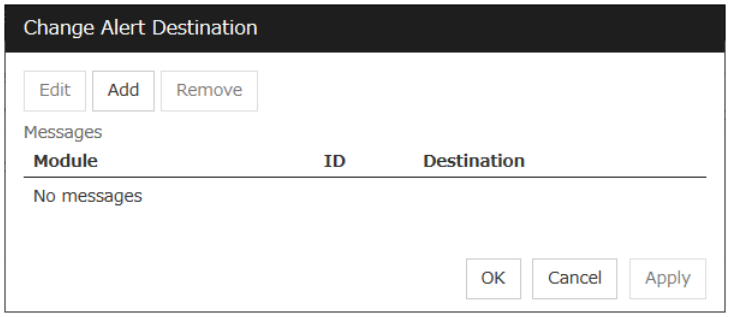
Not repeat Chassis Identify Command.

Use Network Warning Light

Specify whether to use a network warning light (specified by NEC) controlled by network. Enter an IP address in server properties.

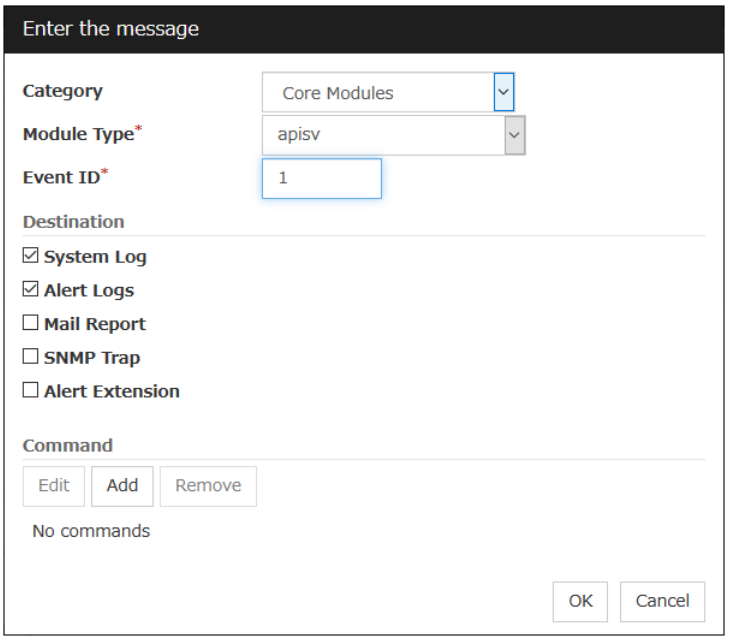
Change Alert Destination

Click **Edit** to display the **Change Alert Destination** dialog box.



Add

Click this to select the event ID and the module type for which you want to customize the report destinations. Click **Add** to open the **Enter the Message** dialog box.



Category

Select a major category of the module type.

Module Type (Within 31 bytes)

Select the name of module type that you want to change the destination address.

Event ID

Enter the event type of the module type for which you want to change the destination address. For details about the event ID, see "*Messages reported by syslog, alert, mail, and SNMP trap*" in "10. *Error messages*" in this guide.

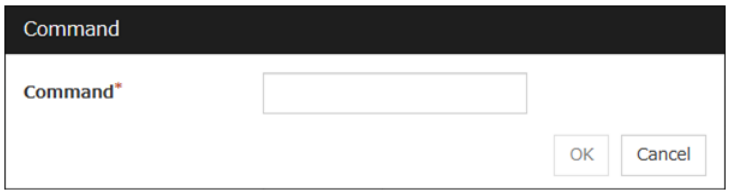
Destination

Select the destination.

- System Log
  This sends message to syslog of the OS.
- Alert Logs
  This sends message to the alert log.
- Mail Report
  This sends message by using the mail report function.
- Alert Extension
  This sends message by the Alert Extension function. Modify the extension settings using **Add** and **Edit**.

Add

Add a command of the alert extension function. Click **Add** to open the **Enter Command** dialog box. Up to 4 commands can be registered with one event ID.



Command (Within 511 bytes)

Enter a command such as SNMP trap to execute reporting with the absolute path. The execution results of the specified command cannot be shown.

- Keyword
  If you specify **%%MSG%%**, the body message of the target event ID is inserted.
  You cannot specify multiple %%MSG%% for one command.
  Configure within 511 bytes including the description of %%MSG%%. Since blank characters can be included in %%MSG%%, if you specify this for an argument of commands, specify this as "%%MSG%%".

  Configuration example

```
/usr/local/bin/snmptrap -v1 -c HOME 10.0.0.2 0 10.0.0.1 1 0 '' 1 s "%%MSG
↪%%"
```

Remove

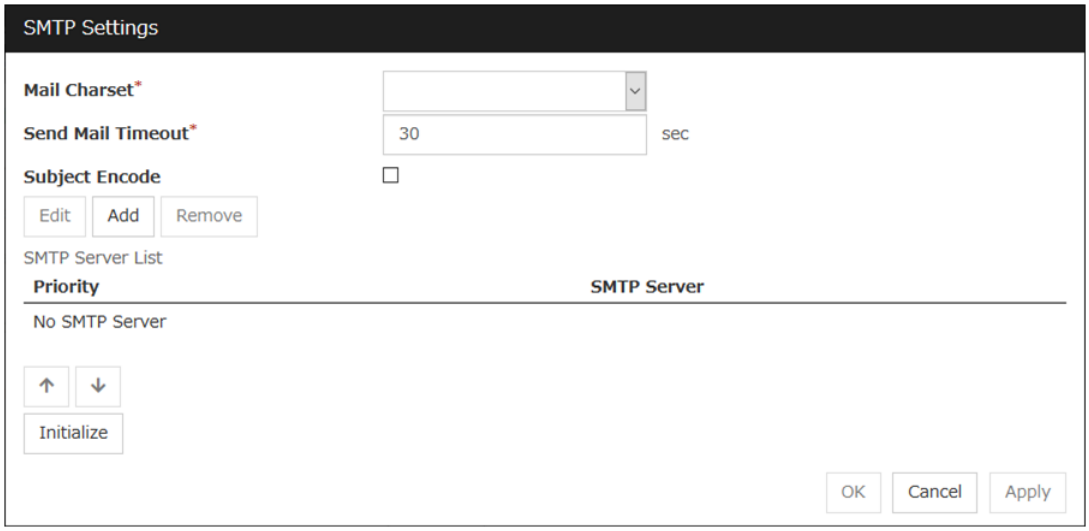
Click this to remove a command of alert extension function. Select the command and then click **Remove**.

Edit

Click this to modify a command of alert extension function. Select the command and then click **Edit**.

SMTP Settings

Click **SMTP Settings** to display the **SMTP Settings** dialog box.



Mail Charset (Within 127 bytes)

Configure the character set of the e-mails sent for mail report.

Send Mail Timeout (1 to 999)

Configure the timeout value for communicating with the SMTP server.

Subject Encode

Select whether or not to encode the subject of e-mails.

SMTP Server List

Use this button to display a SMTP server that is configured. Four SMTP servers can be configured in this version.

Add

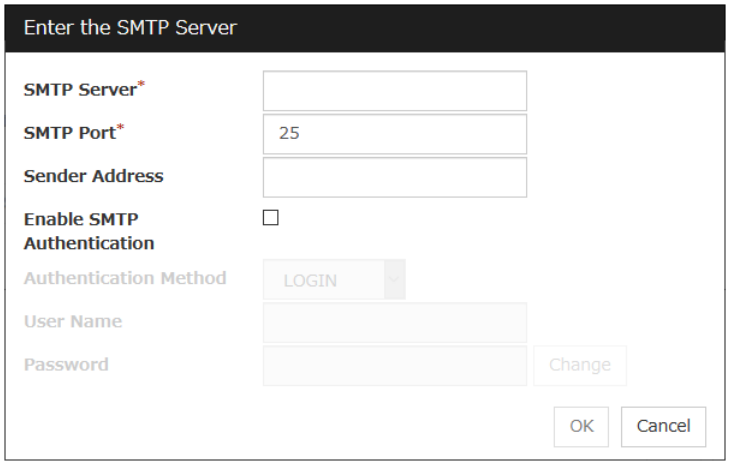
Use this button to add a SMTP server. Click **Add** to display the **Enter the SMTP Server** dialog box.

Remove

Use **Remove** to remove the SMTP server settings.

Edit

Use **Edit** to modify the SMTP server settings.



SMTP Server (Within 255 bytes)

Configure the IP address or host name of the SMTP server.

SMTP Port (1 to 65535)

Configure the port number of the SMTP server.

Sender Address (Within 255 bytes)

Configure the address from which an e-mail of mail report is sent.

Enable SMTP Authentication

Configure whether or not to enable SMTP authentication.

Method

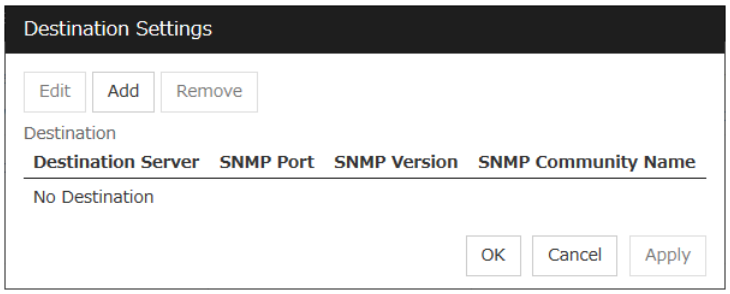
Select a method of SMTP authentication.

User Name (Within 255 bytes)

Configure the user name used for SMTP authentication.

Password (Within 255 bytes)

Configure the password used for SMTP authentication.



Destination

Displays the set SNMP trap transmission destinations. With this version, up to 32 SNMP trap transmission destinations can be set.

Add

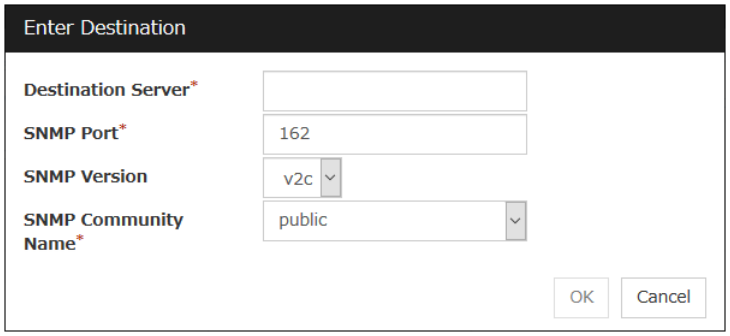
Adds an SNMP trap transmission destination. Click **Add** to display the Change SNMP Destination dialog box.

Remove

Use **Remove** to remove the SNMP trap transmission destination settings.

Edit

Use **Edit** to modify the SNMP trap transmission destination settings.



Destination Server (Within 255 bytes)

Configure the name of the SNMP trap transmission destination server.

SNMP Port No. (1 to 65535)

Configure the port number of the SNMP trap transmission destination.

SNMP Version

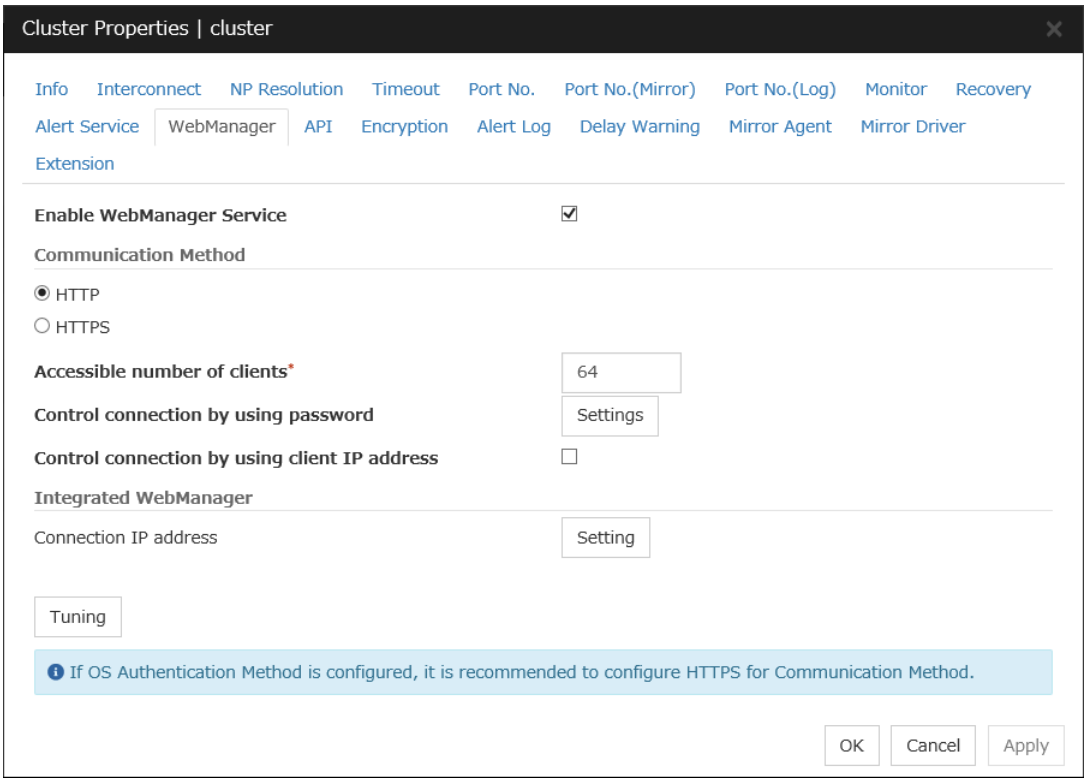
Configure the SNMP version of the SNMP trap transmission destination.

SNMP Community Name (Within 255 bytes)

Configure the SNMP community name of the SNMP trap transmission destination.

2.2.11 WebManager tab

Use this tab to configure the settings for the WebManager Server.



Enable WebManager Service

Enables the WebManager Service.

- When the check box is selected:
  The WebManager service is enabled.
- When the check box is not selected:
  The WebManager service is disabled.

Communication Method

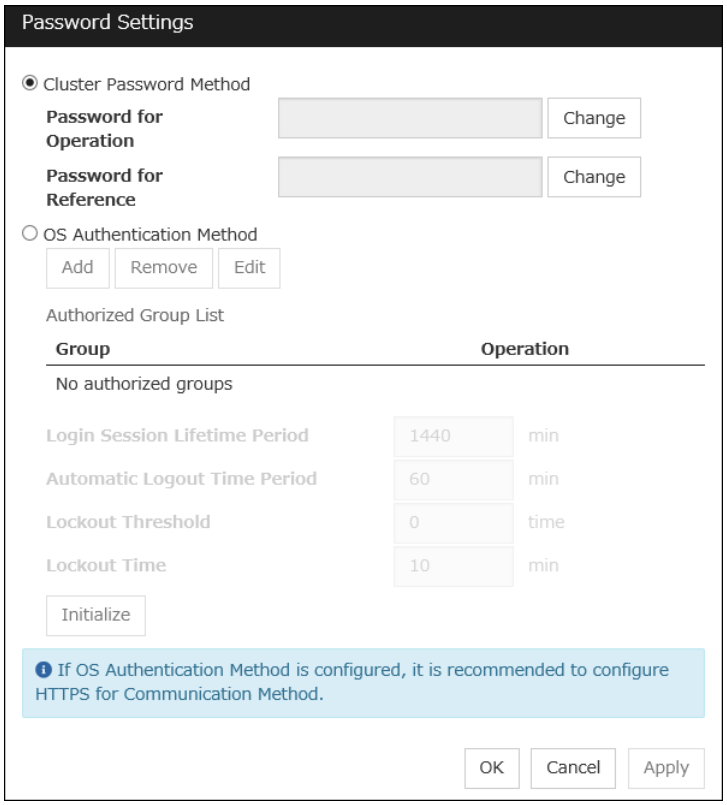
- HTTP
  No encryption is used for communicating with a client.
- HTTPS
  Encryption is used for communicating with a client.

Accessible number of clients (1 to 999)

Limits the number of concurrent requests from clients. If the concurrent requests exceed the limit, the overflowed requests are discarded.

Control connection by using password

Click **Settings** to show the **Password** dialog box.



Cluster Password Method / OS Authentication Method

Choose a login method for Cluster WebUI from below.

- Cluster Password Method
  Performs authentication with an operation/reference password you set.
- OS Authentication Method
  Performs authentication with user and password of OS .

Cluster Password Method

- **Password for Operation**
  Set a password that must be entered to enable connection to the Cluster WebUI in operation mode, config mode, or simulate mode.
  Click **Change** to display the **Enter Password** dialog box.
- **Password for Reference**
  Set a password that must be entered to enable connection to the Cluster WebUI in reference mode.
  Click **Change** to display the **Enter Password** dialog box.

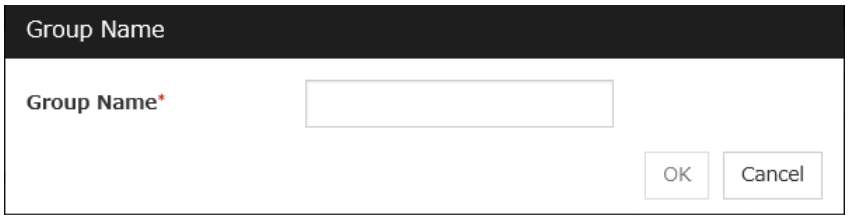
- **Old Password: (Within 255 bytes)**
  Enter the current password. If the password is not set, leave it blank.
- **New Password**: **(Within 255 bytes)**
  Enter a new password. When deleting the old password, leave it blank.
- **Password Confirmation**: **(Within 255 bytes)**
  Enter the password again which you entered in **New Password**.
  Passwords can consist of one-byte upper- and lower-case letters, digits, symbols, and spaces (0x20 to 0x7E in ASCII code).

OS Authentication Method

Users must be registered to the server in advance to login to Cluster WebUI. More specifically, a group must be registered to the server and the users must belong to it as the control permission of a cluster is assigned per group,

Add

Used to add a group to **Authorized Group List**. The **Group Name** dialog box appears when **Add** is clicked. To add a group, the **Operation** checkbox must be selected.



- Group name (Within 255 bytes)
  Enter a group name to which you want to give permission. The permission will be applied to the users belong to the group you entered. Groups must be registered to a server in advance.

Remove

Used to delete a group from **Authorized Group List**. Select a group you want to delete from **Authorized Group List**, and click **Remove**.

Edit

Used to edit a group. Select a group you want to edit from **Authorized Group List**, and click **Edit**. The **Group Name** dialog box with the selected group entered appears. The control permission does not change in this procedure.

Operation

Set control permission to a group registered in **Authorized Group List**.

- When the checkbox is selected:
  Users belong to the group can control the cluster and view the status.
- When the checkbox is not selected:
  Users belongs to the group can view the status only.

Login Session Lifetime Period (0 to 52560)

Time frame of login session. If this value is set to zero (0), the period becomes limitless.

Automatic Logout Time Period (0 to 99999)

Sets wait time for automatic logout if there is no communication between Cluster WebUI and the Web-Manager server. If this value is set to zero (0), no automatic logout occurs.

Lockout Threshold (0 to 999)

Locks out a client IP address which fails to login continuously. The client cannot login until **Lockout Time** passes once a client is locked out. If this value is set to zero (0), no client IP address is not be locked out.

Lockout Time (1 to 99999)

Sets lockout time for a client IP address. Once the time passes, the lockout is automatically released.

Initialize

Restores the default value. If **Initialize** is clicked, the values of **Login Session Lifetime Period**, **Automatic Logout Time Period**, **Lockout Threshold** and **Lockout Time** are restored to the default values.

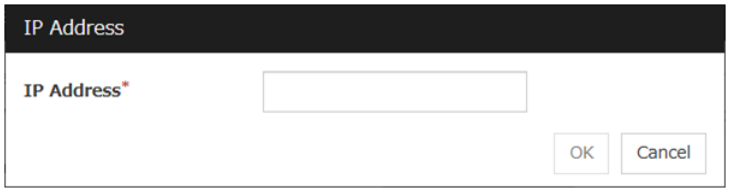
Control connection by using client IP address

If selected, accesses are controlled by client IP addresses.

- When the check box is selected:
  Add, **Remove** and **Edit** are displayed.
- When the check box is not selected:
  Add, **Remove** and **Edit** are not displayed.

Add

Use **Add** to add an IP address in **Connection Permit Client IP Address List**. Click **Add** to display the **IP Address** dialog box. Newly added IP addresses have the rights for the operation.



- **IP Address (Within 80 bytes)**

  Specify a client IP address that can be connected.

  - IP address: 10.0.0.21
  - Network address: 10.0.1.0/24

Remove

Use **Remove** to remove an IP address from **Connection Permit Client IP Address List**. Select the IP address to be removed from **Connection Permit Client IP Address List** and then click **Remove**.

Edit

Use **Edit** to edit an IP address. Select the IP address you want to edit from **Connection Permit Client IP Address List** and then click **Edit**. A dialog box where the specified IP address is preset is displayed. The rights for operating the edited IP addresses remain the same.

Note: The Connection Permit Client IP Address List specified here are also used to restrict connections for external operations using clprexec.

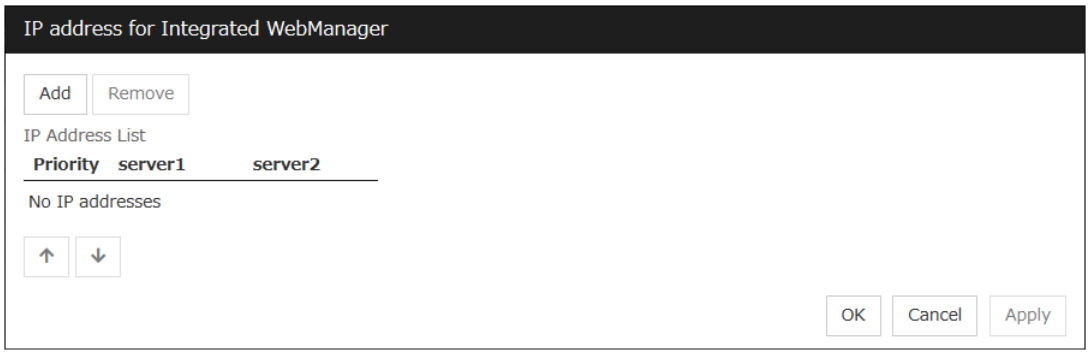
Operation

Sets the operation rights for IP addresses that are registered in **Connection Permit Client IP Address List**.

- When the check box is selected:
  A client can operate a cluster and display its status.
- When the check box is not selected:
  A client can only view the status of a cluster.

IP address for Integrated WebManager

Click **Settings** to open the IP address dialog box for the Integrated WebManager.



- **Add**

  Add IP addresses for the Integrated WebManager. Click the column cell of each server and select or enter IP address for the IP address of each server. For the communication path not connected to some server, set blank to the server cell of which the server is not connected.

- **Remove**

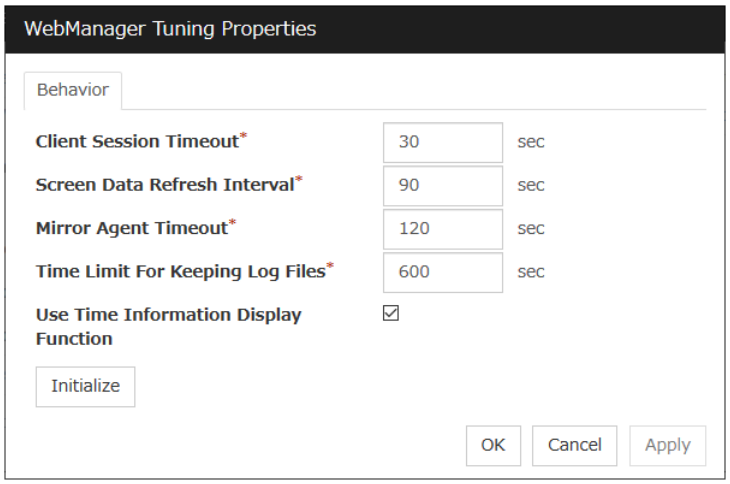
  Remove the communication path. Select the communication path to be removed and click **Remove**, then the selected path is removed.

- **Priority**

  When multiple IP addresses for Integrated WebManager are configured, the communication path with the smallest number in the **Priority** column is used preferentially for the internal communication among cluster servers. When changing the priority, click the arrows to change the order of the selected row.

Tuning

Use **Tuning** to tune the WebManager Server. Clicking **Tuning** displays the **WebManager Tuning Properties** dialog box.

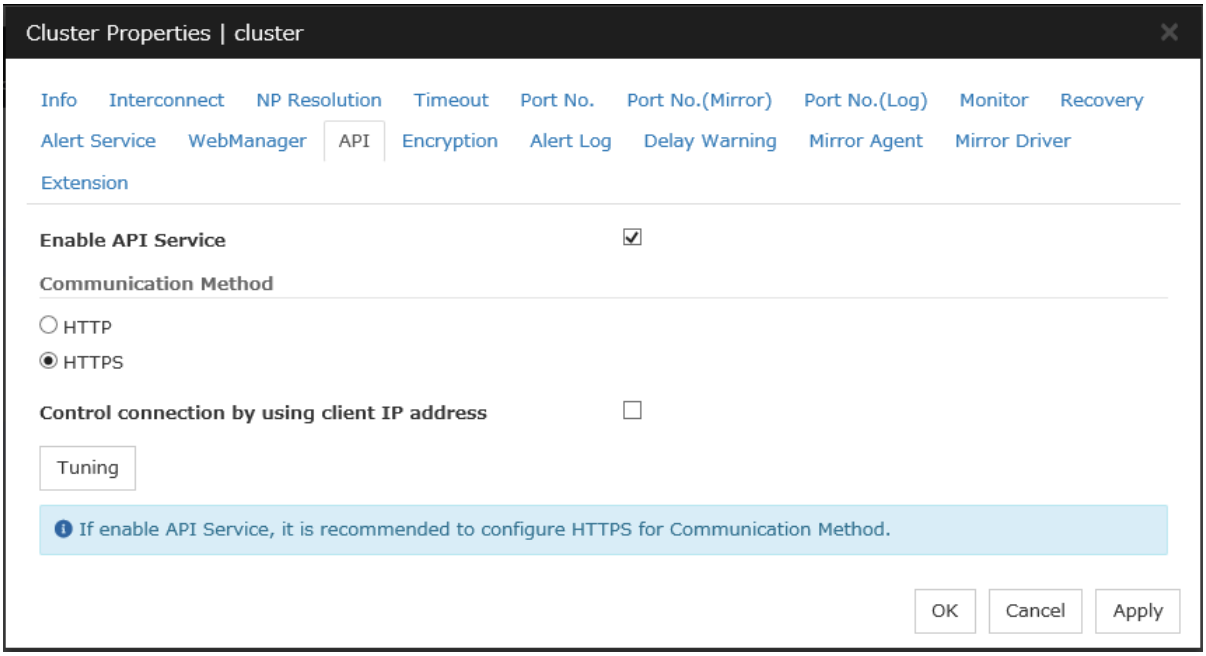


- **Client Session Timeout** (1 to 999)
  Specify the client session time-out. A time-out is determined if the time specified here elapses after the last communication between the WebManager Server and the Cluster WebUI.
- **Reload Interval** (0 to 999)
  Specify the screen data update interval. At this time interval, the Cluster WebUI screen is refreshed.
- **Mirror Agent Timeout** (1 to 999)
  Set the data waiting time output from the mirror agent.
- **Time Limit For Keeping Log Files** (60 to 43200)
  Specify the expiration period for deleting log collection information that is temporarily stored on a server. Log information on a server will be deleted if the expiration period is exceeded after the dialog box prompting saving log collection information is displayed.
- **Use Time Info Display Function**
  Specify whether the time information display function is enabled or disabled.
  - When the check box is selected:
    The time information display function is enabled.
  - When the check box is not selected:
    The time information display function is disabled.
- **Initialize**

  Click **Initialize** to reset all settings on this dialog to default. Click **Initialize** to set all the items to their default values.

2.2.12 API tab

This tab allows you to set API services.



Enable API Service

Enables API services.

- When the checkbox is selected:
  API services are enabled.
- When the checkbox is not selected:
  API services are disabled.

Communication Method

- HTTP:
  Does not use encryption for client communication.
- HTTPS:
  Use encryption for client communication.

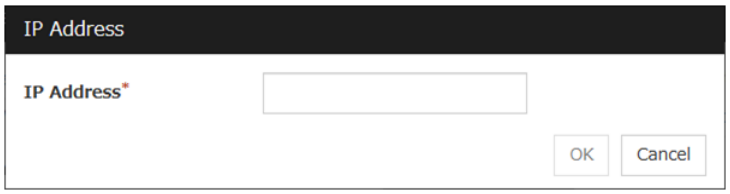
Control connection by using client IP address

Controls connections using client IP addresses.

- When the checkbox is selected:
  Add, **Remove** and **Edit** are displayed.
- When the checkbox is not selected:
  Add, **Remove** and **Edit** are not displayed.

Add

Use **Add** to add an IP address in **Connection Permit Client IP Address List**. Click **Add** to display the **IP Address** dialog box. Newly added IP addresses have the rights for the operation.



- **IP Address (Within 80 bytes)**

  Specify a client IP address allowed for the connection.

  - IP address: 10.0.0.21
  - Network address: 10.0.1.0/24

Remove

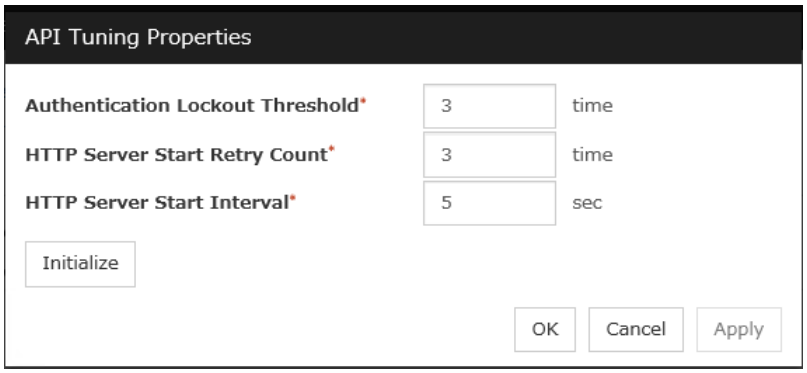
Use **Remove** to remove an IP address from **Connection Permit Client IP Address List**. Select the IP address to be removed from **Connection Permit Client IP Address List** and then click **Remove**.

Edit

Use **Edit** to edit an IP address. Select the IP address you want to edit from **Connection Permit Client IP Address List** and then click **Edit**. A dialog box where the specified IP address is preset is displayed.

Tuning.

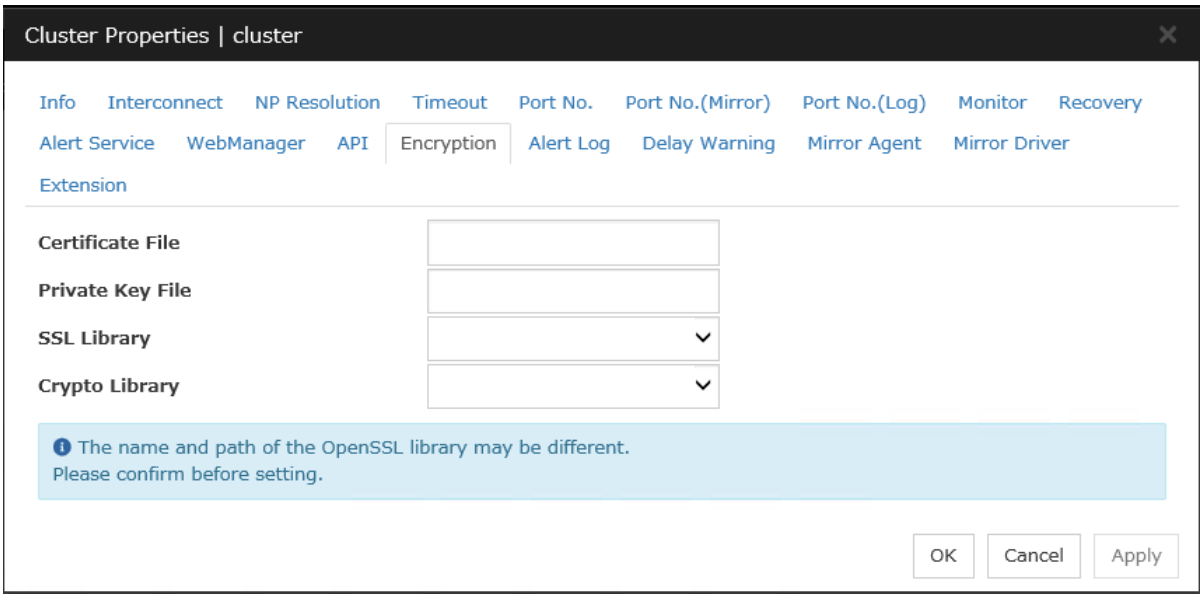
Adjusts API services. Click **Tuning** to display **API Tuning Properties** dialog box.



- Authentication Lockout Threshold
  Specify the number that counts continuous HTTP server authentication failures. If the counts reach this threshold, lockout is performed.
- HTTP Server Start Retry Count
  Specify the retry number that counts API services failed to start a HTTP server.
- HTTP Server Start Interval
  Specify the period of time between the time HTTP server start failure occurs and the time retry starts.
- Initialize
  Use **Initialize** to restore the default value. All the items restore the default values when **Initialize** is clicked.

2.2.13 Encryption tab

Sets files and libraries used for encryption of the cluster elated services.



Certificate File

Sets server certificate files used for connecting to a client. Server certificate files must be prepared at user side.

Private Key File

Sets private key files used for connecting to a client. Private key files must be prepared at user side.

SSL Library

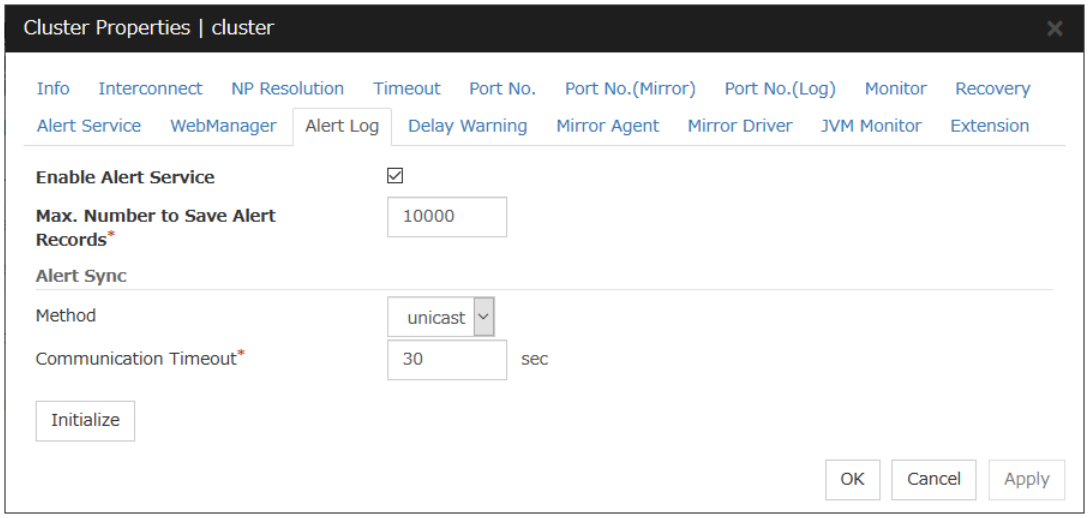
Sets SSL library files used for encryption and selects SSL library files included in OpenSSL. Some settings such as installation locations need to be changed depending on the environment.

Crypto Library

Sets Crypto library files used for encryption and selects Crypto library files included in OpenSSL. Some settings such as installation locations need to be changed depending on the environment.

2.2.14 Alert Log tab

Configure the settings for the alert log.



Enable Alert Service

Select this to start alert service for the server.

- When the check box is selected:
  Alert service is enabled.
- When the check box is not selected:
  Alert service is disabled.

Max. Number to Save Alert Records (1 to 99999)

Specify the maximum number of alert records that can be retained. Alert service for server can retain alert messages up to this number.

Alert Sync: Method

This communication mode is used for Alert Log synchronization. Only unicast is available in **Method** list box for this version.

Alert Sync: Communication Timeout (1 to 300)

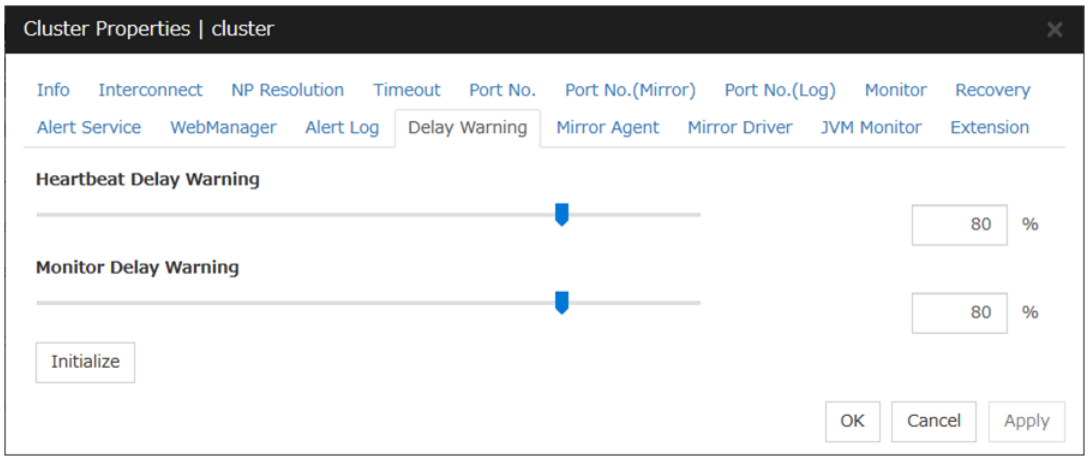
Specify a communication time-out. A communication time-out is determined if the time specified here elapses after the last communication between Alert service and servers.

Initialize

Click **Initialize** to reset all settings on this tab to default. Click **Initialize** to set all the items to their default values.

2.2.15 Delay Warning tab

Configure the settings for Delay Warning on this tab. For details, see "*Delay warning of monitor resources*" in "*Monitor resource*" in "*4. Monitor resource details*" in this guide.



Heartbeat Delay Warning (0 to 100)

Set a percentage of heartbeat time-out at which the heartbeat delay warning is issued. If the time for the percentage passes without any heartbeat response, the warning will be produced in an alert log. If you set 100, the warning will not be issued.

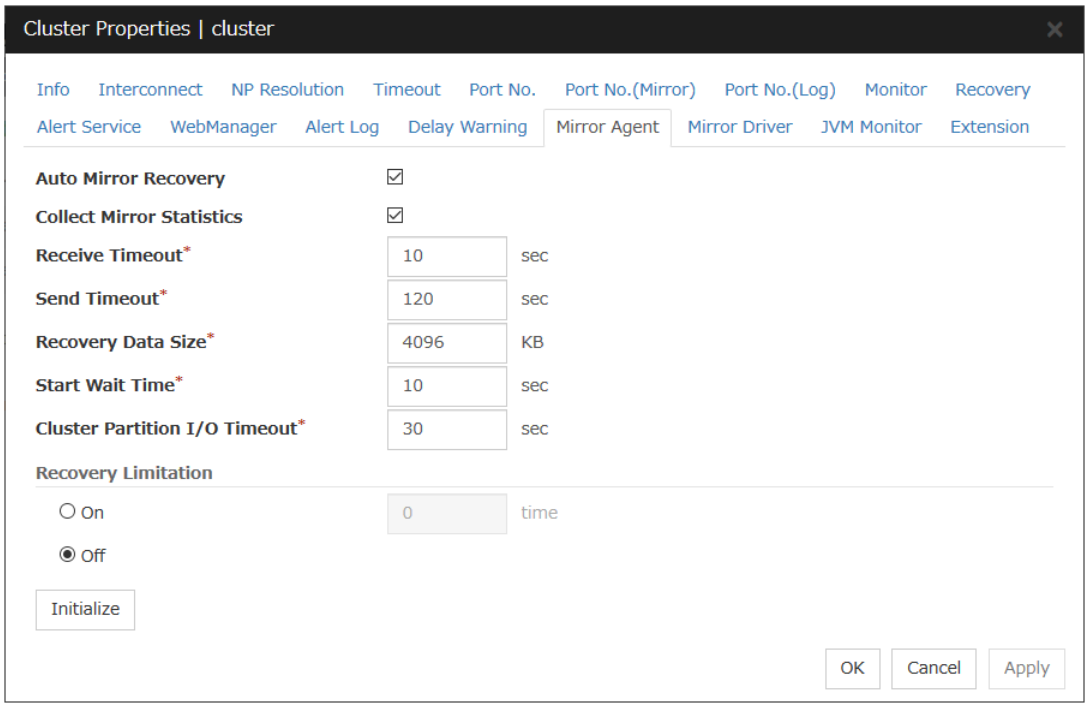
Monitor Delay Warning (0 to 100)

Set a percentage of monitor time-out at which the monitor delay warning is issued. If the time for the percentage passes without any monitor response, the warning will be produced in an alert log. If you set 100, the warning will not be issued.

Note: If you specify 0% for the delay warning, an alert log is shown in every heartbeat interval and monitor interval. Setting 0% allows you to see the time spent for monitoring. This will be helpful particularly in a test operation. Make sure not to set low values such as 0% in the production environment.

2.2.16 Mirror Agent tab ~ For the Replicator/Replicator DR~

Configure the settings for the Mirror Agent on this tab.



Auto Mirror Recovery

When the check box is selected, the mirror recovery is automatically performed if there is any difference between mirror disks on both servers. In some cases, you cannot perform the auto-mirror recovery even if this is selected. For details, see "*Automatically recovering from mirroring*" in "*9. Troubleshooting*" in this guide.

- When the check box is selected:
  The mirror recovery is automatically performed.
- When the check box is not selected:
  The mirror recovery is not automatically performed.

Collect Mirror Statistics

This function can be used to collect and reference information about the mirroring performance. For details, see " Mirror statistics information collection function" in" The system maintenance information" in the "Maintenance Guide".

- When the check box is selected
  Mirror Statistics Collection is performed.
- When the check box is not selected
  Mirror Statistics Collection is not performed.

Receive Timeout (1 to 600)

Set the time-out for the Mirror Agent waiting to receive data after establishing the connection.

Send Timeout (1 to 600)

Set the time-out for the Mirror Agent to send data to the Mirror Agent of the other server and wait it to be processed.

Recovery Data Size (64 to 32768)

Specify the recovery data size.

Start wait time (10 to 600)

For using a hybrid disk resource in a shared disk, set the waiting time to synchronize the starts of the servers connected to the shared disk. If another server does not start within the time configured here, the current right is obtained temporarily.

Cluster partition I/O timeout (5 to 300)

For using hybrid disk resource, set the timeout value for accessing the cluster partition.

- The time-out value must be smaller than the heartbeat time-out specified at the **Timeout** tab.

Recovery Limitation

Specify the retry count to perform mirror recovery again if the data has been updated during a mirror recovery.

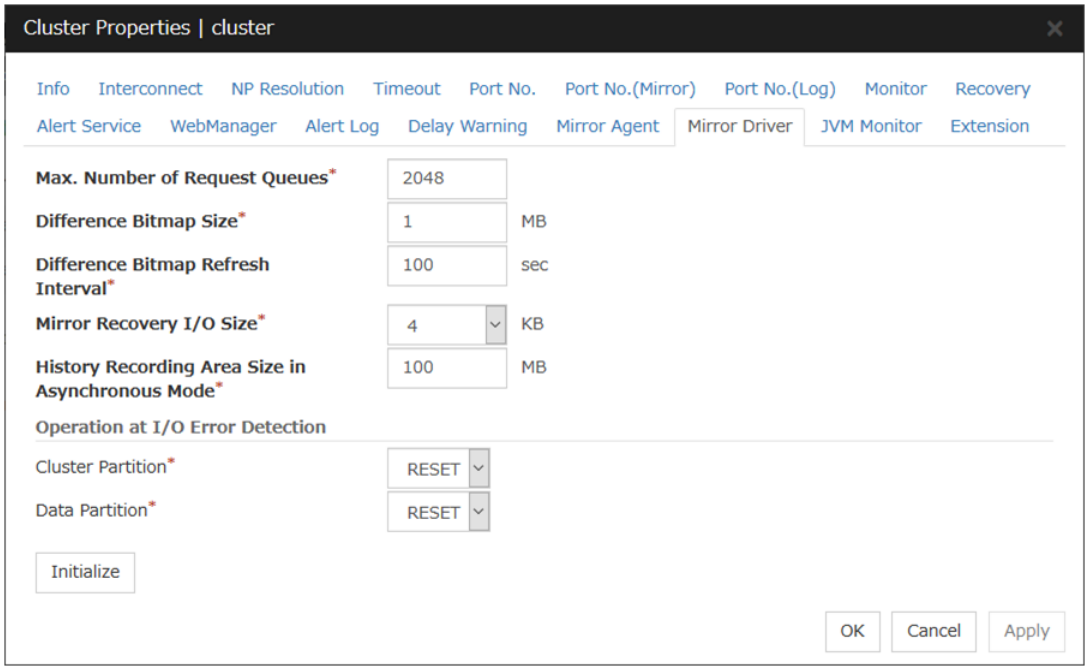
- On (1 to 100)
  The mirror recovery retry is performed the times specified on the box.
- Off
  When there is update data, mirror recovery is performed until there is no difference.

Initialize

This is used to reset the values to the default value. Clicking **Initialize** sets all the items to their default values.

2.2.17 Mirror driver tab ~ For Replicator/Replicator DR ~

Configure the settings for the mirror driver on this tab.



Max. Number of Request Queues (2048 to 65535)

Set the number of queues for mirror disk driver for queuing I/O requests from the upper system.

Difference Bitmap Size (1 to 5)

Users can specify the length of Record Area of the Difference Bitmap. Only when the mirror disk resource and/or hybrid disk resource do not exist in the cluster, the setting can be changed.

Difference Bitmap Refresh Interval (1 to 600)

Set the interval to check if the standby system writes the difference bitmap.

Mirror Recovery I/O size (4, 64)

Specify the size per I/O in the copy process of mirror recovery.

History Recording Area Size in Asynchronous Mode (1 to 200)

Specify the capacity of the mirror disk driver that, according to I/O requests from the upper system, stores data about unsent requests. Only when the mirror disk resource and/or hybrid disk resource do not exist in the cluster, the setting can be changed.

Operation at I/O Error Detection

- Cluster Partition
  Set an operation when an I/O error occurs in a cluster partition.
- Data Partition
  Set an operation when an I/O error occurs in a data partition.

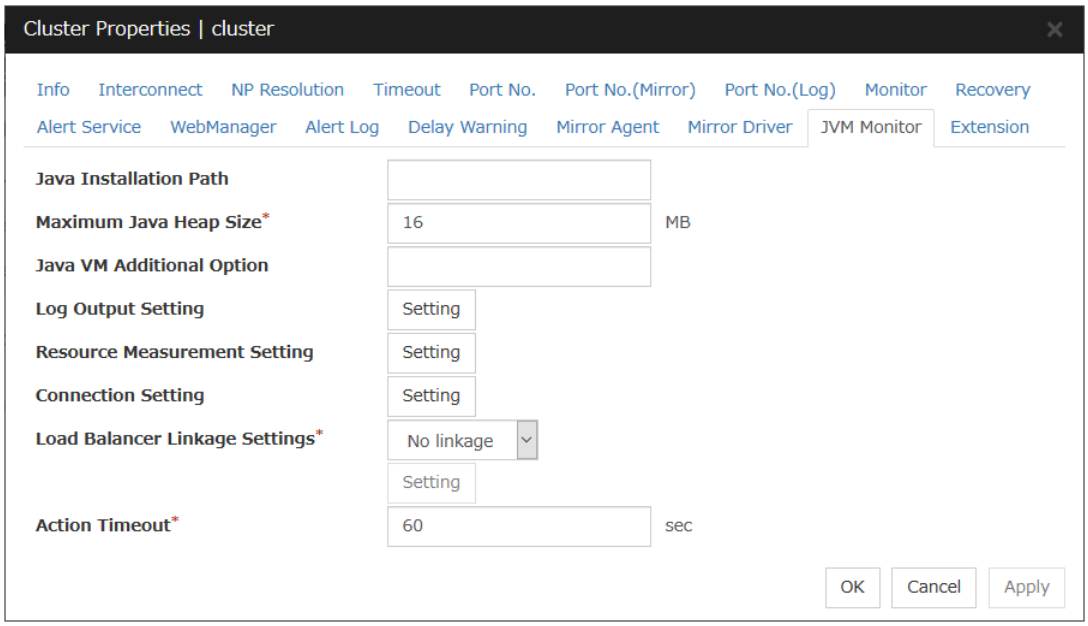
Initialize

Use **Initialize** to reset the values to the default value. Click **Initialize** to set all the items to their default values.

2.2.18 JVM monitor tab

Configure detailed parameters for the JVM monitor.

Note: To display the **JVM monitor** tab on the the config mode of Cluster WebUI, you need to execute **Update Server Info** after the license for Java Resource Agent is registered.



Java Installation Path (**Within** 255 bytes)

Set the Java VM install path used by the JVM monitor. Specify an absolute path using ASCII characters. Do not add "/" to the end of the path. This setting becomes common for all servers in the cluster.

Specification example: /usr/java/jdk-9

Maximum Java Heap Size (7 to 4096)

Set, in megabytes, the maximum Java VM heap size used by the JVM monitor (equivalent to -Xmx of the Java VM startup option). This setting becomes common for all servers in the cluster.

Java VM Additional Option (**Within** 1024 bytes)

Set the Java VM startup option used by the JVM monitor. However, specify -Xmx in the [Maximum Java Heap Size]. This setting becomes common for all servers in the cluster.

Specification example: -XX:+UseSerialGC

Log Output Setting

Click the Setting button to open the Log Output Setting dialog box.

Resource Measurement Setting

Click the Setting button to open the Resource Measurement Setting dialog box.

Connection Setting

Click the **Setting** button to open the **Connection Setting** dialog box.

Load Balancer Linkage Settings

Select the load balancer type and then click the **Settings** button. The **Load Balancer Linkage Settings** dialog box appears.

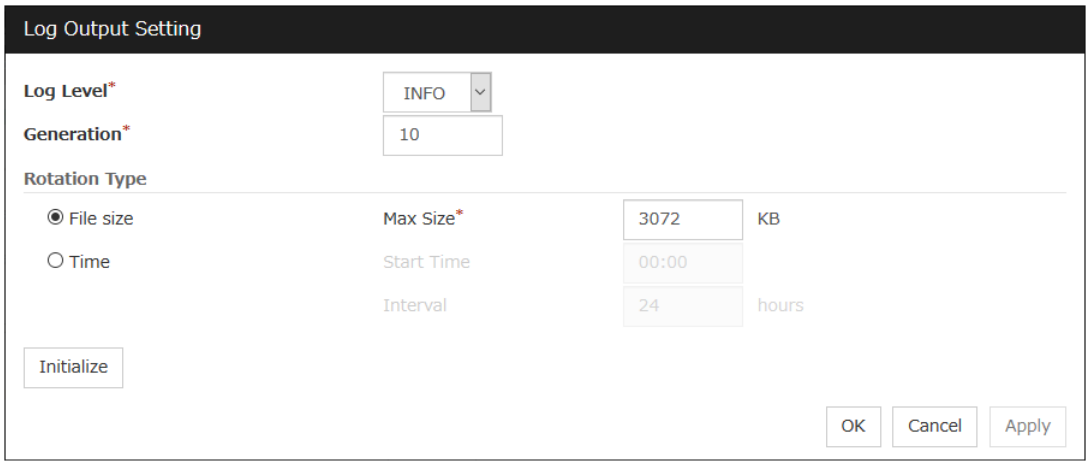
Select the load balancer type from the list. To perform load balancer linkage, select the load balancer you are using. To cancel the load balancer linkage, select **No linkage**.

Action Timeout (30 to 300)

Set the timeout value of [Command] specified in each window of the JVM monitor. This setting becomes common for all the [Command] items.

Log Output Setting

Clicking **Setting** displays the **Log Output Setting** dialog box.



Log Level

Select the log level of the log output by the JVM monitor.

Generation (2 to 100)

Set the number of generations to be retained for log output by the JVM monitor. When **Period** is selected for **Rotation Type**, the rotation count is reset when cluster is suspended. Therefore, note that log files under the <EXPRESSCLUSTER_install_path>log\ha\jra increase per cluster suspend.

Rotation Type

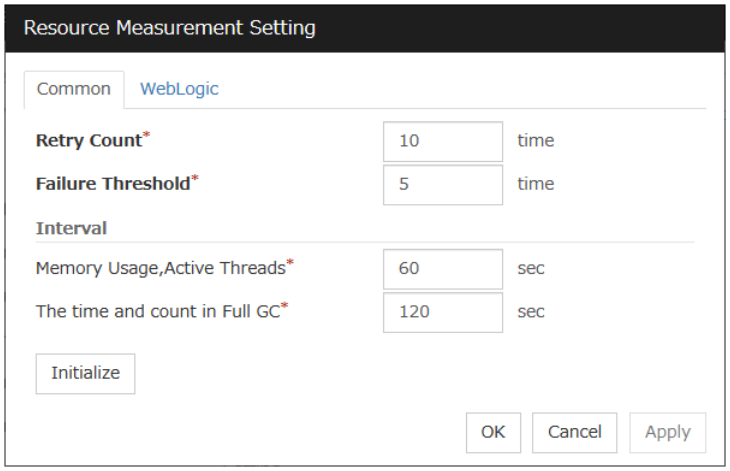
Select a rotation type for the log output by the JVM monitor. If you select **File Capacity** as the rotation type, set the maximum size (200 to 2097151), in kilobytes, for each log file such as the JVM operation log. If you select **Period** as the rotation type, set the log rotation start time in "hh:mm" format (hh: 0 to 23, mm: 0 to 59) and the rotation interval (1 to 8784) in hours.

Initialize

Clicking **Initialize** returns the log level, generation, and rotation type items to their default values.

Resource Measurement Setting [Common]

Clicking **Setting** displays the **Resource Measurement Setting** dialog box. For details about the scheme for error judgment by the JVM monitor, see "*Monitor resource details*".



Retry Count (1 to 1440)

Set a resource measurement retry count to be applied if the JVM monitor fails in resource measurement.

Error Threshold (1 to 10)

Set the number of times abnormal judgment is performed when the usage of the Java VM or the application server resources collected by the JVM monitor via resource measurement continuously exceed the customer-defined threshold.

Memory Usage, Active Threads (15 to 600)

Set the interval at which the JVM monitor measures the memory usage and active thread count.

The time and count in Full GC (15 to 600)

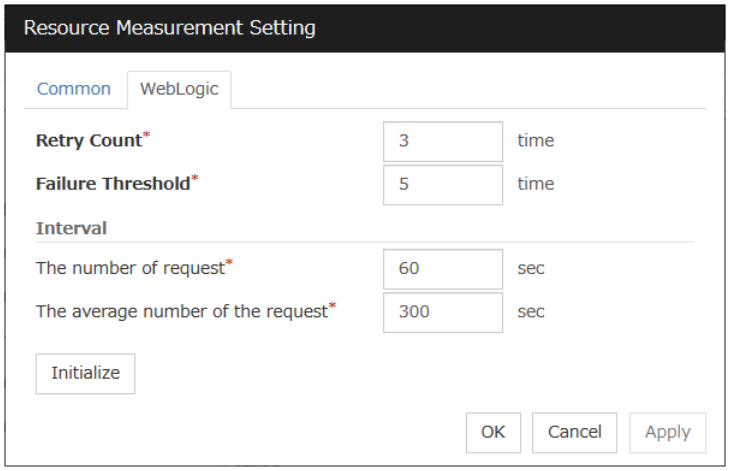
Set the **interval** at which the JVM monitor measures the time and count in Full GC execution.

Initialize

Clicking **Initialize** returns the retry count, error threshold, and interval items to their default values.

Resource Measurement Setting [WebLogic]

Clicking **Setting** displays the **Resource Measurement Setting** dialog box. For details about the scheme for error judgment by the JVM monitor, see "Monitor resource details".



Retry Count (1 to 5)

Set the resource measurement retry count to be applied if the JVM monitor fails in resource measurement.

Error Threshold (1 to 10)

Set the number of times abnormal judgment is to be performed when the usage of the Java VM or the application server resources collected by the JVM monitor via resource measurement continuously exceed the customer-defined threshold.

The number of request (15 to 600)

Set the interval at which the JVM monitor measures the number of work manager or thread pool requests during WebLogic monitor.

The average number of the request (15 to 600)

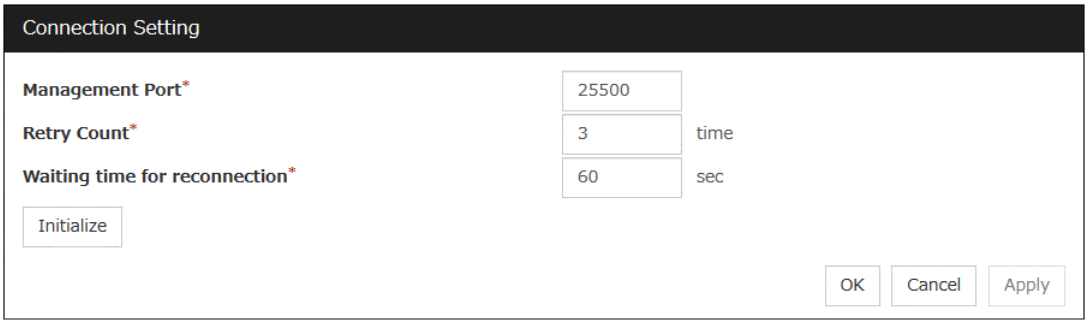
Set the interval at which the JVM monitor measures the average number of work manager or thread pool requests during WebLogic monitor. Set a value that is an integer multiple of the value set in **The number of request**.

Initialize

Clicking **Initialize** returns the retry count, error threshold, and interval items to their default values.

Connection Setting

Clicking **Setting** displays the Connection Settings dialog box.



Management Port (1 to 65535)

Sets the port number internally used by the JVM monitor resource. Make sure not to set the port number that has been used by other functions or programs. This setting becomes common for all the servers in the cluster. Do not set 32768 to 61000.

Retry Count (1 to 5)

Set the retry count to be applied if connection to the monitor target Java VM fails.

Waiting time for reconnection (15 to 60)

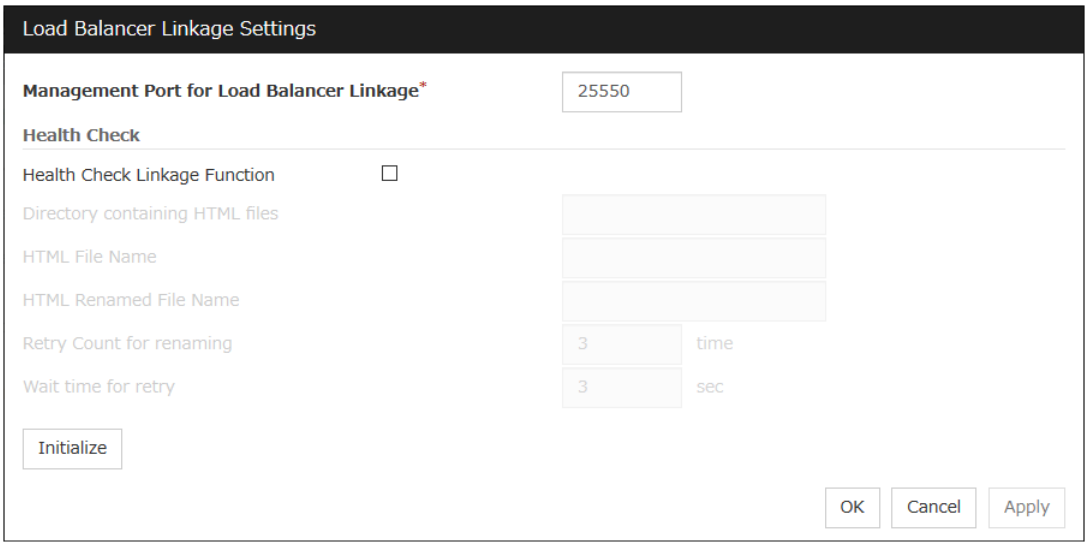
Set the interval at which the JVM monitor retries connection if it fails in Java VM connection.

Initialize

Clicking **Initialize** sets the management port, retry count, and wait time for reconnection items to their default values.

Load Balancer Linkage Settings

If you select other than BIG-IP LTM as the load balancer type and then click the **Settings** button, the **Load Balancer Linkage Settings** dialog box appears.



Management Port for Load Balancer Linkage (1 to 65535)

Set the port number used by the load balancer linkage function. This setting becomes common to all the servers in the cluster. Do not set 32768 to 61000.

Health Check Linkage Function

Set whether to use the load balancer health check function if the monitor target Java VM detects a failure.

Directory containing HTML files (**Within** 255 bytes)

Set the directory in which the HTML file used by the load balancer health check function is stored. Specify an absolute path using ASCII characters. Do not add "/" to the end of the path.

HTML File Name (**Within** 255 bytes)

Set the HTML file name used by the load balancer health check function. Specify this filename using ASCII characters.

HTML Renamed File Name (**Within** 255 bytes)

Set the HTML renamed file name used by the load balancer health check function. Specify this file name using ASCII characters. Specify an HTML renamed file name that is different from the HTML file name.

Retry count for renaming (0 to 5)

Set the number of times HTML file renaming is retried if it fails.

Wait time for retry (1 to 60)

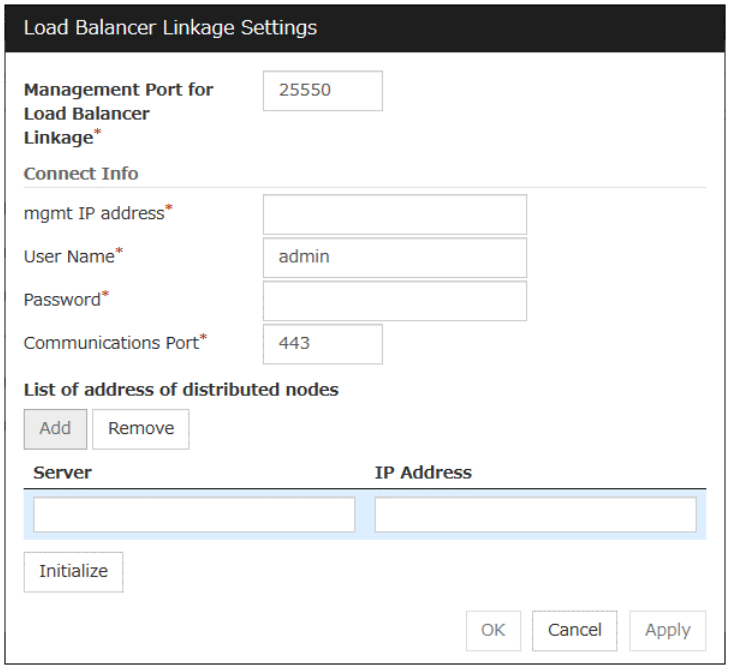
Set the interval at which HTML file renaming is retried if it fails.

Initialize

Clicking **Initialize** returns the management port for load balancer linkage, health check linkage function, directory containing HTML files, HTML file name, HTML renamed file name, retry count for renaming and wait time for retry items to their default values.

Load Balancer Linkage Settings

Select BIG-IP LTM as the load balancer type and then click the **Settings** button. The **Load Balancer Linkage Settings** dialog box appears.



Management Port for Load Balancer Linkage (1 to 65535)

Set the port number used by the load balancer linkage function. This setting becomes common to all the servers in the cluster. Do not set 42424 to 61000.

mgmt IP address

Set the BIG-IP LTM IP address.

Management User Name (Within 255 bytes)

Set the BIG-IP LTM management user name.

Password (Within 255 bytes)

Set the BIG-IP LTM management user password.

Communications Port (1 to 65535)

Set the communication port number for BIG-IP LTM.

Add

Add the server name and IP address for the distributed node. For the server name, specify the EXPRESSCLUSTER server name. For the IP address, specify the value set to **Members** in **LocalTrafic** - **Pools:PoolList** - **Relevant pool** - **Members** of BIG-IP Configuration Utility. To change the value, select the line and directly edit the description.

Remove

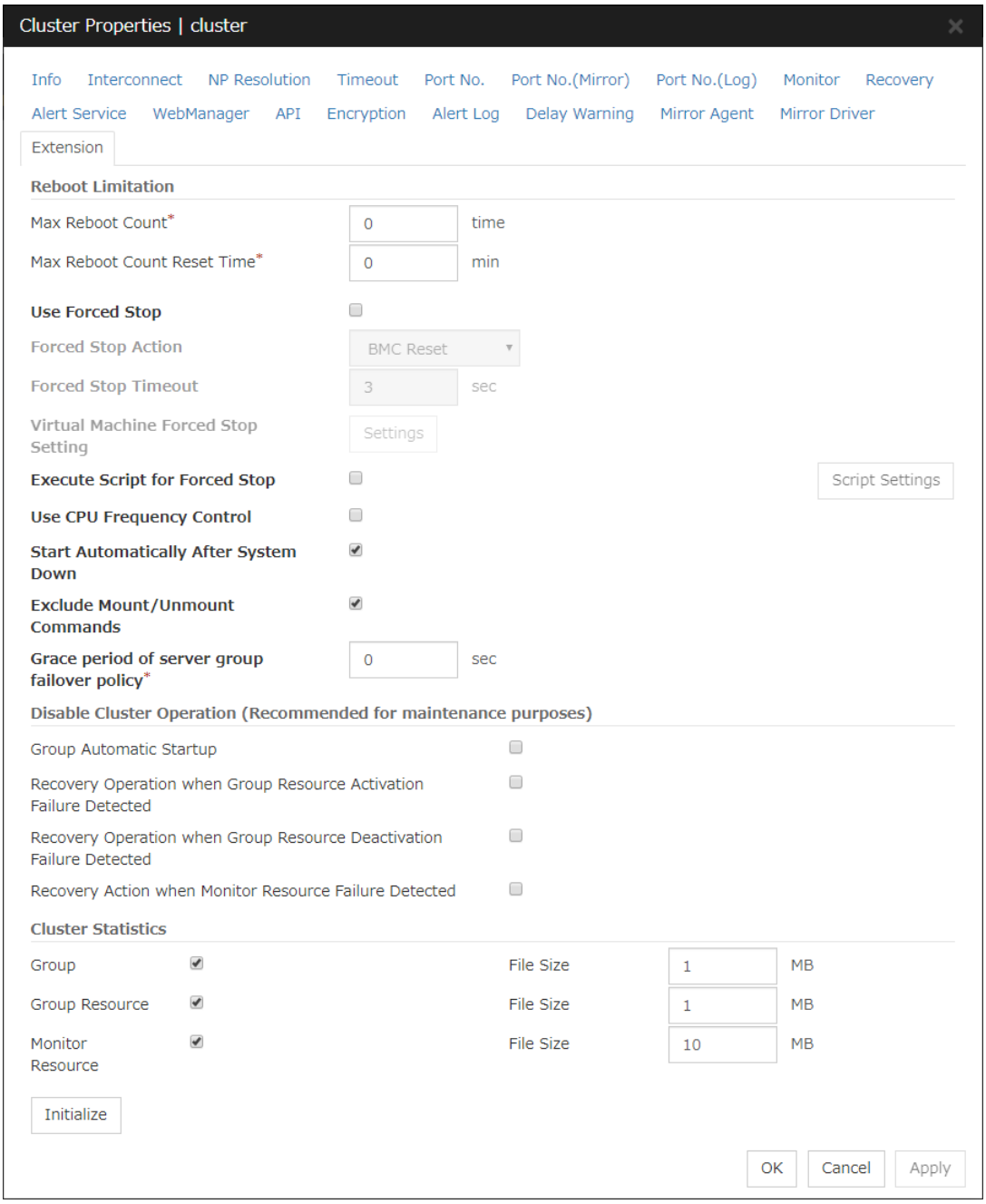
Remove the server name and IP address for the distributed node. Select the line to be removed and then click **Remove**. The selected server is removed.

Initialize

Clicking **Initialize** returns the management port for load balancer linkage, management user name, and communication port number to the default settings.

2.2.19 Extension tab

Other cluster functions are set.



Reboot Limitation

If the final action at abnormality detection for group resources and monitor resources is specified with the setting accompanied by OS reboot, reboot may be repeated infinitely. By setting the reboot limit, you can prevent repeated reboots.

- **Max Reboot Count** (0 to 99)
  Specify how many times the operating system can reboot. The number specified here is separately counted for group resource and monitor resource.
- **Max Reboot Count Reset Time** (0 to 999)
  When the max reboot count is specified, if the operation from the cluster startup keeps running normally for the time specified here, the reboot count is reset. The time specified here is separately

counted for group resource and monitor resource.

Note: If **Max Reboot Count Reset Time** is set to 0, the reboot count is not reset. If you want to reset the reboot count, use clpregctrl command.

Use Forced Stop

Use this to select whether or not to enable the forced stop.

- On

  If selected, the forced stop function is enabled.

  For a physical machine, configure the settings on the **BMC** tab of the server properties. For a virtual machine (guest OS), configure the **Virtual Machine** setting on the **Info** tab of the server properties.

- Off

  If selected, the forced stop function is disabled.

Forced Stop Action

Specify an action of the forced stop.

- BMC Reset

  Use this to perform a hardware reset of the server by using the ipmitool command.

- BMC Power Off

  Use this to power off the server by using the ipmitool command. The OS may be shut down depending on how the ACPI of OS is configured.

- BMC Power Cycle

  Use this to perform the Power Cycle (powering on/off) by using the ipmitool command. The OS may be shut down depending on how the ACPI of OS is configured.

- BMC NMI

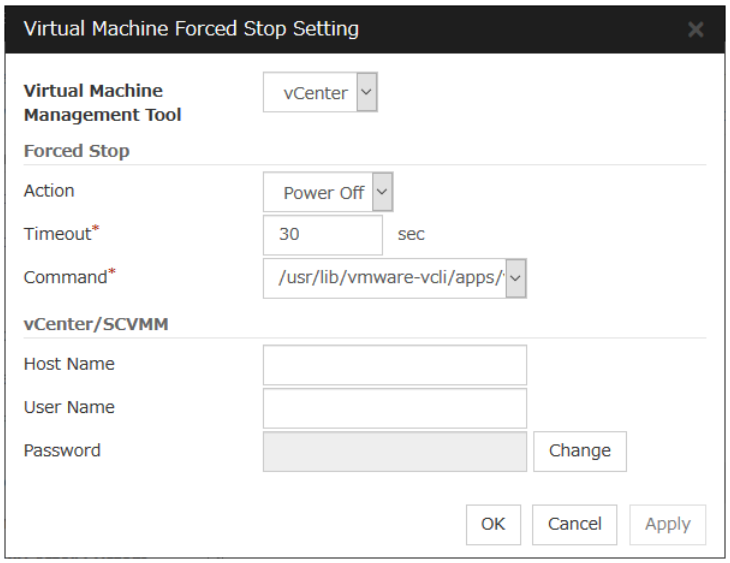
  Use this to generate NMI by using the ipmitool command. The performance after the generation of NMI depends on the OS setting.

Forced Stop Timeout (0 to 99)

Configure the timeout value when performing Forced Stop. After the above commands are executed, activating failover groups starts when the time specified elapses

Virtual Machine Forced Stop Setting

Configure forced stop for the virtual machine (guest OS). Click **Setting** to display the **Virtual Machine Forced Stop Setting** dialog box.



Virtual Machine Management Tool

- vCenter
  Select this when you want to use vCenter to control the virtual machine.

Forced Stop

- Action
  Specify the action performed upon a forced stop.
- poweroff
  Use this to power off the server by using the command specified in **Command**.
- Timeout **(0 to 99)**
  Set the timeout value to be used when performing a forced stop. After the above command is executed, the activation of failover groups starts when the time specified here elapses.
- Command **(Within 1023 bytes)**
  Specify the command for forced stop.

vCenter

- Host Name **(Within 255 bytes)**
  Specify the host name of the virtual machine management tool.
- User Name **(Within 255 bytes)**
  Specify the user name of the virtual machine management tool.
- Password
  Specify the password for the virtual machine management tool.

Note: Do not use a double quotation mark (") in the password.

Execute Script for Forced Stop

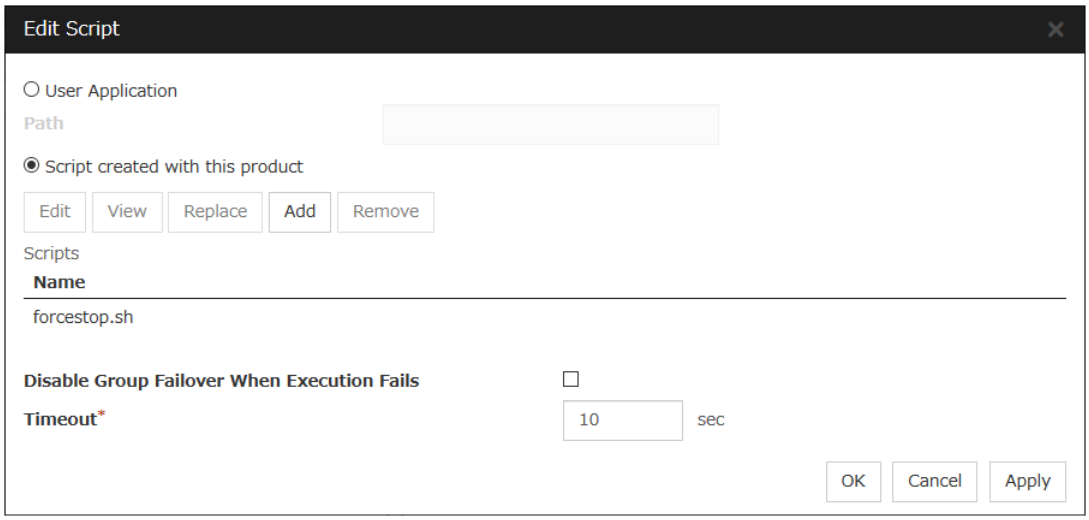
Use this to select whether or not to execute a script for the forced stop.

- On
  If selected, the script is executed for the forced stop.

- Off
  If selected, the script is not executed.

Script Setting

Make settings on the script for the forced stop. Click **Script Setting** play the **Edit Script** dialog box. The default script file names, **forcestop.sh**, are listed on **Scripts**.



User Application

Use an executable file (executable shell script file or execution file) on the server as a script. For the file name, specify an absolute path or name of the executable file of the local disk on the server. If there is any blank in the absolute path or the file name, put them in double quotation marks ("") as follows.

Example:

"/tmp/user application/script.sh"

Each executable file is not included in the cluster configuration information of the Cluster WebUI. They must be prepared on each server because they cannot be edited or uploaded by the Cluster WebUI.

Path (Within 1023 bytes)

Specify a script to be executed (executable shell script file or execution file) when you select **User Application**.

Script created with this product

Use a script file which is prepared by the Cluster WebUI as a script. You can edit the script file with the Cluster WebUI if you need. The script file is included in the cluster configuration information.

Add

Use this button to add a script other than **forcestop.sh** script when you select **Script created with this product**.

Note:

Do not use 2-byte characters for the name of a script to be added.

Do not use "&(ampersand)" or "= (equal sign)" for a script file name to be added.

Remove

Use this button to delete a script when you select **Script created with this product**. The **forcestop.sh** script cannot be deleted.

View

Click here to display the script file when you select **Script created with this product**.

Edit

Click here to edit the script file when you select **Script created with this product**. Click **Save** to apply the change. You cannot modify the name of the script file.

Replace

Click here to replace the contents of a script file with the contents of the script file which you selected in the **file selection** dialog box when you select **Script created with this product**. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not select binary files (applications), and so on.

Disable Group Failover When Execution Fails

If a forced stop script fails, a failover is disabled. If the failover is controlled, no group starts at the failover destination. Check the failover source and if necessary, perform the group operation.

Timeout (1 to 999)

Specify the maximum time to wait for completion of script to be executed. The default value is set as 10.

Use CPU Frequency Control

Select the check box when you use CPU frequency control.

When CPU frequency control is used, the CPU frequency of the server where a failover group is activated is set to high, and that of the server where a failover group is stopped is set to low.

When CPU frequency control is performed by a command or Cluster WebUI, the settings changed by the command or Cluster WebUI are given higher priority regardless of whether the failover group is started or stopped. Note that the settings changed by the command or Cluster WebUI is discarded after the cluster is stopped/started or suspended/resumed, so that CPU frequency is controlled by the cluster.

- When the check box is selected
  CPU frequency control is performed.
- When the check box is cleared
  CPU frequency control is not performed.

Note: For using CPU frequency control, it is required that the frequency is changeable in BIOS settings and the CPU supports the frequency control by OS power management function and that kernel is supported.

Start Automatically After System Down

Set whether to prohibit automatic startup of the cluster service at the next OS startup when the server has been stopped by a means other than cluster shutdown or cluster stop, or when cluster shutdown or stop does not terminate normally.

For the conditions to prohibit automatic startup of the cluster service after system down, see "*Conditions for automatic startup prohibition*" in "*7. Information on other settings*".

Exclude Mount/Unmount Commands

Specify the exclusion of mount and unmount of the file systems executed in disk resource, mirror disk resource, hybrid disk resource, NAS resource and VxVOL resource. If this option is selected, problems such as mount or unmount command failure can be avoided due to the /etc/mounttab lock. It may take time

to activate and deactivate a resource if there are many resources because mount and unmount processes are executed in order.

- When the check box is selected:
  The exclusion is performed.
- When the check box is not selected:
  The exclusion is not performed.

Grace period of server group failover policy (0 to 999)

Specify the time by which a failover start is delayed when the automatic failover is performed between the server groups. After a server failure is detected and then the specified time elapses, the failover is performed.
If you specify 0, no delay occurs.

Disable cluster operation

- Group Automatic Startup
  - When the checkbox is selected:
    The group does not start automatically.
  - When the checkbox is not selected:
    The group starts automatically.
- Recovery operation when a group resource activation error is detected
  - When the checkbox is selected:
    The recovery operation is disabled.
  - When the checkbox is not selected:
    The recovery operation is not disabled.
- Recovery operation when a group resource deactivation error is detected
  - When the checkbox is selected:
    The recovery operation is disabled.
  - When the checkbox is not selected:
    The recovery operation is not disabled.
- Recovery action when a monitor resource error is detected
  - When the checkbox is selected:
    The recovery action is disabled.
  - When the checkbox is not selected:
    The recovery action is not disabled.

Note: The **Recovery action when a monitor resource error is detected** feature does not support external monitor resources.

Cluster Statistics

You can collect and see data on the cluster operation such as the required time of a group failover and that of resource activation.
For more information, see " Cluster statistics information collection function" in " The system maintenance information" in the " Maintenance Guide".

- When the check box is selected

The cluster statistical information is collected.

- **File Size** (1 to 99)
  Specify the size of the cluster statistical information file.
  When the collected information reaches the specified size, rotation occurs to save up to two generations of the data.

- When the check box is cleared
  The cluster statistical information is not collected.

Initialize

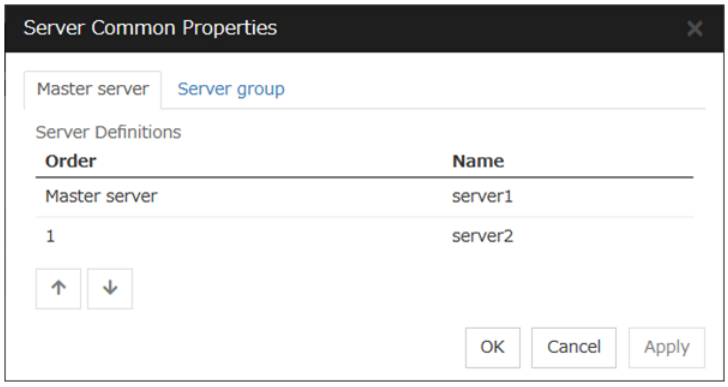
Use **Initialize** to reset the values to the default value. Clicking **Initialize** sets all the items to their default values.

2.3 Server Common Properties

Configure setting information of all servers in Servers Properties.

2.3.1 Master server tab

Configure the priority order of the servers. All the registered servers are displayed. Master server is the server to keep the master of cluster configuration information. And also, it is the server of the highest priority order.

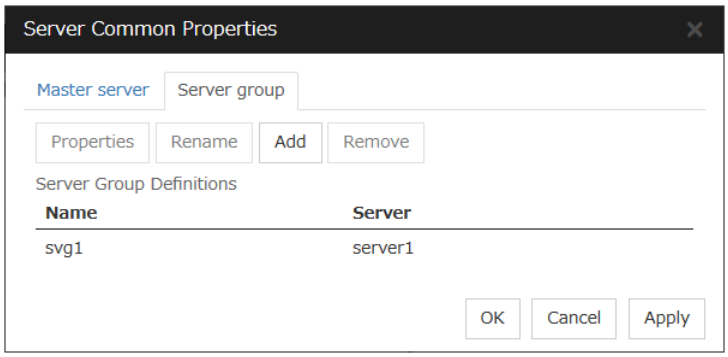


Order

Used when changing the priority order of the servers. Select the server to be changed from the server definition list, and Click the arrows selected row moves.

2.3.2 Server group tab

Set server groups.



Add

Add server groups. The wizard windows for adding the server group is displayed. For the details, see "Creating the cluster configuration data" in "Installation and Configuration Guide".

Remove

Then the selected server group is removed.

When the following conditions are matched, the server group cannot be removed.

Selected target	Conditions that the server group cannot be removed	Application method
Server group name	The server group is registered as the server group of the failover group.	Cluster stop Mirror agent stop Mirror agent start Cluster start

Rename

The change server group name dialog box of the selected server group is displayed.

There are the following naming rules

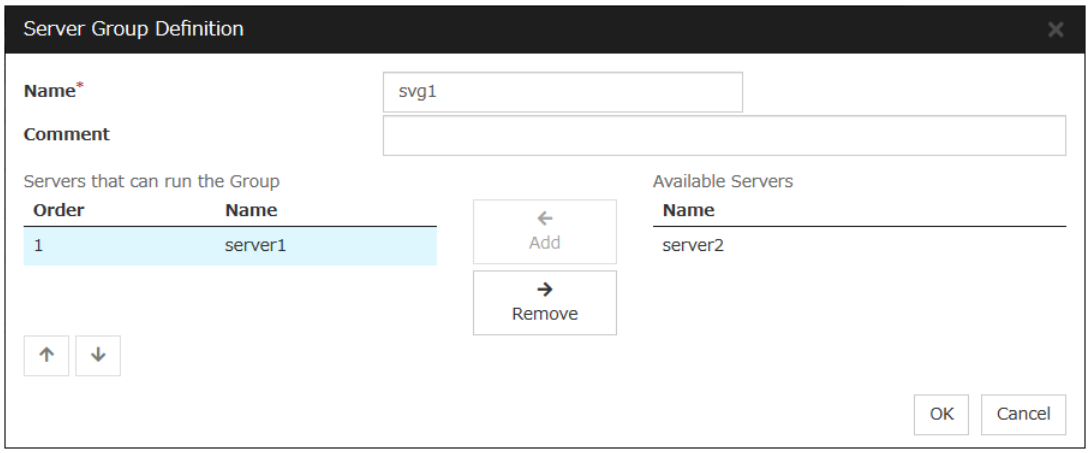
Selected target	Naming rules	Application method
Server group name	• There are naming rules that are the same as the host name of TCP/IP that can be set by the OS. • Up to 31 characters (31 bytes). • Names cannot start or end with a hyphen (-) or a space. • A name consisting of only numbers is not allowed.	Cluster stop Mirror agent stop Mirror agent start Cluster start

Names should be unique (case-insensitive) in the server group.

Properties

Display the properties of the selected server group.

Server Group Definition



Name

Display the server group name.

Add

Add the selected server in **Available Servers** to **Servers that can run the Group**.

Remove

Remove the selected server in **Servers that can run the Group** from the list.

Order

Used when changing the priority order of the server. Select the server to be changed from **Servers that can run the Group** and click the arrows. The selected row moves.

Servers

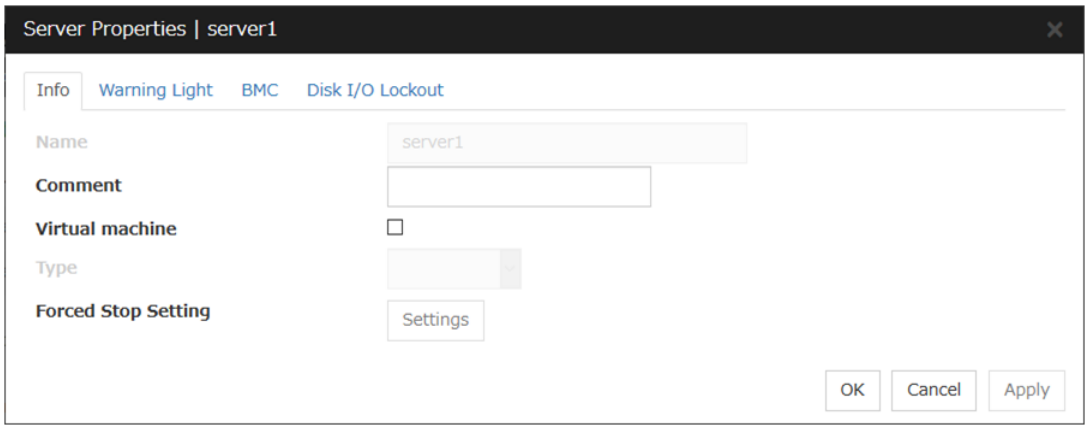
Display the server names which belong to the server group.

2.4 Server properties

Configure individual settings on each server constructing the cluster in Server Properties.

2.4.1 Info tab

You can display the server name and make a change to a comment on this tab.



Name

The selected server name is displayed. You cannot change the name here.

Comment (Within 127 bytes)

You can specify a comment for the server. Only alphanumeric characters are allowed.

Virtual Machine

Specify whether this server is a virtual machine (guest OS).

- On
  If selected, the server is a virtual machine (guest OS). You can configure this virtual machine.
- Off
  If selected, the server is a physical machine. You cannot configure a virtual machine.

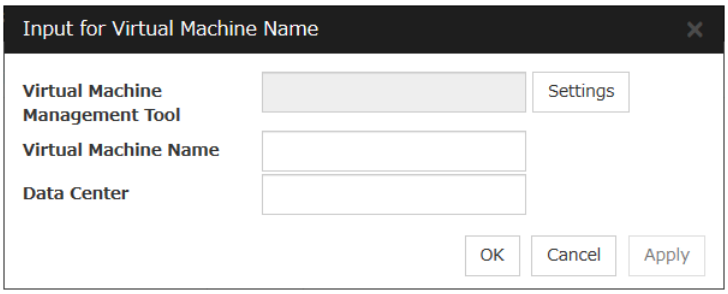
Type

Specify the type of virtual infrastructure.

- vSphere
  Virtual infrastructure provided by VMware, Inc.
- KVM
  Linux kernel virtual infrastructure.
- XenServer
  Virtual infrastructure provided by Citrix Systems, Inc.
- Container
  Virtual infrastructure provided by Oracle Systems, Inc.
- Hyper-V
  Virtual infrastructure provided by Microsoft Corporation.
- other
  Specify this option to use any other virtual infrastructure.

Forced Stop Setting

Set the information about the virtual machine (guest OS). Click **Setting** to display the **Input for Virtual Machine name** dialog box.



Virtual Machine Management Tool

Set the vCenter server that manages the virtual machine (guest OS). Click **Setting** to display the **Virtual Machine Forced Stop Setting** dialog box.

For more information on **Virtual Machine Forced Stop Setting**, refer to the description of the "*Extension tab*".

Virtual Machine name (Within 80 bytes)

Set the virtual machine (guest OS) name.

Note: Do not use a double quotation mark (") or percent sign (%) in the virtual machine name.

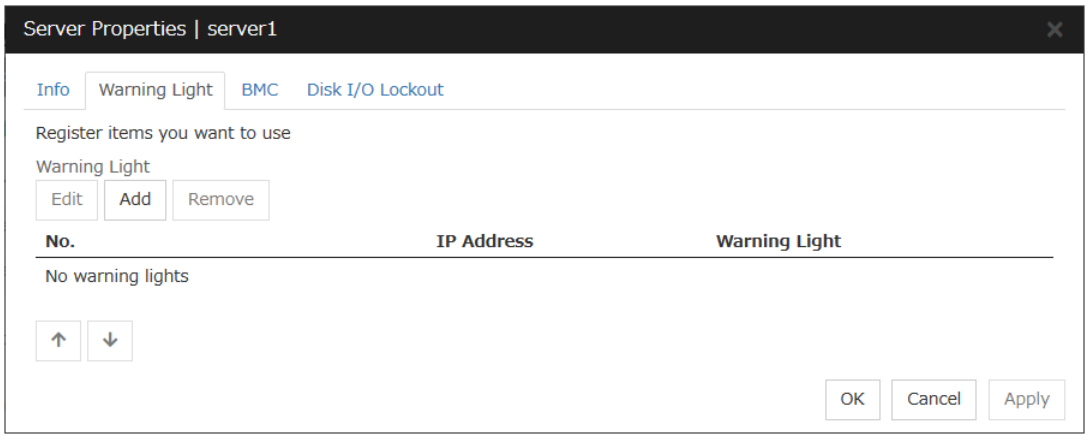
Data Center (Within 80 bytes)

Set the name of the data center that manages the virtual machine (guest OS).

Note: Do not use a double quotation mark (") or percent sign (%) in the virtual machine name.

2.4.2 Warning Light tab

Set an IP address of warning light (specified by NEC) controlled by network.



Add

Use **Add** to add an interface. Clicking **Add** displays the **Warning Light Settings** dialog box.

- **Warning Light**
  Select the product number of the warning light you use. The products corresponding to each number are as follows.

Product Number	Product Name
DN-1000S/DN-1000R/DN-1300GL	DN-1000S/DN-1000R/DN-1300GL
DN-1500GL	DN-1500GL
NH-FB series/NH-FB1 series	NH-FB series/NH-FB1 series
NH-FV1 series	NH-FV1 series

- **IP Address (Within 80 bytes)**
  Enter an IP address of the warning light.

Note: One warning light is required per one server. Do not set an IP address of the same warning light to multiple servers.

- **Playback of an audio file**
  Playback of an audio file is enabled when DN1500GL or NH-FV1 series is selected as the warning light type.
  If you change the warning light type to other than DN1500GL or NH-FV1 series after playback of an audio file was enabled, playback of an audio file will be disabled.

Alert When Server Starts

- When the check box is selected:
  Reproduces the audio file at server start. The audio file is reproduced only once.
- When the check box is not selected:
  Does not reproduce the audio file at server start.

Voice File No. (DN1500GL:01 to 20, NH-FV1 series: 01 to 70)

Set the number of the voice file to be played when the server starts

Alert When Server Stops

- When the check box is selected:
  Reproduces the audio file at server stop. The audio file is continuously reproduced until it is stopped manually.
- When the check box is not selected:
  Does not reproduce the audio file at server stop.

Voice File No. (DN1500GL:01 to 20, NH-FV1 series: 01 to 70)

Set the number of the voice file to be played when the server stops.

Edit

Use **Edit** to edit the warning light setting.

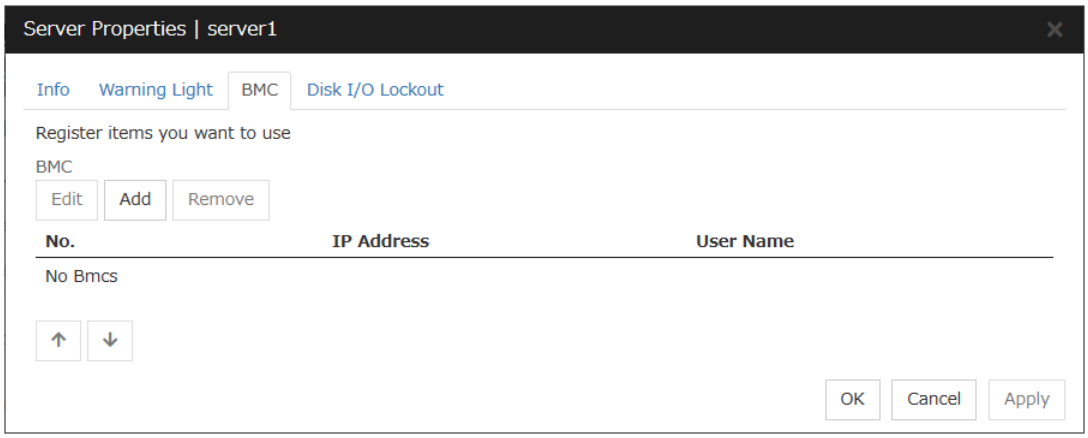
Note:

To play back the audio file, it must be registered in the network warning light.
For more information on audio file registration, refer to the instruction manual of the network warning light to be used.
Set the audio file number corresponding to the audio file that is registered for the network warning light.

2.4.3 BMC tab

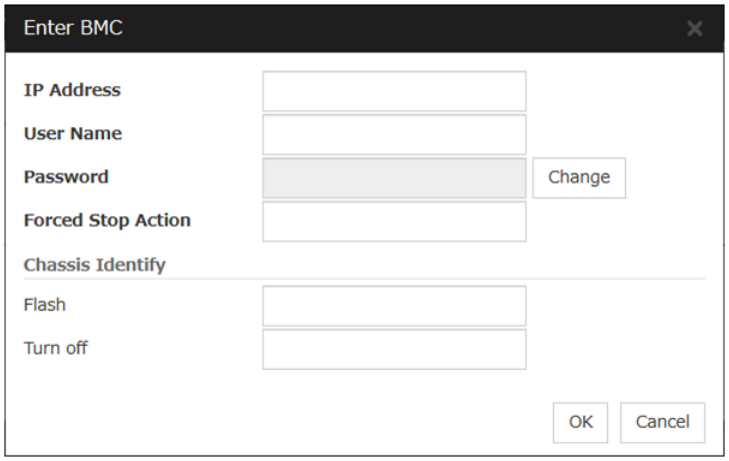
Configure a LAN port for managing BMC when using the forced stop and the chassis identify.

Configure one for each server.



Add

Use this button to newly configure a server. Click **Add** to opens the **BMC Settings** dialog box.



- IP Address **(Within 80 bytes)**
  Enter the IP address set for the LAN port for managing BMC.

- User Name (**Within** 255 bytes)
  Enter the user name with administrator privilege from the user names configured in BMC.
  If you do not enter anything, the argument of user name is not configured when the ipmitool command.
  The valid length of user name varies depending on the ipmitool command and the specification of BMC of the server.
- Password **(Within 255 bytes)**
  Enter the password of the user configured above.
  The valid length of password varies depending on the specifications of ipmitool command and the BMC of the server.
  For more information on user name and password, refer to the manual of the server.
- Forced Stop Action (**Within 255 bytes)**
  Enter a command of forced stop action.
  For details, see "*Forced stop*" in "*7. Information on other settings*" in this guide.
- Flash **(Within 255 bytes)**
  Enter a flashing command of chassis identify.
  For details, see "*Chassis Identify*" in "*7. Information on other settings*" in this guide.
- Turn off **(Within 255 bytes)**
  Enter a turn-off command of chassis identify.
  For details, see "*Chassis Identify*" in "*7. Information on other settings*" in this guide.

Remove

Use this button to remove the settings. Select the target setting, and then, click **Remove**.

Edit

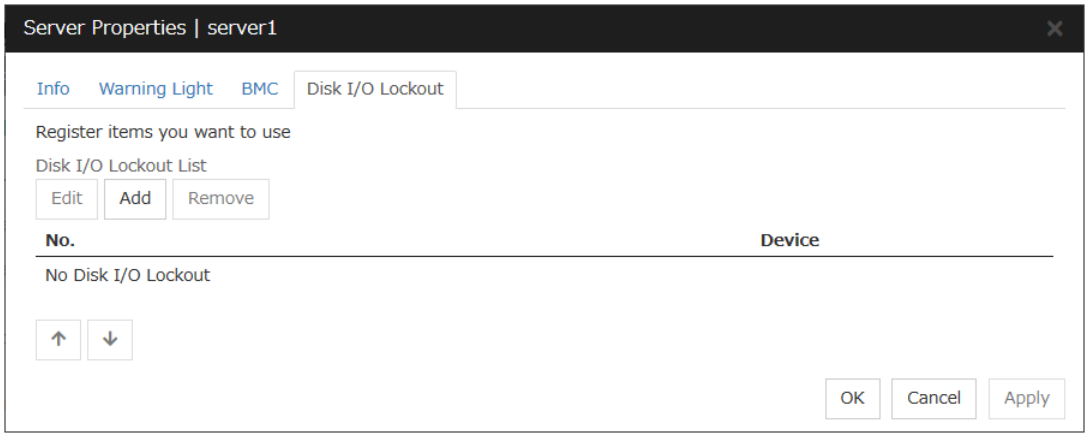
Use this button to modify the settings. Select the target setting, and then, click **Edit**. The **BMC Settings** dialog box is displayed.

When a cluster consists of the different types of servers and includes a server which does not have BMC function, do not configure the **BMC** tab for the server.

In such a configuration, if **Chassis Identify** and/or the forced stop function, the alert telling you "failed in the BMC action" is displayed.

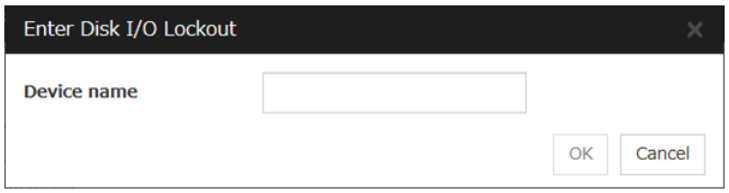
2.4.4 Disk I/O Lockout tab

Configure the settings for disk I/O lockout devices.



Add

Use **Add** to add lockout devices. Clicking **Add** displays the **Enter Disk I/O Lockout** dialog box.



- Device Name **(Within 1023 bytes)**
  Enter a disk I/O lockout device.

Remove

Use **Remove** to remove lockout devices. Select the device to remove from the **Disk I/O Lockout List** device and then click **Remove**.

Edit

Use **Edit** to edit disk I/O lockout devices. Clicking **Edit** opens the **Enter Disk I/O Lockout** dialog box.

No.

Use the arrows to change the I/F number. Select the I/F you want to change from the I/F list and then click the arrows. The selected raw moves up and down accordingly.

2.4.5 Proxy tab

Sets proxy information.

Proxy Scheme

Sets protocols you want to use.

None: Proxy is used.
HTTP: HTTP is used.

Proxy Server

Sets the DNS host name (or IP address) you want to connect.

Proxy Port

Sets the port number you want to connect.

2.5 Group Properties

For more information, see "3. *Group resource details*" in this guide.

2.6 Group Resource Properties

For more information, see "3. *Group resource details*" in this guide.

2.7 Monitor Resource Properties

For more information, see "4. *Monitor resource details*" in this guide.

2.8 Parameters list

Parameters you can specify in the Cluster WebUI and their default values are listed below.

"How to change [1]-[11]" represents the way you apply changes of parameters on servers. Applicable method is marked with "O."

Priority	How to apply	Refer to:
1	Uploading data and shutting down, restarting a cluster	"Installation and Configuration Guide" "Modifying the cluster configuration data"
2	Stopping a cluster, and stopping a mirror agent, and then uploading data	"Installation and Configuration Guide" "Modifying the cluster configuration data"
3	Uploading data after stopping a cluster	"Installation and Configuration Guide" "Modifying the cluster configuration data"
4	Uploading data after stopping a group	"Installation and Configuration Guide" "Modifying the cluster configuration data"
5	Uploading data after stopping a resource	"Installation and Configuration Guide" "Modifying the cluster configuration data"
6	Uploading data after suspending a cluster	"Installation and Configuration Guide" "Modifying the cluster configuration data"
7	Uploading data after suspending a monitor	"Installation and Configuration Guide" "Modifying the cluster configuration data"
8	Uploading data and restarting an Information Base service	"Installation and Configuration Guide" "Modifying the cluster configuration data"

Continued on next page

Table 2.3 – continued from previous page

Priority	How to apply	Refer to:
9	Uploading data and restarting WebManager Server	"Installation and Configuration Guide" "Modifying the cluster configuration data"
10	Uploading data and restarting an API service	"Installation and Configuration Guide" "Modifying the cluster configuration data"
11	Uploading data only	"Installation and Configuration Guide" "Modifying the cluster configuration data"

When creating the cluster configuration data for the first time, see "Creating the Cluster configuration data" in the "Installation and Configuration Guide".

Cluster

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Cluster Properties												
Info Tab												
Cluster Name	-						O					
Comment	-											O
Language	English						O			O		
Interconnect Tab												
Communication Path (Add, Remove)	-		O									
Type							O			O		
MDC			O									
Kernel mode, User mode, IP Address							O			O		
DISK Device		O					O			O		
COM Device							O			O		
BMC IP Address							O			O		
Witness HB Use							O			O		
Mirror Communication Only			O									
MDC Use			O									
Server Down Notification	On											O
Disk Heart Beat Properties												
Raw Device							O					
Witness Heart Beat Properties												
Target Host							O					
Service Port	80						O					
Use SSL	Off						O					
Use Proxy	Off						O					
HTTP Timeout	10 seconds						O					
Heart Beat I/F Tuning Properties												
DISK tab												
Open/Close Timing				O								
Bind Check			O									
Network Partition Resolution Definition Tab												
Ping Target							O					
Server							O					
Ping NP Properties												
Interval	5 seconds						O					
Timeout	3 seconds						O					
Retry Count	3 times						O					
HTTP NP Properties												
Use Witness HB Resource Settings							O					
Target Host							O					
Service Port	80						O					
Use SSL	Off						O					
Interval	5 seconds						O					
Timeout	20 seconds						O					
HTTP Timeout	10 seconds						O					
Network Partition Resolution Tuning Properties												
Action at NP Occurrence	Shutdown						O					
MDC Tab												
MDC			O									
Server			O									
Add			O									
Remove			O									
Timeout Tab												
Server Sync Wait Time	5 minutes											O
Heartbeat Interval	3 seconds						O					
Heartbeat Timeout	90 seconds						O					
Server Internal Timeout	180 seconds						O			O		
Port No. Tab												
Server Internal Port Number	29001						O			O		
Information Base Port Number	29008								O			
Data Transfer Port Number	29002	O										
WebManager HTTP Port Number	29003									O		
API HTTP Port Number	29009										O	
API Server Internal Port Number	29010										O	
Heartbeat Port Number	29002						O					
Kernel Mode Heartbeat Port Number	29006						O					
Alert Sync Port Number	29003									O		
Port No. (Mirror) Tab [1]												
Mirror Agent Port Number	29004		O									
Port No. (Log) Tab												
Communication Method for Internal Logs	Unix Domain	O										
Port Number	-	O										
Monitor Tab												
Shutdown Monitor	Execute when the group deactivation has been failed											O
Method	keepalive											O
Operation at Timeout Detection	RESET											O
Enable SIGTERM handler	Off											O
Timeout	Use Heartbeat Timeout											O
Set Timeout	90 seconds											O

Collect the System Resource Information	Off						O					
Recovery Tab												
Action for Cluster Service Process Error	OS shutdown											O
Max Restart Count	3 times					O						
Recovery Action over Max Restart Count	No operation					O						
Action at Group Resource Activation or Deactivation Stall	Stop the cluster service and shutdown OS						O					
Disable the Final Action when OS Stops Due to Failure Detection												
Group Resource When Activation Failure Detected	Off						O					
Group Resource When Deactivation Failure Detected	Off						O					
Monitor Resource When Failure Detected	Off						O					
Disable Shutdown When Multi-Failover-Service Detected												
Server Group Survives When Multi-Failover-Service Detected	-						O					
Server doesn't Shutdown When Multi-Failover-Service Detected	-						O					
Alert Service Tab												
Enable Alert Setting	Off						O					
E-mail Address	Blank (Function disabled)											O
Subject	EXPRESSCLUSTER											O
Mail Method	MAIL											O
Output the log level to syslog	On						O					
Use Chassis Identify	Off											O
Repeat Chassis Identify Command	Execute Repeatedly											O
Interval	120 seconds											O
User Network Warning Light[2]	Off						O					
Alert Destination Tab												
Messages (Add, Remove, Edit)	-											O
Message Tab												
Category	Core Modules											O
Module Type	apisv											O
Event ID	-											O
Destination System Log	On											O
Destination Alert Logs	On											O
Destination Mail Report	Off											O
Destination SNMP Trap	Off											O
Destination Alert Extension	Off											O
Command (Add, Remove, Edit)	-											O
SMTP Settings Tab												
Mail Charset	-											O
Send Mail Timeout	30 seconds											O
Subject Encode	Off											O
SMTP Server	-											O
SMTP Server List (Add, Remove)	-											O
Enter the SMTP Server												
SMTP Server	-											O
SMTP Port	25											O
Sender Address	-											O
Enable SMTP Authentication	Off											O
Authority Method	LOGIN											O
User Name	-											O
Password	-											O
Behavior Tab												
Destination (Add, Remove, Edit)	-											O
Destination Tab												
Destination Server	-											O
SNMP Port No.	162											O
SNMP Version	v2c											O
SNMP Community Name	public											O
WebManager Tab												
Enable WebManager Service	On									O		
Communication Method	HTTP									O		
Accessible number of clients	64									O		
Control connection by using client IP address	Off									O		
IP Addresses of the Accessible Clients (Add, Remove, Edit)	-									O		
Operation	On									O		
Password												
Cluster Password Method / OS Authentication Method	Cluster Password Method									O		
Cluster Password Method												
Password for Operation	-											O
Password for Reference	-											O
OS Authentication Method												
Authorized Group List(Add, Remove, Edit)	-									O		
Operation	On									O		
Login Session Lifetime Period	1440 minutes									O		
Automatic Logout Time Period	60 minutes									O		

Lockout Threshold	0 time									O		
Lockout Time	10 minutes									O		
IP address for Integrated WebManager												
IP address							O					
WebManager Tuning Properties												
Behavior Tab												
Client Session Timeout	30 seconds									O		
Reload Interval	90 seconds									O		
Mirror Agent Tab	120 seconds									O		
Time Limit For Keeping Log Files	600 seconds									O		
Use Time Information Display Function	On						O			O		
API Tab												
Enable API Service	Off										O	
Communication Method	HTTP										O	
Control connection by using client IP address	Off										O	
IP Addresses of the Accessible Clients (Add, Remove, Edit)	-										O	
API Tuning Properties												
Authentication Lockout Threshold	3 times										O	
HTTP Server Start Retry Count	3 times										O	
HTTP Server Start Interval	5 seconds										O	
Encryption Tab												
Certificate File	-									O		
Private Key File	-									O		
SSL Library	-									O		
Crypto Library	-									O		
Alert Log Tab												
Enable Alert Service	On									O		
Max. Number to Save Alert Records	10000									O		
Alert Sync Method	Unicast (fixed)									O		
Alert Sync Communication Timeout	30 seconds									O		
Delay Warning Tab												
Heartbeat Delay Warning	80%						O					
Monitor Delay Warning	80%						O					
Mirror Agent Tab [3]												
Auto Mirror Recovery	On											O
Collect Mirror Statistics	On		O									
Receive Timeout	10 seconds		O									
Send Timeout	120 seconds											O
Recovery Data Size	4096 kilobytes											O
Recovery Limitation	Off											O
Start Wait Time	10 seconds		O									
Cluster Partition I/O Timeout	30 seconds		O									
Mirror Driver Tab [4]												
Max. Number of Request Queues	2048		O									
Difference Bitmap Size	1 [MB]		O									
Difference Bitmap Refresh Interval	100 seconds		O									
Mirror Recovery I/O Size	4 kilobytes		O									
History Recording Area Size in Asynchronous Mode	100 megabytes		O									
Operation at I/O Error Detection Cluster Partition	RESET		O									
Operation at I/O Error Detection Data Partition	RESET		O									
JVM monitor Tab[5]												
Java Installation Path	-						O					
Maximum Java Heap Size	16 megabytes						O					
Java VM Additional Option	-						O					
Action Timeout	60 seconds						O					
Log Output Settings												
Log Level	INFO						O					
Generation	10 generations						O					
Rotation Type	File capacity						O					
Rotation Type, File Capacity, Max Size	3072 kilobytes						O					
Rotation Type, Period, Start Time	0:00						O					
Rotation Type, Period, Interval	24 hours						O					
Resource Measurement Settings [Common]												
Retry Count	10 times						O					
Error Threshold	5 times						O					
Interval, Memory Usage, Active Threads	60 seconds						O					
Interval, The time and count in Full GC	120 seconds						O					
Resource Measurement Settings [WebLogic]												
Retry Count	3 times						O					
Error Threshold	5 times						O					
Interval, The number of request	60 seconds						O					
Interval, The average number of the request	300 seconds						O					
Connection Settings												
Management Port	25500						O					
Retry Count	3 times						O					

Waiting time for reconnection	60 seconds						O					
Load Balancer Linkage Settings (for other than BIG-IP)												
Management Port for Load Balancer Linkage	25550						O					
Directory containing HTML files	-						O					
HTML File Name	-						O					
HTML Renamed File Name	-						O					
Retry Count for renaming	3 times						O					
Wait time for retry	3 seconds						O					
Load Balancer Linkage Settings (for BIG-IP LTM)												
Management Port for Load Balancer Linkage	25550						O					
mgmt IP address	-						O					
Management User Name	admin						O					
Password	-						O					
Communication Port Number	443						O					
Server Name	-						O					
IP Address	-						O					
Oracle Clusterware linkage Tab[6]												
Use Oracle Clusterware linkage	Off			O								
Extension Tab												
Max Reboot Count	zero						O					
Max Reboot Count Reset Time	0 minute						O					
Use Forced Stop	Off						O					
Forced Stop Action	BMC reset						O					
Forced Stop Timeout	3 seconds						O					
Virtual Machine Forced Stop												
Virtual Machine Management Tool	vCenter						O					
Action	poweroff						O					
Timeout	30 seconds						O					
Command	/usr/lib/vmware-viperl/apps/vm/vmcontrol.pl						O					
Host Name	-						O					
User Name	-						O					
Password	-						O					
Execute Script for Forced Stop	Off											O
Script Setting												
Select User Application Enter application path (Edit)	-											O
Script created with this product Add,Remove,Edit,Replace	-											O
Disable Group Failover When Execution Fails	Off											O
Timeout	10 seconds											O
Use CPU Frequency Control	Off											O
Start Automatically After System Down	On						O					
Exclude Mount/Unmount Commands	On											O
Grace period of server group failover policy	0 seconds											O
Disable cluster operation												
Group Automatic Startup	Off											O
Recovery operation when a group resource activation error is detected	Off											O
Recovery operation when a group resource deactivation error is detected	Off											O
Recovery action when a monitor resource error is detected	Off											O
Cluster Statistics Group	On						O					
Cluster Statistics File Size	1 megabyte						O					
Cluster Statistics Group Resource	On						O					
Cluster Statistics File Size	1 megabyte						O					
Cluster Statistics Monitor Resource	On						O					
Cluster Statistics File Size	10 megabytes						O					

[1] It does not apply to PPC64 and PPC64LE.
[2] It does not apply to PPC64 and PPC64LE.
[3] It does not apply to PPC64 and PPC64LE.
[4] It does not apply to PPC64 and PPC64LE.
[5] It does not apply to PPC64 and PPC64LE.
[6] It does not apply to PPC64 and PPC64LE.

Servers

		How to change										
Parameters	**Default**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Server Common Properties												
Master Server Tab												
Order	-			O						O		
Server Group Definition												
Server Group Tab												
Add	The order you added to "Servers that can run the Group."		O									
Remove	-		O									

Rename	-		O									
Server Group Properties												
Comment												O
Add	-		O									
Remove	-		O									
Order	The order you added to "Servers that can run the Group."		O									

Server

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Add Server [7]	-											
Remove Server [7]	-											
Server Properties												
Info Tab												
Name [8]	-											
Comment	-											O
Virtual machine	Off						O					
Type	vSphere											O
Input for Virtual Machine name												
Virtual Machine name												O
Data Center												O
Warning Light Tab												
I/F No. (Add, Remove)	The order you added I/Fs						O					
IP Address (Edit)	-						O			O		
Warning Light	DN-1000S / DN-1000R / DN-1300GL						O					
Alert When Server Starts	Off											O
Alert When Server Stops	Off											O
Voice File No.	-											O
Voice File No.	-											O
BMC Tab												
No (Add, Remove)	The order you added						O					
IP Address (Edit)	-						O					
User Name	-						O					
Password	-						O					
Forced Stop Action	-						O					
Flash	-											O
Turn off	-											O
BMC(High-End Server Option) Tab[9]												
No (Add, Remove)	The order you added						O					
IP Address (Edit)	-						O					
Disk I/O Lockout Tab												
I/F No. (Add, Remove)	The order you added I/Fs						O					
Device (Edit)	-	O										
PCI Slot Fencing(High-End Server Option) tab[10]												
PCI slot 1 to PCI slot 16	Off						O					
Proxy Tab												
Proxy Scheme	None						O					
Proxy Server	-						O					
Proxy Port	-						O					

[7] For details about how to add or remove a server, see the Maintenance Guide.
[8] Be careful when you change the host name or IP address of a server. For how to change the host name or IP address, see the Maintenance Guide.
[9] It does not apply to PPC64 and PPC64LE.
[10] It does not apply to PPC64 and PPC64LE.

Groups

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Group Common Properties												
Exclusion tab												
Exclusive Rule List												
Add	-						O					
Remove	-						O					
Rename	-						O					
Properties	-						O					
Exclusive Rule Properties												
Comment	-						O					
Add	-						O					
Remove	-						O					

Group

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Add Group	-						O					
Remove Group	-				O		O					

Group Properties												
Info Tab												
Use Server Group Settings(Changes to On)	Off		O									
Use Server Group Settings(Changes to Off)	Off		O									
Name	failover				O		O					
Comment	-											O
Startup Server Tab(Server)												
Failover is possible on all servers (Changes to On)	On						O					
Failover is possible on all servers (Changes to Off)	On						O					
Order	The order you added to "Servers that can run the Group."						O					
Name (Add)	-						O					
Name(Delete)	-				O		O					
Startup Server Tab (Server Group)												
Order	The order you added to "Servers that can run the Group."		O									
Name (Add)	-		O									
Name(Delete)	-		O									
Attributes Tab												
Startup Attribute	Auto Startup						O					
Execute Multi-Failover-Service Check	Off						O					
Timeout	300 seconds						O					
Failover Attribute	Auto Failover - Use the startup server settings						O					
Perform a Forced Failover	Off						O					
Prioritize failover policy in the server group	Off						O					
Perform a Smart Failover	Off						O					
Enable only manual failover among the server groups	Off						O					
Failback Attribute	Manual Failback						O					
Dynamic Failover Exclusive List	IP monitor NIC Link Up/Down monitor						O					
Start Dependency Tab												
Dependent Group (Add)	-						O					
Dependent Group (Delete)	-						O					
Target group start wait time	1800 seconds						O					
Property												
Wait Only when on the Same Server	Off						O					
Stop Dependency Tab												
Dependent Group (Add)	-						O					
Dependent Group (Delete)	-						O					
Target group stop wait time	1800 seconds						O					
Wait the Dependent Groups when a Cluster Stops	On											O
Wait the Dependent Groups when a Server Stops	Off											O
Wait the Dependent Groups when a Group Stops	Off						O					

Group Resource (Common)

		How to change										
Parameters	**Default**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Add Group Resource[11]	-				O		O					
Remove Group Resource	-					O	O					
Add Group Resource (Mirror Disk Resource, Hybrid Disk Resource)			O									
Remove Group Resource (Mirror Disk Resource, Hybrid Disk Resource)			O									
Group Resource Common Properties												
Info Tab												
Name	Each resource default value				O		O					
Name (Mirror Disk Resource, Hybrid Disk Resource)	Each resource default value		O									
Comment	-											O
Recovery Operation												
Execute Script before or after Activation or Deactivation												
Execute Script before Activation	Off											O
Execute Script after Activation	Off											O
Execute Script before Deactivation	Off											O
Execute Script after Deactivation	Off											O
Edit Script												
Select User Application Enter application path (Edit)	-											O
Select Script created with this product Script content (Edit)	-											O

Timeout	30 seconds											O
Edit Script before Final Action												
Select User Application Enter application path (Edit)	-											O
Select Script created with this product Script content (Edit)	-											O
Timeout	5 seconds											O

[11] You can add a resource to support dynamic resource addition without stopping the group. For details, refer to “Adding a resource without stopping the group” in “The system maintenance information” in the Maintenance guide.

Exec resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Exec Resource Properties												
Dependency Tab												
Follow the default dependence	On • floating IP resources • virtual IP resources • disk resources • mirror disk resources • hybrid disk resources • NAS resources • Dynamic DNS resource • Volume manager resource • AWS elastic ip resource • AWS virtual ip resource • AWS DNS resource • Azure probe port resource • Azure DNS resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	zero						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Not activate next resources)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster daemon and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
Type (User Application, Script Created with this product)	Script Created with this product											O
User Application Enter the application path (Edit)	-											O
Script Created with this product Script codes (Edit)	-											O
Exec Resource Tuning Properties												
Parameter Tab												
Start Script Synchronous, Asynchronous	Synchronous					O						
Start Script Timeout	1800 seconds						O					
Start Script Execute on standby server	Off					O						
Start Script Timeout (on standby server)	10 seconds						O					
Stop Script Synchronous, Asynchronous	Synchronous											O
Stop Script Timeout	1800 seconds						O					
Stop Script Execute on standby server	Off											O
Stop Script Timeout (on standby server)	10 seconds						O					
Maintenance Tab												

Log Output Path	Blank (/dev/null)											O
Rotate Log	Off					O						
Rotation Size	1000000					O						

Disk resource

		How to change										
Parameters	**Default**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Disk Resource Properties												
Dependency Tab												
Follow the default dependence	On • floating IP resources • virtual IP resources • Dynamic DNS resource • Volume manager resource • AWS elastic ip resource • AWS virtual ip resource • AWS DNS resource • Azure probe port resource • Azure DNS resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	zero						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Not activate next resources)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
Device Name	-					O						
Raw Device Name	-					O						
Mount Point	-					O						
File System	-											O
Disk Type	disk					O						
Disk Resource Tuning Properties												
Mount Tab												
Mount Option	rw											O
Timeout	180 seconds						O					
Retry Count	3 times						O					
Unmount Tab												
Timeout	120 seconds						O					
Retry Count	3 times						O					
Retry Interval	5 seconds						O					
Forced operation when failure is detected	kill											O
Fsck Tab (when other than xfs is selected for File System)												
fsck Option	-y											O
fsck Timeout	7200 seconds						O					
fsck Action Before Mount	Execute at Specified Count											O
Count	10 times											O
fsck Action When Mount Failed Execute	On											O
Rebuilding of reiserfs	Off						O					
xfs_repair Tab (when xfs is selected for File System)												
xfs_repair Option	-											O
xfs_repair Timeout	7200 seconds						O					
xfs_repair Action When Mount Failed Execute	Off											O

Floating IP resource

		How to change										
Parameters	**Default**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
FIP Resource Tuning Properties												
Dependency Tab												
Follow the default dependence	On (No default is set)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					

Final Action at Activation Failure	No Operation (Next resources are not activated).						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
IP Address	-					O						
FIP Resource Tuning Properties												
Parameter Tab												
Ifconfig Timeout	60 seconds						O					
ping Interval	1 second						O					
ping Timeout	1 second						O					
ping Retry Count	zero						O					
ping Forced FIP Activation	Off											O
ARP Send Count	1 time						O					
Judge NIC Link Down as Failure	Off						O					
Deactivity Check Tab												
Confirm I/F Deletion	On											O
Status at Failure	Not Failure											O
Confirm I/F Response	On											O
Status at Failure	Not Failure											O

Virtual IP resource

		How to change										
Parameters	**Default**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Virtual IP Resource Properties												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	1 time						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Next resources are not activated).						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	1 time						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
IP Address	-					O						
NIC Alias Name	-					O						
Destination IP Address	-					O						
Source IP Address	-					O						
Send Interval	10 seconds					O						
Use Routing Protocol	-					O						
Virtual IP Resource Tuning Properties												
Parameter Tab												
ifconfig Timeout	60 seconds						O					
Ping Interval	1 second						O					
Ping Timeout	1 second						O					
Ping Retry Count	Zero						O					
Ping Forced VIP Activation	Off											O
ARP Send Count	1 time						O					
Judge NIC Link Down as Failure	Off						O					
Deactivity Check Tab												
Confirm I/F Deletion	On											O
Status at Failure	Not Failure											O
Confirm I/F Response	On											O
Status at Failure	Not Failure											O
RIP Tab												
Next Hop IP Address	-					O						
Metric	1					O						
Port Number	520					O						
RIPng Tab												
Metric	1					O						
Port Number	521					O						

NAS resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
NAS Resource Properties												
Dependency Tab												
Follow the default dependence	On • floating IP resources • virtual IP resources • Dynamic DNS resources • AWS elastic ip resource • AWS virtual ip resource • AWS DNS resource • Azure probe port resource • Azure DNS resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	zero						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Next resources are not activated).						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
Server Name	-					O						
Shared Name	-					O						
Mount Point	-					O						
File System	nfs											O
NAS Resource Tuning Properties												
Mount Tab												
Mount Option	rw											O
Timeout	60 seconds						O					
Retry Count	3 times						O					
Unmount Tab												
Timeout	60 seconds						O					
Retry Count	3 times						O					
Retry Interval	5 seconds						O					
Forced operation when failure is detected	kill											O
NAS Tab												
ping Timeout	10 seconds						O					

Mirror disk resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Mirror Disk Resource Properties [12]												
Dependency Tab												
Follow the default dependence	On • floating IP resources • virtual IP resources • AWS elastic ip resource • AWS virtual ip resource • AWS DNS resource • Azure probe port resource • Azure DNS resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	Zero						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Not activate next resource)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	Zero						O					

Final Action at Deactivation Failure	Stop the cluster service and shutdown OS						O					
Execute Script before Final Action	Off											O
Details Tab												
Mirror Partition Device Name	/dev/NMP1~		O									
Mount Point	-		O									
Data Partition Device Name	-		O									
Cluster Partition Device Name	-		O									
File System	ext3		O									
Selection of Mirror Disk Connect												
Mirror Disk Connect Tab												
I/F No. (Add, Remove)	Top two I/F No. on the mirror disk connect I/F tab of the server properties		O									
Mirror Disk Resource Tuning Properties												
Mount Tab												
Mount Option	rw		O									
Timeout	120 seconds						O					
Retry Count	3 times						O					
Unmount Tab												
Timeout	120 seconds						O					
Retry Count	3 times						O					
Retry Interval	5 seconds						O					
Forced operation when failure is detected	kill											O
Fsck Tab (when other than xfs is selected for File System)												
fsck Option	-y											O
fsck Timeout	7200 seconds						O					
fsck Action Before Mount	Execute at Specified Count											O
Count	10 times											O
fsck Action When Mount Failed	Execute											O
Rebuilding of Reiserfs	Off						O					
xfs_repair Tab (when xfs is selected for File System)												
xfs_repair Option	-											O
xfs_repair Timeout	7200 seconds						O					
xfs_repair Action When Mount Failed Execute	Off											O
Mirror Tab												
Execute the initial mirror construction	On (valid only for the initial mirror construction)											
Execute initial mkfs	On (valid only for the initial mirror construction)											
Perform Data Synchronization	On		O									
Mode	Synchronous		O									
Number of Queues	Set Number 2048		O									
Rate limitation of Mirror Connect	Off (Unlimited)		O									
History Files Store Directory	Blank		O									
Size Limitation of History File	0 megabytes (Unlimited)		O									
Compress data	Off		O									
Compress data when recovering	Off		O									
Mirror Driver Tab												
Mirror Data Port Number	29051~		O									
Heartbeat Port Number	29031~		O									
ACK2 Port Number	29071~		O									
Send Timeout	30 seconds		O									
Connection Timeout	10 seconds		O									
Ack Timeout	100 seconds		O									
Receive Timeout	100 seconds		O									
Heartbeat Interval	10 seconds		O									
ICMP Echo Reply Receive Timeout	2 seconds		O									
ICMP Echo Request Retry Count	8 times		O									
High Speed SSD Tab												
Data Partition	Off		O									
Cluster Partition	Off		O									

[12] It does not apply to PPC64 and PPC64LE.

Hybrid disk resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Hybrid Disk Resource Properties [13]												
Dependency Tab												
Follow the default dependence	On • floating IP resources • virtual IP resources • AWS elastic ip resource • AWS virtual ip resource • AWS DNS resource • Azure probe port resource • Azure DNS resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	Zero						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Not activate next resource)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	Zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shutdown OS						O					
Execute Script before Final Action	Off											O
Details Tab												
Mirror Partition Device Name	/dev/NMP1~		O									
Mount Point	-		O									
Data Partition Device Name	-		O									
Cluster Partition Device Name	-		O									
File System	ext3		O									
Selection of Mirror Disk Connect												
Mirror Disk Connect Tab												
I/F No. (Add, Remove)	Top two I/F No. on the mirror disk connect I/F tab of the server properties		O									
Hybrid Disk Resource Tuning Properties												
Mount Tab												
Mount Option	rw		O									
Timeout	120 seconds						O					
Retry Count	3 times						O					
Unmount Tab												
Timeout	120 seconds						O					
Retry Count	3 times						O					
Retry Interval	5 seconds						O					
Forced operation when error is detected	kill											O
Fsck Tab (when other than xfs is selected for File System)												
fsck Option	-y											O
fsck Timeout	7200 seconds						O					
fsck Action Before Mount	Execute at Specified Count											O
Count	10 times											O
fsck Action When Mount Failed	Execute											O
Rebuilding of reiserfs	Off						O					
xfs_repair Tab (when xfs is selected for File System)												
xfs_repair Option	-											O
xfs_repair Timeout	7200 seconds						O					
xfs_repair Action When Mount Failed Execute	Off											O
Mirror Tab												
Execute the initial mirror construction	On (valid only for the initial mirror construction)											
Perform Data Synchronization	On		O									
Mode	Synchronous		O									
Number of Queues	Set Number 2048		O									
Rate limitation of Mirror Connect	Off (Unlimited)		O									
History Files Store Directory	Blank		O									
Size Limitation of History File	0 megabytes (Unlimited)		O									
Compress data	Off		O									
Compress data when recovering	Off		O									
Mirror Driver Tab												
Mirror Data Port Number	29051~		O									
Heartbeat Port Number	29031~		O									
ACK2 Port Number	29071~		O									

Send Timeout	30 seconds		O									
Connection Timeout	10 seconds		O									
Ack Timeout	100 seconds		O									
Receive Timeout	100 seconds		O									
Heartbeat Interval	10 seconds		O									
ICMP Echo Reply Receive Timeout	2 seconds		O									
ICMP Echo Request Retry Count	8 times		O									
High Speed SSD Tab												
Data Partition	Off		O									
Cluster Partition	Off		O									

[13] It does not apply to PPC64 and PPC64LE.

Volume manager resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Volume Manager Resource Properties												
Dependency Tab												
Follow the default dependence	On • Floating IP resources • Virtual IP resources • Dynamic DNS resources • AWS elastic ip resource • AWS virtual ip resource • AWS DNS resource • Azure probe port resource • Azure DNS resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Activation Retry Threshold	0 times						O					
Maximum Failover Count	One time						O					
Final Action at Activation Failure	No operation (Do not activate the next resource.)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	0 times						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down the OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
Volume Manager	LVM					O						
Target Name	-					O						
Volume Manager Resource Tuning Properties (When other than [zfspool] is selected for [Volume Manager])												
Import Tab												
Import Timeout	300 seconds						O					
Start Volume Timeout	60 seconds						O					
Volume Status Check Timeout	60 seconds						O					
Clear Host ID	On						O					
Force Option at Import	On						O					
Export Tab												
Stop Volume Timeout	60 seconds						O					
Flush Timeout	60 seconds						O					
Export Timeout	300 seconds						O					
Volume Status Check Timeout	60 seconds						O					
Volume Manager Resource Tuning Properties (When [zfspool] is selected for [Volume Manager])												
Import Tab												
Import Timeout	300 seconds						O					
Forced Import	On						O					
Execute Ping Check	On						O					
Export Tab												
Export Timeout	300 seconds						O					
Forced Export	On						O					

VM resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
VM Resource Properties[14]												
Dependency Tab												
Follow the default dependence	On •disk resource •mirror disk resource •hybrid disk resource •NAS resource •Volume manager resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Activation Retry Threshold	0 times						O					
Maximum Failover Count	One time						O					
Final Action at Activation Failure	No operation (Do not activate the next resource.)						O					
Execute Script before Final Action	Off											O
Deactivation Retry Threshold	0 times						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down the OS.						O					
Execute Script before Final Action	Off											O
Details Tab (when the virtual machine type is vSphere and the cluster service installation destination is host OS)												
Virtual Machine Name	-					O	O					
Data Store Name	-						O					
VM Configuration File Path	-					O	O					
IP Address of Host	-						O					
User Name	-						O					
Password	-						O					
Use vCenter	Off						O					
vCenter	-						O					
User Name for vCenter	-						O					
Password for vCenter	-						O					
Resource Pool Name	-						O					
Details Tab (when the virtual machine type is vSphere and the cluster service installation destination is guest)												
Virtual Machine Name	-					O	O					
Data Store Name	-						O					
IP Address of Host	-						O					
User Name	-						O					
Password	-						O					
Use vCenter	On (uneditable)						O					
vCenter	-						O					
User Name for vCenter	-						O					
Password for vCenter	-						O					
Resource Pool Name	-						O					
Details Tab (when the virtual machine type is XenServer)												
Virtual Machine Name	-					O	O					
UUID	-					O	O					
Library Path	-					O	O					
User Name	-						O					O
Password	-						O					O
Details Tab (when the virtual machine type is KVM)												
Virtual Machine Name	-					O	O					
UUID	-					O	O					
Library Path	-					O	O					
VM Resource Tuning Properties												
Parameter Tab												
Request Timeout	30 seconds						O					
Virtual Machine Start Waiting Time	0 seconds						O					
Virtual Machine Stop Waiting Time	240 seconds						O					

[14] It does not apply to PPC64 and PPC64LE.

Dynamic DNS resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Dynamic DNS Resource Properties												
Dependency Tab												
Follow the default dependence	On • Floating IP resources • Virtual IP resource3s • AWS elastic ip resource • AWS virtual ip resource • Azure probe port resource						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Activation Retry Threshold	One time						O					
Maximum Failover Count	One time						O					
Final Action at Activation Failure	No operation (Do not activate the next resource.)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	One time						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down the OS						O					
Execute Script before Final Action	Off											O
Details Tab												
Virtual Host Name	-					O						
IP Address	-					O						
DDNS Server	-					O						
Port No.	53					O						
Authentication Key Name	-					O						
Authentication Key Value	-					O						

AWS Elastic IP resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS elastic ip Resource Properties[15]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Next resources are not activated.)						O					
Execute Script before Final Action at Activation Failure	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action at Deactivation Failure	Off											O
Details Tab												
EIP ALLOCATION ID	-					O						
ENI ID	-					O						
AWS elastic ip Resource Tuning Properties												
Parameter Tab												
AWS CLI Timeout	100 seconds					O						

[15] It does not apply to PPC64 and PPC64LE.

AWS Virtual IP resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS virtual ip Resource Properties[16]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					

Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Next resources are not activated.)						O					
Execute Script before Final Action at Activation Failure	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action at Deactivation Failure	Off											O
Details Tab												
IP Address	-					O						
VPC ID	-					O						
ENI ID	-					O						
AWS virtual ip Resource Tuning Properties												
Parameter Tab												
AWS CLI Timeout	100 seconds					O						

[16] It does not apply to PPC64 and PPC64LE.

AWS DNS resource

Parameter	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS DNS Resource Properties[17]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Next resources are not activated.)						O					
Execute Script before Final Action at Activation Failure	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster service and shut down OS						O					
Execute Script before Final Action at Deactivation Failure	Off											O
Details Tab												
Hosted Zone ID	-					O						
Resource Record Set Name	-					O						
IP Address	-					O						
TTL	300 seconds					O						
Delete a resource record set at deactivation	On											O
AWS DNS Resource Tuning Properties												
Parameter Tab												
AWS CLI Timeout	100 seconds											O

[17] It does not apply to PPC64 and PPC64LE.

Azure probe port resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Azure probe port Resource Properties[18]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					

Final Action at Activation Failure	No Operation (Not activate next resources)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster daemon and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
Probeport	-					O						
Azure probe port Resource Tuning Properties												
Parameter Tab												
Probe wait timeout	30 seconds					O						

[18] It does not apply to PPC64 and PPC64LE.

Azure DNS resource

Parameter	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Azure DNS Resource Properties[19]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	1 time						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (not activate next resource)						O					
Execute Script before Final Action at Activation Failure	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure Detection	Stop the cluster service and shut down OS.						O					
Execute Script before Final Action at Deactivation Failure	Off											O
Details Tab												
Record Set Name	-					O						
Zone Name	-					O						
IP Address	-					O						
TTL	3600 seconds					O						
Resource Group Name	-					O						
User URI	-					O						
Tenant ID	-					O						
File Path of Service Principal	-					O						
Thumbprint of Service Principal	-					O						
Azure CLI File Path	-					O						
Delete a record set at deactivation	On											O
Azure DNS Resource Tuning Properties												
Parameter Tab												
Azure CLI Timeout	100 seconds											O

[19] It does not apply to PPC64 and PPC64LE.

Google Cloud Virtual IP resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Google Cloud Virtual IP Resource Properties[20]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Not activate next resources)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster daemon and shut down OS.						O					

Execute Script before Final Action	Off											O
Details Tab												
Port Number	-					O						
Google Cloud Virtual IP Resource Tuning Properties												
Parameter Tab												
Health check timeout	30 seconds					O						

[20] It does not apply to PPC64 and PPC64LE.

Oracle Cloud Virtual IP resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Oracle Cloud Virtual IP Resource Properties[21]												
Dependency Tab												
Follow the default dependence	On (No default dependence)						O					
Dependent Resources (Add, Remove)	-						O					
Recovery Operation Tab												
Retry Count at Activation Failure	5 times						O					
Maximum Failover Count	1 time						O					
Final Action at Activation Failure	No Operation (Not activate next resources)						O					
Execute Script before Final Action	Off											O
Retry Count at Deactivation Failure	zero						O					
Final Action at Deactivation Failure	Stop the cluster daemon and shut down OS.						O					
Execute Script before Final Action	Off											O
Details Tab												
Port Number	-					O						
Oracle Cloud Virtual IP Resource Tuning Properties												
Parameter Tab												
Health check timeout	30 seconds					O						

[21] It does not apply to PPC64 and PPC64LE.

Monitor resource (common)

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Add monitor resource	-						O					
Remove Monitor Resource	-						O					
Monitor Resources Common Properties												
Info Tab												
Name	-						O					
Comment	-											O
Recovery Action Tab												
Edit Script												
Select User Application Enter application path (Edit)	-											O
Select Script created with this product Script content (Edit)	-											O
Timeout	5 secconds											O

Disk monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Disk Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	One time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					

Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					
Monitor(special) Tab												
Method	READ(O_DIRECT)											O
Monitor Target	-											O
Monitor Target RAW Device Name	-											O
I/O size	512 bytes											O
Action When Diskfull is Detected	The recovery action enabled											O

IP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
IP Monitor Resource Properties												
Monitor(common)Tab												
Interval	30 seconds						O					
Timeout	30 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
IP Address(Add, Remove, Edit)	-											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

Virtual IP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Virtual IP Monitor Resource Properties [22]												
Monitor(common)												
Interval	3 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	Virtual IP resource name						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Recovery Action Tab												
Recovery Target	Virtual IP resource name						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					

Maximum Failover Count	1 time						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[22] You can upload the data if a cluster is suspended. However, you need to stop and resume the cluster to apply the changed setting.

PID monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Pid Monitor Resource Properties												
Monitor(common)Tab												
Interval	5 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	3 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

User mode monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
User mode Monitor Resource Properties												
Monitor(common) Tab												
Interval	3 seconds						O					
Timeout	90 seconds						O					
Wait Time to Start Monitoring	0 seconds						O					
Nice Value	-20						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Use heartbeat interval and timeout	On						O					
Method	keepalive						O					
Operation at Timeout Detection	RESET						O					
Open/Close Temporary File	Off						O					
Write	Off						O					
Size	10000 bytes						O					
Create Temporary Thread	Off						O					

NIC Link Up/Down monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
NIC Link Up/Down Monitor Resource Properties												
Monitor(common) Tab												
Interval	10 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	3 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					

Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Recovery Target	-											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	zero						O					
Execute Script before Failover	Off											O
Execute migration before Failover	off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

Multi target monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Multi Target Monitor Resource Properties												
Monitor(common) Tab												
Interval	30 seconds						O					
Timeout	30 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Monitor(special) Tab												
Recovery Target	-											O
Multi Target Monitor Resource Tuning Properties												
Parameter Tab												
Error Threshold	Same as Number of Members											O
Specify Number	64											O
Warning Threshold	Off											O
Specify Number	-											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

Mirror disk monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Mirror Disk Monitor Resource Properties [23]												
Monitor(common) Tab												
Interval	10 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Monitor(special) Tab												
Mirror Disk Resource	Mirror disk resource name											O
Recovery Action Tab												
Execute Script before Final Action	Off											O

[23] It does not apply to PPC64 and PPC64LE.

Mirror disk connect monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11

Mirror Disk Connect Monitor Resource Properties [24]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Monitor(special) Tab												
Mirror Disk Resource	Mirror disk resource name											O
Recovery Action Tab												
Execute Script before Final Action	Off											O

[24] It does not apply to PPC64 and PPC64LE.

Hybrid disk monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Hybrid Disk Monitor Resource Properties [25]												
Monitor(common) Tab												
Interval	10 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Monitor(special) Tab												
Hybrid Disk Resource	Hybrid disk resource name											O
Recovery Action Tab												
Execute Script before Final Action	Off											O

[25] It does not apply to PPC64 and PPC64LE.

Hybrid disk connect monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Hybrid Disk Connect Monitor Resource Properties [26]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Monitor(special) Tab												
Hybrid Disk Resource	Hybrid disk resource name											O
Recovery Action Tab												
Execute Script before Final Action	Off											O

[26] It does not apply to PPC64 and PPC64LE.

ARP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
ARP Monitor Resource Properties												
Monitor(common) Tab												
Interval	30 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					

Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Monitor(special) Tab												
Target Resource	-						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

Custom monitor resource

Parameters	Default	How to change 1	2	3	4	5	6	7	8	9	10	11
Custom Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitor Script Path Type	Script created with this product						O					
Monitor Script Type	Synchronous						O					
Wait a period of time for Application/Script monitor to start	0											O
Log Output Path	Blank (/dev/null)						O					
Rotate Log	Off						O					
Rotation Size	1000000						O					
Normal Return Value of Monitor Script	0						O					
Wait for activation monitoring to stop before stopping the cluster	Off											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop group						O					

Volume manager monitor resource

Parameters	Default	How to change 1	2	3	4	5	6	7	8	9	10	11
Volume Manager Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	1						O					
Wait Time to Start Monitoring	0 seconds						O					

Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Volume Manager	LVM						O					
Target Name	-											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is not a cluster)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	0 times (if the recovery target is not a cluster)						O					
Execute Script before Final Action	On											O
Final Action	No action is taken.						O					

VM monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
VM Monitor Resource Properties[27]												
Monitor(common) Tab												
Interval	10 seconds						O					
Timeout	30 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Wait Time When External Migration Occurs	15 seconds											
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time						O					
Execute Script before Final Action	On											O
Final Action	No action is taken.						O					

[27] It does not apply to PPC64 and PPC64LE.

Message receive monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Message Receive Monitor Resource Properties												
Monitor(common) Tab												
Interval	10 seconds						O					
Timeout	30 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Category	NIC						O					
Keyword	-						O					
Change the monitor status to abnormal as a result of a predictive failure detected by BMC	Off						O					
Change the monitor status to abnormal as a result of a performance deterioration failure	Off						O					
Recovery Action Tab												

Recovery Action	Run failover for recovery target						O					
Recovery Target	-						O					
Execute migration before Failover	Off						O					
Execute Failover to outside the Server Group	Off						O					
Execute Script before Recovery Action	Off											O
Final Action	No Operation						O					

Dynamic DNS monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Dynamic DNS Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	Dynamic DNS resource name						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Recovery Action Tab												
Recovery Target	Dynamic DNS resource name						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Three times						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	One time (if the recovery target is not a cluster)						O					
Execute Script before Final Action	Off											O
Final Action	No action is taken.						O					

Process name monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Process Monitor Resource Properties												
Monitor(common) tab												
Interval	5 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	3 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Process name	-						O					
Minimum Monitored Process Count	1						O					
Recovery Action tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (When the recovery target is other than the cluster)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

BMC monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
BMC Monitor Resource Properties[28]												
Monitor (common) Tab												
Interval	5 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Recovery Action Tab												
Recovery Action	Final action only						O					
Recovery Target	LocalServer						O					
Recovery Script Execution Count	-						O					
Execute Script before Reactivation	-											O
Maximum Reactivation Count	-						O					
Execute Script before Failover	-											O
Execute migration before Failover	-						O					
Maximum Failover Count	-						O					
Execute Script before Final Action	Off											O
Final Action	I/O fencing						O					

[28] It does not apply to PPC64 and PPC64LE.

DB2 monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
DB2 Monitor Resource Properties[29]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitor Level	Level 2 (monitoring by update/select)						O					
Database Name	-						O					
Instance	db2inst1						O					
User Name	db2inst1						O					
Password	-						O					
Table	db2watch						O					
Character Set	ja_JP.eucJP						O					
Library Path	/opt/ibm/db2/V11.1/lib64/libdb2.so						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster daemon and shutdown OS						O					

[29] It does not apply to PPC64LE.

FTP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
FTP Monitor Resource Properties[30]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	3 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
IP Address	127.0.0.1											O
Port Number	21											O
User Name	-											O
Password	-											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[30] It does not apply to PPC64 and PPC64LE.

HTTP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
HTTP Monitor Resource Properties[31]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	10 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	3 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Connecting Destination	localhost											O
Port	80											O
Request URI	-											O
Protocol	HTTP											O
User Name	-											O
Password	-											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O

Final Action	Stop cluster service and shutdown OS						O					

[31] It does not apply to PPC64 and PPC64LE.

IMAP4 monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
IMAP4 Monitor Resource Properties[32]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	3 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
IP Address	127.0.0.1											O
Port Number	3306											O
User Name	-											O
Password	-											O
Authentication Method	AUTHENTICATE LOGIN											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[32] It does not apply to PPC64 and PPC64LE.

MySQL monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
MySQL Monitor Resource Properties[33]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitor Level	Level 2 (monitoring by update/select)						O					
Database Name	-						O					
IP Address	127.0.0.1						O					
Port	3306						O					
User Name	-						O					
Password	-						O					
Table	mysqlwatch						O					
Storage Engine	InnoDB						O					
Library Path	/usr/lib64/mysql/libmysqlclient.so.20						O					

Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[33] It does not apply to PPC64 and PPC64LE.

NFS monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
NFS Monitor Resource Properties[34]												
Monitor(common) Tab												
Interval	30 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	5 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Share Directory	-											O
NFS Server	127.0.0.1											O
NFS Version	v2											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[34] It does not apply to PPC64 and PPC64LE.

ODBC monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
ODBC Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					

Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Monitor Level	Level 2 (monitoring by update/select)						O					
Database Name	-						O					
User Name	-						O					
Password	-						O					
Table	odbcwatch						O					
Message Character Set	UTF-8						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

Oracle monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Oracle Monitor Resource Properties[35]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Monitor Type	listener and instance monitor						O					
Monitor Level	Level 2 (monitoring by update/select)						O					
Connect Command	-						O					
User Name	sys						O					
Password	-						O					
Authority Method	SYSDBA						O					
Table	orawatch						O					
ORACLE_HOME	-						O					
Character Set	-						O					
Library Path	/u01/app/oracle/product/12.2.0/dbhome_1/lib/libclntsh.so.12.1						O					
Collect detailed application information at failure occurrence	disabled						O					
Collection Timeout	600 seconds						O					
Set error during Oracle initialization or shutdown	disabled						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[35] It does not apply to PPC64LE.

Oracle Clusterware Synchronization Management monitor resource[36]

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Oracle Clusterware Synchronization Management Monitor Resource Properties[37]												
Monitor (common) Tab												
Interval	5 seconds						O					
Timeout	10 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Recovery Action Tab												
Recovery Action	Final action only						O					
Recovery Target	LocalServer						O					
Recovery Script Execution Count	-						O					
Execute Script before Reactivation	-											O
Maximum Reactivation Count	-						O					
Execute Script before Failover	-											O
Execute migration before Failover	-						O					
Maximum Failover Count	-						O					
Execute Script before Final Action	Off											O
Final Action	No operation						O					

[36] It does not apply to PPC64 and PPC64LE.
[37] It does not apply to PPC64 and PPC64LE.

POP3 monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
POP3 Monitor Resource Properties[38]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	3 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
IP Address	127.0.0.1											O
Port Number	110											O
User Name	-											O
Password	-											O
Authentication Method	APOP											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[38] It does not apply to PPC64 and PPC64LE.

PostgreSQL monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
PostgreSQL Monitor Resource Properties[39]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitor Level	Level 2 (monitoring by update/select)						O					
Database Name	-						O					
IP Address	127.0.0.1						O					
Port	5432						O					
User Name	postgres						O					
Password	-						O					
Table	psqlwatch						O					
Library Path	/opt/PostgreSQL/10/lib/libpq.so.5.10						O					
Set error during PostgreSQL initialization or shutdown	On						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[39] It does not apply to PPC64LE.

Samba monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Samba Monitor Resource Properties[40]												
Monitor(common) Tab												
Interval	30 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	5 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Share Name	-											O
IP Address	127.0.0.1											O
Port	139											O
User Name	-											O
Password	-											O
Recovery Action Tab												
Recovery Target	-						O					

Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[40] It does not apply to PPC64 and PPC64LE.

SMTP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
SMTP Monitor Resource Properties[41]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	3 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
IP Address	127.0.0.1											O
Port	25											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[41] It does not apply to PPC64 and PPC64LE.

SQL Server monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
SQL Server Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Monitor Level	Level 2 (monitoring by update/select)						O					
Database Name	-						O					
Server Name	Localhost						O					
User Name	SA						O					

Password	-						O					
Table	sqlwatch						O					
ODBC Driver Name	ODBC Driver 13 for SQL Server						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

Sybase monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Sybase Monitor Resource Properties[42]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Monitor Level	Level 2 (monitoring by update/select)						O					
Database Name	-						O					
Database Server Name	-						O					
User Name	sa						O					
Password	-						O					
Table	sybwatch						O					
Library Path	/opt/sap/OCS-16_0/lib/libsybdb64.so						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[42] It does not apply to PPC64 and PPC64LE.

Tuxedo monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Tuxedo Monitor Resource Properties[43]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					

Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Application Server Name	BBL											O
Config File	-											O
Library Path	/home/Oracle/tuxedo/tuxedo12.1.3.0.0/lib/libtux.so											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[43] It does not apply to PPC64 and PPC64LE.

Weblogic monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Weblogic Monitor Resource Properties[44]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
IP Address	127.0.0.1											O
Port	7002											O
Account Shadow	Off											O
On Config File	-											O
On Key File	-											O
Off User Name	weblogic											O
Off Password	weblogic											O
Authority Method	DemoTrust											O
Key Store File	-											O
Domain Environment File	/home/Oracle/product/Oracle_Home/user_projects/domains/base_domain/bin/setDomainEn											O
Additional Command Option	-Dwlst.offline.log=disable -Duser.language=en_U											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[44] It does not apply to PPC64 and PPC64LE.

Websphere monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Websphere Monitor Resource Properties[45]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	2 times						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Application Server Name	server1											O
Profile Name	default											O
User Name	-											O
Password	-											O
Install Path	/opt/IBM/WebSphere/AppServer											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[45] It does not apply to PPC64 and PPC64LE.

WebOTX monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Tuxedo Monitor Resource Properties[46]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	120 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)							O					
Monitor(special) Tab												
Connecting Destination	localhost											O
Port	6212											O
User Name	-											O
Password	-											O
Install Path	/opt/WebOTX											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	Zero (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O

Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Stop cluster service and shutdown OS						O					

[46] It does not apply to PPC64 and PPC64LE.

JVM monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
JVM Monitor Resource Properties[47]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump files of the monitor process at timeout occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Target	-						O					
JVM Type	-						O					
Identifier	-						O					
Connection Port	-						O					
Process Name	-						O					
User	-						O					
Password	-						O					
Command	-						O					
Memory Tab (when Oracle Java is selected for JVM Type)												
Monitor Heap Memory Rate	On						O					
Total Usage	80[%]						O					
Eden Space	100[%]						O					
Survivor Space	100[%]						O					
Tenured Gen	80[%]						O					
Monitor Non-Heap Memory Rate	On						O					
Total Usage	80[%]						O					
Code Cache	100[%]						O					
Perm Gen	80[%]						O					
Perm Gen[shared-ro]	80[%]						O					
Perm Gen[shared-rw]	80[%]						O					
Command	-						O					
Memory Tab (when Oracle JRockit is selected for JVM Type)												
Monitor Heap Memory Rate	On						O					
Total Usage	80[%]						O					
Nursery Space	80[%]						O					
Old Space	80[%]						O					
Monitor Non-Heap Memory Rate	On						O					
Total Usage	80[%]						O					
Class Memory	100[%]						O					
Command	-						O					
Memory Tab(when Oracle Java(usage monitoring) is selected for JVM Type)												
Monitor Heap Memory Usage	Off						O					
Total Usage	0 megabytes						O					
Eden Space	0 megabytes						O					
Survivor Space	0 megabytes						O					
Tenured Gen(Old Gen)	0 megabytes						O					
Monitor Non-Heap Memory Usage	Off						O					
Total Usage	0 megabytes						O					
Code Cache	0 megabytes						O					
CodeHeap non-nmethods	0 megabytes						O					
CodeHeap profiled	0 megabytes						O					
CodeHeap non-profiled	0 megabytes						O					
Compressed Class Space	0 megabytes						O					
Metaspace	0 megabytes						O					
Command	-						O					
Thread Tab												
Monitor the number of Active Threads	65535 threads						O					
Command	-						O					
GC Tab												
Monitor the time in Full GC	65535 milliseconds						O					

Monitor the count of Full GC execution	1 time						O					
Command	-						O					
WebLogic Tab												
Monitor the requests in Work Manager	Off						O					
Target Work Managers	-						O					
The number	65535						O					
Average	65535						O					
Increment from the last	80[%]						O					
Monitor the requests in Thread Pool	On						O					
Waiting Requests, The number	65535						O					
Waiting Requests, Average	65535						O					
Waiting Requests, Increment from the last	80[%]						O					
Executing Requests, The number	65535						O					
Executing Requests, Average	65535						O					
Executing Requests, Increment from the last	80[%]						O					
Command	-						O					
Load Balancer Linkage												
Memory Pool Monitor	Off						O					
Disconnect Failure Node Dynamically	Off						O					
Reboot Command	-						O					
Timeout	3600						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	0 time (when the recovery target is other than the						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (when the recovery target is other than the						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[47] It does not apply to PPC64 and PPC64LE.

System monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
System Monitor Resource Properties[48]												
Monitor(common) Tab												
Interval	30 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitoring CPU usage	ON						O					
CPU usage	90[%]						O					
Duration time	60 minutes						O					
Monitoring total usage of memory	ON						O					
Total usage of memory	90[%]						O					
Duration time	60 minutes						O					
Monitoring total usage of virtual memory	ON						O					
Total usage of virtual memory	90[%]						O					
Duration Time	60 minutes						O					
Monitoring total number of opening files	ON						O					
Total number of opening files (in a ratio comparing with the system upper limit)	90[%]						O					
Duration time	60 minutes						O					
Monitoring total number of running threads	ON						O					
Total number of running threads	90[%]						O					
Duration time	60 minutes						O					
Monitoring number of running processes for each user	ON						O					

Number of running processes for each user	90[%]						O					
Duration time	60 minutes						O					
Mount point							O					
Utilization rate	ON						O					
Warning level	90%						O					
Notice level	80%						O					
Duration time	1440 minutes						O					
Free space	ON						O					
Warning level	500 MB						O					
Notice level	1000 MB						O					
Duration time	1440 minutes						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	0 times (when the recovery target is other than the						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	0 times (when the recovery target is other than the						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[48] It does not apply to PPC64 and PPC64LE.

Process resource monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Process Resource Monitor Resource Properties[49]												
Monitor(common) Tab												
Interval	30 seconds						O					
Timeout	60 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	Off						O					
Do not Execute Recovery Action at Timeout Occurrence	Off						O					
Retry Count	zero						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitoring CPU usage	ON						O					
CPU usage	90[%]						O					
Duration time	1440 minutes						O					
Monitoring total usage of memory	ON						O					
Rate of Increase from the First Monitoring Point	10[%]						O					
Duration time	1440 minutes						O					
Monitoring number of opening files(maximum number)	ON						O					
Refresh Count	1000 times						O					
Monitoring number of opening files(kernel limit)	ON						O					
Ratio	90[%]						O					
Monitoring number of running threads	ON						O					
Duration time	1440 minutes						O					
Monitoring Zombie Processes	ON						O					
Duration time	1440 minutes						O					
Monitoring Processes of the Same Name	Off						O					
Count	100						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	0 times (when the recovery target is other than the						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	0 times (when the recovery target is other than the						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[49] It does not apply to PPC64 and PPC64LE.

Floating IP monitor resources

Parameter	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Floating IP Monitor Resource Properties												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump files of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Monitor NIC Link Up/Down	Off											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	0 times						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (when the recovery target is other than the cluster)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (when the recovery target is other than the cluster)						O					
Execute Script before Final Action	Off											O
Final Action	No operation						O					

AWS Elastic IP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS elastic IP Monitor Resource Properties[50]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	awseip						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can start (Add, Remove)	-						O					
Monitor(special) Tab												
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Do Operation						O					

[50] It does not apply to PPC64 and PPC64LE.

AWS Virtual IP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS virtual ip Monitor Resource Properties[51]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	awsvip						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can start (Add, Remove)	-						O					
Monitor(special) Tab												
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	Do Operation						O					

[51] It does not apply to PPC64 and PPC64LE.

AWS AZ monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS AZ Monitor Resource Properties[52]												
Monitor(common)Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed)						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the group (Add, Remove)	-						O					
Monitor(special) Tab												
Availability Zone	-						O					
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	0 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[52] It does not apply to PPC64 and PPC64LE.

AWS DNS monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
AWS DNS Monitor Resource Properties[53]												
Monitor (Common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	60 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	awsdns						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run (Add, Remove)	-						O					
Monitor (Special) Tab												
Monitor Resource Record Set	On											O
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)											O
Check Name Resolution	On											O
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[53] It does not apply to PPC64 and PPC64LE.

Azure probe port monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Azure probe port Monitor Resource Properties[54]												
Monitor (common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	azurepp						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Action when Probe port wait timeout	Disable recovery action(Display warning)						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[54] It does not apply to PPC64 and PPC64LE.

Azure load balance monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Azure load balance monitor resource Properties[55]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed))						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Target Resource	-						O					
Recovery Action Tab												
Recovery Target	-											
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[55] It does not apply to PPC64 and PPC64LE.

Azure DNS monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Azure DNS Monitor Resource Properties[56]												
Monitor (Common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	60 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	azuredns						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run (Add, Remove)	-						O					
Monitor (Special) Tab												
Check Name Resolution	On											O
Recovery Action Tab												
Recovery Action	azuredns						O					
Recovery Script Execution Count	0 time						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[56] It does not apply to PPC64 and PPC64LE.

Google Cloud Virtual IP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Google Cloud Virtual IP Monitor Resource Properties[57]												
Monitor (common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	gcvip						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Action when Health check wait timeout	Disable recovery action(Do nothing)						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[57] It does not apply to PPC64 and PPC64LE.

Google Cloud load balance monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Google Cloud load balance monitor resource Properties[58]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed))						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Target Resource	-						O					
Recovery Action Tab												
Recovery Target	-											
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[58] It does not apply to PPC64 and PPC64LE.

Oracle Cloud Virtual IP monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Oracle Cloud Virtual IP Monitor Resource Properties[59]												
Monitor (common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Active (fixed)						O					
Target Resource	ocvip						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Action when Health check wait timeout	Disable recovery action(Do nothing)						O					
Recovery Action Tab												
Recovery Target	-						O					
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[59] It does not apply to PPC64 and PPC64LE.

Oracle Cloud load balance monitor resource

Parameters	Default	How to change										
		1	2	3	4	5	6	7	8	9	10	11
Oracle Cloud load balance monitor resource Properties[60]												
Monitor(common) Tab												
Interval	60 seconds						O					
Timeout	180 seconds						O					
Collect the dump file of the monitor process at timeout occurrence	Off						O					
Do Not Retry at Timeout Occurrence	On						O					
Do not Execute Recovery Action at Timeout Occurrence	On						O					
Retry Count	1 time						O					
Wait Time to Start Monitoring	0 seconds						O					
Monitor Timing	Always (fixed))						O					
Target Resource	-						O					
Nice Value	0						O					
Failure Detection Server												
Failure Detection Server	All Servers						O					
Servers that can run the Group (Add, Remove)	-						O					
Monitor(special) Tab												
Target Resource	-						O					
Recovery Action Tab												
Recovery Target	-											
Recovery Script Execution Count	zero						O					
Execute Script before Reactivation	Off											O
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)						O					
Execute Script before Failover	Off											O
Execute migration before Failover	Off						O					
Maximum Failover Count	1 time (if the recovery target is other than clusters)						O					
Execute Script before Final Action	Off											O
Final Action	No Operation						O					

[60] It does not apply to PPC64 and PPC64LE.

2.9 Upper limits of registration

	version	You can register up to
Cluster	4.0.0-1 or later	1
Server	4.0.0-1 or later	32
Server group	4.0.0-1 or later	9
Group	4.0.0-1 or later	128
Group resource (Per group)	4.0.0-1 or later	256
Monitor resource	4.0.0-1 or later	512
Heartbeat resource	4.0.0-1 or later	128
BMC Heartbeat resource	4.0.0-1 or later	1
Witness heartbeat resource	4.0.0-1 or later	1
Oracle Clusterware Synchronization Management monitor resource	4.0.0-1 or later	1
Network partition resolution resource	4.0.0-1 or later	64
Mirror disk resources and hybrid disk resources (Per cluster) in total	4.0.0-1 or later	32
Mirror disk connect	4.0.0-1 or later	16
System monitor resource	4.0.0-1 or later	1
Process resource monitor resource	4.1.0-1 or later	1

CHAPTER

THREE

GROUP RESOURCE DETAILS

This chapter provides information on group resources that constitute a failover group.

For overview of group resources, see " Configuring a cluster system" in the "Installation and Configuration Guide".

This chapter covers:

- 3.1. *Group resources and supported EXPRESSCLUSTER versions*
- 3.2. *Attributes common to group resources*
- 3.3. *Group common properties*
- 3.4. *Group properties*
- 3.5. *Resource Properties*
- 3.6. *Understanding EXEC resources*
- 3.7. *Understanding Disk resource*
- 3.8. *Understanding Floating IP resource*
- 3.9. *Understanding Virtual IP resources*
- 3.10. *Understanding Mirror disk resources*
- 3.11. *Understanding Hybrid disk resources*
- 3.12. *Understanding NAS resource*
- 3.13. *Understanding Volume manager resources*
- 3.14. *Understanding VM resources*
- 3.15. *Understanding Dynamic DNS resources*
- 3.16. *Understanding AWS Elastic IP resources*
- 3.17. *Understanding AWS Virtual IP resources*
- 3.18. *Understanding AWS DNS resources*
- 3.19. *Understanding Azure probe port resources*
- 3.20. *Understanding Azure DNS resources*
- 3.21. *Understanding Google Cloud Virtual IP resources*
- 3.22. *Understanding Oracle Cloud Virtual IP resources*

3.1 Group resources and supported EXPRESSCLUSTER versions

The following is the number of group resources that can be registered with a group:

Version	Number of group resources(per group)
4.0.0-1 or later	256

Currently supported group resources are:

Group resource name	Abbreviation	Functional overview	Supported version
Exec resource	exec	See "*Understanding EXEC resources*"	4.0.0-1 or later
Disk resource	disk	See "*Understanding Disk resource*"	4.0.0-1 or later
Floating IP resource	fip	See "*Understanding Floating IP resource*"	4.0.0-1 or later
Virtual IP resource	vip	See "*Understanding Virtual IP resources*"	4.0.0-1 or later
Mirror disk resource	md	See "*Understanding Mirror disk resources*"	4.0.0-1 or later
Hybrid disk resource	hd	See "*Understanding Hybrid disk resources*"	4.0.0-1 or later
NAS resource	nas	See "*Understanding NAS resource*"	4.0.0-1 or later
Volume manager resource	volmgr	See "*Understanding Volume manager resources*"	4.0.0-1 or later
VM resource	vm	See "*Understanding VM resources*"	4.0.0-1 or later
Dynamic DNS resource	ddns	See "*Understanding Dynamic DNS resources*"	4.0.0-1 or later
AWS Elastic IP resource	awseip	See "*Understanding AWS Elastic IP resources*"	4.0.0-1 or later
AWS Virtual IP resource	awsvip	See "*Understanding AWS Virtual IP resources*"	4.0.0-1 or later
AWS DNS resource	awsdns	See "*Understanding AWS DNS resources*"	4.0.0-1 or later
Azure probe port resource	azurepp	See "*Understanding Azure probe port resources*"	4.0.0-1 or later
Azure DNS resource	azuredns	See "*Understanding Azure DNS resources*"	4.0.0-1 or later
Google Cloud Virtual IP resource	gcvip	See "*Understanding Google Cloud Virtual IP resources*"	4.2.0-1 or later
Oracle Cloud Virtual IP resource	ocvip	See "*Understanding Oracle Cloud Virtual IP resources*"	4.2.0-1 or later

The group resources that currently support dynamic resource addition are as follows:

Group resource name	Abbreviation	Functional overview	Supported version
Exec resource	exec	See "*Understanding EXEC resources*"	4.0.0-1 or later
Disk resource	disk	See "*Understanding Disk resource*"	4.0.0-1 or later
Floating IP resource	fip	See "*Understanding Floating IP resource*"	4.0.0-1 or later
Virtual IP resource	vip	See "*Understanding Virtual IP resources*"	4.0.0-1 or later
Volume manager resource	volmgr	See "*Understanding Volume manager resources*"	4.0.0-1 or later

3.2 Attributes common to group resources

A group is a failover unit. Rules regarding the failover operations (failover policies) can be specified for a group.

3.2.1 Understanding the group type

The following two types of groups exist: virtual machine groups and failover groups.

- **Virtual machine groups**
  Failovers (migration) are performed on a virtual machine basis. The following resources can be registered with this group: virtual machine resource, mirror disk resource, disk resource, hybrid disk resource, EXEC resource, NAS resource, and volume manager resource. A virtual machine group automatically follows even when the virtual machine is moved to a different server by a means other than EXPRESSCLUSTER.
- **Failover groups**
  Resources necessary to continue operations are grouped and failovers are performed on an operation basis. Up to 256 group resources can be registered with each group. However, no VM resource can be registered.

3.2.2 Understanding the group properties

The following properties can be specified for each group:

- **Servers that can run the Group**
  Select a server that can run the group from the servers in the cluster.
  Specify the order of servers that can run the group and the priority according to which the group is started.
- **Startup Attribute**
  Specify automatic or manual startup as the group startup attribute.
  For automatic startup, the group is automatically started on the server that can run the group and has the highest priority when the cluster is started.
  For manual startup, the group is not started when the server is started. Manually start the group by using the Cluster WebUI or clpgrp command after the server is started. For details about the Cluster WebUI, see the online manual. For details about the clpgrp command, see "*Operating groups (clpgrp command)*" in "*8. EXPRESSCLUSTER command reference*" in this guide.
- **Failover attribute**
  The failover attribute can be used to specify the failover mode. The following failover attributes can be specified.

  Automatic failover

  A heartbeat timeout or error detection by a group or monitor resource triggers an automatic failover.

  For an automatic failover, the following options can be specified.

  - Use the startup server settings
    The failover destination is determined according to the priority of the servers that can run the group.
  - Fail over dynamically
    The failover destination is determined by considering the statuses of each server's monitor resource or failover group, and then a failover is performed.

  The failover destination is determined in the following way.

Determination factor	Condition	Result
Status of exclusion target monitor resource	Error (all servers)	When there is no failover destination, proceed to the processing for determining a forced failover judgment .
	Normal (single server)	A normal server is used as the failover destination.
	Normal (multiple servers)	Proceed to the process that compares error levels.
Perform a forced failover	Set	Proceed to the process that ignores the status of the exclusion target monitor resource and which compares error levels for all the activated servers.
	Not set	Failover is not performed.
Number of servers with the lowest error level	1	The server that has the lowest error level is used as the failover destination.
	Two or more	The operation levels are compared for those servers that have the lowest error level.
Prioritize failover policy in the server group	Set and Within the same server group as the failover source, there is a server that can perform failover.	The server in the same server group is used as the failover destination.
	Set and Within the same server group as the failover source, there is no server that can perform failover.	Proceed to the smart failover judgment process.
	Not set	Proceed to the smart failover judgment process.
Perform a smart failover	Set and The number of servers recommended as the failover destination is 1.	The server recommended by the smart failover is used as the failover destination.

Continued on next page

Table 3.4 – continued from previous page

Determination factor	Condition	Result
	Set and The number of servers recommended as the failover destination is 2 or more.	Proceed to the running level judgment process.
	Not set	Proceed to the running level judgment process.
Number of servers with the lowest running level	1	The server with the lowest running level is used as the failover destination.
	Two or more	Of the activated servers, the server with the highest priority is used as the failover destination.

Note:

Critical monitor resource
Exclude the server that detected an error in a monitor resource from the failover destination. The exclusive list is set with the Cluster WebUI.

Error level
Number of monitor resources that detected errors

Smart failover
A function that assigns the server with the smallest load as the failover destination, based on the system resource information collected by the System Resource Agent. To enable this function, a System Resource Agent license must be registered on all the servers set as the failover destination and the system monitor resources must be set as the monitor resource. For detail about the system monitor resources, see "*Understanding System monitor resources*" in "*4. Monitor resource details*" in this guide.

Running level
Number of started failover groups or number of failover groups that are being started, excluding management groups

- Prioritize failover policy in the server group
  If a server in the same server group can be used as the failover destination, this server is preferably used. The server that can run the failover group and has the highest priority among the running servers is used as the failover destination.
  If no server in the same server group can be used as the failover destination, a server in another server group is used as the failover destination.
- Allow only a manual failover between server groups
  This can be selected only when the above **Prioritize failover policy in the server group** is set.

An automatic failover is performed only if a server within the same server group is the destination.

If no servers in the same server group can be used as the failover destination, failing over to a server in another server group is not automatically performed.

To move the group to a server in another server group, use the Cluster WebUI or clpgrp command.

Manual failover

A failover is not automatically performed when a heartbeat timeout occurs. Manually start a failover by using the Cluster WebUI or clpgrp command. However, even when manual failover is specified, an automatic failover is performed if a group resource or monitor resource detects an error.

Note: If **Execute Failover to outside the Server Group** is set in message receive monitor resource setting, dynamic failover setting and failover setting between server groups will be invalid. A failover is applied to the server that is in a server group other than the server group to which the failover source server belongs and which has the highest priority.

- **Failback attribute**

  Specify automatic or manual failback. However, This cannot be specified when the following conditions match.

  - Mirror disk resource or hybrid disk resource is set to fail over group.
  - Failover attribute is **Fail over dynamically**.

  For automatic failback, an automatic failback is performed when the server that has the highest priority is started after a failover.

  For manual failback, no failback occurs even when the server is started.

3.2.3 Understanding failover policy

A failover policy is a priority that determines a server to be the failover destination from multiple servers. When you configure the failover policy, avoid making certain servers heavily loaded at a failover.

The following describes how servers behave differently depending on failover policies when a failover occurs using example of the server list that can fail over and failover priority in the list.

<Symbols and meaning>

Server status	Description
O	Normal (properly working as a cluster)
X	Stopped (cluster is stopped)

3-node configuration:

Group	Priority order of servers		
	1st priority server	**2nd priority server**	**3rd priority server**
A	server1	server3	server2
B	server2	server3	server1

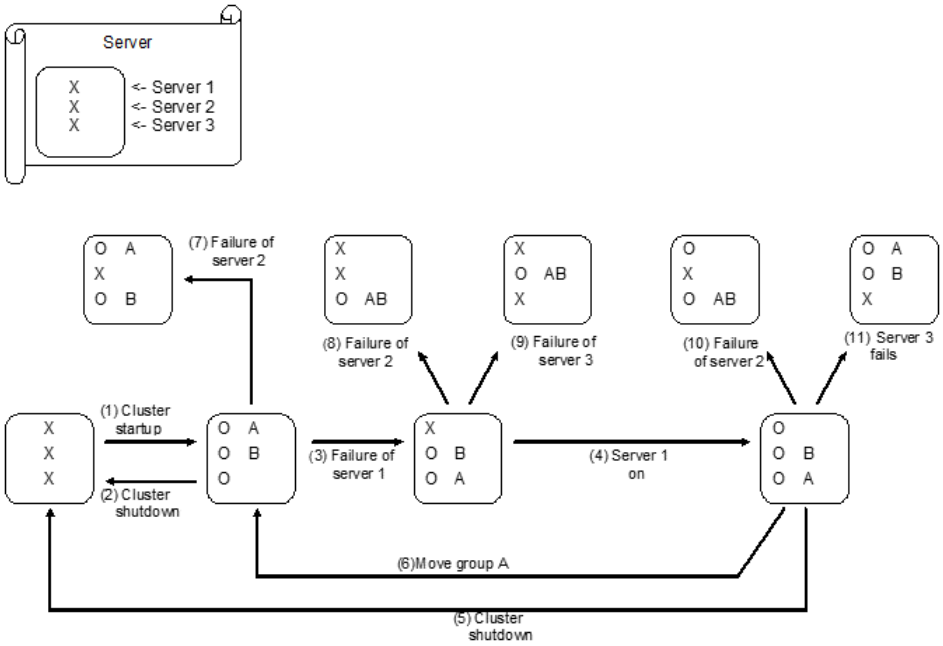
2-node configuration:

Group	Priority order of servers	
	1st priority server	**2nd priority server**
A	server1	server2
B	server2	server1

It is assumed that the group startup attributes are set to auto startup and the failback attributes are set to manual failback for both Group A and B.

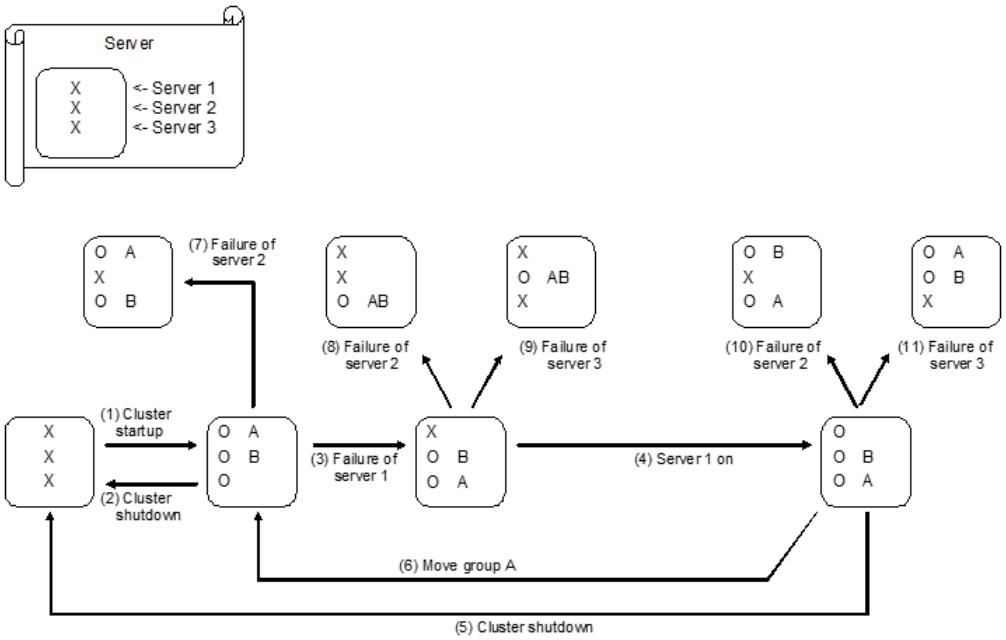
- For groups belonging to exclusion rules in which exclusive attributes are Normal or Absolute, the server which they start up or fail over is determined by the failover priority to the server. If a group has two or more servers of the same failover priority, it is determined by the order of numbers, the specific symbols and alphabets of the group name. For details on the failover exclusive attribute, refer to "*Understanding Exclusive Control of Group*".

  When Group A and B do not belong to the exclusion rules:



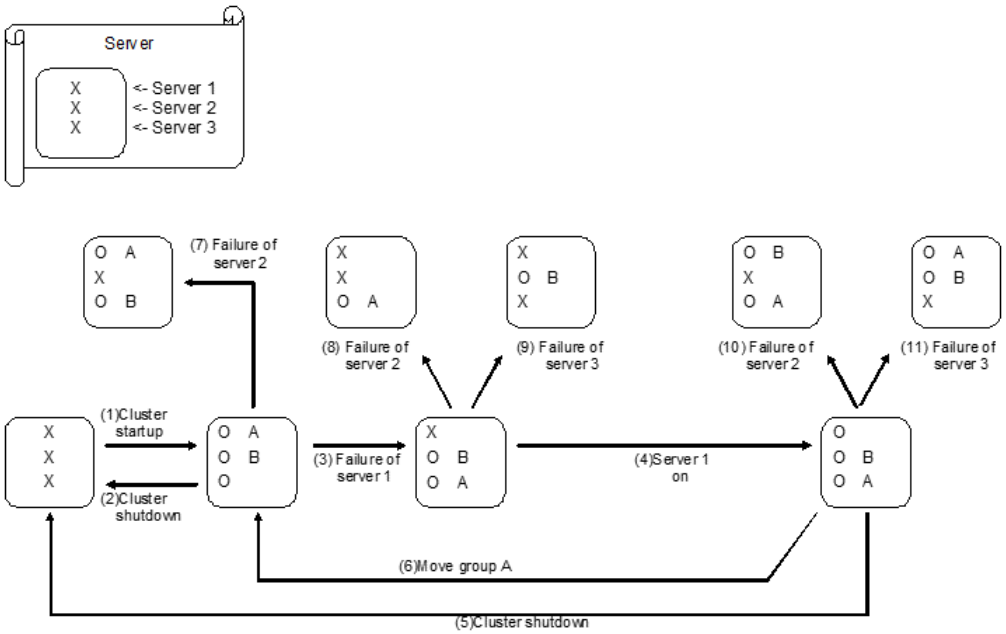
1. Cluster startup
2. Cluster shutdown
3. Failure of server1 Fails over to the next priority server.
4. Server1 power on
5. Cluster shutdown
6. Move group A
7. Failure of server2: Fails over to the next priority server.
8. Failure of server2: Fails over to the next priority server.
9. Failure of server3: Fails over to the next priority server.
10. Failure of server2: Fails over to the next priority server.
11. Failure of server3: Fails over to the next priority server.

When Group A and B belong to the exclusion rules in which the exclusive attribute is set to Normal:



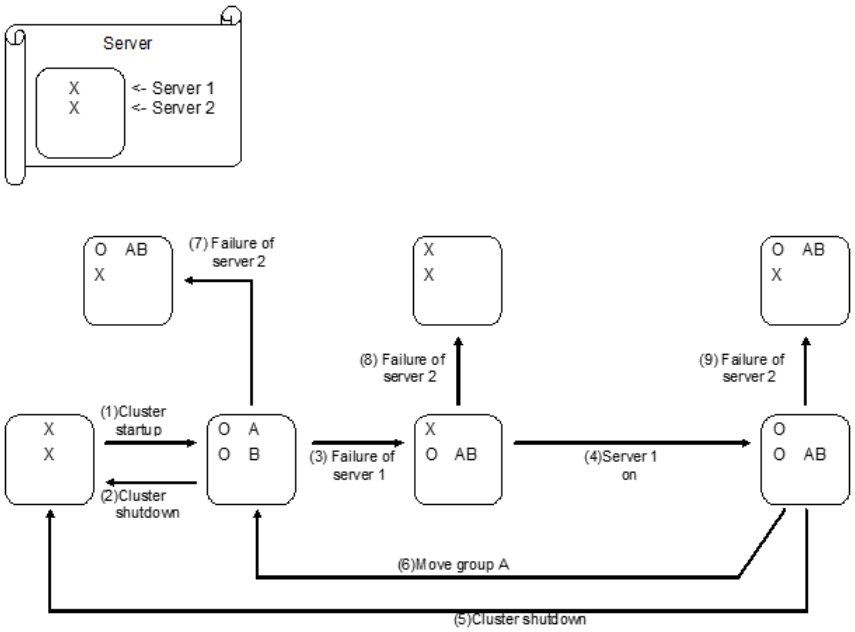
1. Cluster startup
2. Cluster shutdown
3. Failure of server1: Fails over to a server where no normal exclusive group is active.
4. Server1 power on
5. Cluster shutdown
6. Move groupA
7. Failure of server2: Fails over to a server where a normal exclusive group is not active.
8. Failure of server2: There is no server where a normal exclusive group is not active, but failover to the server because there is a server that can be started.
9. Failure of server3: There is no server where a normal exclusive group is not active, but failover to the server because there is a server that can be started.
10. Failure of server2: Fails over to a server where a normal exclusive group is not active.
11. Failure of server3: Fails over to a server where a normal exclusive group is not active.

When Group A and B belong to the exclusion rules in which the exclusive attribute is set to Absolute:



1. Cluster startup
2. Cluster shutdown
3. Failure of server1: Fails over to the next priority server.
4. server1 power on
5. Cluster shutdown
6. Move groupA
7. Failure of server2: Fails over to the next priority server.
8. Failure of server2: Does not failover (GroupB stops).
9. Failure of server3: Does not failover (GroupA stops).
10. Failure of server2: Fails over to the server where no full exclusive group is active.
11. Failure of server3: Fails over to the server where no full exclusive group is active.

For Replicator (two-server configuration) When Group A and B do not belong to the exclusion rules:



1. Cluster startup
2. Cluster shutdown
3. Failure of server1: Fails over to the standby server of GroupA.
4. Server1 power on
5. Cluster shutdown
6. Move groupA
7. Failure of server2: Fails over to the standby server of GroupB.
8. Failure of server2
9. Failure of server3: Fails over to the standby server.

3.2.4 Operations at detection of activation and deactivation failure

When an activation or deactivation error is detected, the following operations are performed:

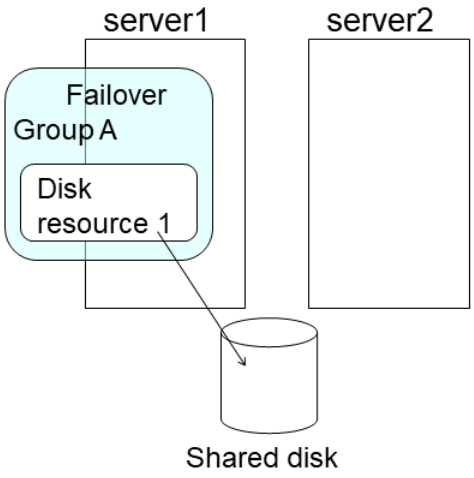
- When an error in activation of group resources is detected:
  - When an error in activation of group resources is detected, activation is retried.
  - When activation retries fail as many times as the number set to **Retry Count at Activation Failure**, a failover takes place.
  - If the failover fails as many times as the number set to **Failover Threshold**, the final action is performed.
- When an error in deactivation of group resources is detected:
  - When an error in deactivation of group resources is detected, deactivation is retried.
  - When deactivation retries fail as many times as the number set to **Retry Count at Deactivation Failure**, the final action is performed.

Note:

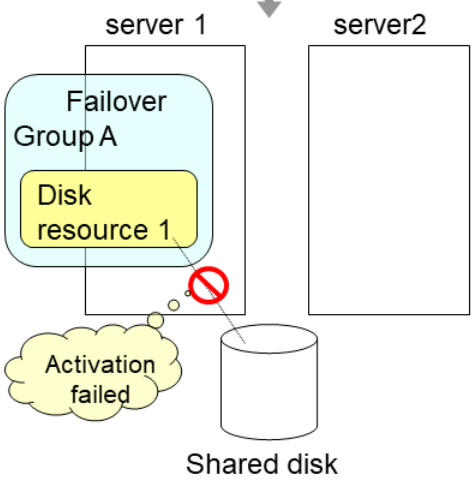
Activation retries and failovers are counted on a server basis. The Retry Count at Activation Failure and Failover Threshold are maximum activation retry count and failover count on a server basis respectively.
The activation retry count and failover count are reset in a server where the group activation is successful.
Note that a failed recovery action is also counted as one for the activation retry count or failover count.

The following describes how an error in activation of a group resource is detected:

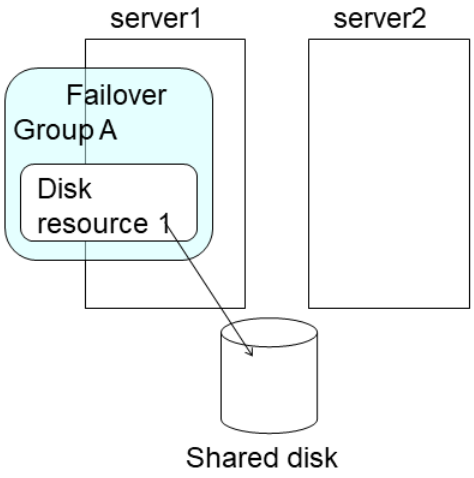
When the following settings are made:
Retry Count at Activation Failure 3 times
Failover Threshold 1 time
Final Action Stop Group



Start activation processing of disk resource 1 (resource under failover group A). (Execute mount processing of the file system and other processings)



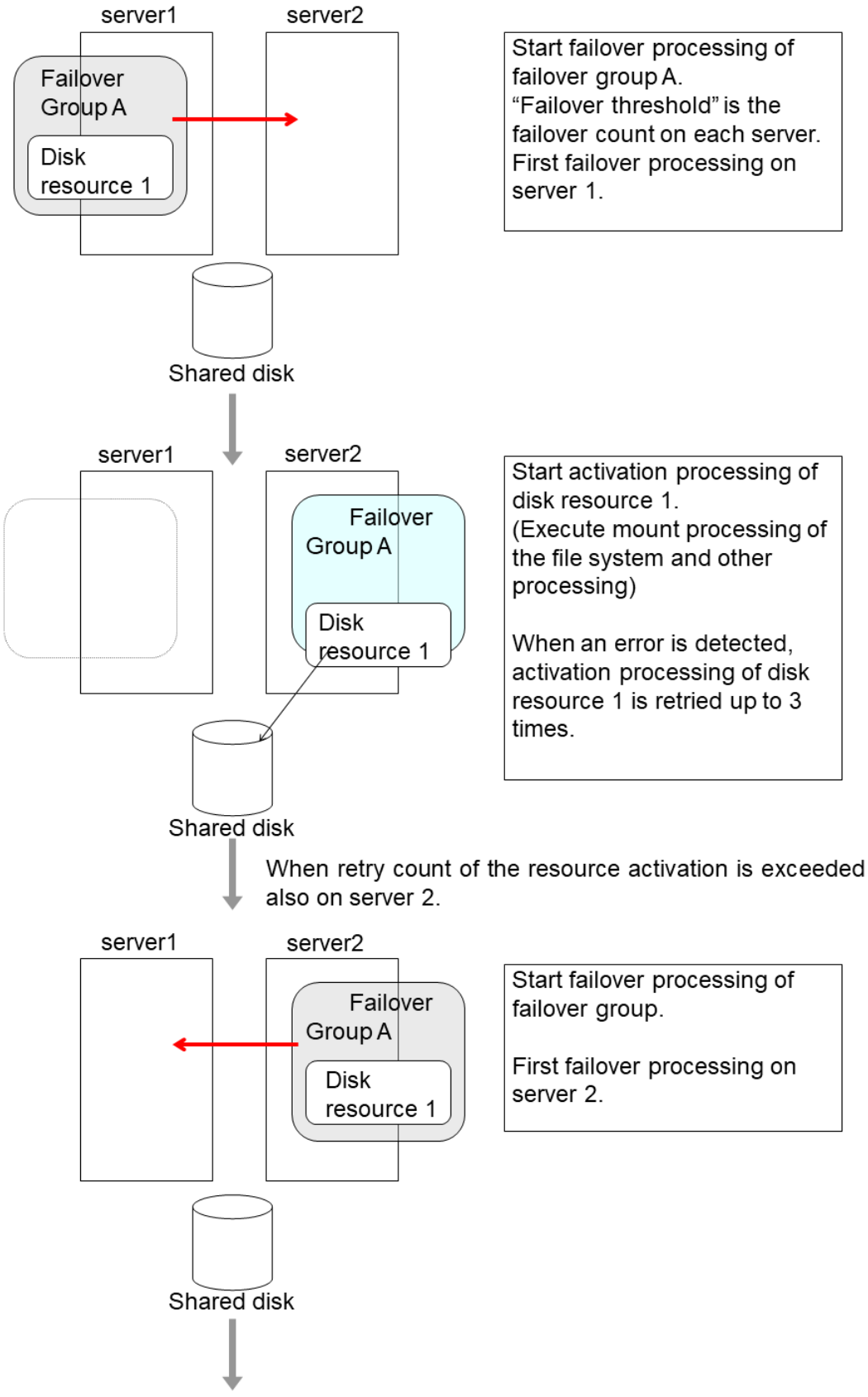
There is an error in activation processing of disk resource 1. (fsck error, mount error)

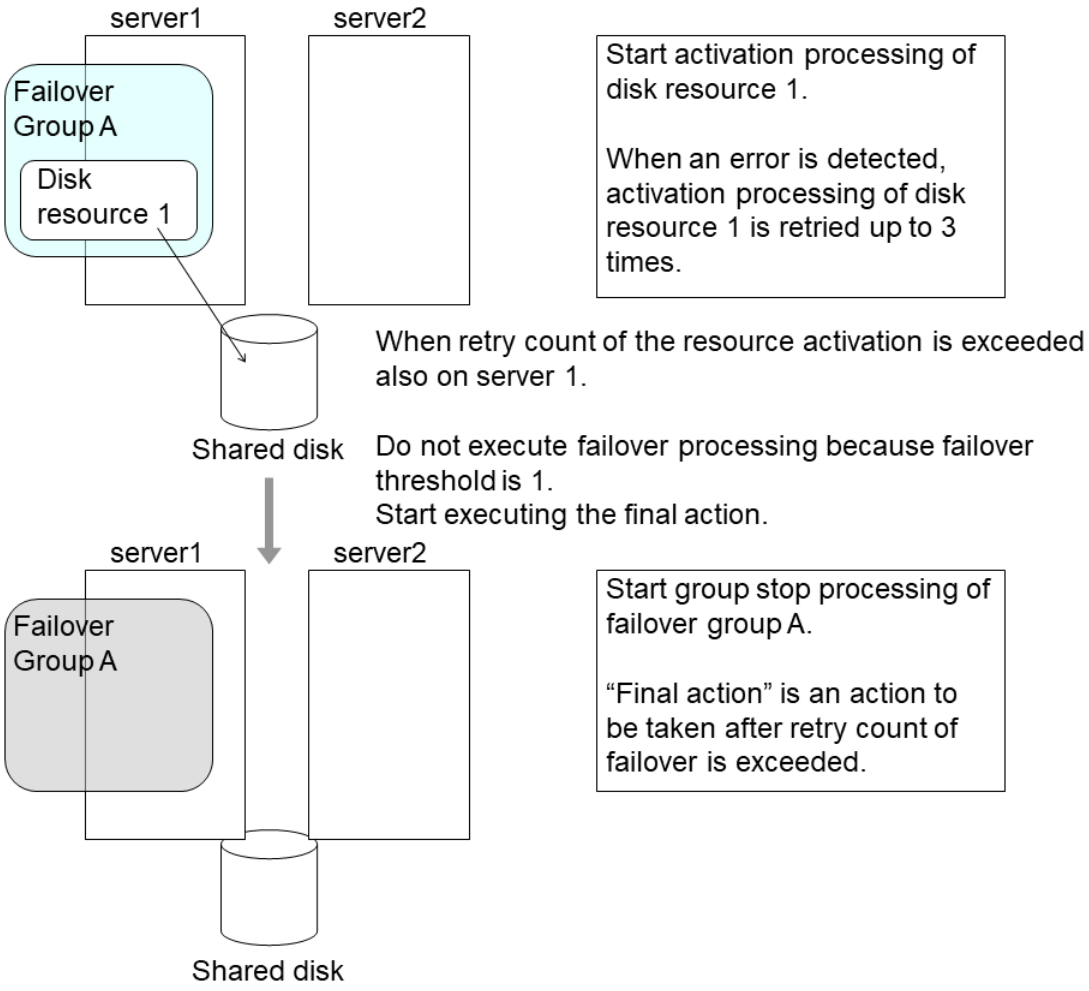


Activation processing of disk resource 1 is retried up to 3 times.

"Activation retry count" indicates this retry count.

When retry count is exceeded


server1
server2
Failover Group A
Disk resource 1
Start failover processing of failover group A.
"Failover threshold" is the failover count on each server.
First failover processing on server 1.
Shared disk
server1
server2
Failover Group A
Disk resource 1
Start activation processing of disk resource 1.
(Execute mount processing of the file system and other processing)
When an error is detected, activation processing of disk resource 1 is retried up to 3 times.
Shared disk
When retry count of the resource activation is exceeded also on server 2.
server1
server2
Failover Group A
Disk resource 1
Start failover processing of failover group.
First failover processing on server 2.
Shared disk



3.2.5 Script before final action

When a group resource activation error is detected, a script before final action can be executed before the last action during detection of a deactivation error.

Environment variables used with a script before final action

When executing a script, EXPRESSCLUSTER sets information such as the state in which it is executed (when an activation error occurs, when a deactivation error occurs) in the environment variables.

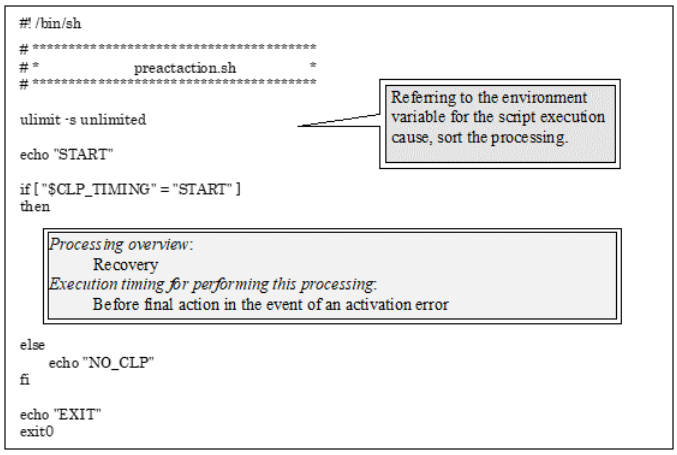
In the script, processing that is appropriate for the system operation can be described using the environment variables listed below as branch conditions.

Environment variable	Value	Description
CLP_TIMING ...Execution timing	START	Executes a script before final action in the event of a group resource activation error.
	STOP	Executes a script before final action in the event of a group resource deactivation error.
CLP_GROUPNAME ...Group name	Group name	Indicates the name of the group containing the group resource in which an error that causes the script before final action to be executed is detected.
CLP_RESOURCENAME ...Group resource name	Group resource name	Indicates the name of the group resource in which an error that causes the script before final action to be executed is detected.

Flow used to describe a script before final action

The following explains the environment variables in the previous topic and an actual script, associating them with each other.

Example of a script before final action in the event of an activation error



Tips for creating a script before final action

Note the following when creating a script:

- If the script contains a command that will take some time to execute, always leave a trace that will indicate the completion of the execution of that command. If a problem occurs, you can use this information to isolate the failure. One way of leaving such a trace is to use clplogcmd.
- Method of describing in a script by using clplogcmd

  Using clplogcmd, you can output messages to the Alert logs of Cluster WebUI or syslog of the OS. For details on the clplogcmd command, see "*Outputting messages (clplogcmd command)*" in "8. *EXPRESSCLUSTER command reference*" in this guide.

  (Example: Script image)

```
clplogcmd -m "recoverystart.."
recoverystart
clplogcmd -m "OK"
```

Notes on script before final action

- Stack size of the commands and application to be started from a script

  A recovery script and a script before recovery action are executed with the stack size set to 2 MB. For this reason, if the commands and applications to be started from the script require a stack size of 2 MB or greater, a stack overflow will occur.
  If a stack overflow occurs, set the stack size before starting the commands and applications.

- Condition that a script before final action is executed

  A script before final action is executed before the final action upon detection of a group resource activation or deactivation failure. Even if **No operation (Next Resources Are Activated/Deactivated)** or **No operation (Next Resources Are Not Activated/Deactivated)** is set as the final action, a script before final action is executed.
  If the final action is not executed because the maximum restart count has reached the upper limit or by the function to suppress the final action when all other servers are being stopped, a script before final action is not executed.

3.2.6 Script Before and After Activation/Deactivation

An arbitrary script can be executed before and after activation/deactivation of group resources.

Environment variables used with a script after activation/deactivation

When executing a script, EXPRESSCLUSTER sets information such as the state in which it is executed (before activation, after activation, before deactivation, or after deactivation) in the environment variables.

Environment variable	Value	Description
CLP_TIMING ...Execution timing	PRESTART	Executes a script before a group resource is activated.
	POSTSTART	Executes a script after a group resource is activated.
	PRESTOP	Executes a script before a group resource is deactivated.
	POSTSTOP	Executes a script after a group resource is deactivated.
CLP_GROUPNAME ...Group name	Group name	Indicates the group name of the group resource containing the script.
CLP_RESOURCENAME ...Group resource name	Group resource name	Indicates the name of the group resource containing the script.

Flow used to describe a script before and after activation/deactivation

The following explains the environment variables in the previous topic and an actual script, associating them with each other.

Example of a script before and after activation/deactivation

```
#! /bin/sh
#***************************************
#*              rscextent.sh           *
#***************************************

ulimit -s unlimited
echo "START"

if [ "$CLP_TIMING" = "PRESTART" ]
then
        echo "$CLP_GROUPNAME"
        echo "$CLP_RESOURCENAME"
    Execution timing for performing this processing: Before activation in resource
elif [ "$CLP_TIMING" = "POSTSTART" ]
then
        echo "$CLP_GROUPNAME"
        echo "$CLP_RESOURCENAME"
    Execution timing for performing this processing: After activation in resource
elif [ "$CLP_TIMING" = "PRESTOP" ]
then
        echo "$CLP_GROUPNAME"
        echo "$CLP_RESOURCENAME"
    Execution timing for performing this processing: Before deactivation in resource
elif [ "$CLP_TIMING" = "POSTSTOP" ]
then
        echo "$CLP_GROUPNAME"
        echo "$CLP_RESOURCENAME"
    Execution timing for performing this processing: After deactivation in resource
fi
echo "EXIT"
exit 0
```

Tips for creating a script before and after activation/deactivation

Note the following when creating a script:

- If the script contains a command that will take some time to execute, always leave a trace that will indicate the completion of the execution of that command. If a problem occurs, you can use this information to isolate the failure. One way of leaving such a trace is to use clplogcmd.
- Method of describing in a script by using clplogcmd

  Using clplogcmd, you can output messages to the Alert logs of Cluster WebUI or syslog of the OS. For details on the clplogcmd command, see "*Outputting messages (clplogcmd command)*" in "*8. EXPRESSCLUSTER command reference*" in this guide.

  (Example: Script image)

  ```
  clplogcmd -m "start.."
  :
  clplogcmd -m "OK"
  ```

Notes on script before and after activation/deactivation

- Stack size of the commands and application to be started from a script

  A script before and after activation/deactivation is executed with the stack size set to 2 MB. For this reason, if the commands and applications to be started from the script require a stack size of 2 MB or greater, a stack overflow will occur.

  If a stack overflow occurs, set the stack size before starting the commands and applications.

3.2.7 Reboot count limit

If the action which is accompanied by OS reboot is selected as the final action to be taken when any error in activation or deactivation is detected, you can limit the number of shutdowns or reboots caused by detection of activation or deactivation errors.

This maximum reboot count is the upper limit of reboot count of each server.

Note: The maximum reboot count is the upper limit of reboot count of a server because the number of reboots is recorded per server.

The number of reboots that are taken as a final action in detection of an error in group activation or deactivation and those by a monitor resource are recorded separately.

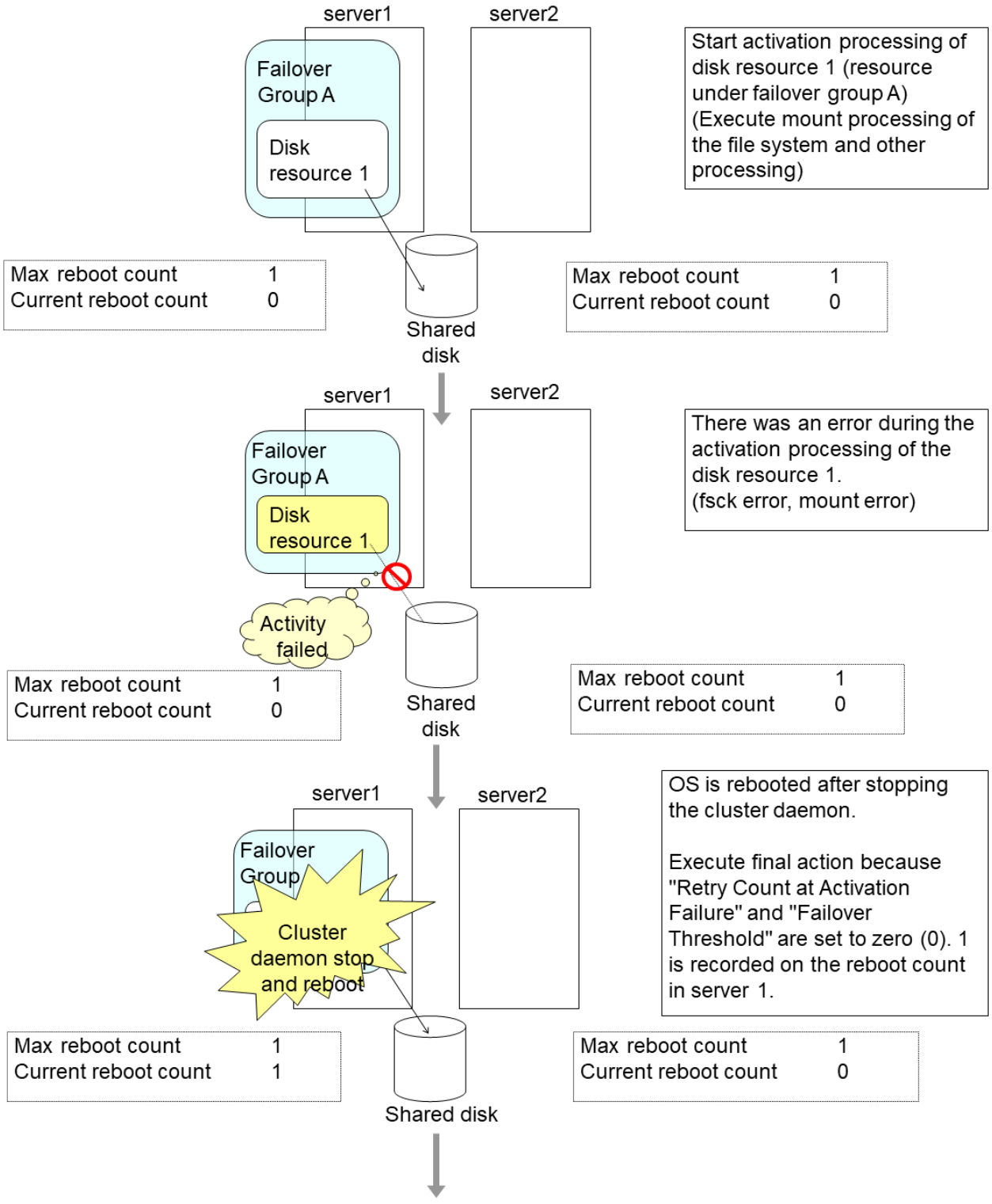
If the time to reset the maximum reboot count is set to zero (0), the number of reboots will not be reset. Run the clpregctrl command to reset this number. For details on the clpregctrl command, see "*Controlling reboot count (clpregctrl command)*" in "8. *EXPRESSCLUSTER command reference*".

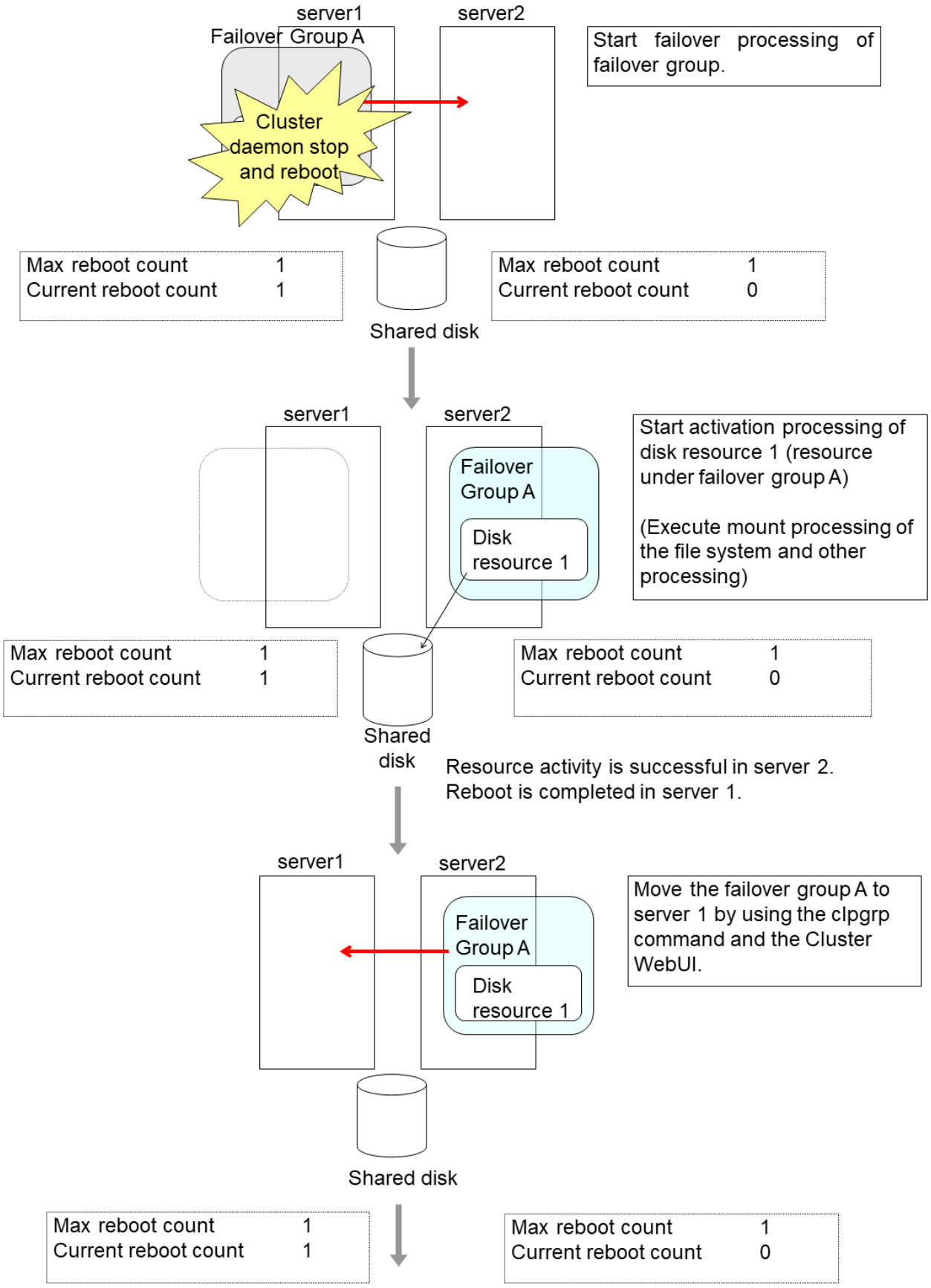
The following describes the flow of operations when the limitation of reboot count is set as shown below:

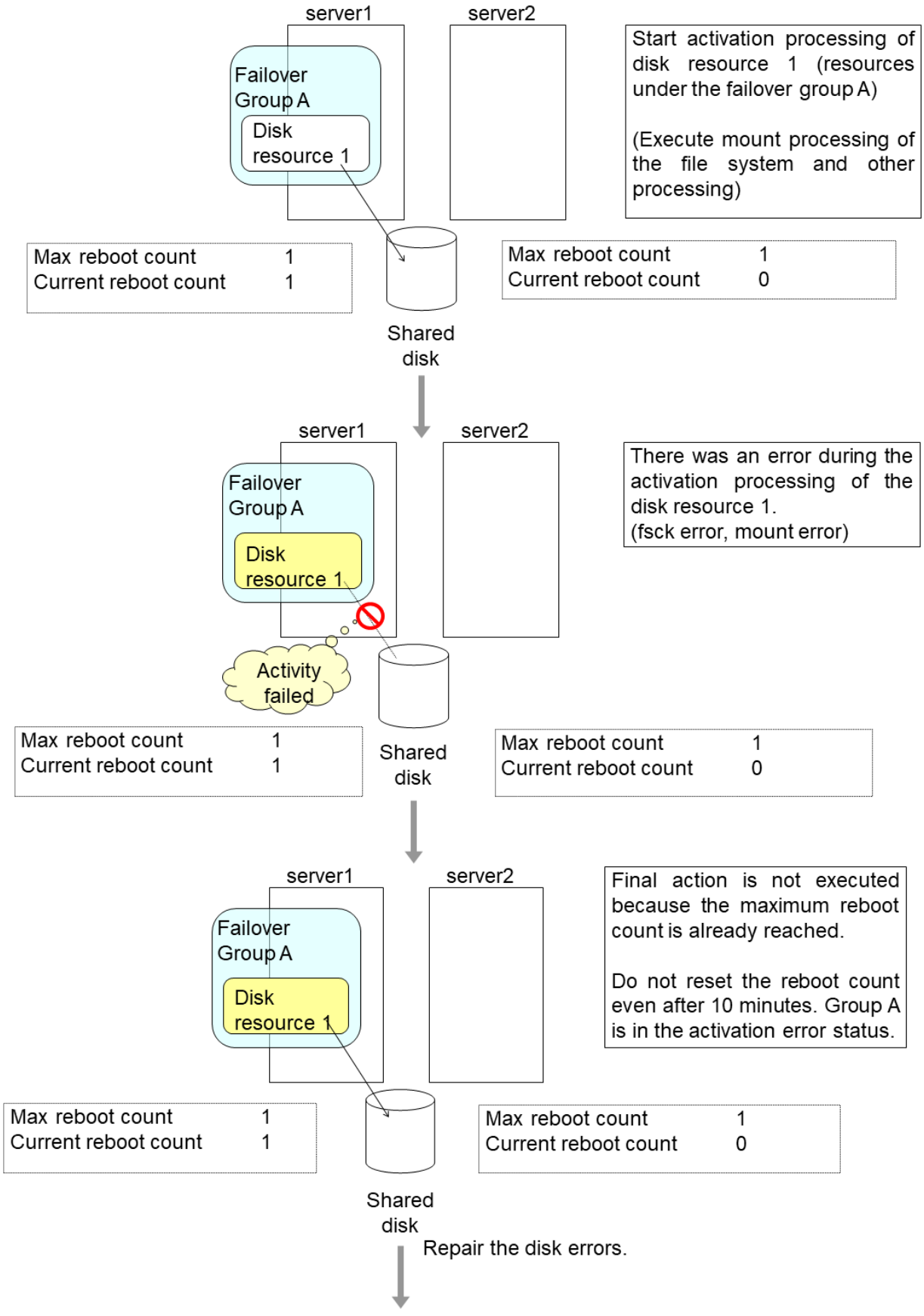
As a final action, **Stop cluster daemon and reboot OS** is executed once because the maximum reboot count is set to one (1).

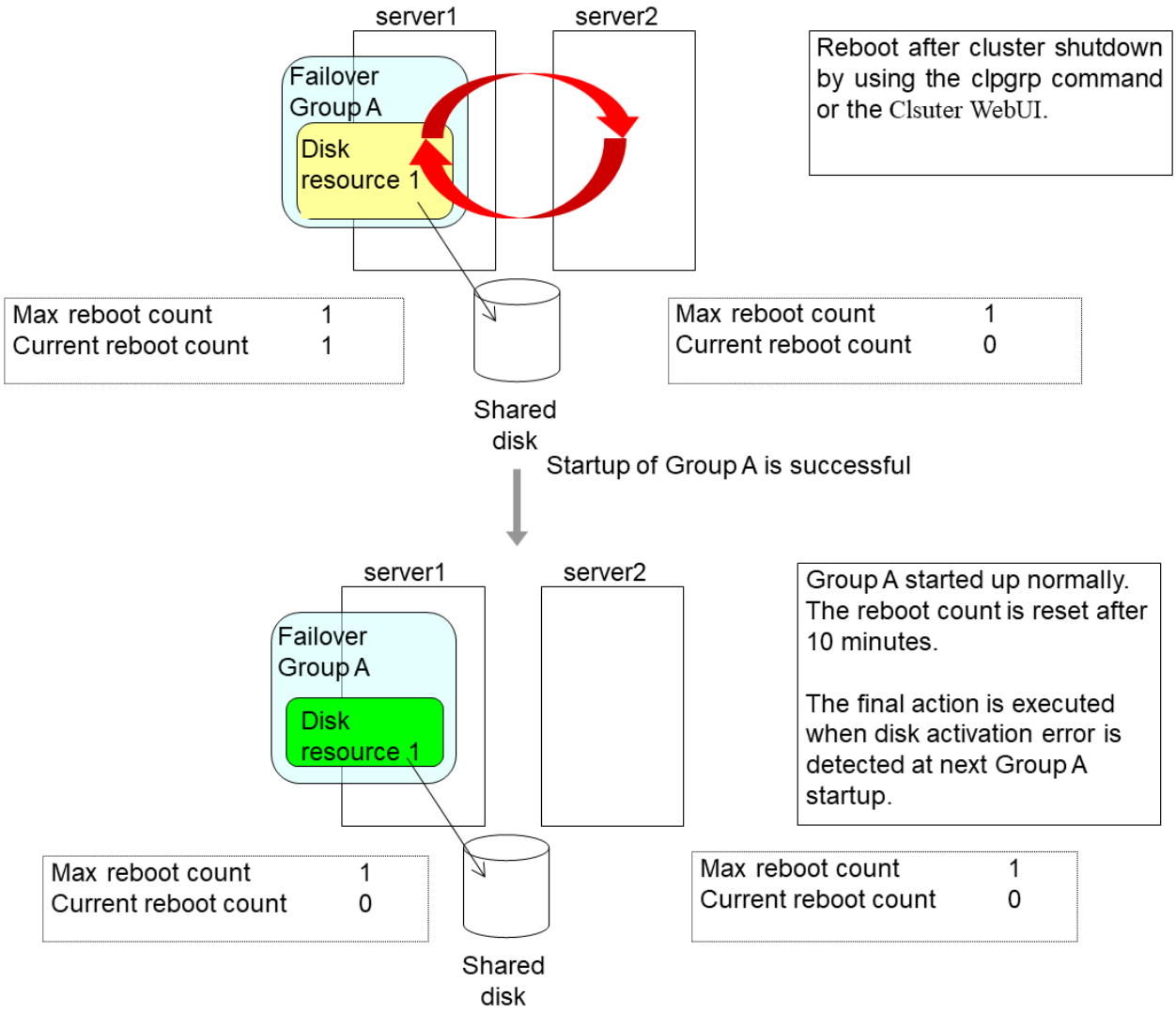
If group activation is successful at a reboot following the cluster shutdown, the reboot count is reset after 10 minutes because the time to reset maximum reboot count is set to 10 minutes.

Setting example
Retry Count at Activation Failure 0 time
Failover Threshold 0 time
Final Action Stop cluster service and reboot OS
Max Reboot Count 1 time
Max Reboot Count Reset Time 10 minutes


server1
server2
Failover Group A
Disk resource 1
Start activation processing of disk resource 1 (resource under failover group A) (Execute mount processing of the file system and other processing)
Max reboot count 1
Current reboot count 0
Max reboot count 1
Current reboot count 0
Shared disk
server1
server2
Failover Group A
Disk resource 1
There was an error during the activation processing of the disk resource 1. (fsck error, mount error)
Activity failed
Max reboot count 1
Current reboot count 0
Max reboot count 1
Current reboot count 0
Shared disk
server1
server2
Failover Group
Cluster daemon stop and reboot
OS is rebooted after stopping the cluster daemon.
Execute final action because "Retry Count at Activation Failure" and "Failover Threshold" are set to zero (0). 1 is recorded on the reboot count in server 1.
Max reboot count 1
Current reboot count 1
Max reboot count 1
Current reboot count 0
Shared disk


server1
Failover Group A
server2
Start failover processing of failover group.
Cluster daemon stop and reboot
Max reboot count 1
Current reboot count 1
Max reboot count 1
Current reboot count 0
Shared disk
server1
server2
Failover Group A
Disk resource 1
Start activation processing of disk resource 1 (resource under failover group A)
(Execute mount processing of the file system and other processing)
Max reboot count 1
Current reboot count 1
Max reboot count 1
Current reboot count 0
Shared disk
Resource activity is successful in server 2.
Reboot is completed in server 1.
server1
server2
Failover Group A
Disk resource 1
Move the failover group A to server 1 by using the clpgrp command and the Cluster WebUI.
Shared disk
Max reboot count 1
Current reboot count 1
Max reboot count 1
Current reboot count 0


server1
server2
Failover Group A
Disk resource 1
Start activation processing of disk resource 1 (resources under the failover group A)
(Execute mount processing of the file system and other processing)
Max reboot count 1
Current reboot count 1
Max reboot count 1
Current reboot count 0
Shared disk
server1
server2
Failover Group A
Disk resource 1
There was an error during the activation processing of the disk resource 1.
(fsck error, mount error)
Activity failed
Max reboot count 1
Current reboot count 1
Shared disk
Max reboot count 1
Current reboot count 0
server1
server2
Failover Group A
Disk resource 1
Final action is not executed because the maximum reboot count is already reached.
Do not reset the reboot count even after 10 minutes. Group A is in the activation error status.
Max reboot count 1
Current reboot count 1
Max reboot count 1
Current reboot count 0
Shared disk
Repair the disk errors.



3.2.8 Resetting the reboot count

Run the clpregctrl command to reset the reboot count. For details on the clpregctrl command, see "*Controlling reboot count (clpregctrl command)*" in "*8. EXPRESSCLUSTER command reference*" in this guide.

3.2.9 Checking a double activation

When a group is started, it is possible to check whether a double activation will occur or not.

- If a double activation is determined not to occur:
  A group startup begins.
- If a double activation is determined to occur (ih a timeout occurs):
  A group startup does not begin. If the server attempts to start up the group, that group is stopped.

Note:

- If a single resource is started while its relevant group is stopped, a double activation check will be performed. However, if a single resource is started while any resource in the group is activated, a double activation check will not be performed.
- If there are no floating IP resources for the group for which **Detect double activation** is selected, a double activation is not executed and the group startup begins.
- If a double activation is determined to occur, the statuses of groups and resources may not match among servers.

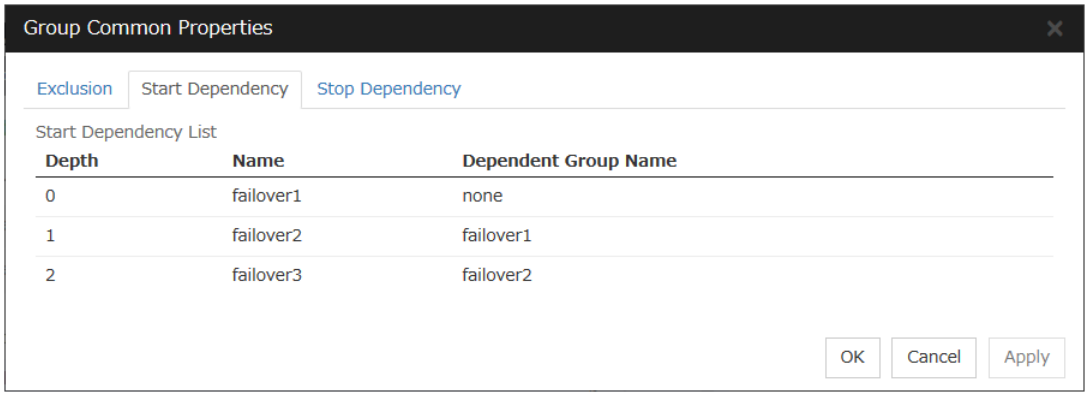
3.2.10 Understanding setting of group start dependence and group stop dependence

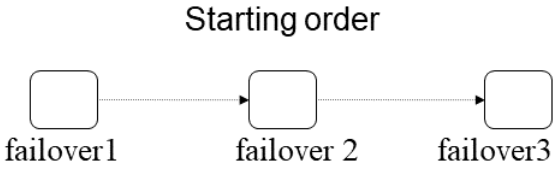
You can set the group start and stop order by setting group start dependence and group stop dependence.

- When group start dependence is set:
  - For group start, start processing of this group is performed after start processing of the group subject to start dependence completes normally.
  - For group start, if a timeout occurs in the group for which start dependence is set, the group does not start.
- When group stop dependence is set:
  - For group stop, stop processing of this group is performed after stop processing of the group subject to stop dependence completes normally.
  - If a timeout occurs in the group for which stop dependence is set, the group stop processing continues.
  - Stop dependence is performed according to the conditions specified in Cluster WebUI.

To display the settings made for group start dependence and group stop dependence, click group properties in the config mode of Cluster WebUI and then click the **Start Dependency** tab and the **Stop Dependency** tab.

Depths for group start dependence are listed below as an example.





The following explains group start execution using examples of simple status transition.

When two servers have three groups

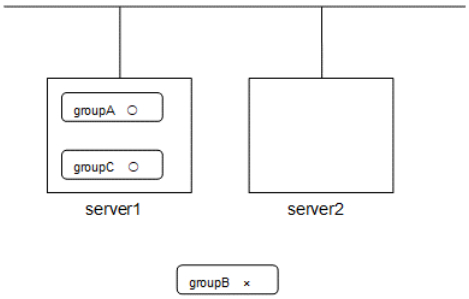
Group failover policy

groupA server1
groupB server2
groupC server1 -> server2

Group start dependence setting

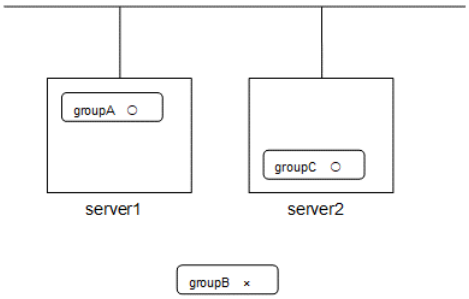
groupA Start dependence is not set.
groupB Start dependence is not set.
groupC groupA start dependence is set.
groupC Start dependence is set when groupC is started by the server of groupB.

1. When server1 starts groupA and groupC



server1 starts groupC after groupA has been started normally.

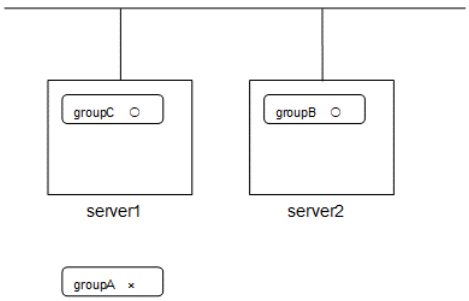
2. When server1 starts groupA and server2 starts groupC



server2 starts groupC after server1 has started groupA normally.

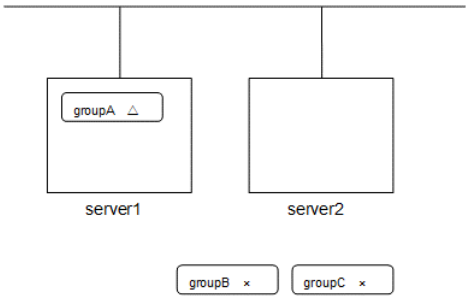
Wait Only when on the Same Server is not set, so groupA start dependence by another server is applied.

3. When server1 starts groupC and server2 starts groupB



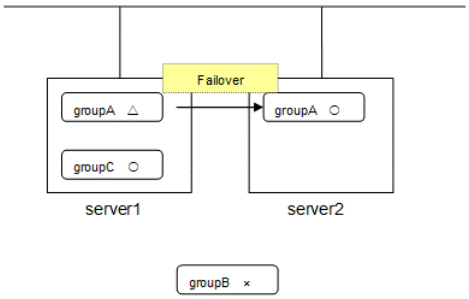
server1 starts groupC without waiting for the normal start of groupB. groupC is set to wait for groupB start only when it is started by the same server. However, start dependence is not applied to groupC because groupB is set such that it is not started by server1.

4. When server1 starts groupA and groupC



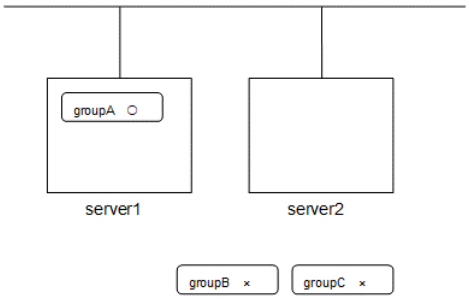
If server1 fails in groupA start, groupC is not started.

5. When server1 starts groupA and groupC



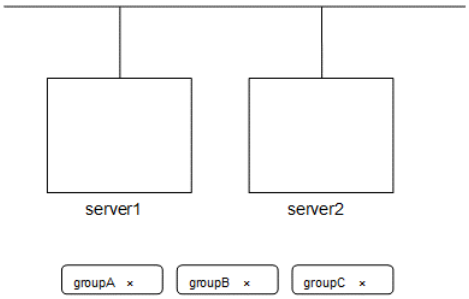
If server1 fails in groupA start and a failover occurs in server2 due to groupA resource recovery, server2 starts groupA and then server1 starts groupC.

6. When server1 starts groupA and groupC



If a groupA start dependence timeout occurs on server1, groupC is not started.

7. When server1 starts only groupC



server1 has not started groupA, so a start dependence timeout occurs. If this timeout occurs, groupC is not started.

Note:

- When a group is started, there is no function to automatically start the group for which start dependence is set.
- The group is not started if a timeout occurs in the group for which start dependence is set.
- The group is not started if the group for which start dependence is set fails to start.
- If the group for which start dependence is set contains a normally started and a normally stopped resource, the group is judged to have started normally.
- When a group is stopped, there is no function to automatically stop the group for which stop dependence is set.
- The group stop processing continues if a timeout occurs in the group for which stop dependence is set.
- The group stop processing continues if the group for which stop dependence is set fails to stop.
- The group stop processing or resource stop processing by the Cluster WebUI or clpgrp command does not apply stop dependence. Stop dependence is applied according to the setting (when the cluster or a server stops) made with the Cluster WebUI.
- If a start waiting timeout occurs at the time of a failover, the failover fails.

3.2.11 Understanding Exclusive Control of Group

The Failover exclusive attributes set exclusive attributes of the group at failover. However, they cannot set any attribute under the following conditions:

- If **Virtual machine group** is specified as the group type
- When failover attribute is one of **Fail over dynamically**, **Prioritize failover policy in the server group** or **Enable only manual failover among the server groups**.

The settable failover exclusive attributes are as follows:

Off

Exclusion is not performed at failover. Failover is performed on the server of the highest priority among the servers that can fail over.

Normal

Exclusion is performed at failover. Failover is performed on the server on which the other normal exclusion groups are not started and which is given the highest priority among the servers that can run the group.

However, if the other normal exclusion groups have already been started on all servers that the failover can be performed, exclusion is not performed. Failover is performed on the server that is given the highest priority among the servers on which failover can be performed.

Absolute

Exclusion is performed at failover. Failover is performed on the server on which the other absolute exclusion groups are not started and which is given the highest priority among the servers that can run the group.

However, failover is not performed if the other absolute exclusion groups have already been started on all servers on which failover can be performed.

Note: Exclusion is not performed to the groups with different exclusion rules. Exclusive control is performed only among the groups with the same exclusion rule, according to the set exclusion attribute. In either case, exclusion is

not performed with the no-exclusion group. For details on the failover exclusive attribute, see "*Understanding failover policy*". Furthermore, For details on the settings of the exclusion rules, see "*Group common properties*".

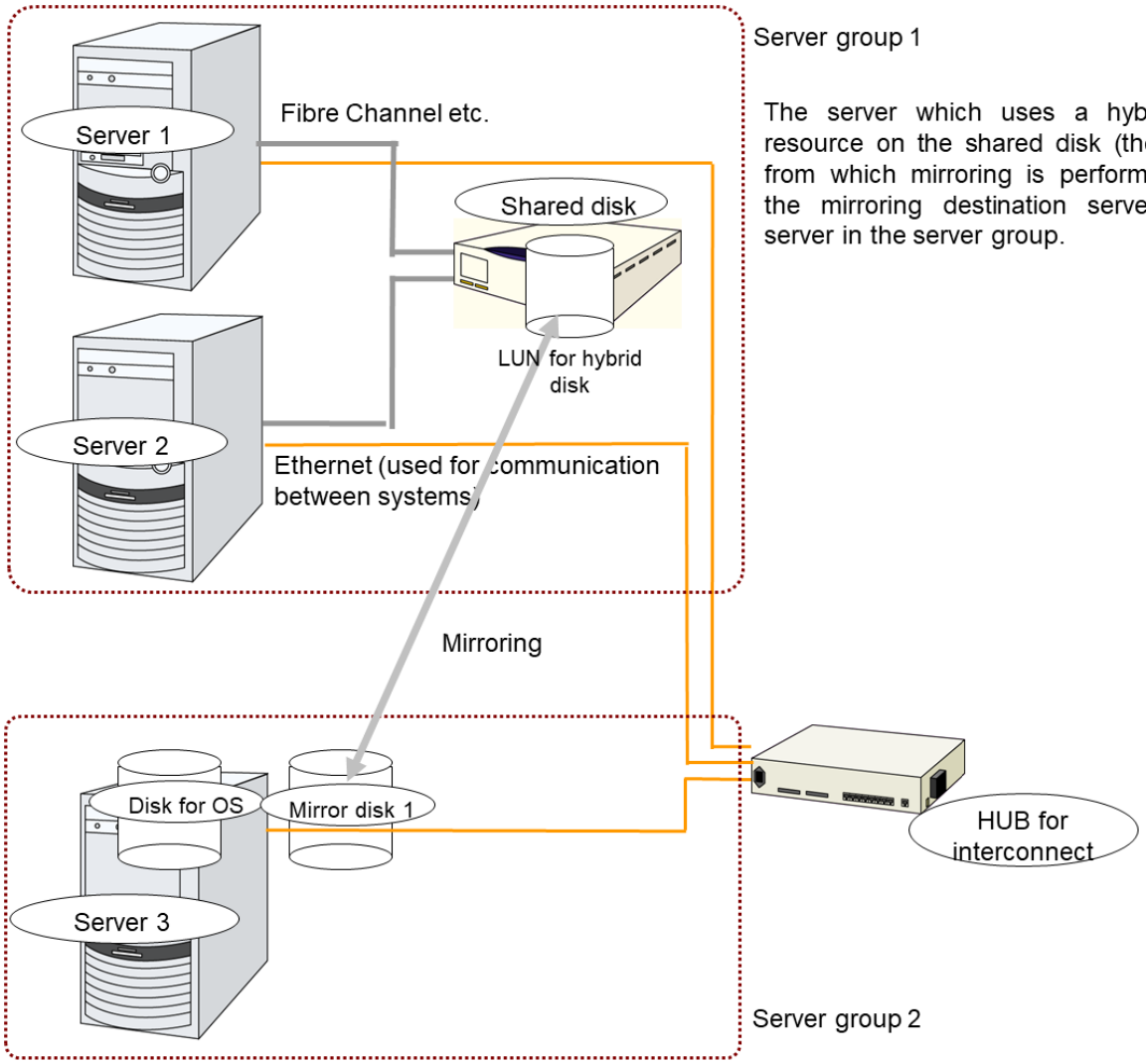
3.2.12 Understanding server groups

This section explains about server groups.

Server groups are mainly groups of servers which are required when hybrid disk resources are used.

Upon using hybrid disk resources in a shared disk device, servers connected by the same shared disk device are configured as a server group.

Upon using hybrid disk resources in a disk which is not shared, a server is configured as a server group.

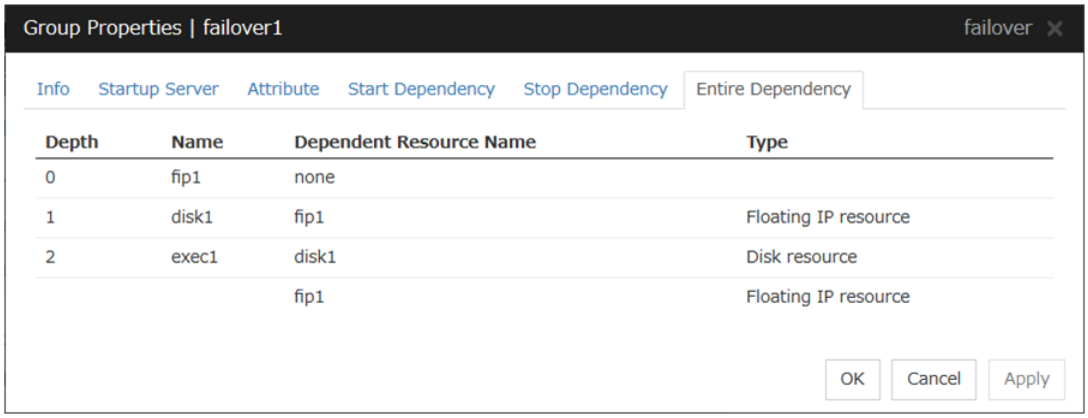


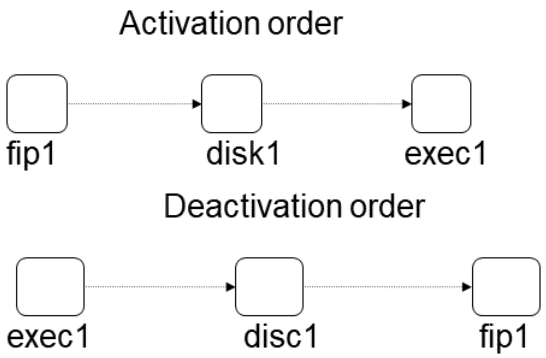
3.2.13 Understanding the settings of dependency among group resources

By specifying dependency among group resources, the order of activating them can be specified.

- When the dependency among group resources is set:
  - When activating a failover group that a group resource belongs to, its activation starts after the activation of the Dependent Resources is completed.
  - When deactivating a group resource, the deactivation of the "Dependent Resources" starts after the deactivation of the group resource is completed.

Depths for group start dependence are listed below as an example.





3.2.14 Setting group resources for individual server

Some setting values of group resources can be configured for individual servers. On the properties of resources which can be set for individual servers, tabs for each server are displayed on the **Details** tab.

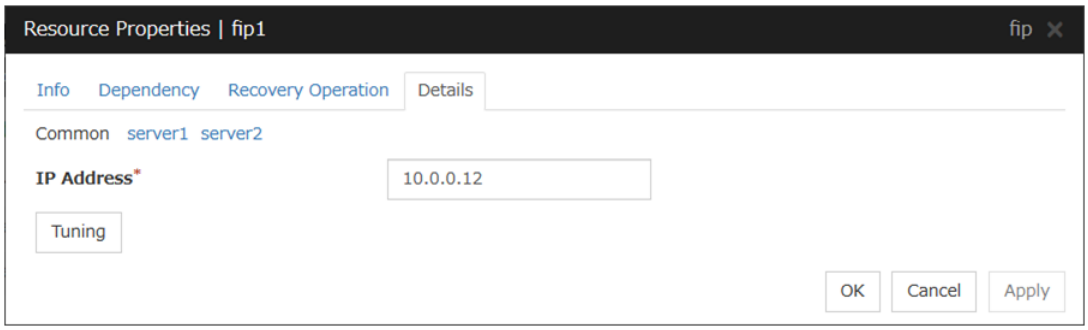
The following resources can be set for individual servers.

Group resource name	Supported version
Disk resource	4.0.0-1 or later
Floating IP resource	4.0.0-1 or later
Virtual IP resource	4.0.0-1 or later
Mirror disk resource	4.0.0-1 or later
Hybrid disk resource	4.0.0-1 or later
Dynamic DNS resource	4.0.0-1 or later
Virtual machine resource	4.0.0-1 or later
AWS Elastic IP resource	4.0.0-1 or later
AWS Virtual IP resource	4.0.0-1 or later
AWS DNS resource	4.0.0-1 or later
Azure DNS resource	4.0.0-1 or later

Note: Some parameters of Virtual IP resources, AWS Elastic IP resources, AWS Virtual IP resources, and Azure DNS resources should be configured for individual servers.

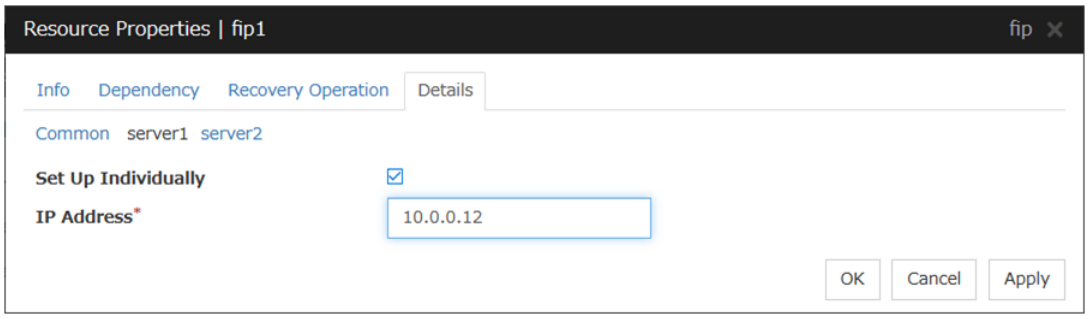
For parameters that can be set for individual servers, see the descriptions of parameters on each group resource. On those parameters, the **Server Individual Setup** icon is displayed.

In this example, the server individual setup for a Floating IP resource is explained.



Server Individual Setup

Parameters that can be set for individual servers on a Floating IP resource are displayed.



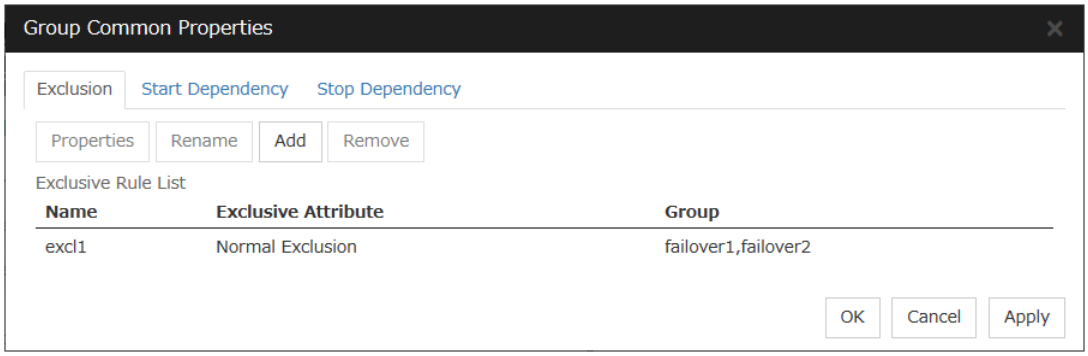
Set Up Individually

Click the tab of the server on which you want to configure the server individual setting, and select this check box. The boxes for parameters that can be configured for individual servers become active. Enter required parameters.

Note: When setting up a server individually, you cannot select **Tuning**.

3.3 Group common properties

3.3.1 Exclusion tab



Add

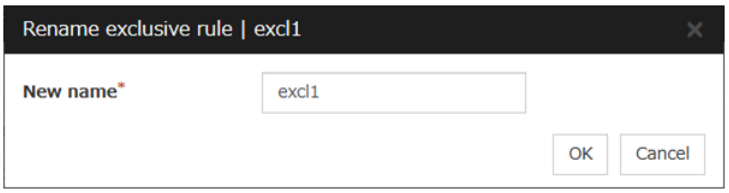
Add exclusion rules. Select **Add** to display the **Definition of Exclusion Rule** dialog box.

Remove

The confirmation dialog box is displayed.

Rename

The change server group name dialog box of the selected exclusion rule is displayed.



There are the following naming rules.

- Up to 31 characters (31 bytes).
- Names cannot start or end with a hyphen (-) or a space.
- A name consisting of only numbers is not allowed.

Names should be unique (case-insensitive) in the exclusion rule.

Properties

Display the properties of the selected exclusion rule.

Definition of exclusion rule

The name of the exclusion rule and the exclusive attribute are set. Either **Normal** or **Absolute** can be set for an exclusive attribute. **Normal** can be set just one time, whereas **Absolute** can be set more than one time. If an exclusion rule in which **Normal** is set already exists, **Normal** cannot be set any more.

Name

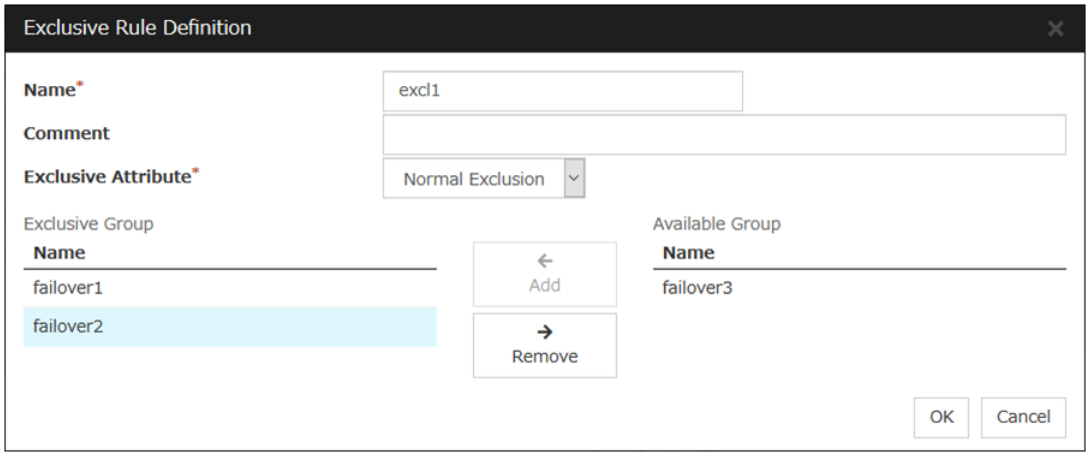
Display the exclusion rule name.

Exclusive Attribute

Display the exclusive attribute set in the exclusion rule.

Group

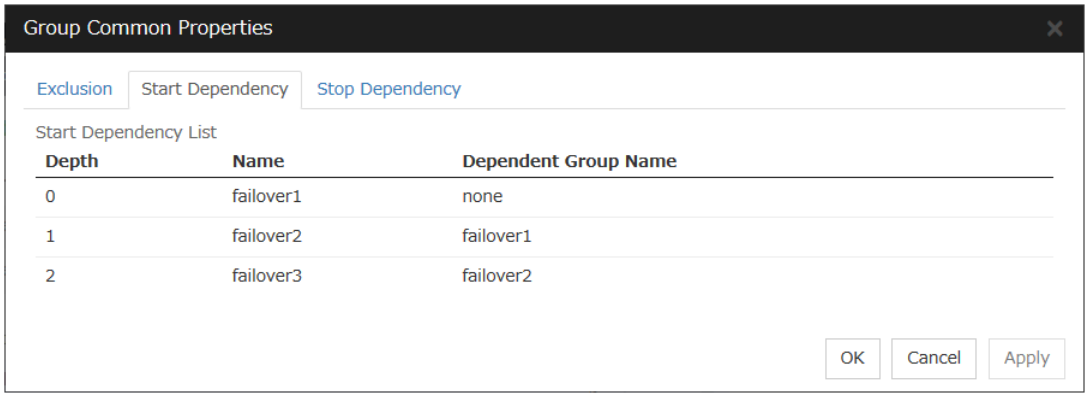
Display the list of failover group names which belong to the exclusion rule.



After selecting a group which you want to register into the exclusion rule from **Available Group**, press **Add**. **Exclusive Group** displays groups registered into the exclusion rule. A failover group added in another exclusion rule is not displayed on **Available Group**.

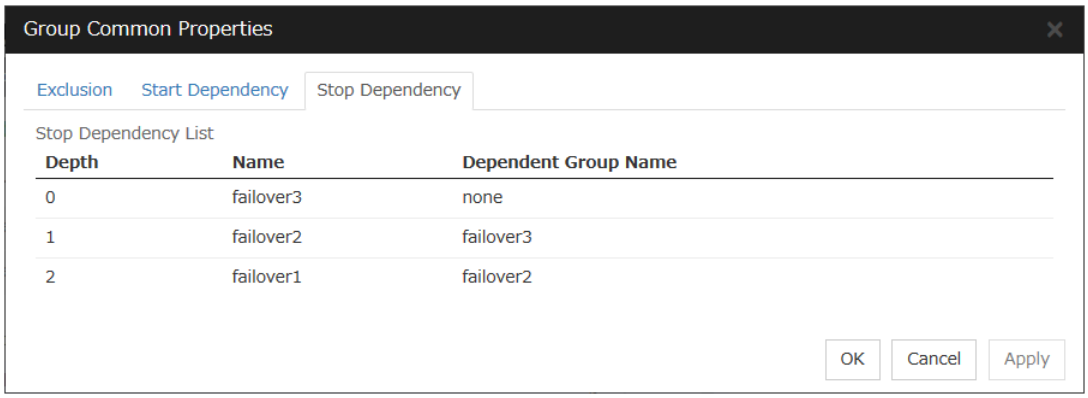
3.3.2 Start Dependency tab

Display the start dependency list.



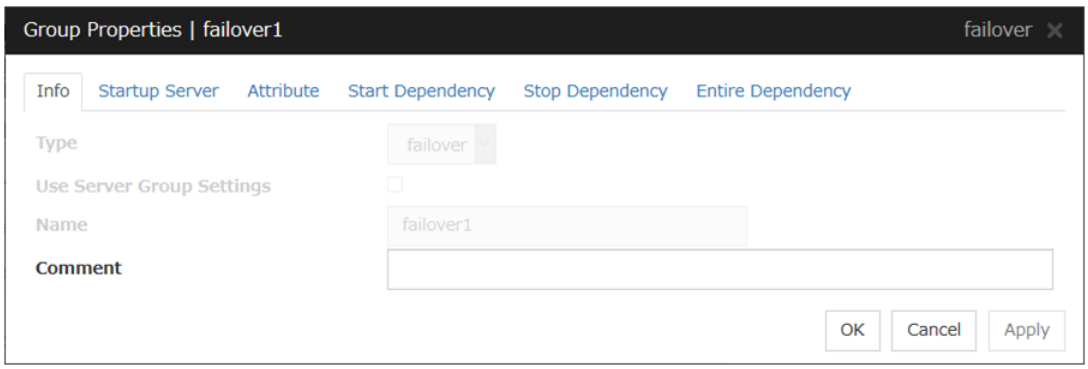
3.3.3 Stop Dependency tab

Display the stop dependency list.



3.4 Group properties

3.4.1 Info tab



Type

The group type is displayed.

Use Server Group Settings

- When the check box is selected
  Server group settings are used.
- When not selected
  Server group settings are not used.

Name

The group name is displayed.

Comment (Within 127 bytes)

Enter a comment for group. Use only one-byte alphabets and numbers.

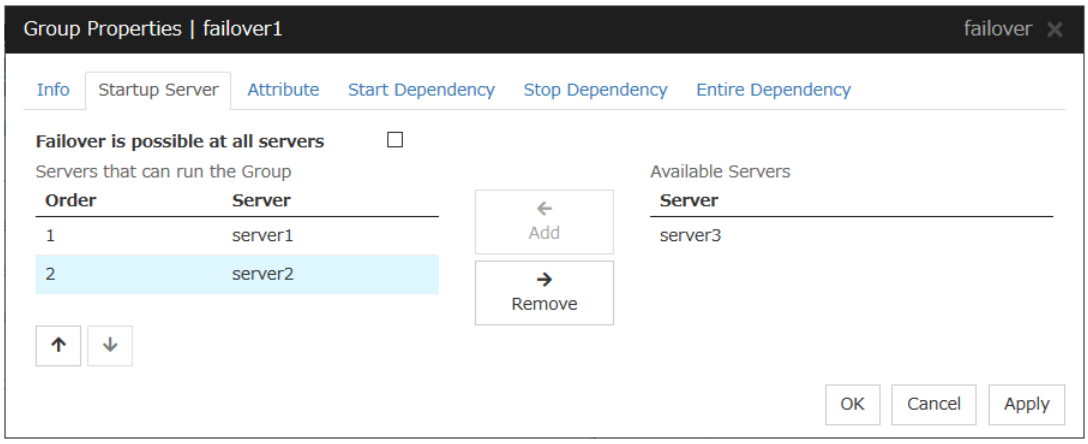
3.4.2 Startup Server tab

There are two types of settings for the server that starts up the group: starting up the group on all servers or on only the specified servers and server groups that can run the group.

If the setting on which the group is started up by all the servers is configured, all the servers in a cluster can start a group. The group startup priority of servers is same as the one of servers. For details on the server priority, see "*Master server tab*" in "*Server Common Properties*" in "*2. Parameter details*" in this guide.

When selecting servers and server groups that can run the group, you can select any server or server group from those registered to the cluster. You can also change the startup priority of servers and server groups that can run the group.

To set the server to start up the failover group:



Failover is possible on all servers

Specify the server that starts a group.

- When the check box is selected:
  All servers registered to a cluster can start a group. The priority of starting up a group is same as the one of the servers.
- When not selected:
  You can select the servers that can start a group, and change the startup priority.

Add

Use this button to add a server. Select a server that you want to add from **Available Servers**, and then click **Add**. The server is added to **Servers that can run the Group**.

Remove

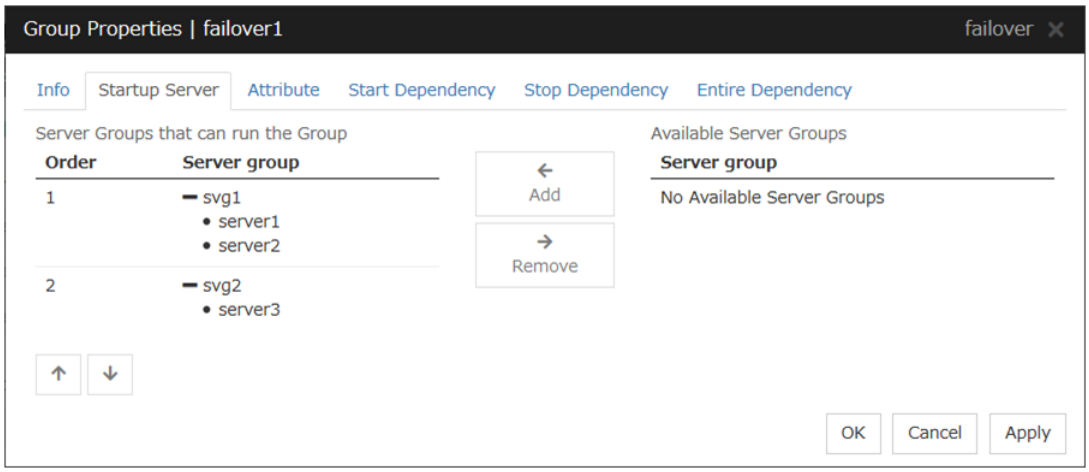
Use this button to remove a server. Select a server that you want to remove from **Servers that can run the Group**, and then click **Remove**. The server is added to **Available Servers**.

Order

Use these buttons to change the priority of the servers that can be started. Select a server whose priority you want to change from **Servers that can run the Group**. Click **the arrows** to move the selected row upward or downward.

To use the server group settings:

It is necessary to configure a server group that starts up the failover group for the settings of a server that starts up a group including a hybrid disk resource.



Add

Use **Add** to add a server group to **Server Groups that can run the Group**. Select a server group that you want to add from **Available Server Groups**, and then click **Add**. The selected server group is added to **Server Groups that can run the Group**.

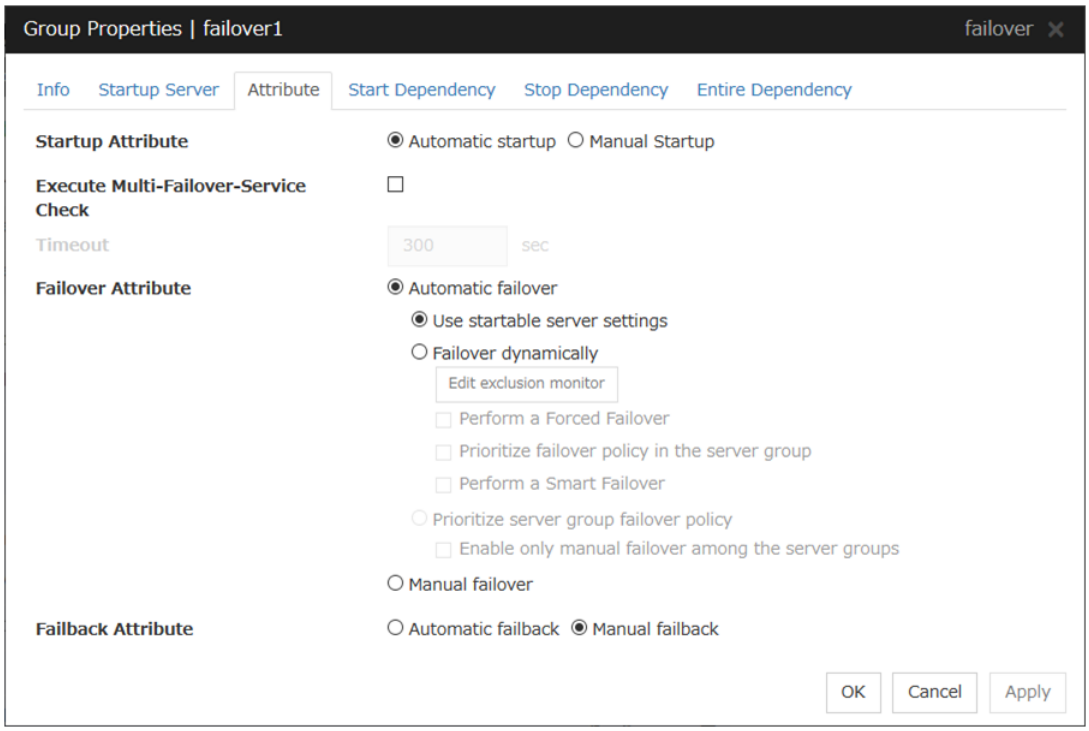
Remove

Use **Remove** to remove a server group from **Server Groups that can run the Group**. Select a server group that you want to remove from **Available Server Groups**, and then click **Remove**. The server is added to **Server Groups that can run the Group**.

Order

Use these buttons to change the priority of a server group. Select a server group whose priority you want to change from **Server Groups that can run the Group**. Click **the arrows** to move the selected row upward or downward.

3.4.3 Attribute tab



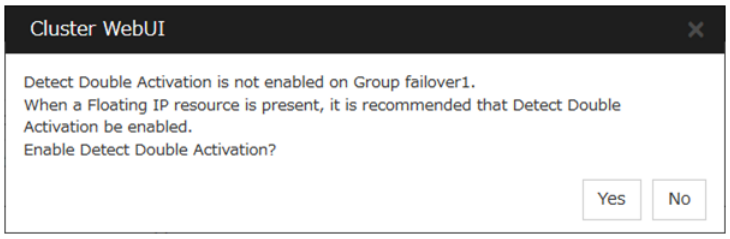
Startup Attribute

Select whether to automatically start the group from EXPRESSCLUSTER (auto startup), or to manually start from the Cluster WebUI or by using the clpgrp command (manual startup) at the cluster startup.

- Auto Startup
  The group will automatically be started at the cluster startup (active state).
- Manual Startup
  The group will not be started at the cluster startup (inactive state).
  You can start the group from the Cluster WebUI or by using the clpgrp command (active state).

Execute Multi-Failover-Service Check

Check whether a double activation will occur or not before a group is started. If this function is set to disabled for the group whose floating IP resource exists, the following pop-up window appears when the cluster configuration information is applied.



If **Yes** is selected, **Detect double activation** is automatically enabled, and the cluster configuration information is uploaded. If **No** is selected, the cluster configuration information is uploaded while **Detect double activation** remains disabled.

Timeout (1 to 9999)

Specify the maximum time to be taken to check a double activation. The default value is set as 300 seconds. Specify a larger value than the one set for **Ping Timeout** of **Floating IP Resource Tuning Properties** for the floating IP resource that belongs to the group.

Failover Attribute

Select if the failover is automatically performed when a server fails.

- Auto Failover
  Failover is executed automatically. In addition, the following options can be selected.
  - Use the startup server settings
    This is the default setting.
  - Fail over dynamically
    The failover destination is determined by considering the statuses of each server's monitor or failover group at the time of the failover.
    If this option button is selected, all the failback attribute parameters are reverted to the default values and grayed out.
    If dynamic failover is selected, each option can be set. For details, see "*Understanding the group properties*".
  - Prioritize failover policy in the server group
    This function controls failovers between sites (between server groups).
    However, if no server group is specified for the failover group, the display for failovers between sites is grayed out.
    The **Enable only manual failover among the server groups** check box can be selected only when this option button is selected.
    If the **Prioritize failover policy in the server group** option button is selected, the failover policies in the same server group take priority when determining the failover destination.
    If the **Prioritize failover policy in the server group** option button and **Enable only manual failover among the server groups** check box are selected, failovers across server groups are not automatically performed. Manually move groups between server groups.
- Manual Failover
  Failover is executed manually.

Failback Attribute

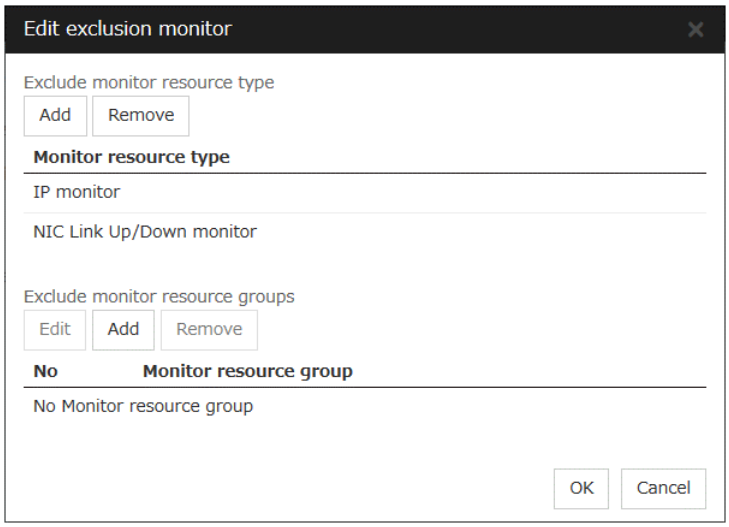
Select if the failback is executed automatically to the group when a server that has a higher priority than other server where the group is active is started. For groups that have mirror disk resources or hybrid disk resources, select manual failback.

- Auto Failback
  Failback is executed automatically.
- Manual Failback
  Failback is not executed automatically.

Edit exclusive monitor

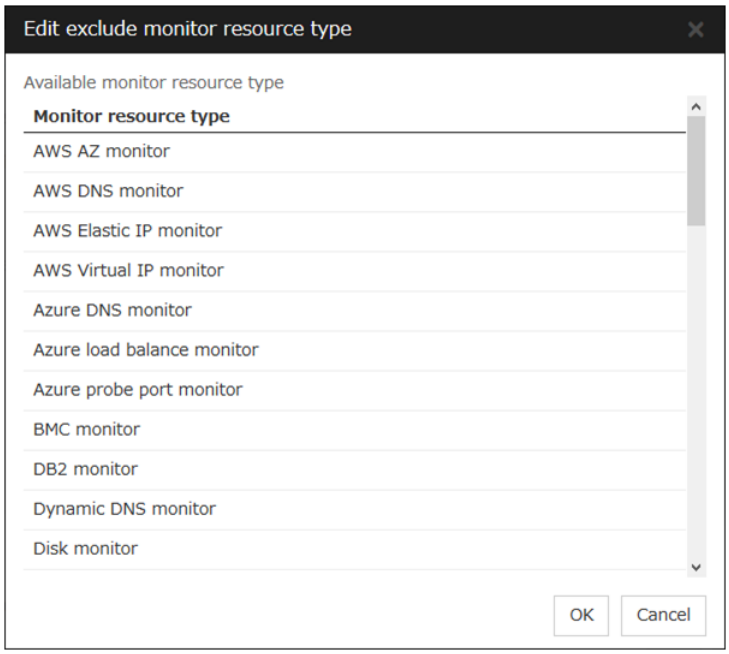
Dynamic failover excludes the server for which the monitor resource has detected an error, from the failover destinations. If **Fail over dynamically** is selected as the failover attribute, you can set the monitor resource to be excluded.

The exclusive list can be set with the monitor resource type and monitor resource name.



- Add exclusive monitor resource type
  Adds the exclusive monitor resource type.

  Any server, in which even one monitor resource of the added monitor resource type is abnormal, is excluded from the failover destinations.



  Adds the selected monitor resource type.

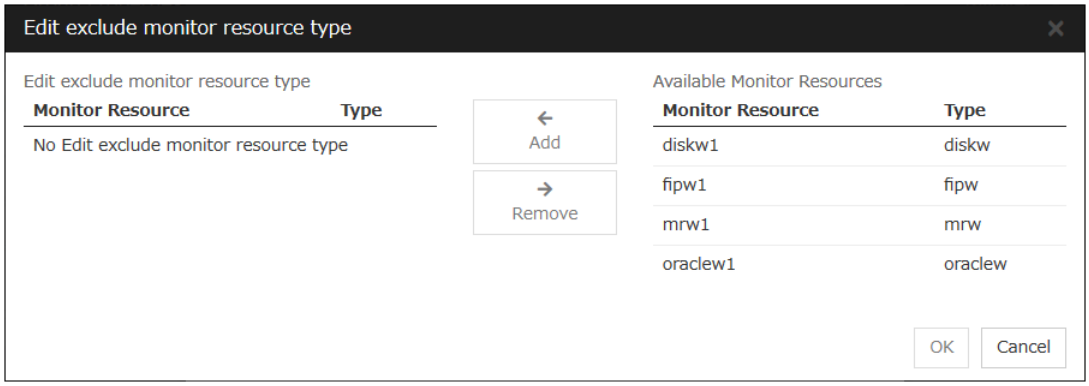
- Remove exclusive monitor resource type
  Removes the selected exclusive monitor resource type.

- Add exclusive monitor resource group
  Adds the exclusive monitor resource group.
  The maximum number of exclusive monitor resource groups to be registered is 32.

If multiple monitor resources are registered in a single exclusive monitor resource group, the server in which all the registered monitor resources are abnormal is excluded from the failover destinations.

Moreover, if multiple exclusive monitor resource groups are registered, a server that satisfies at least one

of the conditions is excluded from the failover destinations.



Add

Adds the monitor resource selected from **Available monitor resource list** to **Monitor resource lis**t.

Remove

Removes the monitor resource selected with **Monitor resource list**, from the list.

- Delete exclusive monitor resource group
  Removes the selected exclusive monitor resource group.
- Edit exclusive monitor resource group
  Edits the selected exclusive monitor resource group.

Note: The following monitor resource types cannot be registered for the exclusive monitor resource type. Moreover, a resource name cannot be registered for the exclusive monitor resource group.

- User mode monitor
- ARP monitor
- Virtual IP monitor
- Mirror disk connect monitor
- Hybrid disk monitor
- Hybrid disk connect monitor

Note:

The monitor resource in the warning status is not handled as being abnormal. The exception to this is the mirror disk monitor resource.

The monitor resource set for monitoring at activation does not enter the abnormal status because it does not perform monitoring for a server other than the group start server.

The monitor resource stopped with the Cluster WebUI or clpmonctrl command enters the normal status.

A server that has not been set to monitor a monitor resource does not enter the abnormal status because it does not perform monitoring.

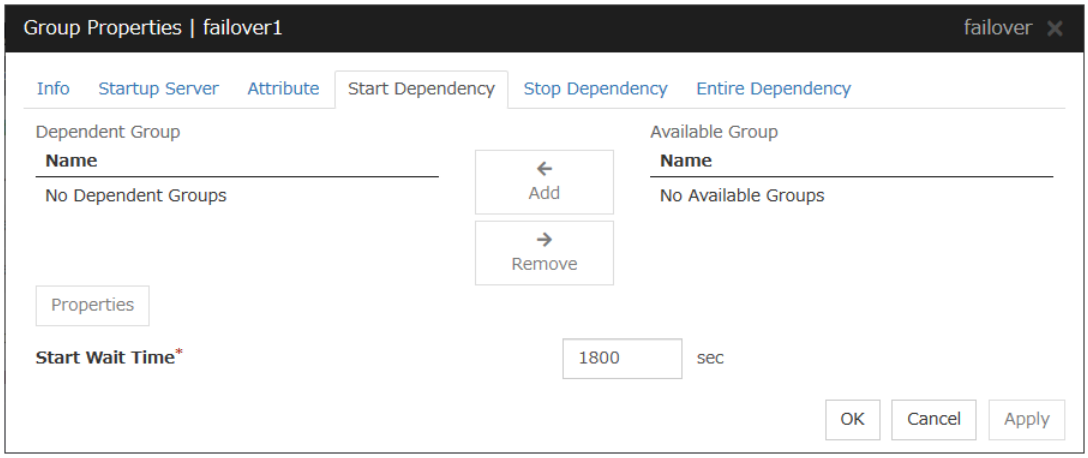
Note:

In the case of the mirror disk monitor resource, a check is made as to whether the mirror disk resource can be activated. There is no dependence on the status of the mirror disk monitor resource.

Even if the mirror disk monitor resource is in the error status, the server on which the mirror disk resource can be activated normally is not excluded from the failover destination.

Even if the mirror disk monitor resource is in the normal or caution status, the server on which the mirror disk resource cannot be activated normally is excluded from the failover destination.

3.4.4 Start Dependency tab



Add

Clicking **Add** adds the group selected from **Available Group** to **Dependent Group**.

Remove

Clicking **Remove** removes the group selected from **Dependent Group**.

Start Wait Time (0 to 9999)

Specify how many seconds you want to wait before a timeout in the target group start process. The default value is 1800 seconds.

Property

Clicking **Property** changes the properties of the group selected from **Dependent Group**.

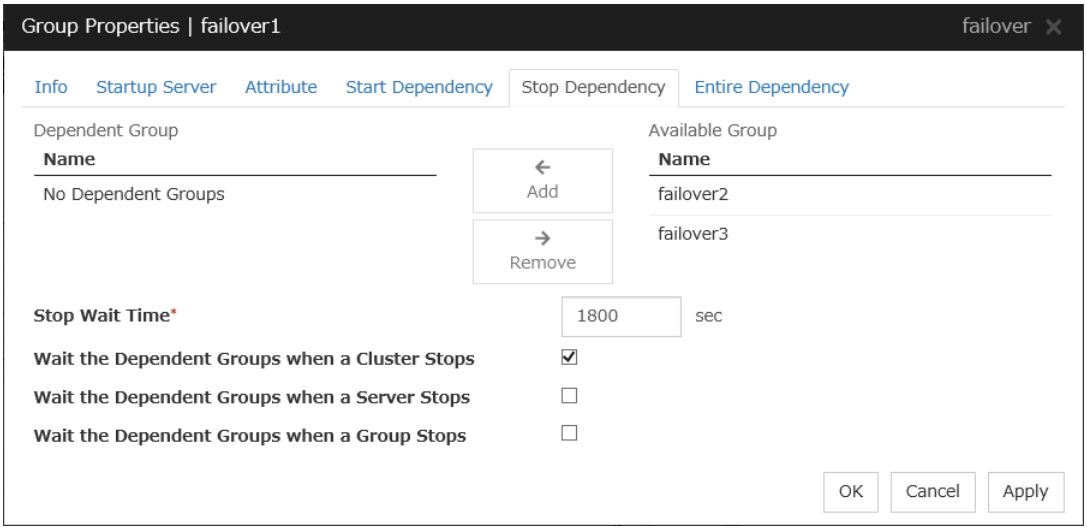
Wait Only when on the Same Server

Specify whether you wait for start waiting only when the group which starts waiting and the target group start on the same server.

- When **Wait Only when on the Same Server** is selected

- When the server which starts the group that starts waiting isn't included in the Startup Server of a target group, you don't wait.
- When a target group fails to start on a server other than the server which starts the group that starts waiting, you don't wait.

3.4.5 Stop Dependency tab



Add

Clicking **Add** adds the group selected from **Available Group** to **Dependent Group**.

Remove

Clicking **Remove** removes the group selected from **Dependent Group**.

Stop Wait Time (0 to 9999)

Specify how many seconds to wait before a timeout occurs in the target group stop processing. The default value is 1800 seconds.

Wait the Dependent Groups when a Cluster Stops

Specify whether to wait for the dependent groups to stop when the cluster stops.

Wait the Dependent Groups when a Server Stops

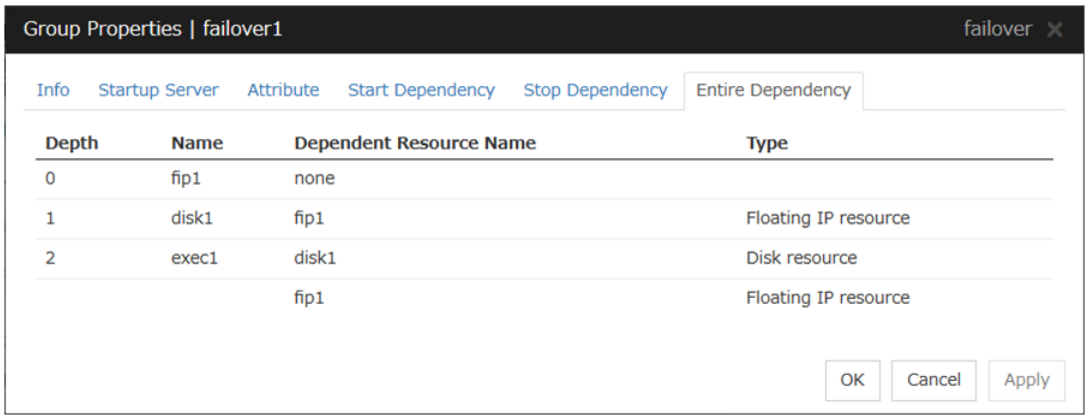
Specify whether to wait for the dependent groups to stop when a single server stops. This option waits for the stop of only those groups running on the same server, among all the dependent groups.

Wait the Dependent Groups when a Group Stops

Specify whether to wait for the dependent groups to stop when the groups are being stopped. This option waits for the stop of only those groups running on the same server, among all the dependent groups.

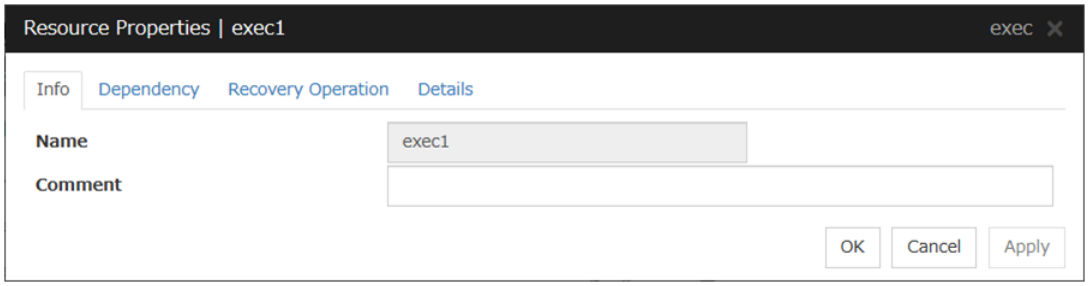
3.4.6 Entire Dependency tab

Displays the settings of dependency among group resources.



3.5 Resource Properties

3.5.1 Info tab



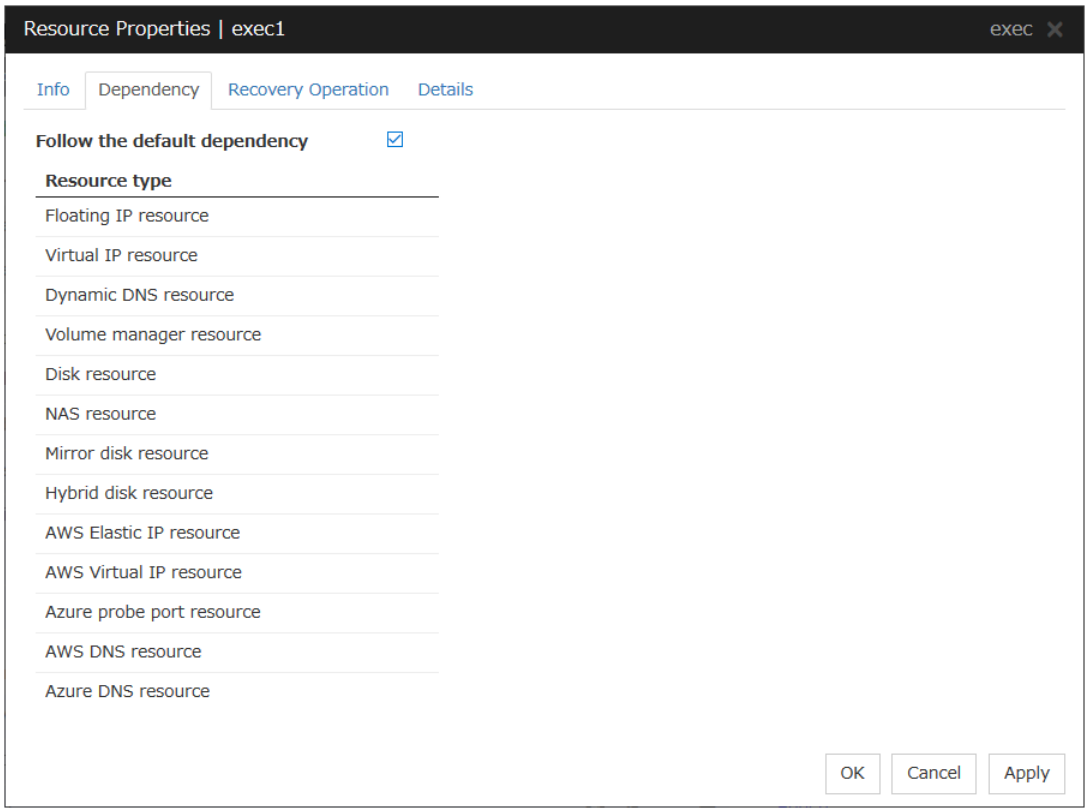
Name

The resource name is displayed.

Comment (Within 127 bytes)

Enter a comment for the resource. Use only one-byte alphabets and numbers.

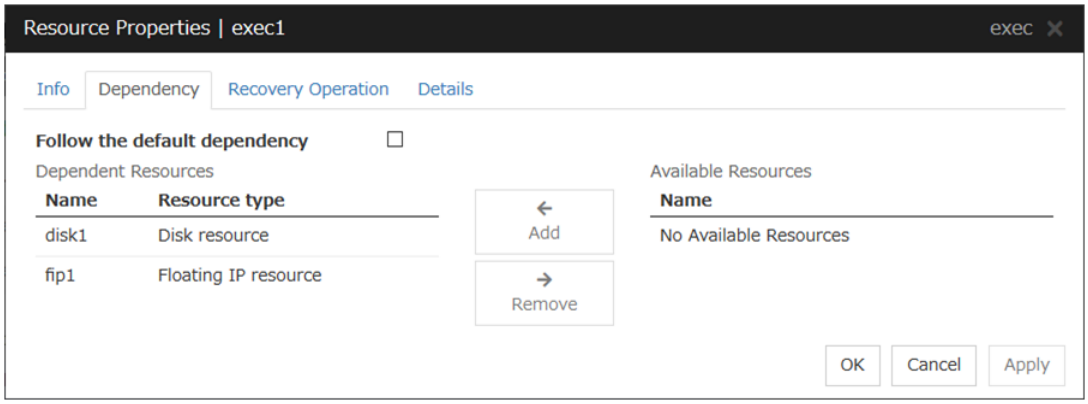
3.5.2 Dependency tab



Follow the default dependence

Select if the selected group resource follows the default EXPRESSCLUSTER dependency.

- When Follow the default dependence is selected:
  The selected group resource depends on the type(s) of resources.
  See "*Parameters list*" in 2. *Parameter details*" for the default dependency of each resource.
  When there is more than one resource of the same type, the selected group resource depends on all resources of that type.
- When Follow the default dependence is not selected:
  The selected group resource depends on the specified resource.



Add

It is used when adding the group resource selected in **Available Resources** to **Dependent Resources**.

Remove

It is used when removing the group resource selected in **Dependent Resources** from **Dependent Resources**.

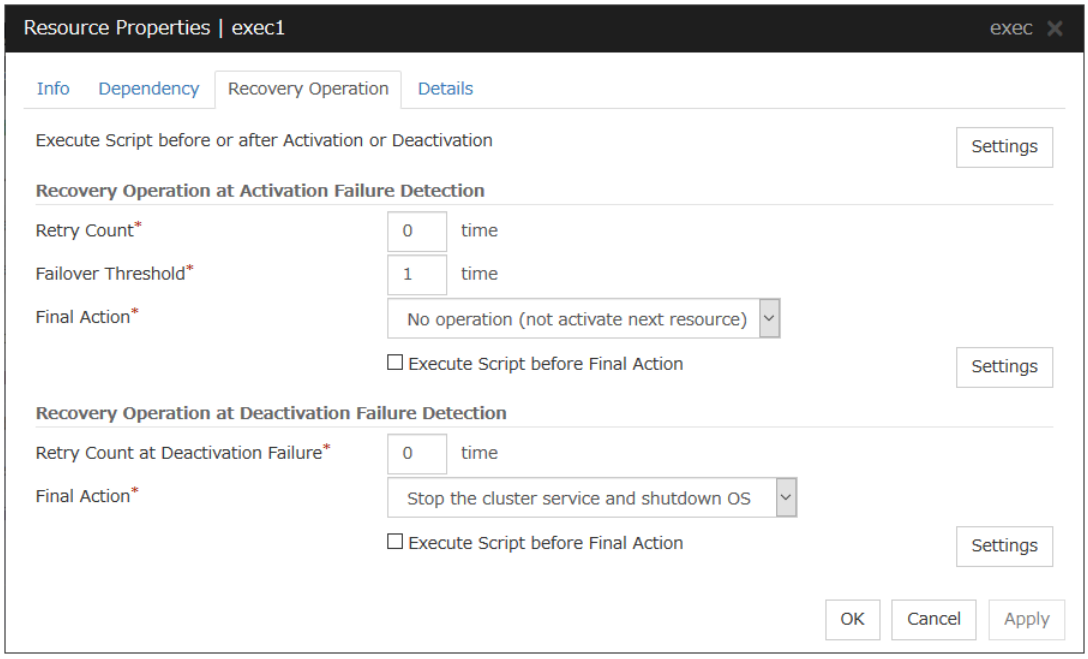
3.5.3 Recovery Operation tab

When an error in activation of the group resource is detected

- When an error is detected while activating the group resource, try activating it again.
- When the activation retry count exceeds the number of times set in **Retry Count at Activation Failure**, failover is executed.
- When the group resource cannot be activated even after executing a failover as many times as specified in **Failover Threshold**, the final action is taken.

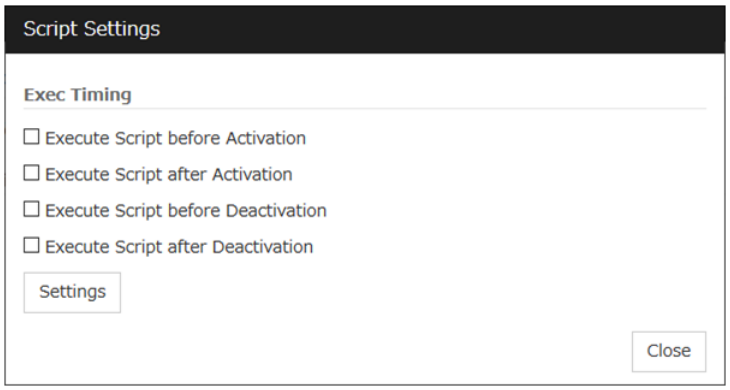
When an error in deactivation of the group resource is detected

- When an error is detected while deactivating the group resource, try deactivating it again.
- When the deactivation retry count exceeds the number of times set in **Retry Count at Deactivation Failure**, the final action is taken.



Execute Script before or after Activation or Deactivation

Select whether script is running or not before and after activation/deactivation of group resources. To configure the script settings, click Script Settings.



The script can be run at the specified timing by selecting the checkbox.

Exec Timing

Execute Script before Activation

- Checkbox is on
  The script is executed before the resource is activated.
- Checkbox is off
  The script is not executed before the resource is activated.

Execute Script after Activation

- Checkbox is on
  The script is executed after the resources is activated.
- Checkbox is off
  The script is not executed after the resources is activated.

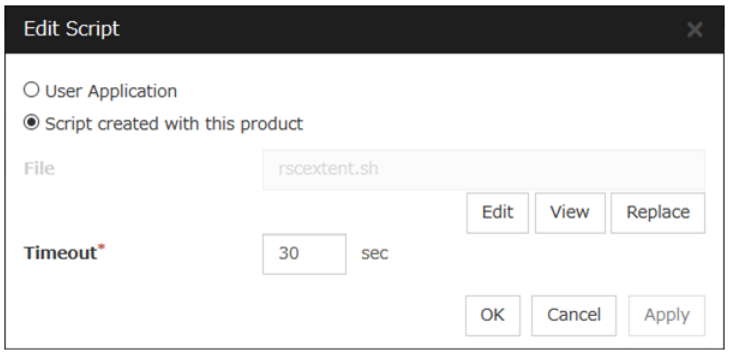
Execute Script before Deactivation

- Checkbox is on
  The script is executed before the resource is deactivated.
- Checkbox is off
  The script is not executed before the resource is deactivated.

Execute Script after Deactivation

- Checkbox is on
  The script is executed after the resource is deactivated.
- Checkbox is off
  The script is not executed after the resource is deactivated.

To configure the script settings, click Script Settings.



User Application

Use an executable file (executable shell script file or execution file) on the server as a script. For the file name, specify an absolute path or name of the executable file of the local disk on the server. If there is any blank in the absolute path or the file name, put them in double quotation marks ("") as follows.

```
Example:
"/tmp/user application/script.sh"
```

Each executable files is not included in the cluster configuration information of the Cluster WebUI. They must be prepared on each server because they cannot be edited nor uploaded by the Cluster WebUI.

Script created with this product

Use a script file which is prepared by the Cluster WebUI as a script. You can edit the script file with the Cluster WebUI if you need. The script file is included in the cluster configuration information.

File (Within 1023 bytes)

Specify a script to be executed (executable shell script file or execution file) when you select **User Application**.

View

Click here to display the script file when you select **Script created with this product**.

Edit

Click here to edit the script file when you select **Script created with this product**. Click **Save** to apply the change. You cannot modify the name of the script file.

Replace

Click here to replace the contents of a script file with the contents of the script file which you selected in the file selection dialog box when you select **Script created with this product**. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not select binary files (applications), and so on.

Timeout (1 to 9999)

Specify the maximum time to wait for completion of script to be executed.

The default value of the time taken to execute script before and after activation/deactivation is 30 seconds.

The default value of the timeout settable from **Settings** button of **Execute Script before Final Action** for **Recovery Operation at Activation Failure Detection** or **Recovery Operation at Deactivation Failure Detection** is 5 seconds.

Recovery Operation at Activation Failure Detection

Retry Count at Activation Failure (0 to 99)

Enter how many times to retry activation when an activation error is detected. If this is set to zero (0), the activation will not be retried.

Failover Threshold (0 to 99)

Enter how many times to retry failover after activation retry fails as many times as the number of times set in **Retry Count at Activation Failure** when an error in activation is detected.

If this is set to zero (0), failover will not be executed.

Final Action

Select an action to be taken when activation retry failed the number of times specified in **Activation Retry Threshold** and failover failed as many times as the number of times specified in **Failover Threshold** when an activation error is detected.

Select a final action from the following:

- No Operation (Activate next resource):
  Continues the group start process.
- No Operation (Not activate next resource):
  Cancels the group start process.
- Stop Group:
  Deactivates all resources in the group of which the group resource that an activation error is detected.
- Stop cluster service:
  Stops the cluster service of the server of which an activation error is detected.
- Stop cluster service and shutdown OS:
  Stops the cluster service of the server of which an activation error is detected, and shuts down the OS.
- Stop cluster service and reboot OS:
  Stops the cluster service of the server where an activation error is detected, and restarts the OS.
- Sysrq Panic:
  Performs the sysrq panic.

  Note: If performing the sysrq panic fails, the OS is shut down.

- Keepalive Reset:
  Resets the OS using the clpkhb or clpka driver.

  Note: If resetting keepalive fails, the OS is shut down. Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported

- Keepalive Panic:
  Performs the OS panic using the clpkhb or clpka driver.

  Note: If performing the keepalive panic fails, the OS is shut down. Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported.

- BMC Reset:

Perform hardware reset on the server by using the ipmi command.

Note: If resetting BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC Power Off:
  Powers off the OS by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

  Note: If powering off BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC Power Cycle:
  Performs the power cycle (powering on/off) of the server by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

  Note: If performing the power cycle of BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC NMI:
  Uses the ipmi command to cause NMI occur on the server. Actions after NMI occurrence depend on the OS settings.

  Note: If BMC NMI fails, the OS shutdown is performed. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- I/O Fencing(High-End Server Option)
  It can't be used.

  Note: If I/O Fencing(High-End Server Option) fails, the OS shutdown is performed.

Execute Script before Final Action

Select whether script is run or not before executing final action when an activation failure is detected.

- When the check box is selected:
  A script/command is run before executing final action. To configure the script/command setting, click **Settings**.
  For the settings of the script, refer to the explanation about the script settings in "Execute Script before or after Activation or Deactivation".
- When the check box is not selected:
  Any script/command is not run.

Recovery Operation at Deactivation Failure Detection

Retry Count at Deactivation Failure (0 to 99)

Enter how many times to retry deactivation when an error in deactivation is detected.

If you set this to zero (0), deactivation will not be retried.

Final Action

Select the action to be taken when deactivation retry failed the number of times specified in **Retry Count at Deactivation Failure** when an error in deactivation is detected.

Select the final action from the following:

- No Operation (Deactivate next resource):
  Continue the group stop process.

  Note:

  If **No Operation** is selected as the final action when a deactivation error is detected, group does not stop but remains in the deactivation error status.
  Make sure not to set **No Operation** in the production environment.

- No Operation (Not deactivate next resource):
  Cancel the group start process.

  Note:

  If **No Operation** is selected as the final action when a deactivation error is detected, group does not stop but remains in the deactivation error status.
  Make sure not to set **No Operation** in the production environment.

- Stop cluster service and shutdown OS:
  Stop the cluster daemon on the server of which error in deactivation is detected, and shut down the OS.
- Stop cluster service and reboot OS:
  Stop the cluster daemon on the server where an error in deactivation is detected, and restart the OS.
- Sysrq Panic:
  Performs the sysrq panic.

  Note: If performing the sysrq panic fails, the OS is shut down.

- Keepalive Reset:
  Resets the OS using the clpkhb or clpka driver.

  Note: If resetting keepalive fails, the OS is shut down. Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported

- Keepalive Panic:
  Performs the OS panic using the clpkhb or clpka driver.

  Note: If performing the keepalive panic fails, the OS is shut down. Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported.

- BMC Reset:

Perform hardware reset on the server by using the ipmi command.

Note: If resetting BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC Power Off:
  Powers off the OS by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

  Note: If powering off BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC Power Cycle:
  Performs the power cycle (powering on/off) of the server by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

  Note: If performing the power cycle of BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC NMI:
  Uses the ipmi command to cause NMI occur on the server. Actions after NMI occurrence depend on the OS settings.

  Note: If BMC NMI fails, the OS shutdown is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- I/O Fencing(High-End Server Option):
  It can't be used.

  Note: If I/O Fencing(High-End Server Option) fails, the OS shutdown is performed.

Execute Script before Final Action

Select whether script is run or not before executing final action when a deactivation failure is detected.

- When the check box is selected:
  A script/command is run before executing final action. To configure the script/command setting, click **Settings**.
  For the settings of the script, refer to the explanation about the script settings in "Execute Script before or after Activation or Deactivation".
- When the check box is not selected:
  Any script/command is not run.

3.5.4 Details tab

The parameters specific to each resource are described in its explanation part.

3.6 Understanding EXEC resources

You can register applications and shell scripts that are managed by EXPRESSCLUSTER and to be run when starting, stopping, failing over or moving groups in EXPRESSCLUSTER. It is also possible to register your own programs and shell scripts in EXEC resources. You can write codes as required for respective application because shell scripts are in the same format as an sh shell script.

Note: The same version of the application to be run from EXEC resources must be installed on all servers in failover policy.

3.6.1 Dependency of EXEC resources

By default, exec resources depend on the following group resource types:

Group resource type
Floating IP resource
Virtual IP resource
Disk resource
Mirror disk resource
Hybrid disk resource
NAS resource
VM resource
Volume manager resource
Dynamic DNS resource
AWS elastic ip resource
AWS virtual ip resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.6.2 Method of judging EXEC resource activation/deactivation results

The activation/deactivation results are judged based on the results of executing the applications and shell scripts registered in the EXEC resources.

If the end code of an application or a shell script is 0, it is judged that activation/deactivation was performed normally and successfully.

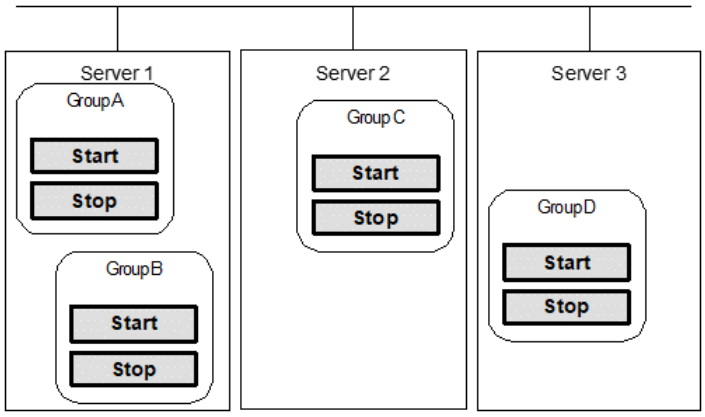
If the end code is other than 0, it is judged that activation/deactivation has failed.

If a start/stop script timeout occurs, it is judged that activation/deactivation has failed.

3.6.3 Scripts in EXEC resources

Types of scripts

Start script and stop script are provided in EXEC resources. EXPRESSCLUSTER runs a script for each EXEC resource when the cluster needs to change its status. You have to write procedures in these scripts about how you want applications to be started, stopped, and restored in your cluster environment.



Start: Start script
Stop: Stop script

3.6.4 Environment variables in EXEC resource script

When EXPRESSCLUSTER runs a script, it records information such as condition when the scrip was run (script starting factor) in environment variables.

You can use the environment variables in the table below as branching condition when you write codes for your system operation.

Stop script returns the contents of the previous start script in the environment variable as a value. Start script does not set environment variables of CLP_FACTOR and CLP_PID.

The environment variable CLP_LASTACTION is set only when the environment variable CLP_FACTOR is CLUSTERSHUTDOWN or SERVERSHUTDOWN.

Environment Variable	Value of environment variable	Meaning
CLP_EVENT ...script starting factor	START	The script was run: • by starting a cluster; • by starting a group; • on the destination server by moving a group; • on the same server by restarting a group due to the detection of a monitor resource error; or • on the same server by restarting a group resource due to the detection of a monitor resource error.

Continued on next page

Table 3.7 – continued from previous page

Environment Variable	Value of environment variable	Meaning
	FAILOVER	The script was run on the failover target server: • by the failure of the server; • due to the detection of a monitor resource error; or • because activation of group resources failed.
CLP_FACTOR ...group stopping factor	CLUSTERSHUTDOWN	The group was stopped by stopping the cluster.
	SERVERSHUTDOWN	The group was stopped by stopping the server.
	GROUPSTOP	The group was stopped by stopping the group.
	GROUPMOVE	The group was moved by moving the group.
	GROUPFAILOVER	The group failed over because an error was detected in monitor resource; or the group failed over because of activation failure in group resources.
	GROUPRESTART	The group was restarted because an error was detected in monitor resource.
	RESOURCERESTART	The group resource was restarted because an error was detected in monitor resource.
CLP_LASTACTION ...process after cluster shutdown	REBOOT	In case of rebooting OS
	HALT	In case of halting OS
	NONE	No action was taken.
CLP_SERVER ...server where the script was run	HOME	The script was run on the primary server of the group.
	OTHER	The script was run on a server other than the primary server of the group.
CLP_DISK[1] ...partition connection information on shared or mirror disks	SUCCESS	There was no partition where connection had failed.
	FAILURE	There was one or more partition where connection had failed.

Continued on next page

Table 3.7 – continued from previous page

Environment Variable	Value of environment variable	Meaning
CLP_PRIORITY ... the order in failover policy of the server where the script is run	1 to the number of servers in the cluster	Represents the priority of the server where the script is run. This number starts from 1 (The smaller the number, the higher the server's priority). If CLP_PRIORITY is 1, it means that the script is run on the primary server.
CLP_GROUPNAME ...Group name	Group name	Represents the name of the group to which the script belongs.
CLP_RESOURCENAME ...Resource name	Resource name	Represents the name of the resource to which the script belongs.
CLP_PID ...Process ID	Process ID	Represents the process ID of start script when the property of start script is set to asynchronous. This environment variable is null when the start script is set to synchronous.
CLP_VERSION_FULL ...EXPRESSCLUSTER full version	EXPRESSCLUSTER full version	Represents the EXPRESSCLUSTER full version. (Example) 4.2.2-1
CLP_VERSION_MAJOR ...EXPRESSCLUSTER major version	EXPRESSCLUSTER major version	Represents the EXPRESSCLUSTER major version. (Example) 4
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER install path	Represents the path where EXPRESSCLUSTER is installed. (Example) /opt/nec/clusterpro
CLP_OSNAME ...Server OS name	Server OS name	Represents the OS name of the server where the script was executed. (Example) 1. When the OS name could be acquired: Red Hat Enterprise Linux Server release 6.8 (Santiago) 2. When the OS name could not be acquired: Linux

Continued on next page

Table 3.7 – continued from previous page

Environment Variable	Value of environment variable	Meaning
CLP_OSVER ...Server OS version	Server OS version	Represents the OS version of the server where the script was executed. (Example) 1. When the OS version could be acquired: 6.8 2. When the OS version could not be acquired: Blank

If the script is executed on the standby server, with **Execute on standby server** of **Exec Resource Tuning Properties** enabled, the following information is recorded in environment variables:

Environment variable	Value of environment variable	Meaning
CLP_EVENT ...script starting factor	STANDBY	The script was run on the standby server.
CLP_SERVER ...server where the script was run	HOME	The script was run on the primary server of the group.
	OTHER	The script was run on a server other than the primary server of the group.
CLP_PRIORITY ... the order in failover policy of the server where the script is run	1 to the number of servers in the cluster	Represents the priority of the server where the script is run. This number starts from 1 (The smaller the number, the higher the server's priority). If CLP_PRIORITY is 1, it means that the script is run on the primary server.
CLP_GROUPNAME ...Group name	Group name	Represents the name of the group to which the script belongs.
CLP_RESOURCENAME ...Resource name	Resource name	Represents the name of the resource to which the script belongs.

Continued on next page

[1] It is available for disk resource, mirror disk resource, hybrid disk resource, NAS resource and volume manager resource.

Table 3.8 – continued from previous page

Environment variable	Value of environment variable	Meaning
CLP_VERSION_FULL ...Full version of EXPRESSCLUSTER	Full version of EXPRESSCLUSTER	Represents the full version of EXPRESSCLUSTER (e.g. 4.2.2-1).
CLP_VERSION_MAJOR ...Major version of EXPRESSCLUSTER	Major version of EXPRESSCLUSTER	Represents the major version of EXPRESSCLUSTER (e.g. 4).
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER installation path	Represents the EXPRESSCLUSTER installation path (e.g. /opt/nec/clusterpro).
CLP_OSNAME ...Server OS name	Server OS name	Represents the OS name of the server where the script was executed. (Example) 1. When the OS name was acquired: Red Hat Enterprise Linux Server release 6.8 (Santiago) 2. When the OS name was not acquired: Linux
CLP_OSVER ...Server OS version	Server OS version	Represents the OS version of the server where the script was executed. (Example) 1. When the OS version was acquired: 6.8 2. When the OS version was not acquired: Blank

3.6.5 Execution timing of EXEC resource script

This section describes the relationships between the execution timings of start and stop scripts and environment variables according to cluster status transition diagram.

- To simplify the explanations, 2-server cluster configuration is used as an example. See the supplements for the relations between possible execution timings and environment variables in 3 or more server configurations.
- O and X in the diagrams represent the server status.

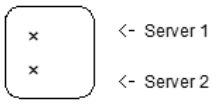
Server	Server status
O	Normal (properly working as a cluster)
X	Stopped (cluster is stopped)

(Example) OA: Group A is working on a normally running server.

- Each group is started on the top priority server among active servers.
- Three Group A, B and C are defined in the cluster, and they have their own failover policies as follows:

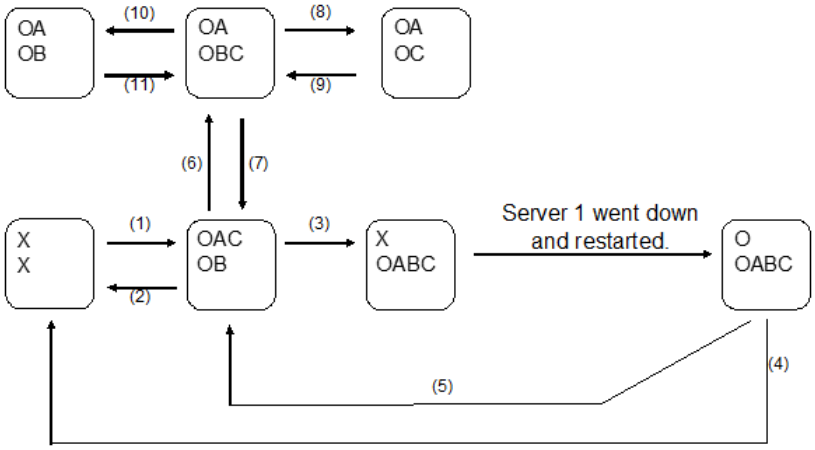
Group	1st priority server	2nd priority server
A	server1	server2
B	server2	server1
C	server1	server2

- The upper server is referred to as server1 and the lower one as server2.



<Cluster status transition diagram>

This diagram illustrates a typical status transition of cluster.

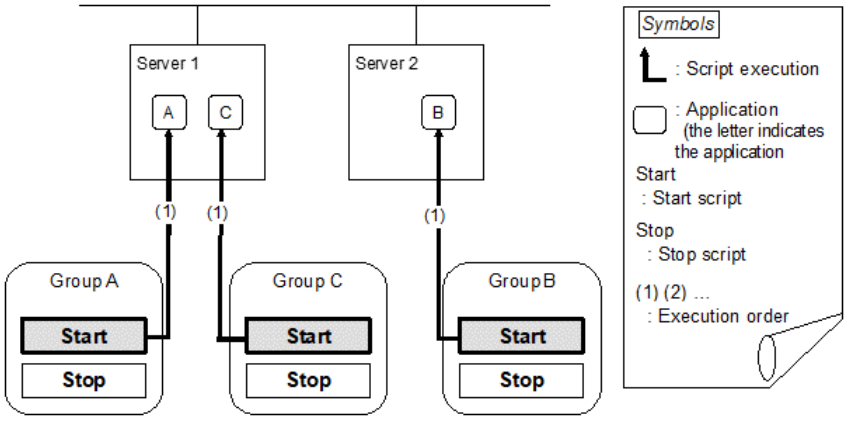


Numbers 1. to 11. in the diagram correspond to descriptions as follows.

1. **Normal startup**

   Normal startup here means that the start script has been run properly on the primary server.

   Each group is started on the server with the highest priority among the active servers.

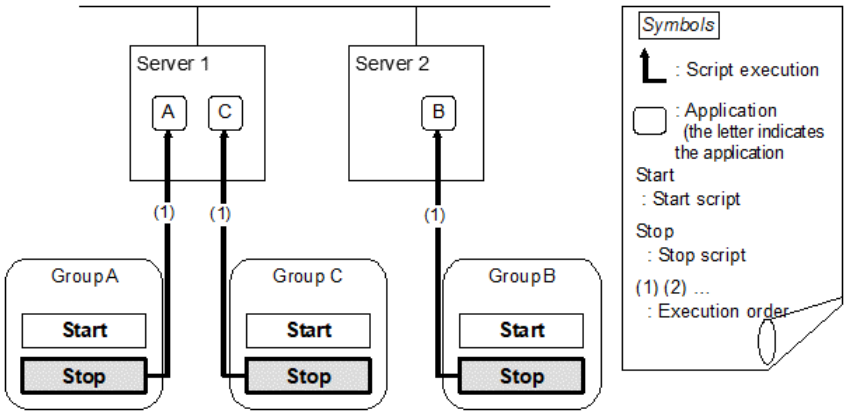


   Environment variables for Start

Group	Environment variable	Value
A	CLP_EVENT	START
	CLP_SERVER	HOME
B	CLP_EVENT	START
	CLP_SERVER	HOME
C	CLP_EVENT	START
	CLP_SERVER	HOME

2. **Normal shutdown**

   Normal shutdown here means a cluster shutdown immediately after the start script corresponding to the stop script that was run by performing normal startup or by moving a group (online failback).



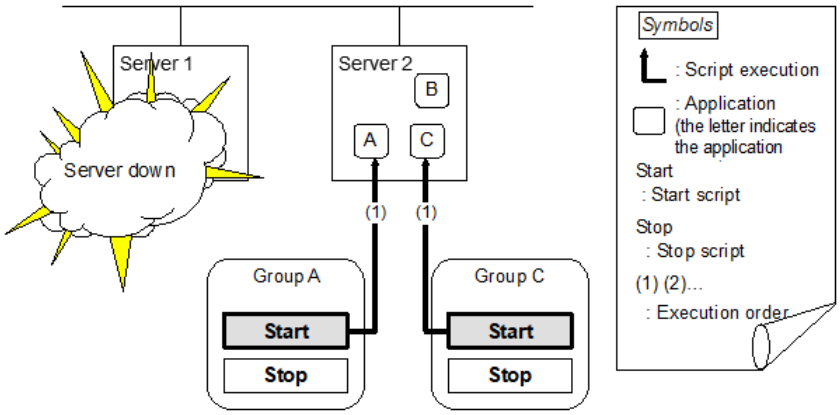
   Environment variables for Stop

Group	Environment variable	Value
A	CLP_EVENT	START
	CLP_SERVER	HOME
B	CLP_EVENT	START
	CLP_SERVER	HOME
C	CLP_EVENT	START
	CLP_SERVER	HOME

3. **Failover at server1 down**

   When the start scrip of a group which has server1 as its primary server, it is run on a lower priority server (server2) when an error occurs. You need to write CLP_EVENT(=FAILOVER) as a branching condition for triggering application startup and recovery processes (such as database rollback process) in the start script in advance.

   For the process to be performed only on a server other than the primary server, specify CLP_SERVER(=OTHER) as a branching condition and describe the process in the script.

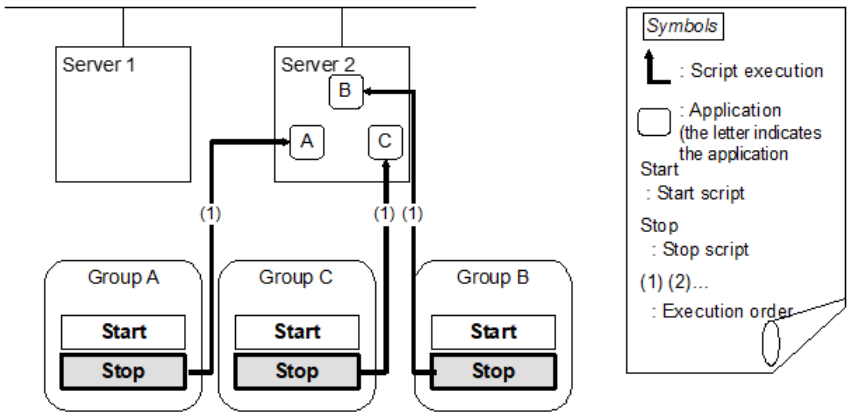


Environment variables for Start

Group	Environment variable	Value
A	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

4. **Cluster shutdown after failover of server1**

   The stop scripts of the Group A and C are run on server2 where the groups fail over (the stop script of Group B is run by a normal shutdown).

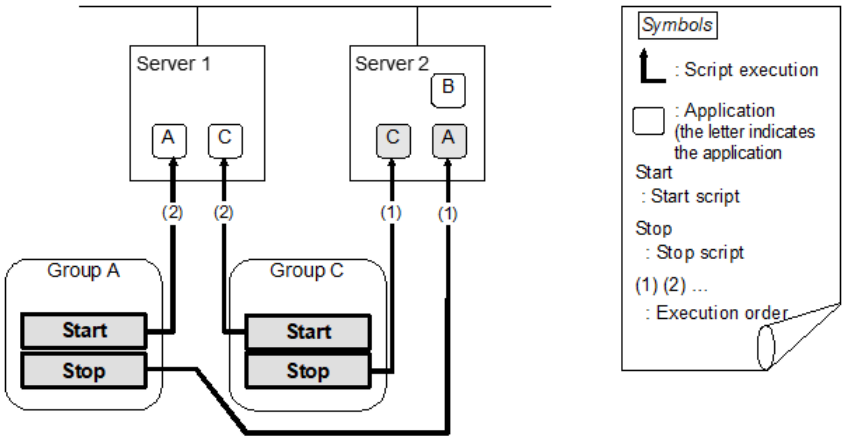


Environment variables for Stop

Group	Environment variable	Value
A	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER
B	CLP_EVENT	START
	CLP_SERVER	HOME
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

5. **Moving of Group A and C**

   After the stop scripts of Group A and C are run on server2 where the groups fail over, their start scripts are run on server1.



Environment variables for Stop

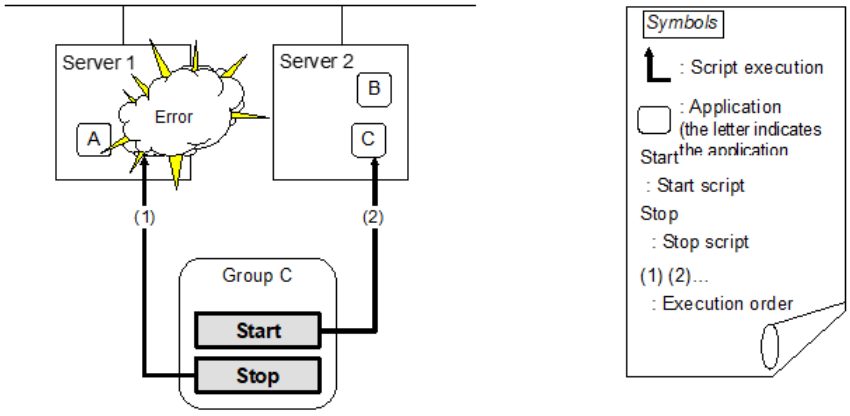
Group	Environment variable	Value
A	CLP_EVENT	FAILOVER[2]
	CLP_SERVER	OTHER
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

Environment variables for Start

Group	Environment variable	Value
A	CLP_EVENT	START
	CLP_SERVER	HOME
C	CLP_EVENT	START
	CLP_SERVER	HOME

6. **Error in Group C and failover**

When an error occurs in Group C, its stop script is run on server1 and start script is run on server2.



2

Environment variables in a stop script take those in the previous start script.
For moving in "5. Moving of Group A and C" because it is not preceded by a cluster shutdown, the environment variable used here is FAILOVER. However, if a cluster shutdown is executed before moving in "5. Moving of Group A and C," the environment variable is START.

Stop for server1

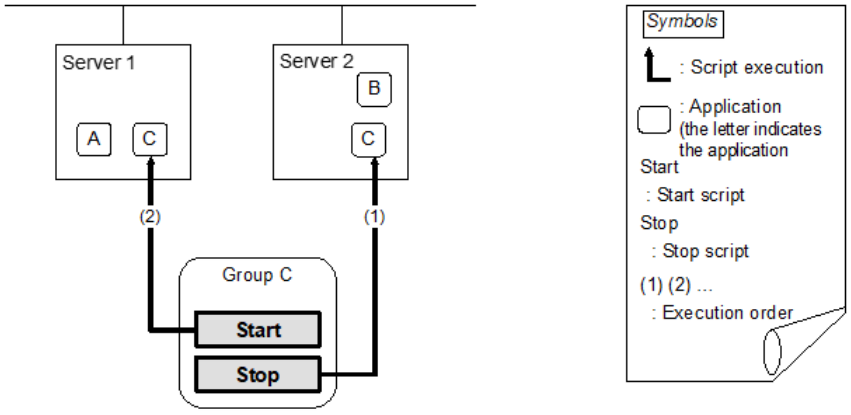
Group	Environment variable	Value
C	CLP_EVENT	START
	CLP_SERVER	HOME

Start for server2

Group	Environment variable	Value
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

7. **Moving of Group C**

Move the Group C that is failed over to server2 in 6. from server2 to server1. Run the stop script on server2, and then run the start script on server1.



Stop (because this is failed over in 6.)

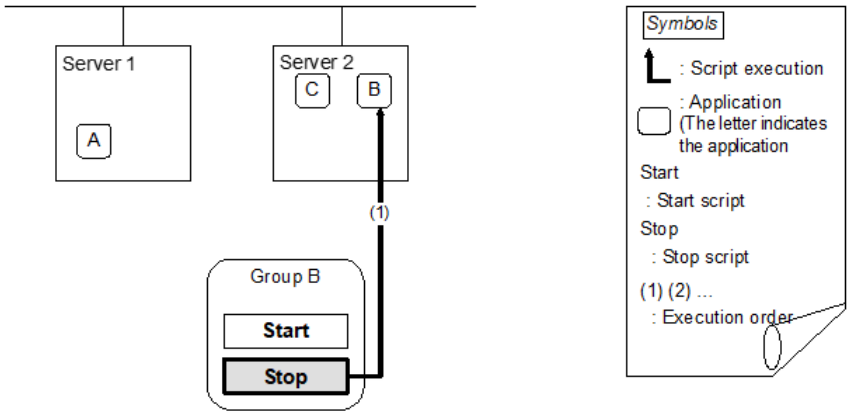
Group	Environment variable	Value
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

Start

Group	Environment variable	Value
C	CLP_EVENT	START
	CLP_SERVER	HOME

8. **Stopping Group B**

The stop script of Group B is run on server2.

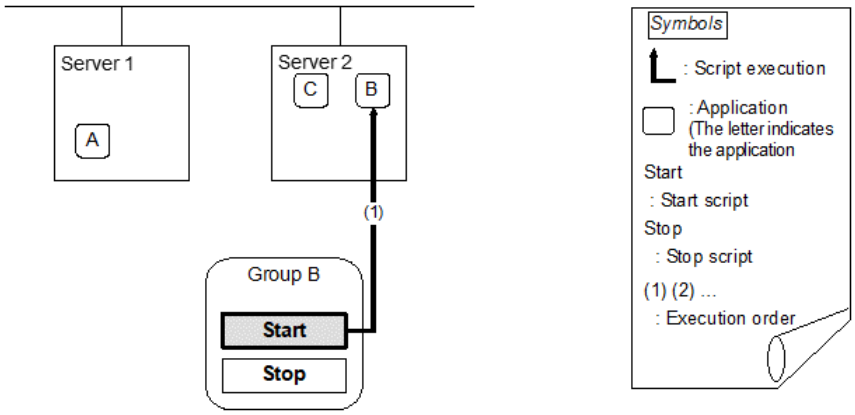


Stop

Group	Environment variable	Value
B	CLP_EVENT	START
	CLP_SERVER	HOME

9. **Starting Group B**

The start script of Group B is run on server2.

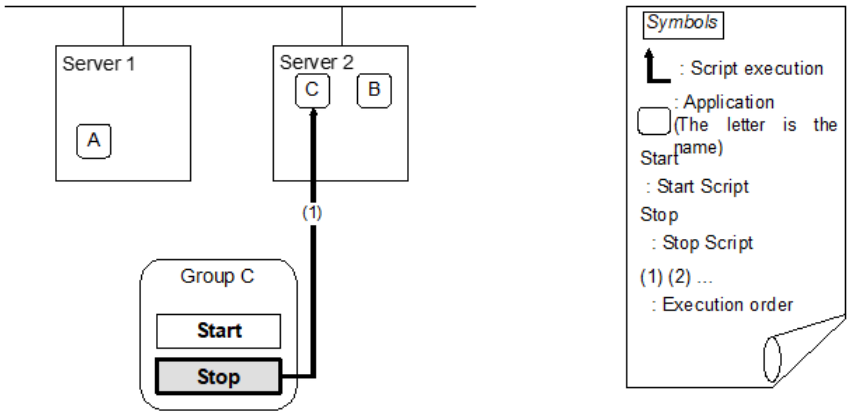


Start

Group	Environment variable	Value
B	CLP_EVENT	START
	CLP_SERVER	HOME

10. **Stopping Group C**

The stop script of Group C is run on server2.

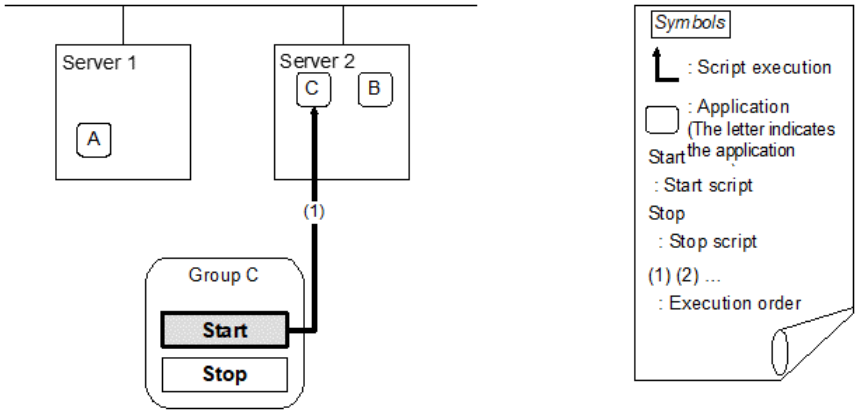


Stop

Group	Environment variable	Value
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

11. **Starting Group C**

The start scrip of Group C is run on server2.

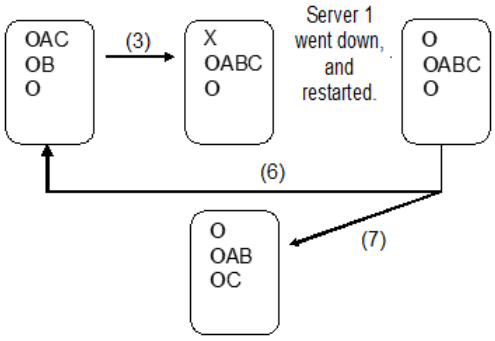


Start

Group	Environment variable	Value
C	CLP_EVENT	START
	CLP_SERVER	OTHER

Supplementary information 1

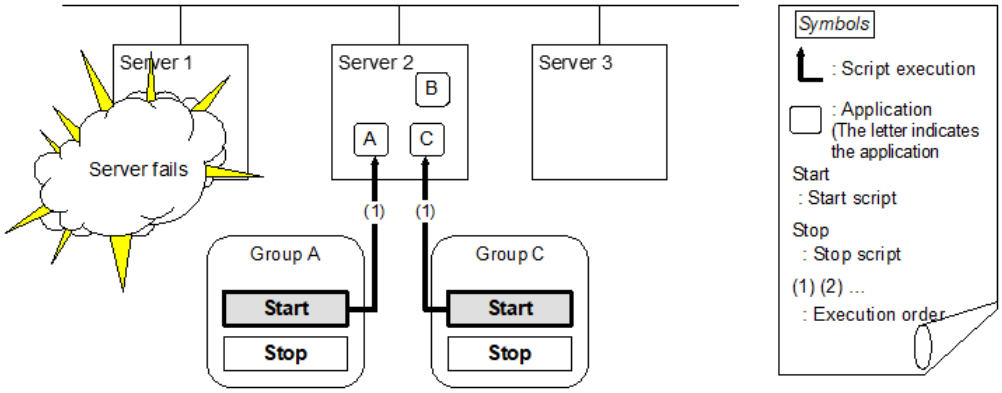
For a group that has three or more servers specified in the failover policy to behave differently on servers other than the primary server, use CLP_PRIORITY instead of CLP_SERVER(HOME/OTHER).



Example 1: "3. Failover at server1 down" in the cluster status transition diagram

A group has server1 as its primary server. If an error occurs on server1, its start script is run on server2 that has next highest priority failover policy. You need to write CLP_EVENT(=FAILOVER) as the branching condition for triggering applications' startup and recovery processes (such as database rollback process) in the start script in advance.

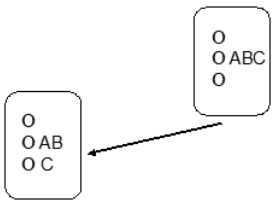
For a process to be performed only on the server that has the second highest priority failover policy, it is necessary to write CLP_PRIORITY(=2) as the branching condition.



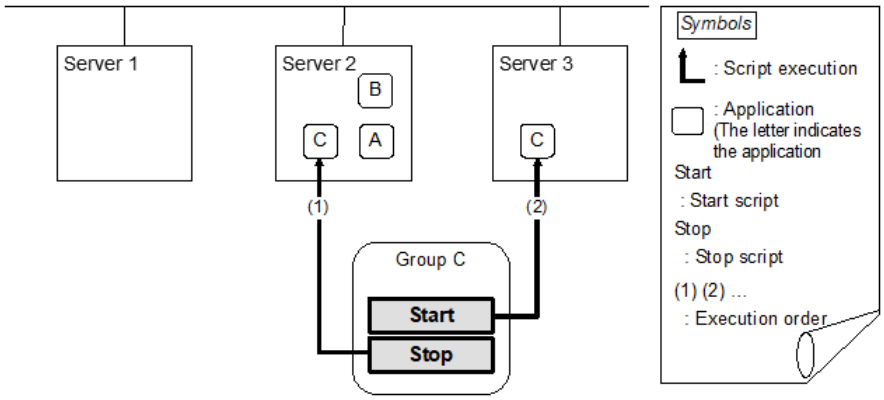
Environment variables for Start

Group	Environment variable	Value
A	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER
	CLP_PRIORITY	2
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER
	CLP_PRIORITY	2

Example 2: "7. Moving of Group C" in the cluster status transition diagram



After the stop scrip of Group C is run on server2 where the group failed over from, the start script is run on server3.



Environment variables for Stop

Group	Environment variable	Value
C	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER
	CLP_PRIORITY	2

Environment variables for Start

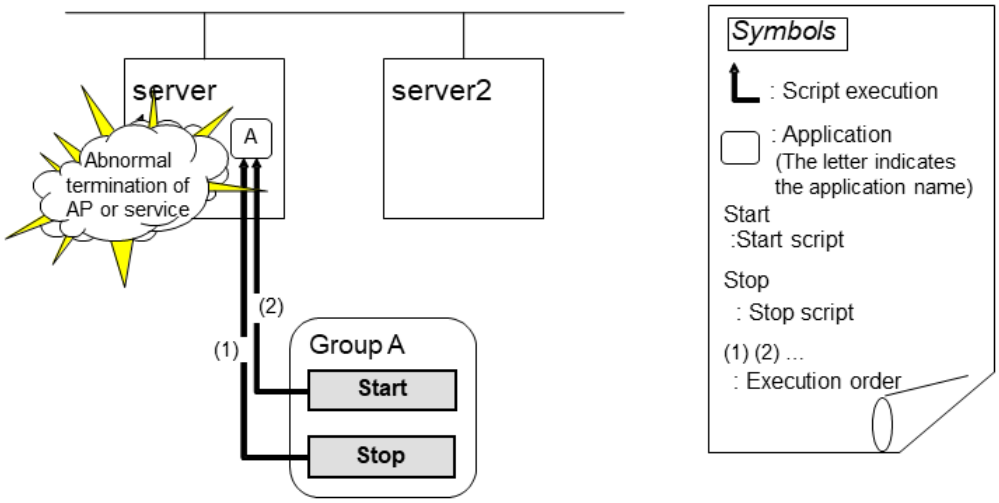
Group	Environment variable	Value
C	CLP_EVENT	START
	CLP_SERVER	OTHER
	CLP_PRIORITY	3

Supplementary information 2

When monitor resource starts or restarts a script:

To run the start script when resource monitor detected an error in application, the environment variables should be as follows:

Example 1: Resource monitor detects abnormal termination of an application that was running on server1 and restarts Group A on the server1.



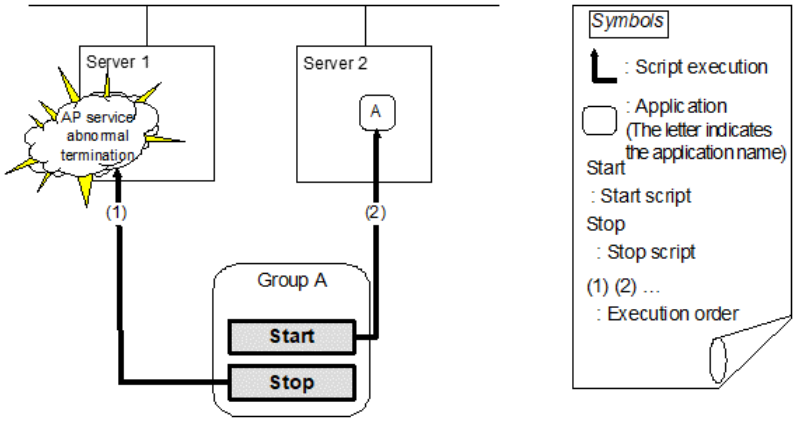
Environment variable for Stop

Group		Environment variable	Value
A	(1)	CLP_EVENT	The same value as when the start script is run

Environment variable for Start

Group		Environment variable	Value
A	(2)	CLP_EVENT	START

Example2: Resource monitor detects abnormal termination of an application that was running on server1, fails over to server2 and restarts Group A on server2



Environment variable for Stop

Group		Environment variable	Value
A	(1)	CLP_EVENT	The same value as when the start script is run

Environment variable for Start

Group		Environment variable	Value
A	(2)	CLP_EVENT	FAILOVER

Supplementary information 3

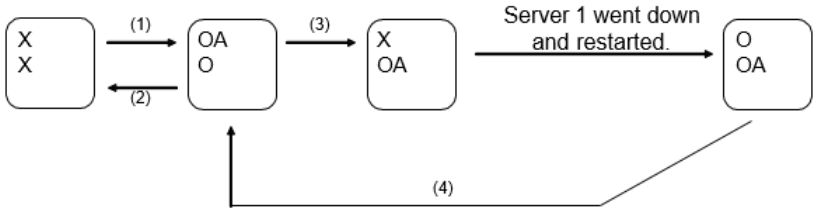
With **Execute on standby server** of **Exec Resource Tuning Properties** enabled, start and stop scripts can also be executed on another server (standby server) that does not start a group--in accordance with the timings of running these scripts on the active server that started a group.

Compared with the script execution on the active server, that on the standby server has the following characteristics:

- The results (error codes) of executing the scripts do not affect the group-resource statuses.
- No script before and after activation/deactivation is executed.
- Monitor resources set for monitoring at activation are not started or stopped.
- Different types and values of environment variables are set. (Refer to "*Environment variables in EXEC resource script*" as described above.)

The following describes the relationships between the execution timings of scripts on the standby server and the environment variables--with cluster status transition diagrams.

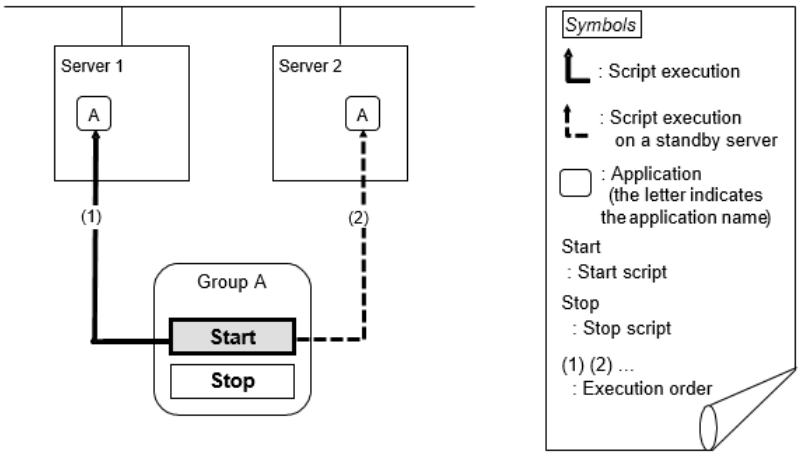
<Cluster status transition diagram>



Numbers 1. to 4. in the diagram correspond to the following descriptions:

1. **Normal startup**

For starting a group, the start script is run on the active server before executed on the standby server.
The start script requires a description, with CLP_EVENT (= STANDBY) as a branch condition, of what to be done on the standby server.

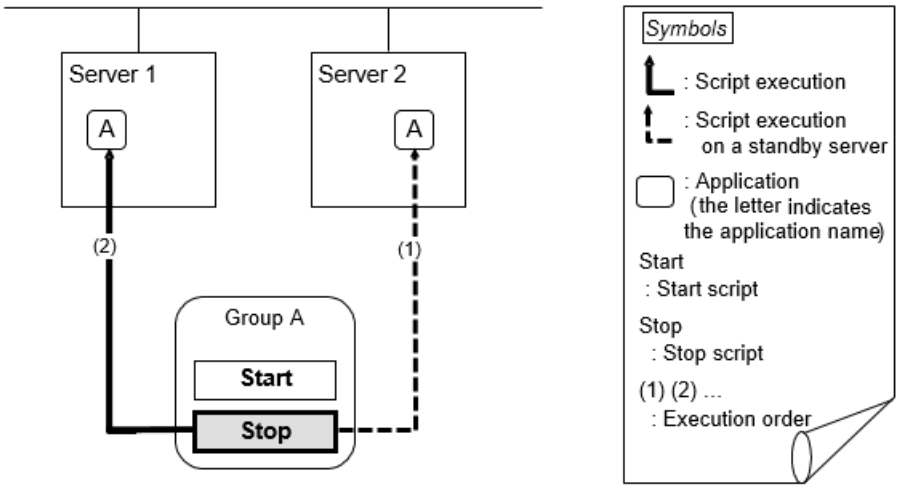


Environment variables for Start

Server	Environment variable	Value
1	CLP_EVENT	START
	CLP_SERVER	HOME
2	CLP_EVENT	STANDBY
	CLP_SERVER	OTHER

2. **Normal shutdown**

For stopping a group, the stop script is run on the standby server before executed on the active server.
The stop script requires a description, with CLP_EVENT (= STANDBY) as a branch condition, of what to be done on the standby server.



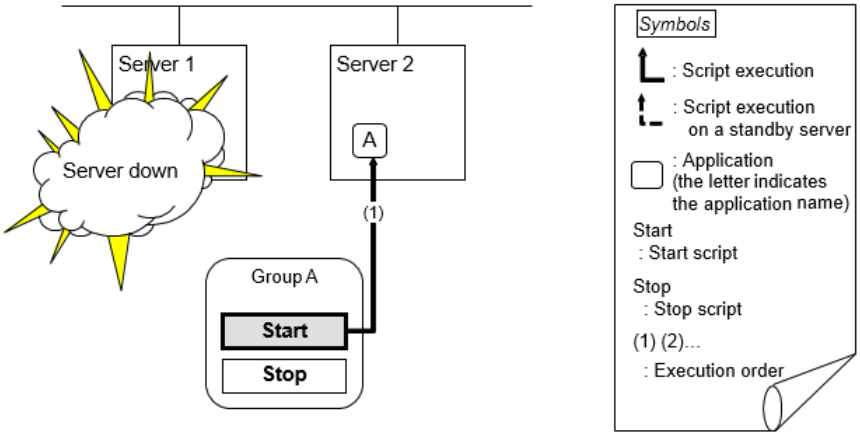
Environment variables for Stop

Server	Environment variable	Value
1	CLP_EVENT	START
	CLP_SERVER	HOME
2	CLP_EVENT	STANDBY
	CLP_SERVER	OTHER

3. **Failover at server1 down**

When an error occurs in server1, the group is failed over to server2, on which (as the active server) the start script is executed.
You need to write CLP_EVENT (= FAILOVER) as a branch condition for triggering application startup and recovery processes (such as a database rollback process) in the start script in advance.

With server1 crashed, the start script is not run on it as the standby server.

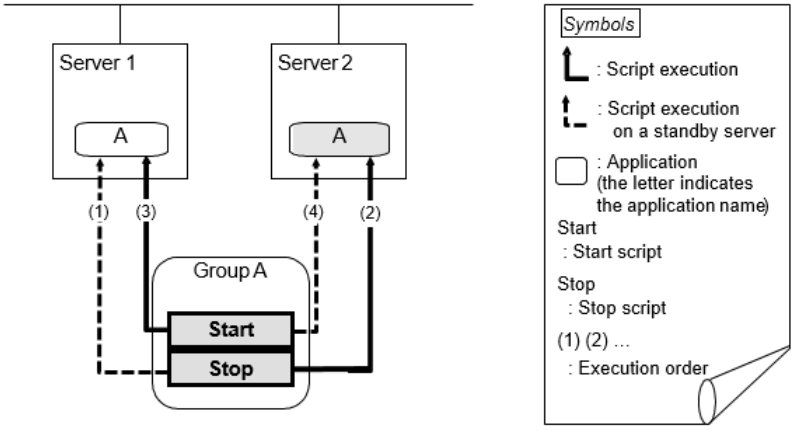


Environment variables for Start

Server	Environment variable	Value
2	CLP_EVENT	FAILOVER
	CLP_SERVER	OTHER

4. **Moving of Group A**

The stop script for Group A is executed on server1 (= standby server) and server2 (= active server). Then the start script is run on server1 (= active server) and server2 (= standby server).



Environment variables for Stop

Server	Environment variable	Value
1	CLP_EVENT	STANDBY
	CLP_SERVER	HOME
2	CLP_EVENT	FAILOVER[3]
	CLP_SERVER	OTHER

Environment variables for Start

Server	Environment variable	Value
1	CLP_EVENT	START
	CLP_SERVER	HOME
2	CLP_EVENT	STANDBY
	CLP_SERVER	OTHER

[3]

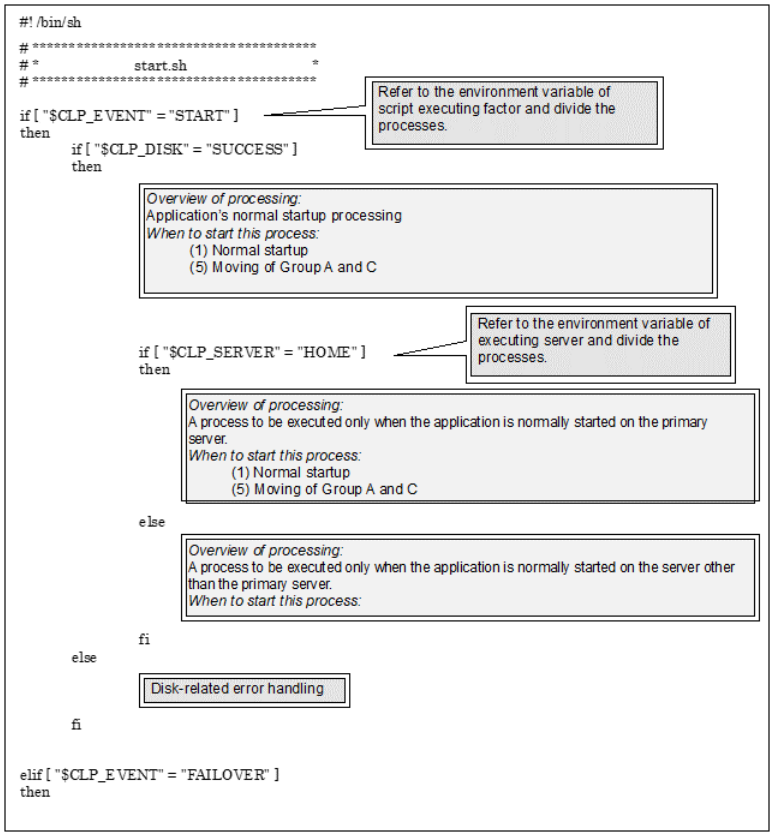
The value of an environment variable for the stop script is changed to that for the last executed start script.
In the transition case of "4. Moving of Group A", FAILOVER is applied without a cluster shutdown immediately preceding, or START is applied with a cluster shutdown done before the phase of "4. Moving of Group A".

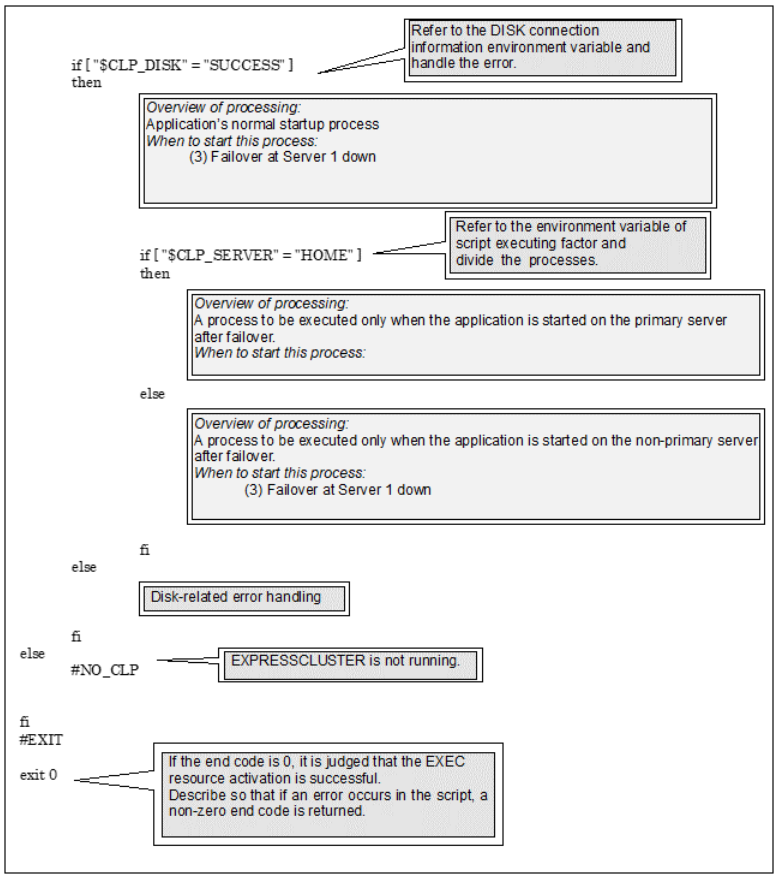
3.6.6 Writing EXEC resource scripts

This section explains timing script execution described in the preceding topic relating to the actual script codes.

Numbers in brackets "(*number*)" in the following example script code represent the actions described in " *Execution timing of EXEC resource script* ".

Group A start script: A sample of **start.sh**




if ["$CLP_DISK" = "SUCCESS"]
then
Refer to the DISK connection information environment variable and handle the error.
Overview of processing:
Application's normal startup process
When to start this process:
(3) Failover at Server 1 down
if ["$CLP_SERVER" = "HOME"]
then
Refer to the environment variable of script executing factor and divide the processes.
Overview of processing:
A process to be executed only when the application is started on the primary server after failover.
When to start this process:
else
Overview of processing:
A process to be executed only when the application is started on the non-primary server after failover.
When to start this process:
(3) Failover at Server 1 down
fi
else
Disk-related error handling
fi
else
#NO_CLP
EXPRESSCLUSTER is not running.
fi
#EXIT
exit 0
If the end code is 0, it is judged that the EXEC resource activation is successful.
Describe so that if an error occurs in the script, a non-zero end code is returned.

Group A stop script: A sample of **stop.sh**

```
#! /bin/sh
# ***************************************
# *                stop.sh                *
# ***************************************
if [ "$CLP_EVENT" = "START" ]
then
        if [ "$CLP_DISK" = "SUCCESS" ]
        then
                Overview of processing:
                Application's normal startup process
                When to start this process:
                        (2) Normal shutdown

                if [ "$CLP_SERVER" = "HOME" ]
                then
                        Overview of processing:
                        A process to be executed only when the application is normally terminated on the primary server.
                        When to start this process:
                                (2) Normal shutdown
                else
                        Overview of processing:
                        A process to be executed only when the application is normally terminated on the server other than the primary server.
                        When to start this process:
                fi
        else
                Disk-related error handling
        fi

elif [ "$CLP_EVENT" = "FAILOVER" ]
then
        if [ "$CLP_DISK" = "SUCCESS" ]
        then
                Overview of processing:
                Normal termination process after failover.
                When to start this process:
                        (4) Cluster shutdown after failover of Server 1
                        (5) Moving of Group A and C

                if [ "$CLP_SERVER" = "HOME" ]
                then
                        Overview of processing:
                        A process to be executed only when the application is terminated on the primary server after failover
                        When to start this process:
                else
                        Overview of processing:
                        A process to be executed only when the application is terminated on the non-primary server after failover.
                        When to start this process:
                                (4) Cluster shutdown after failover of Server 1
                                (5) Moving of Group A and C
                fi
        else
                Disk-related error handling
        fi
else
        #NO_CLP

fi
#EXIT
exit 0
```

Refer to the environment variable of script executing factor and divide the processes.

Refer to the environment variable of executing server and divide the processes.

EXPRESSCLUSTER is not running.

If the end code is 0, it is judged that the EXEC resource deactivation is successful. Describe so that if an error occurs in the script, a non-zero end code is returned.

3.6.7 Tips for creating EXEC resource script

- If your script has a command that requires some time to complete, it is recommended to configure command completion messages to be always produced. This message can be used to determine the error when a problem occurs. There are two ways to produce the message:
- Specify the log output path of EXEC resource by writing the echo command in the script.

  The message can be produced with the echo command. Specify the log output path in the resource properties that contain the script.

  The message is not logged by default. For how to configure the settings for the log output path, see"Maintenance tab" in "*Details tab* - Tuning Properties" . If the **Rotate Log** check box is not selected, pay attention to the available disk space of a file system because messages are sent to the file specified as the log output destination file regardless of the size of available disk space.

  (Example: sample script)

```
echo "appstart.."
appstart
echo "OK"
```

- Write the clplogcmd command in the script.

  The message can be produced to the Alert logs of the Cluster WebUI or syslog in OS with the clplogcmd command. For details on the clplogcmd command, see "*Outputting messages (clplogcmd command)*" in "*8. EXPRESSCLUSTER command reference*" in this guide.

  (Example: sample script)

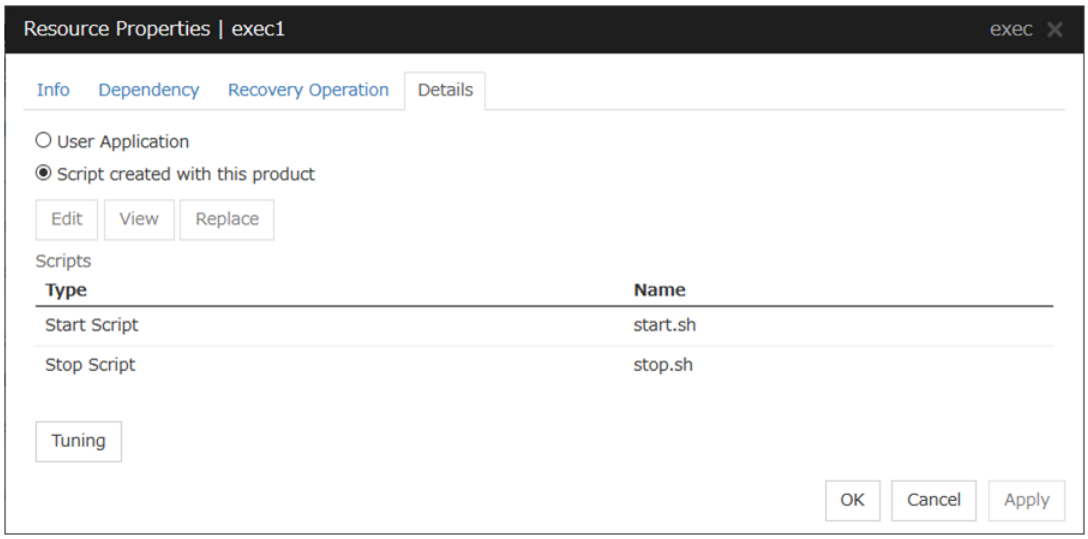
```
clplogcmd -m "appstart.."
appstart
clplogcmd -m "OK"
```

3.6.8 Notes on EXEC Resource

- Script Log Rotate

  When the Script Log Rotate function is enabled, a process is generated to mediate the log output. This intermediate process continues to work until the file descriptor is closed (i.e. until all the logs stop being output from the start and stop scripts and from a descendant process that takes over the standard output and/or the standard error output from the start and stop scripts). To exclude output from the descendant process from the log, redirect the standard output and/or the standard error output when the process is generated with the script.
- The start script and the stop script are executed by the root user.
- To start an application dependent on an environment variable, the script must set the environment variable as needed.

3.6.9 Details tab



User Application

Select this option to use executable files (executable shell scripts and binary files) on your server as scripts. Specify the local disk path on the server for each executable file name.

The executable files will not be distributed to each server. They should be placed on each server in advance. The cluster configuration data created by the Cluster WebUI does not contain these files. You cannot edit the script files using the Cluster WebUI.

Script created with this product

Select this option to use script files created by the Cluster WebUI as scripts. You can edit them using the Cluster WebUI as necessary. The cluster configuration data contains these script files.

View

Click here to display the script file when you select **Script created with this product**.

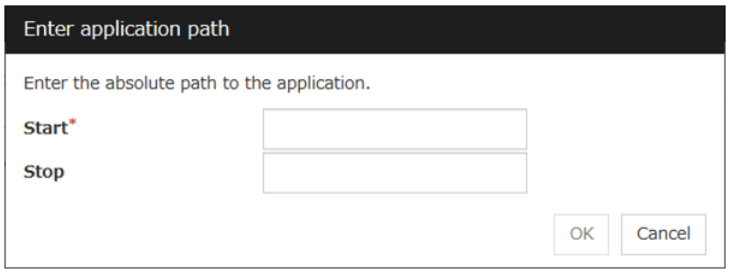
Edit

Click here to edit the script file when you select **Script created with this product**. Click Save to apply changes. You cannot rename the script file

With the **User Application** option selected, the **Enter application path** dialog box appears.

Enter application path

Specify an exec resource executable file name.



Start (Within 1023 bytes)

Enter an executable file name to be run when the exec resource starts. The name should begin with "/." Arguments can also be specified.

Stop (Within 1023 bytes)

Enter an executable file name to be run when the exec resource exits. The name should begin with "/." The stop script is optional.

For the executable file name, specify a full path name starting with "/" to a file on your cluster server.

Arguments can also be specified.

Replace

Opens the **Open** dialog box with the **Script created with this product** option selected.

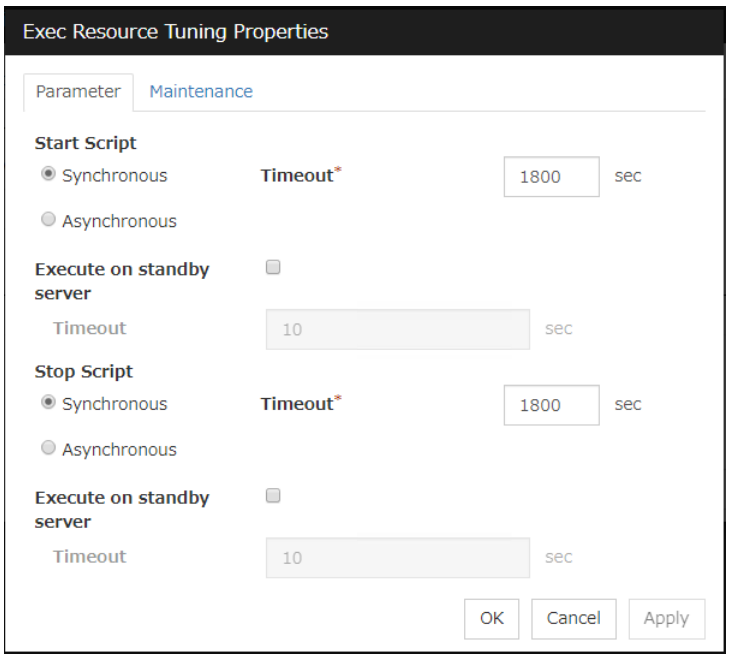
The contents of the script file selected in the **Resource Properties** are replaced with the one selected in the **Open** dialog box. If the selected script file is being viewed or edited, you cannot replace it. Select a script file, not a binary file such as an application program.

Tuning

Opens the EXEC resource tuning properties dialog box. You can make advanced settings for the EXEC resource. If you want the PID monitor resource to monitor the exec resources, you have to set the start script to asynchronous.

Exec Resource Tuning Properties

Parameter tab



Common to all start scripts and stop scripts

Synchronous

Waits for the script to end when it is run. Select this option for executable files that are not resident (the process is returned immediately after the script completion).

Asynchronous

Does not wait for the script to end when it is run. Select this for resident executable files. The script can be monitored by PID monitor resource if **Asynchronous** is selected.

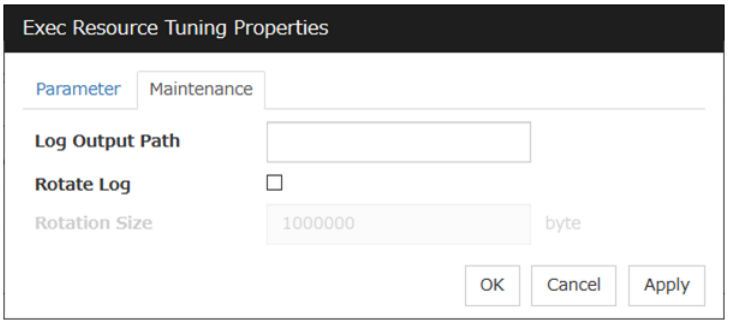
Timeout (1 to 9999)

When you want to wait for a script termination (when selecting **Synchronous**), specify how many seconds you want to wait before a timeout. This box is enabled when **Synchronous** is selected. Unless the script completes within the specified time, it is determined as an error.

Execute on standby server

Set whether the scripts are to be executed on the standby server. Enabling this parameter allows you to specify the timeout value (1 to 9999) for the execution.

Maintenance tab



Log Output Path (Within 1023 bytes)

Specify the redirect destination path of standard output and standard error output for EXEC resource scripts and executable files. If this box is left blank, messages are directed to /dev/null. The name should begin with "/."

If the **Rotate Log** check box is off, note the amount of available disk space in the file system because no limit is imposed on message output.

If the **Rotate Log** check box is on, the log file to be output is rotated. Note the following items.

You must specify a log output path within 1009 bytes. If you specify a path of 1010 bytes or more, the log is not output.

You must specify a log file name within 31 bytes. If you specify a log file name of 32 bytes or more, the log is not output.

When using multiple EXEC resources, the rotation size may not be normally recognized if you specify resources with the same file name, even if the paths differ (for example, /home/foo01/log/exec.log, /home/foo02/log/exec.log).

Rotate Log

Clicking **Rotate Log** when the **Rotate Log** check box is not checked outputs the execution logs of the EXEC resource script and the executable file without imposing any limit on the file size. Clicking **Rotate Log** when the **Rotate Log** check box is selected rotates and outputs messages.

Rotation Size (1 to 999999999)

If the **Rotate Log** check box is selected, specify a rotation size.

The structures of the log files to be rotated and output are as follows:

File name	Description
file_name for the **Log Output Path** specification	Newest log
file_name.pre for the **Log Output Path** specification	Previously rotated log

3.7 Understanding Disk resource

3.7.1 Dependencies of Disk resource

Disk resource is supported by the following versions of EXPRESSCLUSTER by default.

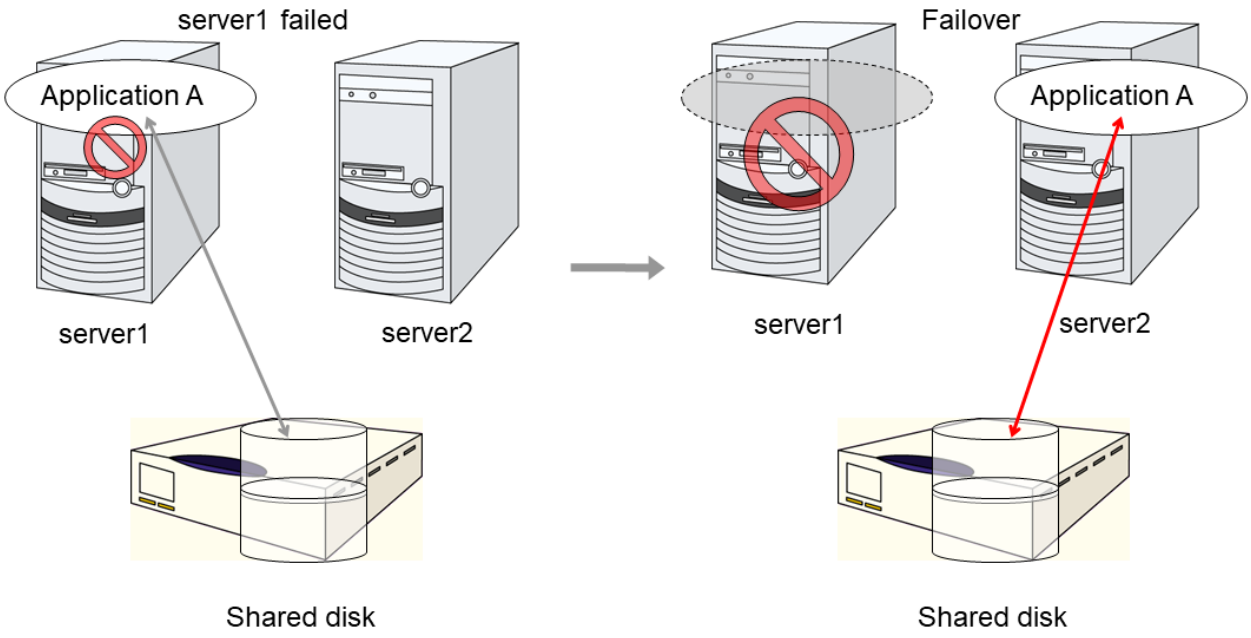
Group Resource Type
Dynamic DNS resource
Floating IP resource
Virtual IP resource
Volume manager resource
AWS Elastic IP resource
AWS Virtual IP resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.7.2 Switching partitions

Switching partitions refer to partitions on shared disks connected to more than one server in a cluster.
Switching is done for each failover group according to the failover policy. By storing data required for applications on switching partitions, the data can be automatically used when failing over or moving failover group.

Note: For "raw" disk type, EXPRESSCLUSTER maps (binds) the switching partition to the raw device of the OS. If Execute Unbind is selected on the Disk Resource Tuning Properties, the unbind process is performed to deactivate the disk resource.

If switching partitions are not accessible with the same device name on all the servers, configure the server individual setup.



3.7.3 Device region expansion on disk resources

Follow the steps below to execute region expansion of the device. Be sure to execute the following steps on the server where the disk resource in question has been activated.

1. Deactivate a group to which the disk resource in question belongs by using a command such as clpgrp.
2. Confirm that no disks have been mounted by using a command such as mount and df.
3. Change the state of the disk from Read Only to Read Write by executing one of the following commands depending on the disk resource type.
   # clproset -w -d <device-name>
4. Execute region expansion of the device.
5. Change the state of the disk from Read Write to Read Only by executing one of the following commands depending on the disk resource type.
   # clproset -o -d <device-name>
6. Activate a group to which the disk resource in question belongs by using a command such as clpgrp.

3.7.4 Notes on disk resources

- EXPRESSCLUSTER controls accesses to the file system (mount/umount). Thus, do not configure the settings about mount/umount on the OS.
  (If the entry to is required /etc/fstab, please use the noauto option is not used ignore option.)
- The partition device name set to the disk resource is in the read-only mode on all servers in a cluster. Read-only status is released when the server is activated.
- If **Exclude Mount/Unmount Commands** is selected on the **Extension** tab of the **Cluster Prosperities**, it may take some time to activate or deactivate a disk resource because mount or unmount of disk resource, VxVM volume resource, NAS resource, and mirror resource is performed exclusively in the same server.
- When specifying path including symbolic link for mount point, Force Operation cannot be done even if it is chosen as operation in Detecting Failure.

Similarly, if a path containing "//" is specified, forced termination will also fail.

- If you want to prevent behalf of the device in OS startup, udev devices the Please set the device name.
  example: /dev/disk/by-label/<device-name>
- When a change is made at the run level on the OS, some device files of a partition device set as a disk resource might be created again. This may reset the read-only setting for the partition device set as a disk resource.

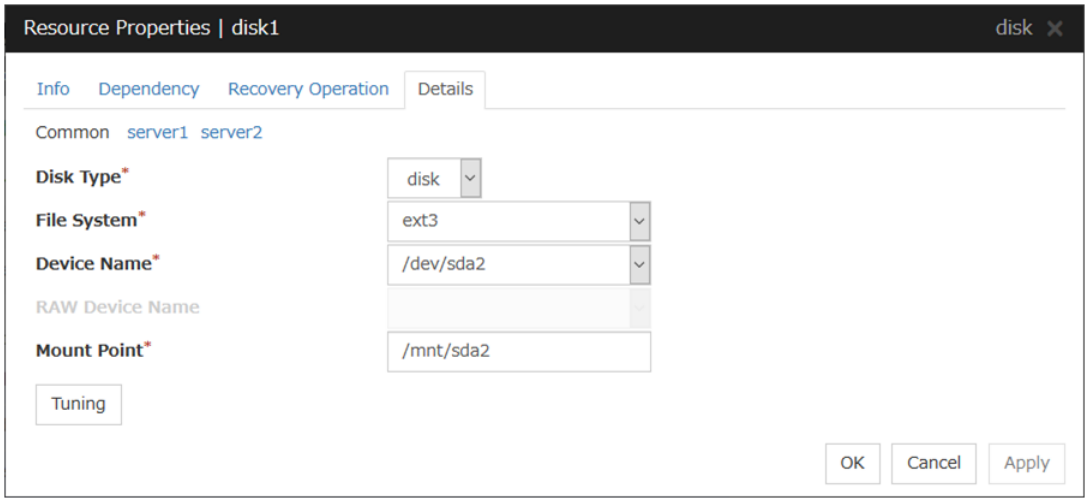
<When using a resource that has the disk type **LVM**>

- When using this setting, it is recommended to control a volume group by using a volume manager resource together. For details, see "*Understanding Volume manager resources*" of this guide.
- The volume is not defined on the EXPRESSCLUSTER side.
- Please do not select [zfs] for the File System.

<When using a resource that has the disk type **VXVM**>

- When using this setting, see "*Understanding Volume manager resources*".
- The volume is not defined on the EXPRESSCLUSTER side.
- No disk resource is needed when using only the accessible raw device (/dev/vx/rdsk/<disk-group-name>/<volume-name>) with the disk group imported and the volume started (raw access without setting up a file system on the volume).
- Please do not select [zfs] for the File System.

3.7.5 Details tab



Disk Type `Server Individual Setup`

Select a disk type. You can only choose [disk].

Choose one of the types below.

- DISK
- RAW
- LVM
- VXVM

File System `Server Individual Setup`

You select a file system type created on the disk device. Choose one from the types described below. You may also directly enter the type. This setting is necessary when the setting to **Disk Type** is other than **raw**.

- ext3
- ext4
- xfs
- reiserfs
- vxfs
- zfs

Device Name (Within **1023 bytes)** `Server Individual Setup`

Select the disk device name to be used for disk resources. Otherwise, you can enter the device name. When other than [zfs] is selected for File System, the name should begin with "/". If File System is [zfs], specify the ZFS data set name.

Raw Device Name (within 1,023 bytes) `Server Individual Setup`

Enter the raw disk device name to be used for disk resources. This setting is necessary when the setting to **Disk Type** is **raw** or **vxvm**.

Mount Point (Within **1023 bytes)** `Server Individual Setup`

Enter the directory to mount the disk device. The name should begin with "/." This setting is necessary when the setting to **Disk Type** is other than **raw**.

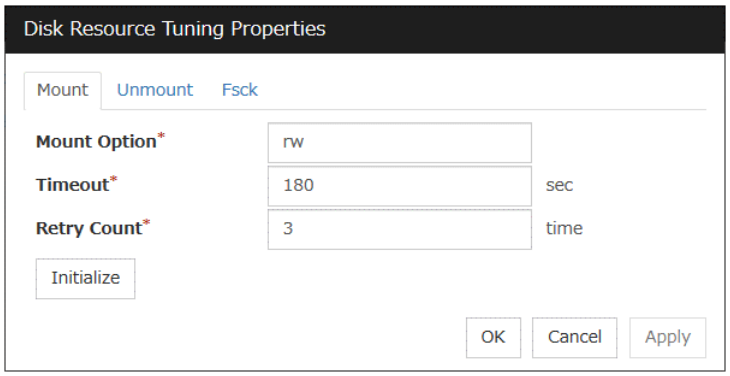
Tuning

Opens the **Disk Resource Tuning Properties** dialog box. Make detailed settings on the dialog box.

Disk Resource Tuning Properties(when the setting to Disk Type is other than raw)

Mount tab

The detailed settings related to mount are displayed.



Mount Option

Enter options to give the mount command when mounting the file system on the disk device. More than one option is delimited with a comma ",".

A mount option sample

Setting item	Setting value
Device name	/dev/sdb5
Mount point	/mnt/sdb5
File system	ext3
Mount option	rw,data=journal

The mount command to be run with the above settings is:

mount -t ext3 -o rw,data=journal /dev/sdb5 /mnt/sdb5

Timeout (1 to 999)

Enter how many seconds you want to wait for the mount command completion before its timeout when you mount the file system on the disk device.
If the file system has a large size of disk space, it may take some time for the command to complete. Make sure to specify the value that is enough for the mount command completion.

Retry Count (0 to 999)

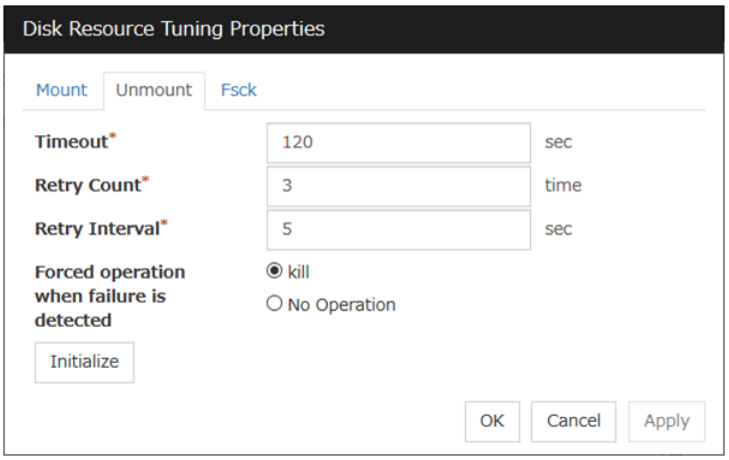
Enter how many times you want to retry to mount the file system on the disk device when one fails.
If you set this to zero (0), mount will not be retried.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

Unmount tab

The detailed settings related to unmount are displayed.



Timeout (1 to 999)

Enter how many seconds you want to wait for the umount command completion before its timeout when you unmount the file system on the disk device.

Retry Count (0 to 999)

Enter how many times you want to retry to unmount the file system on the disk device when one fails. If this is set to zero (0), unmount will not be retried.

Retry Interval (0 to 999)

Enter the interval in which you want to retry unmounting the file system on the disk device when unmounting fails.

Forced operation when failure is detected

Select an action to be taken at an unmount retry if unmount is failed.

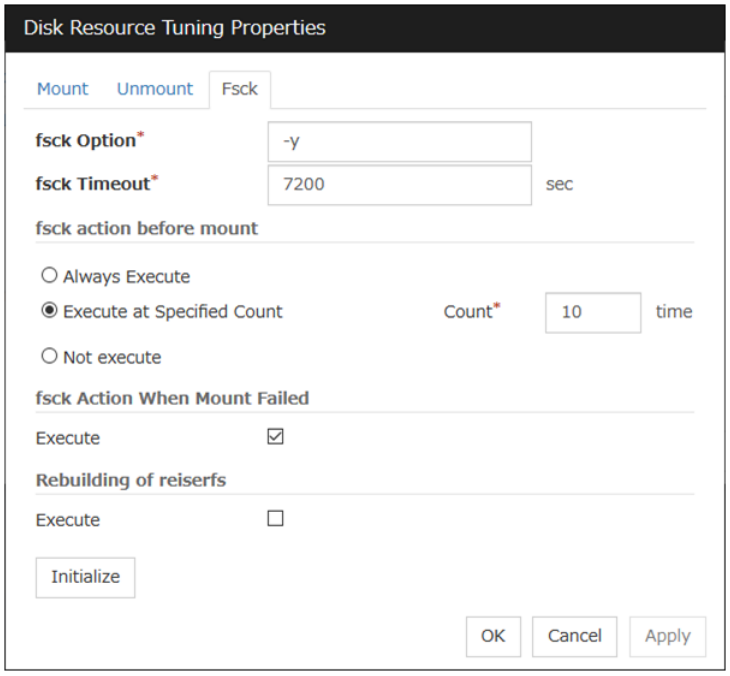
- kill
  Select this to try to kill the processes that are accessing the mount point. Not always the process can be killed.
- No Operation
  Select this not to try to kill the processes that are accessing the mount point.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

Fsck tab

The detailed settings related to fsck are displayed. The tab appears only if [xfs] is set for the file system. If [zfs] is selected for the file system, it will be invalid.



fsck Option (Within 1023 bytes)

Enter options to give to the fsck command when checking the file system on disk device. Options are delimited with a space. Specify options so that the fsck command does not work interactively.
Otherwise, you may not be allowed to mount until the "fsck timeout" elapses. When the file system is reiserfs, the fsck command works interactively. However, it can be avoided if EXPRESSCLUSTER gives "Yes" to reiserfsck.

fsck Timeout (1 to 9999)

Enter how many seconds you want to wait for the fsck command completion before its timeout when you check the file system on the disk device. If the file system has a large size of disk space, it may take some time for the command to complete. Make sure to specify the value that is enough for the mount command completion.

fsck action before mount

Select an fsck action before mounting file system on a disk device from the following choices:

- Always Execute
  fsck is executed before mounting the file system.
- Execute at Specified Count
  fsck is executed when resource is activated successfully within the count specified by **Count**.
  = Count (0 to 999)
- Not Execute
  fsck is not executed before mounting the file system.

Note: The number of times to execute fsck is not related to the check interval managed by a file system.

---

fsck Action When Mount Failed

Set an fsck action when detecting a mount failure on a disk device.
This setting is enabled when the setting of Mount **Retry Count** is other than zero.

- When the check box is selected:
  Mount is retried after running fsck.
- When the check box is not selected:
  Mount is retried without running fsck.

Note: It is not recommended to set "Not Execute" fsck action before performing mount. With this setting, disk resource does not execute fsck and disk resource cannot be failed over when there is an error that can be recovered by fsck in the switchable partition.

Rebuilding of reiserfs

Specify the action when reiserfsck fails with a recoverable error.

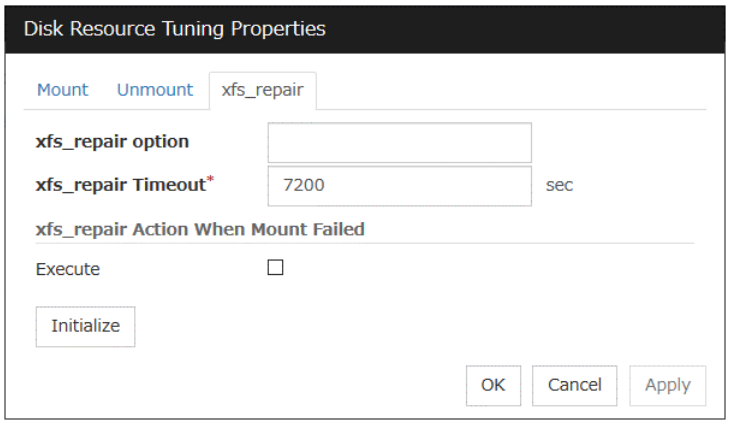
- When the checkbox is selected
  reiserfsck --fix-fixable is executed.
- When the checkbox is not selected
  Recovery is not performed even if reiserfsck fails with a recoverable error.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

xfs_repair tab

The detailed settings related to [xfs_repair] are displayed. The tab appears only if [xfs] is set for the file system.



xfs_repair Option (Within 1023 bytes)

Enter the option to give to the [xfs_repair] command when checking the file system on the disk device. To enter multiple options, delimit each with a space.

xfs_repair Timeout (1 to 9999)

Enter how many seconds you want to wait for the [xfs_repair] command completion before its timeout when you check the file system on the disk device. If the file system has a large size of disk space, it may take some time for the command to complete. Make sure that the value to set is not too small.

xfs_repair Action When Mount Failed

Set the [xfs_repair] action when mounting the file system on the disk device fails. This setting is enabled when the setting of **Mount Retry Count** is other than zero.

- When the check box is selected:
  Mount is retried after running [xfs_repair].
- When the check box is not selected:
  Mount is retried without running [xfs_repair].

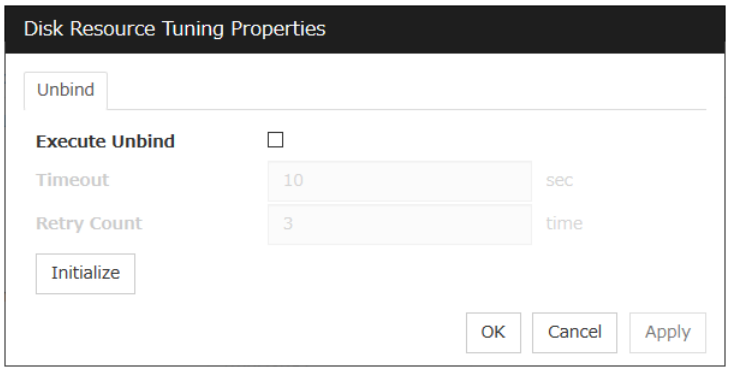
Initialize

Clicking **Initialize** resets the values of all items to the default values.

Disk Resource Tuning Properties (when the setting to Disk Type is raw)

Unbind tab

The detailed settings related to unbind are displayed.



Execute Unbind

Specify whether to execute unbind a raw disk device.

- When the check box is selected:
  Execute unbind a raw disk device.
- When the check box is not selected:
  Do not execute unbind a raw disk device.

Timeout (1 to 999)

When the **Execute Unbind** check box is selected, Set the time-out for the unbind completion of the raw disk device.

Retry Count (1 to 999)

When the **Execute Unbind** check box is selected, Specify the retry count to unbind the raw disk device when one fails.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

3.8 Understanding Floating IP resource

3.8.1 Dependencies of Floating IP resource

By default, this function does not depend on any group resource type.

3.8.2 Floating IP

Client applications can use floating IP addresses to access cluster servers. By using floating IP addresses, clients do not need to be aware of switching access destination server when a failover occurs or moving a group migration.

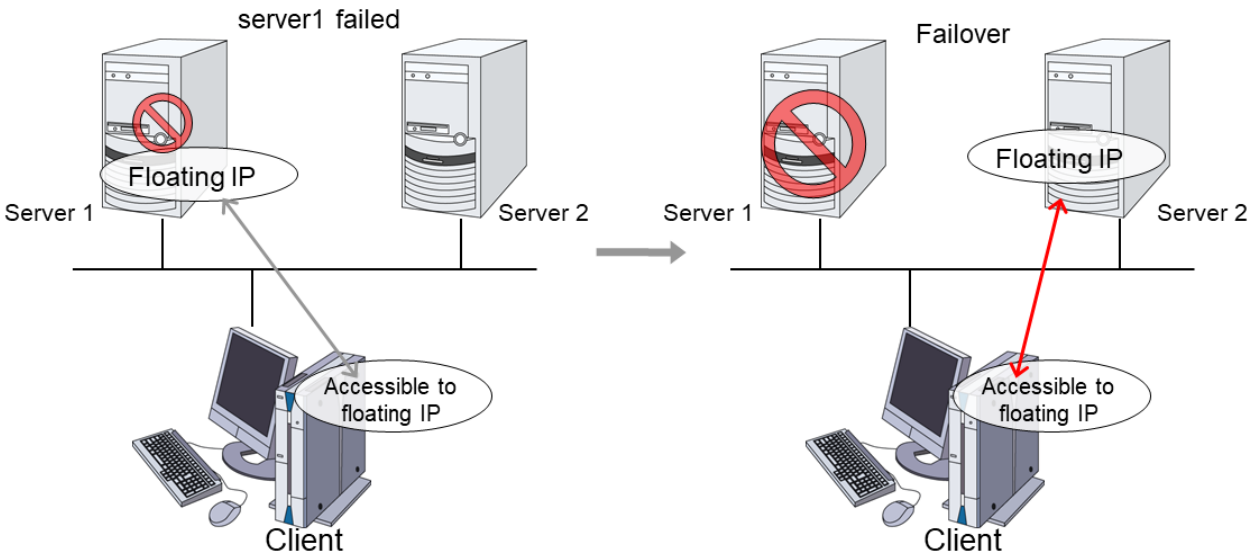
Floating IP addresses can be used on the same LAN and over the remote LAN.

Execute the [ifconfig] command or the API to assign an IP address to the OS. The floating IP resource automatically determines whether to execute the [ifconfig] command or the API.

When [ifconfig] command has a format other than the following, excute API.

```
eth0    Link encap:Ethernet HWaddr 00:50:56:B7:1B:C0
        inet addr:192.168.1.113 Bcast:192.168.1.255 Mask:255.255.255.0
        inet6 addr: fe80::250:56ff:feb7:1bc0/64 Scope:Link

(The following is omitted.)
```



Address assignment

An IP address to assign for floating IP address needs to meet the condition described below:

- Available host address which is in the same network address as the LAN that the cluster server belongs

Allocate as many IP addresses that meet the above condition as required (generally as many as failover groups). These IP addresses are the same as general host addresses, therefore, global IP addresses can be assigned such as Internet.

Switching method

For IPv4, MAC addresses on the ARP table are switched by sending ARP broadcasting packets from the server on which FIP resources are activated.

For IPv6, ARP broadcasting packets are not sent.

The table below shows the information of ARP broadcasting packets sent by EXPRESSCLUSTER:

0	1	2	3
ff	ff	ff	ff
ff	ff	MAC address	
(6byte)			
08	06	00	01
08	00	06	04
00	02		
MACaddress(6bytes)			
FIP address (4 bytes)			
MACaddress(6bytes)			
		FIP address	
(4byte)		00	00
00	00	00	00
00	00	00	00
00	00	00	00
00	00	00	00

Routing

You do not need to configure the settings for the routing table.

Conditions to use

Floating IP addresses are accessible to the following machines:

- Cluster server itself
- Other servers in the same cluster and the servers in other clusters
- Clients on the same LAN as the cluster server and clients on remote LANs

If the following conditions are satisfied, machines other than the above can also access floating IP addresses. However, connection is not guaranteed for all models or architectures of machines. Test the connection thoroughly by yourself before using those machines.

- TCP/IP is used for the communication protocol.
- ARP protocol is supported.

Even over LANs configured with switching hubs, floating IP address mechanism works properly. When a server goes down, the TCP/IP connection the server is accessing will be disconnected.

3.8.3 Notes on Floating IP resource

- Do not execute a network restart on a server on which floating IP resources are active. If the network is restarted, any IP addresses that have been added as floating IP resources are deleted.
- **IP address overlaps due to time-lag of the [ifconfig] command**

  If the following is set to the floating IP resource, the failover of resources may fail:

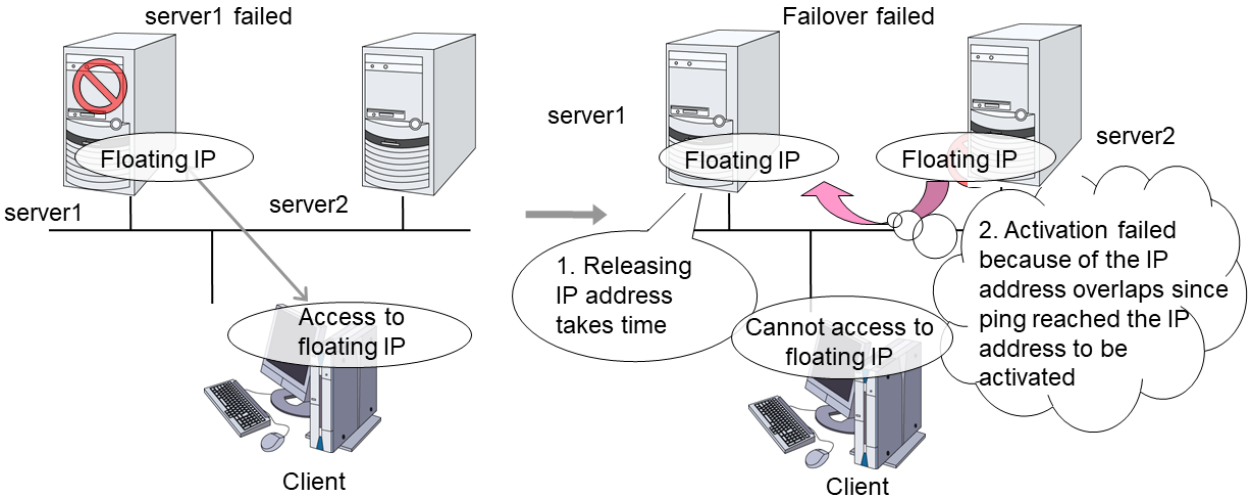
  - When a value smaller than the default is set to **Retry Count at Activation Failure**.
  - When **Ping Retry Count** and **Ping Interval** are not set.

  This problem occurs due to the following causes:

  - Releasing IP address may take time depending on the specification of the **[ifconfig]** command after deactivating the floating IP address on the server from which the resource is failed over.
  - On the activation of the floating IP address on the server to which the resource is failed over, if the ping command is run to the IP address to be activated in order to prevent dual activation, ping reaches the IP address because of the reason above, and the resource activation error occurs.

  Make the following settings to avoid this problem:

  - Set a greater value to **Retry Count at Activation Failure** of the resource (default: 5 times).
  - Set greater values to **Ping Retry Count** and **Ping Interval**.



- IP address overlaps when OS is stalled

  If OS stalls with the floating IP address activated, the resource failover may fail when the following settings are made:

  - A value other than 0 is set to **Ping Timeout**.
  - **Forced FIP Activation** is off.

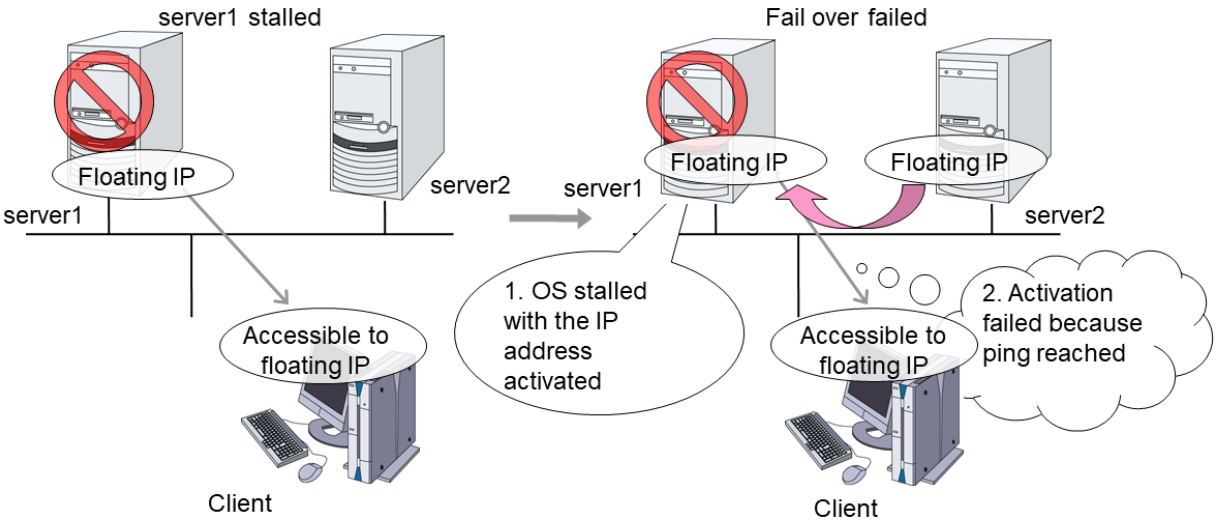
  This problem occurs due to the following causes:

  - A part of OS stalls (as examples below) with the floating IP address activated.
    - Network modules are running and respond to ping from other nodes
    - A stall cannot be detected in the user-mode monitor resource
  - When activating the floating IP address on the server to which the resource is failed over, if the ping command is executed to the IP address to be activated in order to prevent redundant activation, ping reaches the IP address because of the reason above, and the resource activation error occurs.

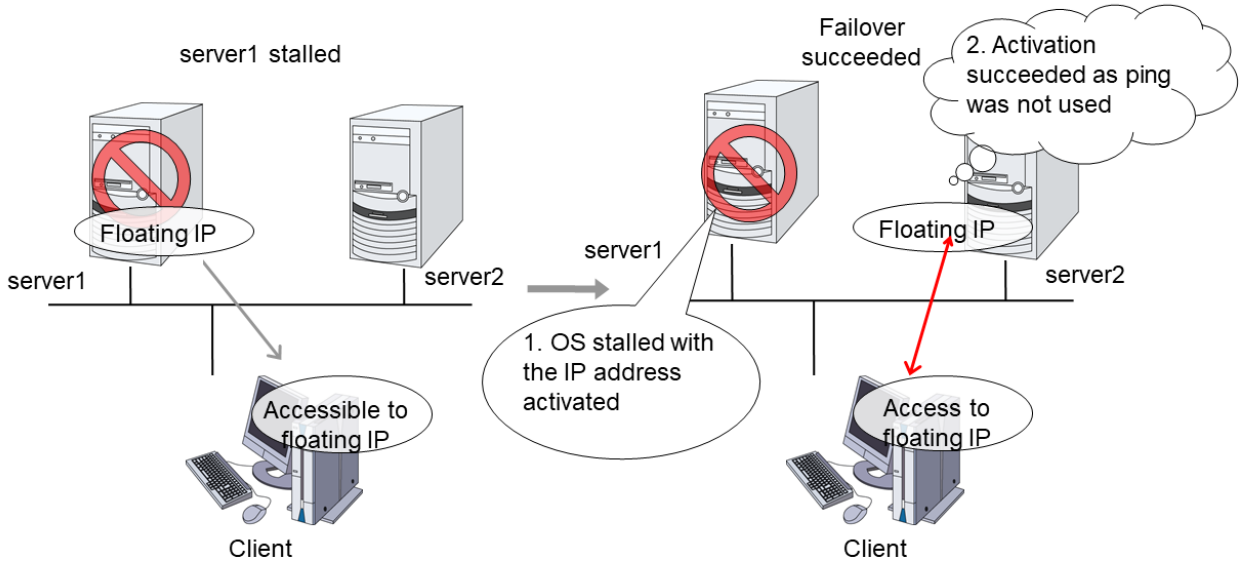
  In the machine environment where this problem often occurs, this can be prevented by the settings below. However, both groups may be activated depending on the status of a stall, and server shutdown may occur depending on the timing of the activation of both groups. For details on activation of both groups, see "What causes servers to shut down" - "Recovery from network partition" in "The system maintenance information" in the "Maintenance Guide".

  - Specify 0 to **Ping Timeout**
    Overlap check is not performed to the floating IP address.
  - Specify "On" to **Forced FIP Activation**
    The floating IP address is activated forcibly even when the address is used on a different server.

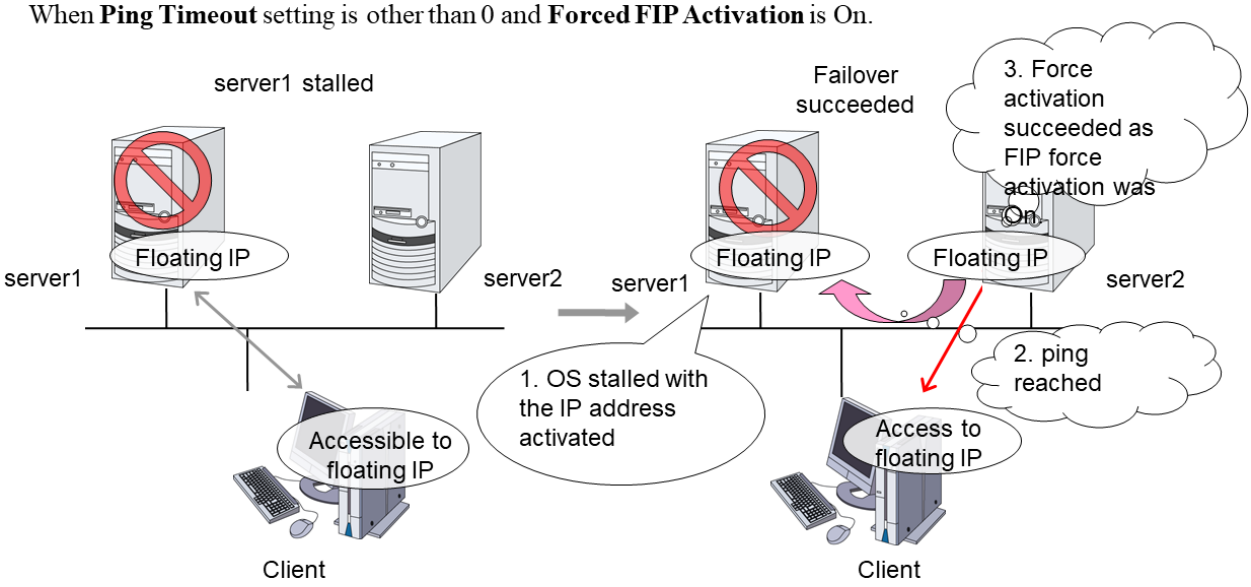
When the **ping Timeout** setting is other than 0 and **Forced FIP Activation** is OFF



When **Ping timeout** setting is 0



When **Ping Timeout** setting is other than 0 and **Forced FIP Activation** is On.



- MAC address of virtual NIC to which floating IP is allocated.
  When the floating IP resource fails over, the corresponding MAC address is changed because the MAC address of virtual NIC to which the floating IP is allocated is the MAC address of real NIC.
- Source address of IP communication from the running server when the resource activation.
  The source address from the server is basically the real IP of the server even though the floating IP resource has activated. When you want to change the source address to the floating IP, the settings are necessary on the application.
- When **Forced FIP Activation** is set to **ON**, if a floating IP address is activated, and then a machine in the same network segment connects to a floating IP address, the connection may be established with a machine that previously used that IP address.
- **floating IP resource does not supported by the environment that OpenVPN has started.**
- The NIC name (the name of a network interface card, such as eth0) is up to 15 characters long. If the length of the name exceeds 15 characters, the activation failure occurs. Modify the NIC name in such a case.
- Before activating a floating IP resource, [ping] is issued to check whether there is a duplicated IP address. Therefore, if rejection of ICMP reception via a firewall is set to a network device that uses a duplicated IP address, a floating IP address might be duplicated because the existence of duplicated IP addresses cannot be checked by using a [ping] command.

3.8.4 Waiting process for Floating IP resource deactivation

The following process takes place after deactivating of floating IP address.

1. Waiting process
   - Execute the [ifconfig] command or the API to acquire a list of IP addresses assigned to the OS. The floating IP resource automatically determines whether to execute the [ifconfig] command or the API. If no floating IP address exists in the IP address list, it is regarded as deactive.
   - If a floating IP address exists in the IP addresses, one-second waiting takes place. This setting cannot be changed with the Cluster WebUI.
   - The operation mentioned above is repeated for up to four times at maximum. This number of times cannot be changed by the Cluster WebUI.

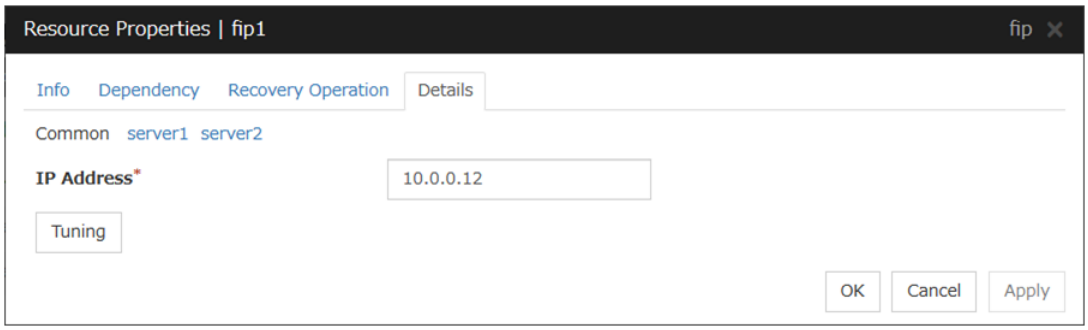
- When it results in an error, whether the floating IP resource is regarded as having a deactivation error can be changed with **Status at Failure** under **Confirm I/F Deletion** on the **Deactivity Check** tab of the floating IP resource.

2. Confirming process by the ping command
   - The ping command is executed to check if there is a response from the floating IP address. If there is no response, it is regarded as deactive.
   - When there is a response from the floating IP address, one-second waiting takes place. This setting cannot be changed with the Cluster WebUI.
   - The operation mentioned above is repeated for up to four times at maximum. This number of times cannot be changed by the Cluster WebUI.
   - The ping command is executed with one-second timeout. This timeout cannot be changed by the Cluster WebUI.
   - When it results in an error, the status of floating IP resource can be changed in **Status at Failure** under **Confirm I/F Response** on the **Deactivity Check** on the **Deactivity Check** tab of the floating IP resource.

Note:

Acquisition of the list of IP addresses and floating address activation/deactivation using the [ifconfig] command timeout in 60 seconds (this is the default value).
This timeout value can be changed by the Clustew WebUI. For details, see the **Parameter tab** of the "*Details tab*".

3.8.5 Details tab



IP Address `Server Individual Setup`

Enter the floating IP address to be used. When setting the bonding, specify the bonding interface name by using "%" to separate. For details, see "*Bonding*" in "*7. Information on other settings*" in this guide.

- Example: 10.0.0.12%bond0

The floating IP resource searches for the address on a local computer having the same subnet mask, assuming there to be, by default, 24 mask bits for IPv4 or 128 bits for IPv6. Then, it assigns an alias to the relevant network interface to add a floating IP address.

To specify a number of mask bits explicitly, specify the address followed by **/number_of_mask_bits**. (For an IPv6 address, be sure to specify **/number_of_mask_bits**.)

Example: fe80::1/8

To specify a network interface explicitly, specify the address followed by **%interface_name**.

Example: fe80::1/8%eth1

In the above example, a floating IP address with eight mask bits is added to network interface eth1.

When setting the tag VLAN Please specify the I / F name of tag VLAN, separated by the "%".

- example in the case of setting the tag VLAN: 10.0.0.12% eth0.1

In an environment in which an IPv6 address and the [ifconfig] command can be used, be sure to match the output format of the [ifconfig] command and the IP address notation of the floating IP because the environment is case sensitive.

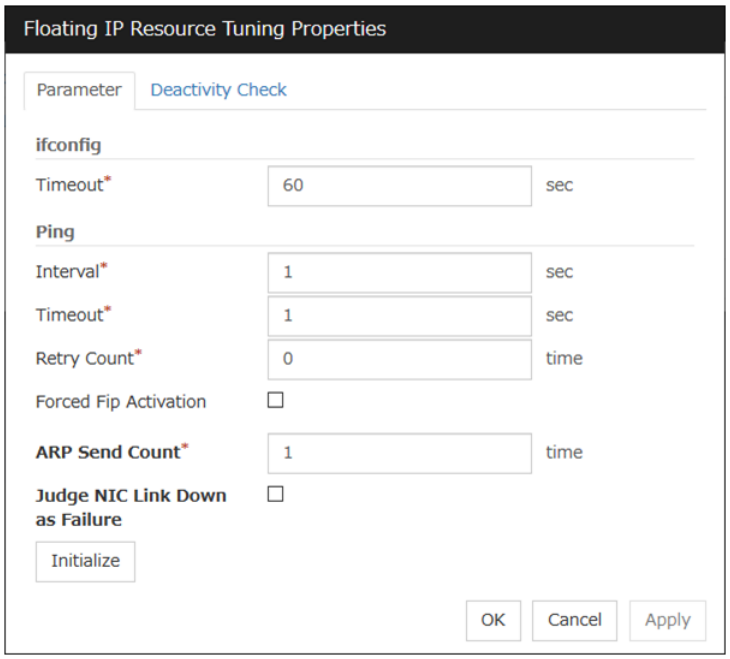
Tuning

Opens the **Floating IP Resource Tuning Properties** dialog box where the detailed settings for the floating IP resource can be configured.

Floating IP Resource Tuning Properties

Parameter tab

Detailed settings on parameters for floating IP resource are displayed.



ifconfig

The following is the detailed settings on getting IP addresses and on the [ifconfig] command executed for the activation and/or deactivation of the floating IP resource.

- **Timeout** (1 to 999)
  Make the setting of the timeout of [ifconfig] command. This parameter is not available in an environment in which the [ifconfig] command cannot be used. Therefore, specify 60 seconds (default value for such an environment).

ping

These are the detailed settings of the ping command is used to check if there is any overlapped IP address before activating floating IP resource.

- **Interval** (0 to 999)
  Set the interval to issue the ping command.

- **Timeout** (0 to 999)
  Set timeout of the ping command.
  If zero is set, the ping command is not run.
- **Retry Count** (0 to 999)
  Set retry count of the ping command.
- **Forced Fip Activation**
  Specify whether to forcibly activate floating IP address when an overlapped IP address is detected by command check.
- When the check box is selected
  Forced activation is performed.
- When the check box is not selected
  Forced activation is not performed.

ARP Send Count (0 to 999)

Specify how many times you want to send ARP packets when activating floating IP resources.

If this is set to zero (0), ARP packets will not be sent.

Judge NIC Link Down as Failure

Specify whether to check for an NIC Link Down before the floating IP resource is activated. In some NIC boards and drivers, the required ioctl( ) may not be supported. To check the availability of the NIC Link Up/Down monitor, use the [ethtool] command provided by the distributor. For the check method using the [ethtool] command, see "*Note on NIC Link Up/Down monitor resources*" in "*Understanding NIC Link Up/Down monitor resources*" in this guide.

For bonding devices, it is judged as a failure when all the NIC composing the bonding are in the state of Link Down at activation.

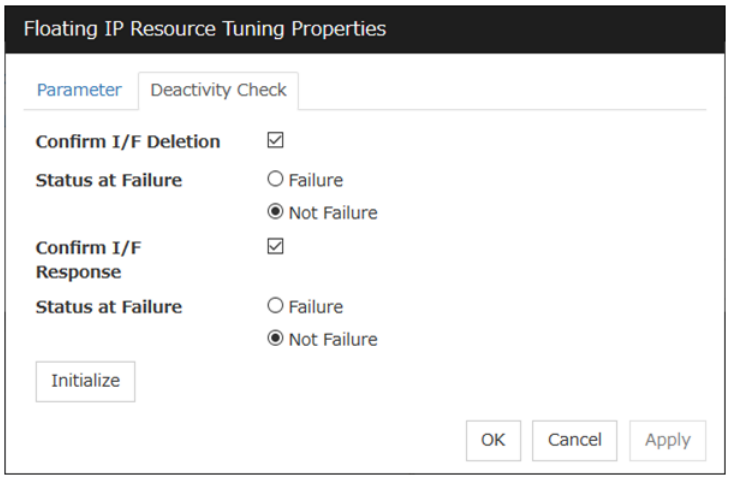
- When the check box is selected
  In the case of an NIC Link Down, the floating IP resource is not activated.
- When the check box is not selected
  Even in the case of an NIC Link Down, the floating IP resource is activated.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

Deactivity Check tab

Detailed settings on deactivity check of floating IP resource are displayed.



Confirm I/F Deletion

- Confirm I/F Deletion
  Specify whether to confirm, whether the target floating IP address has been deleted successfully after the floating IP is deactivated.
- When the check box is selected
  Confirmation is performed.
- When the check box is not selected
  Confirmation is not performed.
- Status at Failure
  Specify how to handle a deactivation error of the floating IP resource.
- Failure:
  Treats as a deactivity failure of a floating IP resource.
- Not Failure:
  Do not treat as a deactivity failure of a floating IP resource.

Confirm I/F Response

- Confirm I/F Response
  Specify whether to confirm, using the ping command, whether the target floating IP address has been deleted successfully after the floating IP is deactivated.
- When the check box is selected
  Confirmation is performed.
- When the check box is not selected
  Confirmation is not performed.
- Status at Failure
  Specify how to handle a deactivation error of the floating IP resource if the floating IP can be reached by the ping command.
- Failure:
  Treats as a deactivity failure of a floating IP resource.
- Not Failure:
  Do not treat as a deactivity failure of a floating IP resource.

3.9 Understanding Virtual IP resources

3.9.1 Dependencies of Virtual IP resources

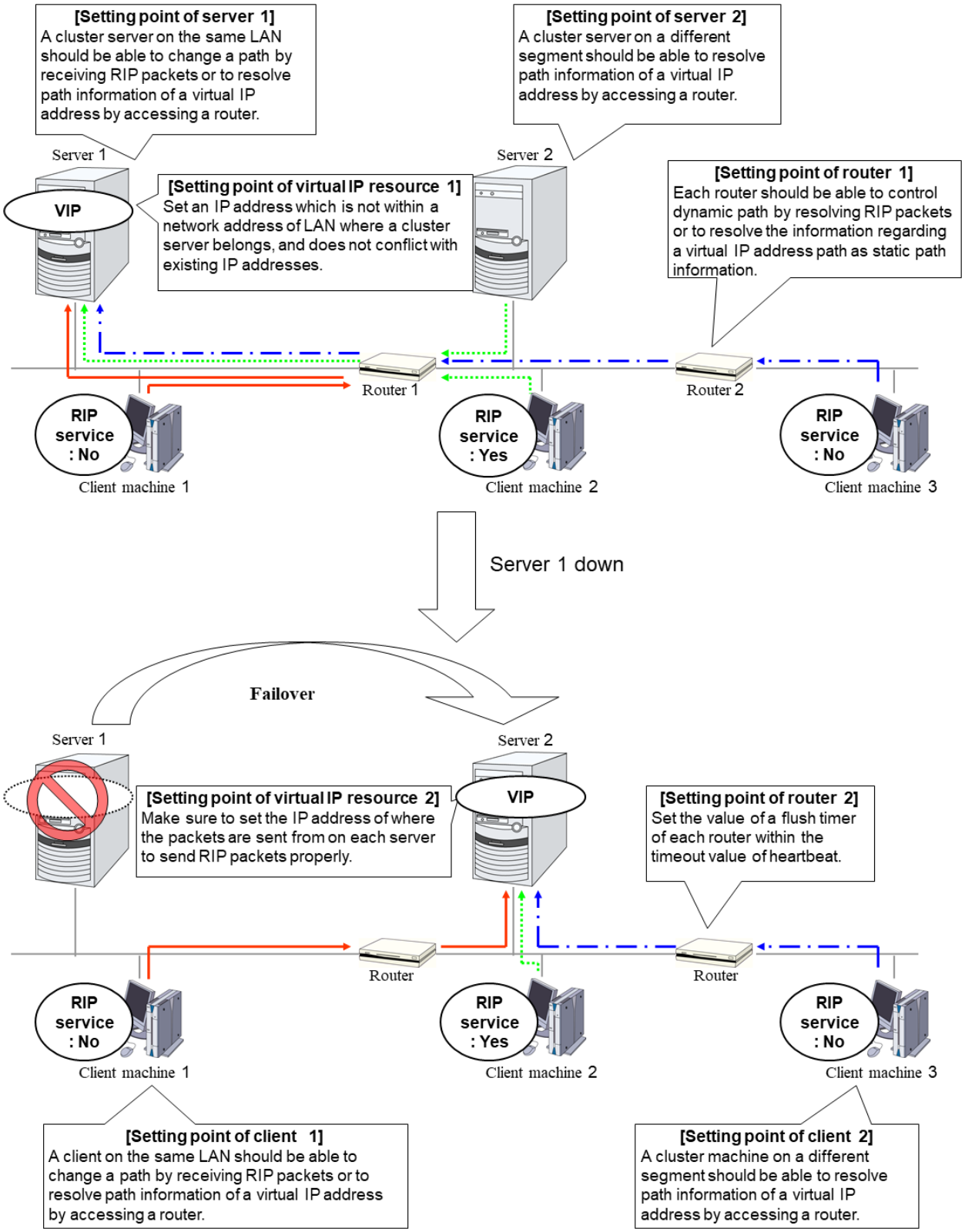
By default, this function does not depend on any group resource type.

3.9.2 Virtual IP resources

Client applications can be connected to a cluster server by using a virtual IP address. The servers can be connected to each other by using a virtual IP address. By using a virtual IP address, switching from one server to the other to which a client is connecting remains transparent even if failover or moving of a failover group occurs. The graphic in the next page shows how virtual IP resources work in the cluster system.

Execute the [ifconfig] command or the API to assign an IP address to the OS. The floating IP resource automatically determines whether to execute the [ifconfig] command or the API. The following shows an example:

- For an environment such as RHEL 7 or later (including RHEL compatible operating systems) on which the [ifconfig] command cannot be used, the API is executed.
- For an environment such as RHEL 7 or later (including RHEL compatible operating systems) on which the net-tools package enables execution of the [ifconfig] command, the API is executed because the output format of the [ifconfig] command is not compatible with that of RHEL 6 or earlier.
- For an environment such as RHEL 6 on which the [ifconfig] command can be used, the [ifconfig] command is executed.


[Setting point of server 1]
A cluster server on the same LAN should be able to change a path by receiving RIP packets or to resolve path information of a virtual IP address by accessing a router.
[Setting point of server 2]
A cluster server on a different segment should be able to resolve path information of a virtual IP address by accessing a router.
Server 1
Server 2
VIP
[Setting point of virtual IP resource 1]
Set an IP address which is not within a network address of LAN where a cluster server belongs, and does not conflict with existing IP addresses.
[Setting point of router 1]
Each router should be able to control dynamic path by resolving RIP packets or to resolve the information regarding a virtual IP address path as static path information.
Router 1
Router 2
RIP service : No
RIP service : Yes
RIP service : No
Client machine 1
Client machine 2
Client machine 3
Server 1 down
Failover
Server 1
Server 2
[Setting point of virtual IP resource 2]
Make sure to set the IP address of where the packets are sent from on each server to send RIP packets properly.
VIP
[Setting point of router 2]
Set the value of a flush timer of each router within the timeout value of heartbeat.
Router
Router
RIP service : No
RIP service : Yes
RIP service : No
Client machine 1
Client machine 2
Client machine 3
[Setting point of client 1]
A client on the same LAN should be able to change a path by receiving RIP packets or to resolve path information of a virtual IP address by accessing a router.
[Setting point of client 2]
A cluster machine on a different segment should be able to resolve path information of a virtual IP address by accessing a router.

3.9.3 Determining virtual IP address

An IP address used as a virtual IP address should satisfy the following conditions:

- The IP address should not be within the network address of the LAN to which the cluster belongs.
- The IP address should not conflict with existing network addresses.

Select one of the following allocation methods to meet the requirements above:

- Obtain a new network IP address for virtual IP address and allocate virtual IP address.
- Determine a network IP address from private IP address space and allocate virtual IP address. The following procedures are given as an example.
- Select one network address from 192.168.0 to 192.168.255 for virtual IP address.
- Allocate up to 64 host IP addresses for virtual IP address from the network address you have selected. (For example, select the network address 192.168.10 and allocate two host IP addresses: 192.168.10.1 and 192.168.10.254)
- Specify 255.255.255.0 to net mask of the virtual IP address.
- When you configure multiple virtual IP addresses, dummy virtual IP addresses may be required. For details, see "*Preparing for using Virtual IP resources*".
  - Private IP addresses are addresses for a closed network and they cannot be accessed using virtual IP address from outside of the network through internet providers.
  - Do not disclose path information of private IP addresses outside the organization.
  - Adjust the private IP addresses to avoid conflict with other address.

3.9.4 Preparing for using Virtual IP resources

If your cluster configuration satisfies the following conditions, you need to set a dummy virtual IP address which has same network address as a virtual IP address on each server.

- When multiple virtual IP resources exist in a cluster.
- Virtual IP resources whose network address and NIC alias name are same exist in a cluster.

Note: If a dummy virtual IP address cannot be configured, other virtual IP addresses assigned to the same NIC alias might be deleted by the OS when any virtual IP resource is deactivated.

A dummy virtual IP address should satisfy the following conditions:

- The IP address has a same network address as of a virtual IP resource, and is unique.
- The IP address can be prepared for each server constructing a cluster.
- The IP address is prepared for each NIC alias.

In the following settings, a dummy virtual IP address should be configured on each server.

- Virtual IP resource 1
  IP address 10.0.1.11/24
  NIC alias name eth1
- Virtual IP resource 2
  IP address 10.0.1.12/24

NIC alias name eth1

For example, set a dummy virtual IP address as follows:

- Dummy virtual IP address of server1
  IP address 10.0.1.100/24
  NIC alias name eth1:0
- Dummy virtual IP address of server2
  IP address 10.0.1.101/24
  NIC alias name eth1:0

Configure the OS by the following procedure so that dummy virtual IP addresses are enabled at OS startup.

In the following procedure, eth1 of server 1 is set to 10.0.1.100/24 as an example.

1. Perform one of the following procedures according to your distribution.

- For SUSE LINUX Enterprise Server:
  Edit the file on the following path. Add the italic parts on the setting information.

  Path

  /etc/sysconfig/network/ifcfg-eth1-"MAC_address_of_eth1"

  Setting information

```
BOOTPROTO='static'
BROADCAST='10.0.0.255'
IPADDR='10.0.0.1'
MTU=''
NETMASK='255.255.255.0'
NETWORK='10.0.0.0'
IPADDR_1='10.0.1.100'
NETMASK_1='255.255.255.0'
NETWORK_1='10.0.1.0'
LABEL_1=1
REMOTE_IPADDR=''
STARTMODE='onboot'
UNIQUE='xxxx'
_nm_name='xxxx'
```

- For other than SUSE LINUX Enterprise Server:
  Create a file on the following path, and add the setting information.

  Path

  /etc/sysconfig/network-scripts/ifcfg-eth1:0

  Setting information

```
DEVICE=eth1:0
BOOTPROTO=static
BROADCAST=10.0.1.255
HWADDR=MAC_address_of_eth1
IPADDR=10.0.1.100
NETMASK_1=255.255.255.0
NETWORK=10.0.1.0
ONBOOT=yes
TYPE=Ethernet
```

2. Restart the OS.

Dummy virtual IP addresses are enabled after the OS restart. Configure server 2 in the same manner.

Follow the procedure below when the settings above is required due to the cluster configuration change.

1. Stop a cluster. For the procedure, see "Suspending EXPRESSCLUSTER Stopping the EXPRESSCLUSTER daemon" in "Preparing to operate a cluster system" in the "Installation and Configuration Guide".
2. Disable the cluster daemon. For the procedure, see "Suspending EXPRESSCLUSTER Disabling the EXPRESSCLUSTER daemon" in "Preparing to operate a cluster system" in the "Installation and Configuration Guide".
3. Change the settings above.
4. Restart the OS, and check that the settings are applied.
5. Enable the cluster daemon. For the procedure, see "Suspending EXPRESSCLUSTER Enabling the disabled EXPRESSCLUSTER daemon" in "Preparing to operate a cluster system" in the "Installation and Configuration Guide".
6. Modify the cluster configuration. For the procedure, see "Modifying the cluster configuration data" in the "Installation and Configuration Guide".

3.9.5 Controlling path

To access to a virtual IP address from a remote LAN, path information of the virtual IP address must be effective to all routers on the path from the remote LAN to the LAN for cluster server. To be specific, the following condition must be satisfied:

- Routers on the cluster servers LAN interpret host RIP.
- Routers on the path from a cluster server to the remote server have the dynamic routing settings or information on the virtual IP address routes has configured as static routing settings.

3.9.6 Requirement to use virtual IP address

Environments where virtual IP address can be used

Virtual IP addresses can be accessed from the machines listed below. Virtual IP address mechanism functions properly even in a LAN where switching hubs are used. However, when a server goes down, TCP/IP that has been connected will be disconnected.

When using virtual IP addresses with a switching HUB that cannot be configured to create a host routing table by receiving host RIP, you need to reserve one new network address and configure virtual IP addresses so that the IP address of each server belongs to a different network address.

- **Cluster servers that belong to the same LAN which the server the virtual IP activates belongs to**

  Virtual IP addresses can be used if the following conditions are satisfied:

  - Machines that can change the path by receiving RIP packets.
  - Machines that can resolve the path information of a virtual IP address by accessing a router.

- **Cluster servers that belongs to the different LAN from which the server the virtual IP activates belongs to**

  Virtual IP addresses can be used if the following condition is satisfied:

  - Machines that can resolve path information of the virtual IP address by accessing a router.

- **Clients that belongs to the same LAN which cluster servers belong to**

  Virtual IP addresses can be used if the following conditions are satisfied:

  - Machines that can change the path by receiving RIP packets.
  - Machines that can resolve the path information of a virtual IP address by accessing a router.

- **Clients on remote LAN**

  Virtual IP addresses can be used if the following condition is satisfied:

  - Machines that can resolve path information of the virtual IP address by accessing a router.

3.9.7 Notes on Virtual IP resources

- Do not execute a network restart on a server on which virtual IP resources are active. If the network is restarted, any IP addresses that have been added as virtual IP resources are deleted.

The following rule applies to virtual IP addresses.

- If virtual IP resources are not inactivated properly (e.g. when a server goes down), the path information of virtual IP resources is not deleted. If virtual IP resources are activated with their path information not deleted, the virtual IP addresses cannot be accessed until their path information is reset by a router or a routing daemon.

  Thus, you need to configure the settings of a flush timer of a router or a routing daemon. For a flush timer, specify the value within the heartbeat timeout value. For details on the heartbeat timeout, see "*Cluster properties*" in "2. *Parameter details*" in this guide.

- MAC address of virtual NIC to which virtual IP is allocated.

  When the virtual IP resource fails over, the corresponding MAC address is changed because the MAC address of virtual NIC to which the virtual IP is allocated is the MAC address of real NIC.

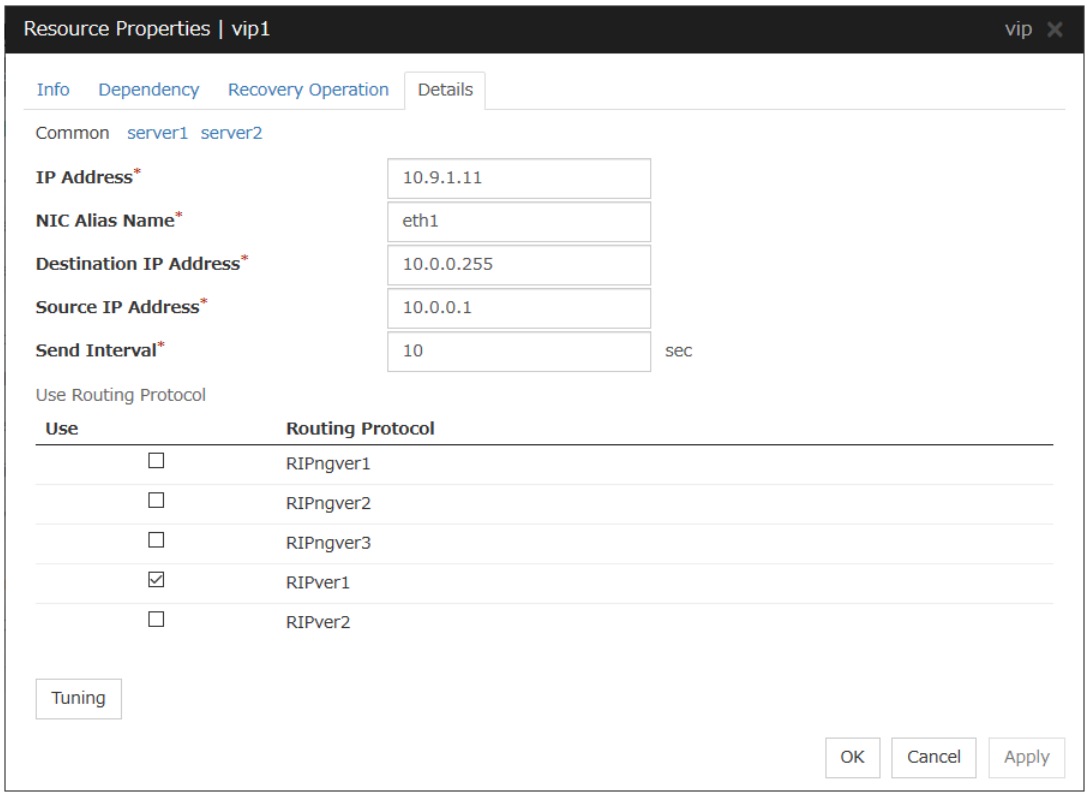
- Source address of IP communication from the running server when the resource activation.

  The source address from the server is basically the real IP of the server even though the virtual IP resource has activated. When you want to change the source address to the virtual IP, the settings are necessary on the application.

- Routing protocol used

  If the routing protocol is set to "RIPver2," the subnet mask for transmitted RIP packets is "255.255.255.255" .

3.9.8 Details tab



IP Address `Server Individual Setup`

Enter the virtual IP address to use. To specify a number of mask bits explicitly, specify the address followed by /number_of_mask_bits. (For an IPv6 address, be sure to specify /number_of_mask_bits.)

NIC Alias Name `Server Individual Setup`

Enter the NIC interface name that activates the virtual IP address to be used.

Destination IP Address `Server Individual Setup`

Enter the destination IP address of RIP packets. IPv4 specifies the broadcast address and IPv6 specifies the router IPv6 address.

Source IP Address `Server Individual Setup`

Enter the IP address to bind when sending RIP packets. Specify the actual IP address activated on NIC which activates the virtual IP address.

To use an IPv6 address, specify a link local address as the source IP address.

Note: The source IP address should be set for individual servers, and set the actual IP address of each server. Virtual IP resources do not operate properly if a source address is invalid. In the **Common** tab, describes the source IP address of any server, other servers, please to perform the individual setting.

Send Interval (1 to 30) `Server Individual Setup`

Specify the send interval of RIP packets.

Use Routing Protocol `Server Individual Setup`

Specify the RIP version to use. For IPv4 environment, select RIPver1 or RIPver2. For IPv6 environment, select RIPngver1 or RIPngver2 or RIPngver3. You can select more than one routing protocols.

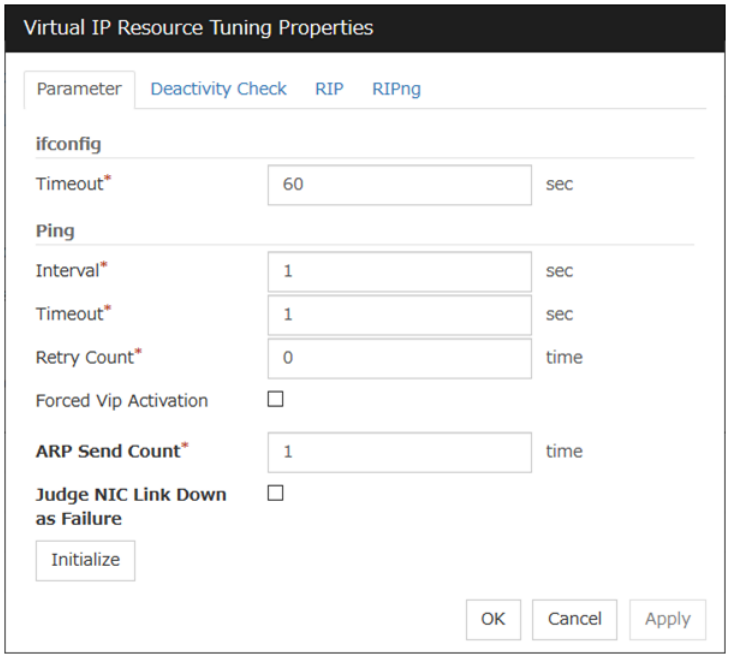
Tuning

Opens **Virtual IP resource Tuning Properties**. You can make the advanced settings for the virtual IP resources.

Virtual IP Resource Tuning Properties

Parameter tab

Detailed setting for virtual IP parameter is displayed.



ifconfig

The following is the detailed settings on getting IP addresses and on the ifconfig command executed for the activation and/or deactivation of the virtual IP resource.

- **Timeout** (1 to 999)
  Make the setting of the timeout of [ifconfig] command. This parameter is not available in an environment in which the [ifconfig] command cannot be used. Therefore, specify 60 seconds (default value for such an environment).

Ping

In this box, make detailed settings of the ping command used to check for any overlapped IP address before activating the virtual IP resource.

- **Interval** (0 to 999)
  Specify the interval to issue the ping command in seconds.
- **Timeout** (0 to 999)
  Specify the time-out for the ping command in seconds.
  When 0 is specified, the ping command is not run.
- **Retry Count** (0 to 999)
  Specify how many retries of issuing the ping command are attempted.

- **Forced Vip Activation**
  Use this button to configure whether to forcibly activate the virtual IP address when an overlapped IP address is found using the ping command.
- When the check box is selected
  Forcefully activate the virtual IP address.
- When the check box is not selected
  Do not forcefully activate the virtual IP address.

ARP Send Count (0 to 999)

Specify how many times you want to send ARP packets when activating virtual IP resources.

If this is set to zero (0), ARP packets will not be sent.

Judge NIC Link Down as Failure

Specify whether to check for an NIC Link Down before the virtual IP resource is activated. In some NIC boards and drivers, the required ioctl( ) may not be supported. To check the availability of the NIC Link Up/Down monitor, use the [ethtool] command provided by the distributor. For the check method using the [ethtool] command, see "*Note on NIC Link Up/Down monitor resources*" in "*Understanding NIC Link Up/Down monitor resources*" in this guide.

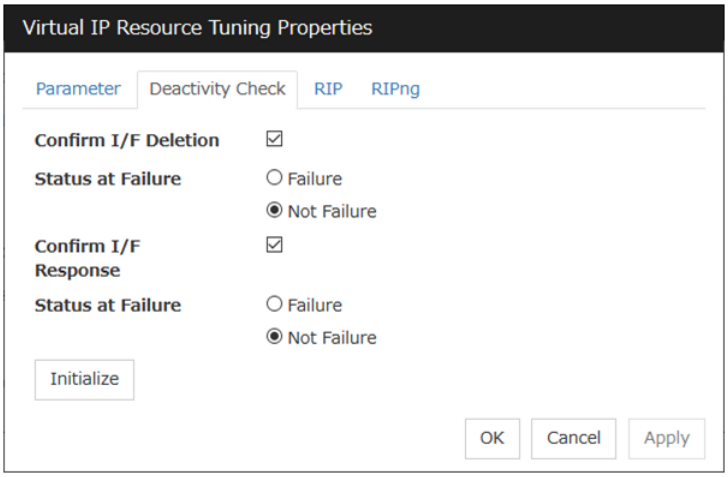
- When the check box is selected
  In the case of an NIC Link Down, the floating IP resource is not activated.
- When the check box is not selected
  Even in the case of an NIC Link Down, the floating IP resource is activated. This operation is the same as before.

Initialize

Click **Initialize** to reset the values of all items to their default values.

Deactivity Check tab

Detailed settings on deactivity check of virtual IP resource are displayed.



Confirm I/F Deletion

After deactivating the virtual IP, the cluster makes sure that the given virtual IP address disappeared successfully. Configure if failure is treated as the IP resource deactivity failure.

- Failure:

Treats as a deactivity failure of a virtual IP resource.

- Not Failure:
  Does not treat as a deactivity failure of a virtual IP resource.

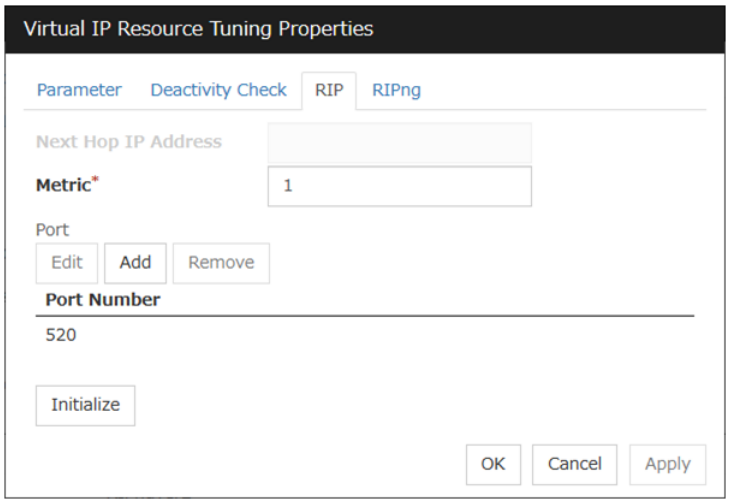
Confirm I/F Response

After deactivating a virtual IP, a cluster makes sure that the given virtual IP address cannot be accessed by the ping command. Configure reaching the virtual IP address by the ping command is treated as deactivity failure.

- Failure:
  Treats as a deactivity failure of a virtual IP resource.
- Not Failure:
  Do not treat as a deactivity failure of a virtual IP resource.

RIP tab

Detailed settings on RIP of virtual IP resource are displayed.



Next Hop IP Address

Enter the next hop address (address of the next router). Next hop IP address can be omitted. It can be specified for RIPver2 only. You cannot specify a netmask or prefix.

Metric (1 to 15)

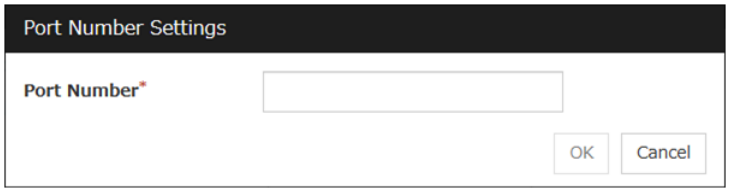
Enter a metric value of RIP. A metric is a hop count to reach the destination address.

Port

On **Port Number**, a list of communication ports used for sending RIP is displayed.

Add

Add a port number used for sending RIP. Clicking this button displays the dialog box to enter a port number.



Port No.

Enter a port number to be used for sending RIP, and click **OK**.

Edit

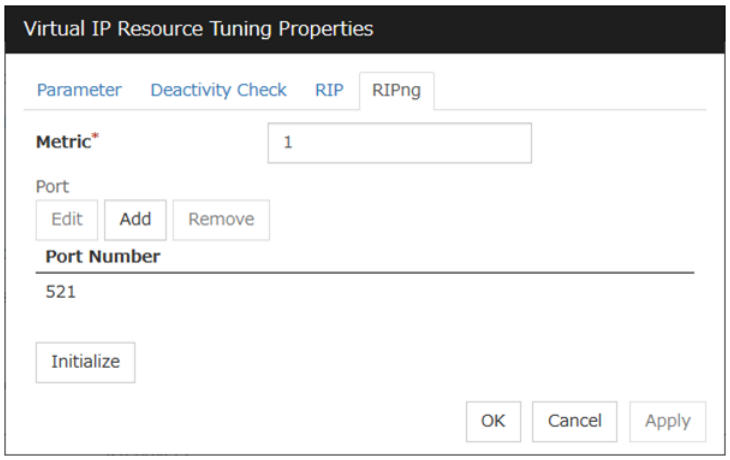
A dialog box to enter a port number is displayed. The port selected in the **Port Number** is displayed. Edit it and click **OK**.

Remove

Click **Remove** to remove the selected port on the **Port Number**.

RIPng tab

Detailed settings on RIPng of virtual IP resource are displayed.



Metric (1 to 15)

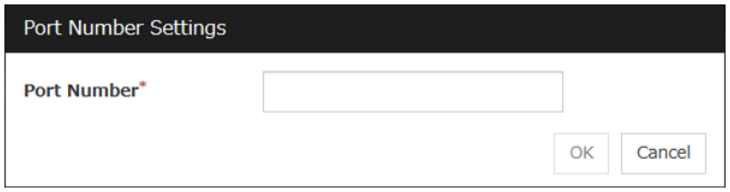
Enter a metric value of RIPng. A metric is a hop count to reach the destination address.

Port

On **Port Number**, a list of ports used for sending RIPng is displayed.

Add

Add a port number used for sending RIPng. Clicking this button displays the dialog box to enter a port number.



Port No.

Enter a port number to be used for sending RIPng, and click **OK**.

Edit

A dialog box to enter a port number is displayed. The port selected in the **Port Number** is displayed. Edit it and click **OK**.

Remove

Click **Remove** to remove the selected port on the **Port Number**.

3.10 Understanding Mirror disk resources

3.10.1 Dependencies of Mirror disk resource

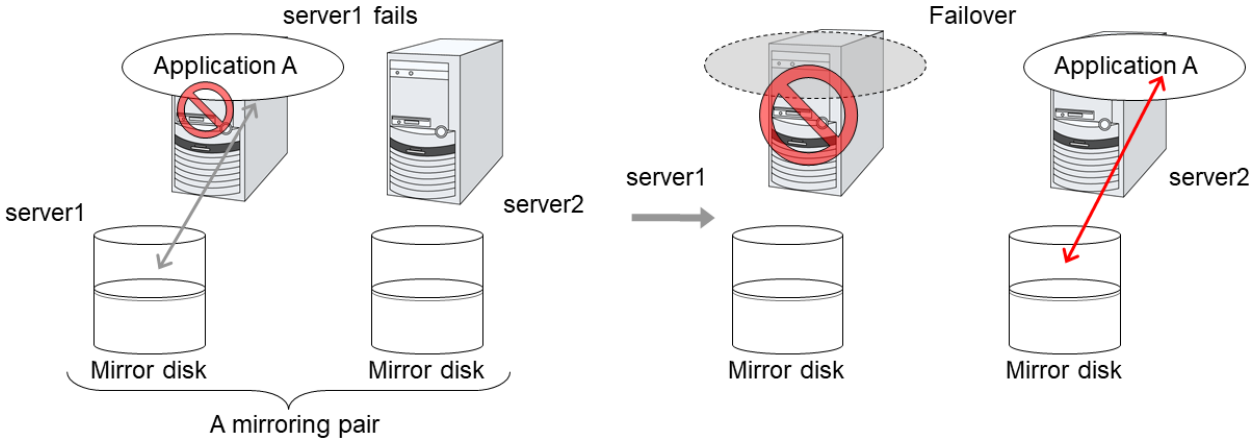
By default, this function depends on the following group resource type.

Group resource type
Floating IP resource
Virtual IP resource
AWS Elastic IP resource
AWS Virtual IP resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.10.2 Mirror disk

Mirror disk

Mirror disks are a pair of disks that mirror disk data between two servers in a cluster.



Data partition

Partitions where data to be mirrored (such as application data) is stored are referred to as data partitions. Allocate data partitions as follows:

- Data partition size
  The size of data partition should be 1GB or larger but smaller than 1TB.
  (Less than 1TB size is recommended from the viewpoint of the construction time and the restoration time of data.)
- Partition ID
  83(Linux)
- If Execute initial mkfs is selected in the cluster configuration information, a file system is automatically created when a cluster is generated.
- EXPRESSCLUSTER is responsible for the access control (mount/umount) of file system. Do not configure the settings that allow the OS to mount or unmount a data partition.

Cluster partition

Dedicated partitions used in EXPRESSCLUSTER for mirror partition controlling are referred to as cluster partition.

Allocate cluster partitions as follows:

- Cluster partition size
  1024MB or more. Depending on the geometry, the size may be larger than 1024MB, but that is not a problem.
- Partition ID
  83(Linux)
- A cluster partition and data partition for data mirroring should be allocated in a pair.
- Do not make the file system on cluster partitions.
- EXPRESSCLUSTER performs the access control of the file system (mount/umount) as a device to mount the mirror partition device. Thus, do not configure the settings to mount or unmount the cluster partition on the OS side.

Mirror Partition Device (/dev/NMPx)

One mirror disk resource provides the file system of the OS with one mirror partition. If a mirror disk resource is registered to the failover group, it can be accessed from only one server (it is generally the primary server of the resource group).

Typically, the mirror partition device (dev/NMPx) remains invisible to users (AP) because they perform I/O via a file system. The device name is assigned so that the name does not overlap with others when the information is created by the Cluster WebUI.

- EXPRESSCLUSTER is responsible for the access control (mount/umount) of file system. Do not configure the settings that allow the OS to mount or unmount a data partition.
  Mirror partition's (mirror disk resource's) accessibility to applications is the same as switching partition (disk resources) that uses shared disks.
- Mirror partition switching is done for each failover group according to the failover policy.

Mirror disk connect

Maximum of two mirror disk connects can be registered per mirror disk resource.

- When two mirror disk connects are registered, operations such as switching etc. are as follows:
  - The paths used to synchronize mirror data can be duplicated. By setting this, mirror data can be synchronized even when one of the mirror disk connects becomes unavailable due to such as disconnection.
  - The speed of mirroring does not change.
  - When mirror disk connects switch during data writing, mirror break may occur temporarily. After switching mirror disk connects completes, differential mirror recovery may be performed.
  - When mirror disk connects switch during mirror recovery, mirror recovery may suspended. If the setting is configured so that the automatic mirror recovery is performed, mirror recovery automatically resumes after switching mirror disk connects completes. If the setting is configured so that the automatic mirror recovery is not performed, you need to perform mirror recovery again after switching mirror disk connects completes.

For the mirror disk connect settings, see "*Cluster properties*""*Interconnect tab*" in "*2. Parameter details*" in this guide.

- Disk partition

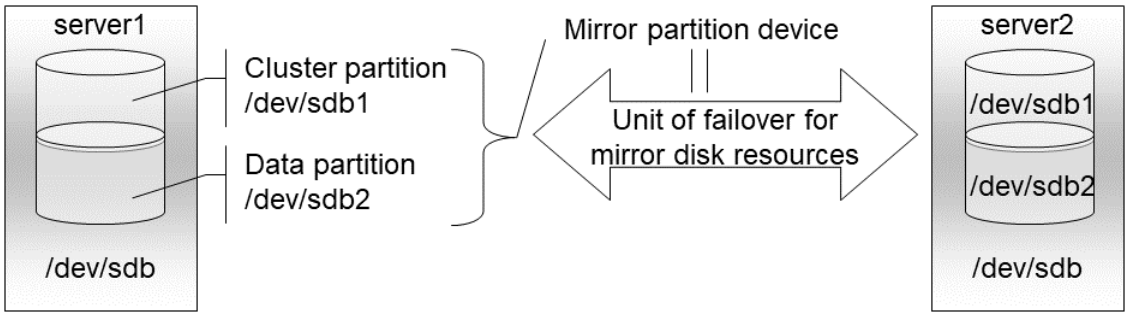
  It is possible to allocate a mirror disk partition (cluster partition, data partition) on a disk, such as root partition or partition, where the OS is located

  - When maintainability at a failure is important:

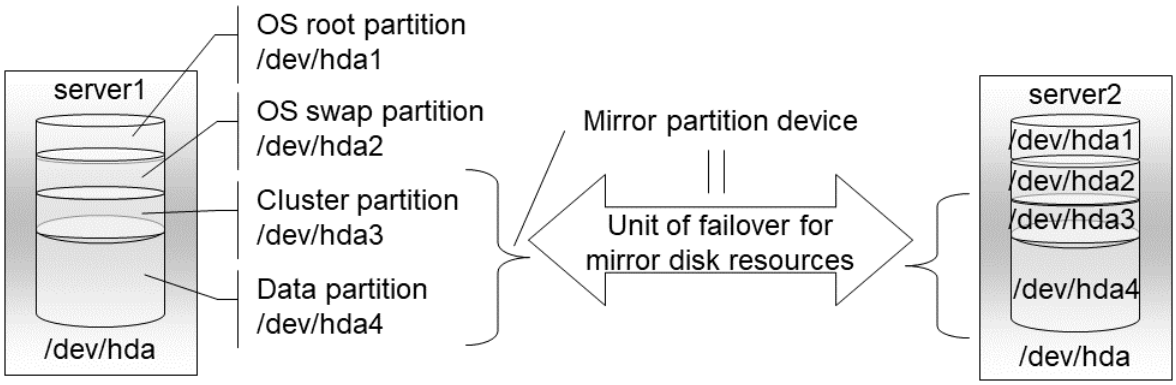
It is recommended to allocate a disk for mirror which is not used by the OS (such as root partition, swap partition).

– If LUN cannot be added due to H/W RAID specifications:
If you are using hardware/RAID preinstall model where the LUN configuration cannot be changed, you can allocate a mirror partition (cluster partition, data partition) in the disk where the OS (root partition, swap partition) is located.

Example: Adding a SCSI disk to both servers to create a pair of mirroring disks.

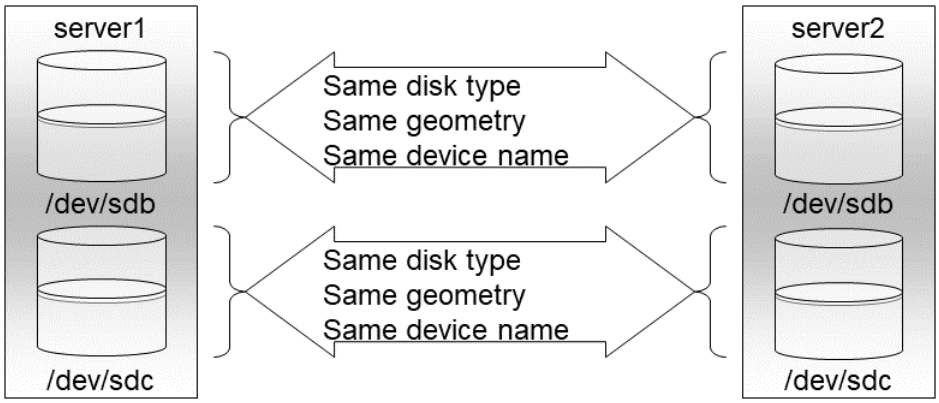


Example: Using available area of the IDE disks of both servers on which OS of is stored to create a pair of mirroring disks.

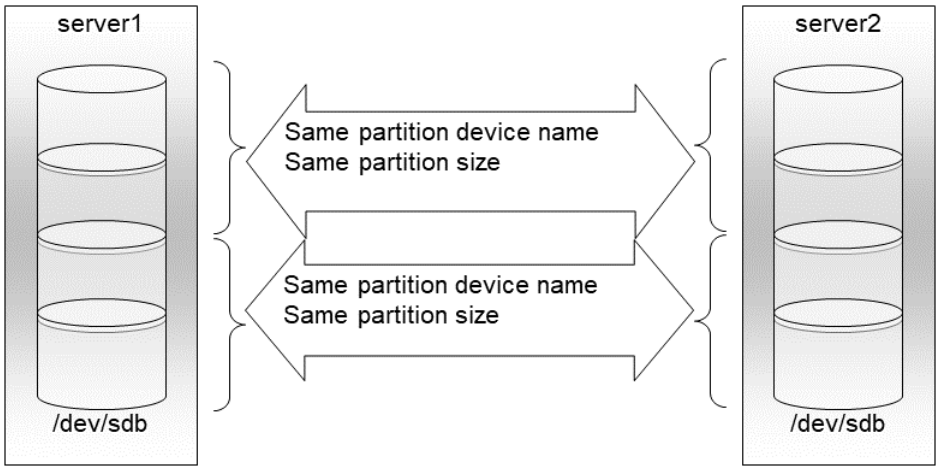


- Disk allocation
You may use more than one disk for mirror disk. You may also allocate multiple mirror partition devices to a single disk.

Example: Adding two SCSI disks to both servers to create two pairs of mirroring disks.



Example: Adding a SCSI disk for both servers to create two mirroring partitions.



3.10.3 Understanding mirror parameters

Mirror Data Port Number

Set the TCP port number used for sending and receiving mirror data between servers. It needs to be configured for individual mirror disk resources.

The default value is displayed when a mirror disk resource is added in Cluster WebUI based on the following condition:

- A port number of 29051 or later which is unused and the smallest

Heartbeat Port Number

Set the port number that a mirror driver uses to communicate control data between servers. It needs to be configured for individual mirror disk resources.

The default value is displayed when a mirror disk resource is added in Cluster WebUI based on the following condition:

- A port number of 29031 or later which is unused and the smallest

ACK2 Port Number

Set the port number that a mirror driver uses to communicate control data between servers. It needs to be configured for individual mirror disk resources.

The default value is displayed when a mirror disk resource is added in Cluster WebUI based on the following condition:

- A port number of 29071 or later which is unused and the smallest

The maximum number of request queues

Configure the number of queues for I/O requests (write requests) from the higher layer of the OS to the mirror disk driver. If a larger value is selected, the write performance will improve but more physical memory will be required.

Note the following when setting the number of queues:

- The improvement in the performance is expected when a larger value is set under the following conditions:
  - Large amount of physical memory is installed on the server and there is plenty of available memory.

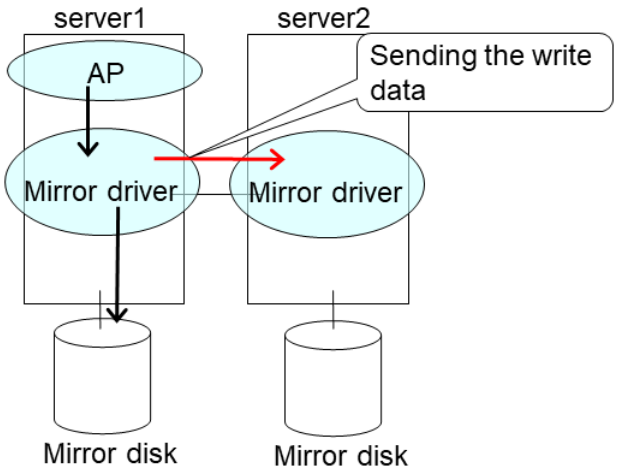
Connection Timeout

This timeout is used for the time passed waiting for a successful connection between servers when recovering mirror or synchronizing data.

Send timeout

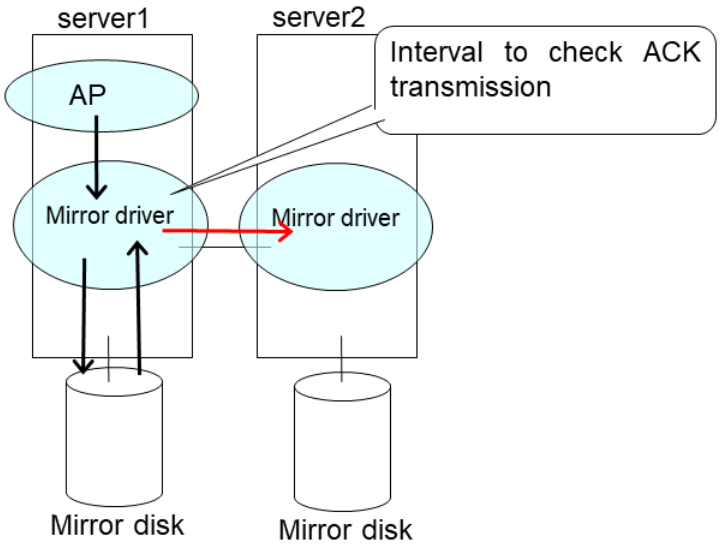
This timeout is used:

- For the time passed waiting for the write data to be completely sent from the active server to the standby server from the beginning of the transmission at mirror return or data synchronization.



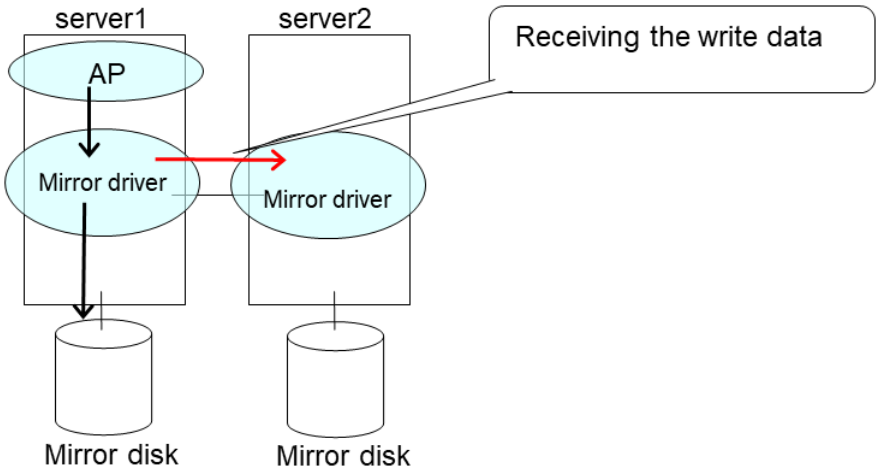
  In detail, this timeout is to wait for write data to be completely stored in the send buffer of a network (TCP) once data storing begins. If the TCP buffer is full and there is no free space, a timeout occurs.

- For the time interval for checking if the ACK send (in which the active server notifies the standby server of write completion) is necessary.



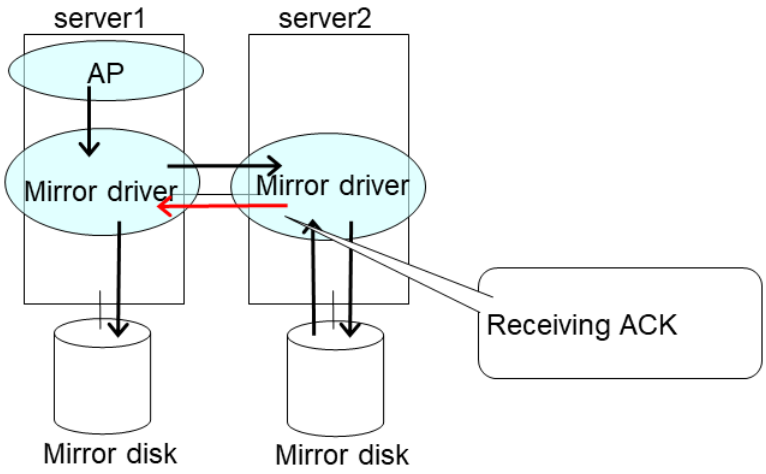
Receiving timeout

- This timeout is used for the time passed waiting for the standby server to completely receive the write data from the active server from the beginning of the transmission.



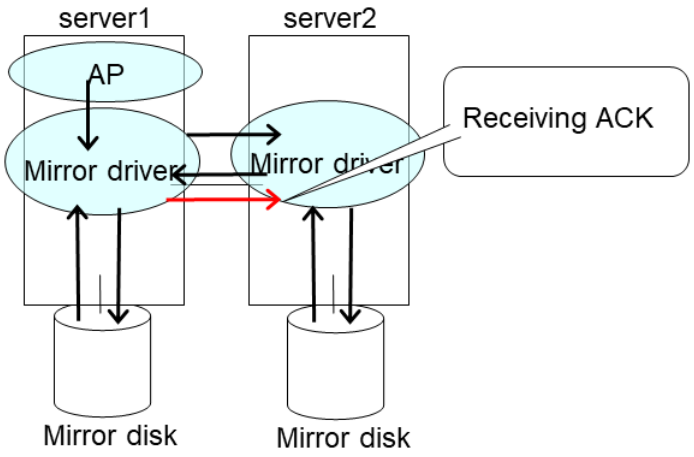
Ack timeout

- This timeout is used for the time passed waiting for the active server to receive the ACK notifying the completion of write once the active server begins sending write data to the standby server.
  If the ACK is not received within the specified timeout time, the difference information is accumulated to the bitmap for difference on the active server.

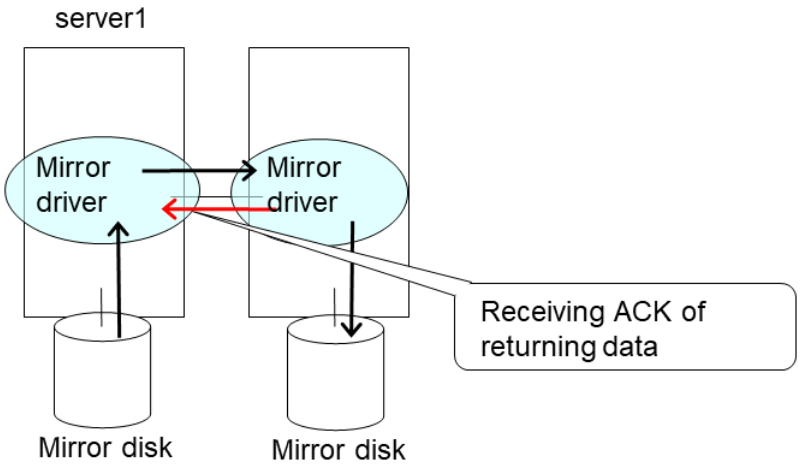


  If you use the synchronous mode, a response to an application might wait until receiving the ACK or until it's timeout.
  If you use the asynchronous mode, a response to an application is returned after writing to the active server's disk. (This response does not wait for ACK).

- This timeout is used for the time passed waiting for the standby server to receive the ACK from the active server after the standby server completely sent the ACK notifying the completion of write.
  If the ACK for the active server is not received within the specified timeout time, the difference information is accumulated to the bitmap for difference on the standby server.



- This timeout is used for the time passed waiting for the copy source server to receive the ACK notifying completion from the copy destination server after it began the data transmission when recovering mirror.



When the sending amount of the recovery data reaches the Recovery Data Size, 1 ACK is returned (Recovery Data Size is described below.)

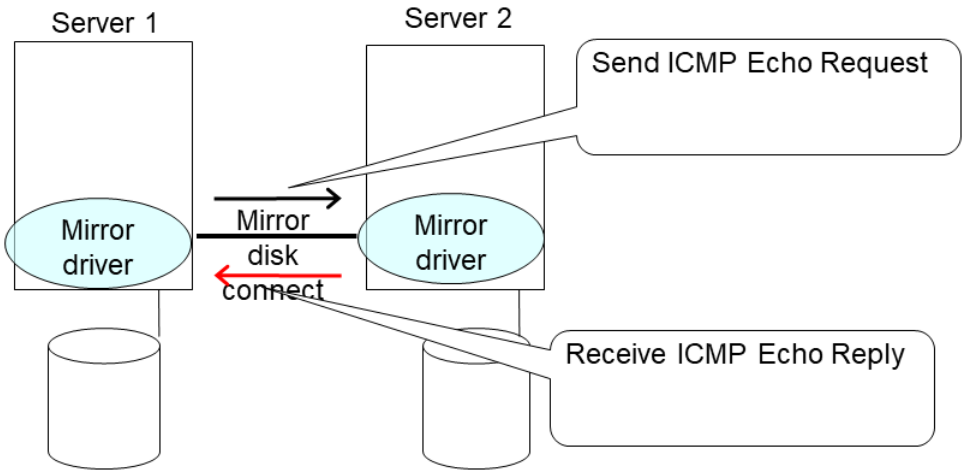
Therefore when the Recovery Data Size becomes larger, sending becomes more efficient. But if an ACK timeout occurred, re-send data size also becomes larger.

Heartbeat Interval (1 to 600)

Heartbeat interval (sec) for checking the soundness of the mirror disk connect between the mirror drivers of two servers. Use the default whenever possible.

ICMP Echo Reply Receive Timeout (1 to 100)

Value used for heartbeat that is performed to check the soundness of the mirror disk connect between the mirror drivers of two servers. The maximum wait time from when ICMP Echo Request is sent until ICMP Echo Reply is received from the destination server. If ICMP Echo Reply is not received even if this timeout elapses, the reception is repeated for up to the ICMP Echo Request retry count, explained later. Use the default whenever possible.



ICMP Echo Request Retry Count (1 to 50)

Enter how many times you want to retry at the maximum to send ICMP Echo Request if ICMP Echo Reply from the destination server to ICMP Echo Request cannot be received before the ICMP Echo Reply receive timeout. Use the default whenever possible.

Adjustment between the ICMP Echo Reply receive timeout and ICMP Echo Request retry count.

You can adjust the sensitivity that determines mirror disk connect disconnection by adjusting the ICMP Echo Reply receive timeout and ICMP Echo Request retry count.

- **Increasing the value**
  - Case in which a network delay occurs in a remote location
  - Case in which a temporary failure occurs in a network
- **Decreasing the value**
  - Case in which the time for detecting a network failure is to be reduced

Difference Bitmap Update Interval

Information to be written to the bit map for difference is temporarily accumulated in memory, and is written to the cluster partition at regular intervals. This interval is used for the standby server to check whether this is information to write to the bit map as well as to perform a write.

Difference Bitmap Size

Users can set the difference bitmap size.

If the data partition size is large, there are times efficiency of differential copy can be better by enlarging the size of difference bitmap.

However, memory efficiency could be deteriorated. Please use the default value under normal conditions.

This setting is needed to be set before establishing a mirror disk resource and/or a hybrid disk resource in the cluster. If the mirror disk resource and/or the hybrid disk resource already exist in the cluster, the setting cannot be changed.

Initial Mirror Construction

Specify if configure initial mirroring[4] when activating cluster for the first time after the cluster is created.

- Execute the initial mirror construction
  An initial mirroring is configured when activating cluster for the first time after the cluster is created.
  The time that takes to construct the initial mirror is different from ext2/ext3/ext4 and other file systems.

[4] Regardless of the existence of the FastSync Option, the entire data partition is copied.

- Do not execute initial mirror construction

  Does not configure initial mirroring after constructing a cluster.

  Before constructing a cluster, it is necessary to make the content of mirror disks identical without using EXPRESSCLUSTER.

Initial mkfs

Specify if initial file creation in the data partition of the mirror disk is configured when activating cluster for the first time after the cluster is created.

- Execute initial mkfs

  The first file system is created when activating cluster for the first time immediately after the cluster is created.

- Do not execute initial mkfs

  Does not create a first file system to the data partition in the mirror disk when activating cluster for the first time immediately after the cluster is created.

  You can configure the settings so that the initial mkfs setting is not executed when a file system has been set up in the data partition of the mirror disk and contains data to be duplicated, which does not require file system construction or initialization by mkfs.

  The mirror disk partition[5] configuration should fulfill mirror disk resource requirements.

If **Does not execute initial mirror construction** is selected, **Execute initial mkfs** cannot be chosen. (Should mkfs be performed for the active and standby data partitions, even immediately after mkfs is performed, differences will arise between the active data partition and standby data partition for which mkfs has been executed. Therefore, when initially executing mkfs, initial mirror construction (copying of the active data partition and the standby data partition) is also required. If [Execute initial mirror construction] is selected, [Execute initial mkfs] can be chosen.)

Number of Queues

In the **Asynchronous** mode, specify the maximum number of queues in which write requests to the remote disk are held. For details on asynchronous mode setting, see "*Details tab*".

In cases such as when a slow network is used or if the amount of data requiring transmission (synchronization) increases as the amount written to the mirror increases, those data waiting for transmission (waiting for synchronization to be complete) are accumulated in these queues. Then, if the network speed becomes fast or if the amount of data transmitted (synchronized) decreases along with reduced writes to the mirror, data in queues waiting for transmission are transmitted. In this way, queues are used to absorb the increase and decrease in written data and the network speed change and to transmit data to the network.

If a larger value is set for the number of queues to absorb the increase and decrease in synchronous data, usually, the maximum time until synchronization is complete (Ack timeout) should also be set to a larger value.

These queues are created in the memory space. However, if the number of data units waiting for synchronization to be completed exceeds the maximum number of queues, then the excess is recorded and stored as a file.

By setting a larger maximum number of queues, the I/O performance may be improved, but more memory space will be used. For information on the required memory size, see " Installation requirements for EXPRESSCLUSTER" - " Software" - " Required memory and disk size" in the "Getting Started Guide".

In the case that the maximum number of queues is too large, if a synchronization timeout (Ack timeout) or a mirror communication break occurs while writing a large amount of data, an enormous volume of queue processes will arise at a time, possibly leading to extremely high load.

Rate limitation of Mirror Connect

[5] There must be a cluster partition in a mirror disk. If you cannot allocate a cluster partition when the single server disk is the mirroring target, take a backup and allocate the partition.

In the **Asynchronous** mode, the server tries to transfer data that has been temporarily queued to the standby server as quickly as possible. For this reason, if the channel for mirror disk connect is used for other applications, the communication band may become busy, hindering other communications.

In this case, by imposing bounds on the communication band for mirror connect communication, the impact on other communications can be reduced.

If, however, the communication band for mirror disk connect is smaller than the average amount of data to be written to the mirror disk, the queued data cannot be fully transferred to the standby server, and at last the maximum number of queues is reached, causing mirroring to interrupt (mirror break). The bandwidth should be large enough to allow data to be written into the business application.

Note: This function imposes a limit on the communication band by having a maximum one-second pause when the total amount of data to be transferred per second exceeds the configured value. If the amount of data to be written to the disk at one time exceeds the configured value, the expected level of performance may not be achieved. For example, when the amount of data to be transferred to a copy of a mirror disk at one time is 64 KB, even if you set a communication band limit of 64 KB or less per second, the actual amount of communication during copy can be greater than the configured value.

History File Store Directory

Specify the directory of a file in which, if the maximum number of queues created in the memory is exceeded in the **Asynchronous** mode, the excess is recorded.

It is recommended to prepare a disk for storing the history file and set the **History File Store Directory** on the disk, because the amount of I/O to/from the mirror disk may increase the I/O load on the **History File Store Directory**.

Size Limitation of History File

Specify the maximum accumulation in the history file in the **Asynchronous** mode. When the accumulation reaches the maximum, a mirror break occurs.

Compress Data

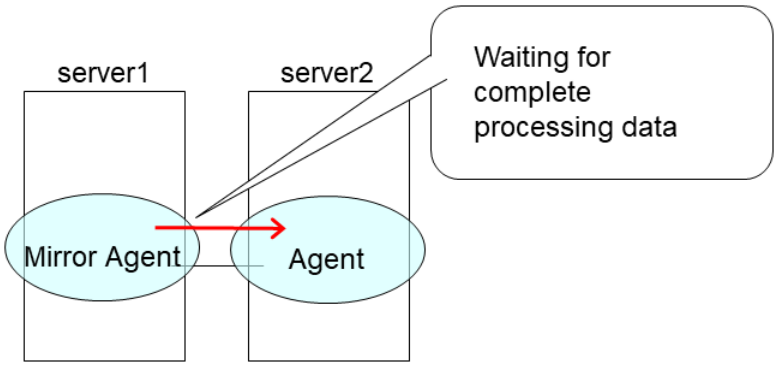
Specify whether to compress mirror synchronous data (in the case of **Asynchronous** mode) or mirror recovery data before transmission. If a slow network is used, compressing transmission data can reduce the amount of data to be transmitted.

Note:

- Compression may increase the CPU load at data transmission.
- In a slow network, compression reduces the amount of data transmitted, so a reduction in time can be expected compared to uncompressed data. Conversely, in a fast network, increases in compression processing time as well as load are more noticeable than a reduction in transfer time, so a reduction in time might not be expected.
- If most of data has a high compression efficiency, compression reduces the amount of data transmitted, so a reduction in time can be expected compared to uncompressed data. Conversely, if most of data has a low compression efficiency, not only the amount of data transmitted is not reduced, but also the compression processing time and load increase, in which case a reduction in time might not be expected.

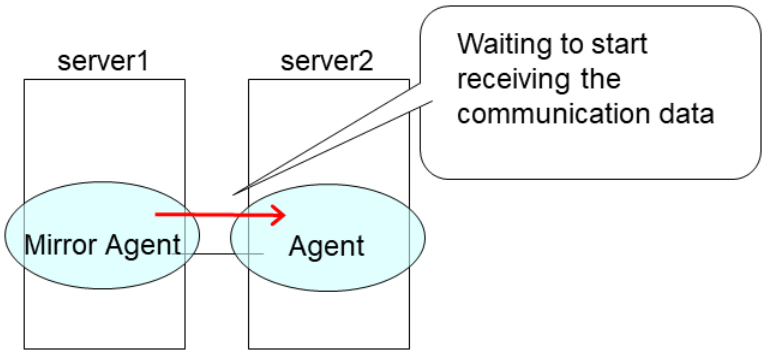
Mirror agent send time-out

Time-out for the mirror agent waiting to complete processing data after sending a request to the other server.



Mirror agent receiving time-out

Time-out for the mirror agent waiting to start receiving data after the mirror agent creates a communication socket with the other server.



Recovery Data Size (64 to 32768)

Specify the size of data in mirror recovery between two servers in one processing. The default size is used in general.

- Specify a larger size
  - It takes less time to completely process mirror recovery because the number of data exchanges between two servers decreases.
  - During mirror recovery, disk performance may degrade.

    (This is because, if the disk read range for mirror recovery data and the disk write range for a file system overlap, access is excluded and a wait occurs until the first processing is complete.

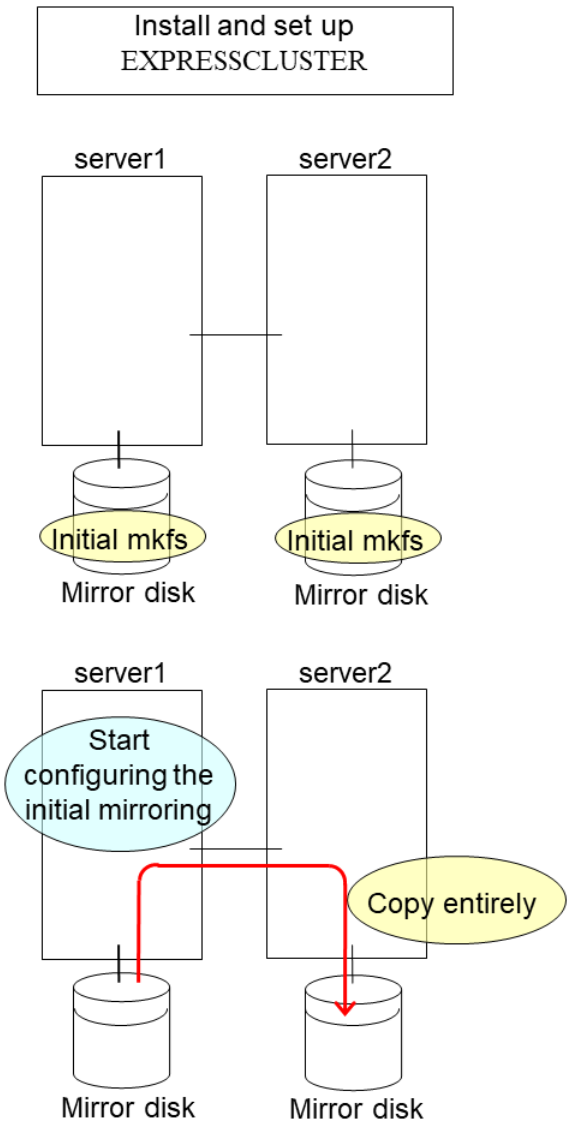
    In a slow network environment, if there is a large amount of recovery data, a single data transfer for mirror recovery will take more time. If a normal disk access for mirror data and this data transfer range for mirror recovery overlap, disk access is awaited until the transfer is complete. This may lead to degraded disk performance.

    Therefore, specify a smaller size, especially for a slow network environment.)
- Specify a smaller size
  - Sending/receiving data between two servers gets segmented and the possibility for a timeout to occur is decreased with a slow network speed or a high server load.
  - Because the number of exchanges between two servers increases, mirror recovery takes more time, especially in a network where delay occurs easily.

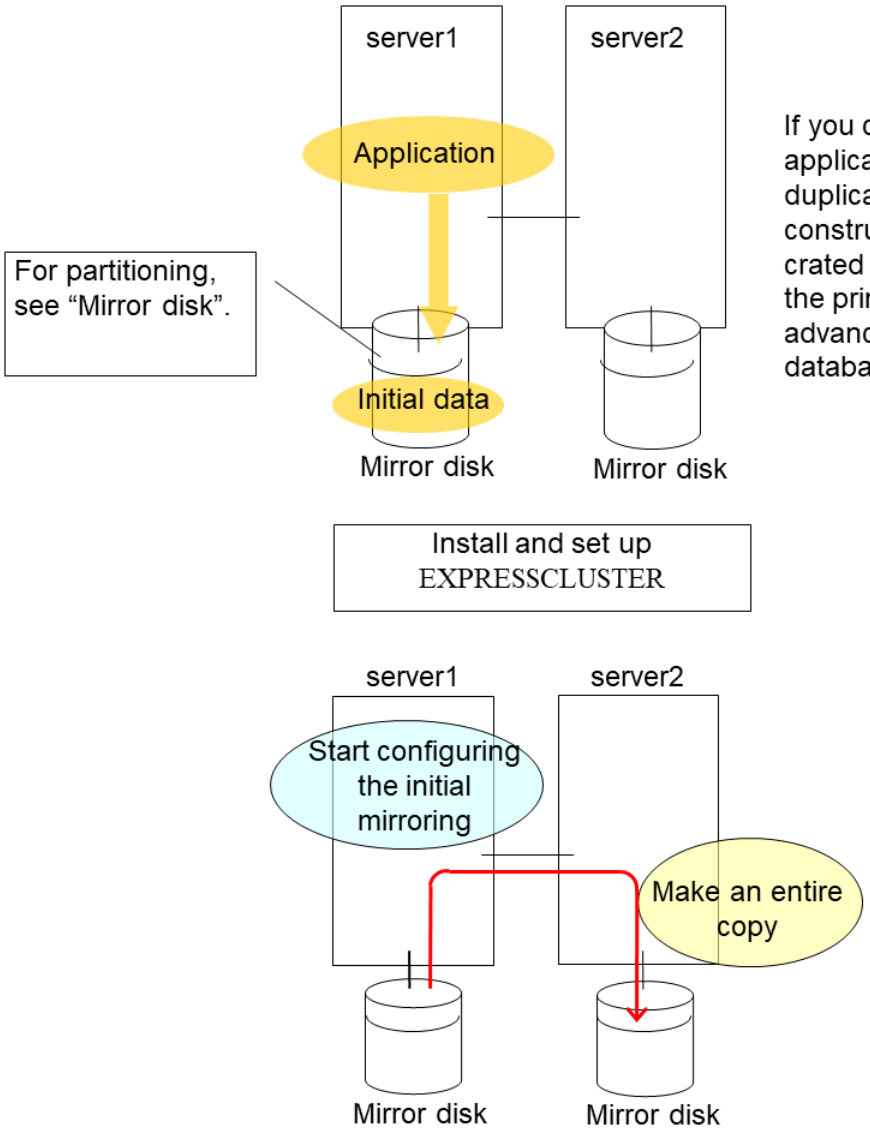
3.10.4 Examples of mirror disk construction

If you are using a disk that has been used as a mirror disk in the past, you must format the disk because old data exists in its cluster partition. For the initialization of a cluster partition, refer to the " Installation and Configuration Guide".

- Execute the initial mirror construction
  Executing initial mkfs



- Execute the initial mirror construction
  Not executing initial mkfs

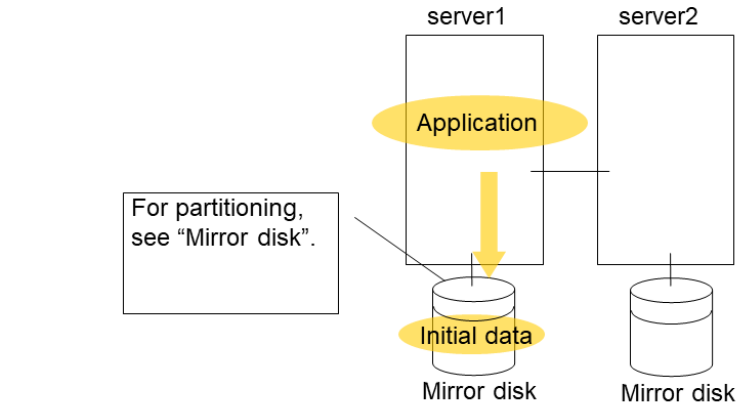


- Do not execute initial mirror construction
  Not executing initial mkfs

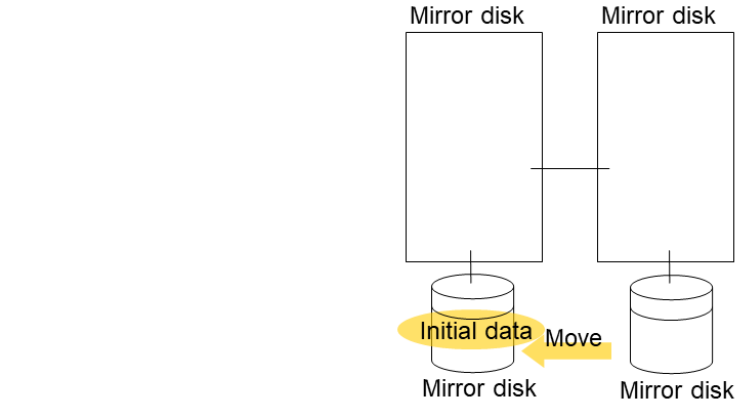
  The following is an example of making the mirror disks of both servers identical. (This cannot be done after constructing the cluster. Be sure to perform this before the cluster construction.)

  Example 1

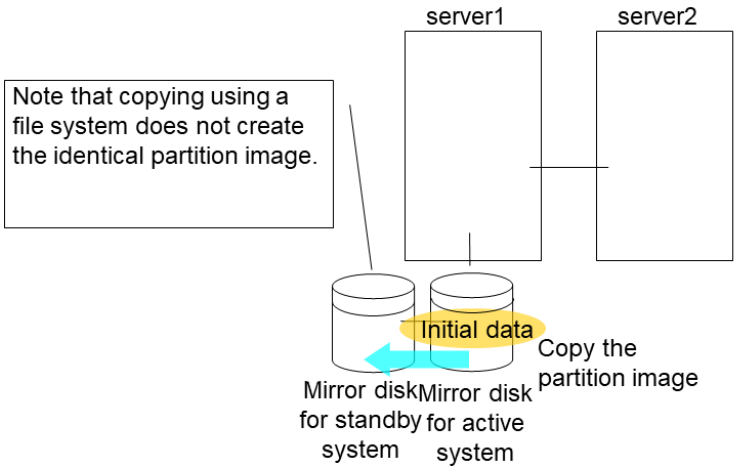
  Copying partition images of a disk



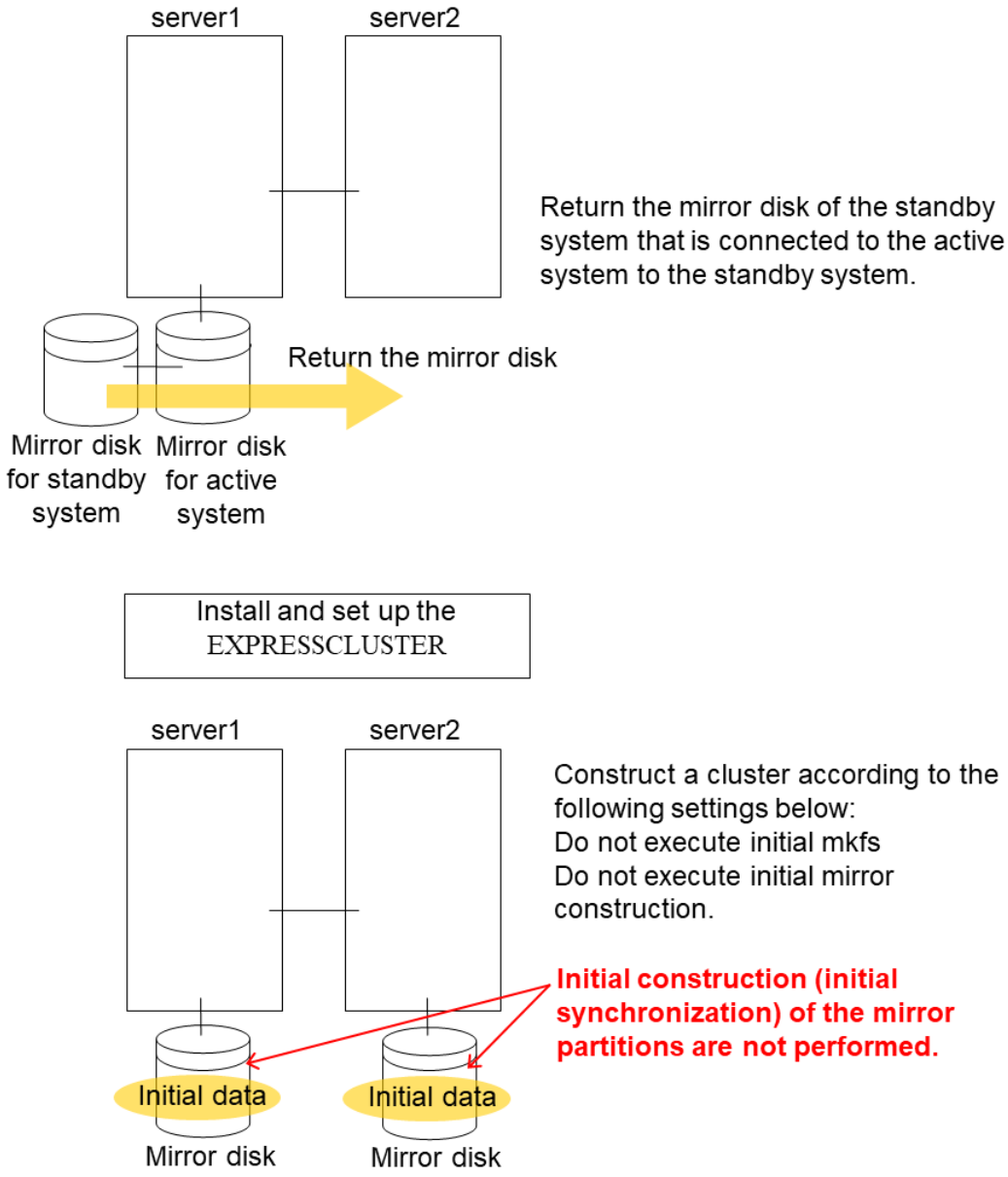
If it is possible to prepare the application data which will be duplicated before cluster construction, it should be created in the data partition of the active mirror disk in advance. (ex. the initial DB of a database)



Remove the mirroring disk of the standby system. Connect it to the active server.
To the active system, connect its mirroring disk and the (moved) disk of the standby system.

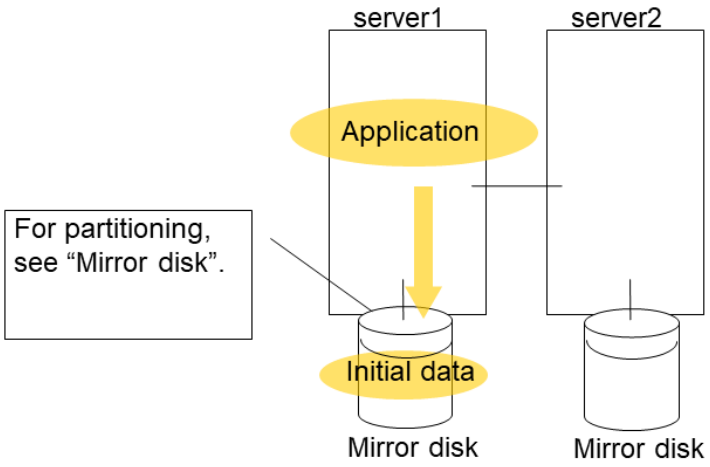


While the mirror disk of the active system is unmounted, copy the entire partition using a method, such as the dd command, from the data partition of the mirror disk of the active system to the data partition of the mirror disk of the standby system.

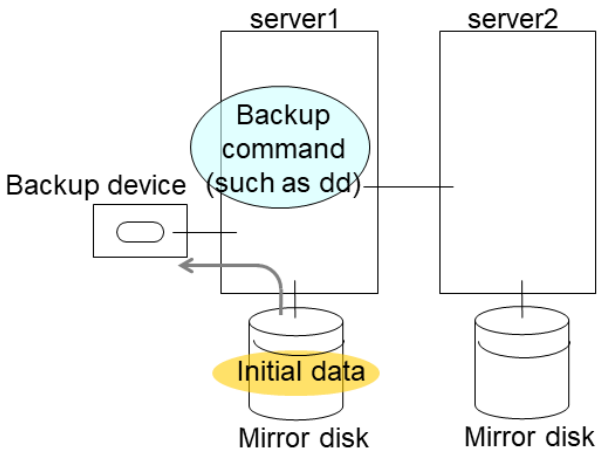


Example 2

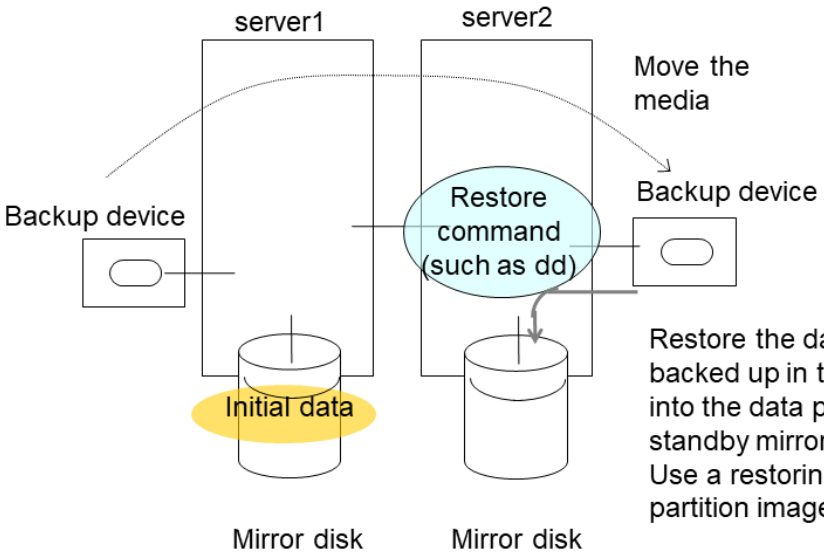
Copying by a backup device



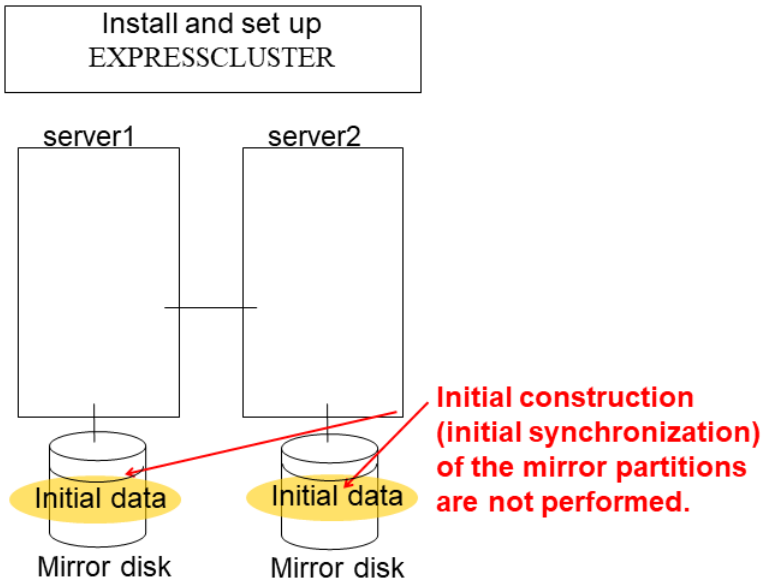
If it is possible prepare the application data which will be duplicated before cluster construction, it should be created in the data partition of the active mirror disk in advance. (ex. the initial DB of a database)



Use a backup device to make a backup of the mirror partition in the mirror disk of the active system.
Use a backup command in the partition image.



Restore the data which has been backed up in the active system into the data partition of the standby mirroring disk.
Use a restoring command in the partition image.



3.10.5 Notes on mirror disk resources

- If both servers cannot access the identical partitions under the identical device name, configure the server individual setting.
- If **Exclude Mount/Unmount Commands** is selected on the **Extension** tab in **Cluster Properties,** activation/deactivation of mirror resource may take time because mount/umount is performed exclusively to disk resource, VxVM volume resource, NAS resource, and mirror resource in the same server.
- When specifying path including symbolic link for mount point, Force Operation cannot be done even if it is chosen as operation in Detecting Failure.
  Similarly, if a path containing "//" is specified, forced termination will also fail.
- Disks using stripe set, volume set, mirroring, stripe set with parity by Linux md cannot be specified for the cluster partition and data partition.
- Volumes by Linux LVM can be specified for the cluster partition and data partition.
  For SuSE Linux, volumes by LVM or MultiPath cannot be used for the cluster partition or data partition.
- Mirror disk resources (mirror partition devices) cannot be the targets of stripe set, volume set, mirroring, stripe set with parity by Linux md or LVM.
- When the geometries of the disks used as mirror disks differ between the servers:

  The size of a partition allocated by the fdisk command is aligned by the number of blocks (units) per cylinder.

  Allocate data partitions to achieve the following data partition size and direction of the initial mirror construction.

  Source server <= Destination server

  "Source server" refers to the server with the higher failover policy in the failover group to which a mirror resource belongs.
  "Destination server" refers to the server with the lower failover policy in the failover group to which a mirror resource belongs.

If the data partition sizes differ significantly between the copy source and the copy destination, initial mirror construction may fail. Be careful, therefore, to secure data partitions of similar sizes.

Make sure that the data partition sizes do not cross over 32GiB, 64GiB, 96GiB, and so on (multiples of 32GiB) on the source server and the destination server. For sizes that cross over multiples of 32GiB, initial mirror construction may fail.

Examples)

Combination	Data partition size		Description
	On server 1	On server 2	
OK	30GiB	31GiB	OK because both are in the range of 0 to 32GiB.
OK	50GiB	60GiB	OK because both are in the range of 32GiB to 64GiB.
NG	30GiB	39GiB	Error because they are crossing over 32GiB.
NG	60GiB	70GiB	Error because they are crossing over 64GiB.

- Do not use the O_DIRECT flag of the open() system call for a file used in a mirror disk resource.
  Examples include the Oracle parameter filesystemio_options = setall.
- Do not specify a mirror partition device (such as /dev/NMP1) as the monitor target in the READ (O_DIRECT) disk monitoring mode.
- For the data partition and the cluster partition of mirror disk resources, use disk devices with the same logical sector size on all servers. If you use devices with different logical sector sizes, they do not operate normally. They can operate even if they have different sizes for the data partition and the cluster partition.

Examples)

Combination	Logical sector size of the partition				Description
	Server 1	Server 1	Server 2	Server 2	
	Data partition	Cluster partition	Data partition	Cluster partition	
OK	512B	512B	512B	512B	The logical sector sizes are uniform.
OK	4KB	512B	4KB	512B	The data partitions have a uniform size of 4 KB, and the cluster partitions have a uniform size of 512 bytes.
NG	4KB	512B	512B	512B	The logical sector sizes for the data partitions are not uniform.
NG	4KB	4KB	4KB	512B	The logical sector sizes for the cluster partitions are not uniform.

- Do not use HDDs and SSDs in combination for the disks used for the data partition and the cluster partition of mirror disk resources. If you used them in combination, optimum performance cannot be obtained. Even if disks with different disk types are used for the data partition and the cluster partition, they can operate.

  Examples)

Combination	Logical sector size of the partition				Description
	Server 1	Server 1	Server 2	Server 2	
	Data partition	Cluster partition	Data partition	Cluster partition	
OK	HDD	HDD	HDD	HDD	The disk types are uniform.
OK	SSD	HDD	SSD	HDD	The data partitions are of the uniform disk type of SSD, and the cluster partitions are of the uniform type of HDD.
NG	SSD	HDD	HDD	HDD	As the data partitions, both HDD and SSD are used.
NG	SSD	SSD	SSD	HDD	As the cluster partitions, both HDD and SSD are used.

- The bit64 format of an ext4 filesystem is not supported.

  To format ext4 manually on RHEL7, Asianux Server 7, and Ubuntu, add the option to disable bit64 to the mkfs command.

  For details, refer to " If using ext4 with a mirror disk resource or a hybrid disk resource" of "Notes and Restrictions" in the "Getting Started Guide".

3.10.6 mount processing flow

The mount processing needed to activate the mirror disk resource is performed as follows:

With **none** specified for the file system, the mount processing does not occur.

1. Is the device already mounted?

   When already mounted -> To X

2. Is fsck set to be run before mounting?

   Timing at which to run fsck -> Run fsck for the device.

3. Mount the device.

   Mounted successfully -> To O

4. Is mounting set to be retried?

   When retry is not set -> To X

5. When fsck(xfs_repair) is set to be run if mounting fails:

   When fsck has run successfully in 2. -> Go to **6.**

   When mounting fails due to a timeout in 3. -> Go to **6.**

   Other than the above -> Run fsck(xfs_repair) for the device.

6. Retry mounting of the device.

   Mounted successfully -> To O

7. Has the retry count for mounting been exceeded?

   Within the retry count -> Go to **6.**

   The retry count has been exceeded -> To X

O The resource is activated (mounted successfully).

X The resource activation has failed (not mounted).

3.10.7 umount processing flow

The umount processing to deactivate the mirror disk resource is performed as follows:

With **none** specified for the file system, the umount processing does not occur.

1. Is the device already unmounted?

   When already unmounted -> To X

2. Unmount the device.

   Unmounted successfully -> To O

3. Is unmount set to be retried?

   When retry is not set -> To X

4. Is the device still mounted? (Is the mount point removed from the mount list and is the mirror device in the unused status?)

   No longer mounted -> To O

5. Try KILL for the process using the mount point.

6. Retry unmount of the device.

   Unmounted successfully -> To O

7. Is the result other than the unmount timeout and is the mount point removed from the mount list?

   The mount point has already been removed.

   -> Wait until the mirror device is no longer used.

   (Wait no more than a length of time equal to the unmount timeout.)

8. Has the retry count for unmount been exceeded?

   Within the retry count -> Go to **4.**

   The retry count is exceeded -> To X

O The resource is stopped (unmounted successfully).

X The resource stop has failed (still mounted, or already unmounted).

3.10.8 Conditions under which the mirror status becomes abnormal

The following lists the most common situations in which the status of a mirror disk resource changes from normal (GREEN) to abnormal (RED).

- Due to the disconnection of communication (mirror disconnect), stoppage of the standby server, etc., mirror synchronization between the active and standby servers fails, leading to differences between the servers.
  The standby server does not retain the latest data, so enters the abnormal (RED) state.
- Settings are made so that mirror data is not synchronized, causing differences between the active and standby servers.
  The standby server does not retain the latest data, so enters the abnormal (RED) state.
- A mirror disk disconnection (mirroring interruption) operation is performed.
  The standby server enters the abnormal (RED) state.
- Mirror recovery is interrupted during mirror recovery (during mirror re-synchronization).
  The standby server has not completed copying, so enters the abnormal (RED) state.
- The active server does not execute cluster shutdown normally due to server down, etc.
  (The activated mirror disk resource stops without switching to the deactivated state.)
  The mirror disk of the server enters the abnormal (RED) state after the server starts.
- After a mirror disk is activated by starting only one server, the server is stopped without performing mirror synchronization, and then the other server is started and the mirror disk is activated.
  Because the mirror disks of the two servers are updated individually,
  those disks enter the abnormal (RED) state.
  If the mirror disks of the two servers are updated individually as described above, it is not possible to automatically judge the mirror disk of which server should act as the copy source, so automatic mirror recovery is not performed. In this case it is necessary to execute forced mirror recovery.
- Due to the disconnection of communication (mirror disconnect), reboot of the standby server, etc., mirror synchronization between the active and standby servers fails, causing differences between the servers and, later, the active server fails to execute cluster shutdown normally due to a server down, etc.
  In this case, if the server normally fails over to the standby server later, both servers enter the abnormal (RED) state after the servers start.
  In this case, automatic mirror recovery is not performed, either. Rather, it is necessary to execute forced mirror recovery.

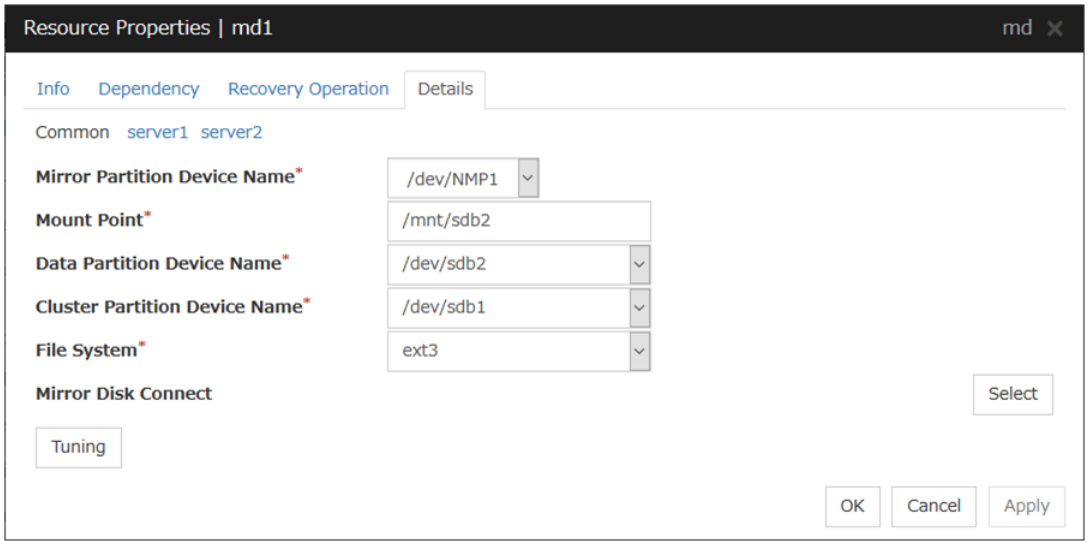
For details on how to refer to the status of a mirror, see the following:

- Online manual
- 8. *EXPRESSCLUSTER command reference*
  - *Displaying the mirror status (clpmdstat command)*
    - *Display examples*
      - Displaying the status of mirror disk resource

For details on how to perform the mirror recovery or forcible mirror recovery, see the following:

- 9. *Troubleshooting*
  - *Troubleshooting*
    - *Recovering from mirror breaks*
    - *Automatically recovering from mirroring*
    - *Checking the mirror break status with a command*
    - *Recovering mirror with a command*
    - *Running the forcible mirror recovery with a command*
    - *Running the forcible mirror recovery with a command only on one server*
    - *Checking the mirror break status from the Cluster WebUI*
    - *Recovering mirror using the Cluster WebUI*
    - *Running the forcible mirror recovery using the Cluster WebUI*
    - *Running the forcible mirror recovery from the Cluster WebUI only on one Server*

3.10.9 Details tab



Mirror Partition Device Name

Select a mirror partition device name to be associated with the mirror partition.

Device names of mirror disk resource/hybrid disk resource that have already been configured are not displayed on the list.

Mount Point (Within 1023 bytes) `Server Individual Setup`

Specify a directory to mount the mirror partition device. The name should begin with "/."

Data Partition Device Name (Within **1023 bytes**) `Server Individual Setup`

Specify a data partition device name to be used for a disk resource.

The name should begin with "/."

Cluster Partition Device Name (Within **1023 bytes**) `Server Individual Setup`

Specify a cluster partition device name to be paired with the data partition.

The name should begin with "/."

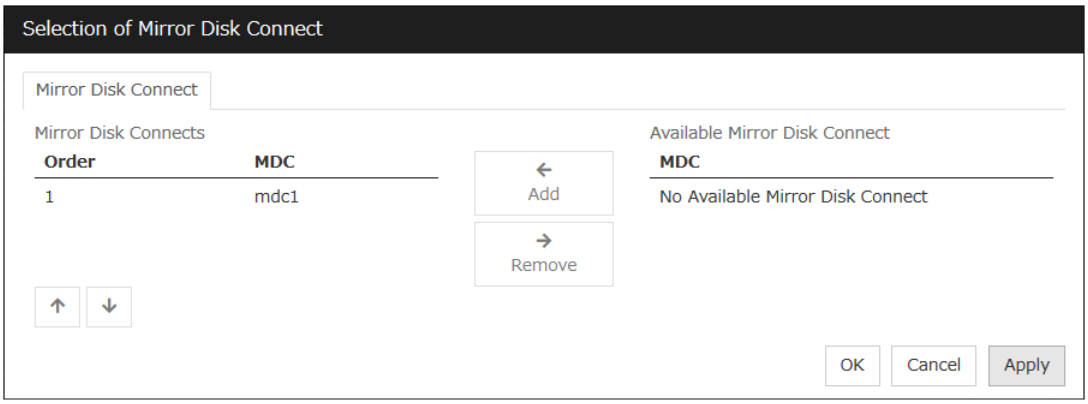
File System

You select a file system type to be used on the mirror partition. Choose one from the list box. You may also directly enter the type.

- ext2
- ext3
- ext4
- xfs
- jfs
- reiserfs
- none (no file system)

Mirror Disk Connect

Add, delete or modify mirror disk connects. In the **Mirror Disk Connects** list, I/F numbers of the mirror disk connects used for mirror disk resources are displayed.



In **Available Mirror Disk Connect**, mirror disk connect I/F numbers that are currently not used are displayed.

- Set mirror disk connects on the Cluster Properties.
- Maximum of two mirror disk connects can be used per mirror disk resource. For the behavior when two mirror disk connects are used, see "*Mirror disk*".
- For details on how to configure mirror disk connects, see the "Installation and Configuration Guide".

Add

Use **Add** to add a mirror disk connect. Select the I/F number you want to add from **Available Mirror Disk Connect** and then click **Add**. The selected number is added to the **Mirror Disk Connects** list.

Remove

Use Remove to remove mirror disk connects to be used. Select the I/F number you want to remove from the **Mirror Disk Connect list** and then click **Remove**. The selected number is added to **Available Mirror Disk Connect**.

Order

Use the arrows to change the priority of mirror disk connects to be used. Select the I/F number you want to change from the **Mirror Disk Connect list** and then click the arrows.

Tuning

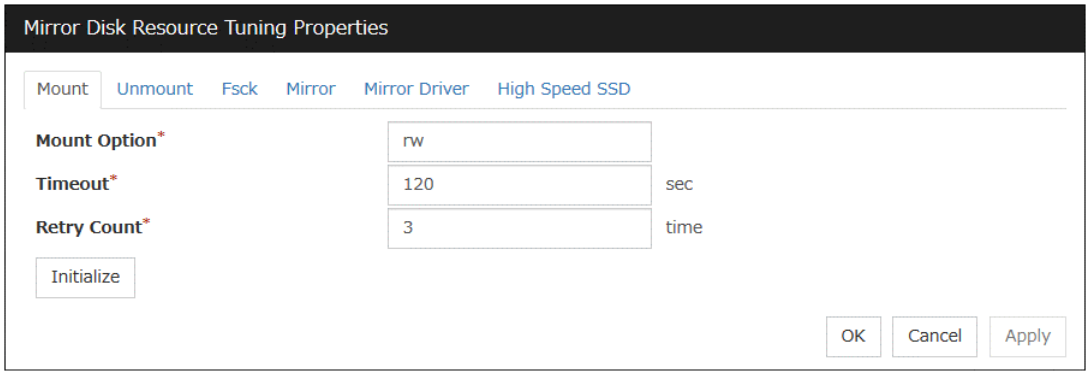
Opens the **Mirror Disk Resource Tuning Properties** dialog box. You make detailed settings for the mirror disk resource there.

Mirror disk resource tuning properties

Mount tab

The advanced settings of mount are displayed.

This does not appear with **none** selected from **File System** under the **Details** tab of the **Resource Properties** dialog box.



Mount Option (Within **1023 bytes**)

Enter options to give the mount command when mounting the file system on the mirror partition device. Use a comma "," to separate multiple options.

Mount option example

Setting item	Setting value
Mirror partition device name	/dev/NMP5
Mirror mount point	/mnt/sdb5
File system	ext3
Mount option	rw,data=journal

The mount command to be run with the above settings is:

```
mount -t ext3 -o rw,data=journal /dev/NMP5 /mnt/sdb5
```

Timeout (1 to 999)

Enter how many seconds you want to wait for the mount command completion before its timeout when you mount the file system on the mirror partition device. Be careful about the value you specify. That is because it may take some time for the command to complete if the capacity of the file system is large.

Retry Count (0 to 999)

Enter how many times you want to retry to mount the file system on the mirror partition device when one fails. If you set this to zero (0), mount will not be retried.

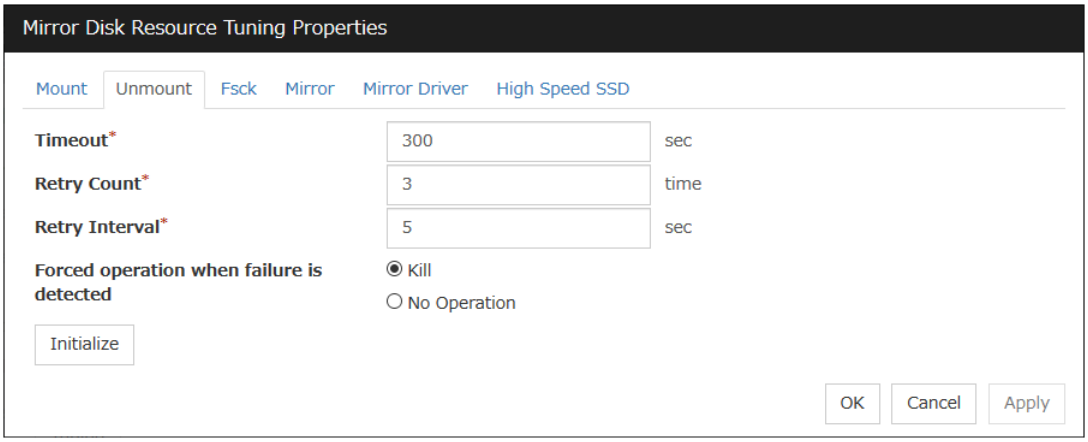
Initialize

Clicking **Initialize** resets the values of all items to the default values.

Unmount tab

The advanced settings for unmounting are displayed.

This does not appear with **none** selected from **File System** under the **Details** tab of the **Resource Properties** dialog box.



Timeout (1 to 999)

Enter how many seconds you want to wait for the unmount command completion before its timeout when you unmount the file system on the mirror partition device.

Retry Count (0 to 999)

Enter how many times you want to retry to unmount the file system on the mirror partition device when one fails. If you set this to zero (0), unmount will not be retried.

Retry Interval (0 to 999)

Enter the interval in which you want to retry unmounting the file system from the mirror partition device when unmounting fails.

Forced operation when failure is detected

Select an action to be taken at an unmount retry if unmount fails.

- kill:
  Select this option to try to forcibly terminate the processes that are accessing the mount point. Not all processes can be terminated.
- No Operation:
  Select this option not to try killing the processes that are accessing the mount point.

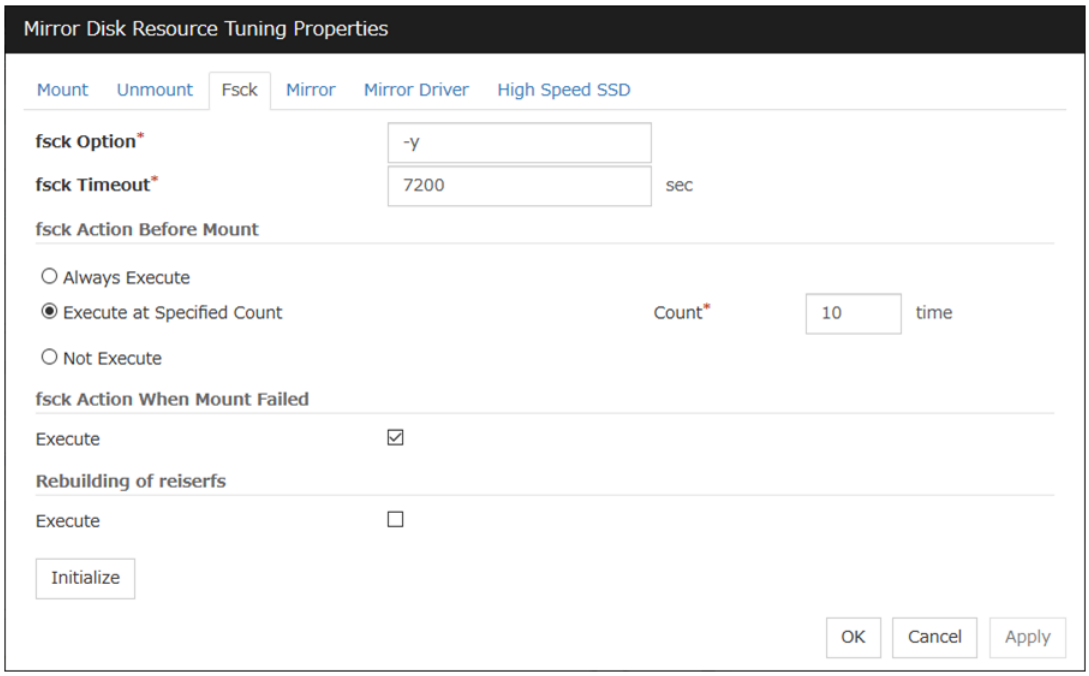
Initialize

Clicking **Initialize** resets the values of all items to the default values.

Fsck tab

The advanced settings of fsck are displayed.

This does not appear with **xfs** or **none** selected from **File System** under the **Details** tab of the **Resource Properties** dialog box.



fsck Option (Within 1023 bytes)

Enter options to give the fsck command when checking the file system on the mirror partition device. Use a space to separate multiple options. Specify options so that the fsck command does not run interactively. Otherwise, activation of resources after the time specified to **fsck Timeout** elapses becomes an error.

fsck Timeout (1 to 9999)

Enter how many seconds you want to wait for the fsck command completion before its timeout when you check the file system on the mirror partition device. Be careful about the value you specify. This is because it may take some time for the command to complete if the capacity of the file system is large.

fsck Action Before Mount

Select an fsck action before mounting file system on a disk device from the following choices:

- Always Execute:
  fsck is executed before mounting the file system.
- Execute at Specified Count:
  fsck is executed when resource is activated successfully within the count specified by Count.
  = Count (0~999)
- Not Execute:
  fsck is not executed before mounting the file system.

Note: The specified count for fsck is not related to the check interval managed by a file system.

fsck Action When Mount Failed

Set an fsck action to take when detecting a mount failure on a disk device.
This setting is enabled when the setting of Mount **Retry Count** is other than zero.

- When the check box is selected:
  Mount is retried after running fsck.

- When the check box is not selected:
  Mount is retried without running fsck.

Note: It is not recommended to set "Not Execute" fsck action before performing mount. With this setting, disk resource does not execute fsck and disk resource cannot be failed over when there is an error that can be recovered by fsck in the switchable partition.

Rebuilding of reiserfs

Specify the action when reiserfsck fails with a recoverable error.

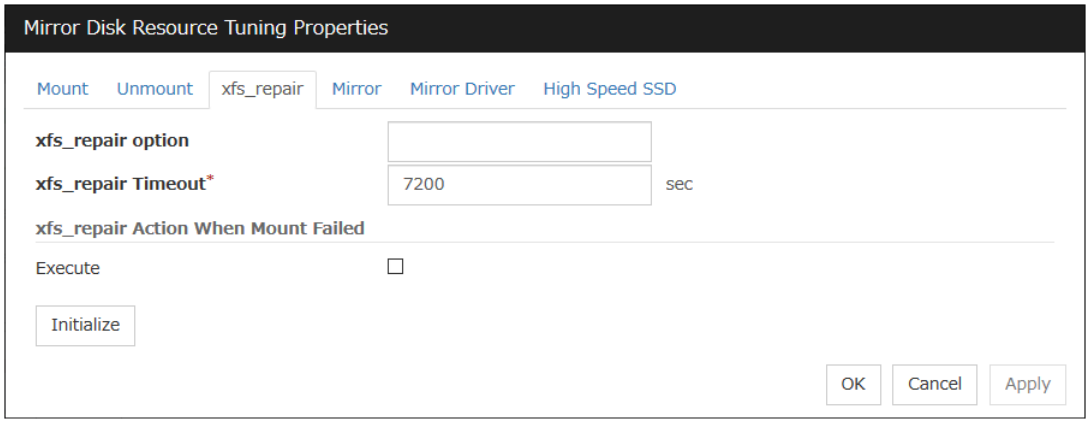
- When the checkbox is selected
  reiserfsck --fix-fixable is executed.
- When the checkbox is not selected
  Recovery is not performed even if reiserfsck fails with a recoverable error.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

xfs_repair tab

The detailed settings related to [xfs_repair] are displayed. The tab appears only if [xfs] is set for the file system.



xfs_repair Option (Within 1023 bytes)

Enter the option to give to the [xfs_repair] command when checking the file system on the disk device. To enter multiple options, delimit each with a space.

xfs_repair Timeout (1 to 999)

Enter how many seconds you want to wait for the [xfs_repair] command completion before its timeout when you check the file system on the disk device. If the file system has a large size of disk space, it may take some time for the command to complete. Make sure that the value to set is not too small.

xfs_repair Action When Mount Failed

Set the [xfs_repair] action when mounting the file system on the disk device fails. This setting is enabled when the setting of **Mount Retry Count** is other than zero.

- When the check box is selected:
  Mount is retried after running [xfs_repair].
- When the check box is not selected:

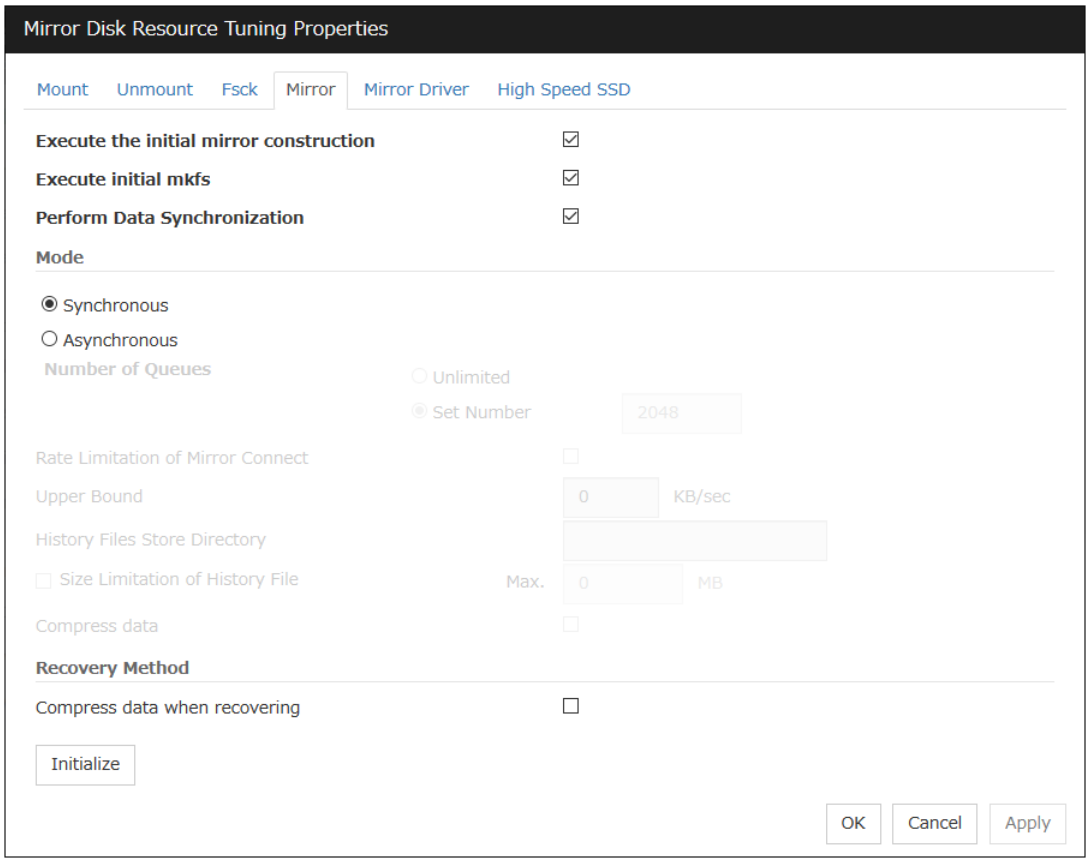
Mount is retried without running [xfs_repair].

Initialize

Clicking **Initialize** resets the values of all items to the default values.

Mirror tab

The advanced settings of mirror disks are displayed.



Execute the initial mirror construction

Specify if an initial mirror configuration is constructed when constructing a cluster.

- When the check box is selected:
  An initial mirror configuration will be constructed.

The time that takes to construct the initial mirror is different from ext2/ext3/ext4 and other file systems.

- When the check box is not selected:
  An initial mirror configuration will not be constructed.

Execute initial mkfs

Specify if an initial mkfs is constructed when constructing a cluster. This option can be set only if the initial mirror is being constructed.

In the case of hybrid disk resources, the clphdinit command behavior is executed instead of initial mkfs behavior upon cluster construction

- When the check box is selected:
  An initial mkfs will be run.

- When the check box is not selected:
  An initial mkfs will not be run.

Perform Data Synchronization

Specify if the mirror data synchronization is executed when mirror disk resource is activated.

- When the check box is selected:
  Mirror data synchronization is executed. The write data is passed from the active server to the standby server. The clpmdctr command and clphdctrl command can be used not to synchronize mirror data.
- When the check box is not selected:
  Mirror data synchronization will not be executed. The write data will not be passed
  from the active server to the standby server and will be accumulated as the finite difference. You can use the clpmdctrl command and clphdctrl command to switch to the status where mirror data is synchronized.

Mode

Specify synchronous mode of mirror data.

- **Synchronous**
  Select when LAN is mainly used for mirror connect.
- **Asynchronous**
  Select when WAN is mainly used for mirror connect. Specify Number of Queues when Asynchronous is chosen. Specify it for each mirror disk resource.
  - Unlimited:
    Queues will be allocated as long as possible to allocate memory. When it failed to allocate memory, mirror breaks.
  - Set Number (1 to 999999):
    Specify maximum number of queues to be allocated. When synchronous data exceeds it, the excess is recorded as a history file.

  When **Asynchronous** is selected, the **Rate limitation of Mirror Connect** check box can be selected.

  - When the check box is selected (1 to 999999)
    The upper rate limitation of mirror connect is set.
  - When the check box is cleared
    The upper rate limitation of mirror connect is not set.

  With **Asynchronous** selected, you can edit the setting in the **History File Store Directory** text box to specify the directory of a file in which, if the maximum number of queues is exceeded, the excess is recorded. Without specifying the directory here, the file is generated under the following directory: (EXPRESSCLUSTER-installed directory)/work.

  With **Asynchronous** selected, you can edit the setting in the **Size Limitation of History File** text box. When the accumulation in the history file reaches the size specified here, a mirror break occurs. Specifying the value as 0 or nothing makes the size unlimited.

  When **Asynchronous** is selected, the **Compress data** check box can be selected.

  - When the check box is selected
    Mirror synchronous communication data is compressed.
  - When the check box is cleared
    Mirror synchronous communication data is not compressed.

Compress data when recovering

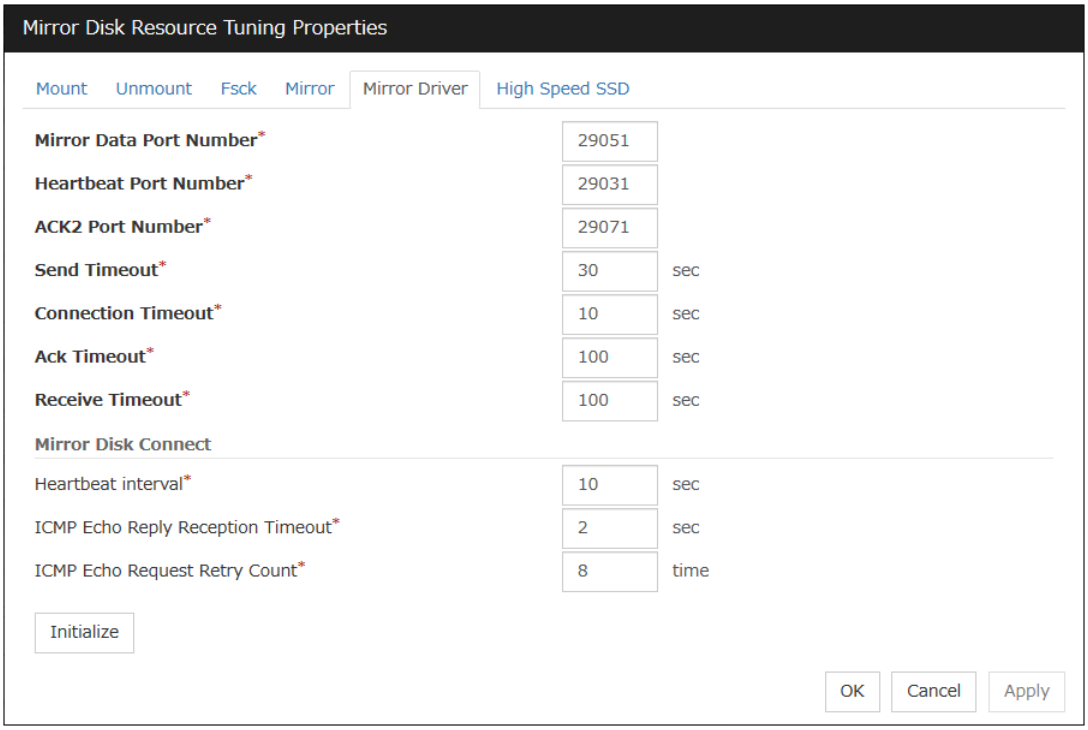
Specify whether to compress mirror recovery communication data.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

Mirror Driver tab

Advanced settings for a mirror driver is displayed.



Mirror Data Port Number (1 to 65535[6])

Set the TCP port number used for sending and receiving disk data between servers. The default value 29051 is set to the mirror disk resource or the hybrid disk resource created first. From a second mirror disk resource or the hybrid disk resource, the value increased by one from default (29052,29053,...) is set accordingly.

Heartbeat Port Number (1 to 65535[7])

Set the port number that a mirror driver uses to communicate control data between servers. The default value 29031 is set to the mirror disk resource or the hybrid disk resource created first. From a second mirror disk resource or the hybrid disk resource, the value increased by one from default (29032, 29033,...) is set accordingly.

ACK2 Port Number (1 to 65535[8])

Set the port number that a mirror driver uses to communicate control data between servers. The default value 29071 is set to the mirror disk resource or the hybrid disk resource created first. From a second mirror disk resource or the hybrid disk resource, the value increased by one from default (29072, 29073,...) is set accordingly.

[6] It is not recommended to use well-known ports, especially reserved ports from 1 to 1023.
[7] It is not recommended to use well-known ports, especially reserved ports from 1 to 1023.
[8] It is not recommended to use well-known ports, especially reserved ports from 1 to 1023.

Send Timeout (10 to 99)

Set the delivery time-out for write data.

Connection Timeout (5 to 99)

Set the time-out for connection.

Ack Timeout (1 to 600)

Set the time-out which waits for Ack response when mirror recovers and data is synchronized.

Receive Timeout (1 to 600)

Set the receive time-out for write confirmation.

Heartbeat interval (1 to 600)

Set the heartbeat interval between mirror disk connects by the mirror driver.

ICMP Echo Reply Reception Timeout (1 to 100)

Set the heartbeat timeout between mirror disk connects by the mirror driver. If no-response is returned for the ICMP Echo Request retry count during the time set here, a mirror disk connect disconnection is assumed.

ICMP Echo Request Retry Count (1 to 50)

Set the heartbeat retry count between mirror disk connects by the mirror driver. This value is related to the mirror connect disconnection judgment sensitivity as well as the ICMP Echo Reply receive timeout.

Initialize

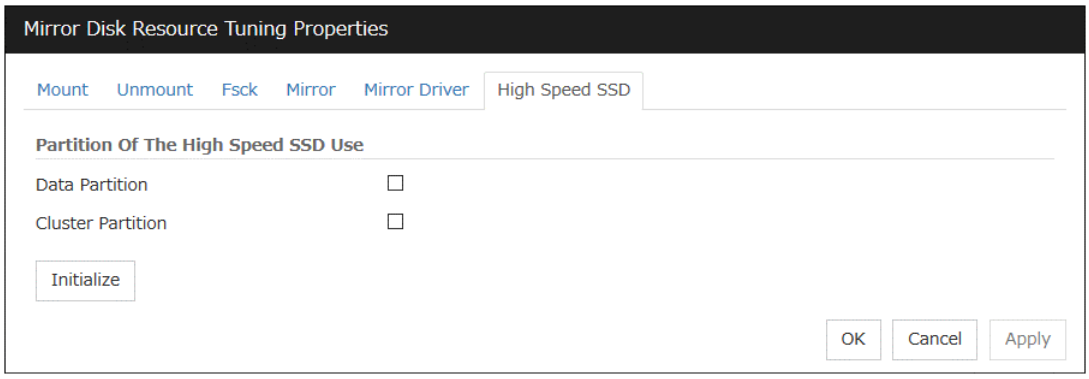
Clicking **Initialize** resets the following values to the default values.

- Send Timeout
- Connection Timeout
- Ack Timeout
- Receive Timeout
- Heartbeat Interval
- ICMP Echo Reply Receive Timeout
- ICMP Echo Request Retry Count

Note: For **Mirror Data Port Number**, **Heartbeat Port Number** and **ACK2 Port Number**, different port numbers should be configured for each resource. Also, those should not be the same as other port numbers used on a cluster. Thus, the initial values are not set even when you click **Initialize**.

High Speed SSD tab

The detailed settings for the high-speed SSD specifications in mirror disk resources are displayed.



Data Partition

Select the check box when you use a high-speed SSD for the data partition of mirror disk resources. Make sure that the disk devices used for the data partitions on all nodes are either HDDs or SSDs. If they are used in combination, optimum performance cannot be exerted.

Cluster Partition

Select the check box when you use a high-speed SSD for the cluster partition of mirror disk resources. Make sure that the disk devices used for the cluster partitions on all nodes are either HDDs or SSDs. If they are used in combination, optimum performance cannot be exerted.

3.11 Understanding Hybrid disk resources

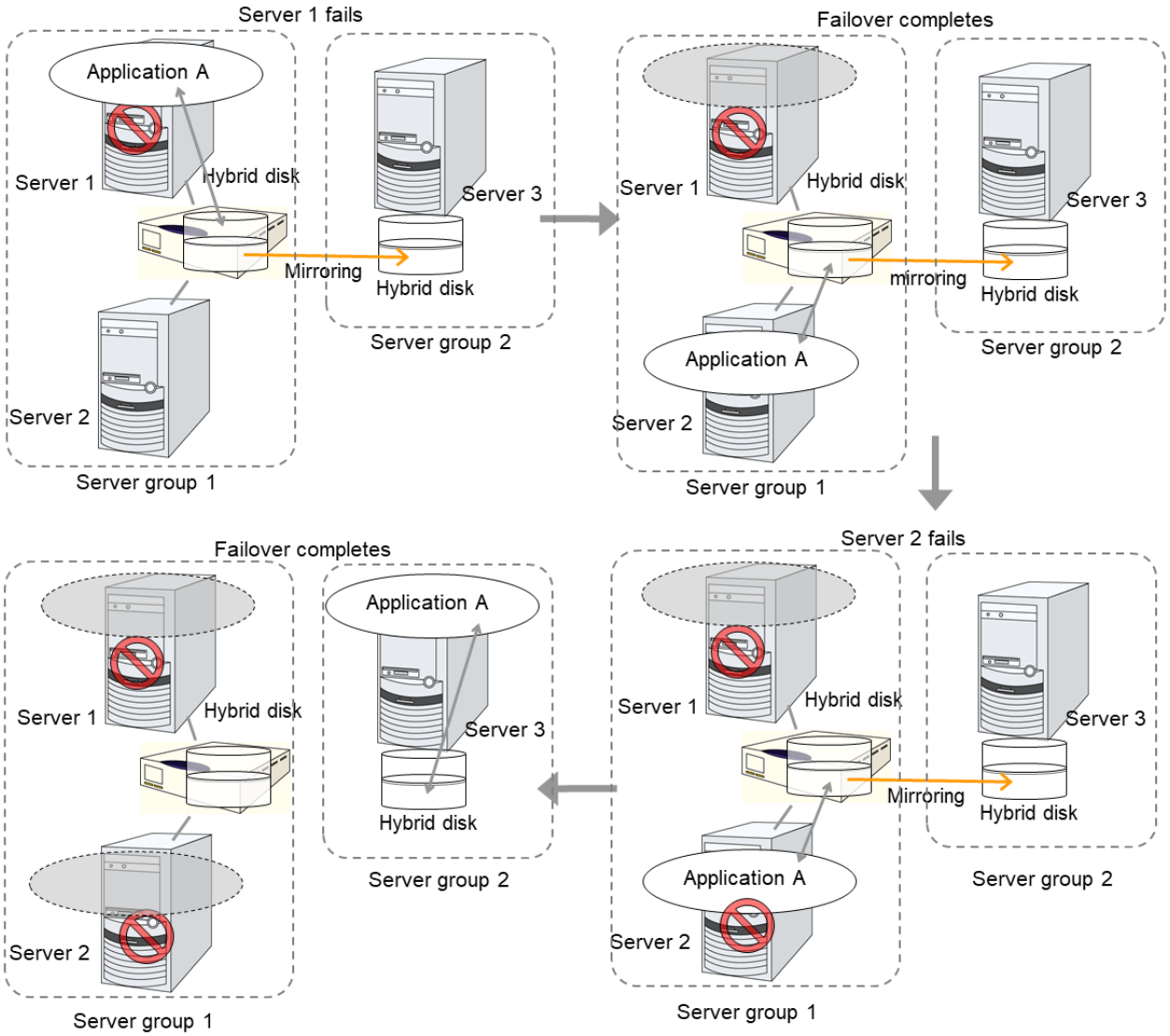
3.11.1 Dependencies of Hybrid disk resource

By default, this function depends on the following group resource types.

Group resource type
Floating IP resource
Virtual IP resource
AWS Elastic IP resource
AWS Virtual IP resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.11.2 What is hybrid disk?

A hybrid disk is a resource which performs data mirroring between two server groups. A server group consists of 1 server or 2 servers. When a server group consists of 2 servers, a shared disk is used. When a server group consists of 1 server, a disk which is not shared type (e.g. a built-in disk, an external disk chassis which is not shared between servers) is used.



Data partition

Partitions where data to be mirrored (such as application data) is stored are referred to as data partitions.

Allocate data partitions as follows:

- Data partition size
  The size of data partition should be 1GB or larger but smaller than 1TB.
  (Less than 1TB size is recommended from the viewpoint of the construction time and the restoration time of data.)
- Partition ID
  83(Linux)
- Please make the file system on data partitions if you need. Automatic initial mkfs is not executed.
- EXPRESSCLUSTER is responsible for the access control (mount/umount) of file system. Do not configure the settings that allow the OS to mount or unmount a data partition.

Cluster partition

Dedicated partitions used in EXPRESSCLUSTER for controlling hybrid disk are referred to as cluster partition.

Allocate cluster partitions as follows:

- Cluster partition size
  1024MB or more. Depending on the geometry, the size may be larger than 1024MB but that is not a problem.
- Partition ID
  83(Linux)
- A cluster partition and data partition for data mirroring should be allocated in a pair.
- Do not make the file system on cluster partitions.

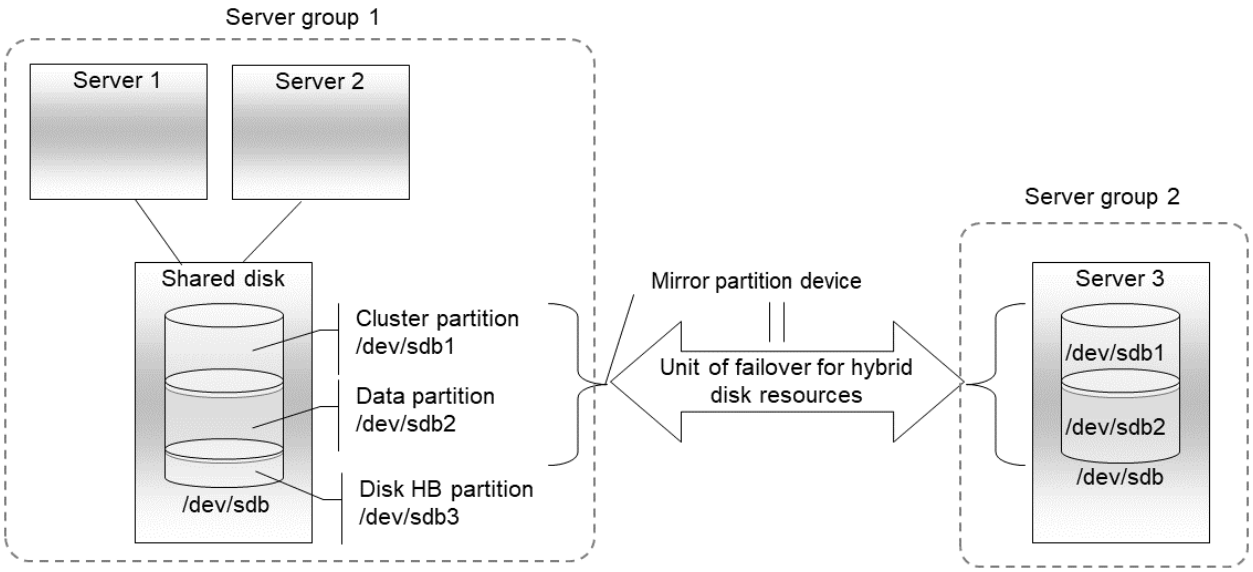
Mirror Partition Device (/dev/NMPx)

One hybrid disk resource provides the file system of the OS with one mirror partition. If a hybrid disk resource is registered with the failover group, it can be accessed only from one server (it is generally the primary server of the resource group).

Typically, the mirror partition device (dev/NMPx) remains transparent to users (AP) because I/O is performed via a file system. When the information is created by the Cluster WebUI, device names should be assigned without overlapping with each other.

- EXPRESSCLUSTER is responsible for the access control (mount/umount) of file system. Do not configure the settings that allow the OS to mount or unmount a data partition.
  Mirror partition's (hybrid disk resource's) accessibility to applications is the same as switching partition (disk resources) that uses shared disks.
- Mirror partition switching is performed on a failover group basis according to the failover policy.
- /dev/NMPx(x is a number between 1 and 8) is used for the special device name of mirror partition. Do not use /dev/NMPx in other device drivers.
- The major number 218 is used for mirror partition. Do not use the major number 218 in other device drivers.

Example 1) When two servers use the shared disk and the third server uses the built-in disk



- When a non-shared disk is used (i.e. when there is one server in the server group), it is possible to secure a partition for the hybrid disk resource (cluster partition and data partition) on the same disk where the OS (root partition and swap partition) is located.
  - When maintainability at a failure is important:

It is recommended to allocate a disk for mirror which is not used by the OS (such as root partition, swap partition).

– If LUN cannot be added due to H/W RAID specifications:
If you are using hardware/RAID preinstall model where the LUN configuration cannot be changed, you can allocate a mirror partition (cluster partition, data partition) in the disk where the OS (root partition, swap partition) is located.

Mirror disk connect

See "Mirror disk connect" for the "*Mirror disk*"

3.11.3 Mirror parameter settings

The following parameters are the same as those of mirror disk resources. See "mirror disk resources".

- Mirror data port number
- Heartbeat port number
- ACK2 port number
- The maximum number of request queues
- Connection timeout
- Send timeout
- Receiving timeout
- Ack timeout
- Difference bitmap update interval (cluster properties)
- Difference Bitmap size (cluster properties)
- Mirror agent send timeout (cluster properties)
- Mirror agent receiving timeout (cluster properties)
- Recovery data size (cluster properties)
- Initial mirror construction
- Number of Queues
- Mode of Communication Band
- History File Store Directory
- Size Limitation of History File
- Heartbeat Interval
- ICMP Echo Reply Receive Timeout
- ICMP Echo Request Retry Count

The following parameter is different from mirror disk resource.

- Initial mkfs
Automatic initial mkfs is not executed. Please execute mkfs manually.

3.11.4 Notes on hybrid disk resources

- If device names for the cluster partitions or the data partitions differ between servers, set up each server separately. In addition, if the device names differ between servers belonging to the same server group, set by-id to the device name.
- If **Exclude Mount/Unmount Commands** is selected on the **Extension** tab in **Cluster Properties,** activation/deactivation of hybrid disk resource may take time because mount/umount is performed exclusively to disk resource, VxVM volume resource, NAS resource, mirror resource and hybrid disk resource in the same server.
- When specifying path including symbolic link for mount point, Force Operation cannot be done even if it is chosen as operation in failure detection.
  Similarly, if a path containing "//" is specified, forced termination will also fail.
- Disks using stripe set, volume set, mirroring, stripe set with parity by Linux md cannot be specified for the cluster partition and data partition.
- Hybrid disk resources (mirror partition devices) cannot be the targets of stripe set, volume set, mirroring, stripe set with parity by Linux md or LVM.
- When the geometries of the disks used as hybrid disks differ between the servers:
  The size of a partition allocated by the fdisk command is aligned by the number of blocks (units) per cylinder. Allocate data partitions to achieve the following data partition size and direction of the initial mirror construction.

  Source server <= Destination server

  "Source server" refers to the server with the higher failover policy in the failover group to which a hybrid disk resource belongs.
  "Destination server" refers to the server with the lower failover policy in the failover group to which a hybrid disk resource belongs.

  If the data partition sizes differ significantly between the copy source and the copy destination, initial mirror construction may fail. Be careful, therefore, to secure data partitions of similar sizes.
  Make sure that the data partition sizes do not cross over 32GiB, 64GiB, 96GiB, and so on (multiples of 32GiB) on the source server and the destination server. For sizes that cross over multiples of 32GiB, initial mirror construction may fail.

Examples)

Combination	Data partition size		Description
	On server 1	On server 2	
OK	30GiB	31GiB	OK because both are in the range of 0 to 32GiB.
OK	50GiB	60GiB	OK because both are in the range of 32GiB to 64GiB.
NG	30GiB	39GiB	Error because they are crossing over 32GiB.
NG	60GiB	70GiB	Error because they are crossing over 64GiB.

- Do not use the O_DIRECT flag of the open() system call for a file used in a hybrid disk resource.
  Examples include the Oracle parameter filesystemio_options = setall.
- Do not specify a mirror partition device (such as /dev/NMP1) as the monitor target in the READ (O_DIRECT) disk monitoring mode.

- For a cluster configuration that uses a hybrid disk, do not set the final action of a monitor resource, etc., to **Stop the cluster service**.
- For the data partition and the cluster partition of hybrid disk resources, use disk devices with the same logical sector size on all servers. If you use devices with different logical sector sizes, they do not operate normally. They can operate even if they have different sizes for the data partition and the cluster partition.

Examples)

Combination	Logical sector size of the partition				Description
	Server 1	Server 1	Server 2	Server 2	
	Data partition	Cluster partition	Data partition	Cluster partition	
OK	512B	512B	512B	512B	The logical sector sizes are uniform.
OK	4KB	512B	4KB	512B	The data partitions have a uniform size of 4 KB, and the cluster partitions have a uniform size of 512 bytes.
NG	4KB	512B	512B	512B	The logical sector sizes for the data partitions are not uniform.
NG	4KB	4KB	4KB	512B	The logical sector sizes for the cluster partitions are not uniform.

- Do not use HDDs and SSDs in combination for the disks used for the data partition and the cluster partition of hybrid disk resources. If you used them in combination, optimum performance cannot be obtained. Even if disks with different disk types are used for the data partition and the cluster partition, they can operate.

Examples)

Combination	Logical sector size of the partition				Description
	Server 1	Server 1	Server 2	Server 2	
	Data partition	Cluster partition	Data partition	Cluster partition	
OK	HDD	HDD	HDD	HDD	The disk types are uniform.
OK	SSD	HDD	SSD	HDD	The data partitions are of the uniform disk type of SSD, and the cluster partitions are of the uniform type of HDD.
NG	SSD	HDD	HDD	HDD	As the data partitions, both HDD and SSD are used.
NG	SSD	SSD	SSD	HDD	As the cluster partitions, both HDD and SSD are used.

- The bit64 format of an ext4 filesystem is not supported.

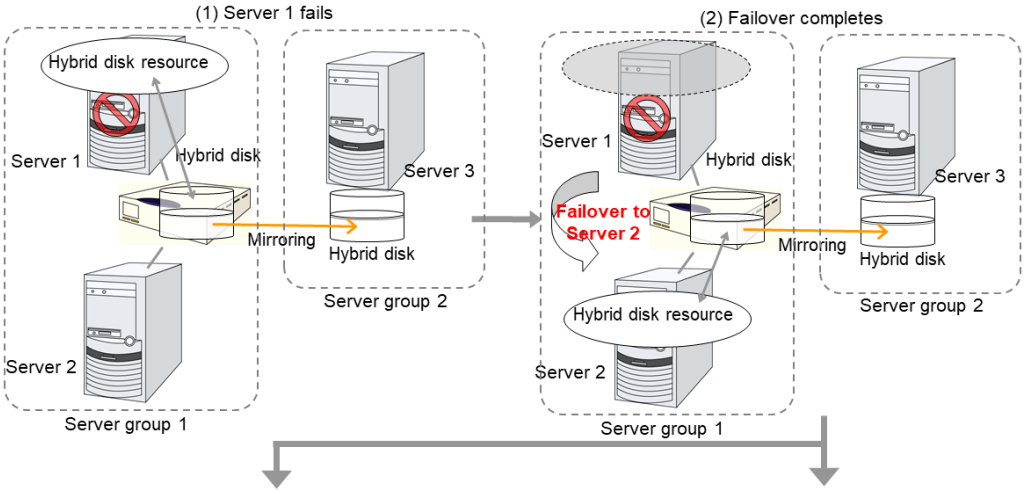
  To format ext4 manually on RHEL7, Asianux Server 7, and Ubuntu, add the option to disable bit64 to the mkfs command.

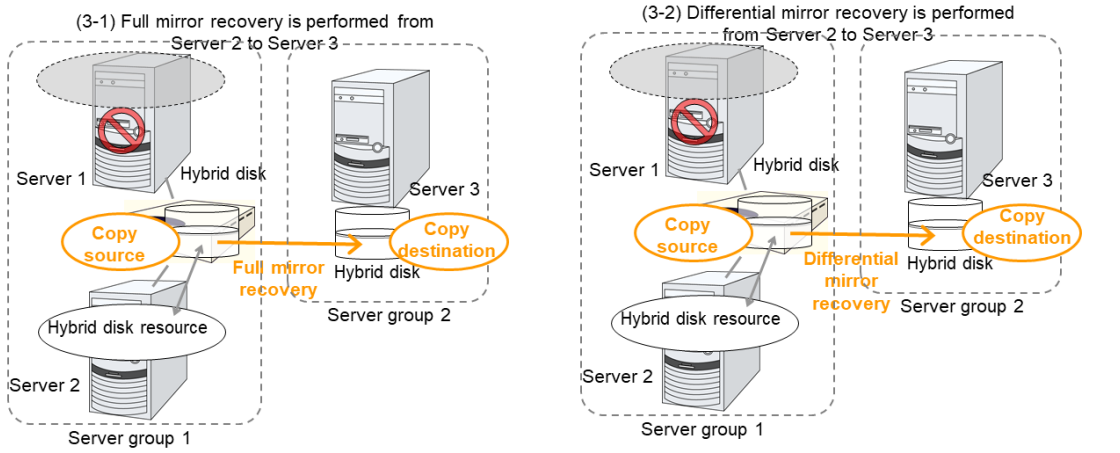
  For details, refer to "If using ext4 with a mirror disk resource or a hybrid disk resource" in "Notes and Restrictions" in the "Getting Started Guide".

- Behavior of mirror recovery after the active server goes down abnormally

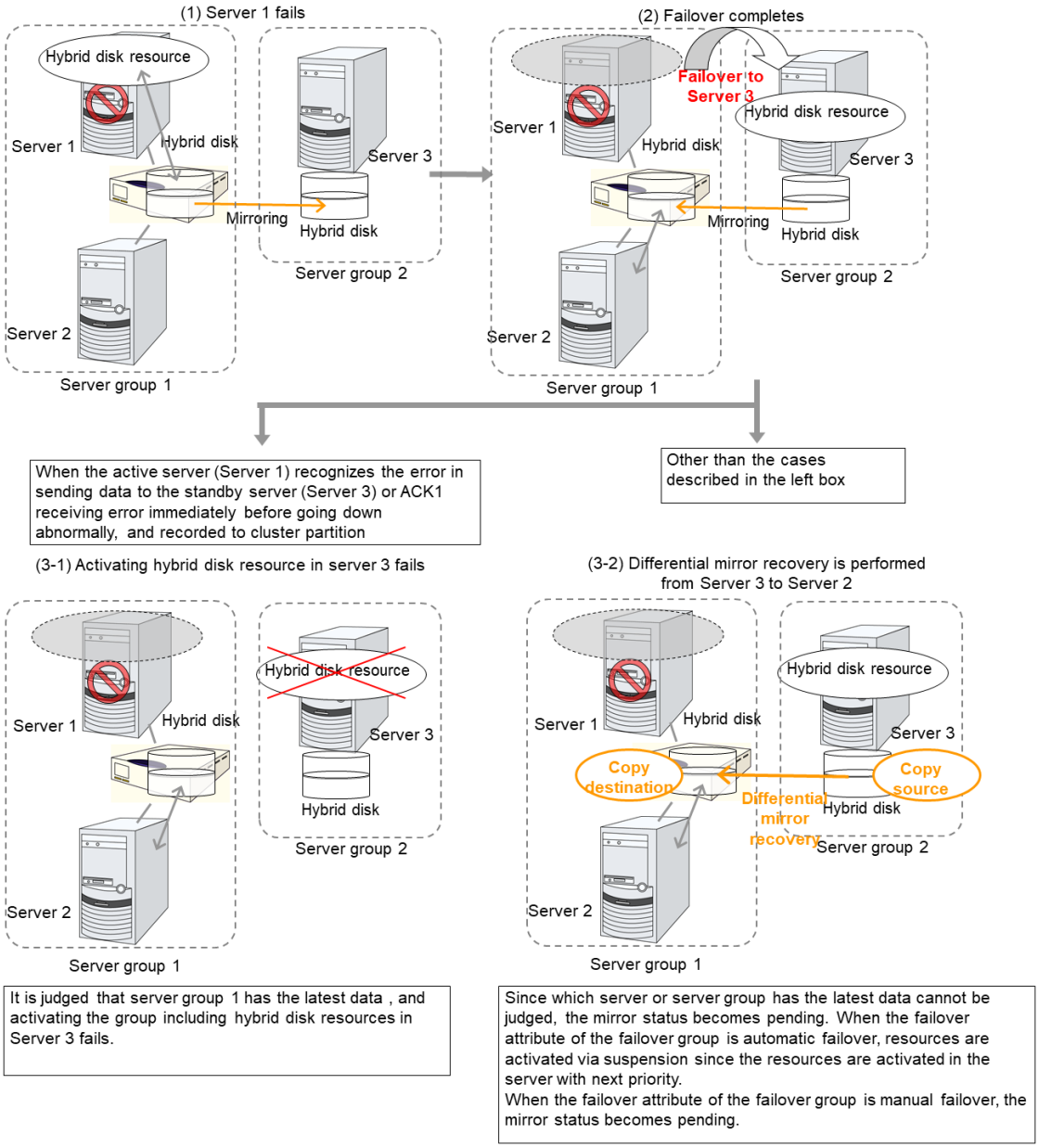
  When the active server goes down abnormally, depending on the timing of the server failure, full mirror recovery or differential mirror recovery is performed.

- When a resource is activated by a server connected via a shared disk (a server in the same server group)





- When a resource is activated by a server in the remote server group



3.11.5 mount processing flow

The mount processing needed to activate the hybrid disk resource is performed as follows:

With **none** specified for the file system, the mount processing does not occur.

1. Is the device already mounted?

   When already mounted -> To X

2. Is fsck set to be run before mounting?

   Timing at which to run fsck -> Run fsck for the device.

3. Mount the device.

Mounted successfully -> To O

4. Is mounting set to be retried?

   When retry is not set -> To X

5. When fsck(xfs_repair) is set to be run if mounting fails:

   When fsck is executed in **2.** and mount is successful -> Go to **6.**

   When mount fails in **3.** due to a timeout -> Go to **6.**

   Other than the above -> Execute fsck(xfs_repair) for the device.

6. Retry mounting of the device.

   Mounted successfully -> To O

7. Has the retry count for mounting been exceeded?

   Within the retry count -> Go to **6.**

   The retry count has been exceeded -> To X

O The resource is activated (mounted successfully).

X The resource activation has failed (not mounted).

3.11.6 umount processing flow

The umount processing to deactivate the hybrid disk resource is performed as follows:

With none specified for the file system, the umount processing does not occur.

1. Is the device already unmounted?

   When already unmounted -> To X

2. Unmount the device.

   Unmounted successfully -> To O

3. Is unmount set to be retried?

   When retry is not set -> To X

4. Is the device still mounted? (Is the mount point removed from the mount list and is the mirror device in the unused status?)

   No longer mounted -> To O

5. Try KILL for the process using the mount point.

6. Retry unmount of the device.

   Unmounted successfully -> To O

7. Is the result other than the unmount timeout and is the mount point removed from the mount list?

   The mount point has already been removed.

   -> Wait until the mirror device is no longer used.

   (Wait no more than a length of time equal to the unmount timeout.)

8. Has the retry count for unmount been exceeded?

   Within the retry count -> Go to **4.**

   The retry count is exceeded -> To X

O The resource is stopped (unmounted successfully).

X The resource stop has failed (still mounted, or already unmounted).

3.11.7 Details tab

The followings are the same as those of mirror disk resources. Refer to "mirror disk resource".

- Hybrid disk detail tab (See mirror disk detail tab)
- Mirror disk connect selection
- Hybrid disk adjustment properties (See mirror disk adjustment properties)
  - Mount tab
  - Unmount tab
  - Fsck tab
  - xfs_repair tab
  - Mirror tab (parameter other than the one for executing the initial mkfs)
  - Mirror drive tab
  - High-speed SSD tab

The following tab is different from that of mirror disk resource:

- Mirror tab of hybrid disk adjustment properties [execute initial mkfs]

Execute initial mkfs

The hybrid disk resource in this version, automatic initial mkfs is not executed.

3.12 Understanding NAS resource

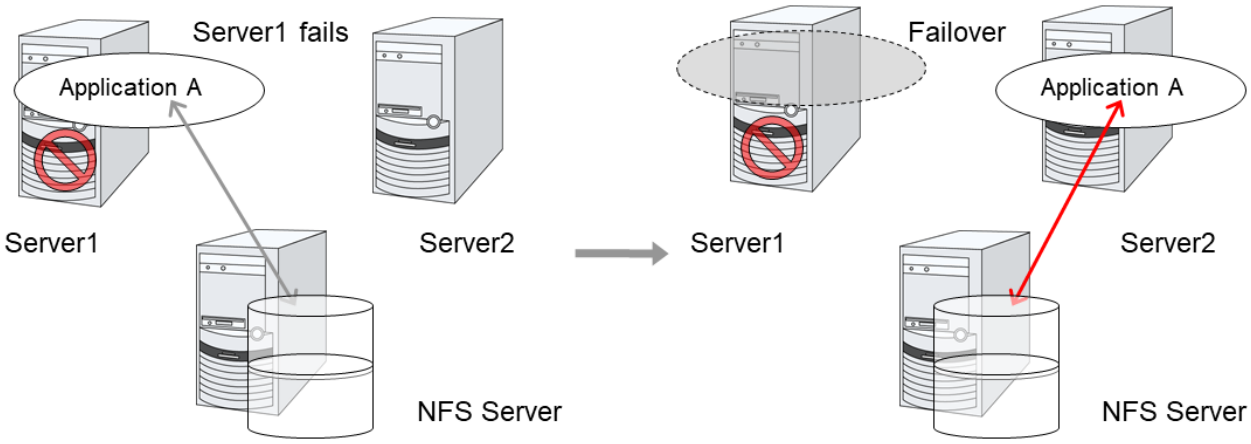
3.12.1 Dependencies of the NAS resource

By default, this function depends on the following group resource type:

Group resource type
Dynamic DNS resource
Floating IP resource
Virtual IP resource
AWS Elastic IP resource
AWS Virtual IP resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.12.2 NAS resource

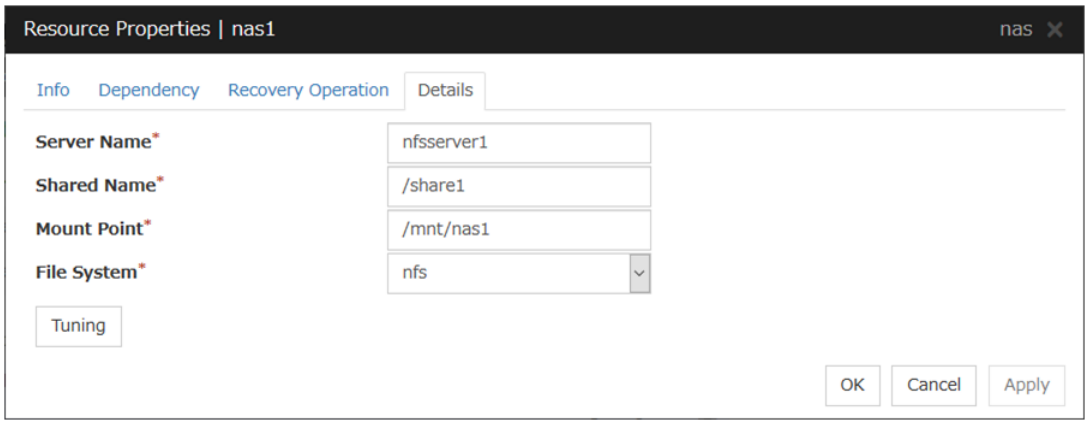
- The NAS resource controls the resources in the NFS server.
- By storing the data that is necessary for business transactions in the NFS server, it is automatically passed on when the failover group is moving during failover.



3.12.3 Notes on NAS resource

- The EXPRESSCLUSTER will control the access (mount and/or umount) to the file system. Thus, do not configure the settings for the OS to run the mount or umount command.
- On the NFS server, it is necessary to configure the settings that allow servers in the cluster for access to NFS resources.
- On the EXPRESSCLUSTER X, configure the settings that start the portmap service.
- If the host name is specified as the NAS server name, make the settings for name resolving.
- If **Exclude Mount/Unmount Commands** is selected on the **Extension** tab of the **Cluster Properties**, it may take some time to activate or deactivate the NAS resource because the mount or unmount of the disk resource, NAS resource, and mirror resource is performed exclusively in the same server.
- When specifying path including symbolic link for mount point, Force Operation cannot be done even if it is chosen as operation in Detecting Failure.
  Similarly, if a path containing "//" is specified, forced termination will also fail.

3.12.4 Details tab



Server Name (Within 255 bytes)

Enter the IP address or the server name of the NFS. If you set the host name, set the name resolution to OS. (ex. By adding entry to /etc/hosts)

Shared Name (Within 1023 bytes)

Enter the share name on the NFS server.

Mount Point (Within 1023 bytes)

Enter the directory where the NFS resource will be mounted. This must start with "/."

File System (Within 15 bytes)

Enter the type of file system of the NFS resource. You may also directly enter the type.

- nfs

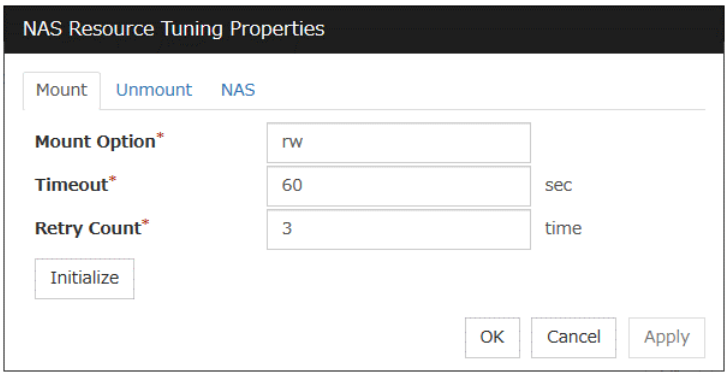
Tuning

Displays the **NAS Resource Tuning Properties** dialog box. Configure the NAS resource detailed settings.

NAS Resource Tuning Properties

Mount tab

The advanced settings for mounting are displayed.



Mount Option (Within 1023 bytes)

Enter the option that is passed to the mount command when mounting a file system. If you are entering more than one option, use "," to separate them.

Examples of the mount option

Setting item	Setting value
Server Name	nfsserver
Shared Name	/share1
Mount Point	/mnt/nas1
File System	nfs
Mount Option	rw

The mount command that is run when the option shown above is set:

mount -t nfs -o rw nfsserver1:/share1 /mnt/nas1

Timeout (1 to 999)

Set the timeout to wait the mount command to be completed when mounting a file system.

It may take a while depending on how heavily network is loaded. Be careful when you are setting the value as the timeout may be detected while a command is running when you set a small value.

Retry Count (0 to 999)

Set the number of mount retries when mounting the file system fails.

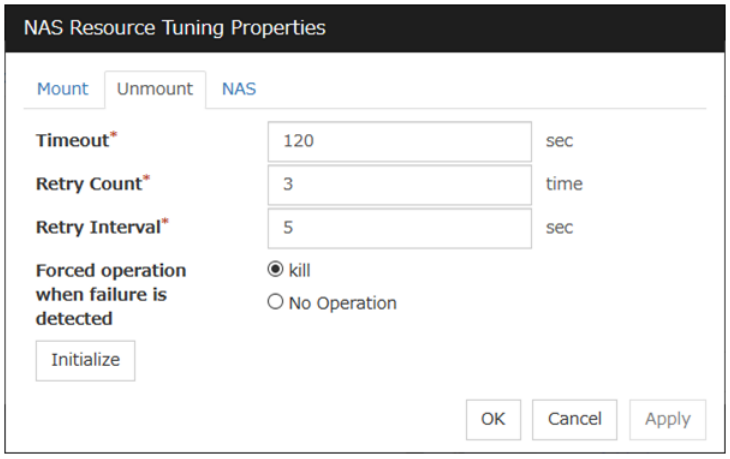
When zero is set, mounting is not retried.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

Unmount tab

The advanced settings for unmounting are displayed.



Timeout (1 to 999)

Set the timeout that waits for the end of the umount command when unmounting a file system.

Retry Count (0 to 999)

Set the number of unmount retries to be made when unmounting the file system fails. When zero is set, unmounting is not retried.

Retry Interval (0 to 999)

Enter the interval in which you want to retry unmounting the file system when unmounting fails.

Forced operation when failure is detected

Select an action to be taken when retrying unmount after unmount fails from the following.

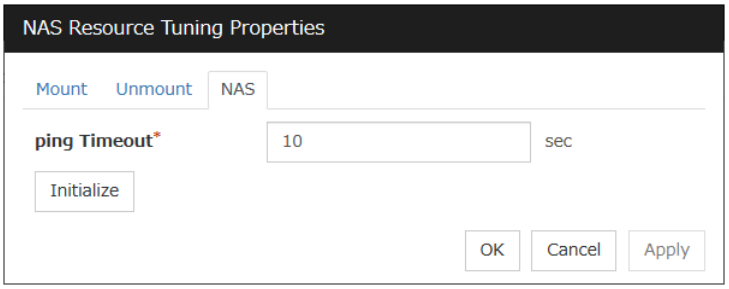
- kill:
  Attempts the forceful termination of the process that is accessing the mount point. This does not always mean that the processes can be forcibly terminated.
- No Operation:
  Does not attempt the forceful termination of the process that is accessing the mount point.

Initialize

Clicking **Initialize** resets the values of all items to the default values.

NAS tab

The advanced settings for NAS are displayed.



Ping Timeout (0 to 999)

Set timeout of the ping command is used to check the connection with the server when activating and deactivating NAS resources. If zero is specified, the ping command is not is used.

Initialize

Clicking **Initialize** sets all the items to their default values.

3.13 Understanding Volume manager resources

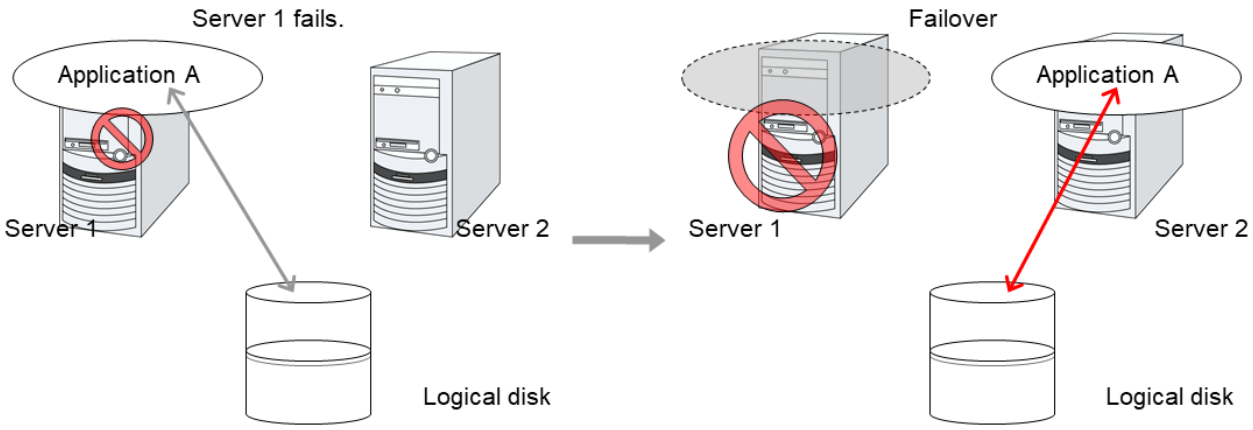
3.13.1 Dependencies of Volume manager resources

The volume manager resources depend on the following group resource types by default.

Group resource type
Dynamic DNS resource
Floating IP resource
Virtual IP resource
AWS Elastic IP resource
AWS Virtual IP resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.13.2 What is a Volume manager resource?

- The volume manager is disk management software that handles multiple storage devices and disks as one logical disk.
- Volume manager resources control logical disks managed by the volume manager.
- If data necessary for operation is stored in a logical disk, it is automatically taken over, for example, when there is a failover or a failover group is moved.



3.13.3 Notes on Volume manager resources

<General>

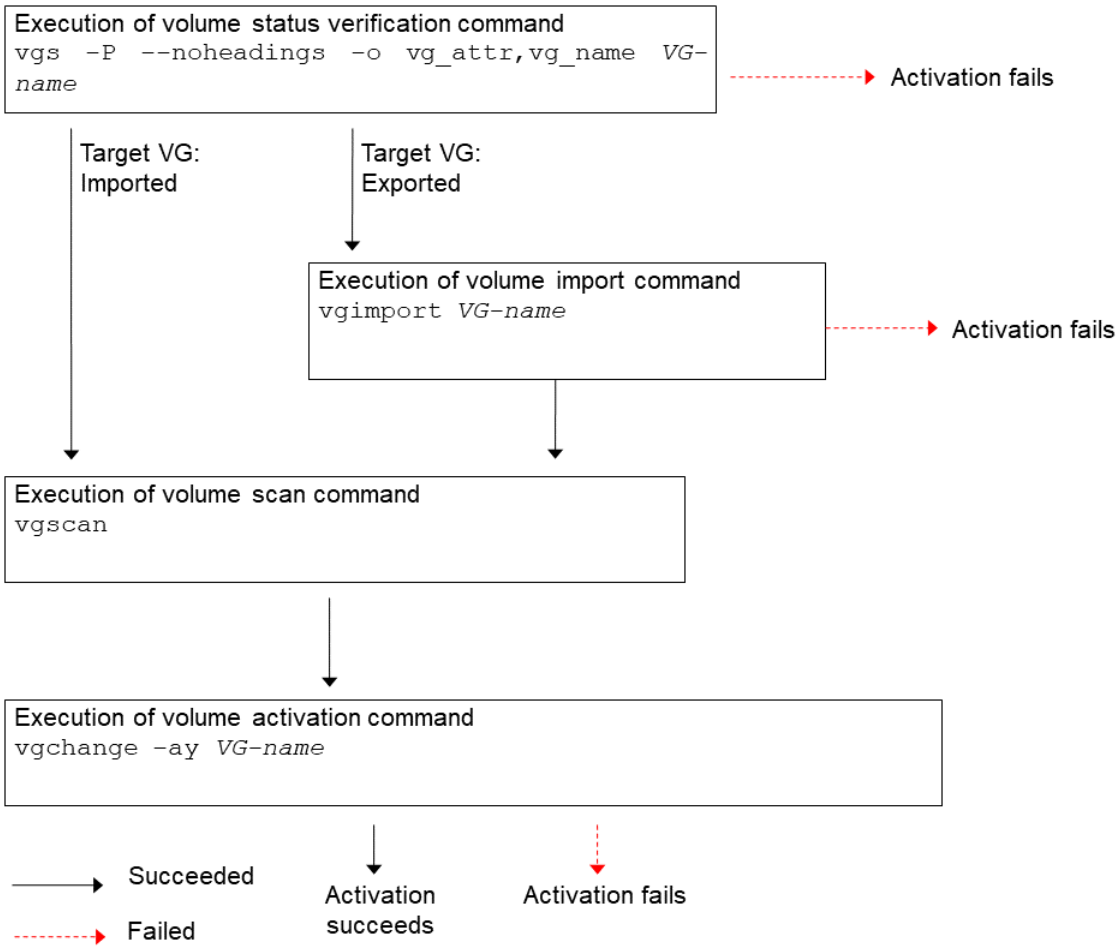
- Do not use volume manager resources to manage a mirror disk.
- Disk resources control each volume.
- Do not specify the import or export settings on the OS because EXPRESSCLUSTER performs access control (importing or exporting) for logical disks.

<Notes on using resources with the volume manager lvm>

- Volume groups are not defined on the EXPRESSCLUSTER side.
- At least one disk resource is required because each volume must be controlled.
- The volume groups included in the EXPRESSCLUSTER configuration data are automatically exported when the OS is started.
- Other volume groups are not exported.
- When a VG created by using a shared disk is specified as a target volume, the import/export status of the VG is recorded on the shared disk according to the LVM specification. Therefore, if activation (import) or deactivation (export) is performed on the active server, it might be assumed that the same operation is performed on the standby server.
- When controlling the LVM by using the volume manager resource in an environment of Red Hat Enterprise Linux 7 or later, the LVM metadata daemon must be disabled.
- Run the following commands when activating resource.

Command	Option	Timing when using command
vgs	-P	Verifying volume group status
	--noheadings	Verifying volume group status
	-o vg_attr,vg_name	Verifying volume group status
vgimport	(Nothing)	Importing volume group
vgscan	(Nothing)	Activating volume group
vgchange	-ay	Activating volume group

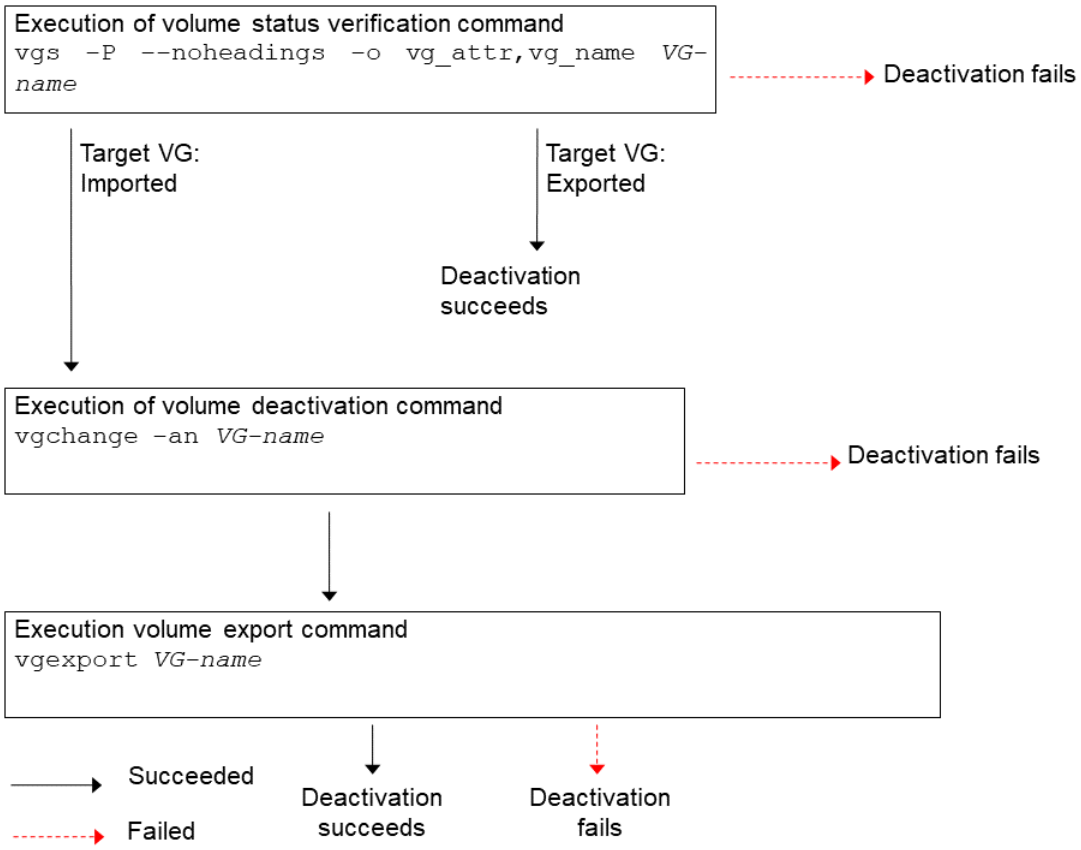
- The resource activation sequence is shown below.



- Run the following commands when deactivating resource.

Command	Option	Timing when using command
vgs	-P	Verifying volume group status
	--noheadings	Verifying volume group status
	-o vg_attr,vg_name	Verifying volume group status
vgchange	-an	Deactivating volume group
vgexport	(Nothing)	Exporting volume group

- The resource deactivation sequence is shown below.

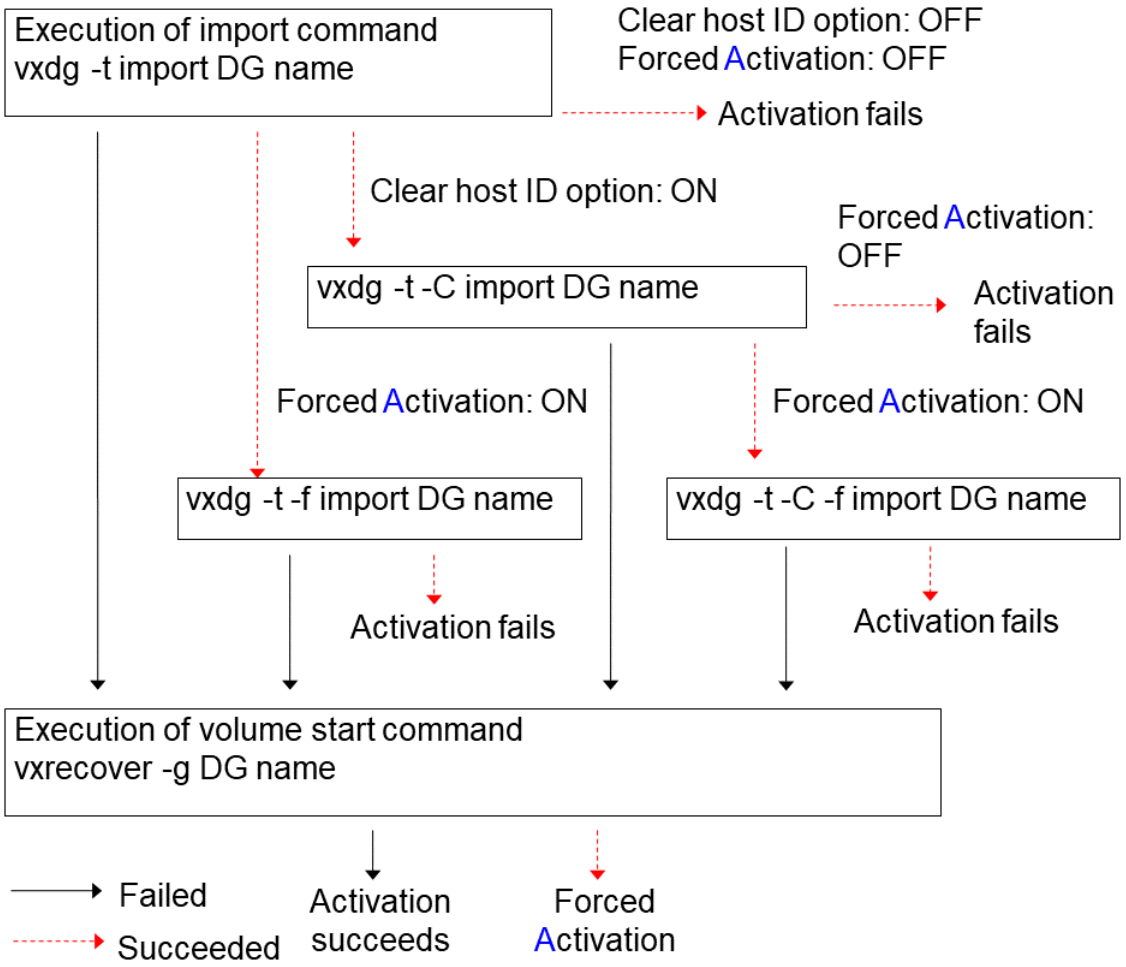


<Notes on using resources with the volume manager vxvm>

- Disk groups are not defined on the EXPRESSCLUSTER side.
- The disk groups included in the EXPRESSCLUSTER configuration data are automatically deported when the OS is started.
- Other disk groups are not deported.
- If the **Clear host ID** option is not selected, disk groups cannot be imported to the failover destination server due to VxVM specifications if the failover source server fails to normally deport the disk groups.
- Even if an import timeout occurs, importing might be successfully completed. This problem can be avoided by specifying the **Clear host ID** or **Forced Option at Import** option, which retries importing.
- Run the following commands when activating a resource.

Command	Option	When to use
vxdg	import	When importing a disk group
	-t	When importing a disk group
	-C	When importing a disk group fails and the **Clear host ID** option is selected
	-f	When importing a disk group fails and the **Forced Activation** option is selected
vxrecover	-g	When the volume for the specified disk group is started
	-sb	When the volume for the specified disk group is started

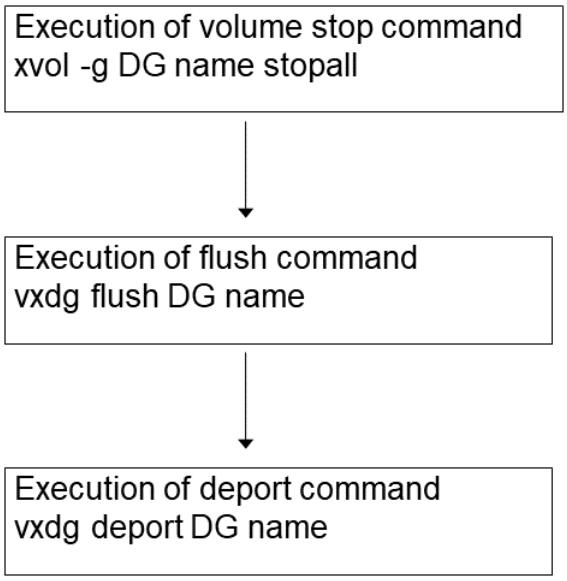
- The resource activation sequence is shown below.



- Run the following commands when activating a resource.

Command	Option	When to use
vxdg	deport	When deporting a disk group
	flush	When flushing data
vxvol	-g	When the volume of the specified disk group is stopped
	stopall	When the volume of the specified disk group is stopped

- The resource deactivation sequence is shown below.



<Notes on using resources with the volume manager zfspool>

- Exporting and other processes for ZFS may be delayed dramatically if iSCSI connection is disconnected when using ZFS storage pool under iSCSI environment.(OS restriction)

  The ZFS operations at the time of iSCSI disconnection is regulated in ZFS property value **failmode.** However, **failmode=panic** is recommended in EXPRESSCLUSTER. When it is **failmode=panic**, it operates as OS panics independently in a given time after iSCSI

- On the data set that the ZFS property value **mountpoint** is configured in legacy, the file system will not be mounted by just importing the storage pool. In this case, it is necessary to mount or unmount ZFS file system by using the disk resource in addition to Volume Manager resource.

- When on Ubuntu 16.04 or later, a failover group may be activated on more than 1 servers, state of "network partition" in other words, depending on the timing of OS startup. Even if the storage pool is automatically imported at OS startup, prevent the file system from being automatically mounted.

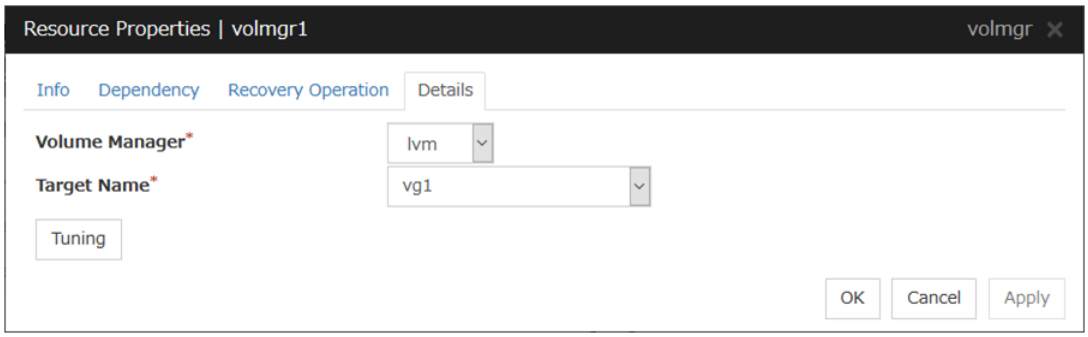
  The way to avoid automatic mounting is either of the below.

  – Set ZFS property value mountpoint to legacy.

  – Set ZFS property value canmount to noauto.

  This setting enables to avoid the automatic mounting even when the automatic import is performed at OS startup, preventing the network partition. In this case, it is necessary to mount or unmount ZFS file system by using the disk resource.

3.13.4 Details tab



Volume Manager

Specify the volume manager to use. The following volume managers can be selected:

- lvm (LVM volume group control)
- vxvm (VxVM disk group control)
- zfspool (ZFS storage pool control)

Target Name (within 1023 bytes)

Specify the volume name in the <VG name> format (only the target name is used).

Combo box options collect volume group information from all the servers and display all the volume groups on one or more servers.

When the volume manager is lvm, it's possible to control multiple volumes together. More than one volume is delimited with an one-byte space.

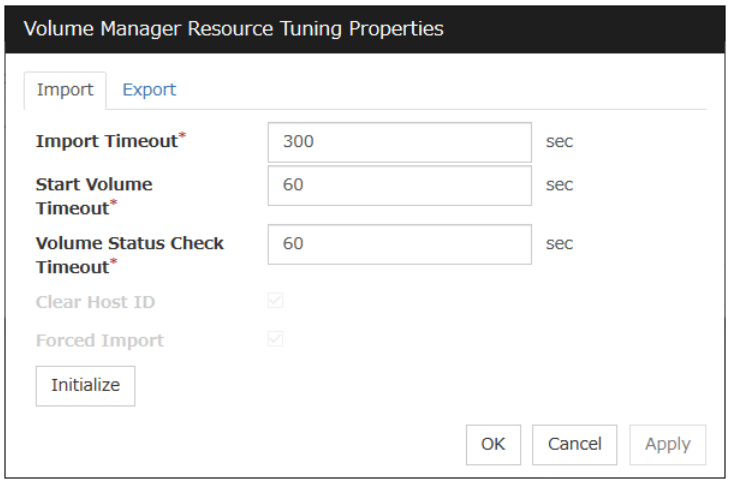
Tuning

This displays the **Volume Manager Resource Tuning Properties** dialog box. Specify detailed settings for the volume manager resource.

Volume Manager Resource Tuning Properties (When Volume Manager is other than [zfspool])

Import Tab

The detailed import settings are displayed.



Import Timeout (1 to 9999)

Specify how long the system waits for completion of the volume import command before it times out.

Start Volume Timeout (1 to 9999)

Specify the startup command timeout.

Volume Status Check Timeout (1 to 9999)

Specify the volume status check command timeout.

This option can be used when the volume manager is **lvm**.

Clear Host ID

When normal importing fails, the clear host ID flag is set and importing is retried. The host ID is cleared when the check box is selected.

This option can be used when the volume manager is **vxvm**.

Forced Import

Specify whether to forcibly import data when importing fails. Data is forcibly imported if the check box is selected.

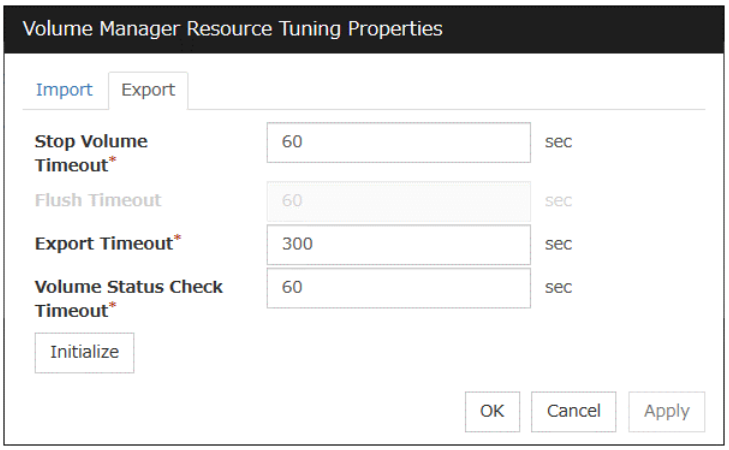
This option can be used when the volume manager is **vxvm**.

Initialize

Clicking **Initialize** resets the values of all items to the defaults.

Export Tab

The detailed export settings are displayed.



Stop Volume Timeout (1 to 9999)

Specify the volume deactivation command timeout.

Flush Timeout (1 to 9999)

Specify the flush command timeout.

This option can be used when the volume manager is **vxvm**.

Export Timeout (1 to 9999)

Specify the export/deport command timeout.

Volume Status Check Timeout (1 to 9999)

Specify the volume status check command timeout.

This option can be used when the volume manager is **lvm**.

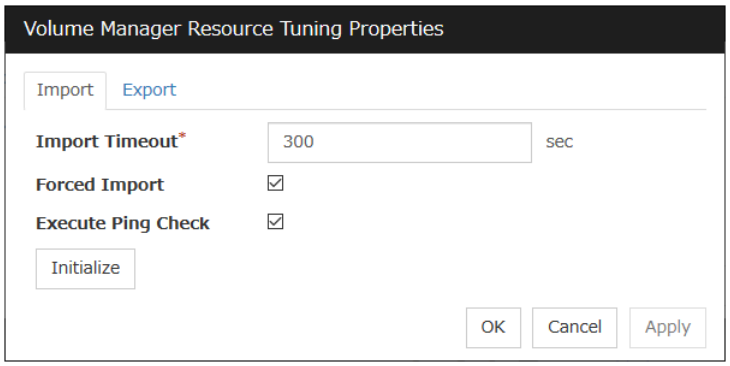
Initialize

Clicking **Initialize** resets the values of all items to the defaults.

Volume Manager Resource Tuning Properties (When Volume Manager is [zfspool])

Import Tab

The detailed import settings are displayed.



Import Timeout (1 to 9999)

Specify how long the system waits for completion of the volume import command before it times out.

Forced Import

Specify whether to forcibly import data when importing fails. Data is forcibly imported if the check box is selected.

Execute Ping Check

This setting is enabled only when **Forced Import** is set to ON.

If an import failure occurs because another host has already performed import, **ping Check** specifies monitoring of whether the host is active using ping before the forced import. If the host becomes active as a result of the monitoring, forced activation is not performed. This prevents more than one host from simultaneously performing import to a single pool. When the check box is ON, activation of the host is monitored.

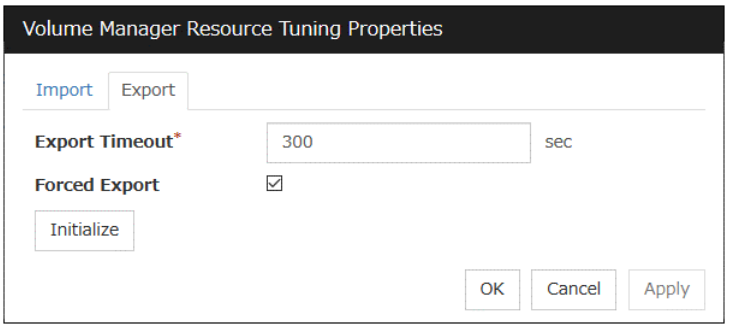
Note: When this setting is enabled, and a considerable time elapses between EXPRESSCLUSTER stopping and the OS shutting down, failover may fail. For example, if a monitor resource detects an abnormality and shuts down the operating server, and if the standby system starts activation of the volume manager before the operating server has stopped, a ping check will cause the activation to fail.

Initialize

Clicking **Initialize** resets the values of all items to the defaults.

Export Tab

The detailed export settings are displayed.



Export Timeout (1 to 9999)

Specify how long the system waits for completion of the volume export command before it times out.

Forced Export

Specify whether to forcibly export data when exporting fails. Data is forcibly exported if the check box is selected.

Initialize

Clicking **Initialize** resets the values of all items to the defaults.

3.14 Understanding VM resources

3.14.1 Dependencies of VM resources

VM resources do not depend on any group resource type by default.

3.14.2 What is a VM resource?

The VM resources control the virtual machines (guest OSs) in the virtualization infrastructure.

The management OS under which EXPRESSCLUSTER is installed starts and stops the virtual machines. For vSphere, EXPRESSCLUSTER can be installed and used under the guest OS of the virtual machine which was prepared for management.

Migration of the virtual machines can also be performed. If, however, vSphere is used, the configuration must also use vCenter.

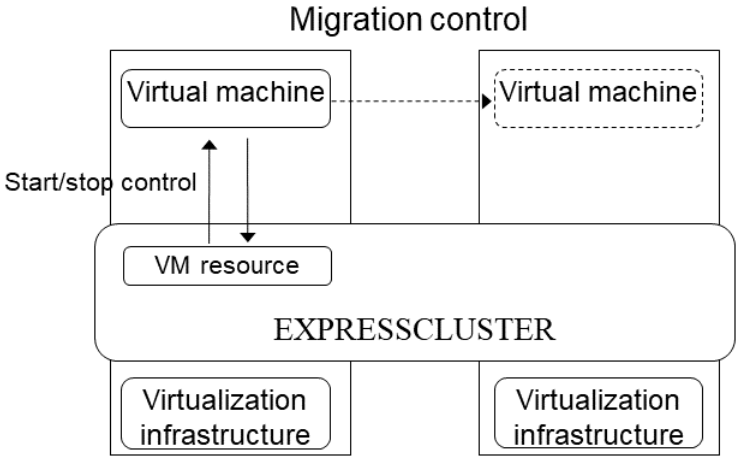


Fig. 1 : Configuration when EXPRESSCLUSTER is installed under the management OS for the virtualization infrastructure

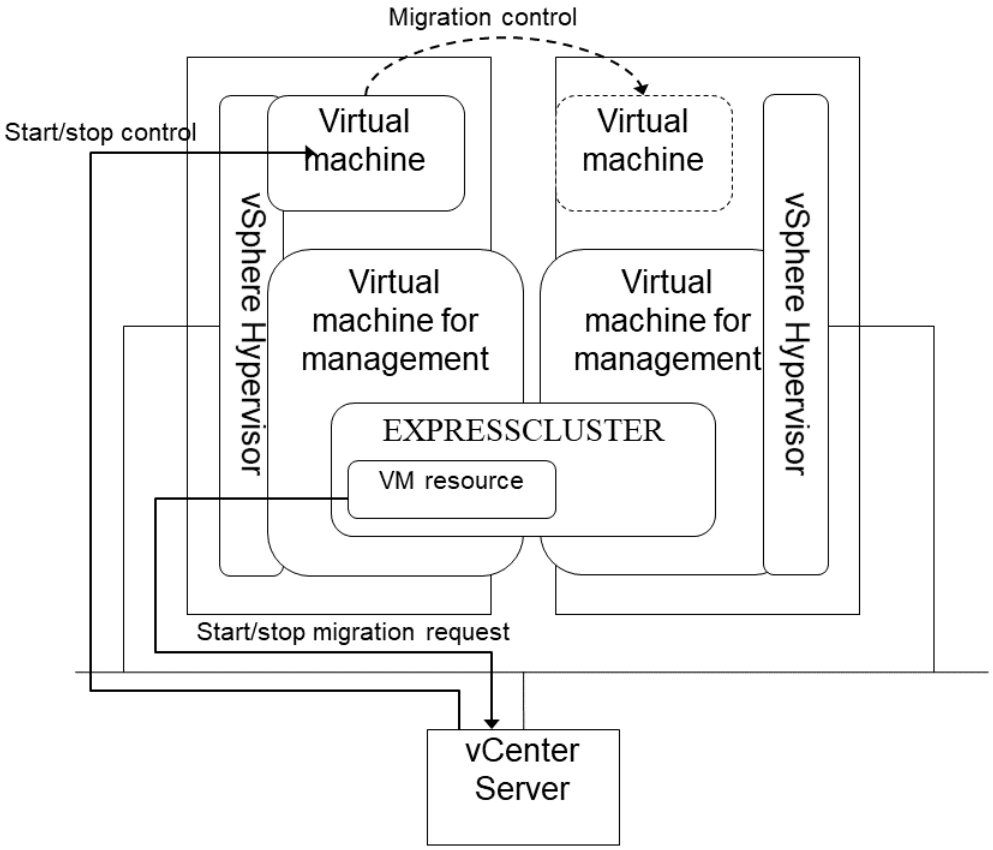


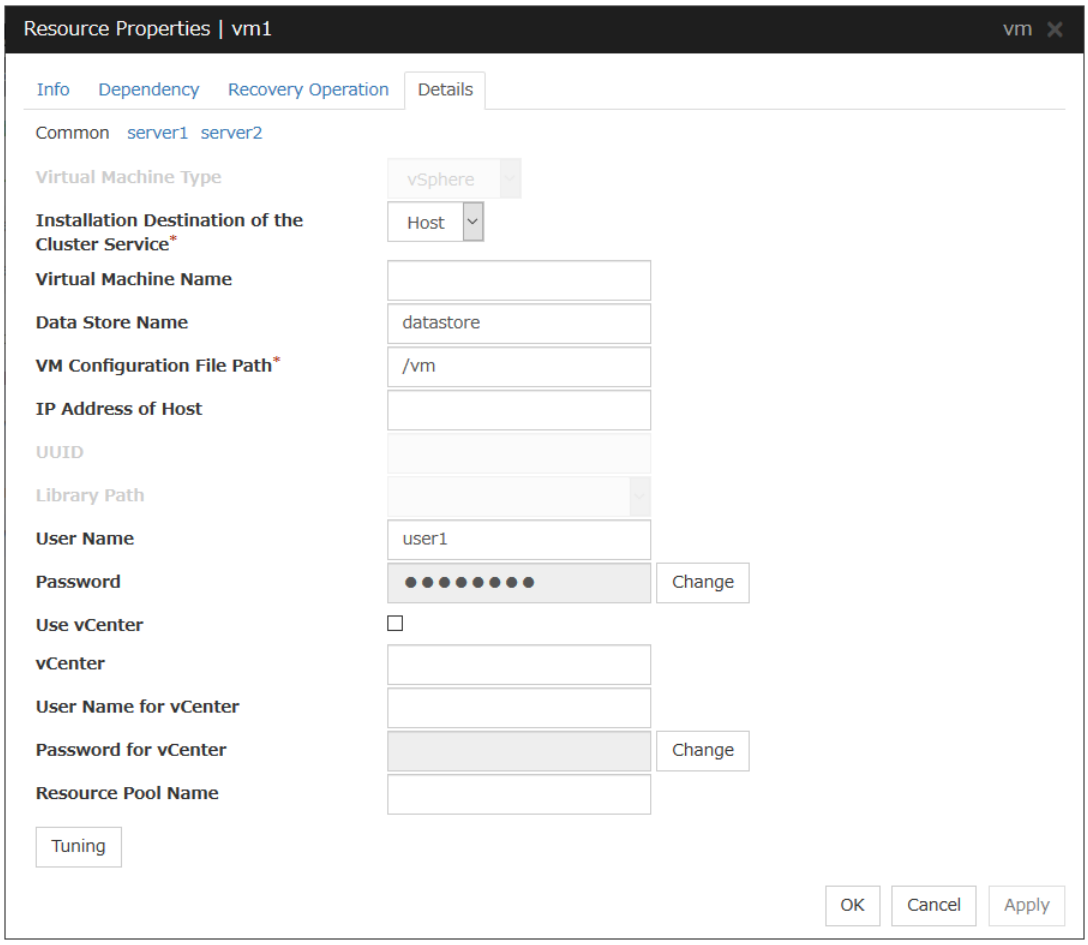
Fig. 2 : Configuration when EXPRESSCLUSTER is installed under the OS on a virtual machine for management (vSphere only)

3.14.3 Notes on VM resources

- If the virtualization infrastructure type is XenServer or KVM, the VM resources are valid only when EXPRESSCLUSTER is installed under the host OS in the virtualization infrastructure.
- If the virtualization infrastructure type is vSphere, the VM resources can be used even if EXPRESSCLUSTER is installed under the guest OS. In this case, however, vCenter must always be used.
- A VM resource can be registered with a group for which the group type is virtual machine.
- Only one VM resource can be registered per group.
- If vSphere is selected as the virtualization infrastructure, **Use vCenter** must be selected (on) to perform migration.
- Confirm the start time of the virtual machine (guest OS) to be controlled with a virtual machine resource, and set **Virtual Machine Start Wait Time** of **Virtual Machine Resource Adjustment Property**.
  The default value of **Virtual Machine Start Wait Time** is 0 seconds, so if it is not changed, the virtual machine monitor resource may mistakenly detect a monitor error.

3.14.4 Details tab

For vSphere



Virtual Machine Type

Specify the virtualization infrastructure type.

Installation Destination of the Cluster Service

Specify the type of OS under which EXPRESSCLUSTER is installed. Selecting the guest OS automatically selects the **Use vCente**r check box.

Virtual Machine Name (within 255 bytes)

Enter the virtual machine name. This setting is not required if the virtual machine path is entered. Specify the virtual machine path if the virtual machine name might be changed in the virtualization infrastructure.

Data Store Name (within 255 bytes)

Specify the name of data store containing the virtual machine configuration information.

VM Configuration File Path (within 1,023 bytes)

Specify the path where the virtual machine configuration information is stored.

IP Address of Host `Server Individual Setup`

Specify the management IP address of the host. You must specify the IP address of host for each server, using individual server settings.

User Name (within 255 bytes) `Server Individual Setup`

Specify the user name used to start the virtual machine.

Password (within 255 bytes) `Server Individual Setup`

Specify the password used to start the virtual machine.

Use vCenter

Specify whether to use vCenter. Use vCenter when performing migration.

vCenter (within 1,023 bytes)

Specify the vCenter host name.

User Name for vCenter (within 255 bytes)

Specify the user name used to connect to vCenter.

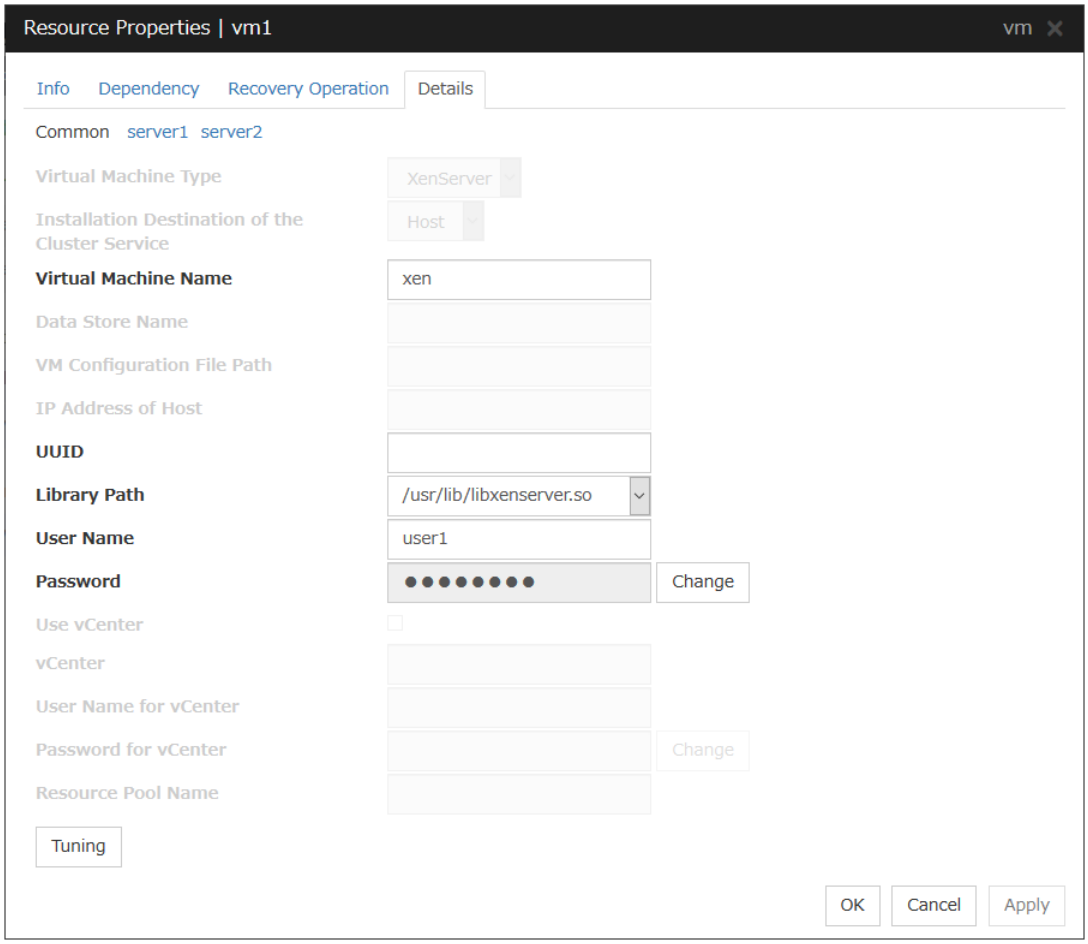
Password for vCenter (within 255 bytes)

Specify the password used to connect to vCenter.

Resource Pool Name (within 255 bytes) `Server Individual Setup`

Specify the resource pool name for starting the virtual machine.

For XenServer



Virtual Machine Type

Specify the virtualization infrastructure type.

Virtual Machine Name (within 255 bytes)

Enter the virtual machine name. This setting is not required if the UUID is specified. Specify the UUID if the virtual machine name might be changed in the virtualization infrastructure.

UUID

Specify the UUID (Universally Unique Identifier) for identifying the virtual machine.

Library Path (within 1,023 bytes)

Specify the library path used to control XenServer.

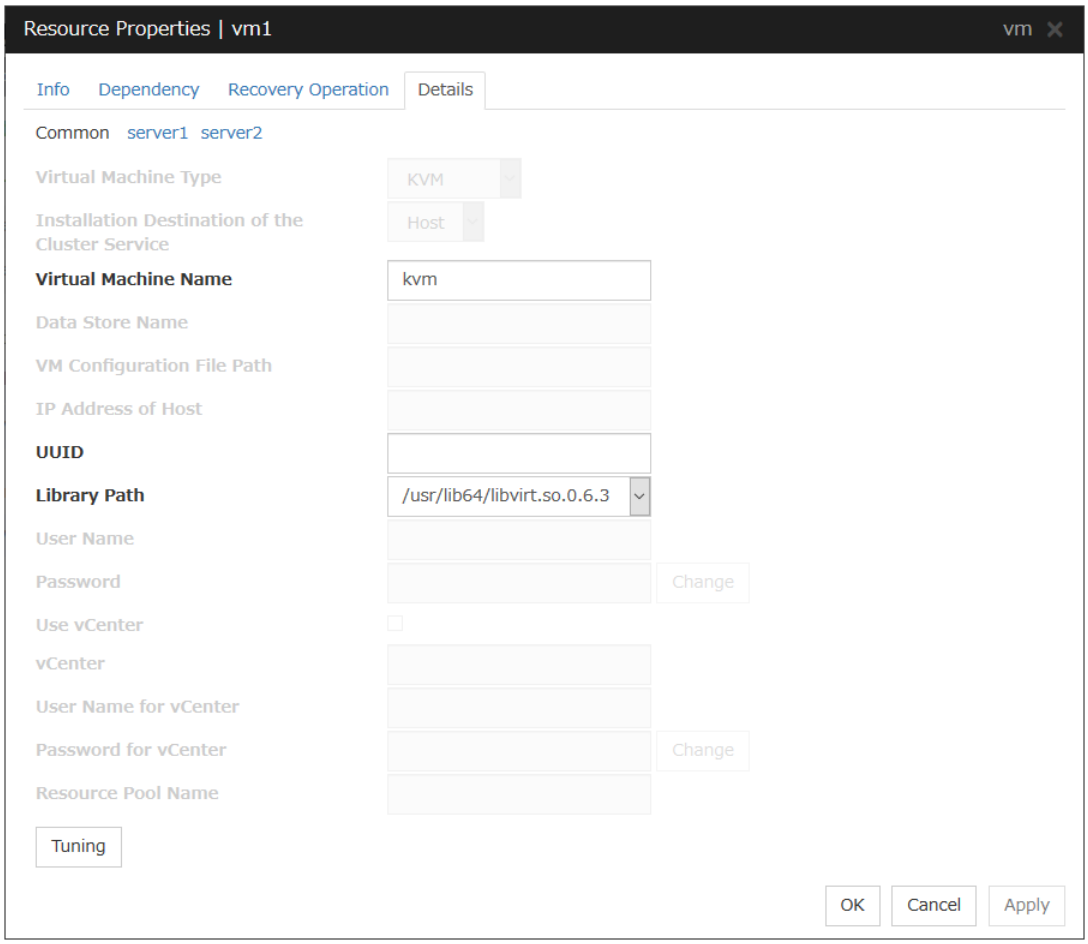
User Name (within 255 bytes)

Specify the user name used to start the virtual machine.

Password (within 255 bytes)

Specify the password used to start the virtual machine.

For KVM



Virtual Machine Type

Specify the virtualization infrastructure type.

Virtual Machine Name (within 255 bytes)

Enter the virtual machine name. This setting is not required if the UUID is specified.

UUID

Specify the UUID (Universally Unique Identifier) for identifying the virtual machine.

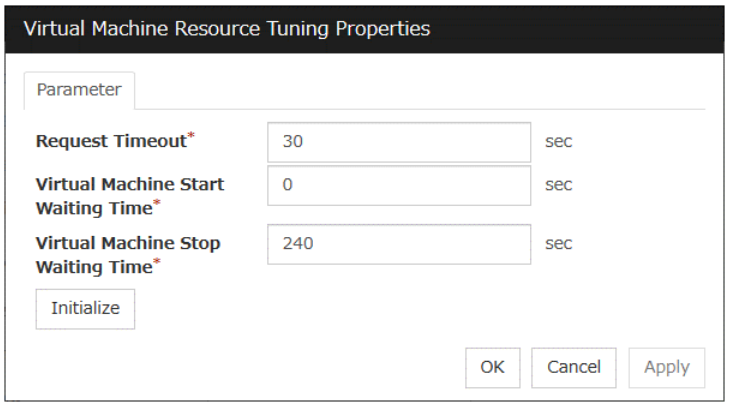
Library Path (within 1,023 bytes)

Specify the library path used to control KVM.

Tuning

This displays the **VM Resource Tuning Properties** dialog box. Specify detailed settings for the VM resource.

VM Resource Tuning Properties



Request Timeout

Specify how long the system waits for completion of a request such as to start or stop a virtual machine.

If the request is not completed within this time, a timeout occurs and resource activation or deactivation fails.

Virtual Machine Start Waiting Time

The system definitely waits this time after requesting the virtual machine to startup.

Virtual Machine Stop Waiting Time

The maximum time to wait for the stop of the virtual machine. Deactivation completes at the timing the stop of the virtual machine.

3.15 Understanding Dynamic DNS resources

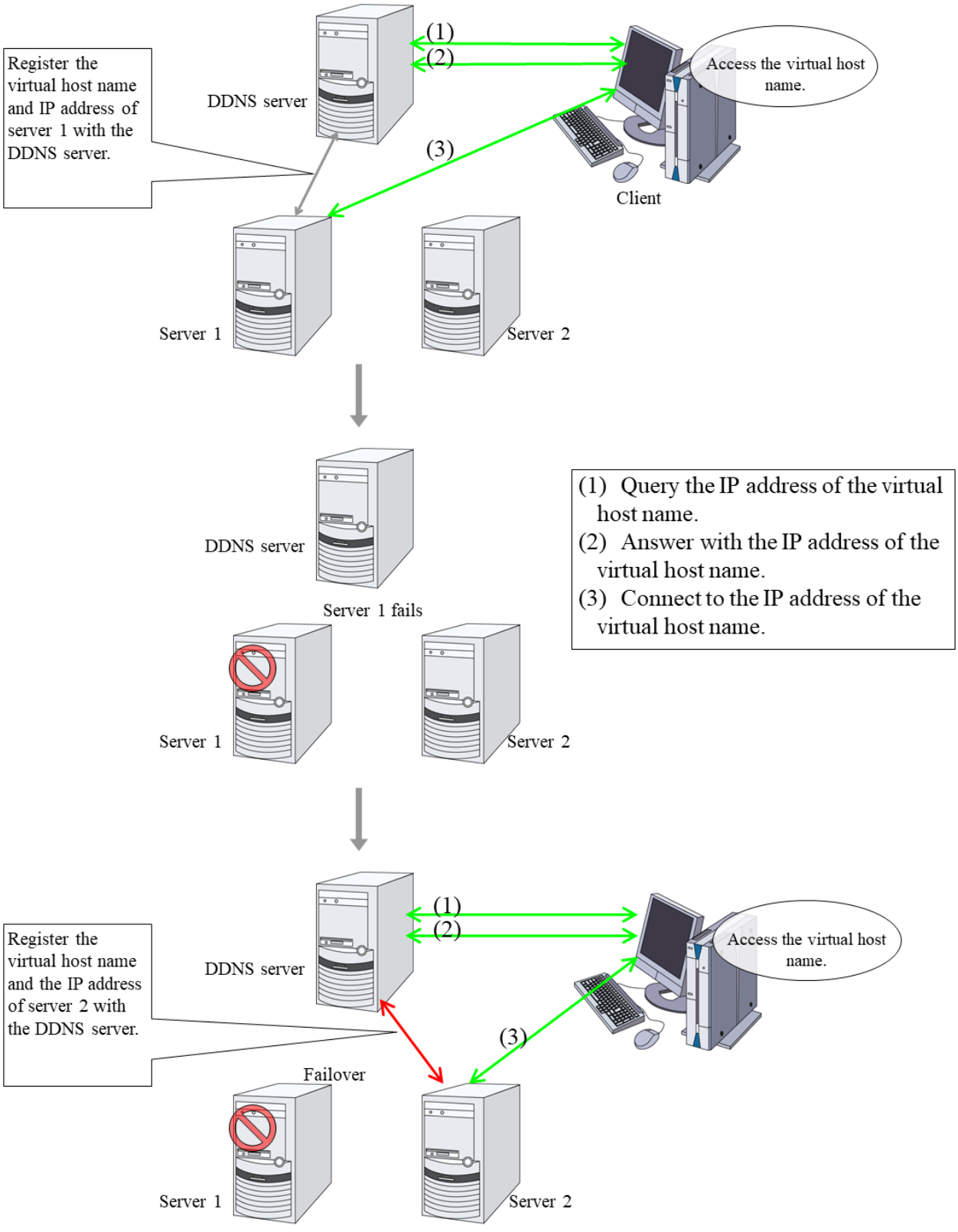
3.15.1 Dependencies of Dynamic DNS resources

By default, NAS resources depend on the following group resources types:

Group resource type
Virtual IP resource
Floating IP resource
AWS Elastic IP resource
AWS Virtual IP resource
Azure probe port resource

3.15.2 What is a Dynamic DNS resource?

- A Dynamic DNS resource registers the virtual host name and the IP address of the active server to the Dynamic DNS server. Client applications can be connected to a cluster server by using a virtual computer name. When the virtual host name is used, the client does not have to be aware of whether the connection destination server is switched when a failover occurs or a group is moved.


Register the virtual host name and IP address of server 1 with the DDNS server.
DDNS server
(1)
(2)
Access the virtual host name.
(3)
Client
Server 1
Server 2
DDNS server
Server 1 fails
Server 1
Server 2
(1) Query the IP address of the virtual host name.
(2) Answer with the IP address of the virtual host name.
(3) Connect to the IP address of the virtual host name.
Register the virtual host name and the IP address of server 2 with the DDNS server.
DDNS server
(1)
(2)
Access the virtual host name.
(3)
Failover
Server 1
Server 2

3.15.3 Preparing to use Dynamic DNS resources

Set up the DDNS server before using Dynamic DNS resources.

The description below assumes the use of BIND9.

One of the two types of /etc/named.conf settings below is used depending on the Dynamic DNS resource use mode when the DDNS server is set up.
Specify /etc/named.conf on the DDNS server in the desired mode.

- When using Dynamic DNS resources with authentication

  Create a shared key on the BIND9 server by using the dnssec-keygen command. Add the shared key to /etc/named.conf and allow the zone file to be updated. When adding a Dynamic DNS resource, enter the shared key name in **Authentication Key Name** and the shared key value in **Authentication Key Value**.

  Note: For details about setting up the DDNS server, using the dnssec-keygen command, and specifying setting other than allow-update, see the BIND manual.

  Example:

  1. **Generate a shared key.**
     #dnssec-keygen -a HMAC-MD5 -b 256 -n HOST example
     example is the shared key name.

     When the dnssec-keygen command is executed, the two files below are generated. The same shared key is used for these files.

     Kexample.+157+09088.key
     Kexample.+157+09088.private

     While the shared key is extracted from Kexample.+157+09088.key when using the named.conf setting below, using Kexample.+157+09088.private leads to the same result.
     The shared key value for Kexample.+157+09088.key is underlined below.

     # cat Kexample.+157+09088.key
     example. IN KEY 512 3 157 **iuBgSUEIBjQUKNJ36NocAgaB**

  2. Add the shared key information to /etc/named.conf.

```
key " example " {
    algorithm hmac-md5;
    secret " iuBgSUEIBjQUKNJ36NocAgaB";
};
```

3. Add the shared key information to the zone statement in /etc/named.conf.

```
zone "example.jp" {
    :
    allow-update{
         key example;
    };
    :
};
```

4. When adding a Dynamic DNS resource by using the Claster WebUI, enter the shared key name (**example**) in **Authentication Key Name** and the shared key value (**iuBgSUEIBjQUKNJ36NocAgaB**) in **Authentication Key Value**.

- When using Dynamic DNS resources without authentication

  Be sure to specify the IP addresses of all servers in the cluster as the IP address range in which the zone file can be updated (allow-update {xxx.xxx.xxx.xxx}) in /etc/named.conf.

  Example:

  IP address for server1 in the cluster: 192.168.10.110
  IP address for server2 in the cluster: 192.168.10.111

  1. Add the IP address range in which updates are allowed to the zone statement in /etc/named.conf.

```
zone "example.jp" {
    :
    //IP address range in which updates are allowed
    allow-update {
        192.168.10.0/24;
    };
    :
};
```

  or

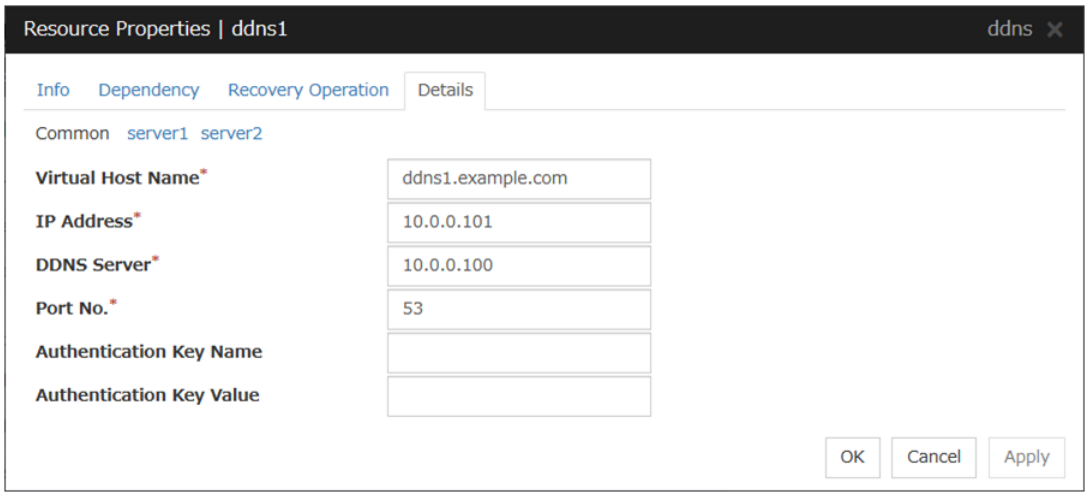
```
zone "example.jp" {
    :
    //IP address range in which updates are allowed
    allow-update {
        192.168.10.110;
        192.168.10.111;
    };
    :
};
```

  2. When adding a Dynamic DNS resource, do not enter any values in **Authentication Key Name or Authentication Key Value**.

3.15.4 Notes on Dynamic DNS resources

- When using Dynamic DNS resources, the bind-utils package is necessary on each server.
- Configuring Dynamic DNS server settings to be used is necessary to /etc/resolve.conf on each server.
- When IP address of each server exists in different segments, FIP address cannot be set as IP address of Dynamic DNS resources.
- To register each server IP address with the DDNS server, specify the addresses in the settings for each server.
- In case of connecting from clients using virtual host name, when the fail over of the group which has Dynamic DNS resources occurs, reconnection may be necessary (restart browsers, etc.).
- This method, which authenticates resources, applies only to a DDNS server set up using BIND9. To use the method without authentication, do not enter any values in **Authentication Key Name** or **Authentication Key Value**.
- The behavior when the Cluster WebUI is connected depends on the Dynamic DNS resource settings.
  - When the IP address of each server is specified for Dynamic DNS resources on a server basis
    If the Cluster WebUI is connected by using the virtual host name from the client, this connection is not automatically switched if a failover occurs for a group containing Dynamic DNS resources.
    To switch the connection, restart the browser, and then connect to the Cluster WebUI again.
  - When the FIP address is specified for the Dynamic DNS resource
    If the Cluster WebUI is connected by using the virtual host name from the client, this connection is automatically switched if a failover occurs for a group containing Dynamic DNS resources.
- If Dynamic DNS resources are used with the method with authentication, the difference between the time of every server in the cluster and that of the DDNS server must be less than five minutes.
  If the time difference is five minutes or more, the virtual host name cannot be registered with the DDNS server.

3.15.5 Details tab



Virtual Host Name

Enter the virtual host name to register with the DDNS service.

IP Address `Server Individual Setup`

Enter the IP address for the virtual host name.

When also using FIP resources, enter the IP address of the resources on the **Common** tab.
When using an IP address for each server, enter the IP address on each server tab.

DDNS Server

Enter the IP address of the DDNS server.

Port No.

Enter the port number of the DDNS server. The default value is 53.

Authentication Key Name

Enter the shared key name if a shared key was generated using the dnssec-keygen command.

Authentication Key Value

Enter the value of the shared key generated using the dnssec-keygen command.

3.16 Understanding AWS Elastic IP resources

3.16.1 Dependencies of AWS Elastic IP resources

By default, this function does not depend on any group resource type.

3.16.2 What is an AWS Elastic IP resource?

Client applications can use AWS Elastic IP addresses(referred to as the EIP) to access the Amazon Virtual Private Cloud (referred to as the VPC) in the Amazon Web Services (referred to as AWS) environment.

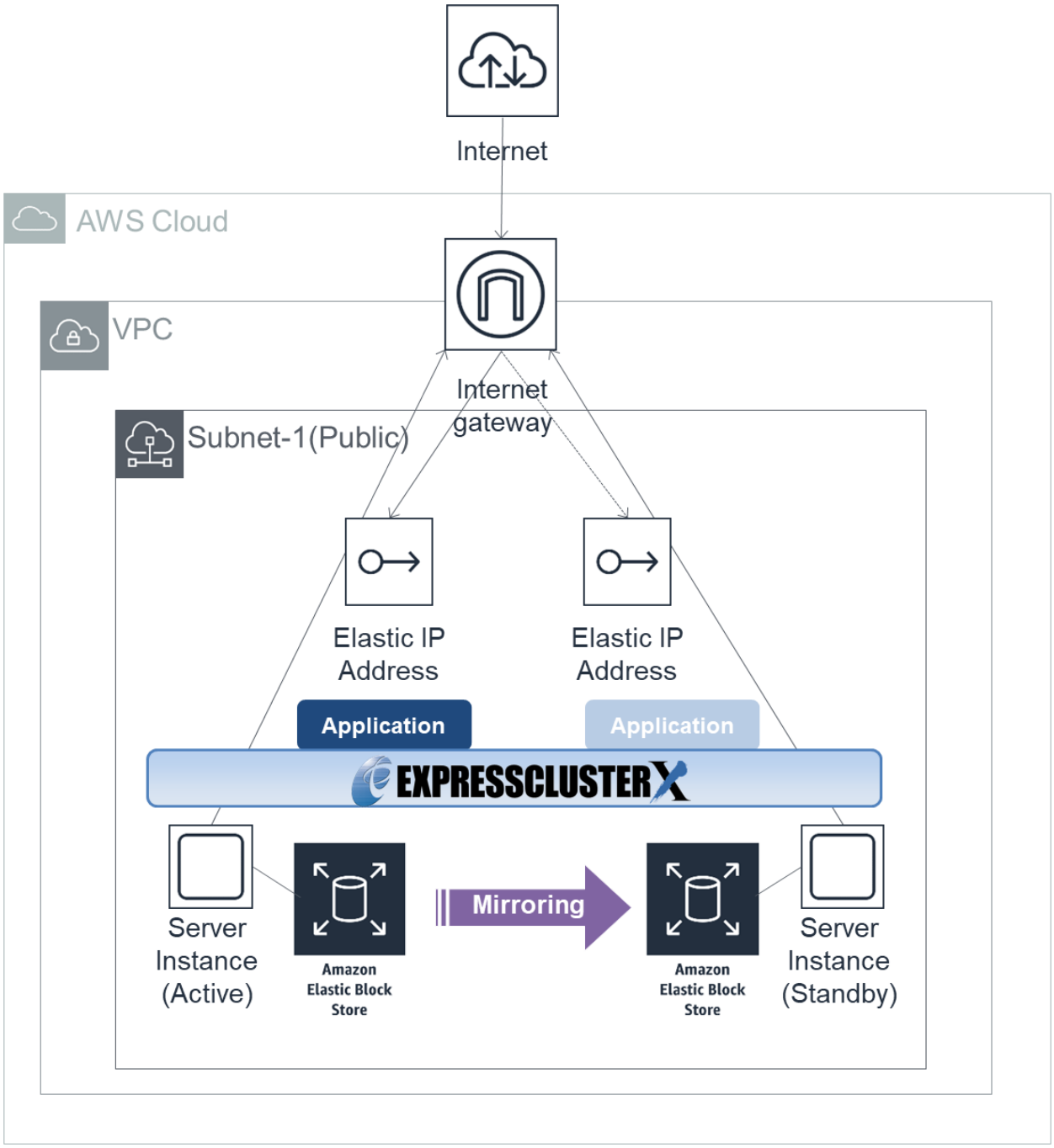
By using EIP, clients do not need to be aware of switching access destination server when a failover occurs or moving a group migration.

An AWS Elastic IP resource, an AWS Virtual IP resource, and an AWS DNS resource can be used together.

HA cluster with EIP control

This is used to place instances on public subnets (release business operations inside the VPC).

A configuration such as the following is assumed: Instances to be clustered are placed on public subnets in each Availability Zone (referred to as AZ), and each instance can access the Internet via the gateway.


Internet
AWS Cloud
VPC
Internet gateway
Subnet-1(Public)
Elastic IP Address
Elastic IP Address
Application
Application
EXPRESSCLUSTER X
Server Instance (Active)
Amazon Elastic Block Store
Mirroring
Amazon Elastic Block Store
Server Instance (Standby)

3.16.3 Notes on AWS Elastic IP resources

- See "Setting up AWS Elastic IP resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.16.4 Applying environment variables to AWS CLI run from the AWS Elastic IP resource

Specify environment variables in the environment variable configuration file to apply environment variables to the AWS CLI run from the AWS Elastic IP resource, AWS Virtual IP resource, AWS Elastic IP monitor resource and AWS AZ monitor resource.

This feature is useful when using a proxy server in an AWS environment.

The envirionment variable configuration file is stored in the following location.

<EXPRESSCLUSTER Installation path>/cloud/aws/clpaws_setting.conf

The format of the environment variable configuration file is as follows:

Envirionment variable name = Value

(Example)

```
[ENVIRONMENT]
HTTP_PROXY = http://10.0.0.1:3128
HTTPS_PROXY = http://10.0.0.1:3128
```

To specify multiple values for a parameter, enter them in comma-delimited format. The following shows an example of specifying more than one non-destination for the environment variable NO_PROXY:

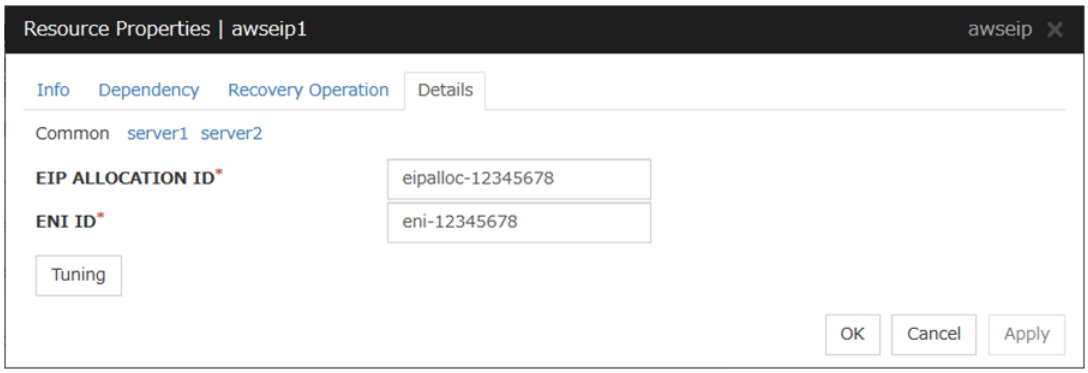
(Example)

```
NO_PROXY = 169.254.169.254,ec2.ap-northeast-1.amazonaws.com
```

The specifications of the environment variable configuration file are as follows:

- Write [ENVIRONMENT] on the first line. If this is not set, the environment variables will not be set.
- If the environment variable configuration file does not exist or you do not have read permission for the file, the variables are ignored. This does not cause an activation failure or a monitor error.
- If the same environment variables already exist in the file, the values are overwritten.
- More than one environment variable can be set. Set one environment variable on each line.
- The settings are valid regardless of whether there are spaces before and after "=" or not.
- The settings are invalid if there is a space or tab in front of the environment variable name or if there are tabs before and after "=".
- Environment variable names are case sensitive.
- Even if a value contains spaces, you do not have to enclose the value in "" (double quotation marks).
- The environment variables configured with the environment variable configuration file are propagated only to the AWS CLI executed from an AWS Elastic IP resource, an AWS Virtual IP resource, an AWS DNS resource, an AWS Elastic IP monitor resource, an AWS Virtual IP monitor resource, an AWS DNS monitor resource, and an AWS AZ monitor resource. Therefore, the configured variables are not propagated to any other script (e.g. a script before final action, a script before and after activation/deactivation, and a script to be run from EXEC resources). To execute the AWS CLI with such a script, configure necessary environment variables with the corresponding script.

3.16.5 Details tab



EIP ALLOCATION ID (Within 45 bytes)

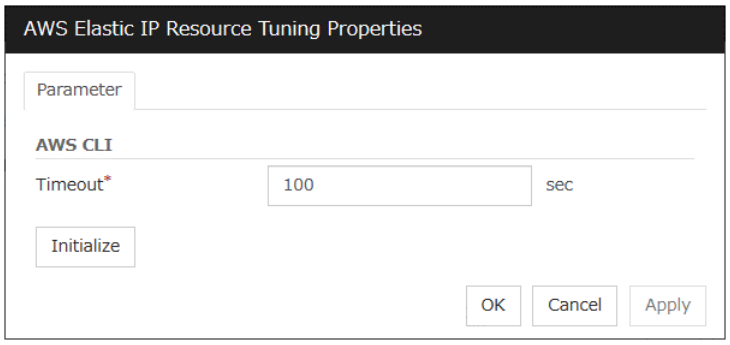
For EIP control, specify the ID of the EIP to replace.

ENI ID (Within 45 bytes) `Server Individual Setup`

For EIP control, specify the ENI ID to which to allocate an EIP. In the **Common** tab, describes the ENI ID of any server, other servers, please to perform the individual setting.

AWS Elastic IP Resource Tuning Properties

Parameter tab



Timeout (1 to 999)

Set the timeout of the AWS CLI command to be executed for AWS Elastic IP resource activation/deactivation.

3.17 Understanding AWS Virtual IP resources

3.17.1 Dependencies of AWS Virtual IP resources

By default, this function does not depend on any group resource type.

3.17.2 What is an AWS Virtual IP resource?

Client applications can use AWS Virtual IP addresses(referred to as the VIP) to access the VPC in AWS environment.

By using VIP, clients do not need to be aware of switching access destination server when a failover occurs or moving a group migration.

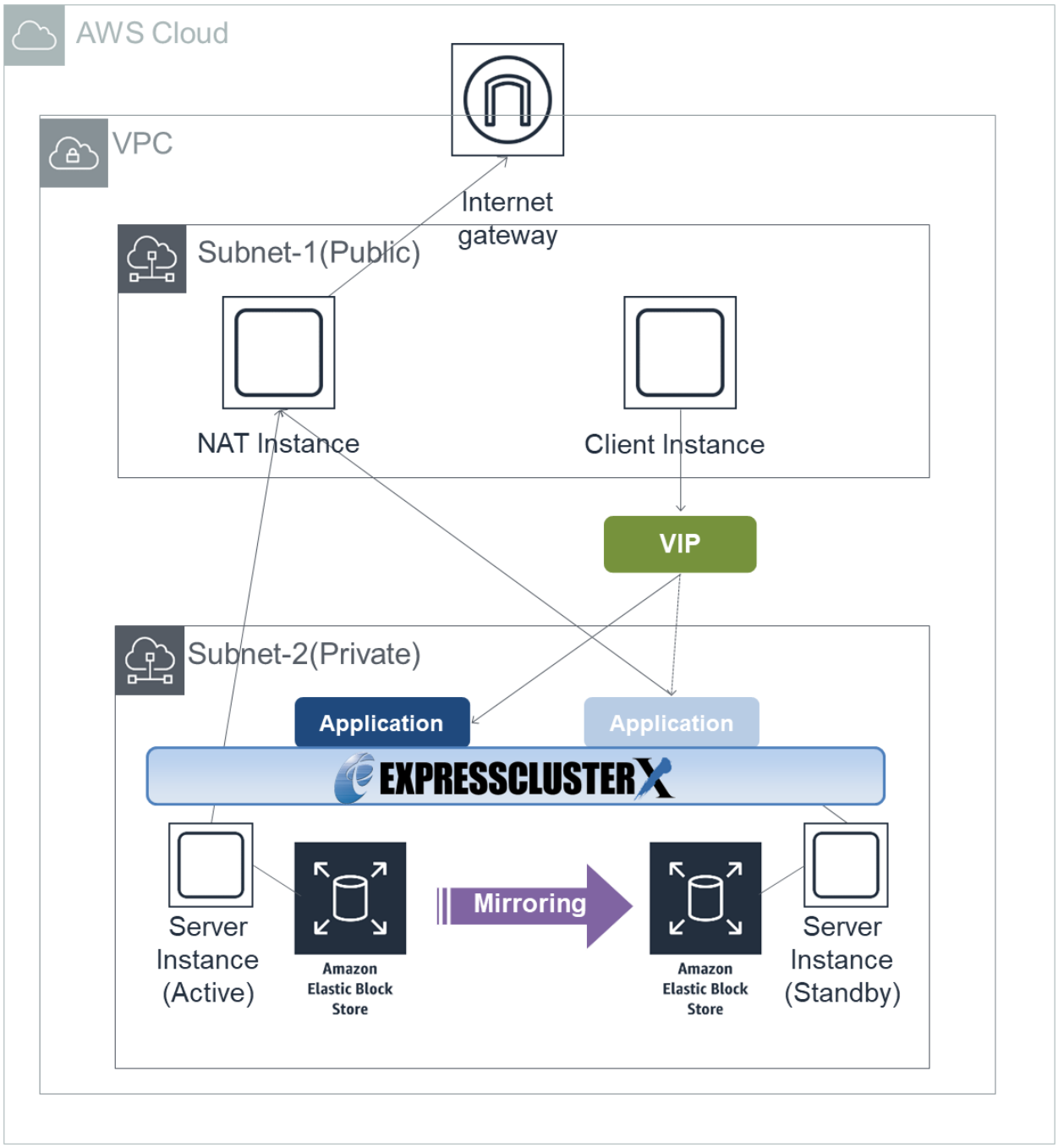
AWS CLI command is executed for AWS Virtual IP resource when it is activated to update the route table information.

An AWS Elastic IP resource, an AWS Virtual IP resource, and an AWS DNS resource can be used together.

HA cluster with VIP control

This is used to place instances on private subnets (release business operations inside the VPC).

A configuration such as the following is assumed: Instances to be clustered, as well as the instance group accessing the instances, are placed on private subnets in each Availability Zone (referred to as AZ), and each instance can access the Internet via the NAT instance placed on the public subnet.


AWS Cloud
VPC
Internet gateway
Subnet-1(Public)
NAT Instance
Client Instance
VIP
Subnet-2(Private)
Application
Application
EXPRESSCLUSTER X
Server Instance (Active)
Amazon Elastic Block Store
Mirroring
Amazon Elastic Block Store
Server Instance (Standby)

3.17.3 Notes on AWS Virtual IP resources

- See "Setting up AWS Virtual IP resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.17.4 Applying environment variables to AWS CLI run from the AWS Virtual IP resource

Specify environment variables in the environment variable configuration file to apply environment variables to the AWS CLI run from the AWS Elastic IP resource, AWS Virtual IP resource, AWS Elastic IP monitor resource and AWS AZ monitor resource.

This feature is useful when using a proxy server in an AWS environment.

The envirionment variable configuration file is stored in the following location.

<EXPRESSCLUSTER Installation path>/cloud/aws/clpaws_setting.conf

The format of the environment variable configuration file is as follows:

Envirionment variable name = Value

(Example)

```
[ENVIRONMENT]
HTTP_PROXY = http://10.0.0.1:3128
HTTPS_PROXY = http://10.0.0.1:3128
```

To specify multiple values for a parameter, enter them in comma-delimited format. The following shows an example of specifying more than one non-destination for the environment variable NO_PROXY:

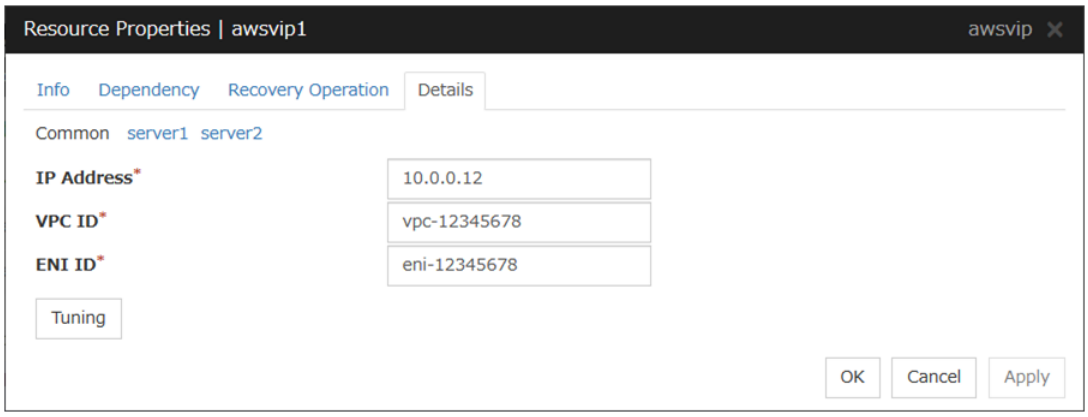
(Example)

```
NO_PROXY = 169.254.169.254,ec2.ap-northeast-1.amazonaws.com
```

The specifications of the environment variable configuration file are as follows:

- Write [ENVIRONMENT] on the first line. If this is not set, the environment variables will not be set.
- If the environment variable configuration file does not exist or you do not have read permission for the file, the variables are ignored. This does not cause an activation failure or a monitor error.
- If the same environment variables already exist in the file, the values are overwritten.
- More than one environment variable can be set. Set one environment variable on each line.
- The settings are valid regardless of whether there are spaces before and after "=" or not.
- The settings are invalid if there is a space or tab in front of the environment variable name or if there are tabs before and after "=".
- Environment variable names are case sensitive.
- Even if a value contains spaces, you do not have to enclose the value in "" (double quotation marks).
- The environment variables configured with the environment variable configuration file are propagated only to the AWS CLI executed from an AWS Elastic IP resource, an AWS Virtual IP resource, an AWS DNS resource, an AWS Elastic IP monitor resource, an AWS Virtual IP monitor resource, an AWS DNS monitor resource, and an AWS AZ monitor resource. Therefore, the configured variables are not propagated to any other script (e.g. a script before final action, a script before and after activation/deactivation, and a script to be run from EXEC resources). To execute the AWS CLI with such a script, configure necessary environment variables with the corresponding script.

3.17.5 Details tab



IP Address (Within 45 bytes)

For VIP control, specify the VIP address to use. As the VIP address, an IP address not belonging to a CIDR in the VPC must be specified.

VPC ID (Within 45 bytes) `Server Individual Setup`

For VIP control, specify the VPC ID to which the server belongs. To specify an individual VPC ID for the servers, enter the VPC ID of any server on the Common tab and specify a VPC ID for the other servers individually.

For how to configure the routing, see the following:

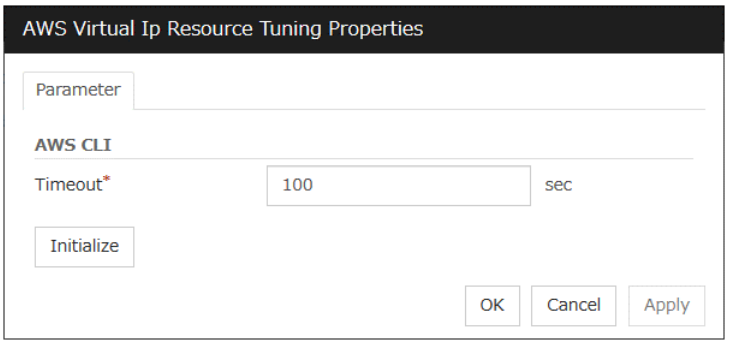
" Configuring the VPC Environment" in the "EXPRESSCLUSTER X HA Cluster Configuration Guide for Amazon Web Services (Linux)"

ENI ID (Within 45 bytes) `Server Individual Setup`

For VIP control, specify the ENI ID of VIP routing destination. For the ENI ID to specify, Source/Dest. Check must be disabled beforehand. This must be set for each server. On the Common tab, enter the ENI ID of any server, and specify an ENI ID for the other servers individually.

AWS Virtual IP Resource Tuning Properties

Parameter tab



Timeout (1 to 999)

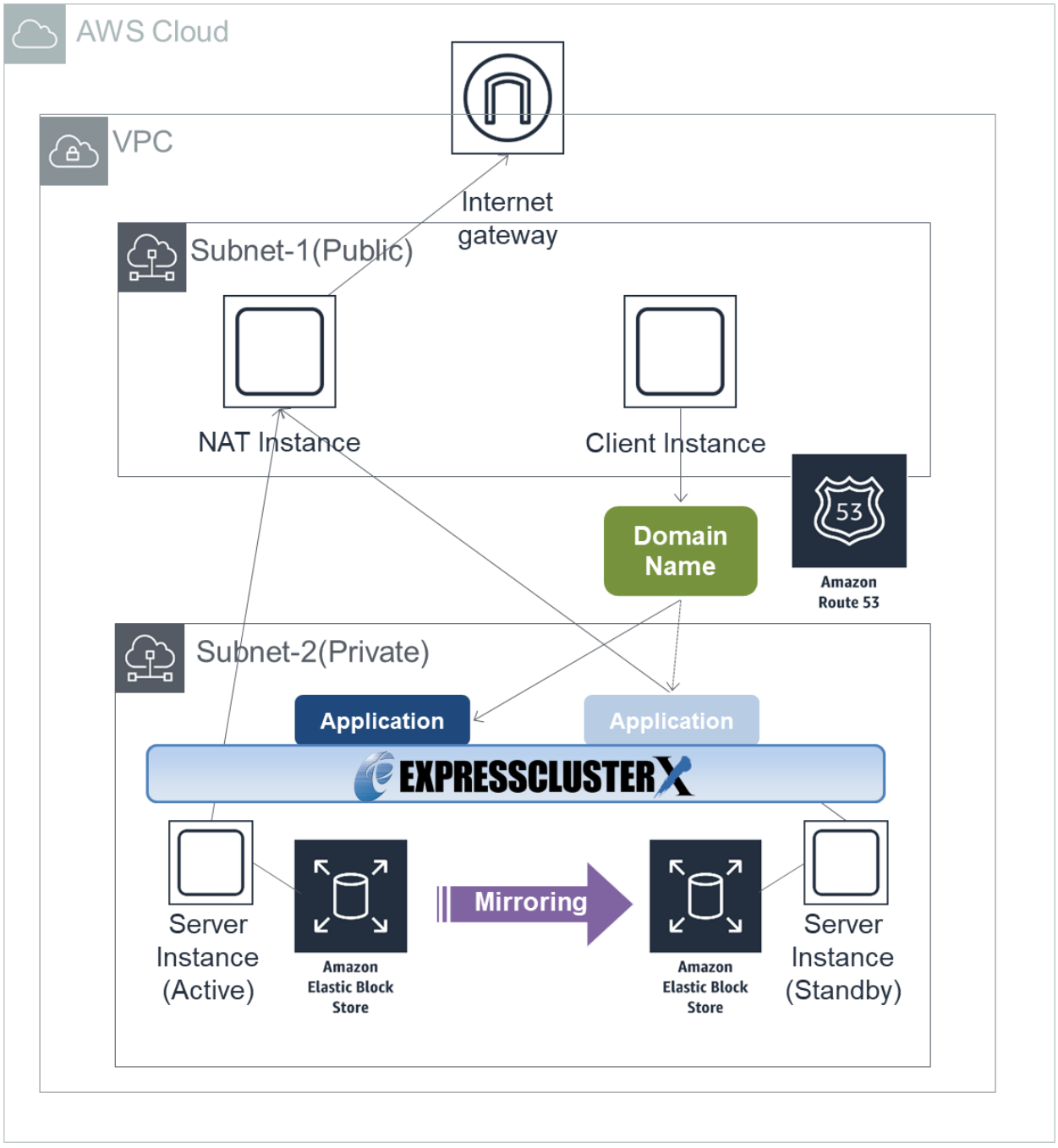
Set the timeout of the AWS CLI command to be executed for AWS Virtual IP resource activation/deactivation.

3.18 Understanding AWS DNS resources

3.18.1 Dependencies of AWS DNS resources

By default, this function does not depend on any group resource type.

3.18.2 What is an AWS DNS resource?



An AWS DNS resource registers an IP address corresponding to the virtual host name (DNS name) used in Amazon

Web Services (hereinafter, referred to as "AWS") by executing AWS CLI at activation, and deletes it by executing AWS CLI at deactivation.

A client can access the node on which failover groups are active with the virtual host name.

By using AWS DNS resources, clients do not need to be aware of switching access destination node when a failover occurs or moving a group migration.

An AWS Elastic IP resource, an AWS Virtual IP resource, and an AWS DNS resource can be used together.

If using AWS DNS resources, you need to take the following preparations before establishing a cluster.

- Creating Hosted Zone of Amazon Route 53
- Installing AWS CLI

3.18.3 Notes on AWS DNS resources

- In client access using a virtual host name (DNS name), if a failover group to which the AWS DNS resource is added resource is failed over, reconnection may be required.
- See "Setting up AWS DNS resources" in "Notes when creating EXPRESSCLUSTER configuration data" in Notes and Restrictions" in the "Getting Started Guide".

3.18.4 Applying environment variables to AWS CLI run from the AWS DNS resource

Specify environment variables in the environment variable configuration file to apply environment variables to the AWS CLI run from the AWS Elastic IP resource, AWS Virtual IP resource, AWS Elastic IP monitor resource and AWS AZ monitor resource.

This feature is useful when using a proxy server in an AWS environment.

The envirionment variable configuration file is stored in the following location.

<EXPRESSCLUSTER Installation path>/cloud/aws/clpaws_setting.conf

The format of the environment variable configuration file is as follows:

Envirionment variable name = Value

(Example)

```
[ENVIRONMENT]
HTTP_PROXY = http://10.0.0.1:3128
HTTPS_PROXY = http://10.0.0.1:3128
```

To specify multiple values for a parameter, enter them in comma-delimited format. The following shows an example of specifying more than one non-destination for the environment variable NO_PROXY:

(Example)

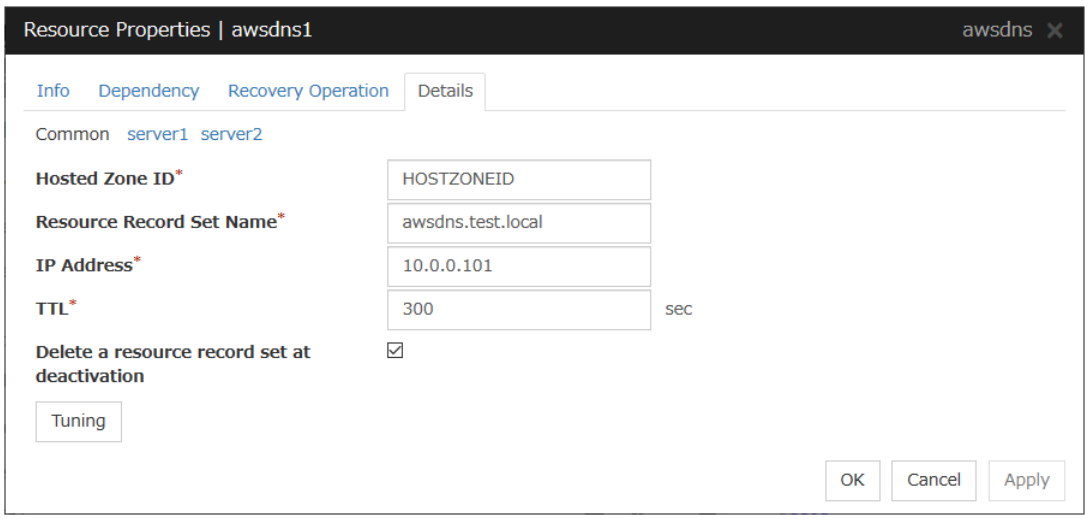
```
NO_PROXY = 169.254.169.254,ec2.ap-northeast-1.amazonaws.com
```

The specifications of the environment variable configuration file are as follows:

- Write [ENVIRONMENT] on the first line. If this is not set, the environment variables will not be set.
- If the environment variable configuration file does not exist or you do not have read permission for the file, the variables are ignored. This does not cause an activation failure or a monitor error.
- If the same environment variables already exist in the file, the values are overwritten.

- More than one environment variable can be set. Set one environment variable on each line.
- The settings are valid regardless of whether there are spaces before and after "=" or not.
- The settings are invalid if there is a space or tab in front of the environment variable name or if there are tabs before and after "=".
- Environment variable names are case sensitive.
- Even if a value contains spaces, you do not have to enclose the value in "" (double quotation marks).
- The environment variables configured with the environment variable configuration file are propagated only to the AWS CLI executed from an AWS Elastic IP resource, an AWS Virtual IP resource, an AWS DNS resource, an AWS Elastic IP monitor resource, an AWS Virtual IP monitor resource, an AWS DNS monitor resource, and an AWS AZ monitor resource. Therefore, the configured variables are not propagated to any other script (e.g. a script before final action, a script before and after activation/deactivation, and a script to be run from EXEC resources). To execute the AWS CLI with such a script, configure necessary environment variables with the corresponding script.

3.18.5 Details tab



Hosted Zone ID (within 255 bytes)

Specify a Hosted Zone ID of Amazon Route 53.

Resource Record Set Name (within 255 bytes)

Specify the name of DNS A record. Put a dot (.) at the end of the name. When an escape character is included in **Resource Record Set Name**, a monitor error occurs. Set **Resource Record Set Name** with no escape character. Specify the value of **Resource Record Set Name** in lowercase letters.

IP Address (within 39 bytes) `Server Individual Setup`

Specify the IP address corresponding to the virtual host name (DNS name) (IPv4). For using the IP address of each server, enter the IP address on the tab of each server. For configuring a setting for each server, enter the IP address of an arbitrary server on **Common** tab, and configure the individual settings for the other servers.

TTL (0 to 2147483647)

Specify the time to live (TTL) of the cache.

Delete a record set at deactivation

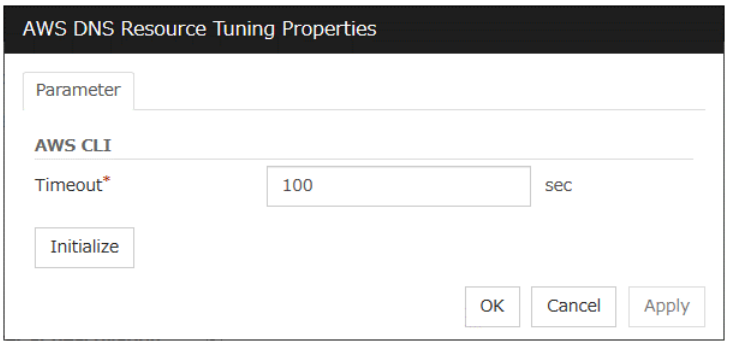
- When the check box is selected (default):
  The record set is delete when it is deactivated.
- When the check box is not selected:
  The record set is not deleted when it is deactivated. If it is not deleted, the remaining virtual host name (DNS name) may be accessed from a client.

Tuning

Opens the AWS DNS Resource Tuning Properties dialog box where you can make detailed settings for the AWS DNS resource.

AWS DNS Resource Tuning Properties

Parameter tab



Timeout (1 to 999)

Make the setting of the timeout of AWS CLI command executed for the activation and/or deactivation of the AWS DNS resource.

3.19 Understanding Azure probe port resources

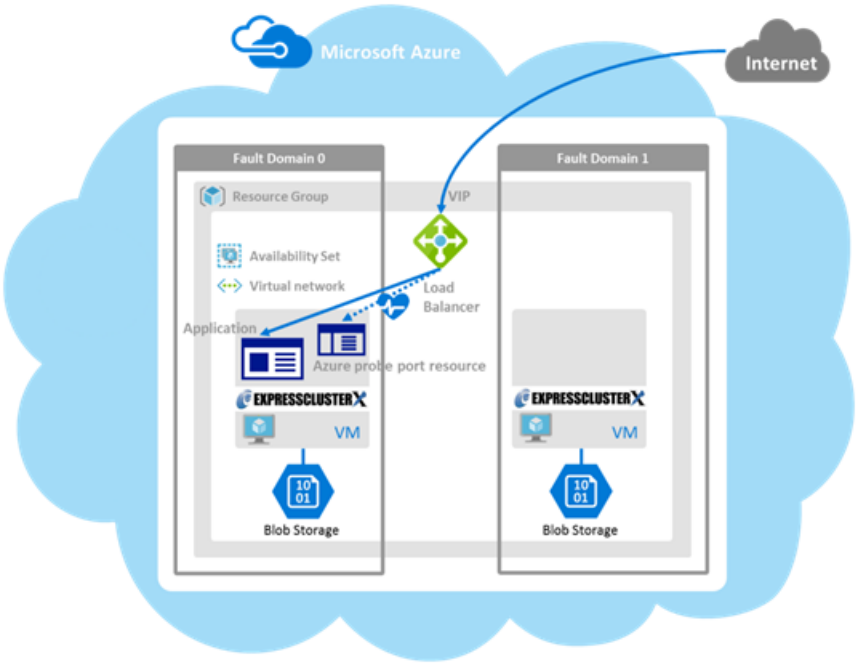
3.19.1 Dependencies of Azure probe port resources

By default, this function does not depend on any group resource type.

3.19.2 What is an Azure probe port resource?

Client applications can use the global IP address called a public virtual IP (VIP) address (referred to as a VIP in the remainder of this document) to access virtual machines on an availability set in the Microsoft Azure environment.

By using VIP, clients do not need to be aware of switching access destination server when a failover occurs or moving a group migration.

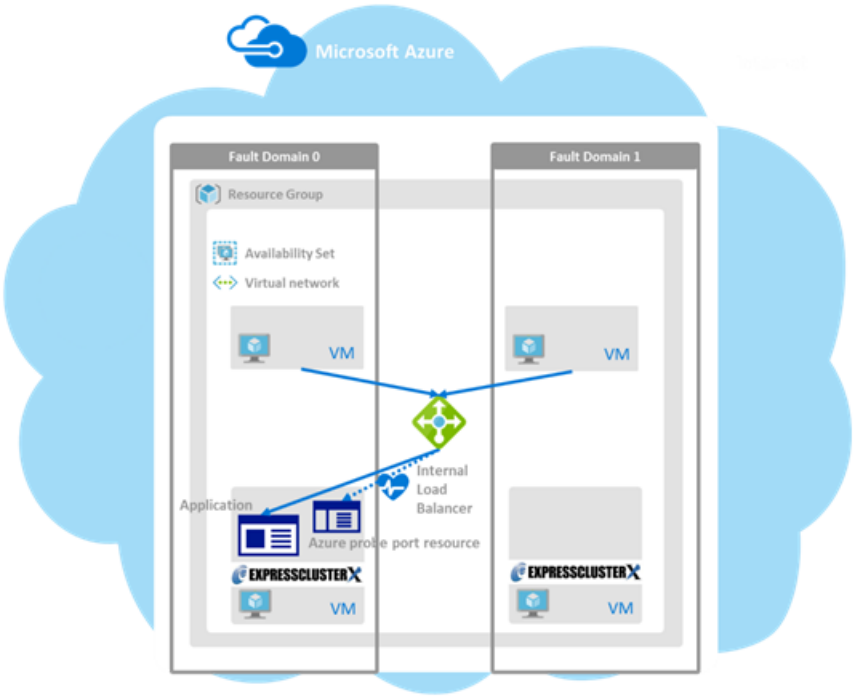


To access the cluster created on the Microsoft Azure environment in the figure above, specify the end point for communicating from the outside with VIP or the end point for communicating from the outside with the DNS name. The active and standby nodes of the cluster are switched by controlling the Microsoft Azure load balancer (Load Balancer in the figure above) from EXPRESSCLUSTER. For control, Health Check is used.

At activation, start the probe port control process for waiting for alive monitoring (access to the probe port) from the Azure load balancer.

At deactivation, stop the probe port control process for waiting for alive monitoring (access to the probe port).

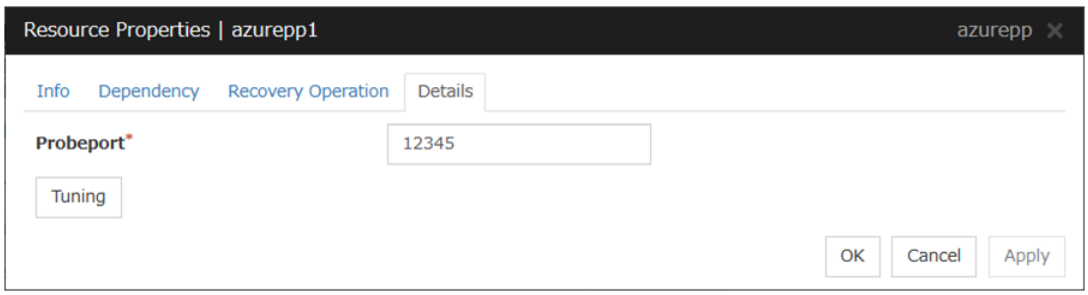
Azure probe port resources also support the Internal Load Balancing of Microsoft Azure. For Internal Load Balancing, the VIP is the private IP address of Azure.



3.19.3 Notes on Azure probe port resources

- If the private port and the probe port are the same, you need not add Azure probe port resources or Azure probe port monitor resources.
- Refer to "Azure probe port resource settings" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.19.4 Details tab



Probeport (1 to 65535)

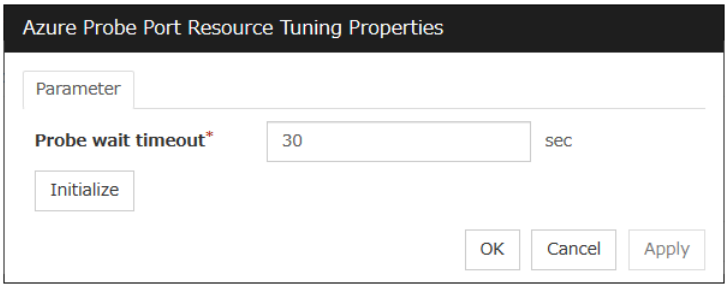
Specify the port number used by the Azure load balancer for the alive monitoring of each server. Specify the value specified for Probe Port when creating an end point. For Probe Protocol, specify TCP.

Tuning

Display the **Azure probe port Resource Tuning Properties** dialog box. Specify detailed settings for the Azure probe port resources.

Azure Probe Port Resource Tuning Properties

Parameter tab



Probe wait timeout (5 to 999999999)

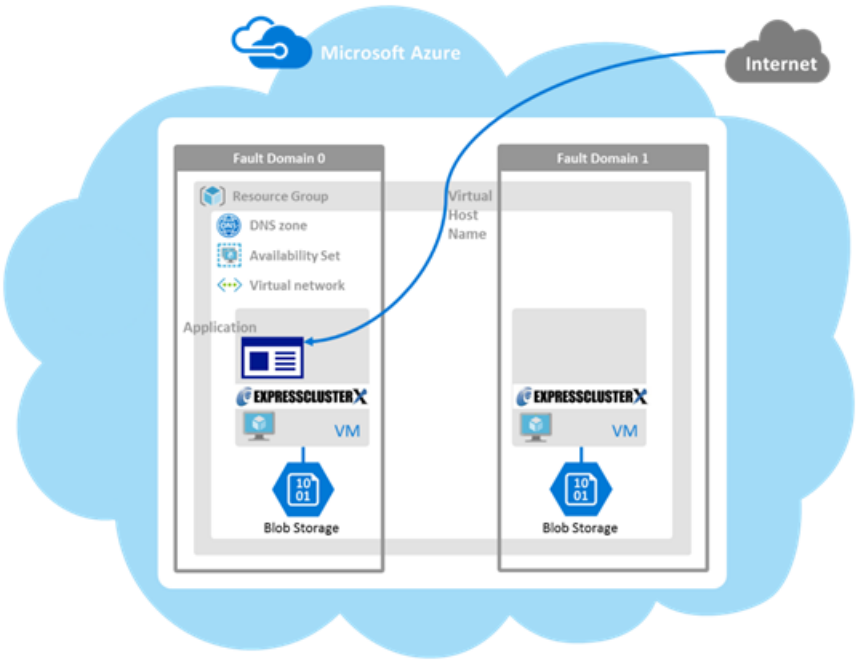
Specify the timeout time for waiting alive monitoring from the Azure load balancer. Check if alive monitoring is performed periodically from the Azure load balancer.

3.20 Understanding Azure DNS resources

3.20.1 Dependencies of Azure DNS resources

By default, this function does not depend on any group resource type.

3.20.2 What is an Azure DNS resource?



An Azure DNS resource controls an Azure DNS record set and DNS A record to obtain an IP address set from the virtual host name (DNS name).

A client can access the node on which failover groups are active with the virtual host name.

By using Azure DNS resources, clients do not need to be aware of switching access destination node on Azure DNS when a failover occurs or moving a group migration.

If using Azure DNS resources, you need to take the following preparations before establishing a cluster. For details, see "EXPRESSCLUSTER X HA Cluster Configuration Guide for Microsoft Azure (Linux)".

- Creating Microsoft Azure Resource Group and DNS zone
- Installing Azure CLI

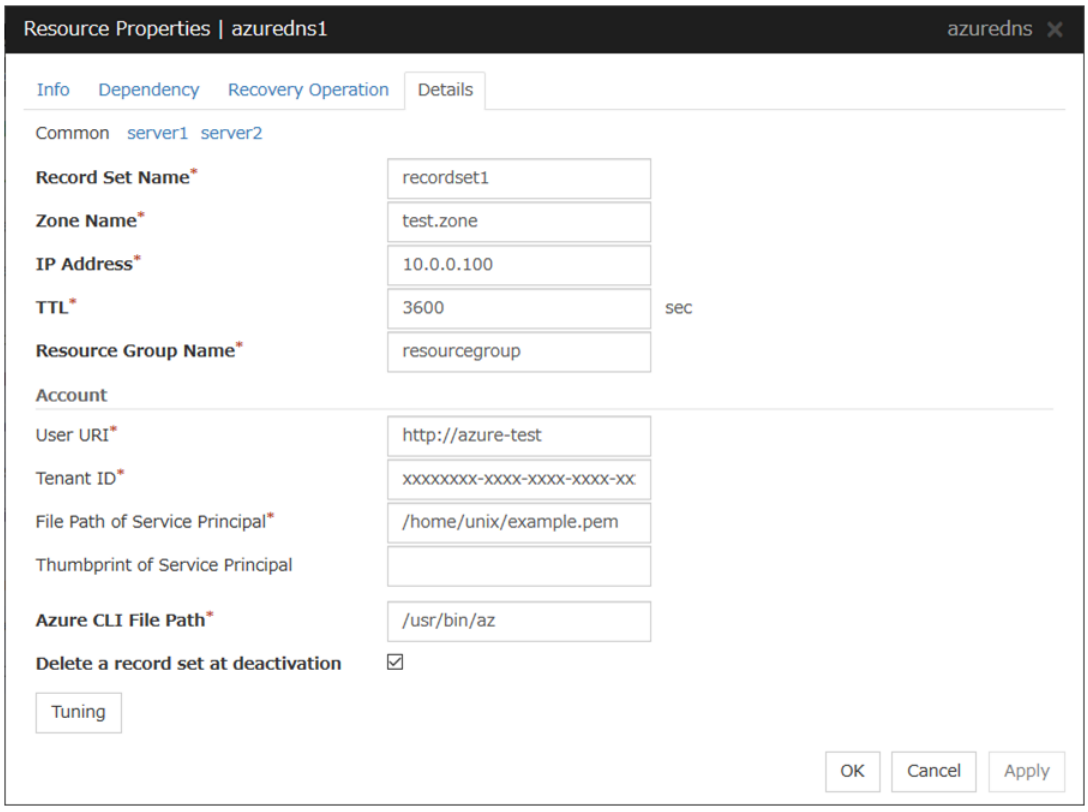
  Use Azure CLI (Azure CLI 1.0) for Red Hat Enterprise Linux 6 and OS with compatibility.

  Use Azure CLI (Azure CLI 2.0) for Red Hat Enterprise Linux 7 and OS with compatibility.
- Installing Python (only when Azure CLI 2.0 is used)

3.20.3 Notes on Azure DNS resources

- In client access using a virtual host name (DNS name), if a failover group to which the Azure DNS resource is added is failed over, reconnection may be required.
- See "Setting up Azure DNS resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- See "Azure DNS resources" in " Before installing EXPRESSCLUSTER" in "Notes and Restrictions" in the "Getting Started Guide".

3.20.4 Details tab



Record Set Name (within 253 bytes)

Specify the name of the record set in which Azure DNS A record is registered.

Zone Name (within 253 bytes)

Specify the name of the DNS zone to which the record set of Azure DNS belongs.

IP Address (within 39 bytes) `Server Individual Setup`

Specify the IP address corresponding to the virtual host name (DNS name) (IPv4). For using the IP address of each server, enter the IP address on the tab of each server. For configuring a setting for each server, enter the IP address of an arbitrary server on Common tab, and configure the individual settings for the other servers.

TTL (0 to 2147483647)

Specify the time to live (TTL) of the cache.

Resource Group Name (within 180 bytes)

Specify the name of Microsoft Azure Resource Group to which the DNS zone belongs.

User URI (within 2083 bytes)

Specify the user URI to log on to Microsoft Azure.

Tenant ID (within 36 bytes)

Specify the tenant ID to log on to Microsoft Azure.

File Path of Service Principal (within 1023 bytes)

Specify the file name of the service principal to log in to Microsoft Azure (file name of the credential. Specify with an absolute path.

Thumbprint of Service Principal (within 256 bytes)

Specify the service principal to log in to Microsoft Azure (Thumbprint on Certificate). Enter only when using Azure CLI 1.0.

Azure CLI File Path (within 1023 bytes)

Specify the installation path of Azure CLI and the file name. Specify with an absolute path.

Delete a record set at deactivation

- When the check box is selected (default):
  The record set is deleted when it is deactivated.
- When the check box is not selected:
  The record set is not deleted when it is deactivated. If it is not deleted, the remaining virtual host name (DNS name) may be accessed from a client.

Tuning

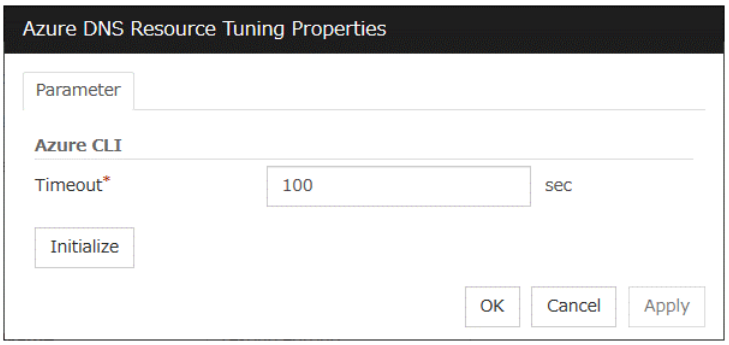
Opens the **AWS DNS Resource Tuning Properties** dialog box where you can make detailed settings for the Azure DNS resource.

Server separate setting

Opens the **Server Separate Setting** dialog box. An IP address different depending on servers is set.

Azure DNS Resource Tuning Properties

Parameter tab



Timeout (1 to 999)

Make the setting of the timeout of the Azure CLI command executed for the activation and/or deactivation of the Azure DNS resource.

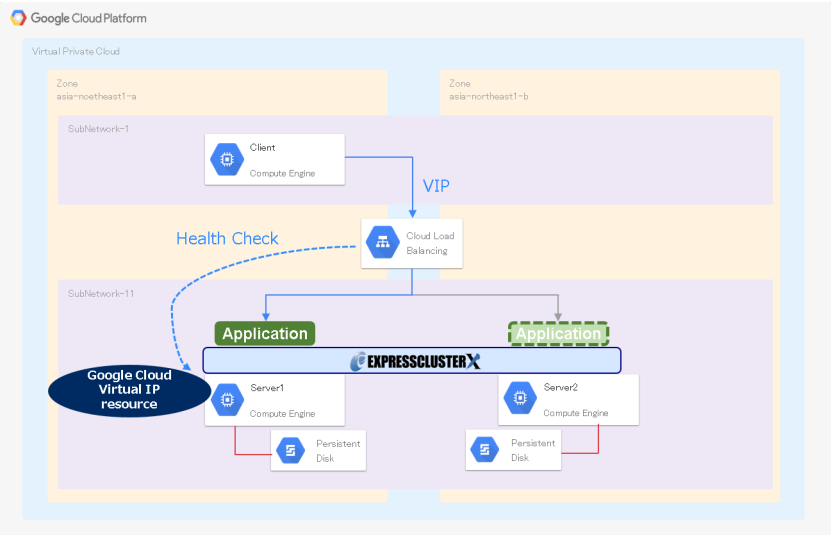
3.21 Understanding Google Cloud Virtual IP resources

3.21.1 Dependencies of Google Cloud Virtual IP resources

By default, this function does not depend on any group resource type.

3.21.2 What is an Google Cloud Virtual IP resource?

For virtual machines in the Google Cloud Platform environment, client applications can use a virtual IP (VIP) address to connect to the node that constitutes a cluster. Using the VIP address eliminates the need for clients to be aware of switching between the virtual machines even after a failover or a group migration occurs.



To access the cluster created in the Google Cloud Platform environment as in the figure above, specify the port for communicating from the outside as well as the VIP address or DNS name. The active and standby nodes of the cluster are switched by controlling the load balancer of Google Cloud Platform (Cloud Load Balancing in the figure above) from EXPRESSCLUSTER. For this control, Health Check (in the figure above) is used.

At activation, start the control process for awaiting a health check from the load balancer of Google Cloud Platform, and open the port specified in **Port Number**.

At deactivation, stop the control process for awaiting the health check, and close the port specified in **Port Number**.

Google Cloud virtual IP resources support the internal load balancing of Google Cloud Platform.

3.21.3 Notes on Google Cloud Virtual IP resources

- According to the GCP specification, External TCP Network Load Balancer requires legacy health checks using the HTTP protocol.

  Google Cloud Virtual IP resources only support health checks that use the TCP protocol and cannot respond to health checks from External TCP Network Load Balancer.

  Therefore, HA cluster using Google Cloud Virtual IP resources by External TCP Network Load Balancer cannot be used. Use an Internal TCP Load Balancer.

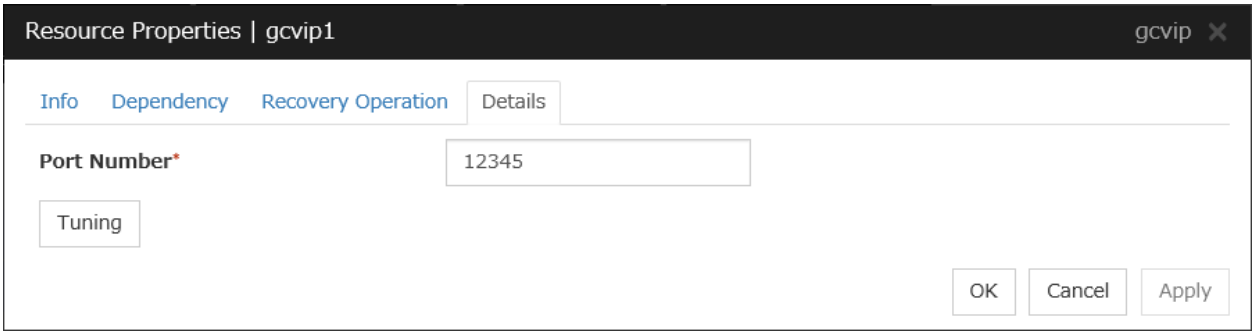
  Refer to the following.

  Health checks overview:

  https://cloud.google.com/load-balancing/docs/health-check-concepts/

- If the private port is the same as the health-check port, you need not add Google Cloud virtual IP resources or Google Cloud virtual IP monitor resources.
- Refer to "Getting Started Guide" -> "Notes and Restrictions" -> "Notes when creating EXPRESSCLUSTER configuration data" -> "Setting up Google Cloud Virtual IP resources".

3.21.4 Details tab



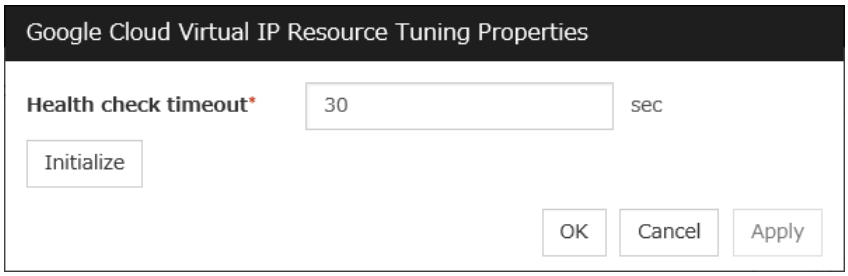
Port Number (1 to 65535)

Specify a port number to be used by the load balancer of Google Cloud Platform for the health check of each node: the value specified as the port number in configuring the load balancer for health checks. For the load balancer, specify **TCP load balancing**.

Tuning

Displays the **Google Cloud Virtual IP Resource Tuning Properties** dialog box, where you can make advanced settings for the Google Cloud virtual IP resource.

Google Cloud Virtual IP Resource Tuning Properties



Health check timeout (5 to 999999999)**

Specify a timeout value for awaiting a health check from the load balancer of Google Cloud Platform, in order to check whether the load balancer periodically performs health checks.

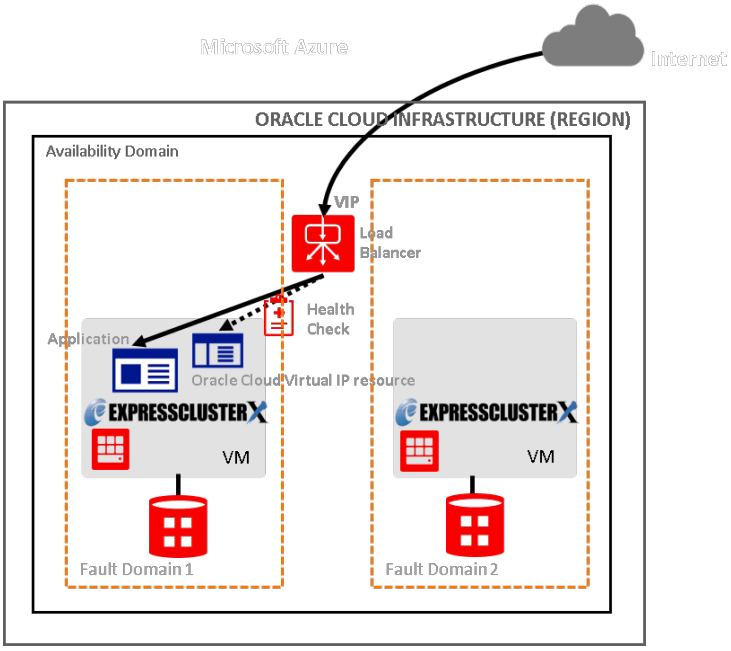
3.22 Understanding Oracle Cloud Virtual IP resources

3.22.1 Dependencies of Oracle Cloud Virtual IP resources

By default, this function does not depend on any group resource type.

3.22.2 What is an Oracle Cloud Virtual IP resource?

For virtual machines in the Oracle Cloud Infrastructure environment, client applications can use a public virtual IP (VIP) address to connect to the node that constitutes a cluster. Using the VIP address eliminates the need for clients to be aware of switching between the virtual machines even after a failover or a group migration occurs.

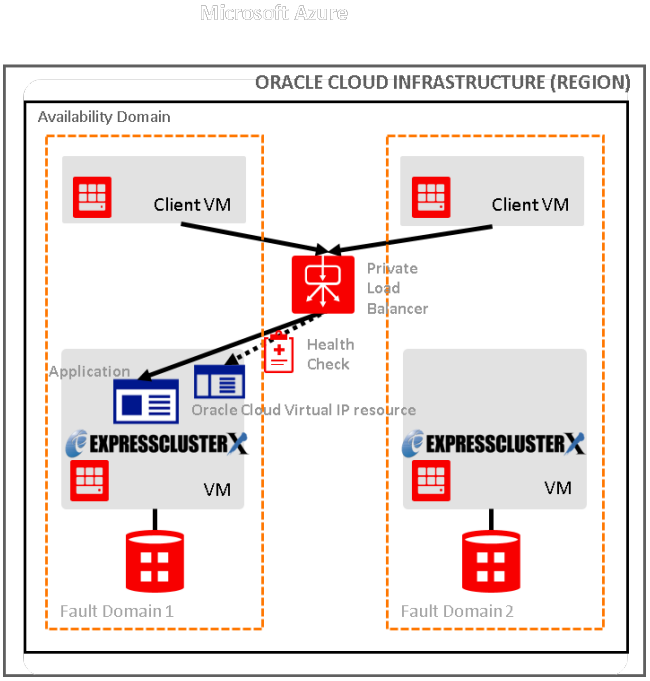


To access the cluster created in the Oracle Cloud Infrastructure environment as in the figure above, specify the port for communicating from the outside as well as the VIP (global IP) address or DNS name. The active and standby nodes of the cluster are switched by controlling the load balancer of Oracle Cloud Infrastructure (Load Balancer in the figure above) from EXPRESSCLUSTER. For this control, Health Check (in the figure above) is used.

At activation, start the control process for awaiting a health check from the load balancer of Oracle Cloud Infrastructure, and open the port specified in **Port Number**.

At deactivation, stop the control process for awaiting the health check, and close the port specified in **Port Number**.

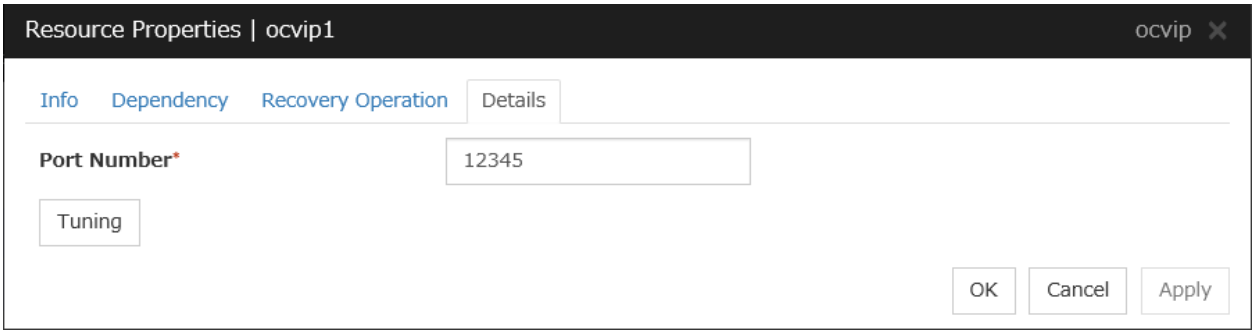
Oracle Cloud virtual IP resources also support private load balancers of Oracle Cloud Infrastructure. For a private load balancer, the VIP address is the private IP address of Oracle Cloud Infrastructure.



3.22.3 Notes on Oracle Cloud Virtual IP resources

- If the private port is the same as the health-check port, you need not add Oracle Cloud virtual IP resources or Oracle Cloud virtual IP monitor resources.
- Refer to "Getting Started Guide" -> "Notes and Restrictions" -> "Notes when creating EXPRESSCLUSTER configuration data" -> "Setting up Oracle Cloud Virtual IP resources".

3.22.4 Details tab



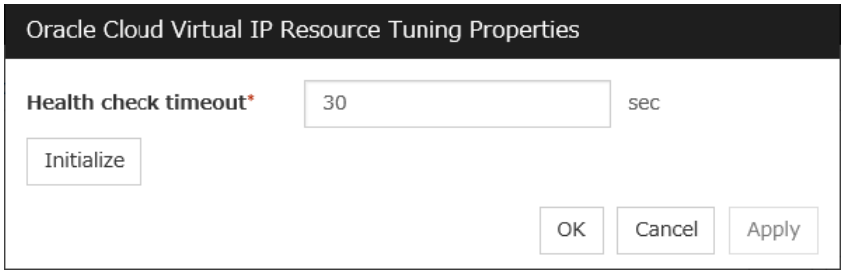
Port Number (1 to 65535)

Specify a port number to be used by the load balancer of Oracle Cloud Infrastructure for the health check of each node: the value specified as the port number in configuring the backend set for health checks. For the health check protocol, specify TCP.

Tuning

Displays the **Oracle Cloud Virtual IP Resource Tuning Properties** dialog box, where you can make advanced settings for the Oracle Cloud virtual IP resource.

Oracle Cloud Virtual IP Resource Tuning Properties



Health check timeout (5 to 999999999)**

Specify a timeout value for awaiting a health check from the load balancer of Oracle Cloud Infrastructure, in order to check whether the load balancer periodically performs health checks.

CHAPTER

FOUR

MONITOR RESOURCE DETAILS

This chapter provides detailed information on monitor resources. Monitor resource is a unit to perform monitoring.

This chapter covers:

- 4.1. *Monitor resource*
- 4.2. *Monitor resource properties*
- 4.3. *Understanding the disk monitor resources*
- 4.4. *Understanding IP monitor resources*
- 4.5. *Understanding floating IP monitor resources*
- 4.6. *Understanding NIC Link Up/Down monitor resources*
- 4.7. *Understanding mirror disk connect monitor resources*
- 4.8. *Understanding mirror disk monitor resources*
- 4.9. *Understanding hybrid disk connect monitor resources*
- 4.10. *Understanding hybrid disk monitor resources*
- 4.11. *Understanding PID monitor resources*
- 4.12. *Understanding User mode monitor resources*
- 4.13. *Understanding multi target monitor resources*
- 4.14. *Understanding virtual IP monitor resources*
- 4.15. *Understanding ARP monitor resources*
- 4.16. *Understanding custom monitor resources*
- 4.17. *Understanding volume manager monitor resources*
- 4.18. *Understanding message receive monitor resources*
- 4.19. *Understanding VM monitor resources*
- 4.20. *Understanding Dynamic DNS monitor resources*
- 4.21. *Understanding process name monitor resources*
- 4.22. *Understanding BMC monitor resources*
- 4.23. *Understanding DB2 monitor resources*
- 4.24. *Understanding FTP monitor resources*
- 4.25. *Understanding HTTP monitor resources*

- 4.26. *Understanding IMAP4 monitor resources*
- 4.27. *Understanding MySQL monitor resources*
- 4.28. *Understanding NFS monitor resources*
- 4.29. *Understanding ODBC monitor resources*
- 4.30. *Understanding Oracle monitor resources*
- 4.31. *Understanding Oracle Clusterware Synchronization Management monitor resources*
- 4.32. *Understanding POP3 monitor resources*
- 4.33. *Understanding PostgreSQL monitor resources*
- 4.34. *Understanding Samba monitor resources*
- 4.35. *Understanding SMTP monitor resources*
- 4.36. *Understanding SQL Server monitor resources*
- 4.37. *Understanding Sybase monitor resources*
- 4.38. *Understanding Tuxedo monitor resources*
- 4.39. *Understanding Weblogic monitor resources*
- 4.40. *Understanding Websphere monitor resources*
- 4.41. *Understanding WebOTX monitor resources*
- 4.42. *Understanding JVM monitor resources*
- 4.43. *Understanding System monitor resources*
- 4.44. *Understanding Process resource monitor resources*
- 4.45. *Understanding AWS Elastic IP monitor resources*
- 4.46. *Understanding AWS Virtual IP monitor resources*
- 4.47. *Understanding AWS AZ monitor resources*
- 4.48. *Understanding AWS DNS monitor resources*
- 4.49. *Understanding Azure probe port monitor resources*
- 4.50. *Understanding Azure load balance monitor resources*
- 4.51. *Understanding Azure DNS monitor resources*
- 4.52. *Understanding Google Cloud Virtual IP monitor resources*
- 4.53. *Understanding Google Cloud load balance monitor resources*
- 4.54. *Understanding Oracle Cloud Virtual IP monitor resources*
- 4.55. *Understanding Oracle Cloud load balance monitor resources*

4.1 Monitor resource

A monitor resource refers to a resource that monitors a specified target to be monitored. When detecting an error in a target to be monitored, a monitor resource restarts a group resource and/or executes failover.

Currently supported monitor resources:

Monitor resource name	Abbreviation	Functional overview	Supported version
Disk Monitor Resrource	diskw	See "*Understanding the disk monitor resources*".	4.0.0-1 or later
IP Monitor Resource	ipw	See "*Understanding IP monitor resources*".	4.0.0-1 or later
Floating IP Monitor Resource	fipw	See "*Understanding floating IP monitor resources*".	4.0.0-1 or later
NIC Link Up/Down Monitor Resource	miiw	See "*Understanding NIC Link Up/Down monitor resources*".	4.0.0-1 or later
Mirror Disk Connect Monitor Resource	mdnw	See " *Understanding mirror disk connect monitor resources* ".	4.0.0-1 or later
Mirror Disk Monitor Resource	mdw	See "*Understanding mirror disk monitor resources*".	4.0.0-1 or later
Hybrid Disk Connect Monitor Resource	hdnw	See "*Understanding hybrid disk connect monitor resources*".	4.0.0-1 or later
Hybrid Disk Monitor Resource	hdw	See "*Understanding hybrid disk monitor resources*".	4.0.0-1 or later
PID Monitor Resource	pidw	See "*Understanding PID monitor resources* ".	4.0.0-1 or later
User-Mode Monitor Resource	userw	See "*Understanding User mode monitor resources*".	4.0.0-1 or later
Multi Target Monitor Resource	mtw	See "*Understanding multi target monitor resources*".	4.0.0-1 or later
Virtual IP Monitor Resource	vipw	See "*Understanding virtual IP monitor resources*".	4.0.0-1 or later
ARP Monitor Resource	arpw	See "*Understanding ARP monitor resources*".	4.0.0-1 or later
Custom Monitor Resource	genw	See "*Understanding custom monitor resources*".	4.0.0-1 or later
Volume Manager Monitor Resource	volmgrw	See "*Understanding volume manager monitor resources*".	4.0.0-1 or later
Message Receive Monitor Resource	mrw	See "*Understanding message receive monitor resources*".	4.0.0-1 or later
VM Monitor Resource	vmw	See "*Understanding VM monitor resources*".	4.0.0-1 or later
Dynamic DNS Monitor Resource	ddns	See "*Understanding Dynamic DNS monitor resources*".	4.0.0-1 or later
Process Name Monitor Resource	psw	See "*Understanding process name monitor resources*".	4.0.0-1 or later
BMC Monitor Resource	bmcw	See "*Understanding BMC monitor resources*".	4.0.0-1 or later
DB2 Monitor Resource[1]	db2w	See "*Understanding DB2 monitor resources*".	4.0.0-1 or later
FTP Monitor Resource[1]	ftpw	See "*Understanding FTP monitor resources*".	4.0.0-1 or later

Continued on next page

Table 4.1 – continued from previous page

Monitor resource name	Abbreviation	Functional overview	Supported version
HTTP Monitor Resource[1]	httpw	See "*Understanding HTTP monitor resources*".	4.0.0-1 or later
IMAP4 Monitor Resource[1]	imap4w	See "*Understanding IMAP4 monitor resources*".	4.0.0-1 or later
MySQL Monitor Resource[1]	mysqlw	See "*Understanding MySQL monitor resources*".	4.0.0-1 or later
NFS Monitor Resource[1]	nfsw	See "*Understanding NFS monitor resources*".	4.0.0-1 or later
ODBC Monitor Resource[1]	odbcw	See "*Understanding ODBC monitor resources*".	4.0.0-1 or later
Oracle Monitor Resource	oraclew	See "*Understanding Oracle monitor resources*".	4.0.0-1 or later
Oracle Clusterware Synchronization Management Monitor Resource	osmw	See "*Understanding Oracle Clusterware Synchronization Management monitor resources*".	4.0.0-1 or later
POP3 Monitor Resource[1]	pop3w	See "*Understanding POP3 monitor resources*".	4.0.0-1 or later
PostgreSQL Monitor Resource[1]	psqlw	See "*Understanding PostgreSQL monitor resources*".	4.0.0-1 or later
Samba Monitor Resource[1]	sambaw	See "*Understanding Samba monitor resources*".	4.0.0-1 or later
SMTP Monitor Resource[1]	smtpw	See "*Understanding SMTP monitor resources*".	4.0.0-1 or later
SQL Server Monitor Resource[1]	sqlserverw	See "*Understanding SQL Server monitor resources*".	4.0.0-1 or later
Sybase Monitor Resource[1]	sybasew	See "*Understanding Sybase monitor resources*".	4.0.0-1 or later
Tuxedo Monitor Resource[1]	tuxw	See "*Understanding Tuxedo monitor resources*".	4.0.0-1 or later
Weblogic Monitor Resource[1]	wlsw	See "*Understanding Weblogic monitor resources*".	4.0.0-1 or later
Websphere Monitor Resource[1]	wasw	See "*Understanding Websphere monitor resources*".	4.0.0-1 or later
WebOTX Monitor Resource[1]	otxw	See "*Understanding WebOTX monitor resources*".	4.0.0-1 or later
JVM Monitor Resource[1]	jraw	See "*Understanding JVM monitor resources*".	4.0.0-1 or later
System Monitor Resource[1]	sraw	See "*Understanding System monitor resources*".	4.0.0-1 or later
Process Resource Monitor Resource[1]	psrw	See "*Understanding Process resource monitor resources*".	4.1.0-1 or later
AWS Elastic IP Monitor Resource	awseipw	See "*Understanding AWS Elastic IP monitor resources*".	4.0.0-1 or later
AWS Virtual IP Monitor Resource	awsvipw	See "*Understanding AWS Virtual IP monitor resources*".	4.0.0-1 or later
AWS AZ Monitor Resource	awsazw	See "*Understanding AWS AZ monitor resources*".	4.0.0-1 or later
AWS DNS Monitor Resource	awsdnsw	See "*Understanding AWS DNS monitor resources*".	4.0.0-1 or later

Continued on next page

Table 4.1 – continued from previous page

Monitor resource name	Abbreviation	Functional overview	Supported version
Azure Probe Port Monitor Resource	azureppw	See "*Understanding Azure probe port monitor resources*".	4.0.0-1 or later
Azure Load Balance Monitor Resource	azurelbw	See "*Understanding Azure load balance monitor resources*".	4.0.0-1 or later
Azure DNS Monitor Resource	azurednsw	See "*Understanding Azure DNS monitor resources*".	4.0.0-1 or later
Google Cloud Virtual IP Monitor Resource	gcvipw	See "*Understanding Google Cloud Virtual IP monitor resources*".	4.2.0-1~
Google Cloud Load Balance Monitor Resource	gclbw	See "*Understanding Google Cloud load balance monitor resources*".	4.2.0-1~
Oracle Cloud Virtual IP Monitor Resource	ocvipw	See "*Understanding Oracle Cloud Virtual IP monitor resources*".	4.2.0-1~
Oracle Cloud Load Balance Monitor Resource	oclbw	See "*Understanding Oracle Cloud load balance monitor resources*".	4.2.0-1~

4.1.1 Status of monitor resources after monitoring starts

The status of some monitor resources might be "Caution" if there is a period of time following the start of monitoring in which monitoring of that resource is not yet ready.

Caution status is possible for the following monitor resources.

Dynamic DNS Monitor Resource
Message Receive Monitor Resource
Custom Monitor Resource (whose monitor type is **Asynchronous**)
Virtual IP Monitor Resource
DB2 Monitor Resource
BMC Monitor Resource
System Monitor Resource
Process Resource Monitor Resource
JVM Monitor Resource
MySQL Monitor Resource
ODBC Monitor Resource
Oracle Monitor Resource
Oracle Clusterware Synchronization Management Monitor Resource
PostgresSQL Monitor Resource
Process Name Monitor Resource
SQL Server Monitor Resource
Sybase Monitor Resource

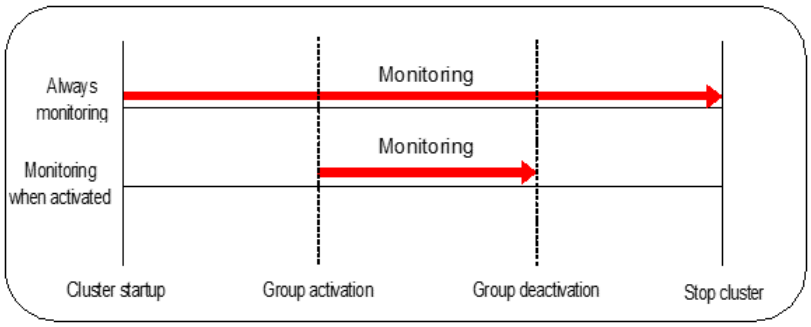
[1] To use this monitor resource, you need to register a license. For details on how to register a license, see the "Installation and Configuration Guide".

4.1.2 Monitor timing of monitor resource

There are two types of monitoring by monitor resources; **Always** and **Active**.

The monitoring timing differs depending on monitor resources:

- Always:
  Monitoring is performed by monitor resource all the time.
- Active:
  Monitoring is performed by monitor recourse while specified group resource is active. Monitor resource does not monitor while group resource is not activated.



Monitor resource	Monitor timing	Target resource
Disk Monitor Resource	Always or when activated	All
IP Monitor Resource	Always or when activated	All
User-Mode Monitor Resource	Always (Fixed)	-
Mirror Disk Monitor Resource	Always (Fixed)	-
Mirror Disk Connect Monitor Resource	Always (Fixed)	-
Hybrid Disk Monitor Resource	Always (Fixed)	-
Hybrid Disk Connect Monitor Resource	Always (Fixed)	-
NIC Link Up/Down Monitor resource	Always or when activated	All
PID Monitor resource	Fixed to while activating	exec
Multi Target Monitor Resource	Always or when activated	All
Virtual IP Monitor Resource	When activated (Fixed)	vip
ARP Monitor Resource	When activated (Fixed)	fip, vip
Custom Monitor resource	Always or when activated	All
VM Monitor Resource	Always (Fixed)	vm
Message Receive Monitor Resource	Always or when activated	mrw
Volume Manager Monitor Resource	Always or when activated	volmgr
Dynamic DNS Monitor Resource	Always (Fixed)	ddns
Process Name Monitor Resource	Always or when activated	All
BMC Monitor Resource	Always (Fixed)	-
DB2 Monitor Resource	When activated (Fixed)	exec
FTP Monitor Resource	Always or when activated	exec
HTTP Monitor Resource	Always or when activated	exec
IMAP4 Monitor Resource	Always or when activated	exec
MySQL Monitor Resource	When activated (Fixed)	exec
NFS Monitor Resource	Always or when activated	exec
ODBC Monitor Resource	When activated (Fixed)	exec
Oracle Monitor Resource	When activated (Fixed)	exec

Continued on next page

Table 4.2 – continued from previous page

Monitor resource	Monitor timing	Target resource
Oracle Clusterware Synchronization Management Monitor Resource	Always (Fixed)	-
POP3 Monitor Resource	When activated (Fixed)	exec
PostgreSQL Monitor Resource	When activated (Fixed)	exec
Samba Monitor Resource	Always or when activated	exec
SMTP Monitor Resource	Always or when activated	exec
SQL Server Monitor Resource	When activated (Fixed)	exec
Sybase Monitor Resource	When activated (Fixed)	exec
Tuxedo Monitor Resource	Always or when activated	exec
Weblogic Monitor Resource	Always or when activated	exec
Websphere Monitor Resource	Always or when activated	exec
WebOTX Monitor Resource	Always or when activated	exec
JVM Monitor Resource	Always or when activated	exec
System Monitor Resource	Always (Fixed)	All
Process Resource Monitor Resource	Always (Fixed)	All
Floating IP Monitor Resource	When activated (Fixed)	fip
AWS Elastic IP Monitor resource	When activated (Fixed)	awseip
AWS Virtual IP Monitor resource	When activated (Fixed)	awsvip
AWS AZ Monitor resource	Always (Fixed)	-
AWS DNS Monitor resource	When activated (Fixed)	awsdns
Azure probe port monitor resource	When activated (Fixed)	azurepp
Azure load balance monitor resource	Always (Fixed)	azurepp
Azure DNS Monitor resource	When activated (Fixed)	azuredns
Google Cloud Virtual IP monitor resource	When activated (Fixed)	gcvip
Google Cloud load balance monitor resource	Always (Fixed)	gcvip
Oracle Cloud Virtual IP monitor resource	When activated (Fixed)	ocvip
Oracle Cloud load balance monitor resource	Always (Fixed)	ocvip

4.1.3 Suspending and resuming monitoring on monitor resources

Monitor resource can temporarily suspend monitoring and resume it.
Monitoring can be suspended and resumed by the following two methods:

- Operation on the Cluster WebUI
- Operation by the clpmonctrl command
  The clpmonctrl command can control monitor resources on a server where the command is run or on a specified server.

Some monitor resources can suspend and resume monitoring and others cannot. For details, see the list below.

Monitor Resource	**Control**
Disk Monitor Resource	Possible
IP Monitor Resource	Possible
User-mode Monitor Resource	Possible
Mirror Disk Monitor Resource	Possible
Mirror Disk Connect Monitor Resource	Possible
Hybrid Disk Monitor Resource	Possible

Continued on next page

Table 4.3 – continued from previous page

Monitor Resource	Control
Hybrid Disk Connect Monitor Resource	Possible
NIC Link Up/Down Monitor Resource	Possible
PID Monitor Resource	Possible
Multi Target Monitor Resource	Possible
Virtual IP Monitor Resource	Impossible
ARP Monitor Resource	Impossible
Custom Monitor Resource	Possible
VM Monitor Resource	Possible
Message Receive Monitor Resource	Possible
Volume Manager Monitor Resource	Possible
Dynamic DNS Monitor Resource	Impossible
Process Name Monitor Resource	Possible
BMC Monitor Resource	Possible
DB2 Monitor Resource	Possible
FTP Monitor Resource	Possible
HTTP Monitor Resource	Possible
IMAP4 Monitor Resource	Possible
MySQL Monitor Resource	Possible
NFS Monitor Resource	Possible
ODBC Monitor Resource	Possible
Oracle Monitor Resource	Possible
Oracle Clusterware Synchronization Management Monitor Resource	Possible
POP3 Monitor Resource	Possible
PostgreSQL Monitor Resource	Possible
Samba Monitor Resource	Possible
SMTP Monitor Resource	Possible
SQl Server Monitor Resource	Possible
Sybase Monitor Resource	Possible
Tuxedo Monitor Resource	Possible
Websphere Monitor Resource	Possible
Weblogic Monitor Resource	Possible
WebOTX Monitor Resource	Possible
JVM Monitor Resource	Possible
System Monitor Resource	Possible
Process Resource Monitor Resource	Possible
Floating IP Monitor Resource	Possible
AWS Elastic IP Monitor resource	Possible
AWS Virtual IP Monitor resource	Possible
AWS AZ Monitor resource	Possible
AWS DNS Monitor resource	Possible
Azure probe port monitor resource	Possible
Azure load balance monitor resource	Possible
Azure DNS Monitor resource	Possible
Google Cloud Virtual IP monitor resource	Possible
Google Cloud load balance monitor resource	Possible
Oracle Cloud Virtual IP monitor resource	Possible
Oracle Cloud load balance monitor resource	Possible

On the Cluster WebUI, shortcut menus of the monitor resources which cannot control monitoring are disabled. The clpmonctrl command only controls the resources which can control monitoring. For monitor resources which cannot

control monitoring, a warning message is displayed and controls are not performed.

Suspending monitoring on a monitor resource is disabled if one of the following operations is performed.

- Resume operation on Cluster WebUI
- Resume operation by using the clpmonctrl command
- Stop the cluster
- Suspend the cluster

4.1.4 Enabling and disabling dummy failure of monitor resources

You can enable and disable dummy failure of monitor resources. Use one of the following methods to enable or disable dummy failure.

- Operation on Cluster WebUI (verification mode)
  On the Cluster WebUI (verification mode), shortcut menus of the monitor resources which cannot control monitoring are disabled.
- Operation by using the clpmonctrl command
  The clpmonctrl command can control the server where this command is run or the monitor resources of the specified server. When the clpmonctrl command is executed on monitor resource which cannot be controlled, dummy failure is not enabled even though the command succeeds.

Some monitor resources can enable and disable dummy failure and others cannot.
For details, see "*Controlling monitor resources (clpmonctrl command)*" in "8. *EXPRESSCLUSTER command reference*" in this guide.

Dummy failure of a monitor resource is disabled if the following operations are performed.

- Dummy failure was disabled on Cluster WebUI (verification mode)
- "Yes" was selected from the dialog box displayed when the Cluster WebUI mode changes from verification mode to a different mode.
- -n was specified to enable dummy failure by using the clpmonctrl command
- Stop the cluster
- Suspend the cluster

4.1.5 Monitoring interval for monitor resource

All monitor resources except the user-mode monitor resource monitors their targets at every monitor interval.

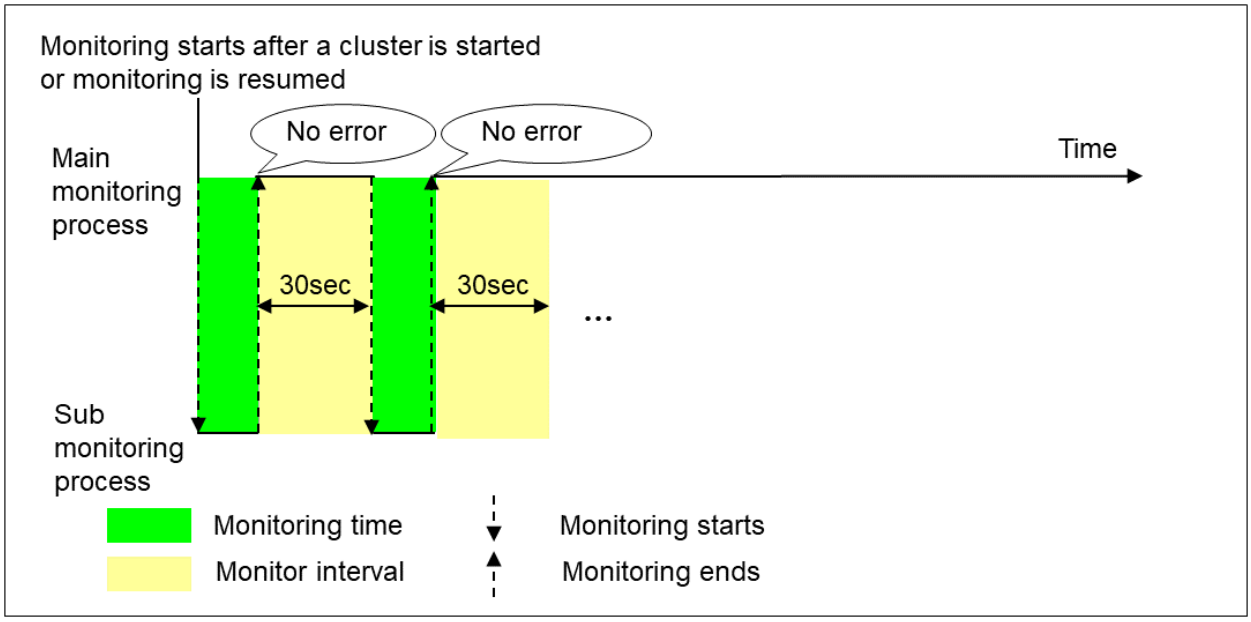
The following illustrates the timeline of how a monitor resource monitors its target and finds error/no error with the configuration below:

When no error is detected

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec

Monitor Timeout 60 sec
Monitor Retry Count 0 times

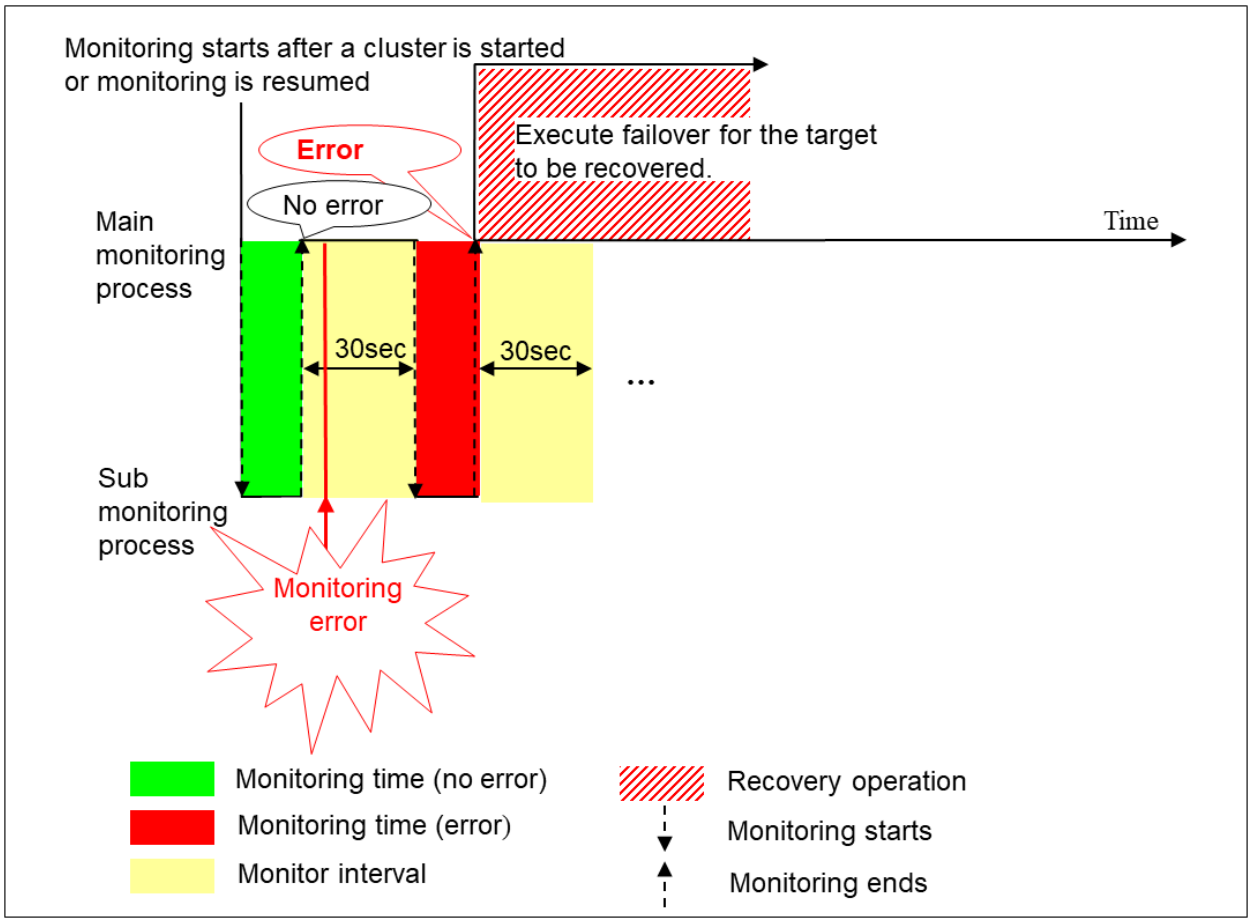


When an error is detected (without monitor retry setting)

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry count 0 times

<Error detection>
Recovery Target group
Recovery Script Execution Count 0 times
Maximum Reactivation Count 0 times
Maximum Failover Count 1 time
Final Action None



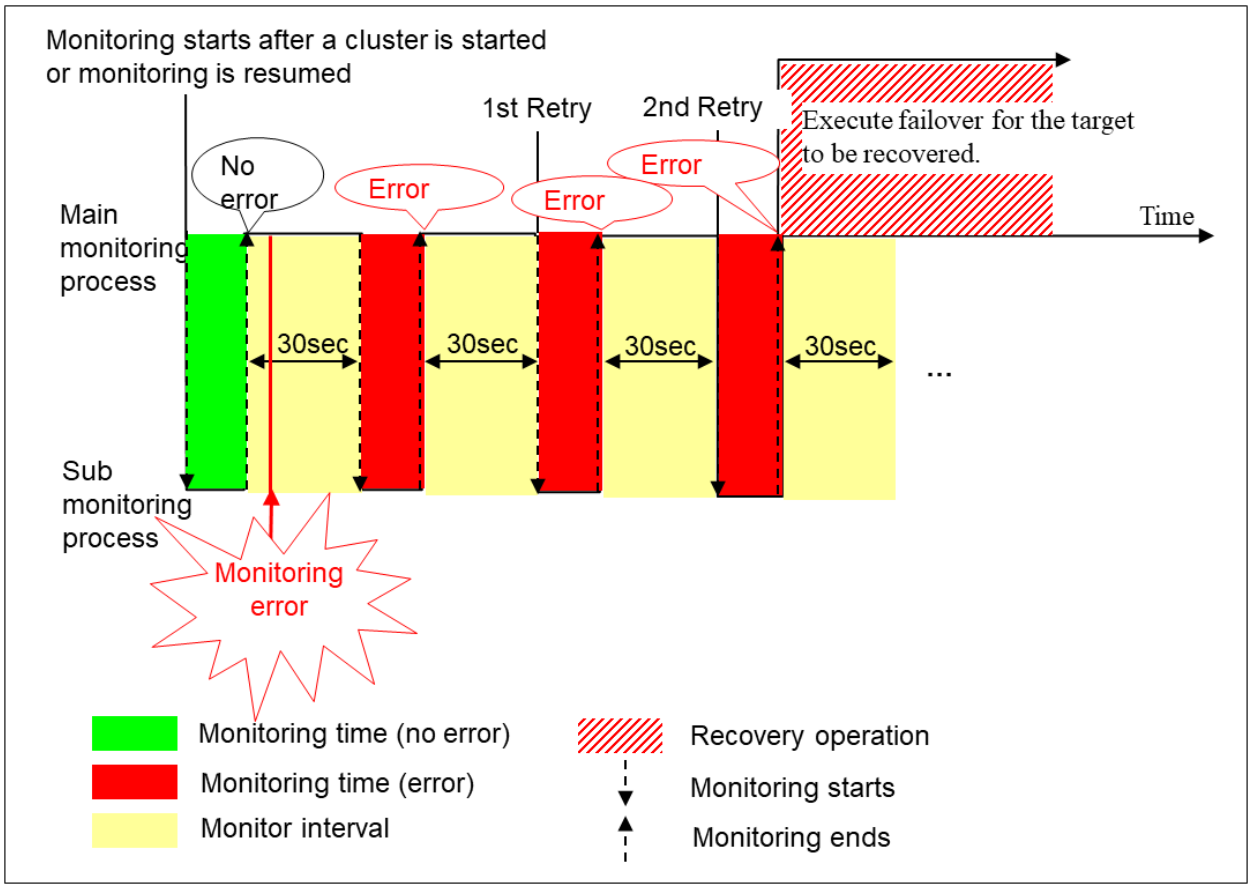
When an error occurs, it is detected at the next monitoring and the recovery operation for the recovery target starts.

When an error is detected (with monitor retry settings)

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 2 times

<Error detection>
Recovery Target group
Recovery Script Execution Count 0 times
Maximum Reactivation Count 0 times
Maximum Failover Count 1 time
Final Action None



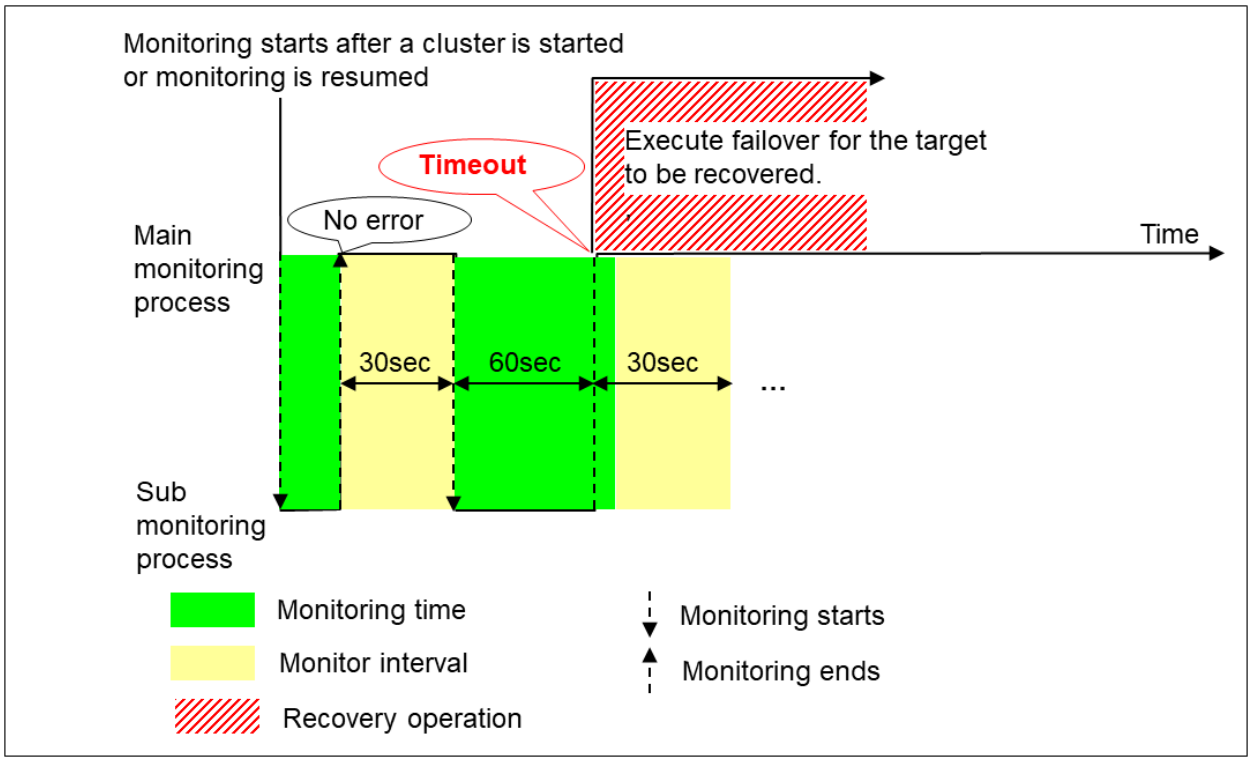
When an error occurs, it is detected at the next monitoring. If recovery cannot be achieved within the monitor retries, the failover is started for the recovery target.

When an error is detected (without monitor retry settings)

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 0 times

<Error detection>
Recovery Target group
Recovery Script Execution Count 0 times
Maximum Reactivation Count 0 times
Maximum Failover Count 1 time
Final Action none



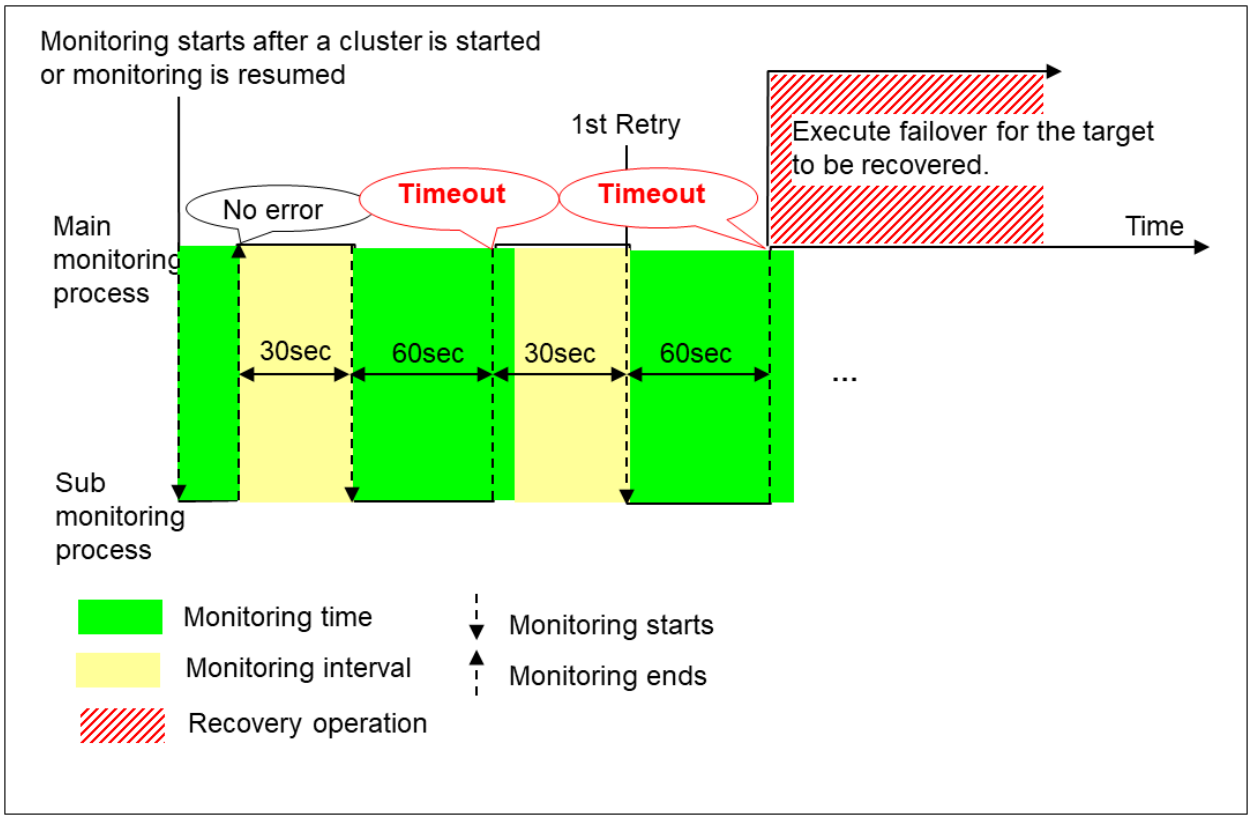
Immediately after an occurrence of a monitoring timeout, the failover for the recovery target starts.

When a monitoring timeout is detected (with monitor retry setting)

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 1 time

<Error detection>
Recovery Target group
Recovery Script Execution Count 0 times
Maximum Reactivation Count 0 times
Maximum Failover Count 1 time
Final Action none



When a monitoring timeout occurs, monitor retry is performed and failover is started for the recovery target.

4.1.6 Action when an error is detected by monitor resource

When an error is detected, the following recovery actions are taken against the recovery target in sequence:

- Execution of recovery script: this takes place when an error is detected in a monitor target.
- Reactivation of the recovery target: this takes place if the recovery script is executed up to the recovery script execution count. When the execution of a pre-reactivation script is specified, reactivation starts after that script has been executed.
- Failover: this takes place when reactivation fails for the number of times set in the reactivation threshold. When the execution of a pre-failover script is specified, failover starts after that script has been executed.
- Final action: this takes place when the error is detected even after the failover is executed for the number of times set in the failover threshold. When the execution of a pre-final-action script is specified, the final action starts after that script has been executed.

No recovery action is taken if the status of the recovery target is:

Recovery target	Status	Reactivation[2]	Failover[3]	Final action[4]
Group resource/ Failover group	Already stopped	No	No	No
	Being activated/stopped	No	No	No

Continued on next page

Table 4.4 – continued from previous page

Recovery target	Status	Reactivation[2]	Failover[3]	Final action[4]
	Already activated	Yes	Yes	Yes
	Error	Yes	Yes	Yes
Local Server	-	-	-	Yes

Yes: Recovery action is taken No: Recovery action is not taken

---

Note: Do not work on the following operations by running commands or using the Cluster WebUI when a group resource (e.g. disk resource, EXEC resource) is set as a recovery target in the settings of error detection for the monitor resource, and recovery is in progress (reactivation -> failover -> final action) after detection of an error:

- Stop/suspend the cluster
- Start/stop/move a group

If you perform the above-mentioned operations while recovery caused by detection of an error by a monitor resource is in progress, other group resources of the group with an error may not stop.

However, the above-mentioned operations can be performed when the final action is completed.

When the status of the monitor resource recovers from an error (becomes normal), the reactivation count, failover count, and whether the final action is executed are all reset.

An unsuccessful recovery action is also counted into reactivation count or failover count.

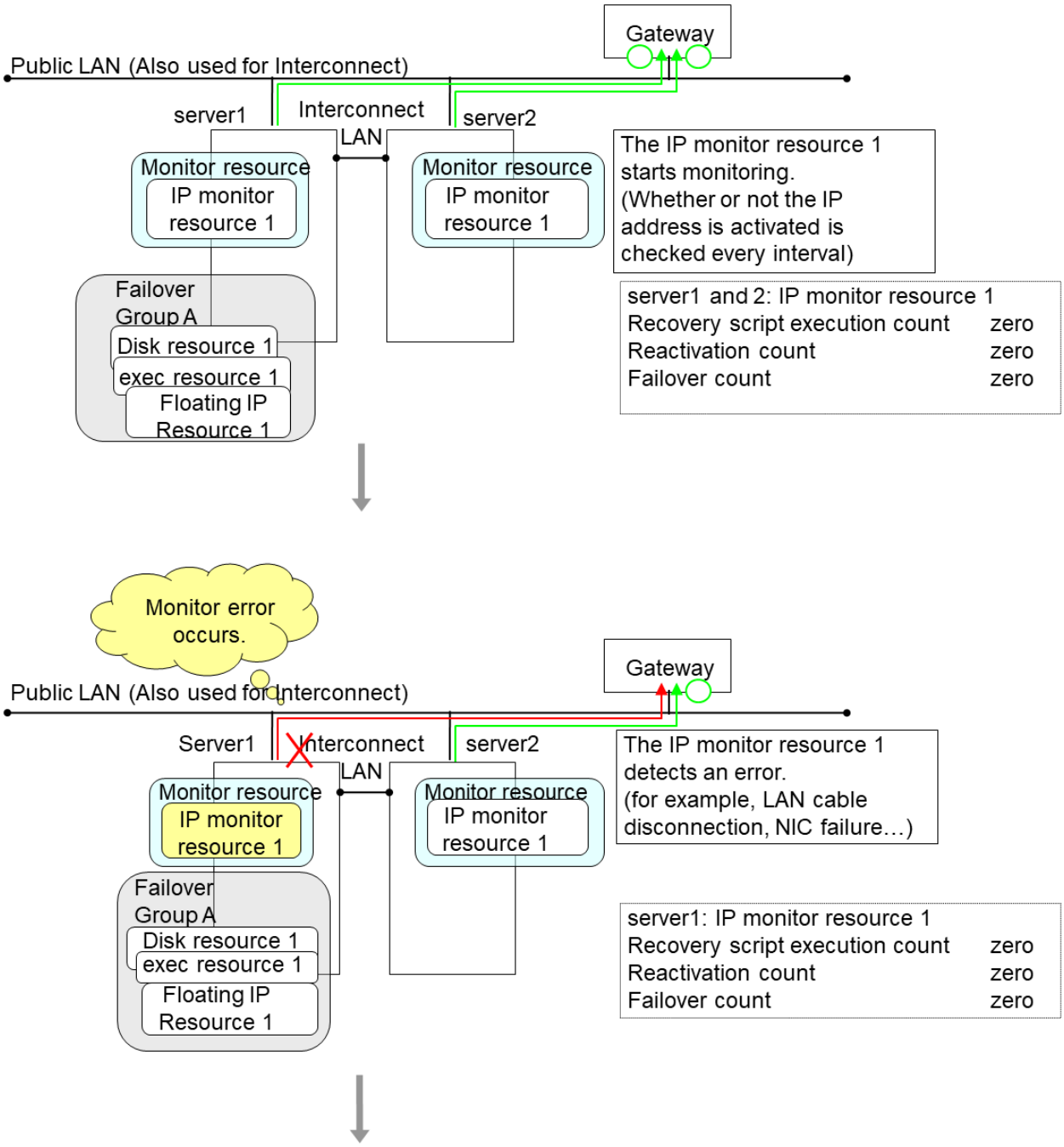
The following is an example of the progress when only one server detects an error while the gateway is specified as an IP resource of the IP monitor resource:

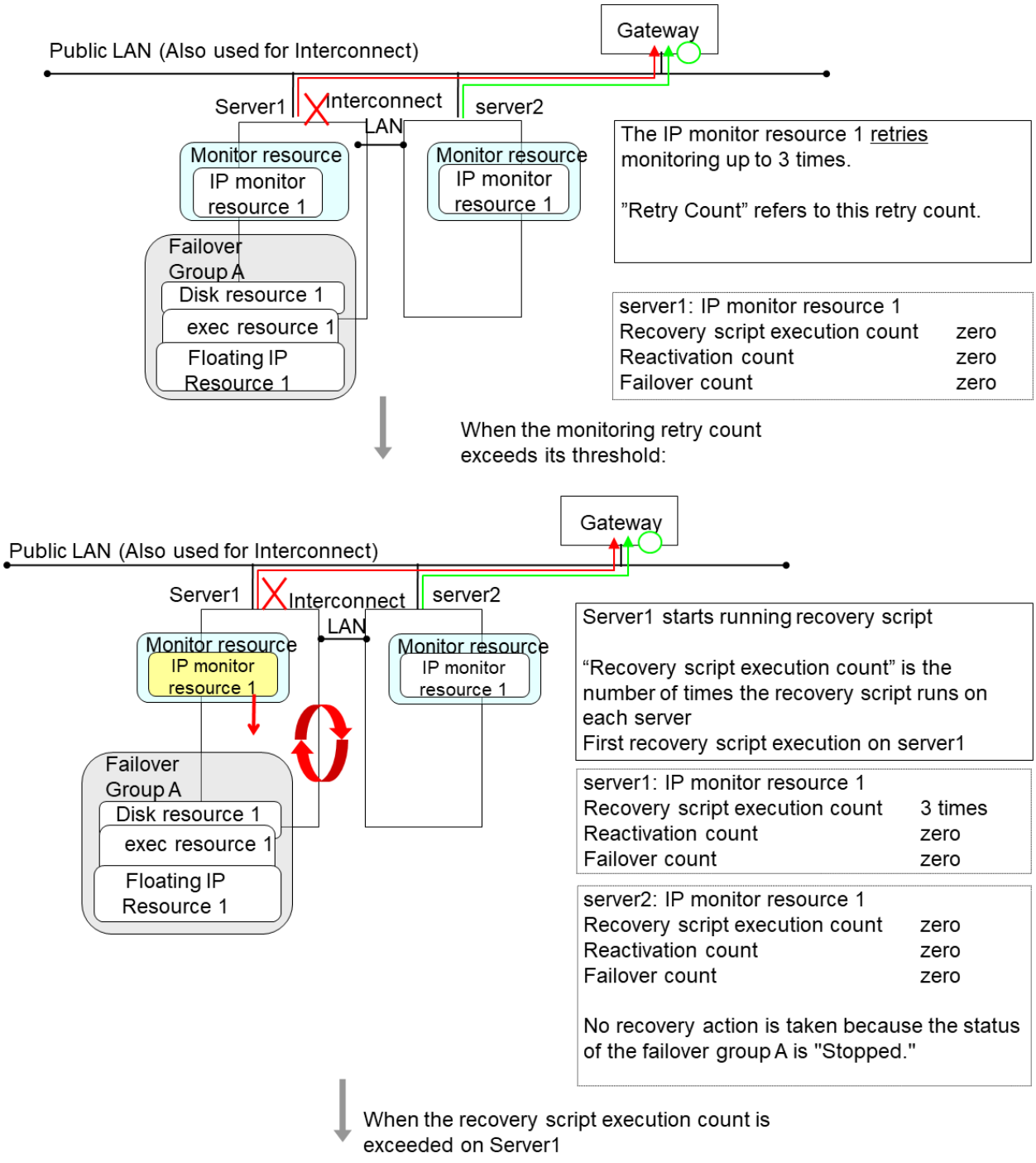
Examples of behavior when the following values are set.

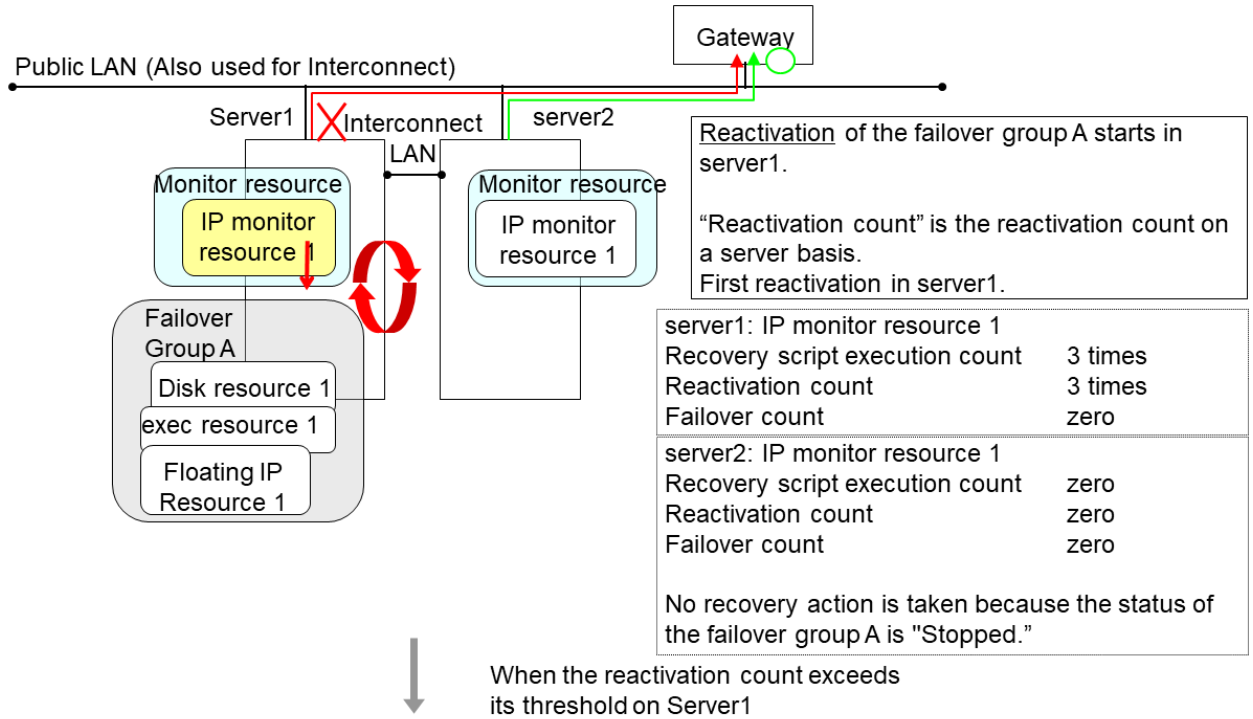
<Monitor>
Interval 30 sec
Timeout 30 sec
Retry Count 3 times

<Error detection>
Recovery Target Failover Group A
Recovery Script Execution Count 3 times
Maximum Reactivation Count 3 times
Maximum Failover Count 1 time
Final Action No Operation

[2] Effective only when the value for the reactivation threshold is set to 1 (one) or greater.
[3] Effective only when the value for the failover threshold is set to 1 (one) or greater.
[4] Effective only when an option other than No Operation is selected.


Gateway
Public LAN (Also used for Interconnect)
server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
The IP monitor resource 1 starts monitoring. (Whether or not the IP address is activated is checked every interval)
Failover Group A
Disk resource 1
exec resource 1
Floating IP Resource 1
server1 and 2: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
Monitor error occurs.
Gateway
Public LAN (Also used for Interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
The IP monitor resource 1 detects an error. (for example, LAN cable disconnection, NIC failure…)
Failover Group A
Disk resource 1
exec resource 1
Floating IP Resource 1
server1: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero


Gateway
Public LAN (Also used for Interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP Resource 1
The IP monitor resource 1 retries monitoring up to 3 times.
"Retry Count" refers to this retry count.
server1: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
When the monitoring retry count exceeds its threshold:
Gateway
Public LAN (Also used for Interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP Resource 1
Server1 starts running recovery script
"Recovery script execution count" is the number of times the recovery script runs on each server
First recovery script execution on server1
server1: IP monitor resource 1
Recovery script execution count 3 times
Reactivation count zero
Failover count zero
server2: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
No recovery action is taken because the status of the failover group A is "Stopped."
When the recovery script execution count is exceeded on Server1



Reactivation of the failover group A starts in server1.

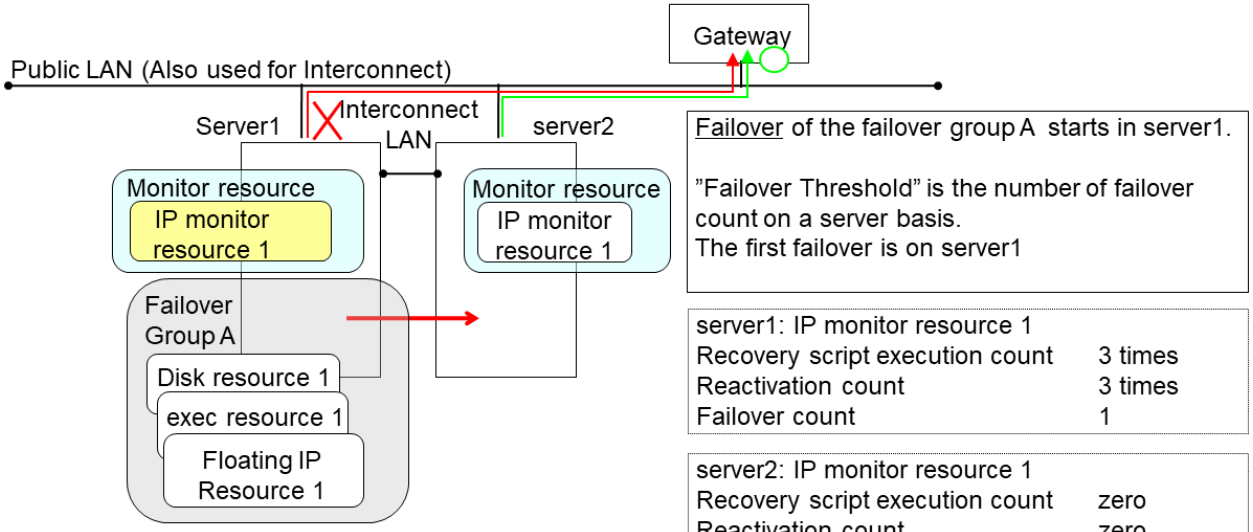
"Reactivation count" is the reactivation count on a server basis.
First reactivation in server1.

server1: IP monitor resource 1	
Recovery script execution count	3 times
Reactivation count	3 times
Failover count	zero

server2: IP monitor resource 1	
Recovery script execution count	zero
Reactivation count	zero
Failover count	zero

No recovery action is taken because the status of the failover group A is "Stopped."

When the reactivation count exceeds its threshold on Server1



Failover of the failover group A starts in server1.

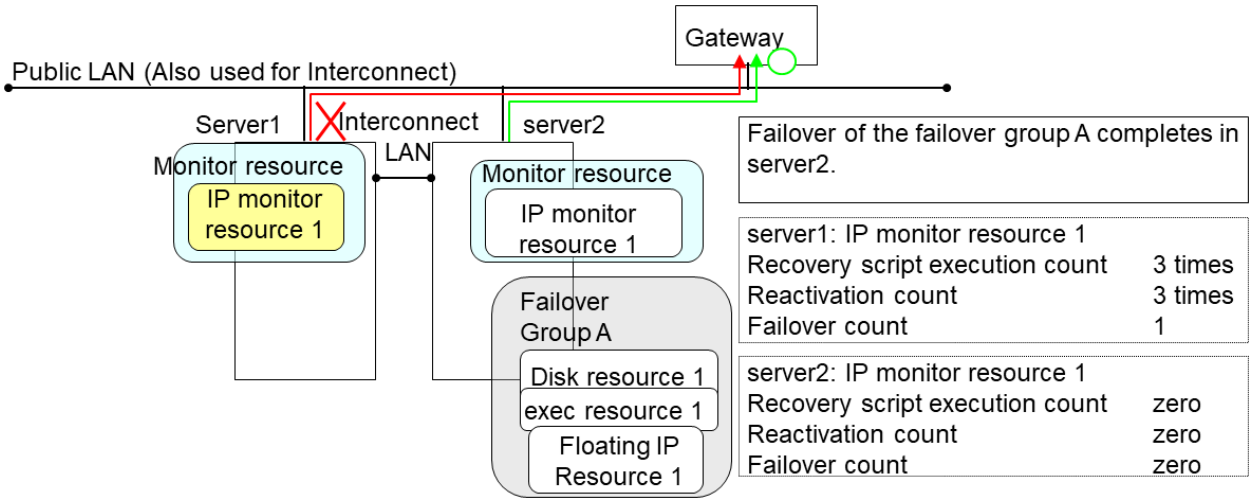
"Failover Threshold" is the number of failover count on a server basis.
The first failover is on server1

server1: IP monitor resource 1	
Recovery script execution count	3 times
Reactivation count	3 times
Failover count	1

server2: IP monitor resource 1	
Recovery script execution count	zero
Reactivation count	zero
Failover count	zero

No recovery action is taken because the status of failover group A is "Stopped."

Failover of the failover group A from server1 to server2



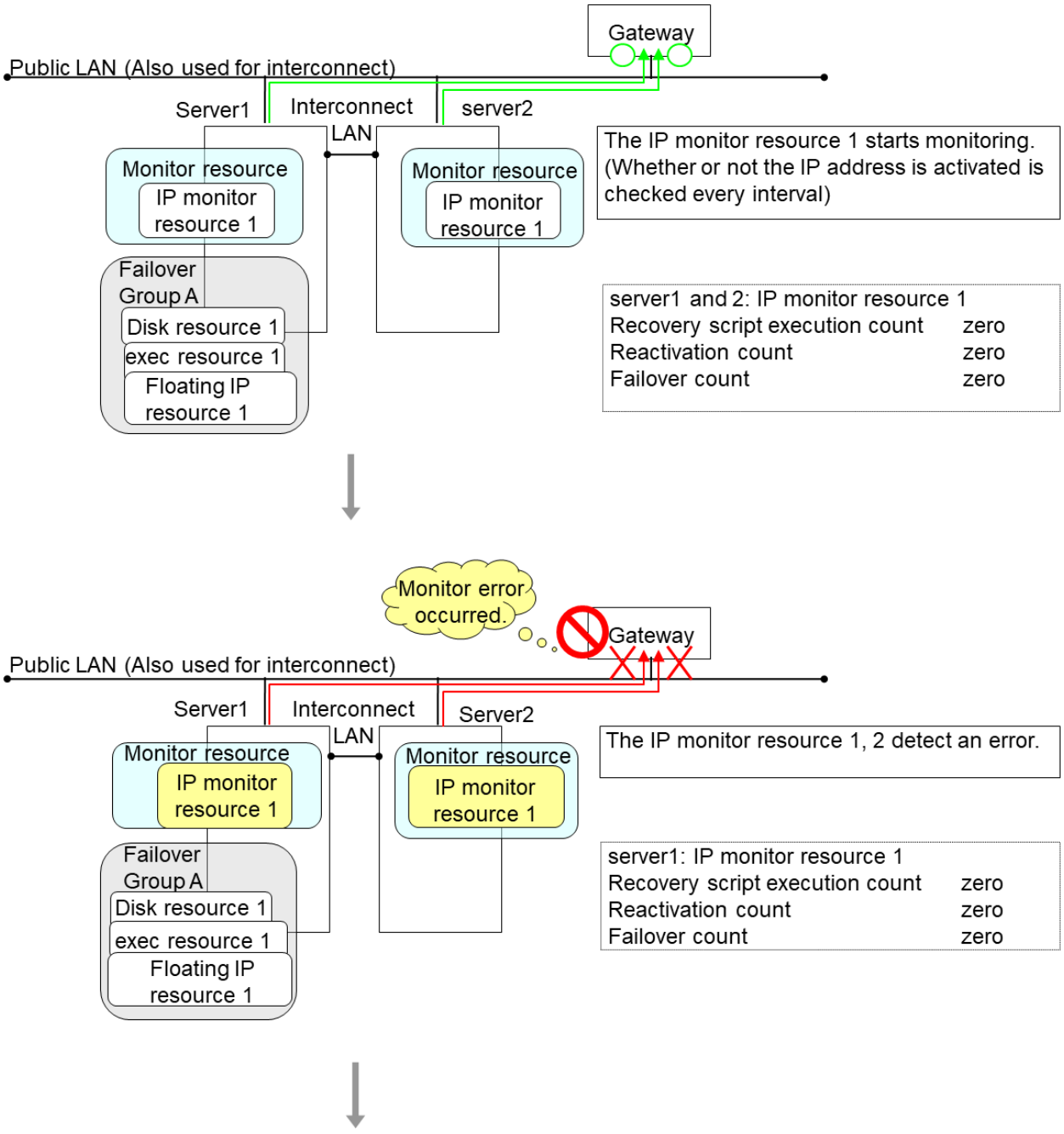
In server2, the operation can continue by failover of the Failover Group A because the IP monitor resource 1 is running properly.

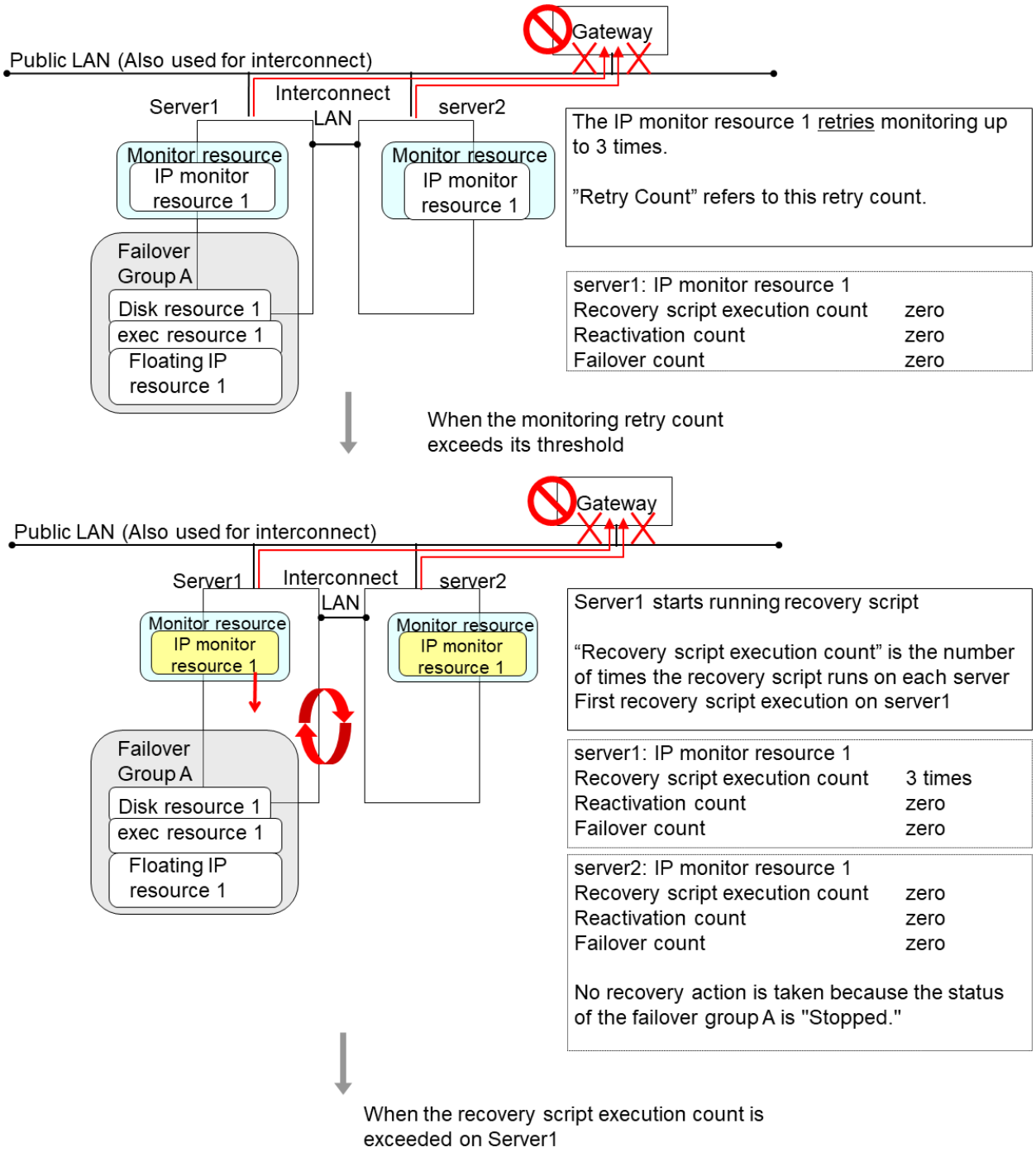
The following is an example of the process when both servers detect an error while the gateway is specified as an IP resource of the IP monitor resource.

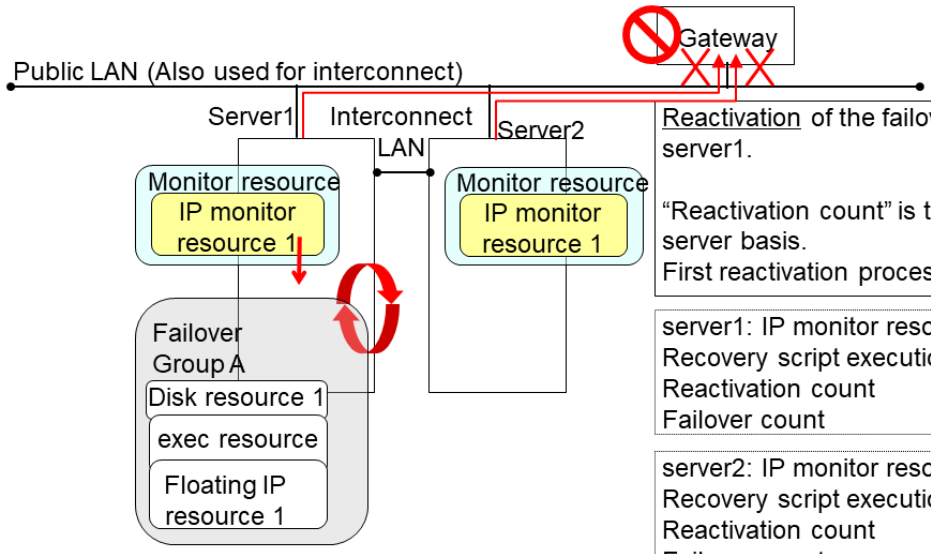
Examples of behavior when the following values are set.

<Monitor>
Interval 30 sec
Timeout 30 sec
Retry Count 3 times

<Error detection>
Recovery Target Failover Group A
Recovery Script Execution Count 3 times
Maximum Reactivation Count 3 times
Maximum Failover Count 1 time
Final Action No Operation


Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
The IP monitor resource 1 starts monitoring. (Whether or not the IP address is activated is checked every interval)
server1 and 2: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
Monitor error occurred.
Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect LAN
Server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
The IP monitor resource 1, 2 detect an error.
server1: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero


Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
The IP monitor resource 1 retries monitoring up to 3 times.
"Retry Count" refers to this retry count.
server1: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
When the monitoring retry count exceeds its threshold
Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
Server1 starts running recovery script
"Recovery script execution count" is the number of times the recovery script runs on each server
First recovery script execution on server1
server1: IP monitor resource 1
Recovery script execution count 3 times
Reactivation count zero
Failover count zero
server2: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
No recovery action is taken because the status of the failover group A is "Stopped."
When the recovery script execution count is exceeded on Server1



Reactivation of the failover group A starts in server1.

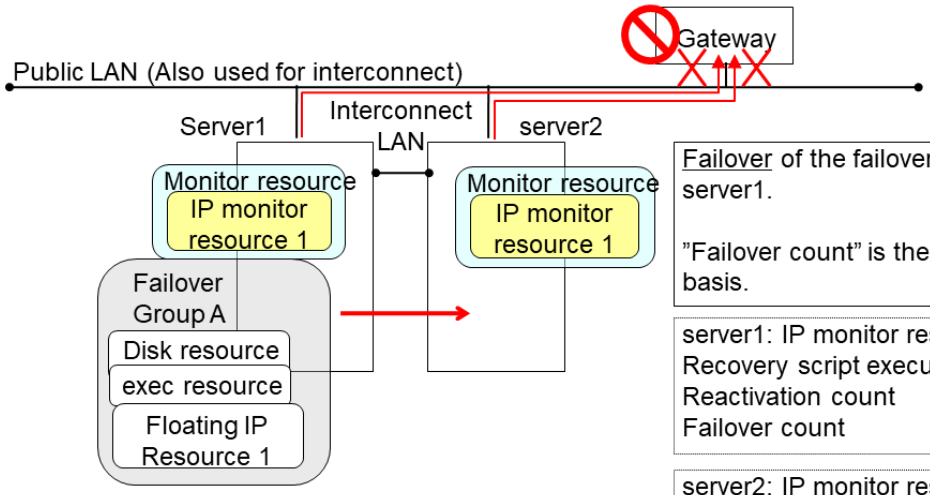
"Reactivation count" is the reactivation count on a server basis.
First reactivation processing on server1.

server1: IP monitor resource 1	
Recovery script execution count	3 times
Reactivation count	3 times
Failover count	zero

server2: IP monitor resource 1	
Recovery script execution count	zero
Reactivation count	zero
Failover count	zero

No recovery action is taken because the status of failover group A is "Stopped."

When reactivation count exceeds the threshold in server1



Failover of the failover group A starts in server1.

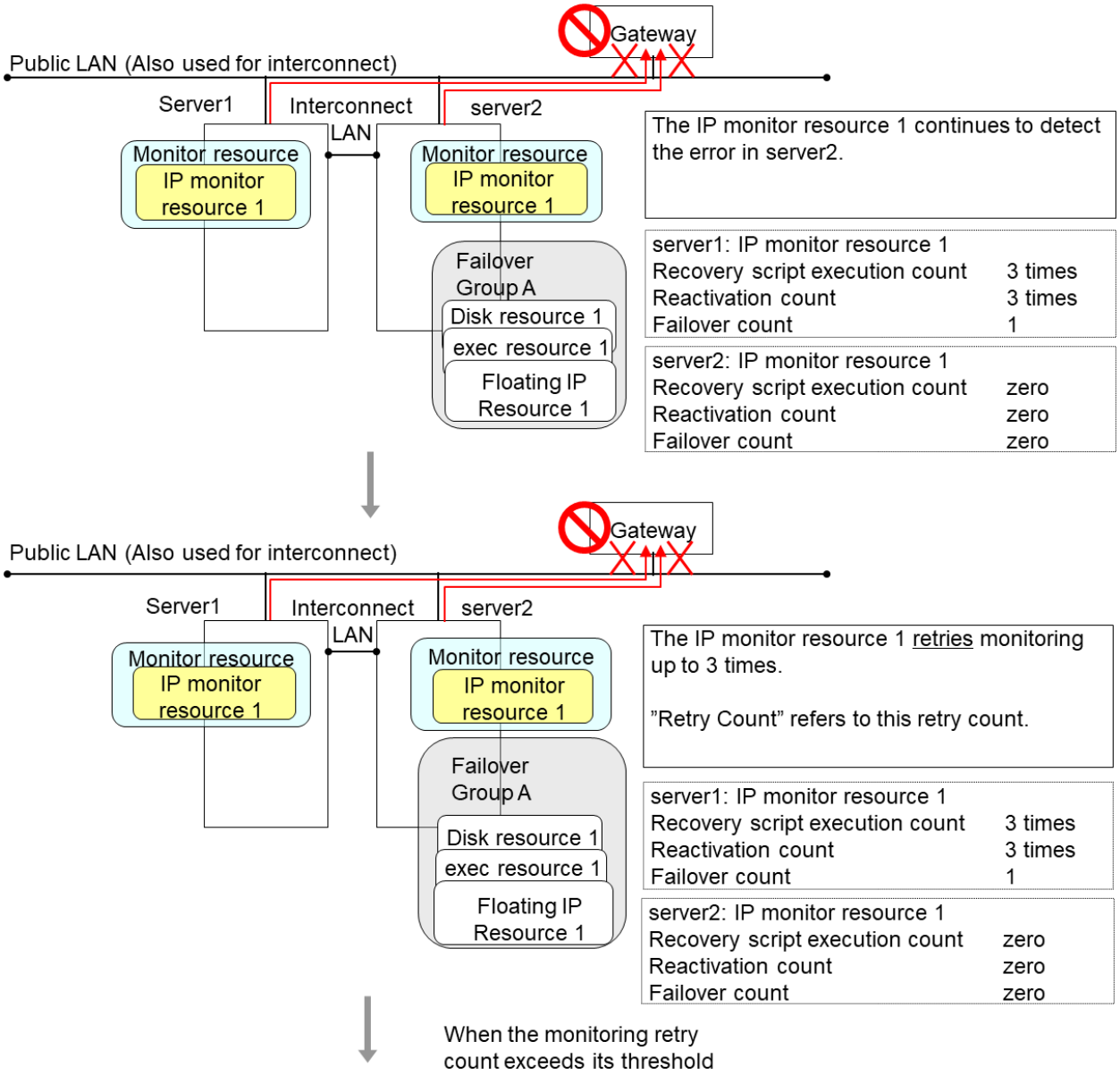
"Failover count" is the failover count on a server basis.

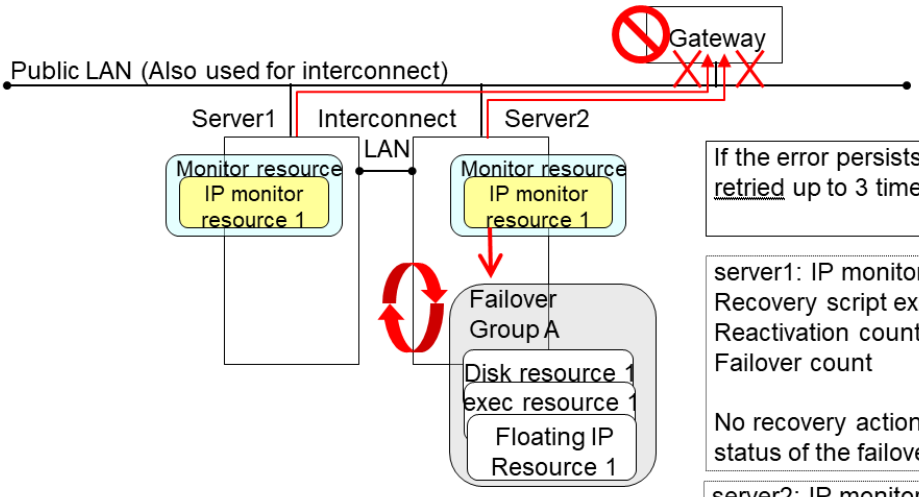
server1: IP monitor resource 1	
Recovery script execution count	3 times
Reactivation count	3 times
Failover count	1

server2: IP monitor resource 1	
Recovery script execution count	zero
Reactivation count	zero
Failover count	zero

No recovery action is taken because the status of failover group A is "Stopped."

Failover the failover group A from server1 to server2


Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect
LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP Resource 1
The IP monitor resource 1 continues to detect the error in server2.
server1: IP monitor resource 1
Recovery script execution count 3 times
Reactivation count 3 times
Failover count 1
server2: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect
LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP Resource 1
The IP monitor resource 1 retries monitoring up to 3 times.
"Retry Count" refers to this retry count.
server1: IP monitor resource 1
Recovery script execution count 3 times
Reactivation count 3 times
Failover count 1
server2: IP monitor resource 1
Recovery script execution count zero
Reactivation count zero
Failover count zero
When the monitoring retry count exceeds its threshold



If the error persists, the recovery script is retried up to 3 times

server1: IP monitor resource 1

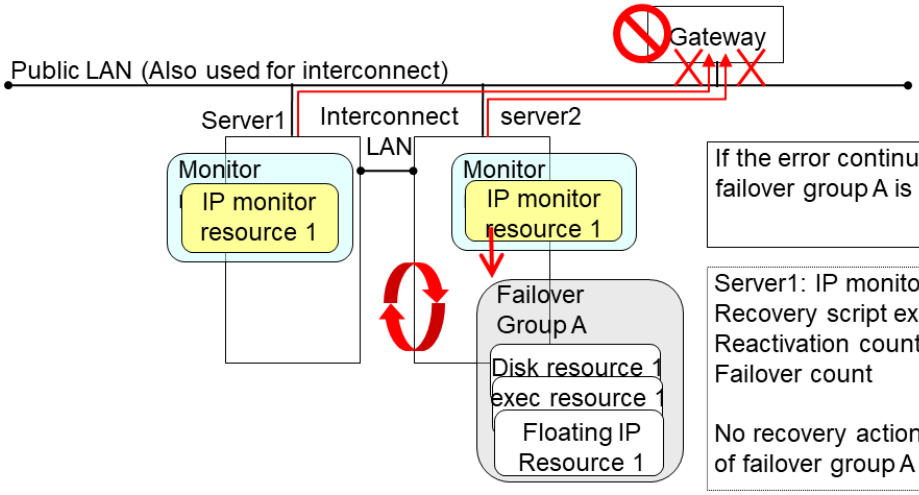
Recovery script execution count	3 times
Reactivation count	3 times
Failover count	1 times

No recovery action is taken because the status of the failover group A is "Stopped."

server2: IP monitor resource 1

Recovery script execution count	3 times
Reactivation count	zero
Failover count	zero

When server2 also fails to retry running of the recovery script



If the error continues, reactivation of the failover group A is retried up to 3 times.

Server1: IP monitor resource 1

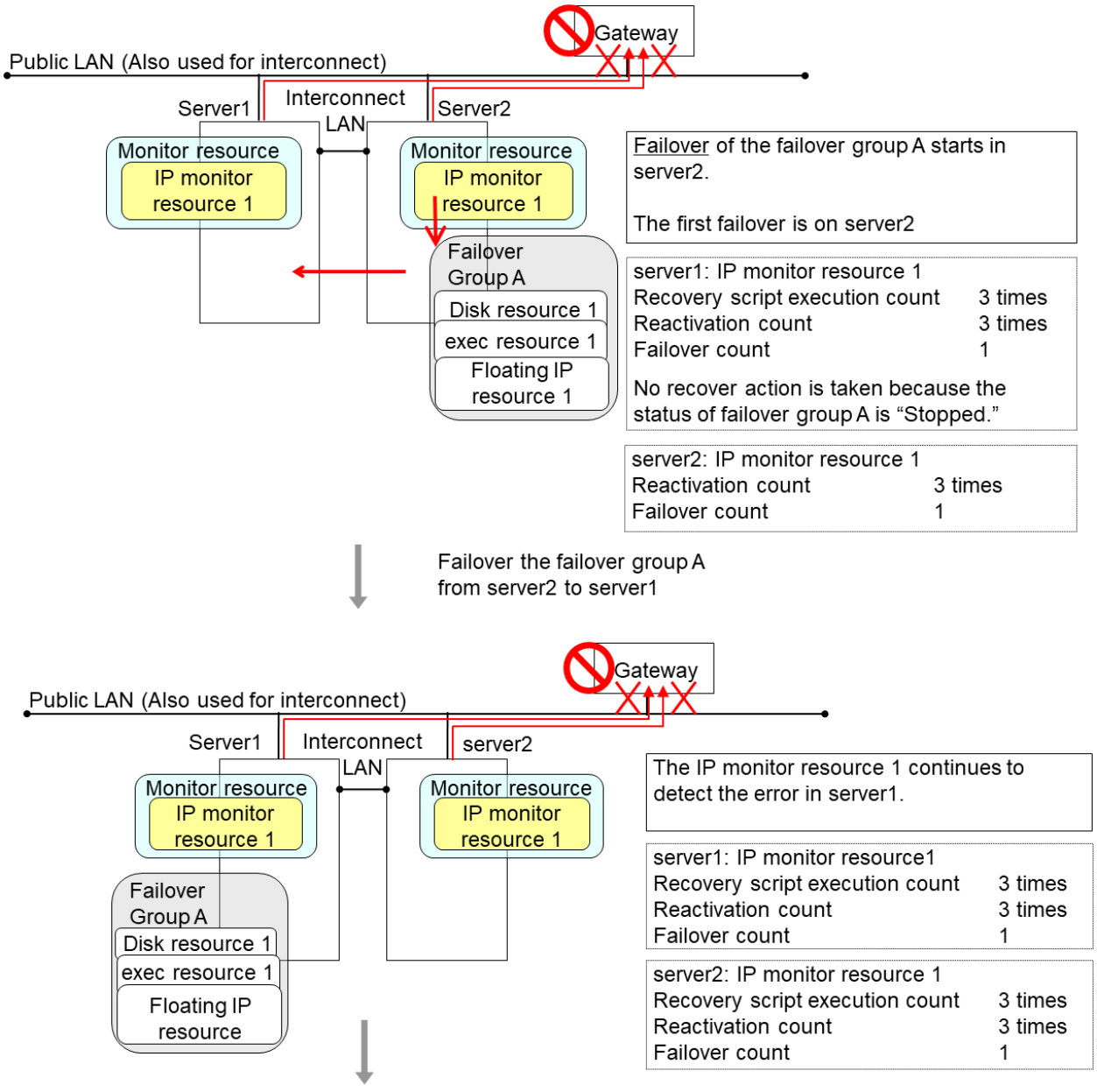
Recovery script execution count	3 times
Reactivation count	3 times
Failover count	1

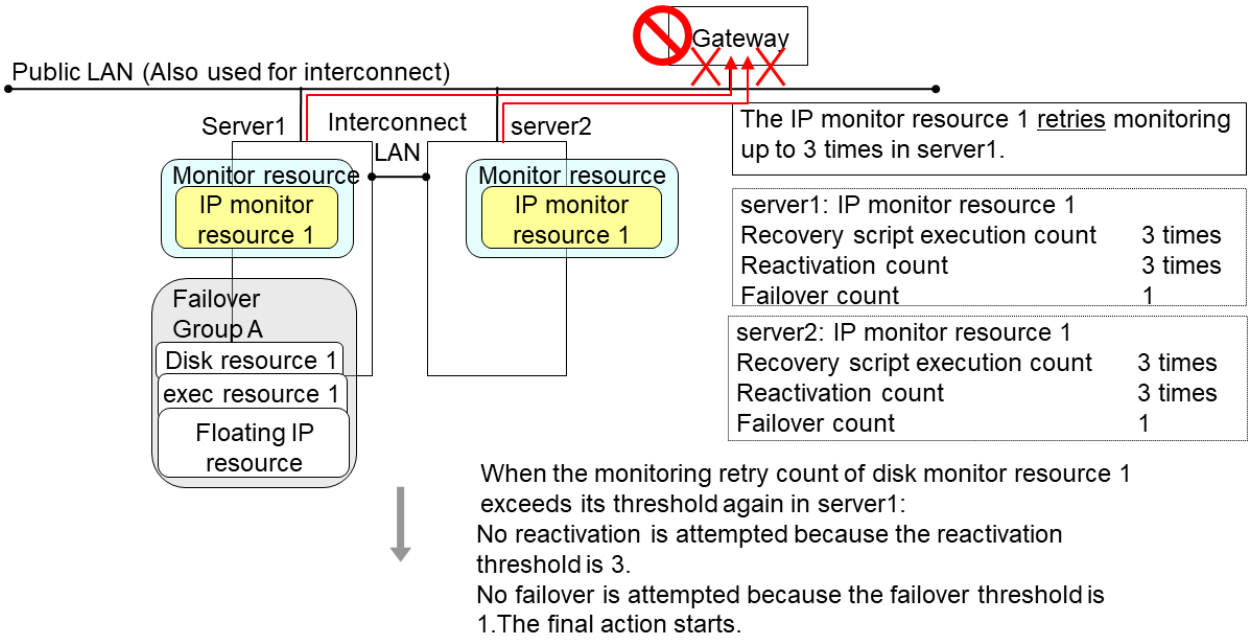
No recovery action is taken because the status of failover group A is “Stopped”

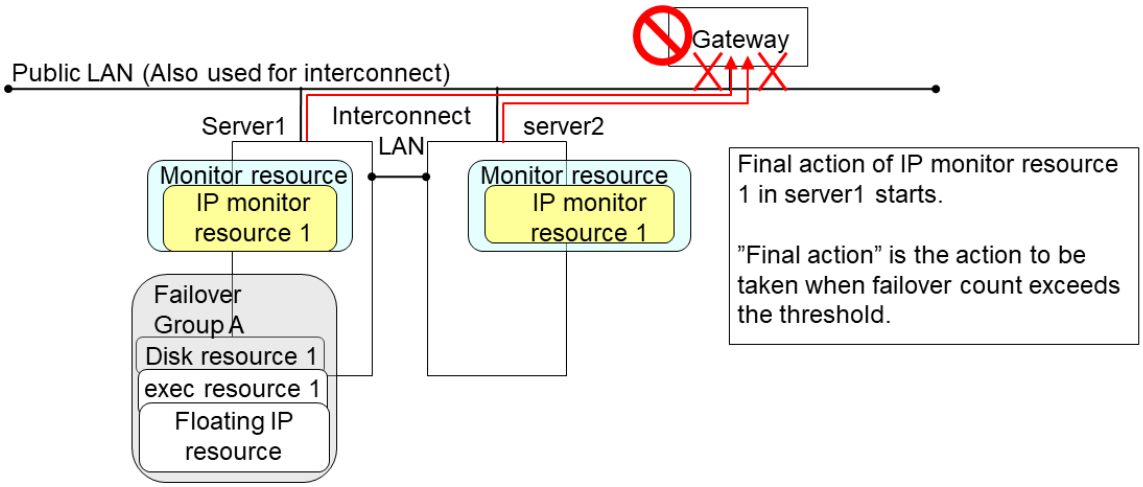
server2: IP monitor resource 1

Recovery script execution count	3 times
Reactivation count	3 times
Failover count	zero

When reactivation count also exceeds its threshold in server2


Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect
LAN
Server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
Failover of the failover group A starts in server2.
The first failover is on server2
server1: IP monitor resource 1
Recovery script execution count 3 times
Reactivation count 3 times
Failover count 1
No recover action is taken because the status of failover group A is “Stopped.”
server2: IP monitor resource 1
Reactivation count 3 times
Failover count 1
Failover the failover group A from server2 to server1
Gateway
Public LAN (Also used for interconnect)
Server1
Interconnect
LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource
The IP monitor resource 1 continues to detect the error in server1.
server1: IP monitor resource1
Recovery script execution count 3 times
Reactivation count 3 times
Failover count 1
server2: IP monitor resource 1
Recovery script execution count 3 times
Reactivation count 3 times
Failover count 1





Additional Information

When the status of the monitor target becomes normal from an error and the monitor resource detects the change, the reactivation count and failover count are reset to zero (0). When an error is detected next time, the process will be exactly the same as what has been described up to here.

The description up to here assumed the interconnect LANs are working properly.

If all interconnect LANs are disconnected, internal communications with other servers are blocked. As a result, even if an error is detected on a monitor target, failover of groups fails.

To fail over a group when all interconnect LANs are disconnected, you can choose to shut down the server where an error is detected. This will allow other servers to detect the server is shut down and to start failover of the group.

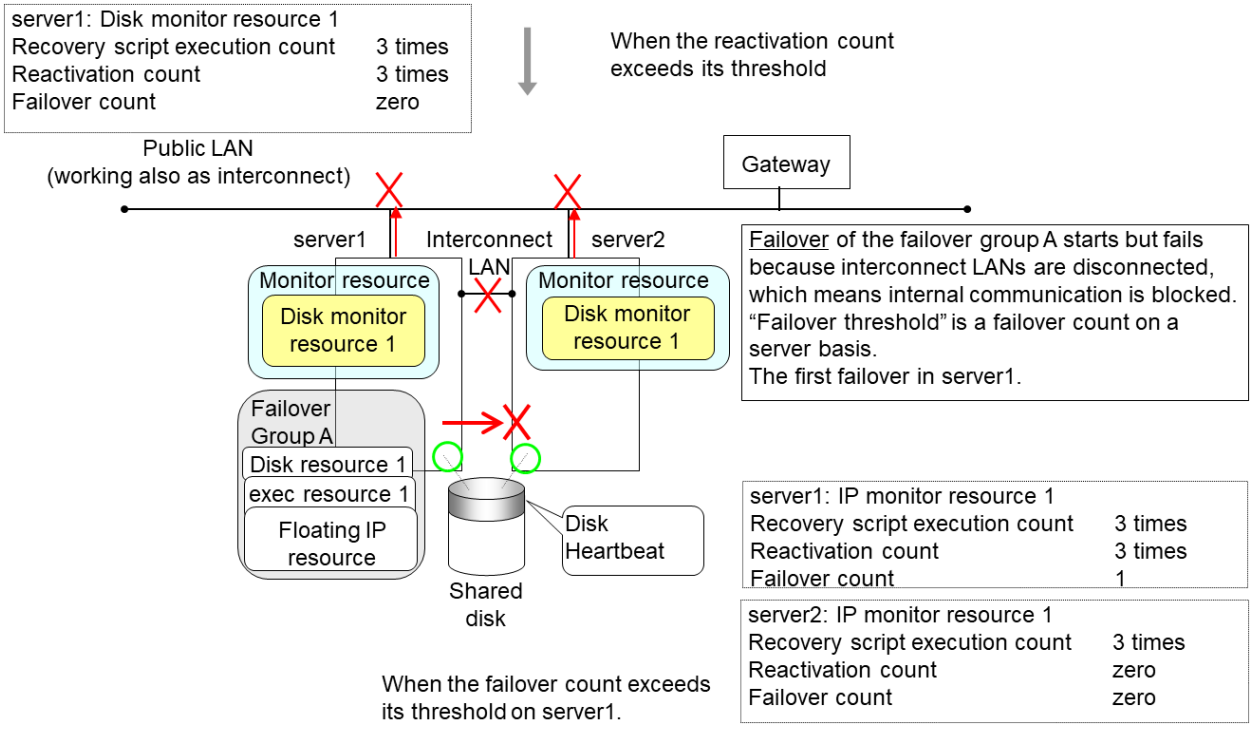
The following is an example of the process when an error is detected while all interconnect LANs are disconnected.

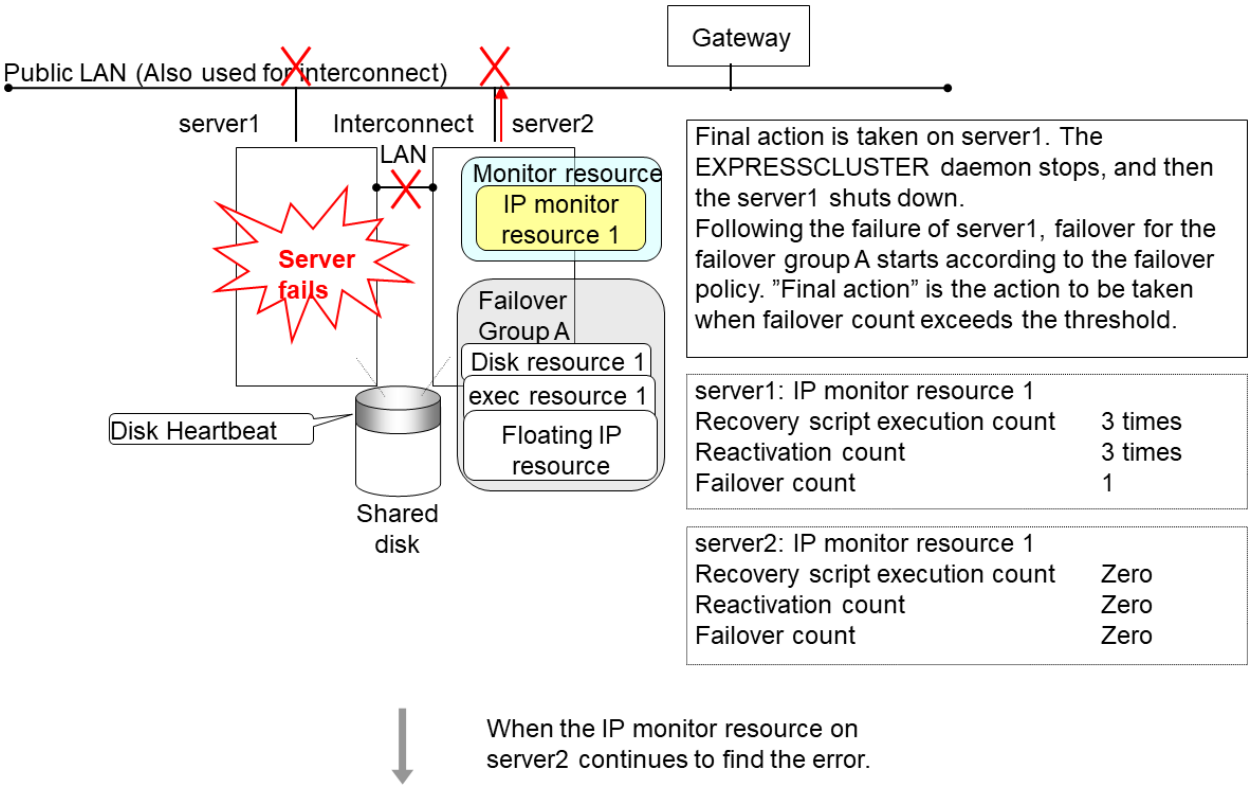
Configuration

<Monitor>
Interval 30 seconds
Timeout 30 seconds
Retry Count 3 times

<Error detection>
Recovery Object Failover Group A
Recovery Script Execution Count 3 times
Maximum Reactivation Count 3 times
Maximum Failover Count 1 time
Final Action Stop cluster daemon and shutdown OS

Reactivation for the recovery target is same as the situation when the interconnect LANs are working properly. The description begins from the failover on server1, which requires interconnect LANs.

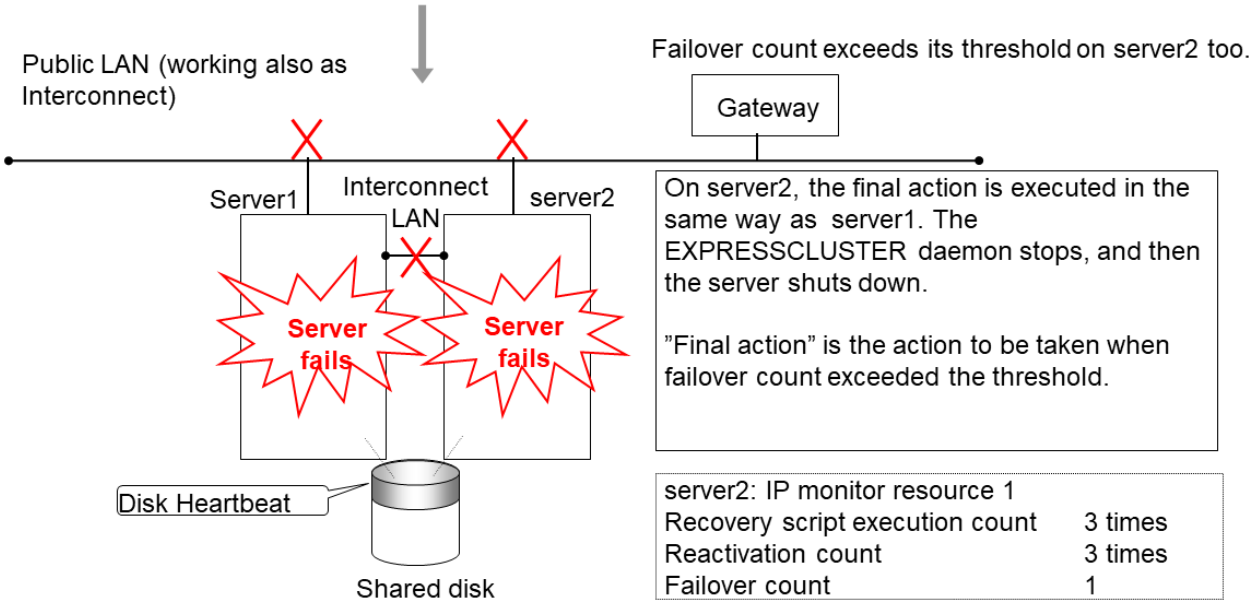




Reactivation of the Failover Group A is executed on server2 in the same way as server1.

Failover is attempted on server2 as well when reactivation of the group A fails. However, the failover cannot be executed because there is no destination server for the failvoer.

When the failover count exceeds its threthhold, the final action is taken on server2 as is the case on server1.



4.1.7 Returning from monitor error (Normal)

When return of the monitor resource is detected during or after recovery actions following the detection of a monitoring error, counts for the thresholds shown below are reset:

- Recovery Script Execution Count
- Reactivation Count
- Failover Count

Whether or not to execute the final action is reset (execution required).

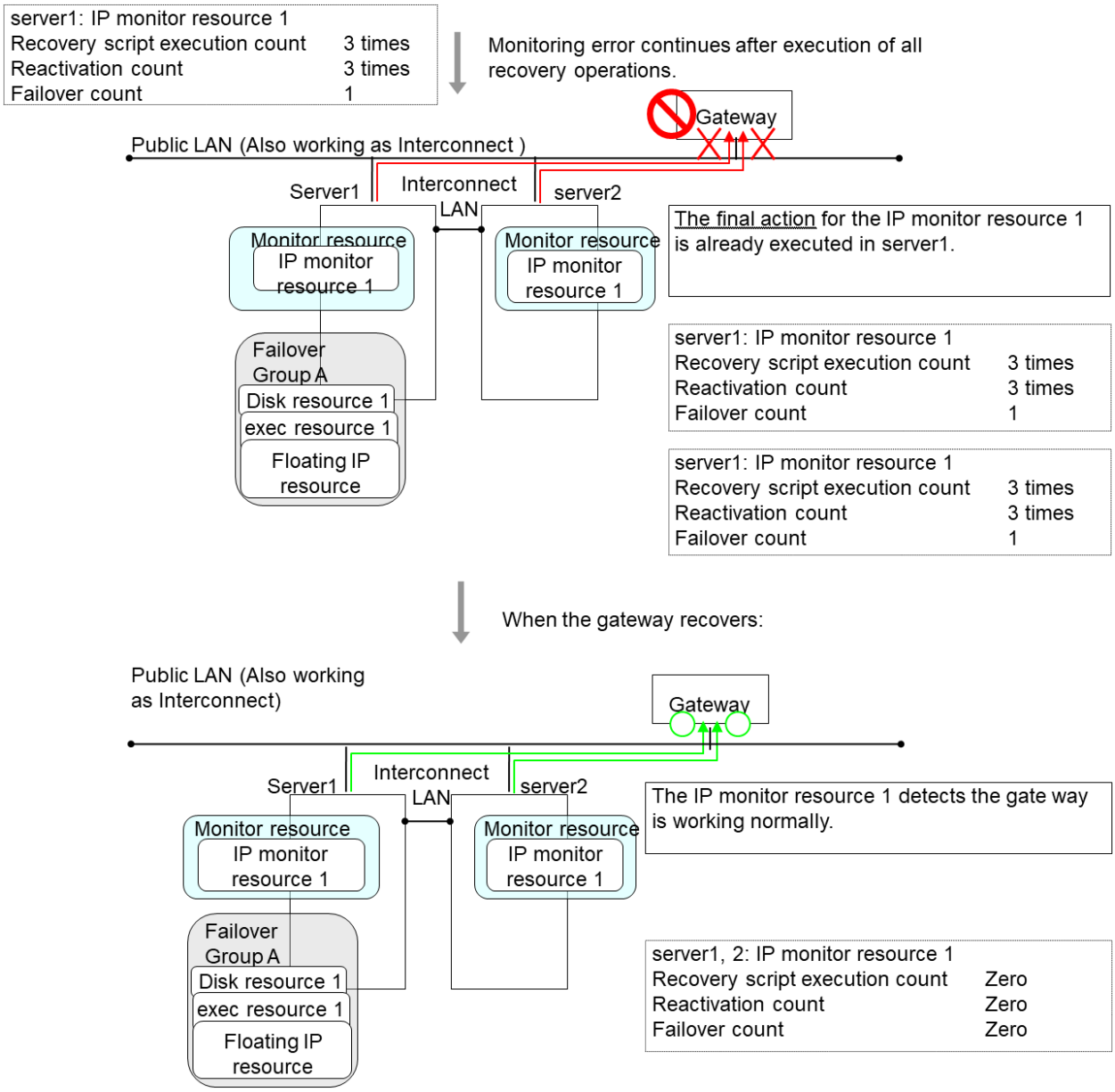
The following pages describe what will be executed from the point when the final action as described in "*Action when an error is detected by monitor resource*" executed and another monitoring error occurs after monitoring returns to normal.

Examples of behavior when the following values are set.

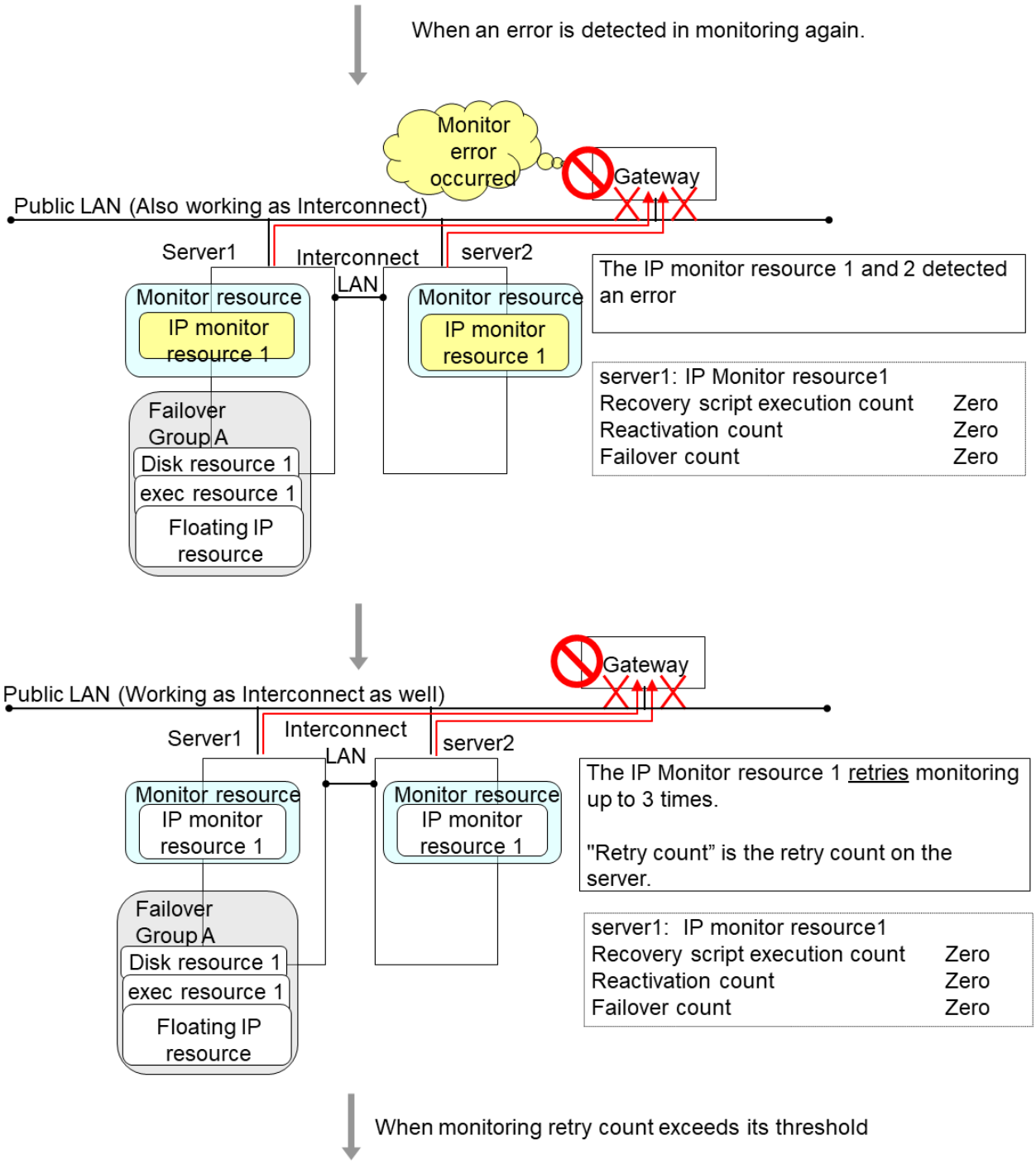
Configuration

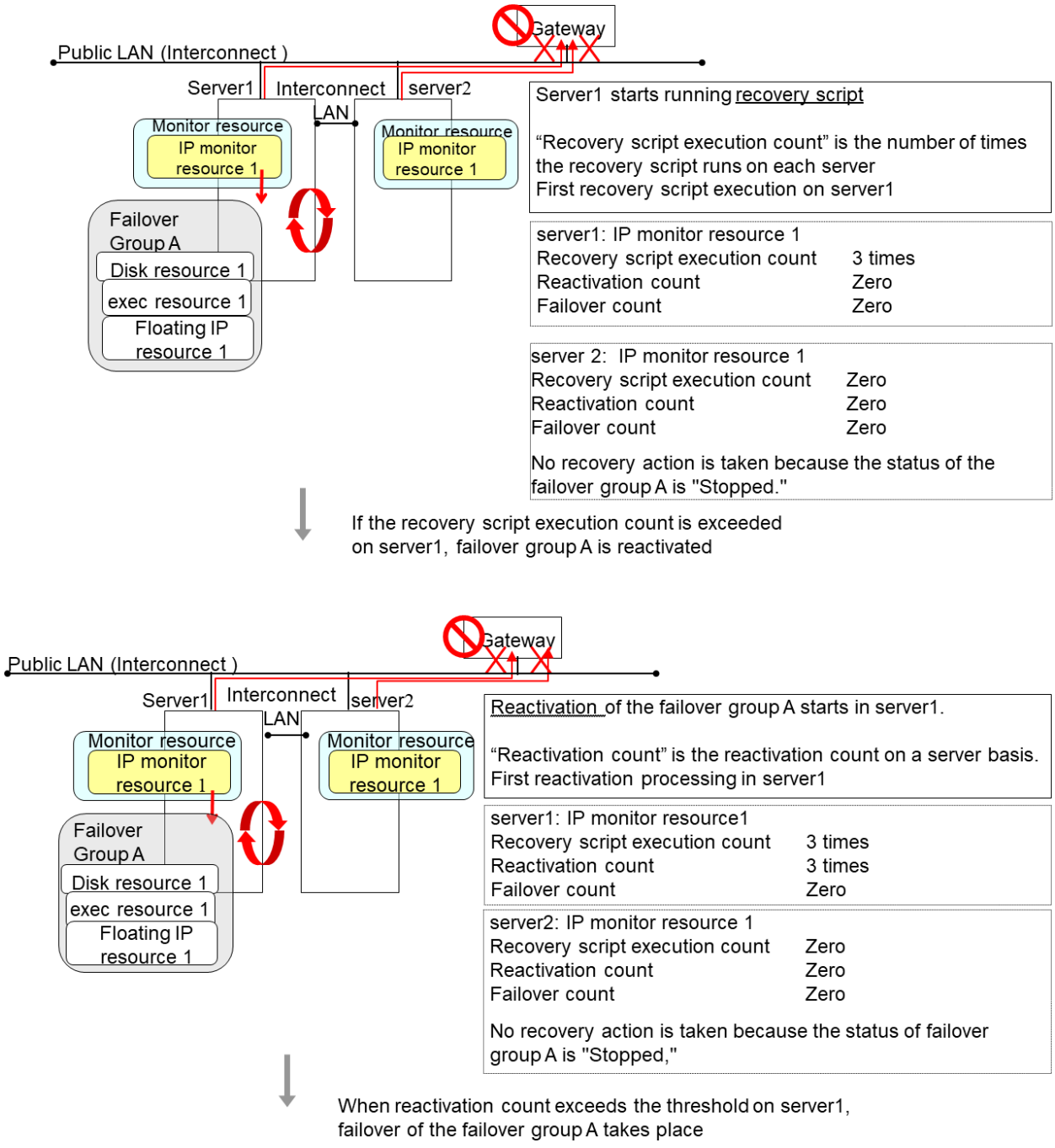
<Monitor>
Interval 30 sec
Timeout 30 sec
Retry Count 3 times

<Error detection>
Recovery Target Failover Group A
Recovery Script Execution Count 3 times
Maximum Reactivation Count 3 times
Maximum Failover Count 1 time
Final Action Stop Failover Group



The number of reactivations and failovers are reset because it has been detected that the status of the monitor target resource became normal.


When an error is detected in monitoring again.
Monitor error occurred
Gateway
Public LAN (Also working as Interconnect)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource
The IP monitor resource 1 and 2 detected an error
server1: IP Monitor resource1
Recovery script execution count Zero
Reactivation count Zero
Failover count Zero
Gateway
Public LAN (Working as Interconnect as well)
Server1
Interconnect LAN
server2
Monitor resource
IP monitor resource 1
Monitor resource
IP monitor resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource
The IP Monitor resource 1 retries monitoring up to 3 times.
"Retry count" is the retry count on the server.
server1: IP monitor resource1
Recovery script execution count Zero
Reactivation count Zero
Failover count Zero
When monitoring retry count exceeds its threshold



Reactivation is executed again because it has been detected that the status of the monitor target resource became normal and reactivation count has been reset before.

4.1.8 Activation and deactivation error of recovery target when executing recovery operation

When the monitoring target of the monitor resource is the device used for the group resource of the recovery target, an activation/deactivation error of the group resource may be detected during recovery when a monitoring error is detected.

The following is an example of the recovery progress when the same device is specified as the monitor target of the disk monitor resource and the disk resource of the Failover Group A:

Configuration of the disk monitor resource

<Monitor>
Interval 60 seconds
Timeout 120 seconds
Retry Count 0 times

<Error detection>
Recovery Target Failover Group A
Recovery Script Execution Count 0 times
Maximum Reactivation Count 0 times
Maximum Failover Count 1 time
Final Action Stop Failover Group

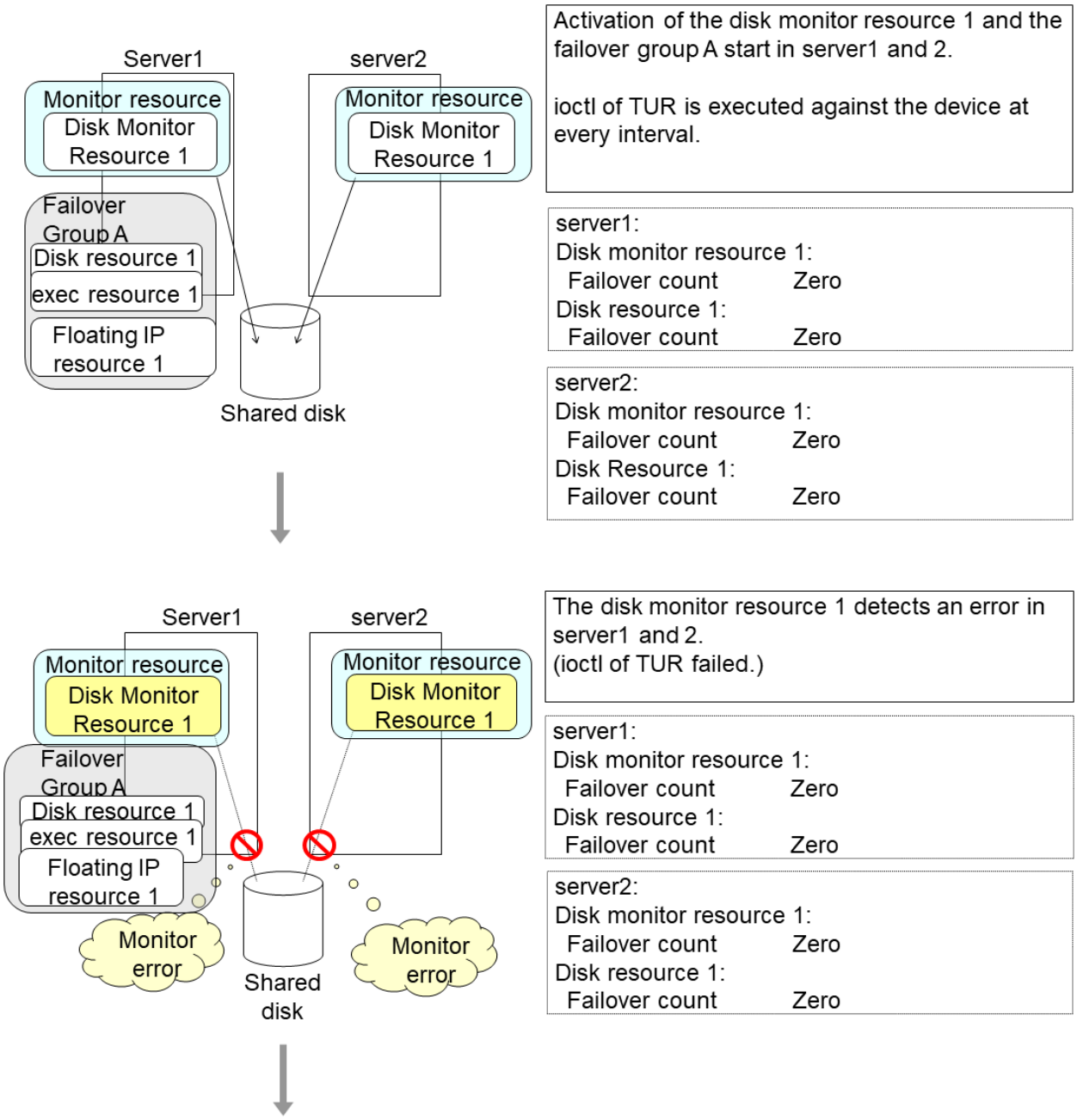
<Parameter>
Method TUR

Configuration of the failover group A: disk resource

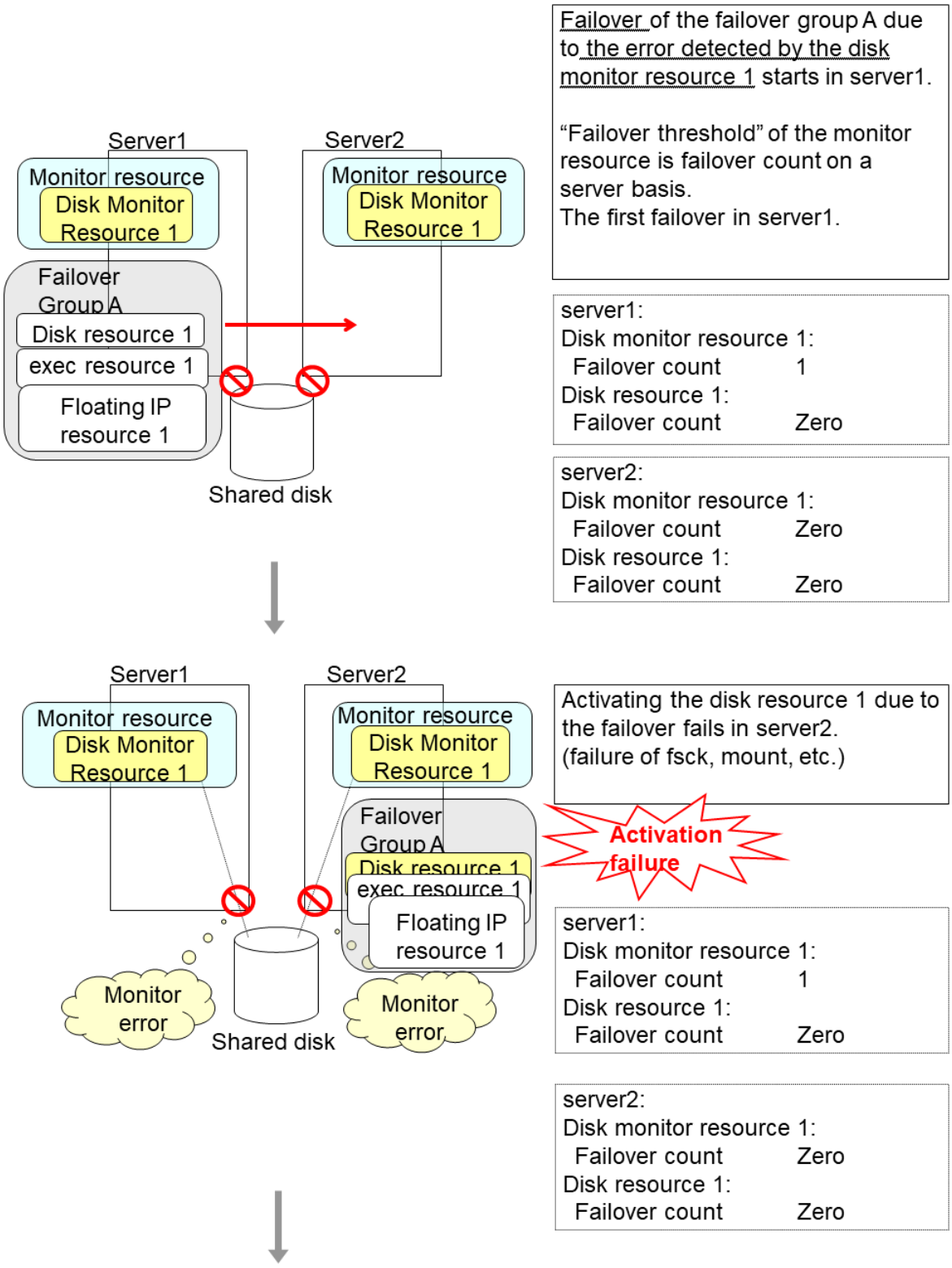
<Activation error>
Activation retry Threshold 0 times
Failover Threshold 1 time
Final Action No Operation (Next resources are not activated)

<Deactivation abnormality>
Deactivation Retry Threshold 0 times
Final Action Stop cluster daemon and shutdown OS

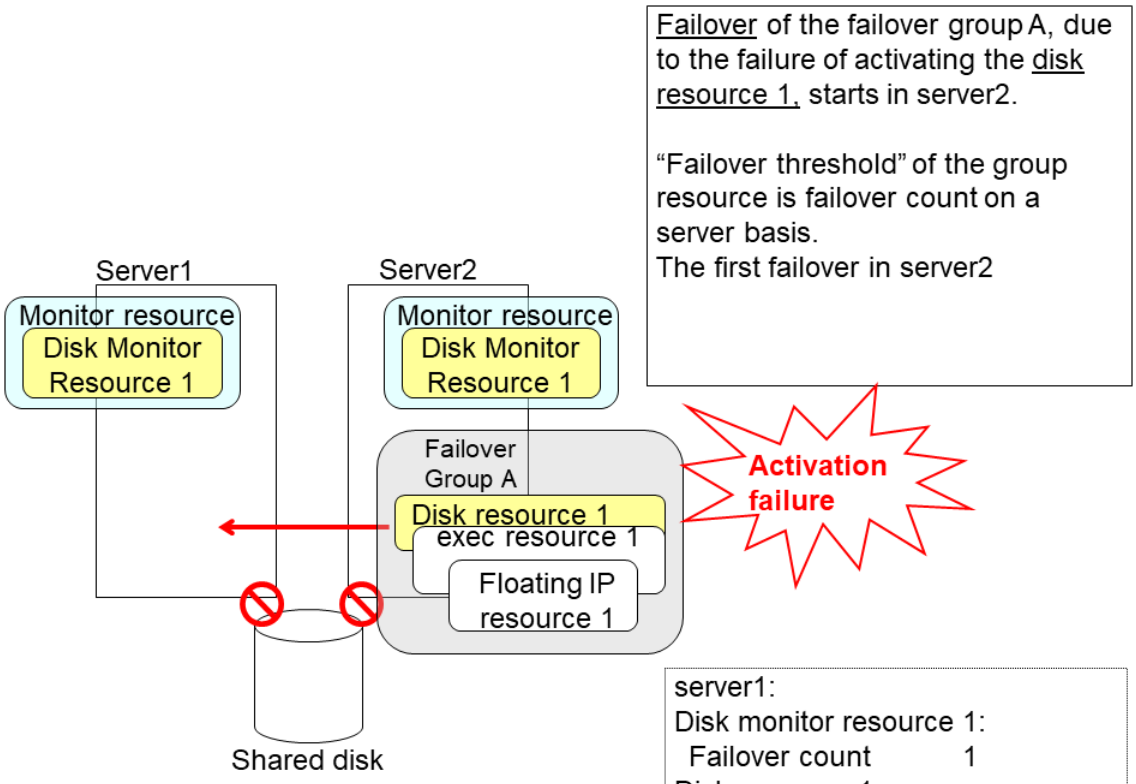
The reactivation threshold of the monitor resource and the activation retry threshold of the group resource are not mentioned in the following diagrams because they are set to zero (0).



An error can be detected in deactivation of the disk resource depending on the location of the disk device failure.

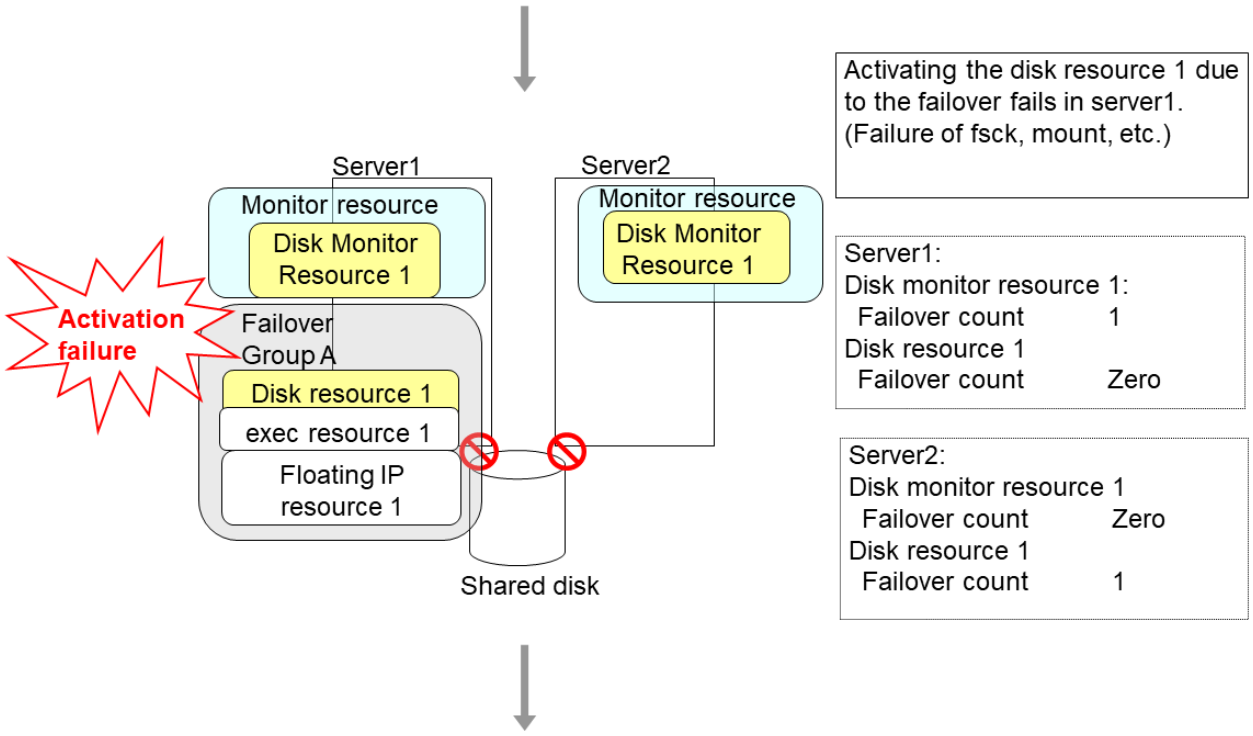


An error can be detected in deactivation of the disk resource depending on the location of the disk device failure.

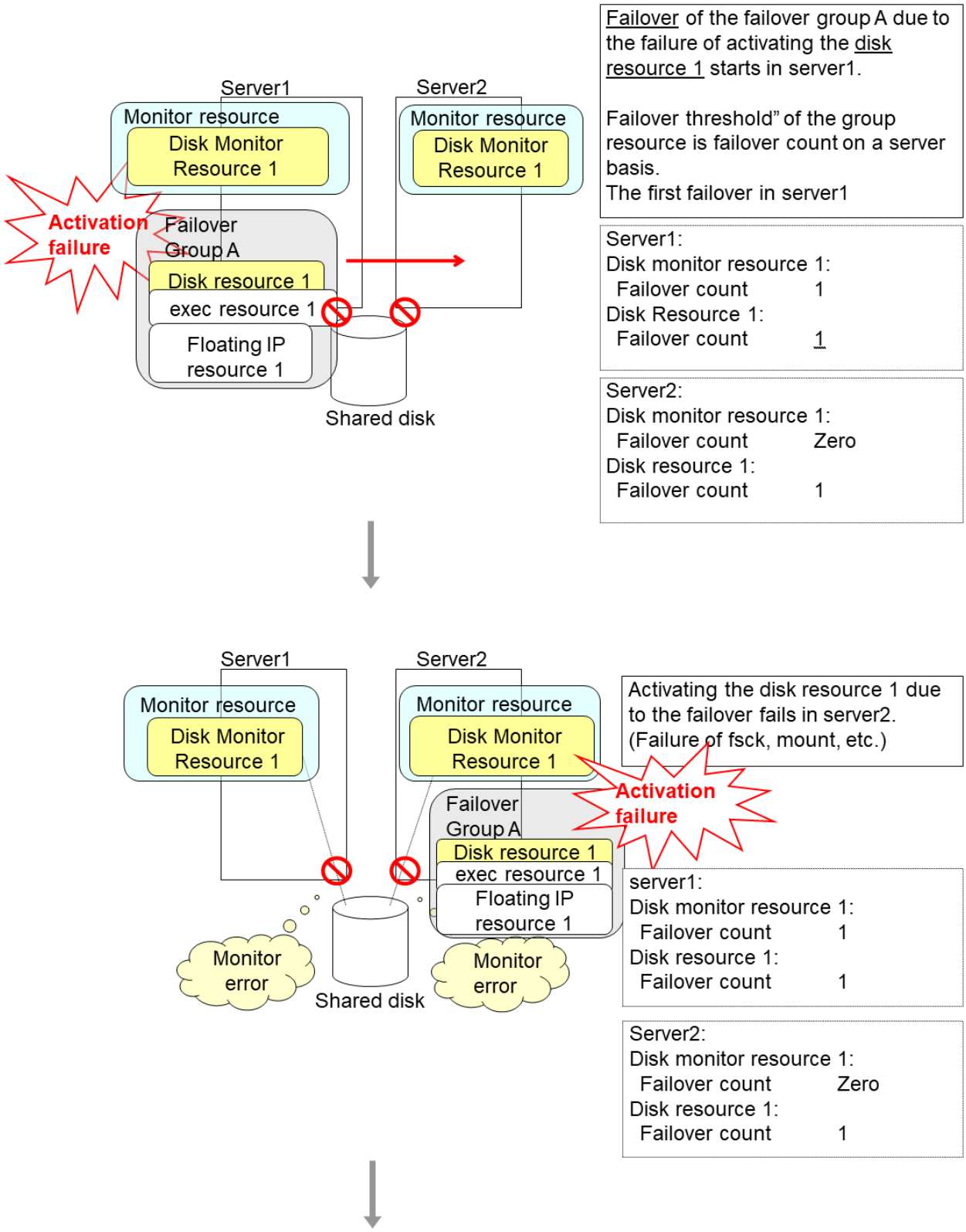


The disk monitor resource 1 detects an error in server2 as is the case in server1. However, no recovery action is taken because the failover group A, the recovery target, is activated.

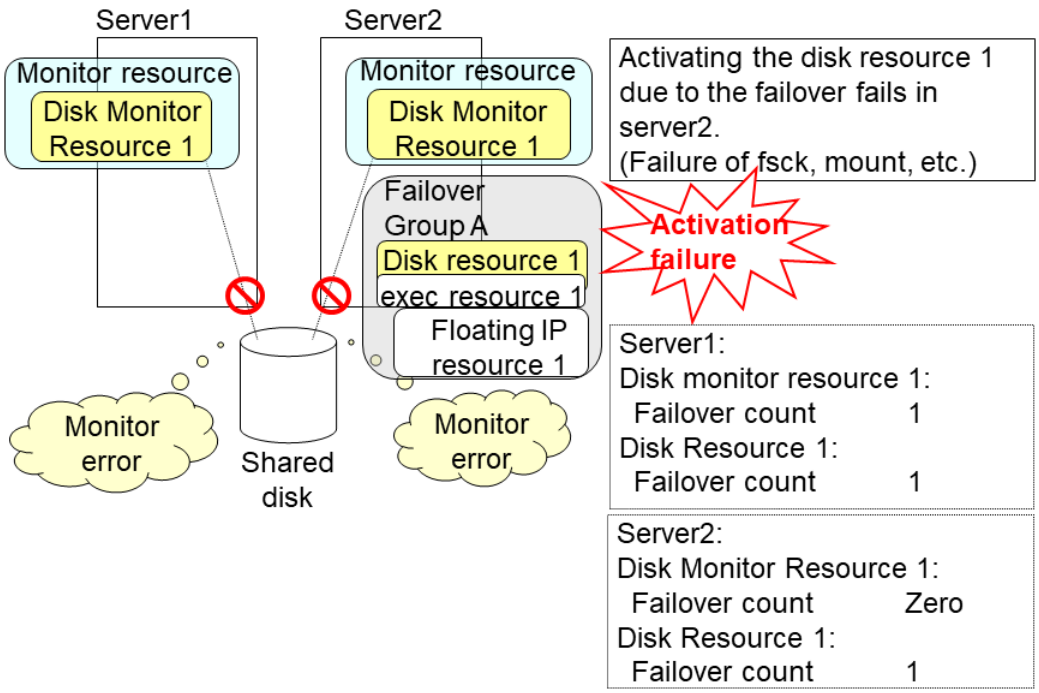
For more information on recovery executed by monitor resources against their recovery targets, see "*Action when an error is detected by monitor resource*".



An error can be detected in deactivation of the disk resource depending on the location of the disk device failure.

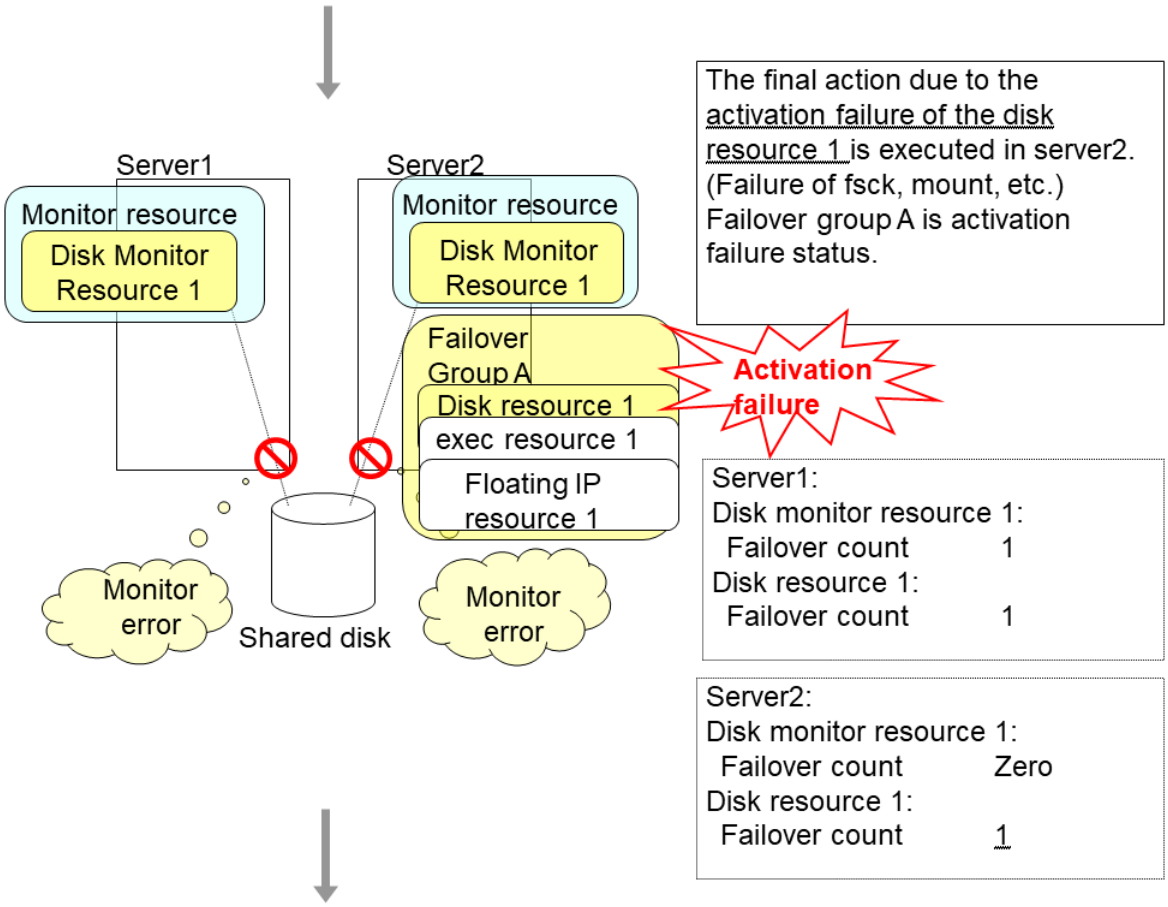


An error can be detected in deactivation of the disk resource depending on the location of the disk device failure.

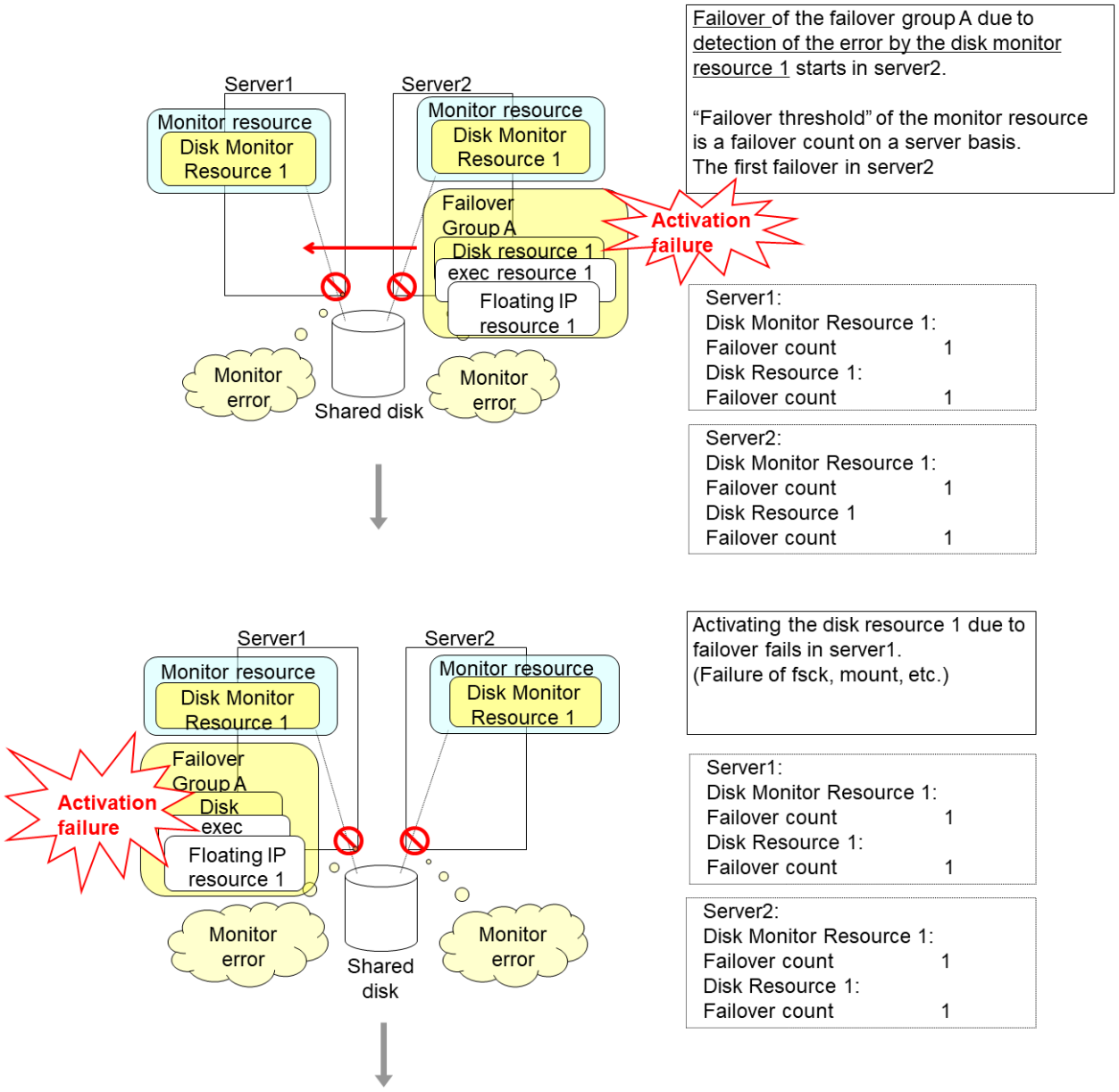


The final action is executed in server2 because the number of failovers due to failure of disk resource activation has exceeded its threshold.

However, note that activation ends abnormally without activating the rest of the group resources in the Failover Group A because "No operation (Next resources are not activated)" is selected as the final action.



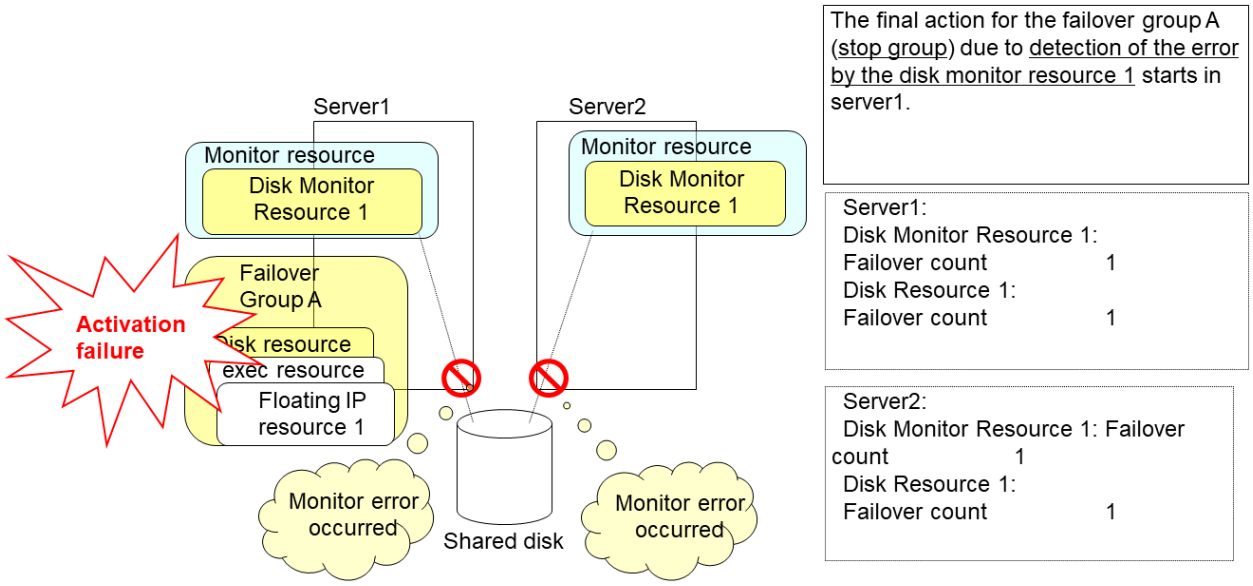
An error can be detected in deactivation of the disk resource depending on the location of the disk device failure.



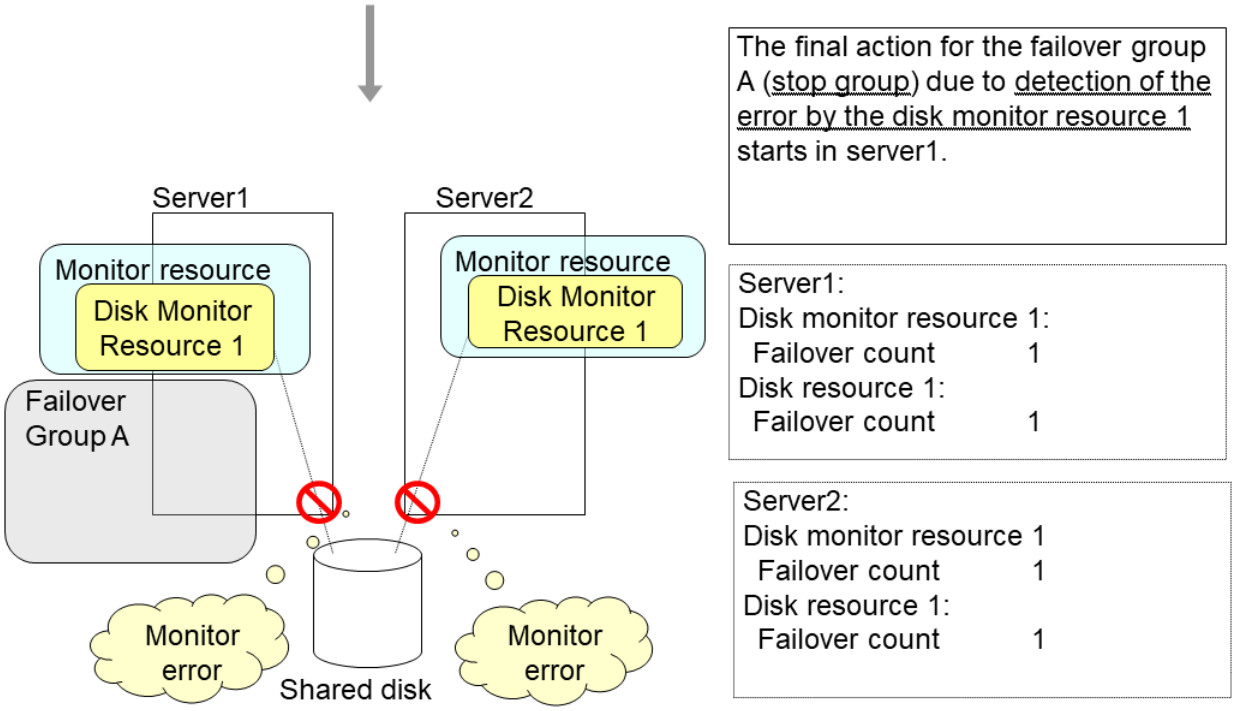
The final action is executed in server1 as is the case in server2 because the number of failovers due to failure of activating the disk resource 1 has exceeded the threshold.

However, note that activation ends abnormally without activating the rest of the group resources in the Failover Group A because "No operation (Next resources are not activated)" is selected as the final action.

An error can be detected in deactivation of the disk resource depending on the location of the disk device failure.



The final action is executed in server1 because the number of failovers due to monitoring error detected by the disk monitor resource 1 has exceeded the threshold.



After the Failover Group A is stopped due to the final action executed for the disk monitor resource 1 in server1, nothing will happen even if an error is detected by the disk monitor resource 1.

However, note that the final action for the disk monitor resource 1 is executed in server2 if the Failover Group A is manually activated because the final action for the disk monitor resource 1 is not executed yet.

4.1.9 Recovery/pre-recovery action script

Upon the detection of a monitor resource error, a recovery script can be configured to run. Alternatively, before the reactivation, failover, or final action of a recovery target, a pre-recovery action script can be configured to run.

The script is a common file.

Environment variables used in the recovery/pre-recovery action script

EXPRESSCLUSTER sets status information (the recovery action type) in the environment variables upon the execution of the script.

The script allows you to specify the following environment variables as branch conditions according to the operation of the system.

Environment variable	Value of the environment variable	Description
CLP_MONITORNAME ...Monitor resource name	Monitor resource name	Name of the monitor resource in which an error that causes the recovery/pre-recovery action script to run is detected.
CLP_VERSION_FULL ...EXPRESSCLUSTER full version number	EXPRESSCLUSTER full version number	EXPRESSCLUSTER full version number. (Example) 4.2.2-1
CLP_VERSION_MAJOR ...EXPRESSCLUSTER major version	EXPRESSCLUSTER major version	EXPRESSCLUSTER major version (Example) 4
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER installation path	Path of EXPRESSCLUSTER installation. (Example) /opt/nec/clusterpro
CLP_OSNAME ...Server OS name	Server OS name	Name of the server OS on which the script is executed. (Example) 1. When the OS name could be acquired: Red Hat Enterprise Linux Server release 6.8 (Santiago) 2. When the OS name could not be acquired: Linux

Continued on next page

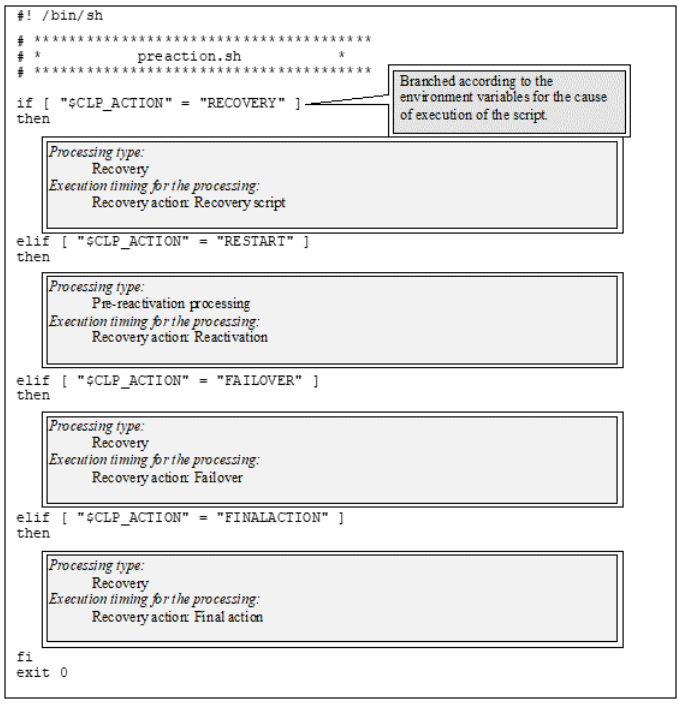
Table 4.5 – continued from previous page

Environment variable	Value of the environment variable	Description
CLP_OSVER ...Server OS version	Server OS version	Version of the server OS on which the script is executed. (Example) 1. When the OS name could be acquired:6.8 2. When the OS version could not be acquired: *None
CLP_ACTION ...Recovery action type	RECOVERY	Execution as a recovery script.
	RESTART	Execution before reactivation.
	FAILOVER	Execution before failover.
	FINALACTION	Execution before final action.
CLP_RECOVERYCOUNT ...Recovery script execution count	Recovery Script Execution Count	Count for recovery script execution.
CLP_RESTARTCOUNT ...Reactivation count	Reactivation count	Count for reactivation.
CLP_FAILOVERCOUNT ...Failover count	Failover count	Count for failover.

Writing recovery/pre-recovery action scripts

This section explains the environment variables mentioned above, using a practical scripting example.

Example of a recovery/pre-recovery action script



Tips for recovery/pre-recovery action script coding

Pay careful attention to the following points when coding the script.

- When the script contains a command that requires a long time to run, log the end of execution of that command. The logged information can be used to identify the nature of the error if a problem occurs. clplogcmd is used to log the information.
- How to use clplogcmd in the script
  With clplogcmd, messages can be output to Cluster WebUI Alert logs or OS syslog. For clplogcmd, see "*Outputting messages (clplogcmd command)*" in "8. *EXPRESSCLUSTER command reference*" in this guide.

  (Ex. : Scripting image)
  clplogcmd -m "recoverystart.."
  recoverystart
  clplogcmd -m "OK"

Note on the recovery/pre-recovery action script

- Stack size for commands and applications activated from the script
  The recovery/pre-recovery action script runs with the stack size configured to 2 MB. If the script has a command or application that requires a stack size of 2 MB or more to run, a stack overflow occurs.
  If a stack overflow error occurs, adjust the stack size before the command or application is activated.
- Condition that a pre-recovery action script is executed as the final action
  A pre-recovery action script is executed as the final action before the final action due to a monitor error detected by a monitor. Even if **No operation** is set as the final action, a pre-recovery action script is executed.
  If the final action is not executed because the maximum restart count has reached the upper limit or by the function to suppress the monitor resource recovery action or the function to suppress the final action when all

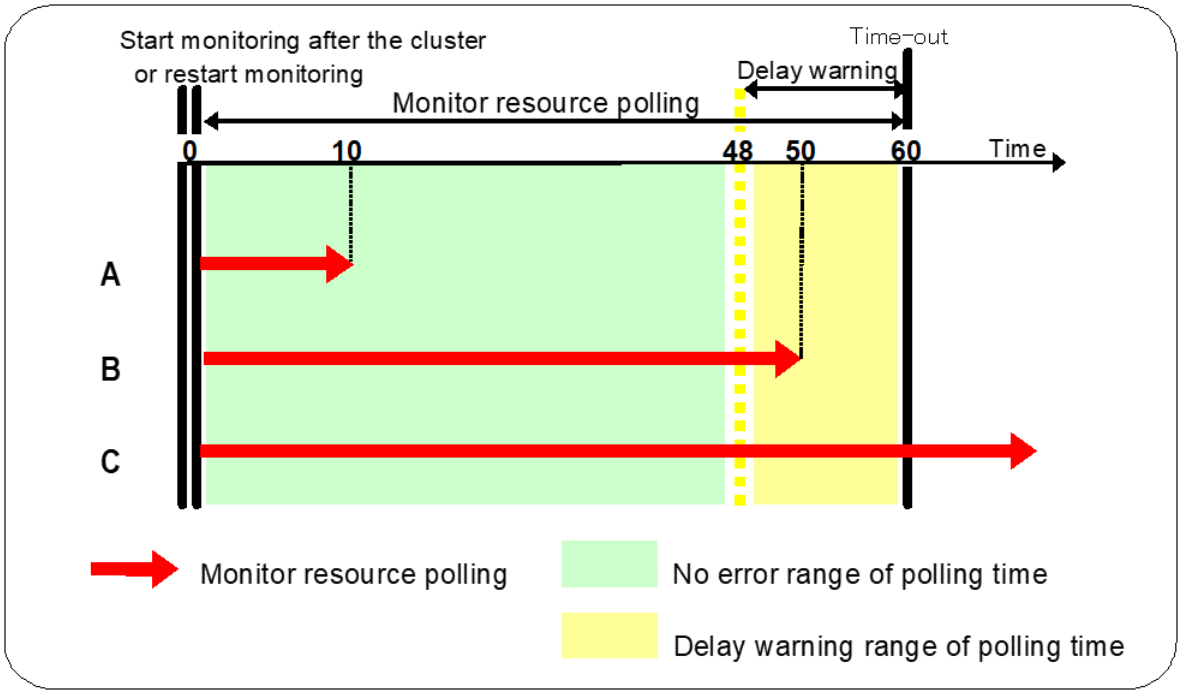
other servers are being stopped, a pre-recovery action script is not executed.

4.1.10 Delay warning of monitor resources

When a server is heavily loaded, due to a reason such as applications running concurrently, a monitor resource may detect a monitoring timeout. It is possible to have settings to issue an alert at the time when polling time (the actual elapsed time) reaches a certain percentages of the monitoring time before a timeout is detected.

The following figure shows timeline until a delay warning of the monitor resource is used.

In this example, the monitoring timeout is set to 60 seconds and the delay warning rate is set to 80%, which is the default value.



A. The polling time of monitoring is 10 seconds. The target of the monitor resource is in normal status.
In this case, no alert is used.

B. The polling time of monitoring is 50 seconds and the delay of monitoring is detected during this time. The target of the monitor resource is in the normal status.
In this case, an alert is used because the delay warning rate has exceeded 80%.

C. The polling time of monitoring has exceeded 60 seconds of the monitoring timeout and the delay of monitoring is detected. The target of the monitor resource has a problem.
In this case, no alert is used.

If the delay warning rate is set to 0 or 100:

- When 0 is set to the delay monitoring rate
  An alert for the delay warning is used at every monitoring.
  By using this feature, the polling time for the monitor resource can be calculated at the time the server is heavily loaded, which will allow you to determine the time for monitoring timeout of a monitor resource.
- When 100 is set to the delay monitoring rate
  The delay warning will not be is used.

Alert for the delay warning is used for the heartbeat resources as well.

For the user-mode monitor resource, the same delay monitoring rate as for the monitor resource is used.

Note: Be sure not to set a low value, such as 0%, except for a test operation.

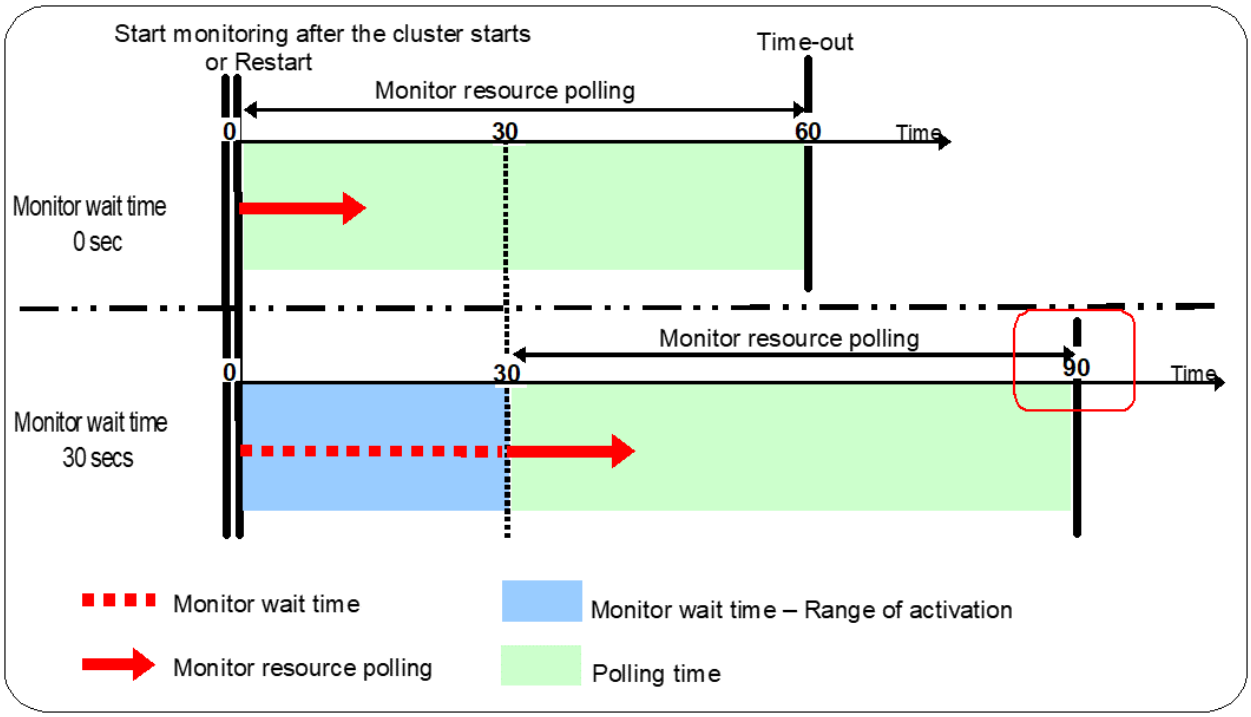
4.1.11 Waiting for monitor resource to start monitoring

"Wait Time to Start Monitoring" refers to start monitoring after the period of time specified as the waiting time elapses.

The following describes how monitoring differs when the wait time to start monitoring is set to 0 second and 30 seconds.

Configuration of monitor resource

<Monitor>
Interval 30 sec
Timeout 60 sec
Retry Count 0 times
Wait Time to Start Monitoring 0 sec / 30 sec



Note: Monitoring will start after the time specified to wait for start monitoring has elapsed even when the monitor resource is suspended and/or resumed by using the monitoring control commands.

The wait time to start monitoring is used when there is a possibility for monitoring to be terminated right after the start of monitoring due to incorrect application settings, such as the exec resource monitored by PID monitor resource, and

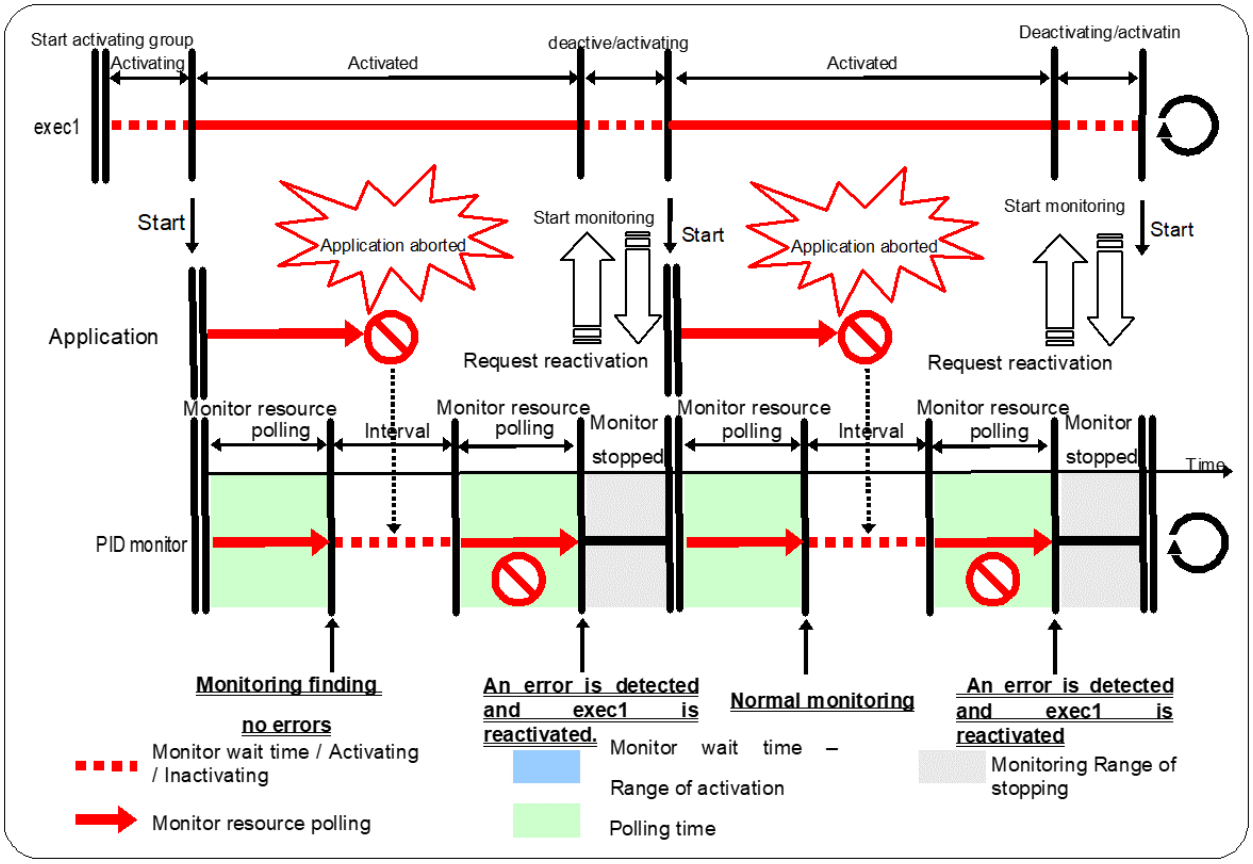
when they cannot be recovered by reactivation.

For example, when the monitor wait time is set to 0 (zero), recovery may be endlessly repeated. See the example below:

Configuration of PID Monitor resource

<Monitor>
Interval 5 sec
Timeout 60 sec
Retry Count 0 times
Wait Time to Start Monitoring 0 sec

<Error Detection>
Recover Target exec1
Maximum Reactivation Count 1 time
Maximum Failover Count 1 time
Final Action Stop Group



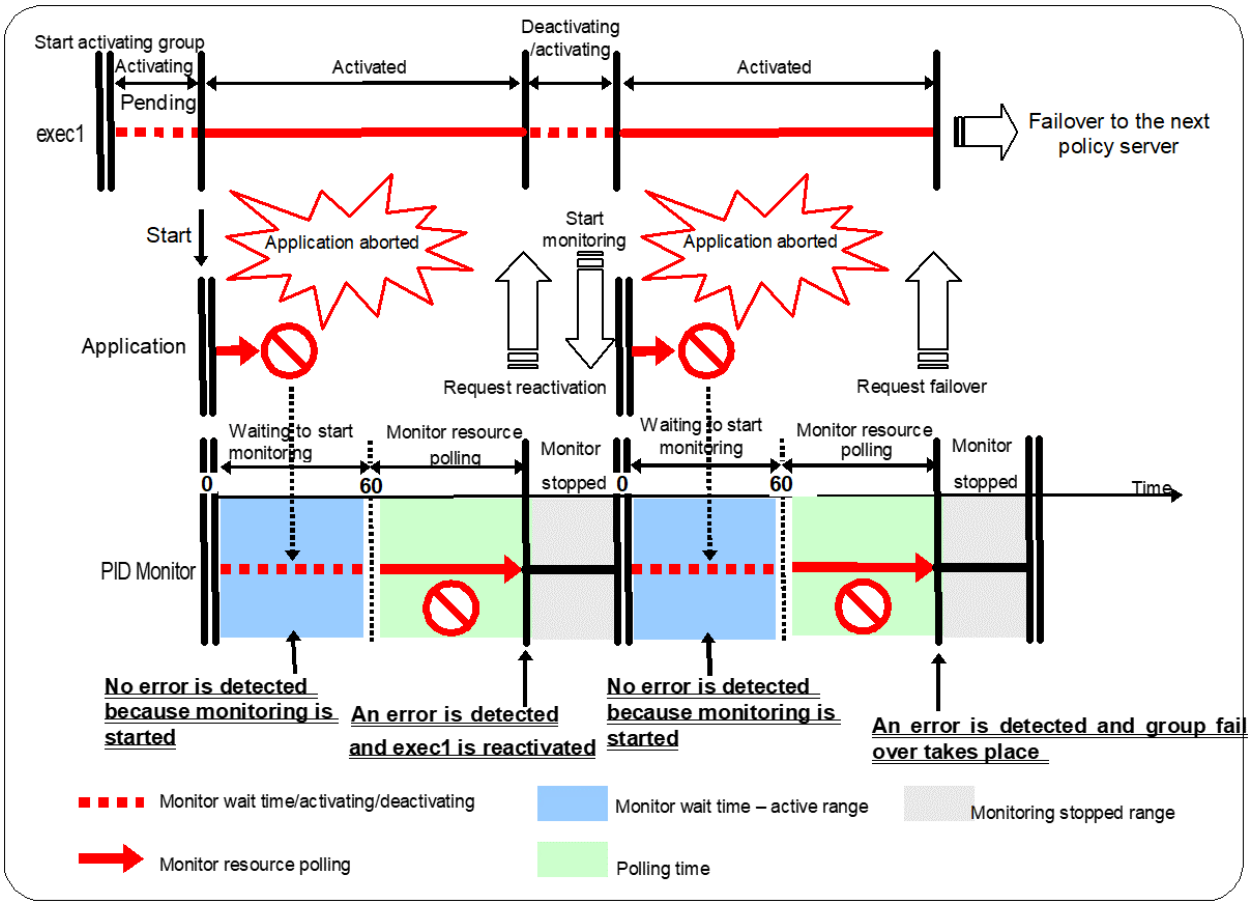
The reason why recovery action is endlessly repeated is because the initial monitor resource polling has terminated successfully. The current count of recoveries the monitor resource has executed is reset when the status of the monitor resource becomes normal (finds no error in the monitor target). Because of this, the current count is always reset to 0 and reactivation for recovery is endlessly repeated.

You can prevent this problem by setting the wait time to start monitoring. By default, 60 seconds is set as the wait time from the application startup to the end.

Configuration of PID monitor resource

<Monitor>
Interval 5 sec
Timeout 60 sec
Retry Count 0 times
Wait Time to Start Monitoring 60 sec

<Error Detection>
Recover Target exec1
Maximum Reactivation Count 1 time
Maximum Failover Count 1 time
Final Action Stop Group



If the application is abnormally terminated in the destination server of the group failover, the group stops as the final action.

4.1.12 Limiting the number of reboots when an error is detected by the monitor resource

When **Stop cluster service and shutdown OS** or **Stop cluster service and reboot OS** is selected as a final action to be taken when an error is detected by the monitor resource, the number of shutdowns or reboots can be limited.

Note:

The maximum reboot count is on a server basis because the number of reboots is recorded on a server basis.

The number of reboots caused by a final action in detection of error in group activation/deactivation and the number of reboots caused by a final action in detection of error by a monitor resource are recorded separately.

If the time to reset the maximum reboot count is set to zero (0), the number of reboots will not be reset.

The following is an example of the process when the number of reboots is limited.

As a final action, **Stop cluster daemon and reboot OS** is executed once because the maximum reboot count is set to one (1).

When the monitor resource finds no error in its target for 10 minutes after reboot following cluster shutdown, the number of reboots is reset because the time to reset the maximum reboot count is set to 10 minutes.

Examples of behavior when the following values are set.

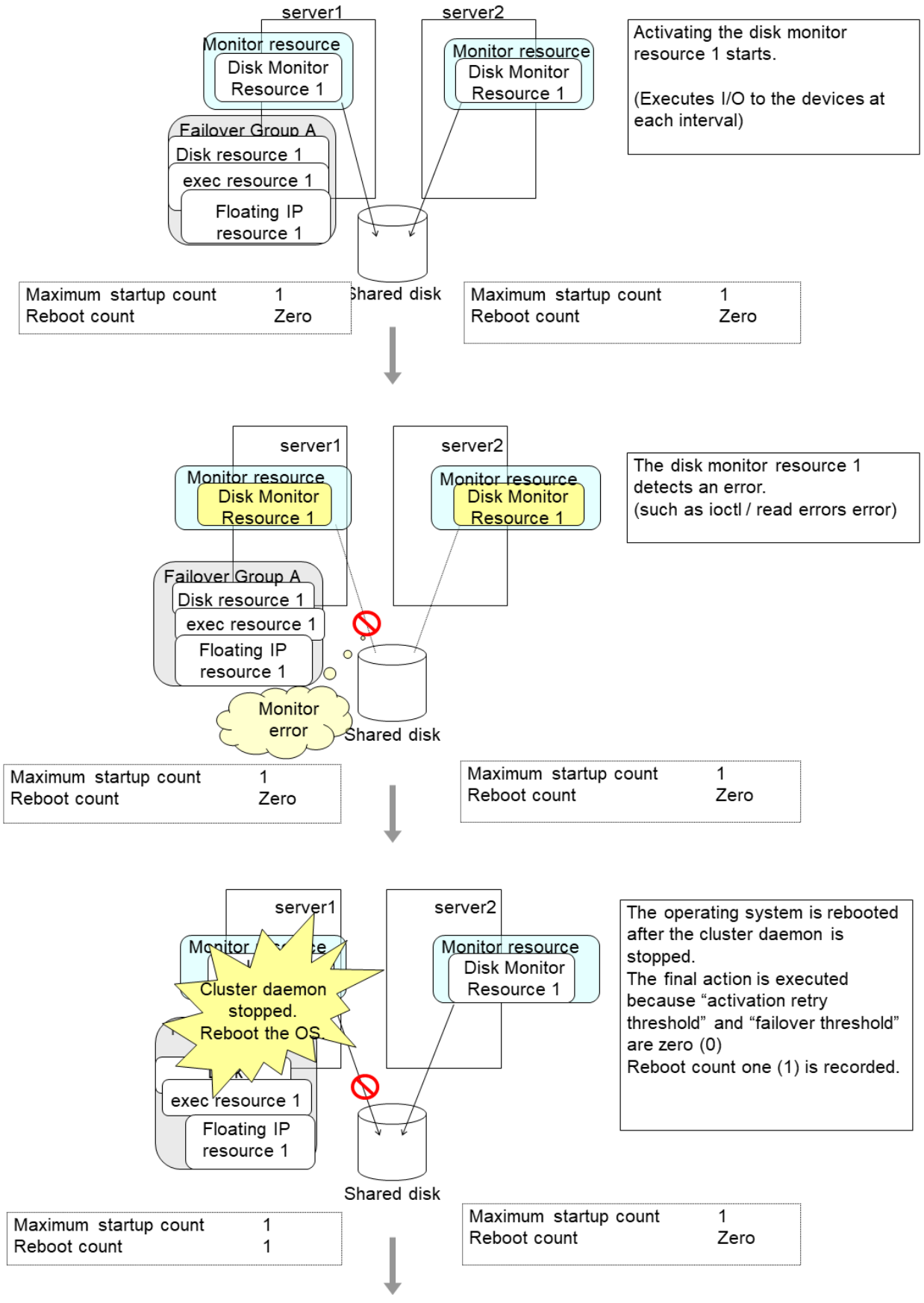
Configuration

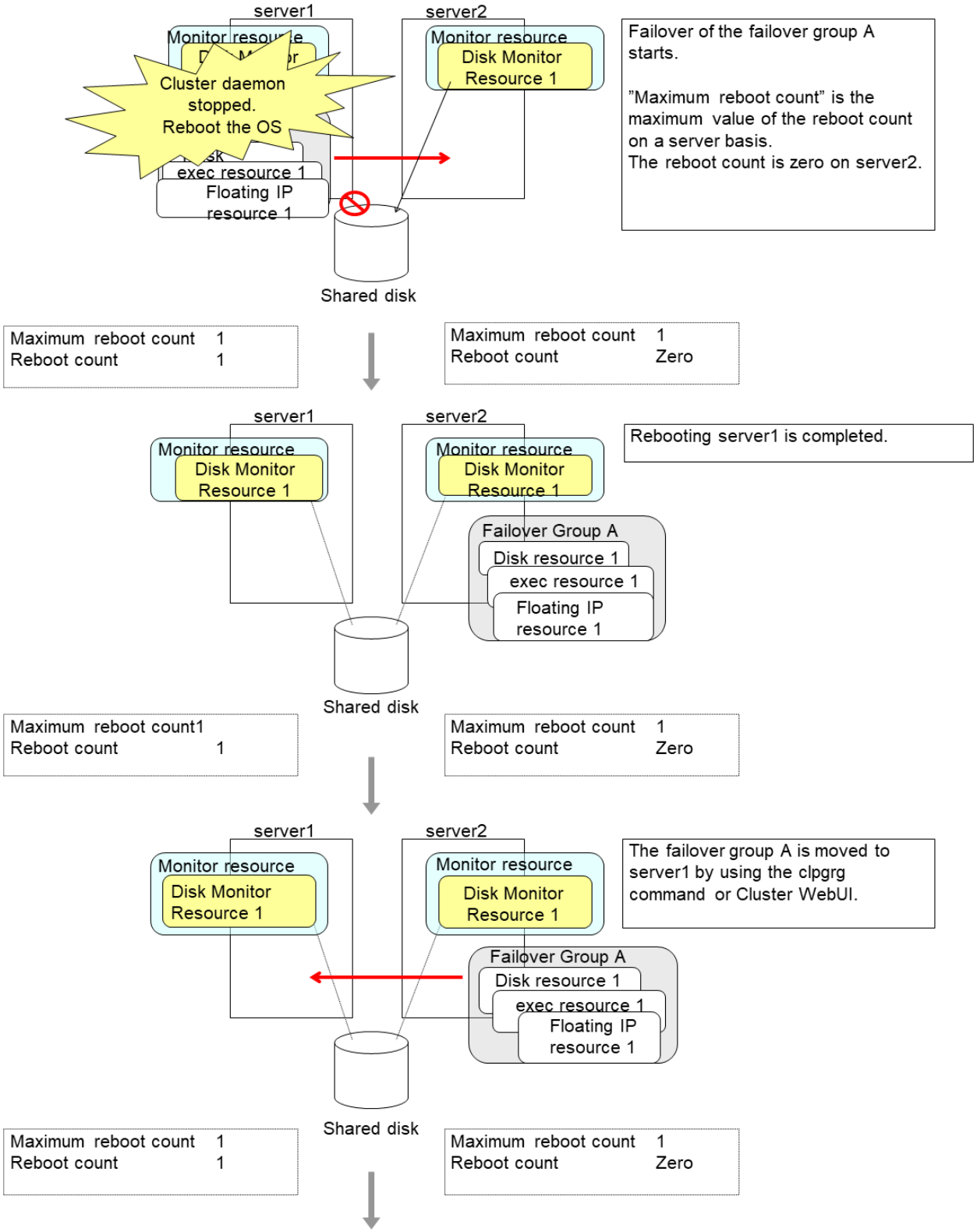
<Monitor>
Interval 60 sec
Timeout 120 sec
Retry Count 3 times

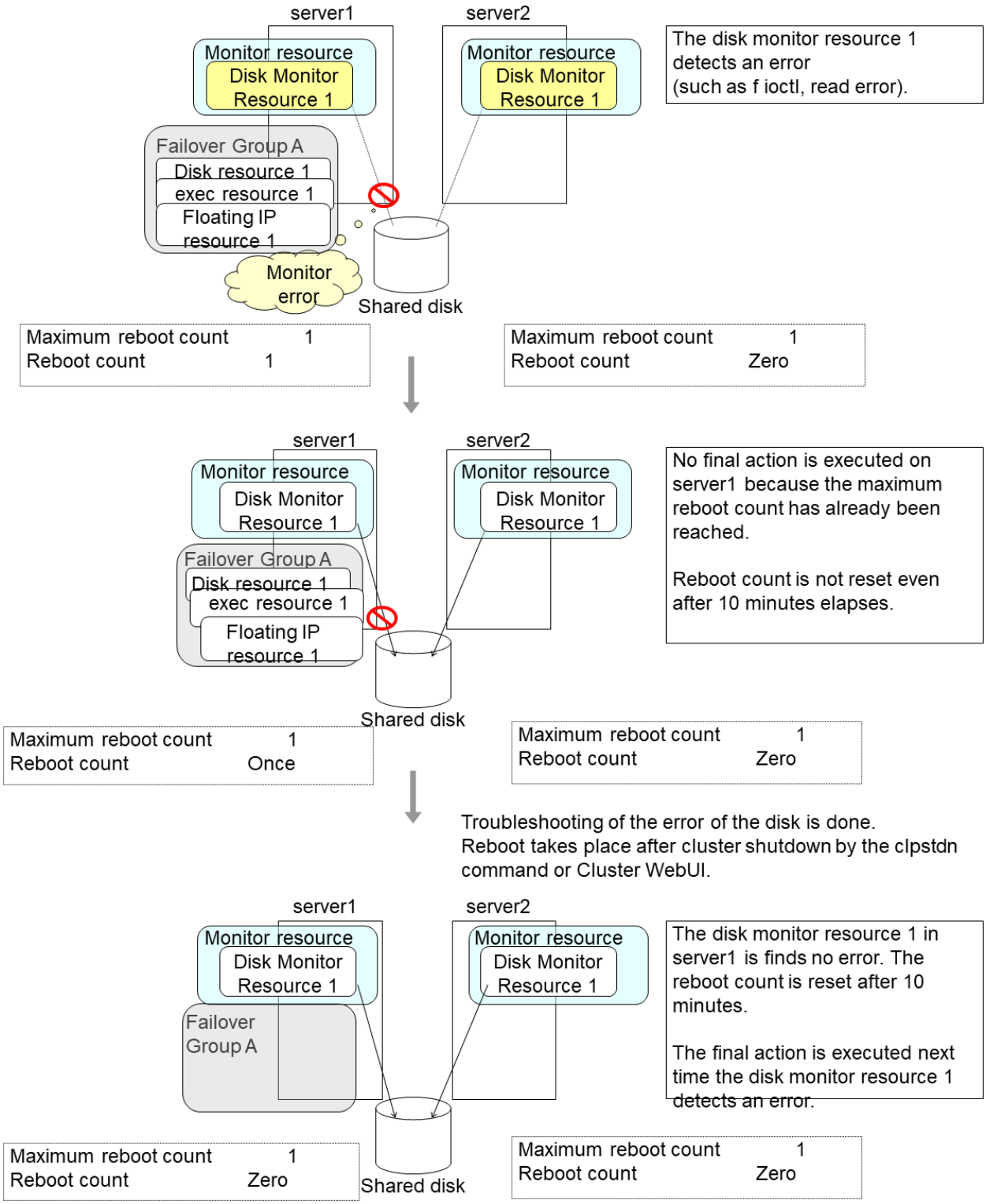
<Error detection>
Recovery Target Failover Group A
Maximum Reactivation Count 0 times
Maximum Failover Count 0 times
Final Action **Stop cluster daemon and reboot OS**

<Reboot count limit >
Maximum reboot count 1 time

Time to reset the maximum reboot count 10 minutes


server1
server2
Monitor resource
Disk Monitor Resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
Shared disk
Activating the disk monitor resource 1 starts.
(Executes I/O to the devices at each interval)
Maximum startup count 1
Reboot count Zero
Maximum startup count 1
Reboot count Zero
The disk monitor resource 1 detects an error.
(such as ioctl / read errors error)
Monitor error
Maximum startup count 1
Reboot count Zero
Maximum startup count 1
Reboot count Zero
Cluster daemon stopped.
Reboot the OS.
The operating system is rebooted after the cluster daemon is stopped.
The final action is executed because “activation retry threshold” and “failover threshold” are zero (0)
Reboot count one (1) is recorded.
Maximum startup count 1
Reboot count 1
Maximum startup count 1
Reboot count Zero


server1
server2
Monitor resource
Disk Monitor Resource 1
Cluster daemon stopped.
Reboot the OS
exec resource 1
Floating IP resource 1
Shared disk
Failover of the failover group A starts.
"Maximum reboot count" is the maximum value of the reboot count on a server basis.
The reboot count is zero on server2.
Maximum reboot count 1
Reboot count 1
Maximum reboot count 1
Reboot count Zero
Rebooting server1 is completed.
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
Maximum reboot count1
Reboot count 1
The failover group A is moved to server1 by using the clpgrg command or Cluster WebUI.


server1
server2
Monitor resource
Disk Monitor Resource 1
Failover Group A
Disk resource 1
exec resource 1
Floating IP resource 1
Monitor error
Shared disk
The disk monitor resource 1 detects an error (such as f ioctl, read error).
Maximum reboot count 1
Reboot count 1
Maximum reboot count 1
Reboot count Zero
No final action is executed on server1 because the maximum reboot count has already been reached.
Reboot count is not reset even after 10 minutes elapses.
Maximum reboot count 1
Reboot count Once
Maximum reboot count 1
Reboot count Zero
Troubleshooting of the error of the disk is done.
Reboot takes place after cluster shutdown by the clpstdn command or Cluster WebUI.
The disk monitor resource 1 in server1 is finds no error. The reboot count is reset after 10 minutes.
The final action is executed next time the disk monitor resource 1 detects an error.
Maximum reboot count 1
Reboot count Zero
Maximum reboot count 1
Reboot count Zero

4.1.13 Monitor priority of the monitor resources

To assign a higher priority for monitor resources to monitor when the operating system is heavily loaded, the nice value can be set.

- The nice value can be specified through minus 19 (low priority) to plus 20 (high priority). Detection of the monitor timeout can be controlled by setting a higher priority to the nice value.

4.1.14 IPMI command

Final actions **BMC Reset**, **BMC Power Off**, **BMC Power Cycle,** and **BMC NMI** use the ipmitool command.

If the commands are not installed, this function cannot be used.

Notes for the final action by ipmi

- Final Action by IPMI is achieved by associating EXPRESSCLUSTER and the ipmitool command.
- ipmitool(OpenIPMI-tools) is not shipped with EXPRESSCLUSTER. Users are required to install the rpm package by themselves.
- When executing the final action by the ipmitool command, the ipmi driver needs to be loaded. It is recommended to load the ipmi driver automatically at OS startup.

Chassis identify uses the ipmitool command.

If the commands are not installed, this function cannot be used.

Notes for chassis identify by ipmi

Chassis identify by ipmi is actualized by combining EXPRESSCLUSTER and the ipmitool command.

ipmitool(OpenIPMI-tools) is not shipped with EXPRESSCLUSTER. Users are required to install the rpm package by themselves.

4.1.15 Setting monitor resources on individual servers

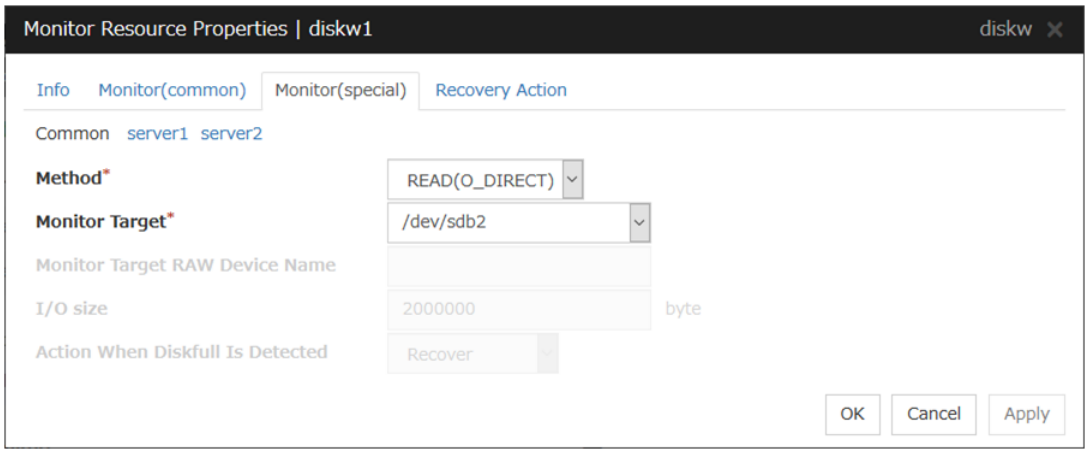
Some setting values of monitor resources can be set for individual servers. For the resources which can be configured on a server basis, the tabs of servers are displayed on the **Monitor(special)** tab.

The following monitor resources can be configured for individual servers.

Monitor resource name	Supported version
Disk monitor resource	4.0.0-1 or later
IP monitor resource	4.0.0-1 or later
NIC Link Up/Down monitor resource	4.0.0-1 or later
Message receive monitor resource	4.0.0-1 or later
AWS Elastic IP monitor resource	4.0.0-1 or later
AWS Virtual IP monitor resource	4.0.0-1 or later
AWS AZ monitor resource	4.0.0-1 or later
AWS DNS monitor resource	4.0.0-1 or later

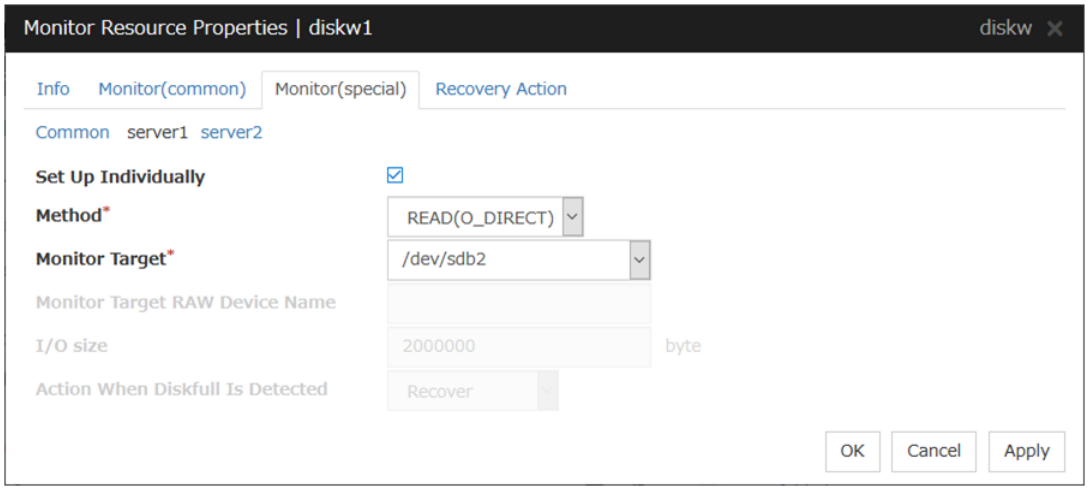
For the parameters that can be configured for individual servers, see the descriptions of parameters on monitor resources. On those parameters, the **Server Individual Setup** icon is displayed.

In the example below, configuring settings for each server on the disk monitor resource is described.



Server Individual Setup

Parameters that can be configured for individual servers on a disk monitor resource are displayed.



Set Up Individually

Click the tab of the server on which you want to configure server individual setting, and select this check box. The boxes for parameters that can be configured for individual servers become active. Enter required parameters.

4.1.16 Common settings for monitor resources of the monitoring option

This section describes the setting procedure for, and cautions related to, monitoring applications by using the monitor resources provided by the Application Server Agent, Database Agent, File Server Agent, Internet Server Agent, Java Resource Agent, and System Resource Agent (hereinafter referred to as "monitoring option").

Setting procedure of monitor resources of monitoring option

Follow the steps below to monitor applications by using monitor resources of the monitoring options.

In this example, DB2 monitor resource is used.

1. Create a failover group (for target monitoring application)

2. Add the EXEC resource for target monitoring application startup

3. Perform the test for target monitoring application startup

4. Add DB2 monitor resource for monitoring target monitoring application

The steps are described below.

Step 1 Create a failover group (for target monitoring application)

Create a failover group for monitoring the target monitoring application and performing a failover when an error occurs. Add group resources as necessary.

Note: For details on how to create failover groups and add group resources, see "Creating the cluster configuration data" in the "Installation and Configuration Guide".

Step 2 Add the EXEC resource for starting the target monitoring application

Add the EXEC resource for starting the target monitoring application to the failover group that you have created in Step 1, and edit it to start and finish the target monitoring application by its Start Script or Stop Script. In this guide, this EXEC resource is called exec 1.

Step 3 Confirmation test for target monitoring application startup

After completing the Steps 1 and 2, check that the monitored application is started normally. Modify the settings to the server, start, stop, move and fail over the group by the Cluster WebUI and confirm that those operations are performed normally.

Step 4 Add the DB2 monitor resource for starting target monitoring application

Add the DB2 monitor resource for monitoring the target monitoring application.

Select **Active** for **Monitor Timing** and specify **exec1** for **Target Resource** on the **Monitor (common)** tab.

Note: For specific information on the monitor resources and settings, see the section on monitoring option monitor resources in "*Monitor resource details*" in this guide.

See also:

For details on the monitoring settings common to monitor resources, see "*Monitor (common) tab*"

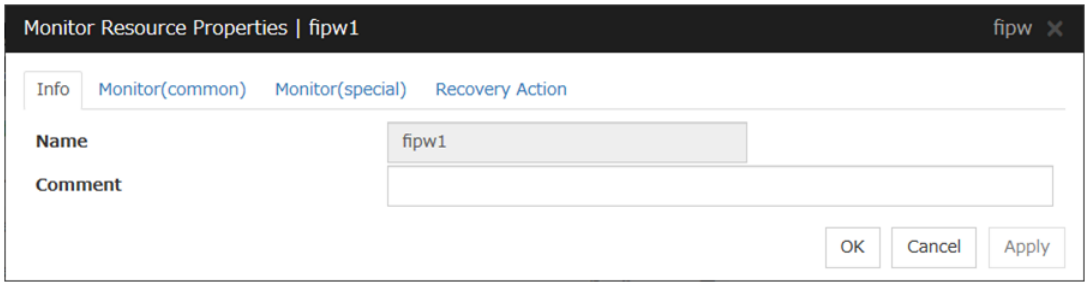
4.1.17 Cautions on monitoring option monitor resources

Cautions for using monitoring option monitor resources are as follows:

- For monitor resource db2w, ftpw, httpw, imap4w, mysqlw, odbcw, oraclew, pop3w, psqlw, sambaw, sqlserverw, sybasew, wasw, wlsw, otxw, and jraw a password is included as a property entry.
  This password is saved in plain text on the cluster configuration data file (clp.conf). Thus, it is recommended to create an account dedicated to monitoring other than for application and use it for security reasons.

4.2 Monitor resource properties

4.2.1 Info tab



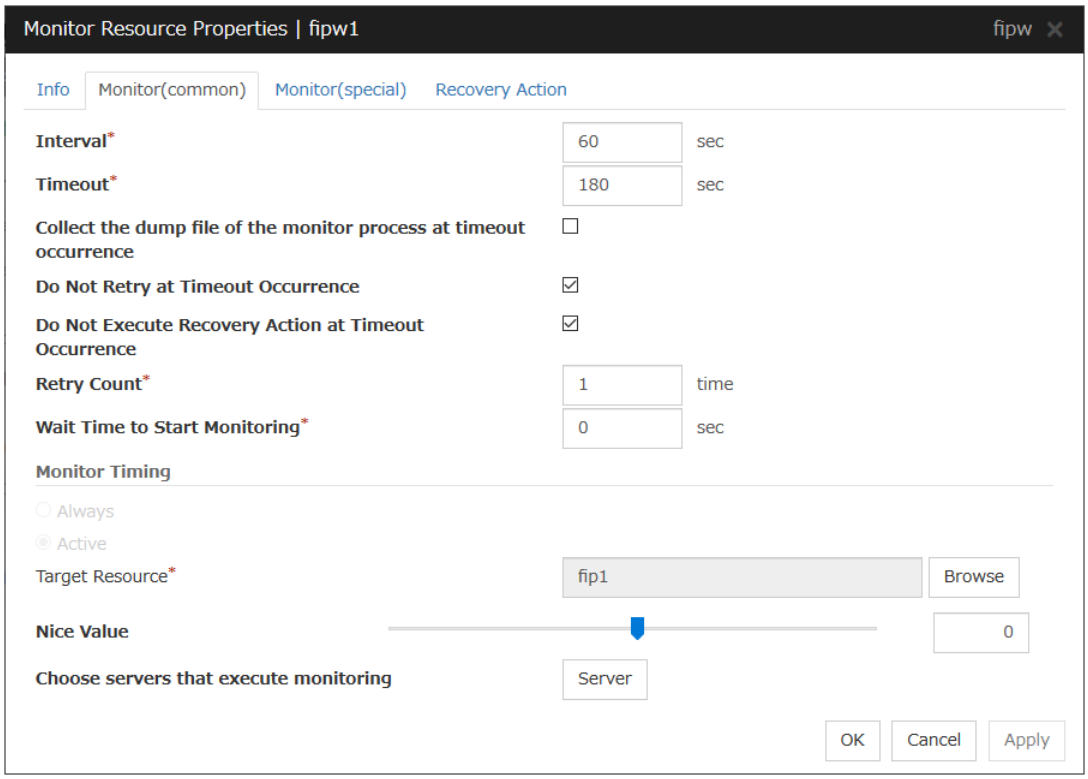
Name

The monitor resource name is displayed.

Comment (within 127 bytes)

Enter a comment for the monitor resource. Use only one-byte alphabets and numbers.

4.2.2 Monitor (common) tab



Interval(1 to 999)

Specify the interval to check the status of monitor target.

Timeout(5 to 999[5])

When the normal status cannot be detected within the time specified here, the status is determined to be error.

Collect the dump file of the monitor process at timeout occurrence

In case that this function is enabled, the dump information of the timed out monitor resource is collected when the monitor resource times out. The collected dump information is written to the /opt/nec/clusterpro/work/rm/"monitor_resource_name"/errinfo.cur folder. When dump is performed more than once, the existing folders are renamed errinfo.1, errinfo.2, and so on. Dump information is collected up to 5 times.

Do Not Retry at Timeout Occurrence

When this function is enabled, recovery action is executed immediately if a monitor resource timeout occurs.

Do Not Execute Recovery Action at Timeout Occurrence

When this function is enabled, recovery action is not executed if a monitor resource timeout occurs.

This can be set only when the Do Not Retry at Timeout Occurrence function is enabled.

Note: For the following monitor resources, the Do Not Retry at Timeout Occurrence and Do Not Execute Recovery Action at Timeout Occurrence functions cannot be set.

- User mode monitor resource
- Multi target monitor resource
- Virtual IP monitor resource
- Custom monitor resource (only when Monitor Type is **Asynchronous**)
- Message receive monitor resource
- VM monitor resource
- Dynamic DNS monitor resource
- BMC monitor resource
- Oracle Clusterware Synchronization Management monitor resource
- JVM monitor resource
- System monitor resource
- Process resource monitor resource

Retry Count(0 to 999)

Specify how many times an error should be detected in a row after the first one is detected before the status is determined as error. If this is set to zero (0), the status is determined as error at the first detection of an error.

Wait Time to Start Monitoring(0 to 9999)

Set the wait time to start monitoring.

Monitor Timing

Set the monitoring timing. Select the timing from:

[5] When ipmi is set as a monitoring method for the user-mode monitor resource, 255 or less should be specified.

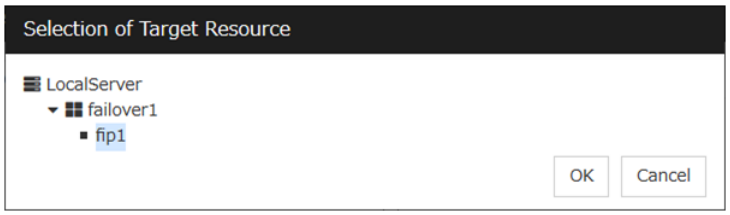
- Always:
  Monitoring is performed all the time.
- Active:
  Monitoring is not started until the specified resource is activated.

Target Resource

The resource which will be monitored when activated is shown.

Browse

Click this button to open the dialog box to select the target resource. The group names and resource names that are registered in the LocalServer and cluster are shown in a tree view. Select the target resource and click **OK**.



Nice Value

Set the nice value of a process.

Choose servers that execute monitoring

Choose the servers that execute monitoring.

All Servers

All servers monitor the resources.

Select

Servers registered in **Available Servers** monitor the resources. One or more servers need to be set to **Available Servers**.

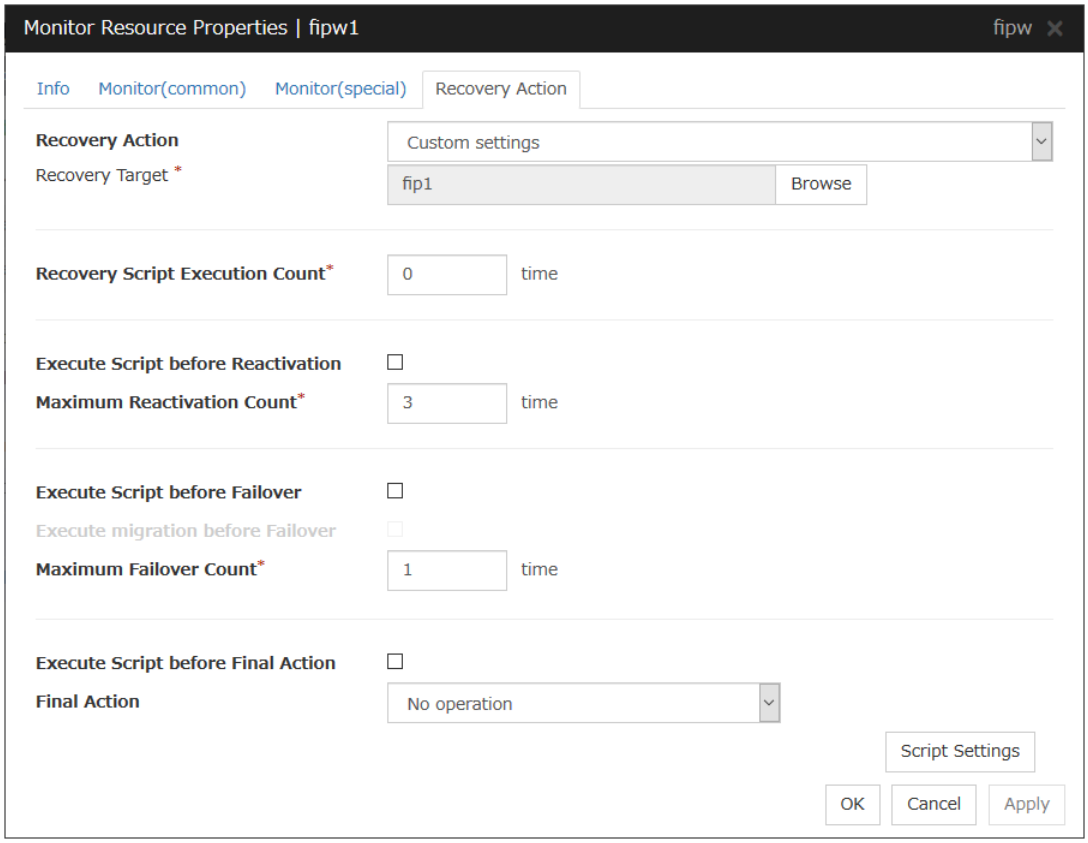
- **Add**
  Click this button to add a server selected in Available Servers **to** Servers that can run the Group**.**
- **Remove**
  Delete a server selected from Servers that can run the Group**.**

4.2.3 Monitor (special) tab

Some monitor resources require the parameters at the monitoring operaion to be configured. The parameters are described in the explanation part about each resource.

4.2.4 Recovery Action tab

In this dialog box, the recovery target and an action to be taken at the time when an error is detected can be configured. By setting this, it allows failover of the group, restart of the resource and cluster when an error is detected. However, recovery will not occur if the recovery target is not activated.



Recovery Action

Select a recovery action when detecting an error.

- Executing failover the recovery target
  When detecting a monitor error, execute failover to the group to which the groups or group resources selected as the recovery target belong.
- Restart the recovery target, and if there is no effect with restart, then failover
  Reactivate groups or group resources selected as the recovery target. If the reactivation fails, or the same error is detected after the reactivation, then execute failover.
- Restart the recovery target
  Reactivate the selected group or group resource as the recovery target.
- Execute only the final action
  Execute the selected action as the final action.

- Custom settings
  Execute the recovery script up until the maximum script execution count. If an error is continuously detected after script execution, reactivate the selected group or group resource as the recovery target up until the maximum reactivation count. If reactivation fails or the same error is continuously detected after reactivation, and the count reaches the maximum reactivation count, execute failover for the selected group or group resource as the recovery target, up until the maximum failover count. When failover fails or the same error is continuously detected after failover, and the count reaches the maximum failover count, execute the selected action as the final action.

Recovery Target

A target is shown, which is to be recovered when it is determined as a resource error.

Browse

Click this button to open the dialog box in which the target resource can be selected. The LocalServer, All Groups and group names and resource names that are registered in the cluster are shown in a tree view. Select the target resource and click **OK**.

Recovery Script Execution Count (0 to 99)

Specify the number of times to allow execution of the script configured by **Script Settings** when an error is detected. If this is set to zero (0), the script does not run.

Execute Script before Reactivation

- When the check box is selected:
  A script/command is executed before reactivation. To configure the script/command setting, click **Script Settings**.
- When the check box is not selected:
  Any script/command is not executed.

Maximum Reactivation Count(0 to 99)

Specify how many times you allow reactivation when an error is detected. If this is set to zero (0), no reactivation is executed. This is enabled when a group or group resource is selected as a recovery target.

When the group to which dynamic failover or a resource which belongs to that group is set as a recovery target of an IP monitor resource or NIC Link Up/Down monitor resource, reactivating the recovery target fails because a monitor resource registered in the exception list detects an error.

Execute Script before Failover

- When the check box is selected:
  A script/command is executed before failover. To configure the script/command setting, click **Script Settings**.
- When the check box is not selected:
  Any script/command is not executed.

Execute migration before Fail over

When the check box is selected, execute migration before executing failover at error detection.

Maximum Failover Count(0 to 99)

Specify how many times you allow failover after reactivation fails for the number of times set in **Maximum Reactivation Count** when an error is detected. If this is set to zero (0), no failover is executed. This can be settable when selecting "All Groups", a group or a group resource as the recovery target. When "All Groups" is selected, execute failover of all groups running on the server of which the monitor resource has detected errors.

Execute Script before Final Action

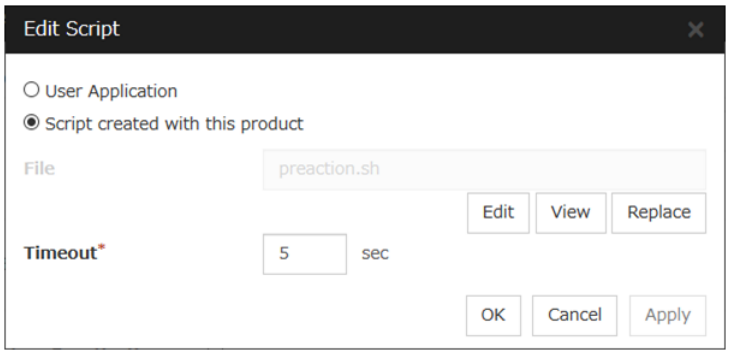
Select whether script is run or not before executing final action.

- When the check box is selected:
  A script/command is run before executing final action. To configure the script/command setting, click **Script Settings**.
- When the check box is not selected:
  Any script/command is not run.

When clicking **Script Settings** of **Execute Script before Final Action, Edit Script** dialogbox **is displayed. Set script or script file, and click OK.**

Script Settings

Click here to display the **Edit Script** dialog box. Configure the recovery or pre-recovery action script or commands.



User Application

Use an executable file (executable shell script file or execution file) on the server as a script. For the file name, specify an absolute path or name of the executable file of the local disk on the server. If there is any blank in the absolute path or the file name, put them in double quotation marks ("") as follows.

Example:
"/tmp/user application/script.sh"

Each executable file is not included in the cluster configuration information of the Cluster WebUI. They must be prepared on each server because they cannot be edited or uploaded by the Cluster WebUI.

Script created with this product

Use a script file which is prepared by the Cluster WebUI as a script. You can edit the script file with the Cluster WebUI if you need. The script file is included in the cluster configuration information.

File(Within 1023 bytes)

Specify a script to be executed (executable shell script file or execution file) when you select **User Application**.

View

Click here to display the script file when you select **Script created with this product**.

Edit

Click here to edit the script file when you select **Script created with this product**. Click **Save** the script file to apply the change. You cannot modify the name of the script file.

Replace

Click here to replace the contents of a script file with the contents of the script file which you selected in the **file selection** dialog box when you select **Script created with this product**. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not select binary files (applications), and so on.

Timeout (1 to 9999)

Specify the maximum time to wait for completion of script to be executed. The default value is set as 5.

Final Action

Select a final action to be taken after reactivation fails for the number of times set in **Maximum Reactivation Count**, and failover fails for the number of times set in **Maximum Failover Count** when an error is detected.

Select the final action from the options below:

- No Operation
  No action is taken.

  Note: Select **No Operation** only when (1) temporarily canceling the final action, (2) displaying only an alert when an error is detected, and (3) executing the final action by multi target monitor resource.

- Stop Resource
  When a group resource is selected as a recovery target, the selected group resource and group resources that depend on the selected group resource are stopped.
  This option is disabled when "LocalServer", "All Groups", or a group is selected.
- Stop Group
  When a group is selected as a recovery target, that group is stopped. When a group resource is selected as a recovery target, the group that the group resource belongs is stopped. When "All Groups" is selected, stop all the groups running on the server of which the monitor resource has detected errors.
  This option is disabled when "LocalServer" is selected as the recovery target.
- Stop cluster service
  Stops the cluster service of the server that detected an error.
- Stop cluster service and shutdown OS
  Stops the cluster service of the server that detected an error, and then shuts down the OS.
- Stop cluster service and reboot OS
  Stops the cluster service of the server that detected an error, and then reboots the OS.
- Generate intentionally stop error

Generate stop error intentionally to the server.

- Sysrq Panic
  Performs the sysrq panic.

Note: If performing the sysrq panic fails, the OS is shut down.

- Keepalive Reset
  Resets the OS using the clpkhb or clpka driver.

Note: If resetting keepalive fails, the OS is shut down. Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported.

- Keepalive Panic
  Performs the OS panic using the clpkhb or clpka driver.

Note: If performing the keepalive panic fails, the OS is shut down. Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported.

- BMC Reset
  Perform hardware reset on the server by using the ipmi command.

Note: If resetting BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC Power Off
  Powers off the OS by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

Note: If powering off BMC fails, the OS is shut down. Do not select this action on the server whereOpenIPMI is not installed, or the ipmitool command does not run.

- BMC Power Cycle
  Performs the power cycle (powering on/off) of the server by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

Note: If performing the power cycle of BMC fails, the OS is shut down. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- BMC NMI
  Uses the ipmi command to cause NMI occur on the server. Actions after NMI occurrence depend on the OS settings.

Note: If BMC NMI fails, the OS shutdown is performed. Do not select this action on the server where OpenIPMI is not installed, or the ipmitool command does not run.

- I/O Fencing(High-End Server Option)
  It can't be used.

Note: If I/O Fencing(High-End Server Option) fails, the OS shutdown is performed.

Collect Dump at Timeout

Select whether to enable this function.

Length: Within 4 bytes

Default value: 0 (disabled)

4.3 Understanding the disk monitor resources

Disk monitor resources monitor disk devices.

It is recommended to use the READ (O_DIRECT) monitoring method for disks where disk monitor resources cannot be used (TUR method).

4.3.1 Monitoring by disk monitor resources

Two ways of monitoring are employed by the disk monitor resource: READ and TUR.

- Notes on TUR:
  - You cannot run the Test Unit Ready and the SG_IO command of SCSI on a disk or disk interface (HBA) that does not support it. Even if your hardware supports this command, consult the driver specifications because the driver may not support it.
  - ioctl may be incorrectly executed for an LVM logical volume (LV) device. Use READ for LV monitoring.
  - A TUR method cannot be used for the IDE interface disk.
  - In the case of the disk of S-ATA interface, it may be recognized as the IDE interface disk (hd) or as the SCSI interface disk (sd) depending on the type of a disk controller and the distribution to be used. When the disk is recognized as the IDE interface, no TUR methods can be used. If the disk is recognized as the SCSI interface, TUR (genetic) cannot be used but TUR (legacy) can be used.
  - Test Unit Ready, compared to Read, burdens OS and disks less.
  - In some cases, Test Unit Ready may not be able to detect actual errors in I/O to media.
  - You cannot use a partition on the disk by setting it as the target to be monitored. A whole device (whole disk) must be specified.
  - Some disk devices may temporarily return Unit Attention at TUR issue, depending on the device status. The temporary return of Unit Attention does not signify a problem. If the TUR retry count is set to 0, however, the above return is determined to be an error and the disk monitor resource becomes abnormal. To avoid this meaningless error detection, set the retry count to one or more.

For the TUR monitoring, one of the following is selected:

- TUR
  - ioctl is used by the following steps and the status of the device is determined by the result of the command:

Run the ioctl (SG_GET_VERSION_NUM) command. The status is determined by the return value of ioctl and the version of SG driver.

If the ioctl command runs successfully and the version of SG driver is 3.0 or later, execute ioctl TUR (SG_IO) using the SG driver.

If the ioctl command fails or the version of SG driver is earlier than 3.0, execute ioctl TUR which is defined as a SCSI command.

- TUR (legacy)
  - Monitoring is performed by using ioctrl (Test Unit Ready). Test Unit Ready (TUR) which is defined as a SCSI command is used against the specified device, and the status of the device is determined by the result of the command.
- TUR (generic)
  - Monitoring is executed by using ioctl TUR (SG_IO). ioctl TUR (SG_IO) which is defined as a SCSI command is used against the specified device, and the status of the device is determined by the result of the command. Even with a SCSI disk, SG_IO may not work successfully depending on the OS or distribution.

The following is the READ monitoring:

- READ
  - The specified size of the specified device (disk device or partition device) or file is read. Judgment is performed by the size that could be read.
  - Dummy Read is for determining if the specified size of data can be read. Validity of the data read is not judged.
  - Burden of the load experienced by the OS and disk is proportional to the size of the data on the specified disk to be read
  - See "*I/O size when READ is selected for disk monitor resources*" to configure the read size.

The following is the READ (O_DIRECT) monitoring:

- READ (O_DIRECT)
  - A single sector on the specified device (disk device or partition device) or the file are read without using the cache (O_DIRECT mode), and the results are (the size of the data successfully read) are used to make a judgment.
  - Judgment is based on whether or not reading has been performed successfully. Validity of the read data is not judged.

The following describes READ (raw) monitoring:

- READ (raw)
  - Like the READ (O_DIRECT) monitoring method, the process to read the specified device is monitored without using the OS cache.
  - Whether reading was successful is checked. The validity of read data is not checked.
  - When the READ (raw) monitoring method is specified, partitions that have been or will possibly be mounted cannot be monitored. In addition, a whole device (whole disk) that includes partitions that have been or will possibly be mounted cannot be monitored. Allocate a partition dedicated to monitoring and specify it as the disk monitor resource. (Allocate 10 MB or more to the monitoring partition).
  - Do not register a raw device that is already registered in the **Disk I/F** list or **Disk Resource** under the server properties. For details on the VxVM volume raw device, see "Notes when creating EXPRESSCLUSTER configuration data" , "Verifying raw device for VxVM" in "Notes and Restrictions" of the "Getting Started Guide".

  - When monitoring the raw device used by the disk heartbeat by using the READ (raw) monitoring method, specify the raw device for **Monitor Target Raw Device Name in Cluster WebUI. Do not fill in Device Name.**

The following describes READ (VXVM) monitoring:

- READ (VXVM)
  - Like the READ (O_DIRECT) monitoring method, the process to read the specified device is monitored without using the OS cache.
  - Whether reading was successful is checked. The validity of read data is not checked.
  - The READ (VXVM) monitoring method can be used only when the file system of the volume raw device is vxfs.

The following is the WRITE (FILE) monitoring:

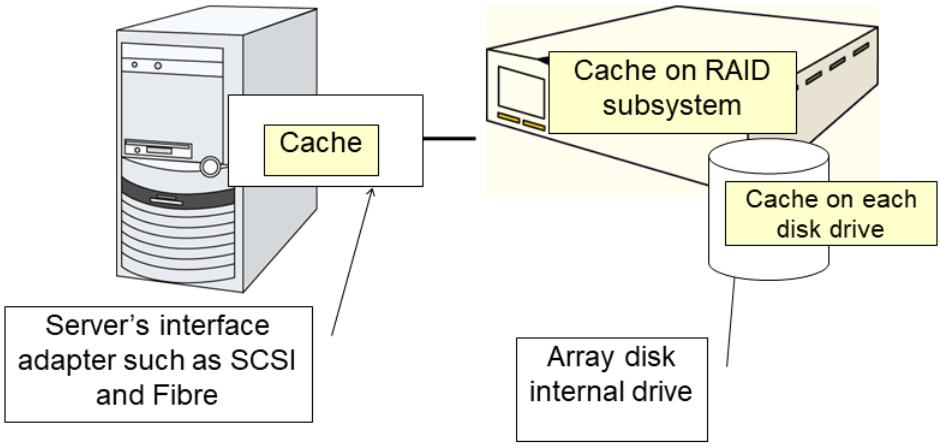
- WRITE (FILE)
  - The file of the specified path is created, written, and deleted to be judged. Validity of the written data is not judged.

4.3.2 I/O size when READ is selected for disk monitor resources

Enter the size of data when READ is selected as a method of monitoring.

Depending on the shared disk and interfaces in your environment, various caches for reading may be implemented. Because of this, when the specified read size is too small, READ may hit in cache, and may not be able to detect read errors.

When you specify a READ I/O size, verify that READ can detect I/O errors on the disk with that size by intentionally creating I/O errors.

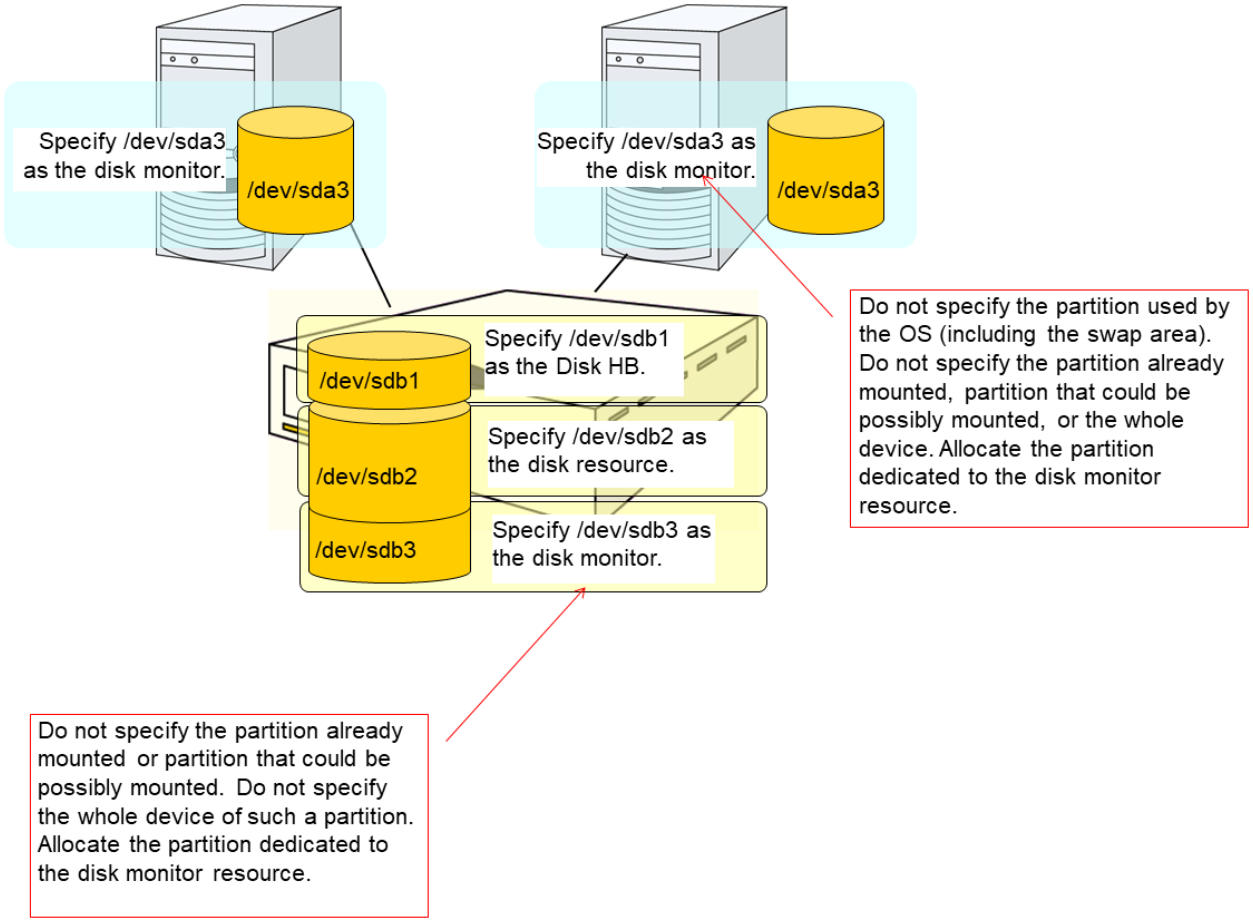


Note: This figure illustrates a typical concept of shared disks. This is not always applicable to array unit universally.

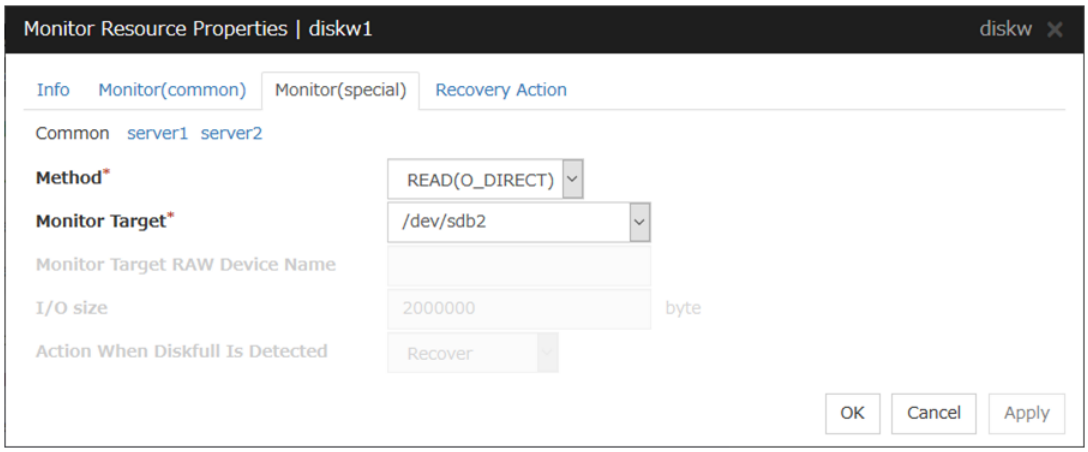
4.3.3 Setup example when READ (raw) is selected for the disk monitor resource

Example of setting up disk resources and disk monitoring

- Disk Resource
- Disk Monitor Resource (The HDDs installed in both servers are monitored in the READ (raw) mode.)
- Disk Monitor Resource (The shared disk is monitored in the READ (raw) mode.



4.3.4 Monitor (special) tab



Method Server `Individual Setup`

Select the method used to monitor the disk device from the following:

- TUR
- TUR(generic)
- TUR(legacy)
- READ
- READ (O_DIRECT)
- WRITE (FILE)
- READ (RAW)
- READ (VXVM)

Monitor Target (Within 1023 bytes) `Server Individual Setup`

- When the monitoring method is WRITE (FILE):
  Specify the path name of the file to be monitored. The name needs to begin with [/].
  Specify the file name with the absolute path. If you specify the file name of an existing file, it is overwritten and the data in the file is lost.
- When the monitoring method is READ (O_DIRECT)
  Specify a path name of the device file or file to monitor. The name must begin with a forward slash (/).
  Use an absolute path of the device file name or file name.
  If a file name is specified, the file must have been created beforehand.
  Do not specify a mirror partition device (such as /dev/NMP1) as the monitor target.
- When the monitoring method is READ (RAW)
  The monitor target may be omitted. However, the monitor target raw device name must be specified. Specify this mode only when binding and monitoring the device. It is not possible to specify the device name for a partition device that has been mounted or will possible be mounted for monitoring.
  In addition, a whole device (whole disk) of a partition device that has been mounted or will possibly be mounted cannot be specified for monitoring. Allocate a partition dedicated to monitoring. (Allocate 10 MB or more to the monitoring partition).The name must begin with a forward slash (/).
- When the monitoring method is READ (VXVM)
  The fields are dim and not selectable.

- When the monitoring method is READ
  Specify the name of the disk device or file to be used to monitor the disk device. The name must begin with a forward slash (/). If a file name is specified, the file must have been created beforehand. If a disk resource exists, the device name specified for the disk resource can be selected. If a mirror disk resource exists, the data partition device name specified for the mirror or hybrid disk resource can be selected.
- When the monitoring method is other than the above
  Specify the name of the disk device to monitor. The name must begin with a forward slash (/). If a disk resource exists, the device name specified for the disk resource can be selected. If a mirror disk resource exists, the data partition device name specified for the mirror or hybrid disk resource can be selected.

Monitor Target RAW Device Name (Within 1023 bytes) `Server Individual Setup`

This can be specified only when the monitoring method is READ (raw) or READ (VXVM).

- When the monitoring method is READ (raw)
  Enter a device name for raw accessing. A raw device that is already registered in the Disk I/F list under the server properties cannot be registered. Select READ (VXVM) as the monitoring method when monitoring a VxVM volume raw device.
- When the monitoring method is READ (VXVM)
  Specify a VxVM volume raw device name. The READ (VXVM) monitoring method can be used only when the file system of the volume raw device is vxfs. The name must begin with a forward slash (/).
  - To create an association with a disk resource, specify the dependent disk resource for **Target Resource** in "*Monitor (common) tab*" Specify that monitoring start after the specified disk resource is activated.

I/O Size (1 to 99999999) `Server Individual Setup`

Specify the size of I/O for reading or reading/writing when READ or WRITE (FILE) is selected as a monitoring method.

- When READ (RAW) , READ(O_DIRECT) or READ (VXVM) is specified, the **I/O size** text box is dim. A single sector is read from the target device.
- If TUR, TUR (generic), or TUR (legacy) is specified, this setting is ignored.

Action When Diskfull is Detected `Server Individual Setup`

Select the action when diskfull (state in which the disk being monitored has no free space) is detected.

- Recover
  The disk monitor resource recognizes an error upon the detection of disk full.
- Do not recover
  The disk monitor resource recognizes a caution upon the detection of disk full.

Note: If READ, READ (RAW), READ (VXVM), READ (O_DIRECT), TUR, TUR (generic), or TUR (legacy) is specified, the **Action when diskfull is detected** option is grayed out.

When a local disk is specified in **Target Device Name**, a local disk on the server can be monitored.

- Example of settings to monitor the local disk /dev/sdb by READ method, and to reboot the OS when an error is detected:

Option	Value	Remarks
Target Device Name	/dev/sdb	SCSI disk in the second machine.
Method	READ	READ method.
Recovery Target	Nothing	-
Final Action	Stop cluster service and reboot OS	Reboot the OS.

- Example of settings to monitor the local disk /dev/sdb by TUR (generic) method, and select No Operation (sending an alert to the Cluster WebUI only) as the final action when an error is detected:

Option	Value	Remarks
Target Device Name	/dev/sdb	SCSI disk in the second machine.
Method	TUR(generic)	SG_IO method
Final Action	No Operation	

4.4 Understanding IP monitor resources

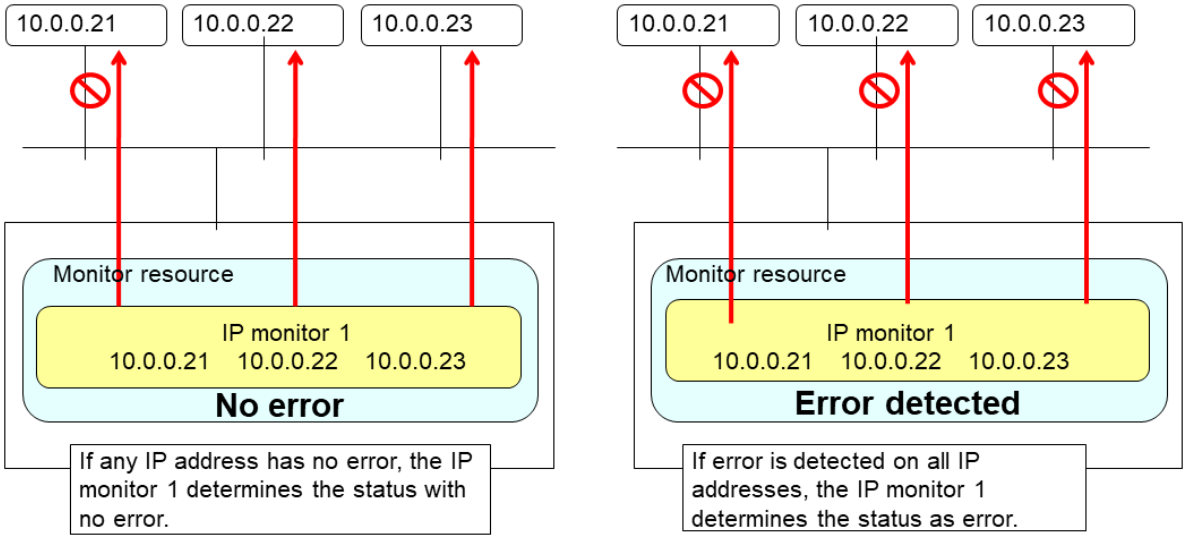
IP monitor resource monitors IP addresses using the ping command.

4.4.1 Monitoring by IP monitor resources

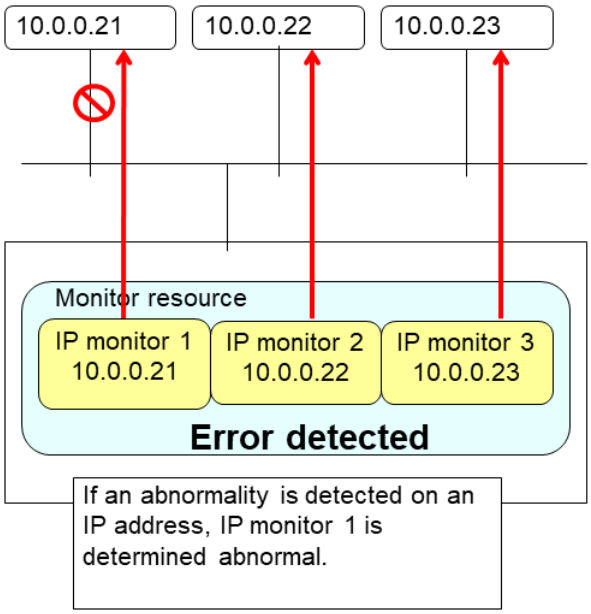
IP monitor resource monitors specified IP addresses by using the ping command. If all IP addresses do not respond, the status is determined to be error.

To check the responses of IP addresses, packet types 0 (Echo Reply) and 8 (Echo Request) of ICMP are used.

- If you want to establish error when all of the multiple IP addresses have error, register all those IP addresses with one IP monitor resource.



- If you want to establish error when any one of IP addresses has an error, create one IP monitor resource for each IP address.

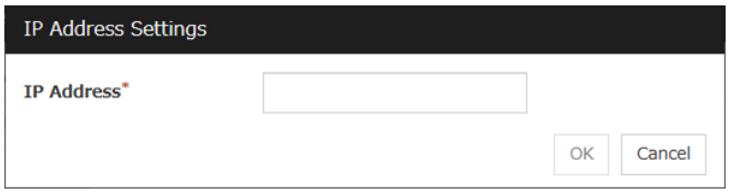


4.4.2 Monitor (special) tab

IP addresses to be monitored are listed in **IP Addresses**.

Add

Click **Add** to add an IP address to be monitored. A dialog box where an IP address can be entered is displayed.



IP Address (Within **255 bytes**) `Server Individual Setup`

Enter an IP address or a host name to be monitored in this field and click **OK**. The IP address or host name you enter here should be the one that exists on the public LAN. If a host name is set, the name resolution in the OS (such as adding an entry to /etc/hosts) should be configured.

Remove

Click **Remove** to remove an IP address selected in **IP Addresses** from the list so that it will no longer be monitored.

Edit

Click **Edit** to display the **IP Address Settings** dialog box. The dialog box shows the IP address selected in **IP Addresses** on the **Parameter** tab. Edit the IP address and click **OK**.

4.5 Understanding floating IP monitor resources

Floating IP monitor resources monitor floating IP resources.

4.5.1 Monitoring by floating IP monitor resources

Floating IP resources monitor floating IP resources in a server where they are activated. Floating IP monitor resources monitor whether floating IP addresses exist in the list of IP addresses. If a floating IP address does not exist in the list of IP addresses, it is determined to be an error.

Floating IP resources monitor Link Up/Down of NIC where a floating IP address is active. If NIC link down is detected, it is considered as an error. In some NIC boards and drivers, the required ioctl() may not be supported. In such a case, monitoring cannot be performed.

You can check the availability of the NIC Link Up/Down monitor by using the [ethtool] command provided by the distributor. For the check method using the [ethtool] command, see "*Note on NIC Link Up/Down monitor resources*" in "*Understanding NIC Link Up/Down monitor resources*" of this guide.

4.5.2 Note on floating IP monitor resources

- This monitor resource is automatically registered when a floating IP resource is added. A floating IP monitor resource corresponding to a floating IP resource is automatically registered.

  Floating IP monitor resources are initially defaulted, so configure appropriate resource settings as needed.

4.5.3 Monitor (special) tab

Monitor NIC Link Up/Down

Specify whether to monitor NIC Link Up/Down. If you have enabled, you can monitor the NIC Link Up/Down for the NIC that granted the floating IP. For this reason, a new set of NIC Link Up/Down monitor resource for the NIC that granted the floating IP is not required.

4.6 Understanding NIC Link Up/Down monitor resources

4.6.1 System requirements for NIC Link Up/Down monitor resource

Network interfaces supporting NIC Link Up/Down monitor resource

NIC Link Up/Down monitor resource has been tested to work in the following network interfaces.

Ethernet Controller(Chip)	Bus	Driver version
Intel 82557/8/9	PCI	3.5.10-k2-NAPI
Intel 82546EB	PCI	7.2.9
Intel 82546GB	PCI	7.3.20-k2-NAPI 7.2.9
Intel 82573L	PCI	7.3.20-k2-NAPI
Intel 80003ES2LAN	PCI	7.3.20-k2-NAPI
Broadcom BCM5721	PCI	7.3.20-k2-NAPI

4.6.2 Note on NIC Link Up/Down monitor resources

Some NIC boards and drivers do not support required ioctl( ).
Use the ethtool command distributors provide to check whether or not NIC Link Up/Down monitor resource runs. .

```
ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supports auto-negotiation: Yes
    Advertised link modes: 10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 0
    Transceiver: internal
    Auto-negotiation: on
    Supports Wake-on: umbg
    Wake-on: g
    Current message level: 0x00000007 (7)
    Link detected: yes
```

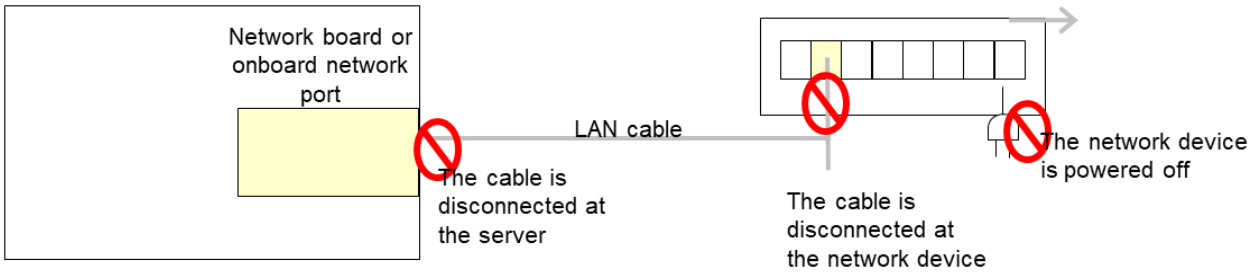
- When the LAN cable link status ("Link detected: yes") is not displayed in the result of the ethtool command:
  - It is highly likely that NIC Link Up/Down monitor resource of EXPRESSCLUSTER is unable to operate. Use the IP monitor resource instead.
- When LAN cable link status ("Link detected: yes") is displayed in the result of the ethtool command:

  - In most cases NIC Link Up/Down monitor resource of EXPRESSCLUSTER can operate, but sometimes it may not operate.
  - Particularly in the following hardware, NIC Link Up/Down monitor resource of EXPRESSCLUSTER may not operate. Use IP monitor resource instead.
    * When hardware is installed between the actual LAN connector and NIC chip such as a blade server

When you check if NIC Link Up/Down monitor resource can be used with the use of EXPRESSCLUSTER on a machine for a production environment, follow the steps below.

1. Register NIC Link Up/Down monitor resource with the configuration data.
   Select **No Operation** for the configuration of recovery operation of NIC Link Up/Down monitor resource upon failure detection.
2. Start the cluster.
3. Check the status of NIC Link Up/Down monitor resource.
   If the status of NIC Link Up/Down monitor resource is abnormal while LAN cable link status is normal, NIC Link Up/Down monitor resource cannot be used.
4. If NIC Link Up/Down monitor resource status becomes abnormal when LAN cable link status is made abnormal status (link down status), (NIC Link Up/Down monitor resource can be used).
   If the status remains to be normal, NIC Link Up/Down monitor resource cannot be used.

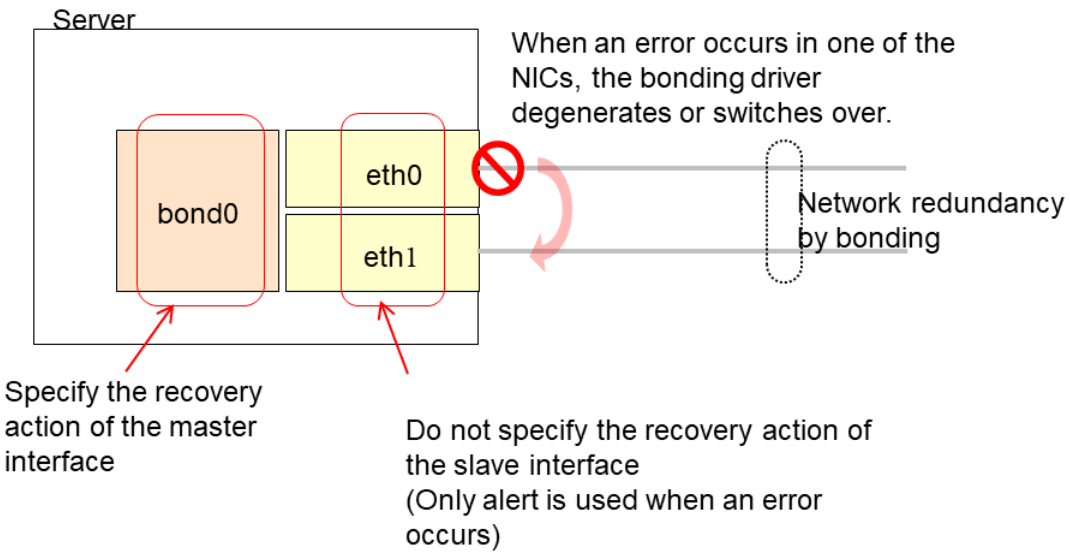
4.6.3 Configuration and range of NIC Link Up/Down monitoring



- The ioctl( ) to the NIC driver is used to find how the server is linked to the network. (For the IP monitoring, the status is judged by the ping response from the specified IP address.)
- You can monitor an NIC dedicated to interconnect (mirror connect). If you do this in the environment where two nodes are directly connected with a LAN cable and one server fails, the other server is considered to be failing. This is because no link is established. The recovery action to be taken at detection of error should be configured with the appropriate value. For example, if **Stop cluster daemon and reboot OS** is selected, other servers will continue to restart the OS endlessly.

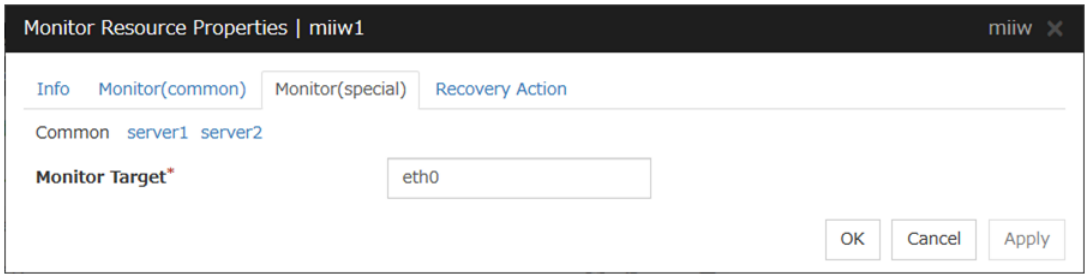
If the network is has a bonding status, it is possible to monitor the master interface (bond0...) as well as the slave interface (eth0, eth1...) in the lower level, while applying the bonding availability. It is recommended to use the settings below.

- Slave Interface Recovery action when an error is detected: Set no action
  - When only one of the network cables (eth0) fails, EXPRESSCLUSTER issues an alert, while no recovery action takes place. The network recovery is performed by bonding.
- Master Interface
  - Recovery action when an error is detected: Set actions such as failover and shutdown. When all slave interfaces fail (and the master interface is down), the EXPRESSCLUSTER performs the recovery action.



4.6.4 Monitor (special) tab

NIC Link Up/Down monitor resource obtains the information on how the specified NIC is linked monitors the linkage is up or down.



Monitor Target (Within 15 bytes) `Server Individual Setup`

Enter the name of the NIC interface you want to monitor. You can monitor Bond devices (e.g. bond.600) and team devices (e.g. team0). You can also monitor VLAN and tagVLAN (setting example: eth0.8).

4.7 Understanding mirror disk connect monitor resources

4.7.1 Note on mirror disk connect monitor resources

- A mirror disk connect monitor resource monitors a network for mirroring. If communication of mirror data using the specified mirror disk connect fails, it is recognized as an error. This resource is automatically registered when the mirror disk resource is added.
- When more than one mirror disk resource is added, the same number of mirror disk connect monitor resources as the one of mirror resources is automatically registered.

4.7.2 Monitor (special) tab

Mirror Disk Resource

The mirror disk resource to be monitored is displayed.

4.8 Understanding mirror disk monitor resources

Mirror disk monitor resources monitor the state of date of mirror disk and the soundness of mirror driver.

4.8.1 Note on mirror disk monitor resources

This resource is automatically registered when a mirror disk resource is added. A mirror disk monitor resource corresponding to a mirror disk resource is automatically registered.

4.8.2 Monitor (special) tab

Mirror Disk Resource

The mirror disk resource to be monitored is displayed.

4.9 Understanding hybrid disk connect monitor resources

4.9.1 Note on hybrid disk connect monitor resources

- A mirror disk connect monitor resource monitors a network for mirroring. If communication of mirror data using the specified mirror disk connect fails, it is recognized as an error. This resource is automatically registered when the hybrid disk resource is added.
- When more than one hybrid disk resource is added, hybrid disk connect monitor resources as many as the number of the hybrid disk resources are automatically registered.

4.9.2 Monitor (special) tab

Hybrid Disk Resource

The hybrid disk resource to be monitored is displayed.

4.10 Understanding hybrid disk monitor resources

Hybrid disk monitor resources monitor the status of the data in the hybrid disk and the health of the mirror driver.

4.10.1 Note on hybrid disk monitor resources

This resource is automatically registered when a hybrid disk resource is added. Hybrid disk monitor resources corresponding to hybrid disk resources are automatically registered.

4.10.2 Monitor (special) tab

Hybrid Disk Resource

The hybrid disk resource for monitoring is displayed.

4.11 Understanding PID monitor resources

4.11.1 Note on PID monitor resources

PID monitor resource monitors a successfully activated EXEC resource. The EXEC resource can be monitored if its settings for activation are configured to **Asynchronous**.

4.11.2 Setting PID monitor resources

PIC monitor resource monitors a successfully activated EXEC resource. By monitoring the presence of process ID, an error is established when the process ID disappears.

The exec resource to be monitored is set according to the steps described in "Target Resource" of "*Monitor (common) tab*". The exec resource can be monitored if its settings for activation are configured to **Asynchronous**. You cannot detect stalled status of the process.

Note: To monitor stalls such as data base, samba, apache, and sendmail, purchase optional EXPRESSCLUSTER product.

4.12 Understanding User mode monitor resources

4.12.1 Drivers that User mode monitor resources depend

Monitor by: softdog

softdog

- If softdog is selected as a monitoring method, the softdog driver is required.
- Use a loadable module configuration. User-mode monitor resources do not work on the static driver.
- If the softdog driver is not available, monitoring cannot be started.

Monitor by: keepalive

clpka
clpkhb

- If keepalive is selected as a monitoring method, the clpkhb driver and the clpka driver of the EXPRESSCLUSTER are required.
- When keepalive is set to the monitoring method, it is recommended to set the kernel mode LAN heartbeat. To use the kernel mode LAN heartbeat, the clpkhb driver is required.
- The clpka driver and the clpkhb driver are provided by EXPRESSCLUSTER. For information on support, refer to "Supported distributions and kernel versions" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".
- You cannot start monitoring if the clpkhb driver and the clpka driver cannot be used.

Monitor by: ipmi, ipmi (High-End Server Option)

ipmi

- If ipmi or ipmi (High-End Server Option) is used as a monitoring method, this driver is required.
- If the ipmi driver is not loaded, monitoring cannot be started.

4.12.2 How monitor User mode monitor resources perform monitoring

You can select how a user-mode monitor resource monitors its target from the following:

Monitor by: softdog

If softdog is selected as a monitoring method, the softdog driver of the OS is used.

Monitor by: keepalive

If keepalive is selected as a monitoring method, the clpkhb and the clpka drivers are used.

Note: Always check the distributions and the kernel versions on which the clpkhb driver and the clpka driver can be operated with "Supported distributions and kernel versions" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide". Check them when applying a security patch released by a distributor to the operating cluster (when the kernel version changes).

Monitor by: ipmi, ipmi (High-End Server Option)

If ipmi or ipmi (High-End Server Option) is selected as a monitoring method, the ipmi driver is used.

Monitor by: none

"none" is a monitoring method is used for evaluation. This only executes operations of the advanced settings of the user-mode monitor resource. Do not use this in a production environment.

4.12.3 Advanced settings of User mode monitor resource

Opening/closing of a dummy file, writing to a dummy file and creating a dummy thread are the configurations that allow advance user-mode monitor resource. If any of these configurations fail, the timer will not be updated. If a configuration continues to fail for the period of time set for the timeout or heartbeat timeout, the OS is reset.

Opening/closing a dummy file

A dummy file is created, opened, closed and then deleted at every monitoring interval repeatedly.

- When this advanced function is set and there is no free disk space, opening the dummy file fails and the OS is reset.

Writing to a dummy file

A specified size of data is written into a dummy file at every monitoring interval.

- This advanced function is not available unless opening/closing a dummy file is set.

Creating a dummy thread

A dummy thread is created at every monitoring interval.

4.12.4 User mode monitor resource logic

The following sections describe how processes and features differ by ways of monitoring.
For the shutdown stall monitoring, only Step 1 in each process overview is performed.

Monitoring method: IPMI

- Process overview

  Steps 2 to 7 of the process are repeated.

  1. Set the IPMI timer
  2. Open a dummy file
  3. Write to the dummy file
  4. Execute fdatasync for the dummy file
  5. Close the dummy file
  6. Create a dummy thread
  7. Updated the IPMI timer

Steps 2 to 6 of the process overview are for advanced settings. To execute these steps, you need to configure the settings.

- What happens when timeout does not occur (i.e. Steps 2 to 7 are performed without any problem):
  Recovery actions such as resetting are not performed.
- What happens when timeout occurs (i.e. any of Steps 2 to 7 is stopped or delayed):
  Reset is performed by BMC (the management function of the server).
- Advantages
  - This method of is less likely to be impacted by a kernel space failure, which makes chance of reset higher because BMC (the management function of the server itself) is used.
- Disadvantages
  - This method is not available on servers not supporting IPMI or on which OpenIPMI does not run. This is because this monitoring method is hardware dependent.
  - This method is not available on a server where NEC ESMPRO Agent is used.
  - This method may not be able to coexist with software programs for server monitoring that are supplied by server vendors.

Monitoring method: softdog

- Process overview

  Steps 2 to 7 of the process are repeated.

  1. Set softdog
  2. Open a dummy file
  3. Write to the dummy file
  4. Execute fdatasync for the dummy file
  5. Close the fumy file
  6. Create a dummy thread

7. Update the softdog timer

Steps 2 to 6 of the process overview are for advanced settings. To execute these steps, you need to configure the settings.

- What happens when timeout does not occur (i.e. Steps 2 to 7 are performed without any problem):
  Recovery actions such as reset are not performed.
- What happens when timeout occurs (i.e. any of Steps 2 to 7 is stopped or delayed):
  Reset is performed by softdog.
- Advantages
  - Since this method is not dependent on hardware, you can use it as long as there is a softdog kernel module.
    (In some distributions, softdog is not provided by default. Check that you have softdog before configuring the settings.)
- Disadvantages
  - Because softdog is dependent on the timer logic of the kernel space, reset may not be performed if an error occurs in the kernel space.

Monitoring method: keepalive

- Process overview

  Steps 2 to 7 are repeated.

  1. Set the keepalive timer
  2. Open a dummy file
  3. Execute write to the dummy file
  4. Execute fdatasync to the dummy file
  5. Close the dummy file
  6. Create a dummy thread
  7. Update the keepalive timer

Steps 2 to 6 of the process overview are for advanced settings. To execute these steps, you need to configure the settings

- When a timeout does not occur (i.e. Steps 2 to 7 are performed without any problem): Recovery actions such as reset are not performed.
- When a timeout occurs (i.e. any of Steps 2 to 7 is stopped or delayed):
  - Reset of the local server is announced to other servers through clpkhb.ko.
  - Reset or panic is performed by clpka.ko according to the action setting.
- Advantage
  - Logs are recorded on other servers by announcement of the reset of the local server through execution of clpkhb.
- Disadvantages
  - Distributions, architectures, kernel versions which can be operated (which provide drivers) are limited.
  - Because clpka is dependent on the timer logic of the kernel space, reset may not be performed if an error occurs in the kernel space.

Monitoring method: ipmi (High-End Server Option)

- It can't be used.

4.12.5 Checking availability of IPMI

You can quickly check if OpenIPMI runs on the server by following the steps below:

1. Install the rpm package of OpenIPMI.
2. Run /usr/bin/ipmitool.
3. Check the result of the execution.

When you see the following (the result of /usr/bin/ipmitool bmc watchdog get):
(This is an example. Different values may be shown depending on your hardware devices.)

```
Watchdog Timer Use: BIOS FRB2 (0x01)
Watchdog Timer Is: Stopped
Watchdog Timer Actions: No action (0x00)
Pre-timeout interval: 0 seconds
Timer Expiration Flags: 0x00
Initial Countdown: 0 sec
Present Countdown: 0 sec
```

You can use OpenIPMI. ipmi can be chosen as a monitoring method.

4.12.6 User mode monitor resources

All monitoring methods:

- When a cluster is added by the Cluster WebUI, a user-mode monitor resource of softdog is automatically created.
- A user-mode monitor resource with different monitoring method can be added. A user-mode monitor resource of softdog that was automatically created can be deleted when a cluster is added.
- When the activation of a user-mode monitor resource fails due to a reason such as the softdog driver of OS or the clpkhb/clpka driver of EXPRESSCLUSTER does not exist, or the rpm for OpenIPMI is not installed, "Monitor userw failed." will be displayed on the Alert logs in the Cluster WebUI,. In the tree view of the Cluster WebUI, as the response to the clpstat command, Normal will be displayed as the resource status, and Offline will be displayed as the status of each server.

Monitoring by IPMI:

- For notes on ipmi, see "*IPMI command*" in "*Monitor resource* " in "4. *Monitor resource details*" in this guide.

Note:

If you are using a software program for server monitoring provided by a server vendor such as NEC ESMPRO Agent, do not choose IPMI as a monitoring method.
Because these software programs for server monitoring and OpenIPMI both use BMC (Baseboard Management Controller) on the server, a conflict occurs, preventing successful monitoring.

Monitoring by ipmi (High-End Server Option)

- It can't be used.

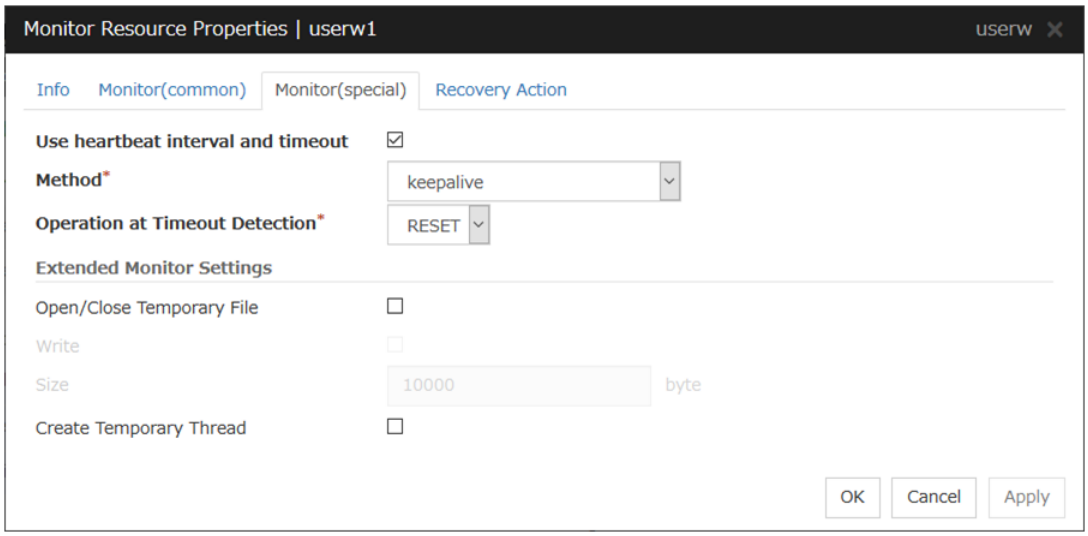
Monitoring by keepalive

- Notification to other servers are performed only when a kernel mode LAN heartbeat resource is set. In this case, the following log is displayed on the syslog.

```
kernel: clpka: <server priority: %d> <reason: %s> <process name: %s>system reboot.
```

4.12.7 Monitor (special) tab

User-mode monitor resource considers stalling in user space as an error.
This resource is automatically registered when a cluster is added. The user-mode monitor resource of softdog is automatically registered. The monitoring method is softdog.



Use heartbeat interval and timeout

Select this check box if you use heartbeat's interval and timeout for monitor's interval and timeout.

- When the check box is selected:
  Heartbeat interval and timeout are used.
- When the check box is not selected:
  Heartbeat is not used. Interval and timeout specified on the **Monitor** tab are used.
  You need to set a larger value for timeout than interval.
  When ipmi is specified to **Method**, you need to specify 255 or less for timeout.

Method

Choose how you want to monitor the user-mode monitor resource from the following.
You can not select a method which has already been used for other user-mode monitor resource.

- softdog:
  Uses softdog driver
- ipmi:
  Uses OpenIPMI

- ipmi(High-End Server Option):
  It can't be used.
- keepalive:
  Uses clpkhb driver and clpka driver.
- No Operation:
  Uses nothing.

Operation at Timeout Detection

Select the final action. This can be set only when the monitoring method is keepalive.

- RESET:
  Resets the server.
- PANIC:
  Performs a panic of the server.
- IOFENCING:
  It can't be used.

Open/Close Temporary File

Select this check box if you want to open/close a dummy file at every interval when you execute monitoring.

- When the check box ix selected:
  A dummy file will be opened/closed.
- When the check box is not selected:
  A dummy file will not be opened/closed.

Write

Select this check box if you have chosen to open/close a dummy file and want to write in dummy data.

- When the check box is selected:
  Dummy data is written into a dummy file.
- When the check box is not selected:
  Dummy data is not written into a dummy file.

Size (1 to 9999999)

If you have chosen to write dummy data into a dummy file, specify the size to write in.

Create Temporary Thread

Select this check box if you want to create a dummy thread when monitoring is performed.

- When the check box is selected:
  Temporary thread will be created.
- When the check box is no selected:
  Temporary thread will not be created.

4.13 Understanding multi target monitor resources

The multi target monitor resource monitors more than one monitor resources.

4.13.1 Notes on multi target monitor resources

- The multi target monitor resources regard the offline status of registered monitor resources as being an error. For this reason, for a monitor resource that performs monitoring when the target is active is registered, the multi target monitor resource might detect an error even when an error is not detected by the monitor resource. Do not, therefore, register monitor resources that perform monitoring when the target is active.

4.13.2 Multi target monitor resource status

The status of the multi target monitor resource is determined by the status of registered monitor resources.

The table below describes status of multi target monitor resource when the multi target monitor resource is configured as follows:

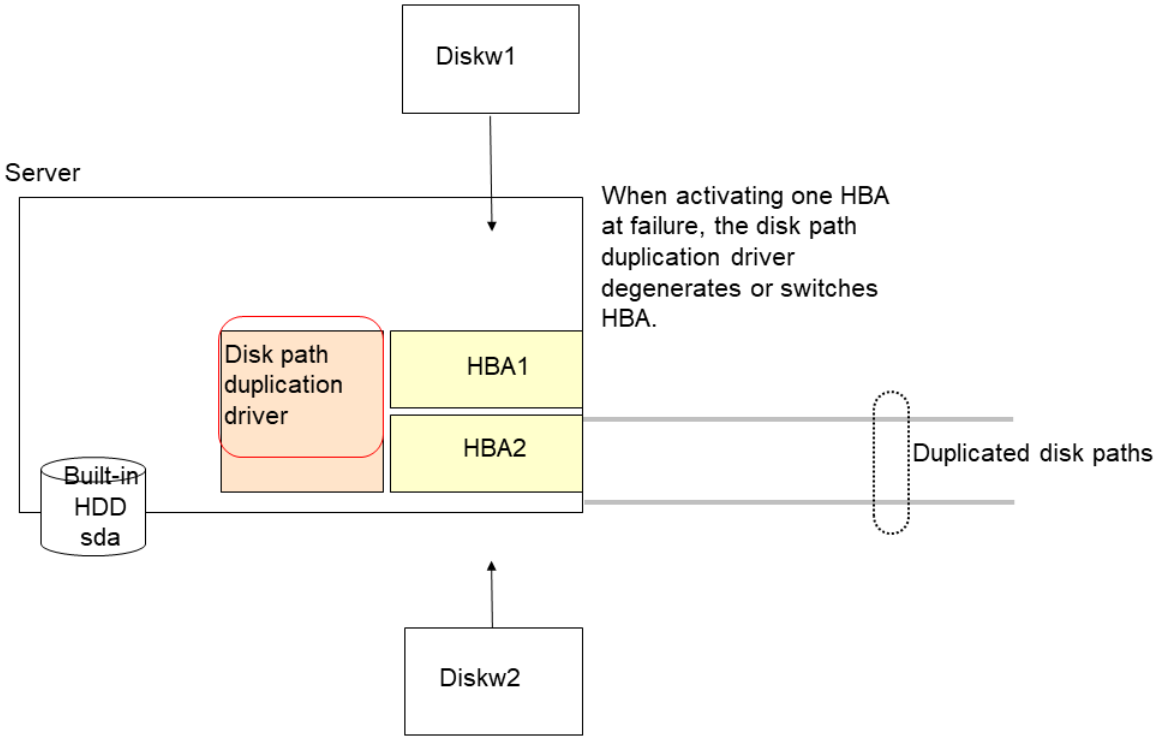
The number of registered monitor resources 2
Error Threshold 2
Warning Threshold 1

Multi target monitor resource status		**Monitor resource1 status**		
		Normal	**Error**	**Offline**
Monitor resource2 status	**Normal**	normal	caution	caution
	Error	caution	error	error
	Offline	caution	error	normal

- Multi target monitor resource monitors status of registered monitor resources.
  If the number of the monitor resources with the error status exceeds the error threshold, the status of the multi target monitor resource becomes error.
  If the number of the monitor resources with the caution status exceeds the caution threshold, the status of the multi target resource becomes caution.
  If all registered monitor resources are in the status of stopped (offline), the status of multi target monitor resource becomes normal. Unless all the registered monitor resources are stopped (offline), the multi target monitor resource recognizes the stopped (offline) status of a monitor resource as error.
- If the status of a registered monitor resource becomes error, actions for the error of the monitoring resource are not executed.
  Actions for error of the multi target monitor resource are executed only when the status of the multi target monitor resource becomes error.

4.13.3 Example of the multi target monitor resource configuration

- An example of disk path duplication driver usage
  The status should be indicating an error only when disk devices (for example, /dev/sdb and /dev/sdc) fail at the same time.



  - Monitor resources to be registered with the multi target monitor resources (mtw1):
    - diskw1
    - diskw2
  - Error Threshold and Warning Threshold of multi target monitor resource (mtw1)
    - Error Threshold 2
    - Warning Threshold 0
  - Detailed settings of the monitor resource to be registered with the multi target monitor resource (mtw1)
    - Disk monitor resource (diskw1)
      Target Device Name: /dev/sdb
      Reactivation Threshold: 0
      Failover Threshold: 0
      Final Action: No Operation
    - Disk monitor resource (diskw2)
      Target Device Name: /dev/sdc
      Reactivation Threshold: 0
      Failover Threshold: 0
      Final Action: No Operation

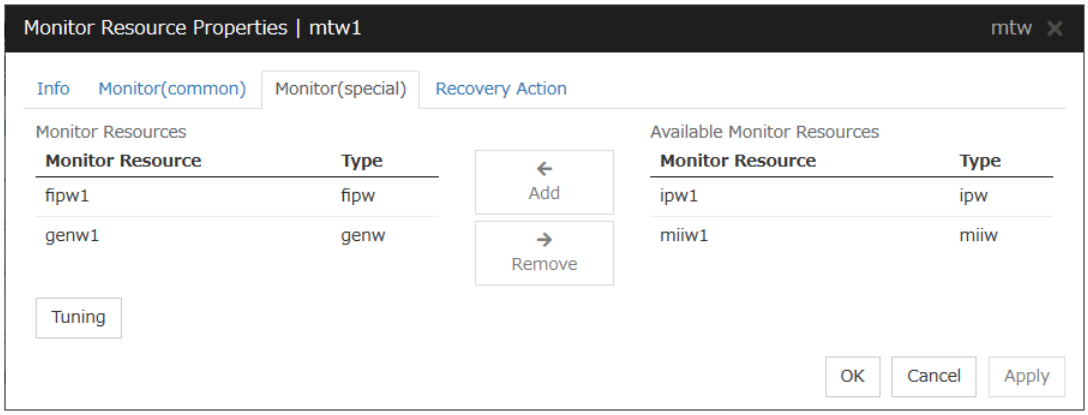
- With the settings above, even if either of diskw1 and diskw2, which are registered as monitor resources of the multi target monitor resource detects an error, no actions for the monitor resource having the error are taken.

- Actions for an error set to the multi target monitor resource are executed when the status of both diskw1 and diskw2 become error, or when the status of two monitor resources become error and offline.

4.13.4 Monitor (special) tab

Monitor resources are grouped and the status of the group is monitored. You can register up to 64 monitor resources in the **Monitor Resources**.

When the only one monitor resource set in the **Monitor Resources** is deleted, the multi target monitor resource is deleted automatically.



Add

Click **Add** to add a selected monitor resource to **Monitor Resources**.

Remove

Click Remove to delete a selected monitor resource from Monitor Resources.

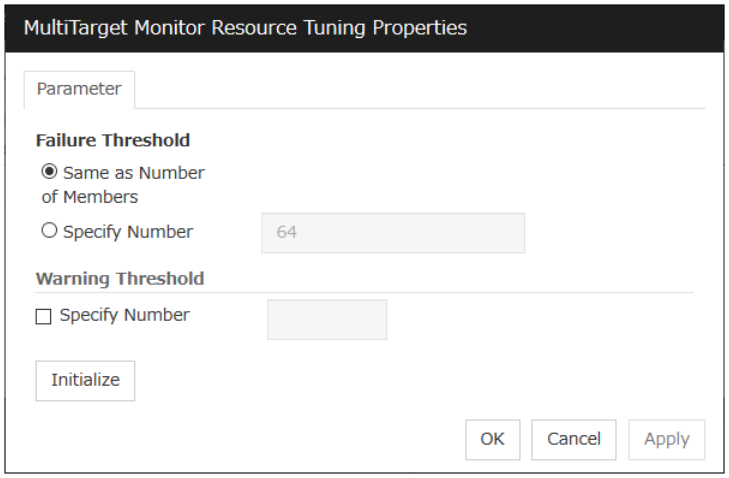
Tuning

Open **Multi Target Monitor Resource Tuning Properties** dialog box. Configure detailed settings for the multi target monitor resource.

MultiTarget Monitor Resource Tuning Properties

Parameter tab

Display the details of setting the parameter



Error Threshold

Select the condition for multi target monitor resources to be determined as an error.

- Same as Number of Members

  The status of multi target monitor resources becomes "Error" when all monitor resources specified to be under the multi target monitor resource are failed, or when "Error" and "Offline" co-exist.

  The status of multi target monitor resources becomes "Normal" when the status of all monitor resources specified to be under the multi target monitor resource are "Offline."

- Specify Number

  The status of multi target monitor resources becomes "Error" when the number of monitor resources specified in **Error Threshold** becomes "Error" or "Offline."

  When the status of some monitor resources among those specified to be under the multi target monitor resource, specify how many monitor resources need to be "Error" or "Offline" to determine that the status of multi target monitor resource is "Error."

Warning Threshold

- When the check box is selected:
  When the status of some monitor resources among those specified to be under the multi target monitor resource, specify how many monitor resources need to be "Error" or "Offline" to determine that the status of multi target monitor resource is "Caution."
- When the check box is not selected:
  Multi target monitor resources do not display an alert.

Initialize

Clicking **Initialize** resets all items to their default values.

4.14 Understanding virtual IP monitor resources

4.14.1 Note on virtual IP monitor resources

Detailed settings are not required for virtual IP monitor resources.
Use the resources when using virtual IP resources of EXPRESSCLUSTER.

- Virtual IP monitor resource is created automatically when the virtual IP resource is created. One virtual IP monitor resource is created per virtual IP resource automatically.
- Virtual IP monitor resource cannot be deleted. It is deleted automatically at deletion of a virtual IP resource.
- Do not change the recovery target.
- Monitoring cannot be suspended or resumed by the clpmonctrl command or the Cluster WebUI.
- Virtual IP monitor resource regularly sends RIP packets to control a path of the virtual IP resource. If the target virtual IP resource is active while the cluster is suspended, the virtual IP monitor resource continues operating.
- The setting of Monitor(common) tab-Retry Count is invalid. When you'd like to delay error detection, please change the setting of Monitor(common) tab-Timeout.

4.14.2 Setting virtual IP monitor resources

Virtual IP monitor resource sends packets for dynamic routing of the routing table the virtual IP resource requires. The status of IP addresses activated by the virtual IP resources is not checked. There is no detailed setting for the virtual IP monitor resource.

4.15 Understanding ARP monitor resources

ARP monitor resource sends ARP packets regularly to maintain and update the ARP table for active floating IP resources or virtual IP resources.

4.15.1 Note on ARP monitor resources

For details on the ARP broadcast packets that ARP monitor resource sends, see "*Understanding Floating IP resource*" of "3. *Group resource details*" in this guide.

The status of the IP address activated by floating IP resource or virtual IP resource is not checked.

Only floating IP resource or virtual IP resource can be selected as a target monitoring resource of ARP monitor resource. On the ARP monitor resource setting, make sure to select a same resource for **Target Resource** on the **Monitor(common)** tab and **Target Resource** on the **Monitor(special)** tab.

Monitoring of the ARP monitor resource cannot be suspended or resumed by the clpmonctrl command or by the Cluster WebUI.

4.15.2 Monitor (special) tab

Target Resource

Click **Browse** to display the dialog box to select a target resource. The names of groups, floating IP resources and virtual IP resources registered to a LocalServer and cluster are displayed in the tree view. Select the resource you want to set as a target resource, and then click **OK**.

Note: When you change the target resource, make sure to change the one configured on the **Monitor(common)** tab.

4.16 Understanding custom monitor resources

Custom monitor resources monitor system by executing an arbitrary script.

4.16.1 Notes on custom resources

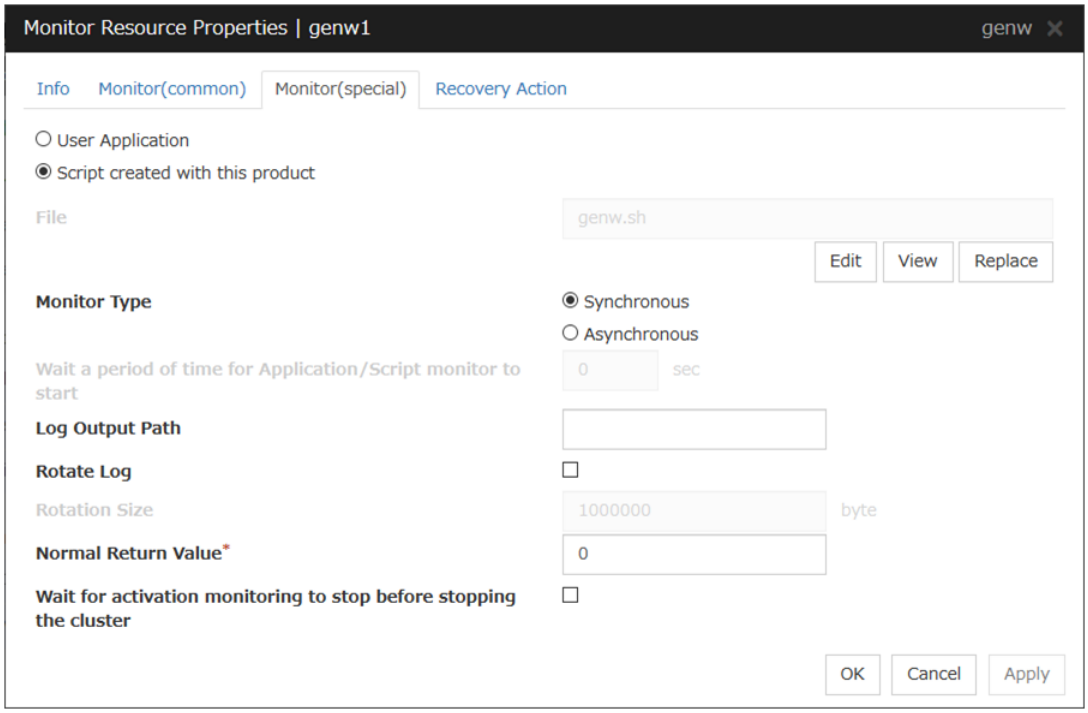
When the monitor type is **Asynchronous**, and the monitoring retry count is set to 1 or more, monitoring cannot be performed correctly. When you set the monitor type to **Asynchronous**, also specify 0 as the monitoring retry count.

When the Script Log Rotate function is enabled, a process is generated to mediate the log output. This intermediate process continues to work until the file descriptor is closed (i.e. until all the logs stop being output from the start and stop scripts and from a descendant process that takes over the standard output and/or the standard error output from the start and stop scripts). To exclude output from the descendant process from the log, redirect the standard output and/or the standard error output when the process is generated with the script.

4.16.2 Monitoring by custom monitor resources

Custom monitor resources monitor system by an arbitrary script.
When Monitor Type is **Synchronous**, custom monitor resources regularly run a script and detect errors from its error code.
When Monitor Type is **Asynchronous**, custom monitor resources run a script upon start monitoring and detect errors if the script process disappears.

4.16.3 Monitor (special) tab



User Application

Use an executable file (executable shell script file or execution file) on the server as a script. For the file name, specify an absolute path or name of the executable file of the local disk on the server.

Each executable files is not included in the cluster configuration information of the Cluster WebUI. They must be prepared on each server because they cannot be edited nor uploaded by the Cluster WebUI.

Script created with this product

Use a script file which is prepared by the Cluster WebUI as a script. You can edit the script file with the Cluster WebUI if you need. The script file is included in the cluster configuration information.

File (Within 1023 bytes)

Specify the script to be executed (executable shell script file or execution file) when you select User Application with its absolute path on the local disk of the server.

View

Click here to display the script file when you select **Script created with this product**.

Edit

Click here to edit the script file when you select **Script created with this product**. Click **Save** to apply the changes. You cannot modify the name of the script file.

Replace

Click here to replace the contents of a script file with the contents of the script file which you selected in the file selection dialog box when you select **Script created with this product**. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not select binary files (applications), and so on.

Monitor Type

Select a monitor type.

- Synchronous (Default)
  Custom monitor resources regularly run a script and detect errors from its error code.
- Asynchronous
  Custom monitor resources run a script upon start monitoring and detect errors if the script process disappears.

Wait for the application/script monitoring to start for a certain period of time (0 to 9999)

Specify the delay time from the start of the application/script and that of monitoring for the **Asynchronous** monitor type. This delay value must be set smaller than the timeout value specified under the **Monitor (common)** tab.

Note: The set value becomes valid next time you start the monitor.

Default value: 0

Log Output Path (Within 1023 bytes)

Specify log output path for the script of custom monitor resource.

Pay careful attention to the free space in the file system because the log is output without any limitations when the file name is specified and the **Rotate Log** check box is unchecked.

When the **Rotate Log** check box is selected, output log files are rotated.

Rotate Log

Turn this off to output execution logs of scripts and executable files with no limit on the file size.

Turn it on to rotate and output the logs. In addition, note the following.

Enter the log path in 1009 bytes or less in Log Output Path. If the path exceeds 1009 bytes, the logs are not output.

The log file name must be 31 bytes or less. If the name exceeded 32 bytes, the logs are not output.

If some custom monitor resources are configured to rotate logs, and the log file names are the same but the log paths are different, the Log Rotate Size may be incorrect.

(for example, /home/foo01/log/genw.log, /home/foo02/log/genw.log)

Rotation Size (1 to 9999999)

Specify a file size for rotating files when the **Rotate Log** check box is selected.

The log files that are rotated and output are configured as described below.

File name	Description
Log Output Path specified_file_name	Latest log file.
Log Output Path specified_file_name.pre	Former log file that has been rotated.

Normal Return Value (Within 1023 bytes)

When **Asynchronous** is selected for **Monitor Type**, set the values of script error code to be determined as normal. If you want to set two or more values here, separate them by commas like 0,2,3 or connect them with a hyphen to specify the range like 0-3.

Default value: 0

Wait for activation monitoring to stop before stopping the cluster

The cluster stop waits until the custom monitor resource is stopped. This is effective only when the monitoring tyming is set to **Active**.

4.17 Understanding volume manager monitor resources

Volume manager monitor resources are used to monitor logical disks managed by the volume manager.

4.17.1 Notes on volume manager monitor resources

When the volume manager is VxVM, volmgrw uses the daemon monitoring method. Therefore, registering multiple items in a single cluster is meaningless.

When specifying VxVM as the volume manager, do not specify the recovery target.

Volume manager monitor resources are automatically registered when a volume manager resource is added. Volume manager monitor resources are automatically registered to the volume manager resource.
Volume manager monitor resources are configured with their default settings; change the settings as needed.
Registering the volmgr resource does not automatically register the volmgrw monitor. The volmgrw monitor must be registered manually.

When monitoring the LVM by using the volume manager monitor resource in an environment of Red Hat Enterprise Linux 7 or later, the LVM metadata daemon must be disabled.

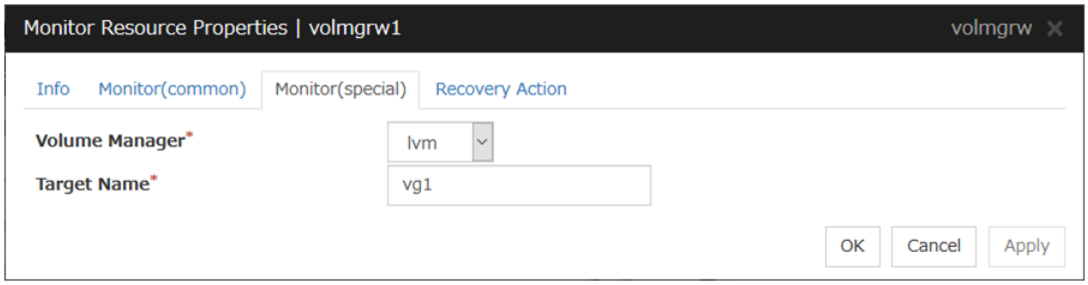
4.17.2 Monitoring by volume manager monitor resources

The monitoring method used by volume manager monitor resources depends on the type of volume manager that manages the target logical disks.

The following volume managers are supported:

- lvm (LVM volume group)
- vxvm (VxVM daemon)
- zfspool (ZFS storage pool)

4.17.3 Monitor (special) tab



Volume Manager

Specify the type of volume manager that manages the monitor target logical disks. The following volume managers are supported:

- lvm (LVM volume group)
- vxvm (VxVM daemon)
- zfspool (ZFS storage pool)

Target Name(within 1023 bytes)

Specify the name of the monitor target in the <VG name> format (only the target name is used).

When the volume manager is lvm, it's possible to control multiple volumes together.

More than one volume is delimited with an one-byte space.

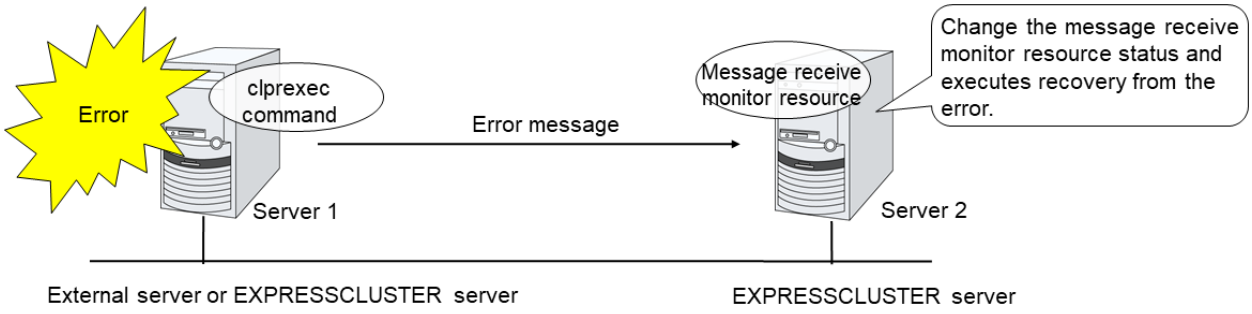
When the volume manager is vxvm, this setting need not be entered.

4.18 Understanding message receive monitor resources

Message receive monitor resources are passive monitors. They do not perform monitoring by themselves.
When an error message issued using the clprexec command is received from outside of EXPRESSCLUSTER, the message receive monitor resources change their status and perform recovery from the error.

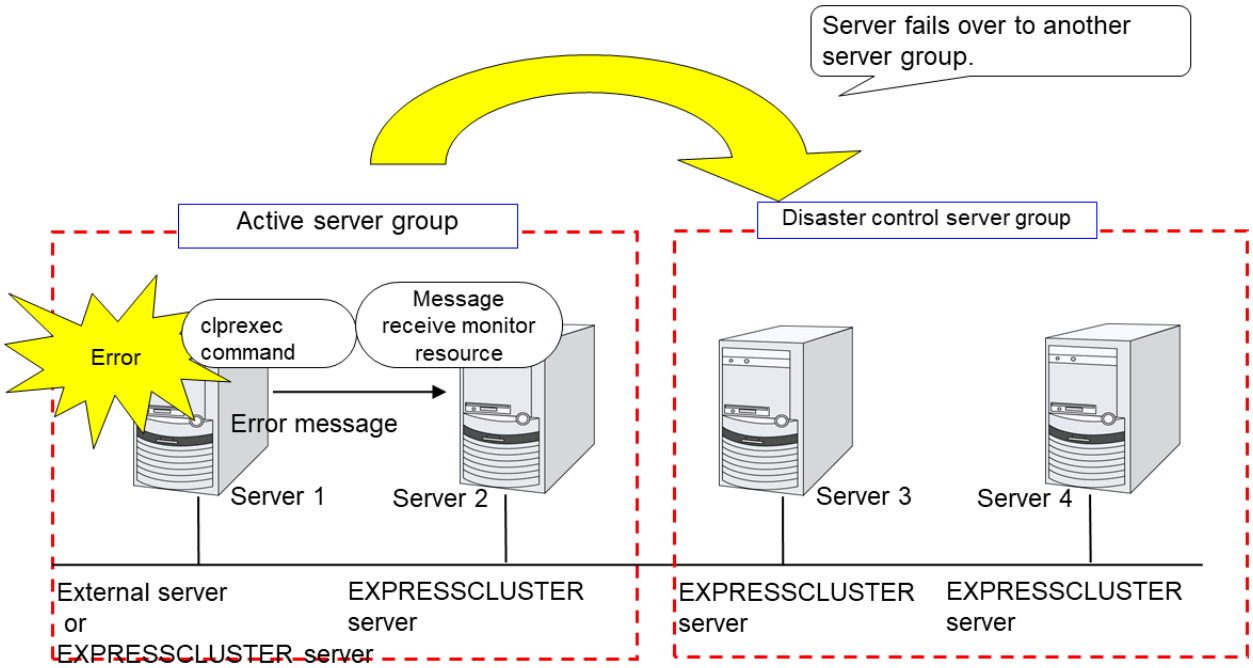
4.18.1 Monitoring by message receive monitor resources

- When an error message is received from an outside source, the resource recovers the message receive monitor resource whose Category and Keyword have been reported. (The Keyword can be omitted.)
  If there are multiple message receive monitor resources whose monitor types and monitor targets have been reported, each monitor resource is recovered.
- Message receive monitors can receive error messages issued by the clprexec command, local server BMC, and expanded device drivers within the server management infrastructure.
- Error messages from local server BMC are available only in Express5800/A1080a or Express5800/A1040a series linkage. For details, see " Express5800/A1080a or Express5800/A1040a series linkage with message receive monitor resources" in "Express5800/A1080a or Express5800/A1040a series linkage" in "Linkage with specific hardware" in the "Hardware Feature Guide".
- For details on the monitoring method that uses linkage with server management infrastructure, see "Linkage with Server Management Infrastructure" in the "Hardware Feature Guide".



4.18.2 Failover to outside the server group

- Upon the reception of notification of the occurrence of an error, failover from the active server group to another server group is allowed.
- The following server group and other settings must be specified.
  - Group resource for recovery
    - [Use Server Group Settings] is selected
  - Message receive monitor
    - [Execute failover to the recovery target] is specified for the recovery target
    - [Execute Failover outside the Server Group] is selected
- Upon the execution of server group failover to outside the server group, the dynamic failover settings and inter-server group failover settings are disabled. The server fails over to the server having the highest priority in a server group other than that to which it belongs.



4.18.3 Notes on message receive monitor resources

Notes on message receive monitor resources

- If a message receive monitor resource is paused when an error message is received from outside, error correction is not performed.
- If an error message is received from outside, the status of the message receive monitor resource becomes "error". The error status of the message receive monitor resource is not automatically restored to "normal". To restore the status to normal, use the clprexec command. For details about this command, see "*Requesting processing to cluster servers (clprexec command)*" in "*8. EXPRESSCLUSTER command reference*" in this guide.
- If an error message is received when the message receive monitor resource is already in the error status due to a previous error message, recovery from the error is not performed.
  When the recovery action is **Executing failover to outside the Server Group**, and if **Execute Failover to outside the Server Group** is selected, the server always fails over to a server in a server group other than the active server group. If, however, the above-mentioned settings are configured but the server group is not configured, the failover destination is determined according to the ordinary failover policy.
- To receive an I/O Fencing completion notification from the BMC, the management LAN port of the BMC must be capable of communicating with the NIC of the OS. Specify a port number by connecting the SNMP Trap-receiving IP addresses of all servers with ; (semicolon). The port number can be omitted (defaults to 162). If it is necessary to set a port number, it must be entered at the end of the IP address, after : (colon).

  Example: 192.168.0.1;192.168.0.2;192.168.0.3:162

Notes on using the Express5800/A1080a or Express5800/A1040a series linkage function

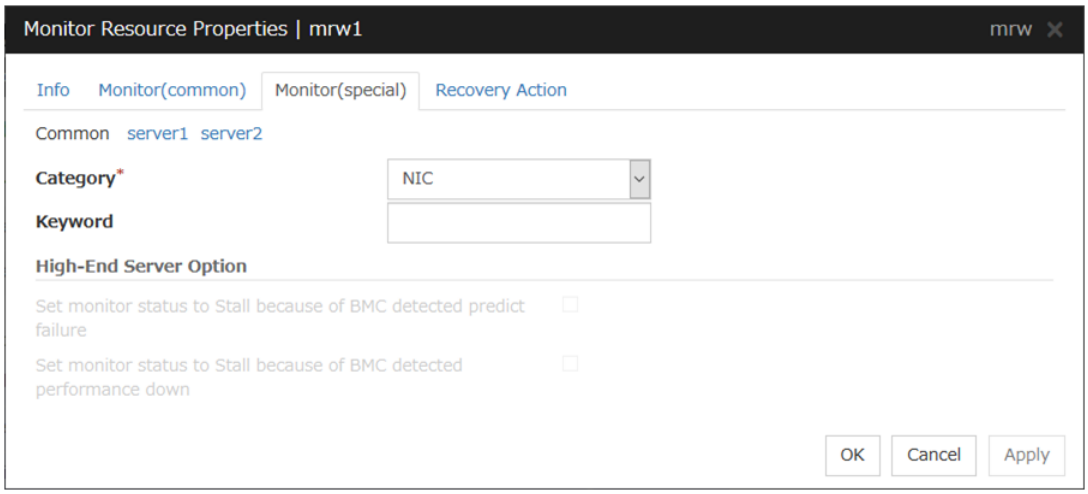
- To enable the reception of error messages from BMC, the hardware and firmware on the server must be configured accordingly. The IPMI service must also be activated. For details on supported hardware, see "Servers supporting Express5800/A1080a or Express5800/A1040a series -related functions" in the "Getting Started Guide".
- To enable the reception of error messages from BMC, communication from the BMC network interface to the OS network interface must be secured.

- To enable the reception of error messages from BMC, specify the IP address for SNMP trap reception and the port number for the server by using server-specific settings. The port number can be omitted (defaults to 162). Configure the same port number for all message receive monitor resources on the server if explicitly specified.

Notes on using linkage with server management infrastructure

- If the Enterprise Linux with Dependable Support server management infrastructure is linked, the settings for and operation of the message receive monitor resources will differ. If linking with the server management infrastructure, see "Linkage with Server Management Infrastructure" in the "Hardware Feature Guide".

4.18.4 Monitor (special) tab



For **Category** and **Keyword**, specify a keyword passed using the -k parameter of the clprexec command. The keyword can be omitted.

Category (within 32 bytes)

Specify a monitor type. To monitor error messages from BMC (SNMP Trap), specify BMCNOTICE.
You can select the default character string from the list box or specify any character string.

Keyword (within 1023 bytes)

Specify a keyword passed using the -k parameter of the clprexec command. When BMCNOTICE is specified for the category, specify the IP address for SNMP trap reception and the port number for each server by using server-specific settings. The port number can be omitted (defaults to 162). Configure the same port number for all the message receive monitor resources for each server if explicitly specified. The specification format is as described below:

<*IP_address*>[:<*port_number*>]

Set monitor status to Stall because of BMC detected predict failure

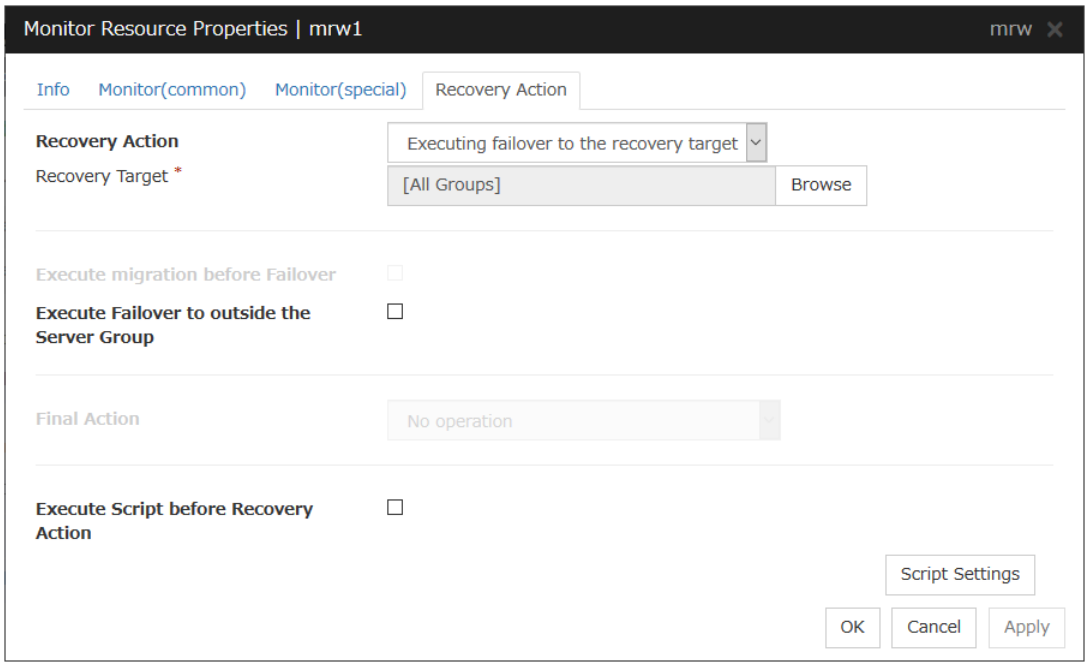
This cannot be used.

Set monitor status to Stall because of BMC detected performance down

This cannot be used.

4.18.5 Recovery Action tab

Specify the recovery target and the action upon detecting an error. For message receive monitor resources, select " Restart the recovery target ", " Executing failover to the recovery target ", or "Execute the final action" as the action to take when an error is detected. However, if the recovery target is inactive, the recovery action is not performed.



Recovery Action

Select the action to take when a monitor error is detected.

- Executing the recovery script
  Execute the recovery script when a monitor error is detected.
- Executing failover to the recovery target
  Perform failover for the group selected as the recovery target or the group to which the group resource selected as the recovery target belongs when a monitor error is detected.
- Restart the recovery target
  Restart the group or group resource selected as the recovery target when a monitor error is detected.
- Execute the final action
  Execute the selected final action when a monitor error is detected.

Execute Failover to outside the Server Group

Can be configured only for message receive monitor resources. Specify whether to fail over to a server group other than the active server group upon the reception of an error message.

Execute Script before Recovery Action

Executes the script before the operation performed upon error detection selected as the recovery action.

- When the check box is selected
  A script/command is executed before reactivation. To configure the script/command setting, click Settings.
- When the check box is not selected

Any script/command is not executed.

* For details on settings other than those above, see "*Recovery Action tab*".

4.19 Understanding VM monitor resources

VM monitor resources check whether the virtual machine is alive.

4.19.1 Notes on VM monitor resources

- This resource is automatically registered when a virtual machine resource is added.
- For the supported virtual infrastructure versions, see "Operation Environment of VM resources" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".
- The times counter of the recovery action kept by the monitor resource is not reset even though the virtual machine monitor resource recovery is detected while recovery action is in transit, or after all the recovery action have completed. Execute either one of the following procedures when you want to reset the times counter of the recovery action.
  - Reset the times counter of the recovery action by the clpmonctrl command.
  - Execute cluster stop/start with the clpcl command or Cluster WebUI.

4.19.2 Monitoring by VM monitor resources

VM monitor resources monitor the following:

If the virtual machine type is vSphere

VM monitor resources monitor the virtual machine by using the VMware vSphere API.

An error is detected if the monitoring result is one of the following:

1. The VM status is POWEROFF, SHUTDOWN, or SUSPENDED.
2. Acquiring the VM status failed.

If the virtual machine type is Xenserver

VM monitor resources monitor the virtual machine by using a general-purpose virtualization library.

An error is detected if the monitoring result is one of the following:

1. The VM status is HALTED, PAUSED, or SUSPENDED.
2. Acquiring the VM status failed.

If the virtual machine type is Kvm

VM monitor resources monitor the virtual machine by using a general-purpose virtualization library.

An error is detected if the monitoring result is one of the following:

1. The VM status is BLOCKED, SHUTDOWN, PAUSED, SHUTOFF, CRASHED, or NOSTATE.
2. Acquiring the VM status failed.

4.19.3 Monitor (special) tab

Wait Time When External Migration Occurs

Specify the time to wait for the completion of the migration.

4.20 Understanding Dynamic DNS monitor resources

4.20.1 Notes on Dynamic DNS monitor resources

There are no detailed settings for Dynamic DNS monitor resources. These monitor resources are used when using the Dynamic DNS resources in EXPRESSCLUSTER.

- A Dynamic DNS monitor resource is automatically created when a Dynamic DNS resource is added. One Dynamic DNS monitor resource is automatically created for each Dynamic DNS resource.
- Dynamic DNS monitor resources cannot be deleted. They are automatically deleted when the Dynamic DNS resource is deleted.
- Do not change the recovery target.
- Monitoring cannot be paused or resumed using the clpmonctrl command or from the Cluster WebUI.
- Dynamic DNS monitor resources periodically register virtual host names with the DDNS server. If the target Dynamic DNS resource is active while the cluster is suspended, the Dynamic DNS monitor resource continues operating.
- The setting of Monitor(common) tab-Retry Count is invalid. When you'd like to delay error detection, please change the setting of Monitor(common) tab-Timeout.

4.20.2 Settings for Dynamic DNS monitor resources

Dynamic DNS monitor resources periodically register virtual host names with the DDNS server.

There are no detailed settings for Dynamic DNS monitor resources.

4.21 Understanding process name monitor resources

Process name monitor resources monitor the process of specified processes. Process stalls cannot be detected.

4.21.1 Notes on process name monitor resources

If there are two or more processes having the name specified for the monitor target, only one process is selected according to the following conditions and is subject to monitoring.

If you set 1 for **Minimum Process Count**, and if there are two or more processes having the process name specified for the monitor target, only one process is selected under the following conditions and is subject to monitoring.

1. When the processes are in a parent-child relationship, the parent process is monitored.
2. When the processes are not in a parent-child relationship, the process having the earliest activation time is monitored.
3. When the processes are not in a parent-child relationship and their activation times are the same, the process having the lowest process ID is monitored.

If monitoring of the number of started processes is performed when there are multiple processes with the same name, specify the process count to be monitored for **Minimum Process Count**. If the number of processes with the same name falls short of the specified minimum count, an error is recognized. You can set 1 to 999 for **Minimum Process Count**. If you set 1, only one process is selected for monitoring.

Up to 1023 bytes can be specified for the monitor target process name. To specify a monitor target process with a name that exceeds 1023 bytes, use a wildcard (such as *).

If the name of the target process is 1024 bytes or longer, only the first 1023 bytes can be recognized as the process name. If you use a wild card (such as *) to specify a process name, specify a string containing the first 1024 or fewer bytes.

If the name of the target process is long, the latter part of the process name is omitted and output to the log.

If the name of the target process includes double quotations("") or a comma (,), the process name might not be correctly output to an alert message.

Check the monitor target process name which is actually running by ps(1) command, etc, and specify the monitor target process name.

Execution result

```
# ps -eaf
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Sep12 ?        00:00:00 init [5]
 :
root      5314     1  0 Sep12 ?        00:00:00 /usr/sbin/acpid
root      5325     1  0 Sep12 ?        00:00:00 /usr/sbin/sshd
htt       5481     1  0 Sep12 ?        00:00:00 /usr/sbin/htt -
retryonerror 0
 :
```

From the above command result, /usr/sbin/htt -retryonerror 0 is specified as monitor target process name in the case of monitoring /usr/sbin/htt.

The process name specified for the name of the target process specifies the target process, using the process arguments as part of the process name. To specify the name of the target process, specify the process name containing the

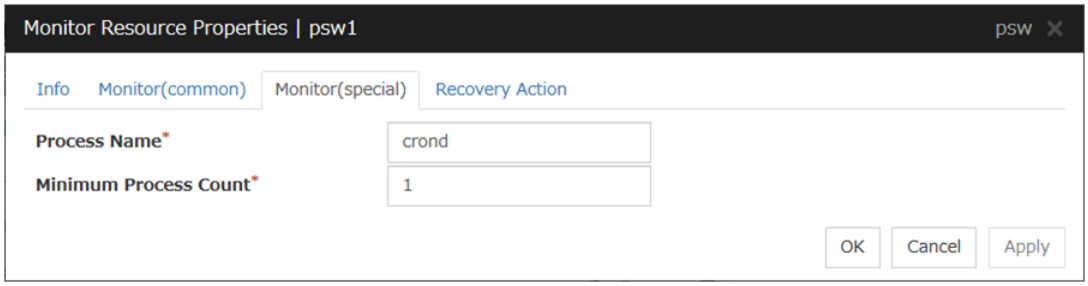
arguments. To monitor only the process name with the arguments excluded, specify it with the wildcard (*) using right truncation or partial match excluding the arguments.

4.21.2 How process name monitor resources perform monitoring

The process name monitor resource monitors a process having the specified process name. If **Minimum Process Count** is set to 1, the process ID is identified from the process name and the deletion of the process ID is treated as an error. Process stalls cannot be detected.

If **Minimum Process Count** is set to a value greater than 1, the number of processes that have the specified process name are monitored. The number of processes to be monitored is calculated using the process name, and if the number falls below the minimum count, an error is recognized. Process stalls cannot be detected.

4.21.3 Monitor (special) tab



Process Name (within 1023 bytes)

Set the name of the target process. The process name can be obtained by using the ps(1) command

Wild cards can be used to specify a process name by using one of the following three patterns. No other wild card pattern is permitted.

[prefix search] <string included in the process name>*

[suffix search] *<string included in the process name>

[partial search] *<string included in the process name>*

Minimum Process Count (1 to 999)

Set the process count to be monitored for the monitor target process. If the number of processes having the specified monitor target process name falls short of the set value, an error is recognized.

4.22 Understanding BMC monitor resources

This cannot be used.

4.23 Understanding DB2 monitor resources

DB2 monitor resource monitors DB2 database that operates on servers.

4.23.1 Note on DB2 monitor resources

For the supported versions of DB2, see "Applications supported by monitoring options" of "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

This monitoring resource monitors DB2, using the CLI library of DB2. For this reason, it is required to execute "source *instance user home*/sqllib/db2profile" as root user. Write this in a start script.

To monitor a DB2 database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the DB2 database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**. Also, set up the DB2 client on the host OS side, where monitor resources run, and register the database on the virtual machine to the database node directory.

If the code page of the database and the one of this monitor resource differ, this monitor resource cannot access to the DB2 database. Set an appropriate character code as necessary.
To check the code page of database, execute "db2 get db cfg for *Database_name*." For details, see DB2 manual.

If values of database name, instance name, user name and password specified by a parameter differ from the DB2 environment for monitoring, DB2 cannot be monitored. Error message is displayed. Check the environment.

Note that the following points about monitor levels described in the next section "How DB2 monitor resources perform monitoring".
A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1". Create the monitor table below in that case.

If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Alert logs does not have the monitor table is displayed.
The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Alphanumeric characters and some symbols (such as underscores) can be used to specify a monitor table name.

Use SQL statements (in the following example, the monitor table is named db2watch)
sql> create table <user_name>.db2watch (num int not null primary key)

sql> insert into db2watch values(0)
sql> commit

Use EXPRESSCLUSTER command
Note that monitor resource settings must be completed beforehand.
clp_db2w --createtable -n <DB2_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_db2w --deletetable -n <DB2_monitor_resource_name>

4.23.2 How DB2 monitor resources perform monitoring

DB2 monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

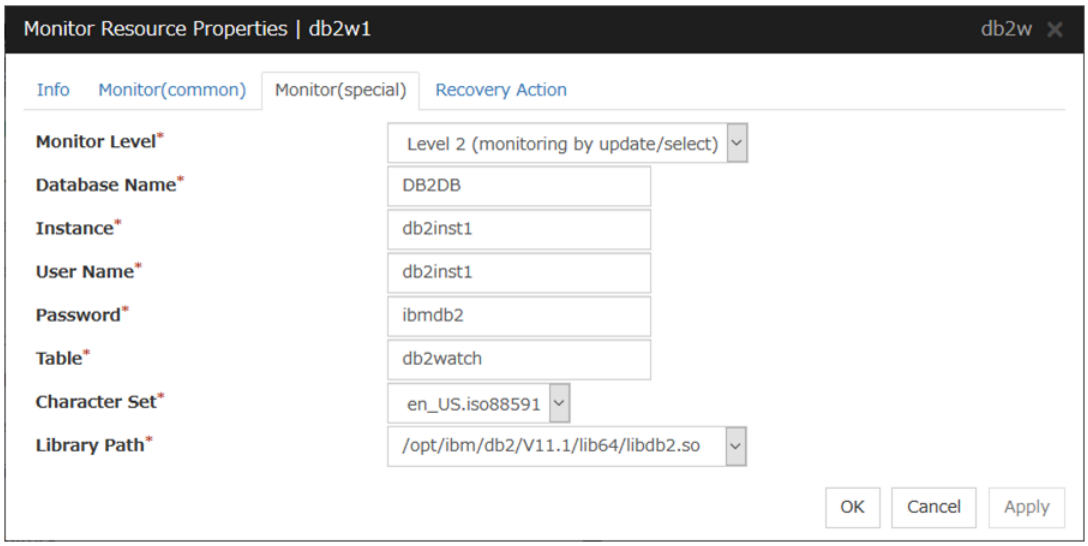
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.23.3 Monitor (special) tab



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (Within 255 bytes)

Specify the database to be monitored. You must specify the database.

Default value: None

Instance (Within 255 bytes)

Specify the instance name of the database to be monitored. You must specify the instance name.

Default value: db2inst1

User Name (Within 255 bytes)

Specify the user name to log on to the database. You must specify the user name.
Specify the DB2 user who can access the specified database.

Default value: db2inst1

Password (Within 255 bytes)

Specify the password to log on to the database. You must specify the password.

Default value: None

Table (Within 255 bytes)

Specify the name of a monitor table created on the database. You must specify the name.
Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Be sure to set the name different from the reserved word in SQL statements. Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database specifications.

Default value: db2watch

Character Set

Specify the character set of DB2. You must specify the character code.

Default value: None

Library Path (Within 1023 bytes)

Specify the home path to DB2. You must specify the path.

Default value: /opt/ibm/db2/V11.1/lib64/libdb2.so

4.24 Understanding FTP monitor resources

FTP monitor resources monitor FTP services that run on the server. FTP monitor resources monitor FTP protocol and they are not intended for monitoring specific applications. FTP monitor resources monitor various applications that use FTP protocol.

4.24.1 FTP monitor resources

For monitoring target resources, specify EXEC resources etc. that start FTP. Monitoring starts after a target resource is activated. However, if FTP cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring.**

To monitor an FTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the FTP server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

FTP service may produce operation logs for each monitoring. Configure FTP settings if this needs to be adjusted.

If a change is made to a default FTP message (such as a banner or welcome message) on the FTP server, it may be handled as an error.

4.24.2 Monitoring by FTP monitor resources

FTP monitor resources connect to the FTP server and execute the command for acquiring the file list. As a result of monitoring, the following is considered as an error:

1. When connection to the FTP service fails.
2. When an error is notified as a response to the FTP command.

4.24.3 Monitor (special) tab

IP Address (Within 79 bytes)

Specify the IP address of the FTP server to be monitored. You must specify this IP address. If it is multi-directional standby server, specify FIP.

Usually, specify the loopback address (127.0.0.1) to connect to the FTP server that runs on the local server. If the addresses for which connection is possible are limited by FTP server settings, specify an address for which connection is possible (such as a floating IP address). To monitor an FTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1-65535)

Specify the FTP port number to be monitored. You must specify a port number.

Default value: 21

User Name (Within 255 bytes)

Specify the user name to log on to FTP.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to FTP.

Default value: None

4.25 Understanding HTTP monitor resources

HTTP monitor resource monitors HTTP daemon that operates on servers.

4.25.1 Note on HTTP monitor resources

For the supported versions of HTTP, see the "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

To monitor an HTTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the HTTP server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

HTTP monitor resource does not support the client authentication and DIGEST authentication..

4.25.2 How HTTP monitor resources perform monitoring

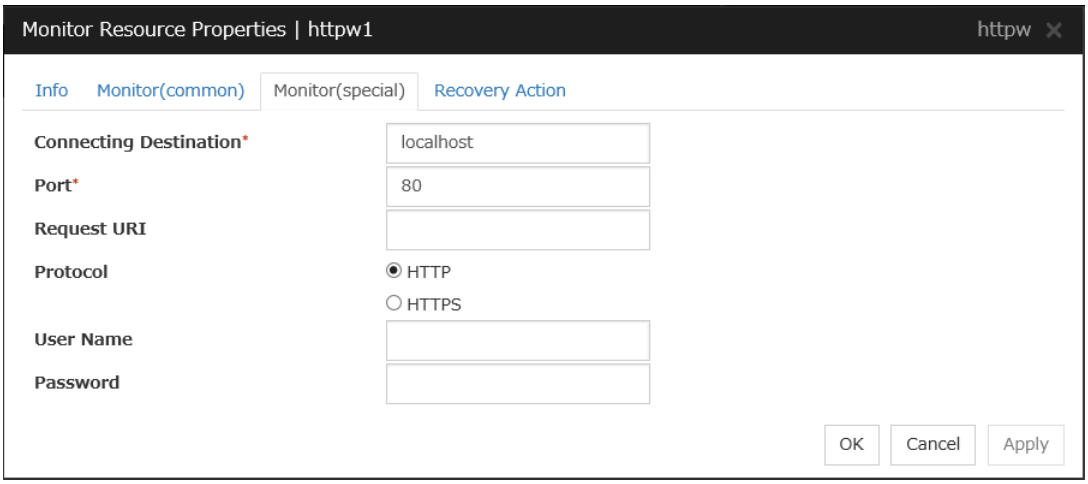
HTTP monitor resource monitors the following:

Monitors the HTTP daemon by connecting to the HTTP daemon on the server and issuing a HEAD request.

This monitor resource determines the following results as an error:

1. an error is notified during the connection to the HTTP daemon.
2. the response message to the HEAD request is not started with "/HTTP"
3. the status code for the response to the HEAD request is in 400s and 500s (when URI other than the default is specified to the request URI)

4.25.3 Monitor (special) tab



Connecting Destination (Within 255 bytes)

Specify the HTTP server name to be monitored. You must specify the name.

Usually, specify the loopback address (127.0.0.1) to connect to the HTTP server that runs on the local server. If the addresses for which connection is possible are limited by HTTP server settings, specify an address for which connection is possible (such as a floating IP address). To monitor an HTTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: localhost

Port (1 to 65535)

Specify the port number used for connecting the HTTP server. You must specify the number.

Default value: 80 (HTTP)
443 (HTTPS)

Request URI (Within 255 bytes)

Set the request URI (for example: "/index.html").

Default value: None

Protocol

Configure protocol used for communication with and HTTP server.. In general, HTTP is selected. If you need to connect with HTTP over SSL, select HTTPS.

Default value: HTTP

Note: OpenSSL is required to use HTTPS.

User Name (Within 255 bytes)

Set a user name to login to HTTP
This field is used only in case that you use BASIC authentication.

Default value: None

Password (Within 255 bytes)

Set a password to login to HTTP
This field is used only in case that you use BASIC authentication.

Default value: None

4.26 Understanding IMAP4 monitor resources

IMAP4 monitor resources monitor IMAP4 services that run on the server. IMAP4 monitor resources monitor IMAP4 protocol but they are not intended for monitoring specific applications. IMAP4 monitor resources monitor various applications that use IMAP4 protocol.

4.26.1 Note on IMAP4 monitor resources

For monitoring target resources, specify EXEC resources that start IMAP4 servers. Monitoring starts after a target resource is activated. However, if IMAP4 servers cannot be started immediately after a target resource is activated, adjust the time using **Wait Time to Start Monitoring.**

To monitor an IMAP4 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the IMAP4 server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

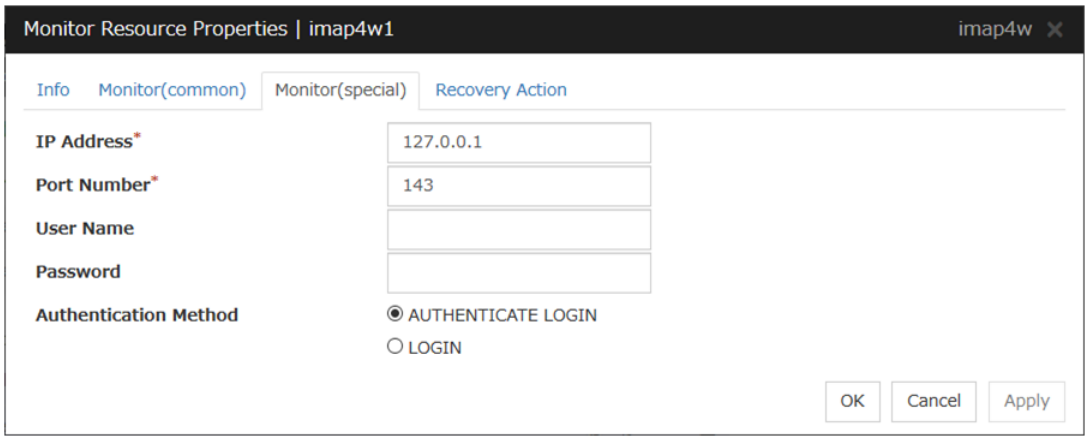
IMAP4 servers may produce operation logs for each monitoring. Configure IMAP4 server settings if this needs to be adjusted.

4.26.2 Monitoring by IMAP4 monitor resources

IMAP4 monitor resources connect to the IMAP4 server and execute the command to verify the operation. As a result of monitoring, the following is considered as an error:

1. When connection to the IMAP4 server fails.
2. When an error is notified as a response to the command.

4.26.3 Monitor (special) tab



IP Address (Within 79 bytes)

Specify the IP address of the IMAP4 server to be monitored. You must specify this IP address. If it is multi-directional standby server, specify FIP.

Usually, specify the loopback address (127.0.0.1) to connect to the IMAP4 server that runs on the local server. If the addresses for which connection is possible are limited by IMAP4 server settings, specify an address for which connection is possible (such as a floating IP address). To monitor an IMAP4 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1-65535)

Specify the port number of the IMAP4 to be monitored. You must specify this port number.

Default value: 143

User Name (Within 255 bytes)

Specify the user name to log on to IMAP4.

Default value: None

Password (Within 189 bytes)

Specify the password to log on to IMAP4. Default value: None

Authentication Method

Select the authentication method to log on to IMAP4. It must follow the settings of IMAP4 being used:

- AUTHENTICATE LOGIN (Default value)
  The encryption authentication method that uses the AUTHENTICATE LOGIN command.

- LOGIN
  The plaintext method that uses the LOGIN command.

4.27 Understanding MySQL monitor resources

MySQL monitor resource monitors MySQL database that operates on servers.

4.27.1 Note on MySQL monitor resources

For the supported versions of MySQL, see the "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

This monitor resource monitors MySQL using the libmysqlclient library of MySQL.
If this monitor resource fails, check that "libmysqlclient.so.xx" exists in the installation directory of the MySQL library.

To monitor a MySQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the MySQL database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

If a value specified by a parameter differs from the MySQL environment for monitoring, an error message is displayed on the Cluster WebUI Alert logs. Check the environment.

Note that the following points about monitor levels described in the next section "How MySQL monitor resources perform monitoring".

A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1". Create the monitor table below in that case.| If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Alert logs does not have the monitor table is displayed.
The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named mysqlwatch)
sql> create table mysqlwatch (num int not null primary key) ENGINE=<engine>;
sql> insert into mysqlwatch values(0);
sql> commit;

Use EXPRESSCLUSTER commands

Note that monitor resource settings must be completed beforehand.

clp_mysqlw --createtable -n <MySQL_monitor_resource_name>

To manually delete a monitor table, execute the following command:

clp_mysqlw --deletetable -n <MySQL_monitor_resource_name>

4.27.2 How MySQL monitor resources perform monitoring

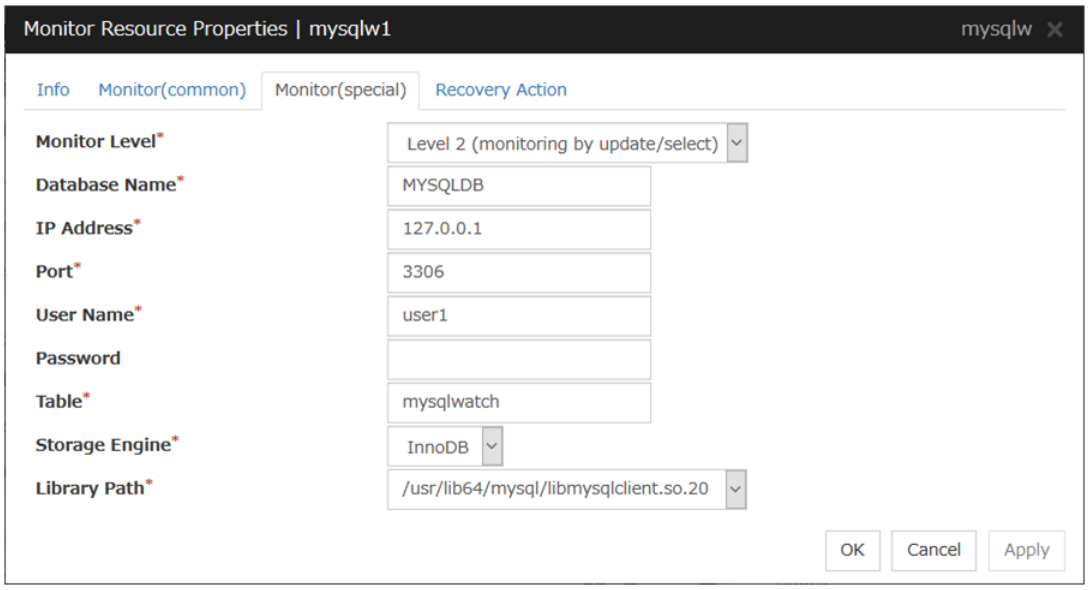
MySQL monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
  An error is recognized if:
  1. An error message is sent in response to a database connection or SQL statement message
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.27.3 Monitor (special) tab



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (Within 255 bytes)

Specify the database name to be monitored. You must specify the name.

Default value: None

IP Address (Within 79 bytes)

Specify the IP address of the server to connect. You must specify the IP address.

Usually, specify the loopback address (127.0.0.1) to connect to the MySQL server that runs on the local server. To monitor a MySQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port 1 to 65535

Specify the port number used for connection. You must specify the port number.

Default value: 3306

User Name (Within 255 bytes)

Specify the user name to log on to the database. You must specify the name.

Specify the MySQL user who can access the specified database.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to the database.

Default value: None

Table (Within 255 bytes)

Specify the name of a monitor table created in the database. You must specify the name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Make sure to set the name different from the reserved word in SQL statements.
Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database.

Default value: mysqlwatch

Storage Engine

Specify the storage engine of MySQL. You must specify the storage engine.

Default value: InnoDB

Library Path (Within 1023 bytes)

Specify the home path to MySQL. You must specify the path.

Default value: /usr/lib64/mysql/libmysqlclient.so.20

4.28 Understanding NFS monitor resources

NFS monitor resource monitors NFS file server that operates on servers.

4.28.1 System requirements for NFS monitor resource

The use of NFS monitor resources requires that the following already be started:

< For Red Hat Enterprise Linux 6, 7 >

- nfs
- rpcbind
- nfslock (unnecessary for NFS v4)

4.28.2 Note on NFS monitor resources

For the supported versions of NFS, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

Specify the exports file for the shared directory to be monitored to enable the connection from a local server.

To monitor an NFS file server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the NFS file server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

It is handled as an error that the deletion of nfsd with the version specified for **NFS version** of the **Monitor(special)** tab and mountd corresponding the nfsd is detected. The correspondence between nfsd versions and mountd versions is as follows.

nfsd version	mountd version
v2 (udp)	v1 (tcp) or v2 (tcp)
v3 (udp)	v3 (tcp)
v4 (tcp)	-

4.28.3 How NFS monitor resources perform monitoring

NFS monitor resource monitors the following:

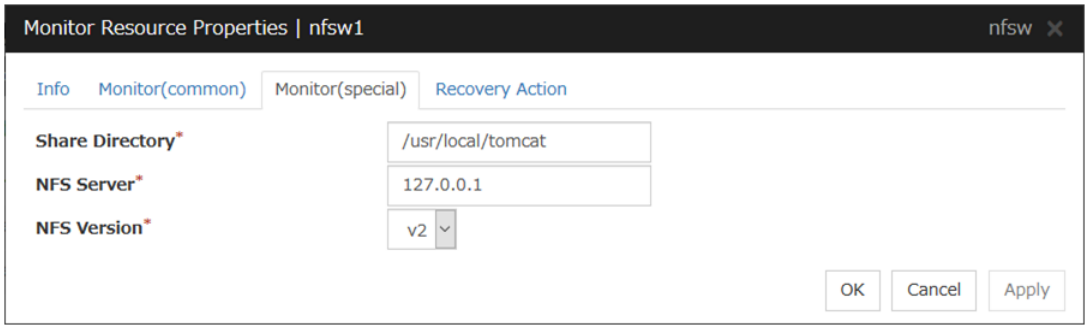
Connect to the NFS server and run NFS test command.

This monitor resource determines the following result as an error:

1. Response to the NFS service request is invalid
2. mountd is deleted (excluding NFS v4)
3. nfsd is deleted
4. The rpcbind service is stopped
5. The export area is deleted(unnecessary for NFS v4)

When an error is repeated the number of times set to retry count, it is considered as NFS error.

4.28.4 Monitor (special) tab



Share Directory (Within 1023 bytes)

Specify a directory for sharing files. You must specify the directory.

Default value: None

NFS Server (Within 255 bytes)

Specify an IP address of the server that monitors NFS. You must specify the IP address.

Usually, specify the loopback address (127.0.0.1) to connect to the NFS file server that runs on the local server. To monitor an NFS file server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

NFS Version

Select one NFS version for NFS monitoring, from the following choices. Be careful to set this NFS version.

For RHEL 7, the NFS version v2 is not supported.

- v2
  Monitors NFS version v2.
- v3
  Monitors NFS version v3.
- v4
  Monitors NFS version v4.

Default value: v2

4.29 Understanding ODBC monitor resources

ODBC monitor resource monitors ODBC database that operates on servers.

4.29.1 Note on ODBC monitor resources

Since unixODBC Driver Manager is used for the monitoring process, installation of ODBC driver for the database to be monitored and settings for the data source on odbc.ini in advance.

To monitor a ODBC database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the ODBC database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

If a value specified by a parameter differs from the ODBC environment for monitoring, an error message is displayed on the Cluster WebUI Alert logs. Check the environment.

Note that the following points about monitor levels described in the next section "How ODBC monitor resources perform monitoring". | A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1". Note that monitor resource settings must be completed beforehand. | If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Aalert logs does not have the monitor table is displayed. | The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named odbcwatch)
sql> create table odbcwatch (num int not null primary key) ENGINE=<engine>;
sql> insert into odbcwatch values(0);
sql> commit;

Use EXPRESSCLUSTER commands
Note that monitor resource settings must be completed beforehand.
clp_odbcw --createtable -n <ODBC_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_odbcw --deletetable -n <ODBC_monitor_resource_name>

4.29.2 How ODBC monitor resources perform monitoring

ODBC monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

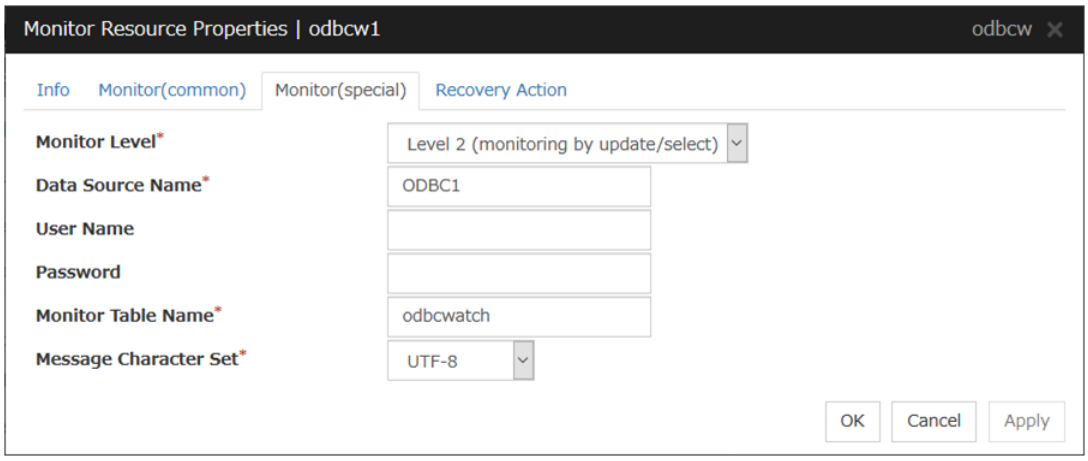
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.29.3 Monitor (special) tab



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Data Source Name (Within 255 bytes)

Specify the data source name to be monitored. You must specify the name.

Default value: None

User Name (Within 255 bytes)

Specify the user name to log on to the database.

If you have specified user name in odbc.ini, you do not need to specify it.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to the database.

Default value: None

Monitor Table Name (Within 255 bytes)

Specify the name of a monitor table created in the database. You must specify the name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Make sure to set the name different from the reserved word in SQL statements.

Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database.

Default value: odbcwatch

Message Character Set

Specify the character code of database messages.

Default value: UTF-8

4.30 Understanding Oracle monitor resources

Oracle monitor resource monitors Oracle database that operates on servers.

4.30.1 Note on Oracle monitor resources

For the supported versions of Oracle, see " Applications supported by monitoring options" in "Software"in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide."

This monitor resource monitors Oracle with the Oracle interface (Oracle Call Interface). For this reason, the library for interface (libclntsh.so) needs to be installed on the server for monitoring.

To monitor an Oracle database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the Oracle database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**. Also, set up the Oracle client on the host OS side, where monitor resources run, and specify the connection string for connecting to the Oracle database on the virtual machine.

If values of a connection string, user name and password specified by a parameter are different from the Oracle environment for monitoring, Oracle monitoring cannot be done. Error message is displayed. Check the environment.

For the user specified with the user name parameter, the default is sys, but when a monitoring-dedicated user has been configured, for each monitor level the following access permissions must be provided for that user (if the sysdba permission is not provided):

Monitor level	Necessary permissions
Level 0 (database status)	SELECT permission for V$INSTANCE
Level 1 (monitoring by select)	SELECT permission for a monitor table
Level 2 (monitoring by update/select)	CREATE TABLE / DROP ANY TABLE / INSERT permission for a monitor table / UPDATE permission for a monitor table /SELECT permission for a monitor table
Level 3 (create/drop table each time)	CREATE TABLE / DROP ANY TABLE / INSERT permission for a monitor table / UPDATE permission for a monitor table /SELECT permission for a monitor table

If the administrator user authentication method is only the OS authentication by setting "NONE" to "REMOTE_LOGIN_PASSWORDFILE" in the initialization parameter file, specify a database user without SYSDBA authority for the user name of the parameter.

When specifying a database user with SYSDBA authority, an error occurs when this monitor resource starts, causing the monitoring process not to be executed.

If sys is specified for the user name, an Oracle audit log may be output. If you do not want to output large audit logs, specify a user name other than sys.

Use the character set supported by OS when creating a database. If Japanese is set to NLS_LANGUAGE in the Oracle initialization parameter file, specify English by NLS_LANG (environment variable of Oracle.) Specify the character set corresponds to the database.
Select the language displayed in the EXPRESSCLUSTER Cluster WebUI Alert logs and OS messages (syslog) for the character code of the monitor resource if an error message is generated from Oracle..
However, as for an error of when connecting to the database such as incorrect user name and alert message may not be displayed correctly.
For the NLS parameter and NLS_LANG settings, see the *Globalization Support Guide* by Oracle Corporation.

The character code settings have no effect on the operation of Oracle.

Note that the following points about monitor levels described in the next section "How Oracle monitor resources perform monitoring".

A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1". Create the monitor table below in that case.
If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Alert logs does not have the monitor table is displayed.
Level 3 monitoring needs more performance power than Level 1 and Level 2 as the table is created/dropped each time. Since also the usage of Oracle resources increases continuously, if you do not restart Oracle instances regularly in the operation, Level 3 monitoring is not recommended.

Selectable monitor level	Prior creation of a monitor table
Level 0 (database status)	Optional
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

When creating by SQL statements (in the following example, the monitor table is named orawatch)
sql> create table orawatch (num number(11,0) primary key);
sql> insert into orawatch values(0);
sql> commit;

*Create this in a schema for the user specified with the user name parameter.

When using EXPRESSCLUSTER commands
Note that monitor resource settings must be completed beforehand.

clp_oraclew --createtable -n <Oracle monitor resource name>
*When the user other than sys is specified for the user name parameter and the sysdba permission is not provided for that user, CREATE TABLE permission is required for that user.
When deleting the created monitor table manually, run the following command:
clp_oraclew --deletetable -n <Oracle monitor resource name>

4.30.2 How Oracle monitor resources perform monitoring

Oracle monitor resources perform monitoring according to the specified monitor level.

- Level 0 (database status)
  The Oracle management table (V$INSTANCE table) is referenced to check the DB status (instance status). This level corresponds to simplified monitoring without SQL statements being executed for the monitor table.

  An error is recognized if:

  1. The Oracle management table (V$INSTANCE table) status is in the inactive state (MOUNTED,STARTED)
  2. The Oracle management table (V$INSTANCE table) database_status is in the inactive state (SUSPENDED,INSTANCE RECOVERY)

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

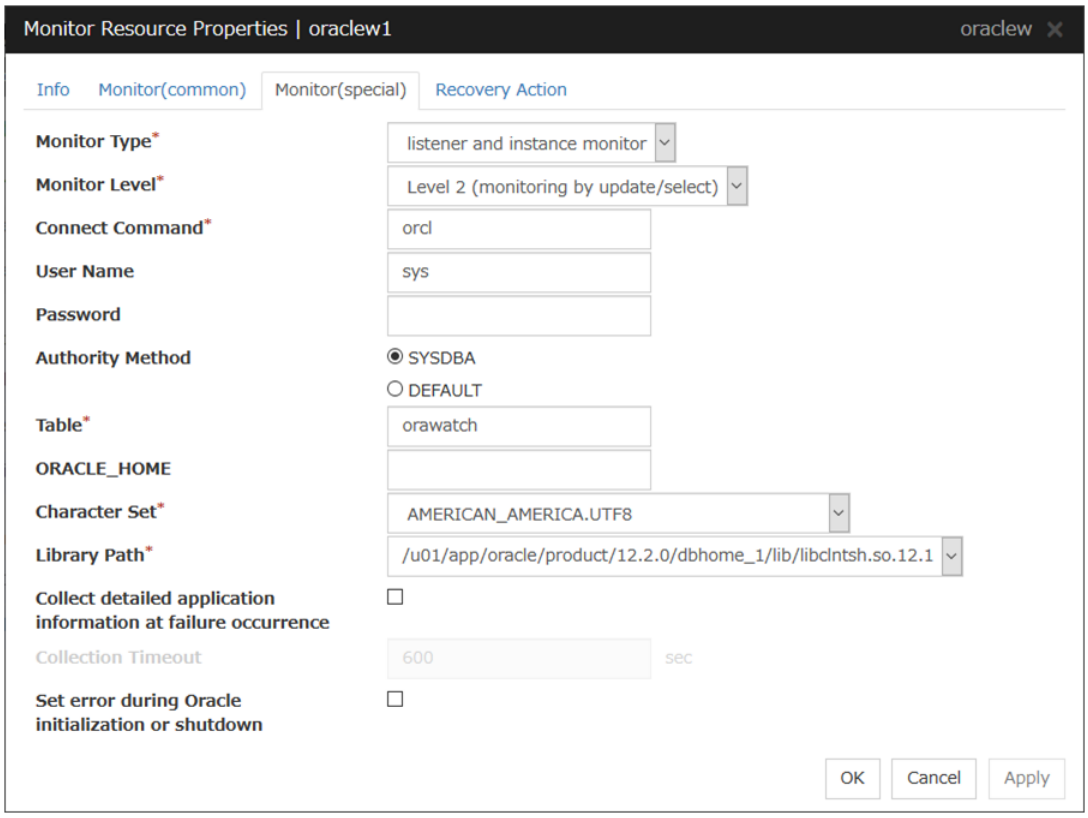
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.30.3 Monitor (special) tab



Monitor Type

Select the Oracle features to be monitored.

- Monitor Listener and Instance (default)
  According to the specified monitor level, database connection, reference, and update operations are monitored.
- Monitor Listener only
  To check for the listener operation, use the tnsping Oracle command. For a monitor resource properties, ORACLE_HOME must be set.

  If ORACLE_HOME is not set, only connection operations for the items specified in the connect string are monitored. Use this to attempt recovery by restarting the Listener service upon a connection error.

  Selecting this setting causes the monitor level setting to be ignored.
- Monitor Instance only
  A direction (BEQ) connection to the database is established, bypassing the listener and, according to the specified monitor level, database connection, reference, and update operations are monitored. For a monitor resource properties, ORACLE_HOME must be set. This is used for direct instance monitoring and recovery action setting without routing through the listener.

  When the monitoring target is a database that has an Oracle12c multi-tenant configuration, monitoring using BEQ connection cannot be performed.

  If ORACLE_HOME is not set, only the connection specified with the connect string is established, and any error in the connection operation is ignored. This is used to set the recovery action for a

non-connection error together with an Oracle monitor resource for which **Monitor Listener only** is specified.

Monitor Level

Select one of the following levels. When the monitor type is set to **Monitor Listener only**, the monitor level setting is ignored.

- Level 0 (database status)
  The Oracle management table (V$INSTANCE table) is referenced to check the DB status (instance status). This level corresponds to simplified monitoring without SQL statements being executed for the monitor table.
- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Connect Command (Within 255 bytes)

Specify the connect string for the database to be monitored. You must specify the connect string.

When **Monitor Type** is set to **Monitor Instance only**, set ORACLE_SID.

Monitor Type	ORACLE_HOME	Connect Command	Monitor Level
Monitor Listener and Instance	Need not be specified	Specify the connect string	As specified
Monitor Listener only	Monitoring dependent on Oracle command if specified	Specify the connect string	Ignored
	Check for connection to the instance through the listener if not specified	Specify the connect string	Ignored
Monitor Instance only	Check for the instance by BEQ connection if specified	Specify ORACLE_SID	As specified
	Check for the instance through the listener if not specified	Specify the connect string	As specified

Default value: None for the connect string

User Name (Within 255 bytes)

Specify the user name to log on to the database. You must specify the name.

Specify the Oracle user who can access the specified database.

Default value: sys

Password (Within 255 bytes)

Specify the password to log on to the database.

Default value: None

Authority Method

Specify the database user authentication.

Default value: SYSDBA

Table (Within 255 bytes)

Specify the name of a monitor table created on the database. You must specify the name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Be sure to set the name different from the reserved word in SQL statements.
Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database.

Default value: orawatch

ORACLE_HOME (Within 255 bytes)

Specify the path name configured in ORACLE_HOME. Begin with [/]. This is used when **Monitor Type** is set to **Monitor Listener only** or **Monitor Instance only**.

Default: None

Character Set

Specify the character set of Oracle. You must specify the character code.

Default value: None

Library Path (Within 1023 bytes)

Specify the library path of Oracle Call Interface (OCI). You must specify the path.

Default value: /u01/app/oracle/product/12.2.0/dbhome_1/lib/libclntsh.so.12.1

Collect detailed application information at failure occurrence

In case that this function is enabled, when Oracle monitor resource detects errors, the detailed Oracle information is collected. The collected information is written to the /opt/nec/clusterpro/work/rm/ "monitor_resource_name"/errinfo.cur folder. When the information is obtained more than once, the existing folders are renamed errinfo.1, errinfo.2, and so on. The detailed Oracle information is collected up to 5 times.

Note: In case of stopping the Oracle service while collecting the information due to the cluster stop, correct information may not be collected.

Default value: disabled

Collection Timeout

Specify the timeout value for collecting detailed information.

Default value: 600

Set error during Oracle initialization or shutdown

If this function is enabled, a monitor error occurs immediately when Oracle initialization or shutdown in progress is detected.

Disable this function when Oracle is automatically restarted during operation in cooperation with Oracle Clusterware or the like. Monitoring becomes normal even during Oracle initialization or shutdown.

However, a monitor error occurs if Oracle initialization or shutdown continues for one hour or more.

Default value: Disabled

4.31 Understanding Oracle Clusterware Synchronization Management monitor resources

It can't be used.

4.32 Understanding POP3 monitor resources

POP3 monitor resources monitor POP3 services that run on the server. POP3 monitor resources monitor POP3 protocol but they are not intended for monitoring specific applications. POP3 monitor resources monitor various applications that use POP3 protocol.

4.32.1 Note on POP3 monitor resources

For monitoring target resources, specify EXEC resources etc. that start POP3 services. Monitoring starts after target resource is activated. However, if POP3 services cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

To monitor a POP3 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the POP3 server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

POP3 services may produce operation logs for each monitoring. Configure the POP3 settings if this needs to be adjusted.

4.32.2 Monitoring by POP3 monitor resources

POP3 monitor resources connect to the POP3 server and execute the command to verify the operation. As a result of monitoring, the following is considered as an error:

1. When connection to the POP3 server fails.
2. When an error is notified as a response to the command.

4.32.3 Monitor (special) tab

IP Address (Within 79 bytes)

Specify the IP address of the POP3 server to be monitored. You must specify this IP address. If it is multi-directional standby server, specify FIP.

Usually, specify the loopback address (127.0.0.1) to connect to the POP3 server that runs on the local server. If the addresses for which connection is possible are limited by POP3 server settings, specify an address for which connection is possible (such as a floating IP address). To monitor a POP3 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1-65535)

Specify the POP3 port number to be monitored. You must specify this port number.

Default value: 110

User Name (Within 255 bytes)

Specify the user name to log on to POP3.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to POP3. Click **Change** and enter the password in the dialog box.

Default value: None

Authentication Method

Select the authentication method to log on to POP3. It must follow the settings of POP3 being used:

- APOP (Default value)
  The encryption authentication method that uses the APOP command.
- USER/PASS
  The plain text method that uses the USER/PASS command.

4.33 Understanding PostgreSQL monitor resources

PostgreSQL monitor resource monitors PostgreSQL database that operates on servers.

4.33.1 Note on PostgreSQL monitor resources

For the supported versions of PostgreSQL, see "Applications supported by monitoring options" in "Software"in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

This monitor resource uses the libpq library of PostgreSQL to monitor PostgreSQL.
If this monitor resource fails, set the application library path to the path where the libpq library of PostgreSQL exists.

To monitor a PostgreSQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the PostgreSQL database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

If a value specified by a parameter differs from the PostgreSQL environment for monitoring, a message indicating an error is displayed on the Alert logs of the Cluster WebUI. Check the environment.

For client authentication, on this monitor resource, the following authentication methods that can be set to the "pg_hba.conf" file has been checked its operation.
trust, md5, password
When this monitor resource is used, messages like those shown below are output to a log on the PostgreSQL side. These messages are output by the monitor processing and do not indicate any problems.

```
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle ERROR: table "psqlwatch" does not exist
YYYY-MM-DD hh:mm:ss JST moodle moodle STATEMENT: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: CREATE TABLE psqlwatch (num␣
↪INTEGER NOT NULL PRIMARY KEY)
YYYY-MM-DD hh:mm:ss JST moodle moodle NOTICE: CREATE TABLE / PRIMARY KEY will create␣
↪implicit index "psqlwatch_pkey" for table "psql watch"
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
```

Note that the following points about monitor levels described in the next section "How PostgreSQL monitor resources perform monitoring".| A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1". Create the monitor table below in that case.
If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Alert logs does not have the monitor table is displayed.
The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named psqlwatch)
sql> CREATE TABLE psqlwatch (num INTEGER NOT NULL PRIMARY KEY);
sql> INSERT INTO psqlwatch VALUES(0) ;
sql> COMMIT;

Use EXPRESSCLUSTER commands
Note that monitor resource settings must be completed beforehand.
clp_psqlw --createtable -n <PostgreSQL_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_psqlw --deletetable -n <PostgreSQL_monitor_resource_name>

4.33.2 How PostgreSQL monitor resources perform monitoring

PostgreSQL monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (update/select/vacuum) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

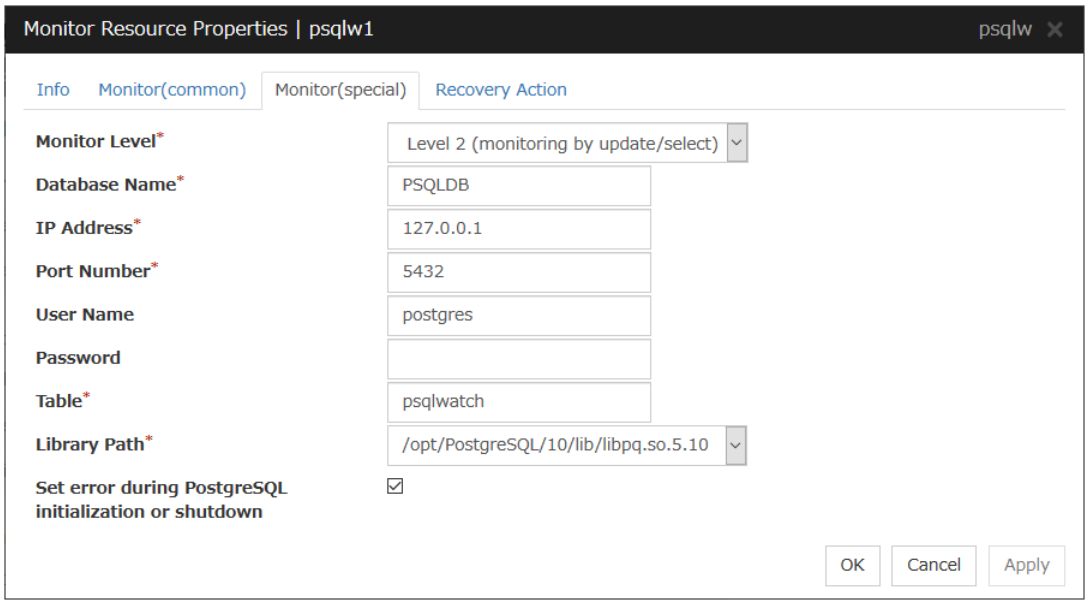
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (create / insert / select / drop / vacuum) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.33.3 Monitor (special) tab



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select/vacuum) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop / vacuum) type.

  Default: Level 2 (monitoring by update/select)

Database Name (Within 255 bytes)

Specify the database name to be monitored. You must specify the name.

Default value: None

IP Address (Within 79 bytes)

Specify the IP address of the server to connect. You must specify the IP address.

Usually, specify the loopback address (127.0.0.1) to connect to the PostgreSQL server that runs on the local server. To monitor a PostgreSQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port (1 to 65535)

Specify the port number for connection. You must specify the number.

Default value: 5432

User Name (Within 255 bytes)

Specify the user name to log on to the database. You must specify the name.

Specify the PostgreSQL user who can access the specified database.

Default value: postgres

Password (Within 255 bytes)

Specify the password to log on to the database.

Default value: None

Table (Within 255 bytes)

Specify the name of a monitor table created in the database. You must specify the table name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Be sure to set the name different from the reserved word in SQL statements.
Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database specifications.

Default value: psqlwatch

Library Path (Within 1023 bytes)

Specify the home path to PostgreSQL. You must specify the path.

Default value: /opt/PostgreSQL/10/lib/libpq.so.5.10

Set error during PostgreSQL initialization or shutdown

When this function is enabled, a monitor error occurs immediately upon the detection of PostgreSQL initialization or shutdown in progress.

When this function is disabled, monitoring becomes normal even during PostgreSQL initialization or shutdown.

However, a monitor error occurs if PostgreSQL initialization or shutdown continues for one hour or more.

Default value: Enabled

4.34 Understanding Samba monitor resources

Samba monitor resource monitors samba file server that operates on servers.

4.34.1 Note on Samba monitor resources

For the supported versions of samba, seesee "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

If this monitor resource fails, the parameter value and samba environment may not match. Check the samba environment

Specify the smb.conf file for the shared name to be monitored to enable a connection from a local server. Allow guest connection when the security parameter of the smb.conf file is "share."

Samba functions except file sharing and print sharing

To monitor a samba file server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the samba file server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

If the smbmount command is run on the monitoring server when the samba authentication mode is "Domain" or "Server," it may be mounted as a user name specified by the parameter of this monitor resource.

4.34.2 How Samba monitor resources perform monitoring

From internal version 4.1.0-1, Samba monitor resources use the shared library libsmbclient.so.0.

Samba monitor resource monitors the following:

By connecting to samba server and verify establishment of tree connection to resources of the samba server.

This monitor resource determines the following results as an error:

1. A response to samba service request is invalid.

4.34.3 Monitor (special) tab

Share Name (Within 255 bytes)

Specify the shared name of samba server to be monitored. You must specify the name.

Default value: None

IP Address (Within 79 bytes)

Specify the IP address of samba server. You must specify the IP address.

Usually, specify the loopback address (127.0.0.1) to connect to the samba file server that runs on the local server. To monitor a samba file server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port (1 to 65535)

Specify the port number to be used by samba daemon. You must specify the port number. If the version of libsmbclient is 3 or earlier (e.g. libsmbclient.so provided with RHEL 6), the **Port** field can accept only 139 or 445. Specify the same value for smb ports of the smb.conf as well.

Default value: 139

User Name (Within 255 bytes)

Specify the user name to log on to the samba service. You must specify the user name.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to the samba service.

Default value: None

4.35 Understanding SMTP monitor resources

SMTP monitor resource monitors SMTP daemon that operates on servers.

4.35.1 Note on SMTP monitor resources

For the supported versions of SMTP,see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

If a state that the load average exceeds the RefuseLA value set in the sendmail.def file for a certain period of time, the monitoring commands may consider this as an error and perform failover.

To monitor an SMTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the SMTP server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

4.35.2 How SMTP monitor resources perform monitoring

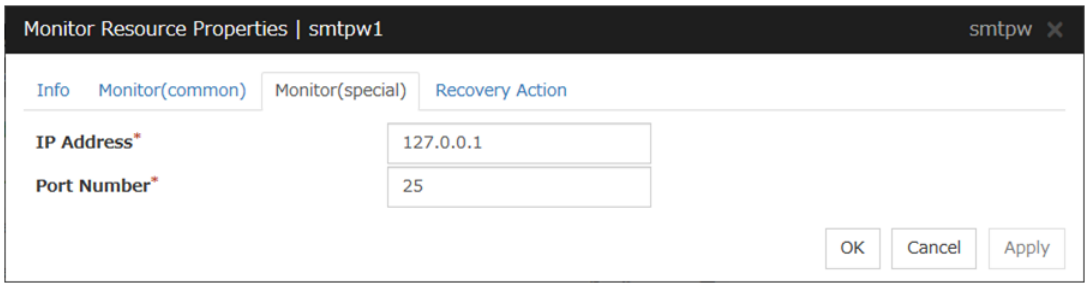
SMTP monitor resource monitors the following:

Monitors the SMTP daemon by connecting to the SMTP daemon on the server and issuing the NOOP command

This monitor resource determines the following result as an error:

1. An error reporting as the response to the SMTP daemon or issued NOOP command.

4.35.3 Monitor (special) tab



IP Address (Within 79 bytes)

Specify the IP address of the SMTP server to be monitored. You must specify the IP address.

Usually, specify the loopback address (127.0.0.1) to connect to the SMTP server that runs on the local server. To monitor an SMTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port (1 to 65535)

Specify the port number used to connect to the SMTP server. You must specify the port number.

Default value: 25

4.36 Understanding SQL Server monitor resources

SQL Server monitor resource monitors SQL Server database that operates on servers.

4.36.1 Note on SQL Server monitor resources

For the supported versions of SQL Server, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

This monitor resource monitors SQL Server using Microsoft ODBC Driver for SQL Server.

If a value specified by a parameter differs from the SQL Server environment for monitoring, an error message is displayed on the Cluster WebUI Alert logs. Check the environment.

If "Level 1" is selected as a monitor level described in the next subsection "How SQL Server monitor resources perform monitoring", monitor tables must be created manually beforehand.
A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1".
If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Alert logs does not have the monitor table is displayed.
The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 0 (database status)	Optional
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:
Alphanumeric characters and some symbols (such as underscores) can be used to specify a monitor table name.

Use SQL statements (in the following example, the monitor table is named sqlwatch)

- When SET IMPLICIT_TRANSACTIONS OFF

  sql> CREATE TABLE sqlwatch (num INT NOT NULL PRIMARY KEY)
  sql> GO
  sql> INSERT INTO sqlwatch VALUES(0)
  sql> GO

- When SET IMPLICIT_TRANSACTIONS ON

  sql> CREATE TABLE sqlwatch (num INT NOT NULL PRIMARY KEY)
  sql> GO
  sql> INSERT INTO sqlwatch VALUES(0)
  sql> GO
  sql> COMMIT
  sql> GO

Use EXPRESSCLUSTER commands
clp_sqlserverw --createtable -n <SQL Server_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_sqlserverw --deletetable -n <SQL Server_monitor_resource_name>

4.36.2 How SQL Server monitor resources perform monitoring

SQL Server monitor resources perform monitoring according to the specified monitor level.

- Level 0 (database status)
  The SQL Server management table is referenced to check the DB status.This level corresponds to simplified monitoring without SQL statements being issued for the monitor table.

  An error is recognized if:

  1. The database status is not online

- Level 1 (monitoring by select)

Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

An error is recognized if:

1. An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to10 digits. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

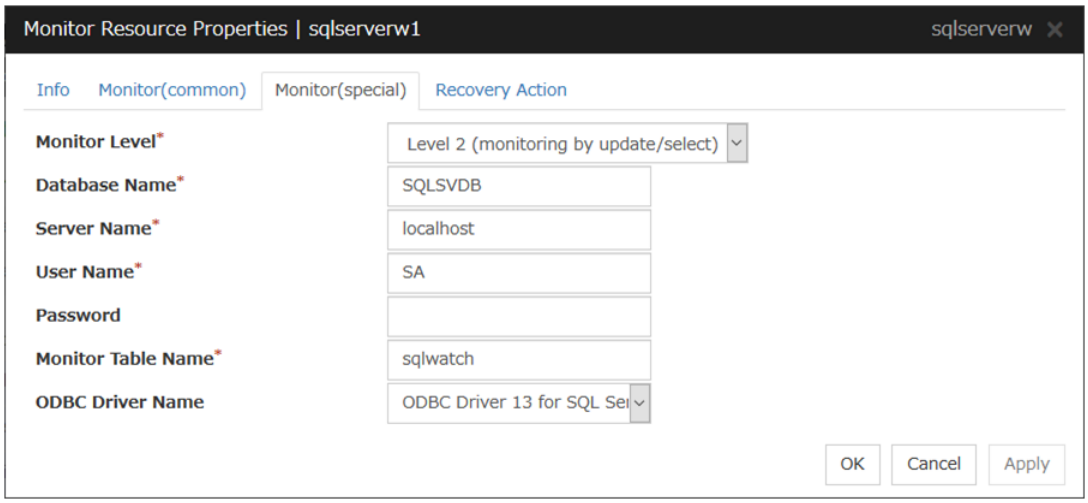
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.36.3 Monitor (special) tab



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 0 (database status)
  The SQL Server management table is referenced to check the DB status. This level corresponds to simplified monitoring without SQL statements being executed for the monitor table.

- Level 1 (monitoring by select)

Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (Within 255 bytes)

Specify the database name to be monitored. You must specify the name.

Default value: None

Server Name (Within 255 bytes)

Specify the database server name to be monitored. You must specify the name.

Default value: localhost

User Name (Within 255 bytes)

Specify the user name to log on to the database. You must specify the name.

Specify the SQL Server user who can access the specified database.

Default value: SA

Password (Within 255 bytes)

Specify the password to log on to the database. You must specify the password.

Default value: None

Monitor Table Name (Within 255 bytes)

Specify the name of a monitor table created in the database. You must specify the name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Make sure to set the name different from the reserved word in SQL statements.
Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database.

Default value: sqlwatch

ODBC Driver Name (Within 255 bytes)

Specify the ODBC driver name of SQL Server. You must specify the name.

Default value: ODBC Driver 13 for SQL Server

4.37 Understanding Sybase monitor resources

Sybase monitor resource monitors Sybase database that operates on servers.

4.37.1 Note on Sybase monitor resources

For the supported versions of Sybase, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

This monitor resource monitors ASE using Open Client DB-Library/C of ASE. If a value specified by a parameter differs from the ASE environment for monitoring, an error message is displayed on the Cluster WebUI Alert logs. Check the environment .

Note that the following points about monitor levels described in the next section "How Sybase monitor resources perform monitoring".

A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1" Create the monitor table below in that case.
If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the Cluster WebUI Alert logs does not have the monitor table is displayed.
The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 0 (database status)	Optional
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Alphanumeric characters and some symbols (such as underscores) can be used to specify a monitor table name.

Use SQL statements (in the following example, the monitor table is named sybwatch)
sql> CREATE TABLE sybwatch (num INT NOT NULL PRIMARY KEY)
sql> GO
sql> INSERT INTO sybwatch VALUES(0)
sql> GO
sql> COMMIT
sql> GO

Use EXPRESSCLUSTER commands
Note that monitor resource settings must be completed beforehand.
clp_sybasew --createtable -n <Sybase_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_sybasew --deletetable -n <Sybase_monitor_resource_name>

4.37.2 How Sybase monitor resources perform monitoring

Sybase monitor resources perform monitoring according to the specified monitor level.

- Level 0 (database status)
  The Sybase management table (sys.sysdatabases) is referenced to check the DB status. This level corresponds to simplified monitoring without SQL statements being issued for the monitor table.

  An error is recognized if:

  1. The database status is in an unusable state, e.g., offline.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

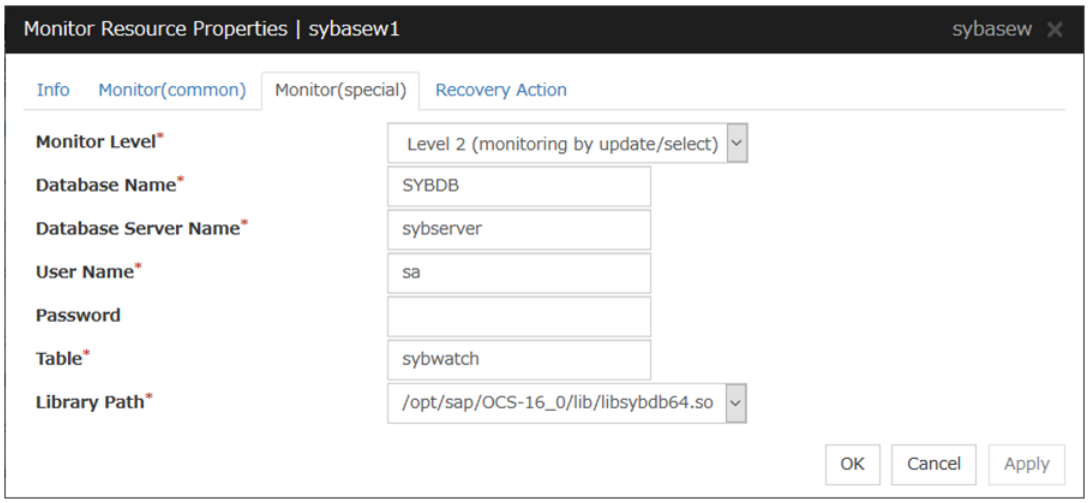
  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 10 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

  1. An error message is sent in response to a database connection or SQL statement message
  2. The written data is not the same as the read data

4.37.3 Monitor (special) tab



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 0 (database status)
  The Sybase management table (sys.sysdatabases) is referenced to check the DB status. This level corresponds to simplified monitoring without SQL statements being issued for the monitor table.
- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.
- Level 2 (monitoring by update/select)
  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.
- Level 3 (create/drop table each time)
  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (Within 255 bytes)

Specify the database to be monitored. You must specify the database.

Default value: None

Database Server Name (Within 255 bytes)

Specify the database server name to be monitored. You must specify the database server.

Default value: None

User Name (Within 255 bytes)

Specify the user name to log on to the database. You must specify the user name.

Specify the Sybase user who can access the specified database.

Default value: sa

Password (Within 255 bytes)

Specify the password to log on to the database.

Default value: None

Table (Within 255 bytes)

Specify the name of a monitor table created in the database. You must specify the name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Make sure to set the name different from the reserved word in SQL statements.
Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database.

Default value: sybwatch

Library Path (Within 1023 bytes)

Specify the home path to Sybase. You must specify the path.

Default value: /opt/sap/OCS-16_0/lib/libsybdb64.so

4.38 Understanding Tuxedo monitor resources

Tuxedo monitor resource monitors Tuxedo that operates on servers.

4.38.1 Note on Tuxedo monitor resources

For the supported versions of Tuxedo, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

If any library of the Tuxedo such as libtux.so does not exist, monitoring cannot be performed.

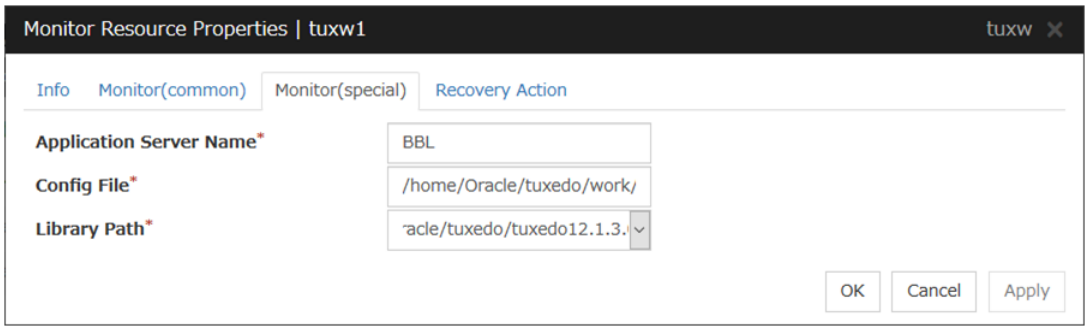
4.38.2 How Tuxedo monitor resources perform monitoring

Tuxedo monitor resource monitors the following:

This monitor resource executes the application server monitoring by using the API of the Tuxedo. The command determines the following results as an error:

1. An error is reported in response to ping.

4.38.3 Monitor (special) tab



Application Server Name (Within 255 bytes)

Specify the IP address of the server to be monitored. You must specify the name.

Default value: BBL

Config File (Within 1023 bytes)

Specify the placement file name of Tuxedo. You must specify the name.

Default value: None

Library Path (Within 1023 bytes)

Specify the library path of Tuxedo. You must specify the path.

Default value: /home/Oracle/tuxedo/tuxedo12.1.3.0.0/lib/libtux.so

4.39 Understanding Weblogic monitor resources

Weblogic monitor resource monitors Weblogic that operates on servers.

4.39.1 Note on Weblogic monitor resources

For the supported versions of Weblogic, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

A Java environment is required to start monitoring with this monitor resource. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

If Weblogic monitor resources are not available at the startup of WebLogic, they will be judged as being abnormal. Adjust [Wait Time to Start Monitoring], or start WebLogic before the startup of the Weblogic monitor resources (for example, specify the EXEC resource for starting Weblogic as a monitor target resource)

4.39.2 How Weblogic monitor resources perform monitoring

Weblogic monitor resource monitors the following:

Monitors the application server by performing connect with the "webLogic.WLST" command.

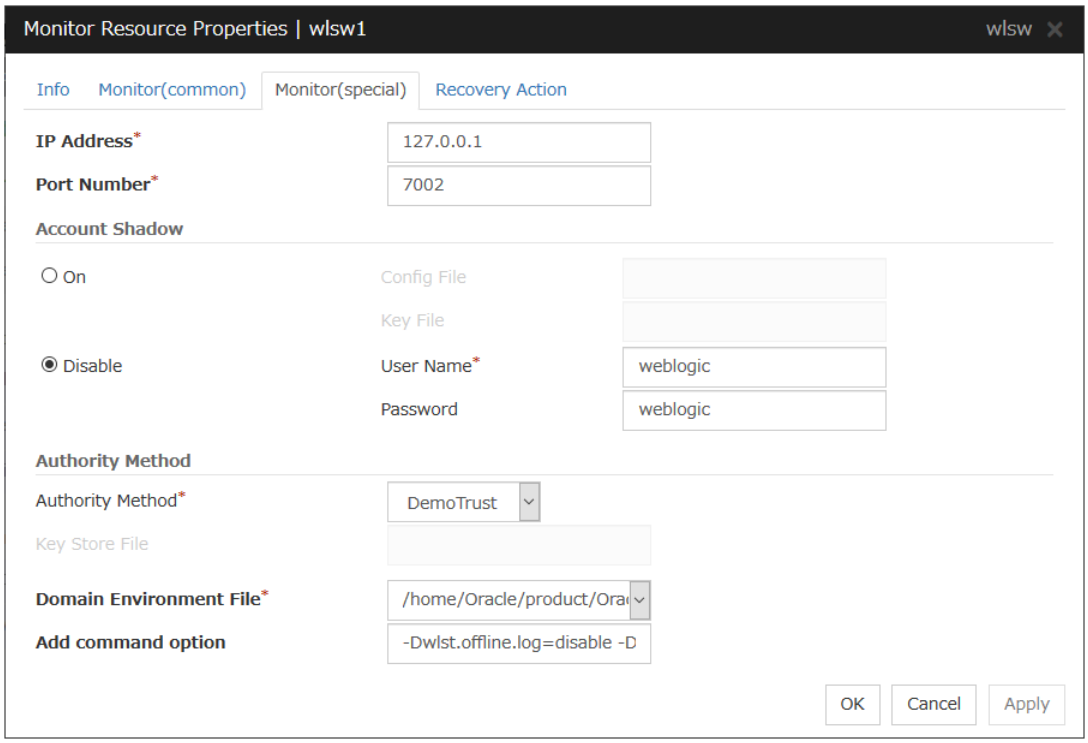
This monitor resource determines the following results as an error:

1. An error reporting as the response to the connect.

The operations are as follows, based on **Authentication Method**.

- DemoTrust: SSL authentication method using authentication files for demonstration of Weblogic
- CustomTrust: SSL authentication method using user-created authentication files
- Not Use SSL: SSL authentication method is not used.

4.39.3 Monitor (special) tab



IP Address (Within 79 bytes)

Specify the IP address of the server to be monitored. You must specify the IP address.

Default value: 127.0.0.1

Port (1 to 65535)

Specify the port number used to connect to the server. You must specify the number.

Default value: 7002

Account Shadow

When you specify a user name and a password directly, select **Off**. If not, select **On**. You must specify the setting.

Default value: Off

Config File (Within 1023 bytes)

Specify the file in which the user information is saved. You must specify the file if **Account Shadow** is **On**.

Default value: None

Key File (Within 1023 bytes)

Specify the file in which the password required to access to a config file path is saved. Specify the full path of the file. You must specify the file if **Account Shadow** is **On**.

Default value: None

User Name (Within 255 bytes)

Specify the user name of Weblogic. You must specify the file if **Account Shadow** is **Off**.

Default value: weblogic

Password (Within 255 bytes)

Specify the password of Weblogic.

Default value: weblogic

Authority Method

Specify the authentication method when connecting to an application server. You must specify the method.

Specify **DemoTrust** or **Custom Trust** for **Authority Method**, in order to execute monitoring by using the SSL communication.

It is determined whether to use **DemoTrust** or **CustomTrust**, according to the setting of Weblogic Administration Console.

When **Keystores** of Weblogic Administration Console is set to **Demo Identity and Demo Trust**, specify **Demo Trust**. In this case, you do not need to make settings for **Key Store File**.

When **Keystores** of Weblogic Administration Console is set to **Custom Identity and Custom Trust**, specify **Custom Trust**. In this case, you need to make settings for **Key Store File**.

Default value: DemoTrust

Key Store File (Within 1023 bytes)

Specify the authentication file when authenticating SSL. You must specify this when the **Authority Method** is **CustomTrust**. Set the file specified in **Custom Identity Key Store File** on Weblogic Administration Console.

Default value: None

Domain Environment File (Within 1023 bytes)

Specify the domain environment file mane of Weblogic. You must specify the file name.

Default value:
/home/Oracle/product/Oracle_Home/user_projects/domains/base_domain/bin/setDomainEnv.sh

Add Command Option (Within 1023 bytes)

Specify the additional command option when changing the option to be passed to the [webLogic.WLST] command.

Default value: -Dwlst.offline.log=disable -Duser.language=en_US

4.40 Understanding Websphere monitor resources

Websphere monitor resource monitors Websphere that operates on servers.

4.40.1 Note on Websphere monitor resources

For the supported versions of Websphere, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

A Java environment is required to start monitoring with this monitor resource. The application server system uses Java functions. If Java stalls, it may be recognized as an error.

4.40.2 How Websphere monitor resources perform monitoring

Websphere monitor resource monitors the following:

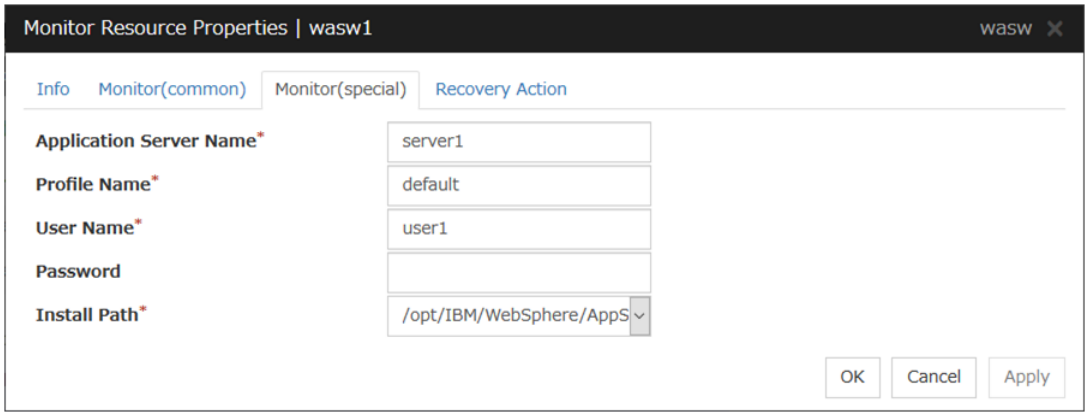
This monitor resource monitors the following:

Executes monitoring of the application server by using the serverStatus.sh command.

The monitor resource determines the following result as an error:

1. an error is reported with the state of the acquired application server.

4.40.3 Monitor (special) tab



Application Server Name (Within 255 bytes)

Specify the application server name to be monitored. You must specify the name.

Default value: server1

Profile Name (Within 1023 bytes)

Specify the profile name of Websphere. You must specify the name.

Default value: default

User Name (Within 255 bytes)

Specify the user name of Websphere. You must specify the name.

Default value: None

Password (Within 255 bytes)

Specify the password of Websphere.

Default value: None

Install Path (Within 1023 bytes)

Specify the installation path of Websphere. You must specify the path.

Default value: /opt/IBM/WebSphere/AppServer

4.41 Understanding WebOTX monitor resources

WebOTX monitor resource monitors WebOTX that operates on servers.

4.41.1 Note on WebOTX monitor resources

For the supported versions of WebOTX, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

A Java environment is required to start monitoring with this monitor resource. The application server system uses Java functions. If Java stalls, it may be recognized as an error.

4.41.2 How WebOTX monitor resources perform monitoring

WebOTX monitor resource monitors the following:

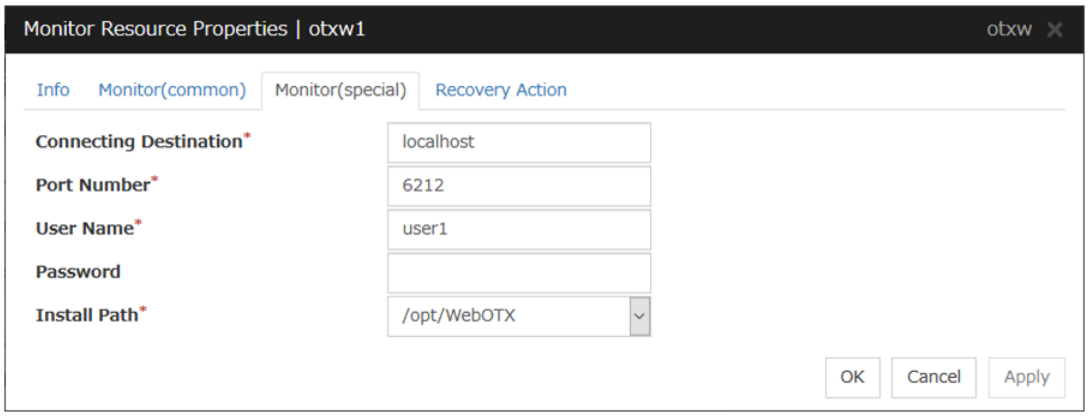
This monitor resource monitors the following:

Executes monitoring of the application server by using the otxadmin.sh command.

The monitor resource determines the following result as an error:

1. an error is reported with the state of the acquired application server.

4.41.3 Monitor (special) tab



Connecting Destination (Within 255 bytes)

Specify the server name to be monitored. You must specify the name.

Default value: localhost

Port (1 to 65535)

Specify the port number used to connect to the server. You must specify the number.

When monitoring a WebOTX user domain, specify the management port number for the WebOTX domain. The management port number is the number which was set for "domain.admin.port" of <domain_name>.properties when the domain was created. Refer to the WebOTX documents for details of <domain_name>.properties.

Default value: 6212

User Name (Within 255 bytes)

Specify the user name of WebOTX. You must specify the name.

When monitoring a WebOTX user domain, specify the login user name for the WebOTX domain.

Default value: None

Password (Within 255 bytes)

Specify the password of WebOTX.

Default value: None

Install Path (Within 1023 bytes)

Specify the installation path of WebOTX. You must specify the path.

Default value: /opt/WebOTX

4.42 Understanding JVM monitor resources

JVM monitor resources monitor information about the utilization of resources that are used by Java VM or an application server running on a server.

4.42.1 Note on JVM monitor resources

The **Java installation path** on the **JVM Monitor** tab of **Cluster Properties** must be set before adding JVM monitor resource.

For a target resource, specify an application server running on Java VM such as WebLogic Server or WebOTX. As soon as the JVM monitor resource has been activated, the Java Resource Agent starts monitoring, but if the target (WebLogic Server or WebOTX) cannot start running immediately after the activation of the JVM monitor resource, use **Wait Time to Start Monitoring** to compensate.

The setting of Monitor(common) tab-Retry Count is invalid. When you'd like to delay error detection, please change the setting of Cluster Properties-JVM monitor Tab-Resource Measurement Settings [Common]-Retry Count.

4.42.2 How JVM monitor resources perform monitoring

JVM monitor resource monitors the following:

Monitors application server by using JMX (Java Management Extensions).

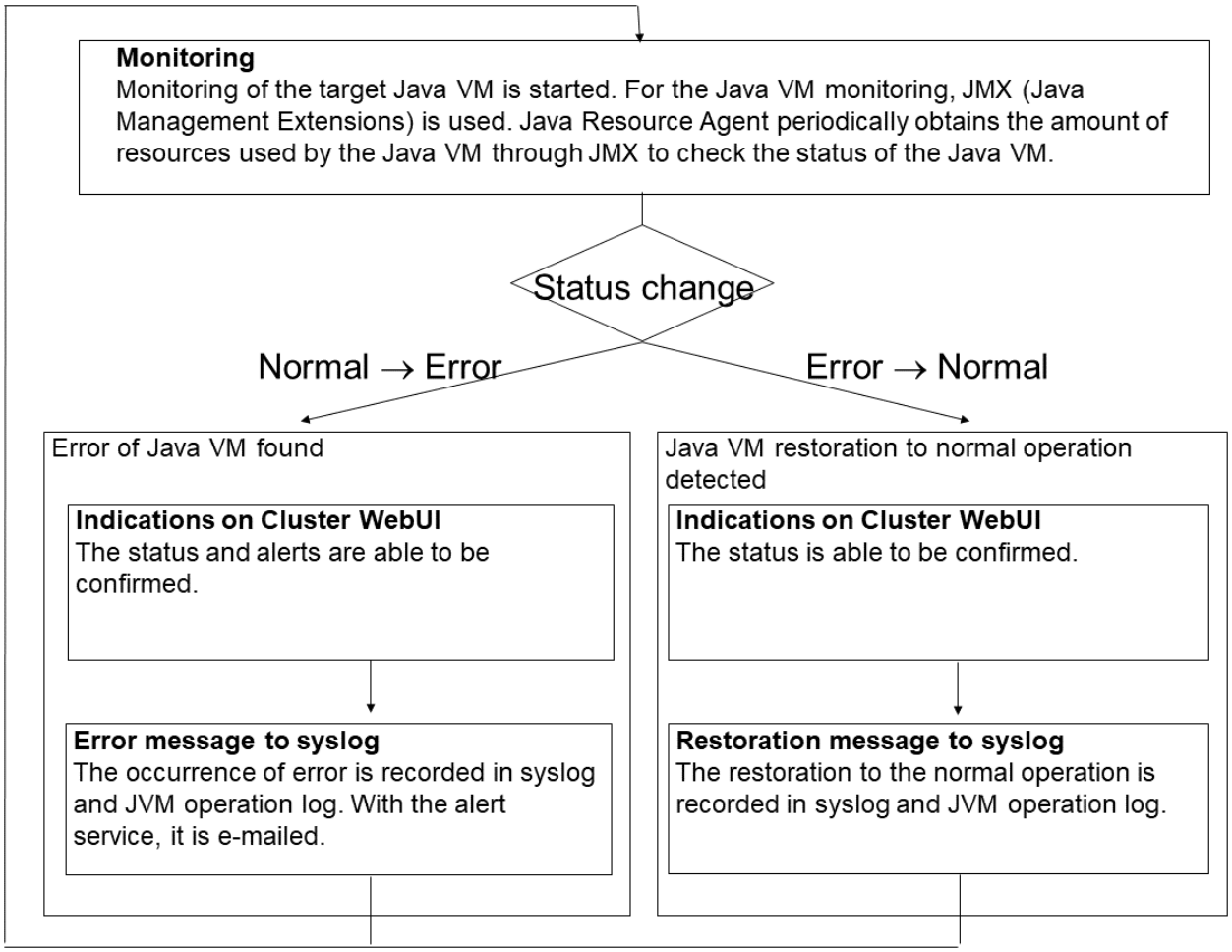
The monitor resource determines the following results as errors:

- Target Java VM or application server cannot be connected
- The value of the used amount of resources obtained for the Java VM or application server exceeds the user-specified threshold a specified number of times (error decision threshold) consecutively

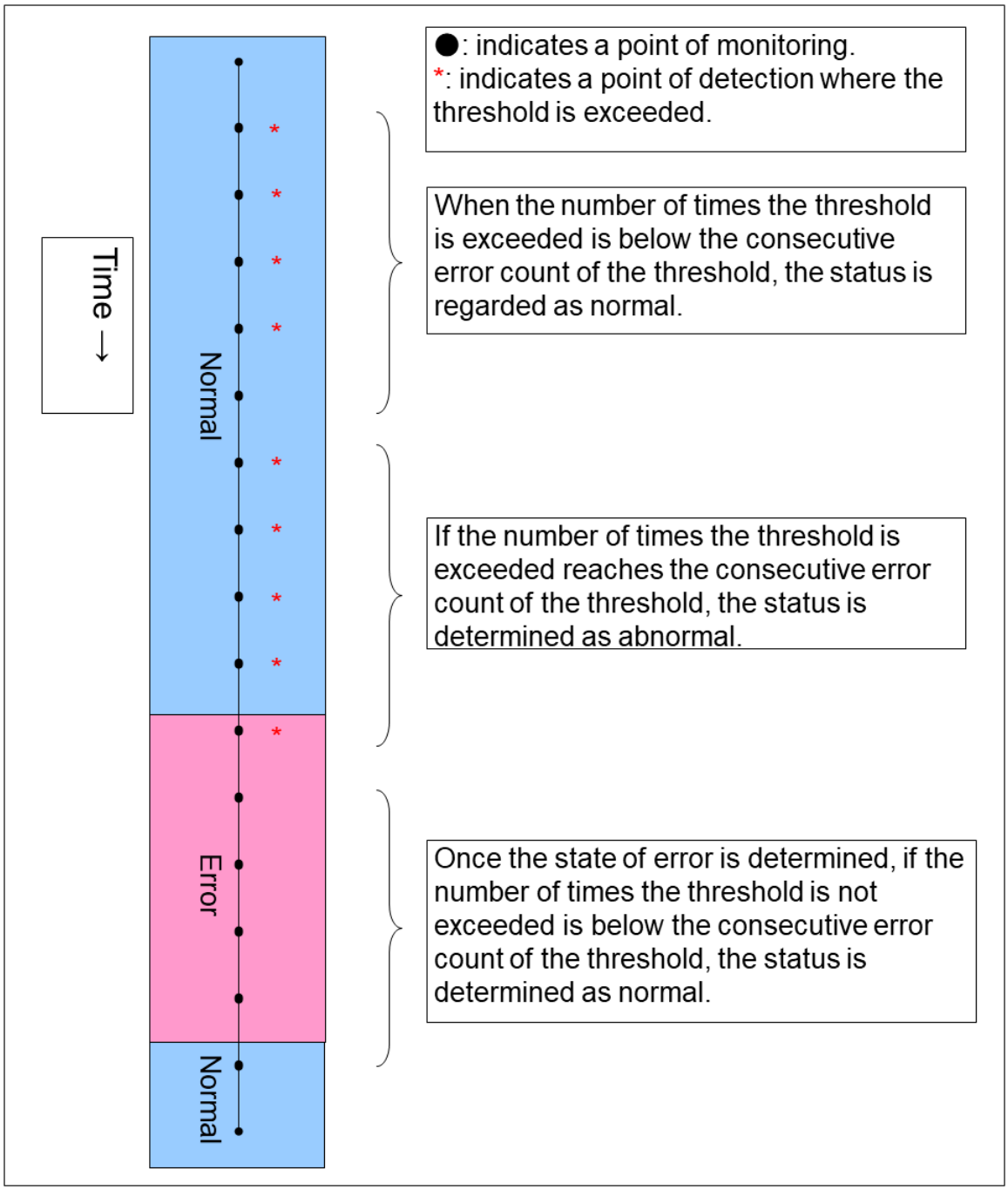
As a result of monitoring, an error is regarded as having been solved if:

- The value falls below the threshold when restarting the monitoring after the recovery action.

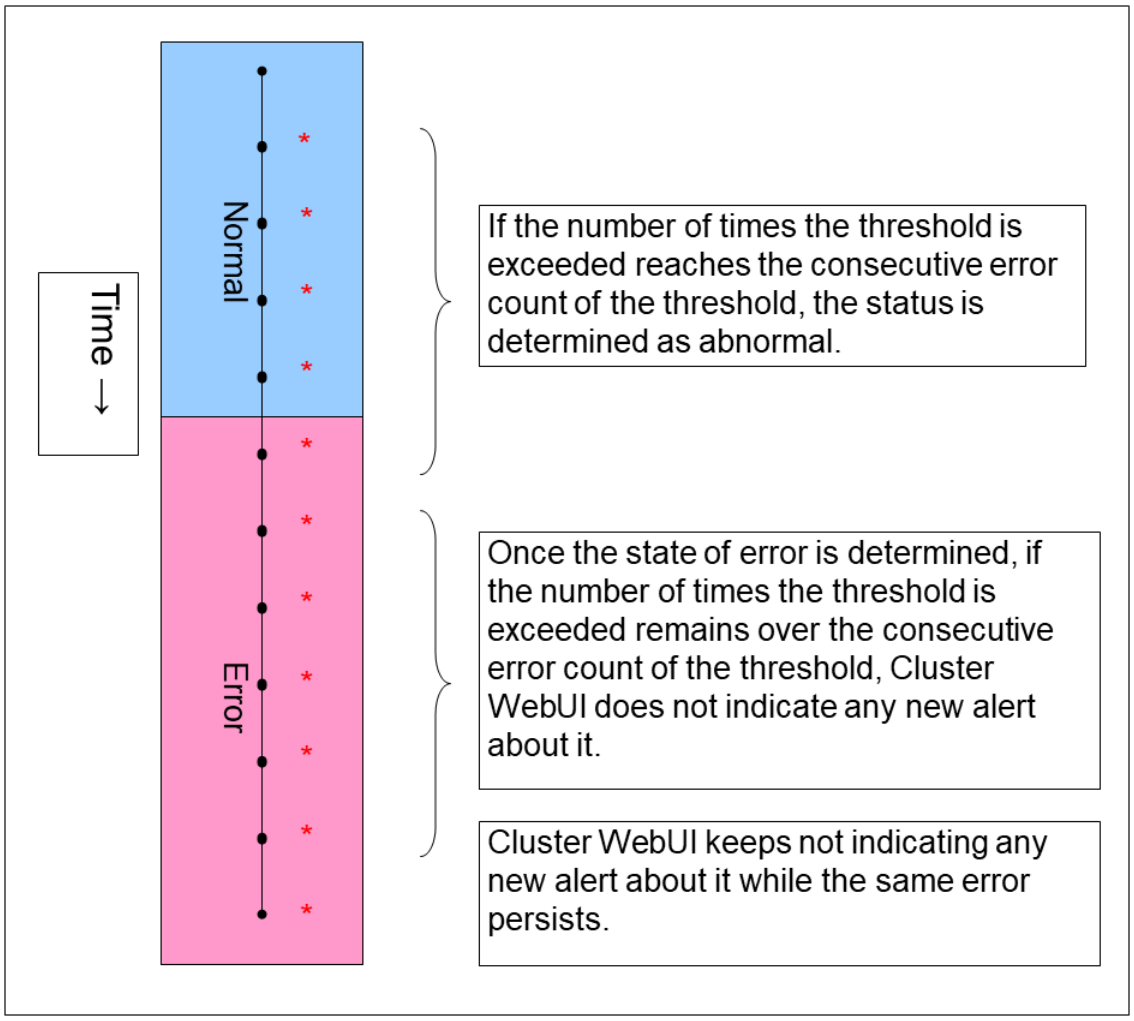
Note: Collect Cluster Logs in the Cluster WebUI does not handle the configuration file and log files of the target (WebLogic Server or WebOTX).



The standard operations when the threshold is exceeded are as described below.



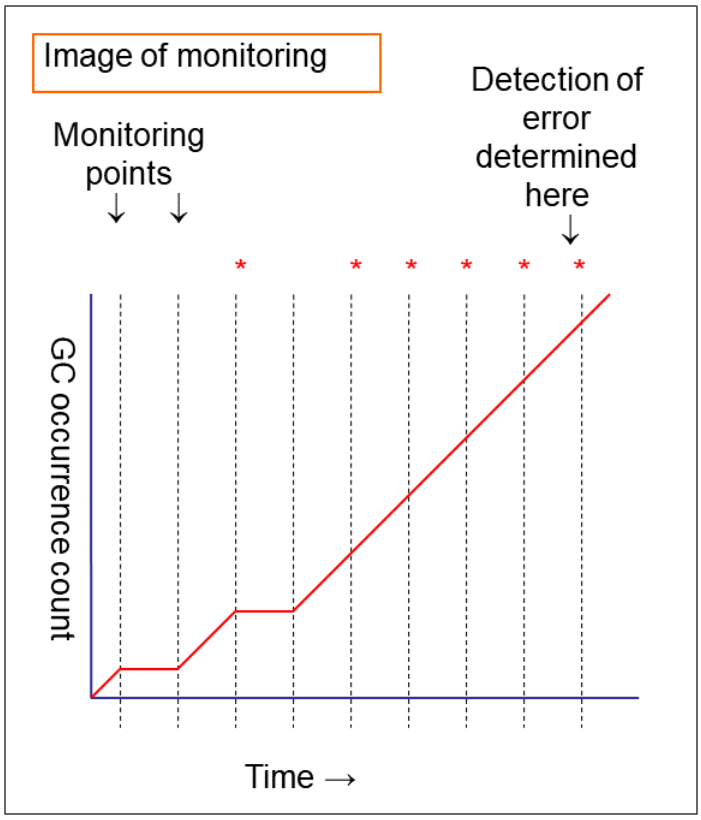
The operations performed if an error persists are as described below.



The following example describes the case of monitoring Full GC (Garbage Collection).

The JVM monitor resource recognizes a monitor error if Full GC is detected consecutively the number of times specified by the error threshold. In the following chart, * indicates that Full GC is detected by the JVM monitor resource when the error threshold is set to 5 (times).

Full GC has a significant influence on the system, thus the recommended error threshold is 1 time.



4.42.3 Linking with the load balancer (health check function)

Target load balancer: Load balancer with health check function for HTML files

JVM monitor resources can link with the load balancer. This section describes an example of linking when WebOTX is used as the application to be monitored. The load balancer linkage provides a health check function and target Java VM load calculation function. To link with the BIG-IP Local Traffic Manager, see "*Linking with the BIG-IP Local Traffic Manager*".

Distributed nodes are servers that are subject to load balancing, while the distributed node module is installed in the distributed nodes. The distributed node module is included in InterSec/LB400*.

To use the function, configure the settings through the Cluster WebUI Cluster Properties - **JVM monitor** tab - **Load Balancer Linkage Settings** dialog box; the health check function of the load balancer is linked.

When a load balancing system is configured with the load balancer on the server, the JVM monitor resource renames the HTML file specified by **HTML File Name** to the name specified by **HTML Renamed File Name** upon the detection of a WebOTX error (for example, exceeding the threshold for collected information).

The JVM monitor resource halts for the wait time, or 20 seconds, after renaming the HTML file. The wait time is intended to prevent WebOTX from being restarted before the load balancer finishes disconnecting the distributed node.

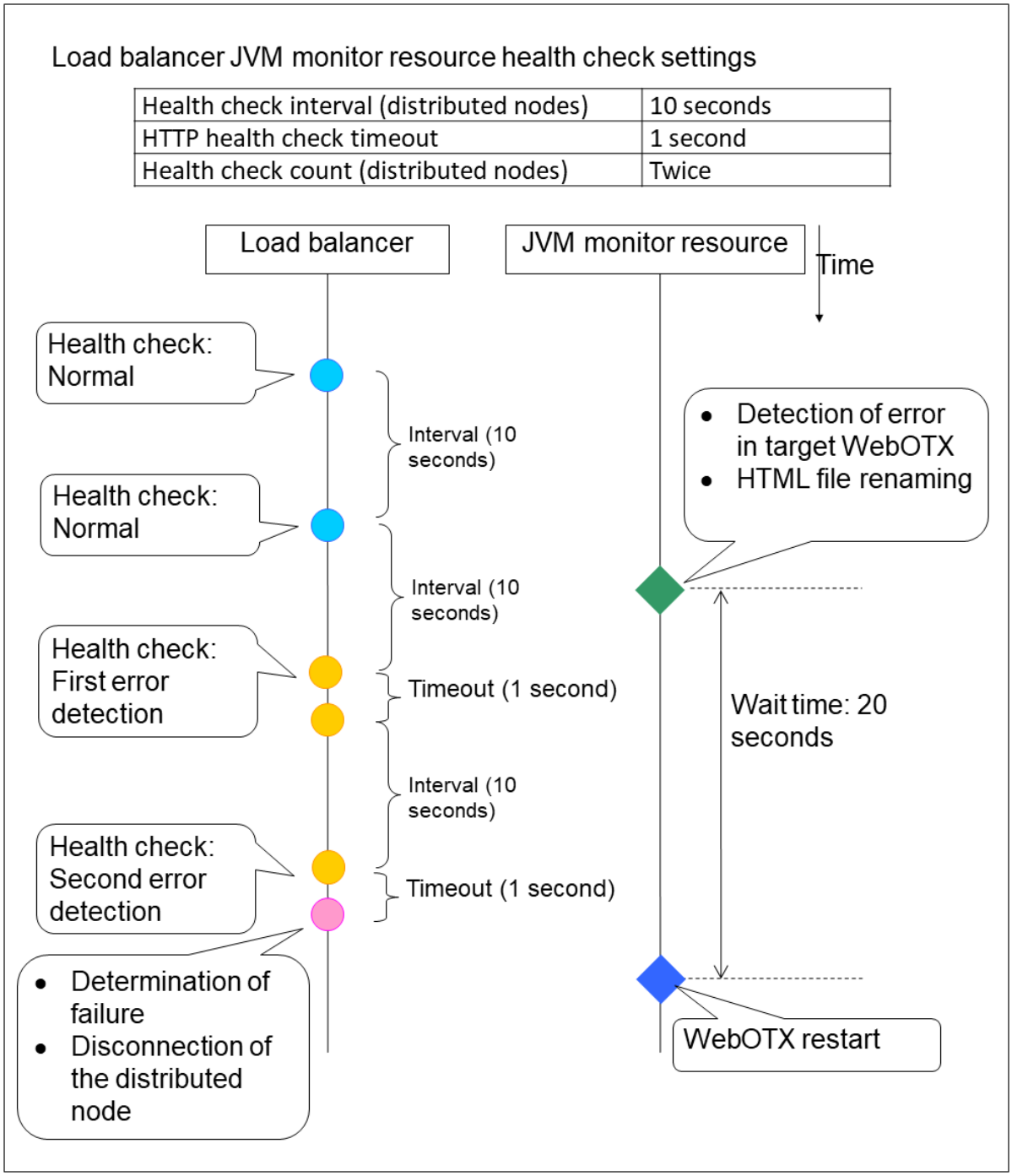
Once the JVM monitor resource detects the normality of WebOTX (e.g., the threshold specified for the collected information is not exceeded after reconnection) after WebOTX rebooting, the HTML file name set with **HTML Renamed File Name** is restored to that specified by **HTML File Name**.

The load balancer periodically health-checks the HTML file, and if a health check fails, the distributed node is determined to be not alive, so that the load balancer disconnects that distributed node. In the case of InterSec/LB400*, configure the health check interval, health check timeout, and retry count to determine the node down state by the health check with the health check (distributed node) interval parameter, HTTP health check timeout parameter, and

health check (distributed node) count parameter, that are accessible from **ManagementConsole** for the load balancer->**LoadBalancer->System Information**.

Configure the parameters using the following as a reference.

20-second wait time >= (health check (distributed node) interval + HTTP health check timeout) x health check (distributed node) count



4.42.4 Linking with the load balancer (target Java VM load calculation function)

Target load balancer: InterSec/LB400*

JVM monitor resources can link with the load balancer. This section describes an example of linking when WebOTX is used as the application to be monitored. The load balancer linkage provides a health check function and target Java VM load calculation function. To link with the BIG-IP Local Traffic Manager, see "*Linking with the BIG-IP Local Traffic Manager*".

Distributed nodes are servers that are subject to load balancing, while the distributed node module is installed in the distributed node. The distributed node module is included in InterSec/LB400*.

To use this function, the following settings are required. This function works together with the CPU load-dependent weighting function of the load balancer.

- **Properties** - **Monitor(special)** tab -> **Tuning** properties - **Memory** dialog box - **Monitor Heap Memory Rate** - **Total Usage**
- **Properties** - **Monitor(special)** tab-> **Tuning** properties - **Load Balancer Linkage** dialog box - **Memory Pool Monitor**

According to the following steps, first install the distributed node module on each server, and then execute the load balancer linkage setup command clpjra_lbsetup.sh to configure the distributed node modules.

Note: Execute the command from an account having the root privilege.

---

1. Execute "<EXPRESSCLUSTER_installation_folder>/ha/jra/bin/clpjra_lbsetup.sh." The functions of the arguments are as described below.

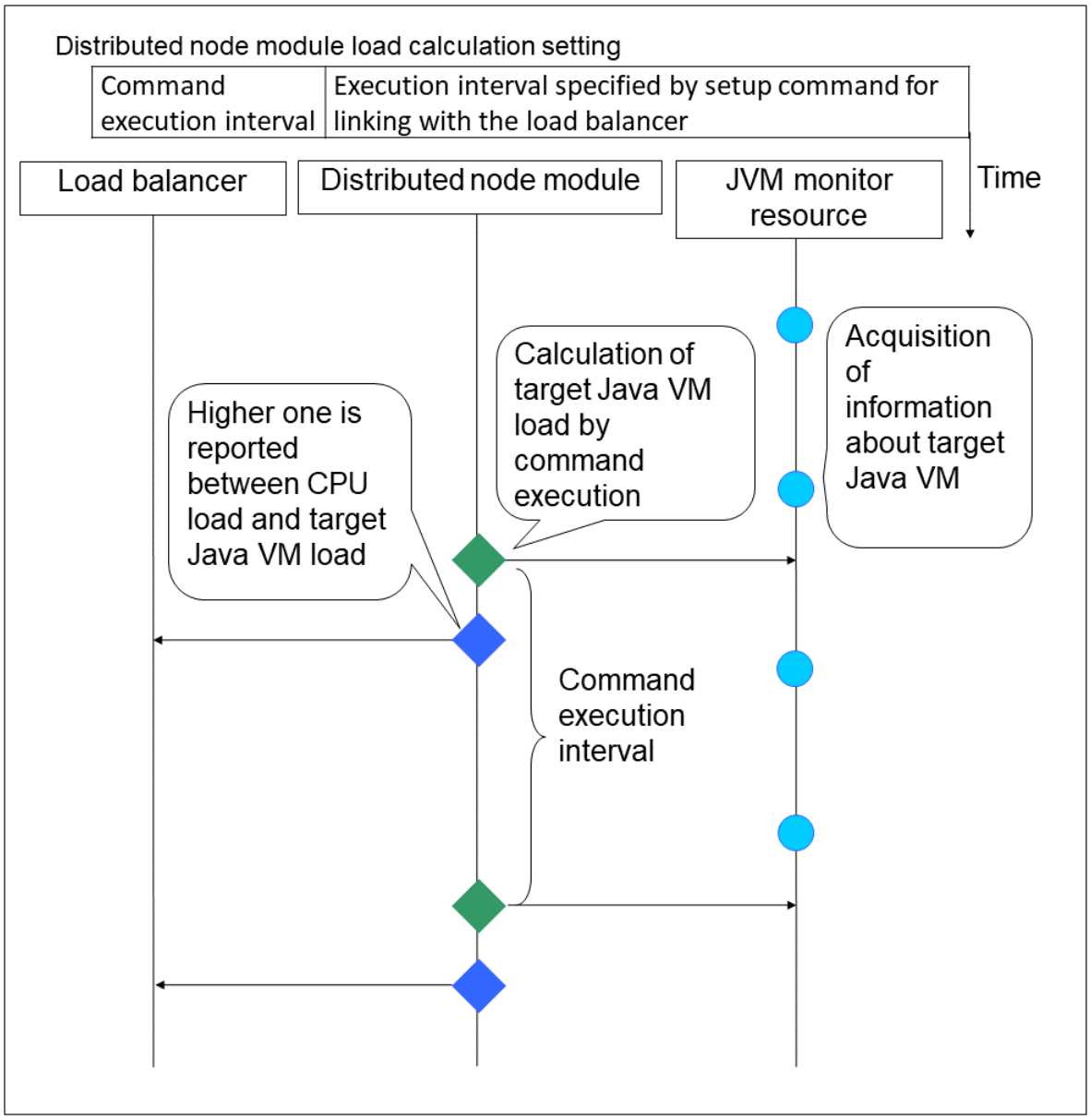
   (Example) *clpjra_lbsetup.sh -e 1 -i 120 -t 180*

Argument	Description	Value
-e	Enables or disables the function.	0 or 1
		0: Disable 1: Enable
-i	Specify the execution interval for the target Java VM load calculation command, in seconds.	1 to 2147483646
-t	Specify the timeout for the target Java VM load calculation command, in seconds.	1 to 2147483646

The JVM monitor resource calculates the load on the target Java VM according to the information obtained about the Java memory. Obtain the Java VM load from the following expression. The threshold is the value obtained by multiplying the entire amount of the Java heap area by the use ratio set with the **Monitor(special)** tab - **Tuning** properties - **Memory** tab - **Monitor Heap Memory Rate** - **Total Usage**.

Java VM load (%) = current memory usage (MB) x 100/threshold (MB)

For the distributed node module installed on a server on which JVM monitor resource is running, commands are periodically executed to compare the obtained target Java VM load with the CPU load obtained separately, and to notify the load balancer of the higher load value as a CPU load. The load balancer distributes the traffic (requests) to the appropriate servers according to the CPU load of the distributed node.



4.42.5 Linking with the BIG-IP Local Traffic Manager

Target load balancer: BIG-IP Local Traffic Manager

The JVM monitor resource can link with BIG-IP LTM. Hereafter, the explanation assumes the use of Tomcat as the application server to be monitored. Linkage with BIG-IP LTM offers the distributed node control function and the target Java VM load calculation function.

The linkage between BIG-IP LTM and the JVM monitor resource is realized with the BIG-IP series API (iControl).

The distributed node is the load distribution server, and the linkage module is that which is installed in each distributed node. The linkage module is contained in Java Resource Agent.

To use the distributed node control function, specify the setting with **Cluster WebUI Cluster Properties** -> **JVM Monitor** tab -> **Load Balancer Linkage Settings** dialog box, **JVM monitor resource Properties** - **Monitor(special)** tab - **Tuning** properties - **Load Balancer Linkage** tab.

To use the target Java VM load calculation function, specify the setting with**Cluster WebUI Cluster Properties** -> **JVM Monitor** tab -> **Load Balancer Linkage Settings** dialog box.

The following BIG-IP LTM linkage error message is output to the JVM operation log. For details, see "*JVM monitor resource log output messages*" in "10. *Error messages*".

```
Error: Failed to operate clpjra_bigip.[error code]
```

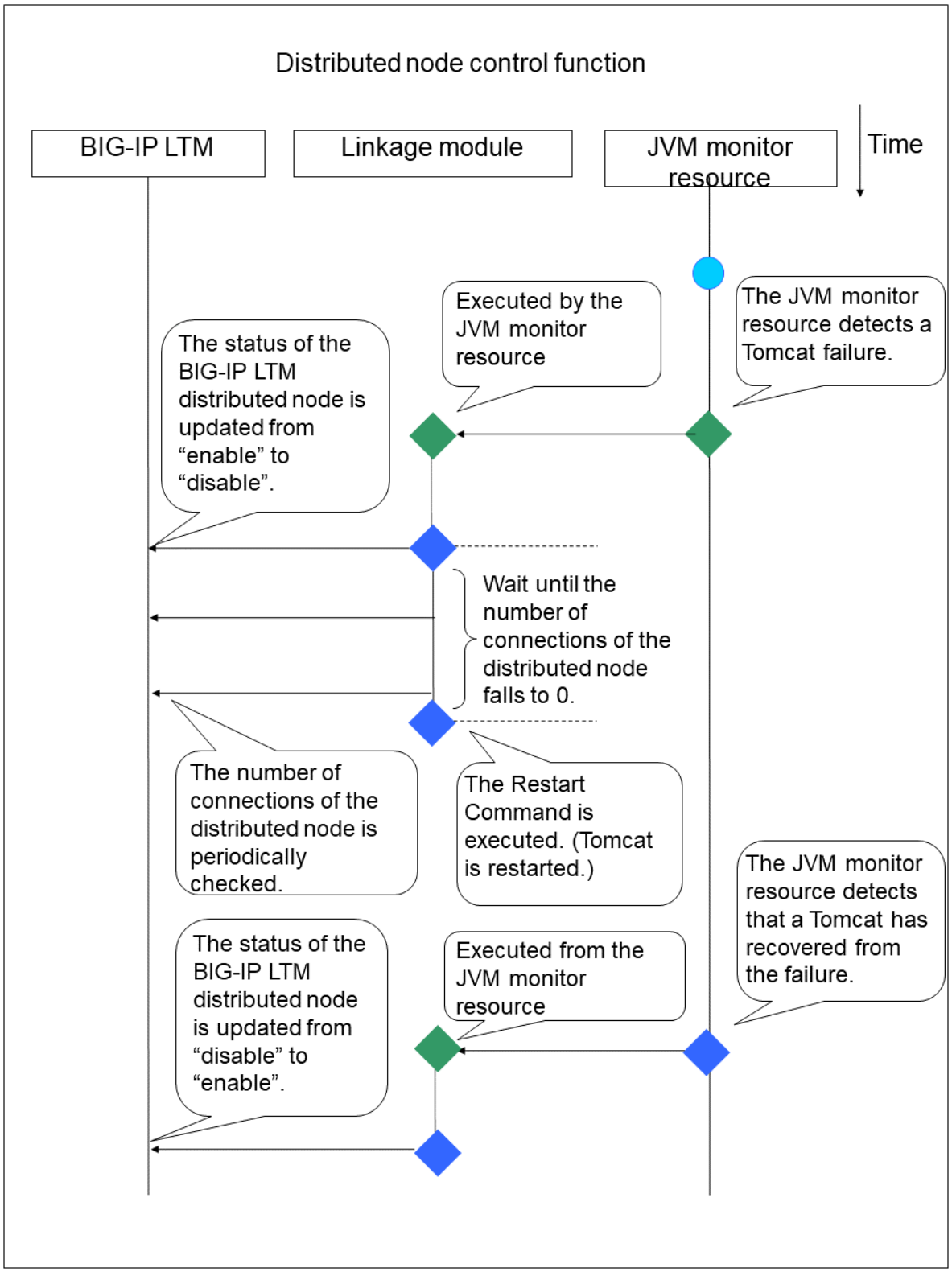
If the relevant server configures the BIG-IP LTM load distribution system, when the JVM monitor detects a Tomcat failure (for example: the amount of collection information exceeds the specified threshold), iControl is used to update the BIG-IP LTM distributed node status from "enable" to "disable."

After updating the status of the distributed node of BIG-IP LTM, the JVM monitor waits until the number of connections of the distributed node falls to 0. After waiting, it executes **Restart Command** specified on the JVM monitor resource **Properties** - **Monitor(special)** tab -> **Tuning** properties - **Load Balancer Linkage** tab. It does not execute the action specified by **Restart Command** if the number of connections of the distributed node does not fall to 0, even if **Timeout** elapses, as specified on the **JVM monitor resource Properties** - **Monitor(special)** tab -> **Tuning** properties - **Load Balancer Linkage** tab.

When the JVM monitor detects a Tomcat failure recovery, it uses iControl to update the status of the BIG-IP LTM distributed node from "disable" to "enable." In this case, it does not execute the action specified by **Restart Command** specified on the JVM monitor resource **Properties** - **Monitor(special)** tab -> **Tuning** properties - **Load Balancer Linkage** tab.

If the distributed node status is "disable", BIG-IP LTM determines the distributed node to be down and therefore disconnects it. Use of the distributed node control function requires no related setting for BIG-IP LTM.

The distributed node status is updated by BIG-IP LTM when the JVM monitor detects a failure or failure recovery. Therefore, after the failover generated by an operation other than JVM monitoring, the distributed node status of BIG-IP LTM may be "enable".



The JVM monitoring calculates the load on the target Java VM according to the information obtained about the Java memory.

Obtain the Java VM load from the following expression. Java VM load (%) is the value obtained by multiplying the

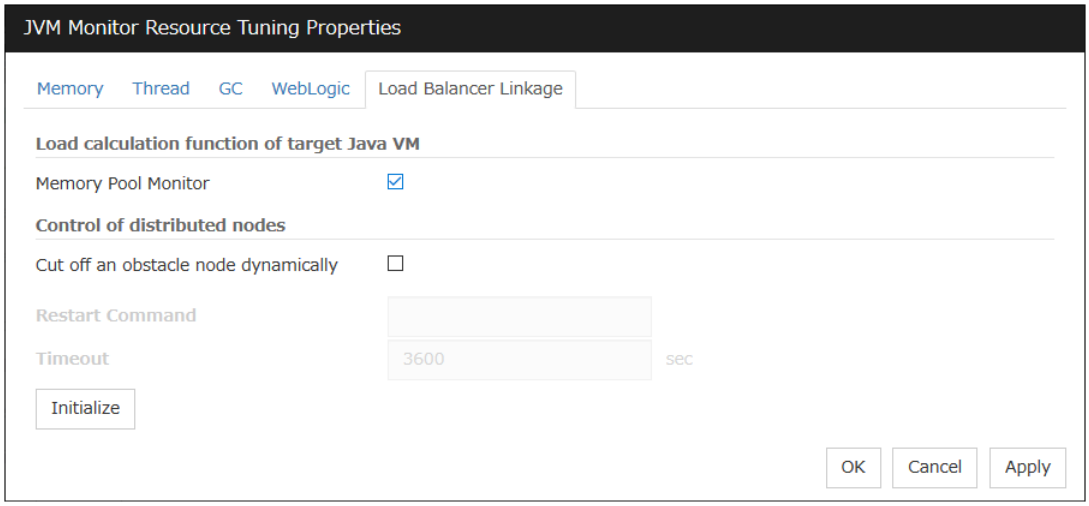
entire amount of the Java heap area by the use ratio set with **Monitor(special)** tab - **Tuning** properties - **Memory** tab - **Monitor Heap Memory Rate** - **Total Usage**.

Java VM load (%) = current memory usage (MB) x 100/threshold (MB)

The linkage module installed on the server on which the JVM monitor runs executes a command at regular intervals, and reports the load collected on the target Java VM to BIG-IP LTM. BIG-IP LTM distributes the traffic (request) to the optimal server according to the load status of Java VM of the distributed node.

Set the following EXPRESSCLUSTER settings with the Cluster WebUI.

- JVM monitor resource



Properties - Monitor(special) tab -> **Tuning properties**- **Load Balancer Linkage** tab
Select the Memory Pool Monitor check box.

- Custom monitor resource
  Properties - Monitor(common) tab
  Select the **Monitor Timing** - **Always** radio button.

  Properties - Monitor(special) tab

  Select **Script created with this product.**

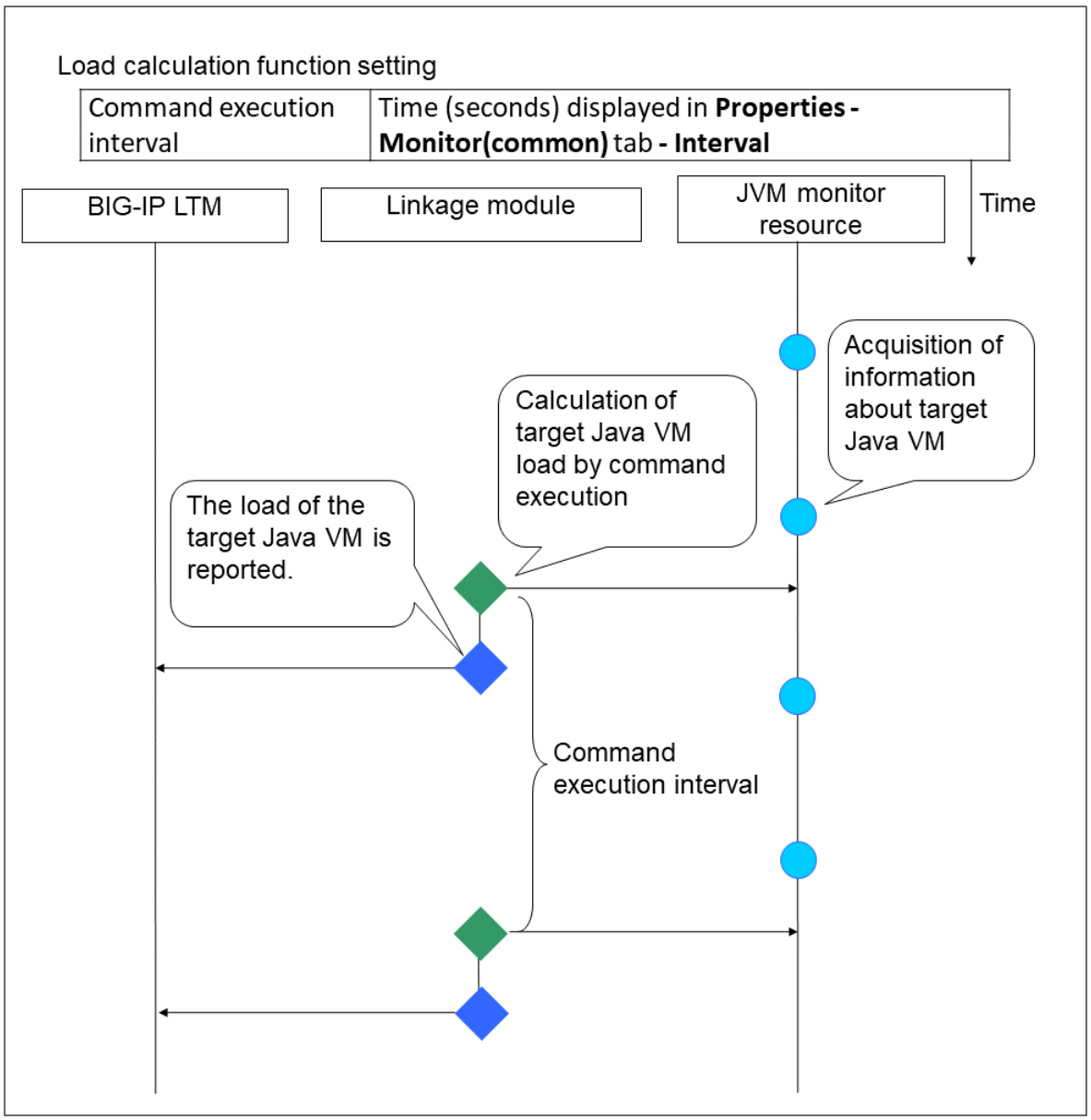
  Select **File** - **Edit** and then add the following **boldfaced** section.

  ```
  #! /bin/sh
  #***************************************************
  #* genw.sh *
  #***************************************************


  ulimit -s unlimited
  ${CLP_PATH}/ha/jra/bin/clpjra_bigip weight
  exit 0
  ```

  Select the **Monitor Type** - **Synchronous** radio button.

In the BIG-IP LTM setting, specify **Ratio(node)** in **LocalTrafic** - **Pools:PoolList** - **Relevant pool** - **Members** - **LoadBalancing** - **Load Balancing Method** of BIG-IP Configuration Utility.



4.42.6 JVM statistics log

JVM monitor resources collect statistics information on the monitor target Java VM. The information is stored in CSV-format files, as JVM statistics logs. The file is created in the following location:

<EXPRESSCLUSTER_install_path>/log/ha/jra/*.stat

The following "monitor items" see the parameters on the [Monitor(special)] tab of [Properties] of the JVM monitor resources.

Statistical information is collected and output to its corresponding JVM statistical log when an item is selected and the threshold value is set for the item. If a monitor item is not selected, statistical information on the item will be neither collected nor output to its corresponding JVM statistical log.

The following table lists the monitor items and the corresponding JVM statistics logs.

Monitor items	Corresponding JVM statistics log
[Memory] tab - [Monitor Heap Memory Rate] [Memory] tab - [Monitor Non-Heap Memory Rate] [Memory] tab-[Monitor Heap Memory Usage] [Memory] tab -[Monitor Non-Heap Memory Usage]	jramemory.stat
[Thread] tab - [Monitor the number of Active Threads]	jrathread.stat
[GC] tab - [Monitor the time in Full GC] [GC] tab - [Monitor the count of Full GC execution]	jragc.stat
[WebLogic] tab - [Monitor the requests in Work Manager] [WebLogic] tab - [Monitor the requests in Thread Pool] When either of the above monitor items is checked, both of the logs, such as wlworkmanager.stat and wlthreadpool.stat, are output. No functions to output only one of the two logs are provided.	wlworkmanager.stat wlthreadpool.stat

4.42.7 Java memory area usage check on monitor target Java VM (jramemory.stat)

The jramemory.stat log file records the size of the Java memory area used by the monitor target Java VM. Its file name will be either of the following, depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: jramemory<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jramemory<*YYYYMMDDhhmm*>.stat

  The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Name of the Java memory pool; for details, refer to "Java memory pool name".
4	Half-size alphanumeric characters and symbols	Type of Java memory pool Heap, Non-Heap

Continued on next page

Table 4.23 – continued from previous page

No	Format	Description
5	Half-size numeric characters	Memory size that the Java VM requests from the OS at startup; this is expressed in bytes. (init) At the startup of the monitor target Java VM, the size can be specified using the following Java VM startup options. • HEAP:-Xms • NON_HEAP permanent area (Perm Gen): -XX:PermSize • NON_HEAP code cache area (Code Cache): -XX:InitialCodeCacheSize
6	Half-size numeric characters	Memory size currently used by the Java VM; this is expressed in bytes. (used)
7	Half-size numeric characters	Memory size guaranteed for use by the operation of the Java VM; this is expressed in bytes. (committed) This size varies depending on the memory use; it is always equal to the value of "used" or larger but equal to or smaller than the value of "max".
8	Half-size numeric characters	Maximum memory size that the Java VM can use; this is expressed in bytes. (max) The size can be specified using the following Java VM startup options. • HEAP:-Xmx • NON_HEAP permanent area (Perm Gen): -XX:MaxPermSize • NON_HEAP code cache area (Code Cache): -XX:ReservedCodeCacheSize Example) java -XX:MaxPermSize=128m -XX:ReservedCodeCacheSize=128m javaAP In this example, max of NON_HEAP becomes 128 m + 128 m = 256 m. (Note) When the same value is specified for -Xms and -Xmx, "init" may become larger than "max". This is because "max" of HEAP is determined by subtracting half the size of the Survivor Space from the area size determined by the specification of -Xmx.
9	Half-size numeric characters	Peak size of the memory used after startup of the measurement target Java VM; when the name of the Java memory pool is HEAP or NON_HEAP, this size becomes equal to that of the memory currently used by the Java VM (used). This is expressed in bytes.

Continued on next page

Table 4.23 – continued from previous page

No	Format	Description
10	Half-size numeric characters	Ignore when Oracle Java (usage monitoring) is selected for [JVM Type]. When an item other than [Oracle Java (usage monitoring)] is selected for JVM Type, memory size equal to "max" (No. 8 field) * the threshold (%) when the Java memory pool type (No. 4 field) is HEAP; it is expressed in bytes. When the Java memory pool type is other than HEAP, it is 0.

4.42.8 Thread operation status check on monitor target Java VM (jrathread.stat)

The jrathread.stat log file records the thread operation status of the monitor target Java VM. Its file name will be either of the following depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: jrathread<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jrathread<*YYYYMMDDhhmm*>.stat

  The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Number of active threads in the monitor target Java VM
4	[Half-size numeric characters: half-size numeric characters:...]	Deadlocked thread ID in the monitor target Java VM; this contains the IDs of all the deadlocked threads, in order.
5	Half-size alphanumeric characters and symbols	Detailed information on deadlocked threads in the monitor target Java VM; it contains information on all the deadlocked threads, in order, in the following format. ThreadName, ThreadID, ThreadStatus, UserTime, CpuTime, WaitedCount, WaitedTime, isInNative, isSuspended <line feed> stacktrace<line feed> : stacktrace<line feed> stacktrace=ClassName, FileName, LineNumber, MethodName, isNativeMethod

4.42.9 GC operation status check on monitor target Java VM (jragc.stat)

The jragc.stat log file records the GC operation status of the monitor target Java VM. Its file name will be either of the following, depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type]-[File Capacity] is selected: jragc<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jragc<*YYYYMMDDhhmm*>.stat

JVM monitor resources output two types of GC information: Copy GC and Full GC.

With Oracle Java, JVM monitor resources count the increment in the count of execution of the following GC as Full GC.

- MarksweepCompact
- MarkSweepCompact
- PS Marksweep
- ConcurrentMarkSweep

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.

Continued on next page

Table 4.25 – continued from previous page

No	Format	Description
3	Half-size alphanumeric characters and symbols	GC name of monitor target Java VM **When the monitor target Java VM is Oracle Java** Copy MarksweepCompact The GC name to be indicated is one of the following. MarkSweepCompact PS Scavenge PS Marksweep ParNew ConcurrentMarkSweep **When the monitor target Java VM is Oracle JRockit** The GC name to be indicated is one of the following. Garbage collection optimized for throughput Old Collector Garbage collection optimized for short pausetimes Old Collector Garbage collection optimized for deterministic pausetimes Old Collector Static Collector Static Old Collector Garbage collection optimized for throughput Young Collector
4	Half-size numeric characters	Count of GC execution during the period from startup of the monitor target Java VM to measurement; the count includes the GC executed before the JVM monitor resource starts monitoring.
5	Half-size numeric characters	Total time in GC execution during the period from startup of the monitor target Java VM to measurement; this is expressed in milliseconds. This includes the time taken for the GC executed before the JVM monitor resource starts monitoring.

4.42.10 Operation status check on Work Manager of WebLogic Server (wlworkmanager.stat)

The wlworkmanager.stat log file records the operation status of the Work Manager of the WebLogic Server. Its file name will be either of the following depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: wlworkmanager<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: wlworkmanager<*YYYYMMDDhhmm*>.stat

  The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Application name
4	Half-size alphanumeric characters and symbols	Work Manager name
5	Half-size numeric characters	Request execution count
6	Half-size numeric characters	Number of wait requests

4.42.11 Operation status check on Thread Pool of WebLogic Server (wlthreadpool.stat)

The wlthreadpool.stat log file records the operation status of the thread pool of the WebLogic Server. Its file name will be either of the following depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: wlthreadpool<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: wlthreadpool<*YYYYMMDDhhmm*>.stat

  The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size numeric characters	Total request execution count
4	Half-size numeric characters	Number of requests queued in the WebLogic Server
5	Half-size numeric characters	Request execution per unit time count (seconds)
6	Half-size numeric characters	Number of threads for executing the application
7	Half-size numeric characters	Number of threads in idle state
8	Half-size numeric characters	Number of executing threads
9	Half-size numeric characters	The number of threads in stand-by state

4.42.12 Java memory pool name

This section describes the Java memory pool name output as memory_name in messages to the JVM operation log file. It also describes the Java memory pool name output to the JVM statistics log file, jramemory.stat log file.

The character strings of the Java memory pool names are not determined by the JVM monitor resources. Character strings received from the monitor target Java VM are output as Java memory pool names.

Their specifications are not open for Java VM, and accordingly, are subject to change without notice with any version upgrade of Java VM.

Therefore, we do not recommend monitoring Java memory pool names contained in messages.

The following monitor items see the parameters on the [Memory] tab of the [Monitor(special)] tab in [Properties] of the JVM monitor resources.

The following Java memory pool names have been confirmed on actual machines running Oracle Java and JRockit.

When **Oracle Java** is selected for **JVM Type**, and "-XX:+UseSerialGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When **Oracle Java** is selected for **JVM Type**, and "-XX:+UseParallelGC" and "-XX:+UseParallelOldGC" are specified as the startup options for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	PS Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	PS Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	PS Old Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	PS Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When **Oracle Java** is selected for **JVM Type**, and "-XX:+UseConcMarkSweepGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	Par Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	Par Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	CMS Old Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	CMS Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]

Continued on next page

Table 4.30 – continued from previous page

Monitor item	Character string output as memory_name
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseSerialGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseParallelGC" and "-XX:+UseParallelOldGC" are specified as startup options for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	PS Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	PS Survivor Space
[Monitor Heap Memory Usage]- [Tenured Gen]	PS Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseConcMarkSweepGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Par Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Par Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	CMS Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseParNewGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows. For Java 9, if -XX:+UseParNewGC is specified, the monitor target Java VM does not start.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Par Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Par Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX::+UseG1GC" is specified as a startup option for the monitor target Java VM the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	G1 Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	G1 Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen (Old Gen)]	G1 Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace

Continued on next page

Table 4.35 – continued from previous page

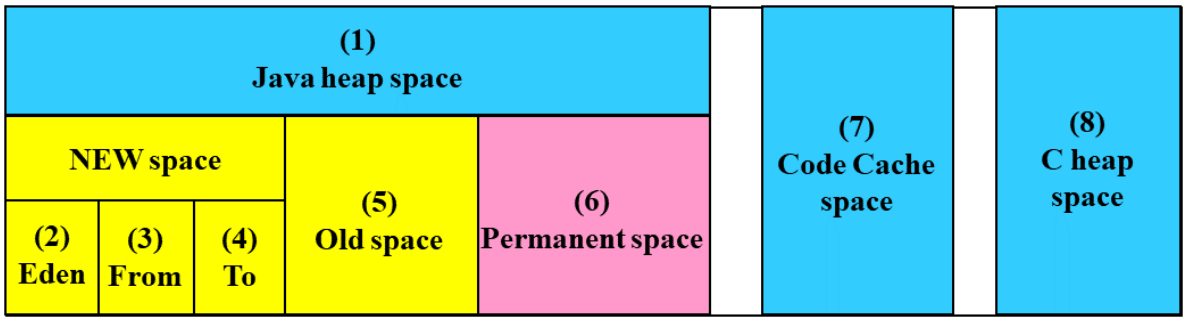
Monitor item	Character string output as memory_name
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When the monitor target Java VM is Oracle JRockit (when [JRockit] is selected for [JVM Type]), the No. 3 Java memory pool name in the jramemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP memory
[Monitor Heap Memory Rate] - [Nursery Space]	Nursery
[Monitor Heap Memory Rate] - [Old Space]	Old Space
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Class Memory]	Class Memory

Java memory pool names appearing in the jramemory.stat log file, a JVM statistics log file, correspond to the Java VM memory space as follows.

- For Oracle Java 7



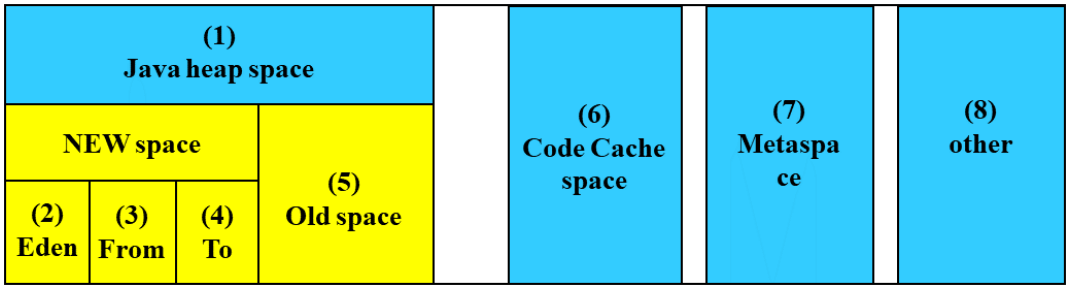
No. in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(1)	[Monitor Heap Memory Rate] - [Total Usage]	HEAP
(2)	[Monitor Heap Memory Rate] - [Eden Space]	EdenSpace PS Eden Space Par Eden Space
(3)+(4)	[Monitor Heap Memory Rate] - [Survivor Space]	Survivor Space PS Survivor Space Par Survivor Space

Continued on next page

Table 4.37 – continued from previous page

No. in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(5)	[Monitor Heap Memory Rate] - [Tenured Gen]	Tenured Gen PS Old Gen CMS Old Gen
(6)	[Monitor Non-Heap Memory Rate] - [Perm Gen] [Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]] [Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen Perm Gen [shared-ro] Perm Gen [shared-rw] PS Perm Gen CMS Perm Gen
(7)	[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
(8)	-	-
(6)+(7)	[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP * No stack trace is included.

- For Oracle Java 8/Oracle Java 9



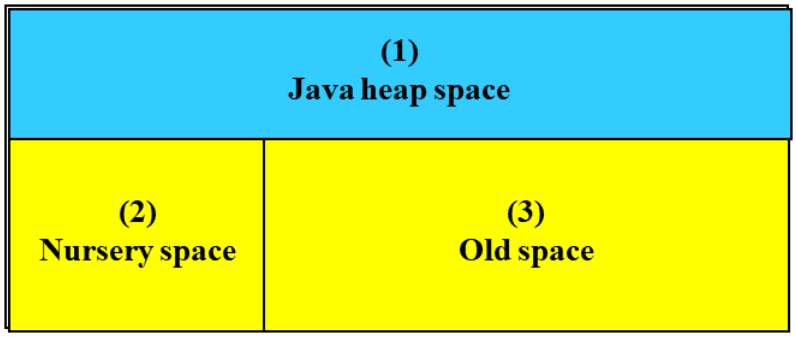
Number in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(1)	[Monitor Heap Memory Usage] - [Total Usage]	HEAP
(2)	[Monitor Heap Memory Usage] - [Eden Space]	EdenSpace PS Eden Space Par Eden Space G1 Eden Space

Continued on next page

Table 4.38 – continued from previous page

Number in diagram	Monitor item	Java memory pool name in jrammemory.stat log file
(3)+(4)	[Monitor Heap Memory Usage] - [Survivor Space]	Survivor Space PS Survivor Space Par Survivor Space G1 Survivor Space
(5)	[Monitor Heap Memory Usage] - [Tenured Gen]	Tenured Gen PS Old Gen CMS Old Gen G1 Old Gen
(6)	[Monitor Non-Heap Memory Usage] - [Code Cache]	Code Cache
(6)	[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods (Only for Java 9, it is output.)
(6)	[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods (Only for Java 9, it is output.)
(6)	[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods (Only for Java 9, it is output.)
(7)	[Monitor Non-Heap Memory Usage] - [Metaspace]	Metaspace
(8)	[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space
(6)+(7)+(8)	[Monitor Non-Heap Memory Usage] - [Total Usage]	NON_HEAP

- For Oracle JRockit



No. in diagram	Monitor item	Java memory pool name in jrammemory.stat log file
(1)	[Monitor Heap Memory Rate] - [Total Usage]	HEAP memory

Continued on next page

Table 4.39 – continued from previous page

No. in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(2)	[Monitor Heap Memory Rate] - [Nursery Space]	Nursery
(3) (Note)	[Monitor Heap Memory Rate] - [Old Space]	Old Space
-	[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
-	[Monitor Non-Heap Memory Rate] - [Class Memory]	Class Memory

Note: "Old Space", a Java memory pool name in the jramemory.stat log file, does not indicate the value corresponding to the old space of the Heap but rather the value corresponding to the entire "Heap memory". Independent measurement of only (3) is not possible.

4.42.13 Executing a command corresponding to cause of each detected error

EXPRESSCLUSTER does not provide a means for executing specific commands based on the causes of detected monitor resource errors.

JVM monitor resources can execute specific commands according to error causes. If an error is detected, JVM monitor resources will execute an appropriate command.

The following setting items specify the commands that will be executed according to the error cause.

Error cause	Setting item
- Failure in connection to the monitor target Java VM - Failure in resource measurement	[Monitor(special)] tab - [Command]
- Heap memory rate - Non-heap memory rate - Heap memory usage - Non-heap memory usage	[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]
- Number of active threads	[Monitor(special)] tab - [Tuning] properties - [Thread] tab - [Command]
- Time in Full GC - Count of Full GC execution	[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]
- Requests in Work Manager of WebLogic - Requests in Thread Pool of WebLogic	[Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Command]

[Command] passes the details of an error cause as the arguments of a command with the arguments attached to the

end of [Command]. A Command that is specialized for dealing with specific error causes can be defined by designing and specifying a script etc. for [Command]. The following character strings are passed as the arguments.

When multiple character strings are stated as possible arguments, one will be passed according to the GC type of the monitor target Java VM. For details about their differences, see "Java memory pool name".

The statements "(For Oracle Java)" and "(For Oracle JRockit)" suggest that different character strings are used according to the JVM type. When there is no such statement, the same character strings are used equally for all JVM types.

Details of error causes	Character string passed as argument
- Failure in connection to the monitor target Java VM - Failure in resource measurement	No character string defined
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Monitor Memory Heap Rate] - [Total Usage] (For Oracle Java)	HEAP
[Memory] tab - [Monitor Memory Heap Rate] - [Eden Space] (For Oracle Java)	EdenSpace PSEdenSpace ParEdenSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Survivor Space] (For Oracle Java)	SurvivorSpace PSSurvivorSpace ParSurvivorSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Tenured Gen] (For Oracle Java)	TenuredGen PSOldGen CMSOldGen
[Memory] tab - [Monitor Non-Heap Memory Rate] - [Total Usage] (For Oracle Java)	NON_HEAP
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Code Cache] (For Oracle Java)	CodeCache
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Perm Gen] (For Oracle Java)	PermGen PSPermGen CMSPermGen

Continued on next page

Table 4.41 – continued from previous page

Details of error causes	Character string passed as argument
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Perm Gen[shared-ro]] (For Oracle Java)	PermGen[shared-ro]
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Perm Gen[shared-rw]] (For Oracle Java)	PermGen[shared-rw]
[Memory] tab - [Monitor Heap Memory Usage] - [Total Usage] (for Oracle Java(usage monitoring))	HEAP
[Memory] tab - [Monitor Heap Memory Usage] - [Eden Space] (for Oracle Java(usage monitoring))	EdenSpace PSEdenSpace ParEdenSpace G1EdenSpace
[Memory] tab - [Monitor Heap Memory Usage]-[Survivor Space] (for Oracle Java(usage monitoring))	SurvivorSpace PSSurvivorSpace ParSurvivorSpace G1SurvivorSpace
[Memory] tab - [Monitor Heap Memory Usage] - [Tenured Gen] (for Oracle Java(usage monitoring))	TenuredGen PSOldGen CMSOldGen G1OldGen
[Memory] tab - [Monitor Non-Heap Memory Usage] - [Total Usage] (for Oracle Java(usage monitoring))	NON_HEAP
[Memory] tab - [Monitor Non-Heap Memory Usage] - [Code Cache] (for Oracle Java(usage monitoring))	CodeCache
[Memory] tab - [Monitor Non-Heap Memory Usage] - [Metaspace] (for Oracle Java(usage monitoring))	Metaspace
[Memory] tab - [Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods] (when Oracle Java (usage monitoring) is selected)	non-nmethods
[Memory] tab - [Monitor Non-Heap Memory Usage]-[CodeHeap profiled] (when Oracle Java (usage monitoring) is selected)	profilednmethods
[Memory] tab - [Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled] (when Oracle Java (usage monitoring) is selected)	non-profilednmethods
[Memory] tab - [Monitor Non-Heap Memory Usage]-[Compressed Class Space] (when Oracle Java (usage monitoring) is selected)	CompressedClassSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Total Usage] (For Oracle JRockit)	HEAP Heap

Continued on next page

Table 4.41 – continued from previous page

Details of error causes	Character string passed as argument
[Memory] tab - [Monitor Memory Heap Rate] - [Nursery Space] (For Oracle JRockit)	Nursery
[Memory] tab - [Monitor Memory Heap Rate] - [Old Space] (For Oracle JRockit)	OldSpace
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Total Usage] (For Oracle JRockit)	NON_HEAP
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Class Memory] (For Oracle JRockit)	ClassMemory
[Thread] tab - [Monitor the number of Active Threads]	Count
[GC] tab - [Monitor the time in Full GC]	Time
[GC] tab - [Monitor the count of Full GC execution]	Count
[WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, The number]	WorkManager_PendingRequests
[WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, The number]	ThreadPool_PendingUserRequestCount
[WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, The number]	ThreadPool_Throughput

The following are examples of execution.

Example 1)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	/usr/local/bin/downcmd
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the count of Full GC execution]	1
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If Full GC is executed as many times, in succession, as specified by the Error Threshold (three times), the JVM monitor resources will detect a monitor error and execute a command corresponding to "/usr/local/bin/downcmd Cont".

Example 2)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	"/usr/local/bin/downcmd" GC
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the time in Full GC]	65536

Continued on next page

Table 4.43 – continued from previous page

Setting item	Setting information
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the time in Full GC exceeds 65535 milliseconds as many times, in succession, as specified by the Error Threshold (three times), the JVM monitor resources will detect a monitor error and execute a command corresponding to "/usr/local/bin/downcmd GC Time".

Example 3)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]	"/usr/local/bin/downcmd" memory
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Monitor Heap Memory Rate]	On
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Eden Space]	80
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Survivor Space]	80
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the usage rate of the Java Eden Space and that of the Java Survivor Space exceed 80% as many times, in succession, as specified by the Error Threshold (three times), the JVM monitor resources will detect a monitor error and execute a command corresponding to "/usr/local/bin/downcmd memory EdenSpace SurvivorSpace".

Timeout (seconds) for waiting for the completion of execution of the command specified by [Command] is set by specifying [Command Timeout] in the [JVM monitor] tab of the Cluster Properties window. The same value is applied to the timeout of [Command] of each of the above-mentioned tabs; the timeout cannot be specified for each [Command] separately.

If a timeout occurs, the system will not perform processing for forced termination of the [Command] process; the operator must perform post-processing (e.g. forced termination) of the [Command] process. When a timeout occurs, the following message is output to the JVM operation log:

> action thread execution did not finish. action is alive = <*command*>.

Note the following.

1. No [Command] is executed when restoration of the Java VM to normal operation (error -> normal operation) is detected.
2. [Command] is executed upon the detection of an error in the Java VM (when threshold exceeding occurs as many times, in succession, as specified by the error threshold). It is not executed at each threshold exceeding.
3. Note that specifying [Command] on multiple tabs allows multiple commands to be executed if multiple errors occur simultaneously, causing a large system load.
4. [Command] may be executed twice simultaneously when the following two items are monitored: [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, The Number]; [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, Average].

   This is because errors may be detected simultaneously for the following two items: [Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [WebLogic] tab - [Interval, The number of request]; [Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [WebLogic] tab - [Interval, The average number of the request]. To prevent this from occurring, specify only one of the two items as a monitor target. This applies to the following combinations of monitor items.

- [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, The Number] and [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, Average]
- [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, The Number] and [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, Average]

4.42.14 Monitoring WebLogic Server

For how to start the operation of the configured target WebLogic Server as an application server, see the manual for WebLogic Server.

This section describes only the settings required for monitoring by the JVM monitor resource.

1. Start WebLogic Server Administration Console.
   For how to start WebLogic Server Administration Console, refer to " Overview of Administration Console" in the WebLogic Server manual.
   Select **Domain Configuration-Domain-Configuration-General**. Make sure that **Enable Management Port is unchecked.**
2. Select **Domain Configuration-Server**, and then select the name of the server to be monitored. Set the selected server name as the identifier on the **Monitor(special)** tab from **Properties** that can be selected in the the config mode of Cluster WebUI. See "*Understanding JVM monitor resources*".
3. Regarding the target server, select **Configuration-General**, and then check the port number though which a management connection is established with **Listen Port**.
4. Stop WebLogic Server. For how to stop WebLogic Server, refer to "Starting and stopping WebLogic Server" in the WebLogic Server manual.
5. Start the management server start script of WebLogic Server (startWebLogic.sh).
6. Write the following instructions in the script.
   - When the target is the WebLogic Server managing server:

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.
↪WLSMBeanServerBuilder"
```

   *Write each line of coding on one line.

   - When the target is a WebLogic Server managed server:

```
if [ "${SERVER_NAME}" = "SERVER_NAME" ]; then
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.
↪WLSMBeanServerBuilder"
```

   *Write all the if statement lines (lines 2 to 5) on one line.

Note: For **n**, specify the number of the port used for monitoring. The specified port number **must be different from that of the listen port for the target Java VM.** If there are other target WebLogic Server entities on the same machine, specify a port number different from those for the listening port and application ports of the other entities.

Note: For **SERVER_NAME**, specify the name of the target server confirmed by **Select Target Server**. If more than one server is targeted, change the server name on the settings (line 1 to 6) for each server.

Note: Place the above addition prior to the following coding:

${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
-Dweblogic.Name=${SERVER_NAME} -Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
${PROXY_SETTINGS} ${SERVER_CLASS}

* Write the above coding on one line.

* The above java arguments differ depending on the WebLogic version. There is no problem by specifying JAVA_OPTIONS before using java.

Note: For monitoring **Perm Gen[shared-ro]** or **Perm Gen[shared-rw]** on the **Memory** tab, add the following line:

-client -Xshare:on -XX:+UseSerialGC

7. If monitoring requests of work manager and thread pool, make the following settings.

   Start WLST (wlst.sh) of the target WebLogic Server. On the console window displayed, execute the following commands:

```
>connect('USERNAME','PASSWORD','t3://SERVER_ADDRESS:SERVER_PORT')
> edit()
> startEdit()
> cd('JMX/DOMAIN_NAME')
> set('PlatformMBeanServerUsed','true')
> activate()
> exit()
```

   Replace the **USERNAME**, **PASSWORD**, **SERVER_ADDRESS**, **SERVER_PORT**, and **DOMAIN_NAME** above with those for the domain environment.

8. Restart the target WebLogic Server.

4.42.15 Monitoring WebOTX

This guide describes how to configure a target WebOTX to enable monitoring by the JVM monitor resource.

Start the WebOTX Administration Console. For how to start the WebOTX Administration Console, refer to "Starting and stopping administration tool" in the *WebOTX Operation (Web Administration Tool)*.

The settings differ depending on whether a Java process of the JMX agent running on WebOTX or the Java process of a process group is to be monitored. Configure the settings according to the target of monitoring.

4.42.16 Monitoring a Java process of the WebOTX domain agent

There is no need to specify any settings.

4.42.17 Monitoring a Java process of a WebOTX process group

1. Connect to the domain by using the administration tool.
2. In the tree view, select **<domain_name>-TP System-Application Group-<application_group_name>-Process Group-<process_group_name>**.
3. For the **Other Arguments** attributes on the **JVM Options** tab on the right, specify the following Java options on one line. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Cluster WebUI (**JVM Monitor Resource Name -> Properties -> Monitor(special)** tab **-> Connection Port**).

   ```
   -Dcom.sun.management.jmxremote.port=n
   -Dcom.sun.management.jmxremote.ssl=false
   -Dcom.sun.management.jmxremote.authenticate=false
   -Djavax.management.builder.initial=com.nec.webotx.jmx.mbeanserver.
   ↪JmxMBeanServerBuilder
   ```

   * In the case of WebOTX V9.2 or later, it is unnecessary to specify -Djavax.management.builder.initial.

4. Then, click **Update**. After the configuration is completed, restart the process group.

   These settings can be made by using **Java System Properties,** accessible from the **Java System Properties** tab of the WebOTX administration tool. When making these settings by using the tool, do not designate -D and set the strings prior to = in name and set the strings subsequent to = in value.

Note: If restart upon a process failure is configured as a function of the WebOTX process group, and when the process group is restarted as the recovery processing by EXPRESSCLUSTER, the WebOTX process group may fail to function correctly. For this reason, when monitoring the WebOTX process group, make the following settings for the JVM monitor resource by using the Cluster WebUI.

Tab name for setting	Item name	Setting value
Monitor(common)	Monitor Timing	Always
Recovery Action	Recovery Action	Execute only the final action
Recovery Action	Final Action	No operation

Linking with the load balancer is not supported for WebOTX process group monitoring.

4.42.18 Receiving WebOTX notifications

By registering a specific listener class, notification is issued when WebOTX detects a failure. The JVM monitor resource receives the notification and outputs the following message to the JVM operation log.

%1$s:Notification received. %2$s.

%1$s and %2$s each indicates the following:

%1$s: Monitored Java VM

%2$s: Message in the notification (ObjectName=**,type=**,message=**)

At present, the following is the detailed information on MBean on the monitorable resource.

ObjectName	[domainname]:j2eeType=J2EEDomain,name=[domainname],category=runtime
notification type	nec.webotx.monitor.alivecheck.not-alive
Message	failed

4.42.19 Monitoring JBoss

The settings are different for monitoring standalone mode and for domain mode. Configure the settings according to the target of monitoring.

This section describes how to configure a target JBoss to be monitored by the JVM monitor resource.

Standalone mode

1. Stop JBoss, and then open (*JBoss_installation_path*)/bin/standalone.conf by using editor software.
2. In the configuration file, specify the following settings. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Cluster WebUI (JVM Monitor Resource Name -> Properties -> Monitor(special) tab -> Connection Port).

   Add the following before "if ["x$JBOSS_MODULES_SYSTEM_PKGS" = "x"]; then".

   ```
   JBOSS_MODULES_SYSTEM_PKGS="org.jboss.logmanager"
   ```

   Add the following after "if ["x$JAVA_OPTS" = "x"]; then ... fi:".

   ```
   JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/org/jboss/logmanager/
   ↪main/jboss-logmanager-1.3.2.Final-redhat-1.jar"
   JAVA_OPTS="$JAVA_OPTS -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
   JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=n -Dcom.sun.management.
   ↪jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"
   ```

   * The storage directory and file name of jboss-logmanager-*.jar differ depending on the JBoss version. Therefore, specify the path accoding to the installation environment.
3. Save the settings, and then start JBoss.
4. With Cluster WebUI (**JVM Monitor Resource Name** -> **Properties** -> **Monitor(special)**tab -> **Identifier**), specify a unique string that is different from those for the other monitor targets (e.g. JBoss).

Domain mode

With Cluster WebUI (**JVM Monitor Resource Name** -> **Properties** -> **Monitor(special)** tab -> **Identifier**), specify a unique string that is different from those for the other monitor targets (e.g. JBoss). With Cluster WebUI (**JVM Monitor Resource Name** -> **Properties** -> **Monitor(special)** tab -> **Process Name**), specify all the Java VM startup options so that JBoss can be uniquely identified.

4.42.20 Monitoring Tomcat

This section describes how to configure a target Tomcat to be monitored by the JVM monitor resource.

1. If Tomcat is installed from an rpm package, stop Tomcat and open /etc/sysconfig/tomcat6 or /etc/sysconfig/tomcat. If Tomcat is not installed from an rpm package, stop Tomcat and create (*Tomcat installation path*)/bin/setenv.sh.
2. In the configuration file, for the Java options, specify the following settings on one line. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Cluster WebUI **(JVM Monitor Resource Name -> Properties -> Monitor(special)** tab **-> Connection Port**).

```
CATALINA_OPTS="${CATALINA_OPTS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false"
```

3. Save the settings, and then start Tomcat.
4. With Cluster WebUI (**JVM Monitor Resource Name -> Properties -> Monitor(special)** tab **-> Identifier**), specify a unique string that is different from those for the other monitor targets (e.g., tomcat).

4.42.21 Monitoring SVF

This section describes how to configure a target SVF to be monitored by the JVM monitor resource.

If the monitor target is Tomcat:

Change the environment variables of the SVF user in the OS as follows. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Cluster WebUI (**JVM Monitor Resource Name -> Properties -> Monitor(special)** tab **-> Connection Port**).

```
JAVA_OPTS="-Xms512m -Xmx512m -Dcom.sun.management.jmxremote.port=n -Dcom.sun.
↪management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false"
export JAVA_OPTS
```

If the monitor target is other than Tomcat:

1. Select a monitor target from the following, and then use an editor to open the corresponding script.

Monitor target	Script to be edited
Simple Httpd Service (for 8.x)	<SVF installation path>/bin/SimpleHttpd
Simple Httpd Service (for 9.x)	<SVF installation path>/bin/UCXServer
RDE Service	<SVF installation path>/rdjava/rdserver/rd_server_startup.sh
	<SVF installation path>/rdjava/rdserver/svf_server_startup.sh
RD Spool Balancer	<SVF installation path>/rdjava/rdbalancer/rd_balancer_startup.sh
SVF Print Spooler Service	<SVF installation path>/bin/spooler

2. In the configuration file, for the Java options, specify the following settings on one line. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Cluster WebUI **(JVM Monitor Resource Name -> Properties -> Monitor(special)** tab **-> Connection Port**).

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
```

3. If the monitor target is RDE Service, add ${JAVA_OPTIONS} into the following startup path and rd_balancer_startup.sh

```
java -Xmx256m -Xms256m -Djava.awt.headless=true ${JAVA_OPTIONS}
-classpath $CLASSPATH jp.co.fit.vfreport.RdSpoolPlayerServer &
```

4.42.22 Monitoring a Java application that you created

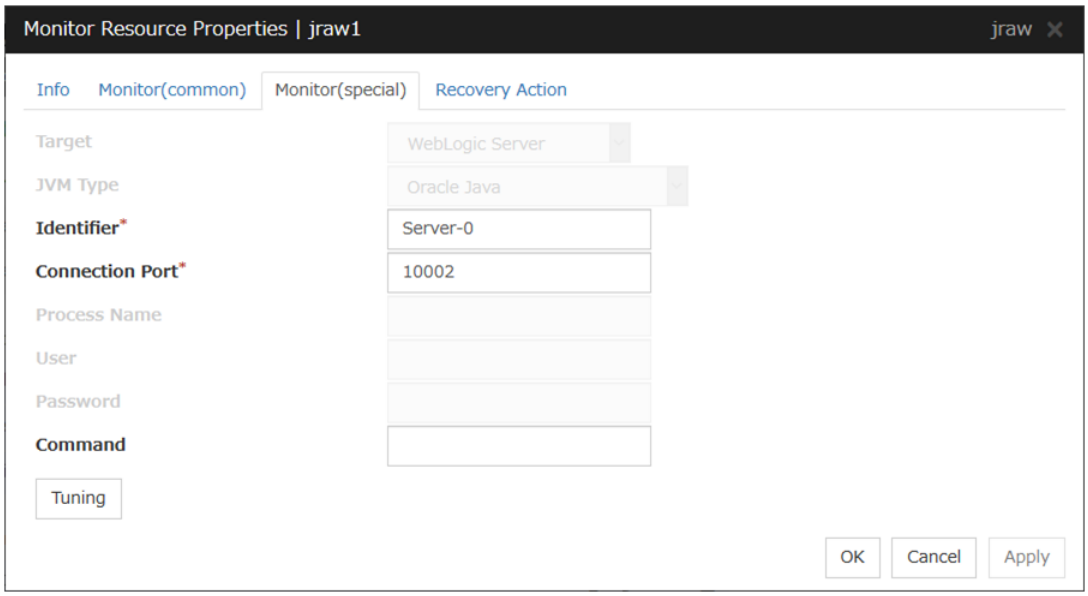
This section describes the procedure to configure Java application which is monitored by JVM monitor resource. Specify the following Java option in one row to the option for Java application startup while Java application (the monitor target) is stopped. For n, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Cluster WebUI (**Monitor Resource Properties** - **Monitor(special)** tab - **Connection Port**).

```
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
```

Some Java applications require the following to be additionally specified.

```
- Djavax.management.builder.initial=<Class name of MBeanServerBuilder>
```

4.42.23 Monitor (special) tab



Target

Select the target to be monitored from the list. When monitoring WebSAM SVF for PDF, WebSAM Report Director Enterprise, or WebSAM Universal Connect/X, select **WebSAM SVF**. When monitoring

a Java application that you created, select **Java Application**.

Select [JBoss] when monitoring standalone mode of JBoss Enterprise Application Platform. Select "JBoss Domain Mode" when monitoring the domain mode of JBoss Enterprise Application Platform.

Default: None

JVM Type

Select the Java VM on which the target application to be monitored is running.

For Java 8 (or later) and OpenJDK 8 (or later) or later, select **Oracle Java(usage monitoring)**. For Java 8, the following specification changes have been made.

- It has become impossible to acquire the maximum value of each memory in a non-heap area.
- Perm Gen has been changed to Metaspace.
- Compressed Class Space was added.

For Java 8, therefore, the monitor items on the **Memory** tab have been changed as below.

- Monitoring for the use rate has been changed to monitoring for the amount used.
- **Perm Gen**, **Perm Gen[shared-ro]**, and **Perm Gen[shared-rw]** cannot be monitored. Clear the check box.
- **Metaspace** and **Compressed Class Space** can be monitored.

For Java 9, the following specification changes have been made.

- **Code Cache** has been divided.

For Java9, therefore, the monitor items on the **Memory** tab have been changed as below.

- **Code Cache** cannot be monitored. Clear the check box.
- **CodeHeap non-nmethods**, **CodeHeap profiled**, and **CodeHeap non-profiled** can be monitored.

For each monitor target, the following are selectable.

- When the target is **WebLogic Server**
  Oracle Java, **Oracle Java(usage monitoring)**, and **Oracle JRockit** are selectable
- When the target is **Tomcat**
  Oracle Java, Oracle Java(usage monitoring), and **OpenJDK** are selectable.
- When the target is other than **WebLogic Server and Tomcat**
  Oracle Java and **Oracle Java(usage monitoring)** are selectable.

Default: None

Identifier (within 255 bytes)

The identifier is set to differentiate the relevant JVM monitor resource from another JVM monitor resource when the information on the application to be monitored is output to the JVM operation log of the relevant JVM monitor resource. For this purpose, set a unique character string between JVM monitor resources. You must specify the identifier.

- When the target is **WebLogic Server**
  Set the name of the server instance to be monitored, according to "*Monitoring WebLogic Server*", item 2.
- When the target is **WebOTX Process Group**
  Specify the name of the process group.
- When the target is **WebOTX Domain Agent**

Specify the name of the domain.

- When the target is **JBoss or JBoss Domain Mode**
  Specify this according to "*Monitoring JBoss*".
- When the target is **Tomcat**
  Specify this according to "Monitoring Tomcat".
- When the target is **WebOTX ESB**
  Same as for **WebOTX Process Group**.
- When the target is **WebSAM SVF**
  Specify this according to "*Monitoring SVF*".
- When the target is **Java Application**
  Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

Connection Port (1024 to 65535)

Set the port number used by the JVM monitor resource when it establishes a JMX connection to the target Java VM. The JVM monitor resource obtains information by establishing a JMX connection to the target Java VM. Therefore, to register the JVM monitor resource, it is necessary to specify the setting by which the JMX connection port is opened for the target Java VM. You must specify the connection port. This is common to all the servers in the cluster. A value between 42424 and 61000 is not recommended.

- When the target is **WebLogic Server**
  Set the connection port number according to "*Monitoring WebLogic Server*", item 6.
- When the target is **WebOTX Process Group**
  Specify this according to "*Monitoring a Java process of a WebOTX process group*".
- When the target is **WebOTX Domain Agent**
  Specify "domain.admin.port" of "(WebOTX_installation_path)/<*domain_name*>.properties".
- When the target is **JBoss**
  Specify as described in "*Monitoring JBoss*".
- When the target is **JBoss Domain Mode**
  The connection port number need not be specified.
- When the target is **Tomcat**
  Specify as described in "Monitoring Tomcat".
- When the target is **WebOTX ESB**
  Same as for **WebOTX Process Group**.
- When the target is **WebSAM SVF**
  Specify this according to "*Monitoring SVF*".
- When the target is **Java Application**
  Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

Process Name (within 1024 bytes)

Set a **Process Name to identify** the target JVM monitor resource when JVM monitor resource is connecting the target Java VM via JMX. Therefore, be sure to specify a character string that is unique among JVM monitor resources.

- When the target is other than **JBoss Domain Mode**
  This does not need to be configured because the monitor target Java VM can be identified by **Conncetion Port Number**. The internal version 3.3.5-1 or earlier required the process name to be specified since this parameter was used for the identification when the data of virtual memory usage amount was obtained or when the data of the monitor target was output to the JVM operation log. However, in and after the internal version 4.0.0-1, **Monitor Virtual Memory Usage** was deleted. Therefore, it cannot be specified.
- When the target is **JBoss domain mode**
  Specify this according to "*Monitoring JBoss*".

Default: None

User (within 255 bytes)

Specify the name of the administrator who will be making a connection with the target Java VM.

- When **WebOTX Domain Agent** is selected as the target
  Specify the "domain.admin.user" value of "/opt/WebOTX/<*domain_name*>.properties".
- When the target is other than **WebOTX Domain Agent**
  This cannot be specified.

Default: None

Password (within 255 bytes)

Specify the password for the administrator who will be making a connection with the target Java VM.

- When **WebOTX Domain Agent** is selected as the target
  Specify the "domain.admin.passwd" value of "/opt/WebOTX/<*domain_name*>.properties".
- When the target is other than **WebOTX Domain Agent**
  This cannot be specified.

Default: None

Command (within 255 bytes)

Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2

Specify the commands that will be executed if connection to the monitor target Java VM cannot be established or if an error is detected in the process for acquiring the amount of resource usage on the Java VM.

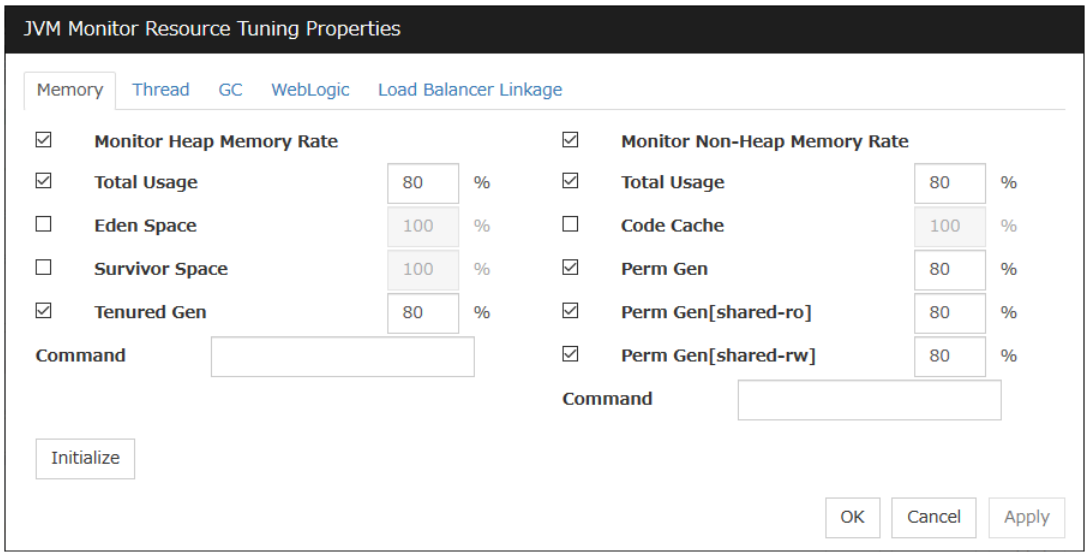
See "*Executing a command corresponding to cause of each detected error*".

Default: None

When you click **Tuning**, the following information is displayed in the pop-up dialog box. Make detailed settings according to the descriptions below.

4.42.24 Memory tab (when Oracle Java or OpenJDK is selected for JVM Type)

Monitor Heap Memory Rate



Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- When the check box is selected (default):
  Monitoring enabled
- When the check box is not selected:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java heap areas used by the target Java VM.

Default: 80[%]

Eden Space (1 to 100)

Specify the threshold for the usage rate of the Java Eden Space used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Eden Space.

Default: 100[%]

Survivor Space (1 to 100)

Specify the threshold for the usage rate of the Java Survivor Space used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Survivor Space.

Default: 100[%]

Tenured Gen (1 to 100)

Specify the threshold for the usage rate of the Java Tenured(Old) Gen area used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Old Gen.

Default: 80[%]

Monitor Non-Heap Memory Rate

Enables the monitoring of the usage rates of the Java non-heap areas used by the target Java VM.

- When the check box is selected (default):

Monitoring enabled

- When the check box is not selected:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java non-heap areas used by the target Java VM.

Default: 80[%]

Code Cache (1 to 100)

Specify the threshold for the usage rate of the Java Code Cache area used by the target Java VM.

Default: 100[%]

Perm Gen (1 to 100)

Specify the threshold for the usage rate of the Java Perm Gen area used by the target Java VM.

Default: 80[%]

Perm Gen[shared-ro] (1 to 100)

Specify the threshold for the usage rate of the Java Perm Gen [shared-ro] area used by the target Java VM.

The **Java Perm Gen [shared-ro]** area is used when -client -Xshare:on -XX:+UseSerialGC is specified as the startup option of the target Java VM.

Default: 80[%]

Perm Gen[shared-rw] (1 to 100)

Specify the threshold for the usage rate of the Java Perm Gen [shared-rw] area used by the target Java VM.

The **Java Perm Gen [shared-rw]** area is used when -client -Xshare:on -XX:+UseSerialGC is specified as the startup option of the target Java VM.

Default: 80[%]

Command (within 255 bytes)

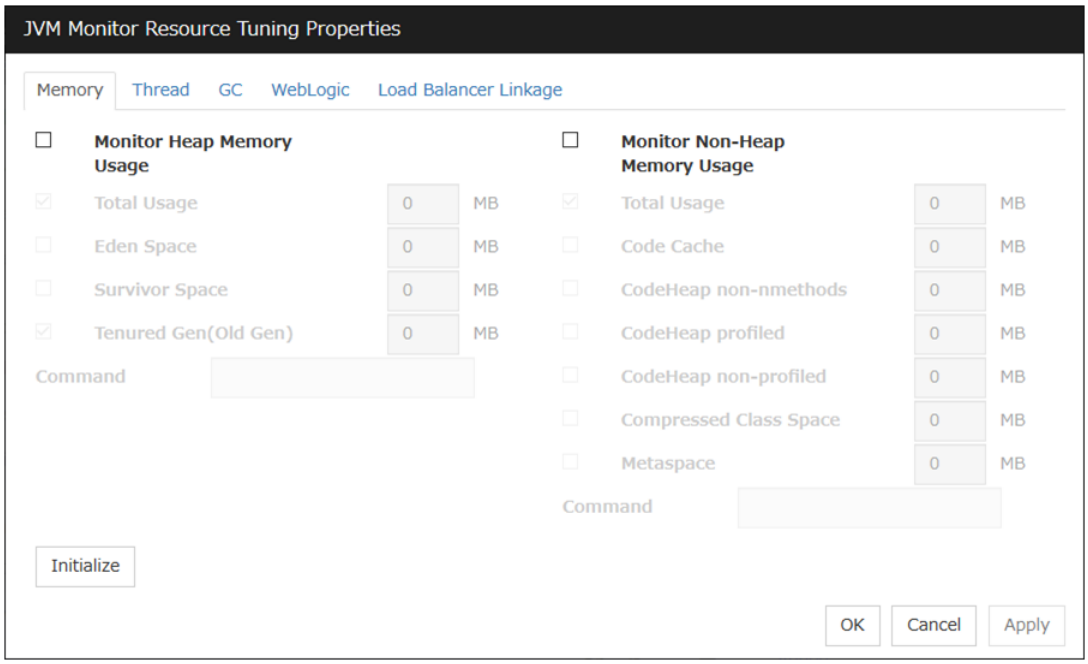
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2
Specify the commands that will be executed if errors are detected in the process for checking the amount of the usage of the Java heap area, Java non-heap area in the monitor target Java VM.
See "*Executing a command corresponding to cause of each detected error*".

Default: None

Initialize

Click **Initialize** to set all the items to their default values.

4.42.25 Memory tab (when Oracle Java(usage monitoring) is selected for JVM Type)



Monitor Heap Memory Usage

Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- When the check box is selected:
  Monitoring is enabled.
- When the check box not selected (default):
  Monitoring is disabled.

Total Usage (0 to 102400)

Specify the threshold for the usage rates of the Java heap areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Eden Space (0 to 102400)

Specify the threshold for the usage rate of the Java Eden Space used by the target Java VM. If zero is specified, this item is not monitored. If G1 GC is specified as the GC method, read it as G1 Eden Space.

Default: 0[MB]

Survivor Space (0 to 102400)

Specify the threshold for the usage rate of the Java Survivor Space used by the target Java VM. If zero is specified, this item is not monitored. If G1 GC is specified as the GC method, read it as G1 Survivor Space.

Default: 0[MB]

Tenured Gen (0 to 102400)

Specify the threshold for the usage rate of the Java Tenured(Old) Gen area used by the target Java VM. If zero is specified, this item is not monitored. If G1 GC is specified as the GC method, read it as G1 Old Gen.

Default: 0[MB]

Monitor Non-Heap Memory Usage

Enables the monitoring of the usage rate of the Java non-heap areas used by the target Java VM.

- When the check box is selected:
  Monitoring is enabled.
- When the check box is not selected (default):
  Monitoring is disabled.

Total Usage (0 to 102400)

Specify the threshold for the usage rate of the Java non-heap areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Code Cache (0 to 102400)

Specify the threshold for the usage rate of the Java Code Cache area used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

CodeHeap non-nmethods (0 to 102400)

Specify the threshold for the usage rate of the Java CodeHeap non-nmethods areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

CodeHeap profiled (0 to 102400)

Specify the threshold for the usage rate of the Java CodeHeap profiled nmethods areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

CodeHeap non-profiled (0 to 102400)

Specify the threshold for the usage rate of the Java CodeHeap non-profiled nmethods areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Compressed Class Space (0 to 102400)

Specify the threshold for the usage rate of the Compressed Class Space areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Metaspace (0 to 102400)

Specify the threshold for the usage rate of the Metaspace area used by the target Java VM.

Default: 0[MB]

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes (""). Example) "/usr/local/bin/command" arg1 arg2

Specify the commands that will be executed if errors are detected in the process for checking the amount of the usage of the Java heap area, Java non-heap area in the monitor target Java VM.

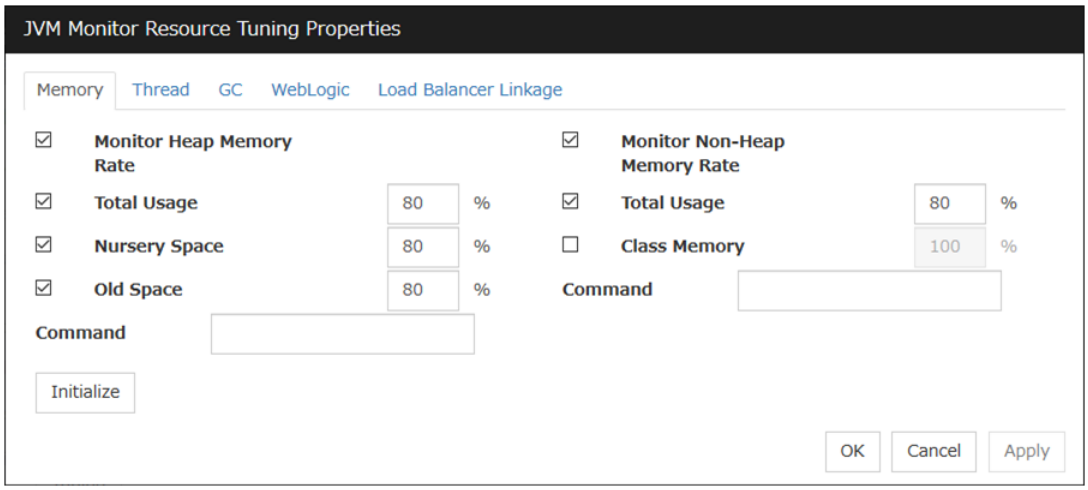
See also "*Executing a command corresponding to cause of each detected error*".

Default: None

Initialize

Click the **Initialize** button to set all the items to their default values.

4.42.26 Memory tab (when Oracle JRockit is selected for JVM Type)



Displayed only when **JRockit** is selected for **JVM Type**.

Monitor Heap Memory Rate

Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- When the check box is selected (default):
  Monitoring enabled
- When the check box is not selected:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java heap areas used by the target Java VM.

Default: 80[%]

Nursery Space (1 to 100)

Specify the threshold for the usage rate of the Java Nursery Space used by the target JRockit JVM.

Default: 80[%]

Old Space (1 to 100)

Specify the threshold for the usage rate of the Java Old Space used by the target JRockit JVM.

Default: 80[%]

Monitor Non-Heap Memory Rate

Enables the monitoring of the usage rates of the Java non-heap areas used by the target Java VM.

- When the check box is selected (default):
  Monitoring enabled

- When the check box is not selected:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java non-heap areas used by the target Java VM.

Default: 80[%]

Class Memory (1 to 100)

Specify the threshold for the usage rate of the Java Class Memory used by the target JRockit JVM.

Default: 100[%]

Command (within 255 bytes)

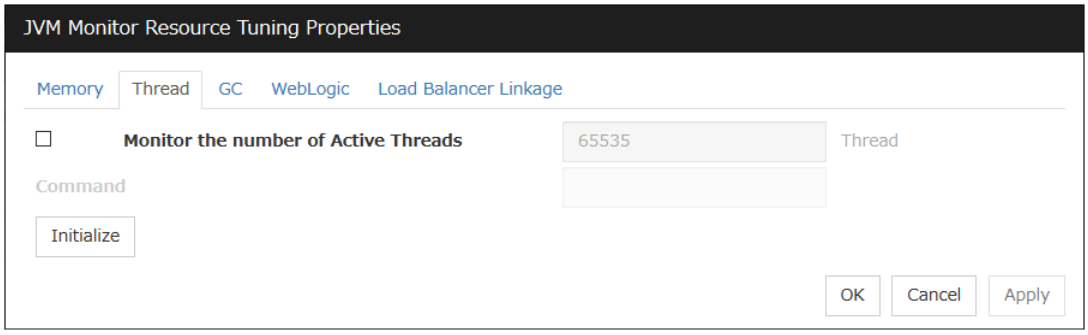
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2
Specify the commands that will be executed if errors are detected in the process for checking the amount of the usage of the Java heap area, Java non-heap area in the monitor target Java VM.
See "*Executing a command corresponding to cause of each detected error*".

Default: None

Initialize

Click **Initialize** to set all the items to their default values.

4.42.27 Thread tab



Monitor the number of Active Threads (1 to 65535)

Specify the upper limit threshold for the number of threads running on the monitor target Java VM.

Default: 65535 [threads]

Command (within 255 bytes)

Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2
Specify the commands that will be executed if errors are detected in the process for checking the number of active threads in the monitor target Java VM.

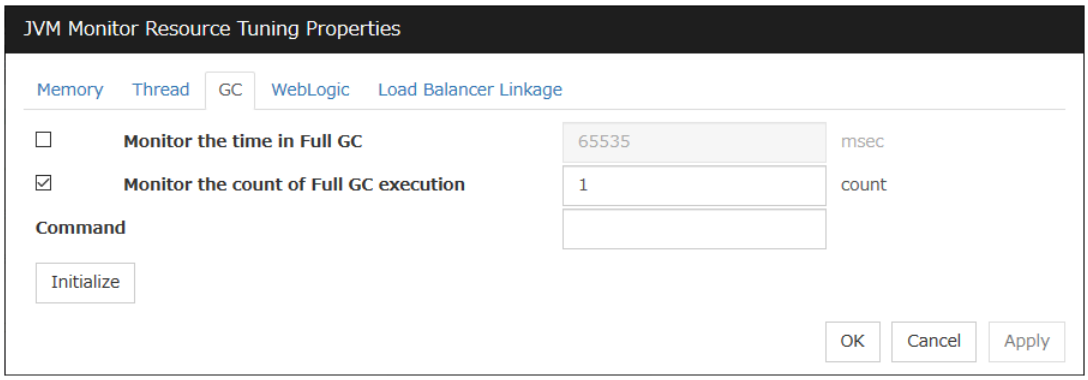
See "*Executing a command corresponding to cause of each detected error*".

Default: None

Initialize

Click **Initialize** to set all the items to their default values.

4.42.28 GC tab



Monitor the time in Full GC (1 to 65535)

Specify the threshold for the Full GC execution time since previous measurement on the target Java VM. The threshold for the Full GC execution time is the average obtained by dividing the Full GC execution time by the number of times Full GC occurs since the previous measurement.

To determine the case in which the Full GC execution time since the previous measurement is 3000 milliseconds and Full GC occurs three times as an error, specify 1000 milliseconds or less.

Default: 65535 [milliseconds]

Monitor the count of Full GC execution (1 to 65535)

Specify the threshold for the number of times Full GC occurs since previous measurement on the target Java VM.

Default: 1 (time)

Command (within 255 bytes)

Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2

Specify the commands that will be executed if errors are detected in the process for measuring time in Full GC and the count of Full GC execution in the monitor target Java VM.

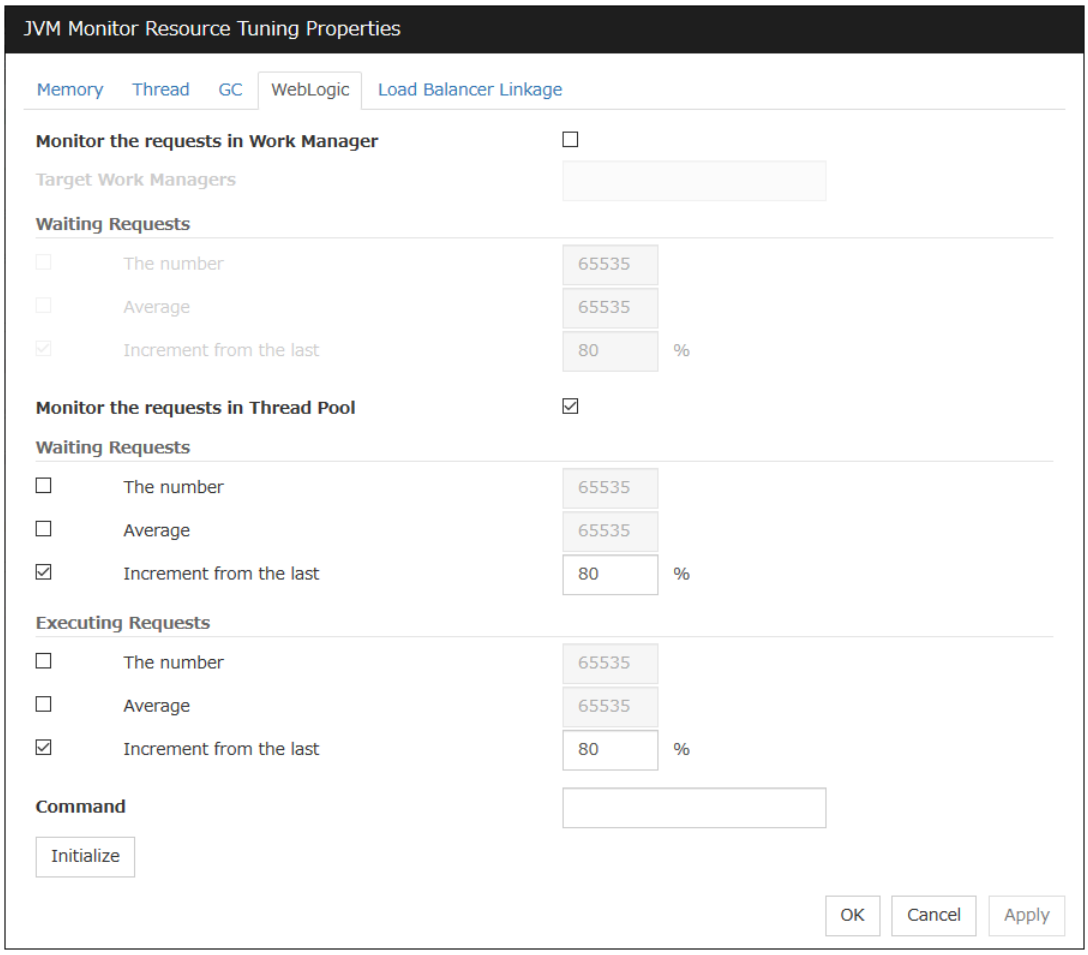
See "*Executing a command corresponding to cause of each detected error*".

Default: None

Initialize

Click **Initialize** to set all the items to their default values.

4.42.29 WebLogic tab



Displayed only when **WebLogic Server** is selected for **Target**.

Monitor the requests in Work Manager

Enables the monitoring of the wait requests by Work Managers on the WebLogic Server.

- When the check box is selected:
  Monitoring enabled
- When the check box is not selected (default):
  Monitoring disabled

Target Work Managers

Specify the names of the Work Managers for the applications to be monitored on the target WebLogic Server. To monitor Work Managers, you must specify this setting.

*App*1[*WM*1,*WM*2,...];*App*2[*WM*1,*WM*2,...];...

For App and *WM,* only ASCII characters are valid (except Shift_JIS codes 0x005C and 0x00A1 to 0x00DF).

To specify an application that has an application archive version, specify "application_name#version" in *App*.

When the name of the application contains "[" and/or "]", prefix it with " \\ ".

(Ex.) When the application name is app[2], enter app\\[2\\].

Default: None

The number (1 to 65535)

Specify the threshold for the wait request count for the target WebLogic Server Work Manager(s).

Default: 65535

Average (1 to 65535)

Specify the threshold for the wait request count average for the target WebLogic Server Work Manager(s).

Default: 65535

Increment from the last (1 to 1024)

Specify the threshold for the wait request count increment since the previous measurement for the target WebLogic Server Work Manager(s).

Default: 80[%]

Monitor the requests in Thread Pool

In WebLogic Server thread pool to be monitored, the number of wait requests, and the monitoring settings of the number of executing request. The number of requests, HTTP requests and the number that was waiting to be processed and run inside WebLogic Server, and includes the number of requests of the processing performed by the internal EJB call and WebLogic Server. However, it can not judge an abnormal state to be increased. Please specify if you want to the collection of JVM statistics log.

- When the check box is selected (default):
  Monitoring enabled
- When the check box is not selected:
  Monitoring disabled

Waiting Requests The number (1 to 65535)

Specify the threshold for the wait request count.

Default: 65535

Waiting Requests Average (1 to 65535)

Specify the threshold for the wait request count average.

Default: 65535

Waiting Requests Increment from the last (1 to 1024)

Specify the threshold for the wait request count increment since the previous measurement.

Default: 80[%]

Executing Requests The number (1 to 65535)

Specify the threshold for the number of requests executed per unit of time.

Default: 65535

Executing Requests Average (1 to 65535)

Specify the threshold for the average count of requests executed per unit of time.

Default: 65535

Executing Requests Increment from the last (1 to 1024)

Specify the threshold for the increment of the number of requests executed per unit of time since the previous measurement.

Default: 80[%]

Command (within 255 bytes)

Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2

Specify the commands that will be executed if errors are detected in the process for executing requests in the Work Manager and Thread Pool of WebLogic Server.

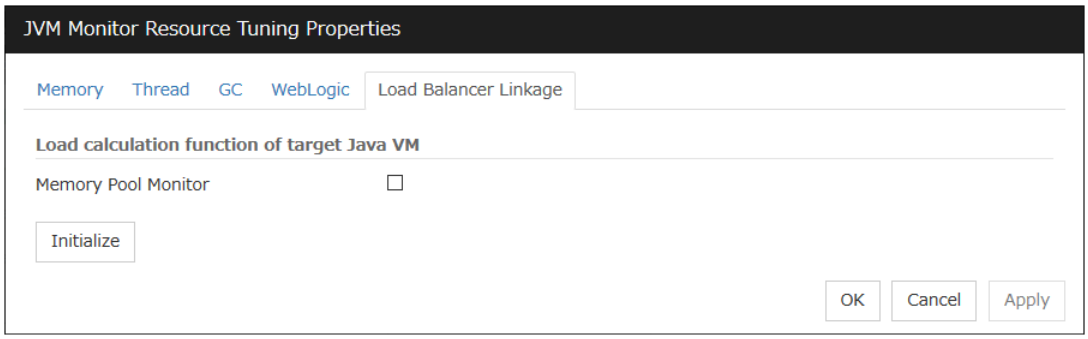
See "*Executing a command corresponding to cause of each detected error*".

Default: None

Initialize

Click **Initialize** to set all the items to their default values.

4.42.30 Load Balancer Linkage tab



This screen appears when an item other than **BIG-IP LTM** is selected as the load balancer type.

Memory Pool Monitor

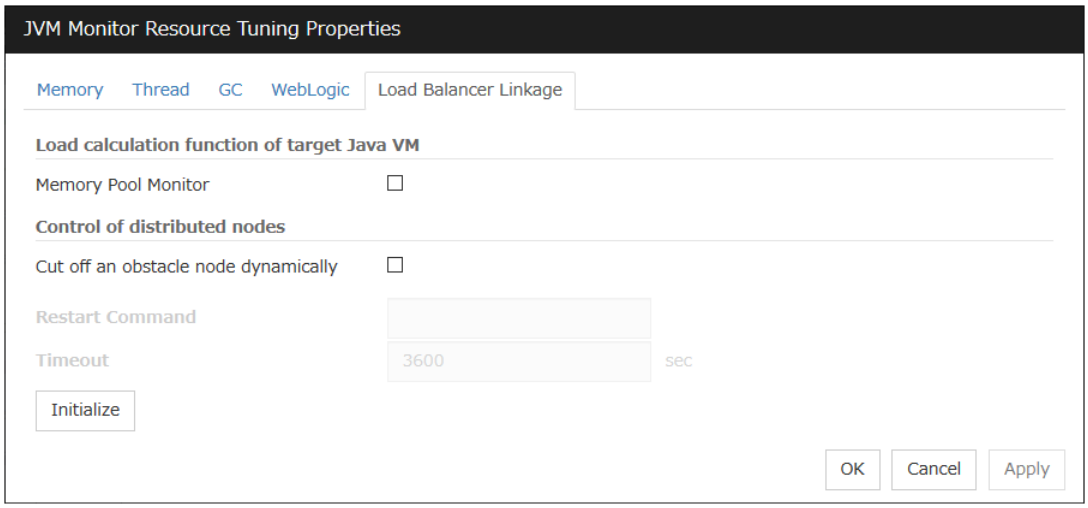
Enables the monitoring of the memory pool when notifying the load balancer of dynamic load information.

- When the check box is selected:
  Monitoring enabled
- When the check box is not selected (default):
  Monitoring disabled

Initialize

Click the **Initialize** button to set all the items to their default values.

4.42.31 Load Balancer Linkage tab



This screen appears when **BIG-IP LTM** is selected as the load balancer type.

Memory Pool Monitor

Enables the monitoring of the memory pool when notifying the load balancer of dynamic load information.

- When the check box is selected:
  Monitoring enabled
- When the check box is not selected (default):
  Monitoring disabled

Cut off an obstacle node dynamically

When the JVM monitor detects a monitor target failure (example: the collection information exceeds the configured threshold), it sets whether to update the status of the BIG-IP LTM distributed node from "enable" to "disable."

- When the check box is selected:
  Update the status from enable to disable.
- When the check box is not selected (default):
  Do not update.

Restart Command

Specify the absolute path of the command to be executed after waiting until the number of connections of the distributed node becomes 0. This function is effective when the monitor target is restarted when resident monitoring is performed and a monitor target failure is detected. Specify the same value between JVM monitor resources.

Timeout (0 to 2592000)

After updating the distributed node status from "enable" to "disable," the JVM monitor sets the timeout used when waiting until the number of connections of the distributed node falls to 0. If the timeout elapses, [**Restart Command**] is not executed.

Default: 3600 [sec]

Initialize

Click the **Initialize** button to set **Memory Pool Monitor**, **Cut off an obstacle node dynamically**, and **Timeout** to their default values.

4.43 Understanding System monitor resources

System monitor resources periodically collect statistical information about System resources analyze the information according to given knowledge data. System monitor resources serve to detect the exhaustion of resources early according to the results of analysis.

4.43.1 Notes on System monitor resource

To use a System monitor resource, zip and unzip packages must have been installed on the servers.

For the supported versions of System Resource Agent, see "Applications supported by monitoring options" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

For the recovery target, specify the resource to which fail-over is performed upon the detection of an error in resource monitoring by System Resource Agent.

The use of the default System Resource Agent settings is recommended.

Errors in resource monitoring may be undetectable when:

- A value repeatedly exceeds and then falls below a threshold during whole system resource monitoring.

If the date or time of the OS has been changed while System Resource Agent is running, resource monitoring may operate incorrectly as described below because the timing of analysis which is normally done at 10 minute intervals may differ the first time after the date or time is changed. If either of the following occur, suspend and resume cluster.

- No error is detected even after the specified duration for detecting errors has passed.
- An error is detected before the specified duration for detecting errors has elapsed.

Once the cluster has been suspended and resumed, the collection of information is started from that point of time.

For the SELinux setting, set permissive or disabled.

The enforcing setting may disable the communication needed by EXPRESSCLUSTER.

The amount of system resources used is analyzed at 10-minute intervals. Thus, an error may be detected up to 10 minutes after the monitoring session.

The amount of disk resources used is analyzed at 60-minute intervals. Thus, an error may be detected up to 60 minutes after the monitoring session.

Specify a value smaller than the actual disk size when specifying the disk size for free space monitoring of a disk resource. If a value is specified that is larger than the actual disk size, an error will be detected due to insufficient free space.

If the monitored disk has been replaced, analyzed information up until the time of the disk replacement will be cleared if one of the following items of information differs between the previous and current disks.

- Total disk capacity
- File system

Disk resource monitoring can only monitor disk devices.

For server for which no swap was allocated, uncheck the monitoring of total virtual memory usage.

Disk usage information collected by System Resource Agent is calculated by using the total disk space and free disk space. This value may slightly differ from the disk usage which df(1) command shows because it uses a different calculation method.

Up to 64 disk units can be simultaneously monitored by the disk resource monitoring function.

If **System monitor** is not displayed in the **Type** column on the monitor resource definition screen, select **Get License Info** and then acquire the license information.

System monitor resource collected statistics information and analysis information, it outputs. When the number of these files reached following biggest number, it's eliminated from an old file.
(<data pass> in following text is "<EXPRESSCLUSTER_install_path >/ha/sra/data/".)

- Statistical information data of system resources.
  Path: <data path>/hasrm_monitor_list.xml.YYYYMMDDhhmmss.zip
  Maximum number of a file: 1500
- Analyzed information data of system resources.
  Path: <data path>/hasrm_analyze_list.xml.YYYYMMDDhhmmss.zip
  Maximum number of a file: 3
- Statistical information data of disk resources.
  Path: <data path>/hasrm_diskcapacity_monitor_list.xml.YYYYMMDDhhmmss.zip
  Maximum number of a file: 10
- Analyzed information data of disk resources.
  Path: <data path>/hasrm_diskcapacity_analyze_list.xml.YYYYMMDDhhmmss.zip
  Maximum number of a file: 3

4.43.2 How System monitor resources perform monitoring

System monitor resources monitor the following:

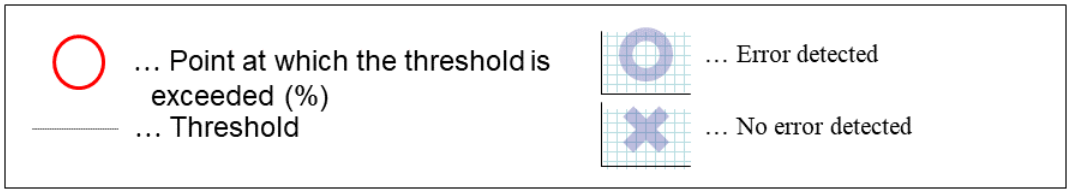
Periodically collect the amounts of system resources and disk resources used and then analyze the amounts.

An error is recognized if the amount of a resource used exceeds a pre-set threshold.

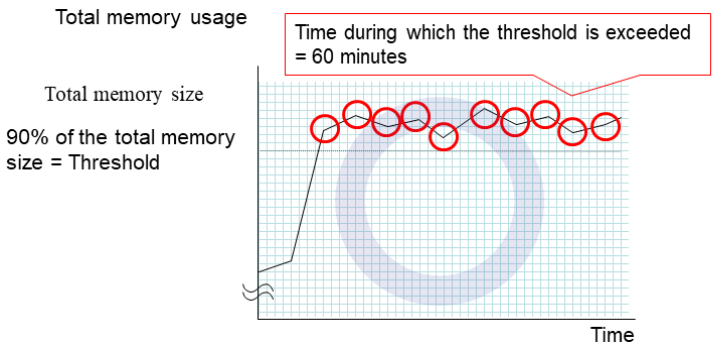
When an error detected state persists for the monitoring duration, it is posted as an error detected during resource monitoring.

System resource monitoring with the default values reports an error found in resource monitoring 60 minutes later if the resource usage does not fall below 90%.

The following shows an example of error detection for the total memory usage in system resource monitoring with the default values.

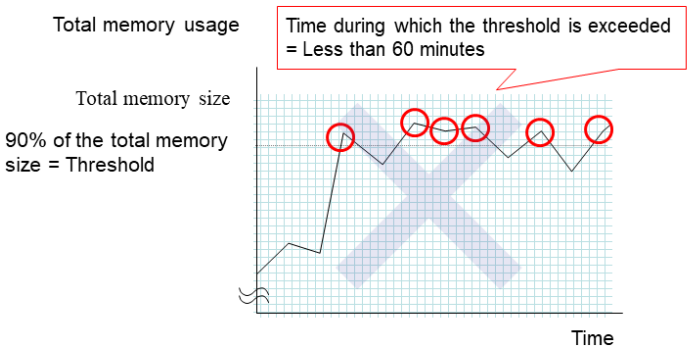


- The total memory usage remains at the total memory usage threshold or higher as time passes, for at least a certain duration of time.



→ The total memory usage remains at the threshold (90%) or higher continuously for the monitoring duration time (60 minutes) or longer; detection of a total memory usage error is recognized.

- The total memory usage rises and falls in the vicinity of the total memory usage threshold as time passes, but always remains under that threshold.



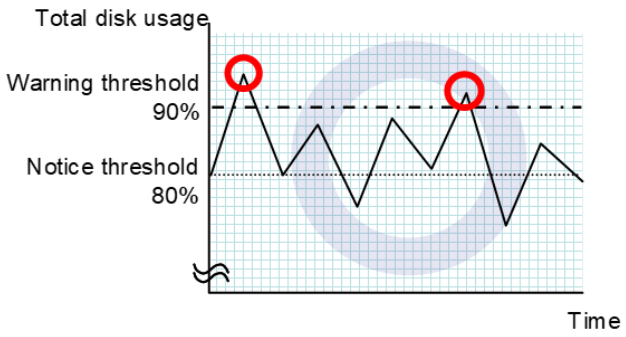
→ The total memory usage is temporarily at the total memory usage threshold (90%) or higher, but goes below the threshold before it remains at the threshold or higher continuously for the monitoring duration time (60 minutes); no total memory usage error is detected.

If disk resource monitoring operated under the default settings, it will report a notice level error after 24 hours.

The following chart describes how disk resource monitoring detects disk usage errors when operating under the default settings.

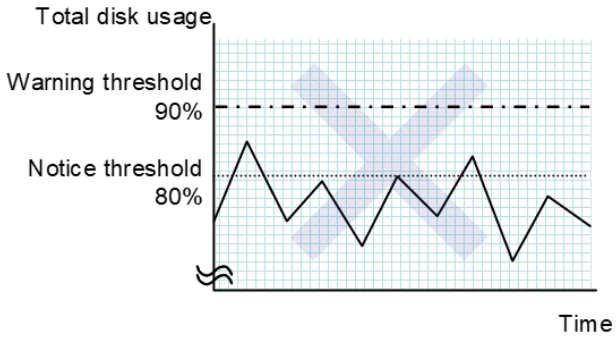
Monitoring disk usage by warning level

- In the following example, disk usage exceeds the threshold which is specified as the warning level upper limit.



→ Disk usage error will be detected as disk usage exceed the threshold which configured as warning level upper limit.

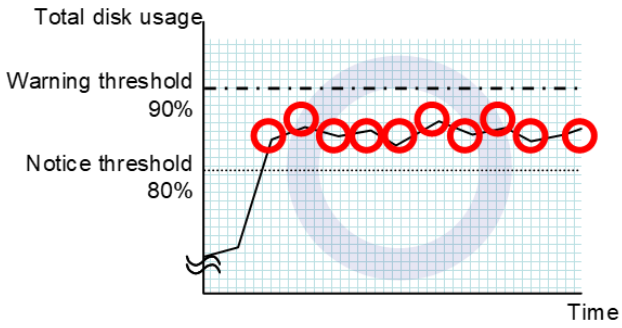
- In the following example, disk usage increases and decreases within certain range, and does not exceed the threshold which is specified as the warning level upper limit.



→ Disk usage error will not be detected as disk usage repeat increasing and decreasing within certain range(below warning level upper limit).

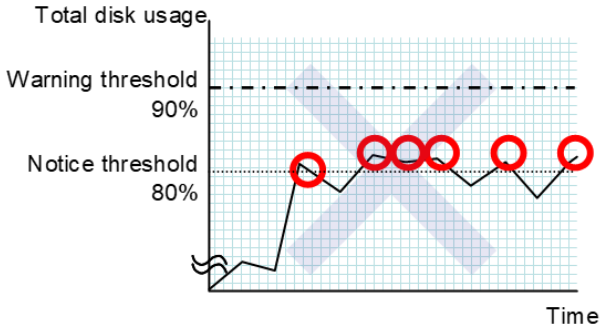
Monitoring disk usage by notice level

- In the following example, disk usage continuously exceeds the threshold specified as the notification level upper limit, and the duration exceeds the set length.



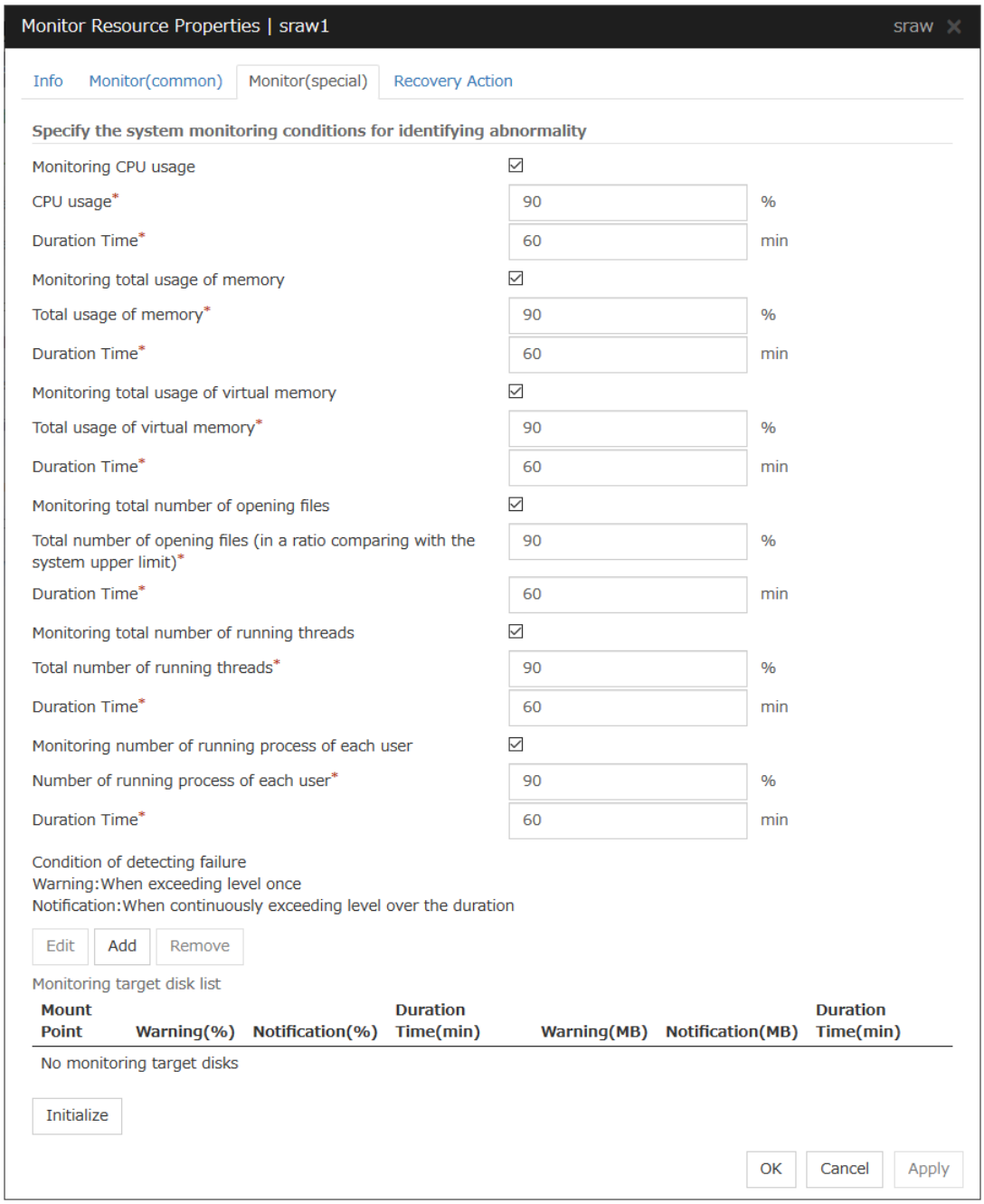
→ Disk usage error will be detected as disk usage continuously exceed notice level upper limit.

- In the following example, disk usage increases and decreases within a certain range, and does not exceed the threshold specified as the notification level upper limit.



→ Disk usage error will not be detected as disk usage repeat increasing and decreasing around notice level upper limit.

4.43.3 Monitor (special) tab



Monitoring CPU usage

Enables CPU usage monitoring.

- When the check box is selected:
  Monitoring is enabled for the CPU usage.
- When the check box is not selected:
  Monitoring is disabled for the CPU usage.

CPU usage (1 to 100)

Specify the threshold for the detection of the CPU usage.

Duration Time (1 to 1440)

Specify the duration for detecting the CPU usage.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total usage of memory

Enables the monitoring of the total usage of memory.

- When the check box is selected:
  Monitoring is enabled for the total usage of memory.
- When the check box is not selected:
  Monitoring is disabled for the total usage of memory.

Total usage of memory (1 to 100)

Specify the threshold for the detection of a memory use amount error (percentage of the memory size implemented on the system).

Duration Time (1 to 1440)

Specify the duration for detecting a total memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total usage of virtual memory

Enables the monitoring of the total **usage of virtual memory**.

- When the check box is selected:
  Monitoring is enabled for the total **usage of virtual memory**.
- When the check box is not selected:
  Monitoring is disabled for the total **usage of virtual memory**.

Total usage of virtual memory (1 to 100)

Specify the threshold for the detection of a virtual memory usage error.

Duration Time (1 to 1440)

Specify the duration for detecting a total virtual memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total number of opening files

Enables the monitoring of the total number of open**ing** files.

- When the check box is selected:
  Monitoring is enabled for the total number of open**ing** files.
- When the check box is not selected:
  Monitoring is disabled for the total number of open**ing** files.

Total number of opening files (in a ratio comparing with the system upper limit) (1 to 100)

Specify the threshold for the detection of an error related to the total number of opening files (percentage of the system upper limit).

Duration Time (1 to 1440)

Specify the duration for detecting an error with the total number of opening files.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total number of running threads

Enables the monitoring of the total number of running threads.

- When the check box is selected:
  Monitoring is enabled for the total number of running threads.
- When the check box is not selected:
  Monitoring is disabled for the total number of running threads.

Total number of running **threads (1 to 100)**

Specify the threshold for the detection of an error related to the total number of running threads (percentage of the system upper limit).

Duration Time (1 to 1440)

Specify the duration for detecting an error with the total number of running threads.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring number of running processes of each user

Enables the monitoring of the number of processes being run **of each user**

- When the check box is selected:
  Monitoring is enabled for the number of processes being run **of each user**.
- When the check box is not selected:
  Monitoring is disabled for the number of processes being run **of each user**.

Number of running processes of each user (1 to 100)

Specify the threshold for the detection of an error related to the number of processes being run **of each user** (percentage of the system upper limit).

Duration Time (1 to 1440)

Specify the duration for detecting an error with the number of processes being run **of each user**.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Add

Click this to add disks to be monitored. The **Input of watch condition** dialog box appears.

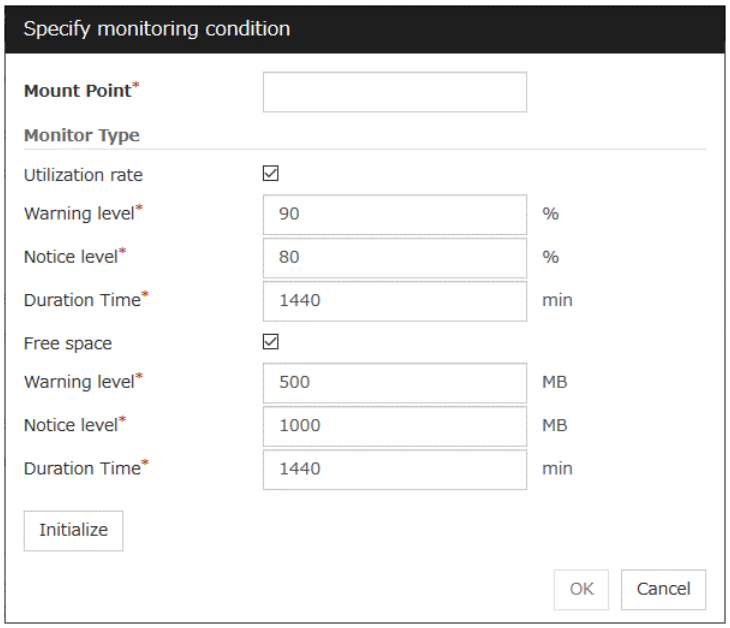
Configure the detailed monitoring conditions for error determination, according to the descriptions given in the **Input of watch condition** dialog box.

Remove

Click this to remove a disk selected in **Disk List so** that it will no longer be monitored.

Edit

Click this to display the **Input of watch condition** dialog box. The dialog box shows the monitoring conditions for the disk selected in **Disk List**. Edit the conditions and click **OK**.



Mount point (within 1024 bytes)

Set the mountpoint to be monitored. The name must begin with a forward slash (/).

Utilization rate

Enables the monitoring of the disk usage.

- When the check box is selected:
  Monitoring is enabled for the disk usage.
- When the check box is not selected:
  Monitoring is disabled for the disk usage.

Warning level (1 to 100)

Specify the threshold for warning level error detection for disk usage.

Notice level (1 to 100)

Specify the threshold for notice level error detection for disk usage.

Duration Time (1 to 43200)

Specify the duration for detecting a notice level error of the disk usage rate.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Free space

Enables the monitoring of the free disk space.

- When the check box is selected:
  Monitoring is enabled for the free disk space.
- When the check box is not selected:
  Monitoring is disabled for the free disk space.

Warning level (1 to 4294967295)

Specify the amount of disk space (in megabytes) for which the detection of an free disk space error at the warning level is recognized.

Notice level (1 to 4294967295)

Specify the amount of disk space (in megabytes) for which the detection of an free disk space error at the notice level is recognized.

Duration Time (1 to 43200)

Specify the duration for detecting a notice level error related to the free disk space.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

4.44 Understanding Process resource monitor resources

Process resource monitor resources periodically collect statistical information about resources used by processes and analyze the information according to given knowledge data. Process resource monitor resources serve to detect the exhaustion of resources early according to the results of analysis.

4.44.1 Notes on Process resource monitor resource

To use a Process resource monitor resource, zip and unzip packages must have been installed on the servers.

For the supported versions, see "Applications supported by monitoring options" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

For the recovery target, specify the resource to which fail-over is performed upon the detection of an error in resource monitoring by Process resource monitor resource.

The use of the default Process resource monitor resource settings is recommended.

Swapped out processes are not subject to the detection of resource errors.

If the date or time of the OS has been changed while System Resource Agent is running, resource monitoring may operate incorrectly as described below because the timing of analysis which is normally done at 10 minute intervals may differ the first time after the date or time is changed.

If either of the following occur, suspend and resume cluster.

- No error is detected even after the specified duration for detecting errors has passed.
- An error is detected before the specified duration for detecting errors has elapsed.

Once the cluster has been suspended and resumed, the collection of information is started from that point of time.

For the SELinux setting, set permissive or disabled.

The enforcing setting may disable the communication needed by EXPRESSCLUSTER.

The amount of process resources used is analyzed at 10-minute intervals. Thus, an error may be detected up to 10 minutes after the monitoring session.

If **Process resource monitor resource** is not displayed in the **Type** column on the monitor resource definition screen, select **Get License Info** and then acquire the license information.

For information on the licenses necessary for process resource monitor resources, see "Function list and necessary license" in "Designing a system configuration" in "Notes and Restrictions" in the "Getting Started Guide".

Process resource monitor resource collected statistics information and analysis information, it outputs. When the number of these files reached following biggest number, it's eliminated from an old file.
(<data path> in following text is "<EXPRESSCLUSTER_install_path >/ha/sra/data/".)

- Statistical information data of process resources.
  Path: <data path>/hasrm_monitor_list.xml.YYYYMMDDhhmmss.zip
  Maximum number of a file: 1500
- Analyzed information data of system resources.
  Path: <data path>/hasrm_analyze_list.xml.YYYYMMDDhhmmss.zip
  Maximum number of a file: 3

To return the status of the process resource monitor resource from error to normal, perform either of the following:

- Suspending and resuming the cluster
- Stopping and starting the cluster

4.44.2 How Process resource monitor resources perform monitoring

Process resource monitor resources monitor the following:

Periodically collect the amounts of process resources used and then analyze the amounts.

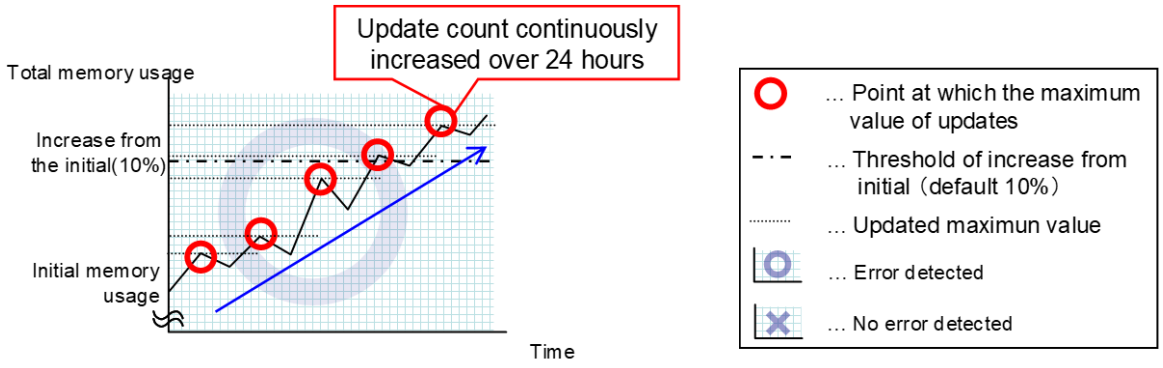
An error is recognized if the amount of a resource used exceeds a pre-set threshold.

When an error detected state persists for the monitoring duration, it is posted as an error detected during resource monitoring.

If process resource monitoring (of the CPU, memory, number of opening files, or number of zombie processes) operated by using the default values, a resource error is reported after 24 hours.

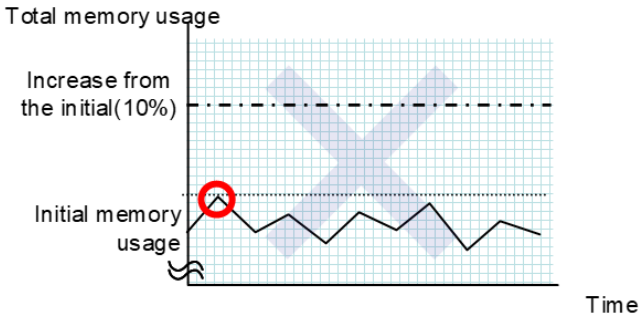
The following chart describes how process resource monitoring detects memory usage errors.

- In the following example, as time progresses, memory usage increases and decreases, the maximum value is updated more times than specified, and increases by more than 10% from its initial value.



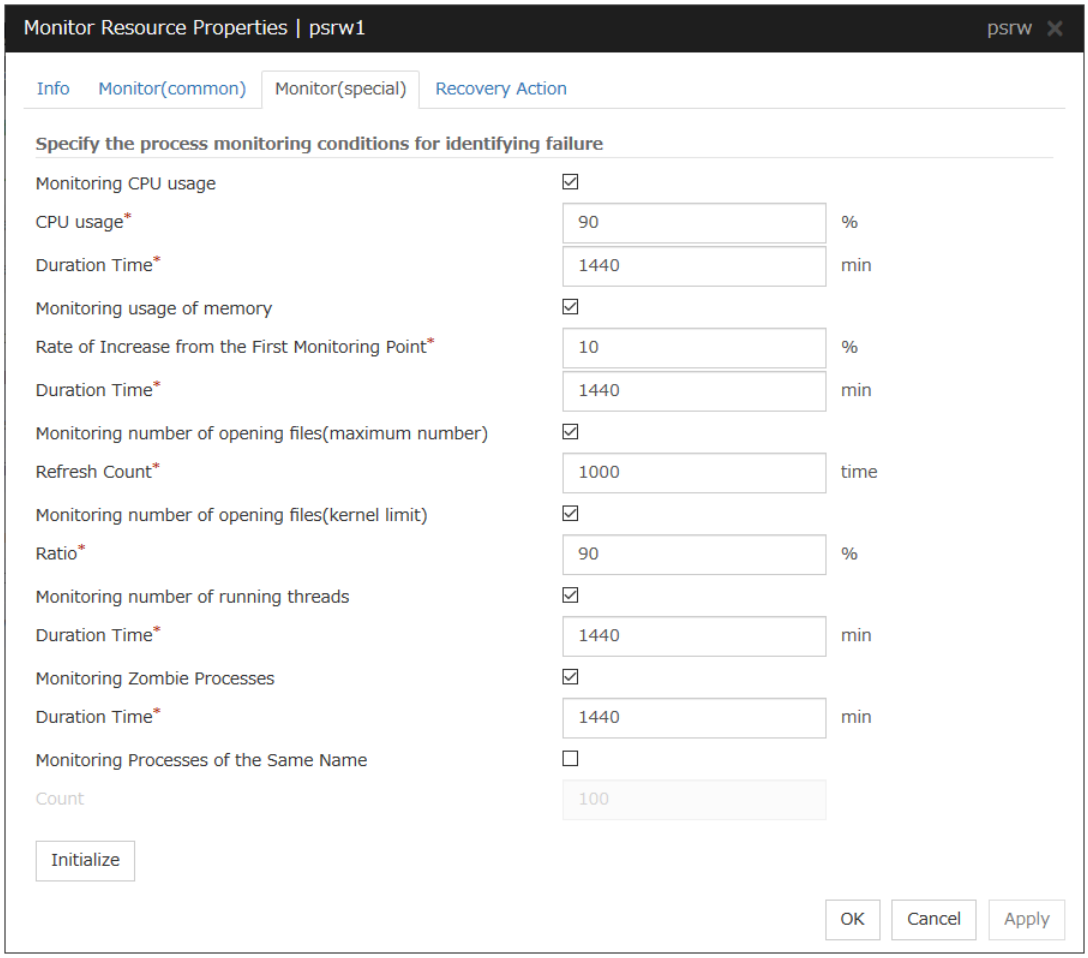
→ Memory leak will be detected as memory usage continuously increased over 24hours (by default), and it increased more than 10% from its initial value.

- In the following example, memory usage increases and decreases, but remains within a set range.



→ Memory leak will not be detected as memory usage repeat increasing and decreasing within certain range (below specific value).

4.44.3 Monitor (special) tab



Monitoring CPU usage

Enables CPU usage monitoring.

- When the check box is selected:
  Monitoring is enabled for the CPU usage.
- When the check box is not selected:
  Monitoring is disabled for the CPU usage.

CPU usage (1 to 100)

Specify the threshold for the detection of the CPU usage.

Duration Time (1 to 129600)

Specify the duration for detecting the CPU usage.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring usage of memory

Enables the monitoring of the usage of memory.

- When the check box is selected:
  Monitoring is enabled for the total usage of memory.
- When the check box is not selected:
  Monitoring is disabled for the total usage of memory.

Rate of Increase from the First Monitoring Point (1 to 1000)

Specify the threshold for the detection of a memory use amount error.

Duration Time (1 to 129600)

Specify the duration for detecting a total memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring number of opening files(maximum number)

Enables the monitoring of the number of opening files(maximum number).

- When the check box is selected:
  Monitoring is enabled for the number of opening files.
- When the check box is not selected:
  Monitoring is disabled for the number of opening files.

Refresh Count (1 to 1024)

Specify the refresh count for the detection of the number of opening files error.
If the number of opening files maximum value is updated more count than specified, the detection of an error is recognized.

Monitoring number of opening files(kernel limit)

Enables the monitoring of the number of opening files(kernel limit).

- When the check box is selected:
  Monitoring is enabled for the number of opening files.
- When the check box is not selected:
  Monitoring is disabled for the number of opening files.

Ratio (1 to 100)

Specify the ration for detection of the opening files(the percentage to the kernel limit).

Monitoring number of running threads

Enables the monitoring of the number of running threads.

- When the check box is selected:
  Monitoring is enabled for the number of running threads.

- When the check box is not selected:
  Monitoring is disabled for the number of running threads.

Duration Time (1 to 129600)

Specify the duration for detecting an error with the total number of running threads.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring Zombie Process

Enables the monitoring of Zombie Processes.

- When the check box is selected:
  Monitoring is enabled for the Zombie Processes.
- When the check box is not selected:
  Monitoring is disabled for the Zombie Processes.

Duration Time (1 to 129600)

Specify the duration for detecting Zombie Processes.

If process is a Zombie Process over the specified duration, the detection of an error is recognized.

Monitoring Processes of the Same Name

Enables the monitoring of Processes of the Same Name.

- When the check box is selected:
  Monitoring is enabled for the Processes of the Same Name.
- When the check box is not selected:
  Monitoring is disabled for the Processes of the Same Name.

Count (1 to 10000)

Specify the count for detecting an error with the processes of the same name.
If the processes of the same name has been exists more than specified numbers, the detection of an error is recognized.

4.45 Understanding AWS Elastic IP monitor resources

For EIP control, AWS Elastic IP monitor resources confirm the existence of EIPs by using the AWS CLI command.

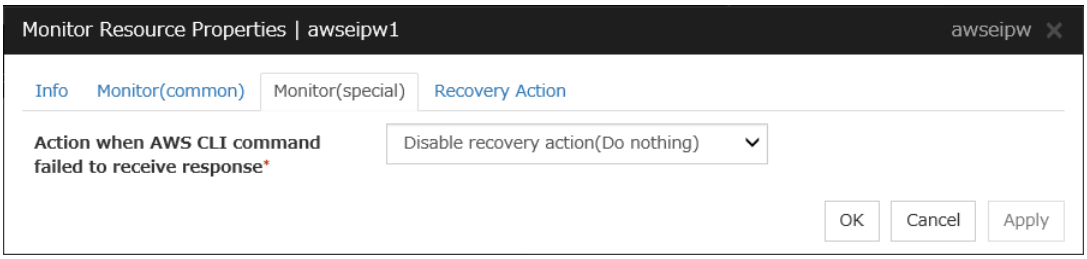
4.45.1 Notes on AWS Elastic IP monitor resources

- AWS Elastic IP monitor resources are automatically created when AWS Elastic IP resources are added. A single AWS Elastic IP monitor resource is automatically created for a single AWS Elastic IP resource.
- See "Setting up AWS Elastic IP resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.45.2 Applying environment variables to AWS CLI run from the AWS Elastic IP monitor resource

See "*Applying environment variables to AWS CLI run from the AWS Elastic IP resource*" in "*Understanding AWS Elastic IP resources*" in "3. *Group resource details*" in this guide.

4.45.3 Monitor (special) tab



Action when AWS CLI command failed to receive response

Specify the action to be taken when acquiring the AWS CLI command response fails. This failure occurs, for example, when a region endpoint is down due to maintenance, when AWS CLI timeout occurs because of connection route troubles, heavy load or delay, or when a credential error occurs. Refer to the following instructions:

- Select **Enable recovery action** if you want to perform failover when AWS CLI command fails.
- Select **Disable recovery action(Display warning)** if you want to show a warning message without failover when AWS CLI command fails.
- Select **Disable recovery action(Do nothing)** if you think this error is CLI command failure (a monitoring target itself is in normal status) and no action needs to be taken. This option is recommended as still error detection can find EIP error (e.g. no EIP is found).

4.46 Understanding AWS Virtual IP monitor resources

For VIP control, AWS Virtual IP monitor resources confirm the existence of VIPs and the soundness of VPC routing by using the OS API and AWS CLI commands. AWS CLI command is executed for AWS Virtual IP monitor resources while monitoring to check the route table information.

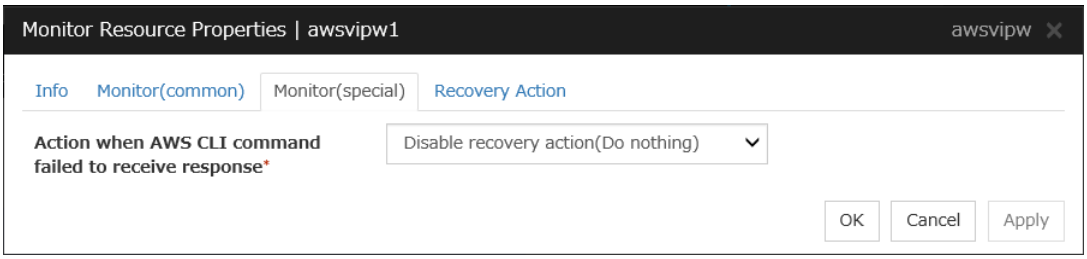
4.46.1 Notes on AWS Virtual IP monitor resources

- AWS Virtual IP monitor resources are automatically created when AWS Virtual IP resources are added. A single AWS Virtual IP monitor resource is automatically created for a single AWS Virtual IP resource.
- See "Setting up AWS Virtual IP resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.46.2 Applying environment variables to AWS CLI run from the AWS Virtual IP monitor resource

See "*Applying environment variables to AWS CLI run from the AWS Virtual IP resource*" in "*Understanding AWS Virtual IP resources*" in "3. *Group resource details*" in this guide

4.46.3 Monitor (special) tab



Action when AWS CLI command failed to receive response

Specify the action to be taken when acquiring the AWS CLI command response fails. This failure occurs, for example, when a region endpoint is down due to maintenance, when AWS CLI timeout occurs because of connection route troubles, heavy load or delay, or when a credential error occurs. Refer to the following instructions:

- Select **Enable recovery action** if you want to perform failover when AWS CLI command fails.
- Select **Disable recovery action(Display warning)** if you want to show a warning message without failover when AWS CLI command fails.
- Select **Disable recovery action(Do nothing)** if you think this error is CLI command failure (a monitoring target itself is in normal status) and no action needs to be taken. This option is recommended as still error detection can find errors, for example when troubles are found in VPC routing condition or no VIP is found.

4.47 Understanding AWS AZ monitor resources

AWS AZ monitor resources monitor the soundness of the AZ to which each server belongs, by using the AWS CLI command. When the command result is available, AZ is in normal status. When information or impaired, AZ is in warning status. When unavailable, AZ is in error status. If you use internal version earlier than 4.2.0.1, only available represents the normal status (other results are categorized in error status).

4.47.1 Notes on AWS AZ monitor resources

- When monitoring an AZ, create a single AWS AZ monitor resource.
- See "Setting up AWS Elastic IP resources" and "Setting up AWS Virtual IP resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.47.2 Applying environment variables to AWS CLI run from the AWS AZ monitor resource

See "*Applying environment variables to AWS CLI run from the AWS Virtual IP resource*" in "*Understanding AWS Virtual IP resources*" in "3. *Group resource details*" in this guide.

4.47.3 Monitor (special) tab

Availability Zone (within 45 bytes) `Server Individual Setup`

Specify the availability zone in which to perform monitoring.

Action when AWS CLI command failed to receive response

Specify the action to be taken when acquiring the AWS CLI command response fails. This failure occurs, for example, when a region endpoint is down due to maintenance, when AWS CLI timeout occurs because of connection route troubles, heavy load or delay, or when a credential error occurs. Refer to the following instructions:

- Select **Enable recovery action** if you want to perform failover when AWS CLI command fails.
- Select **Disable recovery action(Display warning)** if you want to show a warning message without failover when AWS CLI command fails.
- Select **Disable recovery action(Do nothing)** if you think this error is CLI command failure (a monitoring target itself is in normal status) and no action needs to be taken. This option is recommended as still error detection can find errors, for example when troubles are found in AZ condition.

4.48 Understanding AWS DNS monitor resources

AWS DNS monitor resources confirm the soundness of the registered IP address by using the OS API and AWS CLI commands.

Errors are detected when:

- The resource record set does not exist.
- The registered **IP Address** cannot obtained by name resolution of the virtual host name (DNS name).

4.48.1 Notes on AWS DNS monitor resources

- AWS DNS monitor resources are automatically created when AWS DNS resources are added. A single AWS DNS monitor resource is automatically created for a single AWS DNS resource.
- See "Setting up AWS DNS resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.48.2 Applying environment variables to AWS CLI run from the AWS DNS monitor resource

See "*Applying environment variables to AWS CLI run from the AWS DNS resource*" in "*Understanding AWS DNS resources*" in "*3. Group resource details*" in this guide.

4.48.3 Monitor (special) tab

Monitor Resource Record Set

- The checkbox is selected (default)
  Checks whether the resource record set exists.
- The checkbox is not selected.
  Monitoring disabled

Action when AWS CLI command failed to receive response

Specify the action to be taken when acquiring the AWS CLI command response fails. This failure occurs, for example, when a region endpoint is down due to maintenance, when AWS CLI timeout occurs because of connection route troubles, heavy load or delay, or when a credential error occurs. Refer to the following instructions:

- Select **Enable recovery action** if you want to perform failover when AWS CLI command fails.
- Select **Disable recovery action(Display warning)** if you want to show a warning message without failover when AWS CLI command fails.
- Select **Disable recovery action(Do nothing)** if you think this error is CLI command failure (a monitoring target itself is in normal status) and no action needs to be taken. This option is recommended as still error detection can find errors, for example when troubles are found in IP addresses.

Check Name Resolution

- The checkbox is selected (default).
  Checks whether to obtain the registered IP address by name resolution of the virtual host name (DNS name).
- The checkbox is not selected.

Monitoring disabled

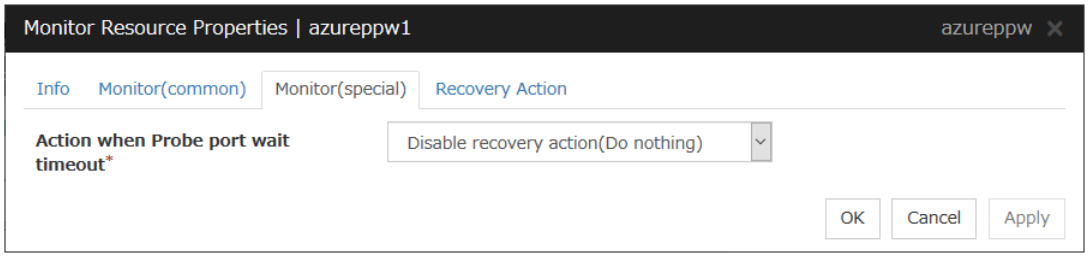
4.49 Understanding Azure probe port monitor resources

Azure probe port monitor resources perform alive monitoring on a probe port control process that starts when Azure probe port resoruces are active on the node on which the Azure probe port resources are active. If the process does not start normally, a monitoring error occurs.

4.49.1 Notes on Azure probe port monitor resources

- Azure probe port monitor resources are automatically created when Azure probe port resources are added. One Azure probe port monitor resource is automatically created per Azure probe port resource.
- In Azure probe port monitor resources, I will monitor the occurrence of probe standby timeout on the Azure probe port resources. Therefore, **Interval** of Azure probe port monitor resource, than the value of the set in the Azure probe port resources monitored **Probe Wait Timeout**, you need to set a large value.
- See "Azure probe port resource settings" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.49.2 Monitor (special) tab



Action when Probe port wait timeout

Specify the recovery action to be taken when a probe port wait timeout occurs in Azure probe port resources.

4.50 Understanding Azure load balance monitor resources

Azure load balance monitor resources monitor to see if a port with the same port number as that of the probe port has been open on the node on which the Azure prove port resources are not active.

4.50.1 Note on Azure load balance monitor resources

- Azure load balance monitor resources are automatically created when Azure probe port resources are added. One Azure load balance monitor resource is automatically created per Azure probe port resource.
- See "Setting up Azure probe port resources" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- See "Setting up Azure load balance monitor resources" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.50.2 Monitor (special) tab

Target Resource

Set Resource to be monitored

4.51 Understanding Azure DNS monitor resources

Azure DNS monitor resources issue a query to the authoritative DNS server and confirm the soundness of the registered IP address.

Errors are detected when:

- The registered IP Address cannot obtained by name resolution of the virtual host name (DNS name).
- Failed to acquire the list of DNS servers.

4.51.1 Notes on Azure DNS monitor resources

- Azure DNS monitor resources are automatically created when Azure DNS resources are added. A single Azure DNS monitor resource is automatically created for a single Azure DNS resource.
- When using public DNS zone, charge occurs for registering the zone and query. Therefore, when **Check Name Resolution** is set to on, the charge occurs per **Interval**.
- See "Setting up Azure resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.51.2 Monitor (special) tab

Check Name Resolution

- The checkbox is selected. (default)
  Checks whether to obtain the registered IP address by name resolution of the virtual host name (DNS name).
- The checkbox is not selected.
  Monitoring disabled

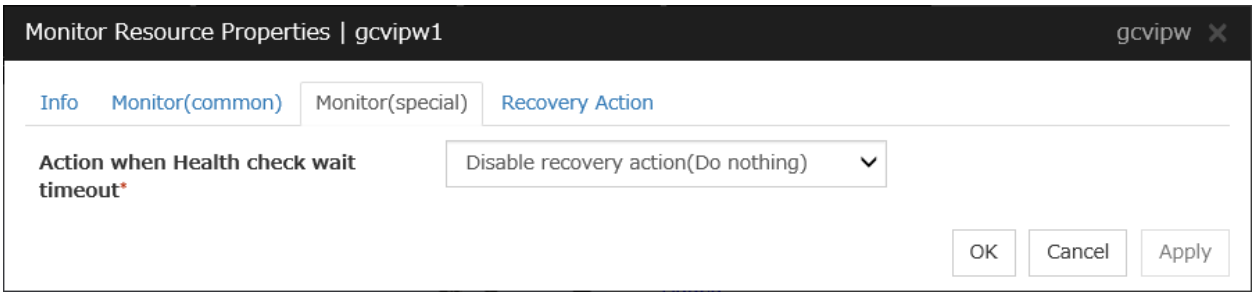
4.52 Understanding Google Cloud Virtual IP monitor resources

Google Cloud Virtual IP monitor resources perform alive monitoring of nodes running Google Cloud Virtual IP resources about control processes which start to run when Google Cloud Virtual IP resources become active. If the process does not start properly, the system takes it as an error. Also, timeout on health check wait time may become an error depending on **Action when Health check wait timeout** settings.

4.52.1 Notes on Google Cloud Virtual IP monitor resources

- Google Cloud Virtual IP monitor resources are added automatically when you add Google Cloud Virtual IP resources. One Google Cloud Virtual IP monitor resource is created automatically for one Google Cloud Virtual IP resource.
- Google Cloud Virtual IP monitor resources check if timeout occurs or not on health check wait time in Google Cloud Virtual IP resources. Therefore the monitor interval values of Google Cloud Virtual IP monitor resources must be larger than the **Health check timeout** values set in the target Google Cloud Virtual IP resources.
- Refer to "Google Cloud Virtual IP resource settings" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.52.2 Monitor (special) tab



Action when Health check wait timeout

Specifies actions when timeout of health check wait time occurs in Google Cloud Virtual IP resources

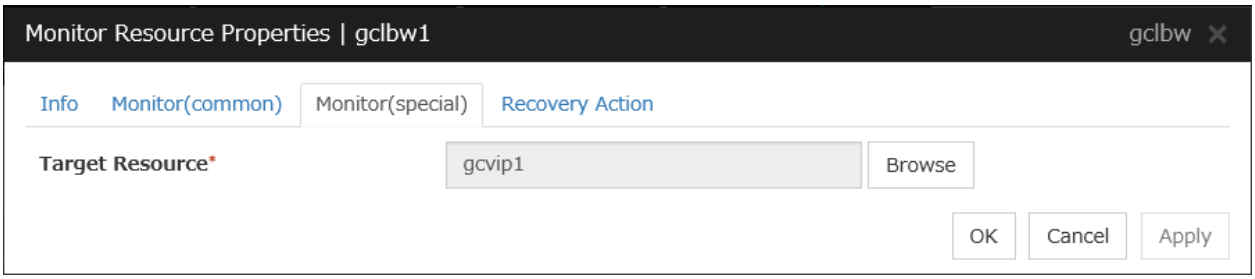
4.53 Understanding Google Cloud load balance monitor resources

Google Cloud load balance monitor resources perform monitoring of nodes not running Google Cloud Virtual IP resources and check if the same port number of the health check port number opens.

4.53.1 Notes on Google Cloud load balance monitor resources

- Google Cloud load balance monitor resources are added automatically when you add Google Cloud Virtual IP resources. One Google Cloud load balance monitor resource is created automatically for one Google Cloud Virtual IP resource.
- Refer to "Setting up Google Cloud Virtual IP resources" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- Refer to "Setting up Google Cloud load balance monitor resources" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.53.2 Monitor (special) tab



Target Resource

Specifies a name of the target Google Cloud Virtual IP resource.

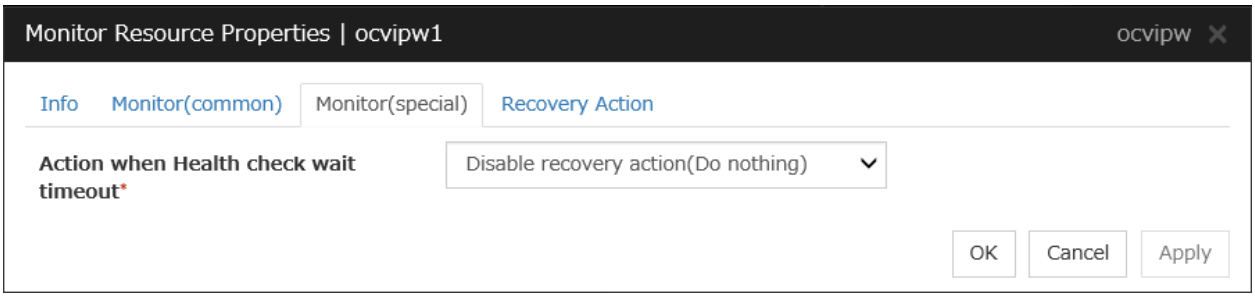
4.54 Understanding Oracle Cloud Virtual IP monitor resources

Oracle Cloud Virtual IP monitor resources perform alive monitoring of nodes running Oracle Cloud Virtual IP resources about control processes which start to run when Oracle Cloud Virtual IP resources become active. If the process does not start properly, the system takes it as an error. Also, timeout on health check wait time may become an error depending on **Action when Health check wait timeout** settings.

4.54.1 Notes on Oracle Cloud Virtual IP monitor resource

- Oracle Cloud Virtual IP monitor resources are added automatically when you add Oracle Cloud Virtual IP resources. One Oracle Cloud Virtual IP monitor resource is created automatically for one Oracle Cloud Virtual IP resource.
- Oracle Cloud Virtual IP monitor resources check if timeout occurs or not on health check wait time in Oracle Cloud Virtual IP resources. Therefore the monitor interval values of Oracle Cloud Virtual IP monitor resources must be larger than the **Health check timeout** values set in the target Oracle Cloud Virtual IP resources.
- Refer to "Oracle Cloud Virtual IP resource settings" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.54.2 Monitor (special) tab



Action when Health check wait timeout

Specifies actions when timeout of health check wait time occurs in Oracle Cloud Virtual IP resources.

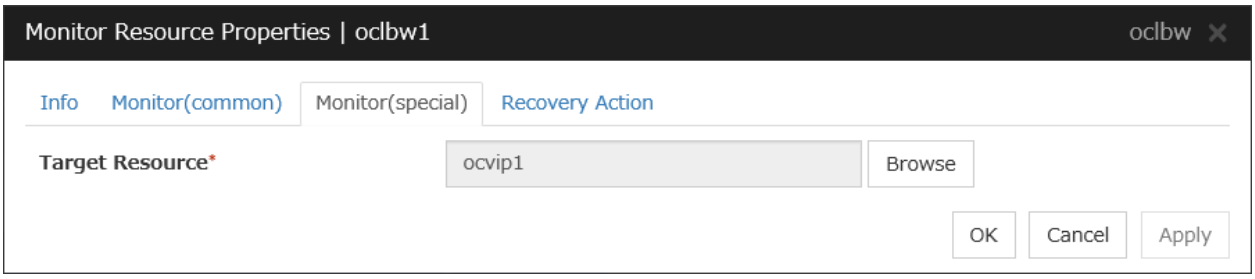
4.55 Understanding Oracle Cloud load balance monitor resources

Oracle Cloud load balance monitor resources perform monitoring of nodes not running Oracle Cloud Virtual IP resources and check if the same port number of the health check port number opens.

4.55.1 Notes on Oracle Cloud load balance monitor resources

- Oracle Cloud load balance monitor resources are added automatically when you add Oracle Cloud Virtual IP resources. One Oracle Cloud load balance monitor resource is created automatically for one Oracle Cloud Virtual IP resource.
- Refer to "Setting up Oracle Cloud Virtual IP resources" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- Refer to "Setting up Oracle Cloud load balance monitor resources" on "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.55.2 Monitor (special) tab



Target Resource

Specifies a name of the target Oracle Cloud Virtual IP resource.

CHAPTER

FIVE

HEARTBEAT RESOURCES DETAILS

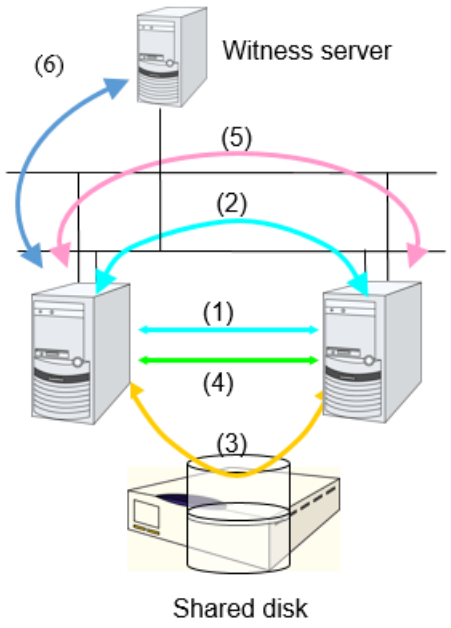
This chapter provides detailed information on heartbeat resources.

This chapter covers:

- 5.1. *What are heartbeat resources?*
- 5.2. *Understanding LAN heartbeat resources*
- 5.3. *Understanding kernel mode LAN heartbeat resources*
- 5.4. *Understanding disk heartbeat resources*
- 5.5. *Understanding COM heartbeat resources*
- 5.6. *Understanding BMC heartbeat resources*
- 5.7. *Understanding Witness heartbeat resources*

5.1 What are heartbeat resources?

A server in a cluster configuration monitors whether the other server is being activated. For this monitoring, heartbeat resources are used.



(1) LAN heartbeat resource dedicated to interconnect
(1) LAN heartbeat resource dedicated to interconnect (kernel mode)
(2) Public LAN heartbeat
(2) Public LAN heartbeat (kernel mode)
(3) Disk heartbeat
(4) COM heartbeat
(5) BMC heartbeat
(6) Witness heartbeat

Heartbeat resource name	Abbreviation	Functional overview
LAN heartbeat resource (1)(2)	lanhb	Uses a LAN to monitor if servers are activated. Used for communication within the cluster as well.
Kernel mode LAN heartbeat resource (1)(2)	lankhb	A kernel mode module uses a LAN to monitor if servers are activated.
Disk heartbeat resource (3)	diskhb	Uses a dedicated partition in the shared disk to monitor if servers are activated.
COM heartbeat resource (4)	comhb	Uses a COM cable connecting two servers to monitor if servers are activated.
BMC heartbeat resource (5)	bmchb	Uses BMC to monitor whether servers are activated.
Witness heartbeat resource (6)	witnesshb	A module uses the Witness server to monitor whether or not servers are active

- At least either one LAN heartbeat resource or one kernel mode LAN heartbeat resource must be configured. It is recommended to set two or more LAN heartbeat resources. It is recommended to set both LAN heartbeat resource and kernel mode LAN heartbeat resource together.
- Please make sure to set 1 or more LAN heartbeats or Kernel mode LAN heartbeats that can communicate among all the servers.
- When you configure the settings of interfaces for disk heartbeat and COM heartbeat resources, follow the specifications described below.

When a shared disk is used:	[Number of servers: up to 2] In principle, COM interface and disk interface [Number of servers: 3 or more] Disk interface
When a shared disk is not used:	[Number of servers: up to 2] COM interface

5.2 Understanding LAN heartbeat resources

5.2.1 LAN heartbeat resources

- You need to set at least one LAN heartbeat resource or kernel mode LAN heartbeat resource. It is recommended to have two or more LAN heartbeat resources; the one dedicated to interconnect and the one shared with interconnect and public.
- Communication data for alert synchronization is transmitted on an interface that is registered with the interconnect. You should consider network traffic when you configure the settings.

5.3 Understanding kernel mode LAN heartbeat resources

5.3.1 Environment where the kernel mode LAN heartbeat resources works

Note: This function is dependent on the distribution and kernel version. Refer to " Supported distributions and kernel versions" in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide" before you configure the settings.

5.3.2 The settings of the kernel mode LAN heartbeat resources

With the kernel mode driver module, kernel mode LAN heartbeat resource offer similar functions that LAN heartbeats provide. The kernel mode LAN heartbeat resources have the following features.

- Kernel mode LAN heartbeat resource is less likely to be impacted by load of OS because it uses the kernel mode driver. This reduces the misinterpreting disconnect of interconnection.
- When used with the keepalive settings to watch user-mode monitor resource, the kernel mode LAN heartbeat resource allows reset to be recorded in other servers when the user mode stalling is detected.

5.3.3 kernel mode LAN heartbeat resources

- It is recommended to specify two or more kernel mode LAN heartbeat resources; the one dedicated to interconnect and the one shared with interconnect and public.

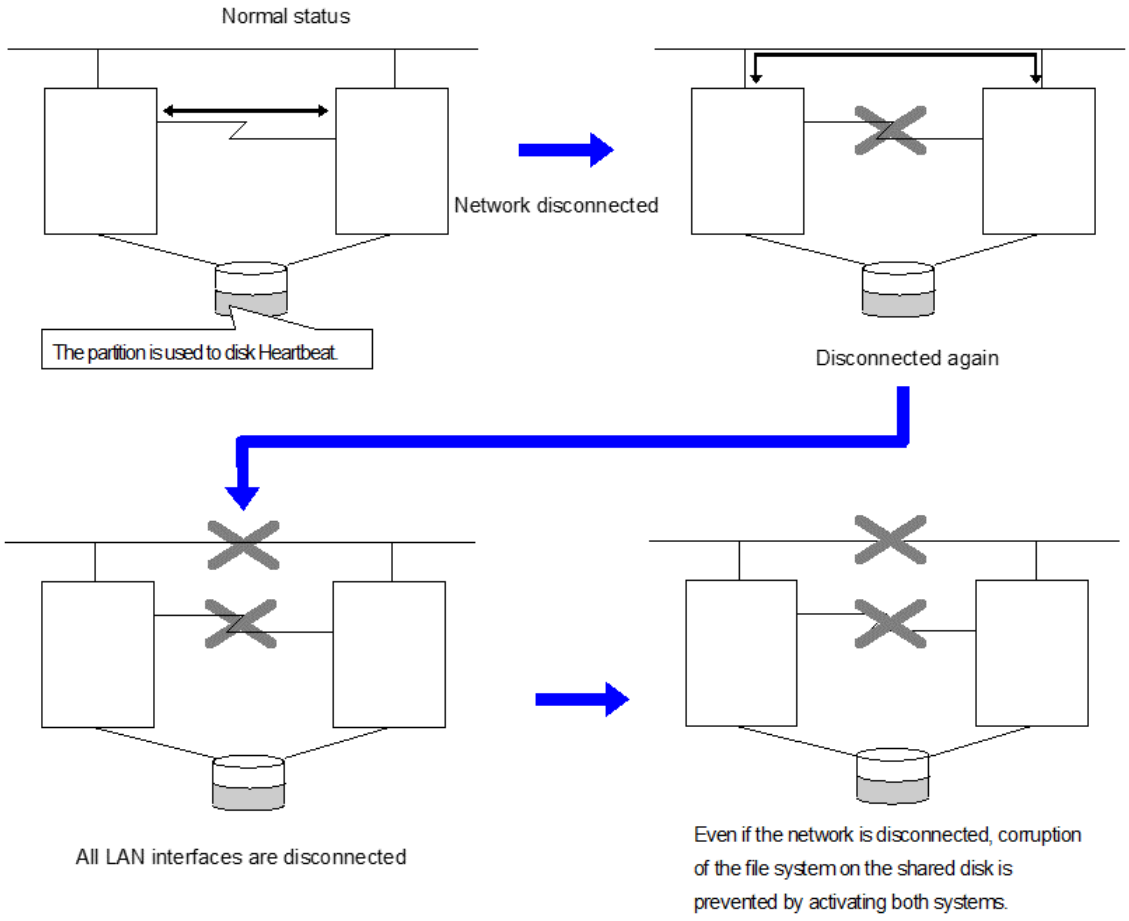
5.4 Understanding disk heartbeat resources

5.4.1 Setting the disk heartbeat resources

To use a heartbeat resource, you need to have the following settings.

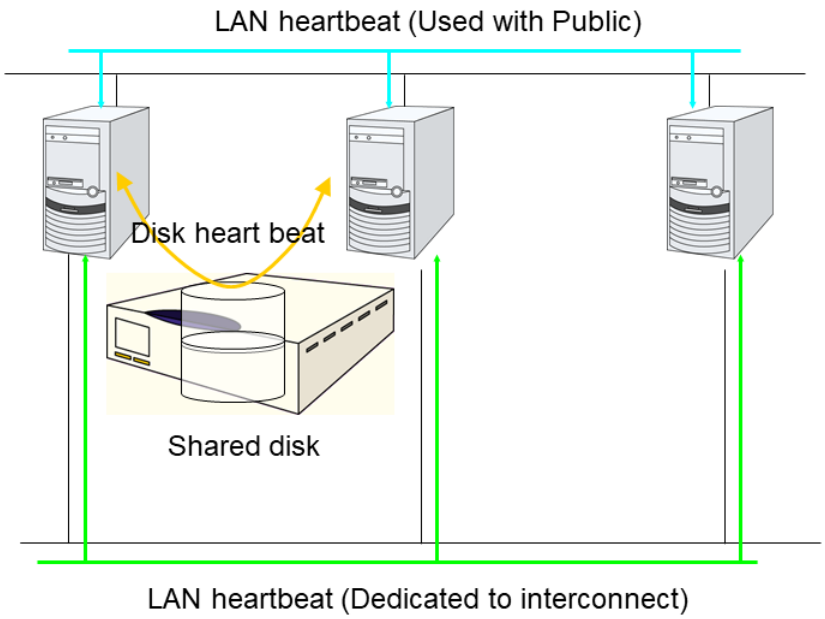
- Allocate a dedicated partition on the shared disk. (You do not need to create any file system.)
- Configure settings that allow all servers to access the dedicated partition on the shared disk by the same device name.

When a disk heartbeat resource is being used, it can be checked if other servers are active even if the network is disconnected.



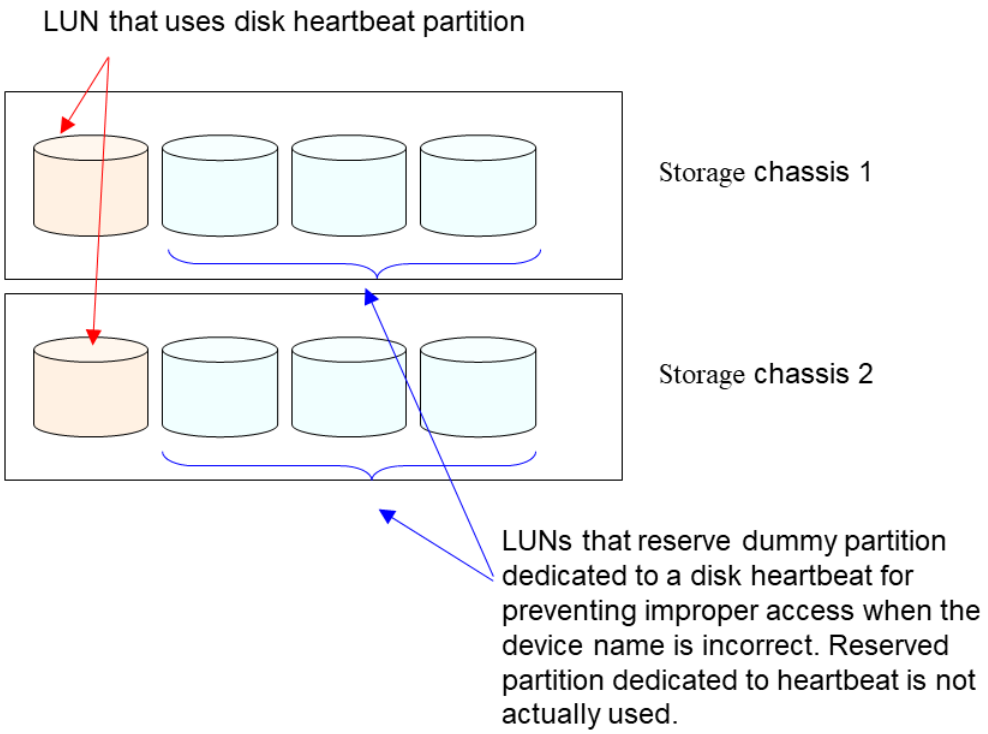
If the cluster consists of three or more servers, you can have a configuration using a disk heartbeat resource as below. You can configure the settings that allow usage of the disk heartbeat resource only among the servers in the cluster using the shared disk.

For details, see "*Interconnect tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.



5.4.2 Disk heartbeat resources

- It is recommended to use both a LAN heartbeat resource and a disk heartbeat resource when you use a shared disk.
- It is recommended to use one or two disk heartbeat resources in the cluster even if you are using two or more LUNs. You should consider how heavy the disk is loaded when you configure the settings because a disk heartbeat resource reads and/or writes to the disk every heartbeat interval.
- In each LUN, allocate a partition dedicated to a disk heartbeat. LUNs that do not use a disk heartbeat should also have a dummy partition because the file system can be damaged if device names are moved due to disk failure or other causes.
  Partitions dedicated to disk heartbeat should have the same number across all the LUNs.



- Do not register to storage pool.

5.5 Understanding COM heartbeat resources

5.5.1 Note on COM heartbeat resources

It is recommended to use a COM heartbeat resource if your environments allows. This is because using a COM heartbeat resource prevents activating both systems when the network is disconnected.

5.6 Understanding BMC heartbeat resources

5.6.1 Notes on BMC heartbeat resources

BMC heartbeat resources provide functions similar to those of the LAN heartbeat resource. BMC heartbeat resources feature the following:

- Activation monitoring is performed with the hardware, and therefore is essentially unaffected by the load on the OS and is less likely to incorrectly recognize the disconnection of interconnects.
- The BMC hardware and firmware must support the BMC heartbeat. For the usable BMC versions, see "Servers supporting Express5800/A1080a" or Express5800/A1040a series -related functions" in "Hardware" in the "Getting Started Guide".

5.7 Understanding Witness heartbeat resources

5.7.1 Settings of the Witness heartbeat resources

To use the Witness heartbeat resources, the following settings are required.

- The communication needs to be available between all the servers using Witness heartbeat resources and the server where the Witness server service operates (Witness server). For the Witness server, refer to "*Witness server service*" in "7. *Information on other settings*".

The Witness heartbeat resources allow to regularly check the server alive information which the Witness server retains. The server alive information is consolidated, which prevents discrepancies with alive information between servers from easily occurring. In addition, by using the HTTP network partition resolution resource as well, "communication disconnection between a local server and Witness server" and "communication disconnection between other servers and Witness server" are distinguished while the Witness heartbeat resources are operated.

5.7.2 Notes on the Witness heartbeat resources

- If spaces are included in cluster names, Witness heartbeat resources do not work correctly. Do not use spaces for cluster names.
- If the Witness server is shared by multiple clusters with overlapped cluster names, the Witness heartbeat resources do not operate normally. Avoid specifying overlapped cluster names.
- In the communication with the Witness server, NIC and a source address are selected according to the OS settings.

CHAPTER

SIX

NETWORK PARTITION RESOLUTION RESOURCES DETAILS

This chapter provides detailed information on network partition resolution resources.

This chapter covers:

- 6.1. *Network partitions*
- 6.2. *Understanding the network partition resolution resources*
- 6.3. *Understanding network partition resolution by PING method*
- 6.4. *Understanding network partition resolution by HTTP method*
- 6.5. *Not resolving network partition*

6.1 Network partitions

Network partitioning status refers to the status where all communication channels have problems and the network between servers is partitioned.
In a cluster system that is not equipped with solutions for network partitioning, a failure on a communication channel cannot be distinguished from an error on a server. This can cause data corruption brought by access from multiple servers to the same resource. EXPRESSCLUSTER, on the other hand, uses resources for network partition resolution to distinguish a failure on a server from network partitioning when a heartbeat from a server is lost. If the lack of heartbeat is determined to be caused by the server's failing, the system performs a failover by activating each resource and rebooting applications on a server running normally. When the lack of heartbeat is determined to be caused by network partitioning, emergency shutdown is executed because protecting data has higher priority over continuity of the operation.

6.2 Understanding the network partition resolution resources

Servers in a cluster monitor other servers by using heartbeat resources. When all heartbeat resources are disconnected or other server is shut down by a server not in a cluster, the network partition is solved using network partition resolution resources. The following network partition resolution resource is provided.

Network partition resolution resources	Abbreviation	Function Overview
PING network partition resolution resource (PING method)	pingnp	A network partition is solved by determining a server that can communicate using the ping command.
HTTP network partition resolution resource (HTTP method)	httpnp	A network partition is solved by determining a server that can communicate, sending HTTP HEAD request to Web server.

If there is only one available LAN on the configuration, set the PING network partition resolution resource or the HTTP network partition resolution resource.

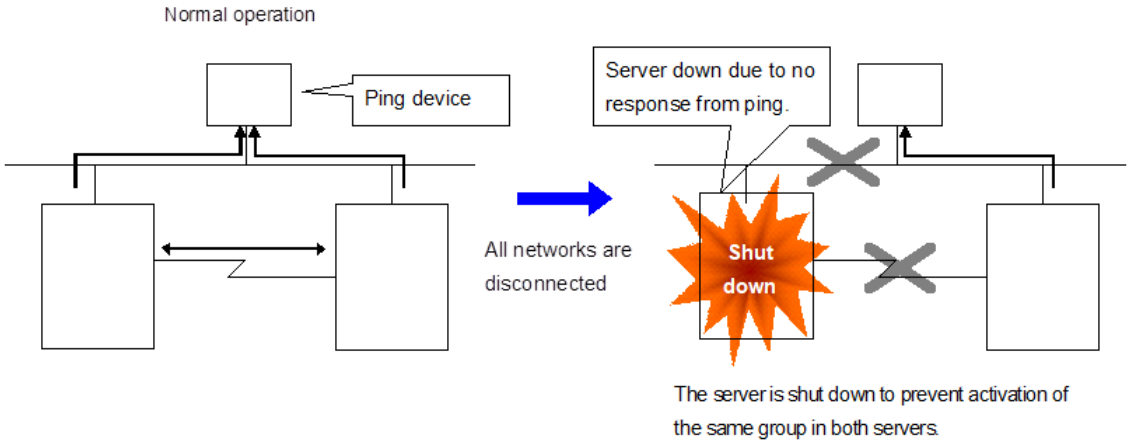
6.3 Understanding network partition resolution by PING method

6.3.1 Settings of the PING network partition resolution resources

To use PING network partition resolution resources, a device that is always active to receive and respond to the ping command (hereafter described as ping device) is required.

When the heartbeat from another server is lost but the ping device is responding to the ping command, the remote server is down. Failover starts.

If there is no response to the ping command, it is determined that the local server is isolated from the network due to network partitioning an action when a network partition occurs is performed.



For details, see "*NP Resolution tab*" in "*Cluster properties*"in "*Parameter details*" in this guide.

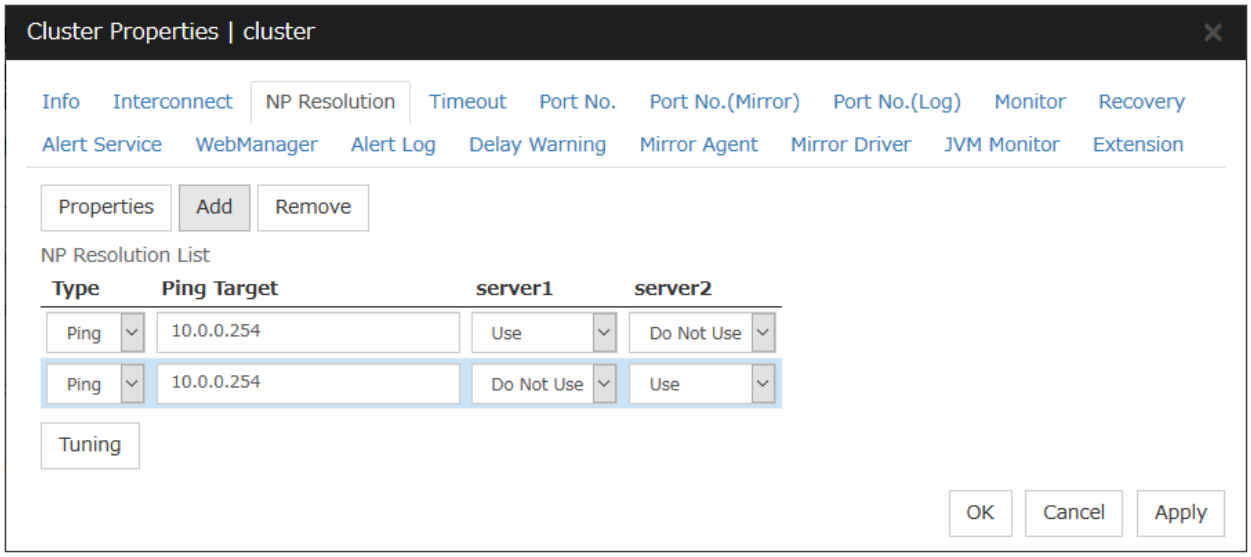
6.3.2 Note on PING network partition resolution resource

When using PING network partition resolution resource, specify addresses which can be sent from and received to through one of the interconnect LANs registered in the configuration information.

In case that response to ping command continues not returning on all the all servers before disconnection of the heartbeat due to ping device failure or other reasons, network partition cannot be resolved. If the heartbeat disconnection is detected in this situation, an action when a network partition occurs is performed on all servers.

It is possible to set **Use** or **Do Not Use** for each server. If **Do Not Use** is set incorrectly, NP resolution processing cannot be performed and a double activation may be detected.

The following is an example of an incorrect setting in which NP resolution processing cannot be performed.



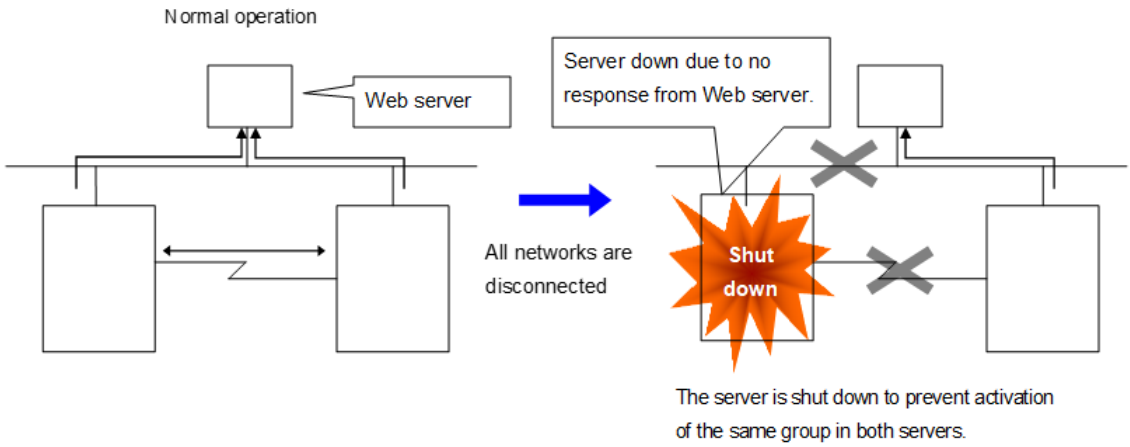
6.4 Understanding network partition resolution by HTTP method

6.4.1 Settings of the HTTP network partition resolution resources

To use the HTTP network partition resolution resources, the following settings are required.

- An all time running server with HTTP communication available (hereafter referred to as Web server) is needed.

When the heartbeat from another server is detected to be stopped, the HTTP network partition resolution resource operates in the following two ways: If there is a response from Web server, it determines it as a failure of another server and executes the failover. If there is no response from Web server, it determines that the network partition status isolated the local server from the network and executes the same operation as when the network partition occurs.



For more information, refer to "*NP Resolution tab*" in "*Cluster properties*" in "*Parameter details*" in this guide.

6.4.2 Note on HTTP network partition resolution resource

In the communication with Web server, NIC and a source address are selected according to the OS settings.

6.5 Not resolving network partition

When this method is selected, network partition resolution is not performed. Therefore, if a failure occurs on all the network channels between servers in a cluster, all servers fail over.

CHAPTER

SEVEN

INFORMATION ON OTHER SETTINGS

This chapter provides the information on the other monitor or notification settings.

This chapter covers:

- 7.1. *Shutdown monitoring*
- 7.2. *Bonding*
- 7.3. *Forced stop*
- 7.4. *Script for forced stop*
- 7.5. *Chassis Identify*
- 7.6. *Alert Service*
- 7.7. *SNMP linkage*
- 7.8. *Cluster service automatic startup prohibition after improper stop*
- 7.9. *Grace period dependence at the automatic failover between server groups*
- 7.10. *Witness server service*

7.1 Shutdown monitoring

7.1.1 Shutdown monitoring

In shutdown monitoring, it is monitored if the OS is stalled when cluster or server shutdown is performed by an EXPRESSCLUSTER command.
If the cluster daemon assumes the OS is stalled, forced reset is executed.

7.1.2 Displaying and changing the shutdown monitoring

- **Performs consistently**
  Shutdown is monitored. The heartbeat (see "5. *Heartbeat resources details*") timeout must be longer than the time required for the OS to shut down, including the applications exiting.
- **Performs only upon the occurrence of a group deactivation failure**
  Shutdowns are monitored only upon the occurrence of a group deactivation failure. The heartbeat timeout (see "5. *Heartbeat resources details*") must be longer than the time required for the OS to shut down, including that needed for the applications to quit.

It is recommended that you set **Performs only upon the occurrence of a group deactivation failure** if you are using shared disks, mirror disks or hybrid disks.

- **Disable**
  Shutdown is not monitored.

7.1.3 Shutdown monitoring method

You can select how to monitor shutdown from:

- Softdog
  For this method, set the timer by using the softdog driver.
- Ipmi
  For this method, set the timer by using OpenIPMI. If OpenIPMI is not installed, you need to install it. For ipmi, see "*Understanding User mode monitor resources*".
- ipmi(High-End Server Option)
  This cannot be used.
- Keepalive
  For this method, set the clpkhb and clpka drivers of EXPRESSCLUSTER are used to set the timer.

Note:

Check the distribution and kernel versions supported by the clpkhb and clpka drivers by referencing Supported distributions and kernel versions"in "Software" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

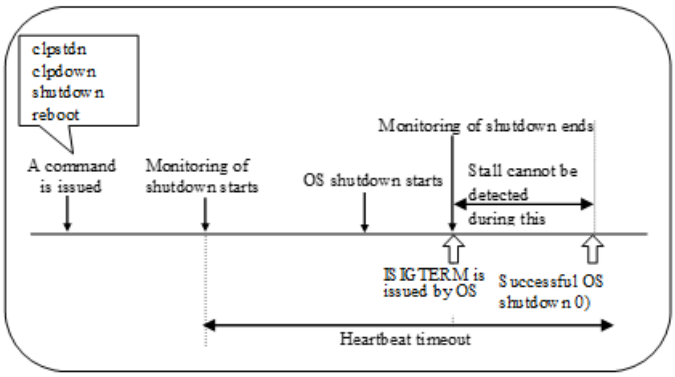
Check them when applying security patches which are released by a distributor to the operating cluster (when the kernel version is changed).

7.1.4 Setting of SIGTERM

SIGTERM is issued when shutting down the OS. The range of shutdown stall monitoring and what will be performed at successful OS shutdown are determined by the setting, "Enable SIGTERM handler." When the monitoring method is set to keepalive, what will be performed is the same as when softdog is set.

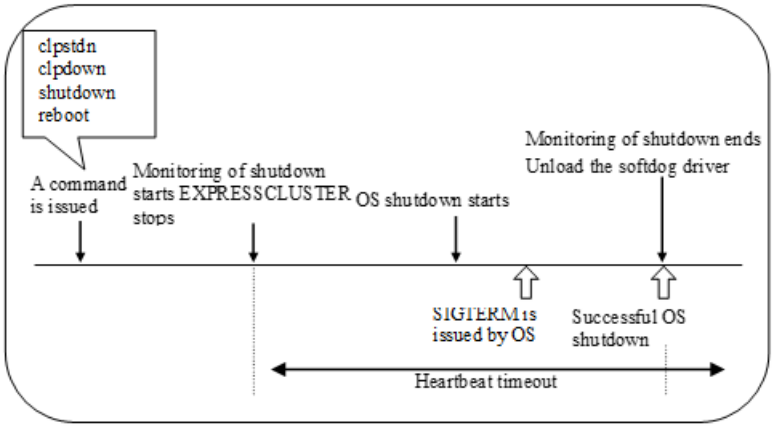
- Monitoring method: softdog

  Successful shutdown (when softdog is selected and SIGTERM is enabled)



When SIGTERM is enabled, the stalled status cannot be detected because monitoring of the shutdown ends if the OS issues SIGTERM during shutdown.

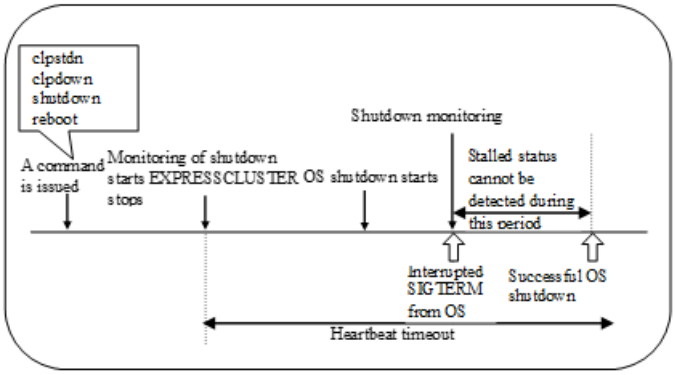
Successful shutdown (when softdog is selected and SIGTERM is disabled)



It is recommended to disable SIGTERM if softdog is selected as a method of monitoring.

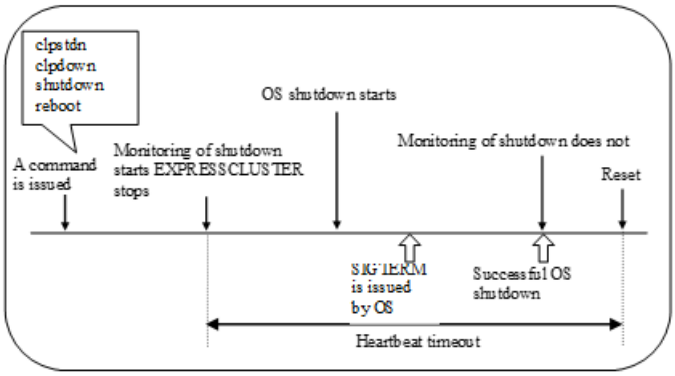
- Monitoring method: ipmi / ipmi(High-End Server Option)

Successful shutdown (when ipmi is selected and SIGTERM is enabled)



When SIGTERM is enabled, the stalled status cannot be detected because monitoring of the shutdown ends if the OS issues SIGTERM during shutdown.

Successful shutdown (when ipmi is selected and SIGTERM is disabled)

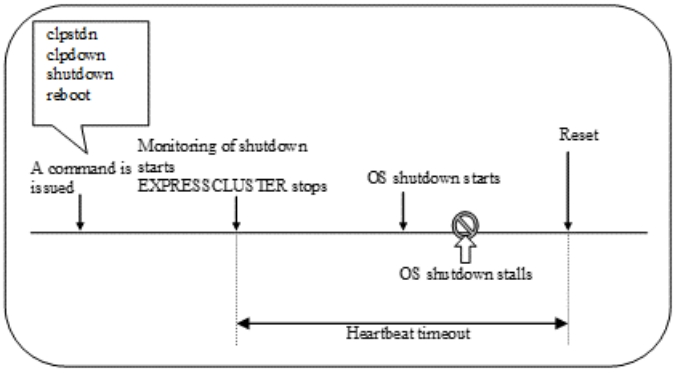


- Even if the shutdown is successful without any stalled status, a server is reset by ipmi.
- On a server that can be powered off by software, reset is not performed.

It is recommended to enable SIGTERM if ipmi is selected as a method of monitoring.

- When a stalled status occurs in OS shutdown.

  When a stalled status in shutdown is detected



7.1.5 Using heartbeat timeout

Use the timeout value for shutdown monitoring with the heartbeat timeout value.

7.1.6 Timeout

Specify the timeout value when the heartbeat timeout value is not used as the timeout value for shutdown monitoring. A value of less than the heartbeat timeout value must be specified to prevent both systems from activating when a failover occurs upon detection of a server down.

7.2 Bonding

7.2.1 Floating IP resource

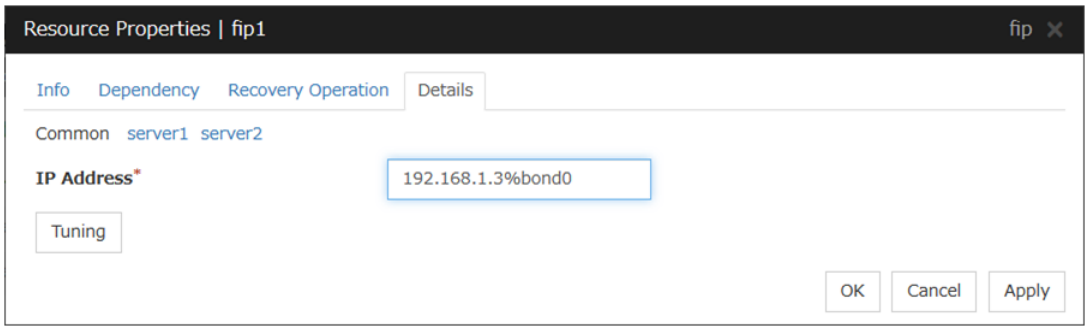
Notes

If you specify "active-backup" to bonding mode, the communication may be temporarily lost when switching slave interfaces.

Bonding setting example

When you configure the settings for FIP resource by the Cluster WebUI, separate the IP address and bonding device with "%" in **Details** tab of **Properties** as described below.

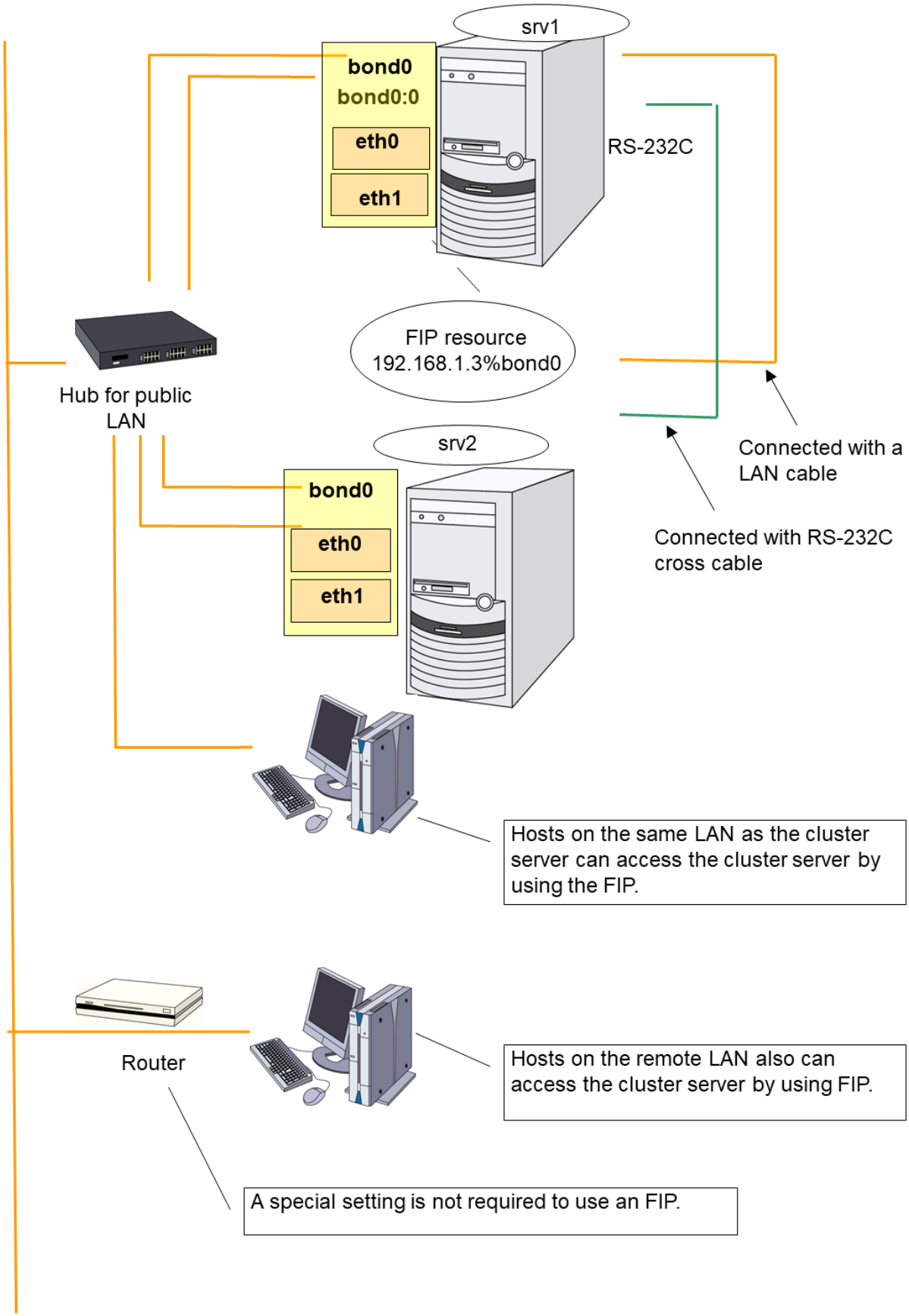
Example: Setting "bond0" as device name, "192.168.1.3" as IP address



Note: For interconnection IP address, specify IP addresses only.

The following shows example settings to use FIP resource on bonding:

Device	Slave	Mode
bond0	eth0 eth1	active-backup(1) balance-tlb(5)
bond0	eth0 eth1	active-backup(1) balance-tlb(5)


srv1
bond0
bond0:0
eth0
eth1
RS-232C
FIP resource
192.168.1.3%bond0
Hub for public
LAN
srv2
bond0
eth0
eth1
Connected with a
LAN cable
Connected with RS-232C
cross cable
Hosts on the same LAN as the cluster server can access the cluster server by using the FIP.
Router
Hosts on the remote LAN also can access the cluster server by using FIP.
A special setting is not required to use an FIP.

When FIP resource is enabled on srv1 by ifconfig: (bonding mode is set to "balance-tlb(5).")

```
$ ifconfig
bond0     Link encap:Ethernet HWaddr 00:00:01:02:03:04
     inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1          (1)
     RX packets:6807errors:0 dropped:0 overruns:0 frame:0
     TX packets:2970errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:670032 (654.3 Kb)  TX bytes:189616 (185.1 Kb)
bond0:0   Link encap:Ethernet HWaddr 00:00:01:02:03:04
     inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.255.0    (2)
     UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
     RX packets:236 errors:0 dropped:0 overruns:0 frame:0
     TX packets:2239 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:78522 (76.6 Kb)  TX bytes:205590 (200.7 Kb)
eth0      Link encap:Ethernet HWaddr 00:00:01:02:03:04
     UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
     RX packets:3434errors:0 dropped:0 overruns:0 frame:0
     TX packets:1494errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:332303 (324.5 Kb)  TX bytes:94113 (91.9 Kb)
     Interrupt:18 Base address:0x2800 Memory:fc041000-fc041038
eth1      Link encap:Ethernet HWaddr 00:00:05:06:07:08
     UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
     RX packets:215 errors:0 dropped:0 overruns:0 frame:0
     TX packets:1627errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:77162 (75.3 Kb)  TX btes:141394 (138.0 Kb)
     Interrupt:19 Base address:0x2840 Memory:fc042000-fc042038
eth2      Link encap:Ethernet HWaddr 00:00:09:10:11:12
     inet addr:192.168.2.1 Bcast:192.168.2.255 Mask: 255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1               (3)
     RX packets:47 errors:0 dropped:0 overruns:0 frame:0
     TX packets:1525 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:2820 (2.7 Kb)  TX bytes:110113 (107.5 Kb)
     Interrupt:24 Base address:0x3000 Memory:fc500000-fc500038
```

1. Device where eth0 and eth1 are bonding.
   Used the public LAN, and 2nd interconnect LAN
2. FIP enabled on bond0
3. Used for the 1st interconnect LAN

7.2.2 Mirror disk connect

Notes

It is not recommended to use a mirror disk connect on bonding because communication may be interrupted temporarily when switching slave interfaces. Depending on the timing of mirroring, mirror recovery may be performed after switching bonding has completed.

An example of bonding setup

The following is an example of setting up bonding on a mirror disk connect:

Cluster Server	Device	Slave	Mode
srv1	bond0	eth1 eth2	balance-rr(0) active-backup(1) balance-tlb(5)
srv2	bond0	eth1 eth2	balance-rr(0) active-backup(1) balance-tlb(5)

7.3 Forced stop

7.3.1 What is Forced stop?

This function forcibly stops the failing server by the another normal server when it is recognized that the server is failing.

This function stops a physical machine by using the IPMI function.

It stops the guest OS on a virtual machine by using the VMware vCenter Server function.

In addition to the functions above, you can execute a script in which the procedure for stopping the failing server is written. For details, refer to "*Script for forced stop*" in "*7. Information on other settings*" in this guide.

7.3.2 Conditions for performing forced stop

- Forced stop is not performed in the following cases:
  - When the failover group successfully stops before the server fails
  - When the server is shut down by the clpdown command, the OS shutdown command or Cluster WebUI and the failover group successfully stops
  - When the cluster is stopped by the clpcl command or Cluster WebUI and the failover group successfully stops
  - When the server fails and there is no failover group to perform failover from the failing server to another server
    (including when the failover group is not activated in the failing server)
- Forced stop is performed in the following case:

– When the server is failing and there is a failover group to perform failover from the failing server to another server

7.3.3 Commands to be used for forced stop

The ipmitool command is used.

Configure the following option values for the command execution on the **BMC** tab of the server properties.

Options for the ipmitool command	Information configured on the BMC tab of the server properties
-H *ip_address*	IP address
-U *username*	User name
-P *password*	Password

When a command line is not specified for **Forced Stop Action** in the BMC tab of the server properties, the following commands are executed.

Forced Stop Action	Parameters
BMC Power Off	ipmitool -H *ip_address* -U *username* -P *password* power off
BMC Reset	ipmitool -H *ip_address* -U *username* -P *password* power reset
BMC Power Cycle	ipmitool -H *ip_address* -U *username* -P *password* power cycle
BMC NMI	ipmitool -H *ip_address* -U *username* -P *password* power diag

If the above commands fail, execute the following commands:

Forced Stop Action	Parameters
BMC Power Off	ipmitool -H *ip_address -I lanplus* -U *username* -P *password* power off
BMC Reset	ipmitool -H *ip_address -I lanplus* -U *username* -P *password* power reset
BMC Power Cycle	ipmitool -H *ip_address -I lanplus* -U *username* -P *password* power cycle
BMC NMI	ipmitool -H *ip_address -I lanplus* -U *username* -P *password* power diag

See "*IPMI command*" in "4. *Monitor resource details*" of "*Monitor resource* " for the options used for the actions.

The vmcontrol command of the VMware vSphere Command Line Interface (vCLI) is used to forcibly stop the guest OS on a virtual machine. This function cannot be used if VMware vSphere Command Line Interface (vCLI) is not installed.

Specify the following option values for the command execution.

Option for the vmcontrol command	Information configured for Virtual Machine Forced Stop Setting on the Extension tab of the cluster properties	Information configured for Input for Virtual Machine name on the Info tab of the server properties
--server *ip_address*	IP address	-
--username *username*	user name	-
--password *password*	password	-
--vmname *virtualmachine*	-	Virtual machine name

The following option is used for action.

Command	Option	Description
vmcontrol	--operation poweroff	Powers off the guest OS on a virtual machine

7.3.4 Specifying the command to be used for forced stop

It is also possible to forcibly stop a physical machine server by specifying an arbitrary command line to be used for the forced stop in **Forced Stop Action** in the BMC tab of the server properties.

To specify the command line, use the following replacement strings so that the setting values of the server properties are applied on the command line.

Replacement string name	Replacement target (Setting item in the BMC tab of the server properties)	Replacement target (Setting item in the forced stop action in the extension tab of the cluster properties)
CLP_BMC_HOST	IP address	-
CLP_BMC_USER	User name	-
CLP_BMC_PASSWORD	Password	-
CLP_BMC_ACTION	-	Forced Stop Action

Characters to be replaced by the replacement string (CLP_BMC_ACTION) for the forced stop action are as follows.

Forced Stop Action	Characters to be replaced by replacement string
BMC Power Off	off
BMC Reset	reset
BMC Power Cycle	cycle
BMC NMI	diag

Note: In the forced stop action, the action to be executed differs depending on whether the replacement string, CLP_BMC_ACTION is specified or not.

- When CLP_BMC_ACTION is included in the command line:
  The action selected in the forced stop action of the cluster properties is executed.
- When CLP_BMC_ACTION is not included in the command line:
  The action selected in the forced stop action of the cluster properties is not applied.

Example of the command specified for the forced stop action by using the replacement strings:

```
ipmitool -H CLP_BMC_HOST -U CLP_BMC_USER -P CLP_BMC_PASSWORD power CLP_BMC_ACTION
```

7.3.5 Displaying and changing the details of forced stop

For the forced stop settings, refer to "*Cluster properties* - *Extension tab*", "*Server properties* - *Info tab*" , and "*Server properties* - *BMC tab*" in "2. *Parameter details*" in this guide.

7.3.6 Notes on the forced stop

- Forcibly stopping the guest OS on a virtual machine
  Only power off operation can be performed. This function cannot be used if communication with VMWare vCenter Server cannot be performed.
- Notes on ipmitool
  See "*IPMI command*" in "4. *Monitor resource details*" of "*Monitor resource*".
- Impacts of forced stop
  When you use the forced stop function, the following functions are influenced because power off, reset, power cycle or NMI is forcibly performed regardless of the OS or server status.
  - Dump collection
    Since it is not recognized that dump files are being collected, power off, reset or power cycle is performed even though dump collection is being performed, so dump collection does not complete.
  - Power on within the heartbeat timeout
    When the server is powered on again for the purpose of maintenance etc. within heartbeat timeout, power off, reset, power cycle or NMI may occur after heartbeat timeout has elapsed.
- BMC network settings
  Configure the settings so that the IP address of the LAN port for BMC management and the IP address which OS uses can communicate with each other. This function cannot be used in the environment where the network for the BMC management is blocked.
  Set the same IP address that is configured in the LAN port for the BMC management to the **BMC** tab of the server properties.
  See the server's manuals etc. for information on how to configure the IP address of the LAN port for the BMC management etc.

7.4 Script for forced stop

7.4.1 What is the script for forced stop?

When it is recognized that the server is failing, any script created by the user can be executed on one of the rest of servers working normally.
The failing server can be stopped forcibly by using the script.
Moreover, using the script enables to check whether the forced stop is successful or unsuccessful and to control whether to execute the failover or not.

7.4.2 Conditions for executing the script for forced stop

- The script for forced stop is not executed when:
  - The failover group successfully stops before the server fails
  - The server is shut down by the clpdown command, the OS shutdown command or Cluster WebUI and the failover group successfully stops
  - The cluster is stopped by the clpcl command or Cluster WebUI and the failover group successfully stops
  - The server fails and there is no failover group to perform failover from the failing server to another server (including when the failover group is not activated in the failing server)
- The script for forced stop is executed when the server is failing and there is a failover group to perform failover from the failing server to another server.

7.4.3 Features of the script for forced stop

Environment variables used in the script for forced stop

EXPRESSCLUSTER stores the data such as the information of a failing server to environment variables.

You can use the following environment variables for branch conditions in the script to describe the procedure tailored to the operations of your system.

Environment variable	Setting value	Description
CLP_SERVER_DOWN ...Down server name	Server name	Specifies the name of the failing server
CLP_SERVER_LOCAL ...Local server name	Server name	Specifies the name of the server where the script is executed.
CLP_VMNAME ...Virtual machine name	Virtual machine name	Specifies the virtual machine name set in the server properties.
CLP_DATACENTER_NAME ...Data center name	Data center name	Specifies the data center name set in the server properties.
CLP_VCENTER_HOST ...Host name for vCenter	Host name	Specifies the host name set in the virtual machine forced stop setting.
CLP_VCENTER_USER ...User name for vCenter	User name	Specifies the user name set in the virtual machine forced stop setting.

Continued on next page

Table 7.10 – continued from previous page

Environment variable	Setting value	Description
CLP_VCENTER_PASSWORD ...Password for vCenter	Password	Specifies the password set in the virtual machine forced stop setting.
CLP_BMC_HOST ...IP address for BMC	IP Address	Specifies the IP address set in the server properties.
CLP_BMC_USER ...User name for BMC	User name	Specifies the user name set in the server properties.
CLP_BMC_PASSWORD ...Password for BMC	Password	Specifies the password set in the server properties.

Return value of the script for forced stop

Return 0 when the script terminates normally.

7.4.4 Displaying and changing the details of the script for forced stop

For the settings of the script for forced stop, refer to "*Extension tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

7.4.5 Notes on the script for forced stop

- Describe the customer-defined process in the script to stop the server.
- When using the script for forced stop, refer to "*Notes on the forced stop* - Impacts on forced stop" of "*Forced stop*" in "*7. Information on other settings*" in this guide.
- When the forced stop function and the script for forced stop is used together, they are executed in the following order.
  1. The forced stop function
  2. The script for forced stop

7.5 Chassis Identify

7.5.1 Chassis identify

This function allows for the other normal server to report the server failure by blinking the chassis ID lamp of a failing server by using the IPMI function when it recognizes that the server is failing

7.5.2 Conditions for chassis ID lamp to blink

- The chassis ID lamp does not blink in the following cases:
  - When the status other than server status becomes abnormal
  - When cluster shutdown is performed
  - When all the servers in the cluster fail
    When the servers do not go down simultaneously, they blink for 250 seconds at the maximum, and eventually the chassis ID lamps of all servers go off.
  - When BMC of the failing server cannot communicate with the normal server
  - When there are normal servers in the cluster but EXPRESSCLUSTER is stopped
- The chassis ID lamp blinks in the following cases (the above conditions for not blinking are given priority over these conditions when they overlap):
  - When some of the servers in the cluster fail due to some abnormality
  - When some of the servers in the cluster are shut down by the shutdown command of the OS.
  - When some of the servers in the cluster are shut down by the clpdown command or Cluster WebUI
  - When EXPRESSCLUSTER is stopped by the clpcl command or Cluster WebUI in some of the servers in the cluster
  - When cluster service automatic startup is off in some of the servers in the cluster
- Chassis ID lamp stops blinking and goes off in the following cases:
  - When there are normal servers in the cluster, and the server status of the failing server returns to normal

7.5.3 Behavior of the chassis ID lamp blinking when the cluster stops

If the chassis ID lamp of a server in the cluster is in the blinking status when the cluster stops, the chassis ID lamp may keep blinking for 250 seconds at the maximum.

7.5.4 Commands to be used for chassis identify

The ipmitool command is used.

If the commands are not installed, this function cannot be used.

Specify the following option values for the command execution in the **BMC** tab of **Server Properties**.

The alarms/ialarms command option	Configured in the BMC tab of the server properties
-N *ip_address*	IP address
-U *username*	Use name
-P *password*	Password

When the command lines are not specified for **Flash** and **Turn off** of the chassis identify lamp in the **BMC** tab of the server properties, the following command is executed.

In case of alarms:

Chassis Identify	Parameters
Flash	ipmitool -H *ip_address* -U *username* -P *password* chassis identify 250
Turn off	ipmitool -H *ip_address* -U *username* -P *password* chassis identify 0

In case of ialarms:

Chassis Identify	Parameters
Flash	ipmitool -H *ip_address* -I lanplus -U *username* -P *password* chassis identify 250
Turn off	ipmitool -H *ip_address* -I lanplus -U *username* -P *password* chassis identify 0

7.5.5 Specifying the command to be used for the chassis identify function

It is also possible to execute the chassis identify function by specifying an arbitrary command line used for the chassis identify function in **Flash** and **Turn off** of the chassis identify lamp in the **BMC** tab of the server properties.

To specify the command line, use the following replacement strings so that the setting values of the server properties are applied to the command line.

replacement strings name	Replacement target (Setting item in the BMC tab of the server properties)
CLP_BMC_HOST	IP address
CLP_BMC_USER	Use name
CLP_BMC_PASSWORD	Password

Example of the chassis identify command specified by using the replacement strings:

ipmitool -H CLP_BMC_HOST -U CLP_BMC_USER -P CLP_BMC_PASSWORD chassis identify 250

7.5.6 Displaying and changing the chassis identify details

For the chassis identify settings, refer to "*Cluster properties* - *Alert Service tab*" and "*Server properties* - *BMC tab*"in "2. *Parameter details*" in this guide.

7.5.7 Notes on Chassis identify

- Notes on ipmitool
  See "*IPMI command*" in "*Monitor resource*" in "4. *Monitor resource details*".
- BMC network settings
  Configure the settings so that the IP address of the LAN port for BMC management and the IP address which OS uses can communicate with each other. This function cannot be used in the environment where the network for the BMC management is blocked.
  Set the same IP address that is configured in the LAN port for the BMC management to the **BMC** tab of the server properties.
  See the server's manuals etc. for information on how to configure the IP address of the LAN port for the BMC management etc.

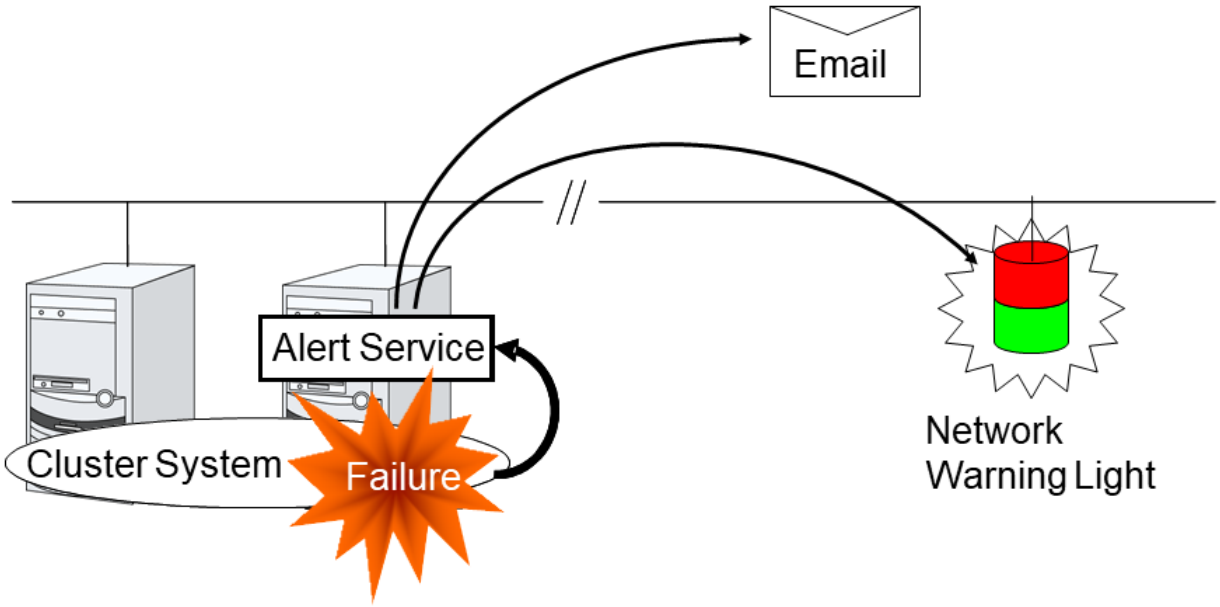
7.6 Alert Service

7.6.1 What is Alert Service?

EXPRESSCLUSTER X Alert Service (hereafter Alert Service) is a function to report failures mentioned above found in EXPRESSCLUSTER-installed cluster systems to system administrators in remote locations.

Failures are reported in three ways, each serving a different purpose.

1. E-mail report
   Alert messages in the Cluster WebUI are sent by e-mail to administrators.
2. Network Warning light
   The network warning light is a visual display of the status of the server. When the server shuts down successfully, the network warning light goes off.
   The e-mail report and the network warning light function work independently of each other.
3. SNMP trap sending
   When a Cluster WebUI alert message is displayed, the contents of the alert are sent with an SNMP trap.



Alert Service allows you to:

- Receive information about failures while not physically located in the same place as the management PC. This is achieved via e-mail reporting function.
- Receive e-mail messages on your mobile phone.
- Visually be alerted of failures by viewing the network warning light.
- Recognize a failure audibly by reproducing the audio file for the network warning light.
- Notify the servers that are configured as the destination of the details of errors by SNMP trap sending.

Mail Report notifies the content of the alert in the following format by e-mail.

Subject:

EXPRESSCLUSTER

Body:

```
Message: Server [down server] has been stopped.
Type: nm
ID: 2
Host: [mail sending source server name]
Date: [send time stamp]
```

7.6.2 Notes on Alert Service

- To use the mail report and network warning light functions, EXPRESSCLUSTER X Alert Service 4.2 for Linux is required.
- The task of Alert Service is to send the first report of failure but not to examine or find the cause of failure. When a failure occurs, instead of using the Alert Service, try other methods, such as viewing EXPRESSCLUSTER logs or syslog, to find out the cause of the error.
- If you use the Linux network warning light function, it may prove necessary to install the rsh package

7.6.3 Mail report actions

- Alert Service sends the same messages as the Cluster WebUI. See "*Messages reported by syslog, alert, mail, and SNMP trap*" in "10. *Error messages*" in this guide for information on which alert messages to be sent.
- You can change the alerts that are reported by e-mail. For more information, see "*Cluster properties - Alert Service tab*" in "2. *Parameter details*" in this guide.

7.6.4 Network Warning Light status

The network warning light performs the following operations.

1. When the server is started
   When the server starts up successfully, warning light changes to green.
2. When the server shuts down
   When the server shuts down successfully, warning light goes off.
3. When the server fails
   When the server fails, its warning light flashes in red. If all servers in the cluster fail, the warning light of the server that failed last will not work because the network warning light is controlled by a normal server that monitors other servers.

Once the network warning light is lit or starts flashing, it will not go off until the cluster shuts down. Run the clplamp command introduced in the following section to put the light out. For more information on the clplamp command, see "*Turning off warning light (clplamp command)*" in "8.2. *EXPRESSCLUSTER commands*" in this *guide*.

For a network warning light (specified by NEC) that supports playback of an audio file, the setting also enables audio file reproduction to link to On/Off.

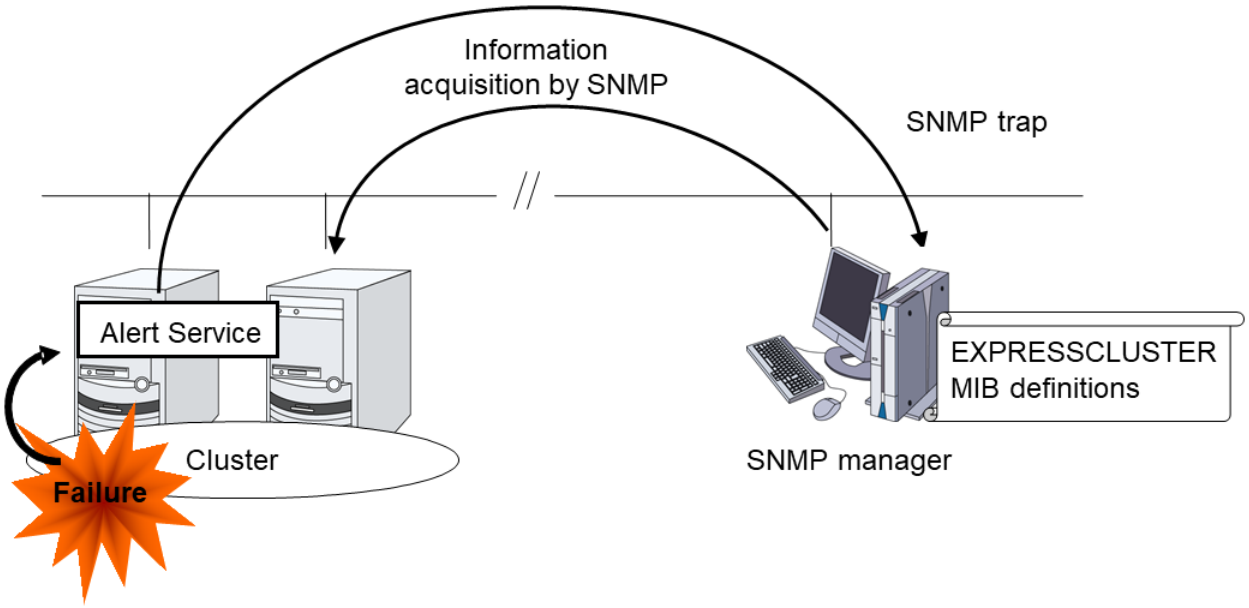
7.6.5 Operations of SNMP trap sending

- The contents of Cluster WebUI alert messages are sent with an SNMP trap. For alert messages subject to SNMP trap sending, see "*Messages reported by syslog, alert, mail, and SNMP trap*" in "10. *Error messages*" in this guide.
- The alerts subject to SNMP trap sending can be changed. For more information, see "*Cluster properties - Alert Service tab*" in "2. *Parameter details*" in this guide.
- For details on the SNMP trap, see "*SNMP trap sending*".

7.7 SNMP linkage

7.7.1 SNMP linkage

SNMP linkage enables SNMP trap sending from EXPRESSCLUSTER and information acquisition by SNMP from an SNMP manager according to the EXPRESSCLUSTER MIB definitions.



7.7.2 EXPRESSCLUSTER MIB definitions

The information sent/acquired with SNMP linkage is configured by the MIB definition files.

To use the functions of SNMP trap sending and information acquisition by SNMP, described later, MIB definition files are required.

To receive SNMP traps from EXPRESSCLUSTER by using an SNMP manager, or to acquire cluster statuses from an SNMP manager, set the EXPRESSCLUSTER MIB definition files in the SNMP manager.

For how to set the MIB definition files in an SNMP manager, refer to the manual for the SNMP manager.

The EXPRESSCLUSTER MIB definition files are placed in the following directory on the EXPRESSCLUSTER X CD-ROM.

<EXPRESSCLUSTER_X_CD-ROM>\Common\<version number>\common\mib

The MIB definition files provide the functions described below.

No.	MIB definition file	Description
1.	NEC-CLUSTER-SMI.mib	Configures the EXPRESSCLUSTER MIB tree root path.
2.	NEC-CLUSTER-EVENT-MIB.mib	Configures the trap and MIB definitions for the EXPRESSCLUSTER SNMP trap sending function.
3.	NEC-CLUSTER-MANAGEMENT-MIB.mib	Configures MIB definitions for the following EXPRESSCLUSTER information: - Cluster information - Server information - Group information

The available functions depend on the files set in the SNMP manager.

To receive SNMP traps from EXPRESSCLUSTER:

1. NEC-CLUSTER-SMI.mib
2. NEC-CLUSTER-EVENT-MIB.mib

To acquire information by SNMP:

1. NEC-CLUSTER-SMI.mib
3. NEC-CLUSTER-MANAGEMENT-MIB.mib

7.7.3 SNMP trap sending

SNMP trap sending serves to send the contents of Cluster WebUI alert messages to the SNMP manager.

To send a trap, the SNMP trap sending destination is required to be configured. Configure it by referring to Destination Settings of SNMP Trap in "*Alert Service tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

The traps to be sent are defined by NEC-CLUSTER-EVENT-MIB.

NEC-CLUSTER-EVENT-MIB defines the following MIB objects.

clusterEventNotifications group

This group defines the traps to be sent. The MIB objects defined for the group function as described below.

No.	SNMP TRAP OID	Description
1.	clusterEventInformation	Trap for information level alerts. A clusterEvent group MIB object is attached.
2.	clusterEventWarning	Trap for warning level alerts. A clusterEvent group MIB object is attached.

Continued on next page

Table 7.16 – continued from previous page

No.	SNMP TRAP OID	Description
3.	clusterEventError	Trap for error level alerts. A clusterEvent group MIB object is attached.

clusterEvent group

This group defines the information appended to the traps. The MIB objects defined for the group function as described below.

No.	SNMP OID	Description
1.	clusterEventMessage	Indicates the alert message.
2.	clusterEventID	Indicates the event ID.
3.	clusterEventDateTime	Indicates the time at which the alert originated.
4.	clusterEventServerName	Indicates the server from which the alert originated.
5.	clusterEventModuleName	Indicates the module from which the alert originated.

7.7.4 Information acquisition by SNMP

By using the SNMP protocol, some information about the EXPRESSCLUSTER configuration and status can be acquired. However, EXPRESSCLUSTER does not include SNMP agent functions. For an SNMP agent, the Net-SNMP snmpd daemon needs to be implemented separately.

SNMP agent

The SNMP agent serves to return a response about the configuration information or status information (GetResponse) to information acquisition requests (GetRequest, GetNextRequest) from an SNMP manager (network management software).

Note: To use information acquisition by SNMP, you must take the steps described in "Setting up the SNMP linkage function" in the "Installation and Configuration Guide".

7.7.5 MIB objects acquirable with SNMP linkage

The MIB objects that can be acquired with the SNMP linkage function are defined by NEC-CLUSTER-MANAGEMENT-MIB.

NEC-CLUSTER-MANAGEMENT-MIB defines the following MIB objects.

clusterGeneral group

This group is used to acquire cluster information. The MIB objects defined for the group function as described below.

No.	SNMP OID	Description
1.	clusterName	Indicates the name of the cluster.
2.	clusterComment	Indicates the comment of the cluster.

3.	clusterStatus	Indicates the current statust of the cluster.
		The correspondence between the MIB value and the Cluster WebUI status is as described below.
		`MIB value status`
		`----------`
		`normal Normal`
		`caution Caution`
		`error Error`
		`unknown -`

clusterServer group

This group is used to acquire server information. Indexes on acquisition of clusterServerTable are sorted by server priority. The MIB objects defined for the group function as described below.

No.	SNMP OID	Description
1.	clusterServerLocalServerIndex	Indicates the index of the server receiving the present SNMP information acquisition request (clusterServerIndex).
2.	clusterServerTable	Indicates the information table for the server.
3.	clusterServerEntry	Indicates the server information list. The index for the list is clusterServerIndex.
4.	clusterServerIndex	Indicates the index for uniquely identifying the server.
5.	clusterServerName	Indicates the name of the server.
6.	clusterServerComment	Indicates a comment for the server.

Continued on next page

Table 7.19 – continued from previous page

No.	SNMP OID	Description

7.	clusterServerStatus	Indicates the current status of the server.
		The correspondence between the MIB value and the Cluster WebUI status is as described below.
		`MIB value Group type`
		`------------------------------`
		`failover Failover group`
		`cluster Management group`
		`virtualMachine Virtual machine group`
		Values other than those indicated above may be acquired depending on the status of the server.

8.	clusterServerPriority	Indicates the priority of the server.
9.	clusterServerProductName	Indicates the name of the EXPRESSCLUSTER product installed on the server.
10.	clusterServerProductVersion	Indicates the version of the EXPRESSCLUSTER product installed on the server.
11.	clusterServerProductInstallPath	Indicates the installation path of EXPRESSCLUSTER on the server.
12.	clusterServerPlatformName	Indicates the name of the platform on the server.

clusterGroup group

This group is used to acquire group information. The MIB objects defined for the group function as described below.

No.	SNMP OID	Description
1.	clusterGroupTable	Indicates the information table for the group.
2.	clusterGroupEntry	Indicates the group information list. The index for the list is clusterGroupIndex.
3.	clusterGroupIndex	Indicates the index for uniquely identifying the group.
4.	clusterGroupName	Indicates the name of the group.
5.	clusterGroupComment	Indicates a comment for the group.

Continued on next page

Table 7.20 – continued from previous page

No.	SNMP OID	Description
6.	clusterGroupType	Indicates the type of the group. The correspondence between the MIB value and the group type is as described below. MIB value / Group type failover / Failover group cluster / Management group virtualMachine / Virtual machine group
7.	clusterGroupStatus	Indicates the current status of the group. The correspondence between the MIB value and the Cluster WebUI status is as described below. MIB value / status online / Online onlineFailure / Online Failure offlineFailure / Offline Failure offline / Offline unknown / Unknown onlinePending / Online Pending offlinePending / Offline Pending
8.	clusterGroupCurrentServerIndex	Indicates the index of the server on which the group is currently active (clusterServerIndex). The return value of a deactivated group is -1.

7.8 Cluster service automatic startup prohibition after improper stop

7.8.1 Cluster service automatic startup prohibition

This function prohibits the EXPRESSCLUSTER service from automatically starting up at the next OS activation after the cluster has been shut down, reboot, or stopped by Cluster WebUI or the EXPRESSCLUSTER service has been stopped by using a command other than the clpstdn command and the clpcl -t -a command.

When the automatic startup prohibition setting is enabled, the EXPRESSCLUSTER service will not automatically start at the next server activation after the cluster has been shut down, reboot, or stopped by Cluster WebUI or the EXPRESSCLUSTER service has been stopped by using a command other than the clpstdn command and the clpcl -t -a command.

Even in cases where cluster shutdown or cluster stop is executed, if an error occurs in the EXPRESSCLUSTER service stop sequence, or if the stop sequence is not executed due to the likes of an OS reset or a power interruption, the EXPRESSCLUSTER service will not automatically start at the next OS activation.

7.8.2 Displaying and changing the automatic startup prohibition setting

- **Cluster service's not stop normal, prohibit automatic startup**
  Prohibits cluster service automatic startup at the next OS activation if the servers are stopped by a means other than cluster shutdown or cluster stop, or if the cluster shutdown or stop sequence does not finish successfully.
- **Not prohibit cluster service automatic startup after improper stop**
  Does not prohibit cluster service automatic startup.

7.8.3 Conditions for automatic startup prohibition

The conditions for automatic startup prohibition are as described below.

- The cluster is stopped by a means other than cluster shutdown or cluster stop.
- The cluster service stop sequence is not executed due to a reason such as an OS reset, panic, or power interruption.
- Group deactivation fails in the cluster service stop sequence as a result of cluster shutdown or stop.
- The cluster is stopped on one of the servers comprising the cluster.

7.8.4 Notes on automatic startup prohibition

- At OS activation, if the EXPRESSCLUSTER service does not start automatically, activate the EXPRESSCLUSTER service by using Cluster WebUI or the clpcl command.
- At OS activation, if the EXPRESSCLUSTER service does not start automatically, Cluster WebUI alert messages and syslog messages are output.

7.9 Grace period dependence at the automatic failover between server groups

7.9.1 What is the grace period dependence?

One server group waits specified time for the other server group to start failover when the automatic failover is executed between server groups. When the grace period elapsed after the server down was detected, the failover is executed.

7.9.2 Condition for the grace period dependence

One server group waits for the other server group with any of the following configurations to start the failover.

- **Use Server Group settings** in the **Info** tab is selected.
- Multiple server groups are specified for **Server Groups that can run the Group** in the **Startup Server t**ab.
- **Prioritize server group failover policy** is selected and **Enable only manual failover among the server group** is not selected for **Auto Failover** of **Failover Attribute** in the **Attribute** tab.

In the following cases, one server group does not wait specified time for the other server group to start failover:

- One server executes the failover to another server within the same server group.
- The server down is detected by the server down notification.

- The script for forced stop is successfully executed while **Execute Script for Forced Stop** is selected, or the condition not to execute the script for forced stop is met.
- The forced stop is successfully executed while **Execute Script for Forced Stop** is not selected and **Use Forced Stop** is selected, or the condition not to execute the forced stop is met.
- The NP resolution resource is configured.

7.9.3 Displaying and changing the grace period dependence

Specify the waiting time fo**r Grace period of server group failover policy**.

If 0 is specified, one server group does not wait for the other server group to start failover.

7.9.4 Notes on the grace period dependence

If any operation is done for the failover target group while the other server group waits during the grace period, the settings to wait during the grace period is cancelled and the other server group does not failover.

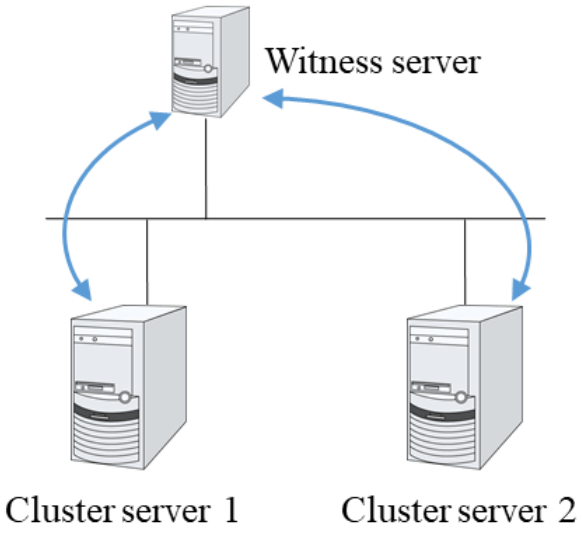
If the once-failed server is detected to be alive while the other server waits during the grace period, the settings to wait during the grace period is cancelled and the failover is not executed.

If the failover target server goes down, the failover may start later than when the grace period ends.

7.10 Witness server service

7.10.1 What is Witness server service?

Witness service is the service to receive Witness heartbeat from each server in the cluster and send back the status information of receiving the heartbeat from each server as a response. It is installed in a server outside of the cluster.



7.10.2 Notes on Witness server service

- Witness server service operates in Node.js environment. Therefore, Node.js needs to be installed before the installation of the Witness server service.

7.10.3 Operation verified environment for Witness server service

Its operation has been verified in the following environments.

OS	Requirement	Version
Windows Server 2012 R2	Node.js 10.13.0	4.1.0
Red Hat Enterprise Linux 7 update4	Node.js 8.12.0	4.1.0

7.10.4 How to install Witness server service

Install the Witness server service by using npm command for Node.js environment. Store the Witness server service module in an arbitrary folder, and execute the following command.

> npm install --global clpwitnessd-<version>.tgz

7.10.5 How to configure Witness server service

To change the settings of Witness server service, edit the configuration file directly. Open the folder indicated in the first row of the execution results of the command below.

> npm list --global clpwitnessd

Example of execution results:

```
C:\Users\Administrator\AppData\Roaming\npm
`-- clpwitnessd@4.1.0
```

Edit clpwitnessd.conf.js that is stored in node_modules\clpwitnessd under the opened folder, with a text editor such as notepad.

Setting items are as follows.

Item	Default	Description
http.enable	True	Specify whether to execute HTTP server or not. true: execute false: not execute
http.port	80	Specify the wait port number for HTTP server.
http.keepalive	10000	Specify the keep alive time for HTTP server in milliseconds.
https.enable	False	Specify whether to execute HTTPS server or not. true: execute false: not execute
https.port	443	Specify the wait port number for HTTPS server.

Continued on next page

Table 7.22 – continued from previous page

Item	Default	Description
https.keepalive	10000	Specify the keep alive time for HTTPS server in milliseconds.
https.ssl.key	server_key.pem	Specify a secret key file to be used for HTTPS server.
https.ssl.crt	server_crt.pem	Specify a certification file to be used for HTTPS server.
log.directory	-	Specify the log output destination folder.
log.level	info	Specify the log output level. error: Only error logs are output. warn: Error logs and warning logs are output. info: Warning logs and information logs are output. debug: Information logs and detailed logs are output.
log.size	1024 * 1024 * 512	Specify the log rotation size in bytes.
data.available	10000	Specify the default time limit for the communication status information of the cluster server in milliseconds.

7.10.6 How to execute Witness server service

Excute the following command to start up Witness server service in the fore ground. For how to execute the Witness server service as Windows service or Linux daemon, refer to the following section, "*Using Witness server service as the OS service*".

> clpwitnessd

7.10.7 Using Witness server service as the OS service

If you want to start Witness server service at the OS startup, the Witness server service requires to be registered as the OS service.

The following exemplifies how to register Witness server service as the OS service (in case of Windows service control manager and Linux systemd). The method of registration for the OS service differs depending on the environment. Configure the registration to suit your environment by referring to the explanation below.

Registration for Windows service control manger

The following exemplifies the procedure to register by using npm package winser.

1. Install winser by npm command. Use the following command so that winser package is downloaded from npm repository and then installed.

   > npm install --global winser

2. Create a folder to execute the service in any location. By default, this folder stores log files, SSL secret key file and SSL certificate file.

3. Create package.json file for the service registration with winser, under the folder created in the above step 2. Enter " \\ " to separate the characters of the path. The path specified for "start" is line-fed for the convenience of character numbers but actually is in one row.

```
{
  "name": "clpwitnessd-service",
  "version": "1.0.0",
  "license": "UNLICENSED",
  "private": true,
  "scripts": {
    "start": "C:¥¥Users¥¥Administrator¥¥AppData¥¥Roaming¥¥npm¥¥clpwitnessd.cmd"
  }
}
```

4. Execute winser command to register and start the Witness server service.

   > winser -i -a

5. Select **Control Panel** -> **Administration Tools** -> **Service**, and confirm that the service (ex. clpwitnessd-service) with the name specified for "name" of pacage.json has been registered.

Registration for Linux systemd

The following exemplifies the procedure to register by creating the unit file of systemd.

1. Create a directory to execute the service in any location. By default, this folder stores log files, SSL secret key file and SSL certificate file.
   (ex. /opt/clpwitnessd) (ex. /opt/clpwitnessd)

2. Create the unit file of the Witness server service in /etc/systemd/system.
   (ex. clpwitnessd.service) (ex. clpwitnessd.service)

```
[Unit]
Description=CLUSTERPRO Witness Server
After=syslog.target network.target
[Service]
Type=simple
ExecStart=/usr/bin/clpwitnessd
WorkingDirectory=/opt/clpwitnessd
KillMode=process
Restart=always
[Install]
WantedBy=multi-user.target
```

3. Execute systemctl command to register and start the Witness server service.

   # systemctl enable clpwitnessd

   # systemctl start clpwitnessd

CHAPTER

EIGHT

EXPRESSCLUSTER COMMAND REFERENCE

This chapter describes commands that are used on EXPRESSCLUSTER.

This chapter covers:

- 8.1. *Operating the cluster from the command line*
- 8.2. *EXPRESSCLUSTER commands*
- 8.3. *Displaying the cluster status (clpstat command)*
- 8.4. *Operating the cluster (clpcl command)*
- 8.5. *Shutting down a specified server (clpdown command)*
- 8.6. *Shutting down the entire cluster (clpstdn command)*
- 8.7. *Operating groups (clpgrp command)*
- 8.8. *Collecting logs (clplogcc command)*
- 8.9. *Changing, backing up, and checking cluster configuration data (clpcfctrl command)*
- 8.10. *Adjusting time-out temporarily (clptoratio command)*
- 8.11. *Modifying the log level and size (clplogcf command)*
- 8.12. *Managing licenses (clplcnsc command)*
- 8.13. *Locking disk I/O (clproset command)*
- 8.14. *Mirror-related commands*
- 8.14.1. *Displaying the mirror status (clpmdstat command)*
- 8.14.2. *Operating mirror disk resource (clpmdctrl command)*
- 8.14.3. *Initializing mirror disks (clpmdinit command)*
- 8.15. *Hybrid-disk-related commands*
- 8.15.1. *Displaying the hybrid disk status (clphdstat command)*
- 8.15.2. *Operating hybrid disk resource (clphdctrl command)*
- 8.15.3. *Initializing hybrid disks (clphdinit command)*
- 8.16. *Outputting messages (clplogcmd command)*
- 8.17. *Controlling monitor resources (clpmonctrl command)*
- 8.18. *Controlling group resources (clprsc command)*
- 8.19. *Controlling reboot count (clpregctrl command)*

- 8.20. *Turning off warning light (clplamp command)*
- 8.21. *Controlling CPU frequency (clpcpufreq command)*
- 8.22. *Controlling chassis identify lamp (clpledctrl command)*
- 8.23. *Processing inter-cluster linkage (clptrnreq command)*
- 8.24. *Requesting processing to cluster servers (clprexec command)*
- 8.25. *Changing BMC information (clpbmccnf command)*
- 8.26. *Controlling cluster activation synchronization wait processing (clpbwctrl command)*
- 8.27. *Estimating the amount of resource usage (clpprer command)*
- 8.28. *Checking the process health (clphealthchk command)*
- 8.29. *Controlling the rest point of DB2 (clpdb2still command)*
- 8.30. *Controlling the rest point of MySQL (clpmysqlstill command)*
- 8.31. *Controlling the rest point of Oracle (clporclstill command)*
- 8.32. *Controlling the rest point of PostgreSQL (clppsqlstill command)*
- 8.33. *Controlling the rest point of SQL Server (clpmssqlstill command)*
- 8.34. *Controlling the rest point of Sybase (clpsybasestill command)*
- 8.35. *Displaying the cluster statistics information (clpperfc command)*
- 8.36. *Checking the cluster configuration information (clpcfchk command)*

8.1 Operating the cluster from the command line

EXPRESSCLUSTER provides various commands to operate a cluster by the command line. These commands are useful for things like constructing a cluster or when you cannot use the Cluster WebUI. You can perform greater number of operations using the command line than Cluster WebUI.

Note: When you have configured a group resource (examples: disk resource and exec resource) as a recovery target in the settings of error detection by a monitor resource, and the monitor resource detects an error, do not perform the following actions by commands related to the actions or by the Cluster WebUI while recovery (reactivation -> failover -> final action) is ongoing.

- terminate/suspend the cluster
- start/terminate/migrate a group

If you perform the actions mentioned above against the cluster while the recovery caused by detection of an error by a monitor resource is ongoing, other group resources of that group may not terminate. However, you can perform these actions as long as the final action has been executed, even if a monitor resource detected an error.

Important: The installation directory contains executable-format files and script files that are not listed in this guide. Do not execute these files by programs or applications other than EXPRESSCLUSTER. Any problems caused by not using EXPRESSCLUSTER will not be supported.

8.2 EXPRESSCLUSTER commands

Commands for configuring a cluster

Command	Description	Page
clpcfctrl	Distributes configuration data created by the Cluster WebUI to servers. Backs up the cluster configuration data to be used by the Cluster WebUI.	8.9.
clplcnsc	Manages the product or trial version license of this product.	8.12.
clpcfchk	Checks the cluster configuration data.	8.36.

Commands for displaying status

Command	Description	Page
clpstat	Displays the cluster status and configuration information.	8.3.
clphealthchk	Check the process health.	8.28.

Commands for cluster operation

Command	Description	Page
clpcl	Starts, stops, suspends, or resumes the EXPRESSCLUSTER daemon.	8.4.
clpdown	Stops the EXPRESSCLUSTER daemon and shuts down the server.	8.5.
clpstdn	Stops the EXPRESSCLUSTER daemon across the whole cluster and shuts down all servers.	8.6.
clpgrp	Starts, stops, or moves groups. This command also migrates the virtual machine.	8.7.
clptoratio	Extends or displays the various time-out values of all servers in the cluster.	8.10.
clproset	Modifies and displays I/O permission of a shared disk partition device.	8.13.
clpmonctrl	Controls monitor resources.	8.17.
clpregctrl	Displays or initializes the reboot count on a single server.	8.19.
clprsc	Stops or resumes group resources	8.18.
clpcpufreq	Controls CPU frequency.	8.21.
clpledctrl	Controls the chassis identify function.	8.22.
clptrnreq	Requests a server to execute a process.	8.23.
clprexec	Requests that an EXPRESSCLUSTER server execute a process from external monitoring.	8.24.
clpbmccnf	Changes the information on BMC user name and password.	8.25.
clpbwctrl	Controls the cluster activation synchronization wait processing.	8.26.

Log-related commands

Command	Description	Page
clplogcc	Collects logs and OS information.	8.8.
clplogcf	Modifies and displays a configuration of log level and the file size of log output.	8.11.
clpperfc	Displays the cluster statistics data about groups and monitor resources.	8.35.

Script-related commands

Command	Description	Page
clplogcmd	Writes texts in the exec resource script to create a desired message to the output destination	8.16.

Mirror-related commands (when the Replicator is used)

Command	Description	Page
clpmdstat	Displays a mirroring status and configuration information.	8.14.1.
clpmdctrl	Activates/deactivates a mirror disk resource, or recovers mirror. Displays or modifies the maximum number of the request queues.	8.14.2.
clpmdinit	Initializes the cluster partition of a mirror disk resource. Creates a file system on the data partition of a mirror disk resource.	8.14.3.

Hybrid disk-related commands (when the Replicator DR is used)

Command	Description	Page
clphdstat	Displays the hybrid disk status and configuration information.	8.15.1.
clphdctrl	Activates/deactivates a hybrid disk resource, or recovers mirror. Displays or modifies the maximum number of the request queues.	8.15.2.
clphdinit	Initializes the cluster partition of a hybrid disk resource.	8.15.3.

System monitor-related commands (when the System Resource Agent is used)

Command	Description	Page
clpprer	Estimates the future value from the tendency of the given resource use amount data.	8.27.

DB rest point-related commands

Command	Description	Page
clpdb2still	Controls the securing/release of the rest point of DB2.	8.29.

Continued on next page

Table 8.9 – continued from previous page

Command	Description	Page
clpmysqlstill	Controls the securing/release of the rest point of MySQL.	8.30.
clporclstill	Controls the securing/release of the rest point of Oracle.	8.31.
clppsqlstill	Controls the securing/release of the rest point of PostgreSQL.	8.32.
clpmssqlstill	Controls the securing/release of the rest point of SQL Server.	8.33.
clpsybasestill	Controls the securing/release of the rest point of Sybase.	8.34.

Other commands

Command	Description	Page
clplamp	Lights off the warning light of the specified server.	8.20.

8.3 Displaying the cluster status (clpstat command)

the clpstat command displays cluster status and configuration information.

Command line

clpstat -s [--long] [-h *hostname*]
clpstat -g [-h *hostname*]
clpstat -m [-h *hostname*]
clpstat -n [-h *hostname*]
clpstat -p [-h *hostname*]
clpstat -i [--detail] [-h *hostname*]
clpstat --cl [--detail] [-h *hostname*]
clpstat --sv [*server_name*] [--detail] [-h *hostname*]
clpstat --hb [*hb_name*] [--detail] [-h *hostname*]
clpstat --np [*np_name*] [--detail] [-h *hostname*]
clpstat --svg [*servergroup_name*] [--detail] [-h *hostname*]
clpstat --grp [*group_name*] [--detail] [-h *hostname*]
clpstat --rsc [*resource_name*] [--detail] [-h *hostname*]
clpstat --mon [*monitor_name*] [--detail] [-h *hostname*]
clpstat --xcl [*xclname*] [--detail] [-h *hostname*]
clpstat --local

Description

This command line displays a cluster status and configuration data.

Option

-s

No option
Displays a cluster status.

--long
Displays a name of the cluster name and resource name until the end.

-g
Displays a cluster group map.

-m
Displays status of each monitor resource on each server.

-n
Displays each heartbeat resource status on each server.

-p
Displays the status of network partition resolution resource on each server.

-i
Displays the configuration information of the whole cluster.

--cl
Displays the cluster configuration data. Displays the Mirror Agent information as well for the Replicator, Replicator DR.

--sv [server_name]
Displays the server configuration information. By specifying the name of a server, you can display information of the specified server.

--hb [hb_name]
Displays heartbeat resource configuration information. By specifying the name of a heartbeat resource, you can display only the information on the specified heartbeat.

--np [np_name]
Displays network partition resolution resource configuration information. By specifying the name of a network partition resolution resource, you can display only the information on the specified network partition resolution resource.

--svg [servergroup_name]
Displays server group configuration information. By specifying the name of a server group, you can display only the information on the specified server group.

--rsc [resource_name]
Displays group resource configuration information. By specifying the name of a group resource, you can display only the information on the specified group resource.

--mon [monitor_name]
Displays monitor resource configuration information. By specifying the name of a monitor resource, you can display only the information on the specified resource.

--xcl [xclname]
Displays configuration information of exclusion rules.By specifying exclusion rule name, only the specified exclusion name information can be displayed.

--detail
Displays more detailed information on the setting.

-h hostname
Acquires information from the server specified with *hostname*. Acquires information from the command running server (local server) when the -h option is omitted.

--local
Displays the cluster status. This option displays the same information when -s option is specified or when no option is specified. However, this option displays only information of the server on which this command is executed, without communicating with other servers.

Return Value
When the -s option is not specified

0	Success
9	The command was run duplicatedly.
Other than the above	Failure

Remarks

According to the combination of options, configuration information shows information in various forms.

Notes

- Run this command as the root user.
- The cluster daemon must be activated on the server where you run this command.
- When you specify the name of a server for the -h option, the server should be in the cluster.
- For the language used for command output, see "*Cluster properties - Info tab*" in "2. *Parameter details*" in this guide.
- When you run the clpstat command with the -s option or without any option, names such as a cluster or a resource will not be displayed halfway.

Example of Execution

Examples of information displayed after running these commands are provided in the next topic.

Error Messages

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid configuration file. Create valid cluster configuration data.	Create valid cluster configuration data by using the Cluster WebUI.
Invalid option.	Specify a valid option.
Could not connect to the server. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Invalid server status.	Check if the cluster daemon is activated.
Server is not active. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid name of a server in the cluster.
Invalid heartbeat resource name. Specify a valid heartbeat resource name in the cluster.	Specify the valid name of a heartbeat resource in the cluster.
Invalid network partition resource name. Specify a valid network partition resource name in the cluster.	Specify the valid name of a network partition resolution resource in the cluster.
Invalid group name. Specify a valid group name in the cluster.	Specify the valid name of a group in the cluster.
Invalid group resource name. Specify a valid group resource name in the cluster.	Specify the valid name of a group resource in the cluster.
Invalid monitor resource name. Specify a valid monitor resource name in the cluster.	Specify the valid name of a monitor resource in the cluster.
Connection was lost. Check if there is a server where the cluster daemon is stopped in the cluster.	Check if there is any server on which the cluster daemon has stopped in the cluster.
Invalid parameter.	The value specified as a command parameter may be invalid.

Continued on next page

Table 8.11 – continued from previous page

Message	Cause/Solution
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set a longer timeout.	A time-out occurred in the EXPRESSCLUSTER internal communication. If time-out keeps occurring, set the internal communication time-out longer.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Invalid server group name. Specify a valid server group name in the cluster.	Specify the correct server group name in the cluster.
The cluster is not created.	Create and apply the cluster configuration data.
Could not connect to the server. Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Cluster is stopped. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Cluster is suspended. To display the cluster status, use --local option.	Cluster is suspended. To display the cluster status, use --local option.

8.3.1 Common entry examples

8.3.2 Displaying the status of the cluster (-s option)

The following is an example of display when you run the clpstat command with the -s option or without any option:

Example of a command entry

```
# clpstat -s
```

Example of the display after running the command

```
========== CLUSTER STATUS ==========
Cluster : cluster
<server>
 *server1.....: Online server1
   lanhb1      : Normal LAN Heartbeat
   lanhb2      : Normal LAN Heartbeat
   diskhb1     : Normal Disk Heartbeat
   comhb1      : Normal COM Heartbeat
   witnesshb1  : Normal Witness Heartbeat
   pingnp1     : Normal ping resolution
   pingnp2     : Normal ping resolution
   httpnp1     : Normal http resolution

 server2.....: Online server2
   lanhb1      : Normal LAN Heartbeat
   lanhb2      : Normal LAN Heartbeat
   diskhb1     : Normal Disk Heartbeat
   comhb1      : Normal COM Heartbeat
   witnesshb1  : Normal Witness Heartbeat
   pingnp1     : Normal ping resolution
```

(continues on next page)

(continued from previous page)

```
   pingnp2           : Normal ping resolution
   httpnp1           : Normal http resolution

<group>
  failover1..........: Online failover group1
   current           : server1
   disk1             : Online /dev/sdb5
   exec1             : Online exec resource1
   fip1              : Online 10.0.0.11
  failover2..........: Online failover group2
   current           : server2
   disk2             : Online /dev/sdb6
   exec2             : Online exec resource2
   fip2              : Online 10.0.0.12
<monitor>
  diskw1             : Normal disk monitor1
  diskw2             : Normal disk monitor2
  ipw1               : Normal ip monitor1
  pidw1              : Normal pidw1
  userw              : Normal usermode monitor
  sraw               : Normal sra monitor
============================================================
```

Information on each status is provided in "*Status Descriptions*".

8.3.3 Displaying a group map (-g option)

To display a group map, run the clpstat command with the -g option.

Example of a command entry

```
# clpstat -g
```

Example of the display after running the command

```
==================== GROUPMAP INFORMATION ================
Cluster : cluster
 *server0 : server1
  server1 : server2
------------------------------------------------------------
  server0 [o] : failover1[o] failover2[o]
  server1 [o] : failover3[o]
============================================================
```

- Groups that are not running are not displayed.
- Information on each status is provided in "*Status Descriptions*".

8.3.4 Displaying the status of monitor resources (-m option)

To display the status of monitor resources, run the clpstat command with the -m option.

Example of a command entry

```
# clpstat -m
```

Example of the display after running the command

```
================== MONITOR RESOURCE STATUS =================
Cluster : cluster
 *server0 : server1
  server1 : server2
 Monitor0 [diskw1 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
 Monitor1 [diskw2 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
 Monitor2 [ipw1 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
 Monitor3 [pidw1 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Offline
 Monitor4 [userw : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
 Monitor5 [sraw : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
=============================================================
```

Information on each status is provided in "*Status Descriptions*".

8.3.5 Displaying the status of heartbeat resources (-n option)

To display the status of heartbeat resources, run clpstat command with the -n option.

Example of a command entry

```
# clpstat -n
```

Example of the display after running the command

```
================== HEARTBEAT RESOURCE STATUS ====================
Cluster : cluster
 *server0 : server1
  server1 : server2
  HB0 : lanhb1
  HB1 : lanhb2
  HB2 : diskhb1
  HB3 : comhb1
  HB4 : witnesshb1

  [on server0 : Online]
         HB   0 1 2 3 4
-----------------------------------------------------------------
  erver0 : o o o o o
  server1 : o o o x o

  [on server1 : Online]
         HB   0   1 2 3 4
-----------------------------------------------------------------
  server0 : o o o x o
  server1 : o o o o o
=================================================================
```

Detailed information on each status is provided in "*Status Descriptions*".

The status of the example shown above

The example above presents the status of all heartbeat resources seen from server0 and server1 when the COM heartbeat resource is disconnected.

Because comhb1, a COM heartbeat resource, is not able to communicate from both servers, communication to server1 on server0 or communication to server0 on server1 is unavailable.

The rest of heartbeat resources on both servers are in the status allowing communications.

8.3.6 Displaying the status of network partition resolution resources (-p option)

To display the status of network partition resolution resources, run clpstat command with the -p option.

Example of a command entry

```
# clpstat -p
```

Example of the display after running the command

```
=============== NETWORK PARTITION RESOURCE STATUS ================
Cluster : cluster
 *server0 : server1
  server1 : server2
  NP0 : pingnp1
  NP1 : pingnp2
  NP2 : httpnp1

  [on server0 : Caution]
       NP    0 1 2
-----------------------------------------------------------------
```

(continues on next page)

(continued from previous page)

```
  server0 : o x o
  server1 : o x o

  [on server1 : Caution]
       NP    0 1 2
----------------------------------------------------------------
  server0 : o x o
  server1 : o x o
================================================================
```

Detailed information on each status is provided in "*Status Descriptions*".

The status of the example shown above
The example above presents the status of all the network partition resolution resources seen from server0 and server1 when the device to which ping of the network partition resolution resource pingnp2 is sent is down.

8.3.7 Displaying the cluster configuration data (--cl option)

To display the configuration data of a cluster, run the clpstat command with the -i, --cl, --svg, --hb, --grp, --rsc, --mon, or --xcl option. You can see more detailed information by specifying the --detail option.

For details of each item of the list, see "*Cluster properties*" in "2. *Parameter details*" in this guide.

To display the cluster configuration data, run the clpstat command with the --cl option.

Example of a command entry

```
# clpstat --cl
```

Example of the display after running the command

```
===================== CLUSTER INFORMATION ==================
[Cluster : cluster]
Comment  : failover cluster
============================================================
```

8.3.8 Displaying only the configuration data of certain servers (--sv option)

When you want to display only the cluster configuration data on a specified server, specify the name of the server after the --sv option in the clpstat command. If you want to see the details, specify the --detail option. When the name of the server is not specified, cluster configuration data of all servers are displayed.

Example of a command entry

```
# clpstat --sv server1
```

Example of the display after running the command

```
===================== CLUSTER INFORMATION ==================
 [Server0 : server1]
```

(continues on next page)

(continued from previous page)

```
   Comment                : server1
   Virtual Infrastructure : vSphere
   Product                : EXPRESSCLUSTER X 4.2 for Linux
   Internal Version       : 4.2.0-1
   Edition                : X
   Platform               : Linux
================================================================
```

8.3.9 Displaying only the resource information of certain heartbeats (--hb option)

When you want to display only the cluster configuration data on a specified heartbeat resource, specify the name of the heartbeat resource after the --hb option in the clpstat command. If you want to see the details, specify the --detail option.

Example of a command entry

For a LAN heartbeat resource:

```
# clpstat --hb lanhb1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
[HB0 : lanhb1]
   Type                 : lanhb
   Comment              : LAN Heartbeat
================================================================
```

Example of a command entry

For disk heartbeat resource:

```
# clpstat --hb diskhb
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
[HB2 : diskhb1]
Type                    : diskhb
Comment                 : Disk Heartbeat
================================================================
```

Example of a command entry

For COM heartbeat resource:

```
# clpstat --hb comhb
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
[HB3 : comhb1]
   Type                 : comhb
   Comment              : COM Heartbeat
================================================================
```

Example of a command entry

For kernel mode LAN heartbeat resource:

```
# clpstat --hb lankhb
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ==================
[HB4 : lankhb1]
   Type                  : lankhb
   Comment               : Kernel Mode LAN Heartbeat
===========================================================
```

Example of a command entry

For a BMC heartbeat resource:

```
# clpstat --hb bmchb1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ======================
   [HB0 : bmchb1]
   Type                  : bmchb
   Comment               : BMC Heartbeat
===============================================================
```

Tips

By using the --sv option and the --hb option together, you can see the information as follows.

Example of a command entry

```
# clpstat --sv --hb
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION =================
 [Server0 : server1]
  Comment                : server1
  Virtual Infrastructure :
  Product                : EXPRESSCLUSTER X 4.2 for Linux
  Internal Version       : 4.2.0-1
  Edition                : X
  Platform               : Linux
 [HB0 : lanhb1]
  Type                   : lanhb
  Comment                : LAN Heartbeat
 [HB1 : lanhb2]
  Type                   : lanhb
  Comment                : LAN Heartbeat
 [HB2 : diskhb1]
  Type                   : diskhb
  Comment                : Disk Heartbeat
 [HB3 : comhb1]
  Type                   : comhb
```

(continues on next page)

(continued from previous page)

```
 Comment                : COM Heartbeat
[HB4 : witnesshb]
 Type                   : witnesshb
 Comment                : Witness Heartbeat
[Server1 : server2]
 Comment                : server2
 Virtual Infrastructure :
 Product                : EXPRESSCLUSTER X 4.2 for Linux
 Internal Version       : 4.2.0-1
 Edition                : X
 Platform               : Linux
[HB0 : lanhb1]
 Type                   : lanhb
 Comment                : LAN Heartbeat
[HB1 : lanhb2]
 Type                   : lanhb
 Comment                : LAN Heartbeat
[HB2 : diskhb1]
 Type                   : diskhb
 Comment                : Disk Heartbeat
[HB3 : comhb1]
 Type                   : comhb
 Comment                : COM Heartbeat
[HB4 : witnesshb]
 Type                   : witnesshb
 Comment                : Witness Heartbeat
================================================================
```

8.3.10 Displaying only the configuration data of certain network partition resolution resources (--np option)

When you want to display only the cluster configuration data on the specified network partition resolution resource, specify the name of the network partition resolution resource after the --np option in the clpstat command. If you want to see the details, specify the --detail option. When you do not specify the name of the network partition resolution resource, the cluster configuration data of all the network partition resolution resources is displayed.

Example of a command entry

For a PING network partition resolution resource:

```
# clpstat --np pingnp1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
 [NP0 : pingnp1]
   Type                 : pingnp
   Comment              : ping resolution
================================================================
```

Example of a command entry

For a HTTP network partition resolution resource:

```
# clpstat --np httpnp1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
 [NP0 : httpnp1]
   Type                  : httpnp
   Comment               : http resolution
=============================================================
```

8.3.11 Displaying only the configuration data of certain server group (--svg option)

To display only the cluster configuration data on a specified server group, specify the name of server group after --svg option in the clpstat command. When you do not specify the name of server group, the cluster configuration data of all the server groups is displayed.

Example of a command entry

```
# clpstat --svg servergroup1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
 [ServerGroup0 : servergroup1]
   server0               : server1
   server1               : server2
   server2               : server3
=============================================================
```

8.3.12 Displaying only the configuration data of certain groups (--grp option)

When you want to display only the cluster configuration data on a specified group, specify the name of the group after the --grp option in the clpstat command. If you want to see the details, specify the --detail option. When you do not specify the name of group, the cluster configuration data of all the groups is displayed.

Example of a command entry

```
# clpstat --grp failover1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ==================
[Group0 : failover1]
   Type                  : failover
   Comment               : failover group1
===========================================================
```

8.3.13 Displaying only the configuration data of a certain group resource (--rsc option)

When you want to display only the cluster configuration data on a specified group resource, specify the group resource after the --rsc option in the clpstat command. If you want to see the details, specify the --detail option. When you do not specify the name of server group, the cluster configuration data of all the group resources is displayed.

Example of a command entry

For floating IP resource:

```
# clpstat --rsc fip1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
 [Resource2 : fip1]
   Type                  : fip
   Comment               : 10.0.0.11
   IP Address            : 10.0.0.11
================================================================
```

Tips

By using the --grp option and the --rsc option together, you can display the information as follows.

Example of a command entry

```
# clpstat --grp --rsc
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ==================
 [Group0 : failover1]
  Type                      : failover
  Comment                   : failover group1
 [Resource0 : disk1]
  Type                      : disk
  Comment                   : /dev/sdb5
  Disk Type                 : disk
  File System               : ext2
  Device Name               : /dev/sdb5
  Raw Device Name           :
  Mount Point               : /mnt/sdb5
 [Resource1 : exec1]
  Type                      : exec
  Comment                   : exec resource1
  Start Script Path         : /opt/userpp/start1.sh
  Stop Script Path          : /opt/userpp/stop1.sh
 [Resource2 : fip1]
  Type                      : fip
  Comment                   : 10.0.0.11
  IP Address                : 10.0.0.11
 [Group1 : failover2]
  Type                      : failover
  Comment                   : failover group2
```

(continues on next page)

(continued from previous page)

```
 [Resource0 : disk2]
  Type                      : disk
  Comment                   : /dev/sdb6
  Disk Type                 : disk
  File System               : ext2
  Device Name               : /dev/sdb6
  Raw Device Name           :
  Mount Point               : /mnt/sdb6
 [Resource1 : exec2]
  Type                      : exec
  Comment                   : exec resource2
  Start Script Path         : /opt/userpp/start2.sh
  Stop Script Path          : /opt/userpp/stop2.sh
 [Resource2 : fip2]
  Type                      : fip
  Comment                   : 10.0.0.12
  IP Address                : 10.0.0.12
================================================================
```

8.3.14 Displaying only the configuration data of a certain monitor resource (--mon option)

When you want to display only the cluster configuration data on a specified monitor resource, specify the name of the monitor resource after the --mon option in the clpstat command. If you want to see the details, specify --detail option. When you do not specify the name of monitor resource, the cluster configuration data of all monitor resources is displayed.

Example of a command entry

For floating IP monitor resource:

```
# clpstat --mon fipw1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ====================
[Monitor2 : fipw1]
Type                          : fipw
Comment                       : fip monitor1
================================================================
```

8.3.15 Displaying the configuration data of a resource specified for an individual server (--rsc option or --mon option)

When you want to display the configuration data on a resource specified for an individual server, specify the name of the resource after the --rsc or --mon option in the clpstat command.

Example of a command entry

When the monitor target IP address of the IP monitor resource is set to an individual server:

```
# clpstat --mon ipw1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ====================
 [Monitor2 : ipw1]
  Type                        : ipw
  Comment                     : ip monitor1
  IP Addresses                : Refer to server's setting
 <server1>
  IP Addresses                : 10.0.0.253
                              : 10.0.0.254
 <server2>
  IP Addresses                : 10.0.1.253
                              : 10.0.1.254
=============================================================
```

8.3.16 Displaying only the configuration data of specific exclusion rules (--xcl option)

When you want to display only the cluster configuration data on a specified exclusion rules, specify the exclusive rule name after the --xcl option in the clpstat command.

Example of a command entry

```
# clpstat --xcl excl1
```

Example of the display after running the command

```
==================== CLUSTER INFORMATION ====================
 [Exclusive Rule0 : excl1]
  Exclusive Attribute         : Normal
  group0                      : failover1
  group1                      : failover2
=============================================================
```

8.3.17 Displaying all configuration data (-i option)

By specifying the -i option, you can display the configuration information that is shown when --cl, --sv, --hb, --svg, --grp, --rsc, --mon, and --xcl options are all specified.

If you run the command with the -i option and the --detail option together, all the detailed cluster configuration data is displayed. Because this option displays large amount of information at a time, use a command, such as the less command, and pipe, or redirect the output in a file for the output.

Tips

Specifying the -i option displays all the information on a console. If you want to display some of the information, it is useful to combine the --cl, --sv, --hb, --svg, --grp, --rsc, and/or --mon option. For example, you can use these options as follows:

Example of a command entry

If you want to display the detailed information of the server whose name is "server0," the group whose name is "failover1," and the group resources of the specified group, enter:

```
# clpstat --sv server0 --grp failover1 --rsc --detail
```

8.3.18 Displaying the status of the cluster (--local option)

By specifying the --local option, you can display only information of the server on which you execute the clpstat command, without communicating with other servers.

Example of a command entry

```
# clpstat --local
```

Example of the display after running the command

```
========================= CLUSTER STATUS ========================
  Cluster : cluster
   cluster...........: Start        cluster
  <server>
  *server1...........: Online       server1
  lanhb1             : Normal       LAN Heartbeat
  lanhb2             : Normal       LAN Heartbeat
  diskhb1            : Normal       DISK Heartbeat
  comhb1             : Normal       COM Heartbeat
  witnesshb1         : Normal       Witness Heartbeat
  pingnp1            : Normal       ping resolution
  pingnp2            : Normal       ping resolution
  httpnp1            : Normal       http resolution

  server2...........: Online       server2
  lanhb1             : -            LAN Heartbeat
  lanhb2             : -            LAN Heartbeat
  diskhb1            : -            DISK Heartbeat
  comhb1             : -            COM Heartbeat
  witnesshb1         : -            Witness Heartbeat
  pingnp1            : -            ping resolution
  pingnp2            : -            ping resolution
  httpnp1            : -            http resolution

  <group>
  failover1.........: Online       failover group1
  current            : server1
  disk1              : Online       /dev/sdb5
  exec1              : Online       exec resource1
  fip1               : Online       10.0.0.11
  failover2.........: -            failover group2
  current            : server2
  disk2              : -            /dev/sdb6
  exec2              : -            exec resource2
  fip2               : -            10.0.0.12
  <monitor>
  diskw1             : Online       disk monitor1
  diskw2             : Online       disk monitor2
  ipw1               : Online       ip monitor1
  pidw1              : Online       pidw1
  userw              : Online       usermode monitor
  sraw               : Online       sra monitor
=================================================================
```

Information on each status is provided in "*Status Descriptions*".

8.3.19 Status Descriptions

Cluster

Function	Status	Description
Status display (--local)	Start	Starting
	Suspend	Being suspended
	Stop	Offline Pending
	Unknown	Status unknown

Server

Function	Status	Description
Status display Heartbeat resource status display	Online	Starting
	Offline	Offline Pending
	Online Pending	Now being started
	Offline Pending	Now being stopped
	Caution	Heartbeat resource failure
	Unknown	Status unknown
	-	Status unknown
Group map display Monitor resource status display	o	Starting
	x	Offline Pending
	-	Status unknown

Heartbeat Resource

Function	Status	Description
Status display	Normal	Normal
	Caution	Failure (Some)
	Error	Failure (All)
	Unused	Not used
	Unknown	Unknown
	-	Status unknown
Heartbeat resource status display	o	Able to communicate
	x	Unable to communicate
	-	Not used or status unknown

Network Partition Resolution Resource

Function	Status	Description
Status display	Normal	Normal
	Error	Failure
	Unused	Not used
	Unknown	Status unknown
	-	Status unknown
Network partition resolution status display	o	Able to communicate
	x	Unable to communicate
	-	Not used or status unknown

Group

Function	Status	Description
Status display	Online	Started
	Offline	Stopped
	Online Pending	Now being started
	Offline Pending	Now being stopped
	Error	Error
	Unknown	Status unknown
	-	Status unknown
Group map display	o	Started
	e	Error
	p	Now being started/stopped

Group Resource

Function	Status	Description
Status display	Online	Started
	Offline	Stopped
	Online Pending	Now being started
	Offline Pending	Now being stopped
	Online Failure	Starting failed
	Offline Failure	Stopping failed
	Unknown	Status unknown
	-	Status unknown

Monitor Resource

Function	Status	Description
Status Display	Normal	Normal
	Caution	Error (Some)
	Error	Error (All)
	Not Used	Not Used
	Unknown	Status Unknown
Status display (--local) Monitor Resource Status Display	Online	Started

Continued on next page

Table 8.18 – continued from previous page

Function	Status	Description
	Offline	Stopped
	Caution	Caution
	Suspend	Stopped temporary
	Online Pending	Now being started
	Offline Pending	Now being stopped
	Online Failure	Starting failed
	Offline Failure	Stopping failed
	Not used	Not used
	Unknown	Status unknown
	-	Status unknown

8.4 Operating the cluster (clpcl command)

the clpcl command operates a cluster

Command line

clpcl -s [-a] [-h *hostname*]
clpcl -t [-a] [-h *hostname*] [-w *timeout*] [--apito *timeout*]
clpcl -r [-a] [-h *hostname*] [-w *timeout*] [--apito *timeout*]
clpcl --suspend [--force] [-w *timeout*] [--apito *timeout*]
clpcl --resume

Description

This command starts, stops, suspends, or resumes the cluster daemon.

Option

-s
Starts the cluster daemon.

-t
Stops the cluster daemon.

-r
Restarts the cluster daemon.

--suspend
Suspends the entire cluster

-w `timeout`
clpcl command specifies the wait time to stop or suspend the cluster daemon to be completed when -t, -r, or --suspend option is used. The unit of time is second.

When a time-out is not specified, it waits for unlimited time.

When "0 (zero)" is specified, it does not wait.

When -w option is not specified, it waits for (heartbeat time-out x 2) seconds.

--resume
Resumes the entire cluster. The status of group resource of the cluster when suspended is kept.

-a
Executed the command on all servers

-h hostname
Makes a request to run the command to the server specified in *hostname*. Makes a processing request to the server on which this command runs (local server) if the -h option is omitted.

--force
When used with the --suspend option, forcefully suspends the cluster regardless of the status of all the servers in the cluster.

--apito timeout

Specify the interval (internal communication timeout) to wait for the EXPRESSCLUSTER daemon start or stop in seconds. A value from 1 to 9999 can be specified.

If the --apito option is not specified, waiting for the EXPRESSCLUSTER daemon start or stop is performed according to the value set to the internal communication timeout of the cluster properties.

Return Value

0	Success
Other than 0	Failure

Remarks

When this command is executed with the -s or --resume option specified, it returns control when processing starts on the target server.

When this command is executed with the -t or --suspend option specified, it returns control after waiting for the processing to complete.

When this command is executed with the -r option specified, it returns control when the EXPRESSCLUSTER daemon restarts on the target server after stopping once.

Run the clpstat command to display the started or resumed status of the EXPRESSCLUSTER daemon.

Notes

Run this command as the root user.

This command cannot be executed while a group is being started or stopped.

For the name of a server for the -h option, specify the name of a server in the cluster.

When you suspend the cluster, the cluster daemon should be activated in all servers in the cluster. When the --force option is used, the cluster is forcefully suspended even if there is any stopped server in the cluster.

When you start up or resume the cluster, access the servers in the cluster in the order below, and use one of the paths that allowed successful access.

1. via the IP address on the interconnect LAN
2. via the IP address on the public LAN

When you resume the cluster, use the clpstat command to see there is no activated server in the cluster.

This command starts, stops, restarts, suspends, or resumes only the EXPRESSCLUSTER daemon. The mirror agent and the like are not started, stopped, restarted, suspended, or resumed together.

Example of a command entry

Example 1: Activating the cluster daemon in the local server

```
# clpcl -s
```

Example 2: Activating the cluster daemon in server1 from server0

```
# clpcl -s -h server1
```

Start server1 : Command succeeded.

If a server name is specified, the display after running the command should look similar to above.

Start *hostname* : Execution result

(If the activation fails, cause of the failure is displayed)

Example 3: Activating the cluster daemon in all servers

```
# clpcl -s -a
```

Start server0 : Command succeeded.

Start server1 : Performed startup processing to the active cluster daemon. When all the servers are activated, the display after running the command should look similar to above. Start *hostname* : Execution result

(If the activation fails, cause of the failure is displayed)

Example 4: Stopping the cluster daemon in all servers

```
# clpcl -t -a
```

If the cluster daemon stops on all the servers, it waits till the EXPRESSCLUSTER daemons stop on all the servers.

If stopping fails, an error message is displayed.

Error Messages

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid configuration file. Create valid cluster configuration data.	Create valid cluster configuration data using the Cluster WebUI.
Invalid option.	Specify a valid option
Performed stop processing to the stopped cluster daemon.	The stopping process has been executed on the stopped cluster daemon.
Performed startup processing to the active cluster daemon.	The startup process has been executed on the activated cluster daemon.
Could not connect to the server. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Could not connect to the data transfer server. Check if the server has started up.	Check if the server is running.
Failed to obtain the list of nodes. Specify a valid server name in the cluster.	Specify the valid name of a server in the cluster.
Failed to obtain the daemon name.	Failed to obtain the cluster name.
Failed to operate the daemon.	Failed to control the cluster.

Continued on next page

Table 8.19 – continued from previous page

Message	Cause/Solution
Resumed the daemon that is not suspended.	Performed the resume process for the HA Cluster daemon that is not suspended.
Invalid server status.	Check that the cluster daemon is activated.
Server is busy. Check if this command is already run.	This command may have already been run.
Server is not active. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
There is one or more servers of which cluster daemon is active. If you want to perform resume, check if there is any server whose cluster daemon is active in the cluster.	When you execute the command to resume, check if there is no server in the cluster on which the cluster daemon is activated.
All servers must be activated. When suspending the server, the cluster daemon need to be active on all servers in the cluster.	When you execute the command to suspend, the cluster daemon must be activated in all servers in the cluster.
Resume the server because there is one or more suspended servers in the cluster.	Execute the command to resume because some server(s) in the cluster is in the suspend status.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid name of a sever in the cluster.
Connection was lost. Check if there is a server where the cluster daemon is stopped in the cluster.	Check if there is any server on which the cluster daemon is stopped in the cluster.
Invalid parameter.	The value specified as a command parameter may be invalid.
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set the longer timeout.	A time-out occurred in the HA Cluster internal communication. If time-out keeps occurring, set the internal communication time-out longer.
Processing failed on some servers. Check the status of failed servers.	If stopping has been executed with all the servers specified, there is one of more servers on which the stopping process has failed. Check the status of the server(s) on which the stopping process has failed.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
There is a server that is not suspended in cluster. Check the status of each server.	There is a server that is not suspended in the cluster. Check the status of each server.
Suspend %s : Could not suspend in time.	The server failed to complete the suspending process of the cluster daemon within the time-out period. Check the status of the server.
Stop %s : Could not stop in time.	The server failed to complete the stopping process of the cluster daemon within the time-out period. Check the status of the server.
Stop %s : Server was suspended. Could not connect to the server. Check if the cluster daemon is active.	The request to stop the cluster daemon was made. However the server was suspended.

Continued on next page

Table 8.19 – continued from previous page

Message	Cause/Solution
Could not connect to the server. Check if the cluster daemon is active.	The request to stop the cluster daemon was made. However connecting to the server failed. Check the status of the server.
Suspend %s : Server already suspended. Could not connect to the server. Check if the cluster daemon is active.	The request to suspend the cluster daemon was made. However the server was suspended.
Event service is not started.	Event service is not started. Check it.
Mirror Agent is not started.	Mirror Agent is not started. Check it.
Event service and Mirror Agent are not started.	Event service and Mirror Agent are not started. Check them.
Some invalid status. Check the status of cluster.	The status of a group may be changing. Try again after the status change of the group is complete.
Failed to shut down the server.	Failed to shut down or reboot the server.

8.5 Shutting down a specified server (clpdown command)

the clpdown command shuts down a specified server.

Command line

clpdown [-r] [-h *hostname*]

Description

This command stops the cluster daemon and shuts down a server.

Option

None

Shuts down a server.

-r

Reboots the server.

-h `hostname`

Makes a processing request to the server specified in *hostname*. Makes a processing request to the server on which this command runs (local server) if the -h option is omitted.

Return Value

0	Success
Other than 0	Failure

Remarks

This command runs the following commands internally after stopping the cluster daemon.

Without any option specified **shutdown**

With the -r option specified **reboot**

This command returns control when the group stop processing is completed.

This command shuts down the server even when the EXPRESSCLUSTER daemon is stopped.

Notes

Run this command as the root user.

This command cannot be executed while a group is being started or stopped.

For the name of a server for the -h option, specify the name of a server in the cluster.

Example of a command entry

Example 1: Stopping and shutting down the cluster daemon in the local server

```
# clpdown
```

Example 2: Shutting down and rebooting server1 **from** server0

```
# clpdown -r -h server1
```

Error Message

See "*Operating the cluster (clpcl command)*".

8.6 Shutting down the entire cluster (clpstdn command)

the clpstdn command shuts down the entire cluster

Command line

clpstdn [-r] [-h *hostname*]

Description

This command stops the cluster daemon in the entire cluster and shuts down all servers.

Option

None

Executes cluster shutdown.

-r

Executes cluster shutdown reboot.

-h hostname

Makes a processing request to the server specified in *hostname*. Makes a processing request to the server on which this command runs (local server) if the -h option is omitted.

Return Value

0	Success
Other than 0	Failure

Remarks

This command returns control when the group stop processing is completed.

Notes

Run this command as the root user.

This command cannot be executed while a group is being started or stopped.

For the name of a server for the -h option, specify the name of a server in the cluster.

A server that cannot be accessed from the server that runs the command (for example, a server with all LAN heartbeat resources are off-line.) will not shut down.

Example of a command entry

Example 1: Shutting down the cluster

```
# clpstdn
```

Example 2: Performing the cluster shutdown reboot

```
# clpstdn -r
```

Error Message

See "*Operating the cluster (clpcl command)*".

8.7 Operating groups (clpgrp command)

the clpgrp command operates groups

Command line

clpgrp -s [*group_name*] [-h *hostname*] [-f] [--apito timeout]
clpgrp -t [*group_name*] [-h *hostname*] [-f] [--apito timeout]
clpgrp -m [*group_name]* [-h *hostname*] [-a *hostname*] [--apito timeout]
clpgrp -l [*group_name*] [-h *hostname*] [-a *hostname*] [--apito timeout]

Description

This command starts, deactivates or moves groups. This command also migrates groups.

Option

-s [group_name]
Starts groups. When you specify the name of a group, only the specified group starts up. If no group name is specified, all groups start up.

-t [group_name]
Stops groups. When you specify the name of a group, only the specified group stops. If no group name is specified, all groups stop.

-m [group_name]
Moves a specified group. If no group name is specified, all the groups are moved. The status of the group resource of the moved group is kept.

-l [group_name]

Migrates the specified group. The group type must always be the migration type.
If no group name is specified, all the active migration groups on the server are migrated.

-h hostname
Makes a processing request to the server specified in *hostname*. Makes a processing request to the server on which this command runs (local server) if the -h option is omitted.

-a hostname
Defines the server which is specified by *hostname* as a destination to which a group will be moved. When the -a option is omitted, the group will be moved according to the failover policy

-f

If you use this option with the -s option against a group activated on a remote server, it will forcefully be started on the server that requested the process.

If this command is used with the -t option, the group will be stopped forcefully.

-n group_name

Displays the name of the server on which the group has been started.

--apito timeout

Specify the interval (internal communication timeout) to wait for the group resource start or stop in seconds. A value from 1 to 9999 can be specified.

If the --apito option is not specified, waiting for the group resource start or stop is performed according to the value set to the internal communication timeout of the cluster properties.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as the root user.

The cluster daemon must be activated on the server that runs this command

Specify a server in the cluster when you specify the name of server name for the -h and -a options.

Make sure to specify a group name, when you use the -m option.

If the group is moved by using the [-m] option, it is determined to be normal at the time of performing the group start process on the destination server. Please be aware that even if this command is executed successfully, the activation of the resource may fail on the server to which the group is moved. In order to check whether or not the group has started by using the return value, execute the following:

 # clpgrp -s [group_name] [-h hostname] -f

In order to move a group belonging to exclusion rules whose exclusion attribute is set to "Normal" by using the [-m] option, explicitly specify a server to which the group is moved by the [-a] option.

With the [-a] option omitted, moving a group fails if a group belonging to exclusion rules whose exclusion attribute is set to "Normal" is activated in all the movable servers.

Example of Execution

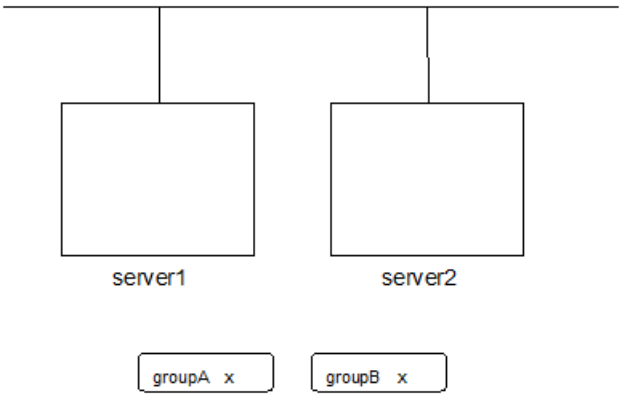
The following is an example of status transition when operating the groups.

Example: The cluster has two servers and two groups.

Failover policy of group

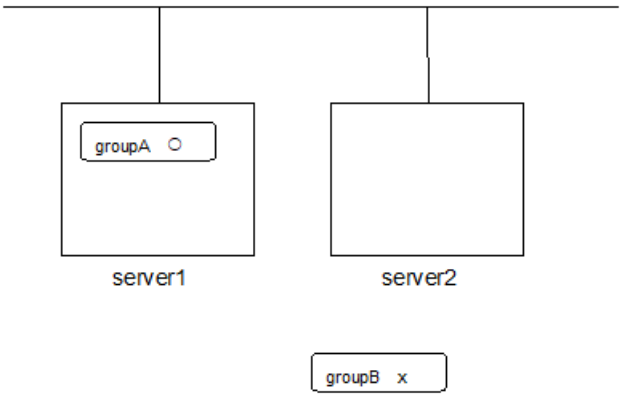
groupA server1 -> server2
groupB server2 -> server1

1. Both groups are stopped.



2. Run the following command on server1.

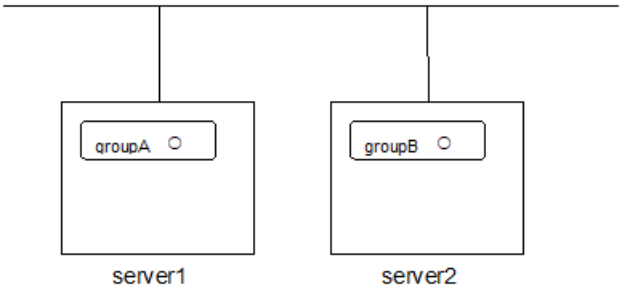
```
# clpgrp -s groupA
```



GroupA starts in server1.

3. Run the following command in server2.

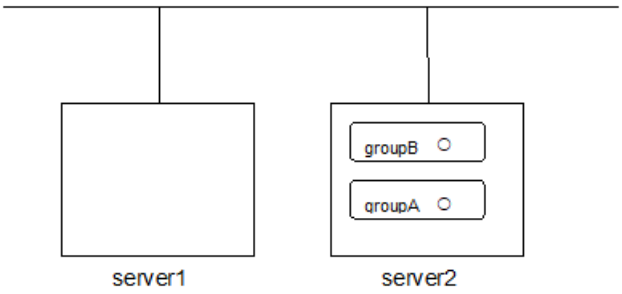
```
# clpgrp -s
```



All groups that are currently stopped but can be started start in server2.

4. Run the following command in server1

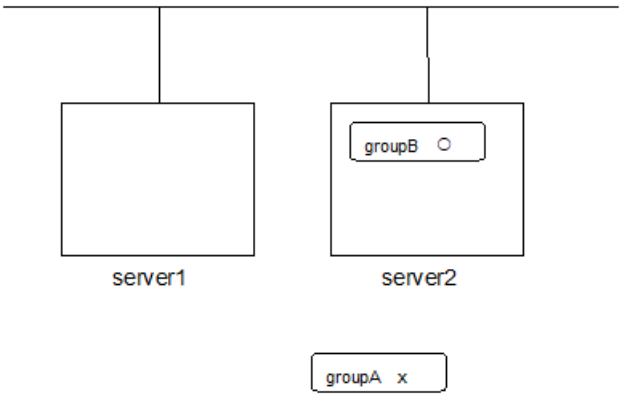
```
# clpgrp -m groupA
```



GroupA moves to server2.

5. Run the following command in server1

```
# clpgrp -t groupA -h server2
```



GroupA stops.

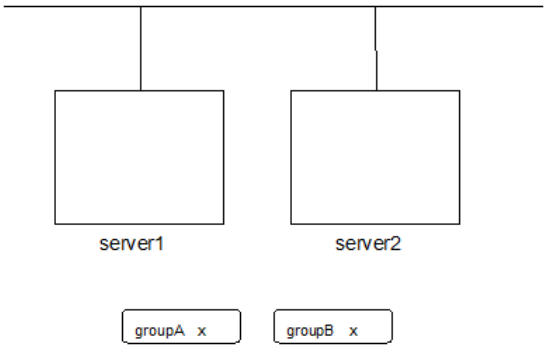
6. Run the following command in server1.

```
# clpgrp -t
Command Succeeded.
```

When the command is executed, there is no group running on server1. So, "Command Succeeded." appears.

7. Add -f to the command you have run in Step 6 and execute it on server1.

```
# clpgrp -t -f
```



Groups which were started in server2 can be forcefully deactivated from server1.

Error message

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid configuration file. Create valid cluster configuration data.	Create valid cluster configuration data using the Cluster WebUI
Invalid option.	Specify a valid option
Could not connect to the server. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Invalid server status.	Check if the cluster daemon is activated.
Server is not active. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid name of sever in the cluster.
Connection was lost. Check if there is a server where the cluster daemon is stopped in the cluster.	Check if there is any server on which the cluster daemon has stopped in the cluster.
Invalid parameter.	The value specified as a command parameter may be invalid.
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set a longer timeout.	A time-out occurred in the EXPRESSCLUSTER internal communication. If time-out keeps occurring, set the internal communication time-out longer.
Invalid server. Specify a server that can run and stop the group, or a server that can be a target when you move the group.	The server that starts/stops the group or to which the group is moved is invalid. Specify a valid server.
Could not start the group. Try it again after the other server is started, or after the Wait Synchronization time is timed out.	Start up the group after waiting for the remote server to start up, or after waiting for the time-out of the start-up wait time.
No operable group exists in the server.	Check if there is any group that is operable in the server which requested the process.
The group has already been started on the local server.	Check the status of the group by using the Cluster WebUI or the clpstat command.
The group has already been started on the other server. To start/stop the group on the local server, use -f option.	Check the status of the group by using the Cluster WebUI or the clpstat command. If you want to start up or stop a group which was started in a remote server from the local server, move the group or run the command with the -f option.
The group has already been started on the other server. To move the group, use "-h <hostname>" option.	Check the status of the group by using the Cluster WebUI or clpstat command. If you want to move a group which was started on a remote server, run the command with the -h hostname option.
The group has already been stopped.	Check the status of the group by using the Cluster WebUI or the clpstat command.
Failed to start one or more group resources. Check the status of group	Check the status of group by using Cluster WebUI or the clpstat command.
Failed to stop one or more group resources. Check the status of group	Check the status of group by using the Cluster WebUI or the clpstat command.
The group is busy. Try again later.	Wait for a while and then try again because the group is now being started up or stopped.

Continued on next page

Table 8.20 – continued from previous page

Message	Cause/Solution
An error occurred on one or more groups. Check the status of group	Check the status of the group by using the Cluster WebUI or the clpstat command.
Invalid group name. Specify a valid group name in the cluster.	Specify the valid name of a group in the cluster.
Server is not in a condition to start group or any critical monitor error is detected.	Check the status of the server by using the Cluster WebUI or clpstat command. An error is detected in a critical monitor on the server on which an attempt was made to start a group.
There is no appropriate destination for the group. Other servers are not in a condition to start group or any critical monitor error is detected.	Check the status of the server by using the Cluster WebUI or clpstat command. An error is detected in a critical monitor on all other servers.
The group has been started on the other server. To migrate the group, use "-h <hostname>" option.	Check the status of the group by using the Cluster WebUI or clpstat command. If you want to move a group which was started on a remote server, run the command with the -h hostname option.
The specified group cannot be migrated.	The specified group cannot be migrated.
The specified group is not vm group.	The specified group is not a virtual machine group.
Migration resource does not exist.	Check the status of the group by using the Cluster WebUI or clpstat command. The resource to be migrated is not found.
Migration resource is not started.	Check the status of the group by using the Cluster WebUI or clpstat command. The resource to be migrated is not started.
Some invalid status. Check the status of cluster.	Invalid status for some sort of reason. Check the status of the cluster.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.8 Collecting logs (clplogcc command)

the clplogcc command collects logs.

Command line

clplogcc [[-h *hostname*] | [-n *targetnode1* -n *targetnode2* .....]] [-t *collect_type*] [-r *syslog_rotate_number*] [-o *path*] [-l]

Description

This command collects information including logs and the OS information by accessing the data transfer server.

Option

None

Collects logs in the cluster.

-h `hostname`

Specifies the name of the access destination server for collecting cluster node information

-t `collect_type`

Specifies a log collection pattern. When this option is omitted, a log collection pattern will be type1. Information on log collection types is provided in "*Collecting logs by specifying a type (-t option)*".

-r syslog_rotate _number
Specifies how many generations of syslog will be collected. When this option is omitted, only one generation will be collected.

-o path
Specifies the output destination of collector files. When this option is skipped, logs are output under tmp of the installation path.

-n targetnode
Specifies the name of a server that collects logs. With this specification, logs of the specified server, rather than of the entire cluster, will be collected.

-l

Collects logs on the local server without going through the data transfer server.

The -h option and the -n option cannot be specified at the same time.

Return Value

0	Success
Other than 0	Failure

Remarks

Since log files are compressed by tar.gz, add the xzf option to the tar command to decompress them.

Notes

Run this command as the root user.

For the name of server for the -h option, specify the name of a server in the cluster that allows name resolution.

For the name of server for the -n option, specify the name of server that allows name resolution. If name resolution is not possible, specify the interconnect or public LAN address.

When you run this command, access the servers in the cluster in the order below, and use one of the paths that allowed successful access.

1. via the IP address on the interconnect LAN
2. via the IP address on the public LAN
3. via the IP address whose name was resolved by the server name in the cluster configuration data

If the log files collected on Linux OS (pax format of the tar command's compression) are decompressed with gnutar format of the tar command, a PaxHeaders.X folder is generated. However, it does not affect the operation.

Example of command execution

Example 1: Collecting logs from all servers in the cluster

```
# clplogcc
Collect Log server1 : Success
Collect Log server2 : Success
```

Log collection results (server status) of servers on which log collection is executed are displayed.

Process *hostname*: result of loc collection (server status)

Execution Result

For this command, the following processes are displayed.

Steps in Process	Meaning
Connect	Displayed when the access fails.
Get File size	Displayed when acquiring the file size fails.
Collect Log	Displayed with the file acquisition result.

The following results (server status) are displayed:

Result (server status)	Meaning
Success	Success
Timeout	Time-out occurred.
Busy	The server is busy.
Not Exist File	The file does not exist.
No Free space	No free space on the disk.
Failed	Failure caused by other errors.

`Error Message`

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid configuration file. Create valid cluster configuration data.	Create valid cluster configuration data using the Cluster WebUI.
Invalid option.	Specify a valid option.
Specify a number in a valid range.	Specify a number within a valid range.
Specify a correct number.	Specify a valid number.
Specify correct generation number of syslog.	Specify a valid number for the syslog generation.
Collect type must be specified 'type1' or 'type2' or 'type3' or 'type4' or 'type5' or 'type6'. Incorrect collection type is specified.	Invalid collection type has been specified.
Specify an absolute path as the destination of the files to be collected.	Specify an absolute path for the output destination of collected files.
Specifiable number of servers are the max number of servers that can constitute a cluster.	The number of servers you can specify is within the maximum number of servers for cluster configuration.
Could not connect to the server. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Failed to obtain the list of nodes. Specify a valid server name in the cluster.	Specify the valid name of a server in the cluster.
Invalid server status.	Check if the cluster daemon is activated.
Server is busy. Check if this command is already run.	This command may have been already activated. Check the status.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.8.1 Collecting logs by specifying a type (-t option)

To collect only the specified types of logs, run the clplogcc command with the -t option.

Specify a type from 1 through 6 for the log collection.

	type1	type2	type3	type4	type5	type6
1. Default collection information	y	y	y	y	n	n
2. syslog	y	y	y	n	n	n
3. core file	y	y	n	y	n	n
4. OS information	y	y	y	y	n	n
5. script	y	y	n	n	n	n
6. ESMPRO/AC	y	y	n	n	n	n
7. HA Logs	n	y	n	n	n	n
8. Mirror statistics information	n	n	n	n	y	n
9. Cluster statistics information	n	n	n	n	n	y
10. System resource statistics information	y	y	y	y	n	y

(y=yes, n=no)

Run this command from the command line as follows.

Example: When collecting logs using type2

```
# clplogcc -t type2
```

When no option is specified, a log type will be type 1.

1. Information to be collected by default

   Information on the following is collected by default:

   - Logs of each module in the EXPRESSCLUSTER Server
   - Alert logs

- Attribute of each module (ls -l) in the EXPRESSCLUSTER Server
  - In bin, lib
  - In cloud
  - In alert/bin, webmgr/bin
  - In ha/jra/bin, ha/sra/bin, ha/jra/lib, ha/sra/lib
  - In drivers/md
  - In drivers/khb
  - In drivers/ka
- All installed packages (rpm -qa expresscls execution result)
- EXPRESSCLUSTER version
- distribution (/etc/*-release)
- License information
- Cluster configuration data file
- Policy file
- Cloud environment configuration directory
- Dump of shared memory used by EXPRESSCLUSTER
- Local node status of EXPRESSCLUSTER (clpstat --local execution results)
- Process and thread information (ps execution result)
- PCI device information (lspci execution result)
- Service information (execution results of the commands such as systemctl, chkconfig, and ls)
- Output result of kernel parameter (result of running sysctl -a)
- glibc version (rpm -qi glibc execution result)
- Kernel loadable module configuration (/etc/modules.conf. /etc/modprobe.conf)
- File system (/etc/fstab)
- IPC resource (ipcs execution result)
- System (uname -a execution result)
- Network statistics (netstat, ss execution result IPv4/IPv6)
- ip (execution results of the command ip addr, link, maddr, route or -s l)
- All network interfaces (ethtool execution result)
- Information collected at an emergency OS shutdown (See "*Collecting information when a failure occurs*".)
- libxml2 version (rpm -qi libxml2 execution result)
- Static host table (/etc/hosts)
- File system export table (exportfs -v execution result)
- User resource limitations (ulimit -a execution result)
- File system exported by kernel-based NFS (/etc/exports)
- OS locale

- Terminal session environment value (export execution result)
- Language locale (/etc/sysconfig/i18n)
- Time zone (env - date execution result)
- Work area of EXPRESSCLUSTER server
- Monitoring options
  This information is collected if options are installed.
- Collected dump information when the monitor resource timeout occurred
- Collected Oracle detailed information when Oracle monitor resource abnormity was detected

2. syslog
   - syslog (/var/log/messages)
   - syslog (/var/log/syslog)
   - Syslogs for the number of generations specified (/var/log/messages.x)
   - journal log (such as files in /var/run/log/journal/)
3. core file
   - core file of EXPRESSCLUSTER module
     Stored in /opt/nec/clusterpro/log by the following archive names.

     Alert related:

     alt**yyyymmdd_x**.tar

     The WebManager server related:

     wm**yyyymmdd_x**.tar

     EXPRESSCLUSTER core related:

     cls**yyyymmdd_x**.tar

     sra**yyyymmdd_x**.tar

     jra**yyyymmdd_x**.tar

     yyyymmdd indicates the date when the logs are collected. **x is a sequence number.**
4. OS information

   OS information on the following is collected by default:
   - Kernel mode LAN heartbeat, keep alive
     - /proc/khb_moninfo
     - /proc/ka_moninfo
   - /proc/devices
   - /proc/mdstat
   - /proc/modules
   - /proc/mounts
   - /proc/meminfo
   - /proc/cpuinfo
   - /proc/partitions

- /proc/pci
- /proc/version
- /proc/ksyms
- /proc/net/bond*
- all files of /proc/scsi/ all files in the directory
- all files of /proc/ide/ all files in the directory
- /etc/fstab
- /etc/rc*.d
- /etc/syslog.conf
- /etc/syslog-ng/syslog-ng.conf
- /etc/snmp/snmpd.conf
- Kernel ring buffer (dmesg execution result)
- ifconfig (the result of running ifconfig)
- iptables (the result of running iptables -L)
- ipchains (the result of running ipchains -L)
- df (the result of running df)
- raw device information (the result of running raw -qa)
- kernel module load information (the result of running lsmod)
- host name, domain name information (the result of running hostname, domainname)
- dmidecode (the result of running dmidecode)
- LVM device information (the result of running vgdisplay -v)
- snmpd version information (snmpd -v execution result)
- Virtual Infrastructure information (the result of running virt-what)
- blockdev (the result of running blockdev --report)

When you collect logs, you may find the following message on the console. This does not mean failure. The logs are collected normally.

```
hd#: bad special flag: 0x03
ip_tables: (C) 2000-2002 Netfilter core team
```

(Where hd# is the name of the IDE device that exists on the server)

5. Script

   Start/stop script for a group that was created with the Cluster WebUI.

   If you specify a user-defined script other than the above (/opt/nec/clusterpro/scripts), it is not included in the log collection information. It must be collected separately.

6. ESMPRO/AC Related logs

   Files that are collected by running the acupslog command.

7. HA logs

   - System resource information

- JVM monitor log
- System monitor log

8. Mirror statistics information
   - Mirror statistics information
     - In perf/disk
9. Cluster statistics information
   - Cluster statistics information
     - In perf/cluster
10. System resource statistics information
    - System resource statistics information
      - In perf/system

8.8.2 Syslog generations (-r option)

To collect syslogs for the number of generations specified, run the following command.

Example: Collecting logs for the 3 generations

```
# clplogcc -r 3
```

The following syslogs are included in the collected logs.

/var/log/messages
/var/log/messages.1
/var/log/messages.2

- When no option is specified, only /var/log/messages is collected.
- You can collect logs for 0 to 99 generations.
- When 0 is specified, all syslogs are collected.

Number of Generation	Number of generations to be acquired
0	All Generations
1	Current
2	Current + Generation 1
3	Current + Generation 1 to 2
:	
:	
x	Current + Generation 1 to (x-1)

8.8.3 Output paths of log files (-o option)

- Log file is named and be saved as "*server name*-log.tar.gz"
- If an IP address is specified for the -n option, a log file is named and saved as "*IP address*-log.tar.gz."
- Since log files are compressed by tar.gz, decompress them by adding the xzf option to the tar command.

If not specifying -o option

Logs are output in tmp of installation path.

```
# clplogcc
Collect Log hostname : Success
# ls /opt/nec/clusterpro/tmp
hostname-log.tar.gz
```

When the -o option is not specified:

If you run the command as follows, logs are located in the specified /home/log directory.

```
# clplogcc -o /home/log
Collect Log hostname: Success
# ls /home/log
hostname-log.tar.gz
```

8.8.4 Specifying log collector server (-n option)

By using the -n option, you can collect logs only from the specified server.

Example: Collecting logs from Server1 and Server3 in the cluster.

```
# clplogcc -n Server1 -n Server3
```

- Specify a server in the same cluster.
- The number of servers you can specify is within the maximum number of servers in the cluster configuration.

8.8.5 Collecting information when a failure occurs

When the following failure occurs, the information for analyzing the failure is collected.

- When a cluster daemon configuring the cluster abnormally terminates due to interruption by a signal (core dump) or internal status error etc.
- When a group resource activation error or deactivation error occurs
- When monitoring error occurs in a monitor resource

Information to be collected is as follows:

- Cluster information
  - Some module logs in EXPRESSCLUSTER servers
  - Dump files in the shared memory used by EXPRESSCLUSTER
  - Cluster configuration information files
  - Core files of EXPRESSCLUSTER module
- OS information (/proc/*)

  - /proc/devices
  - /proc/partitions
  - /proc/mdstat
  - /proc/modules
  - /proc/mounts
  - /proc/meminfo
  - /proc/net/bond*
- Information created by running a command
  - Results of the sysctl -a
  - Results of the ps
  - Results of the top
  - Results of the ipcs
  - Results of the netstat -in
  - Results of the netstat -apn
  - Results of the netstat -gn
  - Results of the netstat -rn
  - Results of the ifconfig
  - Results of the ip addr
  - Results of the ip -s l
  - Results of the df
  - Results of the raw -qa
  - journalctl -e execution result

These are collected by default in the log collection. You do not need to collect them separately.

8.9 Changing, backing up, and checking cluster configuration data (clpcfctrl command)

8.9.1 Creating a cluster and changing the cluster configuration data

the clpcfctrl --push command delivers cluster configuration data to servers.

Command line
clpcfctrl --push -ll-w [-c *hostname|IP*] [-h *hostname|IP*] [-p *portnumber*] [-x *directory*] [--force] [--nocheck]

Description
This command delivers the configuration data created by the Cluster WebUI to servers.

Option

--push
Specify this option when delivering the data. You cannot omit this option.

-l

Specify this option when using the configuration data saved by the Cluster WebUI on Linux.

-w

Specify this option when using the configuration data saved by the Cluster WebUI on Windows.
You cannot specify -l and -w together.

-c hostname | IP

Specifies a server to access for acquiring a list of servers. Specify a host name or IP address.
When this option is omitted, address in configuration data will be used.

-h hostname | IP

Specifies a server to which configuration data is delivered. Specify host name or IP address.
If this option is omitted, configuration data is delivered to all servers.

-p portnumber

Specifies a port number of data transfer port.
When this option is omitted, the default value will be used. In general, it is not necessary to specify this option.

-x directory

Specify this option when delivering configuration data to the specified directory.
This option is used with -l or -w.
When -l is specified, configuration data saved on the file system by the Cluster WebUI on Linux is used.
When -w is specified, configuration data saved by the Cluster WebUI on Windows is used.

--force

Even if there is a server that has not started, the configuration data is delivered forcefully.

--nocheck

When this option is specified, cluster configuration data is not checked. Use this option only when deleting a server.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as the root user.

When you run this command, access the servers in the order below, and use one of the paths that allowed successful access.

1. via the IP address on the interconnect LAN
2. via the IP address on the public LAN

Example of command execution

Example 1: Delivering configuration data that was saved on the file system using the Cluster WebUI on Linux

```
# clpcfctrl --push -l -x /mnt/config
file delivery to server 10.0.0.11 success.
file delivery to server 10.0.0.12 success.
The upload is completed successfully.(cfmgr:0)
Command succeeded.(code:0)
```

Example 2: Delivering the configuration data to the server which has been reinstalled.

```
# clpcfctrl --push -h server2
The upload is completed successfully.(cfmgr:0)
Command succeeded.(code:0)
```

Error Message

Message	Cause/Solution
Log in as root.	Log on as the root user.
This command is already run.	This command has been already started.
Invalid option.	The option is invalid. Check the option.
Invalid mode. Check if --push is specified.	Check if the --push option is specified.
The target directory does not exist.	The specified directory is not found.
Invalid host name. Server specified by -h option is not included in the configuration data	The server specified with -h is not included in configuration data. Check if the specified server name or IP address is valid.
Canceled.	Displayed when anything other than "y" is entered for command inquiry.
Failed to initialize the xml library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to load the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to change the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to load the policy files. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.

Continued on next page

Table 8.26 – continued from previous page

Message	Cause/Solution
Failed to load the cfctrl policy file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the install path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the cfctrl path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the list of group.	Failed to acquire the list of group.
Failed to get the list of resource.	Failed to acquire the list of resource.
Failed to initialize the trncl library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to connect to server %s. Check if the other server is active and then run the command again.	Accessing the server has failed. Check if other server(s) has been started. Run the command again after the server has started up.
Failed to connect to trnsv. Check if the other server is active.	Accessing the server has failed. Check that other server has been started up.
Failed to get the collect size.	Getting the size of the collector file has failed. Check if other server(s) has been started.
Failed to collect the file.	Collecting of the file has failed. Check if other server(s) has been started.
Failed to get the list of node. Check if the server specified by -c is a member of the cluster.	Check to see if the server specified by -c is a cluster member.
Failed to check server property. Check if the server name or ip addresses are correct.	Check if the server name and the IP address in the configuration information have been set correctly.
File delivery failed. Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.

Continued on next page

Table 8.26 – continued from previous page

Message	Cause/Solution
Multi file delivery failed. Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.
Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.
The directory "/work" is not found. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to make a working directory.	Check to see if the memory or OS resource is sufficient.
The directory does not exist.	Same as above.
This is not a directory.	Same as above.
The source file does not exist.	Same as above.
The source file is a directory.	Same as above.
The source directory does not exist.	Same as above.
The source file is a directory.	Same as above.
The source directory does not exist.	Same as above.
The source file is not a directory.	Same as above.
Failed to change the character code set (EUC to SJIS).	Same as above.
Failed to change the character code set (SJIS to EUC).	Same as above.
Command error.	Same as above.
Failed to initialize the cfmgr library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to get size from the cfmgr library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to allocate memory.	Check to see if the memory or OS resource is sufficient.
Failed to change the directory.	Same as above.
Failed to run the command.	Same as above.
Failed to make a directory.	Same as above.
Failed to remove the directory.	Same as above.
Failed to remove the file.	Same as above.
Failed to open the file.	Same as above.
Failed to read the file.	Same as above.
Failed to write the file.	Same as above.

Continued on next page

Table 8.26 – continued from previous page

Message	Cause/Solution
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
The upload is completed successfully. To start the cluster, refer to "How to create a cluster" in the Installation and Configuration Guide.	The upload is successfully completed. To start the cluster, refer to "Creating a cluster" in "Creating the cluster configuration data" in the "Installation and Configuration Guide".
The upload is completed successfully. To apply the changes you made, shutdown and reboot the cluster.	The upload is successfully completed. To apply the changes you made, shut down the cluster, and reboot it.
The upload was stopped. To upload the cluster configuration data, stop the cluster.	The upload was stopped. To upload the cluster configuration data, stop the cluster.
The upload was stopped. To upload the cluster configuration data, stop the Mirror Agent.	The upload was stopped. To upload the cluster configuration data, stop the Mirror Agent.
The upload was stopped. To upload the cluster configuration data, stop the resources to which you made changes.	The upload was stopped. To upload the cluster configuration data, stop the resources to which you made changes.
The upload was stopped. To upload the cluster configuration data, stop the groups to which you made changes.	The upload was stopped. To upload the cluster configuration data, suspend the cluster. To upload, stop the group to which you made changes.
The upload was stopped. To upload the cluster configuration data, suspend the cluster.	The upload was stopped. To upload the cluster configuration data, suspend the cluster.
The upload is completed successfully. To apply the changes you made, restart the Alert Sync. To apply the changes you made, restart the WebManager.	The upload is completed successfully. To apply the changes you made, restart the Alert Sync. To apply the changes you made, restart the WebManager service.

Continued on next page

Table 8.26 – continued from previous page

Message	Cause/Solution
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
The upload is completed successfully.	The upload is successfully completed.
The upload was stopped. Failed to deliver the configuration data. Check if the other server is active and run the command again.	The upload was stopped. Failed to deliver the configuration data. Check if the other server is active and run the command again.
The upload was stopped. There is one or more servers that cannot be connected to. To apply cluster configuration information forcibly, run the command again with "--force" option.	The upload was stopped. The server that cannot connect exists. To forcibly upload the cluster configuration information, run the command again with the --force option.

8.9.2 Backing up the Cluster configuration data

the clpcfctrl --pull command backups cluster configuration data.

Command line

clpcfctrl --pull -ll-w [-h *hostnamelIP*] [-p *portnumber*] [-x *directory*]

Description

This command backs up cluster configuration data to be used for the Cluster WebUI.

Option

--pull

Specify this option when performing backup. You cannot omit this option.

-l

Specify this option when backing up configuration data that is used for the Cluster WebUI on Linux.
You cannot specify both -l and -w together.

-w

Specify this option when backing up configuration data that is used for the Cluster WebUI on Windows.
You cannot specify both -l and -w together.

-h `hostname | IP`

Specifies the source server for backup. Specify a host name or IP address.
When this option is omitted, the configuration data on the server running the command is used.

-p `portnumber`

Specifies a port number of data transfer port.
When this option is omitted, the default value is used. In general, it is not necessary to specify this option.

-x directory

Backs up the configuration data in the specified directory.
Use this option with either -l or -w.
When -l is specified, configuration data is backed up in the format which can be loaded by the Cluster WebUI on Linux.
When -w is specified, configuration data is saved in the format which can be loaded by the Cluster WebUI on Windows.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as the root user.

When you run this command, access the servers in the cluster in the order below, and use one of the paths that allowed successful access.

1. via the IP address on the interconnect LAN
2. via the IP address on the public LAN

Example of command execution

Example 1: Backing up configuration data to the specified directory so that the data can be loaded by the Cluster WebUI on Linux

```
# clpcfctrl --pull -l -x /mnt/config
Command succeeded.(code:0)
```

Error Message

Message	Cause/Solution
Log in as root.	Log on as the root user.
This command is already run.	This command has been already started.
Invalid option.	The option is invalid. Check the option.
Invalid mode. Check if --push or --pull option is specified.	Check to see if the --pull is specified.
The target directory does not exist.	The specified directory does not exist.
Canceled.	Displayed when anything other than "y" is entered for command inquiry.
Failed to initialize the xml library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

Continued on next page

Table 8.27 – continued from previous page

Message	Cause/Solution
Failed to load the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to change the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to load the all.pol file. Reinstall the RPM	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to load the cfctrl.pol file. Reinstall the RPM	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the install path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the cfctrl path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM
Failed to initialize the trncl library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to connect to server %1.	Accessing the server has failed. Check if other server(s) has been started.
Check if the other server is active and then run the command again.	Run the command again after the server has started up.
Failed to connect to trnsv. Check if the other server is active.	Accessing the server has failed. Check if other server(s) has been started.
Failed to get configuration data. Check if the other server is active.	Acquiring configuration data has failed. Check if other(s) server has been started.
The directory "/work" is not found. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM
Failed to make a working directory.	Check to see if the memory or OS resource is sufficient.
The directory does not exist.	Same as above.
This is not a directory.	Same as above.
The source file does not exist.	Same as above.

Continued on next page

Table 8.27 – continued from previous page

Message	Cause/Solution
The source file is a directory.	Same as above.
The source directory does not exist.	Same as above.
The source file is not a directory.	Same as above.
Failed to change the character code set (EUC to SJIS).	Same as above.
Failed to change the character code set (SJIS to EUC).	Same as above.
Command error.	Same as above.
Failed to initialize the cfmgr library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to get size from the cfmgr library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to allocate memory.	Check to see if the memory or OS resource is sufficient.
Failed to change the directory.	Same as above.
Failed to run the command.	Same as above.
Failed to make a directory.	Same as above.
Failed to remove the directory.	Same as above.
Failed to remove the file.	Same as above.
Failed to open the file.	Same as above.
Failed to read the file.	Same as above.
Failed to write the file.	Same as above.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.9.3 Adding a resource without stopping the group

the clpcfctrl --dpush command adds a resource without stopping the group.

Command line

clpcfctrl --dpush -l|-w [-c *hostname|IP*] [-p *portnumber*] [-x *directory*] [--force]

Description

This command dynamically adds a resource without stopping the group.

Option

--dpush

Specify this option when dynamically adding a resource. You cannot omit this option.

-l

Specify this option when using the configuration data saved by the Cluster WebUI on Linux.
You cannot specify -l and -w together.

-w

Specify this option whe using the configuration data saved by the Cluster WebUI on Linux.
You cannot specify -l and -w together.

-c hostname | IP

Specifies a server to access for acquiring a list of servers. Specify a host name or IP address.
When this option is omitted, configuration data in the floppy disk will be used.

-p portnumber

Specifies a port number of data transfer port.
When this option is omitted, the default value will be used. In general, it is not necessary to specify this option.

-x directory

Specify this option when delivering configuration data to the specified directory.
This option is used with -l or -w.
When -l is specified, configuration data saved on the file system by the Cluster WebUI on Linux is used.
When -w is specified, configuration data saved by the Cluster WebUI on Windows is used.

--force
Even if there is a server that has not started, the configuration data is delivered forcefully.

Return Value

0	Success
Other than 0	Failure

Notes
Run this command as the root user.

When you run this command, access the servers in the order below, and use one of the paths that allowed successful access.

1. via the IP address on the interconnect LAN
2. via the IP address on the public LAN

For details on resources that support dynamic resource addition, refer to "How to add a resource without stopping the group" in "The system maintenance information" in the "Maintenance Guide".

To use this command, the internal version of EXPRESSCLUSTER of all the nodes in the cluster must be 3.2.1-1 or later.

While the dynamic resource addition command is running, do not resume the command. Otherwise, the cluster configuration data may become inconsistent, and the cluster may stop or the server may shut down.

If you abort the dynamic resource addition command, the activation status of the resource to be added may become undefined. In this case, run the command again or reboot the cluster manually.

Example of command execution
Example 1: Dynamically adding a resource using configuration data that was saved on the file system using the Cluster WebUI on Linux

```
# clpcfctrl --dpush -l -x /mnt/config
file delivery to server 10.0.0.11 success.
file delivery to server 10.0.0.12 success.
The upload is completed successfully.(cfmgr:0)
Command succeeded.(code:0)
```

Error Message

Message	Cause/Solution
Log in as root.	Log on as the root user.
This command is already run.	This command has been already started.
Invalid option.	The option is invalid. Check the option.
Invalid mode. Check if --push or --pull option is specified.	Check if the --push option is specified.
The target directory does not exist.	The specified directory is not found.
Invalid host name. Server specified by -h option is not included in the configuration data.	The server specified with -h is not included in configuration data. Check if the specified server name or IP address is valid.
Canceled.	Displayed when anything other than "y" is entered for command inquiry.
Failed to initialize the xml library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to load the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to change the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to load the all.pol file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to load the cfctrl.pol file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.

Continued on next page

Table 8.28 – continued from previous page

Message	Cause/Solution
Failed to get the install path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the cfctrl path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the list of group.	Failed to acquire the list of groups.
Failed to get the list of resource.	Failed to acquire the list of resources.
Failed to initialize the trncl library. Check if memory or OS resources are sufficient.	Check to see if memory or OS resource is sufficient.
Failed to connect to server %1. Check if the other server is active and then run the command again.	Accessing the server has failed. Check if other server(s) has been started. Run the command again after the server has started up.
Failed to connect to trnsv. Check if the other server is active.	Accessing the server has failed. Check if other server(s) has been started up.
Failed to get the collect size.	Getting the size of the collector file has failed. Check if other server(s) has been started.
Failed to collect the file.	Collecting the file has failed. Check if other server(s) has been started.
Failed to check server property. Check if the server name or ip addresses are correct.	Check if the server name and the IP address in the configuration information have been set correctly.
File delivery failed. Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.
Multi file delivery failed. Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.

Continued on next page

Table 8.28 – continued from previous page

Message	Cause/Solution
Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.
The directory "work" is not found. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to make a working directory.	Check if the memory or OS resource is sufficient.
The directory does not exist.	Same as above.
This is not a directory.	Same as above.
The source file does not exist.	Same as above.
The source file is a directory.	Same as above.
The source directory does not exist.	Same as above.
The source file is not a directory.	Same as above.
Failed to change the character code set (EUC to SJIS).	Same as above.
Failed to change the character code set (SJIS to EUC).	Same as above.
Command error.	Same as above.
Failed to initialize the cfmgr library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to get size from the cfmgr library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to allocate memory.	Check if the memory or OS resource is sufficient.
Failed to change the directory.	Same as above.
Failed to run the command.	Same as above.
Failed to make a directory.	Same as above.
Failed to remove the directory.	Same as above.
Failed to remove the file.	Same as above.
Failed to open the file.	Same as above.
Failed to read the file.	Same as above.
Failed to write the file.	Same as above.
Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
The upload is completed successfully. To start the cluster, refer to "How to create a cluster" in the Installation and Configration Guide.	The upload is successfully completed. To start the cluster, refer to "Creating a cluster" in "Creating the cluster configuration data" in the "Installation and Configuration Guide".

Continued on next page

Table 8.28 – continued from previous page

Message	Cause/Solution
The upload is completed successfully. To apply the changes you made, shutdown and reboot the cluster.	The upload is successfully completed. To apply the changes you made, shut down the cluster, and reboot it.
The upload was stopped. To upload the cluster configuration data, stop the cluster.	The upload was stopped. To upload the cluster configuration data, stop the cluster.
The upload was stopped. To upload the cluster configuration data, stop the Mirror Agent.	The upload was stopped. To upload the cluster configuration data, stop the Mirror Agent.
The upload was stopped. To upload the cluster configuration data, stop the resources to which you made changes.	The uploaded was stopped. To upload the cluster configuration data, stop the resource to which you made changes.
The upload was stopped. To upload the cluster configuration data, stop the groups to which you made changes.	The upload was stopped. To upload the cluster configuration data, suspend the cluster. To upload, stop the group to which you made changes.
The upload was stopped. To upload the cluster configuration data, suspend the cluster.	The upload was stopped. To upload the cluster configuration data, suspend the cluster.
The upload is completed successfully. To apply the changes you made, restart the Alert Sync. To apply the changes you made, restart the WebManager.	The upload is completed successfully. To apply the changes you made, restart the Alert Sync service. To apply the changes you made, restart the WebManager service.
The upload is completed successfully.	The upload is successfully completed.
The upload was stopped. Failed to deliver the configuration data. Check if the other server is active and run the command again.	The upload was stopped. Failed to deliver the cluster configuration data. Check if the other server is active and run the command again.

Continued on next page

Table 8.28 – continued from previous page

Message	Cause/Solution
The upload was stopped. There is one or more servers that cannot be connected to. To apply cluster configuration information forcibly, run the command again with "--force" option.	The upload was stopped. The server that cannot connect exists. To forcibly upload the cluster configuration information, run the command again with the --force option.
The upload was stopped. Failed to active resource. Please check the setting of resource.	The upload was stopped. Failed to activate the resource. Check the setting of the resource.

8.9.4 Checking cluster configuration data

the clpcfctrl -- compcheck command checks cluster configuration data.

Comand line

clpcfctrl --compcheck -ll-w [-c *hostname|IP*] [-p *portnumber*] [-x *directory*]

Description

This command checks whether or not cluster configuration data is correct.

Option

--compcheck

Specify this option when checking configuration data.
You cannot omit this option.

-l

Specify this option when using the configuration data saved by the Cluster WebUI on Linux.
You cannot specify -l and -w together.

-w

Specify this option whe using the configuration data saved by the Cluster WebUI on Linux.
You cannot specify -l and -w together.

-x directory

Specify this option when delivering configuration data to the specified directory.
This option is used with -l or -w.
When -l is specified, configuration data saved on the file system by the Cluster WebUI on Linux is used.
When -w is specified, configuration data saved by the Cluster WebUI on Windows is used.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as the root user.

When you run this command, access the cluster servers in the order below, and use one of the paths that allowed successful access.

1. Via the IP address on the interconnect LAN
2. Via the IP address on the public LAN

This command finds the difference between the new and existing configuration data, and checks the resource configuration data in the added configuration data.

Example of command execution

Example 1: Checking configuration data that was saved on the file system using the Cluster WebUI on Linux

```
# clpcfctrl --compcheck -l -x /mnt/config
The check is completed successfully.(cfmgr:0)
Command succeeded.(code:0)
```

Error Message

Message	Cause/Solution
Log in as root.	Log in as the root user.
This command is already run.	This command has been already started.
Invalid option.	The option is invalid. Check the option.
The target directory does not exist.	The specified directory is not found.
Canceled.	Displayed when anything other than "y" is entered for command inquiry.
Failed to initialize the xml library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to load the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to change the configuration file. Check if memory or OS resources are sufficient.	Same as above.
Failed to load the all.pol file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.

Continued on next page

Table 8.29 – continued from previous page

Message	Cause/Solution
Failed to load the cfctrl.pol file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the install path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the cfctrl path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the list of group.	Failed to acquire the list of group.
Failed to get the list of resource.	Failed to acquire the list of resource.
Failed to initialize the trncl library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to connect to server %1. Check if the other server is active and then run the command again.	Accessing the server has failed. Check if other server(s) has been started. Run the command again after the server has started up.
Failed to connect to trnsv. Check if the other server is active.	Accessing the server has failed. Check that other server has been started up.
Failed to get the collect size.	Getting the size of the collector file has failed. Check if other server(s) has been started.
Failed to collect the file.	Collecting of the file has failed. Check if other server(s) has been started.
Failed to get the list of node. Check if the server specified by -c is a member of the cluster.	Check to see if the server specified by -c is a cluster member.
Failed to check server property. Check if the server name or ip addresses are correct.	Check if the server name and the IP address in the configuration information have been set correctly.
File delivery failed. Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.

Continued on next page

Table 8.29 – continued from previous page

Message	Cause/Solution
Multi file delivery failed. Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.
Failed to deliver the configuration data. Check if the other server is active and run the command again.	Delivering configuration data has failed. Check if other server(s) has been started. Run the command again after the server has started up.
The directory "work" is not found. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to make a working directory.	Check if the memory or OS resource is sufficient.
The directory does not exist.	Same as above.
This is not a directory.	Same as above.
The source file does not exist.	Same as above.
The source file is a directory.	Same as above.
The source directory does not exist.	Same as above.
The source file is not a directory.	Same as above.
Failed to change the character code set (EUC to SJIS).	Same as above.
Failed to change the character code set (SJIS to EUC).	Same as above.
Command error.	
Failed to initialize the cfmgr library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to get size from the cfmgr library. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.
Failed to allocate memory.	Check if the memory or OS resource is sufficient.
Failed to change the directory.	Same as above.
Failed to run the command.	Same as above.
Failed to make a directory.	Same as above.
Failed to remove the directory.	Same as above.
Failed to remove the file.	Same as above.
Failed to open the file.	Same as above.
Failed to read the file.	Same as above.
Failed to write the file.	Same as above.
Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.

8.10 Adjusting time-out temporarily (clptoratio command)

the clptoratio command extends or displays the current time-out ratio.

Command line

clptoratio -r *ratio* -t *time*
clptoratio -i
clptoratio -s

Description

This command displays or temporarily extends the various time-out values of the following on all servers in the cluster.

- Monitor resource
- Heartbeat resource (except kernel heartbet resource)
- Mirror Agent
- Mirror driver
- Alert synchronous service
- WebManager service

Option

-r ratio

Specifies the time-out ratio. Use 1 or larger integer. The maxim time-out ratio is 10,000.
If you specify "1," you can return the modified time-out ratio to the original as you can do so when you are using the -i option.

-t time

Specifies the extension period.
You can specify minutes for m, hours for h, and days for d. The maximum period of time is 30 days.
Example: 2m, 3h, 4d

-i

Sets back the modified time-out ratio.

-s

Refers to the current time-out ratio.

Return Value

0	Success
Other than 0	Failure

Remarks

When the cluster is shutdown, the time-out ratio you have set will become ineffective. However, if any server in the cluster is not shutdown, the time-out ratio and the extension period that you have set will be maintained.

With the -s option, you can only refer to the current time-out ratio. You cannot see other information such as remaining time of extended period.

You can see the original time-out value by using the status display command.

Heartbeat time-out

```
# clpstat --cl --detail
```

Monitor resource time-out

```
# clpstat --mon monitor resource name --detail
```

Notes

Run this command as the root user.

Make sure that the cluster daemon is activated in all servers in the cluster.

When you set the time-out ratio, make sure to specify the extension period. However, if you set "1" for the time-out ratio, you cannot specify the extension period.

You cannot specify a combination such as "2m3h," for the extension period.

When the server restarts within the ratio extension period, the time-out ratio is not returned to the original even after the extension period. In this case, run the clptoratio -i command to return it to the original.

Example of a command entry

Example 1: Doubling the time-out ratio for three days

```
# clptoratio -r 2 -t 3d
```

Example 2: Setting back the time-out ratio to original

```
# clptoratio -i
```

Example 3: Referring to the current time-out ratio

```
# clptoratio -s
present toratio : 2
```

The current time-out ratio is set to 2.

Error Message

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid configuration file. Create valid cluster configuration data.	Create valid cluster configuration data by using the Cluster WebUI.
Invalid option.	Specify a valid option.
Specify a number in a valid range.	Specify a number within a valid range.
Specify a correct number.	Specify a valid number.
Scale factor must be specified by integer value of 1 or more.	Specify 1 or larger integer for ratio.
Specify scale factor in a range less than the maximum scale factor.	Specify a ratio that is not larger than the maximum ratio.
Set the correct extension period.	Set a valid extension period.
Ex) 2m, 3h, 4d	Set the extension period which does not exceed the maximum ratio.

Continued on next page

Table 8.30 – continued from previous page

Message	Cause/Solution
Set the extension period in a range less than the maximum extension period.	Check if the cluster daemon is activated.
Could not connect to the server. Check if the cluster daemon is active.	Check if the cluster daemon is activated.
Server is not active. Check if the cluster daemon is active.	Check if there is any server in the cluster with the cluster daemon stopped.
Connection was lost. Check if there is a server where the cluster daemon is stopped in the cluster.	Check if there is any server in the cluster with the cluster daemon stopped.
Invalid parameter.	The value specified as a parameter of the command may be invalid.
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set the longer timeout.	Time-out has occurred in the internal communication of EXPRESSCLUSTER. If it occurs frequently, set the internal communication time-out longer.
Processing failed on some servers. Check the status of failed servers.	There are servers that failed in processing. Check the status of server in the cluster. Operate it while all the servers in the cluster are up and running.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.11 Modifying the log level and size (clplogcf command)

the clplogcf command modifies and displays log level and log output file size.

Command line

clplogcf -t *type* -l *level* -s *size*

Description

This command modifies the log level and log output file size, or displays the values currently configured.

Option

-t type

Specifies a module type whose settings will be changed.
If both -l and -s are omitted, the information set to the specified module will be displayed. For the types which can be specified, see the list of "**Types that can be specified for the -t option**".

-l level

Specifies a log level.
You can specify one of the following for a log level.
1, 2, 4, 8, 16, 32
You can see more detailed information as the log level increases.
For the default values for each module type, see the list of "Default log levels and log file sizes".

-s size

Specifies the size of a file for log output.
The unit is byte.

None

None Displays the entire configuration information currently set.

Return Value

0	Success
Other than 0	Failure

Remarks

Each type of output logs from EXPRESSCLUSTER uses four log files. Therefore, it is necessary to have the disk space that is four times larger than what is specified by -s.

Notes

Run this command as the root user.

To run this command, the EXPRESSCLUSTER event service must be started.

The changes made are effective only for the server on which this command was run.
The settings revert to the default values when the server restarts.

Example of command execution

Example 1: Modifying the pm log level

```
# clplogcf -t pm -l 8
```

Example 2: Seeing the pm log level and log file size

```
# clplogcf -t pm
TYPE, LEVEL, SIZE
pm, 8, 1000000
```

Example 3: Displaying the values currently configured

```
# clplogcf
TYPE, LEVEL, SIZE
trnsv, 4, 1000000
xml, 4, 1000000
logcf, 4, 1000000
```

Error Message

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid option.	The option is invalid. Check the option.
Failed to change the configuration. Check if clpevent is running.	clpevent may not have been started.
Invalid level	The specified level is invalid.
Invalid size	The specified size is invalid.
Failed to load the configuration file. Check if memory or OS resources are sufficient.	Non-clustered server
Failed to initialize the xml library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to print the configuration. Check if clpevent is running.	clpevent may not be started yet.

Types that can be specified for the -t option (y=yes, n=no)

Type	Module	Description	The EXPRESSCLUSTER Server	Replicator	Replicator DR
apicl	libclpapicl.so.1.0	API client library	y	y	y
apisv	libclpapisv.so.1.0	API server	y	y	y
bmccnf	clpbmccnf	BMC information update command	y	y	y
cl	clpcl	Cluster startup and stop command	y	y	y
cfctrl	clpcfctrl	Cluster generation, cluster information and backup command	y	y	y
cfmgr	libclpcfmgr.so.1.0	Cluster configuration data operation library	y	y	y
cpufreq	clpcpufreq	CPU Frequency control command	y	y	y
down	clpdown	Server stopping command	y	y	y
grp	clpgrp	Group startup, stop, move, and migration command	y	y	y
rsc	clprsc	Group resource startup and stop command	y	y	y
haltp	clpuserw	Shutdown monitoring	y	y	y
healthchk	clphealthchk	Process health check command	y	y	y
ibsv	clpibsv	Information Base server	y	y	y
lcns	libclplcns.so.1.0	License library	y	y	y
lcnsc	clplcnsc	License registration command	y	y	y
ledctrl	clpledctrl	Chassis identify control command	y	y	y
logcc	clplogcc	Collect Logs command	y	y	y
logcf	clplogcf	Log level and size modification command	y	y	y

Continued on next page

Table 8.32 – continued from previous page

Type	Module	Description	The EXPRESS-CLUSTER Server	Replicator	Replicator DR
logcmd	clplogcmd	Alert producing command	y	y	y
mail	clpmail	Mail Report	y	y	y
mgtmib	libclpmgtmib.so.1.0	SNMP coordination library	y	y	y
mm	libclpmm.so.1.0	External monitoring coordination library	y	y	y
monctrl	clpmonctrl	Monitoring control command	y	y	y
nm	clpnm	Node map management	y	y	y
pm	clppm	Process management	y	y	y
rc/rc_ex	clprc	Group and group resource management	y	y	y
reg	libclpreg.so.1.0	Reboot count control library	y	y	y
regctrl	clpregctrl	Reboot count control command	y	y	y
rm	clprm	Monitor management	y	y	y
roset	clproset	Disk control	y	y	y
relpath	clprelpath	Process kill command	y	y	y
scrpc	clpscrpc	Script log rotation command	y	y	y
skgxnr	libclpskgxnr.so.1.0	Oracle Clusterware linkage library	y	y	y
stat	clpstat	Status display command	y	y	y
stdn	clpstdn	Cluster shutdown command	y	y	y
toratio	clptoratio	Time-out ratio modification command	y	y	y
trap	clptrap	SNMP trap command	y	y	y
trncl	libclptrncl.so.1.0	Transaction library	y	y	y
trnreq	clptrnreq	Inter-cluster processing request command	y	y	y
rexec	clprexec	External monitoring link processing request command	y	y	y
bwctrl	clpbwctrl	Cluster activation synchronization wait processing control command	y	y	y
trnsv	clptrnsv	Transaction server	y	y	y
vxdgc	clpvxdgc	VxVM disk group import/deport command	y	y	y
alert	clpaltinsert	Alert	y	y	y
webmgr	clpwebmc	WebManager server	y	y	y
webalert	clpaltd	Alert synchronization	y	y	y

Continued on next page

Table 8.32 – continued from previous page

Type	Module	Description	The EXPRESS-CLUSTER Server	Replicator	Replicator DR
rd	clprd	Process for smart failover	y	y	y
rdl	libclprdl.so.1.0	Library for smart failover	y	y	y
disk	clpdisk	Disk resource	y	y	y
disk_fsck	clpdisk	Disk resource	y	Y	Y
exec	clpexec	Exec resource	y	y	y
fip	clpfip	FIP resource	y	y	y
fipw	clpfipw	FIP monitor resource	y	y	y
nas	clpnas	NAS resource	y	y	y
volmgr	clpvolmgr	Volume manager resource	y	y	y
vip	clpvip	Virtual IP resource	y	y	y
vm	clpvm	VM resource	y	y	y
ddns	clpddns	Dynamic DNS resource	y	y	y
arpw	clparpw	ARP monitor resource	y	y	y
bmcw	clpbmcw	BMC monitor resource	y	y	y
diskw	clpdiskw	Disk monitor resource	y	y	y
ipw	clpipw	IP monitor resource	y	y	y
miiw	clpmiiw	NIC link up/down monitor resource	y	y	y
mtw	clpmtw	Multi target monitor resource	y	y	y
osmw	clposmw	Oracle Clusterware Synchronization Management monitor resource	y	y	y
pidw	clppidw	PID monitor resource	y	y	y
volmgrw	clpvolmgrw	Volume manager monitor resource	y	y	y
userw	clpuserw	User-mode monitor resource	y	y	y
vipw	clpvipw	Virtual IP monitor resource	y	y	y
vmw	clpvmw	VM monitor resource	y	y	y
ddnsw	clpddnsw	Dynamic DNS monitor resource	y	y	y
mrw	clpmrw	Message receive monitor resource	y	y	y
genw	clpgenw	Custom monitor resource	y	y	y
bmchb	clpbmchb	BMC heartbeat	y	y	y
bmccmd	libclpbmc	BMC heartbeat library	y	y	y
snmpmgr	libclp snmpmgr	SNMP trap reception library	y	y	y
comhb	clpcomhb	COM heartbeat	y	y	y
diskhb	clpdiskhb	Disk heartbeat	y	y	y
lanhb	clplanhb	LAN heartbeat	y	y	y

Continued on next page

Table 8.32 – continued from previous page

Type	Module	Description	The EXPRESS-CLUSTER Server	Replicator	Replicator DR
lankhb	clplankhb	Kernel mode LAN heartbeat	y	y	y
pingnp	libclppingnp.so.1.0	PING network partition resolution	y	y	y
exping	libclppingnp.so.1.0	PING network partition resolution	y	y	y
mdadmn	libclpmdadmn.so.1.0	Mirror disk admin library	n	y	y
mdfunc	libclpmdfunc.so.1.0	Mirror disk function library	n	y	y
mdagent	clpmdagent	Mirror agent	n	y	y
mdctrl	clpmdctrl	Mirror disk resource operation command	n	y	n
mdinit	clpmdinit	Mirror disk initialization command	n	y	n
mdstat	clpmdstat	Mirror status display command	n	y	n
hdctrl	clphdctrl	Hybrid disk resource operation command	n	n	y
hdinit	clphdinit	Hybrid disk resource initialization command	n	n	y
hdstat	clphdstat	Hybrid status display command	n	n	y
md	clpmd	Mirror disk resource	n	y	n
md_fsck	clpmd	Mirror disk resource	n	y	n
mdw	clpmdw	Mirror disk monitor resource	n	y	n
mdnw	clpmdnw	Mirror disk connect monitor resource	n	y	n
hd	clphd	Hybrid disk resource	n	n	y
hd_fsck	clphd	Hybrid disk resource	n	n	y
hdw	clphdw	Hybrid disk monitor resource	n	n	y
hdnw	clphdnw	Hybrid disk connect monitor resource	n	n	y
oraclew	clp_oraclew	Oracle monitor resource	y	y	y
db2w	clp_db2w	DB2 monitor resource	y	y	y
psqlw	clp_psqlw	PostgreSQL monitor resource	y	y	y
mysqlw	clp_mysqlw	MySQL monitor resource	y	y	y
sybasew	clp_sybasew	Sybase monitor resource	y	y	y
odbcw	clp_odbcw	ODBC monitor resource	y	y	y
sqlserverw	clp_sqlserverw	SQL Server monitor resource	y	y	y

Continued on next page

Table 8.32 – continued from previous page

Type	Module	Description	The EXPRESS-CLUSTER Server	Replicator	Replicator DR
sambaw	clp_sambaw	Samba monitor resource	y	y	y
nfsw	clp_nfsw	NFS monitor resource	y	y	y
httpw	clp_httpw	HTTP monitor resource	y	y	y
ftpw	clp_ftpw	FTP monitor resource	y	y	y
smtpw	clp_smtpw	SMTP monitor resource	y	y	y
pop3w	clp_pop3w	POP3 monitor resource	y	y	y
imap4w	clp_imap4w	IMAP4 monitor resource	y	y	y
tuxw	clp_tuxw	Tuxedo monitor resource	y	y	y
wlsw	clp_wlsw	WebLogic monitor resource	y	y	y
wasw	clp_wasw	WebSphere monitor resource	y	y	y
otxw	clp_otxw	WebOTX monitor resource	y	y	y
jraw	clp_jraw	JVM monitor resource	y	y	y
sraw	clp_sraw	System monitor resource	y	y	y
psrw	clp_psrw	Process resource monitor resource	y	y	y
psw	clppsw	Process name monitor resource	y	y	y
mdperf	clpmdperf	Disk related information	n	y	y
vmctrl	libclpvmctrl.so.1.0	VMCtrl library	y	y	y
vmwcmd	clpvmwcmd	VMW command	y	y	y
awseip	clpawseip	AWS Elastic IP resource	y	y	y
awsvip	clpawsvip	AWS Virtual IP resource	y	y	y
awsdns	clpawsdns	AWS DNS resource	y	y	y
awseipw	clpawseipw	AWS Elastic IP monitor resource	y	y	y
awsvipw	clpawsvipw	AWS Virtual IP monitor resource	y	y	y
awsazw	clpawsazw	AWS AZ monitor resource	y	y	y
awsdnsw	clpawsdnsw	AWS DNS monitor resource	y	y	y
azurepp	clpazurepp	Azure probe port resource	y	y	y
azuredns	clpazuredns	Azure DNS resource	y	y	y
azureppw	clpazureppw	Azure probe port monitor resource	y	y	y

Continued on next page

Table 8.32 – continued from previous page

Type	Module	Description	The EXPRESS-CLUSTER Server	Replicator	Replicator DR
azurelbw	clpazurelbw	Azure load balance monitor resource	y	y	y
azurednsw	clpazurednsw	Azure DNS monitor resource	y	y	y
gcvip	clpgcvip	Google Cloud Virtual IP resource	y	y	y
gcvipw	clpgcvipw	Google Cloud Virtual IP monitor resource	y	y	y
gclbw	clpgclbw	Google Cloud load balance monitor resource	y	y	y
ocvip	clpocvip	Oracle Cloud Virtual IP resource	y	y	y
ocvipw	clpocvipw	Oracle Cloud Virtual IP monitor resource	y	y	y
oclbw	clpoclbw	Oracle Cloud load balance monitor resource	y	y	y
perfc	clpperfc	Cluster statistics information display command	y	y	y
cfchk	clpcfchk	Cluster configuration information check command	y	y	y

Default log levels and log file sizes

Type	Level	Size (byte)
apicl	4	5000000
apisv	4	5000000
bmccnf	4	1000000
cfmgr	4	1000000
cl	4	1000000
cfctrl	4	1000000
cpufreq	4	1000000
down	4	1000000
grp	4	1000000
rsc	4	1000000
haltp	4	1000000
healthck	4	1000000
ibsv	4	5000000
lcns	4	1000000
lcnsc	4	1000000
ledctrl	4	1000000
logcc	4	1000000
logcf	4	1000000
logcmd	4	1000000
mail	4	1000000
mgtmib	4	1000000

Continued on next page

Table 8.33 – continued from previous page

Type	Level	Size (byte)
mm	4	2000000
monctrl	4	1000000
nm	4	2000000
pm	4	1000000
rc	4	5000000
rc_ex	4	5000000
rd	4	1000000
rdl	4	1000000
reg	4	1000000
regctrl	4	1000000
rm	4	5000000
roset	4	1000000
relpath	4	1000000
scrpc	4	1000000
skgxnr	4	1000000
stat	4	1000000
stdn	4	1000000
toratio	4	1000000
trap	4	1000000
trncl	4	2000000
trnreq	4	1000000
rexec	4	1000000
trnsv	4	2000000
vxdgc	4	1000000
alert	4	1000000
webmgr	4	1000000
webalert	4	1000000
disk	4	2000000
disk_fsck	4	1000000
exec	4	1000000
fip	4	1000000
fipw	4	1000000
nas	4	1000000
volmgr	4	1000000
vip	4	1000000
vm	4	1000000
ddns	4	1000000
bwctrl	4	1000000
arpw	4	1000000
bmcw	4	1000000
db2w	4	4000000
diskw	4	1000000
ftpw	4	1000000
httpw	4	1000000
imap4w	4	1000000
ipw	4	1000000
miiw	4	1000000
mtw	4	1000000
mysqlw	4	4000000

Continued on next page

Table 8.33 – continued from previous page

Type	Level	Size (byte)
nfsw	4	1000000
odbcw	4	4000000
oraclew	4	4000000
osmw	4	1000000
otxw	4	1000000
pidw	4	1000000
pop3w	4	1000000
psqlw	4	4000000
volmgrw	4	1000000
sambaw	4	1000000
smtpw	4	1000000
sqlserverw	4	4000000
sybasew	4	4000000
tuxw	4	1000000
userw	4	1000000
vipw	4	1000000
vmw	4	1000000
ddnsw	4	1000000
mrw	4	1000000
genw	4	1000000
wasw	4	1000000
wlsw	4	1000000
jraw	4	1000000
sraw	4	1000000
psrw	4	1000000
psw	4	1000000
bmchb	4	1000000
bmccmd	4	1000000
snmpmgr	4	1000000
comhb	4	1000000
diskhb	4	1000000
lanhb	4	1000000
lankhb	4	1000000
pingnp	4	1000000
exping	4	1000000
mdadmn	4	10000000
mdfunc	4	10000000
mdagent	4	10000000
mdctrl	4	10000000
mdinit	4	10000000
mdstat	4	10000000
hdctrl	4	10000000
hdinit	4	10000000
hdstat	4	10000000
md	4	10000000
md_fsck	4	10000000
mdw	4	10000000
mdnw	4	10000000
hd	4	10000000

Continued on next page

Table 8.33 – continued from previous page

Type	Level	Size (byte)
hd_fsck	4	10000000
hdw	4	10000000
hdnw	4	10000000
vmctrl	4	10000000
vmwcmd	4	1000000
liscal[1]	-	0
clpka[1]	-	0
clpkhb[1]	-	0
awseip	4	10000000
awsvip	4	10000000
awsdns	4	10000000
awseipw	4	10000000
awsvipw	4	10000000
awsazw	4	10000000
awsdnsw	4	10000000
azurepp	4	10000000
azuredns	4	10000000
azureppw	4	10000000
azurelbw	4	10000000
azurednsw	4	10000000
gcvip	4	10000000
gcvipw	4	10000000
gclbw	4	10000000
ocvip	4	10000000
ocvipw	4	10000000
perfc	4	1000000
cfchk	4	1000000

* If the module's size is zero, its log will not be produced.

8.12 Managing licenses (clplcnsc command)

the clplcnsc command manages licenses.

Command line

clplcnsc -i [*licensefile...*]
clplcnsc -l *[-a]*
clplcnsc -d *serialno [-q]*
clplcnsc *-d -t [-q]*
clplcnsc -d -a [-q]
clplcnsc --distribute
clplcnsc --reregister *licensefile...*

Description

This command registers, refers to and remove the licenses of the product version and trial version of this product.

[1] Output destination of log is syslog.

Option

-i [licensefile...]
When a license file is specified, license information is acquired from the file for registration. You can specify multiple licenses. If nothing is specified, you need to enter license information interactively.

-l [-a]
References the registered license. The name of displayed items are as follows.

Item	Explanation
Serial No	Serial number (product version only)
User name	User name (trial version only)
Key	License key
Licensed Number of CPU	The number of license (per CPU)
Licensed Number of Computers	The number of license (per node)
Start date	Start date of valid period[2][3]
End date	End date of valid period[2][3]
Status	Status of the license

Status	Explanation
valid	valid
invalid	invalid
unknown	unknown
inactive	Before valid period[2][3]
expired	After valid period[2][3]

When -a option not specifed, the license status of "invalid", "unknown" and "expired" are not displayed.

When specifying -a option, all the licenses are displayed regardless of the license status.

-d <param>
param

serialno Deletes the license with the specified serial number.

-t Deletes all the registered licenses of the trial version.

-a Deletes all the registered licenses.

-q
Deletes licenses without displaying a warning message. This is used with -d option.

--distribute
License files are delivered to all servers in the cluster. Generally, it is not necessary to run the command with this option.

--reregister licensefile...
Reregisters the fixed term license. Generally, it is not necessary to run the command with this option.

Return Value

[2] Displayed in the case of the fixed term license
[3] Displayed in the case of the license of trial version

0	Normal termination
1	Cancel
2	Normal termination (with licenses not synchronized) * This means that license synchronization failed in the cluster at the time of license registration. For the actions to be taken, refer to "Troubleshooting for licensing" in Appendix A "Troubleshooting" in the "Installation and Configuration Guide".
3	Initialization error
5	Invalid option
8	Other internal error

Example of a command entry

- for registration
  - Registering the license interactively

```
# clplcnsc -i
```

Product Version/Product Version (Fixed Term)

Select a product division

```
Selection of License Version
  1. Product Version
  2. Trial Version
  e. Exit
Select License Version. [1, 2, or e (default:1)] ...
```

Enter a serial number

```
Enter serial number [ Ex. XXXXXXXX000000] .
```

Enter a license key

```
Enter license key
[ Ex. XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX] ...
```

Trial Version

Select a product division

```
Selection of License Version
  1. Product Version
  2. Trial Version
  e. Exit
Select License Version. [1, 2, or e (default:1)] ...
```

Enter a user name

```
Enter user name [ 1 to 63byte ] .
```

Enter a license key

```
Enter license key
[Ex. XXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX].
```

  - Specify a license file

```
# clplcnsc -i /tmp/cpulcns.key
```

- for referring to the license

```
# clplcnsc -l
```

Product version

```
< EXPRESSCLUSTER X <PRODUCT> >
Seq... 1
    Key..... A1234567-B1234567-C1234567-D1234567
    Licensed Number of CPU... 2
    Status... valid
Seq... 2
    Serial No..... AAAAAAAA000002
    Key..... E1234567-F1234567-G1234567-H1234567
    Licensed Number of Computers... 1
    Status... valid
```

Product version (fixed term)

```
< EXPRESSCLUSTER X <PRODUCT> >

Seq... 1
    Serial No..... AAAAAAAA000001
    Key..... A1234567-B1234567-C1234567-D1234567
    Start date..... 2018/01/01
    End date...... 2018/01/31
    Status.......... valid
Seq... 2
    Serial No..... AAAAAAAA000002
    Key..... E1234567-F1234567-G1234567-H1234567
    Status.......... inactive
```

Trial version

```
< EXPRESSCLUSTER X <TRIAL> >
Seq... 1
    Key..... A1234567-B1234567-C1234567-D1234567
    User name... NEC
    Start date..... 2018/01/01
    End date...... 2018/02/28
    Status.......... valid
```

- for deleting the license

```
# clplcnsc -d AAAAAAAA000001 -q
```

- for referring todeleting the license

```
# clplcnsc -d -t -q
```

- for deleting the license

```
# clplcnsc -d -a
```

Deletion confirmation

```
Are you sure to remove the license? [y/n] ...
```

Notes

Run this command as the root user.

When you register a license, verify that the data transfer server is started up and a cluster has been generated for license synchronization.

When synchronizing the licenses, access the cluster servers in the order below, and use one of the paths that allowed successful access:

1. via the IP address on the interconnect LAN
2. via the IP address on the public LAN
3. via the IP address whose name was resolved by the server name in the cluster configuration data.

When you delete a license, only the license information on the server where this command was run is deleted. The license information on other servers is not deleted. To delete the license information in the entire cluster, run this command in all servers.

Furthermore, when you use -d option and -a option together, all the trial version licenses and product version licenses will be deleted. To delete only the trial license, also specify the -t option. If the licenses including the product license have been deleted, register the product license again.

When you refer to a license which includes multiple licenses, all included licenses information are displayed.

If one or more servers in the cluster are not working, it may take time to execute this command.

Error Messages

Message	Cause/Solution
Processed license num (success : %d error : %d).	The number of processed licenses (success:%d error:%d) If error is not 0, check if the license information is correct.
Command succeeded.	The command ran successfully.
Command failed.	The command did not run successfully.
Command succeeded. But the license was not applied to all the servers in the cluster because there are one or more servers that are not started up.	There is one or more server that is not running in the cluster. Perform the cluster generation steps in all servers in the cluster. Refer to "Installing EXPRESSCLUSTER" the "Installation and Configuration Guide" for information on cluster generation.
Log in as root.	You are not authorized to run this command. Log on as the root user.
Invalid cluster configuration data. Check the cluster configuration information.	The cluster configuration data is invalid. Check the cluster configuration data by using the Cluster WebUI.

Continued on next page

Table 8.34 – continued from previous page

Message	Cause/Solution
Initialization error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
The command is already run.	The command is already running. Check the running status by using a command such as the ps command.
The license is not registered.	The license has not been registered yet.
Could not open the license file. Check if the license file exists on the specified path.	Input/Output cannot be done to the license file. Check to see if the license file exists in the specified path.
Could not read the license file. Check if the license file exists on the specified path.	Same as above.
The field format of the license file is invalid. The license file may be corrupted. Check the destination from where the file is sent.	The field format of the license file is invalid. The license file may be corrupted. Check it with the file sender.
The cluster configuration data may be invalid or not registered.	The cluster configuration data may be invalid or not registered. Check the configuration data.
Failed to terminate the library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to register the license. Check if the entered license information is correct.	Check to see if the entered license information is correct.
Failed to open the license. Check if the entered license information is correct.	Same as above.
Failed to remove the license.	License deletion failed. Parameter error may have occurred or resources (memory or OS) may not be sufficient.
This license is already registered.	This license has already been registered. Check the registered license.
This license is already activated.	This license has already been activated. Check the registered license.
This license is unavailable for this product.	This license is unavailable for this product. Check the license.
The maximum number of licenses was reached.	The maximum number of registrable licenses was reached. Delete the expired licenses.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.13 Locking disk I/O (clproset command)

the clproset command modifies and displays I/O permission of the partition device.

Command line

clproset -o [-d *device_name* | -r *resource_name* -t *resource_type* | -a | --lockout]
clproset -w [-d *device_name* | -r *resource_name* -t *resource_type* | -a | --lockout]
clproset -s [-d *device_name* | -r *resource_name* -t *resource_type* | -a | --lockout]

Description

This command configures the partition device I/O permission of a shared disk to ReadOnly/ReadWrite possible.

This command displays the configured I/O permission status of the partition device.

Option

-o
Sets the partition device I/O to ReadOnly. When ReadOnly is set to a partition device, you cannot write the data into the partition device.

-w
Sets the partition device I/O to ReadWrite possible. When ReadWrite is set to a partition device, you may read from and write the data into the partition device.

-s
Displays the I/O permission status of the partition device.

-d `device_name`
Specifies a partition device.

-r `resource_name`
Specifies a disk resource name.

-t `resource_type`
Specifies a group resource type. For the current EXPRESSCLUSTER version, always specify "disk" as group resource type.

-a
Runs this command against all disk resources.

--lockout
Runs this command against the device specified as a disk lock device.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as the root user.

This command can only be used on shared disk resources. It cannot be used for mirror disk resources and hybrid disk resources.

Make sure to specify a group resource type when specifying a resource name.

Example of command execution

Example 1: When changing the I/O of disk resource name, disk1, to RW:

```
# clproset -w -r disk1 -t disk
/dev/sdb5 : success
```

Example 2: When acquiring I/O information of all resources:

```
# clproset -s -a
/dev/sdb5 : rw (disk)
/dev/sdb6 : ro (raw)
/dev/sdb7 : ro (lockout)
```

Error Messages

Message	Cause/Solution
Log in as root.	Log on as the root user.
Invalid configuration file. Create valid cluster configuration data.	Create valid cluster configuration data by using the Cluster WebUI.
Invalid option.	Specify a valid option.
The -t option must be specified for the -r option.	Be sure to specify the -t option when using the -r option.
Specify 'disk' or 'raw to specify a group resource.	Specify "disk" or "raw" when specifying a group resource type.
Invalid group resource name. Specify a valid group resource name in the cluster.	Specify a valid group resource name.
Invalid device name.	Specify a valid device name.
Command timeout.	The OS may be heavily loaded. Check to see how heavily it is loaded.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

Note:

Do not use this command for the purposes other than those mentioned in "Verifying operation" in the "Installation and Configuration Guide".

If you run this command while the cluster daemon is activated, the file system may get corrupted.

8.14 Mirror-related commands

8.14.1 Displaying the mirror status (clpmdstat command)

the clpmdstat command displays status related to mirroring and configuration information.

Command line

clpmdstat {--connect | -c} *mirrordisk-alias*
clpmdstat {--mirror | -m} *mirrordisk-alias*
clpmdstat {--active | -a} *mirrordisk-alias*

clpmdstat {--detail | -d} *mirrordisk-alias*
clpmdstat {--list | -l}
clpmdstat {--perf | -p} [*interval* [*count*]] *mirrordisk-alias*

Description

This command displays the status related to mirroring.

This command displays mirror disk resources configuration information.

Option

--connect,-c
Displays mirror disk connect status.

--mirror,-m
Displays mirror disk resource status.

--active,-a
Displays status of mirror disk activation.

--detail,-d
Displays mirror disk resources configuration information.

--list,-l
Displays mirror disk resources list.

--perf
Displays statistical information on mirror disk resources.

Parameter

mirrordisk-alias
Specifies a mirror disk resource name.

interval

Specifies the sampling interval for statistical information.
If no value is specified, 60 (sec) is specified by default.
You can specify a value from 1 to 9999.

count

Specifies the number of times statistical information is displayed.
This parameter is used together with the *interval*. You can specify a value from 1 to 9999.
When *count* is omitted, statistical information is displayed indefinitely.
To stop displaying statistical information, press [Ctrl] + [C].
Both the default value of *interval*, 60, and of *count*, 1, are used if these parameters are omitted.

Return value

0	Success
Other than 0	Failure

Notes

Run this command as the root user.

Example display after running this command

An example of the display after running this command is provided in the next topic.

Error Messages

Message	Cause/Solution
Error: Log in as root.	Log on as the root user.
Error: Failed to read the configuration file. Check if it exists or is configured properly.	Reading the configuration file has failed. Check to see if the configuration file exists and is configured correctly.
Error: Failed to acquire mirror disk resource name. Check if the Mirror Agent is operating normally.	Acquiring a mirror disk resource name has failed. Check to see if the Mirror Agent is operating normally.
Error: Specified mirror disk resource was not found. Specify a valid mirror disk resource name.	Failed to the specified mirror disk resource. Specify a valid mirror disk resource name.
Error: Invalid mirror-alias. Specify a valid mirror disk resource name.	Specify a valid mirror disk resource name.
Error: Failed to get the server name. Check if the configuration file is correct and the Mirror Agent is operating normally.	Acquiring a server name has failed. Check to see if the configuration file is valid and the Mirror Agent is operating normally.
Error: Failed to communicate with other servers. Check if the Mirror Agent of the other server is operating normally and the interconnect LAN is connected.	Communicating with the remote server has failed. Check if the Mirror Agent in the remote server is operating normally and the interconnect is connected.
Error: Mirror disks of the remote server may be down. Check if the Mirror Agent of the remote server is operating normally and the interconnect LAN is connected.	Communicating with the remote server has failed. Check to see if the Mirror Agent in the remote server is operating normally, and the interconnect is connected.
Error: Failed to get the mirror disk status. Check if the Mirror Agent on the local server is operating normally.	Acquiring the mirror disk status has failed. Check to see if the Mirror Agent in the local server is operating normally.

Continued on next page

Table 8.36 – continued from previous page

Message	Cause/Solution
Error: Failed to acquire the mirror index. Check if the Mirror Agent is operating normally.	Check to see if the Mirror Agent is operating normally.
Error: mirror agent is not running Check if the Mirror Agent is active.	The Mirror Agent is not started up. Check the syslog or the alert message of the module type, mdagent.
Error: Failed to acquire the active status of the Mirror Agent of the local server. Shut down the cluster and reboot both servers	Acquiring the active status of mirror disk resource of the local server has failed. Shut down the cluster and restart both servers.
Error: Failed to acquire the active status of the Mirror Agent of the other server. Shut down the cluster and reboot both servers	Acquiring the active status of a mirror disk resource of the remote server has failed. Shut down the cluster and restart both servers.
Error: Failed to acquire mirror recovery status. Reboot the local server.	Acquiring the mirror recovery status has failed. Restart the local server.
Error: Failed to acquire the list of mirror disks. Reboot the local server.	Acquiring a list of mirror disks has failed. Restart the local server.
Error: Failed to acquire the mirror configuration information. Check if the Mirror Agent is operating normally.	Acquiring the mirror configuration data has failed. Check to see if the Mirror Agent is operating normally.
Error: Failed to acquire the mirror configuration information error. Check if the Mirror Agent is operating normally.	Acquiring the mirror disk configuration data of both servers has failed. Check if the Mirror Agent is operating normally.
Error: Failed to get acquire mirror- disk configuration information. Reboot the local server.	Acquiring the mirror disk configuration data. Restart the local server.
Error: get local and remote Failed to acquire the mirror- disk configuration information error of both servers. Shut down the cluster and reboot both servers	Acquiring the mirror disk configuration data of both servers failed. Shut down and restart both servers.

Continued on next page

Table 8.36 – continued from previous page

Message	Cause/Solution
Error: The number of the bits of the bitmap is invalid. The mirror difference information of the cluster partition is invalid. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see the Reference Guide.	Acquiring the mirror difference information in the cluster partition has failed. Shut down the cluster. If this error happens again, replace the disk.
Error: Failed to get bitmap information. Failed to acquire the mirror difference information of the local server. Reboot the local server.	The mirror difference information in the cluster partition is invalid. Shut down the cluster. If this error happens again, replace the disk.
Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Reading the mirror difference information of the local server has failed. Restart the local server.
Error: Failed to acquire semaphore. Reboot the local server.	Acquiring semaphore has failed. Restart the local server.
Error: A malloc error. Failed to reserve the memory space. Reboot the local server.	Reserving memory space has failed. Restart the local server.
Error: Mirror driver of the local server is not loaded. Refer to the Reference Guide to load the driver.	The mirror driver in the local server is not loaded. Check this by referring to "9. *Troubleshooting*" in this guide.
Error: Internal error (errorcode: 0xxxx). Shut down the cluster and reboot the server.	Shut down the cluster and restart the server.
Error: Failed to communicate with server %1 and %2. Check if both Mirror Agents of the two servers are operating normally and the interconnect LANs are connected.	Failed to communicate with both servers represented in the message. Make sure that the mirror agents of both servers are running and the interconnect LANs are connected. The server names are displayed where "%1" and "%2" are represented.

Continued on next page

Table 8.36 – continued from previous page

Message	Cause/Solution
Error: Failed to communicate with server %1. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected.	Failed to communicate with the server %1. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Failed to acquire the mirror disk detail information of the server %2. Shut down the cluster and reboot both servers. Failed to acquire the mirror disk detail information of the server %2. Shut down the cluster, and then restart the both servers. The server names are displayed where "%1" and "%2" are represented.
Error: Failed to acquire the mirror disk detail information of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with server %2. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. The server name is displayed where "%1" or "%2" is represented.	Failed to acquire the mirror disk detail information of the server %1. Shut down the cluster, and then restart the both servers. Failed to communicate with the server %2. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected.
Error: Failed to acquire the mirror disk detail information of the server %1 and server %2. Shut down the cluster and reboot both servers."	Failed to acquire the mirror disk detail information of both servers. Shut down the cluster, and then restart the servers. The server name is displayed where "%1" or "%2" is represented.
Error: Failed to communicate with server %1. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. Failed to acquire mirror disk %3 net interface status of the server %2. Shut down the cluster and reboot both servers. The server name is displayed where "%1" or "%2" is represented.	Failed to communicate with the server %1. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Failed to acquire the status of mirror disk connect of mirror disk resource %3 of server %2. Shut down the cluster and reboot both servers. Where %3 is represented, the mirror resource name is displayed.

Continued on next page

Table 8.36 – continued from previous page

Message	Cause/Solution
Error: Failed to acquire mirror disk %3 net interface status of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with server %2. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. The server name is displayed where "%1" or "%2" is represented.	Failed to acquire the status of mirror disk connect of mirror disk resource %3 of server %1. Shut down the cluster and reboot both servers. Failed to communicate with the server %2. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Where %3 is represented, the mirror resource name is displayed.
Error: Failed to acquire mirror disk %3 net interface status of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire the status of mirror disk connect of both servers. Shut down the cluster, and then, restart the servers. The server name is displayed where "%1" or "%2" is represented. Where %3 is represented, the mirror resource name is displayed.
Error: Failed to communicate with server %1. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. Failed to acquire the active status of the Mirror disk %3 of the server %2. Shut down the cluster and reboot both servers.	Failed to communicate with the server %1. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Failed to acquire the active status of the Mirror disk resource %3 of the server %2. Shut down the cluster and reboot both servers. The server name is displayed where "%1" or "%2" is represented. Where %3 is represented, the mirror resource name is displayed.
Error: Failed to acquire the active status of the Mirror disk %3 of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with server %2. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected.	Failed to acquire the active status of the mirror disk resource %3 of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with the server %2. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Where %1 or %2 is represented, the server name is displayed. Where %3 is represented, the mirror resource name is displayed.

Continued on next page

Table 8.36 – continued from previous page

Message	Cause/Solution
Error: Failed to acquire the active status of the Mirror disk %3 of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire the mirror disk detail information of both servers. Shut down the cluster, and then restart the servers. Where %1 or %2 is represented, the server name is displayed. Where %3 is represented, the mirror resource name is displayed.
Error: Failed to get all server names. Check if the configuration file is correct and the Mirror Agent is operating normally.	Failed to acquire the server name. Check if the configuration file is correct and the Mirror Agent is operating normally.
Error: The disk alias does not match the command.	The resource type of the specified resource name (mirror alias name) is invalid. Use clpmdctrl for md resource, and clphdctrl for hd resource.
Error: Invalid command name.	The command name is invalid. Do not change the file name of the clphdctrl command.
Error: The function of collecting statistics is disabled.	The statistical information collection function is disabled. Check the setting of Collect Mirror Statistics in the Mirror Agent tab in Cluster Properties by using the Cluster WebUI.
Error: Collecting mirror statistics failed. Please retry in a few seconds later.	It failed to collect statistical information because of a temporarily high-load or other issue. Wait, and then execute the command again. If this message displays again, make sure that mdagent is running normally.

Display examples

- Mirror disk connect status display

  When the --connect option is specified, the status of mirror disk connect is displayed.

```
Mirror Name : md1

[Server : server1]

    192.168.0.1                     : Using

[Server : server2]

    192.168.0.2                     : Using
```

  Explanation of each item

Item	Description
Server Name	Name of the server
IP Address	IP address specified by mirror disk connect
Status	Status of mirror disk connect Status Description --- Using Being used Free Not used Error Error -- Unknown

- Displaying the status of mirror disk resource

  The status of specified mirror disk resource is displayed by specifying the --mirror option. There are three types of display depending on the status of mirror disk resource:

  – When the status of mirror disk resource is Normal:

```
Mirror Status: Normal
md1                 server1             server2
-------------------------------------------------
Mirror Color        GREEN               GREEN
```

  Explanation of each item

Item	Description
Mirror Status	Status of mirror disk resource Status Description --- Normal Normal Recovering Mirror is recovering Abnormal Abnormal No Construction Initial mirror construction is not done
Mirror Color	Status of mirror disk on each server Status Description --- GREEN Normal YELLOW Mirror is recovering RED Abnormal GRAY Being stopped, Unknownstatus BLACK Initial mirror construction is not done, error found in cluster partition data, etc. BLUE Both disks are active

  – When the status of mirror disk resource is abnormal

```
Mirror Status: Abnormal

md1                 server1                 server2
-------------------------------------------------------
Mirror Color         GREEN                  RED
Lastupdate Time      2018/03/05 15:41:07     --
```

(continues on next page)

(continued from previous page)

```
Break Time          2018/03/05 15:40:38     --
Disk Error          OK                      OK
Difference Percent  1%                      0%
```

Explanation of each item

Item	Description
Mirror Status	Status of mirror disk resource[4]
Mirror Color	Status of mirror disk on each server[4]
Last update Time	Last time when the data was updated on the server.
Break Time	Time when mirror break has occurred
Disk Error	Status of disk I/O Status Description --- OK Normal ERROR Error (No I/O) -- Unknown
Difference Percent	Percentage of differences in the data on each server.

– During mirror recovery:

```
Mirror Status: Recovering

md1                 server1               server2
-------------------------------------------------------------
Mirror Color        YELLOW                YELLOW

Recovery Status   Value
---------------------------------------
Status:           Recovering
Direction: src    server1
           dst    server2
Percent:          3%
Used Time:        00:00:01
Remain Time:      00:00:32
Iteration Times:  1/1
```

Explanation of each item

Item	Description
Mirror Status	Status of mirror disk resource[5]
Mirror Color	Status of mirror disk on each server[5]

Continued on next page

[4] See "When the status of mirror disk resource is Normal:"

Table 8.40 – continued from previous page

Item	Description
Status	Status of mirror recovery Status Description ---------- Preparing Preparing for copy (This status may last for a while if I/O load is high when resource is getting started during recovery) Recovering Being recovered Completing Recovering is being completed Nothing Canceling recovery
Direction	src : source server dst : destination server
Percent	Percentage of how much data is already recovered
Used Time	Elapsed time since recovering has started
Remain Time	Estimated time to complete recovering the remaining data. It is estimated by the speed of already recovered data. The time may be different depending on server load.
Iteration Times	The current repeat counts and the setting value of the mirror recovery.

- Displaying active status of mirror disk resource

  Active status of the specified mirror disk resource is displayed when the --active option is specified:

```
md1               server1     server2
-------------------------------------------------------
Active Status     Active      Inactive
```

  Status of mirror partition device

Active Status	Description
Active	Active
Inactive	Not active
--	Unknown

- Displaying mirror disk resource information

  Configuration information of the specified mirror disk resource is displayed when the --detail option is specified:

```
Mirror Name           : md1
    Sync Switch       : On
    Sync Mode         : Sync
    Diff Recovery     : --
    Compress          :
        Sync Data     : Off
        Recovery Data : On

[Server : server1]
    NMP/Disk Size(MB) : 2447/2447
```

(continues on next page)

[5] See "When the status of mirror disk resource is Normal:"

(continued from previous page)

```
    DP Device          : /dev/sdb2
    CP Device          : /dev/sdb1
[Server : server2]
    NMP/Disk Size(MB) : 2447/2447
    DP Device          : /dev/sdb2
    CP Device          : /dev/sdb1
```

Explanation of each item

Item	Description
Mirror Name	Mirror disk resource name
Sync Switch	Perform data synchronization / Do not perform data synchronization
Sync Mode	Synchronization Mode / Asynchronization Mode
Compress	Sync Data – Compress mirror synchronization data / Do not compress mirror synchronization data RecoveryData – Compress mirror recovery data / Do not compress mirror recovery data
Server Name	Server name
NMP/Disk Size(MB)	NMP – the smaller size of data partition of servers Disk Size – actual data partition size
DP Device	Data partition device name
CP Device	Cluster partition device name

- Displaying the list of mirror disk resources

  The list of mirror disk resources is displayed when the --list option is specified:

```
[Replicator Option]

 server1 : Installed
 server2 : Installed
 server3 : Installed

[Servers Which Can Be Started]
 <md1>
   server1
   server3

 <md2>
   server2
   server3
```

Explanation of each item

Item	Description
Replicator Option	License status of the Replicator
Servers Which Can Be Started	Servers which can be started of mirror disk resources

- Displaying statistical information

  Performance figures for the mirroring function are displayed when the --perf option is specified:

```
md1
---Write(MB)---- ---Read(MB)---- ---Send(MB)---- --SyncTime(s)-- -SyncDiff(MB)
Total    Avg       Total    Avg      Total    Avg      Max      Avg       Max    Cur
0.14     0.00      0.10     0.00     0.02     0.00     0.04     0.02      0.07   None
```

  Explanation of each item

Item	Description
Write (Total)	Total amount of data written in mirror partitions. The unit is MB. The output value indicates the amount of data written during each sampling interval.
Write (Avg)	Amount per unit time of data written in mirror partitions. The unit is MB/s.
Read (Total)	Total amount of data read from mirror partitions. The unit is MB. The output value indicates the amount of data read during each sampling interval.
Read (Avg)	Amount per unit time of data read from mirror partitions. The unit is MB/s.
Send (Total)	Total amount of mirror communication data sent using mirror disk connects. The unit is MB. The output value indicates the amount of communication data sent during each sampling interval. TCP control information and others are not included.
Send (Avg)	Amount per unit time of mirror communication data sent using mirror disk connects. The unit is MB/s.
SyncTime (Max)	Time required for synchronizing one mirror synchronization data item. The output value indicates the longest time required for synchronizing a mirror synchronization data item. The unit is seconds/synchronization. The time required for synchronizing mirror synchronization data which cannot be synchronized due to disabled communication or another cause (which causes a mirror brake) is not output. The output value indicates the time required for communication during each sampling interval.

Continued on next page

Table 8.42 – continued from previous page

Item	Description
SyncTime (Avg)	Time required for synchronizing one mirror synchronization data item. The output value indicates the average time per communication. The unit is seconds/communication. The time required for synchronizing mirror synchronization data which cannot be synchronized due to disabled communication or another cause (which causes a mirror break) is not included. The output value indicates the average time required for communication during each sampling interval.
SyncDiff (Max)	Amount of mirror synchronization data which has not been synchronized with that on a remote server. The output value indicates the maximum value during each sampling interval. The unit is MB. The amount of mirror synchronization data which cannot be synchronized due to disabled communication or another cause (which causes a mirror break) is not included.
SyncDiff (Cur)	Amount of mirror synchronization data which has not been synchronized with that on a remote server. The output value indicates the latest amount at collection. The unit is MB. The amount of mirror synchronization data which cannot be synchronized due to disabled communication or another cause (which causes a mirror break) is not included.

- The clpmdstat command displays statistical information to two decimal places. Actually collected data is converted to an appropriate unit and truncated to two decimal places when displayed. The following rules are used for conversion:

  1 KB = 1024 bytes, 1 MB = 1048576 bytes

- When the result of truncating data is 0, "0.00" is displayed. When not that result, but the actual data is 0, "None" is displayed.
- The output value becomes information in the server that executed the command. Valid values are output only in the active server for Write (Total), Write (Avg), Read (Total), Read (Avg), SyncTime (Max), SyncTime (Avg), SyncDiff (Max), and SyncDiff (Cur). The status of these values is either hold or "none" in a standby server. Valid values are output in both active and standby servers for Send (Total) and Send (Avg).

8.14.2 Operating mirror disk resource (clpmdctrl command)

the clpmdctrl command operates mirror disk resources.

Command line

clpmdctrl {--active | -a} *mirrordisk-alias*
clpmdctrl {--active | -a} -nomount *mirrordisk-alias*
clpmdctrl {--active | -a} -force [-ro] *mirrordisk-alias*
clpmdctrl {--active | -a} -force -nomount *mirrordisk-alias*

clpmdctrl {--deactive | -d} *mirrordisk-alias*
clpmdctrl {--break | -b} *mirrordisk-alias*
clpmdctrl {--recovery | -r} *mirrordisk-alias*
clpmdctrl {--force | -f} [-v] *recovery-source-servername mirrordisk-alias*
clpmdctrl {--force | -f} *mirrordisk-alias*
clpmdctrl {--cancel | -c} *mirrordisk-alias*
clpmdctrl {--rwait | -w} [-timeout *time* [-rcancel]] *mirrordisk-alias*
clpmdctrl --getreq
clpmdctrl --setreq *request-count*
clpmdctrl --sync [*mirrordisk-alias*]
clpmdctrl --nosync [*mirrordisk-alias*]
clpmdctrl {--compress | -p} [*mirrordisk-alias*]
clpmdctrl {--nocompress | -n} [*mirrordisk-alias*]
clpmdctrl {--mdcswitch | -s} [*mdc-priority*] *mirrordisk-alias*
clpmdctrl {--resize | -z} [-force] *partition-size mirrordisk-alias*

Important:

After releasing the access limitation to the mirror disk partition by --active option, make sure to put the access limitation again by --deactive option.

Additionally, do not use --deactive option while the resource is in active status.

If the resource in the active status is started or stopped, the file system may be corrupted.

Note: When you extend the data partition of the mirror disk resource by using --resize option, extend both servers by following "Maintenance Guide" -> "The system maintenance information" -> "Changing offset or size of a partition on mirror disk resource".

Note: When you extend the data partition of the mirror disk resource by using --resize option, the data partition must be configured with LVM and the amount of unused PE (physical extent) of the volume group must be sufficient.

Description

This command activates, deactivates or forcibly activates mirror disk resource and recovers or forcibly recovers mirror.

This command disconnects a mirror disk.

This command performs mirror recovery, forced mirror recovery, cancellation of mirror recovery, and waiting for the completion of mirror recovery.

This command displays and/or modifies the settings of maximum number of request queues.

This command switches the synchronization status of the mirror data.

This command is used to set whether mirror data is to be compressed.

This command switches the communication path (mirror disk connect) to be used.

This command extends the data partition size.

Option

--active, -a

Activates the mirror disk resource on the local server.
If the status of mirror disk resource is normal, mirroring is performed.
If the status of mirror disk resource is not normal, mirroring will not be performed.

-force

Forcibly activates a mirror disk resource.
This command can be run on a server where mirroring is stopped.
This option is used with the --active option.

-nomount

It allows access to mirror partition device without mounting the file system.
This option is used with the --active option.
This option has no meaning if none is specified for the file system.

-ro

Forcibly activates a mirror disk resource in ReadOnly mode.
This option is used with the --active -force options.

--deactive, -d

Deactivates the activated mirror disk resource on the local server.

--break, -b

Disconnects the mirror disk resources forcibly specified with *mirrordisk-alias on* the server where the command is run.
The status of mirror disk resource on the server where the command is run becomes an error. The status on the server where the command is not run does not change.
When a mirror is recovered, disconnection is canceled.
Mirror data is not synchronized even when any data is written to a mirror disk.
Auto mirror recovery is not automatically started until reboot is performed or disconnection is canceled after completion of mirror recovery.

--recovery, -r

Performs either full mirror recovery or differential mirror recovery for the specified mirror disk resource.
Whether to perform full or differential mirror recovery is determined automatically.

--force, -f

Forcefully performs mirror recovery for the specified mirror disk resource.
If only mirrordisk-alias is specified, the status of mirror disk where the command is run becomes normal forcibly. Mirror resynchronization is not performed.
If recovery-source-servername and mirrordisk-alias are specified, full mirror recovery is performed using recovery-source-servername as source data.
The status of mirror disk becomes normal when a full mirror recovery completes.

-v

Forcefully performs mirror recovery without an analysis of the file system.

--cancel, -c

Cancels mirror recovery.

When **Auto Mirror Recovery** is selected and a mirror disk monitor resource is operating, mirror recovery is automatically resumed a while after it is canceled. In this case, suspend the mirror disk monitor resource by using the Cluster WebUI or clpmonctrl command, then run the command for canceling mirror recovery.

--rwait, -w

Waits for the completion of the mirror recovery of the specified mirror disk resource.

-timeout

Specifies the timeout period of mirror recovery completion (second). This option can be omitted.

When this option is omitted, timeout is not executed and waits for the completion of mirror recovery.

-rcancel

Cancels mirror recovery when the timeout of waiting of mirror recovery completion occurred. This option can be set when -timeout option is set.

When this option is omitted, the mirror recovery continues even after the timeout occurrence.

--getreq

Displays the current maximum number of request queues.

--setreq

Configures the maximum number of request queues.

When the server shuts down, what you have configured here returns to the value set in the cluster configuration data. Use the Cluster WebUI if you want to modify the cluster configuration data. For details, see "*Cluster properties*" "*Mirror driver tab ~ For Replicator/Replicator DR ~*" in "*2. Parameter details*" in this guide.

The command is only effective on the server that runs the command.

--sync

This option switches the operation to the mirror synchronization.

When the mirror disk resource name is not specified, the operation is switched to synchronizing the mirror data to all mirror resources.

--nosync

This option switched the operation to the one that does not synchronize the mirror data.

When the mirror disk resource name is not specified, the operation is switched to not performing the synchronization of the mirror data to all mirror resources.

However, the data updated to a disk during a mirror recovery is synchronized to a standby server.

If auto mirror recovery is set to ON and the mirror disk monitor resource is operating, automatic mirror recovery will operate.

Even after the completion of mirror recovery, the operation will still not synchronize. To cancel this, execute the command with the --sync option specified.

When the server is shut down, the state will return to the synchronization operation that is set in the cluster configuration information. To change the cluster configuration information, use the Cluster WebUI. For details, see "Mirror tab" in "Mirror disk resource tuning properties" in " *Details tab*" in "Understanding mirror disk resources" in "3. *Group resource details*" in this guide.

--compress, -p

Temporarily switches on the compression mode of mirror transfer data.

If the synchronous mode of mirror data is "Synchronous", only the recovery transfer data is compressed.

If the synchronous mode of mirror data is "Asynchronous", both the asynchronous transfer data and the recovery transfer data are compressed.

When the mirror disk resource name is not specified, the operation is performed to all mirror disk resources.

--nocompress, -n

Temporarily switches off the compression mode of mirror transfer data.

When the mirror disk resource name is not specified, the operation is performed to all mirror disk resources.

--mdcswitch, -s

Switches the mirror connection to another mdc that has the specified priority.

If the priority is not specified, the mirror connection is switched to the mdc that has the next highest priority after the current mdc. If the mirror connection is connected to the mdc that has the lowest priority, it is switched to the one that has the highest priority.

If the mirror connection has already been switched to the specified mdc, the command terminates normally without performing any processing.

If the specified mdc does not exist, an error occurs.

--resize

Extends the data partition size of mirror disk resource.

The extension is available only when the status of mirror disk resource is normal.

When the -force option is specified, forcibly executes the extension regardless of the status of mirror disk resource.

If this option is used, full copy of the mirror disk will be executed for the next time.

In addition, even if this option is used, the extension is unavailable during the mirror recovery.

Parameter

recovery-source-servername
Specifies a server name of the copy source.

mirrordisk-alias
Specifies a mirror disk resource name.

request-count

Specifies a maximum number of request queues.

You can specify a number from *2048* through 65535.

time
Specifies the timeout period of mirror recovery completion (second).

mdc-priority

Specifies the priority of mdc.
This is not the priority number of mdc in whole cluster, but the priority number (1 or 2) of mdc used by the mirror disk resource.

partition-size

Specifies the new size of data partition. For the unit, use the following symbol. If "500G" is specified, the size is extended to 500 gibibytes. If the symbol of the unit is not used, the amount is regarded as in byte.

- K (Kibi byte)
- M (Mibi byte)
- G (Gibi byte)
- T (Tebi byte)

Return Value

0	Success
255 (-1)	Failure
254 (-2)	Target mirror disk is not configuring mirror, or the mirror configuring failed on the process. (Only when --rwait option is specified, including the case when mirror recovery is interrupted by -rcancel.)
253 (-3)	Timeout of mirror recovery of target mirror disk occurs (Only when --rwait -timeout option is specified)

Remarks
request-count, which is displayed by specifying the --getreq option, is the same as "Max. Number of Request Queues" which is displayed by using the clpstat command.

```
# clpstat --cl --detail
```

This command returns control when the specified processing starts. Run the clpmdstat command to check the processing status.

Notes
Run this command as the root user.

When performing mirror recovery again after mirror recovery failed, specify the same server you used last time for mirror recovery as a copy source.

To resume the forced mirror recovery that was suspended by selecting **Cancel**, use this command for forced mirror recovery.

In a cluster with more than three nodes, if the server where the command is run is not included in a startup server of a group including mirror disk resources, this command results in error. Do not run this command if the server is not included in a startup server of a group.

If, during mirror synchronization, mirror synchronization is interrupted with either the --break (-b) or --nosync option or if, during mirror recovery, mirror recovery is interrupted, the file system and application data may prove

to be abnormal even if the mirror disk to be synchronized is made accessible by performing forced activation or forced mirror recovery. For details, see "Mirror data reference at the synchronization destination if mirror synchronization is interrupted" in "Notes and Restrictions" in the "Getting Started Guide".

Example of command execution

Example 1: When activating the mirror disk resource md1:

```
# clpmdctrl --active md1
<md1@server1>: active successfully
```

Example 2: When deactivating the mirror disk resource md1:

```
# clpmdctrl --deactive md1
<md1@server1>: deactive successfully
```

Example 3: When disconnecting the mirror disk resource md1:

```
# clpmdctrl --break md1
md1: isolate successfully
```

Example 4: When the status of both servers is error, and you need to recover the operation which uses the resource md1 as soon as possible:

```
# clpmdctrl --force md1
The data of mirror disk in local server maybe is not latest.
Do you still want to continue? (Y/N)
md1: Force recovery successful.

# clpgrp -s failover1
Command succeeded.
```

When **Auto Mirror Recovery** is selected, mirror recovery is performed at this timing. When **Auto Mirror Recovery** is cleared, run the following command.

```
# clpmdctrl --recovery md1
```

Example 5: When mirror recovering the mirror disk resource md1:

```
# clpmdctrl --recovery md1
```

Example 6: When setting the maximum number of request queues to 2048:

```
# clpmdctrl --setreq 2048
current I/O request count <2048>
```

Example 7: When configure the setting that does not perform the data synchronization to the mirror disk resource md1:

```
# clpmdctrl --nosync md1
```

Error Messages

Message	Cause/Solution
Error: Log in as root.	Log on as the root user.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
Error: Failed to read the configuration file. Check if it exists or is configured properly.	Reading the configuration file has failed. Check to see if the configuration file exists and is configured correctly.
Error: Specified mirror disk resource was not found. Specify a valid mirror disk resource name.	Locating the specified mirror disk resource has failed. Specify a valid mirror disk resource name.
Error: Invalid mirror-alias. Specify a valid mirror disk resource name.	Specify a valid mirror disk resource name.
Error: Failed to get the server name. Check if the configuration file is correct and the Mirror Agent is operating normally.	Acquiring the server name has failed. Check if configuration file is correct and the Mirror Agent is operating normally.
Error: Specified server name was not found. Check if the server name exists in the configuration file.	The specified server name was not found. Check to see if the entered server name exists in the configuration file.
Error: Invalid server name. Specify a valid server name.	Specify a valid sever name.
Error: Failed to communicate with other servers. Check if the Mirror Agent of the other server is operating normally and the mirror disk connect is connected.	Communicating with the remote server has failed. Check to see if the Mirror Agent of the remote server is operating and the mirror disk is connected.
Error: Failed to get the mirror disk status. Check if the Mirror Agent on the local server is operating normally.	Acquiring the mirror disk status has failed. Check to see if the Mirror Agent of the local server is operating normally.
Error: Failed to get the mirror index. Check if the Mirror Agent is operating normally.	Check to see if the Mirror Agent is operating normally.
Error: The status of mirror disk resource of the local server is abnormal.	The mirror disk resource of the local server has a problem.
Error: Specified mirror disk resource is already active. Check active status of mirror disk resource by running the following command: clpmdstat --active <alias>	The specified mirror disk resource is already activated. Check the status of the mirror disk resource using the following command. clpmdstat --active <alias>
Error: A hardware error has occurred on the disk. Check the disk.	A hardware error has occurred on the disk. Check the disk.
Error: The sizes of data partition of the servers do not match.	Data partition sizes of both servers do not match.
Error: Specified mirror disk is not active. Check the active status of mirror disk resource.	The specified mirror disk resource is not activated. Check the status of mirror disk resource.
Error: There is no recovering mirror disk resource.	There is no mirror disk under mirror recovery process.
Error: Mirror disk resource is recovering. Wait until mirror recovery completes.	The mirror disk resource is under mirror recovery process. Wait until mirror recovery is completed
Error: Failed to cancel the mirror recovery. The system may be highly loaded. Wait for a while and try again.	Stopping mirror recovery has failed. The system may be heavily loaded. Wait for a while and try again.
Error: Performed mirror recovery to the mirror disk resource that is not necessary to recover the mirror. Run the clpmdctrl--force command if you want to perform forced mirror recovery.	Mirror recovery has been performed on the mirror disk resource that is in normal status and not requiring mirror recovery. To perform forced mirror recovery, use "clpmdctrl --force."

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
Error: Specification of the server that is copied from is incorrect. When executing mirror recovery again after a failure end of mirror recovery, specify the same server as the previous one.	The server specified for a copy source is invalid. When performing the mirror recovery again after the mirror recovery has failed, specify the same server that you specified last time for the failed mirror recovery as a copy source.
Error: Forced mirror recovery is required. Run the clpmdctrl --force command to perform the recovery.	Forced mirror recovery is necessary. Use "clpmdctrl --force" and perform forced mirror recovery.
Error: Server with old data is specified as the server which is copied from. Specify a correct recovery direction.	The server with old data is specified as a copy source. Specify a correct recovery direction.
Error: Failed to acquire mirror recovery status. Reboot the local server.	Acquiring the mirror recovery status has failed. Restart the local server.
Error: Both of the mirrors are not constructed. Initial mirror configuration of the mirror disks by running the clpmdctrl --force command is necessary.	Initial mirror construction of mirror disk is necessary. Construct initial mirror configuration using "clpmdctrl --force."
Error: Initial mirror configuration of mirror disk of local server is necessary. Specify the other server as the one that is copied from by using the clpmdctrl --force command to configure an initial mirror.	Initial mirror construction is necessary for the mirror disk of the local server. Specify the remote server as a copy source and construct initial mirror using "clpmdctrl --force."
Error: Initial mirror configuration of mirror disk of the other server is necessary. Specify the local server as the one that is copied from by using the clpmdctrl--force command to configure an initial mirror.	Initial mirror construction is necessary for the mirror disk of the remote server. Specify the local server as a copy source and construct initial mirror using "clpmdctrl --force."
Error: Mirror flag error. Use "clpmdinit" to construct the mirror. The status of cluster partition of the mirror disk resource is abnormal. When the server with the error has the latest data, backup the data, initialize the cluster partition, and replace the same disk by using the same disk. If the error persists, change the disk to new one.	The cluster partition of the mirror disk resource has a problem. When the server with error has the latest data, back up the data, initialize the cluster partition according to Chapter 8 "Verifying Operation" in the Installation and Configuration Guide, and follow the same way as described in "How to replace a mirror disk with a new one" in Chapter 1, "The system maintenance information" in the maintenance guide, using the same disk. If this occurs again, replace the disk with a new disk.
Error: Both local and remote mirrors are active. Shut down the cluster and execute forced mirror recovery after rebooting the server.	Both systems are active. Shut down the cluster and perform forced mirror recovery after reactivating the server.
Error: Mirror Agent is not running. Check if the Mirror Agent is active.	The Mirror Agent is not started up. Check to see if the Mirror Agent is running.
Error: System calls error. Failed to run the system command when active and/or inactive. Check if the search path is set to an environment variables.	Running the system command when active/inactive has failed. Check to see if a search path is set as an environmental variable.
Error: Failed to create a mount point. The disk space may not be sufficient.	Creating a mount point has failed. Disk space may be insufficient. Check it.
Error: Timeout has occurred on active fsck. When it is not journaling file system, it may take time to run fsck if the size of data partition of mirror disk is large. Set timeout of fsck longer.	fsck time-out has occurred. In case it is not the journaling file system, running fsck may take time when the data partition of the mirror disk is large. Set the longer timer for the fsck time-out using the Cluster WebUI.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
Error: Timeout occurs at activation mount. Set mount timeout longer	Time-out has occurred at active mounting. Set the mounting time-out longer by using the Cluster WebUI.
Error: Timeout occurs at deactivation mount. Set unmount timeout longer.	Time-out has occurred at inactive unmounting of the file system. Set the mount time-out period longer by using the Cluster WebUI.
Error: fsck failed. Check if file system type of data partition does not match configuration file, fsck option is incorrect or partition is incorrect.	Running fsck has failed. Check to see if the file system type of the data partition matches to the configuration file, fsck option is valid, and partition is not destroyed.
Error: Failed to mount when active. The file system type of the data partition does not match the settings of the configuration file, or the partition may be corrupted.	Mounting during activation has failed. Check to see if the file system type of the data partition matches to the configuration file, fsck option is valid, and the partition is not destroyed.
Error: Failed to unmount when inactive. Check if the file system on the data partition is busy.	Unmount during deactivation has failed. Check to see if the file system on data partition is not busy.
Error: Mirror disk resource is on process of activation. Execute after activation is completed.	The mirror disk is in the process of activation. Try after activation is completed.
Error: Failed to perform forced mirror recovery or activate a single server. Check if any hardware error has occurred on the disk.	Performing forced recovery or activating a standalone server has failed. Check to see if any hardware error has occurred on the disk.
Error: Entered incorrect maximum number of request queues. Check the specifiable range.	Invalid maximum number of request queues is entered. Check the range of numbers that can be specified.
Error: Failed to set the maximum number of request queues. Reboot the local server.	Setting a maximum number of request queues has failed. Restart the local server.
Error: Failed to acquire the maximum number of request queues. Reboot the local server.	Acquiring a maximum number of request queues has failed. Restart the local server.
Mirror disk resource was not found on local server. Cannot perform this action.	The mirror disk resource was not defined on the local server. Cannot configure the maximum number of request queues. Check the status of the mirror disk resource.
Error: Failed to get the NMP path. Check if the Mirror Agent is operating normally. Reboot the local server.	Check to see if the Mirror Agent is operating normally. Restart the local server.
Error: Failed to acquire the mirror configuration information. Check if the Mirror Agent is operating normally.	Acquiring the mirror configuration information has failed. Check to see if the Mirror Agent is operating normally.
Error: Failed to acquire the mirror disk configuration information. Reboot the local server.	Acquiring mirror disk configuration data has failed. Restart the local server.
Error: Failed to acquire the mirror disk configuration information of both local and remote servers. Shut down the cluster and reboot both servers	Acquiring mirroring disk configuration data of both servers has failed. Shut down the cluster and restart both servers.
Error: Failed to get the number of bits of the bitmap due to the errors occurred when acquiring the mirror difference information of the cluster partition. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see the Reference Guide.	Acquiring the information of mirror differences on the cluster partition has failed. Shut down the cluster. If the error occurs again, replace the disk. For information on how to replace a disk, see "The system maintenance information" in the "Maintenance Guide".

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
Error: The number of the bits in the bitmap is invalid. The mirror difference information of the cluster partition is invalid. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see Reference Guide.	The information of the mirror differences in the cluster partition is invalid. Shut down the cluster. If the error occurs again, replace the disk. For information on how to replace a disk, see Chapter 1 "The system maintenance information" in the Maintenance Guide.
Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Reading the information of mirror differences on the local server has failed. Restart the local server.
Error: Failed to read the mirror difference information of the other server. Reboot the other server.	Reading the information of the mirror differences on the remote server has failed. Restart the remote server.
Error: Failed to get the bitmap information of the local server due to the errors occurred when acquiring the mirror difference information of the local server. Reboot the local server.	Acquiring the information of the mirror differences on the local server has failed. Restart the local server.
Error: Failed to read the disk space. Shut down the cluster and reboot the server	Acquiring the disk space has failed. Shut down the cluster and restart the server.
Error: Failed to acquire the disk space of the other server. Shut down the cluster and reboot both servers.	Acquiring the disk space of the remote server has failed. Shut down the cluster and restart the server.
Error: Setting of cluster partition failed. Restart local server.	Configuring the cluster partition has failed. Restart the local server.
Error: Error occurred on the settings of the mirror disk resource. Reboot the local server.	Error occurred in the status settings of mirror disk resource. Restart the local server.
Error: Failed to create a thread. Reboot the local server.	Creating thread has failed. Restart the local server.
Error: Internal error. Failed to create process. Reboot the local server.	Creating the process has failed. Restart the local server.
Error: Failed to acquire semaphore. Reboot the local server.	Acquiring semaphore has failed. Restart the local server.
Error: A malloc error. Failed to reserve the memory space. Reboot the local server.	Reserving memory has failed. Restart the local server.
Error: Mirror driver of the local server is not loaded. Confirm kernel version.	The mirror driver of the local server is not loaded. Check the kernel version.
Error: Mirror recovery cannot be executed as NMP size of mirror recovery destination is smaller than the size of where the mirror is recovered from. Change the recovery destination and try again.	Mirror recovery cannot be performed because NMP size of recovery destination is smaller than the recovery source. Change the destination and try again.
Error: NMP size of local server is bigger, cannot active. Initial mirror configuration is not completed. Execute mirror recovery from server of smaller NMP size to that of larger one.	Initial mirror configuration is not completed. Perform forced mirror recovery from the server whose NMP size is smaller to the larger one.
Local and remote recovery mode do not match. Reboot a server other than the master server to keep the same contents of configuration file among servers. Note that a failover may occur at server reboot.	The both servers are different on the recovery mode. The recovery is not performed. Restart the servers other than master server to make the information file be the same among servers. Note that a failover may occur at server reboot.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
Failed to get remote recovery mode. Recovery will not be interrupted. Check the communication status of mirror connect.	Failed to get remote recovery mode. Recovery will not be interrupted. Check the communication status of mirror connect.
Failed to get local recovery mode. Recovery will not be interrupted. Note that a failover may occur at server reboot.	Failed to get local recovery mode. Recovery will not be interrupted. Restart the local server. Note that a failover may occur when the server is restarted.
Local or remote mirror is forced activated. Cannot to perform this action.	Mirror disks are forcibly activated. Cannot perform the mirror recovery. Check the status of local or remote mirror.
The recovery destination of mirror disk is activated. Cannot perform this action.	The recovery destination of mirror disk is activated. Cannot perform the mirror recovery. Check the status of the mirror disk.
Mirror disk connection is disconnected. Cannot perform this action.	The communication status of mirror disk connect is error. Cannot perform the mirror recovery. Check the status of the mirror disk connect.
Failed to get mirror disk list and failed to set all NMP sync flag. Reboot the local server. Note that a failover may occur at server reboot.	The setting of synchronizing data for all the mirror disks failed since acquiring the mirror disk list failed. Reboot the local server. Note that a failover may occur at server reboot.
Failed to get mirror disk list and failed to set all NMP sync flag to OFF. Reboot the local server. Note that a failover may occur at server reboot.	The setting of not to synchronize data for all the mirror disks failed since acquiring the mirror disk list failed. Reboot the local server. Note that a failover may occur at server reboot.
Failed to set sync flag on both servers. Shut down a cluster and reboot server.	The setting of synchronizing data failed on the both servers. Shut down the cluster and restart it.
Failed to set sync flag to OFF on both servers. Shut down a cluster and reboot server.	The setting of not to synchronize data failed on the both servers. Shut down the cluster and restart it.
%1: Succeeded to set sync flag ON on %2 Failed to set sync flag ON on %3 Check the communication status of mirror connect	The setting of synchronizing data of %1 succeeded on the server %2, failed on the server %3. Check the running status of the server or the communication status of the mirror disk connect. The mirror disk resource name is displayed where %1 is represented. The server name of which the setting succeeded is displayed where %2 is represented. The server name of which the setting failed is displayed where %3 is represented.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
%1: Succeeded to set sync flag OFF on %2 Failed to set sync flag OFF on %3 Check the communication status of mirror connect	The setting of not synchronizing data of %1 succeeded on the server %2, failed on the server %3. Check the running status of the server or the communication status of the mirror disk connect. The mirror disk resource name is displayed where %1 is represented. The server name of which the setting succeeded is displayed where %2 is represented. The server name of which the setting failed is displayed where %3 is represented.
Succeeded to set sync flag on remote server and failed on local server. Note that a failover may occur at server reboot.	The setting of synchronizing data failed on the local server, yet succeeded in the other server. Restart the local server. Note that a failover may occur when the server is restarted.
Succeeded to set sync flag to OFF on remote server and failed on local server. Note that a failover may occur at server reboot.	The setting of not to synchronize data failed on the local server, yet succeeded in the other server. Restart the local server. Note that a failover may occur when the server is restarted.
Cannot change the settings of sync status during mirror recovery. Change the settings after mirror recovery is completed.	The setting of synchronizing data cannot be changed during mirror recovery. Change the settings after mirror recovery is completed.
Mirror disk resource was not found on local server. Cannot perform this action.	The mirror disk resource is not defined on the local server. The setting of synchronizing data cannot be changed.
The status of the mirror disk does not satisfy the conditions to perform this action. A probable cause: 1. Local mirror disk is not initialized or is already force activated. 2. Local mirror disk is not RED or remote is GREEN or remote is already activated.	The status of mirror is invalid. Cannot perform a forced recovery.
The data of mirror disk in the local server may not be the latest. Do you still want to continue? (Y/N)	The data of the local server may not be the latest. Cannot check the status of mirror disk on the other server.
Forced recovery has completed successfully.	The forced mirror recovery has successfully completed.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
The status of mirror disk in local server is not GREEN or is already activated. Cannot perform this action.	The status of mirror is invalid. Cannot disconnect a mirror.
Failed to set an isolate flag in the local server.	Cannot update the flag for mirror disconnect.
Isolated completed successfully.	The mirror disconnect is successfully completed.
The status of the mirror disk does not satisfy the conditions to perform this action. A probable cause: 1. Mirror disk is not initialized or is not RED. 2. Mirror disk is already activated.	The status of mirror is invalid. Cannot perform the forced activation.
sync flag of %1 is successfully set to ON.	The data synchronization is set to on for %1. A name of the mirror disk resource is displayed where %1 is represented.
Failed to set sync flag of %1 on both servers.	Failed to set the data synchronization flag on the both servers.
Shut down the cluster and reboot server.	A name of the mirror disk resource is displayed where %1 is represented.
%3: Succeeded to set sync flag ON on %1 Failed to set sync flag ON on %2 Check the communication status of mirror connect.	Failed to set the data synchronization flag on either of the servers. Check if the mirror disk connect can properly communicate. A name of the successfully-set server is displayed where %1 is represented. A name of the faulty-set server is displayed where %2 is represented. A name of the mirror disk resource is displayed where %3 is represented.
%1: Cannot change the settings of sync status during mirror recovery. Change the settings after mirror recovery is completed.	Cannot change the data synchronization flag during mirror recovery. Change the settings after mirror recovery is completed. A name of the mirror disk resource is displayed where %1 is represented.
sync flag of %1 is successfully set to OFF.	The mirror synchronization is set to off for %1. A name of the mirror disk resource is displayed where %1 is represented.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
%3: Succeeded to set sync flag OFF on %1 Failed to set sync flag OFF on %2 Check the communication status of mirror connect.	Failed to set the data synchronization flag on either server. Check if the mirror disk connect can normally communicate. A name of the successfully-set server is displayed where %1 is represented. A name of the faulty-set server is displayed where %2 is represented. A name of the mirror disk resource is displayed where %3 is represented.
The specified mirror disk is not defined on this server.	The specified mirror disk is not defined on the local server.
Failed to acquire the path of mirror device. Check if the Mirror Agent is operating normally. Reboot the local server.	Failed to acquire the device name of the mirror disk. Check if the mirror agent is running.
The disk alias does not match the command.	The resource type of the specified resource name (mirror alias name) is invalid. Use clpmdctrl for md resource, and clphdctrl for hd resource.
Invalid command name.	The command name is invalid. Do not change the file name of the clpmdctrl command.
Failed to get host name.	Acquiring the server name failed.
<%1>: mirror broken	The status of mirror is invalid. Target mirror disk is not configuring mirror, or the mirror configuring failed on the process. A name of the mirror disk resource is displayed where %1 is represented.
<%1>: recovery timeout	Mirror recovery timed out. Check if the specified timeout period is appropriate, or if the disk I/O or communication delay is not occurring due to heavy loads. A name of the mirror disk resource is displayed where %1 is represented.
Cannot perform this action.(Device: %1). Check if the Cluster Partition or Data Partition is OK.	Could not operate the mirror disk resource because the mirror disk resource is not running due to abnormity with the cluster partition or data partition.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
<%1> : Succeeded to set compress flag ON.	The compression of mirror transfer data of resource %1 was switched on. The mirror disk resource name is displayed where %1 is represented.
<%1> : Succeeded to set compress flag OFF.	The compression of mirror transfer data of resource %1 was switched off. The mirror disk resource name is displayed where %1 is represented.
<%1> : Failed to set compress flag ON.	Switching on the compression of mirror transfer data of the resource %1 failed. The mirror disk resource name is displayed where %1 is represented.
<%1> : Failed to set compress flag OFF.	Switching off the compression of mirror transfer data of the resource %1 failed. The mirror disk resource name is displayed where %1 is represented.
<%1> : Failed to set compress flag ON on %2.	Switching on the compression of mirror transfer data of the resource %1 failed on the server %2. Check the running status of the server or the communication status of the mirror disk connection. The mirror disk resource name is displayed where %1 is represented. The server name is displayed where %2 is represented.
<%1> : Failed to set compress flag OFF on %2.	Switching off the compression of mirror transfer data of the resource %1 failed on the server %2. Check the running status of the server or the communication status of the mirror disk connection. The mirror disk resource name is displayed where %1 is represented. The server name is displayed where %2 is represented.

Continued on next page

Table 8.43 – continued from previous page

Message	Cause/Solution
<%1>: Succeeded to switch mirror disk connection. Now using mdc <priority:%2>.	The mirror disk connection was switched to the mdc of priority number %2 of the resource %1. The mirror disk resource name is displayed where %1 is represented. The number of the priority of the newly used mirror disk connection is displayed where %2 is represented.
Error: There is no need to switch mirror disk connection.	The specified mirror disk connection has already been used. Switching is not needed.
Error: Failed to switch mirror disk connection. | The specified mirror disk connection is ERROR.	The specified mirror disk connection was not switched to because it was in the ERROR status.
Error: Failed to switch mirror disk connection. The other mirror disk connections are ERROR.	The other mirror disk connections were not switched to because they all were in the ERROR status.
Error: Failed to switch mirror disk connection.	Switching mirror disk connection failed.
Error: Specified mdc priority does not exist.	The specified priority number is invalid. It has not been defined in the configuration information.
Error: Failed to resize data partition.	Failed to extend the data partition size. Check if the data partition has been configured with LVM. Check if the amount of unused PE of the volume group is sufficient.
Error: NMP sizes of both servers are different. Cannot perform this action.	Mirror recovery is unavailable because the data size information of mirror disk resource is different between both servers. Check if mirror recovery is performed while mirror extension is being processed.
Error: The status of mirror disk resource is abnormal.	The process cannot be executed because the status of mirror disk resource is abnormal.

8.14.3 Initializing mirror disks (clpmdinit command)

the clpmdinit initializes a mirror disk.

Command line

clpmdinit {--create | -c} normal [*mirrordisk-alias*]
clpmdinit {--create | -c} quick [*mirrordisk-alias*]
clpmdinit {--create | -c} force [*mirrordisk-alias*]

Important: Generally you do not need to run this command when constructing or operating a cluster. You should exercise caution when you use this command because the partition used for the data will be initialized.

Description

This command initializes the cluster partition of a mirror disk resource.

This command creates a file system on the data partition of a mirror disk resource (except when none is specified for the file system).

Option

{--create, -c} <mode>
mode

normal

Initializes a cluster partition and creates a file system of the data partition, if necessary.[6]
The necessity is determined by the magic number set by EXPRESSCLUSTER on the cluster partition.
Generally, it is not necessary to run the command with this option.

quick

Initializes the cluster partition, if necessary.
Whether or not it is necessary to initialize the cluster partition is determined by the magic number set by EXPRESSCLUSTER on the cluster partition.
Generally, it is not necessary to run the command with this option.

force

Forcefully initializes the cluster partition and creates a file system of the data partition.[6]
This option is used when using the disk that was once used as a mirror disk of EXPRESSCLUSTER again.

Parameter

mirrordisk-alias

Specifies a mirror disk resource name.
If this parameter is not specified, the process is performed on all mirror disk resources.

Return Value

[6] Unless "Execute initial mkfs" is selected in the cluster configuration data, the file system will not be created.

0	Success
Other than 0	Failure

Notes

You should exercise caution when you run this command because the mirror disk will be initialized.

Run this command as the root user.

Do not run other commands, until this command is returned.

When running this command, make sure that the Mirror Agent in all servers in the cluster is stopped.

- To check the Mirror Agent is stopped on all servers, run the following command:

  ```
  # ps -e | grep clpmdagent
  ```

  In a cluster with more than three nodes, if the server where the command is run is not included in a startup server of a group including mirror disk resources, this command results in error. Do not run this command if the server is not included in a startup server of a group.

Example of command execution

Example 1: When forcefully initializing the cluster partition because the disk to be used for the mirror disk resource md1 was once used as a mirror disk of EXPRESSCLUSTER:

```
# clpmdinit --create force md1
mirror info will be set as default
the main handle on initializing mirror disk <md1> success
initializing mirror disk complete
```

Error Messages

Message	Causes/Solution
Log in as root.	Log on as the root user.
Stop the Mirror Agent.	Stop the mirror agent.
The clpmdinit command is currently running. Execute after it is completed.	This command is running. Run after it is completed.
Invalid mirror-alias. Specify a valid mirror disk resource name.	Specify a valid mirror disk resource name.
The mirror disk resource was not found. Set the mirror disk resource properly.	The mirror disk resource was not found. Set a mirror disk resource properly.
Specified mirror disk resource <%1> was not found. Specify a valid mirror disk resource name.	The specified mirror disk resource was not found. Specify a valid mirror disk resource name.
The partition does not exist . Check if the cluster partition of specified mirror disk resource exists (<%1>).	Check to see if the cluster partition of the specified mirror disk resource exists.
Check if the cluster partition size of specified mirror disk resource is larger than 1GB. <%1>	Check to see if the cluster partition size of the specified mirror disk resource is 1GB or larger.
Internal error (open error <%1>). The cluster partition of the mirror disk resource may not exist or the OS resource may be insufficient.	Check to see if the cluster partition of the specified mirror disk resource exists or OS resource is sufficient.
Internal error (<%1> cluster partition: unknown error). Failed to initialize the cluster partition. Check if any hardware error has occurred on the disk.	Initializing the cluster partition has failed. Check to see if there is any hardware error on the disk.

Continued on next page

Table 8.44 – continued from previous page

Message	Causes/Solution
Internal error (<%1> cluster partition: %2). Check if the size of cluster partition is sufficient and any hardware error has occurred on the disk.	Setting a cluster partition has failed. Check to see if the cluster partition space is sufficient and a hardware error has not occurred on the disk.
The data partition does not exist (<%1>). Check if the data partition of the specified mirror disk resource exists. Data Partition is: %2	Check to see if the data partition of the specified mirror disk resource exists.
Failed to initialize the cluster partition <%1>. The data partition of the specified mirror disk resource may not exist, hardware error may have occurred on the disk, or specified file system may not be supported by OS. Check them. mirror<%2>: fstype<%3>	Initializing the data partition has failed. Check to see if the data partition of the specified mirror disk resource exists, hardware error has not occurred on the disk and the specified file system is supported by OS.
Unknown error occurred when formatting mirrordisk<%1>. The data partition of the specified mirror disk resource may not exist or hardware error may have occurred on the disk. Check them.	Initializing the data partition has failed. Check to see if the data partition of the specified mirror disk resource exists and a hardware error has not occurred on the disk.
Internal error (Failed to open the data partition:<%1>). Failed to initialize the data partition. The data partition of the specified mirror disk resource may not exist or OS resource may not be sufficient. Data Partition is: %2	Initializing the data partition has failed. Check to see if the data partition of the specified mirror disk resource exists and OS resource is sufficient.
Internal error (data partition check error---<%1>). Failed to initialize the data partition. Check if any hardware error has occurred on the disk.	Initializing the data partition has failed. Check to see if any hardware error has not occurred on the disk.
Failed to acquire mirror disk list information. Reboot the local server.	Acquiring a list of mirror disk has failed. Restart the local server.
Internal error (PID write failed). Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Internal error (initialization failed) Failed to read the configuration file, or failed to initialize the shared memory or semaphore. Check if the file is configured properly and reboot the local server.	Reading the configuration file, initialize the shared memory or semaphore has failed. Check to see if configuration file is correct, and restart the local server.
Internal error (termination failed) Failed to release the shared memory. Check if any system error has occurred while running the program.	Freeing up the shared memory has failed. Check to see if any system error has not occurred while running the program.
A malloc error. Failed to reserve the memory space. Reboot the local server.	Reserving memory space has failed. Restart the local server.
An error has occurred when the data partition is set to writable mode. <Device:%1>. Reboot the local server.	An error occurred when the data partition was set to the writable mode. Restart the local server.
An error has occurred when the data partition is set to read-only mode.<Device:%1>. Reboot the local server.	An error occurred when the data partition was set to the read-only mode. Restart the local server.
Cluster Partition or Data Partition does not exist.	No cluster partition or data partition exists. Check if a partition is created.

Continued on next page

Table 8.44 – continued from previous page

Message	Causes/Solution
Failed to upgrade the cluster partition of <%s>.	Upgrading a cluster partition failed. Check if there is an error on the disk.
Specified mirror disk resource was not found on local server. Cannot perform this action.	The mirror disk resource is not defined on the local server. Cannot perform initialization. Check the status of the mirror disk resource.
The disk alias does not match the command.	The resource type of the specified resource name (mirror alias name) is invalid. Use clpmdinit for md resource, and clphdinit for hd resource.
Invalid command name.	The command name is invalid. Do not change the file name of the clphdinit command.
Initializing mirror disk of %1 failed. Check if the Cluster Partition or Data Partition is OK.	Failed to initialize the mirror disk resource because the cluster partition or the data partition is abnormal.

8.15 Hybrid-disk-related commands

8.15.1 Displaying the hybrid disk status (clphdstat command)

the clphdstat command displays status related to mirroring and configuration information.

Command line

clphdstat {--connect | -c} *hybriddisk-alias*
clphdstat {--mirror | -m} *hybriddisk-alias*
clphdstat {--active | -a} *hybriddisk-alias*
clphdstat {--detail | -d} *hybriddisk-alias*
clphdstat {--list | -l}
clphdstat {--perf | -p} [*interval* [*count*]] *hybriddisk-alias*

Description

This command displays the status related to mirroring of hybrid disk.

This command displays hybrid disk resources configuration information.

Option

--connect, -c
Displays the status of mirror connect used by hybrid disk resource.

--mirror, -m
Displays the mirroring status of hybrid disk resource.

--active, -a
Displays status of hybrid disk resource activation.

--detail, -d
Displays hybrid disk resources configuration information.

--list, -l
Displays hybrid disk resources list.

--perf
Displays statistical information on hybrid disk resources.

Parameter

hybriddisk-alias
Specifies a hybrid disk resource name.

interval

Specifies the sampling interval for statistical information. If no value is specified, 60 (sec) is specified by default.

You can specify a value from 1 to 9999.

count

Specifies the number of times statistical information is displayed. This parameter is used together with the *interval*. You can specify a value from 1 to 9999.

When *count* is omitted, statistical information displays indefinitely. To stop displaying statistical information, press [Ctrl] + [C].

Both the default value of *interval*, 60, and of *count*, 1, are used if these parameters are omitted.

Return value

0	Success
Other than 0	Failure

Notes
Run this command as the root user.

If there is no current server in the server group, the server in which a mirror agent is working normally becomes the current server.

The server having the highest priority in server priority in **Server Group Properties** is selected.

Example display after running this command
An example of the display after running this command is provided in the next topic.

Error Messages

Message	Cause/Solution
Error: Log in as root.	Log on as the root user.
Error: Failed to read the configuration file. Check if it exists or is configured properly.	Reading the configuration file has failed. Check to see if the configuration file exists and is configured correctly.
Error: Failed to acquire hybrid disk resource name. Check if the Mirror Agent is operating normally.	Acquiring a hybrid disk resource name has failed. Check to see if the Mirror Agent is operating normally.
Error: Specified hybrid disk resource was not found. Specify a valid hybrid disk resource name.	Failed to the specified hybrid disk resource. Specify a valid mirror disk resource name.
Error: Invalid hybrid-alias. Specify a valid hybrid disk resource name.	Specify a valid hybrid disk resource name.

Continued on next page

Table 8.45 – continued from previous page

Message	Cause/Solution
Error: Failed to get the server name. Check if the configuration file is correct and the Mirror Agent is operating normally.	Acquiring a server name has failed. Check to see if the configuration file is valid and the Mirror Agent is operating normally.
Error: Failed to communicate with other servers. Check if the Mirror Agent of the other server is operating normally and the interconnect LAN is connected.	Communicating with the remote server has failed. Check if the Mirror Agent in the remote server is operating normally and the interconnect is connected.
Error: Hybrid disks of the remote server may be down. Check if the Mirror Agent of the remote server is operating normally and the interconnect LAN is connected.	Communicating with the remote server has failed. Check to see if the Mirror Agent in the remote server is operating normally, and the interconnect is connected.
Error: Failed to get the hybrid disk status. Check if the Mirror Agent on the local server is operating normally.	Acquiring the hybrid disk status has failed. Check to see if the Mirror Agent in the local server is operating normally.
Error: Failed to acquire the mirror index. Check if the Mirror Agent is operating normally.	Check to see if the Mirror Agent is operating normally.
Error: mirror agent is not running Check if the Mirror Agent is active.	The Mirror Agent is not started up. Check the syslog or the alert message of the module type, mdagent.
Error: Failed to acquire the active status of the Mirror Agent of the local server. Shut down the cluster and reboot both servers	Acquiring the active status of mirror disk resource of the local server has failed. Shut down the cluster and restart both servers.
Error: Failed to acquire the active status of the Mirror Agent of the other server. Shut down the cluster and reboot both servers	Acquiring the active status of a mirror disk resource of the remote server has failed. Shut down the cluster and restart both servers.
Error: Failed to acquire mirror recovery status. Reboot the local server.	Acquiring the mirror recovery status has failed. Restart the local server.
Error: Failed to acquire the list of hybrid disks. Reboot the local server.	Acquiring a list of hybrid disks has failed. Restart the local server.
Error: Failed to acquire the mirror configuration information. Check if the Mirror Agent is operating normally.	Acquiring the mirror configuration data has failed. Check to see if the Mirror Agent is operating normally.
Error: Failed to acquire the hybrid disk configuration information of both servers. Shut down the cluster and reboot both servers	Acquiring the hybrid disk configuration data of both servers failed. Perform cluster shut down and restart both servers.
Error: The number of the bits of the bitmap is invalid. The mirror difference information of the cluster partition is invalid. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see the Reference Guide.	Acquiring the mirror difference information in the cluster partition has failed. Shut down the cluster. If this error happens again, replace the disk.
Error: Failed to get bitmap information. Failed to acquire the mirror difference information of the local server. Reboot the local server.	The mirror difference information in the cluster partition is invalid. Shut down the cluster. If this error happens again, replace the disk.
Error: Failed to get bitmap information. Failed to acquire the mirror difference information of the local server. Reboot the local server.	Acquiring the mirror difference information has failed of the local server. Restart the local server.
Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Reading the mirror difference information of the local server has failed. Restart the local server.
Error: Failed to acquire semaphore. Reboot the local server.	Acquiring semaphore has failed. Restart the local server.

Continued on next page

Table 8.45 – continued from previous page

Message	Cause/Solution
Error: A malloc error. Failed to reserve the memory space. Reboot the local server.	Reserving memory space has failed. Restart the local server.
Error: Mirror driver of the local server is not loaded. Refer to the Reference Guide to load the driver.	The mirror driver in the local server is not loaded. Check this by referring to "9. *Troubleshooting*" in this guide.
Error: Internal error (errorcode: 0xxxx). Shut down the cluster and reboot the server.	Shut down the cluster and restart the server.
Error: Failed to communicate with server %1 and %2. Check if both Mirror Agents of the two servers are operating normally and the interconnect LANs are connected. The server names are displayed where "%1" and "%2" are represented.	Failed to communicate with both servers represented in the message. Make sure that the mirror agents of both servers are running and the interconnect LANs are connected.
Error: Failed to communicate with server %1. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. Failed to acquire the hybrid disk detail information of the server %2. Shut down the cluster and reboot both servers.	Failed to communicate with the server %1. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Failed to acquire the hybrid disk detail information of the server %2. Shut down the cluster, and then restart the both servers. The server names are displayed where "%1" and "%2" are represented.
Error: Failed to acquire the hybrid disk detail information of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with server %2. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected.	Failed to acquire the hybrid disk detail information of the server %1. Shut down the cluster, and then restart the both servers. Failed to communicate with the server %2. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. The server name is displayed where "%1" or "%2" is represented.
Error: Failed to acquire the hybrid disk detail information of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire the hybrid disk detail information of both servers. Shut down the cluster, and then restart the servers. The server name is displayed where "%1" or "%2" is represented.

Continued on next page

Table 8.45 – continued from previous page

Message	Cause/Solution
Error: Failed to communicate with server %1. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. Failed to acquire mirror disk %3 net interface status of the server %2. Shut down the cluster and reboot both servers.	Failed to communicate with the server %1. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Failed to acquire the status of mirror disk connect of mirror disk resource %3 of server %2. Shut down the cluster and reboot both servers. The server name is displayed where "%1" or "%2" is represented. Where %3 is represented, the hybrid resource name is displayed.
Error: Failed to acquire hybrid disk %3 net interface status of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with server %2 . Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected.	Failed to acquire the status of hybrid disk connect of mirror disk resource %3 of server %1. Shut down the cluster and reboot both servers. Failed to communicate with the server %2. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. The server name is displayed where "%1" or "%2" is represented. Where %3 is represented, the hybrid resource name is displayed.
Error: Failed to acquire mirror disk %3 net interface status of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire the status of hybrid disk connect of both servers. Shut down the cluster, and then, restart the servers. The server name is displayed where "%1" or "%2" is represented. Where %3 is represented, the hybrid resource name is displayed.
Error: Failed to communicate with server %1. Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected. Failed to acquire the active status of the Hybrid disk %3 of the server %2. Shut down the cluster and reboot both servers.	Failed to communicate with the server %1. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Failed to acquire the active status of the Hybrid disk resource %3 of the server %2. Shut down the cluster and reboot both servers. The server name is displayed where "%1" or "%2" is represented. Where %3 is represented, the hybrid resource name is displayed.

Continued on next page

Table 8.45 – continued from previous page

Message	Cause/Solution
Error: Failed to acquire the active status of the Hybrid Mirror disk %3 of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with server %2 . Check if Mirror Agent of the server is operating normally and the interconnect LAN is connected.	Failed to acquire the active status of the hybrid disk resource %3 of the server %1. Shut down the cluster and reboot both servers. Failed to communicate with the server %2. Check if the Mirror Agent of the other server is running and the interconnect LAN is connected. Where %1 or %2 is represented, the server name is displayed. Where %3 is represented, the hybrid resource name is displayed.
Error: Failed to acquire the active status of the Hybrid disk %3 of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire the hybrid disk detail information of both servers. Shut down the cluster, and then restart the servers. Where %1 or %2 is represented, the server name is displayed. Where %3 is represented, the hybrid resource name is displayed.
Error: Failed to get all server names. Check if the configuration file is correct and the Mirror Agent is operating normally.	Failed to acquire the server name. Check if the configuration file is correct and the Mirror Agent is operating normally.
Error: The disk alias does not match the command.	The resource type of the specified resource name (mirror alias name) is invalid. Use clpmdstat for md resource, and clphdstat for hd resource.
Error: Invalid command name.	The command name is invalid. Do not change the file name of the clphdstat command.
Error: This server is not current server. Cannot perform this action.	This command cannot be executed because this server is not current server.
Error: Hybrid disk internal error.	An internal error occurred.
Error: The function of collecting statistics is disabled.	The statistical information collection function is disabled. Check the setting of Collect Mirror Statistics in the Mirror Agent tab in Cluster Properties by using the Cluster WebUI.
Error: Collecting mirror statistics failed. Please retry in a few seconds later.	Failed to collect statistical information because of a temporarily high load or other issue. Wait, and then execute the command again. If this message appears again, make sure that mdagent is running normally.

Display examples

- Hybrid disk connect status display

  When the --connect option is specified, the status of mirror connect that is used by hybrid disk resource is displayed.

```
Hybrid Disk Name : hd1

[Server : server1]
   192.168.0.1                          : Using

[Server : server2]
   192.168.0.2                          : Using
```

  Explanation of each item

Item	Description
Server Name	Name of the server
IP Address	IP address specified by hybrid disk connect
Status	Status of mirror connect Status Description ---------- Using Being used Free Not used Error Error -- Unknown

- Displaying the status of mirroring of hybrid disk resource

  The status of mirroring of the specified hybrid disk resource is displayed by specifying the --mirror option.

  – When the status of mirror disk resource is Normal:

```
Mirror Status: Normal

hd1                 server1               server2
----------------------------------------------------------------
Mirror Color        GREEN                 GREEN
```

  Explanation of each item

Item	Description
Mirror Status	Mirroring status of hybrid disk resource Status Description ---------- Normal Normal Recovering Mirror is recovering Abnormal Abnormal No Construction Initial mirror construction is not done

Continued on next page

Table 8.47 – continued from previous page

Item	Description
Mirror Color	Status of hybrid disk on each server Status Description --- GREEN Normal YELLOW Mirror is recovering RED Abnormal ORANGE Suspension (The server having the latest cannot be determined.) GRAY Being stopped, Unknown status BLACK Initial mirror construction is not done, error found in cluster partition data, etc. BLUE Both disks are active

– When the status of mirror disk resource is abnormal

```
Mirror Status: Abnormal

hd1                 server1               server2
-------------------------------------------------
Mirror Color        GREEN                 RED
Lastupdate Time     2018/03/24 15:41:07   --
Break Time          2018/03/24 15:40:38   --
Disk Error          OK                    OK
Difference Percent  1%                    --
```

Explanation of each item

Item	Description
Mirror Status	Status of hybrid disk resource[7]
Mirror Color	Status of hybrid disk on each server[7]
Last update Time	Last time when the data was updated on the server. This is not displayed when the hybrid disk status is unknown.
Break Time	Time when mirror break has occurred This is not displayed when the hybrid disk status is unknown.
Disk Error	Status of disk I/O Status Description --- OK Normal ERROR Error (No I/O) -- Unknown This is not displayed when the hybrid disk status is unknown.
Difference Percent	Percentage of differences in the data on each server. This is not displayed when the hybrid disk status is unknown.

– During mirror recovery

```
Mirror Status: Recovering
```

(continues on next page)

[7] See "Explanation of each item" in "When the status of mirror disk resource is Normal:"

(continued from previous page)

```
hd1                 server1               server2
-------------------------------------------------------------
Mirror Color        YELLOW                YELLOW

Recovery Status   Value
----------------------------------------
Status:           Recovering
Direction: src    server1
           dst    server2
Percent:          3%
Used Time:        00:00:01
Remain Time:      00:00:32
Iteration Times:  1/1
```

Explanation of each item

See "Explanation of each item" of "*Displaying the mirror status (clpmdstat command)*."

- Displaying active status of hybrid disk resource

  Active status of the specified hybrid disk resource is displayed when the --active option is specified:

```
hd1                server1           server2
-------------------------------------------------------------
Active Status      Active            Inactive
```

Status of mirror partition device

See "Status of mirror partition device" of "*Displaying the mirror status (clpmdstat command)*."

- Displaying hybrid disk resource information

  Configuration information of the specified hybrid disk resource is displayed when the --detail option is specified:

```
Hybrid Disk Name     : hd1
  Sync Switch        : On
  Sync Mode          : Sync
  Diff Recovery      : Disable
  Compress           :
       Sync Data     : Off
       Recovery Data : Off

[Server : server1]
  NMP/Disk Size(MB)  : 2447/2447
  DP Device          : /dev/sdb2
  CP Device          : /dev/sdb1

[Server : server2]
   NMP/Disk Size(MB) : 2447/2447
   DP Device         : /dev/sdb2
   CP Device         : /dev/sdb1
```

Explanation of each item

Item	Description
Hybrid Name	Hybrid disk resource name
Sync Switch	Perform data synchronization
Sync Mode	Synchronization Mode
Server Name	Current server name
NMP/Disk Size(MB)	NMP: the smaller size of data partition of servers Disk Size: actual data partition size
DP Device	Data partition device name
CP Device	Cluster partition device name

- Displaying the list of hybrid disk resources

  The list of hybrid disk resources is displayed when the --list option is specified:

```
[HybridDisk Option]
  server1 : Installed
  server2 : Installed
  server3 : Installed

[Servers Which Can Be Started]
 <hd1>
  [ServerGroup0 : server_group1]
   *server1
    server2
  [ServerGroup1 : server_group2]
   *server3
 <hd2>
  [ServerGroup0 : server_group1]
    server1
   *server2
  [ServerGroup1 : server_group2]
   *server3
```

  Explanation of each item

Item	Description
HybridDisk Option	License status of the Replicator DR
Servers Which Can Be Started	The server group of the hybrid disk resource and servers that can be started
*	Current server of each server group

- Displaying statistical information

  See "Displaying statistical information" of "*Displaying the mirror status (clpmdstat command)*"

8.15.2 Operating hybrid disk resource (clphdctrl command)

the clphdctrl command operates hybrid disk resources.

Command line

clphdctrl {--active | -a} *hybriddisk-alias*
clphdctrl {--active | -a} -nomount *hybriddisk-alias*
clphdctrl {--active | -a} -force [-ro] *hybriddisk-alias*
clphdctrl {--active | -a} -force -nomount *hybriddisk -alias*

clphdctrl {--deactive | -d} *hybriddisk-alias*
clphdctrl {--break | -b} *hybriddisk-alias*
clphdctrl {--force | -f} [-v] *recovery-source-servername hybriddisk-alias*
clphdctrl {--force | -f} *hybriddisk-alias*
clphdctrl {--recovery | -r} *hybriddisk-alias*
clphdctrl {--cancel | -c} *hybriddisk-alias*
clphdctrl {--rwait | -w} [-timeout *time* [-rcancel]] *hybriddisk-alias*
clphdctrl --getreq
clphdctrl --setreq *request-count*
clphdctrl --sync [*hybriddisk-alias*]
clphdctrl --nosync [*hybriddisk-alias*]
clphdctrl --setcur [*hybriddisk-alias*]
clphdctrl {--compress | -p} [*hybriddisk-alias*]
clphdctrl {--nocompress | -n} [*hybriddisk-alias*]
clphdctrl {--mdcswitch | -s} [*mdc-priority*] *hybriddisk-alias*

Important:

After releasing the access limitation to the mirror disk partition by --active option, make sure to put the access limitation again by --deactive option.
Additionally, do not use --deactive option while the resource is in active status.
If the resource in the active status is started or stopped, the file system may be corrupted.

Description

This command activates, deactivates or forcibly activates hybrid disk resource and recovers or forcibly recovers mirror.

This command disconnects a hybrid disk.

This command performs mirror recovery, forced mirror recovery, cancellation of mirror recovery, and waiting for the completion of mirror recovery.

This command displays and/or modifies the settings of maximum number of request queues.

This command switches the synchronization status of the mirror data.

This command acquires the current right of hybrid disk resource.

This command is used to set whether mirror data is to be compressed.

This command switches the communication path (mirror disk connect) to be used.

Option

--active,-a

Activates the hybrid disk resource on the local server.
If the status of hybrid disk resource is normal, mirroring is performed.
If the status of hybrid disk resource is not normal, mirroring will not be performed.

-force

Forcibly activates a hybrid disk resource. This command can be run on a server where mirroring is stopped.

-nomount

It allows access to hybrid partition device without mounting the file system.
This option is used with the --active option.
This option has no meaning if none is specified for the file system.

-ro

Forcibly activates a mirror disk resource in ReadOnly mode.
This option is used with the --active -force options.

--deactive,-d
Deactivates the activated hybrid disk resource on the local server.

--break,-b

Disconnects the hybrid disk resources forcibly specified with *hybriddisk-alias on* the server where the command is run.
The status of the hybrid disk resource on the server where the command is run becomes an error.
The status of the hybrid disk resource on the server where the command is not run does not change.
When a mirror is recovered, disconnection is canceled.
Hybrid disk data is not synchronized even when any data is written to a hybrid disk.
Auto mirror recovery is not automatically started until reboot is performed or disconnection is canceled after completion of mirror recovery.

--recovery,-r

Performs either full mirror recovery or differential mirror recovery for the specified hybrid disk resource.
Whether to perform full or differential mirror recovery is determined automatically.

--force,-f

Forcefully performs mirror recovery for the specified hybrid disk resource.
If only hybriddisk-alias is specified, the status of the hybrid disk where the command is run becomes normal forcibly. Mirror resynchronization is not performed.
If recovery-source-servername and hybriddisk-alias are specified, full mirror recovery is performed using recovery-source-servername as source data. The status of the hybrid disk becomes normal when the full mirror recovery completes.

-v
Forcefully performs mirror recovery without an analysis of the file system.

--cancel,-c

Cancels mirror recovery.
If auto mirror recovery is set to ON and the hybrid disk monitor resource is operating, mirror recovery will be automatically restarted a short while after mirror recovery is canceled. In this case, first suspend the hybrid disk monitor resource with either Cluster WebUI or the clpmonctrl command and then cancel mirror recovery.

--rwaitm,-w
Waits for the completion of the mirror recovery of the specified disk resource.

-timeout

Specifies the timeout period of mirror recovery completion (second). This option can be omitted.

When this option is omitted, timeout is not executed and waits for the completion of mirror recovery.

-rcancel

Cancels mirror recovery when the timeout of waiting of mirror recovery completion occurred. This option can be set when -timeout option is set.

When this option is omitted, the mirror recovery continues even after the timeout occurrence.

--getreq

Displays the current maximum number of request queues.

--setreq

Configures the maximum number of request queues.

When the server shuts down, what you have configured here returns to the value set in the cluster configuration data. Use the Cluster WebUI if you want to modify the cluster configuration data. For details, see "*Cluster properties*" "*Mirror driver tab ~ For Replicator/Replicator DR ~*" in "*2. Parameter details*."

The command is only effective on the server that runs the command.

--sync

This option switches the operation to the mirror synchronization.

When the hybrid disk resource name is not specified, the operation is switched to synchronizing the mirror data to all hybrid resources.

--nosync

This option switched the operation to the one that does not synchronize the mirror data.

When the hybrid disk resource name is not specified, the operation is switched to not performing the synchronization of the mirror data to all hybrid resources.

However, the data updated to a disk during a mirror recovery is synchronized to a standby server.

If auto mirror recovery is set to ON and the mirror disk monitor resource is operating, automatic mirror recovery will operate.

Even after the completion of mirror recovery, the operation will still not synchronize. To cancel this, execute the command with the --sync option specified.

When the server is shut down, the state will return to the synchronization operation that is set in the cluster configuration information. To change the cluster configuration information, use the Cluster WebUI. For details, see "Mirror tab" in "Mirror disk resource tuning properties" in "*Details tab*" in "*Understanding Mirror disk resources*" in "*3. Group resource details*" in this guide.

--setcur

This option acquires the current right of hybrid disk resource specified by *hybriddisk-alias on the server on which the command is executed.*

--compress,-p

Temporarily switches on the compression mode of mirror transfer data.

If the synchronous mode of mirror data is "Synchronous", only the recovery transfer data is compressed.

If the synchronous mode of mirror data is "Asynchronous", both the asynchronous transfer data and the recovery transfer data are compressed

When the hybrid disk resource name is not specified, the operation is performed to all hybrid disk resources.

--nocompress,-n

Temporarily switches off the compression mode of mirror transfer data.

When the mirror disk resource name is not specified, the operation is performed to all hybrid disk resources.

--mdcswitch,-s

Switches the mirror connection to another mdc that has the specified priority.

If the priority is not specified, the mirror connection is switched to the mdc that has the next highest priority after the current mdc.

If the mirror connection is connected to the mdc that has the lowest priority, it is switched to the one that has the highest priority.

If the mirror connection has already been switched to the specified mdc, the command terminates normally without performing any processing.

If the specified mdc does not exist, an error occurs.

Parameter

recovery-source-servername
Specifies a server name of the copy source.

hybriddisk-alias
Specifies a hybrid disk resource name.

request-count
Specifies a maximum number of request queues. You can specify a number from 2048 through 65535.

time
Specifies the timeout period of mirror recovery completion (seconds).

mdc-priority

Specifies the priority of mdc.

This is not the priority number of mdc in whole cluster, but the priority number (1 or 2) of mdc used by the hybrid disk resource.

Return Value

0	Success
255 (-1)	Failure
254 (-2)	Target disk is not configuring mirror, or the mirror configuring failed on the process. (Only when --rwait option is specified, including the case when mirror recovery is interrupted by -rcancel.)
253 (-3)	Timeout of mirror recovery of target disk occurs (Only when --rwait -timeout option is specified)

Remarks

request-count, which is displayed by specifying the --getreq option, is the same as "Max. Number of Request Queues" which is displayed by using the clpstat command.

```
# clpstat --cl --detail
```

This command returns control when the specified processing starts. Run the clphdstat command to check the processing status.

Notes

Run this command as the root user.

--active/--force (Forced mirror recovery) /--setcur can be executed on a server that has a current right or that can have a current right.

You can execute --recovery or --force (full mirror recovery with *recovery-source-servername* specified) in the following condition.

- The server of copy source has the current right or can have a current right.
- The server of copy target has the current right or can have a current right.
  (Mirror recovery cannot be performed on the server without current right in the cluster where hybrid disk resource is configured on the shared disk.)

--break/--cancel/--setreq/--sync/--nosync/--setreq can be executed on the server that has a current right.

For further information on the conditions for using this command to change the current server, see "*List of operations to switch a current server*".

When performing mirror recovery again after mirror recovery failed, specify the same server you used last time for mirror recovery as a copy source.

To resume the forced mirror recovery that was suspended by selecting **Cancel**, use this command for forced mirror recovery.

In a cluster with more than three nodes, if the server where the command is run is not included in a startup server of a group including hybrid disk resources, this command results in error. Do not run this command if the server is not included in a startup server of a group.

If, during mirror synchronization, mirror synchronization is interrupted with either the --break (-b) or --nosync option or if, during mirror recovery, mirror recovery is interrupted, the file system and application data may prove to be abnormal even if the mirror disk to be synchronized is made accessible by performing forced activation or forced mirror recovery. For details, see "Mirror data reference at the synchronization destination if mirror synchronization is interrupted" in "Notes and Restrictions" in the "Getting Started Guide".

Example of command execution

Example 1: When activating the hybrid disk resource hd1:

```
# clphdctrl --active hd1
<hd1@server1>: active successfully
```

Example 2: When deactivating the hybrid disk resource md1:

```
# clphdctrl --deactive hd1
<hd1@server1>: deactive successfully
```

Example 3: When disconnecting the hybrid disk resource hd1:

```
# clphdctrl --break hd1
hd1: isolate successfully
```

Example 4: When the status of hybrid disks both servers is error, and you need to recover the operation that uses the resource hd1 (group name: failover1) as soon as possible:

```
# clphdctrl --force hd1
The data of mirror disk in local server maybe is not latest.
Do you still want to continue? (Y/N)
```

Example 5: When recovering mirroring of the hybrid disk resource hd1 :

```
# clphdctrl --recovery hd1
```

Example 6: When setting the maximum number of request queues to 2048:

```
# clphdctrl --setreq 2048
current I/O request count <2048>
```

Example 7: When configure the setting that does not perform the data synchronization to the hybrid disk resource hd1:

```
# clphdctrl --nosync hd1
```

Error Messages

Message	Cause/Solution
Error: Log in as root.	Log on as the root user.
Error: Failed to read the configuration file. Check if it exists or is configured properly.	Reading the configuration file has failed. Check to see if the configuration file exists and is configured correctly.
Error: Specified hybrid disk resource was not found. Specify a valid mirror disk resource name.	Locating the specified hybrid disk resource has failed. Specify a valid hybrid disk resource name.
Error: Invalid hybrid-alias. Specify a valid mirror disk resource name.	Specify a valid hybrid disk resource name.
Error: Failed to get the server name. Check if the configuration file is correct and the Mirror Agent is operating normally.	Acquiring the server name has failed. Check if configuration file is correct and the Mirror Agent is operating normally.
Error: Specified server name was not found. Check if the server name exists in the configuration file.	The specified server name was not found. Check to see if the entered server name exists in the configuration file.
Error: Invalid server name. Specify a valid server name.	Specify a valid sever name.
Error: Failed to communicate with other servers. Check if the Mirror Agent of the other server is operating normally and the mirror disk connect is connected.	Communicating with the remote server has failed. Check to see if the Mirror Agent of the remote server is operating and the mirror disk is connected.
Error: Failed to get the hybrid disk status. Check if the Mirror Agent on the local server is operating normally.	Acquiring the hybrid disk status has failed. Check to see if the Mirror Agent of the local server is operating normally.
Error: Failed to get the mirror index. Check if the Mirror Agent is operating normally.	Check to see if the Mirror Agent is operating normally.
Error: The status of hybrid disk resource of the local server is abnormal.	The hybrid disk resource of the local server has a problem.
Error: Specified hybrid disk resource is already active. Check active status of hybrid disk resource by running the following command: clpmdstat --active <alias>	The specified hybrid disk resource is already activated. Check the status of the hybrid disk resource using the following command. clpmdstat --active <alias>
Error: A hardware error has occurred on the disk. Check the disk.	A hardware error has occurred on the disk. Check the disk.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Error: The sizes of data partition of the servers do not match.	Data partition sizes of both servers do not match.
Error: Specified hybrid disk is not active. Check the active status of hybrid disk resource.	The specified hybrid disk resource is not activated. Check the status of hybrid disk resource.
Error: There is no recovering hybrid disk resource.	There is no hybrid disk under mirror recovery process.
Error: Mirror hybrid resource is recovering. Wait until mirror recovery completes.	The hybrid disk resource is under mirror recovery process. Wait until mirror recovery is completed
Error: Failed to cancel the mirror recovery. The system may be highly loaded. Wait for a while and try again.	Stopping mirror recovery has failed. The system may be heavily loaded. Wait for a while and try again.
Error: Performed mirror recovery to the hybrid disk resource that is not necessary to recover the mirror. Run the clpmdctrl--force command if you want to perform forced mirror recovery.	Mirror recovery has been performed on the hybrid disk resource that is in normal status and not requiring mirror recovery. To perform forced mirror recovery, use "clpmdctrl --force."
Error: Specification of the server that is copied from is incorrect. When executing mirror recovery again after a failure end of mirror recovery, specify the same server as the previous one.	The server specified for a copy source is invalid. When performing the mirror recovery again after the mirror recovery has failed, specify the same server that you specified last time for the failed mirror recovery as a copy source.
Error: Forced mirror recovery is required. Run the clphdctrl --force command to perform the recovery.	Forced mirror recovery is necessary. Use "clphdctrl --force" and perform forced mirror recovery.
Error: Server with old data is specified as the server which is copied from. Specify a correct recovery direction.	The server with old data is specified as a copy source. Specify a correct recovery direction.
Error: Failed to acquire mirror recovery status. Reboot the local server.	Acquiring the mirror recovery status has failed. Restart the local server.
Error: Both of the mirrors are not constructed. Initial mirror configuration of the hybrid disks by running the clpmdctrl --force command is necessary.	Initial mirror construction of hybrid disk is necessary. Construct initial mirror configuration using "clphdctrl --force."
Error: Initial mirror configuration of mirror disk of local server is necessary. Specify the other server as the one that is copied from by using the clphdctrl --force command to configure an initial mirror.	Initial mirror construction is necessary for the hybrid disk of the local server. Specify the remote server as a copy source and construct initial mirror using "clphdctrl --force."
Error: Initial mirror configuration of mirror disk of the other server is necessary. Specify the local server as the one that is copied from by using the clphdctrl--force command to configure an initial mirror.	Initial mirror construction is necessary for the hybrid disk of the remote server. Specify the local server as a copy source and construct initial mirror using "clphdctrl --force."
Error: Mirror flag error. Use "clphdinit" to construct the mirror. The status of cluster partition of the hybrid disk resource is abnormal. When the server with the error has the latest data, backup the data, initialize the cluster partition, and replace the same disk by using the same disk. If the error persists, change the disk to new one.	The cluster partition of the hybrid disk resource has a problem. When the server with error has the latest data, back up the data, initialize the cluster partition according to Chapter 8 "Verifying Operation" in the Installation and Configuration Guide, and follow the same way as described in "How to replace a mirror disk with a new one" in Chapter 1, "The system maintenance information" in the maintenance guide, using the same disk. If this occurs again, replace the disk with a new disk.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Error: Both local and remote mirrors are active. Shut down the cluster and execute forced mirror recovery after rebooting the server.	Both systems are active. Shut down the cluster and perform forced mirror recovery after reactivating the server.
Error: Mirror Agent is not running. Check if the Mirror Agent is active.	The Mirror Agent is not started up. Check to see if the Mirror Agent is running.
Error: System calls error. Failed to run the system command when active and/or inactive. Check if the search path is set to an environment variables.	Running the system command when active/inactive has failed. Check to see if a search path is set as an environmental variable.
Error: Failed to create a mount point. The disk space may not be sufficient.	Creating a mount point has failed. Disk space may be insufficient. Check it.
Error: Timeout has occurred on active fsck. When it is not journaling file system, it may take time to run fsck if the size of data partition of hybrid disk is large. Set timeout of fsck longer.	fsck time-out has occurred. In case it is not the journaling file system, running fsck may take time when the data partition of the hybrid disk is large. Set the longer time for the fsck time-out using the Cluster WebUI.
Error: Timeout occurs at activation mount. Set mount timeout longer	Time-out has occurred at active mounting. Set the mounting time-out longer by using the Cluster WebUI.
Error: Timeout occurs at deactivation mount. Set unmount timeout longer.	Time-out has occurred at inactive unmounting of the file system. Set the mount time-out period longer by using the Cluster WebUI.
Error: fsck failed. Check if file system type of data partition does not match configuration file, fsck option is incorrect or partition is incorrect.	Running fsck has failed. Check to see if the file system type of the data partition matches to the configuration file, fsck option is valid, and partition is not destroyed.
Error: Failed to mount when active. The file system type of the data partition does not match the settings of the configuration file, or the partition may be corrupted.	Mounting during activation has failed. Check to see if the file system type of the data partition matches to the configuration file, fsck option is valid, and the partition is not destroyed.
Error: Failed to unmount when inactive. Check if the file system on the data partition is busy.	Unmount during deactivation has failed. Check to see if the file system on data partition is not busy.
Error: Hybrid disk resource is on process of activation. Execute after activation is completed.	The hybrid disk resource is in the process of activation. Try after activation is completed.
Error: Failed to perform forced mirror recovery or activate a single server. Check if any hardware error has occurred on the disk.	Performing forced recovery or activating a standalone server has failed. Check to see if any hardware error has occurred on the disk.
Error: Entered incorrect maximum number of request queues. Check the specifiable range.	Invalid maximum number of request queues is entered. Check the range of numbers that can be specified.
Error: Failed to set the maximum number of request queues. Reboot the local server.	Setting a maximum number of request queues has failed. Restart the local server.
Error: Failed to acquire the maximum number of request queues. Reboot the local server.	Acquiring a maximum number of request queues has failed. Restart the local server.
Hybrid disk resource was not found on local server. Cannot perform this action.	The hybrid disk resource was not defined on the local server. Cannot configure the maximum number of request que. Check the status of the mirror disk resource.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Error: Failed to get the NMP path. Check if the Mirror Agent is operating normally. Reboot the local server.	Check to see if the Mirror Agent is operating normally. Restart the local server.
Error: Failed to acquire the mirror configuration information. Check if the Mirror Agent is operating normally.	Acquiring the mirror configuration information has failed. Check to see if the Mirror Agent is operating normally.
Error: Failed to acquire the hybrid disk configuration information. Reboot the local server.	Acquiring hybrid disk configuration data has failed. Restart the local server.
Error: Failed to acquire the hybrid disk configuration information of both local and remote servers. Shut down the cluster and reboot both servers	Acquiring hybrid disk configuration data of both servers has failed. Shut down the cluster and restart both servers.
Error: Failed to get the number of bits of the bitmap due to the errors occurred when acquiring the mirror difference information of the cluster partition. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see the Reference Guide.	Acquiring the information of mirror differences on the cluster partition has failed. Shut down the cluster. If the error occurs again, replace the disk. For information on how to replace a disk, see "The system maintenance information" in the "Maintenance Guide".
Error: The number of the bits in the bitmap is invalid. The mirror difference information of the cluster partition is invalid. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see Reference Guide.	The information of the mirror differences in the cluster partition is invalid. Shut down the cluster. If the error occurs again, replace the disk. For information on how to replace a disk, see "The system maintenance information" in the "Maintenance Guide".
Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Reading the information of mirror differences on the local server has failed. Restart the local server.
Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Reading the information of the mirror differences on the remote server has failed. Restart the remote server.
Error: Failed to get the bitmap information of the local server due to the errors occurred when acquiring the mirror difference information of the local server. Reboot the local server.	Acquiring the information of the mirror differences on the local server has failed. Restart the local server.
Error: Failed to read the disk space. Shut down the cluster and reboot the server	Acquiring the disk space has failed. Shut down the cluster and restart the server.
Error: Failed to acquire the disk space of the other server. Shut down the cluster and reboot both servers.	Acquiring the disk space of the remote server has failed. Shut down the cluster and restart the server.
Error: Setting of cluster partition failed. Restart local server.	Configuring the cluster partition has failed. Restart the local server.
Error: Error occurred on the settings of the hybrid disk resource. Reboot the local server.	Error occurred in the status settings of hybrid disk resource. Restart the local server.
Error: Failed to create a thread. Reboot the local server.	Creating thread has failed. Restart the local server.
Error: Internal error. Failed to create process. Reboot the local server.	Creating the process has failed. Restart the local server.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Error: Failed to acquire semaphore. Reboot the local server.	Acquiring semaphore has failed. Restart the local server.
Error: A malloc error. Failed to reserve the memory space. Reboot the local server.	Reserving memory has failed. Restart the local server.
Error: Mirror driver of the local server is not loaded. Confirm kernel version.	The mirror driver of the local server is not loaded. Check the kernel version.
Error: Mirror recovery cannot be executed as NMP size of mirror recovery destination is smaller than the size of where the mirror is recovered from. Change the recovery destination and try again.	Mirror recovery cannot be performed because NMP size of recovery destination is smaller than the recovery source. Change the destination and try again.
Error: NMP size of local server is bigger, cannot active. Initial mirror configuration is not completed. Execute mirror recovery from server of smaller NMP size to that of larger one.	Initial mirror configuration is not completed. Perform forced mirror recovery from the server whose NMP size is smaller to the larger one.
Local and remote recovery mode do not match. Reboot a server other than the master server to keep the same contents of configuration file among servers. Note that a failover may occur at server reboot.	The both servers are different on the recovery mode. The recovery is not performed. Restart the servers other than master server to make the information file be the same among servers. Note that a failover may occur at server reboot.
Failed to get remote recovery mode. Recovery will not be interrupted. Check the communication status of mirror connect.	Failed to get remote recovery mode. Recovery will not be interrupted. Check the communication status of mirror connect.
Failed to get local recovery mode. Recovery will not be interrupted. Note that a failover may occur at server reboot.	Failed to get local recovery mode. Recovery will not be interrupted. Restart the local server. Note that a failover may occur when the server is restarted.
Local or remote mirror is forced activated. Cannot to perform this action.	Hybrid disk is forcibly activated. Cannot perform the mirror recovery. Check the status of local or remote mirror.
The recovery destination of hybrid disk is activated. Cannot perform this action.	The recovery destination of mirror disk is activated. Cannot perform the mirror recovery. Check the status of the mirror disk.
Hybrid disk connection is disconnected. Cannot perform this action.	The communication status of hybrid disk connect is error. Cannot perform the mirror recovery. Check the status of the mirror disk connect.
Failed to get hybrid disk list and failed to set all NMP sync flag. Reboot the local server. Note that a failover may occur at server reboot.	The setting for synchronizing the data of all hybrid disks failed since acquiring a list of hybrid disks failed. Reboot the local server. Note that a failover may occur at server reboot.
Failed to get hybrid disk list and failed to set all NMP sync flag to OFF. Reboot the local server. Note that a failover may occur at server reboot.	The setting for not synchronizing the data of all hybrid disks failed since acquiring a list of hybrid disks failed. Reboot the local server. Note that a failover may occur at server reboot.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Failed to set sync flag on both servers. Shut down a cluster and reboot server.	The setting for synchronizing the data failed on both servers. Shut down the cluster and restart it.
Failed to set sync flag to OFF on both servers. Shut down a cluster and reboot server.	The setting for not synchronizing data failed on both servers. Shut down the cluster and restart it.
%1: Succeeded to set sync flag ON on %2 Failed to set sync flag ON on %3 Check the communication status of mirror connect	The setting of synchronizing data of %1 succeeded on the server %2, failed on the server %3. Check the running status of the server or the communication status of the mirror disk connect. The resource name is displayed where %1 is represented. The server name of which the setting succeeded is displayed where %2 is represented. The server name of which the setting failed is displayed where %3 is represented.
%1: Succeeded to set sync flag OFF on %2 Failed to set sync flag OFF on %3 Check the communication status of mirror connect	The setting of not synchronizing data of %1 succeeded on the server %2, failed on the server %3. Check the running status of the server or the communication status of the mirror disk connect. The resource name is displayed where %1 is represented. The server name of which the setting succeeded is displayed where %2 is represented. The server name of which the setting failed is displayed where %3 is represented.
Succeeded to set sync flag on remote server and failed on local server. Note that a failover may occur at server reboot.	The setting for synchronizing the data failed on the local server, yet succeeded on the other server. Restart the local server. Note that a failover may occur when the server is restarted.
Succeeded to set sync flag to OFF on remote server and failed on local server. Note that a failover may occur at server reboot.	The setting for not synchronizing the data failed on the local server, yet succeeded on the other server. Restart the local server. Note that a failover may occur when the server is restarted.
Cannot change the settings of sync status during mirror recovery. Change the settings after mirror recovery is completed.	The setting of synchronizing data cannot be changed during mirror recovery. Change the settings after mirror recovery is completed.
Hybrid disk resource was not found on local server. Cannot perform this action.	The hybrid disk resource is not defined on the local server. The setting of synchronizing data cannot be changed.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
The status of the hybrid disk does not satisfy the conditions to perform this action. A probable cause: 1. Local hybrid disk is not initialized or is already force activated. 2. Local hybrid disk is not RED or remote is GREEN or remote is already activated.	The status of mirror is invalid. Cannot perform a forced recovery.
The data of hybrid disk in the local server may not be the latest. Do you still want to continue? (Y/N)	The data of the local server may not be the latest. Cannot check the status of hybrid disk on the other server.
Forced recovery has completed successfully.	The forced mirror recovery has successfully completed.
The status of hybrid disk in local server is not GREEN or is already activated. Cannot perform this action.	The status of mirror is invalid. Cannot disconnect a mirror.
Failed to set an isolate flag in the local server.	Cannot update the flag for mirror disconnect.
Isolated completed successfully.	The mirror disconnect is successfully completed.
The status of the hybrid disk does not satisfy the conditions to perform this action. A probable cause: 1. Hybrid disk is not initialized or is not RED. 2. Hybrid disk is already activated.	The status of mirror is invalid. Cannot perform the forced activation.
sync flag of %1 is successfully set to ON.	The data synchronization is set to on. A name of the mirror resource is displayed where %1 is represented.
Failed to set sync flag of %1 on both servers. Shut down the cluster and reboot server.	Failed to set the data synchronization flag on the both servers. A name of the mirror resource is displayed where %1 is represented.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
%3: Succeeded to set sync flag ON on %1 Failed to set sync flag ON on %2 Check the communication status of mirror connect.	Failed to set the data synchronization flag on either of the servers. Check if the mirror disk connect can properly communicate. A name of the successfully-set server is displayed where %1 is represented. A name of the faulty-set server is displayed where %2 is represented. A name of the mirror resource is displayed where %3 is represented.
%1: Cannot change the settings of sync status during mirror recovery. Change the settings after mirror recovery is completed.	Cannot change the data synchronization flag during mirror recovery. Change the settings after mirror recovery is completed. A name of the mirror resource is displayed where %1 is represented.
sync flag of %1 is successfully set to OFF.	The mirror synchronization is set to off for %1. A name of the mirror resource is displayed where %1 is represented.
%3: Succeeded to set sync flag OFF on %1 Failed to set sync flag OFF on %2 Check the communication status of mirror connect.	Failed to set the data synchronization flag on either server. Check if the mirror disk connect can normally communicate. A name of the successfully-set server is displayed where %1 is represented. A name of the faulty-set server is displayed where %2 is represented. A name of the mirror resource is displayed where %3 is represented.
The specified hybrid disk is not defined on this server.	The specified hybrid disk is not defined on the local server.
Failed to acquire the path of mirror device. Check if the Mirror Agent is operating normally. Reboot the local server.	Failed to acquire the device name of the mirror disk. Check if the mirror agent is running.
The disk alias does not match the command.	The resource type of specified resource name (mirror alias name) is invalid. Use clpmdctrl for md resource, clphdctrl for hd resource.
Invalid command name.	The command name is invalid. Do not change the file name of clphdctrl command.
There is an error when the server gets current priority.	An error has occurred when the server acquired the current priority.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Data synchronizing. Cannot perform this action.	This action cannot be performed on the data synchronization.
The other server is already active. Cannot perform this action.	This action cannot be performed because the resource is activated on the other server.
Cannot judge which side has the nearest data. Cannot perform this action. Reboot or execute force recovery.	Because which server has the latest data cannot be determined, this action cannot be performed. Perform the Forced Mirror Recovery.
Failed to get host name.	Acquiring the server name has failed.
This server is not current server. Cannot perform this action.	This command cannot be performed because the specified server is not the current server.
Hybrid disk internal error.	An internal error has occurred.
The current server is being forced to activated, cannot release current right.	The current priority cannot be released while the resource is activated on the server with the current priority.
The current server is changing. Cannot perform this action.	This command cannot be performed because the current priority is being shifted from the current server.
<%1>: mirror broken	The status of mirror is invalid. The target disk is in not configuring a mirror, or mirror configuring failed during the process. A name of the mirror resource is displayed where %1 is represented.
<%1>: recovery timeout	Mirror recovery timed out. Check if the specified timeout period is appropriate, and if the disk I/O or communication delay is not occurring due to heavy loads. A name of the mirror resource is displayed where %1 is represented.
Cannot perform this action.(Device: %1). Check if the Cluster Partition or Data Partition is OK.	Could not operate the hybrid disk resource because the hybrid disk resource is not running due to abnormity with the cluster partition or data partition.
<%1> : Succeeded to set compress flag ON.	The compression of mirror transfer data of resource %1 was switched on. The resource name is displayed where %1 is represented.
<%1> : Succeeded to set compress flag OFF.	The compression of mirror transfer data of resource %1 was switched off. The resource name is displayed where %1 is represented.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
<%1> : Failed to set compress flag ON.	Switching on the compression of mirror transfer data of the resource %1 failed. The mirror disk resource name is displayed where %1 is represented.
<%1> : Failed to set compress flag OFF.	Switching off the compression of mirror transfer data of the resource %1 failed. The mirror disk resource name is displayed where %1 is represented.
<%1> : Failed to set compress flag ON on %2.	Switching on the compression of mirror transfer data of the resource %1 failed on the server %2. Check the running status of the server or the communication status of the mirror disk connection. The mirror disk resource name is displayed where %1 is represented. The server name is displayed where %2 is represented.
<%1> : Failed to set compress flag OFF on %2.	Switching off the compression of mirror transfer data of the resource %1 failed on the server %2. Check the running status of the server or the communication status of the mirror disk connection. The mirror disk resource name is displayed where %1 is represented. The server name is displayed where %2 is represented.
<%1>: Succeeded to switch mirror disk connection. Now using mdc <priority:%2>.	The mirror disk connection was switched to the mdc of priority number %2 of the resource %1. The mirror disk resource name is displayed where %1 is represented. The number of the priority of the newly used mirror disk connection is displayed where %2 is represented.
Error: There is no need to switch mirror disk connection.	The specified mirror disk connection has already been used. Switching is not needed.
Error: Failed to switch mirror disk connection. The specified mirror disk connection is ERROR.	The specified mirror disk connection was not switched to because it was in the ERROR status.

Continued on next page

Table 8.49 – continued from previous page

Message	Cause/Solution
Error: Failed to switch mirror disk connection. The other mirror disk connections are ERROR.	The other mirror disk connections were not switched to because they all were in the ERROR status.
Error: Failed to switch mirror disk connection.	Switching mirror disk connection failed.
Error: Specified mdc priority does not exist.	The specified priority number is invalid. It has not been defined in the configuration information.

List of operations to switch a current server

Current server is also switched when the following operations are performed with this command.

Hybrid disk status		Whether or not current server can be changed		Possible operation	
Server group 1	Server group 2	Server group 1	Server group 2	Server group 1	Server group 2
normal/ inactive	normal/ inactive	Yes	Yes	1	1
normal/ inactive	error/ inactive	Yes	Yes	1	1,3
normal/ inactive	error/ inactive	No	Yes	-	1,3
error/ inactive	error/ inactive	Yes	Yes	1,2,3	1,2,3
error/ inactive	error/ forcibly activated	Yes	No	2,3	-
error/ inactive	Unknown	Yes	No	2,3	-
pending/ inactive	pending/ inactive	Yes	Yes	1	1
pending/ inactive	Unknown	Yes	No	2	-

1	Recovering mirror (differential/entire data)
2	Forcefully recovering mirror on one server
3	Canceling access restriction (Forcible activation)
4	Disconnecting a mirror disk

Note: See the online manual to perform the operations like those above on Cluster WebUI.

8.15.3 Initializing hybrid disks (clphdinit command)

the clpmdinit command initializes a hybrid disk.

Command line

clphdinit {--create | -c} normal [*hybriddisk-alias*]
clphdinit {--create | -c} quick [*hybriddisk-alias*]
clphdinit {--create | -c} force [*hybriddisk-alias*]

Important: Generally you do not need to run this command when constructing or operating a cluster. You should exercise caution when you use this command because the partition used for the data will be initialized.

Description

This command initializes the cluster partition of a hybrid disk resource.

File systems are not created automatically to the data partition of the hybrid disk resource in this version. Create file systems in advance as necessary.

Option

{--create, -c} <mode>
mode

normal

Initializes a cluster partition, if necessary.

The necessity is determined by the magic number set by EXPRESSCLUSTER on the cluster partition.

Generally, it is not necessary to run the command with this option.

quick

Initializes the cluster partition, if necessary.

Whether or not it is necessary to initialize the cluster partition is determined by the magic number set by EXPRESSCLUSTER on the cluster partition.

Generally, it is not necessary to run the command with this option.

force Forcefully initializes the cluster partition.

Forcefully initializes the cluster partition.

This option is used when using the disk that was once used as a hybrid disk of EXPRESSCLUSTER again.

Parameter

hybriddisk-alias
Specifies a hybrid disk resource name. If this parameter is not specified, the process is performed on all hybrid disk resources.

Return Value

0	Success
Other than 0	Failure

Notes

You should exercise caution when you run this command because the hybrid disk will be initialized.

When there are multiple servers in one server group, execute the command on one of the servers to initialize a cluster partition.

Run this command as the root user.

Do not run other commands, until this command is returned.

When running this command, make sure that the MirrorAgent is stopped in all servers in the cluster. To check the Hybrid Agent is stopped on all servers, run the following command:

```
# ps -e | grep clpmdagent
```

In a cluster with more than three nodes, if the server where the command is run is not included in a startup server of a group including hybrid disk resources, this command results in error. Do not run this command if the server is not included in a startup server of a group.

Example of command execution

Example 1: When forcefully initializing the cluster partition because the disk to be used for the hybrid disk resource hd1 was once used as a hybrid disk of EXPRESSCLUSTER:

```
# clphdinit --create force hd1
mirror info will be set as default
the main handle on initializing hybrid disk <hd1> success
initializing hybrid disk complete
```

Error Messages

Message	Causes/Solution
Log in as root.	Log on as the root user.
Stop the Mirror Agent.	Stop the mirror agent.
The clphdinit command is currently running. Execute after it is completed.	This command is running. Run after it is completed.
Invalid hybrid-alias. Specify a valid hybrid disk resource name.	Specify a valid hybrid disk resource name.
The mirror hybrid disk resource was not found. Set the hybrid disk resource properly.	The hybrid disk resource was not found. Set a hybrid disk resource properly.
Specified hybrid disk resource <%1> was not found. Specify a valid hybrid disk resource name.	The specified hybrid disk resource was not found. Specify a valid mirror disk resource name.
The partition does not exist. Check if the cluster partition of specified hybrid disk resource exists (<%1>).	Check to see if the specified cluster partition of the hybrid disk resource exists.
Check if the cluster partition size of specified hybrid disk resource is larger than 1GB. <%1>	Check to see if the cluster partition size of the specified hybrid disk resource is 1GB or larger.
Internal error (open error <%1>). The cluster partition of the hybrid disk resource may not exist or the OS resource may be insufficient.	Check to see if the cluster partition of the specified hybrid disk resource exists or OS resource is sufficient.
Internal error (<%1> cluster partition: unknown error). Failed to initialize the cluster partition. Check if any hardware error has occurred on the disk.	Initializing the cluster partition has failed. Check to see if there is any hardware error on the disk.

Continued on next page

Table 8.50 – continued from previous page

Message	Causes/Solution
Internal error (<%1> cluster partition: %2). Check if the size of cluster partition is sufficient and if there is any hardware error on the desk.	Setting a cluster partition has failed. Check to see if the cluster partition space is sufficient and a hardware error has not occurred on the disk.
The data partition does not exist (<%1>). Check if the data partition of the specified hybrid disk resource exists. Data Partition is: %2	Check to see if the data partition of the specified hybrid disk resource exists.
Failed to initialize the cluster partition <%1>. The data partition of the specified hybrid disk resource may not exist, hardware error may have occurred on the disk, or specified file system may not be supported by OS. Check them. mirror<%2>: fstype<%3>	Initializing the data partition has failed. Check to see if the data partition of the specified hybrid disk resource exists, hardware error has not occurred on the disk and the specified file system is supported by OS.
Unknown error occurred when formatting mirrordisk<%1>. The data partition of the specified hybrid disk resource may not exist or hardware error may have occurred on the disk. Check them.	Initializing the data partition has failed. Check to see if the data partition of the specified hybrid disk resource exists and a hardware error has not occurred on the disk.
Internal error (Failed to open the data partition:<%1>). Failed to initialize the data partition. The data partition of the specified hybrid disk resource may not exist or OS resource may not be sufficient. Data Partition is: %2	Initializing the data partition has failed. Check to see if the data partition of the specified hybrid disk resource exists and OS resource is sufficient.
Internal error (data partition check error---<%1>). Failed to initialize the data partition. Check if any hardware error has occurred on the disk.	Initializing the data partition has failed. Check to see if any hardware error has not occurred on the disk.
Failed to acquire hybrid disk list information. Reboot the local server.	Acquiring a list of hybrid disk has failed. Restart the local server.
Internal error (PID write failed). Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Internal error (initialization failed) Failed to read the configuration file, or failed to initialize the shared memory or semaphore. Check if the file is configured properly and reboot the local server.	Reading the configuration file, initialize the shared memory or semaphore has failed. Check to see if configuration file is correct, and restart the local server.
Internal error (termination failed) Failed to release the shared memory. Check if any system error has occurred while running the program.	Freeing up the shared memory has failed. Check to see if any system error has not occurred while running the program.
A malloc error. Failed to reserve the memory space. Reboot the local server.	Reserving memory space has failed. Restart the local server.
An error has occurred when the data partition is set to writable mode. <Device:%1>. Reboot the local server.	An error occurred when the data partition was set to the writable mode. Restart the local server.
An error has occurred when the data partition is set to read-only mode. <Device:%1>. Reboot the local server.	An error occurred when the data partition was set to the read-only mode. Restart the local server.
Cluster Partition or Data Partition does not exist.	No cluster partition or data partition exists. Check if a partition is created.

Continued on next page

Table 8.50 – continued from previous page

Message	Causes/Solution
Failed to upgrade the cluster partition of <%s>.	Upgrading a cluster partition failed. Check if there is an error on the disk.
Specified hybrid disk resource was not found on local server. Cannot perform this action.	The hybrid disk resource is not defined on the local server. Cannot perform initialization. Check the status of the mirror disk resource.
The disk alias does not match the command.	The resource type of the specified resource name (mirror alias name) is invalid. Use clpmdinit for md resource, clphdinit for hd resource.
Invalid command name.	The command name is invalid. Do not change the file name of clphdinit command.
Initializing hybrid disk of %1 failed. Check if the Cluster Partition or Data Partition is OK.	Failed to initialize the hybrid disk resource because the cluster partition or the data partition is abnormal.

8.16 Outputting messages (clplogcmd command)

the clplogcmd command registers the specified message with syslog and alert, reports the message by mail, or sends it as an SNMP trap.

Command line

clplogcmd -m *message* [--syslog] [--alert] [--mail] [--trap] [-i *eventID*] [-l *level*]

Note: Generally, it is not necessary to run this command for constructing or operating the cluster. You need to write the command in the exec resource script.

Description

Write this command in the exec resource script and output messages you want to send to the destination.

Options

-m message

Specifies a message. This option cannot be omitted. The maximum size of message is 511 bytes. (When syslog is specified as an output destination, the maximum size is 485 bytes.) The message exceeding the maximum size will not be shown.

You may use alphabets, numbers, and symbols. See below[8] for notes on them.

[8] **Notes on using symbols in the message:**
The symbols below must be enclosed in double quotes (" "):
& ' ( ) ~ | ; : * < > , .
(For example, if you specify "#" in the message, # is produced.)
The symbols below must have a backslash \ in the beginning:
\ ! " & ' ( ) ~ | ; : * < > , .
(For example, if you specify \\ in the message, \ is produced.)
The symbol that must be enclosed in double quotes (" ") and have a backslash \ in the beginning:
(For example, if you specify "\`" in the message, ` will is produced.)

- When there is a space in the **message**, it must be placed in enclosed in double quotes (" ").
- The symbol % cannot be used in the **message**.

--syslog

--alert

--mail

--trap
Specify the output destination from syslog, alert, mail, and trap. (Multiple destinations can be specified.)

This parameter can be omitted. The syslog and alert will be the output destinations when the parameter is omitted.

For more information on output destinations, see "Directory structure of EXPRESSCLUSTER" in "The system maintenance information" in the "Maintenance Guide".

-i eventID
Specify event ID. The maximum value of event ID is 10000.

This parameter can be omitted. The default value 1 is set when the parameter is omitted.

-l level
Select a level of alert output from ERR, WARN, or INFO. The icon on the alert logs of the Cluster WebUI is determined according to the level you select here.

This parameter can be omitted. The default value INFO is set when the parameter is omitted. For more information, see the online manual.

Return Value

0	Success
Other than 0	Failure

Notes
Run this command as the root user.

When mail is specified as the output destination, you need to make the settings to send mails by using the mail command.

Example of command execution
Example 1: When specifying only message (output destinations are syslog and alert):

When the following is written in the exec resource script, the **message** is produced in syslog and alert.

```
clplogcmd -m test1.
```

The following log is the log output in syslog:

Sep 1 14:00:00 server1 expresscls: <type: logcmd><event: 1> test1

Example 2: When specifying message, output destination, event ID, and level (output destination is mail):

When the following is written in the exec resource script, the message is sent to the mail address set in the **Cluster Properties**. For more information on the mail address settings, see "*Alert Service tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

```
clplogcmd -m test2 --mail -i 100 -l ERR
```

The following information is sent to the mail destination:

Message:test2
Type: logcmd
ID: 100

Host: server1
Date: 2004/09/01 14:00:00

Example 3: When specifying a message, output destination, event ID, and level (output destination is trap):

When the following is written in the exec resource script, the message is set to the SNMP trap destination set in **Cluster Properties** of the Cluster WebUI. For more information on the SNMP trap destination settings, see "*Alert Service tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

```
clplogcmd -m test3 --trap -i 200 -l ERR
```

The following information is sent to the SNMP trap destination:

Trap OID: clusterEventError
Attached data 1: clusterEventMessage = test3
Attached data 2: clusterEventID = 200
Attached data 3: clusterEventDateTime = 2011/08/01 09:00:00
Attached data 4: clusterEventServerName = server1
Attached data 5: clusterEventModuleName = logcmd

8.17 Controlling monitor resources (clpmonctrl command)

the clpmonctrl command controls the monitor resources.

Command line

clpmonctrl -s [-h <*hostname*>] [-m *resource_name ...*] [-w *wait_time*]
clpmonctrl -r [-h <*hostname*>] [-m *resource_name ...*] [-w *wait_time*]
clpmonctrl -c [-m *resource_name ...*]
clpmonctrl -v [-m *resource_name ...*]
clpmonctrl -e [-h <*hostname*>] -m *resource_name*
clpmonctrl -n [-h <*hostname*>] **[-m resource_name]**

Note:

The -c and -v options must be run on all servers that control monitoring because the command controls the monitor resources on a single server.
It is recommended to use the Cluster WebUI if you suspend or resume monitor resources on all the servers in a cluster.

Description

This command suspends and/or resumes the monitor resources, displays and/or resets the times counter of the recovery action, and enable and/or disable Dummy Failure.

Option

-s

Suspends monitoring

-r

Resumes monitoring

-c

Resets the times counter of the recovery action.

-v

Displays the times counter of the recovery action.

-e

Enables the Dummy Failure. Be sure to specify a monitor resource name with the -m option.

-n

Disables the Dummy Failure. When a monitor resource name is specified with the -m option, the function is disabled only for the resource. When the -m option is omitted, the function is disabled for all monitor resources.

-m resource_name ...

Specifies one or more monitor resources to be controlled.
This option can be omitted. All monitor resources are controlled when the option is omitted.

-w wait_time

Waits for control monitoring on a monitor resource basis (in seconds).
This option can be omitted. The default value 5 is set when the option is omitted.

-h

Makes a processing request to the server specified in hostname. Makes a processing request to the server on which this command runs (local server) if the -h option is omitted. The -c and -v options cannot specify the server.

Return Value

0	Normal termination
1	Privilege for execution is invalid
2	The option is invalid
3	Initialization error
4	The cluster configuration data is invalid
5	Monitor resource is not registered.
6	The specified monitor resource is invalid
10	The cluster is not activated
11	The cluster daemon is suspended
12	Waiting for cluster synchronization
90	Monitoring control wait time-out
128	Duplicated activation
200	Server connection error
201	Invalid status
202	Invalid server name
255	Other internal error

Example of command execution

Example 1: When suspending all monitor resources:

```
# clpmonctrl -s
Command succeeded.
```

Example 2: When resuming all monitor resources:

```
# clpmonctrl -r
Command succeeded.
```

Remarks

If you suspend a monitor resource that is already suspended or resume that is already resumed, this command terminates with error, without changing the status of the monitor resource.

Notes

Run this command as the root user.

Check the status of monitor resource by using the status display clpstat command or Cluster WebUI.

Before you run this command, use the clpstat command or Cluster WebUI to verify that the status of monitor resources is in either "Online" or "Suspend."

If the recovery action for the monitor resource is set as follows, "Final Action Count", which displayed by the -v option, means the number of times "Execute Script before Final Action" is executed.

- Execute Script before Final Action: Enable
- final action: No Operation

Error Messages

Message	Causes/Solution
Command succeeded.	The command ran successfully.
Log in as root.	You are not authorized to run this command. Log on as the root user.
Initialization error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Invalid cluster configuration data. Check the cluster configuration information.	The cluster configuration data is invalid. Check the cluster configuration data by using the Cluster WebUI.
Monitor resource is not registered.	The monitor resource is not registered.
Specified monitor resource is not registered. Check the cluster configuration information.	The specified monitor resource is not registered. Check the cluster configuration data by using the Cluster WebUI.
The cluster has been stopped. Check the active status of the cluster daemon by using the command such as ps command.	The cluster has been stopped. Check the activation status of the cluster daemon by using a command such as ps command.
The cluster has been suspended. The cluster daemon has been suspended. Check activation status of the cluster daemon by using a command such as the ps command.	The cluster daemon has been suspended. Check the activation status of the cluster daemon by using a command such as ps command.
Waiting for synchronization of the cluster. The cluster is waiting for synchronization. Wait for a while and try again.	Synchronization of the cluster is awaited. Try again after cluster synchronization is completed.

Continued on next page

Table 8.51 – continued from previous page

Message	Causes/Solution
Monitor %1 was unregistered, ignored. The specified monitor resources %1 is not registered, but continue processing. Check the cluster configuration data.	There is an unregistered monitor resource in the specified monitor resources but it is ignored and the process is continued Check the cluster configuration data by using the Cluster WebUI. %1: Monitor resource name
Monitor %1 denied control permission, ignored. but continue processing.	The specified monitor resources contain the monitor resource which cannot be controlled, but it does not affect the process. %1: Monitor resource name
This command is already run.	The command is already running. Check the running status by using a command such as ps command.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Could not connect to the server. Check if the cluster service is active.	Check if the cluster service has started.
Some invalid status. Check the status of cluster.	The status is invalid. Check the status of the cluster.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid server name in the cluster.

Monitor resource types that can be specified for the -m option

Type	Suspending/resuming monitoring	Resetting the times counter of the recovery action	Enabling/disabling
			Dummy Failure
arpw	n	y	n
bmcw	y	y	y
diskw	y	y	y
fipw	y	y	y
ipw	y	y	y
miiw	y	y	y
mtw	y	y	y
pidw	y	y	y
volmgrw	y	y	y
userw	y	y	n
vipw	n	y	n
vmw	y	y	n
ddnsw	n	y	n
mrw	y	y	n

Continued on next page

Table 8.52 – continued from previous page

Type	Suspending/resuming monitoring	Resetting the times counter of the recovery action	Enabling/disabling
genw	y	y	y
mdw	y	y	n
mdnw	y	y	n
hdw	y	y	n
hdnw	y	y	n
oraclew	y	y	y
osmw	y	y	y
db2w	y	y	y
psqlw	y	y	y
mysqlw	y	y	y
sybasew	y	y	y
odbcw	y	y	y
sqlserverw	y	y	y
sambaw	y	y	y
nfsw	y	y	y
httpw	y	y	y
ftpw	y	y	y
smtpw	y	y	y
pop3w	y	y	y
imap4w	y	y	y
tuxw	y	y	y
wlsw	y	y	y
wasw	y	y	y
otxw	y	y	y
jraw	y	y	y
sraw	y	y	y
psrw	y	y	y
psw	y	y	y
awsazw	y	y	y
awsdnsw	y	y	y
awseipw	y	y	y
awsvipw	y	y	y
azurednsw	y	y	y
azurelbw	y	y	y
azureppw	y	y	y
gclbw	y	y	y
gcvipw	y	y	y
oclbw	y	y	y
ocvipw	y	y	y

8.18 Controlling group resources (clprsc command)

the clprsc command controls group resources

Command line

clprsc -s *resource_name* [-h *hostname*] [-f] [--apito timeout]
clprsc -t *resource_name* [-h *hostname*] [-f] [--apito timeout]
clprsc -n *resource_name*
clprsc -v *resource_name*

Description

This command starts and stops group resources.

Option

-s

Starts group resources.

-t

Stops group resources.

-h

Requests processing to the server specified by the hostname.

When this option is skipped, request for processing is made to the following servers.

- When the group is offline, the command execution server (local server).
- When the group is online, the server where group is activated.

-f

When the group resource is online, all group resources that the specified group resource depends starts up.

When the group resource is offline, all group resources that the specified group resource depends stop.

-n

Displays the name of the server on which the group resource has been started.

--apito timeout

Specify the interval (internal communication timeout) to wait for the group resource start or stop in seconds. A value from 1 to 9999 can be specified.

If the --apito option is not specified, waiting for the group resource start or stop is performed according to the value set to the internal communication timeout of the cluster properties.

-v

Displays the failover counter of the group resource.

Return Value

0	success
Other than 0	failure

Example

Group resource configuration

```
# clpstat

========== CLUSTER STATUS ==========
 Cluster : cluster
 <server>
  *server1...................: Online
     lanhb1                  : Normal
     lanhb2                  : Normal
     pingnp1                 : Normal
   server2...................: Online
     lanhb1                  : Normal
     lanhb2                  : Normal
     pingnp1                 : Normal
 <group>
     ManagementGroup........: Online
      current                : server1
      ManagementIP           : Online
     failover1..............: Online
      current                : server1
      fip1                   : Online
      md1                    : Online
      exec1                  : Online
     failover2..............: Online
      current                : server2
      fip2                   : Online
      md2                    : Online
      exec2                  : Online
 <monitor>
     ipw1                    : Normal
     mdnw1                   : Normal
     mdnw2                   : Normal
     mdw1                    : Normal
     mdw2                    : Normal
====================================
```

Example 1: When stopping the resource (fip1) of the group (failover 1)

```
# clprsc -t fip1
Command succeeded.
```

```
#clpstat

========== CLUSTER STATUS =============
 <abbreviation>
 <group>
     ManagementGroup........: Online
      current                : server1
      ManagementIP           : Online
     failover1..............:Online
      current                : server1
      fip1                   : Offline
      md1                    : Online
      exec1                  : Online
     failover2..............: Online
      current                : server2
      fip2                   : Online
      md2                    : Online
```

(continues on next page)

(continued from previous page)

```
      exec2                : Online
  <abbreviation>
```

Example 2: When starting the resource (fip1) of the group(failover 1)

```
# clprsc -s fip1
Command succeeded.
```

```
# clpstat

========== CLUSTER STATUS ============
 <Abbreviation>
 <group>
      ManagementGroup.......: Online
       current              : server1
       ManagementIP         : Online
      failover1.............: Online
       current              : server1
       fip1                 : Online
       md1                  : Online
       exect1               : Online
      failover2.............: Online
       current              : server2
       fip2                 : Online
       md2                  : Online
       exec2                : Online
 <Abbreviation>
```

Notes

Run this command as a user with root privileges.

Check the status of the group resources by the status display or the Cluster WebUI.

When there is an active group resource in the group, the group resources that are offline cannot be started on another server.

Error Messages

Message	Causes/Solution
Log in as root.	Run this command as a user with root privileges.
Invalid cluster configuration data. Check the cluster configuration information.	The cluster construction information is not correct. Check the cluster construction information by Cluster WebUI.
Invalid option.	Specify a correct option.
Could not connect server. Check if the cluster service is active.	Check if the EXPRESSCLUSTER is activated.
Invalid server status. Check if the cluster service is active.	Check if the EXPRESSCLUSTER is activated.
Server is not active. Check if the cluster service is active.	Check if the EXPRESSCLUSTER is activated.
Invalid server name. Specify a valid server name in the cluster.	Specify a correct server name in the cluster.
Connection was lost. Check if there is a server where the cluster service is stopped in the cluster.	Check if there is any server with EXPRESSCLUSTER service stopped in the cluster,

Continued on next page

Table 8.53 – continued from previous page

Message	Causes/Solution
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set the longer timeout.	Timeout has occurred in internal communication in the EXPRESSCLUSTER. Set the internal communication timeout longer if this error occurs frequently.
The group resource is busy. Try again later.	Because the group resource is in the process of starting or stopping, wait for a while and try again.
An error occurred on group resource. Check the status of group resource.	Check the group resource status by using the Cluster WebUI or the clpstat command.
Could not start the group resource. Try it again after the other server is started, or after the Wait Synchronization time is timed out.	Wait until the other server starts or the wait time times out, and then start the group resources.
No operable group resource exists in the server.	Check there is a processable group resource on the specified server.
The group resource has already been started on the local server.	Check the group resource status by using the Cluster WebUI or clpstat command.
The group resource has already been started on the other server.	Check the group resource status by using the Cluster WebUI or clpstat command. Stop the group to start the group resources on the local server.
The group resource has already been stopped.	Check the group resource status by using the Cluster WebUI or clpstat command.
Failed to start group resource. Check the status of group resource.	Check the group resource status by using the Cluster WebUI or clpstat command.
Failed to stop resource. Check the status of group resource.	Check the group resource status by using the Cluster WebUI or clpstat command.
Depended resource is not offline. Check the status of resource.	Because the status of the depended group resource is not offline, the group resource cannot be stopped. Stop the depended group resource or specify the -f option.
Depending resource is not online. Check the status of resource.	Because the status of the depended group is not online, the group resource cannot be started. Start the depended group resource or specify the -f option.
Invalid group resource name. Specify a valid group resource name in the cluster.	The group resource is not registered.
Server is not in a condition to start resource or any critical monitor error is detected.	Check the group resource status by using the Cluster WebUI or clpstat command. An error is detected in a critical monitor on the server on which an attempt to start a group resource was made.
Internal error. Check if memory or OS resources are sufficient.	Memory or OS resources may be insufficient. Check them.

8.19 Controlling reboot count (clpregctrl command)

the clpregctrl command controls reboot count limitation.

Command line

clpregctrl --get
clpregctrl -g
clpregctrl --clear -t **type** -r **registry**
clpregctrl -c -t **type** -r **registry**

Note: This command must be run on all servers that control the reboot count limitation because the command controls the reboot count limitation on a single server.

Description

This command displays and/or initializes reboot count on a single server.

Option

-g, --get
Displays reboot count information.

-c, --clear
Initializes reboot count.

-t type
Specifies the type to initialize the reboot count. The type that can be specified is *rc* or *rm*.

-r registry
Specifies the registry name. The registry name that can be specified is haltcount.

Return Value

0	Normal termination
1	Privilege for execution is invalid
2	Duplicated activation
3	Option is invalid
4	The cluster configuration data is invalid
10 to 17	Internal error
20 to 22	Obtaining reboot count information has failed.
90	Allocating memory has failed.
91	Changing the work directory as failed.

Example of command execution

Display of reboot count information

```
# clpregctrl -g
```

```
*****************************

-------------------------
  type        : rc
```

(continues on next page)

(continued from previous page)

```
   registry   : haltcount
   comment    : halt count
   kind       : int
   value      : 0
   default    : 0

-------------------------
   type       : rm
   registry   : haltcount
   comment    : halt count
   kind       : int
   value      : 3
   default    : 0

*****************************
Command succeeded.(code:0)
```

The reboot count is initialized in the following examples.

Run this command on server2 when you want to control the reboot count of server2.

Example1: When initializing the count of reboots caused by group resource error:

```
# clpregctrl -c -t rc -r haltcount
Command succeeded.(code:0)
#
```

Example2: When initializing the count of reboots caused by monitor resource error:

```
# clpregctrl -c -t rm -r haltcount
Command succeeded.(code:0)
#
```

Remarks

For information on the reboot count limit, see "*Attributes common to group resources*" "*Reboot count limit*" in "3. *Group resource details*" in this guide.

Notes

Run this command as the root user.

Error Messages

Message	Causes/Solution
Command succeeded.	The command ran successfully.
Log in as root.	You are not authorized to run this command. Log on as the root user.
The command is already executed. Check the execution state by using the "ps" command or some other command.	The command is already running. Check the running status by using a command such as ps command.
Invalid option.	Specify a valid option.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.20 Turning off warning light (clplamp command)

The clplamp command turns the warning light off.

Command line

clplamp -h *hostname*

Description

Turns the warning light of the specified server off.

If the reproduction of audio file is set, audio file reproduction is stopped.

Option

-h hostname

Specify a server whose warning light you want to turn off.

Return Value

0	Normal termination
Other than 0	Abnormal termination

Example

Example 1: When turning off the warning light and audio alert for server1

```
# clplamp -h server1
Command succeeded
```

Notes

This command should be performed by the user with root privilege.

8.21 Controlling CPU frequency (clpcpufreq command)

The clpcpufreq command controls CPU frequency.

Command line:

clpcpufreq --high [-h *hostname*]
clpcpufreq --low [-h *hostname*]
clpcpufreq -i [-h *hostname*]
clpcpufreq -s [-h *hostname*]

Description

This command enables/disables power-saving mode by CPU frequency control.

Option

--high

Sets CPU frequency to highest.

--low

Sets CPU frequency to lowest.

-i
Switch to automatic control by cluster.

-s
Displays the current CPU frequency level.

- high: Frequency is highest
- low: Frequency is lowered and it is in power-saving mode

-h hostname
Requests the server specified in hostname for processing.

If this is omitted, it requests the local server for processing.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Example

```
# clpcpufreq -s
performance
Command succeeded.
```

```
# clpcpufreq --high
Command succeeded.
```

```
# clpcpufreq --low -h server1
Command succeeded.
```

```
# clpcpufreq -i
Command succeeded
```

Remark
If the driver for CPU frequency control is not loaded, an error occurs.

If the Use CPU Frequency Control checkbox is not selected in the power saving settings in cluster properties, this command results in error.

Notes
This command must be executed by a user with the root privilege.

When you use CPU frequency control, it is required that frequency is changeable in the BIOS settings, and that the CPU supports frequency control by Windows OS power management function.

Error Messages

Message	Cause/Solution
Log in as root.	Log in as the root user.
This command is already run.	This command has already been run.
Invalid option.	Specify a valid option.

Continued on next page

Table 8.55 – continued from previous page

Message	Cause/Solution
Invalid mode. Check if --high or --low or -i or -s option is specified.	Check if either of the --high, --low, -I or -s option is specified.
Failed to initialize the xml library. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to load the configuration file. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Failed to load the all.pol file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to load the cpufreq.pol file. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the install path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to get the cpufreq path. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server RPM.
Failed to initialize the apicl library. Reinstall the RPM.	Check to see if the memory or OS resource is sufficient.
Failed to change CPU frequency settings. Check the BIOS settings and the OS settings. Check if the cluster is started. Check if the setting is configured so that CPU frequency control is used.	Check the BIOS settings and the OS settings. Check if the cluster service is started. Check if the setting is configured so that CPU frequency control is used.

Continued on next page

Table 8.55 – continued from previous page

Message	Cause/Solution
Failed to change CPU frequency settings. Check the BIOS settings and the OS settings. Check if the cluster is started. Check if the setting is configured so that CPU frequency control is used.	Check the BIOS settings and the OS settings. Check if the cluster service is started. Check if the setting is configured so that CPU frequency control is used.
Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.

8.22 Controlling chassis identify lamp (clpledctrl command)

The clpledctrl command controls the chassis identify function.

Command line

clpledctrl -d [-h *hostname*] [-a] [-w *timeout*]
clpledctrl -i [-h *hostname*] [-a] [-w *timeout*]

Description

This command disables/enables chassis identify function.

Option

-d
Disables the chassis identify function.

-i
Enables the chassis identify function.

-h `hostname`
Specifies the name of the server which enables/disables the chassis identify function. Specify -a to omit this.

-a
All servers in the cluster are the targets.

The -a option can be omitted. If so, specify hostname.

-w `timeout`
Specifies the timeout value of the command by the second.

If the -w option is not specified, it waits for 30 seconds.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Notes

This command must be executed by a user with the root privilege.

Execute this command in the server operating normally in the same cluster as the one which the target server belongs to.

If you disable the chassis identify function by this command, it is canceled when the cluster is restarted or when the target server recovers the normal status.

Examples

Example 1: When disabling (i.e. turn off the lamp which is turned on) the chassis identify function in server1 (specify the command timeout as 60 seconds)

```
# clpledctrl -d server1 -w 60
```

Example 2: When disabling chassis identify in all servers in the cluster

```
# clpledctrl -d -a
```

Example 3: When enabling the chassis identify function in server1 where the function was disabled

```
# clpledctrl -i server1
```

The result of command execution is displayed as follows:

Detail of the processing Server name: Result (Cause if failed)

Error messages

Message	Cause/solution
Log in as root.	Log in as the root user.
Invalid option.	The command line option is invalid. Specify the correct option.
Could not connect to the data transfer server. Check if the server has started up.	Check if the server has started up.
Could not connect to all data transfer servers. Check if the servers have started up.	Check the all servers in the cluster have started up.
Command timeout.	The cause may be heavy load on OS and so on. Check this.
Chassis identify is not setting or active at all servers.	Chassis identify is disabled or not used.
Failed to obtain the list of nodes. Specify a valid server name in the cluster.	Specify a valid server name in the cluster.
All servers are busy. Check if this command is already run.	This command may be run already. Check it.
Internal error. Check if memory or OS resource is sufficient.	Check if the memory or OS resource is sufficient.

8.23 Processing inter-cluster linkage (clptrnreq command)

The clptrnreq command requests a server to execute a process.

Command line

clptrnreq -t *request_code* -h IP [-r *resource_name*] [-s *script_file*] [-w *timeout*]

Description

The command issues the request to execute specified process to the server in another cluster.

Option

-t request_code

Specifies the request code of the process to be executed.
The following request codes can be specified:

GRP_FAILOVER Group failover
EXEC_SCRIPT Execute script

-h IP

Specifies the server to issue the request to execute the process with IP address. You can specify more than one server by separating by commas.

When you specify group failover for request code, specify the IP addresses of all the servers in the cluster.

-r resource_name

Specifies the resource name which belongs to the target group for the request for process when GRP_FAILOVER is specified for request code.

If GRP_FAILOVER is specified, -r cannot be omitted.

-s script_file

Specifies the file name of the script to be executed (e.g. batch file or executable file) when EXEC_SCRIPT is specified for request code.

The script needs to be created in the work\trnreq folder in the folder where EXPRESSCLUSTER is installed in each server specified with -h.de.

If EXEC_SCRIPT is specified, -s cannot be omitted.

-w timeout

Specifies the timeout value of the command by the second.

If the -w option is not specified, the command waits 30 seconds.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Notes

This command must be executed by a user with the root privilege.

Examples

Example 1: When performing a failover on the group having the exec1 resource of another cluster

```
# clptrnreq -t GRP_FAILOVER -h 10.0.0.1,10.0.0.2 -r exec1
Command succeeded.
```

Example 2: When executing the scrpit1.bat script by the server with IP address 10.0.0.1

```
# clptrnreq -t EXEC_SCRIPT -h 10.0.0.1 -s script1.bat
Command Succeeded.
```

Error messages

Message	Cause/solution
Log in as root.	Log in as the root user.
Invalid option.	The command line option is invalid. Specify the correct option.
Could not connect to the data transfer server. Check if the server has started up.	Check if the server has started up.
Could not connect to all data transfer servers. Check if the servers have started up.	Check if all the servers in the cluster have started up.
Command timeout.	The cause may be heavy load on OS and so on. Check this.
All servers are busy. Check if this command is already run.	This command may be run already. Check it.
GRP_FAILOVER %s : Group that specified resource(%s) belongs to is offline.	Failover process is not performed because the group to which the specified resource belongs is not started.
EXEC_SCRIPT %s : Specified script(%s) does not exist.	The specified script does not exist. Check it.
EXEC_SCRIPT %s : Specified script(%s) is not executable.	The specified script could not be executed. Check that execution is permitted.
%s %s : This server is not permitted to execute clptrnreq.	The server that executed the command does not have permission. Check that the server is registered to the connection restriction IP list of Cluster WebUI.
GRP_FAILOVER %s : Specified resource(%s) does not exist.	The specified resource does not exist. Check it.
%s %s : %s failed in execute..	Failed to execute the specified action.
Internal error. Check if memory or OS resource is sufficient.	Check if the memory or OS resource is sufficient.

8.24 Requesting processing to cluster servers (clprexec command)

This command requests a server to execute a process.

Command line

clprexec --failover ([*group_name*] | [-r *resource_name*]) -h *IP* [-w *timeout*] [-p *port_number*] [-o *logfile_path*]

clprexec --script *script_file* -h *IP* [-p *port_number*] [-w *timeout*] [-o *logfile_path*]

clprexec --notice ([*mrw_name*] | [-k *category*[.*keyword*]]) -h *IP* [-p *port_number*] [-w *timeout*] [-o *logfile_path*]

clprexec --clear ([*mrw_name*] | [-k *category*[.*keyword*]]) -h *IP* [-p *port_number*] [-w *timeout*] [-o *logfile_path*]

Description

This command is an expansion of the existing clptrnreq command and has additional functions such as issuing a processing request (error message) from the external monitor to the EXPRESSCLUSTER server.

Option

--failover

Requests group failover. Specify a group name for *group_name*.

When not specifying the group name, specify the name of a resource that belongs to the group by using the -r option.

--script script_name

Requests script execution.

For *script_name*, specify the file name of the script to execute (such as a shell script or executable file).

The script must be created in the work/rexec directory, which is in the directory where EXPRESSCLUSTER is installed, on each server specified using -h.

--notice

Sends an error message to the EXPRESSCLUSTER server.

Specify a message receive monitor resource name for *mrw_name*.

When not specifying the monitor resource name, specify the category and keyword of the message receive monitor resource by using the -k option.

--clear

Requests changing the status of the message receive monitor resource from "Abnormal" to "Normal."

Specify a message receive monitor resource name for *mrw_name*.

When not specifying the monitor resource name, specify the category and keyword of the message receive monitor resource by using the -k option.

-h IP Address

Specify the IP addresses of EXPRESSCLUSTER servers that receive the processing request.

Up to 32 IP addresses can be specified by separating them with commas.

* If this option is omitted, the processing request is issued to the local server.

-r resource_name

Specify the name of a resource that belongs to the target group for the processing request when the --failover option is specified.

-k `category[.keyword]`
For *category*, specify the category specified for the message receive monitor when the --notice or --clear option is specified.

To specify the keyword of the message receive monitor resource, specify them by separating them with dot after *category*.

-p `port_number`
Specify the port number.

For *port_number*, specify the data transfer port number specified for the server that receives the processing request.

The default value, 29002, is used if this option is omitted.

-o `logfile_path`
For *logfile_path*, specify the file path along which the detailed log of this command is output.

The file contains the log of one command execution.

* If this option is not specified on a server where EXPRESSCLUSTER is not installed, the log is always output to the standard output.

-w `timeout`
Specify the command timeout time. The default, 180 seconds, is used if this option is not specified.

A value from 5 to MAXINT can be specified.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Notes

When issuing error messages by using the clprexec command, the message receive monitor resources for which an action to take in EXPRESSCLUSTER server when an error occurs is specified must be registered and started.

The server that has the IP address specified for the -h option must satisfy the following conditions:

- EXPRESSCLUSTER X3.0 or later must be installed.
- EXPRESSCLUSTER must be running.
  (When an option other than --script is used)
- mrw must be set up and running.
  (When the --notice or --clear option is used)

When using the **Controlling connection by using client IP address function, add the IP address of the device in which the clprexec command is executed to the IP Addresses of the Accessible Clients list.**

For details of the Controlling connection by using client IP address function, see "*WebManager tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

Examples

Example 1: This example shows how to issue a request to fail over the group failover1 to EXPRESSCLUSTER server 1 (10.0.0.1):

```
# clprexec --failover failover1 -h 10.0.0.1 -p 29002
```

Example 2: This example shows how to issue a request to fail over the group to which the group resource (exec1) belongs to EXPRESSCLUSTER server 1 (10.0.0.1):

```
# clprexec --failover -r exec1 -h 10.0.0.1
```

Example 3: This example shows how to issue a request to execute the script (script1.sh) on EXPRESSCLUSTER server 1 (10.0.0.1):

```
# clprexec --script script1.sh -h 10.0.0.1
```

Example 4: This example shows how to issue an error message to EXPRESSCLUSTER server 1 (10.0.0.1):

*mrw1 set, category: earthquake, keyword: scale3

- This example shows how to specify a message receive monitor resource name:

```
# clprexec --notice mrw1 -h 10.0.0.1 -w 30 -p /tmp/clprexec/ lprexec.
↪log
```

- This example shows how to specify the category and keyword specified for the message receive monitor resource:

```
# clprexec --notice -k earthquake.scale3 -h 10.0.0.1 -w 30 -p /tmp/
↪clprexec/clprexec.log
```

Example 5: This example shows how to issue a request to change the monitor status of mrw1 to EXPRESSCLUSTER server 1 (10.0.0.1):

*mrw1 set, category: earthquake, keyword: scale3

- This example shows how to specify a message receive monitor resource name:

```
# clprexec --clear mrw1 -h 10.0.0.1
```

- This example shows how to specify the category and keyword specified for the message receive monitor resource:

```
# clprexec --clear -k earthquake.scale3 -h 10.0.0.1
```

Error messages

Message	Cause/solution
rexec_ver:%s	-
%s %s : %s succeeded.	-
%s %s : %s will be executed from now.	Check the processing result on the server that received the request.
%s %s : Group Failover did not execute because Group(%s) is offline.	-
%s %s : Group migration did not execute because Group(%s) is offline.	-
Invalid option.	Check the command argument.
Could not connect to the data transfer servers. Check if the servers have started up.	Check whether the specified IP address is correct and whether the server that has the IP address is running.
Command timeout.	Check whether the processing is complete on the server that has the specified IP address.
All servers are busy.Check if this command is already run.	This command might already be running. Check whether this is so.

Continued on next page

Table 8.58 – continued from previous page

Message	Cause/solution
%s %s : This server is not permitted to execute clprexec.	Check whether the IP address of the server that executes the command is registered in the list of client IP addresses that are not allowed to connect to the Cluster WebUI.
%s %s : Specified monitor resource(%s) does not exist.	Check the command argument.
%s %s : Specified resource(Category:%s, Keyword:%s) does not exist.	Check the command argument.
%s failed in execute.	Check the status of the EXPRESSCLUSTER server that received the request.

8.25 Changing BMC information (clpbmccnf command)

The clpbmccnf command changes the information on BMC user name and password.

Command line

clpbmccnf [-u *username*] [-p *password*]

Description

This command changes the user name/password for the LAN access of the baseboard management controller (BMC) which EXPRESSCLUSTER uses for chassis identify or forced stop.

Option

-u username

Specifies the user name for BMC LAN access used by EXPRESSCLUSTER. A user name with root privilege needs to be specified.

The -u option can be omitted. Upon omission, when the -p option is specified, the value currently set for user name is used. If there is no option specified, it is configured interactively.

-p password

Specifies the password for BMC LAN access used by EXPRESSCLUSTER. The -p option can be omitted.

Upon omission, when the -u option is specified, the value currently set for password is used. If there is no option specified, it is configured interactively.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Notes

This command must be executed by a user with root privilege.

Execute this command when the cluster is in normal status.

BMC information update by this command is enabled when the cluster is started/resumed next time.

This command does not change the BMC settings. Use a tool attached with the server or other tools in conformity with IPMI standard to check or change the BMC account settings.

Examples

When you changed the IPMI account password of the BMC in server1 to mypassword, execute the following on server1:

```
# clpbmccnf -p mypassword
```

Alternatively, enter the data interactively as follows:

```
# clpbmccnf
New user name: <- If there is no change, press Return to skip
New password: *********
Retype new password: *********
Cluster configuration updated successfully.
```

Error messages

Message	Cause/solution
Log in as root	Log in as the root user.
Invalid option.	The command line option is invalid. Specify the correct option.
Failed to download the cluster configuration data. Check if the cluster status is normal.	Downloading the cluster configuration data has been failed. Check if the cluster status is normal.
Failed to upload the cluster configuration data. Check if the cluster status is normal.	Uploading the cluster configuration data has been failed. Check if the cluster status is normal.
Invalid configuration file. Create valid cluster configuration data.	The cluster configuration data is invalid. Check the cluster configuration data by using the Cluster WebUI.
Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.

8.26 Controlling cluster activation synchronization wait processing (clpbwctrl command)

The clpbwctrl command controls the cluster activation synchronization wait processing.

Command line

clpbwctrl -c
clpbwctrl -h

Description

This command skips the cluster activation synchronization wait time that occurs if the server is started when the cluster services for all the servers in the cluster are stopped.

Option

-c, --cancel
Cancels the cluster activation synchronization wait processing.

-h, --help
Displays the usage.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Notes

This command must be executed by a user with root privileges.

Examples

This example shows how to cancel the cluster activation synchronization wait processing:

```
# clpbwctrl -c
Command succeeded.
```

Error messages

Message	Cause/solution
Log in as root	Log in as a root user.
Invalid option.	The command option is invalid. Specify correct option.
Cluster service has already been started.	The cluster has already been started. It is not in startup synchronization waiting status.
The cluster is not waiting for synchronization.	The cluster is not in startup synchronization waiting processing. The cluster service stop or other causes are possible.
Command Timeout.	Command execution timeout.
Internal error.	Internal error occurred.

8.27 Estimating the amount of resource usage (clpprer command)

Estimates the future value from the transition of the resource use amount data listed in the input file, and then outputs the estimate data to a file. Also, the result of threshold judgment on the estimate data can be confirmed.

Command line

clpprer -i *inputfile* -o *outputfile* [-p *number*] [-t *number* [-l]]

Description

Estimates the future value from the tendency of the given resource use amount data.

Option

-i inputfile
Specifies the resource data for which a future value is to be obtained.

-o outputfile
Specifies the name of the file to which the estimate result is output.

-p number
Specifies the number of estimate data items.

If omitted, 30 items of estimate data are obtained.

-t number
Specifies the threshold to be compared with the estimate data.

-l
Valid only when the threshold is set with the -t option. Judges the status to be an error when the data value is less than the threshold.

Return Value

0	Normal end without threshold judgment
1	Error occurrence
2	As a result of threshold judgment, the input data is determined to have exceeded the threshold.
3	As a result of threshold judgment, the estimate data is determined to have exceeded the threshold.
4	As a result of threshold judgment, the data is determined to have not exceeded the threshold.
5	If the number of data items to be analyzed is less than the recommended number of data items to be analyzed (120), the input data is determined to have exceeded the threshold as a result of threshold judgment.
6	If the number of data items to be analyzed is less than the recommended number of data items to be analyzed (120), the estimate data is determined to have exceeded the threshold as a result of threshold judgment.
7	If the number of data items to be analyzed is less than the recommended number of data items to be analyzed (120), the data is determined to have not exceeded the threshold as a result of threshold judgment.

Notes

This command can be used only when the license for the system monitor resource (System Resource Agent) is registered. (If the license is registered, you do not have to set up the system monitor resource when configuring a cluster.)

The maximum number of input data items of the resource data file specified with the -i option is 500. A certain number of input data items are required to estimate the amount of resource usage. However, if the number of input data items is large, it takes a considerable amount of time to perform the analysis. So, it is recommended that the number of input data items be restricted to about 120. Moreover, the maximum number of output data items that can be specified in option -p is 500.

If the time data for the input file is not arranged in ascending order, the estimate will not be appropriate. In the input file, therefore, set the time data arranged in ascending order.

Input file

The input file format is explained below. Prepare an input file which contains the resource usage data for which to obtain an estimate, in the following format.

The input file format is CSV. One piece of data is coded in the form of *date and time*, *numeric value*.

Moreover, the data and time format is *YYYY/MM/DD hh:mm:ss*.

File example

```
2012/06/14 10:00:00,10.0
2012/06/14 10:01:00,10.5
2012/06/14 10:02:00,11.0
```

Examples

The estimation of the future value is explained using a simple example.

When an error is detected in the input data:

If the latest value of the input data exceeds the threshold, an error is assumed and a return value of 2 is returned. If the number of input data items is less than the recommended value (=120), a return value of 5 is returned.

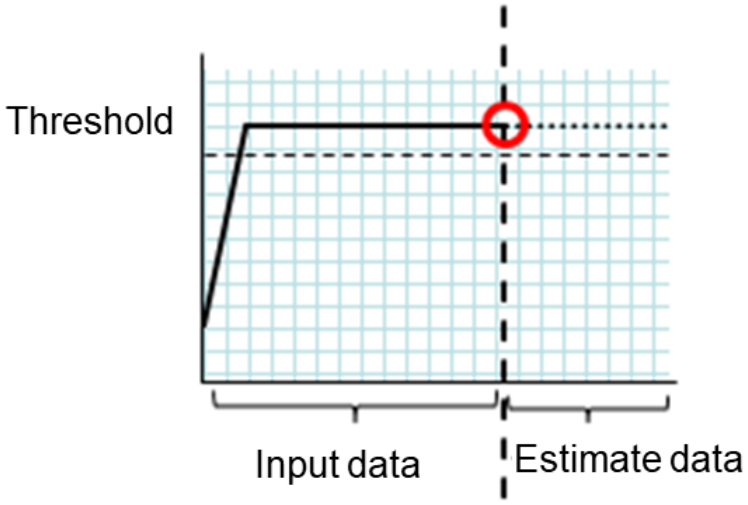


Figure: Error detection in the input data

When an error is detected in the estimate data:

If the estimate data exceeds the threshold, an error is assumed and a return value of 3 is returned. If the number of input data items is less than the recommended value (=120), a return value of 6 is returned.

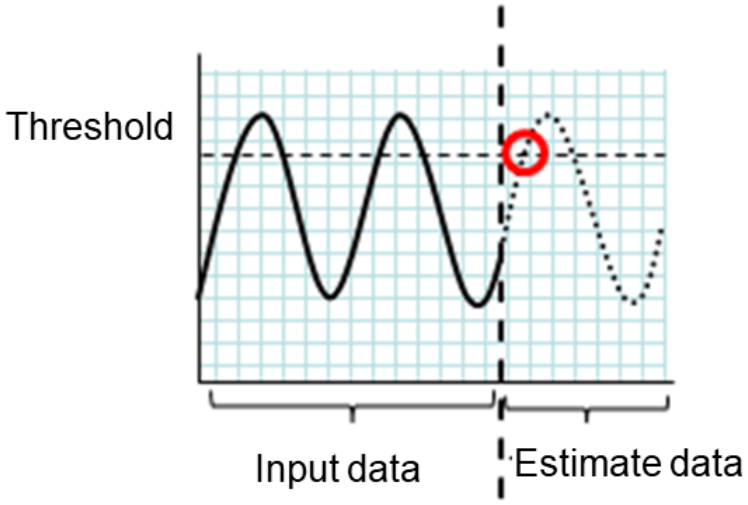


Figure: Error detection in the estimate data

When no threshold error is detected:

If neither the input data nor the estimate data exceeds the threshold, a return value of 4 is returned. If the number of input data items is less than the recommended value (=120), a return value of 7 is returned.

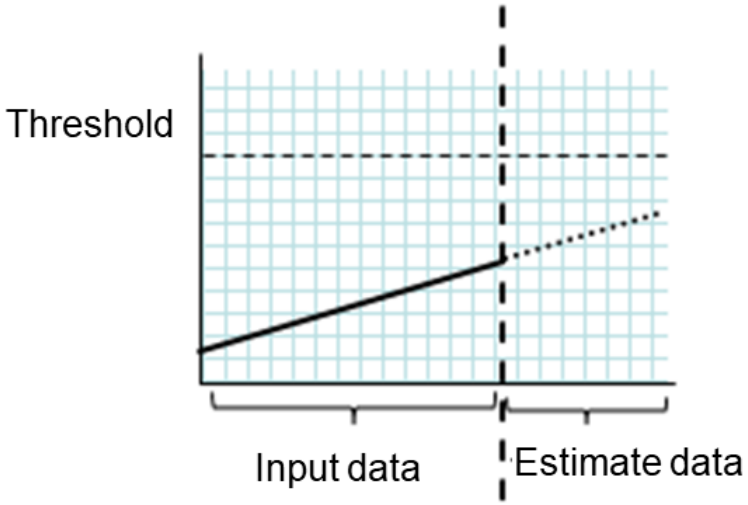


Figure: When no threshold error is detected

When the -l option is used:

If the -l option is used, an error is assumed when the data is less than the threshold.

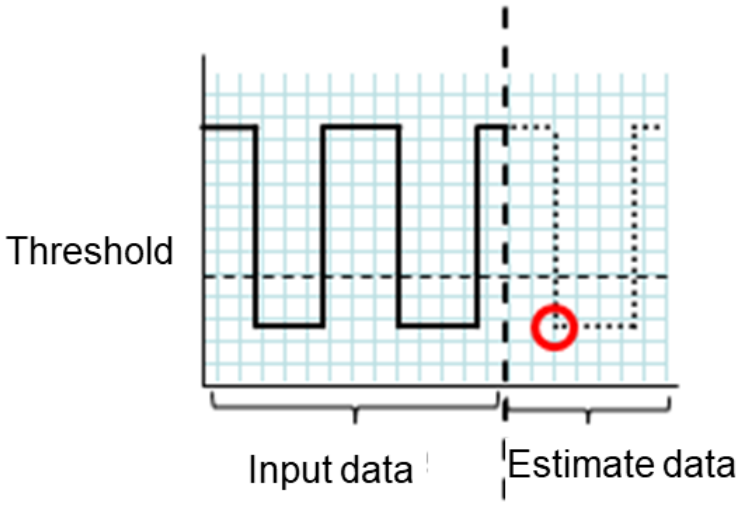


Figure: Use of the -l option

Examples

Prepare a file which contains data in the specified format, and then execute the clpprer command. The estimate result can be confirmed as the output file.

Input file: test.csv

```
2012/06/14 10:00:00,10.0
2012/06/14 10:01:00,10.5
2012/06/14 10:02:00,11.0
```

```
# clpprer -i test.csv -o result.csv
```

Output result: result.csv

```
2012/06/14 10:03:00,11.5
2012/06/14 10:04:00,12.0
2012/06/14 10:05:00,12.5
2012/06/14 10:06:00,13.0
2012/06/14 10:07:00,13.5

:
```

Also, by specifying a threshold as an option, you can confirm the threshold judgment result for the estimate at the command prompt.

```
# clpprer -i test.csv -o result.csv -t 12.5
```

Execution result

Detect over threshold. datetime = 2012/06/14 10:06:00, data = 13.00, threshold = 12.5

Error messages

Message	Causes/Solution
Normal state.	As a result of threshold judgment, no data exceeding the threshold is detected.
Detect over threshold. datetime = %s, data = %s, threshold = %s	As a result of threshold judgment, data exceeding the threshold is detected.
Detect under threshold. datetime = %s, data = %s, threshold = %s	As a result of threshold judgment with the -l option, data less than the threshold is detected.
License is nothing.	The license for the valid System Resource Agent is not registered. Check to see the license.
Inputfile is none.	The specified input data file does not exist.
Inputfile length error.	The path for the specified input data file is too long. Specify no more than 1023 bytes.
Output directory does not exist.	The directory specified with the output file does not exist. Check whether the specified directory exists.
Outputfile length error.	The path for the specified output file is too long. Specify no more than 1023 bytes.
Invalid number of -p.	The value specified in the -p option is invalid.
Invalid number of -t.	The value specified in the -t option is invalid.
Not analyze under threshold(not set -t) .	The -t option is not specified. When using the -I option, also specify the -t option.
File open error [%s]. errno = %s	The file failed to open. The amount of memory or OS resources may be insufficient. Check for any insufficiency.
Inputfile is invalid. cols = %s	The number of input data items is not correct. Set the number of input data items to 2 or more.
Inputfile is invalid. rows = %s	The input data format is incorrect. One line needs to be divided into two rows.
Invalid date format. [expected YYYY/MM/DD HH:MM:SS]	The date of the input data is not of the correct format. Check to see the data.
Invalid date format. Not sorted in ascending order.	Input data is not arranged in ascending order of date and time. Check the data.
File read error.	An invalid value is set in the input data. Check the data.

Continued on next page

Table 8.61 – continued from previous page

Message	Causes/Solution
Too large number of data [%s]. Max number of data is %s.	The number of input data items exceeds the maximum value (500). Reduce the number of data items.
Input number of data is smaller than recommendable number.	The number of input data items is less than the recommended number of data items to be analyzed (120). * Data is analyzed even if the recommended number of data items to be analyzed is small.
Internal error.	An internal error has occurred.

8.28 Checking the process health (clphealthchk command)

Checks the process health.

Command line

clphealthchk [-t pm | -t rc | -t rm | -t nm | -h]

Note: This command must be run on the server whose process health is to be checked because this command checks the process health of a single server.

Description

This command checks the process health of a single server.

Option

None

Checks the health of all of pm, rc, rm, and nm.

-t <process>

process

pm Checks the health of pm.

rc Checks the health of rc.

rm Checks the health of rm.

nm Checks the health of nm.

-h

Displays the usage.

Return Value

0	Normal termination
1	Privilege for execution is invalid
2	Duplicated activation
3	Initialization error
4	The option is invalid
10	The process stall monitoring function has not been enabled.
11	The cluster is not activated (waiting for the cluster to start or the cluster has been stopped.)
12	The cluster daemon is suspended
100	There is a process whose health information has not been updated within a certain period. If the -t option is specified, the health information of the specified process is not updated within a certain period.
255	Other internal error

Examples

Example 1: When the processes are healthy

```
# clphealthchk
pm OK
rc NG
rm OK
nm OK
```

Example 2: When **clprc is stalled**

```
# clphealthchk
pm OK
rc NG
rm OK
nm OK
```

```
# clphealthchk -t rc
rc NG
```

Example 3: When the cluster has been stopped

```
# clphealthchk
The cluster has been stopped
```

Remarks

If the cluster has been stopped or suspended, the process is also stopped.

Notes

Run this command as the root user.

Error Messages

Message	Cause/Solution
Log in as root.	You are not authorized to run this command. Log on as the root user.
Initialization error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.
Invalid option.	Specify a valid option.
The function of process stall monitor is disabled.	The process stall monitoring function has not been enabled.

Continued on next page

Table 8.62 – continued from previous page

Message	Cause/Solution
The cluster has been stopped.	The cluster has been stopped.
The cluster has been suspended.	The cluster has been suspended.
This command is already run.	The command has already been started. Check the running status by using a command such as ps command.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

8.29 Controlling the rest point of DB2 (clpdb2still command)

Controls the rest point of DB2.

Command line

clpdb2still -d *databasename* -u *username* -s
clpdb2still -d *databasename* -u *username* -r

Description

Controls the securing/release of the rest point of DB2.

Option

-d databasename
Specifies the name of the target database for the rest point control.

-u username
Specifies the name of a user who executes the rest point control.

-s
Secures the rest point.

-r
Releases the rest point.

Return Value

0	Normal completion
2	Invalid command option
5	Failed to secure the rest point.
6	Failed to release the rest point.

Examples

```
# clpdb2still -d sample -u db2inst1 -s

Database Connection Information

Database server = DB2/LINUXX8664 11.1.0
SQL authorization ID = DB2INST1
Local database alias = SAMPLE
```

(continues on next page)

(continued from previous page)

```
DB20000I The SET WRITE command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL DISCONNECT command completed successfully.
```

```
# clpdb2still -d sample -u db2inst1 -r

Database Connection Information

Database server = DB2/LINUXX8664 11.1.0
SQL authorization ID = DB2INST1
Local database alias = SAMPLE

DB20000I The SET WRITE command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL DISCONNECT command completed successfully.
```

Notes

Run this command as the root user.

A user specified in the -u option needs to have the privilege to run the SET WRITE command of DB2.

Error Messages

Message	Cause/Solution
invalid database name	The database name is invalid. Check the database name.
invalid user name	The user name is invalid. Check the user name.
missing database name	No database name is specified. Specify a database name.
missing user name	No user name is specified. Specify a user name.
missing operation '-s' or '-r'	Neither the securing nor release of the rest point is specified. Specify either the securing or release of the rest point.

Continued on next page

Table 8.63 – continued from previous page

Message	Cause/Solution
suspend command return code = n	Failed to secure the rest point. If an error message of the su command is output at the last minute, check the user name and password. Additionally, if an error message of the db2 command is output, take appropriate actions based on the error message.
resume command return code = n	Failed to release the rest point. If an error message of the su command is output at the last minute, check the user name and password. Additionally, if an error message of the db2 command is output, take appropriate actions based on the error message.

8.30 Controlling the rest point of MySQL (clpmysqlstill command)

Controls the rest point of MySQL.

Command line.

clpmysqlstill -d *databasename* [-u *username*] -s
clmypsqlstill -d *databasename* -r

Description

Controls the securing/release of the rest point of MySQL.

Option

-d databasename
Specifies the name of the target database for rest point control.

-u username
Specifies the name of the database user who executes rest point control. This option can be specified only when the -s option is specified. If it is omitted, root is automatically set as a default user.

-s
Secures the rest point.

-r
Releases the rest point.

Return Value

0	Normal completion
2	Invalid command option
3	DB connection error
4	Authentication error for the user specified in the -u option
5	Failed to secure the rest point.
6	Failed to release the rest point.
99	Internal error

Examples

```
# clpmysqlstill -d mysql -u root -s
Command succeeded.
```

```
# clpmysqlstill -d mysql -r
Command succeeded.
```

Notes

Run this command as the root user.

Configure a directory, where libmysqlclient.so client library of MySQL exists, to LD_LIBRARY_PATH, an environment variable.

Preliminarily configure the password of a user specified in the -u option, in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the password. Put a colon ":" at the end of the row.

"*User name*:*Password*:"

Example of file path: /opt/nec/clusterpro/etc/stillpoint.conf

Example of password setting: root:password:

A user specified in the -u option needs to have privileges to execute FLUSH TABLES WITH READ LOCK statement of MySQL.

If the rest point has been secured by running the command for securing the rest point with the -s option, the control is not returned while the command remains resident. By running the command for releasing the rest point with the -r option at a different process, the resident command for securing the rest point finishes and the control is returned.

Error Messages

Message	Cause/Solution
Invalid option.	Invalid command option. Check the command option.
Cannot connect to database.	Failed to connect to the database. Check the name and the status of the database.

Continued on next page

Table 8.64 – continued from previous page

Message	Cause/Solution
Username or password is not correct.	User authentication failed. Check your user name and password.
Suspend database failed.	Failed to secure the rest point. Check the user privileges and the database settings.
Resume database failed.	Failed to release the rest point. Check the user privileges and the database settings.
Internal error.	An internal error has occurred.

8.31 Controlling the rest point of Oracle (clporclstill command)

Controls the rest point of Oracle.

Command line

clporclstill -d *connectionstring* [-u *username*] -s
clporclstill -d connectionstring -r

Description

Controls the securing/release of the rest point of Oracle.

Option

-d `connectionstring`
Specifies the connection string for the target database for rest point control.

-u `username`
Specifies the name of a database user who executes rest point control. This option can be specified only when the -s option is specified. If it is omitted, OS authentication is used.

-s
Secures the rest point.

-r
Releases the rest point.

Return Value

0	Normal completion
2	Invalid command option
3	DB connection error
4	User authentication error
5	Failed to secure the rest point.
6	Failed to release the rest point.
99	Internal error

Examples

```
# clporclstill -d orcl -u oracle -s
Command succeeded.
```

```
# clporclstill -d orcl -r
Command succeeded.
```

Notes

Run this command as the root user.

Configure a directory, where libclntsh.so client library of Oracle exists, to LD_LIBRARY_PATH, an environment variable.

Additionally, configure the home directory of Oracle to ORACLE_HOME, an environment variable.

If OS authentication is used without specifying the -u option, a user who runs this command needs to belong to the dba group, in order to gain administrative privileges for Oracle.

Preliminarily configure the password of a user specified in the -u option, in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the password. Put a colon ":" at the end of the row.

"*User name*:*Password*:"

Example of file path: /opt/nec/clusterpro/etc/stillpoint.conf

Example of password setting: root:password:

A user specified in the -u option needs to have administrative privileges for Oracle.

If the rest point has been secured by running the command for securing the rest point with the -s option, the control is not returned while the command remains resident. By running the command for releasing the rest point with the -r option at a different process, the resident command for securing the rest point finishes and the control is returned.

Configure Oracle in the ARCHIVELOG mode in advance to run this command.

If an Oracle data file is acquired while this command is used to secure the rest point, the backup mode will be set for the data file. To restore and use the data file, disable the backup mode on Oracle to restore the data file.

Error Messages

Message	Cause/Solution
Invalid option.	Invalid command option. Check the command option.
Cannot connect to database.	Failed to connect to the database. Check the name and the status of the database.
Username or password is not correct.	User authentication failed. Check your user name and password.

Continued on next page

Table 8.65 – continued from previous page

Message	Cause/Solution
Suspend database failed.	Failed to secure the rest point. Check the user privileges and the database settings.
Resume database failed.	Failed to release the rest point. Check the user privileges and the database settings.
Internal error.	An internal error has occurred.

8.32 Controlling the rest point of PostgreSQL (clppsqlstill command)

Controls the rest point of PostgreSQL.

Command line

clppsqlstill -d *databasename* -u *username* -s
clppsqlstill -d *databasename* -r

Description

Controls the securing/release of the rest point of PostgreSQL.

Option

-d databasename
Specifies the name of the target database for rest point control.

-u username
Specifies the name of the database user who executes rest point control.

-s
Secures the rest point.

-r
Releases the rest point.

Return Value

0	Normal completion
2	Invalid command option
3	DB connection error
4	Authentication error for the user specified in the -u option
5	Failed to secure the rest point.
6	Failed to release the rest point.
99	Internal error

Examples

```
# clppsqlstill -d postgres -u postgres -s
Command succeeded.
```

```
# clppsqlstill -d postgres -r
Command succeeded.
```

Notes

Run this command as the root user.

Configure a directory, where libpq.so client library of PostgreSQL exists, to LD_LIBRARY_PATH, an environment variable.

If any number other than the default value (5432) is set to the port number connected to PostgreSQL, configure the port number in PQPORT, an environment variable.

Preliminarily configure the password of a user specified in the -u option, in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the password. Put a colon ":" at the end of the row.

"*User name*:*Password*:"

Example of file path: /opt/nec/clusterpro/etc/stillpoint.conf

Example of password setting: root:password:

A user specified in the -u option needs to have superuser privileges for PostgreSQL.

Enable WAL archive of PostgresSQL in advance to run this command.

If the rest point has been secured by running the command for securing the rest point with the -s option, the control is not returned while the command remains resident. By running the command for releasing the rest point with the -r option at a different process, the resident command for securing the rest point finishes and the control is returned.

Error Messages

Message	Cause/Solution
Invalid option.	Invalid command option. Check the command option.
Cannot connect to database.	Failed to connect to the database. Check the name and the status of the database.
Username or password is not correct.	User authentication failed. Check your user name and password.
Suspend database failed.	Failed to secure the rest point. Check the user privileges and the database settings.
Resume database failed.	Failed to release the rest point. Check the user privileges and the database settings.
Internal error.	An internal error has occurred.

8.33 Controlling the rest point of SQL Server (clpmssqlstill command)

Controls the rest point of SQL Server.

Command line

clpmssqlstill -d *databasename* -u *username* -v *vdiusername* -s
clpmssqlstill -d *databasename* -v v*diusername* -r

Description

Controls the securing/release of the rest point of SQL Server.

Option

-d databasename
Specifies the name of the target database for rest point control.

-u username
Specifies the name of the database user who executes rest point control.

-v vdiusername
Specifies the name of an OS user who executes vdi

-s
Secures the rest point.

-r
Releases the rest point.

Return Value

0	Normal completion
2	Invalid command option
3	DB connection error
4	Authentication error for the user specified in the -u option
5	Failed to secure the rest point.
6	Failed to release the rest point.
7	Timeout error
99	Internal error

Examples

```
# clpmssqlstill -d userdb -u sa -v mssql -s
Command succeeded.
```

```
# clpmssqlstill -d userdb -v mssql -r
Command succeeded.
```

Notes

Run this command as the root user.

Configure directories, where libsqlvdi.so VDI client library of SQL Server and libodbc.so ODBC library exist, to LD_LIBRARY_PATH, an environment variable.

Preliminarily configure the password of a user specified in the -u option, in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the password. Put a colon ":" at the end of the row.

"*User name*:*Password*:"

Example of file path: **/opt/nec/clusterpro/etc/stillpoint.conf**

Example of password setting: **sa:password:**

A user specified in the -u option needs to have privileges to execute the BACKUP DATABASE statement of SQL Server.

An OS user specified in the -v option needs to have privileges to execute VDI client.

You need to preliminarily configure the timeout value of this command in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the timeout time. Put a colon ":" at the last row. Unless it is set, the value described in the following example will be used as the default value.

"*Timeout name*: *number of seconds*:"

Example of file path: /opt/nec/clusterpro/etc/stillpoint.conf

Example of time-out (GetConfiguration) configured: cfgtimeout:1:

Example of time-out (GetCommand) configured: cmdtimeout:90:

Example of time-out (SQL) configured: sqltimeout:60:

You need to preliminarily configure the ODBC driver used for operating the database, in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the ODBC driver. Put a colon ":" at the end of the row. Unless it is set, the value described in the following example is used as the default value.

"*ODBC driver*: *Name of ODBC driver to be used*:"

Example of file path: /opt/nec/clusterpro/etc/stillpoint.conf

Example of ODBC driver: odbcdriver:ODBC Driver 13 for SQL Server:

If the rest point has been secured by running the command for securing the rest point with the -s option, the control is not returned while the command remains resident. By running the command for releasing the rest point with the -r option at a different process, the resident command for securing the rest point finishes and the control is returned.

Error Messages

Message	Cause/Solution
Invalid option.	Invalid command option. Check the command option.
Cannot connect to database.	Failed to connect to the database. Check the name and the status of the database.

Continued on next page

Table 8.67 – continued from previous page

Message	Cause/Solution
Username or password is not correct.	User authentication failed. Check your user name and password.
Suspend database failed.	Failed to secure the rest point. Check the user privileges and the database settings.
Resume database failed.	Failed to release the rest point. Check the user privileges and the database settings.
Timeout.	The command timed out.
Internal error.	An internal error has occurred.

8.34 Controlling the rest point of Sybase (clpsybasestill command)

Controls the rest point of Sybase.

Command line

clpsybasestill -d *databasename* -u *username* -s
clpsybasestill -d *databasename* -r

Description

Controls the securing/release of the rest point of Sybase.

Option

-d databasename
Specifies the name of the target database for rest point control.

-u username
Specifies the name of the database user who executes rest point control.

-s
Secures the rest point.

-r
Releases the rest point.

Return Value

0	Normal completion
2	Invalid command option
3	DB connection error
4	Authentication error for the user specified in the -u option
5	Failed to secure the rest point.
6	Failed to release the rest point.
99	Internal error

Examples

```
# clpsybasestill -d master -u sa -s
Command succeeded.
```

```
# clpsybasestill -d master -r
Command succeeded.
```

Notes

Run this command as the root user. Configure a directory, where libsybdb64.so client library of Sybase exists, to LD_LIBRARY_PATH, an environment variable. Additionally, configure appropriate settings for the following environment variables.

SYBASE: Install directory of Sybase.

LANG: Languages which the installed Sybase can accommodate.

DSQUERY: Database server name of Sysbase.

Preliminarily configure the password of a user specified in the -u option, in the stillpoint.conf file of the etc directory under EXPRESSCLUSTER install directory. Use the following format for the password. Put a colon ":" at the end of the row.

"*User name*:*Password*:"

Example of file path: /opt/nec/clusterpro/etc/stillpoint.conf

Example of password setting: root:password:

A user specified in the -u option needs to have privileges to execute the quiesce database command of Sybase.

If the rest point has been secured by running the command for securing the rest point with the -s option, the control is not returned while the command remains resident. By running the command for releasing the rest point with the -r option at a different process, the resident command for securing the rest point finishes and the control is returned.

Error Messages

Message	Cause/Solution
Invalid option.	Invalid command option. Check the command option.
Cannot connect to database.	Failed to connect to the database. Check the name and the status of the database.
Username or password is not correct.	User authentication failed. Check your user name and password.
Suspend database failed.	Failed to secure the rest point. Check the user privileges and the database settings.

Continued on next page

Table 8.68 – continued from previous page

Message	Cause/Solution
Resume database failed.	Failed to release the rest point. Check the user privileges and the database settings.
Internal error.	An internal error has occurred.

8.35 Displaying the cluster statistics information (clpperfc command)

the clpperfc command displays the cluster statistics information.

Command line

clpperfc --starttime -g *group_name*
clpperfc --stoptime -g *group_name*
clpperfc -g [*group_name*]
clpperfc -m *monitor_name*

Description

This command displays the median values (millisecond) of the group start time and group stop time.

This command displays the monitoring processing time (millisecond) of the monitor resource.

Option

--starttime -g group_name
Displays the median value of the group start time.

--stoptime -g group_name
Displays the median value of the group stop time.

-g [group_name]
Displays the each median value of the group start time and group stop time.

If groupname is omitted, it displays the each median value of the start time and stop time of all the groups.

-m monitor_name
Displays the last monitor processing time of the monitor resource.

Return value

0	Normal termination
1	Invalid command option
2	User authentication error
3	Configuration information load error
4	Configuration information load error
5	Initialization error
6	Internal error
7	Internal communication initialization error
8	Internal communication connection error
9	Internal communication processing error
10	Target group check error
12	Timeout error

Example of Execution

When displaying the median value of the group start time:

```
# clpperfc --starttime -g failover1
200
```

When displaying each median value of the start time and stop time of the specific group:

```
# clpperfc -g failover1
            start time    stop time
failover1          200          150
```

When displaying the monitor processing time of the monitor resource:

```
# clpperfc -m monitor1
100
```

Remarks

The time is output in millisecond by this commands.

If the valid start time or stop time of the group was not obtained, - is displayed.

If the valid monitoring time of the monitor resource was not obtained, 0 is displayed.

Notes

Execute this command as a root user.

Error Messages

Message	Cause/Solution
Log in as root.	Run this command as the root user.
Invalid option.	The command option is invalid. Check the command option.
Command timeout.	Command execution timed out.
Internal error.	Check if memory or OS resources are sufficient.

8.36 Checking the cluster configuration information (clpcfchk command)

This command checks the cluster configuration information.

Command line

clpcfchk -o *path* [-i *conf_path*]

Description

This command checks the validness of the setting values based on the cluster configuration information.

Option

-o path
Specifies the directory to store the check results.

-i conf_path
Specifies the directory which stored the configuration information to check.

If this option is omitted, the applied configuration information is checked.

Return Value

0	Normal termination
Other	than 0 Termination with an error

Example of Execution

When checking the applied configuration information:

```
# clpcfchk -o /tmp
server1 : PASS
server2 : PASS
```

When checking the stored configuration information:

```
# clpcfchk -o /tmp -i /tmp/config
server1 : PASS
server2 : FAIL
```

Execution Result

For this command, the following check results (total results) are displayed.

Check Results (Total Results)	Description
PASS	No error found.
FAIL	An error found. Check the check results.

Remarks

Only the total results of each server are displayed.

Notes

Run this command as a root user.

When checking the configuration information exported through Cluster WebUI, decompress it in advance.

Error Messages

Message	Cause/Solution
Log in as root.	Log in as a root user.
Invalid option.	Specify a valid option.
Could not opened the configuration file. Check if the configuration file exists on the specified path.	The specified path does not exist. Specify a valid path.
Server is busy. Check if this command is already run.	This command has been already activated.
Failed to obtain properties.	Failed to obtain the properties.
Failed to check validation.	Failed to check the cluster configuration.
Internal error. Check if memory or OS resources are sufficient.	The amount of memory or OS resources may be insufficient. Check for any insufficiency.

CHAPTER

NINE

TROUBLESHOOTING

This chapter provides instructions for troubleshooting problems with EXPRESSCLUSTER.

This chapter covers:

- 9.1. *Troubleshooting*
- 9.2. *Troubleshooting problems with VERITAS volume manager*
- 9.3. *To confirm the progress of the fsck / xfs_repair command*

9.1 Troubleshooting

The following provides instructions for troubleshooting problems you experience in operating the EXPRESSCLUSTER system.

9.1.1 When the EXPRESSCLUSTER system does not start or end

A cluster system starts working by restarting servers after installing EXPRESSCLUSTER. If your cluster system does not behave properly, check the following:

1. Registration of cluster configuration data

   The cluster configuration data should be registered with all servers (which will form a cluster system) when you cluster them. If the cluster configuration data does not exist in the following path, the data may not be registered yet. Check it is registered.

   /opt/nec/clusterpro/etc/clp.conf

   If the cluster configuration data does not exist in the above path, see "Creating the Cluster Configuration Data" in the "Installation and Configuration Guide" for registering the data.

2. Server names and IP addresses in the cluster configuration data

   Check the server names and IP addresses are valid.
   (# hostname,# ifconfig....)

3. License registration

   The license may not be registered yet. Run the following command on all servers in the cluster to confirm the license is registered:

   # clplcnsc -l -a

See "*Managing licenses (clplcnsc command)*" in "8.2. *EXPRESSCLUSTER commands*" in this guide for more information on the above command.

If you are using the trial version license or fixed term license, confirm if it is not expired yet.

4. EXPRESSCLUSTER service start status

   Run the following command to check the settings for starting service of EXPRESSCLUSTER:

   For init.d environment:

```
# chkconfig --list clusterpro
clusterpro 0:off 1:off 2:off 3:on 4:off 5:on 6:off
```

   For systemd environment:

```
# systemctl is-enabled clusterpro
```

5. Cluster process status

   Run the following command to check if EXPRESSCLUSTER is working properly:

```
# ps -ef | grep clp

root 1669    1 0 00:00 ? 00:00:00 clpmonp -event -a 2 -r 0 -w 0
root 1670 1669 0 00:00 ? 00:00:00 clpevent
root 1684    1 0 00:00 ? 00:00:00 clpmonp -trnsv -a 2 -r 0 -w 0
root 1685 1684 0 00:00 ? 00:00:00 clptrnsv
root 1784    1 0 00:00 ? 00:00:00 /opt/nec/clusterpro/bin/clppm
root 1796 1795 0 00:00 ? 00:00:00 clprc
root 1809 1808 0 00:00 ? 00:00:00 clprm
root 1813 1812 0 00:00 ? 00:00:00 clpnm
root 1818 1813 0 00:00 ? 00:00:00 clplanhb
root 1820 1813 0 00:00 ? 00:00:00 clpdiskhb
root 1822 1813 0 00:00 ? 00:00:00 clpcomhb
root 1823 1813 0 00:00 ? 00:00:00 clplankhb
root 1935    1 0 00:00 ? 00:00:00 clpmonp -webmgr -a 2 -o -start -r 0 -w 0
root 1936 1935 0 00:00 ? 00:00:00 clpwebmc -start
root 1947    1 0 00:00 ? 00:00:00 clpmonp -webalert -a 2 -r 0 -w 0
root 1948 1947 0 00:00 ? 00:00:00 clpaltd
```

   If you can check the run statuses of the following processes by executing the ps command, EXPRESSCLUSTER is working properly.

   - Event process and data transfer process

```
root 1685 1684 0 00:00 ? 00:00:00 clptrnsv
root 1669    1 0 00:00 ? 00:00:00 clpmonp -event
root 1670 1669 0 00:00 ? 00:00:00 clpevent
root 1684    1 0 00:00 ? 00:00:00 clpmonp -trnsv
```

   If the event process is not started yet, the process manager described in the following section will not start.

   - Process manager

```
root 1784 1 0 00:00 ? 00:00:00 /opt/nec/clusterpro/bin/clppm
```

     By starting up this process, the following processes are generated. Therefore, if any error such as error in cluster configuration data file is detected, EXPRESSCLUSTER will not start.

     clprc

clprm
clpnm

- Resource control process:

```
root 1796 1795 0 00:00 ? 00:00:00 clprc
```

  * This process can start up even if no group resources are registered yet.

- Resource monitor process:

```
root 1809 1808 0 00:00 ? 00:00:00 clprm
```

  * This process can start up even if no monitor resources are registered yet.

- Server management process:

```
root 1813 1812 0 00:00 ? 00:00:00 clpnm
```

- Heartbeat process:

```
root 1813 1821 0 00:00 ? 00:00:00 clpcomhb
root 1813 1817 0 00:00 ? 00:00:00 clplanhb
root 1813 1819 0 00:00 ? 00:00:00 clpdiskhb
root 1823 1813 0 00:00 ? 00:00:00 clplankhb
```

  If a disk heartbeat resource has been added to the heartbeat resources in the cluster configuration data, clpdiskhb is started. If a COM interface has been added, clpcomhb is started. If a kernel mode LAN heartbeat resource has been added, clplankhb is started.

- WebManager process:

```
root 1936 1935 0 00:00 ? 00:00:00 clpwebmc -start
```

- Alert process:

```
root 1948 1947 0 00:00 ? 00:00:00 clpaltd
```

The display style of the ps command may look different from the above depending on the distribution.

6. Cluster process status ~ For Replicator~

   Run the following commands to check if EXPRESSCLUSTER is working properly:

```
# ps -ef | grep clp

root 1669    1 0 00:00 ? 00:00:00 clpmonp -event -a 2 -r 0 -w 0
root 1670 1669 0 00:00 ? 00:00:00 clpevent
root 1684    1 0 00:00 ? 00:00:00 clpmonp -trnsv -a 2 -r 0 -w 0
root 1685 1684 0 00:00 ? 00:00:00 clptrnsv
root 1696    1 0 00:00 ? 00:00:00 clpmonp -mdagent -a 5 -r 0 -w 30
root 1697 1696 0 00:00 ? 00:00:00 clpmdagent
root 1784    1 0 00:00 ? 00:00:00 /opt/nec/clusterpro/bin/clppm
root 1796 1795 0 00:00 ? 00:00:00 clprc
root 1809 1808 0 00:00 ? 00:00:00 clprm
root 1813 1812 0 00:00 ? 00:00:00 clpnm
root 1818 1813 0 00:00 ? 00:00:00 clplanhb
root 1822 1813 0 00:00 ? 00:00:00 clpcomhb
root 1823 1813 0 00:00 ? 00:00:00 clplankhb
```

(continues on next page)

(continued from previous page)

```
root 1935    1 0 00:00 ? 00:00:00 clpmonp -webmgr -a 2 -o -start -r 0 -w 0
root 1936 1935 0 00:00 ? 00:00:00 clpwebmc -start
root 1947    1 0 00:00 ? 00:00:00 clpmonp -webalert -a 2 -r 0 -w 0
root 1948 1947 0 00:00 ? 00:00:00 clpaltd
```

If you can check the run statuses of the following processes by executing the ps command, EXPRESSCLUSTER is working properly.

- Event process, data transfer process, and mirror agent

```
root 1696    1 0 00:00 ? 00:00:00 clpmonp --mdagent -a 5 -r 0 -w 30
root 1697 1696 0 00:00 ? 00:00:00 clpmdagent
```

If the event process is not started yet, the process manager in the following section will not start.

- Process manager

```
root 1784 1 0 00:00 ? 00:00:00 /opt/nec/clusterpro/bin/clppm
```

  By starting up this process, the following processes are generated. Therefore, if any error such as error in cluster configuration data file is detected, EXPRESSCLUSTER will not start.

  clprc
  clprm
  clpnm

- Resources control process:

```
root 1796 1795 0 00:00 ? 00:00:00 clprc
```

  * This process can start up even if no group resources are registered yet.

- Resource monitor process:

```
root 1809 1808 0 00:00 ? 00:00:00 clprm
```

  * This process can start up even if no monitor resources are registered yet.

- Server management process:

```
root 1813 1812 0 00:00 ? 00:00:00 clpnm
```

- Heartbeat process:

```
root 1822 1813 0 00:00 ? 00:00:00 clpcomhb
root 1818 1813 0 00:00 ? 00:00:00 clplanhb
root 1823 1813 0 00:00 ? 00:00:00 clplankhb
```

  If a COM heartbeat resource has been added to the heartbeat resources in the cluster configuration data, clpcomhb is started. If a kernel mode LAN heartbeat resource has been added, clplankhb is started.

- WebManager process:

```
root 1936 1935 0 00:00 ? 00:00:00 clpwebmc - start
```

- Alert process:

```
root 1948 1947 0 00:00 ? 00:00:00 clpaltd
```

The display style of the ps command may look different from the above depending on the distribution.

7. Loading of the mirror driver ~For Replicator~

   Run the lsmod command. Check that the run result of lsmod contains the following loadable module.

   Liscal

8. Loading of the kernel mode LAN heartbeat driver ~For kernel mode LAN heartbeat resource~

   Run the lsmod command. Check that the run result of lsmod contains the following loadable module.

   clpkhb

9. Loading of the keepalive driver ~For userw User mode monitor resource (keepalive)~

   Run the lsmod command. Check that the run result of lsmod contains the following loadable module.

   clpka

10. Normal startup of the cluster from syslog

    To see EXPRESSCLUSTER processes are working properly by looking into syslog, find the following messages.

    - To check the process manager's startup:

```
<type: pm><event: 1> Starting the cluster daemon...
```

    - To check heartbeat resources' activation:

```
<type: nm><event: 3> Resource lanhb1 of server server1 has started.
<type: nm><event: 3> Resource diskhb1 of server server1 has started.
<type: nm><event: 1> Server server1 has started.
<type: nm><event: 3> Resource diskhb1 of server server2 has started.
<type: nm><event: 1> Server server2 has started.
<type: nm><event: 3> Resource lanhb1 of server server2 has started.
```

      You will see the above messages when the followings are specified for heartbeat resources in a 2-node configuration.

      lanhb1 LAN heartbeat resources
      diskhb1 Disk heartbeat resources

    - To check group resources' activation:

```
<type: rc><event: 10> Activating group grp1 has started.
<type: rc><event: 30> Activating fip1 resource has started.
<type: rc><event: 31> Activating fip1 resource has completed.
<type: rc><event: 30> Activating disk1 resource has started.
<type: rc><event: 31> Activating disk1 resource has completed.
<type: rc><event: 11> Activating group grp1 has completed.
```

      You will see the above messages when the group resource, grp1, is activated on server1. The group resources' configuration data is as follows:

      fip1 Floating IP addresses resources
      disk1 Shared disk resources

    - To check monitor resources' startup:

```
<type: rm><event: 1> Monitoring userw has started.
<type: rm><event: 1> Monitoring ipw1 has started.
```

You will see the above messages when the monitor resources are specified as follows:

userw User mode monitor resources
ipw1 IP monitor resources

- To check license consistency:

Product version

```
<type: lcns><event: 1> The number of licenses is 2. (Product␣
↪name:EXPRESSCLUSTER X)
```

You will see the above message when 2-CPU license is registered.

Trial version

```
<type: lcns><event: 2> The trial license is valid until yyyy/mm/dd. (Product␣
↪name: EXPRESSCLUSTER X)
```

11. Successful startup of the cluster ~For Replicator~

To see EXPRESSCLUSTER processes are working properly by looking into syslog, find the following messages.

- To check the mirror agent's startup:

```
<type: mdagent><event: 1> Agent has started successfully.
```

- To check the mirror driver's startup:

```
<type: liscal><event: 101> Registered blkdev with major=218.
```

- To check the process manager's startup:

```
<type: pm><event: 1> Starting the cluster daemon...
```

- To check heartbeat resources' activation:

```
<type: nm><event: 3> Resource lanhb1 of server server1 has started.
<type: nm><event: 1> Server server1 has started.
<type: nm><event: 3> Resource lanhb1 of server server2 has started.
<type: nm><event: 1> Server server2 has started.
```

You will see the above messages when the following is specified for heartbeat resources in a 2-node configuration.

lanhb1 LAN heartbeat resources

- To check group resources' activation:

```
<type: rc><event: 10> Activating group grp1 has started.
<type: rc><event: 30> Activating fip1 resource has started.
<type: rc><event: 31> Activating fip1 resource has completed.
<type: rc><event: 30> Activating md1 resource has started.
<type: rc><event: 31> Activating md1 resource has completed.
<type: rc><event: 11> Activating group grp1 has completed.
```

You will see the above messages when the group resource, grp1, is activated on server1. The group resources' configuration data is as follows;

fip1 Floating IP addresses resources

md1 Mirror disk resources

- To check start of monitoring by monitoring resources:

```
<type: rm><event: 1> Monitoring userw has started.
<type: rm><event: 1> Monitoring ipw1 has started.
<type: rm><event: 1> Monitoring mdw1 has started.
<type: rm><event: 1> Monitoring mdnw1 has started.
```

You will see the above messages when the monitor resources are specified as follows;

userw User mode monitor resources
ipw1 IP monitor resources
mdw1 Mirror disk monitor resources
mdnw1 Mirror disks connect monitor resources

- To check license consistency:

Product version

```
<type: lcns><event: 1> The number of licenses is 2. (Product name:␣
↪EXPRESSCLUSTER X)
```

You will see the above message when a 2-CPU license is registered.

Trial version

```
<type: lcns><event: 2> The trial license is valid until yyyy/mm/dd. (Product␣
↪name:EXPRESSCLUSTER X)
```

12. Free disk space

    Run the df command to check the size of the free disk space in the file system that contains /opt/nec/clusterpro. For details on the disk space to be used by the EXPRESSCLUSTER Server, see "Installation requirements for EXPRESSCLUSTER" in "Getting Started with Guide".

13. Usage of memory or OS resource

    Run the top or free command to check the OS memory usage and CPU utilization.

9.1.2 When activating or deactivating group resources fails

If any error is detected in activation of a group resource, detailed error information is logged in the alert and syslog. Examine the logs to find the cause of the error and take appropriate action for it.

1. Floating IP resource
   Check that the specified IP address is not already used on the network or you have not specified an IP address of a wrong network segment.
   For more information on errors, see "*Floating IP resources*".
2. Disk resources
   Check that the device and mount point exist, and the file system is configured.
   For more information on errors, see "*Disk resources*".
3. EXEC resources
   Check that the script path is correct and what is scripted is appropriate.
   For more information on errors, see "*EXEC resources*".
4. Mirror disk resources ~For Replicator~

Check that the devices and mount points exist, and the cluster partitions and data partitions are allocated. Check the file system specified for mirror disk resources is available as well.

For more information on errors, see "*Mirror disk resources*".

5. Hybrid disk resources ~For Replicator DR~

   Check that the devices and mount points exist, and the cluster partitions and data partitions are allocated. Check the file system specified for mirror disk resources is available as well.

   For more information on errors, see "*Hybrid disk resources*".

9.1.3 When a monitor resource error occurs

If a monitor resource detects any error, detailed information on error is logged in the alert and syslog. Examine the logs to find the cause of the error and take appropriate action for it.

1. Error detected by the IP monitor resource

   Check that you can send packets with the ping command, and other network segments are routed if any.

   For more information on errors, see "*IP monitor resources*".

2. Error detected by the disk monitor resource

   Check that a disk device exists. If you are using a shared disk, check SCSI or fibre cables are securely connected to the shared disk.

   For more information on errors, see "*Disk monitor resources*".

3. Error detected by the PID monitor resource

   Check that the process to be monitored exists by using a command, such as ps command.

   For more information on errors, see "*PID monitor resources*".

4. Error detected by the User mode monitor resource (monitor method: softdog)

   When "initialization failure" is detected, confirm that the softdog driver can be loaded by using the insmod command of OS.

   Furthermore, when "server reset" occurs, check the load status of the user space.

   For more information on errors, see "*User mode monitor resources*".

5. Error detected by the mirror disk monitor resource ~For Replicator~

   Check that the disk devices exist, and the cluster partitions and data partitions are allocated. Confirm that the Mirror Agent is active.

   For more information on errors, see "*Mirror disk monitor resources*".

6. Error detected by the mirror disks connect monitor resource ~For Replicator~

   Check that the mirror disk is connected and the Mirror Agent is active.

   For more information on errors, see "*Mirror disk connect monitor resources*".

7. Error detected by the hybrid disk monitor resource ~For Replicator DR~

   Check that the mirror disk is connected and the Mirror Agent is active.

   For more information on errors, see "*Hybrid disk monitor resources*".

8. Error detected by the hybrid disk connect monitor resource ~For Replicator DR~

   Check that the mirror disk is connected and the Mirror Agent is active.

   For more information on errors, see "*Hybrid disk connect monitor resources*".

9. Error detected by the NIC Link Up/Down monitor resource

   Check how the NIC of the server is connected to the network device.

   For more information on errors, see "*NIC link up/down monitor resources*".

9.1.4 When a heartbeat time-out occurs

Possible causes of heartbeat time-out between servers are listed below:

Cause	Solution
Disconnection of LAN/disk/COM cables	For disk or COM cables, check if the cables are connected securely. For LAN cables, check that you can send packets with the ping command.
Heavily loaded user space (resulting in misinterpreted heartbeat time-out)	Run the following command in advance to extend the heartbeat time-out when running an application that can make the OS heavily loaded for a long time. `# clptoratio -r 3 -t 1d` The above mentioned command triples the heartbeat time-out for 24 hours.

9.1.5 When network partitioning occurs

Network partitioning indicates that all communication routes are blocked between servers. This section describes how you can check whether or not the network is partitioned and what you should do about it. The following examples assume that you have registered LAN kernel mode LAN, disk and COM for heartbeat resources in a 2-node cluster configuration.

When all heartbeat resources are normal (the network is not partitioned), the result of executing the clpstat command is:

When you run the command on server1

 # clpstat -n

```
==================== HEARTBEAT RESOURCE STATUS =================
Cluster : cluster
  *server0 : server1
   server1 : server2

   HB0 : lanhb1
   HB1 : lanhb2
   HB2 : lankhb1
   HB3 : lankhb2
   HB4 : diskhb1
   HB5 : comhb1

[on server0 : Online]
       HB   0   1   2   3   4   5

-----------------------------------------------------------------
  server0 : o   o   o   o   o   o
  server1 : o   o   o   o   o   o

[on server1 : Online]
       HB   0   1   2   3   4   5
```

(continues on next page)

(continued from previous page)

```
----------------------------------------------------------------
  server0 : o   o   o   o   o   o
  server1 : o   o   o   o   o   o
```

When you run the command on server2

 # clpstat -n

```
==================== HEARTBEAT RESOURCE STATUS =================
    Cluster : cluster
    server0 : server1
   *server1 : server2

    HB0 : lanhb1
    HB1 : lanhb2
    HB2 : lankhb1
    HB3 : lankhb2
    HB4 : diskhb1
    HB5 : comhb1

[on server0 : Online]
       HB   0   1   2   3   4   5

----------------------------------------------------------------
  server0 : o   o   o   o   o   o
  server1 : o   o   o   o   o   o

[on server1 : Online]
       HB   0   1   2   3   4   5

----------------------------------------------------------------
  server0 : o   o   o   o   o   o
  server1 : o   o   o   o   o   o

================================================================
```

When the network is partitioned, the result of executing the clpstat command is what is described below. Both servers recognize each other that the counterpart is down.

When you run the command on server1

 # clpstat -n

```
==================== HEARTBEAT RESOURCE STATUS =================
 Cluster : cluster
   *server0 : server1
    server1 : server2

    HB0 : lanhb1
    HB1 : lanhb2
    HB2 : lankhb1
    HB3 : lankhb2
    HB4 : diskhb1
    HB5 : comhb1

   [on server0 : Caution]
         HB   0   1   2   3   4   5
```

(continues on next page)

(continued from previous page)

```
----------------------------------------------------------------
    server0 : o   o   o   o   o   o
    server1 : x   x   x   x   x   x

   [on server1 : Offline]
         HB   0   1   2   3   4   5

----------------------------------------------------------------
    server0 : -   -   -   -   -   -
    server1 : -   -   -   -   -   -
================================================================
```

When you run the command on server2

 # clpstat -n

```
=================== HEARTBEAT RESOURCE STATUS ================
 Cluster : cluster
    server0 : server1
   *server1 : server2

    HB0 : lanhb1
    HB1 : lanhb2
    HB2 : lankhb1
    HB3 : lankhb2
    HB4 : diskhb1
    HB5 : comhb1

   [on server0 : Offline]
         HB   0   1   2   3   4   5

----------------------------------------------------------------
    server0 : -   -   -   -   -   -
    server1 : -   -   -   -   -   -

   [on server1 : Caution]
         HB   0   1   2   3   4   5
----------------------------------------------------------------
    server0 : x   x   x   x   x   x
    server1 : o   o   o   o   o   o
================================================================
```

Shut down both servers immediately if the network is partitioned. Check the following for heartbeat resources.

1. LAN heartbeat resource
   - LAN cable status
   - Network interface status
2. Kernel mode LAN heartbeat resource

- LAN cable status
- Network interface status

3. Disk heartbeat resource
   - Disk cable status

- Disk device status

4. COM heartbeat resource
    - COM cable status

If interconnection LAN is recovered from the network partitioning, EXPRESSCLUSTER causes the servers to shut down.

If EXPRESSCLUSTER detects that the same group is active on multiple servers, it causes the servers to shut down.

For the replicator, depending on the server shutdown timing, the statuses of mirror disk resources may not be the same after rebooting the server.

Depending on the timing of server shutdown, the status of mirror disk resources may be the one requiring forced mirror recovery, mirror recovery, or normal.

9.1.6 When all interconnection LANs are disconnected

This section describes how to check the status when all interconnections (LAN heartbeat resources, kernel mode LAN heartbeat resources) between the servers are disconnected. The following examples assume that you have registered LAN, disk and COM for heartbeat resources in a 2-node cluster configuration. (You cannot register disks for the replicator.)

The following shows that the results of executing the clpstat command when all interconnections are disconnected and the disk and COM are normal. Both servers recognize that the other server is running.

When you run the command on server1

 # clpstat -n

```
==================== HEARTBEAT RESOURCE STATUS =================
 Cluster : cluster
   *server0 : server1
    server1 : server2

    HB0 : lanhb1
    HB1 : lanhb2
    HB2 : lankhb1
    HB3 : lankhb2
    HB4 : diskhb1
    HB5 : comhb1

    [on server0 : Warning]
           HB 0   1   2   3   4   5

----------------------------------------------------------------
    server0 : o   o   o   o   o   o
    server1 : x   x   x   x   o   o

[on server1 : Warning]
          HB 0   1   2   3   4   5

----------------------------------------------------------------
   server0 : -   -   -   -   -   -
   server1 : -   -   -   -   -   -
================================================================
```

When you run the command on server2

 # clpstat -n

```
==================== HEARTBEAT RESOURCE STATUS =================
 Cluster : cluster
    server0 : server1
   *server1 : server2

    HB0 : lanhb1
    HB1 : lanhb2
    HB2 : lankhb1
    HB3 : lankhb2
    HB4 : diskhb1
    HB5 : comhb1

    [on server0 : Warning]
           HB 0   1   2   3   4   5

----------------------------------------------------------------
    server0 : -   -   -   -   -   -
    server1 : -   -   -   -   -   -

    [on server1 : Warning]
           HB 0   1   2   3   4   5

----------------------------------------------------------------
    server0 : x   x   x   x   o   o
    server1 : o   o   o   o   o   o
================================================================
```

A failover does not occur when all interconnections are disconnected like the example above because communication can be achieved by disk heartbeats and COM heartbeats.

However, interconnections must be recovered as soon as possible because commands communicated by interconnections become unavailable.

Check the following for heartbeat resources:

1. LAN heartbeat resources
    - LAN cable status
    - Network interface status
2. Kernel mode LAN heartbeat resources
    - LAN cable status
    - Network interface status

When interconnects are also used as mirror disk connect in the replicator, a mirror break occurs if the interconnections (mirror disconnects) are disconnected. Run mirror recovery after restoring the interconnections.

9.1.7 Unavailable commands when interconnections are disconnected

Commands for cluster construction

Command	Description	Remarks
clpcfctrl	Distributes the configuration information created by the Cluster WebUI to the servers registered in the configuration information. Backs up the cluster configuration information to be used by the Cluster WebUI.	The configuration information cannot be distributed to other servers.
clplcnsc	Registers and displays the licenses of the product and trial versions of this product.	The license cannot be distributed to other servers.

Commands for showing status

Command	Description	Remarks
clpstat	Displays the cluster status and settings information.	Statuses of other servers cannot be retrieved.

Commands for cluster operation

Command	Description	Remarks
clpcl	Starts, stops, suspends and resumes the EXPRESSCLUSTER daemon.	Other servers cannot be operated, suspended or resumed.
clpdown	Stops the EXPRESSCLUSTER daemon and shuts down a server registered in the configuration information.	Other servers cannot be operated.
clpstdn	Stops the EXPRESSCLUSTER daemon in the entire cluster, and shuts down all servers.	Other servers cannot be operated.
clpgrp	Starts, stops, and moves groups. This command also migrates the virtual machine.	Only groups on the local server can be stopped.
clprsc	Starts, stops and moves resources.	Resources of other servers cannot be operated.
clptoratio	Extends and displays time-out values of all servers in the cluster.	Time-out ratios of other servers cannot be set.
clprexec	Issues a request to execute the error correction action from the external monitor.	Some error correction actions cannot be executed on the local server.

Commands for logs

Command	Description	Remarks
clplogcc	Collects logs and OS information.	Logs of other servers cannot be collected.

Commands for mirror (only for the Replicator)

Command	Description	Remarks
clpmdstat	Displays the status and settings information of mirroring	The mirror status of the remote server cannot be retrieved.
clpmdctrl	Activates/inactivates mirror disk resources and recovers mirroring. Displays/changes the settings of the maximum number of request queues.	Do not use this command. because mirror disk resources of both servers may be activated.

Commands for hybrid disk (only for the Replicator DR)

Command	Description	Remarks
clphdstat	Displays the status and settings information of hybrid disk resource.	The status of the remote server cannot be retrieved.
clphdctrl	Activates/inactivates mirror disk resources and recovers mirroring. Displays/changes the settings of the maximum number of request queues.	Do not use this command because hybrid disk resources of both servers may be activated.
clpledctrl	Disable or Enable chassis identify on the specified server.	The control notification of chassis identify lamp to the specified server cannot be executed.

9.1.8 Mounting mirror disks manually

This section describes how to manually mount mirror disks when you cannot start EXPRESSCLUSTER due to some sort of failure.

9.1.9 Normally mounting mirror disk when mirroring is available

Follow the steps below when the mirror agent (EXPRESSCLUSTER data mirror daemon) can be activated while the EXPRESSCLUSTER daemon cannot.

1. Run the following command on the server where you want to mount disks.

```
clpmdctrl --active <mirror_disk_resource_name (Example: md1)>
```

2. The mount point of mirror disk resources becomes accessible. Written data is mirrored to the other server.

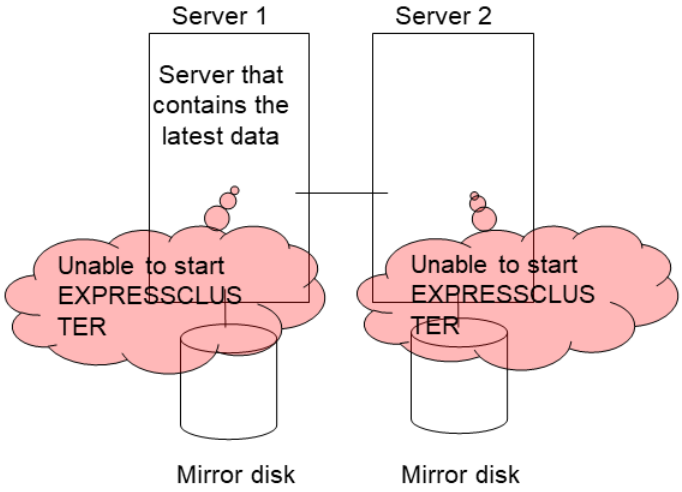
9.1.10 Forcibly mounting mirror disk when mirroring is not available

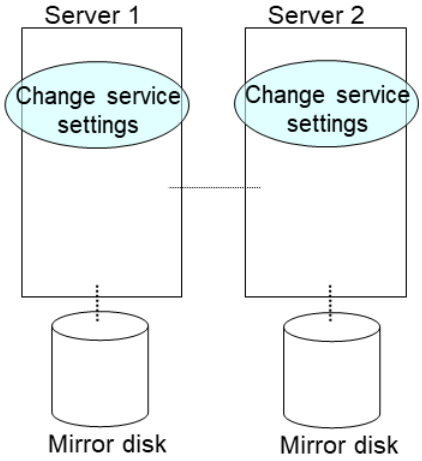
Follow the steps below to save data to mirror disks when neither the EXPRESSCLUSTER daemon nor the mirror agent (EXPRESSCLUSTER data mirror daemon) can be activated.

However, the mirroring status up to the moment just before both the EXPRESSCLUSTER daemon and EXPRESSCLUSTER data mirror daemon became unable to be activated must be normal, or you must know which server has the latest data.

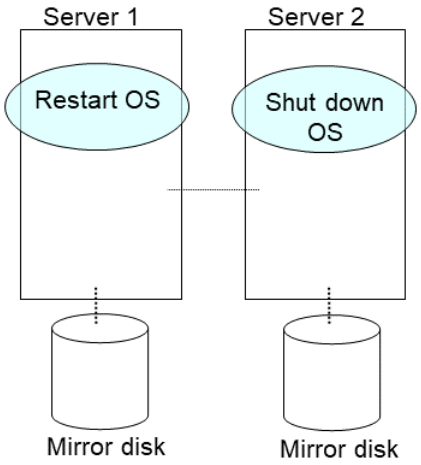
1. Set the EXPRESSCLUSTER service not to start.

```
clpsvcctrl.sh --disable -a
```



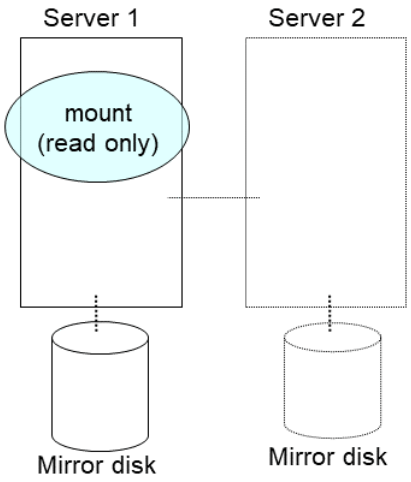


2. Run the reboot command to restart the server that has the latest data or that activated the mirror disk resources last time. Shut down the other server with the shutdown command.

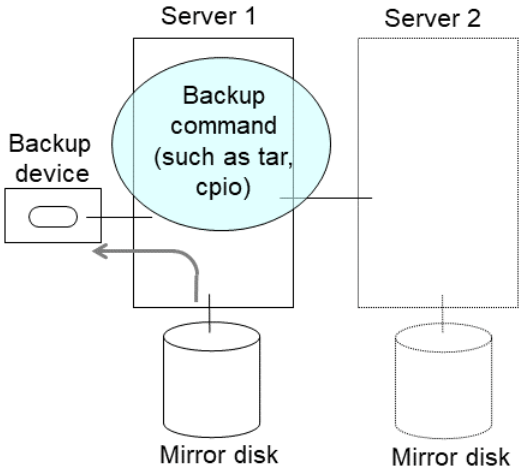


3. Run the mount command to mount a data partition on a mirror disk in the read-only mode.

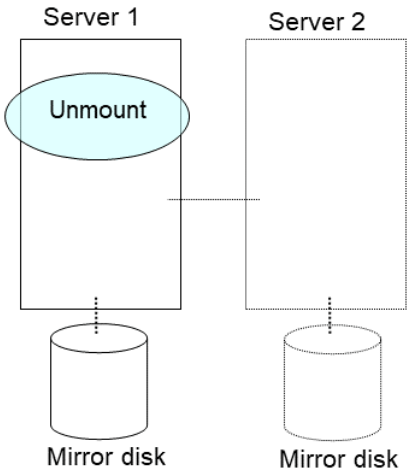
```
(Example) mount -r -t ext3 /dev/sdb5 /mnt
```



4. Back up the data in the data partition on a DAT tape or other media.



5. Unmount the mounted data partition.



9.1.11 Mounting hybrid disks manually

This section describes how to manually mount hybrid disks when you cannot start EXPRESSCLUSTER due to a failure or any other reasons.

9.1.12 Normally mounting mirror disk when mirroring is available

Follow the steps below when the mirror agent (EXPRESSCLUSTER data mirror daemon) can be activated while the EXPRESSCLUSTER daemon cannot.

1. Run the following command on the server where you want to a mount disk.

```
clphdctrl --active <hybrid_disk_resource_name (Example: hd1)>
```

2. The mount point of hybrid disk resource becomes accessible. Written data is mirrored to the other server group.

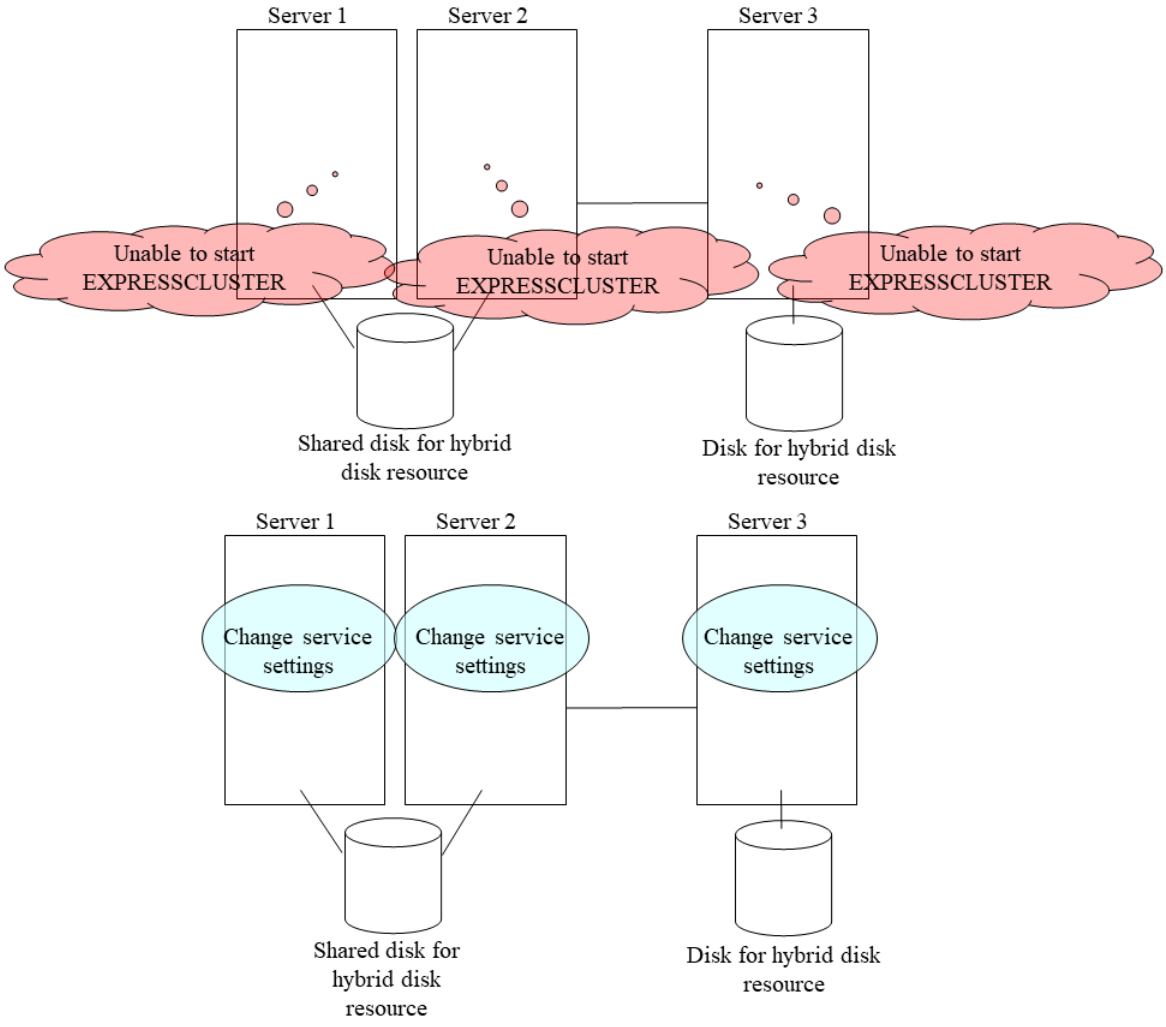
9.1.13 Forcibly mounting mirror disk when mirroring is not available

Follow the steps below to save data to hybrid disks when neither the EXPRESSCLUSTER daemon nor the mirror agent (EXPRESSCLUSTER data mirror daemon) can be activated.

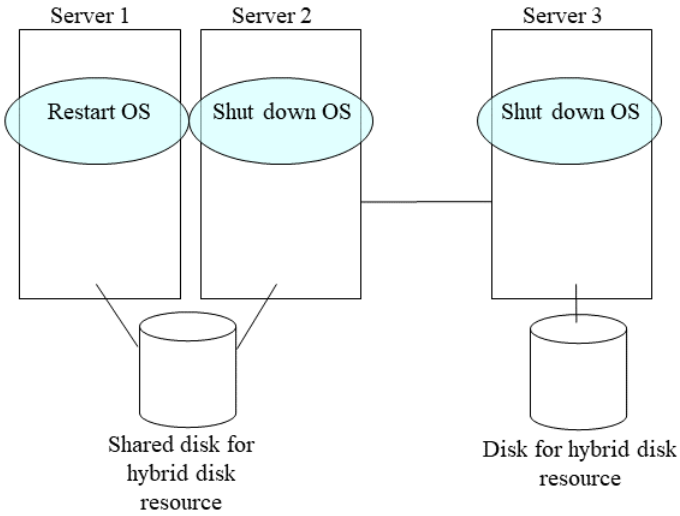
This can be performed provided the mirroring status up to the moment just before both the EXPRESSCLUSTER daemon and EXPRESSCLUSTER data mirror daemon became unable to be activated was normal, or you know which server has the latest data.

1. Set the EXPRESSCLUSTER service not to start.

```
clpsvcctrl.sh --disable -a
```

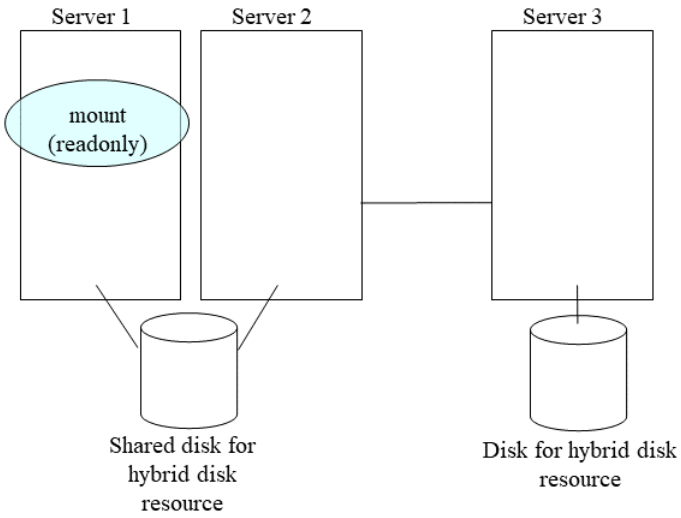


2. Run the reboot command to restart the server that has the latest data or that activated the hybrid disk resources last time. Shut down other servers with the shutdown command.

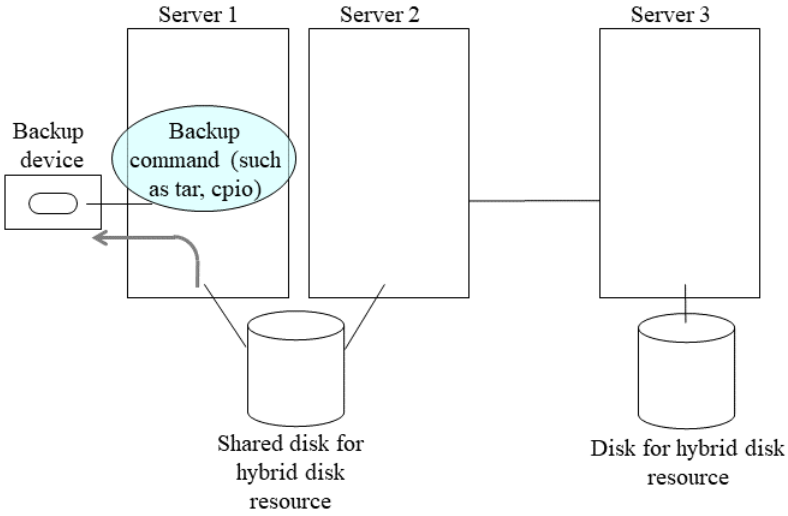


3. Run the mount command to mount the data partition on the hybrid disk in the read-only mode.

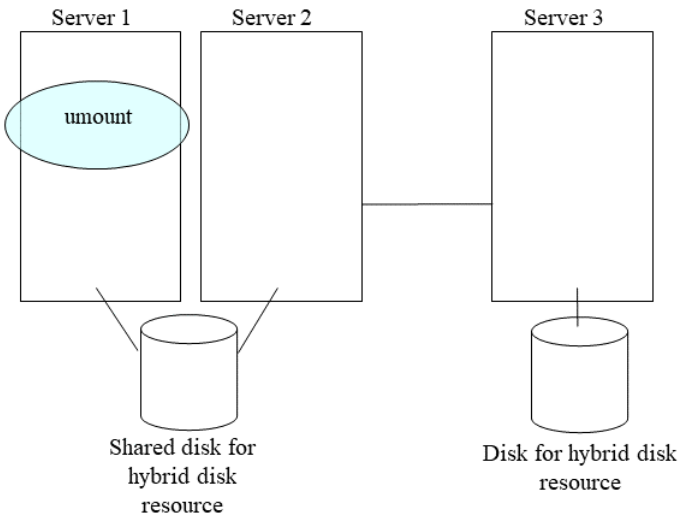
```
(Example) mount -r -t ext3 /dev/sdb5 /mnt
```



4. Back up the data in the data partition on a DAT tape or other medium.



5. Unmount the mounted data partition.



9.1.14 Manually running mkfs to mirror disk or hybrid disk

To recreate the file system of a mirror partition without changing the cluster or mirror configuration, follow the steps below:

1. Confirm that the cluster is in the normal status.
2. If you need to back up the data, see "Backup procedures" and "Restoration procedures" in "Verifying operation" in the "Installation and Configuration Guide" for the procedure.
3. Stop the group which has the mirror disk resources that you want to run the mkfs command.
4. Run the following command on the server where you will run mkfs.

   For mirror disk:

   ```
   clpmdctrl --active -nomount <mirror_disk_resource_name (Example: md1)>
   ```

   For hybrid disk:

   ```
   clphdctrl --active -nomount <hybrid_disk_resource_name (Example: hd1)>
   ```

5. Run the mkfs command to configure a file system.
   Because disks are mirrored, the mkfs command is also run on the other server.

   ```
   (Example) mkfs -t ext3 <mirror_partition_device_name (Example: /dev/NMP1)>
   ```

6. If you need to restore the backup data, see "Backup procedures" or "Restoration procedures" in "Verifying operation" in the "Installation and Configuration Guide" for the procedure.
7. After confirming the completion of the file system creation, run the following command:

   For mirror disk:

   ```
   clpmdctrl --deactive <mirror_disk_resource_name (Example: md1)>
   ```

   For mirror disk:

   ```
   clphdctrl --deactive <hybrid_disk_resource_name (Example: md1)>
   ```

9.1.15 Recovering from mirror breaks

When the auto-mirror recovery is enabled, no special operation is required. Mirroring is automatically recovered.

However, if mirroring needs to be recovered forcibly, execution of a command or operations for forcible mirror recovery using the Cluster WebUI are required.

The difference mirror recovery function is disabled in the forcible mirror recovery and the data is fully copied.

If the auto-mirror recovery is disabled, you have to recover mirroring by executing a command or using the Cluster WebUI.

9.1.16 Automatically recovering from mirroring

When the auto-mirror recovery is enabled, mirroring is recovered under the following conditions:

1. Mirror disk resources or hybrid disk resources are active.
2. The server where mirror disk resources or hybrid disk resources are active contains the latest data.
3. Servers in the cluster are in the normal status, and you can verify their mirroring statuses.
4. The data among the servers is not the same.

The auto-mirror recovery is not performed if any of the following applies.

1. One of the servers is not started.
2. You cannot confirm the mirroring status of the other server.
   (For example, communication is impossible or the cluster of the other server stops.)
3. There is no server whose mirror status is normal.
4. The mirror status is pending (hybrid disk resources only)
5. Mirror synchronization is stopped manually.
   (For example, synchronization is stopped by executing the --break option with the clpmdctrl or clphdctrl command, or the GREEN-GREEN status is changed to the GREEN-RED status by clicking the **Mirror break** icon on the **Mirror disks** tab of the Cluster WebUI. This excludes, however, the case in which the server is restarted after synchronization stops or in which synchronization is started manually.)
6. The mirror disk monitor resource and hybrid disk monitor resource stopped.
   (For example, the relevant monitor resource is temporarily stopped by the clpmonctrl command or Cluster WebUI.)

For information on how to verify the progress of recovering mirroring, see "*Checking the mirror recovery progress with a command*" and "*Checking the mirror recovery progress from the Cluster WebUI*".

9.1.17 Checking the mirror break status with a command

Run the following command to view the mirror break statuses.

For mirror disk:

```
clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>
```

For hybrid disk:

```
clphdstat --mirror <hybrid_disk_resource_name (Example: hd1)>
```

You can view the statuses of mirror disk resource or hybrid disk resource by running the clpmdstat command or clphdstat command.

1. When normal:

```
Mirror Status: Normal

md1                 server1               server2
-------------------------------------------------------
Mirror Color        GREEN                 GREEN
```

2. When the mirror recovery is required:

```
Mirror Status: Abnormal
Total Difference: 1%

md1                 server1                server2
-------------------------------------------------------------
Mirror Color        GREEN                  RED
Lastupdate Time     2018/03/04 17:30:05    --
Break Time          2018/03/04 17:30:05    --
Disk Error          OK                     OK
Difference Persent  1%                     --
```

3. When the forcible mirror recovery is required:

```
Mirror Status: Abnormal
Total Difference: 1%

md1                  server1                server2
-------------------------------------------------------------------
Mirror Color         RED                    RED
Lastupdate Time      2018/03/09 14:07:10    2004/03/09 13:41:34
Break Time           2018/03/09 14:06:21    2004/03/09 13:41:34
Disk Error           OK                     OK
Difference Persent   1%                     1%
```

4. While the mirroring is being recovered:

   See "*Checking the mirror recovery progress with a command*".

9.1.18 Checking the mirror recovery progress with a command

Run the following command to view the progress of recovering mirroring.

For mirror disk:

```
clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>
```

For hybrid disk:

```
clphdstat --mirror <hybrid_disk_resource_name (Example: hd1)>
```

You will see the following data while mirroring is being recovered.

```
Mirror Status: Recovering
```

(continues on next page)

(continued from previous page)

```
md1              server1            server2
-------------------------------------------------
Mirror Color     YELLOW              YELLOW

Recovery Status   Value
--------------------------------------
Status:            Recovering
Direction:         server1 -> server2
Percent:           7%
Used Time:         00:00:09
Remain Time:       00:01:59
```

You will see the following information when the mirror recovery is successfully completed.

```
Mirror Status: Normal

md1              server1            server2
-------------------------------------------------------
Mirror Color     GREEN               GREEN
```

9.1.19 Recovering mirror with a command

Run the following command to start the mirror recovery.

For mirror disk:

```
clpmdctrl --recovery <mirror_disk_resource_name (Example: md1)>
```

For hybrid disk:

```
clphdctrl --recovery <hybrid_disk_resource_name (Example: hd1)>
```

When FastSync Option is enabled, only the difference data is recovered. Therefore, the mirror recovery takes less time than when FastSync Option is disabled(FastSync technology).

This command immediately returns the control once the mirror recovery starts. For information on how to verify the mirror recovery progress, see "*Checking the mirror recovery progress with a command*" and "*Checking the mirror recovery progress with a command*".

9.1.20 Running the forcible mirror recovery with a command

If EXPRESSCLUSTER cannot determine which server contains the latest data, you have to run the forcible mirror recovery.

In this case, you have to manually identify the server that holds the latest data, and perform the forcible mirror recovery.

Identify the server that holds the latest data by any of the following means:

- Using the Cluster WebUI
  1. In the **Mirror disks** tab of Cluster WebUI, click the mirror disk resource to be checked.
  2. Click **Details** icon.
  3. See the last update time stamp (Last Data Updated Time) to identify the server which has the latest data. However, this Last Data Updated Time depends on the operating system's clock.

- Using the clpmdstat or clphdstat command

  Confirmation method is the same as Cluster WebUI except that you use a command.

  1. Run the following command.

     For mirror disk:

     ```
     clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>
     ```

     For hybrid disk:

     ```
     clphdstat --mirror <hybrid_disk_resource_name (Example: hd1)>
     ```

  2. See the last update time stamp (Last Data Updated Time) to identify the server which has the latest data. However, this Last Data Updated Time depends on the operating system's clock.

- Using data on mirror disks

  This method is not recommended because the data may be corrupted if anything goes wrong in the procedure. Perform the following steps on both servers to identify which has the latest data.

  1. Confirm all groups are stopped.

  2. Mount the data partition in the read only mode by referring to "*Forcibly mounting mirror disk when mirroring is not available*".

  3. Logically examine the data on the mount point.

  4. Unmount the data partition.

Identify the server that holds the latest data and then start forcible mirror recovery by any of the following means:

- Method (1) Using full-scale copy while the group is active

  Forcible mirror recovery by this method disables the difference mirror recovery function and instead uses full-scale copy.

  If the group stops during forcible mirror recovery, you cannot start the group until forcible mirror recovery is completed. Once forcible mirror recovery completion has been confirmed, the mirror disk can be used by starting the group.

  If full-scale copy is performed while the group is active, the system load may be high because forcible mirror recovery must be performed while the group is active.

  If the group contains two or more mirror disk resources or hybrid disk resources, these resources must all contain the latest data *on the same server*.

  1. Execute the clpmdctrl or clphdctrl command to start full-scale copy.

     (specify the name of the server containing the latest data and the resource name for command arguments.)

     For mirror disk:

     ```
     clpmdctrl --force <server_containing_the_latest_data> <mirror_disk_resource_
     ↪name (Example: md1)>
     ```

     For hybrid disk:

     ```
     clphdctrl --force <server_containing_the_latest_data> <hybrid_disk_resource_
     ↪name (Example: hd1)>
     ```

  2. When mirror recovery is started by the command, the command returns control immediately. Confirm the mirror recovery status and then wait for mirror recovery to complete.

  3. When the group is not active, after confirming the completion of mirror recovery, start the group.

- Method (2) Performing full copy while the group is active

With forcible mirror recovery using this method, the difference mirror recovery function is disabled, and full copy is performed instead.

Depending on the file system type, disk usage, and load status, this takes less copying time than the procedures of methods (1) and (3), which are performed in the active state.

Perform this method while the group is stopped. Until forcible mirror recovery is completed, you cannot start the group. Once forcible mirror recovery completion has been confirmed, the mirror disk can be used by starting the group.

If the group contains two or more mirror disk resources or hybrid disk resources, these resources all need to contain the latest data *on the same server*.

1. If the group is active, stop the group.
2. Execute the clpmdctrl or clphdctrl command to start full-scale copy.
   (Specify the latest data holding server name and resource name in the command argument.)

   For mirror disk

   ```
   clpmdctrl --force <server_containing_the_latest_data> <mirror_disk_resource_
   ↪name (Example: md1)>
   ```

   For hybrid disk

   ```
   clphdctrl --force <server_containing_the_latest_data> <hybrid _disk _resource␣
   ↪_ name (Example: hd1)>
   ```

3. When mirror recovery is started by the command, the command returns control immediately. Confirm the mirror recovery status and then wait for mirror recovery to complete.
4. After confirming the completion of mirror recovery, start the group.

- Method (3) Performing full copy by changing the group from the deactivated state to the active state

  With forcible mirror recovery using this method, the difference mirror recovery function is disabled, and full copy is performed instead.

  If the group is stopped during forcible mirror recovery, the group cannot be started until forcible mirror recovery is complete. In such a case, once forcible mirror recovery completion has been confirmed, the mirror disk can be used by starting the group.

  Note that, because forcible mirror recovery is performed concurrently while the group is active, the system load may be high.

  If the group contains two or more mirror disk or hybrid disk resources, these resources must all contain the latest data *on the same server*.

  1. While the group is not active, suspend the mirror disk monitor resource or the hybrid disk monitor resource being used to monitor a mirror disk resource or a hybrid disk resource.

     On each server, execute the command below.

     This causes auto-mirror recovery to be temporarily unavailable.

     ```
     clpmonctrl -s -m <relevant_monitor_resource_name (example: mdw1)>
     ```

     (To suspend a monitor resource by using Cluster WebUI instead of the command, click the relevant mirror disk monitor resource or hybrid disk monitor resource, and then execute **Suspend monitor**. In the confirmation window, select **Suspend**. The monitor will enter the "suspended" state.)

  2. **On the server holding the latest data,** execute the clpmdctrl or clphdctrl command to change the mirror disk status of the relevant server to the latest status.

     (Do not specify the latest data holding server name in the command argument.)

     For mirror disk

```
clpmdctrl --force <mirror_disk_resource_name (Example: md1)>
```

For hybrid disk

```
clphdctrl --force <hybrid_disk_resource_name (Example: hd1)>
```

3. Confirm that the relevant mirror disk resource and hybrid disk resource have entered the latest status (Normal) by using the Cluster WebUI, clpmdstat command, or clphdstat command.
   After confirming the status, start the relevant group **on the server holding the latest data** using the clpgrp command or Cluster WebUI.
4. Upon the completion of group start, execute the clpmdctrl or clphdctrl command to start full copy.
   (specify the name of the server containing the latest data and the resource name for command arguments.)

   For mirror disk :

```
clpmdctrl --force <server_containing_the_latest_data> <mirror_disk_resource_
↪name (Example: md1)>
```

   For hybrid disk :

```
clphdctrl --force <server_containing_the_latest_data> <hybrid_disk_resource_
↪name (Example: hd1)>
```

5. When you start mirror recovery with the command, the command will return control immediately.
   Then, return the suspended monitor resource to its original state.
   On each server, execute the following command.

```
clpmonctrl -s -m <relevant_monitor_resource_name (example: mdw1)>
```

   (To resume a monitor resource by using Cluster WebUI instead of the command, click the relevant mirror disk monitor resource or hybrid disk monitor resource, and then execute **Resume monitor**. In the confirmation window, select **Resume**.)

- Method (4) Using auto mirror recovery and difference mirror recovery
  If difference mirror recovery is possible, perform recovery using the difference information.
  Since mirror recovery is performed while the group is activated, the system load may be high.
  If the group contains two or more mirror disk resources or hybrid disk resources, these resources all need to hold the latest data **on the same server**.

  1. **On the server holding the latest data,** execute the clpmdctrl or clphdctrl command to change the mirror disk status of the relevant server to the latest status.
     (Do not specify the latest data holding server name in the command argument.)

     For mirror disk

```
clpmdctrl --force <mirror_disk_resource_name (Example: md1)>
```

     For hybrid disk

```
clphdctrl --force <hybrid_disk_resource_name (Example: hd1)>
```

  2. When the group is not active, confirm that the relevant mirror disk resource and hybrid disk resource have entered the latest status (Normal) by using the Cluster WebUI, clpmdstat command, or clphdstat command.
     After confirming the status, start the relevant group **on the server holding the latest data** using the clpgrp command or Cluster WebUI.

3. When the group is not active, auto mirror recovery starts after the relevant group starts (after activation).
   When the group is active, auto mirror recovery starts after the operation in 1.
   If auto mirror recovery is not started because, for example, **Auto Mirror Recovery** is cleared, use the clpmdctrl or clphdctrl command or Cluster WebUI to start mirror recovery manually.

   For mirror disk

```
clpmdctrl --recovery <mirror_disk_resource_name (Example: md1)>
```

   For hybrid disk

```
clphdctrl --recovery <hybrid_disk_resource_name (Example: hd1)>
```

The clpmdctrl or clphdctrl command immediately returns control once mirror recovery starts. For information on how to check the mirror recovery progress, see "Checking the mirror recovery progress with a command" and "Checking the mirror recovery progress from the Cluster WebUI".

9.1.21 Running the forcible mirror recovery with a command only on one server

In some cases, you cannot start one of the servers due to a hardware or OS failure, and the server that can be started may not have the latest data. If you want to start applications at least on the server that can be started, you can perform the forcible mirror recovery on that server.

However, remember that if you do this, the data on the server where you run this command becomes the latest data no matter which server actually has it. Therefore, even if you are able to start the other server later, you cannot handle the data in that server as the latest one. Make sure you understand the consequence before running the following command.

Run the following command to start the forcible mirror recovery:

For mirror disk:

```
clpmdctrl --force <mirror_disk_resource_name (Example: md1)>
```

For hybrid disk:

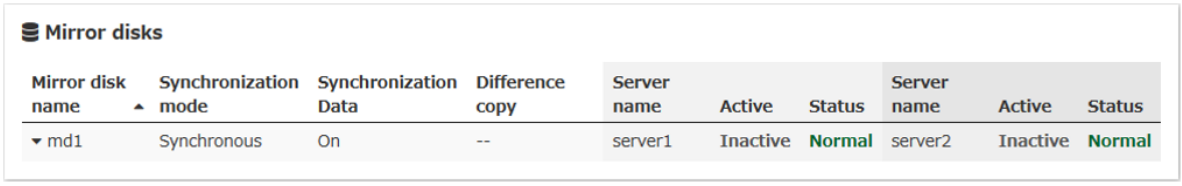
```
clphdctrl --force <hybrid_disk_resource_name (Example: hd1)>
```

After running the command, you can activate the groups and use the mirror disks or hybrid disks.

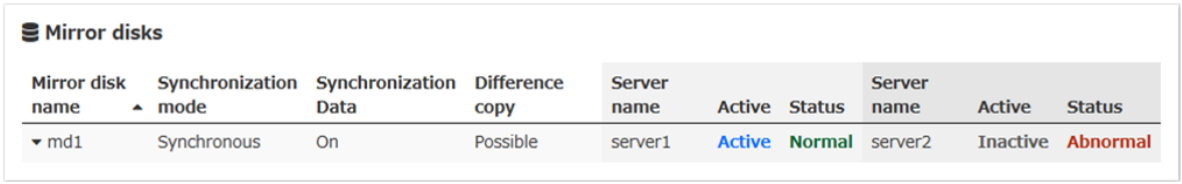
9.1.22 Checking the mirror break status from the Cluster WebUI

You can see the mirror break status by using the Cluster WebUI.
(The following is an example of mirror disk resource. What the statuses mean and description are the same for hybrid disk resources, although the screen display is different.)

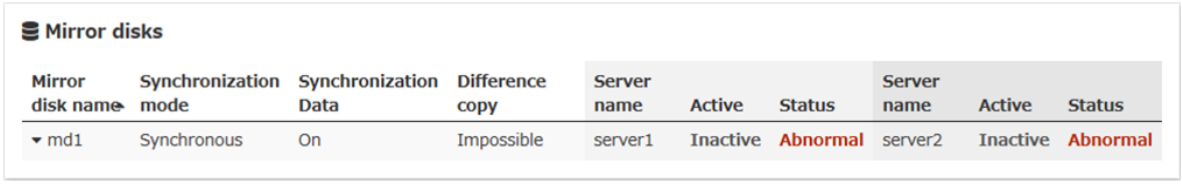
- When normal:



- When mirror recovery is required:



- When forcible mirror recovery is required:



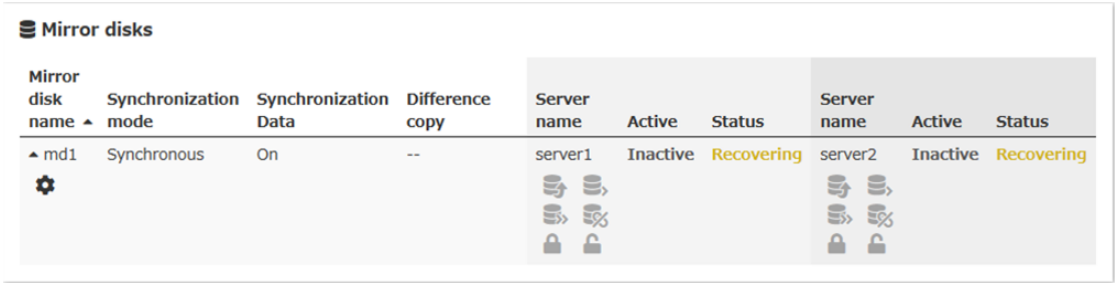
- While mirror recovery is in progress:

See "*Checking the mirror recovery progress from the Cluster WebUI*".

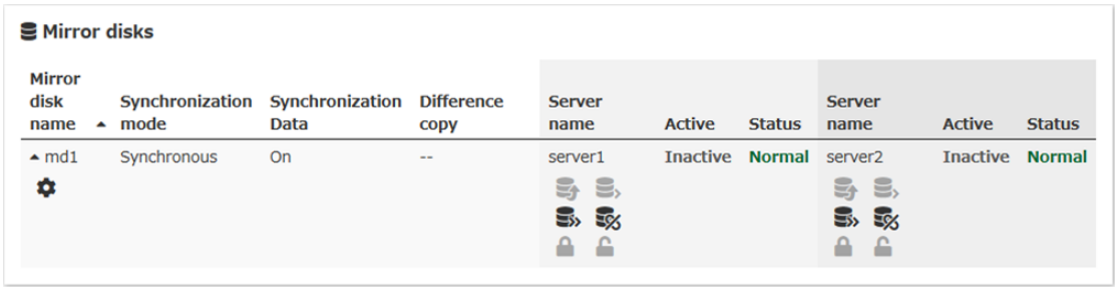
9.1.23 Checking the mirror recovery progress from the Cluster WebUI

Click **Mirror disks** tab on the Cluster WebUI to view the mirror recovery progress. (The following is an example of mirror disk resource. What the statuses mean and description are the same for hybrid disk resources, although the screen display is different.)

You will see the following screen during the mirror recovery.



You will see the following screen when the mirror recovery is successfully completed.



9.1.24 Recovering mirror using the Cluster WebUI

Click **Mirror disks** tab of the ClusterWebUI and display the detailed data of the mirror disk resources you want to start mirror recovery. For information on the **Mirror disks** tab, see the online manual of the Cluster WebUI.

For information on how to check the mirror recovery progress, see "*Checking the mirror recovery progress with a command*" and "*Checking the mirror recovery progress from the Cluster WebUI*".

9.1.25 Running the forcible mirror recovery using the Cluster WebUI

When EXPRESSCLUSTER cannot determine which server has the latest data, you have to perform the forcible mirror recovery.

In this case, you have to manually identify the server which holds the latest data, and perform the forcible mirror recovery.

Identify the server that has the latest data by any of the following methods:

- Using Cluster WebUI
  1. On the screen of the **Mirror disks** tab of the Cluster WebUI, display the detailed data of the mirror disk resources you want to see.
  2. Click **Details** icon.
  3. See the last update time stamp (Last Data Updated Time) to identify the server which has the latest data. However, this Last Data Updated Time depends on the operating system's clock.
- Using the clpmdstat command or clphdstat command

  Confirm method is the same as Cluster WebUI except that you use a command.
  1. Run the following command:

     For mirror disk:

     ```
     clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>
     ```

     For hybrid disk:

     ```
     clphdstat --mirror <hybrid_disk_resource_name (Example: hd1)>
     ```
  2. See the last update time stamp (Last Data Updated Time) to identify the server which contains the latest data. However, this Last Data Updated Time depends on the operating system's clock.
- Using data on mirror disks
  This is not recommended because the data may be corrupted destroyed if anything goes wrong in the procedure.
  Perform the following steps on both servers to identify which has the latest data.
  1. Confirm that all groups are inactive.
  2. See "*Forcibly mounting mirror disk when mirroring is not available*".
  3. Logically examine the data on the mount point.
  4. Unmount the data partition.

When you have identified the server containing the latest data, start the forcible mirror recovery from the **Mirror disks** tab of the Cluster WebUI. For information on the **Mirror disks** tab, see the online manual of the Cluster WebUI.

Start forcible mirror recovery using any of the following methods:

- Method (1) Using full-scale copy

Forcible mirror recovery by this method disables the difference mirror recovery function and instead uses full-scale copy.

Note that the group cannot be started until forcible mirror recovery is complete. Once forcible mirror recovery completion has been confirmed, the mirror disk can be used by starting the group.

1. In the **Mirror disks** tab, select **Full copy** icon to execute full-scale copy from the server holding the latest data to the copy destination server and then start mirror recovery.

   (When the group has already been started, **Full copy** icon cannot be selected from the **Mirror disks**. In this case, stop the group, or perform forcible mirror recovery with the relevant command.)

2. After confirming the completion of mirror recovery, start the group.

- Method (2) Using auto mirror recovery and difference mirror recovery

  If difference mirror recovery is possible, perform recovery using the difference information. The mirror recovery takes less time than when the forcible mirror recovery is performed (FastSync technology).

  Because mirror recovery is performed while the group is activated, the system load may be high.

  If the group contains two or more mirror disk resources or hybrid disk resources, these resources all need to hold the latest data **on the same server**.

  1. In the **Mirror disks** tab, select **Mirror recovery** icon to change the mirror disk status of **the server holding the latest data** from Abnormal to Normal.

     (When the group has already been started, this **Mirror recovery** operation cannot be executed from the **Mirror disks**. In this case, stop the group, or perform forcible mirror recovery with the relevant command.)

  2. Confirm that the relevant mirror disk resource and hybrid disk resource have entered the latest status (Normal).

     After confirming the status, start the relevant group **on the server holding the latest data**.

  3. After the relevant group starts (after activation), auto mirror recovery starts.

     If difference mirror recovery is possible, it is performed.

     If difference mirror recovery is impossible, full-scale copy is performed.

     If auto mirror recovery is not started such as the auto mirror recovery is OFF, start the mirror recovery manually from the **Mirror disks**.

For information on how to check the forcible mirror recovery progress, see "*Checking the mirror recovery progress with a command*" and "*Checking the mirror recovery progress from the Cluster WebUI*".

9.1.26 Running the forcible mirror recovery from the Cluster WebUI only on one Server

In some cases, you cannot start one of the servers due to a hardware or OS failure, and the server that can be started may not have the latest data.

If you want to start applications at least on the server that can be started, you can perform the forcible mirror recovery on that server.

However, remember that if you do this, the data on the server where you run this command becomes the latest data regardless of which server actually contains the data. Therefore, even if the other server becomes available later, you cannot handle the data in that server as the latest one. Make sure you understand the consequence before running the following command.

Start the forcible mirror recovery from the **Mirror disks** tab of Cluster WebUI. For information on the **Mirror disks** tab of the Cluster WebUI, seethe online manual of the Cluster WebUI.

When the forcible mirror recovery is successfully completed, you can activate the groups and use the mirror disks.

9.1.27 Changing current server on hybrid disk

Conditions in which current server can be changed is as follows:

Hybrid disk status		Whether or not current server can be changed	
Server group 1	Server group 2	Server group 1	Server group 2
error/deactivated	error/deactivated	Yes	Yes
normal/deactivated	error/deactivated	Yes	Yes
error/deactivated	normal/deactivated	Yes	Yes
normal/deactivated	normal/deactivated	Yes	Yes
normal/activated	error/deactivated	No	Yes
error/deactivated	normal/activated	Yes	No
normal/activated	normal/deactivated	No	No
pending/deactivated	pending/deactivated	Yes	Yes

9.1.28 Changing current server with a command

Run the following command on the server which you want to make current server to change the current server of hybrid disk.

```
clphdctrl --setcur <hybrid_disk_resource_name(Example:hd1)>
```

9.1.29 Changing current server with Cluster WebUI

For information on the Mirror disks tab of Cluster WebUI, see the online manual of the Cluster WebUI.

9.2 Troubleshooting problems with VERITAS volume manager

This section describes how to handle trouble when using VERITAS volume manager.

9.2.1 Modifying the VERITAS volume manager configuration

Whether or not the OS needs to be restarted determines the steps for changing the VERITAS Volume Manager configuration.

- If the OS does not need to be restarted when changing the configuration, see "When the OS does not need to be restarted to change the configuration of VERITAS Volume Manager".
- If the OS needs to be restarted when changing the configuration, see "When restart of the OS is necessary to change the configuration of VERITAS Volume Manager".

When the OS does not need to be restarted to change the configuration of VERITAS Volume Manager

1. Connect to the Cluster WebUI with a management IP address. If you do not have any management IP address, connect to it by using the actual IP address of any server.
2. On the Cluster WebUI, click **Stop Cluster** icon.
3. Change the configuration of VERITAS Volume Manager.
4. Change the settings of the resource in the **Config mode** of Cluster WebUI.
5. Upload the cluster configuration data in the **Config mode** of Cluster WebUI.

6. In the **Operation mode** of Cluster WebUI, click **Start Cluster** icon.

The settings will be effective.

When restart of the OS is necessary to change the configuration of VERITAS Volume Manager

1. Back up the cluster configuration data. Choose Step A or B depending on the type of OS that uses the Cluster WebUI.
   - Run the command below to make a backup of the Cluster WebUI which operates on the Web browser of Linux.

```
clpcfctrl --pull -l -x <path of configuration data file>
```

   - Run the command below to make a backup of the Cluster WebUI which operates on the Web browser of Windows.

```
clpcfctrl --pull -w -x <path of configuration data file>
```

   For information on troubleshooting clpcfctrl problems, see "*Changing, backing up, and checking cluster configuration data (clpcfctrl command)*" in "8.2. *EXPRESSCLUSTER commands*" in this guide.

2. Set the EXPRESSCLUSTER services not to start on all servers.

   For systemd environment:

```
clpsvcctrl.sh --disable core
```

3. Stop the EXPRESSCLUSTER daemon.

```
clpcl -t -a
```

4. Change the configuration of VERITAS Volume Manager, and restart the OS.
5. Change the settings of resources in the **Config mode** of Cluster WebUI.
6. Upload the cluster configuration data in the **Config mode** of Cluster WebUI.
7. Set the EXPRESSCLUSTER services to start on all servers.

```
clpsvcctrl.sh --enable core
```

8. Restart all servers.

The services will be effective next time the OS is started.

9.2.2 Operations of EXPRESSCLUSTER when VERITAS volume manager fails

See procedures in "To change the cluster configuration data," if you do not wish to failover groups or the final action to take place when a problem occurs in VERITAS Volume Manager and an error is detected in the disk resource and/or VxVM volume manager resource.

See procedures in "Restoring the cluster configuration information," if you wish to recover from a VERITAS Volume Manager error and to establish control again by using the EXPRESSCLUSTER.

To change the cluster configuration data

1. Start all servers at run level 1.
2. Set the EXPRESSCLUSTER services not to start on all servers

```
clpsvcctrl.sh --disable core
```

3. Restart all servers.
4. Make a backup of the cluster configuration data. Choose Step A or B depending on the type of OS that uses the Cluster WebUI.
   - Run the command shown below to make a backup of the Cluster WebUI which operates on the Web browser of Linux.

     ```
     clpcfctrl --pull -l -x <path of configuration data file>
     ```

   - Run the command below to make a backup of the Cluster WebUI which operates on the Web browser of Windows.

     ```
     clpcfctrl --pull -w -x <path of configuration data file>
     ```

   For information on troubleshooting clpcfctrl problems, see "*Changing, backing up, and checking cluster configuration data (clpcfctrl command)*" in "8.2. *EXPRESSCLUSTER commands*" in this guide.
5. Change the settings of resources in the **Config mode** of Cluster WebUI.
   - disk resource
   - VxVM volume manager resource

     For these group resources, make the following settings on the **Recovery operation** tab of the **Resource Properties** window:

     – Recovery operation at activation failure
       Retry Count at Activation Failure 0 time
       Failover Threshold 0 time
       Final Action No Operation (Next Resource Are Activated)

     – Recovery operation at deactivation failure
       Retry Count at Deactivation Failure 0 time
       Final Action No Operation (Next Resource Are Deactivated)
   - VxVM volume manager monitor resource
   - disk monitor resource

     For these monitor resources, make the following settings on the **Recovery Action** tab of the **Monitor Resources Properties** window:

     – Error Detection
       Recovery Action Execute only the final action
       Final Action No Operation
6. Upload the cluster configuration data in the **Config mode** of Cluster WebUI.
7. Set the EXPRESSCLUSTER services to start on all servers.

   ```
   clpsvcctrl.sh --enable core
   ```

8. Restart all servers.

The services will be effective next time the OS is started.

Restoring the cluster configuration information

1. Stop the EXPRESSCLUSTER daemon using the command shown below if the EXPRESSCLUSTER daemon is running.

```
clpcl -t -a
```

2. Load the configuration information created in Step 5 of "To change the cluster configuration data" to the server. Choose Step A or B depending on the version of the configuration data that you backed up.
   - Run the command below to use the configuration data that you backed up for Linux.

```
clpcfctrl --push -l -x <path of configuration data file>
```

   - Run the command below to use the configuration data that you backed up for Windows.

```
clpcfctrl --push -w -x <path of configuration data file>
```

   For information on troubleshooting clpcfctrl problems, see "*Changing, backing up, and checking cluster configuration data (clpcfctrl command)*" in "8.2. *EXPRESSCLUSTER commands*" in this guide.

The setting will be effective next time the EXPRESSCLUSTER daemon is activated.

9.3 To confirm the progress of the fsck / xfs_repair command

Fsck or xfs_repair carried out when activating a disk resource, a mirror disk resource and a hybrid disk resource may needs long time by completion by the size of the partition and the state of the file system.

It's possible to refer to the following logfile for progress of the fsck or xfs_repair command a disk resource, a mirror disk resource and a hybrid disk resource issued and check it:

Resource type	Log file
Disk resource	disk_fsck.log.cur
Mirror disk resource	md_fsck.log.cur
Hybrid disk resource	hd_fsck.log.cur

CHAPTER

TEN

ERROR MESSAGES

This chapter provides information on error messages you might encounter in operating EXPRESSCLUSTER.

This chapter covers:

- 10.1. *Messages*
- 10.2. *Messages reported by syslog, alert, mail, and SNMP trap*
- 10.3. *Driver syslog messages*
- 10.4. *Detailed information in activating and deactivating group resources*
- 10.5. *Detailed info of monitor resource errors*
- 10.6. *JVM monitor resource log output messages*

10.1 Messages

EXPRESSCLUSTER X 4.2 does not support event log (syslog) monitoring of NEC ESMPRO Agent.

EXPRESSCLUSTER X 4.2 does not notify events occurring on EXPRESSCLUSTER to NEC Express Report Service.

10.2 Messages reported by syslog, alert, mail, and SNMP trap

If the "o" mark is shown in the alert column or the syslog column, the message on that row is output to the Alert logs of the Cluster WebUI or syslog of OS, respectively.

If the "o" mark is shown in the mail column, the message on that row is reported when E-mail report function of Alert Service is enabled.

If the "o" mark is shown in the SNMP Trap column, the message on that row is reported when SNMP trap sending function of Alert Service is enabled.

For details of E-mail report and SNMP trapsending, see "*Alert Service tab*" in "*2. Parameter details*" and "*Alert Service*" in "*Information on other settings*".

Note: facility = daemon (0x00000018), identity = "expresscls" are displayed on syslogs. The "Event type" on the following list is the log level of the syslog.

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
pm	Info	1	Starting the cluster daemon...	The EXPRESSCLUSTER daemon has started normally.	-	o	o		
pm	Info	2	Shutting down the cluster daemon...	The EXPRESSCLUSTER daemon is stopping.	-	o	o		
pm	Info	3	Shutdown monitoring is started...	Shutdown monitoring has started.	-	o	o		
pm	Error	10	The cluster daemon has already started.	The EXPRESSCLUSTER daemon has already started.	Check the status of the EXPRESSCLUSTER daemon.	o	o		
pm	Error	11	A critical error occurred in the cluster daemon.	A critical error has occurred in the EXPRESSCLUSTER daemon.	Check the following possible causes: the execution user has no root permission, there is a memory shortage, or OS resources are insufficient.	o	o	o	o
pm	Error	12	A problem was detected in XML library.	A problem was detected in the XML library.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
pm	Error	13	A problem was detected in cluster configuration data.	A problem was detected in the cluster configuration data.	Using the Cluster WebUI, check the cluster configuration data.	o	o	o	o
pm	Error	14	No cluster configuration data is found.	There is no cluster configuration data.	Create the cluster configuration with the Cluster WebUI and upload it to all servers in the cluster.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
pm	Error	15	No information about this server is found in the cluster configuration data.	Information about the local server is not found in the cluster configuration data.	Using the Cluster WebUI, check the cluster configuration data.	o	o		
pm	Error	20	Process %1 was terminated abnormally.	Process %1 was terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o	o	o
pm	Error	21	The system will be stopped because the cluster daemon process terminated abnormally.	The system will stop because the EXPRESSCLUSTER daemon process terminated abnormally.	Deactivation of the group resource may fail. Take appropriate action according to the group resource message.	o	o		
pm	Error	22	An error occurred when initializing process %1.(return code:%2)	An error occurred in initializing process %1.	The event process may not yet have been started. See "*Troubleshooting*".	o	o	o	o
pm	Info	23	The system will be stopped.	The system will be stopped.	-	o	o		
pm	Info	24	The cluster daemon will be stopped.	The EXPRESSCLUSTER daemon will be stopped.	-	o	o		
pm	Info	25	The system will be rebooted.	The system will be rebooted.	-	o	o		
pm	Info	26	Process %1 will be restarted.	Process %1 will be restarted.	-	o	o		
pm	Info	30	Received a request to stop the system from %1.	A system stop request was received from %1.	-	o	o		
pm	Info	31	Received a request to stop the cluster daemon from %1.	An EXPRESSCLUSTER daemon stop request was received from %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
pm	Info	32	Received a request to reboot the system from %1.	A system reboot request was received from %1.	-	o	o		
pm	Info	33	Received a request to restart the cluster daemon from %1.	An EXPRESSCLUSTER daemon reboot request was received from %1.	-	o	o		
pm	Info	34	Received a request to resume the cluster daemon from %1.	A cluster resume request was received from %1.	-	o	o		
pm	Info	35	Received a request to suspend the cluster daemon from %1.	A cluster suspend request was received from %1.	-	o	o		
pm	Info	36	Received a request to panic by sysrq from %1.	A panic request by sysrq was received from %1.	-	o	o		
pm	Info	37	Received a request to reset by keepalive driver from %1.	A reset request by the keepalive driver was received from %1.	-	o	o		
pm	Info	38	Received a request to panic by keepalive driver from %1.	A panic request by the keepalive driver was received from %1.	-	o	o		
pm	Info	39	Received a request to reset by BMC from %1.	A reset request by BMC was received from %1.	-	o	o		
pm	Info	40	Received a request to power down by BMC from %1.	A power down request by BMC was received from %1.	-	o	o		
pm	Info	41	Received a request to power cycle by BMC from %1.	A power cycle request by BMC was received from %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
pm	Info	42	Received a request to send NMI by BMC from %1.	An NMI send request by BMC was received from %1.	-	o	o		
pm	Error	43	Received a request to send IO Fencing by ACPI driver from %1.	An IO Fencing send request by ACPI driver was received from %1.		o	o		
pm	Error	66	An attempt to panic by sysrq from %1 failed.	An attempt was made to cause a panic by sysrq from %1, but failed.	Check whether the system is configured so that it can use sysrq.	o	o		
pm	Error	67	An attempt to reset by keepalive driver from %1 failed.	An attempt was made to cause a reset by the keepalive driver from %1, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
pm	Error	68	An attempt to panic by keepalive driver from %1 failed.	An attempt was made to cause a panic by the keepalive driver from %1, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
pm	Error	69	An attempt to reset by BMC from %1 failed.	An attempt was made to cause a reset by BMC from %1, but failed.	Check whether the ipmitool command can be used.	o	o		
pm	Error	70	An attempt to power down by BMC from %1 failed.	An attempt was made to cause power down by BMC from %1, but failed.	Check whether the ipmitool command can be used.	o	o		
pm	Error	71	An attempt to power cycle by BMC from %1 failed.	An attempt was made to cause a power cycle by BMC from %1, but failed.	Check whether the ipmitool command can be used.	o	o		
pm	Error	72	An attempt to send NMI by BMC from %1 failed.	An attempt was made to perform an NMI transmission by BMC from %1, but failed.	Check whether the ipmitool command can be used.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
pm	Error	73	An attempt to send IO Fencing by ACPI driver from %1 failed.	An attempt was made to perform I/O fencing with the ACPI driver from %1, but failed.	Confirm whether the ACPI driver for EXPRESSCLUSTER linkage is available.	o	o		
pm	Info	100	The system will be panic by sysrq.	The system will be panicked by sysrq.	-	o	o		
pm	Info	101	The system will be reset by ka.	The system will be reset by the keep alive driver.	-	o	o		
pm	Info	102	The system will be panic by ka.	The system will be panicked by the keep alive driver.	-	o	o		
pm	Info	103	The system will be reset by bmc.	The system will be reset by BMC.	-	o	o		
pm	Info	104	The system will be off by bmc.	The system will be turned OFF by BMC.	-	o	o		
pm	Info	105	The system will be cycle by bmc.	The system will be turned OFF and then back ON by BMC.	-	o	o		
pm	Info	106	The system will be nmi by bmc.	The system will be NMI-transmitted by BMC.	-	o	o		
pm	Info	107	The system will be iofencing.	The system will be subject to I/O fencing.	-	o	o		
nm	Info	1	Server %1 has started.	Server %1 has started.	-	o	o		
nm	Info	2	Server %1 has been stopped.	Server %1 has stopped.	-	o	o	o	o
nm	Info	3	Resource %1 of server %2 has started.	Resource %1 of server %2 has started.	-	o	o		
nm	Info	4	Resource %1 of server %2 has stopped.	Resource %1 of server %2 has stopped.	-	o	o		
nm	Info	5	Waiting for all servers to start.	Waiting for all servers to start has started.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Info	6	All servers have started.	All servers have started.	-	o	o		
nm	Info	7	Timeout occurred during the wait for startup of all servers.	Waiting for all servers to start has timed out.	-	o	o		
nm	Error	8	Timeout occurred during the wait for startup of all servers. (Cannot communicate with some servers.)	Waiting for all servers to start has timed out. (Internal communication with some servers is impossible.)	Check whether there is a network adaptor error and that the network is connected properly.	o	o		
nm	Info	9	Waiting for startup of all servers has been canceled.	Waiting for servers to start has been canceled.	-	o	o		
nm	Error	10	Status of resource %1 of server %2 is unknown.	The status of resource %1 of server %2 is unknown.	Check that cable for resource %1 and the network are set correctly.	o	o	o	o
nm	Error	20	Process %1 was terminated abnormally.	Process %1 was terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o	o	o
nm	Info	21	The system will be stopped.	The system will be stopped.	-	o	o		
nm	Info	22	The cluster daemon will be stopped.	The EXPRESSCLUSTER daemon will be stopped.	-	o	o		
nm	Info	23	The system will be rebooted.	The system will be rebooted.	-	o	o		
nm	Info	24	Process %1 will be restarted.	Process %1 will be restarted.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Error	30	Network partition was detected. Shut down the server %1 to protect data.	A network partition was detected. Server %1 is shut down to protect the data.	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		
nm	Error	31	An error occurred while confirming the network partition. Shut down the server %1.	A problem occurred while the network partition was being checked. Server %1 is shut down to protect data.	Check whether there is an error in the network partition resolution resource.	o	o		
nm	Error	32	Shut down the server %1. (reason:%2)	Server %1 is shut down. (Reason: %2)	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Error	33	Cluster service will be stopped. (reason:%1)	The cluster service will be stopped. (Reason: %1)	Remove the factor indicated in "reason".	o	o		
nm	Error	34	The combination of the network partition resources is invalid. (server name:%1)	The combination of the network partition resolution resources is invalid. (Server name: %1)	Check the cluster configuration data.	o	o		
nm	Error	35	Failed to start the resource %1. Server name:%2	Resource %1 failed to start. (Server name: %2)	Check whether there is an error in the network partition resolution resource.	o	o		
nm	Info	36	The network partition %1 of the server %2 has been recovered to the normal status.	Network partition %1 of server %2 has been recovered to the normal status.	-	o	o		
nm	Error	37	The network partition %1 of the server %2 has an error.	Network partition %1 of server %2 is abnormal.	Check whether there is an error in the network partition resolution resource.	o	o		
nm	Error	38	The resource %1 of the server %2 is unknown.	Resource %1 of server %2 is unknown.	Check the cluster configuration data.	o	o		
nm	Info	39	The server %1 cancelled the pending failover.	Server %1 canceled the failover.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Error	40	Network partition was detected. Stop the cluster service on the server %1 to protect data.	A network partition was detected. The cluster service of server %1 is stopped to protect the data.	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		
nm	Error	41	An error occurred while confirming the network partition. Stop the cluster service on the server %1.	A problem occurred while the network partition was being checked. The cluster service of server %1 is stopped to protect data.	Check whether there is an error in the network partition resolution resource.	o	o		
nm	Error	42	Network partition was detected. Reboot the cluster service on the server %1 to protect data.	A network partition was detected. Server %1 is reboot to protect the data.	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Error	43	Network partition was detected. Execute action(%1) on the server %2 to protect data.	A network partition was detected. Execute action(%1) on the server %2 to protect data.	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		
nm	Error	44	An error occurred while confirming the network partition. Reboot the server %1.	A problem occurred while the network partition was being checked. Server %1 is reboot to protect data.	Check whether there is an error in the network partition resolution resource.	o	o		
nm	Error	45	An error occurred while confirming the network partition. Execute action(%1) on the server %2.	A problem occurred while the network partition was being checked. Execute action(%1) on the server %2.	Check whether there is an error in the network partition resolution resource.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Error	46	Reboot the server %1. (reason:%2)	Server %1 is reboot. (Reason: %2)	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		
nm	Error	47	Execute action(%1) on the server %2. (reason:%3)	Execute action(%1) on the server %2. (reason:%3)	All heartbeats cannot be used. Check whether there is a network adaptor error and that the network is connected properly. Check the status of the shared disk if DISKHB is in use. Check that the COM cable is properly connected if COMHB is in use.	o	o		
nm	Error	80	Cannot communicate with server %1.	Internal communication with server %1 is impossible.	Check whether there is a network adaptor error and that the network is connected properly.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
nm	Info	81	Recovered from internal communication error with server %1.	Internal communication with server %1 has been recovered from the abnormal status.	-	o	o		
rc	Info	10	Activating group %1 has started.	Activating group %1 has started.	-	o	o		
rc	Info	11	Activating group %1 has completed.	Activating group %1 has been completed.	-	o	o		
rc	Error	12	Activating group %1 has failed.	Activating group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Info	15	Waiting for group %1 to start has started.	Waiting for the group to start has started.	-	o	o		
rc	Info	16	Waiting for group %1 to start has been completed.	Waiting for the group to start has been normally completed.	-	o	o		
rc	Error	17	Group start has been cancelled because waiting for group %1 to start has timed out.	Waiting for the group to start has timed out.	Check the status of the group waiting to start. If the group has not yet been started, re-perform the group operation after starting that group.	o	o		
rc	Warning	18	Waiting for group %1 to start has timed out. However, group start continues.	Waiting for the group to start has timed out. However, group start continues.	-	o	o		
rc	Info	20	Stopping group %1 has started.	Stopping group %1 has started.	-	o	o		
rc	Info	21	Stopping group %1 has completed.	Stopping group %1 has been completed.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	22	Stopping group %1 has failed.	Stopping group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Warning	23	Server %1 is not in a condition to start group %2.	Server %1 cannot start group %2.	A server on which an absolute exclusion group has already started cannot start another absolute exclusion group. Stop the existing absolute exclusion group and then reexecute.	o	o		
rc	Info	25	Waiting for group %1 to stop has started.	Waiting for the group to stop has started.	-	o	o		
rc	Info	26	Waiting for group %1 to stop has been completed.	Waiting for the dependent group to stop has been normally completed.	-	o	o		
rc	Error	27	Group stop has been cancelled because waiting for group %1 to stop has timed out.	Waiting for the group to stop has timed out.	Check the status of the group waiting to stop. If the group has not yet been stopped, re-perform the group operation after stopping that group.	o	o		
rc	Warning	28	Waiting for group %1 to stop has timed out. However, group stop continues.	Stop waiting has timed out. However, group stop continues.	-	o	o		
rc	Info	30	Activating %1 resource has started.	Activating resource %1 has started.	-		o		
rc	Info	31	Activating %1 resource has completed.	Activating resource %1 has been completed.	-		o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	32	Activating %1 resource has failed.(%2 : %3)	Activating resource %1 has failed.	See "*Detailed information in activating and deactivating group resources*". If a stall occurs during start processing, "Activating %1 resource has failed.(99 : command is timeout)" is output.	o	o	o	o
rc	Info	33	A request to activate %1 resource on server %2 has been started.	A request to activate resource %1 on server %2 has been started.	-	o	o		
rc	Info	34	A request to activate %1 resource on server %2 has been completed.	A request to activate resource %1 on server %2 has been completed.	-	o	o		
rc	Error	35	A request to activate %1 resource on server %2 has been failed.	A request to activate resource %1 on server %2 has been failed.	Check if there is a network error or there is an error with the remote server.	o	o		
rc	Info	40	Stopping %1 resource has started.	Stopping resource %1 has started.	-		o		
rc	Info	41	Stopping %1 resource has completed.	Stopping resource %1 has been completed.	-		o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	42	Stopping %1 resource has failed.(%2 : %3)	Stopping resource %1 has failed.	See "*Detailed information in activating and deactivating group resources*". If a stall occurs during stop processing, "Stopping %1 resource has failed.(99 : command is timeout)" is output.	o	o	o	o
rc	Info	44	A request to stop %1 resource on server %2 has been started.	A request to stop resource %1 on server %2 has been started.	-	o	o		
rc	Info	45	A request to stop %1 resource on server %2 has been completed.	A request to stop resource %1 on server %2 has been completed.	-	o	o		
rc	Error	46	A request to stop %1 resource on server %2 has been failed.	A request to stop resource %1 on server %2 has been failed.	Check if there is a network error or there is an error with the remote server.	o	o		
rc	Info	50	Moving group %1 has started.	Moving group %1 has started.	-	o	o		
rc	Info	51	Moving group %1 has completed.	Moving group %1 has been completed.	-	o	o		
rc	Error	52	Moving group %1 has failed.	Moving group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Info	55	Migrating group %1 has started.	Migrating group %1 has started.	-	o	o		
rc	Info	56	Migrating group %1 has completed.	Migrating group %1 has been completed.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	57	Migrating group %1 has failed.	Migrating group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Warning	58	Server %1 is not in a condition to migrate group %2.	Server %1 cannot make group %2 migrate.	Check the status of the migration destination server. If no migration destination server exists, the server name is not output to %1.	o	o		
rc	Info	60	Failover group %1 has started.	Failover of group %1 has started.	-	o	o		
rc	Info	61	Failover group %1 has completed.	Failover of group %1 has been completed.	-	o	o		
rc	Error	62	Failover group %1 has failed.	Failover of group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Warning	63	Server %1 is not in a condition to move group %2.	Server %1 cannot move group %2.	Check the status of the movement destination server. If no movement destination server exists, the server name is not output to %1.	o	o		
rc	Info	64	Server %1 has been set as the destination for the group %2 (reason: %3).	Server %1 has been set as the failover destination of group %2. (Reason: %3)	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	65	There is no appropriate destination for the group %1 (reason: %2).	There is no appropriate failover destination for group %1. (Reason: %2)	There is no server that can provide failover. The server is stopping or a monitor resource error disabling failover is occurring. Start the server, remove the cause of the monitor resource error, or stop the monitor resource in which the error is detected.	o	o		
rc	Warning	66	Server %1 is not in a condition to start group %2 (reason: %3).	Server %1 cannot start group %2. (Reason: %2)	There is a monitor resource error that is disabling group start. Remove the cause of the monitor resource error, or stop the monitor resource in which the error is detected.	o	o		
rc	Info	67	Server %1 in the same server group (%2) has been set as the destination for the group %3.	Server %1 in the same server group %2 has been set as the failover destination of group %3.	-	o	o		
rc	Info	68	Server %1 not in the same server group (%2) has been set as the destination for the group %3.	Server %1 in a server group other than server group %2 has been set as the failover destination of group %3.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Warning	69	Can not failover the group %1 because there is no appropriate destination in the same server group %2.	Server group %2 does not contain the server that can perform failover for group %1.	Start the group after starting the server in the server group or start the group with the server in another server group.	o	o		
rc	Info	70	Restarting group %1 has started.	Reactivating group %1 has started.	-	o	o		
rc	Info	71	Restarting group %1 has completed.	Reactivating group %1 has been completed.	-	o	o		
rc	Error	72	Restarting group %1 has failed.	Reactivating group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Info	74	Failback group %1 has started.	Failback group %1 has started.	-	o	o		
rc	Info	75	Failback group %1 has completed.	Failback group %1 has been completed.	-	o	o		
rc	Error	76	Failback group %1 has failed.	Failback group %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Error	77	Failover some groups have failed since the server cannot communicate with some servers.	Failed to failover some groups because of no internal communication to some servers.	Check the status of LAN heartbeat and kernel mode LAN heartbeat. After recovering the internal communication, restart the group.	o	o		
rc	Info	80	Restarting resource %1 has started.	Reactivating resource %1 has started.	-	o	o		
rc	Info	81	Restarting resource %1 has completed.	Reactivating resource %1 has been completed.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	82	Restarting resource %1 has failed.	Reactivating resource %1 has failed.	Take appropriate action according to the group resource message.	o	o		
rc	Info	83	Starting a single resource %1.	Single resource %1 is started.	-	o	o		
rc	Info	84	A single resource %1 has been started.	Single resource %1 has been started.	-	o	o		
rc	Error	85	Failed to start a single resource %1.	Single resource %1 failed to start.	Take appropriate action according to the group resource message.	o	o		
rc	Warning	86	Server %1 is not in a condition to start a single resource %2.	Server %1 cannot start single source %2.	Check the server and group status.	o	o		
rc	Info	87	Stopping a single resource %1.	Single resource %1 is stopped.	-	o	o		
rc	Info	88	A single resource %1 has been stopped.	Single resource %1 has been stopped.	-	o	o		
rc	Error	89	Failed to stop a single resource %1.	Single resource %1 failed to stop.	Take appropriate action according to the group resource message.	o	o		
rc	Info	90	All the servers in the cluster were shut down.	The cluster has been stopped.	-	o	o		
rc	Info	91	The server was shut down.	The server has been stopped.	-	o	o		
rc	Error	92	Group %1 has started on more than one server.	Group %1 has started on two or more servers.	The server is automatically shut down. See "Recovery from network partitioning" in "The system maintenance information" in the "Maintenance Guide".	o	o	o	o

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Warning	100	Restart count exceeded the maximum value %1. Final action of resource %2 will not be executed.	The restart count exceeded the maximum value %1. The final action of resource %2 is not executed.	Take appropriate action according to the group resource message.	o	o		
rc	Info	121	The CPU frequency has been set to high.	The CPU clock level has been set to its highest value.	-	o	o		
rc	Info	122	The CPU frequency has been set to low.	The CPU clock level has been set to its lowest value.	-	o	o		
rc	Info	124	CPU frequency setting has been switched to automatic control by cluster.	The CPU clock setting has been switched to automatic control by the cluster.	-	o	o		
rc	Error	140	CPU frequency control cannot be used.	The CPU clock control function cannot be used.	Check the BIOS and kernel settings.	o	o		
rc	Error	141	Failed to set the CPU frequency to high.	The CPU clock level could not be set to the highest value.	Check the BIOS and kernel settings. Check whether the EXPRESSCLUSTER daemon is started. Check whether the setting to use the CPU clock control function is specified.	o	o		
rc	Error	142	Failed to set the CPU frequency to low.	The CPU clock level could not be set to the lowest value.	Same as above.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	144	Failed to switch the CPU frequency setting to automatic control by cluster.	The CPU clock setting could not be switched to automatic control by the cluster.	Check whether the EXPRESSCLUSTER daemon is started. Check whether the setting to use the CPU clock control function is specified.	o	o		
rc	Info	160	Script before final action upon %1 failure in resource %2 started.	The script (%1) before the final action at failure in resource (%2) has started.	-	o	o		
rc	Info	161	Script before final action upon %1 failure in resource %2 completed.	The script (%1) before the final action at failure in resource (%2) has been completed.	-	o	o		
rc	Info	162	Script %1 in resource %2 started	Script (%1) of resource (%2) has started.	-	o	o		
rc	Info	163	Script %1 in resource %2 completed	Script (%1) of resource (%2) has been completed.	-	o	o		
rc	Error	180	Script %1 before final action upon failure in resource %2 failed.	The script (%1) before the final action at failure in resource (%2) has failed.	Check the cause of the script failure and take appropriate action.	o	o		
rc	Error	181	Failed to execute script %1 in resource %2.(%3)	Script (%1) of resource (%2) has failed.	Same as above.	o	o		
rc	Info	200	Resource(%1) will be reactivated since activating resource(%2) failed.	Resource %2 is reactivated since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Info	201	Group(%1) will be moved to server(%2) since activating resource(%3) failed.	Group %1 is moved to server %2 since resource %3 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	202	Group(%1) will be stopped since activating resource(%2) failed.	Group %1 is stopped since resource %2 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	203	Cluster daemon will be stopped since activating resource(%1) failed.	The cluster daemon is stopped since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	204	System will be halted since activating resource(%1) failed.	The OS is shut down since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	205	System will be rebooted since activating resource(%1) failed.	The OS is rebooted since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	206	Activating group(%1) will be continued since failover process failed.	Activating group %1 is continued since the failover failed.	Take appropriate action according to the group resource message.	o	o		
rc	Info	220	Resource(%1) will be stopping again since stopping resource(%2) failed.	Deactivation of resource %1 is retried since resource %2 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	222	Group(%1) will be stopped since stopping resource(%2) failed.	Group %1 is stopped since resource %2 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	223	Cluster daemon will be stopped since stopping resource(%1) failed.	The cluster daemon is stopped since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Info	224	System will be halted since stopping resource(%1) failed.	The OS is stopped since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	225	System will be rebooted since stopping resource(%1) failed.	The OS is rebooted since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	240	System panic by sysrq is requested since activating resource(%1) failed.	A system panic by sysrq is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	241	System reset by keepalive driver is requested since activating resource(%1) failed.	A system reset by the keepalive driver is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	242	System panic by keepalive driver is requested since activating resource(%1) failed.	A system panic by the keepalive driver is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	243	System reset by BMC is requested since activating resource(%1) failed.	A system reset by BMC is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	244	System power down by BMC is requested since activating resource(%1) failed.	System power down by BMC is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Info	245	System power cycle by BMC is requested since activating resource(%1) failed.	A system power cycle by BMC is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	246	NMI send by BMC is requested since activating resource(%1) failed.	NMI transmission by BMC is requested since resource %1 could not be activated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	247	IO Fencing by ACPI driver is requested since activating resource(%1) failed.	I/O fencing with the ACPI driver was requested due to an activation failure in resource %1.	Take appropriate action according to the group resource message.	o	o		
rc	Error	260	An attempt to panic system by sysrq due to failure of resource(%1) activation failed.	An attempt was made to cause a system panic by sysrq due to an activation failure in resource %1, but failed.	Check whether the system is configured so that it can use sysrq.	o	o		
rc	Error	261	An attempt to reset system by keepalive driver due to failure of resource(%1) activation failed.	An attempt was made to cause a system reset by the keepalive driver due to an activation failure in resource %1, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
rc	Error	262	An attempt to panic system by keepalive driver due to failure of resource(%1) activation failed.	An attempt was made to cause a system panic by the keepalive driver due to an activation failure in resource %1, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	263	An attempt to reset system by BMC due to failure of resource(%1) activation failed.	An attempt was made to cause a system reset by BMC due to an activation failure in resource %1, but failed.	Check whether the ipmitoo command can be used.	o	o		
rc	Error	264	An attempt to power down system by BMC due to failure of resource(%1) activation failed.	An attempt was made to cause system power down by BMC due to an activation failure in resource %1, but failed.	Check whether the ipmitool command can be used.	o	o		
rc	Error	265	An attempt to power cycle system by BMC due to failure of resource(%1) activation failed.	An attempt was made to cause system power cycle by BMC due to an activation failure in resource %1, but failed.	Check whether the ipmitool command can be used.	o	o		
rc	Error	266	An attempt to send NMI by BMC due to failure of resource(%1) activation failed.	An attempt was made to perform NMI transmission by BMC due to an activation failure in resource %1, but failed.	Check whether the ipmitool command can be used.	o	o		
rc	Error	267	An attempt to IO Fencing by ACPI driver due to failure of resource(%1) activation failed.	An attempt was made to perform I/O fencing by the ACPI driver due to an activation failure in resource %1, but failed.	Confirm whether the ACPI driver for EXPRESSCLUSTER linkage is available.	o	o		
rc	Info	280	System panic by sysrq is requested since deactivating resource(%1) failed.	A system panic by sysrq is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Info	281	System reset by keepalive driver is requested since deactivating resource(%1) failed.	A system reset by the keepalive driver is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	282	System panic by keepalive driver is requested since deactivating resource(%1) failed.	A system panic by the keepalive driver is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	283	System reset by BMC is requested since deactivating resource(%1) failed.	A system reset by BMC is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	284	System power down by BMC is requested since deactivating resource(%1) failed.	System power down by BMC is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	285	System power cycle by BMC is requested since deactivating resource(%1) failed.	A system power cycle by BMC is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	286	Sending NMI by BMC is requested since deactivating resource(%1) failed.	NMI transmission by BMC is requested since resource %1 could not be deactivated.	Take appropriate action according to the group resource message.	o	o		
rc	Info	287	IO Fencing by ACPI driver is requested since deactivating resource(%1) failed.	I/O fencing is executed by using the ACPI driver due to an activation failure in resource %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	300	An attempt to panic system by sysrq due to failure of resource(%1) deactivation failed.	An attempt was made to cause a system panic by sysrq due to a deactivation failure in resource %1, but failed.	Check whether the system is configured so that it can use sysrq.	o	o		
rc	Error	301	An attempt to reset system by keepalive driver due to failure of resource(%1) deactivation failed.	An attempt was made to cause a system reset by the keepalive driver due to a deactivation failure in resource %1, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
rc	Error	302	An attempt to panic system by keepalive driver due to failure of resource(%1) deactivation failed.	An attempt was made to cause a system panic by the keepalive driver due to a deactivation failure in resource %1, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
rc	Error	303	An attempt to reset system by BMC due to failure of resource(%1) deactivation failed.	An attempt was made to cause a system reset by BMC due to a deactivation failure in resource %1, but failed.	Check whether the ipmitool command can be used.	o	o		
rc	Error	304	An attempt to power down system by BMC due to failure of resource(%1) deactivation failed.	An attempt was made to cause system power down by BMC due to an deactivation failure in resource %1, but failed.	Check whether the ipmitool command can be used.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	305	An attempt to power cycle system by BMC due to failure of resource(%1) deactivation failed.	An attempt was made to cause system power cycle by BMC due to a deactivation failure in resource %1, but failed.	Check whether the ipmitool command can be used.	o	o		
rc	Error	306	An attempt to send NMI by BMC due to failure of resource(%1) deactivation failed.	An attempt was made to perform NMI transmission by BMC due to a deactivation failure in resource %1, but failed.	Check whether the ipmitoo command can be used.	o	o		
rc	Error	307	An attempt to IO Fencing by ACPI driver due to failure of resource(%1) deactivation failed.	An attempt was made to perform I/O fencing by the ACPI driver due to an activation error in resource %1, but failed.	Confirm whether the ACPI driver for EXPRESSCLUSTER linkage is available.	o	o		
rc	Error	340	Group start has been cancelled because waiting for group %1 to start has failed.	An error has occurred while waiting for the group to start.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rc	Info	350	Group %1 started to check the double activation.	Checking the double activation started.	-				
rc	Info	351	Group %1 completed to check the double activation.	Checking the double activation ended.	-				
rc	Error	352	Group %1 failed to check the double activation.	Checking the double activation failed.	Check the status of the group.	o	o		
rc	Info	353	Waiting for group %1 to start for check the double activation.	Group start continues for check the double activation.	Check the status of the group.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Info	400	System power down by BMC is requested. (destination server : %1)	A system power down by BMC is requested. (Target server: %1)	-	o	o		
rc	Info	401	System power cycle by BMC is requested. (destination server : %1)	System power cycle by BMC is requested. (Target server: %1)	-	o	o		
rc	Info	402	System reset by BMC is requested. (destination server : %1)	A system reset by BMC is requested. (Target server: %1)	-	o	o		
rc	Info	403	Sending NMI by BMC is requested. (destination server : %1)	NMI transmission by BMC is requested. (Target server: %1)	-	o	o		
rc	Info	410	Forced stop of virtual machine is requested. (destination server : %s)	Forced stop of a virtual machine is requested. (Target server: %1)	-	o	o		
rc	Info	411	Script for forced stop has started.	Script for forced-stop has started.	-	o	o		
rc	Info	412	Script for forced stop has completed.	Script for forced-stop has completed.	-	o	o		
rc	Error	420	An attempt to power down system by BMC failed. (destination server : %1)	System power down by BMC is requested, but this request failed. (Target server: %1)	Check whether the ipmitool command can be used.	o	o		
rc	Error	421	An attempt to power cycle system by BMC failed. (destination server : %1)	System power cycle by BMC is requested, but this request failed. (Target server: %1)	Check whether the ipmitool command can be used.	o	o		
rc	Error	422	An attempt to reset system by BMC failed. (destination server : %1)	A system reset by BMC is requested, but this request failed. (Target server: %1)	Check whether the ipmitool command can be used.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Error	423	An attempt to send NMI by BMC failed. (destination server : %1)	NMI transmission by BMC is requested, but this request failed. (Target server: %1)	Check whether the ipmitool command can be used.	o	o		
rc	Error	430	An attempt to force stop virtual machine failed. (destination server : %s)	Forced stop of a virtual machine is requested, but this request failed. (Target server: %1)	Check whether VMware vSphere CLI can be used.	o	o		
rc	Error	431	Script for forced stop has failed. (%1)	Script for forced stop has failed. (%1)	Check the cause of the script failure and take measures.	o	o		
rc	Error	432	Script for forced stop has timed out.	Script for forced stop has timed out.	Check the cause of the timeout and take measures.	o	o		
rc	Warning	433	Group failover has been canceled because forced stop of server %1 failed.	Suppression of failover for forced stop failed	Check the cause of the forced stop failed and take measures.	o	o		
rc	Warning	441	Waiting for group %1 to stop has failed. However, group stop continues.	An error has occurred while waiting for the group to stop.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rc	Warning	500	Since there is no other normally running server, the final action for an activation error of group resource %1 was suppressed.	Suppression of final action for activation error.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Warning	501	Since there is no other normally running server, the final action for a deactivation error of group resource %1 was suppressed.	Suppression of final action for deactivation error.	-	o	o		
rc	Warning	502	Since server %1 is specified as that which suppresses shutdown at both-system activation detection, it ignored the shutdown request.	Suppression of shutdown caused by both-system activation detection.	-	o	o		
rc	Warning	503	A mismatch in the group %1 status occurs between the servers.	Generation of group status mismatch	Restart the group or reboot the cluster.	o	o		
rc	Info	504	Since server %1 is not specified as that which suppresses shutdown at both-system activation detection, it executed the shutdown request.	Since server %1 is not specified as that which suppresses shutdown at both-system activation detection, it executed the shutdown request.	-	o	o		
rc	Warning	510	Cluster action is disabled.	Cluster action is disabled.	-	o	o		
rc	Warning	511	Ignored the automatic start of groups because automatic group startup is disabled.	The automatic start of groups was ignored because automatic group start has been disabled.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rc	Warning	512	Ignored the recovery action in resource activation because recovery action caused by group resource activation error is disabled.	The recovery action in resource activation was ignored because recovery action against group resource activation error has been disabled.	-	o	o		
rc	Warning	513	Ignored the recovery action in resource deactivation because recovery action caused by group resource deactivation error is disabled.	The recovery action in resource deactivation was ignored because recovery action against group resource deactivation error has been disabled.	-	o	o		
rc	Info	514	Cluster action is set disabled.	Cluster action is disabled.	-	o	o		
rc	Info	515	Cluster action is set enabled.	Cluster action is enabled.	-	o	o		
rm	Info	1	Monitoring %1 has started.	Monitoring %1 has started.	-	o	o		
rm	Info	2	Monitoring %1 has stopped.	Monitoring %1 has stopped.	-	o	o		
rm	Info	3	%1 is not monitored by this server.	%1 is not monitored by this server.	-	o	o		
rm	Warning	4	Warn monitoring %1. (%2 : %3)	Warning of monitoring %1 is issued.	See "*Detailed info of monitor resource errors*". If a monitor resource is preparing for monitoring, the following message may be set in (). No action is required for this message. (100 : not ready for monitoring.)	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm	Warning	5	The maximum number of monitor resources has been exceeded. (registered resource is %1)	The maximum number of monitor resources has been exceeded.	Using the Cluster WebUI, check the cluster configuration data.	o	o		
rm	Warning	6	Monitor configuration of %1 is invalid. (%2 : %3)	The monitor configuration of %1 is invalid.	Using the Cluster WebUI, check the cluster configuration data.	o	o		
rm	Error	7	Failed to start monitoring %1.	Starting of monitoring %1 failed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o	o	o
rm	Error	8	Failed to stop monitoring %1.	Stopping of monitoring %1 failed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Error	9	Detected an error in monitoring %1. (%2 : %3)	An error was detected in monitoring %1.	See "*Detailed info of monitor resource errors*".	o	o	o	o
					If a monitoring timeout is detected, the following message is set in (). (99 : Monitor was timeout.)	o	o	o	o
					If Dummy Failure is enabled, the following message is set in (). No action is needed in the latter case. (201 : Monitor failed for failure verification.)	o	o	o	o

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
					If no response is returned from a monitor resource for a certain period of time, the following message is set in (). (202: couldn't receive reply from monitor resource in time.)	o	o	o	o
rm	Info	10	%1 is not monitored.	%1 is not monitored.	-	o	o		
rm / mm	Info	12	Recovery target %1 has stopped because an error was detected in monitoring %2.	Recovery target %1 has been stopped because an error was detected in monitoring %2.	-	o	o		
rm / mm	Info	13	Recovery target %1 has restarted because an error was detected in monitoring %2.	Recovery target %1 has been restarted because an error was detected in monitoring %2.	-	o	o		
rm / mm	Info	14	Recovery target %1 failed over because an error was detected in monitoring %2.	Recovery target %1 has failed over because an error was detected in monitoring %2.	-	o	o		
rm / mm	Info	15	Stopping the cluster has been required because an error was detected in monitoring %1.	A cluster stop is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Info	16	Stopping the system has been required because an error was detected in monitoring %1.	A system stop is requested because an error was detected in monitoring %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm / mm	Info	17	Rebooting the system has been required because an error was detected in monitoring %1.	A system restart is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Error	18	Attempted to stop the recovery target %1 due to the error detected in monitoring %2, but failed.	An attempt was made to stop recovery target %1 due to a %2 monitoring failure, but failed.	Check the status of resource %1.	o	o		
rm / mm	Error	19	Attempted to restart the recovery target %1 due to the error detected in monitoring %2, but failed.	An attempt was made to restart recovery target %1 due to a %2 monitoring failure, but failed.	Check the status of resource %1.	o	o		
rm / mm	Error	20	Attempted to fail over %1 due to the error detected in monitoring %2, but failed.	An attempt was made to provide failover for recovery target %1 due to a %2 monitoring failure, but failed.	Check the status of resource %1.	o	o		
rm / mm	Error	21	Attempted to stop the cluster due to the error detected in monitoring %1, but failed.	An attempt was made to stop the cluster due to a %1 monitoring failure, but failed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm / mm	Error	22	Attempted to stop the system due to the error detected in monitoring %1, but failed.	An attempt was made to stop the system due to a %1 monitoring failure, but failed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm / mm	Error	23	Attempted to reboot the system due to the error detected in monitoring %1, but failed.	An attempt was made to restart the system due to a %1 monitoring failure, but failed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm	Error	24	The group of %1 resource is unknown.	The group of resource %1 is unknown.	The cluster configuration information may be mismatched. Check it.	o	o		
rm / mm	Warning	25	Recovery will not be executed since the recovery target %1 is not active.	Recovery is not performed since recovery target %1 is not active.	-	o	o		
rm / mm	Info	26	%1 status changed from error to normal.	Monitoring %1 has changed from error to normal.	-	o	o		
rm / mm	Info	27	%1 status changed from error or normal to unknown.	Monitoring %1 has changed from abnormal or normal to unknown.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Error	28	Initialization error of monitor process. (%1 : %2)	An error occurred while initializing the monitor process.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Info	29	Monitoring %1 was suspended.	Monitoring %1 has temporarily stopped.	-	o	o		
rm	Info	30	Monitoring %1 was resumed.	Monitoring %1 has restarted.	-	o	o		
rm	Info	31	All monitors were suspended.	All monitoring processes have temporarily stopped.	-	o	o		
rm	Info	32	All monitors were resumed.	All monitoring processes have restarted.	-	o	o		
rm / mm	Info	35	System panic by sysrq has been required because an error was detected in monitoring %1.	A system panic by sysrq is requested because an error was detected in monitoring %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm / mm	Error	36	Attempted to panic system by sysrq due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system panic by sysrq due to a %1 monitoring failure, but failed.	Check whether the system is configured so that it can use sysrq.	o	o		
rm / mm	Info	37	System reset by keepalive driver has been required because an error was detected in monitoring %1.	A system reset by the keepalive driver is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Error	38	Attempted to reset system by keepalive driver due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system reset by the keepalive driver due to a %1 monitoring failure, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
rm / mm	Info	39	System panic by keepalive driver has been required because an error was detected in monitoring %1.	A system panic by the keepalive driver is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Error	40	Attempted to panic system by keepalive driver due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system panic by the keepalive driver due to a %1 monitoring failure, but failed.	Check whether the established environment supports the use of the keepalive driver.	o	o		
rm / mm	Info	41	System reset by BMC has been required because an error was detected in monitoring %1.	A system reset by BMC is requested because an error was detected in monitoring %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm / mm	Error	42	Attempted to reset system by BMC due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system reset by BMC due to a %1 monitoring failure, but failed.	Check whether the ipmitool command can be used.	o	o		
rm / mm	Info	43	System power down by BMC has been required because an error was detected in monitoring %1.	System power down by BMC is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Error	44	Attempted to power down system by BMC due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system power down by BMC due to a %1 monitoring failure, but failed.	Check whether the ipmitool command can be used.	o	o		
rm / mm	Info	45	System power cycle by BMC has been required because an error was detected in monitoring %1.	System power cycle by BMC is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Error	46	Attempted to power cycle system by BMC due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system power down by BMC due to a %1 monitoring failure, but failed.	Check whether the ipmitool command can be used.	o	o		
rm / mm	Info	47	NMI send by BMC has been required because an error was detected in monitoring %1.	System NMI transmission by BMC is requested because an error was detected in monitoring %1.	-	o	o		
rm / mm	Error	48	Attempted to send NMI by BMC due to the error detected in monitoring %1, but failed.	An attempt was made to cause a system NMI transmission by BMC due to a %1 monitoring failure, but failed.	Check whether the ipmitool command can be used.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm	Info	49	%1 status changed from warning to normal.	%1 status changed from warning to normal.	-	o	o		
rm	Error	57	Stopping the cluster is required since license (%1) is invalid.	Stopping the cluster is requested due to an invalid license.	Register a valid license.	o	o	o	o
rm	Error	58	Stopping the cluster due to invalid license (%1) failed.	Stopping the cluster due to an invalid license has failed.	Register a valid license.	o	o		
rm	Warning	71	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value at delay detection is %4 (tick count) and exceeded the delay warning rate %5 (%).	Check the load status of the server on which a monitoring delay was detected and remove the load. If a monitoring timeout is detected, extend it.	o	o		
rm	Warning	72	%1 could not Monitoring.	%1 could not perform monitoring.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
			Script before %1 upon failure in monitor resource %2 started.	Script before %1 of monitor resource %2 has started.	-	o	o		
rm / mm	Info	82	Script before %1 upon failure in monitor resource %2 completed.	Script before %1 of monitor resource %2 has been completed.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm / mm	Error	83	Script before %1 upon failure in monitor resource %2 failed.	Script before %1 of monitor resource %2 has failed.	Check the cause of the script failure and take appropriate action.	o	o		
rm	Warning	100	Restart count exceeded the maximum of %1. Final action of monitoring %2 will not be executed.	Because the restart count has exceeded the maximum value %1, the final action of %2 was not executed.	-	o	o		
rm	Warning	120	The virtual machine (%1) has been migrated to %2 by an external operation.	The virtual machine managed by resource %1 was made to migrate to server %2 through external operation.	-	o	o		
rm	Warning	121	The virtual machine (%1) has been started by an external operation.	The virtual machine managed by resource %1 was started by external operation.	-	o	o		
rm	Info	130	The collecting of detailed information triggered by monitor resource %1 error has been started (timeout=%2).	Collecting of detailed information triggered by detection of a monitor resource %1 monitoring error has started. The timeout is %2 seconds.	-	o	o		
rm	Info	131	The collection of detailed information triggered by monitor resource %1 error has been completed.	Collecting of detailed information triggered by detection of a monitor resource %1 monitoring error has been completed.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm	Warning	132	The collection of detailed information triggered by monitor resource %1 error has been failed (%2).	Collecting of detailed information triggered by detection of a monitor resource %1 monitoring error has failed.	-	o	o		
rm	Info	140	Process %1 has started.	Process %1 has started.	-	o	o		
rm	Warning	141	Process %1 has restarted.	Process %1 has restarted.	-	o	o		
rm	Warning	142	Process %1 does not exist.	Process %1 does not exist.	-	o	o		
rm	Error	143	Process %1 was restarted %2 times, but terminated abnormally.	Process %1 was restarted %2 times, but terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Error	150	The cluster is stopped since process %1 was terminated abnormally.	The cluster is stopped since process %1 was terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Error	151	The server is shut down since process %1 was terminated abnormally.	The server is shut down since process %1 was terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Error	152	The server is restarted since process %1 was terminated abnormally.	The server is restarted since process %1 was terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
rm	Error	160	Monitor resource %1 cannot be controlled since the license is invalid.	Monitor resource %1 cannot be controlled since the license is invalid.	Register a valid license.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm	Info	170	Recovery script has been executed since an error was detected in monitoring %1.	Recovery script has been executed since an error was detected in monitoring %1.	-	o	o		
rm	Error	171	An attempt was made to execute the recovery script due to a %1 monitoring failure, but failed.	An attempt was made to execute the recovery script due to a %1 monitoring failure, but failed.	Check the cause of the recovery script failure and take appropriate action.	o	o		
rm	Info	180	Dummy Failure of monitor resource %1 is enabled.	Dummy Failure of monitor resource %1 is enabled.	-	o	o		
rm	Info	181	Dummy Failure of monitor resource %1 is disabled.	Dummy Failure of monitor resource %1 is disabled.	-	o	o		
rm	Info	182	Dummy Failure of all monitor will be enabled.	Dummy Failure of all monitor will be enabled.	-	o	o		
rm	Info	183	Dummy Failure of all monitor will be disabled.	Dummy Failure of all monitor will be disabled.	-	o	o		
rm	Warning	184	An attempt was made to enable Dummy Failure of monitor resource %1, but failed.	An attempt was made to enable Dummy Failure of monitor resource %1, but failed.	Check whether monitor resource %1 corresponds to Dummy Failure.	o	o		
rm	Warning	185	An attempt was made to disable Dummy Failure of monitor resource %1, but failed.	An attempt was made to disable Dummy Failure of monitor resource %1, but failed.	Check whether monitor resource %1 corresponds to Dummy Failure.	o	o		
rm	Info	190	Recovery action caused by monitor resource error is disabled.	Recovery action caused by monitor resource error is disabled.	-	o	o		
rm	Info	191	Recovery action caused by monitor resource error is enabled.	Recovery action caused by monitor resource error is enabled.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
rm	Warning	192	Ignored the recovery action in monitoring %1 because recovery action caused by monitor resource error is disabled.	Ignored the recovery action in monitoring %1 because recovery action caused by monitor resource error is disabled.	-	o	o		
rm	Warning	193	Recovery action at timeout occurrence was disabled, so the recovery action of monitor %1 was not executed.	Recovery action at timeout occurrence was disabled, so the recovery action of monitor %1 was not executed.	-	o	o		
rm	Warning	200	Since there is no other normally running server, the final action(%1) for the error detection of monitor resource %2 was suppressed.	Suppression of final action for error detection.	-	o	o		
rm/mm	Info	210	IO Fencing by ACPI driver has been required because an error was detected in monitoring %1.	I/O fencing by the ACPI driver is necessary because an error was detected in monitoring %1.	-	o	o		
rm/mm	Error	211	Attempted to IO Fencing by ACPI driver due to the error detected in monitoring %1, but failed.	An attempt was made to perform I/O fencing by the ACPI driver in response to the error detected in monitoring %1, but failed.	Confirm whether the ACPI driver for EXPRESSCLUSTER linkage can be used in the environment.	o	o		
rm	Warning	220	Recovery will not be executed since any recovery target is not active.	Recovery will not be executed since any recovery target is not active.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mm	Info	51	The trial license is effective until %1. (%2)	The trial license is effective until %1.	-	o	o		
mm	Error	53	The license is not registered. (%1)	The license is not registered.	Purchase the license and then register it.	o	o		
mm	Error	54	The trial license has expired in %1. (%2)	The validity term of the trial license has expired.	Register a valid license.	o	o		
mm	Error	55	The registered license is invalid. (%1)	The registered license is invalid.	Register a valid license.	o	o		
mm	Error	56	The registered license is unknown. (%1)	The registered license is unknown.	Register a valid license.	o	o		
mm	Error	59	The trial license is valid from %1. (%2)	The validity term of the trial license is not reached.	Register a valid license.	o	o		
mm	Info	901	Message monitor has been started.	Message monitor (external linkage monitor module) has been started.	-	o	o		
mm	Error	902	Failed to initialize message monitor. (%1 : %2)	Message monitor (external linkage monitor module) could not be initialized.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
mm	Warning	903	An error of %1 type and %2 device has been detected. (%3)	External error %3 of category %1 and keyword %2 has been received.	-	o	o		
mm	Error	905	An error has been detected in monitoring %1. (%2)	An error was detected in monitor resource %1 monitoring.	Take appropriate action according to the %2 message.	o	o	o	o
mm	Error	906	Message monitor was terminated abnormally.	Message monitor (external linkage monitor module) has been terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mm	Error	907	Failed to execute action. (%1)	Executing recovery action has failed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
mm	Info	908	The system will be stopped.	The OS will be shut down.	-	o	o		
mm	Info	909	The cluster daemon will be stopped.	The cluster will be stopped.	-	o	o		
mm	Info	910	The system will be rebooted.	The OS will be rebooted.	-	o	o		
mm	Info	911	Message monitor will be restarted.	Message monitor (external linkage monitor module) will be restarted.	-	o	o		
mm	Info	912	Received a message by SNMP Trap from external. (%1 : %2)	Received a message by SNMP Trap from external.	-	o	o		
mm	Info	913	Received a Fatal Trap from %1. (msg : No data)	A Fatal Trap was received from the server %1. The message does not contain any information .	-	o	o		
mm	Info	914	Received a Fatal Trap from %1. (msg : %2)	A Fatal Trap was received from the server %1. The message contains information (%2). For information about %2 (failure region), see the Device Maintenance Guide[1]..	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mm	Warning	915	Received a Recoverble Trap.(Performance degradation) (msg : %1)	A Recoverable Trap was received. (Performance degradation was detected.). The message contains information (%1). For information about %1 (failure region), see the Device Maintenance Guide1.	-	o	o		
mm	Warning	916	Received a Recoverble Trap.(Predict) (msg : %1)	A Recoverable Trap was received. (A predictive failure was detected.). The message contains information (%1). For information about %1 (failure region), see the Device Maintenance Guide1.	-	o	o		
mm	Warning	917	Received a Recoverble Trap.(Performance degradation & Predict) (msg : %1)	A Recoverble Trap was received. (A predictive failure was detected.) The message contains information (%1). For information about %1 (failure region), see the Device Maintenance Guide1.	-	o	o		
trnsv	Error	1	There was a notification from external (IP=%1), but it was denied.	A notification was received from %1, but was not permitted.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
trnsv	Info	10	There was a notification (%1) from external (IP=%2).	A notification (%1) from %2 was accepted.	-	o	o		
trnsv	Info	20	Recovery action (%1) of monitoring %2 has been executed because a notification arrived from external.	Recovery action (%1) of monitor resource %2 has started through an external notification.	-	o	o		
trnsv	Info	21	Recovery action (%1) of monitoring %2 has been completed.	Recovery action (%1) of monitor resource %2 has been successful.	-	o	o		
trnsv	Error	22	Attempted to recovery action (%1) of monitoring %2, but it failed.	An attempt was made to perform recovery action (%1) of monitor resource %2, but failed.	Check whether the environment supports the recovery action.	o	o		
trnsv	Info	30	Action (%1) has been completed.	Action (%1) has been successful.	-	o	o		
trnsv	Error	31	Attempted to execute action (%1), but it failed.	An attempt was made to perform action (%1), but failed.	Check whether the environment supports the action.	o	o		
trnsv	Info	40	Script before action of monitoring %1 has been executed.	Script before the recovery action of monitor resource (%1) has been executed.	-	o			
trnsv	Info	41	Script before action of monitoring %1 has been completed.	Script before the recovery action of monitor resource (%1) has been executed successfully.	-	o			

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
trnsv	Error	42	Attempted to execute script before action of monitoring %1, but it failed.	Script before the recovery action of monitor resource (%1) could not be executed.	Check whether the script before the recovery action is executable.	o			
trnsv	Error	50	The system will be shutdown because cluster resume was failed.	The system will be shutdown because cluster resume was failed.	-		o		
trnsv	Error	51	An attempt to shutdown the system failed.	An attempt to shutdown the system failed.	The system may not be able to operate properly.		o		
trnsv	Info	83	Starting a dynamic adding resource %1.	Resource %1 has been dynamically added.	-	o	o		
trnsv	Info	84	A dynamic adding resource %1 has been started.	Resource %1 succeeded in being dynamically added.	-	o	o		
trnsv	Error	85	Failed to a dynamic adding resource %1.	Resource %1 failed to be dynamically added.	Take appropriate action according to the group resource message.	o	o		
trnsv	Warning	86	Server %1 is not in a condition to start a dynamic adding resource %2.	Server %1 cannot dynamically add Resource %2.	Check the server and group status.	o	o		
trnsv	Info	87	Deleting a resource %1.	Resource %1 has been deleted.	-	o	o		
trnsv	Info	88	Deleting a resource %1 has been stopped.	Resource %1 succeeded in being deleted.	-	o	o		
trnsv	Error	89	Failed to Delete a resource %1.	Resource %1 failed to be deleted.	Take appropriate action according to the group resource message.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
lanhb	Warning	71	Heartbeats sent from HB resource %1 of server %2 are delayed. (timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats from HB resource %1 of server %2 are delayed. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server %2 and remove the load. If an HB timeout occurs, extend it.	o	o		
lanhb	Warning	72	Heartbeats sent from HB resource %1 are delayed.(server=%2 time-out=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats sent from HB resource %1 are delayed. The transmission destination server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
lanhb	Warning	73	Heartbeats received by HB resource %1 are delayed.(server=%2 timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats received by HB resource %1 are delayed. The transmission source server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				
lankhb	Warning	71	Heartbeats sent from HB resource %1 of server %2 are delayed. (timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats from HB resource %1 of server %2 are delayed. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server %2 and remove the load. If an HB timeout occurs, extend it.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
lankhb	Warning	73	Heartbeats received from HB resource %1 is delayed. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	Heartbeats received by HB resource %1 are delayed. The transmission source server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				
diskhb	Error	10	Device(%1) of resource(%2) does not exist.	No device exists.	Check the cluster configuration data.	o	o		
diskhb	Error	11	Device(%1) of resource(%2) is not a block device.	No device exists.	Check the cluster configuration data.	o	o		
diskhb	Error	12	Raw device(%1) of resource(%2) does not exist.	No device exists.	Check the cluster configuration data.	o	o		
diskhb	Error	13	Binding device(%1) of resource(%2) to raw device(%3) failed.	No device exists.	Check the cluster configuration data.	o	o		
diskhb	Error	14	Raw device(%1) of resource(%2) has already been bound to other device.	Raw device %1 of resource %2 has already been bound to another device.	Set the raw device that is not in use.	o	o		
diskhb	Error	15	File system exists on device(%1) of resource(%2).	Device %1 of resource %2 contains the file system.	To use device %1, delete the file system.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
diskhb	Info	20	Resource %1 recovered from initialization error.	Resource %1 was recovered from an initialization error.	-	o	o		
diskhb	Warning	71	Heartbeats sent from HB resource %1 of server %2 are delayed. (timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats from HB resource %1 of server %2 are delayed. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server %2 and remove the load. If an HB timeout occurs, extend it.	o	o		
diskhb	Warning	72	Heartbeat write of HB resource %1 is delayed.(server=%2 timeout=%3*%4 actual-time=%5 delay warning rate=%6).	Heartbeats written by HB resource %1 are delayed. The write destination server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
diskhb	Warning	73	Heartbeat read of HB resource %1 is delayed.(server=%2 timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats read by HB resource %1 are delayed. The read source server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				
comhb	Info	1	Device (%1) does not exist.	No device exists.	Check the cluster configuration data.	o	o		
comhb	Info	2	Failed to open the device (%1).	The device could not be opened.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
comhb	Warning	71	Heartbeats sent from HB resource %1 of server %2 are delayed. (timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats from HB resource %1 of server %2 are delayed. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server %2 and remove the load. If an HB timeout occurs, extend it.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
comhb	Warning	72	Heartbeat write of HB resource %1 is delayed.(server=%2 timeout=%3*%4 actual-time=%5 delay warning rate=%6).	Heartbeats written by HB resource %1 are delayed. The transmission destination server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				
comhb	Warning	73	Heartbeat read of HB resource %1 is delayed.(server=%2 timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats read by HB resource %1 are delayed. The transmission source server is %2. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server to which a delay warning was issued and remove the load. If an HB timeout occurs, extend it.				
bmchb	Error	10	Failed to initialize to BMC.	BMC initialization failed.	Check whether the hardware can use the BMC linkage function.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
bmchb	Warning	71	Heartbeats sent from HB resource %1 of server %2 are delayed. (timeout=%3*%4 actual-time=%5 delay warning rate=%6)	Heartbeats from HB resource %1 of server %2 are delayed. The current timeout value is %3 (second) x %4 (tick count per second). The actual measurement value at delay generation is %5 (tick count) and exceeded the delay warning rate %6 (%).	Check the load status of the server %2 and remove the load. If an HB timeout occurs, extend it.	o	o		
monp	Error	1	An error occurred when initializing monitored process %1. (status=%2)	An error occurred in initializing monitored process %1.	Check the following possible causes: memory shortage, OS resource insufficiency, or cluster configuration data mismatching. If cluster configuration data has not yet been registered, the following process message is output. However, there is no problem. • mdagnt • webmgr • webalert	o	o		
monp	Error	2	Monitor target process %1 terminated abnormally. (status=%2)	Monitored process %1 has terminated abnormally.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
monp	Info	3	Monitor target process %1 will be restarted.	Monitored process %1 will be restarted.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
monp	Info	4	The cluster daemon will be stopped since the monitor target process %1 terminated abnormally.	The cluster will be stopped since monitored process %1 has terminated abnormally.	-	o	o		
monp	Error	5	Attempted to stop the cluster daemon, but failed.	An attempt was made to stop the cluster, but failed.	Check the following possible causes: cluster not yet activated, memory shortage, or OS resource insufficiency.	o	o		
monp	Info	6	The system will be stopped since the monitor target process %1 terminated abnormally.	The system will be stopped since monitored process %1 has terminated abnormally.	-	o	o		
monp	Error	7	Attempted to stop the system, but failed. (status=%#x)	An attempt was made to stop the system, but failed.	Check the following possible causes: cluster not yet activated, memory shortage, or OS resource insufficiency.	o	o		
monp	Info	8	System will be rebooted since monitor target process %1 terminated abnormally.	The system will be restarted since monitored process %1 has terminated abnormally.	-	o	o		
monp	Error	9	Attempted to reboot the system, but failed. (status=%#x)	An attempt was made to restart the system, but failed.	Check the following possible causes: cluster not yet activated, memory shortage, or OS resource insufficiency.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
md hd	Error	1	Failed to activate mirror disk. %1(Device:%2)	Activating %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				Failed to open I/O port.	The port could not be opened. Check the cluster configuration data.	o	o		
				The local server doesn't have the latest data.	The local server does not have the latest data. Mirror recovery is needed.	o	o		
				Communication to the remote server failed.	Communication with a remote server failed. Check the connection status of the mirror disk connection.	o	o		
				The remote server is active.	The remote server has already been activated. Check the status of the mirror disk resource.	o	o		
				The local server is already active.	The local server has already been activated. Check the status of the mirror disk resource.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				Mount operation failed.	The mount operation failed. Check whether the mount point exists. Alternatively, check whether the mount option of the cluster configuration data is correct.	o	o		
				NMP size of the local server is greater than that of the remote server.	The NMP size of the local server is greater than that of the remote server. Execute forced mirror recovery using the remote server as the mirror recovery source server.	o	o		
				Failed to set writable mode for data partition	Restart the server which tried to activate the resource. Note that failover may occur when the server is restarted.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
md hd	Info	2	fsck to %1 has started.	fsck of %1 has started.	-	o	o		
md hd	Info	3	fsck to %1 was successful.	fsck of %1 has been successful.	-	o	o		
md hd	Error	4	Failed to deactivate mirror disk. %1(Device:%2)	Deactivating %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				The mirror disk has already been deactivated.	The mirror disk has already been deactivated. Check the status of the mirror disk resource.	o	o		
				Unmount operation failed.	The unmount operation failed. Check whether the file system of the mirror disk resource is busy.	o	o		
md hd	Info	16	Initial mirror recovery of %1 has started.	Preparation for initial mirror construction of %1 has started.	-	o	o		
md hd	Info	18	Initial mirror recovery of %1 was successful.	Preparation for initial mirror construction of %1 has been successful.	-	o	o		
md hd	Warning	24	One of the servers is active, but the NMP size of mirror disks are not the same. (Device:%1)	One of the servers is active. The NMP sizes do not match, however.	Execute forced mirror recovery using the active server as the mirror recovery source server.	o	o		
md hd	Error	37	%1 of %2 failed(ret=%3).	Command %1 of device %2 failed with return value %3.	See the manual for command %1.	o	o		
md hd	Warning	38	Executing %1 of %2 with %3 option is necessary. Execute the command manually.	Executing command %1 of device %2 with option %3 specified is necessary. Execute the command manually.	Execute command %1 manually with option %3 specified.	o	o		
md hd	Info	39	%1 of %2 with %3 option has started.	Command %1 of device %2 with option %3 specified has started.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
md hd	Info	44	Mirror recovery of %1 was canceled.	Mirror recovery of %1 has been canceled.	-	o	o		
md hd	Info	45	Failed to cancel mirror recovery of %1.	Mirror recovery of %1 could not be canceled.	Stop the mirror recovery again.	o	o		
md hd	Error	46	umount timeout. Make sure that the length of Unmount Timeout is appropriate. (Device:%1)	Unmount of mirror %1 has timed out.	Check whether the unmount timeout setting is sufficiently long. (Refer to "Notes when terminating the Mirror disk resource or the Hybrid disk resource" and "Cache swell by a massive I/O" in "Notes and Restrictions" in the "Getting Started Guide".)	o	o		
md hd	Error	47	fsck timeout. Make sure that the length of Fsck Timeout is appropriate. (Device:%1)	fsck that was run prior to mount of mirror %1 has timed out.	Check whether the fsck timeout setting is sufficiently long. (Refer to "fsck execution" in "Notes and Restrictions" in the "Getting Started Guide".)	o	o		
mdadmn	Error	2	Failed to activate mirror disk. %1(Device:%2)	Activating %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				Failed to open I/O port.	The port could not be opened. Check the cluster configuration data.	o	o		
				The local server doesn't have the latest data.	The local server does not have the latest data. Mirror recovery is needed.	o	o		
				Communication to the remote server failed.	Communication with a remote server failed. Check the connection status of the mirror disk connection.	o	o		
				The remote server is active.	The remote server has already been activated. Check the status of the mirror disk resource.	o	o		
				The local server is already active.	The local server has already been activated. Check the status of the mirror disk resource.	o	o		
				Mount operation failed.	The mount operation failed. Check whether the mount point exists. Alternatively, check whether the mount option of the cluster configuration data is correct.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				NMP size of the local server is greater than that of the remote server.	The NMP size of the local server is greater than that of the remote server. Execute forced mirror recovery using the remote server as the mirror recovery source server.	o	o		
				One of other interconnection works well except mirror disk connections.	Check that the LAN for mirror connection is normal.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdadmn	Info	2	fsck to %1 has started.	fsck of %1 has started.	-	o	o		
mdadmn	Info	3	fsck to %1 was successful.	fsck of %1 has been successful.	-	o	o		
mdadmn	Error	4	Failed to deactivate mirror disk. %1(Device:%2)	Deactivating %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The mirror disk has already been deactivated.	The mirror disk has already been deactivated. Check the status of the mirror disk resource.	o	o		
				Unmount operation failed.	The unmount operation failed. Check whether the file system of the mirror disk resource is busy.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdadmn	Error	5	Failed to recover the mirror. %1(Device:%2)	Mirror recovery of %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The recovery is in progress.	Mirror recovery is in progress. Wait for the completion of the mirror recovery and then reexecute.	o	o		
				The destination server is active.	The mirror disk resource has already been activated on the copy destination server. Check the status of the mirror disk resource.	o	o		
				Cannot determine the mirror recovery direction.	The mirror recovery direction cannot be determined. Perform forced mirror recovery.	o	o		
				The source server is abnormal.	The copy source server is abnormal. Check the status of the mirror agent.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				NMP size of recovery destination is smaller.	Change the mirror recovery direction. If the mirror recovery direction cannot be changed, exchange the mirror recovery destination mirror disk and allocate a data partition of sufficient size. Alternatively, allocate a data partition of sufficient size using the fdisk command or the like.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdadmn	Info	6	Mirror recovery of %1 was completed successfully.	Mirror recovery of %1 has been successful.	-	o	o		
mdadmn	Info	7	Mirror recovery mode is %1.(Device:%2)	The mirror recovery mode is %1. When %1 is "NORMAL", full-scale mirror recovery (Full Copy) is performed. When %1 is "FAST", difference mirror recovery is performed.	-	o	o		
mdadmn	Info	8	The number of Replicator Option licenses is %1. (%2)	The number of Replicator Option licenses is %1.	-	o	o		
mdadmn	Info	9	The trial license is effective until %1. (%2)	The trial license is effective until %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdadmn	Error	10	The registered license is unknown. (%1)	The registered license is unknown.	Register a valid license.	o	o		
mdadmn	Error	11	The registered license is invalid. (%1)	The registered license is invalid.	Register a valid license.	o	o		
mdadmn	Error	12	The license is not registered. (%1)	The license is not registered.	Purchase the license and then register it.	o	o		
mdadmn	Warning	13	The number of licenses %1 is insufficient. (%2)	The number of licenses is insufficient.	Purchase the required number of licenses and then register them.	o	o		
mdadmn	Error	14	The trial license expired in %1. (%2)	The validity term of the trial license has expired.	Register a valid license.	o	o		
mdadmn	Error	15	The trial license is effective from %1. (%2)	The validity term of the trial license is not reached.	Register a valid license.	o	o		
mdadmn	Info	16	Initial mirror recovery of %1 has started.	Initial mirror construction of %1 has started.	-	o	o		
mdadmn	Info	17	Mirror recovery of %s has started.(%d bytes)	Mirror recovery of %1 has started.	-	o	o		
mdadmn	Info	18	Initial mirror recovery of %1 was successful.	Initial mirror construction of %1 has been successful.	-	o	o		
mdadmn	Error	19	Failed to perform initial mirror recovery. %1(Device:%2)	Initial mirror construction of %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The recovery is in progress.	Mirror recovery is in progress. Wait for the completion of the mirror recovery and then reexecute.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				The destination server is active.	The resource has already been activated on the copy destination server. Check the status of the mirror disk resource.	o	o		
				Cannot determine the mirror recovery direction.	The mirror recovery direction cannot be determined. Perform forced mirror recovery.	o	o		
				The source server is abnormal.	The copy source server is abnormal. Check the status of the mirror agent.	o	o		
mdadmn	Info	20	Initial mirror recovery was not executed following the configuration. (Device:%1)	Initial mirror construction was not performed according to the setting.	-	o	o		
mdadmn	Info	21	Mirror partition mkfs was executed. (Device:%1)	mkfs of the mirror partition has been executed.	-	o	o		
mdadmn	Info	22	Mirror partition mkfs was not executed following the configuration. (Device:%1)	mkfs of the mirror partition was not executed according to the setting.	-	o	o		
mdadmn	Info	23	Forced mirror recovery was canceled. Execute the command "clpmdctrl --force" to resume the mirror recovery. (Device:%1)	Forced mirror recovery has been canceled. To restart the mirror recovery, execute clpmdctrl --force.	To restart the mirror recovery, execute clpmdctrl --force.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdadmn	Warning	24	One of the servers is active, but NMP size of mirror disks are not the same. (Device:%1)	One of the servers is active. The NMP sizes do not match, however.	Execute forced mirror recovery using the active server as the mirror recovery source server.	o	o		
mdadmn	Info	25	The NMP sizes of both servers' disks has been successfully synchronized. (Device:%1)	The NMP sizes of both servers have been successfully synchronized.	-	o	o		
mdadmn	Error	28	Mirror recovery data has been successfully synchronized. NMP size synchronization has failed. (Device:%1)	Mirror recovery data has been successfully synchronized. However, the NMP sizes could not be synchronized.	Reexecute the forced mirror recovery.	o	o		
mdadmn	Error	30	The license information was removed after the cluster was started.	The license was valid when the cluster was started. However, the license was deleted.	Register a valid license.	o	o		
mdadmn	Error	31	Failed to isolate the mirror. %1(Device:%2)	%2 could not be isolated. The following message is output to %1: Replicator license is invalid or expired.	Register a valid license.	o	o		
mdadmn	Error	32	Forced activation of the mirror failed. %1 (Device:%2)	Forced activation of %2 failed. The following messages may be output output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				Failed to open I/O port.	The port could not be opened. Check the cluster configuration data.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				Mount operation failed.	The mount operation failed. Check whether the mount point exists. Alternatively, check whether the mount option of the cluster configuration data is correct.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdadmn	Error	33	Forced recovery of the mirror failed. %1(Device:%2)	Forced recovery of %2 failed. The following message may be output output to %1: Register a valid license.	Register a valid license.	o	o		
mdadmn	Info	34	Isolating the mirror %1 completed successfully.	Mirror resource %1 has been successfully isolated.	-	o	o		
mdadmn	Info	35	Mirror force active of %1 was completed successfully.	Forced activation of %1 has been successful.	-	o	o		
mdadmn	Info	36	Forced recovery of the mirror %1 completed successfully.	Forced recovery of %1 has been successful.	-	o	o		
mdadmn	Error	37	%1 of %2 failed(ret=%3).	Command %1 of device %2 failed with return value %3.	See the manual for command %1.	o	o		
mdadmn	Warning	38	Executing %1 of %2 with %3 option is necessary. Execute the command manually.	Executing command %1 of device %2 with option %3 specified is necessary. Execute the command manually.	Execute command %1 manually with option %3 specified.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdadmn	Info	39	%1 of %2 with %3 option has started.	Command %1 of device %2 with option %3 specified has started.	-	o	o		
mdadmn	Info	40	Failed to write to cluster partition of hybrid disk(%1).	Writing to cluster partition of %1 has failed.	Restart the server.	o	o		
mdadmn	Info	41	Timeout in writing to cluster partition of hybrid disk(%1).	Writing to the cluster partition of %1 has timed out.	The disk load may be high. Increase the value of Cluster Properties - Mirror Agent tab - Cluster Partition I/O Timeout. Alternatively, increase the timeout value of the monitor resource (hdw, hdnw) along with the increase in the former value.	o	o		
mdadmn	Info	42	Failed to read from cluster partition of hybrid disk(%1).	Reading of the cluster partition of %1 has failed.	Restart the server.	o	o		
mdadmn	Info	43	Timeout in reading from cluster partition of hybrid disk(%1).	Reading of the cluster partition of %1 has timed out.	The disk load may be high. Increase the value of Cluster Properties - Mirror Agent tab - Cluster Partition I/O Timeout. Alternatively, increase the timeout value of the monitor resource (hdw, hdnw) along with the increase in the former value.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdadmn	Info	44	Mirror recovery of %1 was canceled.	Mirror recovery of %1 has been canceled.	-	o	o		
mdadmn	Info	45	Failed to cancel mirror recovery of %1.	Mirror recovery of %1 could not be canceled.	Stop the mirror recovery again.	o	o		
mdadmn	Error	46	unmount timeout. Make sure that the length of Unmount Timeout is appropriate. (Device:%1)	Unmount of mirror %1 has timed out.	Check whether the unmount timeout setting is sufficiently long. (Refer to "Notes when terminating the Mirror disk resource or the Hybrid disk resource" and "Cache swell by a massive I/O" in "Notes and Restrictions" in the "Getting Started Guide".)	o	o		
mdadmn	Error	47	fsck timeout. Make sure that the length of Fsck Timeout is appropriate. (Device:%1)	fsck that was run prior to mount of mirror %1 has timed out.	Check whether the fsck timeout setting is sufficiently long. (Refer to "fsck execution" in "Notes and Restrictions" in the "Getting Started Guide".)	o	o		
mdagent	Info	1	The Mirror Agent has started successfully.	The mirror agent has been started normally.	-	o	o		
mdagent	Error	2	Failed to start Mirror Agent. %1	The mirror agent could not be started. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				Agent is running.	The agent has already been started.	o	o		
				Command clpmdinit is running.	The clpmdini command has already been started. Check the end of the command and then restart it.	o	o		
				IP address in the config file is invalid.	Check the cluster configuration data.	o	o		
				Server name in the config file is invalid.	Check the cluster configuration data.	o	o		
				There is an error in config file.	Check the cluster configuration data.	o	o		
				Failed to initialize socket server.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
				Disk error had occurred before reboot. Agent will stop starting..	Disk error occurred. Check the mirror disk and if necessary, see "How to replace a mirror disk with a new one" in "The system maintenance information" in the "Maintenance Guide", and replace it.	o	o		
mdagent	Info	3	The Mirror Agent has stopped successfully.	The mirror agent has been stopped normally.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdagent	Error	4	Failed to stop the Mirror Agent.	The mirror agent has failed to stop.	Check the following possible causes: cluster not yet activated, memory shortage, or OS resource insufficiency.	o	o		
					It is probable that an attempt to stop the mirror agent or server was made while the mirror disk resource or hybrid disk resource was activated.	o	o		
					Use the Cluster WebUI or an EXPRESSCLUSTER command to stop the mirror agent or server.	o	o		
					It is probable that an attempt to stop the mirror agent or server was made while the mirror disk resource or hybrid disk resource was still mounted.	o	o		
					If an unmount timeout occurred, set a larger value for unmount timeout.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
					If the user mounted the mirror partition at multiple mount points, unmount the additional mount point before deactivating the mirror.	o	o		
					It is also probable that mirror recovery was in progress.	o	o		
					If mirror recovery is in progress, stop the mirror agent or server after mirror recovery is completed or after stopping mirror recovery.	o	o		
mdagent	Warning	5	Failed to load the resource(%1). Check if the Cluster Partition or Data Partition is OK.	Resource %1 could not be loaded.	Check whether the paths of the cluster and data partitions of resource %1 are correct or whether those paths may be destroyed.	o	o		
mdctrl hdctrl	Error	1	Failed to activate mirror disk.%1 (Device:%2)	Activating %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				Failed to open I/O port.	The port could not be opened. Check the cluster configuration data.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				The local server doesn't have the latest data.	The local server does not have the latest data. Mirror recovery is needed.	o	o		
				Communication to the remote server failed.	Communication with a remote server failed. Check the connection status of the mirror disk connection.	o	o		
				The remote server is active.	The remote server has already been activated. Check the status of the mirror disk resource.	o	o		
				The local server is already active.	The local server has already been activated. Check the status of the mirror disk resource.	o	o		
				Mount operation failed.	The mount operation failed. Check whether the mount point exists. Alternatively, check whether the mount option of the cluster configuration data is correct.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				NMP size of the local server is greater than that of the remote server.	The NMP size of the local server is greater than that of the remote server. Execute forced mirror recovery using the remote server as the mirror recovery source server.	o	o		
				Failed to set writable mode for data partition	Restart the server which tried to activate the resource. Note that failover may occur when the server is restarted.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdctrl hdctrl	Info	2	fsck of %1 has started.	fsck of %1 has started.	-	o	o		
mdctrl hdctrl	Info	3	fsck of %1 was successful.	fsck of %1 has been successful.	-	o	o		
mdctrl hdctrl	Error	4	Failed to deactivate mirror disk.%1 (Device:%2)	Deactivating %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The mirror disk has already been deactivated.	The mirror disk has already been deactivated. Check the status of the mirror disk resource.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				Unmount operation failed.	The unmount operation failed. Check whether the file system of the mirror disk resource is busy.	o	o		
mdctrl hdctrl	Error	5	Failed to recover mirror.%1 (Device:%2)	Mirror recovery of %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The recovery is in progress.	Mirror recovery is in progress. Wait for the completion of the mirror recovery and then reexecute.	o	o		
				The destination server is active.	The mirror disk resource has already been activated on the copy destination server. Check the status of the mirror disk resource.	o	o		
				Can not judge the recovery direction.	The mirror recovery direction cannot be determined. Perform forced mirror recovery.	o	o		
				The source server is abnormal.	The copy source server is abnormal. Check the status of the mirror agent.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				NMP size of recovery destination is smaller.	Execute the forced mirror recovery using the remote server as the mirror recovery source server. Alternatively, replace the mirror recovery destination disk with a disk of sufficient size or allocate a data partition of sufficient size with the fdisk command.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdctrl hdctrl	Info	7	Mirror recovery mode is %1.(Device:%2)	The mirror recovery mode is %1. When %1 is "NORMAL", full-scale mirror recovery (Full Copy) is performed. When %1 is "FAST", difference mirror recovery is performed.	-	o	o		
mdctrl hdctrl	Info	16	Initial mirror recovery of %1 has started.	Initial mirror construction of %1 has started.	-	o	o		
mdctrl hdctrl	Info	17	Mirror recovery of %1 has started.	Mirror recovery of %1 has started.	-	o	o		
mdctrl hdctrl	Info	18	Initial mirror recovery of %1 was successful.	Initial mirror construction of %1 has been successful.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdctrl hdctrl	Error	19	Failed to perform initial mirror recovery. %1(Device:%2)	Initial mirror construction of %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The recovery is in progress.	Mirror recovery is in progress. Wait for the completion of the mirror recovery and then reexecute.	o	o		
				The destination server is active.	The resource has already been activated on the copy destination server. Check the status of the mirror disk resource.	o	o		
				Cannot judge the recovery direction.	The mirror recovery direction cannot be determined. Perform forced mirror recovery.	o	o		
				The source server is abnormal.	The copy source server is abnormal. Check the status of the mirror agent.	o	o		
mdctrl hdctrl	Info	20	Initial mirror recovery was not executed following the configuration. (Device:%1)	Initial mirror construction was not performed according to the setting.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdctrl hdctrl	Error	31	Failed to isolate the mirror. %1(Device:%2)	%2 failed to be isolated. The following message may be output to %1: Replicator license is invalid or expired.	Register a valid license.	o	o		
mdctrl hdctrl	Error	32	Forced activation of the mirror failed. %1 (Device:%2)	Forced activation of %2 failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				Failed to open I/O port.	The port could not be opened. Check the cluster configuration data.	o	o		
				Mount operation failed.	The mount operation failed. Check whether the mount point exists. Alternatively, check whether the mount option of the cluster configuration data is correct.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdctrl hdctrl	Error	33	Forced recovery of the mirror failed. %1(Device:%2)	Forced recovery of %2 failed. The following messages may be output to %1:		o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdctrl hdctrl	Info	34	Isolating the mirror %1 completed successfully.	Mirror resource %1 has been successfully isolated.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdctrl hdctrl	Info	35	Mirror force active of %1 was completed successfully.	Forced activation of %1 has been successful.	-	o	o		
mdctrl hdctrl	Info	36	Forced recovery of the mirror %1 completed successfully.	Forced recovery of %1 has been successful.	-	o	o		
mdctrl hdctrl	Error	37	%1 of %2 failed(ret=%3).	Command %1 of device %2 failed with return value %3.	See the manual for command %1.	o	o		
mdctrl hdctrl	Warning	38	Executing %1 of %2 with %3 option is necessary. Execute the command manually.	Executing command %1 of device %2 with option %3 specified is necessary. Execute the command manually.	Execute command %1 manually with option %3 specified.	o	o		
mdctrl hdctrl	Info	39	%1 of %2 with %3 option has started.	Command %1 of device %2 with option %3 specified has started.	-	o	o		
mdctrl hdctrl	Info	44	Mirror recovery of %1 was canceled.	Mirror recovery of %1 has been canceled.	-	o	o		
mdctrl hdctrl	Info	45	Failed to cancel mirror recovery of %1.	Mirror recovery of %1 could not be canceled.	Stop the mirror recovery again.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdctrl hdctrl	Error	46	umount time-out. Make sure that the length of Unmount Timeout is appropriate. (Device:%1)	Unmount of mirror %1 has timed out.	Check whether the unmount timeout setting is sufficiently long. (Refer to "Notes when terminating the Mirror disk resource or the Hybrid disk resource" and "Cache swell by a massive I/O:ref:*Cache swell by a massive I/O<l_sg:cache-swell-by-a-massive-i-o>*" in "Notes and Restrictions" in the "Getting Started Guide".)	o	o		
mdctrl hdctrl	Error	47	fsck timeout. Make sure that the length of Fsck Timeout is appropriate. (Device:%1)	fsck that was run prior to mount of mirror %1 has timed out.	Check whether the fsck timeout setting is sufficiently long. (Refer to "fsck execution" in "Notes and Restrictions" in the "Getting Started Guide")	o	o		
mdctrl	Info	50	Extension of mirror disk %1 was succeeded.	The data partition extension of mirror disk resource %1 succeeded.		o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdctrl	Error	51	Failed to extend mirror disk %1.	The data partition extension of mirror disk resource %1 failed.	Check if the data partition is configured with LVM. Check if the amount of unused PE of the volume group is sufficient.	o	o		
mdinit hdinit	Info	21	Mirror partition mkfs was executed. (Device:%1)	mkfs of the mirror partition has been executed.	-	o	o		
mdinit hdinit	Info	22	Mirror partition mkfs was not executed following the configuration. (Device:%1)	mkfs of the mirror partition was not executed according to the setting.	-	o	o		
mdw hdw	Error	5	Failed to recover the mirror.%1 (Device:%2)	Mirror recovery of %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The recovery is in progress.	An attempt was made to start auto mirror recovery, but mirror recovery was already started.	o	o		
				The destination server is active.	The mirror disk resource has already been activated on the copy destination server. Check the status of the mirror disk resource.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
				Cannot determine the mirror recovery direction.	The mirror recovery direction cannot be determined. Perform forced mirror recovery.	o	o		
				The source server is abnormal.	The copy source server is abnormal. Check the status of the mirror agent.	o	o		
				NMP size of recovery destination is smaller.	Execute the forced mirror recovery using the remote server as the mirror recovery source server. Alternatively, replace the mirror recovery destination disk with a disk of sufficient size or allocate a data partition of sufficient size with the fdisk command.	o	o		
				Replicator license is invalid or expired.	Register a valid license.	o	o		
mdw hdw	Info	7	Mirror recovery mode is %1.(Device:%2)	The mirror recovery mode is %1. When %1 is "NORMAL", full-scale mirror recovery (Full Copy) is performed. When %1 is "FAST", difference mirror recovery is performed.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdw hdw	Info	16	Initial mirror recovery of %1 has started.	Initial mirror construction of %1 has started.	-	o	o		
mdw hdw	Info	17	Mirror recovery of %1 has started.	Mirror recovery of %1 has started.	-	o	o		
mdw hdw	Info	18	Initial mirror recovery of %1 was successful.	Initial mirror construction of %1 has been successful.	-	o	o		
mdw hdw	Error	19	Failed to perform initial mirror recovery.%1 (Device:%2)	Initial mirror construction of %2 has failed. The following messages may be output to %1:	Take appropriate action according to the message displayed in %1.	o	o		
				The recovery is in progress.	Mirror recovery is in progress. Wait for the completion of the mirror recovery and then reexecute.	o	o		
				The destination server is active.	The resource has already been activated on the copy destination server. Check the status of the mirror disk resource.	o	o		
				Cannot determine the mirror recovery direction.	The mirror recovery direction cannot be determined. Perform forced mirror recovery.	o	o		
				The source server is abnormal.	The copy source server is abnormal. Check the status of the mirror agent.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mdw hdw	Info	20	Initial mirror recovery was not executed following the configuration. (Device:%1)	Initial mirror construction was not performed according to the setting.	-	o	o		
fip	Error	10	IP address %1 already exists on the network.	IP address %1 exists in the network.	Check whether the IP address is already in use in the network.	o	o		
fip	Info	11	IP address %1 will be forcefully activated.	IP address %1 is forcibly activated.	-	o	o		
vip	Error	10	IP address %1 already exists on the network.	IP address %1 exists in the network.	Check whether the IP address is already in use in the network.	o	o		
vip	Info	11	IP address %1 will be forcefully activated.	IP address %1 is forcibly activated.	-	o	o		
disk	Info	10	%1 of %2 has started.	Command %1 of device %2 has started.	-	o	o		
disk	Info	11	%1 of %2 was successful.	Command %1 of device %2 has been successful.	-	o	o		
disk	Error	12	%1 of %2 failed (ret=%3).	Command %1 of device %2 failed with return value %3.	See the manual for command %1.	o	o		
disk	Warning	13	Executing %1 of %2 with %3 option is necessary. Execute the command manually.	Executing command %1 of device %2 with option %3 specified is necessary. Execute the command manually.	Execute command %1 manually with option %3 specified.	o	o		
disk	Info	14	%1 of %2 with %3 option has started.	Command %1 of device %2 with option %3 specified has started.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
disk	Error	15	Timeout occurred during %1 of %2.	Execution of Command %1 of device %2 has timed out.	Check the cause of the execution timeout of Command %1 and take appropriate action.	o	o		
disk	Warning	16	Executing xfs_repair of %1 is necessary. Execute the command manually.	Executing the xfs_repair command is necessary. Execute the command manually.	Execute the xfs_repair command.	o	o		
disk	Warning	17	Setting of Disktype=%1 and Filesystem=%2 can't be combined.	Disk type %1 and file system %2 cannot be used in combination.	Review the setting.	o	o		
cl	Info	1	There was a request to start %1 from the %2.	A request to start %1 was issued from %2.	-	o	o		
cl	Info	2	There was a request to stop %1 from the %2.	A request to stop %1 was issued from %2.	-	o	o		
cl	Info	3	There was a request to suspend %1 from the %2.	A request to suspend %1 was issued from %2.	-	o	o		
cl	Info	4	There was a request to resume %s from the %s.	A request to resume %1 was issued from %2.	-	o	o		
cl	Error	11	A request to start %1 failed(%2).	A request to start %1 has failed.	Check the status of the cluster.	o	o		
cl	Error	12	A request to stop %1 failed(%2).	A request to stop %1 has failed.	Check the status of the cluster.	o	o		
cl	Error	13	A request to suspend %1 failed(%2).	A request to suspend %1 has failed.	Check the status of the cluster.	o	o		
cl	Error	14	A request to resume %1 failed(%2).	A request to resume %1 has failed.	Check the status of the cluster.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
cl	Error	15	A request to %1 cluster failed on some servers(%2).	A %1 request of the cluster failed on some servers.	Check the status of the cluster.	o	o		
cl	Error	16	A request to start %1 failed on some servers(%2).	Starting %1 failed on some servers.	Check the status of %1.	o	o		
cl	Error	17	A request to stop %1 failed on some servers(%2).	Stopping %1 failed on some servers.	Check the status of %1.	o	o		
cl	Warning	18	Automatic start is suspended because the cluster service was not stopped according to the normal procedure.	Automatic start has been suspended because Automatic startup after the system down was not set.	To start the cluster service, use the Cluster WebUI or clpcl command.	o	o		
cl	Warning	20	A request to start %1 failed because cluster is running(%2).	Starting %1 has failed because the cluster is running.	Check the status of the cluster.	o	o		
cl	Warning	21	A request to stop %1 failed because cluster is running(%2).	Stopping %1 has failed because the cluster is running.	Check the status of the cluster.	o	o		
mail	Error	1	The license is not registered. (%1)	Purchase the license and then register it.	-	o	o		
mail	Error	2	The trial license has expired in %1. (%2)	Register a valid license.	-	o	o		
mail	Error	3	The registered license is invalid. (%1)	Register a valid license.	-	o	o		
mail	Error	4	The registered license is unknown. (%1)	Register a valid license.	-	o	o		
mail	Error	5	mail failed(%s).(SMTP server: %s)	Mail report failed.	Check whether there is an error in the SMTP server and that there is no problem with communicating with the SMTP server.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
mail	Info	6	mail successed.(SMTP server: %s)	Mail report has been successful.	-	o	o		
down	Info	1	There was a request to shutdown %1 from the %2.	There was a request to shut down %1 from %2.	-	o	o		
down	Info	2	There was a request to reboot %1 from the %2.	There was a request to reboot %1 from %2.	-	o	o		
down	Error	11	A request to shutdown %1 failed(%2).	A request to shut down %1 failed.	Check the status of the server.	o	o		
down	Error	12	A request to reboot %1 failed(%2).	A request to reboot %1 failed.	Check the status of the server.	o	o		
userw	Warning	1	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value at delay detection is %4 (tick count) and exceeded the delay warning rate %5 (%).	Check the load condition of the server on which the monitoring delay was detected, and lessen the load appropriately. If a monitoring timeout is likely to be detected, you should increase the monitoring timeout setting.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
vipw	Warning	1	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value at delay detection is %4 (tick count) and exceeded the delay warning rate %5 (%).	Check the load condition of the server on which the monitoring delay was detected, and lessen the load appropriately. If a monitoring timeout is likely to be detected, you should increase the monitoring timeout setting.	o	o		
ddnsw	Warning	1	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value at delay detection is %4 (tick count) and exceeded the delay warning rate %5 (%).	Check the load condition of the server on which the monitoring delay was detected, and lessen the load appropriately. If a monitoring timeout is likely to be detected, you should increase the monitoring timeout setting.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
vmw	Warning	1	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value at delay detection is %4 (tick count) and exceeded the delay warning rate %5 (%).	Check the load condition of the server on which the monitoring delay was detected, and lessen the load appropriately. If a monitoring timeout is likely to be detected, you should increase the monitoring timeout setting.	o	o		
bmcw	Warning	1	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value upon delay detection is %4 (tick count) which exceeds the delay warning rate %5 (%).	Check the load status of the server on which a monitoring delay was detected and then remove that load. If a monitoring timeout is likely to be detected, increase the monitoring timeout setting.	o	o		
apisv	Info	1	There was a request to stop cluster from the %1(IP=%2).	A request to stop the cluster was issued from %1.	-	o	o		
apisv	Info	2	There was a request to shutdown cluster from the %1(IP=%2).	A request to shut down the cluster was issued from %1.	-	o	o		
apisv	Info	3	There was a request to reboot cluster from the %1(IP=%2).	A request to reboot the cluster was issued from %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Info	4	There was a request to suspend cluster from the %1(IP=%2).	A request to suspend the cluster was issued from %1.	-	o	o		
apisv	Info	10	There was a request to stop server from the %1(IP=%2).	A request to stop the server was issued from %1.	-	o	o		
apisv	Info	11	There was a request to shutdown server from the %1(IP=%2).	A request to shut down the server was issued from %1.	-	o	o		
apisv	Info	12	There was a request to reboot server from the %1(IP=%2).	A request to reboot the server was issued from %1.	-	o	o		
apisv	Info	13	There was a request to server panic from the %1(IP=%2).	A server panic request was issued from %1.	-	o	o		
apisv	Info	14	There was a request to server reset from the %1(IP=%2).	A server reset request was issued from %1.	-	o	o		
apisv	Info	15	There was a request to server sysrq from the %1(IP=%2).	An SYSRQ panic request was issued from %1.	-	o	o		
apisv	Info	16	There was a request to KA RESET from the %1(IP=%2).	A keepalive reset request was issued from %1.	-	o	o		
apisv	Info	17	There was a request to KA PANIC from the %1(IP=%2).	A keepalive panic request was issued from %1.	-	o	o		
apisv	Info	18	There was a request to BMC reset from the %1(IP=%2).	A BMC reset request was issued from %1.	-	o	o		
apisv	Info	19	There was a request to BMC PowerOff from the %1(IP=%2).	A BMC power-off request was issued from %1.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Info	20	There was a request to BMC Power-Cycle from the %1(IP=%2).	A BMC power cycle request was issued from %1.	-	o	o		
apisv	Info	21	There was a request to BMC NMI from the %1(IP=%2).	A BMC NMI request was issued from %1.	-	o	o		
apisv	Info	22	There was a request to IO Fencing from the %1(IP=%2).	An I/O fencing request was received from %1.	-	o	o		
apisv	Info	30	There was a request to start group(%1) from the %2(IP=%3).	A request to start group %1 was issued from %2.	-	o	o		
apisv	Info	31	There was a request to start all groups from the %1(IP=%2).	A request to start all groups was issued from %1.	-	o	o		
apisv	Info	32	There was a request to stop group(%1) from the %2(IP=%3).	A request to stop group %1 was issued from %2.	-	o	o		
apisv	Info	33	There was a request to stop all groups from the %1(IP=%2).	A request to stop all groups was issued from %1.	-	o	o		
apisv	Info	34	There was a request to restart group(%1) from the %2(IP=%3).	A request to restart group %1 was issued from %2.	-	o	o		
apisv	Info	35	There was a request to restart all groups from the %1(IP=%2).	A request to restart all groups was issued from %1.	-	o	o		
apisv	Info	36	There was a request to move group(%1) from the %2(IP=%3).	A request to move group %1 was issued from %2.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Info	37	There was a request to move all groups from the %1(IP=%2).	A request to move the group was issued from %1.	-	o	o		
apisv	Info	38	There was a request to failover group(%1) from the %2(IP=%3).	A group %1 failover request was issued from %2.	-	o	o		
apisv	Info	39	There was a request to failover all groups from the %1(IP=%2).	A group failover request was issued from %1.	-	o	o		
apisv	Info	40	There was a request to migrate group(%1) from the %2(IP=%3).	A group %1 migration request was issued from %2.	-	o	o		
apisv	Info	41	There was a request to migrate all groups from the %1(IP=%2).	A request to make all groups migrate was issued from %2.	-	o	o		
apisv	Info	42	There was a request to failover all groups from the %1(IP=%2).	A request to provide failover for all groups was issued from %2.	-	o	o		
apisv	Info	43	There was a request to cancel waiting for the dependence destination group of group the %1 was issued from %2.	A request to cancel waiting for the dependence destination group of group %1 was issued from %2.	-	o	o		
apisv	Info	50	There was a request to start resource(%1) from the %2(IP=%3).	A request to start resource %1 was issued from %2.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Info	51	There was a request to start all resources from the %1(IP=%2).	A request to start all resources was issued from %1.	-	o	o		
apisv	Info	52	There was a request to stop resource(%1) from the %2(IP=%3).	A request to stop resource %1 was issued from %2.	-	o	o		
apisv	Info	53	There was a request to stop all resources from the %1(IP=%2).	A request to stop all resources was issued from %1.	-	o	o		
apisv	Info	54	There was a request to restart resource(%1) from the %2(IP=%3).	A request to restart resource %1 was issued from %2.	-	o	o		
apisv	Info	55	There was a request to restart all resources from the %1(IP=%2).	A request to restart all resources was issued from %1.	-	o	o		
apisv	Info	60	There was a request to suspend monitor resources from the %1(IP=%2).	A request to suspend the monitor resource was issued from %1.	-	o	o		
apisv	Info	61	There was a request to resume monitor resources from the %1(IP=%2).	A request to resume the monitor resource was issued from %1.	-	o	o		
apisv	Info	62	There was a request to enable Dummy Failure of monitor resource(%1) from the %2(IP=%3).	A request to enable Dummy Failure of monitor resource %1 was issued from%2.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Info	63	There was a request to disable Dummy Failure of monitor resource(%1) from the %2(IP=%3).	A request to disable Dummy Failure of monitor resource%1 was issued from%2.	-	o	o		
apisv	Info	64	There was a request to disable Dummy Failure of all monitor resources from the %1(IP=%2).	A request to disable Dummy Failure of all the monitor resources was issued from %1.	-	o	o		
apisv	Info	70	There was a request to set CPU frequency from the %1(IP=%2).	A request to set the CPU clock was issued from %1.	-	o	o		
apisv	Error	101	A request to stop cluster was failed(0x%08x).	The cluster could not be stopped.	Check the status of the cluster.	o	o		
apisv	Error	102	A request to shutdown cluster was failed(0x%08x).	The cluster could not be shut down.	Check the status of the cluster.	o	o		
apisv	Error	103	A request to reboot cluster was failed(0x%08x).	The cluster could not be rebooted.	Check the status of the cluster.	o	o		
apisv	Error	104	A request to suspend cluster was failed(0x%08x).	The cluster could not be suspended.	Check the status of the cluster.	o	o		
apisv	Error	110	A request to stop server was failed(0x%08x).	The server could not be stopped.	Check the status of the server.	o	o		
apisv	Error	111	A request to shutdown server was failed(0x%08x).	The server could not be shut down.	Check the status of the server.	o	o		
apisv	Error	112	A request to reboot server was failed(0x%08x).	The server could not be rebooted.	Check the status of the server.	o	o		
apisv	Error	113	A request to server panic was failed(0x%08x).	Server panic has failed.	Check the status of the server.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Error	114	A request to server reset was failed(0x%08x).	Server reset has failed.	Check the status of the server.	o	o		
apisv	Error	115	A request to server sysrq was failed(0x%08x).	SYSRQ panic has failed.	Check the status of the server.	o	o		
apisv	Error	116	A request to KA RESET was failed(0x%08x).	Keepalive reset has failed.	Check the status of the server.	o	o		
apisv	Error	117	A request to KA PANIC was failed(0x%08x).	Keepalive panic has failed.	Check the status of the server.	o	o		
apisv	Error	118	A request to BMC RESET was failed(0x%08x).	BMC reset has failed.	Check the status of the server.	o	o		
apisv	Error	119	A request to BMC PowerOff was failed(0x%08x).	BMC power-off has failed.	Check the status of the server.	o	o		
apisv	Error	120	A request to BMC PowerCycle was failed(0x%08x).	BMC power cycle has failed.	Check the status of the server.	o	o		
apisv	Error	121	A request to BMC NMI was failed(0x%08x).	BMC NMI has failed.	Check the status of the server.	o	o		
apisv	Error	122	A request to IO Fencing was failed(0x%08x).	I/O fencing has failed.	Check the status of the server.	o	o		
apisv	Error	130	A request to start group(%1) was failed(0x%08x).	Starting group (%1) has failed.	Take appropriate action according to the group start failure message issued by rc.	o	o		
apisv	Error	131	A request to start all groups was failed(0x%08x).	Starting all groups has failed.	Same as above.	o	o		
apisv	Error	132	A request to stop group(%1) was failed(0x%08x).	Stopping group (%1) has failed.	Take appropriate action according to the group stop failure message issued by rc.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Error	133	A request to stop all groups was failed(0x%08x).	Stopping all groups has failed.	Same as above.	o	o		
apisv	Error	134	A request to restart group(%1) was failed(0x%08x).	Restarting group (%1) has failed.	Take appropriate action according to the group stop failure message issued by rc.	o	o		
apisv	Error	135	A request to restart all groups was failed(0x%08x).	Restarting all groups has failed.	Same as above.	o	o		
apisv	Error	136	A request to move group(%1) was failed(0x%08x).	Moving group (%1) has failed.	Take appropriate action according to the group movement failure message issued by rc.	o	o		
apisv	Error	137	A request to move all groups was failed(0x%08x).	Moving all groups has failed.	Same as above.	o	o		
apisv	Error	138	A request to failover group(%1) was failed(0x%08x).	Failover for group (%1) has failed.	Take appropriate action according to the group failover failure message issued by rc.	o	o		
apisv	Error	139	A request to failover all groups was failed(0x%08x).	Failover for all groups has failed.	Same as above.	o	o		
apisv	Error	140	A request to migrate group(%1) was failed(0x%08x).	Migration of group (%1) has failed.	Take appropriate action according to the group failover failure message issued by rc.	o	o		
apisv	Error	141	A request to migrate all groups was failed(0x%08x).	Migration of all groups has failed.	Same as above.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Error	142	A request to failover all groups was failed(0x%08x).	Failover for all groups has failed.	Same as above.	o	o		
apisv	Error	143	A request to cancel waiting for the dependency destination group of group %1 has failed(0x%08x).	Canceling waiting for the dependency destination group of group %1 has failed.	Same as above.	o	o		
apisv	Error	150	A request to start resource(%1) was failed(0x%08x).	Resource (%1) has failed to start.	Take appropriate action according to the resource start failure message issued by rc.	o	o		
apisv	Error	151	A request to start all resources was failed(0x%08x).	Starting all resources has failed.	Same as above.	o	o		
apisv	Error	152	A request to stop resource(%1) was failed(0x%08x).	Resource (%1) has failed to stop.	Take appropriate action according to the resource stop failure message issued by rc.	o	o		
apisv	Error	153	A request to stop all resources was failed(0x%08x).	Stopping all resources has failed.	Same as above.	o	o		
apisv	Error	154	A request to restart resource(%1) was failed(0x%08x).	Resource (%1) has failed to restart.	Take appropriate action according to the resource restart failure message issued by rc.	o	o		
apisv	Error	155	A request to restart all resources was failed(0x%08x).	Restarting all resources has failed.	Same as above.	o	o		
apisv	Error	160	A request to suspend monitor resource was failed(0x%08x).	The monitor resource could not be suspended.	Check the status of the monitor resource.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
apisv	Error	161	A request to resume monitor resource was failed(0x%08x).	The monitor resource could not be resumed.	Same as above.	o	o		
apisv	Error	162	A request to enable Dummy Failure of monitor resource(%1) was failed(0x%08x).	The monitor resource %1 failed to start Dummy Failure.	Check the status of the monitor resource.	o	o		
apisv	Error	163	A request to disable Dummy Failure of monitor resource(%1) was failed(0x%08x).	The monitor resource %1 failed to stop Dummy Failure.	Same as above.	o	o		
apisv	Error	164	A request to disable Dummy Failure of all monitor resources was failed(0x%08x).	All the monitor resources failed to stop Dummy Failure.	Same as above.	o	o		
apisv	Error	170	A request to set CPU frequency was failed(0x%08x).	The CPU clock level could not be set.	Take appropriate action according to the CPU clock level setting failure message issued by rc.	o	o		
lamp	Error	1	The license is not registered. (%1)	The license is not registered.	Purchase the license and then register it.	o	o		
lamp	Error	2	The trial license has expired in %1. (%2)	The validity term of the trial license has expired.	Register a valid license.	o	o		
lamp	Error	3	The registered license is invalid. (%1)	The registered license is invalid.	Register a valid license.	o	o		
lamp	Error	4	The registered license is unknown. (%1)	The registered license is unknown.	Register a valid license.	o	o		
lamp	Info	5	Notice by the network warming light succeeded.	Report by the network warning light has been successful.	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
lamp	Error	6	Error in executing result of warning light command.(%d)	An error occurred during execution of the network warning light report command.	Take appropriate action according to the error code.	o	o		
lamp	Error	7	Failed to execute warning light command.(%d)	The network warning light report command could not be executed.	Check the following possible causes: memory shortage or OS resource insufficiency.	o	o		
cfmgr	Info	1	The cluster configuration data has been uploaded by %1.	Cluster configuration data has been uploaded.	-	o	o		
sra	Error	1	system monitor closed because reading the SG file failed.	An error occurred in reading the SG file.	Check the message separately issued.		o		
sra	Error	2	Opening an ignore file failed. file name = %1, errno = %2. %1:File name %2:errno	The SG file (%1) failed to be opened.	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	3	Reading a configuration file failed.	An error occurred in reading the SG file.	Check the message separately issued.		o		
sra	Error	4	Trace log initialization failed.	The internal log file could not be initialized.	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	5	Creating a daemon process failed.	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Error	6	Reading a service configuration file failed.	An error occurred in reading the SG file.	Check the message separately issued.		o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
sra	Error	7	mlock() failed.	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Error	8	A daemon process could not be created.	SystemResource Agent has failed to start (turning the process into a daemon).	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Error	9	stdio and stderr could not be closed.	SystemResource Agent has failed to start (closing the standard I/O).	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Error	10	A signal mask could not be set up.	SystemResource Agent has failed to start (setting the signal mask).	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Error	11	A configuration file error occurred. (1) [line = %1, %2] %1:Line %2:Setting value	SystemResource Agent has failed to start (reading the SG file).	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	12	A configuration file error occurred. (2) [line=%1, %2] %1:Line %2:Setting value	SystemResource Agent has failed to start (reading the SG file).	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	13	A plugin event configuration file error occurred. The DLL pointer was not found. [line = %1, %2] %1:Line %2:Setting value	SystemResource Agent has failed to start (registering the plugin event).	Restart the cluster, or execute the suspend and resume.		o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
sra	Error	14	malloc failed. [event structure]	SystemResource Agent has failed to start (registering the plugin event).	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	15	A service configuration file error occurred due to an invalid event. [%1] %1:Setting value	SystemResource Agent has failed to start (reading the service file).	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	16	A plugin event configuration file error occurred due to %1. %1:Cause of error	SystemResource Agent has failed to start (reading the plugin event file).	Restart the cluster, or execute the suspend and resume.		o		
sra	Error	17	Internal error occurred.	A shared memory access error has occurred.	-		o		
sra	Warning	101	Opening an SG file failed. file name = %1, errno = %2 %1:File name %2:errno	The SG file (%1) failed to be opened.	Recreate the SG file and restart the cluster, or execute the suspend and resume.		o		
sra	Warning	102	malloc(3) fail(1) . [%1] %1:Function name	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Warning	103	malloc(3) fail(2). [%1] %1:Function name	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Warning	104	An internal error occurred. rename(2) error (errno = %1) %1:errno	This product has terminated abnormally.	See the most recently issued system log message.		o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
sra	Warning	105	realloc(3) fail. [%1]. %1:Function name	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Warning	106	A script timed out. (%1 %2) %1:Script file name %2:Argument	An external error has occurred.	Check the load status of the server and remove the load.		o		
sra	Warning	107	[%1] execvp(2) fail (%2). %1:Script file name %2:errno	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Warning	108	[%1] fork fail (%2). Suspended. %1:Script file name %2:errno	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Warning	109	malloc(3) fail. [%1] %1:Function name	An external error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.		o		
sra	Info	201	A script was executed. (%1) %1:Script name	Script (%1) has been executed.	-		o		
sra	Info	202	Running a script finished. (%1) %1:Script name	Script has ended normally.	-		o		
sra	Info	203	An %1 event succeeded. %1:Executed event type	The operation management command has been executed. The executed event type (boot, shutdown, stop, start, or flush) is output.	-		o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
sra	Error	301	A process resource error was detected. (type = cpu, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the CPU usage rates of specific processes.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	301	A process resource error was detected. (type = memory leak, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the memory usage of specific processes.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	301	A process resource error was detected. (type = file leak, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the number (maximum) of open files of specific processes.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	301	A process resource error was detected. (type = open file, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the number (upper kernel limit) of open files of specific processes.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	301	A process resource error was detected. (type = thread leak, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the number of threads of specific processes.	Check the possible causes of the monitoring failure.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
sra	Error	301	A process resource error was detected. (type = defunct, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the zombie processes.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	301	A process resource error was detected. (type = same name process, pid = %1, %2) %1:Process ID %2:Process name	An error was detected in monitoring the same-name processes.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	302	A system resource error was detected. (type = cpu)	An error was detected in monitoring the CPU usage rates of the system.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	302	A system resource error was detected. (type = memory)	An error was detected in monitoring the total usage of memory of the system.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	302	A system resource error was detected. (type = swap)	An error was detected in monitoring the total usage of virtual memory of the system.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	302	A system resource error was detected. (type = file)	An error was detected in monitoring the total number of open files of the system.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	302	A system resource error was detected. (type = thread)	An error was detected in monitoring the total number of threads of the system.	Check the possible causes of the monitoring failure.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
sra	Error	303	A system resource error was detected. (type = number of process, user name = %1) %1:User name	An error was detected in monitoring the number of running processes for each user of the system.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	304	A disk resource error was detected. (type = used rate, level = NOTICE, %1) %1:mount point	A notice level error was detected in monitoring the disk usage rates.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	304	A disk resource error was detected. (type = used rate, level = WARNING, %1) %1:mount point	A warning level error was detected in monitoring the disk usage rates.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	304	A disk resource error was detected. (type = free space, level = NOTICE, %1) %1:mount point	A notice level error was detected in monitoring the free disk space.	Check the possible causes of the monitoring failure.	o	o		
sra	Error	304	A disk resource error was detected. (type = free space, level = WARNING, %1) %1:mount point	A warning level error was detected in monitoring the free disk space.	Check the possible causes of the monitoring failure.	o	o		
lcns	Info	1	The number of licenses is %1. (Product name:%2)	The number of cluster licenses is %1. %1: Number of licenses %2: Product name	-	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
lcns	Info	2	The trial license is valid until %1. (Product name:%2)	The trial license is effective until %1. %1: Trial end date %2: Product name	-	o	o		
lcns	Warning	3	The number of licenses is insufficient. The number of insufficient licenses is %1. (Product name:%2)	The number of licenses is insufficient. The number of insufficient licenses is %1. %1: Required number of licenses %2: Product name	Purchase the required number of licenses and then register them.	o	o		
lcns	Error	4	The license is not registered. (Product name:%1)	The license is not registered. %1: Product name	Purchase the license and then register it.	o	o		
lcns	Error	5	The trial license has expired in %1. (Product name:%2)	The validity term of the trial license has expired. %1: Trial end date %2: Product name	Register a valid license.	o	o		
lcns	Error	6	The registered license is invalid. (Product name:%1, Serial No:%2)	The registered license is invalid. %1: Product name %2: Serial number	Register a valid license.	o	o		
lcns	Error	7	The registered license is unknown. (Product name:%1)	The registered license is unknown. %1: Product name	Register a valid license.	o	o		
lcns	Error	8	The trial license is valid from %1. (Product name:%2)	The validity term of the trial license is not reached. %1: Trial start date %2: Product name	Register a valid license.	o	o		

Continued on next page

Table 10.1 – continued from previous page

Module type	Event type	Event ID	Message	Description	Solution	alert	syslog	mail	SNMP Trap
lcns	Info	9	The fixed term license is valid until %1. (Product name:%2)	The validity term of the fixed-term license is effective until %1. %1:End date of validity term %2: Product name	-	o	o		
lcns	Error	10	The fixed term license has expired in %1. (Product name:%2)	The validity term of the fixed-term license has expired. %1: End date of validity term %2: Product name	Register a valid license.	o	o		
webmgr	Warning	21	HTTPS configuration isn't correct, HTTPS mode doesn't work. Please access WebManager by HTTP mode.	HTTPS configuration isn't correct, HTTPS mode doesn't work.	Access WebManager by HTTP mode.	o	o		

10.3 Driver syslog messages

The syslog messages by EXPRESSCLUSTER driver in this version are output as follows:

[Event class] <type: Module type><event: Event ID> Message

Item	Display content	Description
Event class	I	Information/Notification
	W	Warning/Caution
	E	Error
Module type	liscal	Mirror Driver
	clpkhb	Kernel Mode LAN Heartbeat Driver
	clpka	Keepalive Driver
Event ID	Digit	
Message	Message	

(Examples of display message)

```
kernel: [I] <type: liscal><event: 101> Registered blkdev with major=218.
```

Continued on next page

Table 10.2 – continued from previous page

kernel: [I] <type: liscal><event: 130> NMP1 new thread: liscal_hb_client_thread (PID=30777).
kernel: [I] <type: liscal><event: 243> NMP1 network is USING 192.168.10.100 - 192.168.10.101 :29031(HB)
kernel: [W] <type: liscal><event: 220> NMP1 failed to create HB client socket. (err=-111: Connection refused)
kernel: [I] <type: clpkhb><event: 101> Kernel Heartbeat was initialized successfully. (major=10, minor=240)
kernel: [E] <type: clpkhb><event: 123> Failed to bind HB socket. (err=-99: Can not assign requested address)

The messages are displayed under the following log level when outputting syslog.

Module Type	liscal	clpkhb	clpka
Information/ Notification[I]	KERN_INFO	KERN_INFO	KERN_INFO
Warning/ Caution[W]	KERN_INFO	KERN_INFO	KERN_INFO
Error [E]	KERN_ERR	KERN_INFO	KERN_INFO

See also the followings for the coping process to the messages:

- "EXPRESSCLUSTER X 4.1 Getting Started Guide" "Notes and Restrictions"
- "EXPRESSCLUSTER X 4.1 Maintenance Guide" "The system maintenance information"
- "EXPRESSCLUSTER X 4.1 Reference Guide " "*Troubleshooting*"

10.3.1 Mirror Driver

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	101	Registered blkdev with major=%1.	Successfully loaded the mirror driver.	-
liscal	Error	102	Failed to register blkdev with major=%1.	Failed to load the mirror driver.	-
liscal	Info	103	Unregistered blkdev with major=%1.	Successfully unloaded the mirror driver.	-
liscal	Warning	104	Failed to unregister blkdev with major=%1.	Unloading the mirror driver failed.	-
liscal	Info	110	Adding disk NMP%1 with major=%2 minor=%3.	The mirror partition NMP[%1] is going to be added.	
liscal	Info	111	Deleting disk NMP%1 with major=%2 minor=%3.	The mirror partition NMP[%1] is going to be deleted.	
liscal	Info	112	Cleaning up NMP%1 queue.	The queue of the mirror partition NMP[%1] is going to be Cleaned up.	
liscal	Error	120	insmod did not pass %1 to liscal with %2.	Loading the mirror driver failed. Invalid parameter had been specified.	Restart the local server.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	121	Failed to create a proc file %1.	Creation of proc file [%1] (liscalstat / liscalinner) failed.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource).
liscal	Info	122	%1 is busy. (proc->count=%2)	The proc file [%1] (liscalstat / liscalinner) is being accessed. Waiting for the end of the access.	Check if there is any process accessing to [%1] (/proc/liscalstat or /proc/liscalinner). The corresponding process is going to be killed.
liscal	Info	123	Forced to remove %1 after waiting %2 seconds.	The proc file[%1] (liscalstat / liscalinner) was deleted forcibly, because killing forcibly all the processes accessing it after waiting for [%2] seconds failed.	-
liscal	Warning	124	NMP%1 waited for all I/O requests to be sent completely, but timeout occurred. Writing differences to bitmap.	Some asynchronous data could not be sent completely in time at deactivation. Their difference information is going to be written to the Cluster Partition.	-
liscal	Warning	125	NMP%1 %2 I/O requests (%3B) %4 not be sent to remote server %5.	The number of I/O requests for which the completion of asynchronization data transmission was not checked is [%2] ([%3] bytes).	-
liscal	Info	130	New thread: %2 (PID=%3). NMP%1 new thread: %2 (PID=%3).	The thread [%2] started. Process id of it is [%3].	-
liscal	Error	131	Failed to fork thread: %2 (err=%3).	Starting the thread [%2] failed. (Error code=[%3])	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource).
			NMP%1 failed to fork thread: %2 (err=%3).	-	
liscal	Info	132	killing thread.....OK. (%2) NMP%1 killing thread.....OK (%2)	Thread [%2] ended normally.	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	133	%1 waiting %2 killed.....	Thread [%1] is waiting for thread [%2] to end.	-
liscal	Info	134	NMP%1 received signal. (%2)	Thread / Procedure [%2] received the termination request signal.	-
liscal	Info	135	NMP%1 exit.....OK. (%2)	Procedure [%2] ended normally.	-
liscal	Error	136	NMP%1 killing thread, but mount port is still opened.	The mounted mirror disk resource exists at unloading the mirror driver.	Check the mirror disk resource status.
liscal	Error	137	NMP%1 killing thread, but %2 I/O request still exist.	The mirror partition device is busy. The thread of the mirror driver is going to stop, but the I/O request to the mirror partition has not been still completed.	Check the mirror disk resources is not accessed.
liscal	Info	140	NMP%1 liscal will shutdown, N/W port closed.	An attempt will be made to perform shutdown with the mirror partition mounted. Mirror data transmission is stopped. Any data that is not transmitted is recorded as the mirror difference to perform mirror break.	Use clpstdn or clpdown to shut down the server. Check whether shutdown and reboot were used erroneously.
liscal	Warning	141	NMP%1 device does not exist. (%2)	NMP[%1] does not exist.	Check the cluster configuration information. Check if there is wrong setting with initial construction steps of the mirror disk or the hybrid disk. No problem in case of the following.
liscal	Info	141	• This message can be recorded on udev environment when liscal is initializing NMPx.	On the environment which udev runs, this message is output when the NMP[%1] is accessed before the mirror driver completes the initialization of NMP[%1].	For the workaround, see "Error message in the load of the mirror driver in the udev environment" of "Notes and Restrictions" in "Getting Started Guide".

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	141	• Ignore this and following messages 'Buffer I/O error on device NMPx' on udev environment.	In this case, this message and buffer I/O error of NMP[%1] are displayed, but there is no problem.	Same as above.
liscal	Warning	142	NMP%1 N/W is not initialized yet. (%2)	The initialization of the driver has not completed yet.	A problem may have occurred with the mirror driver. Restart the system.
liscal	Warning	143	NMP%1 cache_table is not initialized. (%2)	The initialization of the driver has not completed yet.	Same as above.
liscal	Warning	144	NMP%1 I/O port has been closed, mount(%2), io(%3).	The mirror partition has not been mounted. But it was going to be accessed.	Check the mirror disk resource status.
					Check if there is any applications trying to access the mirror partition device directly.
					If output is made at deactivation, it takes time to write memory cache into a disk during unmount processing. This may cause a timeout. While referencing "Cache swell by a massive I/O" below, increase the unmount timeout value sufficiently.
					If the user specified an additional mount point to be created in a different location for the mirror partition device or mirror mount point, check if that mount point is configured to be unmounted before deactivation. See "When multiple mounts are specified for a resource like a mirror disk resource" below.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
					For others, the following may be applicable.
liscal	Info	144	• This message can be recorded by fsck command when NMPx becomes active.	This message can be output in case that the mirror partition is accessed by fsck command before being mounted.	• See the following in "Notes and Restrictions" in the " Getting Started Guide". • "Buffer I/O error log for the mirror partition device" • "Messages written to syslog when multiple mirror disk resources or hybrid disk resources are used" • "Cache swell by a massive I/O" • "When multiple mounts are specified for a resource like a mirror disk resource"
liscal	Info	144	• This message can be recorded on hotplug service starting when NMPx is not active.	And also, this message can be output when the hotplug service searches devices.	
liscal	Info	144	• Ignore this and following messages 'Buffer I/O error on device NMPx' on such environment.	This message and buffer I/O error of NMP[%1] are displayed in this case, but there is no problem.	
liscal	Error	145	Failed to allocate %2 or NMP%1 failed to allocate %2	Allocation of memory failed.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource).

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	146	Failed to allocate %2, retrying. or NMP%1 failed to allocate %2, retrying.	Allocation of memory failed. Memory allocation is retried.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource).
liscal	Warning	147	Failed to allocate %2, other area used instead.	Allocation of memory failed. The reserved area is used.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource).
liscal	Info	148	NMP%1 holder %2. (%3)	The exclusive access count before or after (timing of [%3]) mount/unmount of NMP[%1] is [%2]. Normally, [%2] is 0before mount or after unmount; [%2] is 1 after mount or before unmount. If the count is other than 0 even after unmount, it is possible that something is holding NMP[%1] or continues to hold it such that unmount cannot be completed.	If the count does not become 0 even after unmount and a file system error occurs, the unmount timeout setting may be insufficiently long. Refer to "Notes when terminating the Mirror disk resource or the Hybrid disk resource" and "Cache swell by a massive I/O" in "Notes and Restrictions" in the "Getting Started Guide". If the count is other than 0 before mount, the fsck timeout setting may be insufficient. Refer to "fsck execution" in "Notes and Restrictions" in the "Getting Started Guide".
liscal	Info	150	NMP%1 mirror break, writing mirror_break_time to Cluster Partition.	Mirror break occurred. Either there is a problem with mirror disk connection, or I/O to the disk failed in the remote server.	Check the mirror disk connection status. Check if the mirror disk connection or OS is highly-loaded.
liscal	Info	151	NMP%1 ACK1 timeout.	Timeout occurred while receiving the response to the sent mirror synchronization data (ACK1).	Same as above.
liscal	Info	152	NMP%1 mirror break has occurred during recovery, recovery failed.	Mirror break occurred while recovering the mirror. Mirror recovery will stop abnormally.	Same as above.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	154	NMP%1 N/W port opened.	The mirror synchronization data connection port opened because the connection became possible.	-
liscal	Info	155	NMP%1 N/W port closed.	The connection port closed because the connection became impossible.	-
liscal	Info	156	NMP%1 failed to %2, because N/W port has been closed.	Sending and receiving of data[%2] failed because the connection port had been closed.	Check the mirror disk connection status. Check if the mirror disk connection or OS is highly-loaded.
liscal	Info	157	NMP%1 failed to recover, because N/W port of remote server has been closed.	Mirror recovery failed because the connection port of the remote server had been closed.	Same as above.
liscal	Warning	158	NMP%1 received sync data, but mount port has been opened, sync failed.	The synchronization data from the remote server was received. But the mirror partition has been mounted on the local server. Then the received data was discarded.	Check if the mirror partition is deactive and is mounted.
liscal	Info	159	NMP%1 received request to stop sending data from remote server.	Synchronization data was sent to the remote server. However, the transmitted synchronization data was discarded because the remote server had mounted the mirror partition or transmission was disabled.	Same as above.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	160	NMP%1 disk I/O error%2	The I/O error to the disk occurred now or in the past. The system will reboot.	The physical defect may have occurred with mirror disk in case of being output while in operation. See "The system maintenance information" in the "Maintenance Guide", exchange the mirror disks and run mirror recovery. Check the cluster partition settings in cluster configuration information in case of being output while constructing the cluster.
liscal	Error	160	• Confirm that the new disk is cleared, if it has been replaced already.	See "The system maintenance information" in the "Maintenance Guide" and clear the cluster partition in case that this message is output at startup even after exchanging the mirror disks.	
liscal	Error	160	• Replace the old error disk with a new cleared disk, if it has not been replaced yet.	See "The system maintenance information" in the Maintenance Guide and exchange the mirror disks in case of not having exchanged the mirror disks.	

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	161	NMP%1 failed to %2 %3 %4 Cluster Partition.	The I/O[%2] (read/write / read / write / clear / flush) to the area in the Cluster Partition failed.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource) when the lack of resource is possible. The physical defect may have occurred with mirror disk in case of being output while in operation. See "The system maintenance information" in the "Maintenance Guide", exchange the mirror disks and run mirror recovery. Check the cluster partition settings in cluster configuration information in case of being output while constructing the cluster.
liscal	Warning	162	NMP%1 failed to clear the bitmap. (%2)	In the processing [%4], the difference bitmap processing [%2] (set/clear) for the [%3] area failed.	Shut down the cluster and restart it.
liscal	Info	163	NMP%1 %2 is null. (%3)	The initialization of the driver has not completed.	A problem may have occurred with the mirror driver. Restart the system.
liscal	Warning	164	NMP%1 sector %2 not found. (%3)	The processing information to the corresponding sector[%2] was not found in the queue in the driver.	-
liscal	Warning	165	NMP%1 requested sector is out of NMP area. (%2)	The I/O request to the area exceeding the size of the mirror partition was received at procedure[%2]. This request was discarded.	-
liscal	Info	166	NMP%1 %2 is null. (%3)	An attempt was made to set a difference bitmap after it had already been set as having a difference.	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	167	NMP%1 %2 is null. (%3)	An attempt was made to send ACK2 after it had already been sent.	-
liscal	Error	168	NMP%1 failed to %2 bitmap. Invalid %3	Processing [%2] on the differential bitmap for the [%3] area failed.	A problem may have occurred with the mirror driver. Check if the sizes of the single sectors of the mirror disks on the two servers differ.
liscal	Warning	170	ioctl() got %1 inode with NULL, exit.	Invalid ioctl() call was detected.	The OS may have become unstable. Restart the system.
liscal	Error	171	NMP%1 requested I/O with wrong command(%2) from FS.	Invalid I/O request was issued to the mirror partition from the file system or others. This request to the NMP device is incorrect.	Same as above.
liscal	Warning	172	request_id(%2) is too big. (%3) or NMP%1 request_id(%2) is too big. (%3)	Invalid procedure number was detected at procedure[%3]. This request was discarded.	-
liscal	Warning	173	NMP%1 failed to send, but its ID was not found in request_queue. (%2)	Sending of the mirror synchronization data failed. An attempt to delete the processing information failed, because the corresponding procedure number was not found in the queue in the driver.	A problem may have occurred with the mirror driver. Restart the system.
liscal	Info	174	NMP%1 request_id(%2) deleted. (%3)	The processing information of procedure number[%2] was deleted normally from the queue in the driver due to the mirror synchronization data send failure.	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	175	request_id(%2) ACK1 timeout, but its NMP%1 not found. (%3)	ACK1 (response to the sent mirror data) of procedure number[%2] had not been received in time. But the corresponding procedure number[%2] was not found in the queue in the driver.	A problem may have occurred with the mirror driver. Restart the system.
liscal	Info	176	NMP%1 received ACK1, but its ID was not found in request_queue.	ACK1 (response to the mirror synchronization data) was received. But the corresponding procedure number[%2] was not found in the queue in the driver. This message is output if ACK1 is received after it has not been received in time.	When Event ID:151 occurs before this event, this event may mean a server received ACK1 of Event ID:151 by high-load on partner or network. In this case, change Ack timeout too long. (process 4)
liscal	Info	177	NMP%1 received ACK2, but its ID was not found in wait_ack2_queue.	ACK2 (response to mirror synchronization completion notification ACK1) was received. But the corresponding procedure number[%2] was not found in the queue in the driver. This message is output if ACK2 is received after it has not been received in time.	-
liscal	Warning	178	request_id(%2) of ACK is not found in trans_table. (%3) or NMP%1 request_id(%2) of ACK is not found in trans_table. (%3)	ACK (response to the sent recovery data) of procedure number[%2] was received. But the corresponding procedure number[%2] was not found in the queue in the driver. This message is output if ACK is received after it has not been received in time.	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	179	NMP%1 received request to stop sending data, but its ID was not found in request_queue.	The request to close communication of the mirror synchronization data was received, instead of ACK1, from the remote server. But the corresponding procedure number[%2] was not found in the queue in the driver. Waiting for ACK1 reception may have already timed out.	-
liscal	Warning	180	%2 (%3) is invalid. The default setting (%4) will be used instead. or NMP%1 %2 (%3) is invalid. The default setting (%4) will be used instead.	The parameter[%2] (value:[%3]) is invalid. The default value[%4] is used instead.	The setting file may have been mistakenly edited directly. Check the setting values by Cluster WebUI. For the details of the parameters, see the aftermentioned coping process 2 [2] .
liscal	Info	181	NMP%1 %2 (%3) is invalid. The maximum number (%4) will be used instead.	The parameter[%2] (value:[%3]) is invalid. The maximum value[%4] is used instead.	In case that the timeout magnification adjustment (clptoratio command) is used, the value may exceed the maximum value. In this case, the maximum value is used. For the details of the parameters, see the aftermentioned coping process 2 [2] .
liscal	Error	182	%2 (%3) is invalid. (%6) or NMP%1 %2 (%3) is invalid. (%6) or %2 (%3) or %4 (%5) is invalid. (%6) or NMP%1 %2 (%3) or %4 (%5) is invalid. (%6)	The parameter[%2] (value:[%3]) or the parameter[%4] (value:[%5]) is invalid.	The setting file may have been mistakenly edited directly. Check the setting values by Cluster WebUI.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	183	NMP%1 %2 is %3. Heartbeat of mirror disk connection will be ignored.	The parameter[%2] (value:[%3]) is specified. The mirror disk connection will not be used.	-
liscal	Info	184	The same %1 Partition is specified. Specify different partitions. (NMP%2, NMP%3)	The [%1] (Cluster/Data) partition specification is invalid. The same partition is specified for multiple (NMP[%2] and NNP[%3]) resources.	For the Linux version, separate cluster partitions and data partitions must be assigned to each resource. Correct the partition specification. If the partition configuration presents problems, also review the partition configuration.
liscal	Info	190	NMP%1 sync switch flag is set to ON. %2	The data synchronization is enabled.	-
liscal	Info	191	NMP%1 sync switch flag is set to OFF. %2	The data synchronization is disabled.	-
liscal	Info	192	NMP%1 open I/O port OK.	The I/O to the Data Partition started.	-
liscal	Info	193	NMP%1 close I/O port OK.	The I/O to the Data Partition stopped.	-
liscal	Info	194	NMP%1 open mount port OK.	The access to the mirror partition becomes possible.	-
liscal	Info	195	NMP%1 close mount port OK.	The access to the mirror partition becomes impossible.	-
liscal	Info	196	NMP%1 open N/W port OK.	The mirror synchronization data connection port is opened.	-
liscal	Info	197	NMP%1 close N/W port OK.	The mirror synchronization data connection port is closed.	-
liscal	Warning	200	NMP%1 bmp_size_in_sec (%2) is invalid.	The size of the area for the difference information is invalid. The Cluster Partition may be set incorrectly.	Check the settings of the cluster partition in the cluster configuration data.
liscal	Warning	201	NMP%1 failed to calculate bitmap offset (%2).	Calculation of the area of the difference information failed.	The OS may have become unstable. Restart the system.
liscal	Error	202	NMP%1 sector size of Data Partition (%2) is invalid.	The sector size of the Data Partition (%2) is too big.	Check if there is any incorrect setting with the mirror disk or the hybrid disk initial construction step.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	203	NMP%1 failed to get total_bitmap_in_bits (%2). (%3)	Getting the mirror difference information failed at procedure[%3].	Same as above.
liscal	Warning	204	NMP%1 no trans_table available,recovery failed.	The mirror recovery failed. The mirror recovery could not utilize the management area of recovery because the number of NMPs recovering mirror has exceeded the upper limit.	Check the number of NMPs in the cluster configuration data. A problem may have occurred with the mirror driver. Restart the system and execute the mirror recovery again.
liscal	Warning	205	NMP%1 failed to lock disk I/O, recovery failed.	The mirror recovery failed. The mirror recovery could not exclude the other disk I/O.	A problem may have occurred with the mirror driver. Restart the system and then execute the mirror recovery again.
liscal	Warning	206	NMP%1 current NMP has been already locked.	Excluding the other disk I/O has been already executed. (A number of mirror recovery processes tried to operate the same data block.)	A problem may have occurred with the mirror driver. Restart the system and execute the mirror recovery again.
liscal	Warning	207	NMP%1 current NMP has not been locked.	The exclusion with the other disk I/O has already been released.	Same as above.
liscal	Warning	208	NMP%1 waited for sync data (sector=%2) written to disk completely, but timeout.	The disk I/O to sector[%2] did not finish in time before reading the mirror recovery data. The mirror recovery is going to be executed.	-
liscal	Info	209	NMP%1 waiting for recovery data to be %2. (%3/%4)	A shutdown request arrived while mirror recovery data is [%2] (read or written). [%3] of [%4] was being processed. The system waits for the remaining I/O to be completed.	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	210	NMP%1 failed to connect to remote server (err=%2).	Connecting to the remote server failed because of the reason[%2].	• Check the settings of the mirror disk connect ion in the cluster configuration data. • Check the mirror disk connection status. Check if the mirror disk connection or OS is highly-loaded. • The connection time-out value may be too small. Increase the number. (see the after-mentioned coping process2 [2] .)
liscall	Info	211	NMP%1 failed to send %2, retrying again.	Sending [%2] failed. It will be sent again.	• Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily. This will not cause a problem on the operation immediately, however, may be a cause of mirror break in the long run. • The send time-out value may be too small. Increase the number. (see the after-mentioned coping process2 [2] .)

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	212	NMP%1 failed to send %2.	Sending [%2] failed.	Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily. Check if the mirror agent on the remote server is running.
liscal	Error	213	NMP%1 failed to read recovery data.	Reading the mirror recovery data failed.	• In case that the lack of resource is possible, execute the after-mentioned coping process 1 [1] (coping process to lack of resource). • The physical defect may have occurred with mirror disk in case of being output while in operation. See "The system maintenance information" in the "Maintenance Guide", exchange the mirror disks and run mirror recovery.
liscal	Warning	214	1. NMP%1 failed to write recovery data. 2. NMP%1 failed to write recovery data at remote server.	1. Writing the mirror recovery data failed at the local server. 2. Writing the mirror recovery data failed at the remote server.	Same as above.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	215	NMP%1 failed to recover because of %2.	• The disconnection of the mirror disk connection was detected before receiving the response to the sent mirror recovery data. • Or the mirror recovery was canceled. • The mirror recovery will stop.	Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Info	216	NMP%1 ACK timeout, %2, retrying again.	The response to the sent data (%2) of the mirror recovery could not be received in time. The data will be sent again.	• Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily. • Increase the timeout values and/or decrease the Recovery Data Size. (See the aftermentioned coping process 4 [4] .)
liscal	Warning	217	NMP%1 ACK timeout, %2, recovery failed.	The response to the sent data (%2) of the mirror recovery could not be received in time again. The mirror recovery failed.	• Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily. • Increase the timeout values and/or decrease the Recovery Data Size. (See the aftermentioned coping process 4 [4] .)

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	218	NMP%1 async send queue is full. Mirror break.	The queue for the data to be sent has become full. The mirror break status is set.	Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Info	219	NMP%1 can not send async data, because N/W port has been closed.	Data in the data transmission queue cannot be transmitted because the mirror disk connect is disconnected.	Check the connection status of the mirror disk connect. Check whether the mirror disk connect, disk I/O, or OS is highly loaded.
liscal	Warning	220	NMP%1 failed to create %2 socket (%3). or NMP%1 failed to create %2 socket.	Creation of the connection for [%2] failed because of the reason[%3].	• Check the settings of the mirror disk connection in the cluster configuration data. • Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily. • Check if other applications or the others are using the resources (port, etc.) for the mirror connection. (See the after-mentioned coping process 3 [3]) - In case that the lack of resource is possible, execute the after-mentioned coping process 1 [1] (coping process to lack of resource).
liscal	Warning	221	NMP%1 failed to bind %2 socket (%3).	Same as above.	Same as above.
liscal	Warning	222	NMP%1 failed to listen %2 socket (%3).	Same as above.	Same as above.
liscal	Warning	223	NMP%1 failed to accept %2 socket (%3).	Same as above.	Same as above.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	224	NMP%1 failed to receive %2 (err=%3). or NMP%1 failed to receive %2 (err=%3), %4.	Receiving data[%2] (of the [%4] area) because of the reason[%3].	• Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily. • The receive time-out value may be too small. Increase the number. See the after-mentioned coping process 2 [2] .

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	225	NMP%1 received wrong head part. (magic=%2 cmd=%3) (%4)	Invalid data was received. (magic=[%2], cmd=[%3])	• Applications other than EXPRESSCLUSTER may be using the mirror disk connect. Keep applications other than EXPRESSCLUSTER from accessing to the mirror connect. For the details of the ports used by EXPRESSCLUSTER, See "Communication ports", "Cluster driver device information" of "The system maintenance information" in the "Maintenance Guide". • A defect may have occurred with the mirror disk connect. Check the mirror disk connection status.
liscal	Warning	226	NMP%1 received wrong command (cmd=%2). or NMP%1 received wrong command (cmd=%2) instead of %3.	Invalid mirror data was received. (cmd=[%2]) Invalid data was received at the port for the [%3] (HB / ACK2). (cmd=[%2])	Same as above.
liscal	Warning	227	NMP%1 failed to uncompress %2.	Uncompression of the data[%2] failed.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource).

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	228	NMP%1 failed to execute received command. (cmd=%2, err=%3)	The request of [%2] had been received and processed, but [%3] error occurred.	For the details of the error, see the log output before this log.
liscal	Warning	229	NMP%1 failed to receive data, because recv_sock is NULL.	Receiving the mirror data failed.	A problem may have occurred with the mirror driver. Restart the system.
liscal	Info	230	NMP%1 recv_sock is NULL, can not delete keepalive timer.	Same as above.	Same as above.
liscal	Warning	231	NMP%1 accepted receive data, but this server is not current server of hybrid disk.	The local server received the mirror data even though the other server is running as the Current server of hybrid disk configuration. The received data was ignored. The received data will be sent again from the source server to the Current server.	-
liscal	Info	232	NMP%1 disconnected %2 N/W. (%3)	The connection to receive [%2] (DATA / HB / ACK2) was disconnected at procedure[%3].	-
liscal	Info	233	NMP%1 failed to receive recovery data at remote server, retrying again.	The remote server could not receive the recovery data. The local server is going to send it again.	Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Warning	234	NMP%1 failed to receive recovery data at remote server, recovery failed.	The remote server could not receive the recovery data again. Recovery was failed.	Same as above.
liscal	Warning	235	NMP%1 gave up ACK before ACK timeout.	Waiting for the response to the sent mirror recovery data (ACK) was suspended before ACK receive timeout occurs due to the disconnection of mirror disk connection.	Same as above.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	236	NMP%1 gave up ACK1 before ACK1 timeout.	Waiting for the response to the sent mirror recovery data (ACK1) was suspended before ACK receive timeout occurs due to the disconnection of mirror disk connection.	Same as above.
liscal	Warning	240	NMP%1 status of current using N/W is ERROR. (%2)	The mirror disk connection is abnormal. Then the data could not be sent.	Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Warning	241	NMP%1 can not find a N/W to use. (%2)	There is no mirror disk connection available for [%2] (DATA / HB / ACK2).	Check the cluster configuration information. Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Warning	242	NMP%1 all of the networks are ERROR.	All the mirror disk connections became abnormal.	Same as above.
liscal	Info	243	NMP%1 N/W is %2 %3 - %4 :%5(%6) or NMP%1 N/W is %2 %3 - %4	The status of the current mirror disk connection for [%6] (DATA / HB / ACK2) was changed to [%2] (ERROR / USING / FREE). IP addresses: [%3] and [%4] Port: [%5]	Check the mirror disk connection status in case that the status is ERROR. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Warning	250	Received ICMP. Length of received ICMP is less than 8.	ICMP packet was received. But its length was Invalid. It was Ignored.	-
liscal	Info	251	Received ICMP. Type=(%1) Code=(%2)	ICMP packet of type [%1] and code [%2] was received. ("Destination unreachable" was received.)	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Info	252	Received ICMP. Type=(%1) Code=(%2). Ignored. or Received ICMP. Type=(%1) with same ID(%3). Ignored.	ICMP packet of type [%1] , code [%2] and ID [%3] was received. It was Ignored.	-
liscal	Warning	260	NMP%1 failed to switch N/W to (priority:%2). (%3)	Switching the mirror disk connection was requested. But it failed because of the reason [%3].	• Check the cluster configuration information. • Check the mirror disk connection status. Check that neither mirror disk connection nor the operating system is loaded heavily.
liscal	Info	261	NMP%1 already switched N/W to (priority:%2).	Switching the mirror disk connection was requested. But it has already been switched to [%2].	-
liscal	Info	262	NMP%1 uses N/W (priority:%2).	The mirror disk connection of the priority [%2] will be used.	-
liscal	Info	263	NMP%1 switched N/W from (priority:%2) to (priority:%3).	Switching the mirror disk connection was requested. Then the mirror disk connection of the priority [%2] will be used instead of the priority [%3].	-
liscal	Info	270	NMP%1 this FS type (%2) is not supported for high speed full copy.	In the current version this file system cannot be processed with the high speed full-copy. Full-copy will be performed without an analysis of the file system instead.	-
liscal	Info	271	NMP%1 FS type is %2.	The target file systems for mirror recovery are [%2] (EXT2 / EXT3 / EXT4).	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Warning	272	NMP%1 could not read %2 of FS.	Reading the [%2] area of the file system failed. Full-copy will be performed without an analysis of the file system instead.	-
liscal	Warning	273	NMP%1 failed to set the bitmap dependent on FS.	Creation of the difference information corresponding to the area used by the file system failed. Full-copy will be performed without an analysis of the file system instead	-
liscal	Info	280	NMP%1 requested to change compress flag. (Sync data : %2) (Recovery data : %3)	Compression of the mirror transfer data was changed to [%2] (ON / OFF) and [%3] (ON / OFF).	-
liscal	Info	281	NMP%1 flag of compress (Sync data:%2) (Recovery data:%3)	The compression function for mirror transfer data is set to [%2](ON/OFF) and [%3](ON/OFF).	-
liscal	Info	290	NMP%1 logging statistics information started. (PID=%2)	Logging of mirror statistic information has started.	-
liscal	Info	291	NMP%1 logging statistics information stopped. (PID=%2)	Logging of mirror statistic information has stopped.	-
liscal	Info	292	NMP%1 logging statistics information cleared.	The mirror statistic information counter has been cleared.	-
liscal	Warning	293	NMP%1 statistics information not found. (PID=%2)	Internal error Processing has not yet been started, or an attempt was made to access a mirror statistic information record that had already ended.	If mirror statistic information was already acquired by a command, reexecute that command.
liscal	Info	294	Perf%1	Output result [%1] of mirror statistic information	-
liscal	Info	300	NMP%1 QoS %2 KB/sec.	The band limitation was set to [%2].	-

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	310	NMP%d failed to delete history information. (%1)	The history of unsent data was not deleted.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource) when the lack of resource is possible. The physical defect may have occurred with mirror disk in case of being output while in operation. See "The system maintenance information" in the "Maintenance Guide", exchange the mirror disks and run mirror recovery.
liscal	Error	311	NMP%d failed to read history information. (%1)	The history of unsent data was not read.	The physical defect may have occurred with mirror disk in case of being output while in operation. See "The system maintenance information" in the "Maintenance Guide", exchange the mirror disks and run mirror recovery.
liscal	Error	312	NMP%d failed to write history information. (%1)	The history of unsent data was not written.	Same as above.
liscal	Error	313	NMP%d failed to write history information. (overflow)	The number of records reached the maximum of the history of unsent data.	• Check the mirror disk connection status. Check if the mirror disk connection or OS is highly-loaded. • Check the setting to make sure that the history recording area size is not too small.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	321	NMP%d failed to read a history file. (%1)	The history file was not read.	• Execute the after-mentioned coping process 1 [1] (coping process to lack of resource) when the lack of resource is possible. • The OS may have become unstable. Restart the system. • The physical defect may have occurred with the disk of the history file directory in case of being output while in operation. Change the settings of the history file directory or replace the disk.

Continued on next page

Table 10.4 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
liscal	Error	322	NMP%d failed to write a history file. (%1)	The history file was not written.	Execute the aftermentioned coping process 1 [1] (coping process to lack of resource) when the lack of resource is possible. The OS may have become unstable. Restart the system. The partition of the history file directory may not have enough free space. Maintain enough free space. The physical defect may have occurred with the disk of the history file directory in case of being output while in operation. Change the settings of the history file directory or replace the disk.
liscal	Error	323	NMP%d failed to write a history file. (overflow)	The total size reached the maximum of the history file.	• Check the mirror disk connection status. Check if the mirror disk connection or OS is highly-loaded. • Check that the setting of the history file capacity is not too small.
liscal	Error	324	NMP%d failed to delete a history file. (%1)	The history file was not deleted.	Check that the history file directory or the file in it has been used by any other application.
liscal	Error	330	NMP%d Internal error. (%1)	Internal error.	A problem may have occurred with the mirror driver. Restart the system.
liscal	Info	331	--- Previous liscal message repeated %1 times ---	The last message was output consecutively %1 times.	-

[1] coping process 1 coping process to lack of resource

The physical memory may be running short. Add more physical memory or stop unnecessary applications.
The upper limit of I/O request queue number ensured by the mirror driver may be too big. In case that a massive amount of I/O over transaction performance are requested to the mirror disk, the kernel memory is used because the I/O requests are queued in the mirror driver. Decrease the maximum number of the request queue in "Mirror Driver" tab of "Cluster Properties" by seeing " 2. *Parameter details*" in this guide.
The file system may ensure a massive amount of the cache. In case that a massive amount of I/O over transaction performance are requested, the memory zone for kernel space may be used for the file system cache in addition to the cache and the memory zone for user space. In that case, as a workaround, keep the memory zone for kernel space used by the driver from being utilized as the cache by setting /proc/sys/vm/lower_zone_protection. See "Cache swell by a massive I/O" in "Notes and Restrictions" in the "Getting Started Guide".

[2] coping process 2 Parameters

Parameter names output in log	Setting Item Names in the Cluster WebUI	Positions of Setting Items in the Cluster WebUI
Bitmap refresh interval	Bitmap Refresh Interval (bpchkinterval)	Cluster Properties Mirror Driver tab
max_cachenum	(maxcache)	(In the configuration file)
send_queue_size	The number of queues (sendqueuesize)	Mirror Disk Resource Tuning Properties Mirror tab
band_limit_mode	Rate limitation of Mirror Connect (mode)	Same as above.
band_limit	Rate limitation of Mirror Connect (bandlimit)	Same as above.
ack_timeout	Ack Timeout (acktimeout)	Mirror Disk Resource Tuning Properties Mirror Driver tab

Continued on next page

Table 10.6 – continued from previous page

Parameter names output in log	Setting Item Names in the Cluster WebUI	Positions of Setting Items in the Cluster WebUI
connect_timeout	Connection Timeout (connecttimeout)	Same as above.
send_timeout	Send Timeout (sendtimeout)	Same as above.
receive_normal_timeout	Receive Timeout (recvnormaltimeout)	Same as above.
hb_interval	Heartbeat Interval (hbinterval)	Same as above.
hb_recv_timeout	ICMP Receive Timeout (pingtimeout)	Same as above.
hb_recv_retry	ICMP Retry Count (pingretry)	Same as above.
keepalive_time	(keepalive/timeout)	(In the configuration file)
keepalive_probe	(keepalive/prob)	Same as above.
keepalive_interval	(keepalive/interval)	Same as above.
lastupdate_delay	(lupdatedelay)	Same as above.

For the details of each parameter, see the following chapters in this Guide.

- "*Cluster properties*" in "2. *Parameter details*"
- "*Understanding Mirror disk resources*" and "*Understanding Hybrid disk resources*" in "3. *Group resource details*"
- "*Adjusting time-out temporarily (clptoratio command)*" in "8. *EXPRESSCLUSTER command reference*"

[3] coping process 3 For the details of the ports used by the mirror driver, see the following.

- "Connection port number" in "Notes and Restrictions" in the "Getting Started Guide"
- "Changing the range of automatic allocation for the communication port numbers" in "Notes and Restrictions" in the "Getting Started Guide"
- "*Understanding mirror parameters*" of "3. *Group resource details*" in the "Reference Guide"
- "Mirror driver tab" of "3. *Group resource details*" in the "Reference Guide"
- "Communication ports" of "The system maintenance information" in the "Maintenance Guide"

- "Settings after configuration hardware" of "Determining a system configuration" in the "Installation and Configuration Guide"

[4] coping process 4 Timeout parameters of mirror

Setting Item Names in the Cluster WebUI	Positions of Setting Items in the Cluster WebUI
Recovery Data Size	Cluster Properties Mirror Agent tab
Ack Timeout	Mirror Disk Resource Tuning Properties
Connection Timeout Mirror Driver tab	Same as above.
Send Timeout	Same as above.
Receive Timeout	Same as above.

For the details of each parameter, see the following chapters in this guide.

- "*Cluster properties*" in "2. *Parameter details*"
- "*Understanding Hybrid disk resources*" and "*Understanding Hybrid disk resources*" in "3. *Group resource details*"
- "*Adjusting time-out temporarily (clptoratio command)*" in "8. *EXPRESSCLUSTER command reference*"

10.3.2 Kernel mode LAN heartbeat driver

Module Type	Event type	Event ID	Message	Description	Solution
clpkhb	Info	101	Kernel Heartbeat was initialized successfully. (major=%1, minor=%2)	The clpkhb driver was successfully loaded.	-
clpkhb	Info	102	Kernel Heartbeat was released successfully.	The clpkhb driver was successfully unloaded.	-
clpkhb	Error	103	Can not register miscdev on minor=%1. (err=%2)	Loading the clpkhb driver failed.	-
clpkhb	Error	104	Can not deregister miscdev on minor=%1. (err=%2)	Unloading the clpkhb driver failed.	-
clpkhb	Info	105	Kernel Heartbeat was initialized by %1.	The clpkhb driver was successfully initialized by [%1] module.	-
clpkhb	Info	106	Kernel Heartbeat was terminated by %1.	The clpkhb driver was successfully terminated by [%1] module.	-
clpkhb	Error	107	Can not register Kernel Heartbeat proc file!	The clpkhb driver failed to create proc file.	-

Continued on next page

Table 10.8 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
clpkhb	Error	108	Version error.	The inside version information of the clpkhb driver is invalid.	Reinstall EXPRESSCLUSTER.
clpkhb	Info	110	1. The send thread has been created. (PID=%1) 2. The recv thread has been created. (PID=%1)	1. The send thread of the clpkhb driver was successfully created. Its process ID is [%1]. 2. The receive thread of the clpkhb driver was successfully created. Its process ID is [%1].	-
clpkhb	Error	111	1. Failed to create send thread. (err=%1) 2. Failed to create recv thread. (err=%1)	1. The clpkhb driver failed to create the send thread due to the error [%1]. 2. The clpkhb driver failed to create the receive thread due to the error [%1].	-
clpkhb	Info	112	1. Killed the send thread successfully. 2. Killed the recv thread successfully.	1. The send thread of clpkhb driver was successfully stopped. 2. The receive thread of clpkhb driver was successfully stopped.	-
clpkhb	Info	113	Killed the recv thread successfully.	The clpkhb driver is going to stop.	-
clpkhb	Info	114	Killed the recv thread successfully.	The clpkhb driver is going to stop.	-
clpkhb	Info	115	Kernel Heartbeat has been stopped	The clpkhb driver successfully stopped.	-

Continued on next page

Table 10.8 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
clpkhb	Error	120	1. Failed to create socket to send %1 packet. (err=%2) 2. Failed to create socket to receive packet. (err=%2)	1. Creating the socket for sending the [%1] (HB / DOWN / KA) packet failed due to the error [%2]. 2. Creating the socket for receiving the packet failed due to the error [%2].	-
clpkhb	Error	121	Failed to create sending %1 socket address. (err=%2)	Setting the socket for sending the [%1] (HB / DOWN / KA) packet failed.	The physical memory may be running out. Add physical memories, or terminate unnecessary applications.
clpkhb	Error	122	Failed to create %1 socket address. (err=%2)	Setting the socket for sending the [%1] (HB / DOWN / KA) packet failed.	The physical memory may be running out. Add physical memories, or terminate unnecessary applications.
clpkhb	Error	123	Failed to bind %1 socket. (err=%2)	Binding the socket for [%1] (HB / DOWN / KA) failed.	• Check the status of the operating system. • The communication port for clpkhb may be used already by other applications or others. Check the usage status of the communication port. • Check the cluster configuration information server property if the IP address set for the interconnect LAN I/F is correct.

Continued on next page

Table 10.8 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
clpkhb	Error	125	Failed to send %1 data to %2. (err=%3)	Sending [%1] (HB / DOWN / KA) data to [%2] failed.	• Check the status of the network for the clpkhb communication. • Check the status of the remote server. • Check that the setting information is correct.
clpkhb	Error	126	Failed to receive data. (err=%3)	Receiving data failed.	• The remote server may be down. Check if the server is active. • If the server is not down, check the status of the network for clpkhb.
clpkhb	Info	127	1. Received an invalid packet. Magic is not correct! 2. Received an invalid packet from %1. Magic(%2) is not correct!	1. An invalid packet was received. It is ignored. 2. An invalid packet [%2] was received from [%1]. It is ignored.	Other applications may be sending the data to the port for clpkhb. Change the Heartbeat Port Number if other applications use it.
clpkhb	Error	128	1. Received an invalid packet. %1 is not correct! 2. Received an invalid packet from %1. %2 is not correct!	1. An invalid packet was received. The invalid part of the packet is [%1] (Resource priority / Source ip address). 2. An invalid packet was received from [%1]. The invalid part of the packet is [%2] (Resource priority/Source ip address).	Same as above.
clpkhb	Info	129	Receiving operation was interrupted by ending signal!	The receive thread ends by termination signal.	-

Continued on next page

Table 10.8 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
clpkhb	Info	130	1. clpka: <server priority: %1> <reason: %2> <process name: %3> system reboot. 2. clpka: <server priority: %1> <source: %2> <exit code: %3> system reboot.	1. A reset message was received from another server. The priority [%1] server is going to be reset because of the reason [%2] in the process [%3]. 2. A reset message was received from another server. The priority [%1] server is going to be reset because [%2] was terminated with the termination code [%3].	Check the status of the server where the reboot occurred.
clpkhb	Info	131	1. clpka: <server priority: %1> <reason: %2> <process name: %3> system panic. 2. clpka: <server priority: %1> <source: %2> <exit code: %3> system panic.	1. A panic message was received from another server. A panic of the priority [%1] server is going to be performed because of the reason [%2] in the process [%3]. 2. A panic message was received from another server. A panic of the priority [%1] server is going to be performed because [%2] was terminated with the termination code [%3].	Check the status of the server where the panic occurred.
clpkhb	Error	140	Reference an inaccessible memory area!	ioctl() failed to pass data to an application.	Check the status of the operating system.
clpkhb	Error	141	Failed to allocate memory!	Memory allocation failed.	The physical memory may be running out. Add physical memories, or terminate unnecessary applications.

Continued on next page

Table 10.8 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
clpkhb	Error	142	Invalid argument, %1!	The parameter passed to the clpkhb driver is not correct.	Check if the settings are correct.
clpkhb	Warning	143	Local node has nothing with current resource.	The heartbeat resource information passed to the clpkhb driver is not correct.	Same as above.

10.3.3 Keepalive driver

Module Type	Event type	Event ID	Message	Description	Solution
clpka	Info	101	Kernel Keepalive was initialized successfully. (major=%1, minor=%2)	The clpka driver was successfully loaded.	-
clpka	Info	102	Kernel Keepalive was released successfully.	The clpka driver was successfully unloaded.	-
clpka	Error	103	Can not register miscdev on minor=%1. (err=%2)	Loading the clpka driver failed.	Check the distribution and kernel support the kernel mode LAN heartbeat.
clpka	Info	105	Kernel Keepalive was Initialized by %1.	The clpka driver was successfully initialized.	-
clpka	Error	107	Can not register Kernel Keepalive proc file!	The clpka driver failed to create proc file.	The kernel may not be running normally because of lack of memory or other reasons. Add physical memories, or terminate unnecessary applications.
clpka	Error	108	Version error.	The version of the clpka driver is invalid.	Check if the installed clpka driver is legitimate.
clpka	Error	111	Failed to create notify thread. (err=%1)	The clpka driver failed to create the thread.	The kernel may not be running normally because of lack of memory or other reasons. Add physical memories, or terminate unnecessary applications.
clpka	Info	130	Reboot tried.	The clpka driver is going to restart the machine according to the action setting.	-
clpka	Info	132	Kernel do nothing.	The clpka driver is not going to do anything according to the action setting.	-

Continued on next page

Table 10.9 – continued from previous page

Module Type	Event type	Event ID	Message	Description	Solution
clpka	Error	140	Reference an inaccessible memory area!	Passing the version information of the clpka driver to the cluster main body failed.	Check if the installed clpka driver is legitimate.
clpka	Error	141	Failed to allocate memory!	The size of physical memory is not sufficient.	The physical memory is running out. Add physical memories, or terminate unnecessary applications.
clpka	Error	142	Invalid argument, %1!	Invalid information was passed from the cluster main body to the clpka driver.	Check if the installed clpka driver is legitimate.
clpka	Error	144	Process (PID=%1) is not set.	A process other than cluster main body tried operation to the clpka driver.	Check if there is any application trying to access to the clpka driver erroneously.

10.4 Detailed information in activating and deactivating group resources

10.4.1 Floating IP resources

Module type	Type	Return value	Message	Description	Solution
fip	Error	3	Command failed. (%1, ret=%2)	Failed in executing the command %1. The return value is %2.	Analyze the failure from the return value of the command.
fip	Error	11	Command failed. (%1(%2), errno=%3)	An error has occurred in executing the command.	Memory or OS resources may not be sufficient. Check them.
fip	Error	14	IP address did not exist.	Failed to get the IP address list.	Confirm that the OS can use the TCP/IP protocol.
fip	Error	15	IP address was already used.	The IP address is already used.	Check the IP address is not already used.
fip	Error	15	This ip address was already used. IP=%1	The specified IP address exists on the same network.	Check if the specified IP address is not used on the network.
fip	Error	17	Fip interface was not found.	Floating IP address interface was not found.	Check if the FIP address network is the same as the server's real IP address.
fip	Error	others	Internal error. (status=%1)	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.2 Virtual IP resource

Module type	Type	Return value	Message	Description	Solution
vip	Error	3	Command failed. (%1, ret=%2)	Failed in executing the command %1. The return value is %2.	Analyze the failure from the return value of the command.
vip	Error	11	Command failed. (%1(%2), errno=%3)	An error has occurred in executing the command.	Memory or OS resources may not be sufficient. Check them.
vip	Error	14	IP address did not exist.	Failed to acquire the list of IP addresses.	Check the OS is in the environment that supports the TCP/IP protocol.
vip	Error	15	IP address was already used.	The IP address is already used.	Check if the IP address is not already used.
vip	Error	15	This ip address was already used. IP=%1	The specified IP address exists on the same network.	Check if the specified IP address is not already used on the network.
vip	Error	17	Vip interface was not found.	The specified interface was not found.	Check if the specified interface exists on the server.
vip	Error	Others	Internal error. (status=%1)	Other internal error was occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.3 Disk resources

Module type	Type	Return value	Message	Description	Solution
disk	Error	1	Resource name was invalid. (%1)	The resource name is invalid.	Check the resource name is consistent with the information in the cluster configuration data.
disk	Error	1	Group name was invalid. (%1)	The group resource name is invalid.	Check the group name is consistent with the information in the cluster configuration data.
disk	Error	1	Resource was not in config. (%1)	The resource name does not exist in the cluster configuration data.	Check the resource name is consistent with the information in the cluster configuration data.
disk	Error	1	Group was not in config. (%1)	The group resource name does not exist in the cluster configuration data.	Check the group resource name is consistent with the information in the cluster configuration data.
disk	Error	1	Getting of config was failed.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.

Continued on next page

Table 10.12 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
disk	Error	1	Mount point was already mounted. (%1)	The device has already been mounted.	Check if the specified device is unmounted.
disk	Error	1	Mount point was not mounted. (%1)	The mount point was not mounted.	An active resource may have been manually unmounted. Check its status.
disk	Error	1	Mount point was invalid. (%1)	The mount point is invalid.	Check the mount point exists.
disk	Error	1	Creating of mount point was failed. (%1)	Failed to create the mount point.	Memory or OS resources may not be sufficient. Check them.
disk	Error	1	Raw device was already bound. (%1)	The RAW device has already been bound by another device.	Check if the unique raw device is set in the cluster.
disk	Error	1	Max recover retry over. (%1, retry=%2)	The number of retires made for activating the device has exceeded the maximum retry count.	Check the cluster configuration data is correct.
disk	Error	1	Command path was invalid. (%1)	The execution path is invalid.	Check the command execution path.
disk	Error	1	Command timeout. (%1, timeout=%2)	Detected an internal timeout.	The OS may be heavily loaded. Check its status.
disk	Error	1	Command failed. (%1, ret=%2)	The command %1 failed. Its return value is %2.	Troubleshoot the problem by using the return value from the command.
disk	Error	1	Command failed. (%1(%2), errno=%3)	The device operation terminated abnormally.	Memory or OS resources may not be sufficient. Check them.
disk	Error	1	Internal error. (status=%1)	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.4 NAS resources

Module Type	Type	Return value	Message	Description	Solution
nas	Error	1	Resource name was invalid. (%1)	The resource name is invalid.	Check the resource name is consistent with the information in the cluster configuration data.
nas	Error	1	Group name was invalid. (%1)	The group resource name is invalid.	Check the group name is consistent with the information in the cluster configuration data.

Continued on next page

Table 10.13 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
nas	Error	1	Resource was not in config. (%1)	The resource name does not exist in the cluster configuration data.	Check the resource name is consistent with the information in the cluster configuration data.
nas	Error	1	Group was not in config. (%1)	The group resource name does not exist in the cluster configuration data.	Check the group resource name is consistent with the information in the cluster configuration data.
nas	Error	1	Getting of config was failed.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.
nas	Error	1	Mount point was already mounted. (%1)	The resource on the NAS server has already been mounted.	Check if the specified resource in the NAS server is unmounted.
nas	Error	1	Mount point was not mounted. (%1)	The mount point was not mounted.	The active resource may have been manually unmounted. Check its status.
nas	Error	1	Mount point was invalid. (%1)	The mount point is invalid.	Check the mount point exists.
nas	Error	1	Creating of mount point was failed. (%1)	Failed to create the mount point.	Memory or OS resources may not be sufficient. Check them.
nas	Error	1	Max recover retry over. (%1, retry=%2)	The number of retries made for mounting resource on the NAS server has exceeded the maximum retry count.	Check that the cluster configuration data is correct.
nas	Error	1	Command path was invalid. (%1)	The execution path is invalid.	Check the command execution path.
nas	Error	1	Command timeout. (%1, timeout=%2)	Detected an internal timeout.	The OS may be heavily loaded. Check its status.
nas	Error	1	Command failed. (%1, ret=%2)	The command %1 failed. Its return value is %2.	Troubleshoot the problem by using the return value from the command.
nas	Error	1	Command failed. (%1(%2), errno=%3)	An error occurred while running the command.	Memory or OS resources may not be sufficient. Check them.
nas	Error	1	Internal error. (status=%1)	Other internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.5 EXEC resources

Module Type	Type	Return value	Message	Description	Solution
exec	Error	1	Termination code %1 was returned.	An exit code other than 0 (zero) was returned as the result of a synchronous script or application.	There may be a problem in the content of the script. Check the script is correct. The application may have abnormally terminated. Check how the application is working.
exec	Error	1	Command was not completed within %1 seconds.	A synchronous script or application did not successfully complete within the specified time.	There may be a problem in the content of the script. Check if the script is correct. The application may be stalling. Check if the application is working properly. You may be able to identify the cause from the logs in both cases. For details about logging settings, see "2. *Parameter details*".
exec	Error	1	Command was aborted.	A synchronous script or application terminated abnormally.	The application may have abnormally terminated. Check how the application is working. Memory or OS resources may not be sufficient. Check them.
exec	Error	1	Command was not found. (error=%1)	The application does not exist.	The path to the application may be invalid. Check it in the cluster configuration data
exec	Error	1	Command string was invalid.	The application path is invalid.	Check the application path in the cluster configuration data.
exec	Error	1	Log string was invalid.	The log output path is invalid.	Check the log output path in the cluster configuration data.

Continued on next page

Table 10.14 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
exec	Error	1	Internal error. (status=%1)	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.6 Mirror disk resources

Module Type	Type	Return value	Message	Description	Solution
md	Error	1	Need to start mirror agent at first.	The Mirror Agent is not active.	Check if the Mirror Agent is activated.
md	Error	2	Options or parameters are invalid.	Parameters are invalid.	Check the cluster configuration data is correct.
md	Error	4	Getting of config was failed.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.
md	Error	10	NMP size of local server is bigger, can not active	The server cannot activate the mirror disk resource because the size of NMP of the local server is larger than that of the remote server.	Execute the forcible mirror recovery using the remote server as the one to be mirrored.
md	Error	30	Internal error[status=%1]	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them. If the status is 2359554, the previous start or execution of a system command such as fsck may have failed. In this case, check the result of the failed command.
md	Error	77	Mirror disk was not in config.(%1)	Configuration data of the mirror disk resource is invalid.	Check the cluster configuration data is correct.
md	Error	79	Failed to get cluster partition information.	Failed to obtain the cluster partition data.	Check the partition is allocated and the operating system can recognize the disk.
md	Error	80	Mount point was already mounted.(%1)	The mount point has already been mounted.	Check if the mount point of the mirror disk resource has been mounted manually.
md	Error	81	The local server has not the latest data.(%1)	The local server does not have the latest data.	Perform the mirror recovery.

Continued on next page

Table 10.15 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
md	Error	82	Failed to set cluster partition information.	Failed to access the cluster partition.	Check if the partition is allocated, and the operating system can recognize the disk.
md	Error	83	Command timeout(%1, timeout=%2)	The system command timed out.	It took longer than expected to run the system command. Tune the mount time-out, unmount time-out, and fsck time-out values. For details, see "2. *Parameter details*"
md	Error	84	Mount point was not mounted. (%1)	The mirror disk resource is not mounted.	Check if it has manually been unmounted. Check the memory. EXPRESSCLUSTER controls mounting and unmounting. Do not mount or unmount it manually.
md	Error	87	Creating of mount point was failed. (%1)	Failed to create the mount point.	Check mount point has been specified in the cluster configuration data. Check if the mount point exists.
md	Error	89	Command failed. (%1)	Failed to run the system command.	Check if mount, unmount and fsck commands exist.

10.4.7 Hybrid disk resources

Module Type	Type	Return value	Message	Description	Solution
hd	Error	1	Need to start mirror agent at first.	The Mirror Agent is not active.	Check if the Mirror Agent is activated.
hd	Error	2	Options or parameters are invalid.	Parameters are invalid.	Check the cluster configuration data is correct.
hd	Error	4	Getting of config was failed.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.

Continued on next page

Table 10.16 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
hd	Error	10	NMP size of local server is bigger, can not active	The server cannot activate the mirror disk resource because the size of NMP of the local server is larger than that of the remote server.	Execute the forcible mirror recovery using the remote server as the one to be mirrored.
hd	Error	12	The local server is not current server.	Resources cannot be operated because the local server is not current server.	Operate the resources after acquiring the condition where current priority can be acquired in the local server or acquiring the current priority.
hd	Error	30	Internal error[status=%1]	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
hd	Warning	48	The Auto mirror recovery check box is not selected. It is necessary to recover the mirror manually, in order to resume mirroring (%1).	The resumption of mirroring requires recovering the mirror manually.	Start the mirror recovery with the command or from the mirror disk list.
hd	Error	77	Hybrid disk was not in config.(%1)	Configuration data of the hybrid disk resource is invalid.	Check the cluster configuration data is correct.
hd	Error	79	Failed to get cluster partition information.	Failed to obtain the cluster partition data.	Check the partition is allocated and the operating system can recognize the disk.
hd	Error	80	Mount point was already mounted.(%1)	The mount point has already been mounted.	Check if the mount point of the mirror disk resource has been mounted manually.
hd	Error	81	The local server has not the latest data.(%1)	The local server does not have the latest data.	Perform the mirror recovery.
hd	Error	82	Failed to set cluster partition information.	Failed to access the cluster partition.	Check if the partition is allocated, and the operating system can recognize the disk.
hd	Error	83	Command timeout(%1, timeout=%2)	The system command timed out.	It took longer than expected to run the system command. Tune the mount time-out, unmount time-out, and fsck time-out values. For details, see "2. *Parameter details*"

Continued on next page

Table 10.16 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
hd	Error	84	Mount point was not mounted. (%1)	The mirror disk resource is not mounted.	Check if it has manually been unmounted. Check the memory. EXPRESSCLUSTER controls mounting and unmounting. Do not mount or unmount it manually.
hd	Error	87	Creating of mount point was failed. (%1)	Failed to create the mount point.	Check mount point has been specified in the cluster configuration data. Check if the mount point exists.
hd	Error	89	Command failed. (%1)	Failed to run the system command.	Check if mount, unmount and fsck commands exist.
hd	Error	90	Failed to be current server.	Current priority cannot be acquired.	Check if hybrid disk resource is activated. If the hybrid disk is being recovered or current priority is being processed in another server, wait for a while.

10.4.8 Volume manager resources

Module Type	Type	Return value	Message	Description	Solution
volmgr	Error	4	Invalid Config.	The cluster configuration information is invalid.	Check if the cluster configuration information is consistent.
volmgr	Error	10	Already Imported.	The target has already been imported.	Check the target has been exported before startup of the cluster.
volmgr	Error	11	Other Host Imported.(host=%1)	The target has already been imported by host %1.	Check whether the target has been exported before startup of the cluster.
volmgr	Error	12 14	Command("%1") Error.(cmdret=%2)	Command %1 failed. The return value of the command is %2.	Analyze the error by the return value of the command.

Continued on next page

Table 10.17 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
volmgr	Error	Other	Internal Error.(ret=%1)	Another internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.9 VM resources

Module Type	Type	Return value	Message	Description	Solution
vm	Error	1 to 6, 8	Initialize error occurred.	An error was detected while initialization.	Check if the cluster configuration information is correct.
vm	Error	7	Parameter is invalid.	The parameter is invalid.	Check if the cluster configuration information is correct.
vm	Error	9 to 13	Failed to %s virtual machine %s.	Failed to control the virtual machine.	Check the status of the virtual machine.
vm	Error	22	Datastore must be setted.	The datastore name must be set for the Cluster WebUI.	Click the Details tab of VM Resources Properties in the Cluster WebUI, enter the name of data store containing the virtual machine configuration information to Data Store Name. And then click Apply the Configuration File.
vm	Error	23	VM configuration file path must be setted.	The VM configuration file path must be set for the Cluster WebUI.	Click the Details tab of VM Resources Properties in the Cluster WebUI, enter the path where the virtual machine configuration information is stored to VM Configuration File Path. And then click Apply the Configuration File.
vm	Error	Other	Internal error occurred.	Another internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.10 Dynamic DNS resources

Module Type	Type	Return value	Message	Description	Solution
ddns	Error	1	Initialize error.	An error was detected during initialization.	There might not be enough memory space or OS resources. Check whether this is so.
ddns	Error	2	open() failed.(err=%1)	Opening the internally used file failed.	There might not be enough memory space or OS resources. Check whether this is so.
ddns	Error	3	write() failed.(err=%1)	Writing to the internally used file failed.	There might not be enough memory space or OS resources. Check whether this is so.
ddns	Error	4	closed() failed.(err=%1)	Closing the internally used file failed.	There might not be enough memory space or OS resources. Check whether this is so.
ddns	Error	5	nsupdate command has failed(%1).	Executing the nsupdate command failed.	Analyze the error by referring to the command return value.
ddns	Error	90	Memory allocation error.(err=%1)	An internal memory allocation error occurred.	There might not be enough memory space or OS resources. Check whether this is so.
ddns	Error	92	Time out.	An internal timeout was detected.	The OS might be heavily loaded. Check whether this is so.
ddns	Error	Other	Internal error.(status=%d)	A different internal error occurred.	There might not be enough memory space or OS resources. Check whether this is so.

10.4.11 AWS elastic ip resources

Module Type	Type	Return value	Message	Description	Solution
awseip	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awseip	Error	5	The allocation ID '%1' does not exist	The specified EIP ALLOCATION ID %1 does not exist.	Check if the value of EIP ALLOCATION ID is correct.
awseip	Error	5	The networkInterface ID '%1' does not exist)	The specified ENI ID %1 does not exist.	Check if the value of ENI ID is correct.
awseip	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.

Continued on next page

Table 10.20 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
awseip	Error	7	ENI ID is invalid.(ENI ID=%1)	ENI ID is invalid.	Check if the ENI ID is correct. Check if ENI ID of other instance is specified mistakenly
awseip	Error	99	Internal error. (status=%1)	An internal error occurred.	Check if Python is installed correctly. Check if AWS CLI is installed correctly. Memory or OS resources may not be sufficient. Check them.

10.4.12 AWS virtual ip resources

Module Type	Type	Return value	Message	Description	Solution
awsvip	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsvip	Error	5	The vpc ID '%1' does not exist	The specified VPC ID %1 does not exist.	Check if the value of VPC ID is correct.
awsvip	Error	5	The networkInterface ID '%1' does not exist)	The specified ENI ID %1 does not exist.	Check if the value of ENI ID is correct.
awsvip	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsvip	Error	7	The VIP address %1 belongs to a VPC subnet.	The VIP address %1 belongs to a VPC CIDR.	For the VIP address, an IP address not belonging to a VPC CIDR must be specified. Check the VIP address.
awsvip	Error	8	Failed to add the VIP address %1.	Failed to add the VIP address %1.	Check the VIP settings. Memory or OS resources may not be sufficient. Check them.
awsvip	Error	9	Failed to delete the VIP address %1.	Failed to delete the VIP address %1.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 10.21 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
awsvip	Error	10	The VIP address %1 is already used.	The VIP address %1 is already used.	Check if the VIP address is already used.
awsvip	Error	11	ENI ID is invalid.(ENI ID=%1)	ENI ID is invalid.	Check if the ENI ID is correct. Check if ENI ID of other instance is specified mistakenly.
awsvip	Error	99	Internal error. (status=%1)	An internal error occurred.	Check if Python is installed correctly. Check if AWS CLI is installed correctly. Memory or OS resources may not be sufficient. Check them.

10.4.13 AWS DNS resource

Module Type	Type	Return value	Message	Description	Solution
awsdns	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsdns	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsdns	Error	99	Internal error. (status=%1)	An internal error occurred.	Confirm that Python is installed correctly. Confirm that AWS CLI is installed correctly. Memory or OS resources may not be sufficient. Check them.

10.4.14 Azure probe port resources

Module Type	Type	Return value	Message	Description	Solution
azurepp	Error	5	Probe port %1 is already used.	Probe port %1 is already used.	Check if the probe port is already opened on the local server.
azurepp	Error	6	Failed to open the probe port %1.	Releasing probe port %1 failed.	Memory or OS resources may not be sufficient. Check them.
azurepp	Error	7	Failed to close the probe port %1.	Closing probe port %1 failed.	Memory or OS resources may not be sufficient. Check them.
azurepp	Error	8	Failed to stop the probe port %1 control process.	Stopping probe port %1 control process failed.	Memory or OS resources may not be sufficient. Check them. Reboot the OS.
azurepp	Error	9	The probe port %1 control process has already started.	Probe port %1 control process is already started.	Memory or OS resources may not be sufficient. Check them. Or, the immediately preceding deactivation may have failed. In that case, stop the cluster and forcibly terminate the probe port control process (clpazureppp) manually.
azurepp	Error	10	Failed to start the probe port %1 control process.	Starting probe port %1 control process failed.	Memory or OS resources may not be sufficient. Check them.
azurepp	Error	99	Internal error. (status=%1)	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.15 Azure DNS resource

Module Type	Type	Return value	Message	Description	Solution
azuredns	Error	41	Timeout occurred when Azure CLI command was executed.	The Azure CLI command was not executed within **Azure CLI Timeout**.	Confirm that the Azure CLI command can be executed properly in the EXPRESSCLUSTER server. Check the load status of the server and remove the load. Check the value of **Azure CLI Timeout**.
azuredns	Error	42	Azure CLI command failed.	The Azure CLI command was executed. However, an error was returned.	Confirm that the setting of the resource is correct.
azuredns	Error	43	Azure CLI command not found.	The Azure CLI command is missing.	Confirm that the setting of **Azure CLI File Path** is correct and that Azure CLI is properly installed.
azuredns	Error	99	Internal error.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.16 Google Cloud virtual IP resources

Module type	Type	Return value	Message	Description	Solution
gcvip	Error	5	Port %1 is already used.	Port %1 is already used.	Check if the port specified for **Port Number** on the local server has not already been opened.
gcvip	Error	6	Failed to open the port %1.	Opening the port %1 failed.	Memory or OS resources may not be sufficient. Check them.
gcvip	Error	7	Failed to close the port %1.	Closing the port %1 failed.	Memory or OS resources may not be sufficient. Check them.
gcvip	Error	8	Failed to stop the port %1 control process.	Stopping the port %1 control process failed.	Memory or OS resources may not be sufficient. Check them. Restart OS.

Continued on next page

Table 10.25 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
gcvip	Error	9	The port %1 control process has already started.	The port %1 control process has already started.	Memory or OS resources may not be sufficient. Check them. Or, the immediately preceding deactivation may have failed. In that case, stop the cluster and forcibly terminate the port control process (clpgcvipp) manually.
gcvip	Error	10	Failed to start the port %1 control process.	Starting the port %1 control process failed.	Memory or OS resources may not be sufficient. Check them.
gcvip	Error	99	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.4.17 Oracle Cloud virtual IP resources

Module type	Type	Return value	Message	Description	Solution
ocvip	Error	5	Port %1 is already used.	Port %1 is already used.	Check if the port specified for **Port Number** on the local server has not already been opened.
ocvip	Error	6	Failed to open the port %1.	Opening the port %1 failed.	Memory or OS resources may not be sufficient. Check them.
ocvip	Error	7	Failed to close the port %1.	Closing the port %1 failed.	Memory or OS resources may not be sufficient. Check them.
ocvip	Error	8	Failed to stop the port %1 control process.	Stopping the port %1 control process failed.	Memory or OS resources may not be sufficient. Check them. Restart OS.

Continued on next page

Table 10.26 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
ocvip	Error	9	The port %1 control process has already started.	The port %1 control process has already started.	Memory or OS resources may not be sufficient. Check them. Or, the immediately preceding deactivation may have failed. In that case, stop the cluster and forcibly terminate the port control process (clpocvipp) manually.
ocvip	Error	10	Failed to start the port %1 control process.	Starting the port %1 control process failed.	Memory or OS resources may not be sufficient. Check them.
ocvip	Error	99	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5 Detailed info of monitor resource errors

10.5.1 IP monitor resources

Module Type	Type	Return value	Message	Description	Solution
ipw	Error	5	Ping was failed by timeout. IP=%s...	The ping command failed due to timeout.	The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.
ipw	Error	31	Ping cannot reach. (ret=%1) IP=%2...	The packet by the ping command did not reach.	Check if you can ping the IP address. If you fail, check the status of the device that has the IP address or the network interface.
ipw	Warning	102	Ping was failed. (ret=%1) IP=%2...	The ping command failed.	Memory or OS resources may not be sufficient. Check them.
ipw	Warning	106 108~121	Internal error. (status=%1)	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
ipw	Warning	189	Internal error. (status=%1)	Monitoring of the IP monitor resource failed by time out.	Memory or OS resources may not be sufficient. Check them.

10.5.2 Disk monitor resources

Module Type	Type	Return value	Message	Description	Solution
diskw	Error	12	Ioctl was failed. (err=%1) Device=%2	Failed to control the device.	Check the disk to be monitored is properly connected, powered on, or does not have any problem.
diskw	Error	14	1. Open was failed. (err=%1) File=%2 2. Open was failed. (err=%1) Device=%2	1. Opening the file failed. 2. Opening the device failed.	Check if there is a directory whose name is similar to the file name, the disk to be monitored is properly connected, powered on, or does not have any problem. Memory or OS resources may not be sufficient. Check them.
diskw	Error	16	Read was failed. (err=%1) Device=%2	Failed to read from the device.	Check the disk to be monitored is properly connected, powered on, or does not have any problem. Memory or OS resources may not be sufficient. Check them.
diskw	Error	18	Write was failed. (err=%1) File=%2	Writing to the file failed.	Check the disk to be monitored is properly connected, powered on, or does not have any problem. Memory or OS resources may not be sufficient. Check them.
diskw	Error	41	SG_IO failed. (sg_io_hdr_t info:%1 SG_INFO_OK_MASK: %2)	SG_IO failed.	Check the disk to be monitored is properly connected, powered on, or does not have any problem.

Continued on next page

Table 10.28 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
diskw	Error	49	Already bound for other. Rawdevice=%1 Device=%2	The RAW device has already been bound by another real device.	The set RAW device has already been bound by another real device. Change the RAW device name on the Cluster WebUI.
diskw	Error	55	Bind was failed. Rawdevice=%1 Device=%2	Bind failed.	Bind failed. Check the RAW device name on the Cluster WebUI.
diskw	Error	56	Lseek was failed by timeout. Device=%1	lseek failed.	The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.
diskw	Error	57	Fdatasync was failed by timeout. Device=%1	fdatasync failed.	Check if the disk to be monitored is properly connected, powered on, or does not have any other problems. The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.
diskw	Warning	101	Ioctl was failed by timeout. Device=%1	The device control failed due to timeout.	Check the disk to be monitored is properly connected, powered on, or does not have any problem. The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.
diskw	Warning	101	1. Open was failed by timeout. File=%1 2. Open was failed by timeout. Device=%1	1. Opening the file failed due to timeout. 2. Opening the device failed due to timeout.	Check the disk to be monitored is properly connected, powered on, or does not have any problem. The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 10.28 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
diskw	Warning	101	Read was failed by timeout. Device=%1	Failed to read from the device due to timeout.	Check the disk to be monitored is properly connected, powered on, or does not have any problem. The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.
diskw	Warning	101	Write was failed by timeout. File=%1	Writing to the file failed due to timeout.	Check the disk to be monitored is properly connected, powered on, or does not have any problem. The system may be heavily loaded, memory or OS resources may not be sufficient. Check them.
diskw	Warning	101	Bind was failed. Rawdevice=%1 Device=%2	Bind failed.	Bind failed. Check the RAW device name on the Cluster WebUI.
diskw	Warning	101	Stat was failed. (err=%1) Device=%2	Stat failed.	Stat failed. Check the device name on the Cluster WebUI.
diskw	Warning	101	Popen was failed. (err=%1)	Popen failed.	Popen failed. Memory or OS resources may not be sufficient. Check them.
diskw	Warning	101 190	Option was invalid.	The option is invalid.	Check the cluster configuration data by using the Cluster WebUI.
diskw	Warning	101 190	Internal error. (status=%1)	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
diskw	Warning	190	Parameter was invalid. File=%1	The specified file name is invalid.	Do not specify the file whose name starts with /dev. Specify a normal file.
diskw	Warning	190	Device was invalid. Device=%1	The specified real device is invalid.	Check the device name of the disk monitor resource on the Cluster WebUI.

Continued on next page

Table 10.28 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
diskw	Warning	191	Ignored disk full error.	A disk full error has been ignored.	Check the usage of the device.

10.5.3 PID monitor resources

Module Type	Type	Return value	Message	Description	Solution
pidw	Error	1	Process does not exist. (pid=%1)	The process does not exist.	The process to be monitored disappeared for some reason.
pidw	Warning	100	Resource %1 was not found.	The resource is not found.	Check the cluster configuration data by using the Cluster WebUI.
pidw	Warning	100	Internal error. (status=%1)	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.4 User mode monitor resources

Module Type	Type	Return value	Message	Description	Solution
userw	Error	1	Initialize error. (%1)	An error was detected while initializing the process.	Check if the driver depended on by the User mode monitor resources exist, or the rpm is installed. The driver or rpm differ depending on the monitor method.

10.5.5 Custom monitor resource

Module Type	Type	Return value	Message	Description	Solution
genw	Error	1	Initialize error. (status=%d)	An error was detected while initialization.	Memory or OS resources may not be sufficient. Check them.
genw	Error	2	Termination code %d was returned.	An unexpected value was returned.	Check if the cluster configuration information is correct.
genw	Error	3	User was not superuser.	User was not root user.	Log in as root user.
genw	Error	4	Getting of config was failed.	Failed to get the cluster configuration information.	Check if the cluster configuration information exists.

Continued on next page

Table 10.31 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
genw	Error	5	Parameter was invalid.	The parameter is invalid.	Check if the cluster configuration information is correct.
genw	Error	6	Option was invalid.	The parameter is invalid.	Check if the cluster configuration information is correct.
genw	Error	7	Monitor Resource %s was not found.	The resource was not found.	Check if the cluster configuration information is correct.
genw	Error	8	Create process failed.	Create process failed.	Memory or OS resources may not be sufficient. Check them.
genw	Error	9	Process does not exist. (pid=%d)	The process did not exist.	Check if the process exists.
genw	Error	10	Process aborted. (pid=%d)	The process did not exist.	Check if the process exists.
genw	Error	11	Asynchronous process does not exist. (pid=%d)	The process did not exist.	Check if the process exists.
genw	Error	12	Asynchronous process aborted. (pid=%d)	The process did not exist.	Check if the process exists.
genw	Error	13	Monitor path was invalid.	The path is invalid.	Check if the cluster configuration information is correct.
genw	Error	others	Internal error. (status=%d)	Another internal error occurred.	-

10.5.6 Multi target monitor resources

Module Type	Type	Return value	Message	Description	Solution
mtw	Error	1	Option was invalid.	The parameter is invalid.	Check if the cluster configuration information is correct.
mtw	Error	2	User was not superuser.	User was not root user.	Log in as root user.
mtw	Error	3	Internal error. (status=%d)	Another internal error occurred.	-

10.5.7 Mirror disk monitor resources

Module Type	Type	Return value	Message	Description	Solution
mdw	Error	1	The Mirror Agent has not started.	The Mirror Agent is not activated.	Check the Mirror Agent is active.
mdw	Error	2	Invalid option or parameter.	The parameter is invalid.	Check the cluster configuration data is correct.

Continued on next page

Table 10.33 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
mdw	Error	4	Failed to obtain the cluster configuration information.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.
mdw	Error	5	The configuration information of the mirror disk monitor resource is invalid.(%s)	The configuration data of the mirror disk monitor resource is incorrect.	Check if the cluster configuration data is correct.
mdw	Error	30	Internal error	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
mdw	Error	51	Failed to obtain the remote server status.	Failed to get the other server status.	Check if the Mirror Agent is activated on the remote server. Check mirror disk connection status. Check if the IP address in the cluster configuration data is correct.
mdw	Error	52	The mirror driver of the remote server is not working.	The remote server cannot be connected because it is stopped, or the mirror driver on the remote server has a problem.	Restart the remote server. This is not an issue if the remote server is intentionally disconnected like being stopped.
mdw	Error	53	The mirror driver of the local server is not working.	The mirror driver on the local server has a problem.	Restart the local server.
mdw	Error	54	Both local and remote drivers are not working.	The mirror drivers on the local and remote servers have a problem.	After cluster shutdown, restart the both servers.
mdw	Error	58	Local mirror disk is unknown or not constructed.(%1)	The mirror disk status is unknown on the local server, or the initial mirror construction is not performed yet.	You have to perform the initial mirror construction.
mdw	Error	63	Local mirror disk is abnormal. (%1)	The mirror disk has a problem on the local server.	The local server does not have the latest data. The mirror recovery needs to be performed.
mdw	Error	64	Remote mirror disk is abnormal.(%1)	Mirror disk is abnormal on the remote server.	The remote server does not have the latest data. The mirror recovery needs to be performed.

Continued on next page

Table 10.33 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
mdw	Error	65	Both local and remote mirror disks are abnormal.(%1)	The mirror drivers on the local and remote servers have a problem.	The forcible mirror recovery needs to be performed.
mdw	Error	66	The mirror disk resource was activated on both servers.(%1)	Mirror disk resources have been activated on both servers.	When activation of mirror disk resource is detected on both servers, the servers shut down automatically. Restart the servers. See the description for the module type rc and event ID 92 in "*Messages reported by syslog, alert, mail, and SNMP trap*" and "Recovery from network partitioning" in "The system maintenance information" in the "Maintenance Guide" for details.
mdw	Error	99	monitor was timeout	Response to the mirror disk monitor resource has timed out. If this error has occurred in the mirror disk monitor resource, there may be a delay in communication between the mirror agents or in the disk I/O with the cluster partition.	Increase the transmission timeout setting for communication between mirror agents. Also, if the timeout setting for the mirror disk monitor resource is smaller than the transmission timeout setting for communication between the mirror agents, adjust the settings so that the former is larger than the latter.
mdw	Warning	100	The mirror recovery is in progress. (%1)	Mirror recovery is in progress.	Wait until mirror recovery is successfully completed.

10.5.8 Mirror disk connect monitor resources

Module Type	Type	Return value	Message	Description	Solution
mdnw hdnw	Error	1	The Mirror Agent has not started.	The Mirror Agent is not activated.	Check the Mirror Agent is active.
mdnw hdnw	Error	2	Invalid option or parameter.	The parameter is invalid	Check the cluster configuration data is correct.
mdnw hdnw	Error	4	Failed to obtain the cluster configuration information.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.
mdnw hdnw	Error	5	The configuration information of the mirror disk monitor resource is invalid.(%s)	The configuration data of the mirror disk connect monitor resource is incorrect.	Check the cluster configuration data is correct.
mdnw hdnw	Error	30	Internal error[status=%1]	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
mdnw hdnw	Error	31	The network is disconnected.	The mirror disk connection is not connected.	Check the mirror disk connection status.
mdnw	Warning	101	One of the mirror disk connection is disconnected.	Among the multiple mirror disk connections that exist, some were disconnected.	Check the mirror disk connection starts.

10.5.9 JVM monitor resources

Module Type	Type	Return value	Message	Description	Solution
jraw	Error	11	An error was detected in accessing the monitor target.	Java VM to be monitored cannot be connected.	Check that the Java VM to be monitored is running.

Continued on next page

Table 10.35 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
jraw	Error	12	JVM status changed to abnormal. cause = %1.	An error was detected in monitoring Java VM. %1: Error generation cause GarbageCollection JavaMemoryPool Thread WorkManagerQueue WebOTXStall	Based on the message, check the Java application that is running on Java VM to be monitored.
jraw	Warning	189	Internal error occurred.	An internal error has occurred.	Execute cluster suspend and cluster resume.

10.5.10 System monitor resources

Module Type	Type	Return value	Message	Description	Solution
sraw	Error	11	Detected an error in monitoring system resource	An error was detected when monitoring system resources.	There may be an error with the resources. Check them.

10.5.11 Process resource monitor resources

Module Type	Type	Return value	Message	Description	Solution
psrw	Error	11	Detected an error in monitoring process resource	An error was detected when monitoring process resources.	There may be an error with the resources. Check them.

10.5.12 Hybrid disk monitor resources

Module Type	Type	Return value	Message	Description	Solution
hdw	Error	1	The Mirror Agent has not started.	The Mirror Agent is not activated.	Check the Mirror Agent is active.
hdw	Error	2	Invalid option or parameter.	The parameter is invalid.	Check the cluster configuration data is correct.
hdw	Error	4	Failed to obtain the cluster configuration information.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.

Continued on next page

Table 10.38 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
hdw	Error	5	The configuration information of the hybrid disk monitor resource is invalid.(%s)	The configuration data of the mirror disk monitor resource is incorrect.	Check if the cluster configuration data is correct.
hdw	Error	13	Both hybrid disks are pending.	Mirror status of both servers is pending.	Confirm the mirror status. Execute full mirror recovery, forced recovery or resource activation.
hdw	Error	15	Local hybrid disk is pending. Remote hybrid disk status is unknown.	Status of hybrid disk of other server cannot be acquired. Local server is pending. It cannot be specified which server has the latest data.	Check the inter connect. When it is confirmed that the local server has the latest data, activate the resource in the local server. When it is confirmed that the other server has the latest data, start the other server and activate the resource in the server.
hdw	Error	30	Internal error	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
hdw	Error	51	Failed to obtain the remote server status.	Failed to get the other server status.	Check if the Mirror Agent is activated on the remote server. Check mirror disk connection status. Check if the IP address in the cluster configuration data is correct.
hdw	Error	52	The mirror driver of the remote server is not working.	The remote server cannot be connected because it is stopped, or the mirror driver on the remote server has a problem.	Restart the remote server. This is not an issue if the remote server is intentionally disconnected like being stopped.
hdw	Error	53	The mirror driver of the local server is not working.	The mirror driver on the local server has a problem.	Restart the local server.
hdw	Error	54	Both local and remote drivers are not working.	The mirror drivers on the local and remote servers have a problem.	After cluster shutdown, restart the both servers.

Continued on next page

Table 10.38 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
hdw	Error	58	Local hybrid disk is unknown or not constructed.(%1)	The hybrid disk status is unknown on the local server, or the initial mirror construction is not performed yet.	You have to perform the initial mirror construction.
hdw	Error	63	Local hybrid disk is abnormal.(%1)	The hybrid disk has a problem on the local server.	The local server does not have the latest data. The mirror recovery needs to be performed.
hdw	Error	64	Remote hybrid disk is abnormal.(%1)	Hybrid disk is abnormal on the remote server.	The remote server does not have the latest data. The mirror recovery needs to be performed.
hdw	Error	65	Both local and remote hybrid disks are abnormal.(%1)	The hybrid drivers on the local and remote servers have a problem.	The forcible mirror recovery needs to be performed.
hdw	Error	66	The hybrid disk resource was activated on both servers.(%1)	Hybrid disk resources have been activated on both servers.	When activation of mirror disk resource is detected on both servers, the servers shut down automatically. Restart the servers. See the description for the module type rc and event ID 92 in "*Messages reported by syslog, alert, mail, and SNMP trap*" and "Recovery from network partitioning" in "The system maintenance information"in the "Maintenance Guide" for details.

Continued on next page

Table 10.38 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
hdw	Error	99	monitor was timeout	Response to the hybrid disk monitor resource has timed out. If this error has occurred in the hybrid disk monitor resource, there may be a delay in communication between the mirror agents or in the disk I/O with the cluster partition.	Increase the transmission timeout setting for communication between mirror agents. Also, if the timeout setting for the hybrid disk monitor resource is smaller than the transmission timeout setting for communication between the mirror agents, adjust the settings so that the former is larger than the latter.
hdw	Warning	100	The mirror recovery is in progress. (%1)	Mirror recovery is in progress.	Wait until mirror recovery is successfully completed.

10.5.13 Hybrid disk connect monitor resources

Module Type	Type	Return value	Message	Description	Solution
hdnw	Error	1	The Mirror Agent has not started.	The Mirror Agent is not activated.	Check the Mirror Agent is active.
hdnw	Error	2	Invalid option or parameter.	The parameter is invalid	Check the cluster configuration data is correct.
hdnw	Error	4	Failed to obtain the cluster configuration information.	Failed to obtain the cluster configuration data.	Check the cluster configuration data exists.
hdnw	Error	5	The configuration information of the hybrid disk monitor resource is invalid.(%s)	The configuration data of the mirror disk connect monitor resource is incorrect.	Check the cluster configuration data is correct.
hdnw	Error	30	Internal error[status=%1]	An error other than the errors mentioned above has occurred.	Memory or OS resources may not be sufficient. Check them.
hdnw	Error	31	The network is disconnected.	The mirror disk connection is not connected.	Check the mirror disk connection status.
hdnw	Warning	101	One of the hybrid disk connection is disconnected.	The mirror disk connection is not connected.	Check the mirror disk connection status.

10.5.14 NIC link up/down monitor resources

Module Type	Type	Return value	Message	Description	Solution
miiw	Error	20	NIC %1 link was down.	NIC link failed.	Check that the LAN cable is connected properly
miiw	Warning	110	Get IP Address information error. (err=%1)	Failed to acquire the socket address of IPv4 or IPv6 address family.	Check that the kernel configuration supports TCP/IP networking (IPv4 or IPv6).
miiw	Warning	111	Socket creation was failed. (err=%1)	Failed to create a socket.	Memory or OS resources may not be sufficient. Check them.
miiw	Warning	112	ioctl was failed. (err=%1) Device=%2 Request=%3	The control request to the network driver has failed.	Check the network driver supports the control request of %3. See "4. *Monitor resource details*" of this guide.
miiw	Warning	113	MII was not supported or no such device. Device=%1	Either MII is not supported by NIC or the monitoring target does not exist.	See "4. *Monitor resource details*" of this guide. Check the network interface name using a command such as ifconfig if the monitoring target does not exist.
miiw	Warning	189	Internal error. (status=%d)	Other internal error has occurred.	-
miiw	Warning	190	Option was invalid.	The option is invalid.	Check the cluster configuration information on the Cluster WebUI.
miiw	Warning	190	Config was invalid. (err=%1) %2	The configuration information is invalid	Check the cluster configuration information on the Cluster WebUI.

10.5.15 ARP monitor resources

Module Type	Type	Return value	Message	Description	Solution
arpw	Warning	102	Not found IP address.	Could not find the IP address.	Check the status of a resource to be monitored.
arpw	Warning	103	Socket creation error.	An error occurred in creating a socket.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 10.41 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
arpw	Warning	104	Socket I/O error.	A failure occurred in control request to the network driver.	-
arpw	Warning	105	Packet send error.	Failed to send ARP packet.	Check if packets can be sent from the IP address using such as the ping command.
arpw	Warning	180	Memory allocate error.	Failed to allocate the internal memory.	Memory or OS resources may not be sufficient. Check them.
arpw	Warning	182	Timeout.	Timeout has occurred in monitoring.	-
arpw	Warning	190	Initialize error.	A failure was detected during initialization.	Memory or OS resources may not be sufficient. Check them.

10.5.16 Virtual IP monitor resources

Module Type	Type	Return value	Message	Description	Solution
vipw	Warning	102	Invalid interface. (err=%1)	Interface name of NIC is invalid.	Check the cluster configuration information using the Cluster WebUI. Or check the interface name of NIC exists.
vipw	Warning	103	Get IP Address information error. (err=%1)	Failed to acquire the socket address of IPv4 or IPv6 address family.	Check that the kernel configuration supports TCP/IP networking (IPv4 or IPv6).
vipw	Warning	104	Socket creation error. (err=%1)	Failed to create a socket.	Memory or OS resources may not be sufficient. Check them.
vipw	Warning	105	Socket option error. (err=%1)	Failed to set the socket option.	Memory or OS resources may not be sufficient. Check them.
vipw	Warning	106	Socket bind error. (err=%1)	Failed to bind a socket with the IP address from which a socket is sent.	Check the cluster configuration information using the Cluster WebUI. Or check the interface name of NIC exists.
vipw	Warning	107	Socket I/O error. (err=%1)	Failed in control request to network driver.	Memory or OS resources may not be sufficient. Check them.
vipw	Warning	108	Packet send error. (err=%1)	Failed to send RIP packet.	Check if packet can be sent from the IP address using such as the ping command.

Continued on next page

Table 10.42 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
vipw	Warning	180	Memory allocation error. (err=%1)	Failed to allocate internal memory.	Memory or OS resources may not be sufficient. Check them.
vipw	Warning	182	Timeout.	Timeout occurred in monitoring.	-
vipw	Warning	189	Internal error. (status=%1)	Other internal error occurred.	-
vipw	Warning	190	Initialize error.	A failure was detected during initialization.	Memory or OS resources may not be sufficient. Check them.

10.5.17 VM monitor resources

Module Type	Type	Return value	Message	Description	Solution
vmw	Error	1	initialize error occurred.	An error was detected while initialization.	Memory or OS resources may not be sufficient. Check them.
vmw	Error	11	monitor success, virtual machine is not running.	Stop of the virtual machine was detected.	Check the status of the virtual machine.
vmw	Error	12	failed to get virtual machine status.	Failed to get the status of the virtual machine.	Check if the virtual machine exists.
vmw	Error	13	timeout occurred.	The monitoring timed out.	The OS may be highly loaded. Check it.

10.5.18 Volume manager monitor resources

Module Type	Type	Return value	Message	Description	Solution
volmgrw	Error	21	Command was failed. (cmd=%1, ret=%2)	%1 command failed. The return value is %2.	The command failed. Check the action status of the volume manager.
volmgrw	Error	22 23	Internal error. (status=%1)	Another internal error occurred.	-
volmgrw	Warning	190	Option was invalid.	The option is invalid.	Check the cluster configuration information on the Cluster WebUI.
volmgrw	Warning	191	%1 %2 is %3 !	The status of the target (%2) of the volume manager (%1) transferred to %3.	Check the status of the volume manager target.
volmgrw	Warning	Others	Internal error. (status=%1)	Another internal error occurred.	-

10.5.19 Dynamic DNS monitor resources

Module Type	Type	Return value	Message	Description	Solution
ddnsw	Error	8	Ping can not reach virtual host(%1).	There was no ping response from the virtual host (%1).	Check the DNS server status.
ddnsw	Warning	102	open() failed.(err = %1)	Opening the internally used file failed.	There might not be enough memory space or OS resources. Check whether this is so.
ddnsw	Warning	103	write() failed.(err = %1)	Writing to the internally used file failed.	There might not be enough memory space or OS resources. Check whether this is so.
ddnsw	Warning	104	close() failed.(err = %1)	Closing the internally used file failed.	There might not be enough memory space or OS resources. Check whether this is so.
ddnsw	Warning	105	nsupdate command has failed.	Executing the nsupdate command failed.	Analyze the error by referring to the command return value.
ddnsw	Warning	106	Ping can not reach the DNS server(%1).	There was no ping response from the DNS server (%1).	Check the DNS server status.
ddnsw	Warning	107	nslookup command has failed.	Executing the nslookup command failed.	Check the DNS server status.
ddnsw	Warning	180	Memory allocation error.(err=%1)	An internal memory allocation error occurred.	There might not be enough memory space or OS resources. Check whether this is so.
ddnsw	Warning	182	Time out.	Monitoring timed out.	The OS might be heavily loaded. Check whether this is so.
ddnsw	Warning	190	Initialize error.	An error was detected during initialization.	There might not be enough memory space or OS resources. Check whether this is so.
ddnsw	Warning	Other	Internal error.(status=%d)	A different internal error occurred.	There might not be enough memory space or OS resources. Check whether this is so.

10.5.20 Process name monitor resources

Module Type	Type	Return value	Message	Description	Solution
psw	Error	11	Process[%1 (pid=%2)] Down	Deletion of a monitored process has been detected.	Check whether the monitored process is running normally.
psw	Error	12	The number of processes is less than the specified minimum process count. %1/%2 (%3)	The number of started processes for the monitor target process is less than the specified minimum count.	Check whether the monitored process is running normally.
psw	Warning	100	Monitoring timeout	Monitoring has timed out.	The OS may be highly loaded. Check that.
psw	Warning	101 190	Internal error	An internal error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.
psw	Warning	190	Initialize error	An error has been detected during initialization.	Check the following possible causes: memory shortage or OS resource insufficiency.

10.5.21 BMC monitor resource

Module Type	Type	Return value	Message	Description	Solution
bmcw	Error	0	Success.	The monitoring process was successful.	
bmcw	Error	1	Initialize error.	An error occurred when the monitor started.	Check the following possible causes: memory shortage, OS resource insufficiency, or failure to install the IPMI driver correctly.
bmcw	Error	32	Not supported platform. (code=%1)	The platform is not supported.	The hardware may be other than the NX7700x series.
bmcw	Error	32	BMC access denied.	The IPMI command for monitoring failed.	Check the operating status of the IPMI driver.
bmcw	Error	64	Internal error. (status=%1)	An internal error occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.
bmcw	Warning	128	The registered license is invalid. (%1)	The registered license is invalid.	Register a valid license.
bmcw	Warning	129	The license is not registered. (%1)	The license is not registered.	Purchase and register a license.

Continued on next page

Table 10.47 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
bmcw	Warning	130	The trial license has expired in %.4s/%.2s/%.2s. (%1)	The trial license has expired.	Register a valid license.
bmcw	Warning	130	The trial license is valid from %.4s/%.2s/%.2s. (%1)	The current date is earlier than the valid period of the trial license.	Register a valid license.
bmcw	Warning	131	The registered license is unknown. (%1)	The registered license is unknown.	Register a valid license.
bmcw	Error	200	Timeout.	Monitoring caused a timeout.	The BMC is highly loaded or has stalled. Check the BMC.

10.5.22 Oracle Clusterware Synchronization Management monitor resource

Module Type	Type	Return value	Message	Description	Solution
osmw	Error	1	Initialize error.	An error occurred when the monitor started.	Check the following possible causes: memory shortage, OS resource insufficiency, or failure to install the IPMI driver correctly.
osmw	Error	1	Oracle Clusterware linkage is not enabled.	Oracle Clusterware linkage function is not enabled.	Enable the Oracle Clusterware linkage function.
osmw	Error	32	All registered Oracle processes do not exist.	A process of any watch targets doesn't exist.	Everything of a watch target process became extinct by some cause. Please check Oracle Clusterware processes.
osmw	Error	64	Internal error. (status=%1)	An internal error occurred.	Check the following possible causes: memory shortage or OS resource insufficiency.
osmw	Warning	128	The registered license is invalid. (%1)	The registered license is invalid.	Register a valid license.
osmw	Warning	129	The license is not registered. (%1)	The license is not registered.	Purchase and register a license.
osmw	Warning	130	The trial license has expired in %.4s/%.2s/%.2s. (%1)	The trial license has expired.	Register a valid license.
osmw	Warning	131	The trial license is valid from %.4s/%.2s/%.2s. (%1)	The current date is earlier than the valid period of the trial license.	Register a valid license.
osmw	Warning	132	The registered license is unknown. (%1)	The registered license is unknown.	Register a valid license.

Continued on next page

Table 10.48 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
osmw	Warning	160	Some registered Oracle processes do not exist.	A process of some watch targets doesn't exist.	Some of the watch target process became extinct by some cause. Please check Oracle Clusterware processes.
osmw	Error	200	Timeout.	Monitoring caused a timeout.	The OS may be highly loaded. Check that.

10.5.23 Floating IP monitor resources

Module Type	Type	Return value	Message	Description	Solution
fipw	Error	4	IP address does not exist.	The IP address does not exist.	NIC may have been disabled. Check if the FIP address exists with the ifconfig command or the ip command.
fipw	Error	5	Adapter Index is different.	The adapter index is different.	NIC may have been disabled. Check if the FIP address exists with the ifconfig command or the ip command.
fipw	Error	9	Detected NIC Link Down.	Link Down of NIC was detected.	Check if the LAN cable is connected properly.
fipw	Warning	106	Failed to get IP address table.	Failed to get the IP address list.	Memory or OS resources may not be sufficient. Check them.
fipw	Warning	107	Failed to get NIC interface name.	Failed to get the NIC interface name.	Memory or OS resources may not be sufficient. Check them.
fipw	Warning	108	Failed to get NIC status.	Failed to get the NIC status.	Check if the NIC device is supported by the device I/O controller.
fipw	Warning	110	Timeout occurred.	A timeout occurred.	Check the load status of the server and remove the load.
fipw	Warning	189	Internal error occurred. (status=%d)	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 10.49 – continued from previous page

Module Type	Type	Return value	Message	Description	Solution
fipw	Warning	190	User is not superuser.	The user does not have the root user right.	The user who executed the operation may not have the root user right. Or, memory or OS resources may not be sufficient. Check them.
fipw	Warning	190	Parameter is invalid.	The parameter is invalid.	Check if the cluster configuration data is correct.
fipw	Warning	190	Failed to get the value from cluster configuration date.	Failed to get the value from cluster configuration data.	Check if the cluster configuration data is correct.

10.5.24 AWS elastic ip monitor resources

Module type	Type	Return value	Message	Description	Solution
awseipw	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awseipw	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awseipw	Error	7	The EIP address does not exist. (EIP ALLOCATION ID=%1)	The EIP address %1 does not exist.	The EIP may have been detached. Check it.
awseipw	Warning	105	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awseipw	Warning	106	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awseipw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Check if Python is installed correctly. Check if AWS CLI is installed correctly. Memory or OS resources may not be sufficient. Check them.

10.5.25 AWS virtual ip monitor resources

Module type	Type	Return value	Message	Description	Solution
awsvipw	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsvipw	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsvipw	Error	7	The VIP address %1 does not exist.	The VIP address %1 does not exist.	NIC may have been disabled. Check if the VIP address exists with the ipconfig command.
awsvipw	Error	8	The routing for VIP %1 was changed.	The routing for VIP %1 was changed.	The VIP routing may have been changed. Check the Route Tables of the VPC.
awsvipw	Warning	105	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsvipw	Warning	106	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsvipw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Check if Python is installed correctly. Check if AWS CLI is installed correctly. Memory or OS resources may not be sufficient. Check them.

10.5.26 AWS AZ monitor resources

Module type	Type	Return value	Message	Description	Solution
awsazw	Error	4	Failed to monitor the availability zone %1	Failed to monitor the availability zone %1.	The availability zone to which the server belongs may have a problem. Check it.

Continued on next page

Table 10.52 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsazw	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsazw	Error	5	Invalid availability zone: [%1]	The specified availability zone %1 does not exist.	Check if the settings of the availability zone are correct.
awsazw	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsazw	Warning	105	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsazw	Warning	105	Invalid availability zone: [%1]	The specified availability zone %1 does not exist.	Check if the settings of the availability zone are correct.
awsazw	Warning	106	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsazw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Check if Python is installed correctly. Check if AWS CLI is installed correctly. Memory or OS resources may not be sufficient. Check them.

10.5.27 AWS DNS monitor resources

Module type	Type	Return value	Message	Description	Solution
awsdnsw	Error	5	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsdnsw	Error	6	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsdnsw	Error	7	The resource record set in Amazon Route 53 does not exist.	Resource record set does not exist in Amazon Route 53.	The record set to be monitored might be deleted. Check the registration status of the resource record set of Amazon Route 53.

Continued on next page

Table 10.53 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsdnsw	Error	8	IP address different from the setting is registered in the resource record set of Amazon Route 53.	A different IP address from the setting value is registered in the resource record set of Amazon Route 53	Confirm that the IP address registered in the resource record set to be monitored is correct.
awsdnsw	Error	9	Failed to resolve domain name.	Failed to check the name resolution of resource record set.	The name resolution failed. Check whether or not an error occurs in the setting of the resolver or the network If the resource record set name uses the escape, the name resolution will fail. Therefore, set **Check Name Resolution** of the monitor resource to off.
awsdnsw	Error	10	IP address which is resolved domain name from the DNS resolver is different from the setting.	The IP address of name resolution result is different from the setting value.	Confirm that the setting of DNS resolver is correct and that an unintended entry does not exist in the hosts file.
awsdnsw	Warning	105	Failed in the AWS CLI command.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsdnsw	Warning	106	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsdnsw	Warning	189	Internal error. (status=%1)	An internal error occurred.	Confirm that Python is installed properly. Confirm that AWS CLI is installed properly. Memory or OS resources may not be sufficient. Check them.

10.5.28 Azure probe port monitor resources

Module type	Type	Return value	Message	Description	Solution
azureppw	Error	4	Probe port %1 is closed.	Probe port is closed.	Probe port is closed. Please confirm the setting of a network of a server.
azureppw	Error	5	Timeout of waiting probe port %1 occurred.	Timeout of waiting probe port occurred.	A probe from a load balancer of Azure couldn't be received in the timeout of waiting probr port. Please confirm or whether a network is connected with whether an error doesn't occur by a network adapter right.
azureppw	Warning	105	Timeout of waiting probe port %1 occurred.	Timeout of waiting probe port occurred.	A probe from a load balancer of Azure couldn't be received in the timeout of waiting probr port. Please confirm or whether a network is connected with whether an error doesn't occur by a network adapter right.
azureppw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.29 Azure load balance monitor resources

Module type	Type	Return value	Message	Description	Solution
azurelbw	Error	4	On server %1, probe port %2 is opened.	On server, probe port is opened.	A probe port is opening by a standby server. Please make sure that the probe port won't be opened by a standby server.
azurelbw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.30 Azure DNS monitor resources

Module type	Type	Return value	Message	Description	Solution
azurednsw	Error	11	Query to the DNS server failed.	For DNS server of Microsoft Azure, a query for the name resolution failed.	Confirm that EXPRESSCLUSTER server can communicate with the DNS server of Microsoft Azure. From the DNS zone of Microsoft Azure portal, confirm that DNS record set and record set are registered correctly.
azurednsw	Error	12	IP address different from the setting is registered in the record set of the Azure DNS zone.	The record set of DNS server might be deleted or rewritten from outside.	For DNS zone of Microsoft Azure portal, check the record set.
azurednsw	Warning	189	Internal error.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.31 Google Cloud virtual IP monitor resources

Module type	Type	Return value	Message	Description	Solution
gcvipw	Error	4	Port %1 is closed.	Port %1 is closed.	The port specified for **Port Number** is closed. Check the network settings of the server.

Continued on next page

Table 10.57 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
gcvipw	Error	5	Timeout of waiting port %1 occurred.	Health check timeout occurred.	The health check could not be received from the load balancer within **Health check timeout**. Check if there is an error with the network adopter or the network is properly connected. Or, extend **Health check timeout**.
gcvipw	Error	6	Monitoring port %1 failed.	Monitoring port %1 failed.	Memory or OS resources may not be sufficient. Check them.
gcvipw	Error	7	Monitoring port %1 is frozen.	Monitoring port %1 is frozen.	Memory or OS resources may not be sufficient. Check them.
gcvipw	Error	99	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
gcvipw	Warning	105	Timeout of waiting port %1 occurred.	Health check timeout occurred.	The health check could not be received from the load balancer within **Health check timeout**. Check if there is an error with the network adopter or the network is properly connected. Or, extend **Health check timeout**.
gcvipw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them. Check them.

10.5.32 Google Cloud load balance monitor resources

Module type	Type	Return value	Message	Description	Solution
gclbw	Error	4	On server %1, port %2 is opened.	On server %1, port %2 is opened.	The port specified for **Port Number** on the standby server is opened. Make sure that the port will not be opened on the standby server.
gclbw	Error	5	Monitoring port %1 failed.	Monitoring port %1 failed.	Memory or OS resources may not be sufficient. Check them.
gclbw	Error	99	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
gclbw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.33 Oracle Cloud virtual IP monitor resources

Module type	Type	Return value	Message	Description	Solution
ocvipw	Error	4	Port %1 is closed.	Port %1 is closed.	The port specified for **Port Number** is closed. Check the network settings of the server.
ocvipw	Error	5	Timeout of waiting port %1 occurred.	Health check timeout occurred.	The health check could not be received from the load balancer within **Health check timeout**. Check if there is an error with the network adopter or the network is properly connected. Or, extend **Health check timeout**.
ocvipw	Error	6	Monitoring port %1 failed.	Monitoring port %1 failed.	Memory or OS resources may not be sufficient. Check them.
ocvipw	Error	7	Monitoring port %1 is frozen.	Monitoring port %1 is frozen.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 10.59 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
ocvipw	Error	99	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
ocvipw	Warning	105	Timeout of waiting port %1 occurred.	Health check timeout occurred.	The health check could not be received from the load balancer within **Health check timeout**. Check if there is an error with the network adopter or the network is properly connected. Or, extend **Health check timeout**.
ocvipw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.34 Oracle Cloud load balance monitor resources

Module type	Type	Return value	Message	Description	Solution
oclbw	Error	4	On server %1, port %2 is opened.	On server %1, port %2 is opened.	The port specified for **Port Number** on the standby server is opened. Make sure that the port will not be opened on the standby server.
oclbw	Error	5	Monitoring port %1 failed.	Monitoring port %1 failed.	Memory or OS resources may not be sufficient. Check them.
oclbw	Error	99	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
oclbw	Warning	189	Internal error. (status=%1)	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

10.5.35 Monitoring option monitor resource

Monitor resources of monitoring options use common messages. Module types are different for each monitoring option monitor resource.

Monitoring option monitor resource	Module type
DB2 monitor resource	db2w
FTP monitor resource	ftpw
HTTP monitor resource	httpw
IMAP4 monitor resource	imap4w
MySQL monitor resource	mysqlw
NFS monitor resource	nfsw
ODBC monitor resource	odbcw
Oracle monitor resource	oracle
POP3 monitor resource	pop3w
PostgreSQL monitor resource	psqlw
Samba monitor resource	sambaw
SMTP monitor resource	smtpw
SQL Server monitor resource	sqlserverw
Sybase monitor resource	sybasew
Tuxedo monitor resource	tuxw
Websphere monitor resource	wasw
Weblogic monitor resource	wlsw
WebOTX monitor resource	otxw

Module type	Type	Return value	Message	Description	Solution
(see the list above)	Error	5	Failed to connect to %1 server. [ret=%2] %3:	Failed to connect to the monitor target.	Check the status of the monitor target. The actual module type is displayed in %1.
(see the list above)	Error	7	Failed to execute SQL statement (%1). [ret=%2] %3:	Failed to execute SQL statement (%1). The actual module type is displayed in %1.	Check the cluster configuration information using the Cluster WebUI.
(see the list above)	Error	8	Failed to access with %1. %2:	Failed in data access with monitor target. The actual module type is displayed in %1.	Check the status of monitor target.

Continued on next page

Table 10.62 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
(see the list above)	Error	9	Detected error in %1. %2:	A failure occurred on monitor target. The actual module type is displayed in %1.	Check the status of monitor target.
(see the list above)	Warning	104	Detected function exception. [%1, ret=%2] %3: function name	A failure was detected.	Check the cluster configuration information using the Cluster WebUI. The OS may be heavily loaded. Check it.
(see the list above)	Warning	106	Detected authority error.	Failed in the user authentication.	Check the user name, password, and access right.
(see the list above)	Warning	111	Detected timeout error.	Communication timeout has occurred.	OS may be heavily loaded. Check it.
(see the list above)	Warning	112	Can not found install path. (install path=%1)	Can not found install path.	Check the install path.
(see the list above)	Warning	113	Can not found library. (libpath=%1, errno=%2)	Failed to load the library from the specified location.	Check where the library is located.
(see the list above)	Warning	171	Detected a monitor delay in monitoring %1. (timeout=%2*%3 actual-time=%4 delay warning rate=%5)	A monitoring delay was detected in monitoring %1. The current timeout value is %2 (second) x %3 (tick count per second). The actual measurement value at delay detection is %4 (tick count) and exceeded the delay warning rate %5 (%).	Check the load status of the server on which a monitoring delay was detected and remove the load. If a monitoring timeout is detected, extend it.
(see the list above)	Info	181	The collecting of detailed information triggered by monitor resource %1 error has been started (timeout=%2).	Collecting of detailed information triggered by the detection of a monitor resource $1 monitoring error has started. The timeout is %2 seconds.	-
(see the list above)	Info	182	The collection of detailed information triggered by monitor resource %1 error has been completed.	Collecting of detailed information triggered by the detection of a monitor resource %1 monitoring error has been completed.	-

Continued on next page

Table 10.62 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
(see the list above)	Warning	183	The collection of detailed information triggered by monitor resource %1 error has been failed (%2).	Collecting of detailed information triggered by the detection of a monitor resource %1 monitoring error has failed. (%2)	-
(see the list above)	Warning	189	Internal error. (status=%1)	An internal error was detected.	-
(see the list above)	Warning	190	Init error. [%1, ret=%2]	license/XML/log/share memory module initialization error Failed in Dynamic Library Load.	OS may be heavily loaded. Check the status of OS.
(see the list above)	Warning	190	Get config information error. [ret=%1]	Failed to acquire the setting information.	Check the cluster configuration information using the Cluster WebUI.
(see the list above)	Warning	190	Invalid parameter.	The setting information of Config file/Policy file is invalid. Command parameter is invalid.	Check the cluster configuration information using the Cluster WebUI.
(see the list above)	Warning	190	Init function error. [%1, ret=%2]	An error was detected while initialization.	OS may be heavily loaded. Check the status of OS.
(see the list above)	Warning	190	User was not superuser.	A user does not have the right as root user.	The user who executed the operation may not have a root user right. Or, memory or OS resources may not be sufficient. Check them.
(see the list above)	Warning	190	The license is not registered.	The license is not registered.	Check if the valid license is registered.
(see the list above)	Warning	190	The registration license overlaps.	The registered license already exists.	Check if the valid license is registered.
(see the list above)	Warning	190	The license is invalid.	The license is invalid.	Check if the valid license is registered.
(see the list above)	Warning	190	The license of trial expired by %1. %2: Validity_date	The license of trial is expired. The actual validity date is displayed in Validity_date.	-

Continued on next page

Table 10.62 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
(see the list above)	Warning	190	The license of trial effective from %1. %2: Validity_date	The trial license has not become effective yet. The actual validity date is displayed in Validity_date.	-

10.6 JVM monitor resource log output messages

The following messages belong to the JVM operation and JVM load balancer linkage log files that are specific to the JVM monitor resources.

The file is created in the following location:

JVM operation log: <*EXPRESSCLUSTER_install_path*>/log/ha/jra/jragent*.log (* indicates a number starting at 0.)

JVM load balancer linkage log: <*EXPRESSCLUSTER_install_path*>/log/ha/jra/lbadmin.log

10.6.1 JVM operation log

Message	Cause of generation	Action
Failed to write the %1$s.stat.	Writing to the JVM statistics log has failed. %1$s.stat: JVM statistics log file name	Check whether there is sufficient free disk space.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: analyze finish[%4$s]. state = %2$s, cause = %3$s	(When the status of the Java VM to be monitored is abnormal) the resource use amount has exceeded the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Status of Java VM to be monitored (1=normal, 0=abnormal) %3$s: Error generation location at abnormality occurrence %4$s: Measurement thread name	Review the Java application that runs on the Java VM to be monitored.
thread stopped by UncaughtException.	The thread of the JVM monitor resource has stopped.	Execute cluster suspend/cluster resume and then restart the JVM monitor resource.
thread wait stopped by Exception.	The thread of the JVM monitor resource has stopped.	Execute cluster suspend/cluster resume and then restart the JVM monitor resource.
%1$s: monitor thread can't connect to JVM.	The Java VM to be monitored could not be connected. %1$s: Name of the Java VM to be monitored	Check that the Java VM to be monitored is running.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: monitor thread can't get the JVM state.	The resource use amount could not be acquired from Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check that the Java VM to be monitored is running.
%1$s: JVM state is changed [abnormal -> normal].	The status of the Java VM to be monitored has changed from abnormal to normal. %1$s: Name of the Java VM to be monitored	-
%1$s: JVM state is changed [normal -> abnormal].	The status of the Java VM to be monitored has changed from normal to abnormal. %1$s: Name of the Java VM to be monitored	Review the Java application that runs on the Java VM to be monitored.
%1$s: Failed to connect to JVM.	The Java VM to be monitored could not be connected. %1$s: Name of the Java VM to be monitored	Check that the Java VM to be monitored is running.
Failed to write exit code.	The JVM monitor resource failed to write data to the file for recording the exit code.	Check whether there is sufficient free disk space.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
Failed to be started JVM Monitor.	Starting of the JVM monitor resource has failed.	Check the JVM operation log, remove the cause preventing the start, execute cluster suspend/cluster resume, and then restart the JVM monitor resource.
JVM Monitor already started.	The JVM monitor resource has already been started.	Execute cluster suspend/cluster resume and then restart the JVM monitor resource.
%1$s: GARBAGE_COLLECTOR_MXBEAN_DOMAIN_TYPE is invalid.	GC information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: GarbageCollectorMXBean is invalid.	GC information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: Failed to measure the GC stat.	GC information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: GC stat is invalid. last.getCount = %2$s, last.getTime = %3$s, now.getCount = %4$s, now.getTime = %5$s.	The GC generation count and GC execution time could not be measured for the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: GC generation count at last measurement %3$s: Total GC execution time at last measurement %4$s: GC generation count at this measurement %5$s: Total GC execution time at this measurement	Check whether the operating environment of the Java VM to be monitored is correct.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: GC average time is too long. av = %6$s, last.getCount = %2$s, last.getTime = %3$s, now.getCount = %4$s, now.getTime = %5$s.	The average GC execution time has exceeded the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: GC generation count at last measurement %3$s: Total GC execution time at last measurement %4$s: GC generation count at this measurement %5$s: Total GC execution time at this measurement %6$s: Average of the GC execution time used from the last measurement to this measurement	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: GC average time is too long compared with the last connection. av = %6$s, last.getCount = %2$s, last.getTime = %3$s, now.getCount = %4$s, now.getTime = %5$s.	After the Java VM to be monitored was reconnected, the average of the GC execution time has exceeded the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: GC generation count at last measurement %3$s: Total GC execution time at last measurement %4$s: GC generation count at this measurement %5$s: Total GC execution time at this measurement %6$s: Average of the GC execution time used from the last measurement to this measurement	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: GC count is too frequently. count = %4$s last.getCount = %2$s, now.getCount = %3$s.	The GC generation count has exceeded the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: GC generation count at last measurement %3$s: GC generation count at this measurement %4$s: GC generation count from the last measurement to this measurement	Review the Java application that runs on the Java VM to be monitored.
%1$s: GC count is too frequently compared with the last connection. count = %4$s last.getCount = %2$s, now.getCount = %3$s.	After the Java VM to be monitored was reconnected, the GC generation count has exceeded the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: GC generation count at last measurement %3$s: GC generation count at this measurement %4$s: GC generation count from the last measurement to this measurement	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: RuntimeMXBean is invalid.	Information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: Failed to measure the runtime stat.	Information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct. Check whether the processing load is high in the Java VM to be monitored.
%1$s: MEMORY_MXBEAN_NAME is invalid. %2$s, %3$s.	Memory information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Memory pool name %3$s: Memory name	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: MemoryMXBean is invalid.	Memory information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Failed to measure the memory stat.	Memory information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct. Check whether the processing load is high in the Java VM to be monitored.
%1$s: MemoryPool name is undefined. memory_name = %2$s.	Memory information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Name of the Java memory pool to be measured	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: MemoryPool capacity is too little. memory_name = %2$s, used = %3$s, max = %4$s, ratio = %5$s%.	The Java memory pool free space has fallen below the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Name of the Java memory pool to be measured %3$s: Use amount of the Java memory pool %4$s: Maximum usable amount of the Java memory pool %5$s: Use rate of the Java memory pool	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: THREAD_MXBEAN_NAME is invalid.	Thread information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: ThreadMXBean is invalid.	Thread information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: Failed to measure the thread stat.	Thread information could not be acquired from Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: Detect Deadlock. threads = %2$s.	Thread deadlock has occurred in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: ID of the deadlock thread	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Thread count is too much(%2$s).	The number of activated threads has exceeded the threshold in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of activated threads at measurement	Review the Java application that runs on the Java VM to be monitored.
%1$s: ThreadInfo is null.Thread count = %2$s.	Thread information could not be acquired in the Java VM to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of activated threads at measurement	Check whether the operating environment of the version of the Java VM to be monitored is correct.
%1$s: Failed to disconnect.	Disconnection from the Java VM to be monitored has failed. %1$s: Name of the Java VM to be monitored	-
%1$s: Failed to connect to WebLogicServer.	WebLogic Server to be monitored could not be connected. %1$s: Name of the Java VM to be monitored	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Failed to connect to Sun JVM.	Java VM and WebOTX to be monitored could not be connected. %1$s: Name of the Java VM to be monitored	Review the Java application that runs on the Java VM and WebOTX to be monitored.
Failed to open the %1$s.	The JVM statistics log could not be output. %1$s: Name of the HA/JVMSaverJVM statistics log file	Check whether the disk has sufficient free space or whether the number of open files has exceeded the upper limit.
%1$s: Can't find monitor file.	No monitoring %1$s: Name of the Java VM to be monitored	-
%1$s: Can't find monitor file, monitor stopped[thread:%2$s].	Monitoring stops. %1$s: Name of the Java VM to be monitored %2$s: Type of the measurement thread	-
%1$s: Failed to create monitor status file.	An internal file could not be created. %1$s: Name of the Java VM to be monitored	Check whether the disk free space and the maximum number of volume files are sufficient.
%1$s: Failed to delete monitor status file.	An internal file could not be deleted. %1$s: Name of the Java VM to be monitored	Check whether there is a problem with the hard disk.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: com.bea:Type=ServerRuntime is invalid.	Information could not be acquired from the Java VM to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1$s: WorkManagerRuntimeMBean or ThreadPoolRuntimeMBean is invalid.	Information could not be acquired from the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the WebLogic Server to be monitored is correct.
%1$s: Failed to measure the WorkManager or ThreadPool stat.	Information could not be acquired from the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored	Check whether the operating environment of the WebLogic Server to be monitored is correct.
%1$s: ThreadPool stat is invalid. last.pending = %2$s, now.pending = %3$s.	The number of waiting requests could not be measured in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s:Number of waiting requests at last measurement %3$s:Number of waiting requests at this measurement	Check whether the operating environment of the version of the WebLogic Server to be monitored is correct.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: WorkManager stat is invalid. last.pending = %2$s, now.pending = %3$s.	The number of waiting requests could not be measured in the work manager of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of waiting requests at last measurement %3$s: Number of waiting requests at this measurement	Check whether the operating environment of the version of the WebLogic Server to be monitored is correct.
%1$s: PendingRequest count is too much. count = %2$s.	The number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of waiting requests at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: PendingRequest increment is too much. increment = %4$s%%, last.pending = %2$s, now.pending = %3$s.	The increment of the number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of waiting requests at last measurement %3$s: Number of waiting requests at this measurement %4$s: Increment of the number of waiting requests from the last measurement to this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: PendingRequest increment is too much compared with the last connection. increment = %4$s, last.pending = %2$s, now.pending = %3$s.	After the WebLogic Server to be monitored was reconnected, the increment of the number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of waiting requests at last measurement %3$s: Number of waiting requests at this measurement %4$s: Increment of the number of waiting requests from the last measurement to this measurement	Review the Java application that runs on the WebLogic Server to be monitored.
%1$s: Throughput count is too much. count = %2$s.	The number of requests executed per unit time has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of requests executed per unit time at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Throughput increment is too much. increment = %4$s, last.throughput = %2$s, now.throughput = %3$s.	The increment of the number of requests executed per unit time has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of requests executed per unit time at last measurement %3$s: Number of requests executed per unit time at this measurement %4$s: Increment of the number of requests executed per unit time from the last measurement to this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Throughput increment is too much compared with the last connection. increment = %4$s, last.throughput = %2$s, now.throughput = %3$s.	After the WebLogic Server to be monitored was reconnected, the increment of the number of requests executed per unit time has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of requests executed per unit time at last measurement %3$s: Number of requests executed per unit time at this measurement %4$s: Increment of the number of requests executed per unit time from the last measurement to this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: PendingRequest count is too much. appName = %2$s, name = %3$s, count = %4$s.	The number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Application name %3$s: Work manager name %4$s: Number of waiting requests	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: PendingRequest increment is too much. appName = %2$s, name = %3$s, increment = %6$s%%, last.pending = %4$s, now.pending = %5$s.	The increment of the number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Application name %3$s: Work manager name %4$s: Number of waiting requests at last measurement %5$s: Number of waiting requests at this measurement %6$s: Increment of the number of waiting requests from the last measurement to this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: PendingRequest increment is too much compared with the last connection. AppName = %2$s, Name = %3$s, increment = %6$s, last.pending = %4$s, now.pending = %5$s.	After the WebLogic Server to be monitored was reconnected, the increment of the number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Application name %3$s: Work manager name %4$s: Number of waiting requests at last measurement %5$s: Number of waiting requests at this measurement %6$s: Increment of the number of waiting requests from the last measurement to this measurement	Review the Java application that runs on the WebLogic Server to be monitored.
%1$s: Can't find WorkManager. appName = %2$s, name = %3$s.	The work manager which was set could not be acquired from the WebLogic Server. %1$s: Name of the Java VM to be monitored %2$s: Application name %3$s: Work manager name	Review the setting of Target WebLogic Work Managers.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: analyze of average start[%2$s].	Analyzing of the average value has started. %1$s: Name of the Java VM to be monitored %2$s: Thread name	-
%1$s: analyze of average finish[%2$s].state = %3$s.	Analyzing of the average value has been completed. %1$s: Name of the Java VM to be monitored %2$s: Thread name %3$s: Status of the target to be monitored	-
%1$s: Average of PendingRequest count is too much. count = %2$s.	The average of the number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of waiting requests at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Average of Throughput count is too much. count = %2$s.	The average of the number of requests executed per unit time has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Number of requests executed per unit time at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.
%1$s: Average of PendingRequest count is too much. AppName = %2$s, Name = %3$s, count = %4$s.	The average of the number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1$s: Name of the Java VM to be monitored %2$s: Application name %3$s: Work manager name %4$s: Number of waiting requests at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.
Error: Failed to operate clpjra_bigip.[%1$s]	%1$s: Error code	Review the setting.
action thread execution did not finish. action is alive = %1$s.	Execution of [Command] has timed out. %1$s: Executable file name specified by [Command]	Forcibly terminate [Command] . Review [Command timeout]. Remove the cause of the timeout, such as a high load.

Continued on next page

Table 10.63 – continued from previous page

Message	Cause of generation	Action
%1$s: Failed to connect to Local JVM. cause = %2$s.	Failed to establish connection to JBoss. %1$s: Monitor target name %2$s: Detailed cause of the failure The detailed cause is one of the following. - Failed to found tool.jar, please set jdk's path for the java path. - Load tool.jar exception - Get Local JVM url path exception - Failed to get process name - Failed to connect to JBoss JVM.	Review [Java Installation Path] and [Process Name]. Specify JDK, instead of JRE, as [Java Installation Path]. Check whether JBoss has started.

10.6.2 JVM load balancer linkage log

Message	Cause of generation	Action
lbadmin command start.	Execution of the load balancer linkage command has started.	-
lbadmin command finish.	Execution of the load balancer linkage command has been completed.	-
Into HealthCheck mode.	The health check function is enabled.	-
Into Weight mode.	The load calculation function of the Java VM to be monitored is valid.	-
The PID of lbadmin.jar is "%1".	ID of the process relating to the load balancer linkage %1: Process ID of lbadmin.jar	-
Thread wait stopped by Exception	Waiting for down judgment has been stopped.	-
Rename Command succeeded.	Renaming of the HTML file has been successful.	-

Continued on next page

Table 10.64 – continued from previous page

Message	Cause of generation	Action
Rename Command failed.	Renaming of the HTML file has failed.	Check the HTML file name and HTML rename destination file name.
%1 doesn't exist.	The rename source HTML file does not exist. %1: HTML file name	Check the HTML file name.
%1 already exists.	The rename destination HTML file already exists. %1: HTML rename destination file name	Check the HTML rename destination file name.
Can't rename file:%1.	Renaming of the HTML file has failed. %1: HTML file name	Check the HTML rename destination file name.
The number of retries exceeded the limit.	The retry count for renaming the HTML file has exceeded the upper limit.	Check the HTML rename destination file name.
The percent of the load is "%1".	Load calculation for the Java VM to be monitored has been successful. %1: Load of Java VM to be monitored	-
stat log (%1) doesn't exist.	There is no JVM statistics log file. %1: JVM statistics log file name	Execute cluster suspend/cluster resume and then restart the Java Resource Agent.
stat log(%1:) cannot be opened for reading.	The JVM statistics log file could not be opened. %1: JVM statistics log file name	Execute cluster suspend/cluster resume and then restart the Java Resource Agent.
format of stat log (%1) is wrong.	The contents of the JVM statistics log file are invalid. %1: JVM statistics log file name	After deleting the JVM statistics log file, execute cluster suspend/cluster resume and then restart the Java Resource Agent.
Failed to get load of application server.	Data for load calculation could not be acquired from the JVM statistics log file.	Review whether the load calculation setting of the Java VM to be monitored is correct.
Can't find lock file(%1s*.stat.lck), maybe HA/JVMSaver did not start yet.	JVM monitoring has not yet started. %1: Internal file name	Start the JVM monitoring.

CHAPTER

ELEVEN

GLOSSARY

GC Abbreviation for garbage collection

Java heap Area in which the Java VM allocates memory according to a memory acquisition request from a Java application. Target of GC

Java memory pool Memory area prepared by the Java VM for Java applications

JMX Abbreviation for Java Management Extensions. Specification used for Java that manages and monitors the hardware and software in the network

JVM operation log File for recording JVM monitor resource operation information. The file is created in the following location:

<*EXPRESSCLUSTER_install_path*>/log/ha/jra/ jragent*.log

(* indicates a number starting at 0.)

JVM statistics log File for recording statistics obtained from JVM monitor resource. The file is created in the following location:

<*EXPRESSCLUSTER_install_path*>/log/ha/jra/*.stat

JVM load balancer linkage log File for recording the load balancer linkage operation information obtained from JVM monitor resource. The file is created in the following location:

<*EXPRESSCLUSTER_install_path*>/log/ha/jra/lbadmin.log

Interconnect A dedicated communication path for server-to-server communication in a cluster.

(Related terms: Private LAN, Public LAN)

Virtual IP address IP address used to configure a remote cluster.

Management client Any machine that uses the Cluster WebUI to access and manage a cluster system.

Startup attribute A failover group attribute that determines whether a failover group should be started up automatically or manually when a cluster is started.

Shared disk A disk that multiple servers can access.

Shared disk type cluster A cluster system that uses one or more shared disks.

Switchable partition A disk partition connected to multiple computers and is switchable among computers.

(Related terms: Disk heartbeat partition)

Cluster system Multiple computers are connected via a LAN (or other network) and behave as if it were a single system.

Cluster shutdown To shut down an entire cluster system (all servers that configure a cluster system).

Cluster partition A partition on a mirror disk or a hybrid disk. Used for managing mirror disks or hybrid disks.

(Related term: Disk heartbeat partition)

Active server A server that is running for an application set.

(Related term: Standby server)

Secondary server A destination server where a failover group fails over to during normal operations.

(Related term: Primary server)

Standby server A server that is not an active server.

(Related term: Active server)

Disk heartbeat partition A partition used for heartbeat communication in a shared disk type cluster.

Data partition A local disk that can be used as a shared disk for switchable partition. Data partition for mirror disks or hybrid disks.

(Related term: Cluster partition)

Network partition All heartbeat is lost and the network between servers is partitioned.

(Related terms: Interconnect, Heartbeat)

Node A server that is part of a cluster in a cluster system. In networking terminology, it refers to devices, including computers and routers, that can transmit, receive, or process signals.

Heartbeat Signals that servers in a cluster send to each other to detect a failure in a cluster.

(Related terms: Interconnect, Network partition)

Public LAN A communication channel between clients and servers.

(Related terms: Interconnect, Private LAN)

Failover The process of a standby server taking over the group of resources that the active server previously was handling due to error detection.

Failback A process of returning an application back to an active server after an application fails over to another server.

Failover group A group of cluster resources and attributes required to execute an application.

Moving failover group Moving an application from an active server to a standby server by a user.

Failover policy A priority list of servers that a group can fail over to.

Private LAN LAN in which only servers configured in a clustered system are connected.

(Related terms: Interconnect, Public LAN)

Primary (server) A server that is the main server for a failover group.

(Related term: Secondary server)

Floating IP address Clients can transparently switch one server from another when a failover occurs.

Any unassigned IP address that has the same network address that a cluster server belongs to can be used as a floating address.

Master server Server displayed on top of the Master Server in Server Common Properties in the Cluster WebUI

Mirror disk connect LAN used for data mirroring in mirror disk or hybrid disk. Mirror connect can be used with primary interconnect.

Mirror disk type cluster A cluster system that does not use a shared disk. Local disks of the servers are mirrored.

CHAPTER

TWELVE

LEGAL NOTICE

12.1 Disclaimer

- Information in this document is subject to change without notice.
- No part of this document may be reproduced or transmitted in any form by any means, electronic or mechanical, for any purpose, without the express written permission of NEC Corporation.

12.2 Trademark Information

- EXPRESSCLUSTER® is a registered trademark of NEC Corporation.
- FastSync™ is a trademark of NEC Corporation.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- Microsoft, Windows, Windows Server, Internet Explorer, Azure, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and other countries.
- SUSE is a registered trademark of SUSE LLC in the United States and other countries.
- Asianux is registered trademark of Cybertrust Japan Co., Ltd. in Japan
- Ubuntu is a registered trademark of Canonical Ltd.
- Amazon Web Services and all AWS-related trademarks, as well as other AWS graphics, logos, page headers, button icons, scripts, and service names are trademarks, registered trademarks or trade dress of AWS in the United States and/or other countries.
- Apache Tomcat, Tomcat, and Apache are registered trademarks or trademarks of Apache Software Foundation.
- Citrix, Citrix XenServer, and Citrix Essentials are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other countries.
- Intel, Pentium, and Xeon are registered trademarks or trademarks of Intel Corporation.
- VMware, vCenter Server, and vSphere is registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- Veritas, the Veritas Logo, and all other Veritas product names and slogans are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the United States and other countries.
- Python is a registered trademark of the Python Software Foundation.
- SVF is a registered trademark of WingArc Technologies, Inc.
- JBoss is a registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.

- Oracle, Oracle Database, Solaris, MySQL, Tuxedo, WebLogic Server, Container, Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates.
- IBM, DB2, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.
- PostgreSQL is a registered trademark of the PostgreSQL Global Development Group.
- Sybase is a registered trademark of Sybase, Inc.
- RPM is a registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.
- F5, F5 Networks, BIG-IP, and iControl are trademarks or registered trademarks of F5 Networks, Inc. in the United States and other countries.
- WebOTX is a registered trademark of NEC Corporation.
- WebSAM is a registered trademark of NEC Corporation.
- Google Cloud Platform (GCP) is a trademark or a registered trademark of Google LLC.
- Other product names and slogans written in this manual are trademarks or registered trademarks of their respective companies.

CHAPTER

THIRTEEN

REVISION HISTORY

Edition	Revised Date	Description
1st	Apr 10, 2020	New manual
2nd	Jul 10, 2020	Corrected the appearance and typographical errors.