EXPRESSCLUSTER X 5.2 for Windows Reference Guide

Release 2

NEC Corporation

Apr 26, 2024

TABLE OF CONTENTS:

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*:Provides information on heartbeat resource.
- 6. *Details on network partition resolution resources*:Provides information on the network partition resolution resource.
- 7. *Forced stop resource details*:Provides information on forced stop resources.
- 8. *Information on other settings*:Provides information on other configurations.
- 9. *EXPRESSCLUSTER command reference*:Provides information on commands available to use in EXPRESSCLUSTER.
- 10. *Troubleshooting*:Provides instruction on how to troubleshoot the problem.
- 11. *Error messages*:Provides explanation on error messages displayed during EXPRESSCLUSTER operation.
- 12. *Glossary*

1.3 EXPRESSCLUSTER X Documentation Set

The EXPRESSCLUSTER X 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.

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 supplement 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.

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


In the figures of this guide, this icon represents EXPRESSCLUSTER.

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

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

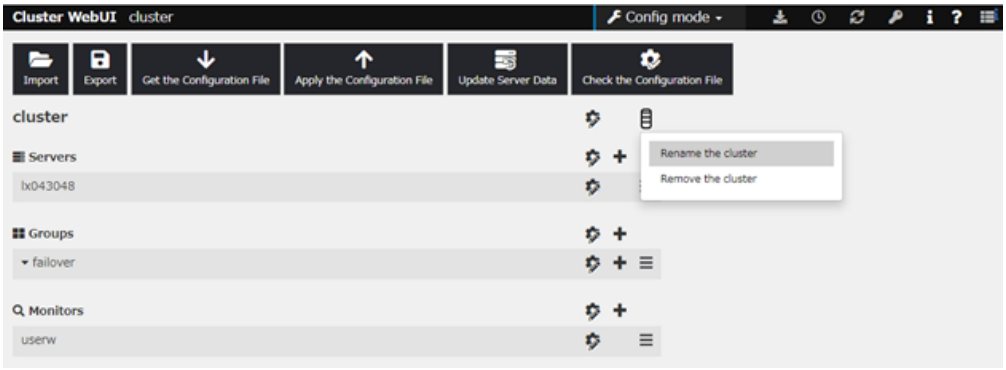
You can view the cluster name, and enter or change a comment for this cluster.

Cluster Name

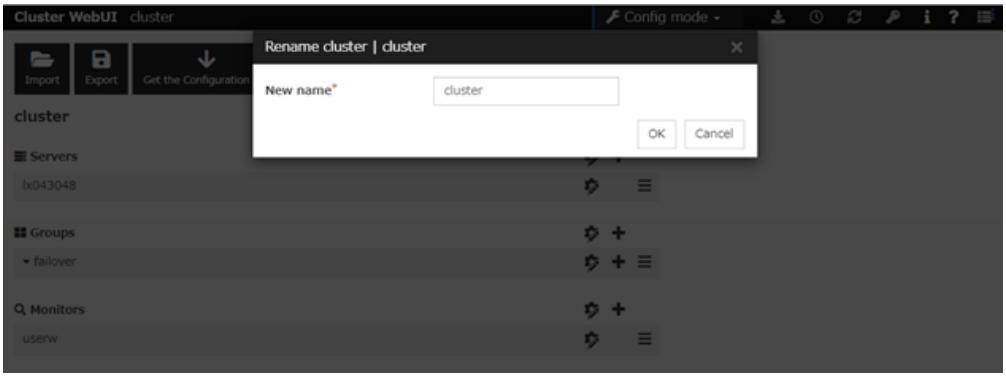
The cluster name is displayed. You cannot change the name here.

Changing the cluster name

1. click **others**, and then select **Rename the cluster**.



2. A dialog box to **rename cluster** is displayed.



Naming rules

- Only alphanumeric characters, hyphen (-), underscore (_) and space are allowed for names.
- Up to 31 characters (31 bytes)

- Names cannot start or end with a hyphen (-) or space.

Comment

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

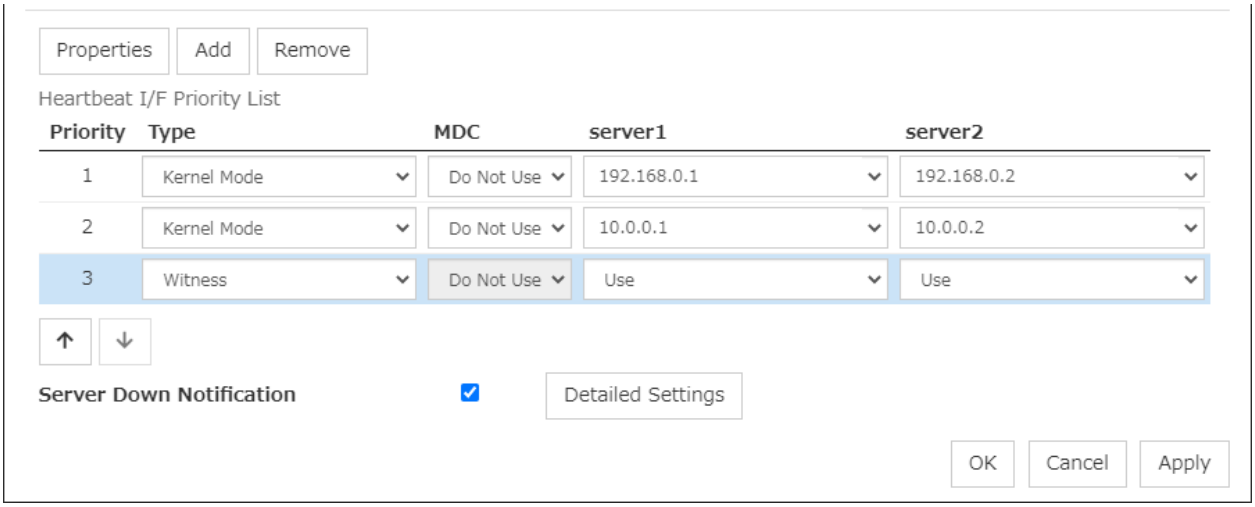
Language

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

- **English**
- **Japanese**
- **Chinese**

2.2.2 Interconnect tab

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



The **Heartbeat I/F Priority 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. For a communication route to which some servers are not connected, leave the cells for the unconnected servers blank.

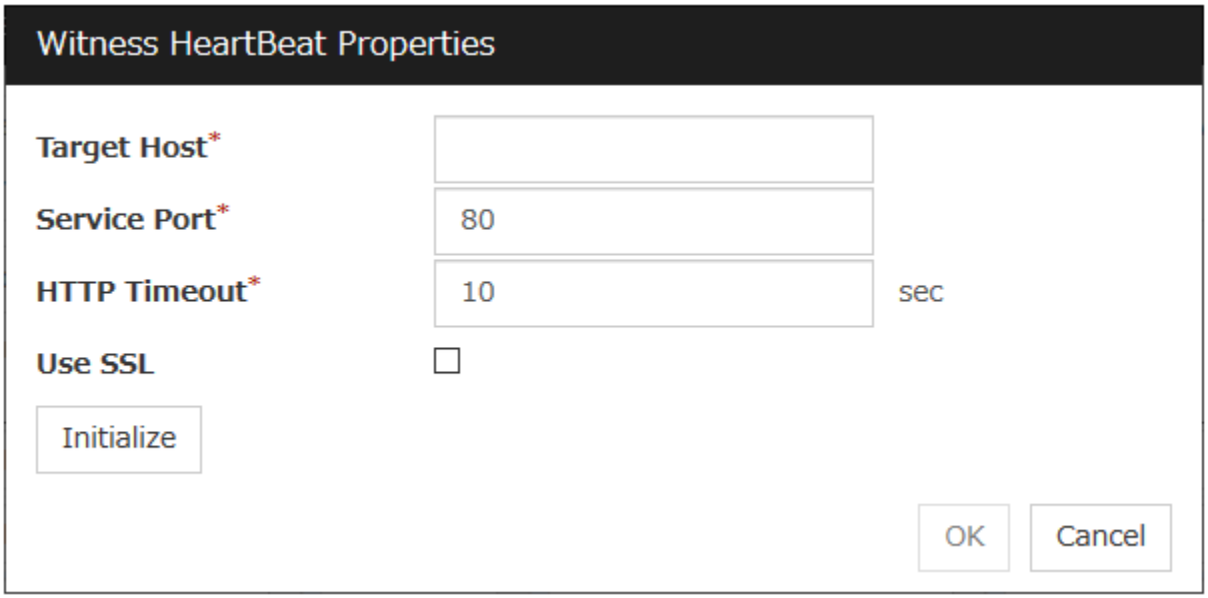
Remove

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 Witness.

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 Proxy

Configures whether or not to use 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

For a communication route used for kernel mode LAN heartbeat transmission (interconnect), click a cell in the **Type** column, and then select **Kernel Mode**.

Specify as many communication routes for the interconnect as possible.

To use Witness heartbeat, select **Witness**.

To prepare a dedicated data mirroring communication path (mirror disk connect), click the **Type** column cell and then select **Mirror Communication Only**.

MDC column

To use a communication path as a mirror disk connect, click the **MDC** column cell and then select a mirror disk connect.

The entry differs depending on the type.

- Kernel Mode or Mirror Communication Only
  Select a mirror disk connect from the combo box.
  When a mirror disk connect is not used, select **Do Not Use**.
- Witness
  No mirror disk connect is available.
  Do Not Use is automatically entered in the **MDC** column cell and the cell cannot be edited.

Server column

The entry differs depending on the type.

- Kernel Mode or Mirror Communication Only
  Enter IP address. Leave the cells for any unused paths blank.
- Witness
  Select either **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

- To list the IP addresses to be set for the interconnect in the list box in the config mode of Cluster WebUI, execute **Update Server Info**.

Server Down Notification

When a server stops successfully (including shutdown and reboot), it is notified to other servers in the cluster. You can perform failover faster by notifying it in advance.

When failing to deactivate groups when a server stops (including shutdown and reboot), or when other abnormalities occur, other servers are not notified of it regardless of the settings of failed server notification.

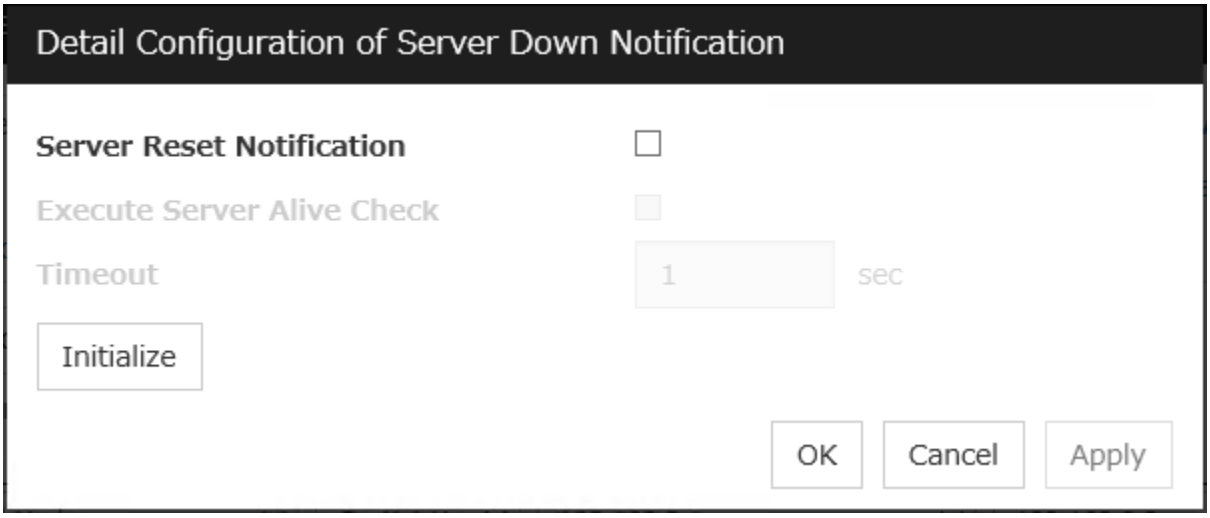
- When the check box is selected:
  Server down will be notified.

- When the check box is not selected:
  Server down will not be notified.

Click **Detailed Settings** to configure the details of server reset notification.

Note:

Making the settings effective requires the following:
The check box of server down notification is checked.



Server Reset Notification

This notification by the server means informing other servers of its stop due to **Reset the hardware** or **Generate an intentional stop error**.

- If the check box is checked:
  With the notification, its source server is regarded as down.
- If the check box is not checked:
  No reaction happens even with the notification.

Execute Server Alive Check

If you enable this option, a server which received the server reset notification checks whether the notification source server is down before the failover.

- If the check box is checked:
  Whether the server is alive is checked before the failover.
- If the check box is not checked:
  Whether the server is alive is not checked before the failover.

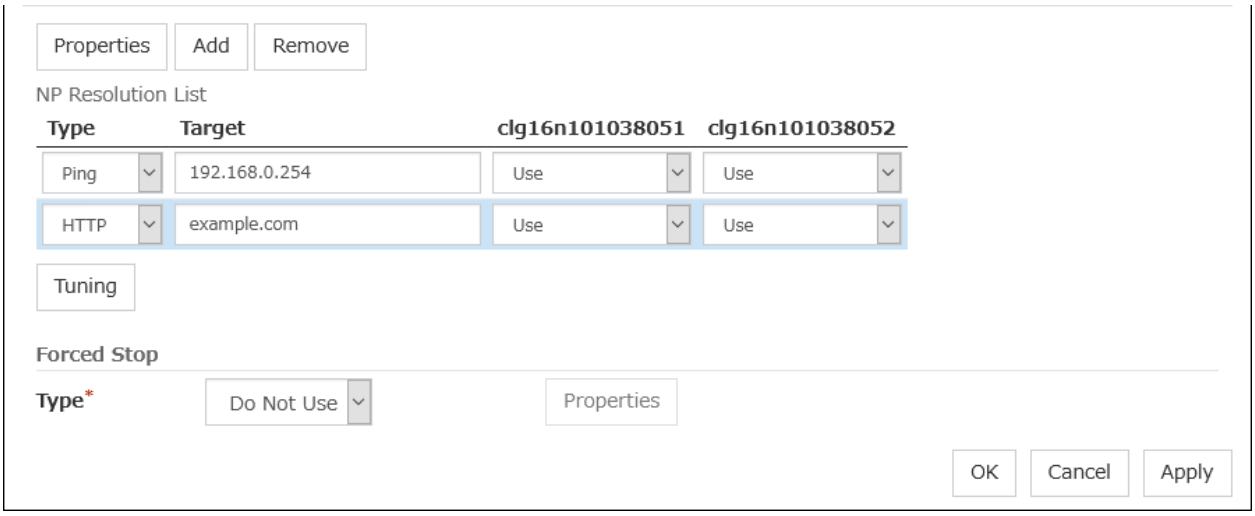
Timeout

Specify a value for the timeout of checking whether the server is alive. If the value is larger than that for the heartbeat timeout, the latter timeout value is applied.

Even if the check is not completed by the time of the timeout occurrence, the failover is performed.

2.2.3 Fencing tab

Set up the network partition (NP) resolution method and the forced stop function.



NP Resolution

The network partition resolution interface used for EXPRESSCLUSTER is displayed on the **NP Resolution List**.

Add

Add network partition resolution (NP resolution) resource. Click the **Type** column cell and select the type of NP resolution (**DISK**, **Ping**, **HTTP**, **Majority**). If the type is **Ping**, click the Ping target column cell and set the IP address of the Ping destination device. Click the cell of each server and set **Use** or **Do Not Use**.

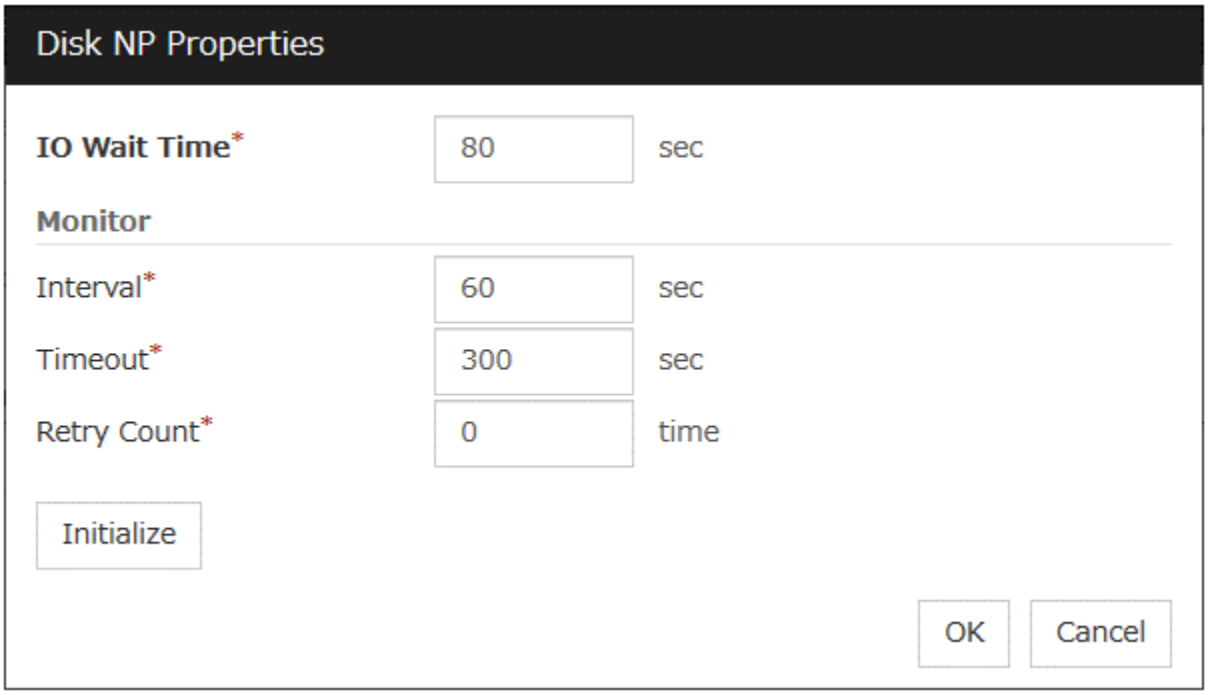
Remove

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

Properties

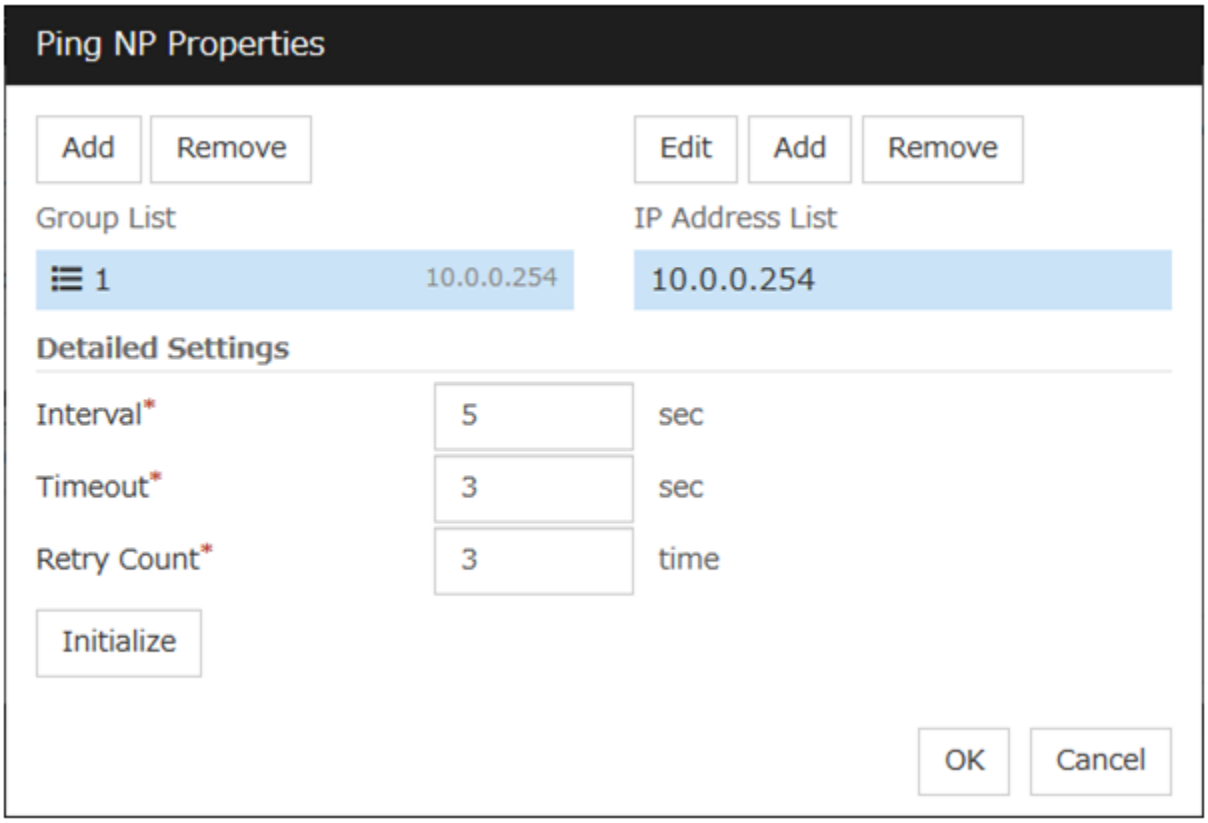
Only available when the selected resource type is **DISK**, **Ping** or **HTTP**. The **DISK NP Properties**, **Ping NP Properties** or **HTTP NP Properties** window is displayed.

DISK NP Properties



- IO Wait Time
  Set the disk I/O wait time. Set the value so that the value exceeds the maximum delay time of the disk I/O of the shared disk device. When the disk path is duplicated, I/O delay caused by switching path needs to be considered.
- Interval
  Set the disk heartbeat interval.
- Timeout
  Set the disk heartbeat timeout.
- Retry Count
  Set the retry count.
- Initialize
  Set the I/O wait time, interval, timeout and retry count to the default values.

Ping NP Properties

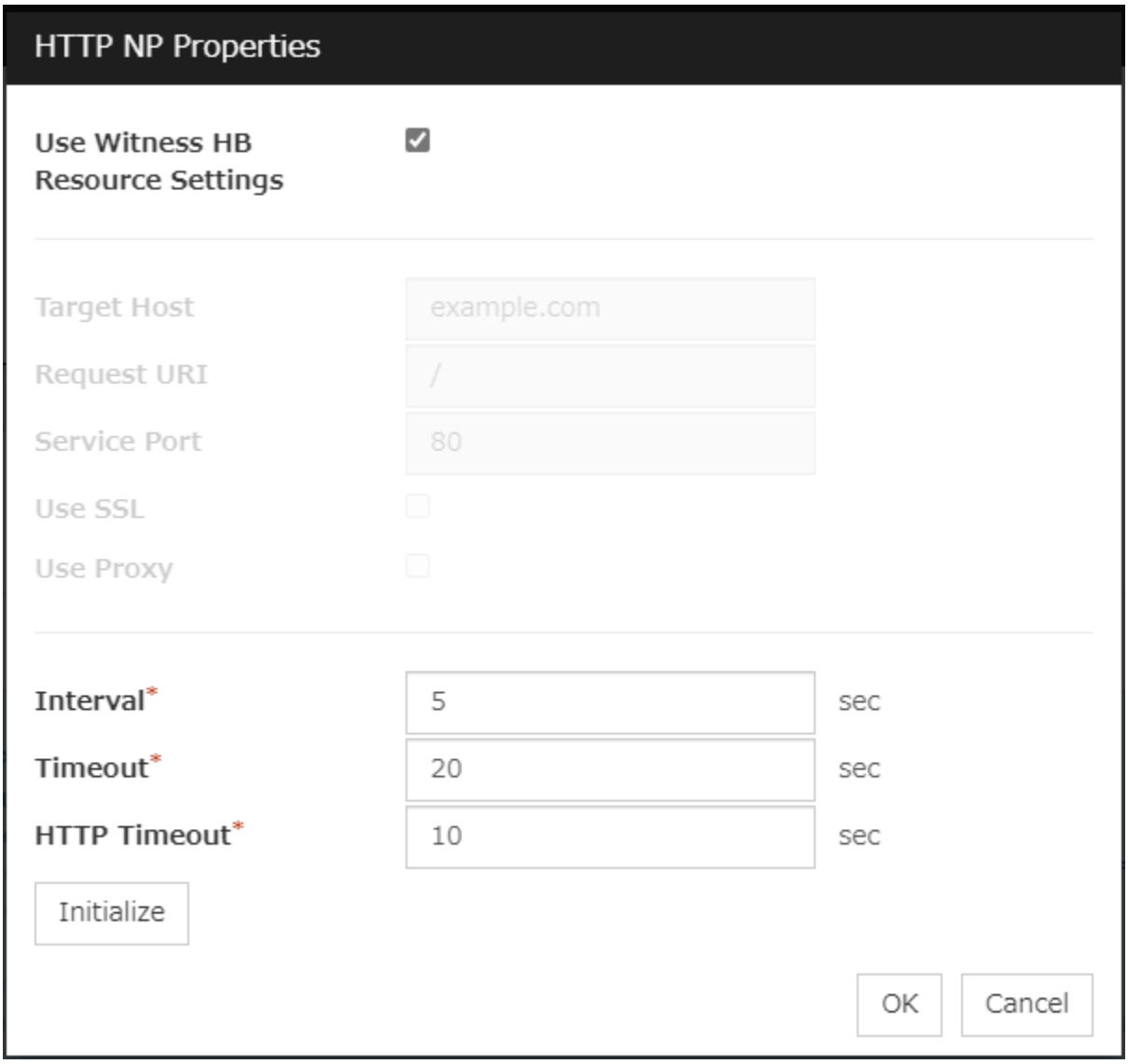


- Add Group List
  - Add IP address group of Ping target.
  - The maximum number of registered group is 16.
  - If two or more IP addresses are registered in one group
    - With a response from one of the IP addresses, no NP state is considered to have occurred.
    - With no response from any of the IP addresses, an NP state is considered to have occurred. Then the action selected in **Action at NP Occurrence** is performed.
  - If two or more groups are registered
    - With a response from one of the IP addresses in a group, the group is considered to be normal.
    - With no response from any of the IP addresses in a group, the group is considered to be abnormal.
    - With one of the groups abnormal, an NP state is considered to have occurred. Then the action selected in **Action at NP Occurrence** is performed.
- 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 resource, 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 timeout of Ping response wait.
- 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 > (interval *retry count)

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.
- Request-URI
  Sets the request-URI of the Web server to be connected: the target host name followed by a string starting from "/".
- 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 Proxy
  Configures whether or not to use proxy for communicating with the Web 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.
- 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 resource. **DISK**, **Ping**, **HTTP**, **Majority** 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 a HTTP request.
- **DISK, Majority**
  N/A

Server

Entry differs depending on the type.

- DISK
  Enter the drive letter for disk heartbeat partition.

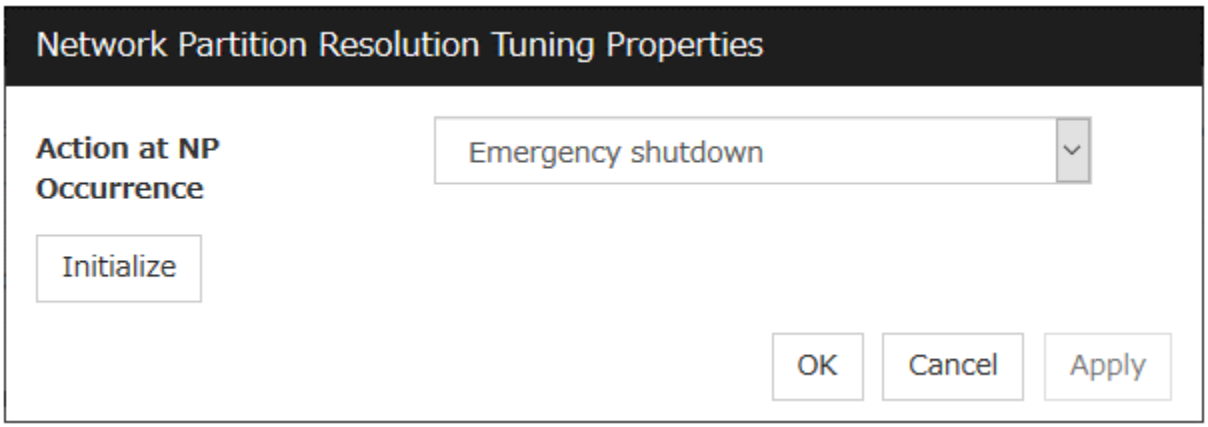
Note: To list the drive letters to be set for the disk heartbeat partition in the list box in the config mode of Cluster WebUI execute **Update Server Info**.

- Ping, HTTP, Majority
  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 EXPRESSCLUSTER Server service of the server in network partition.
  - Stop the cluster service and shutdown OS
    Stop the EXPRESSCLUSTER Server service of the server in network partition, and then shuts down the OS.
  - Stop the cluster service and reboot OS
    Stop the EXPRESSCLUSTER Server service of the server in network partition, and then reboots the OS.
  - Emergency shutdown
    Shutdown the server in network partition.
  - Generate an intentional stop error
    Intentionally cause stop error for the server in network partition.
  - Reset the hardware[1]
    Restart the server by HW reset in network partition.

Note:

When mirror disk resources or hybrid disk resources are used, it is not recommended that you set **Stop the cluster service** for **Action at NP Occurrence**.
If **Stop the cluster service** is set, you might have to run the forcible mirror recovery at the time of recovery from NP occurrence.

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

[1] This function does not require ipmiutil, unlike the forced stop function.

Forced Stop

Type

Specify a type of forced stop resource to be used. If no forced stop resources are to be used, select **Do Not Use**.

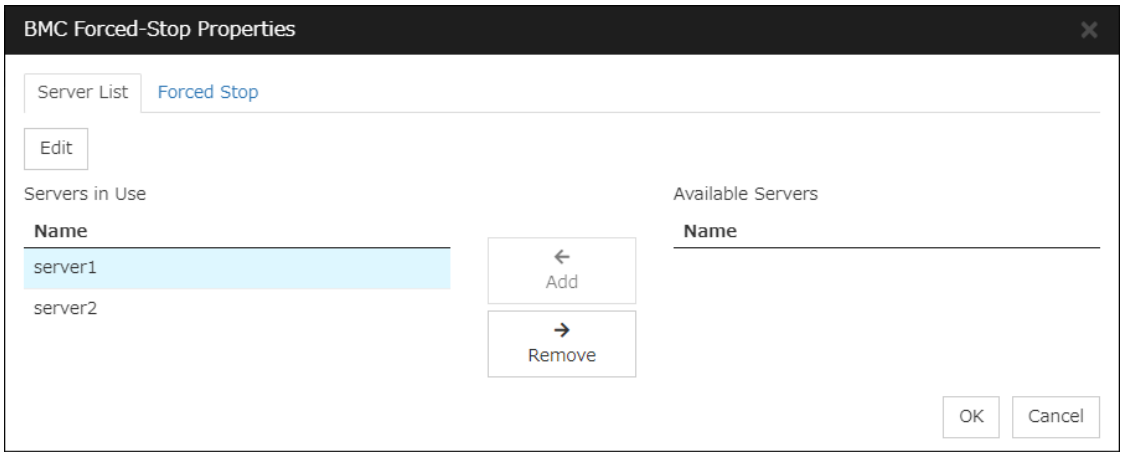
Properties

Displays the properties window of a forced stop resource corresponding to the specified type.

BMC Forced Stop Properties

Configure the forced stop of a physical machine. The **BMC Forced Stop Properties** dialog box is displayed by selecting **BMC** as a type of forced stop resource and then clicking **Properties**.

Server List tab



Add

Adds, from available servers, a server to be configured. Selecting a server and clicking **Add** displays the **Enter BMC** 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 name of a user with administrator privilege from the user names configured in BMC.
  If you do not enter anything, do not configure the user name argument when executing the ipmiutil command.

The length of the actually valid user name depends on the ipmiutil command and the BMC specifications of the server.

- Password (Within 255 bytes)

  Enter the password of user configured above.

  The length of the actually valid user name depends on the ipmiutil command and the BMC specifications of the server.

  For information on user name of IPMI and how to configure the password, refer to the manual of the server.

Remove

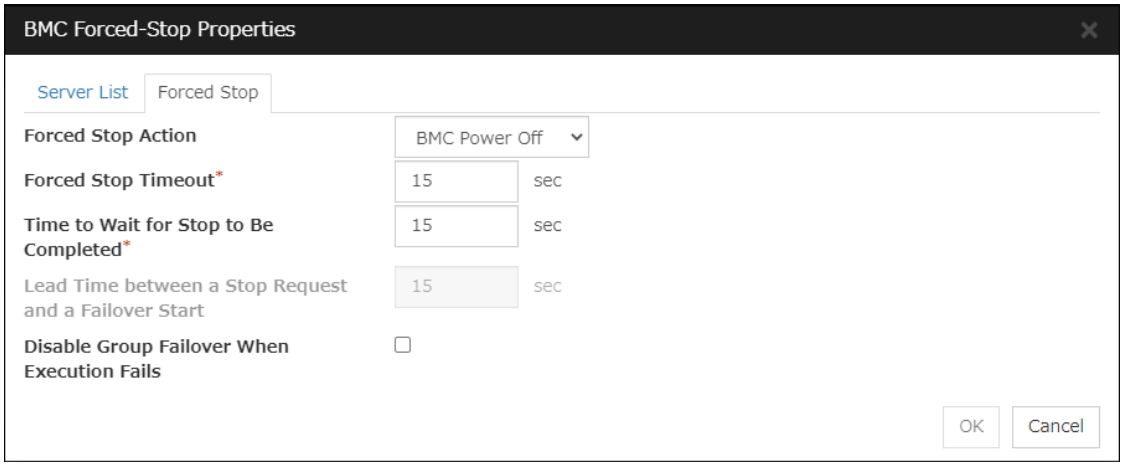
Removes a server in use. Select an unnecessary server, then click **Remove**.

Edit

Use this for changing the settings of a server. Select a desired server, then click **Edit**. This displays the **Enter BMC** dialog box.

When configuring a cluster with different server models, exclude a server having no BMC. If you added such a server, the forced stop function would alert you to a failure in a periodical check on forcibly stopping the BMC.

Forced stop tab



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 ipmiutil command.

- BMC Power Off

  Use this to power off the server by using the ipmiutil command.

  OS may be shut down depending on how the Power Options of OS is configured. The OS may be shut down depending on how the **Power Options** of OS is configured. For details, see "*Notes on BMC forced stop resource*" in "*Understanding forced stop on physical environment*" in "7. *Forced stop resource details*" in this guide.

- BMC Power Cycle

  Use this to perform the Power Cycle (powering on/off) by using the ipmiutil command. The OS may be shut down depending on how the ACPI of OS is configured. For details, see "*Notes on BMC forced stop resource*" in "*Understanding forced stop on physical environment*" in "7. *Forced stop resource details*" in this guide.

- BMC NMI
  Use this to generate NMI by using the ipmiutil command. The behavior after NMI is generated depends on the OS settings.

Forced Stop Timeout (0 to 999)

Specify a value for the timeout of awaiting the completion of a forced stop in action.

Time to Wait for Stop to Be Completed (0 to 999)

Specify a value for awaiting the completion of a forced stop in action. During the specified time period from the time of requesting a forced stop, whether the forced stop is completed is checked.

Specify this value with **BMC Power Off** selected for **Forced Stop Action**.

Lead Time between a Stop Request and a Failover Start (0 to 999)

Specify a value for awaiting the start of a failover with a forced stop in action. The failover occurs after a forced stop is requested and the specified time passes.

Specify this value with **BMC Reset**, **BMC Power Cycle**, or **BMC NMI** selected for **Forced Stop Action**.

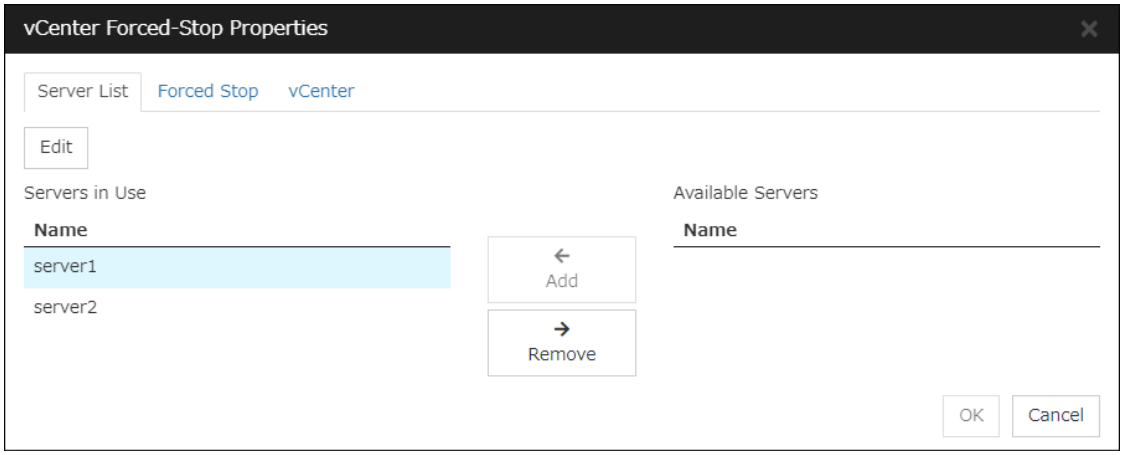
Disable Group Failover When Execution Fails

Suppresses group failover if a forced stop fails. Since the group is not started in the failover destination in this case, check the state of the failover source, then manipulate the group as needed.

vCenter Forced Stop Properties

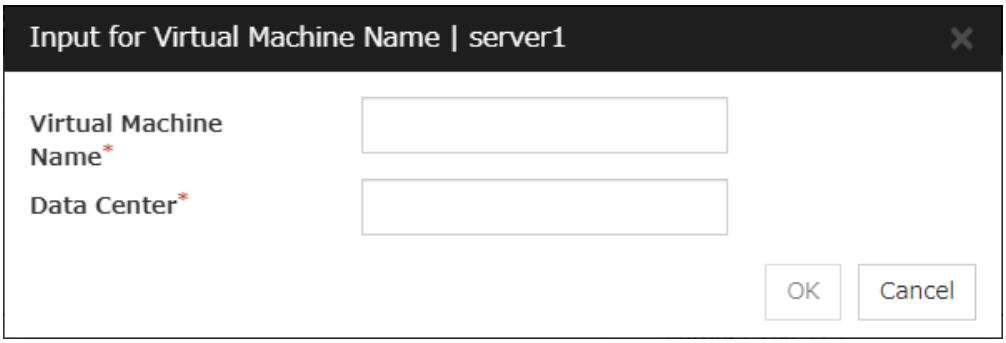
Configure the forced stop of a virtual machine (guest OS). The **vCenter Forced Stop Properties** dialog box is displayed by selecting **vCenter** as a type of forced stop resource and then clicking **Properties**.

Server List tab



Add

Adds, from available servers, a server to be configured. Selecting a server and clicking **Add** displays the **Input for Virtual Machine name** dialog box.



- 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 data center name.

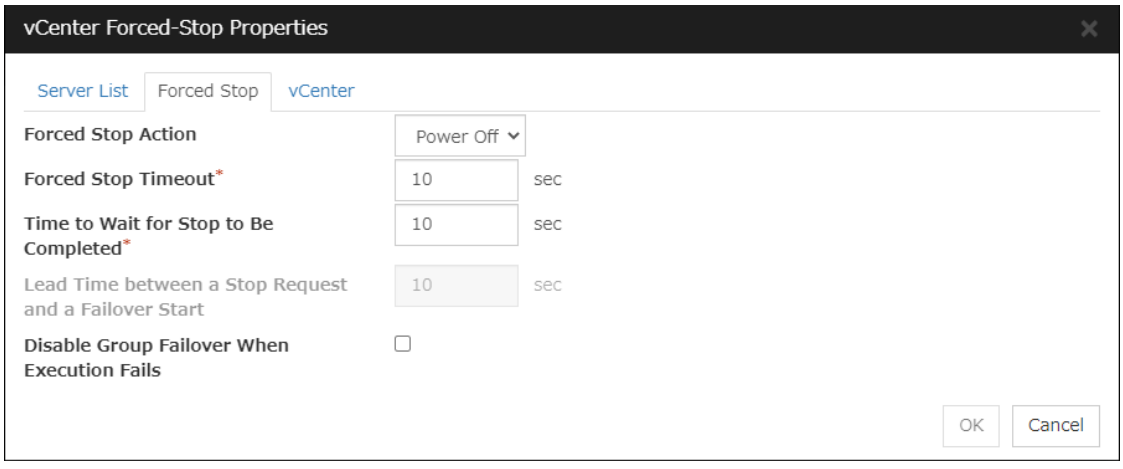
Remove

Removes a server in use. Select an unnecessary server, then click **Remove**.

Edit

Use this for changing the settings of a server. Select a desired server, then click **Edit**. This displays the **Input for Virtual Machine name** dialog box.

Forced stop tab



Forced Stop Action

Specify an action of the forced stop.

- Power Off
  Use this to power off the server by using the vmcontrol command.

- Reset
  Use this to perform a hardware reset of the server by using the vmcontrol command.

Forced Stop Timeout (0 to 999)

Specify a value for the timeout of awaiting the completion of a forced stop in action.

Time to Wait for Stop to Be Completed (0 to 999)

Specify a value for awaiting the completion of a forced stop in action. During the specified time period from the time of requesting a forced stop, whether the forced stop is completed is checked.

Specify this value with **Power Off** selected for **Forced Stop Action**.

Lead Time between a Stop Request and a Failover Start (0 to 999)

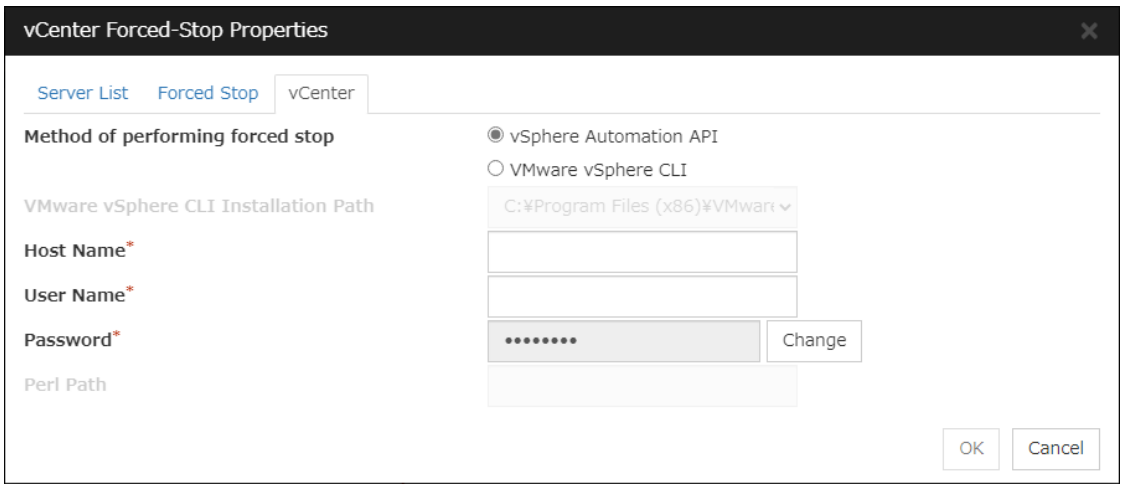
Specify a value for awaiting the start of a failover with a forced stop in action. The failover occurs after a forced stop is requested and the specified time passes.

Specify this value with **Reset** selected for **Forced Stop Action**.

Disable Group Failover When Execution Fails

Suppresses group failover if a forced stop fails. Since the group is not started in the failover destination in this case, check the state of the failover source, then manipulate the group as needed.

vCenter tab



Method of performing forced stop

Specify the Method of performing forced stop.

- vSphere Automation API
  Perform a forced stop by using the REST API.
- VMware vSphere CLI
  Perform a forced stop by using the VMware vSphere Command Line Interface.

VMware vSphere CLI Installation Path (Within 1023 bytes)

Specify the installation path of the VMware vSphere CLI.

This setting is required with **VMware vSphere CLI** specified as the method of performing a forced stop.

Specification example:`C:\Program Files (x86)\VMware\VMware vSphere CLI`

Host name (Within 255 bytes)

Specify the IP address of the virtual machine management tool.

User Name (Within 255 bytes)

Specify the user name of the virtual machine management tool.

Password (Within 255 bytes)

Specify the password for the virtual machine management tool.

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

Perl Path (Within 255 bytes)

Specify the Perl path to be used when executing the virtual machine forced stop. Specify an absolute path using ASCII characters. Do not add "" to the end of the path.

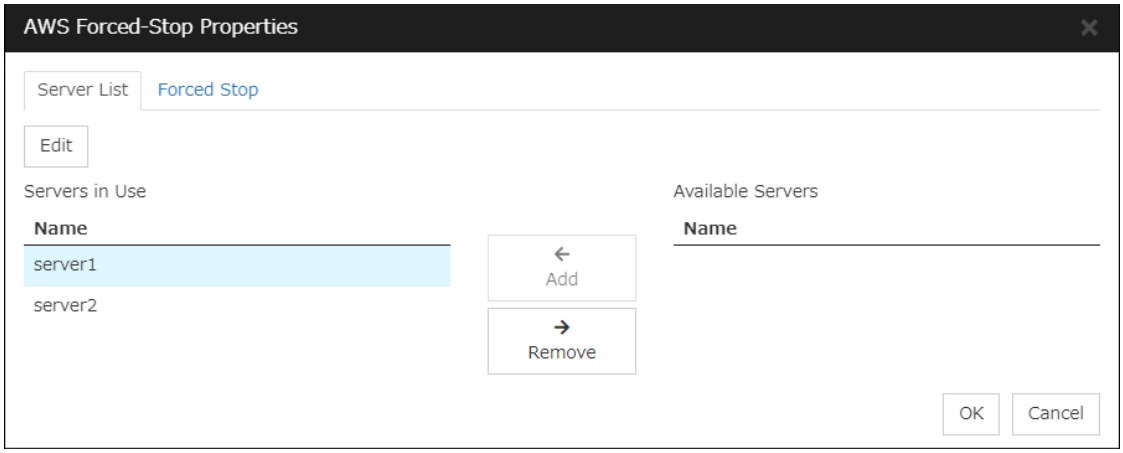
This setting is required with **VMware vSphere CLI** specified as the method of performing a forced stop.

Specification example:`C:\Perl64\bin\perl.exe`

AWS Forced Stop Properties

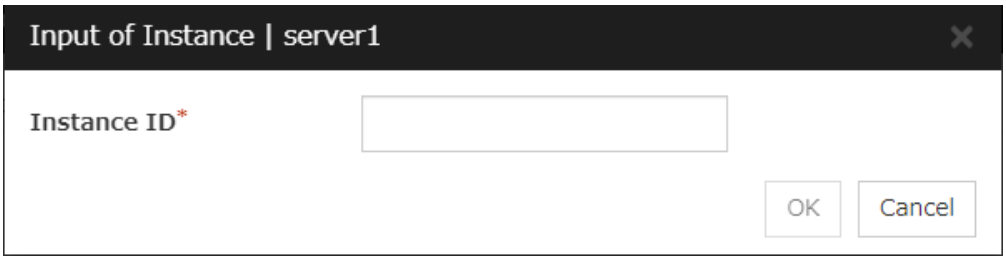
Configure the forced stop of Amazon Web Services. The **AWS Forced Stop Properties** dialog box is displayed by selecting **AWS** as a type of forced stop resource and then clicking **Properties**.

Server List tab



Add

Adds, from available servers, a server to be configured. Selecting a server and clicking **Add** displays the **Input of Instance** dialog box.



- Instance ID (Within 32 bytes)
  Specify the instance ID of AWS.

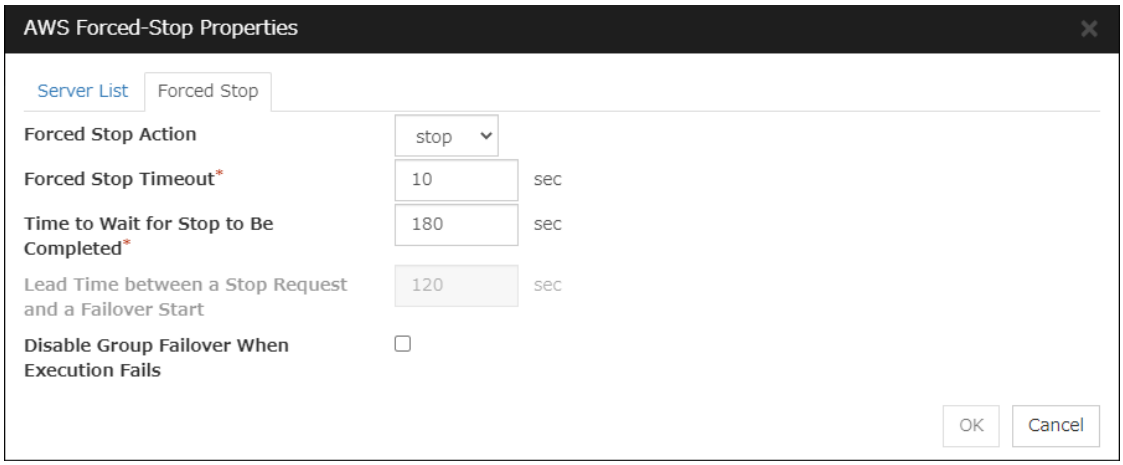
Remove

Removes a server in use. Select an unnecessary server, then click **Remove**.

Edit

Use this for changing the settings of a server. Select a desired server, then click **Edit**. This displays the **Input of Instance** dialog box.

Forced stop tab



Forced Stop Action

Specify an action of the forced stop.

- stop
  Uses the AWS CLI to stop the instance.
- reboot
  Uses the AWS CLI to reboot the instance.

Forced Stop Timeout (0 to 999)

Specify a value for the timeout of awaiting the completion of a forced stop in action.

Time to Wait for Stop to Be Completed (0 to 999)

Specify a value for awaiting the completion of a forced stop in action. During the specified time period from the time of requesting a forced stop, whether the forced stop is completed is checked.

Specify this value with **stop** selected for **Forced Stop Action**.

Lead Time between a Stop Request and a Failover Start (0 to 999)

Specify a value for awaiting the start of a failover with a forced stop in action. The failover occurs after a forced stop is requested and the specified time passes.

Specify this value with **reboot** selected for **Forced Stop Action**.

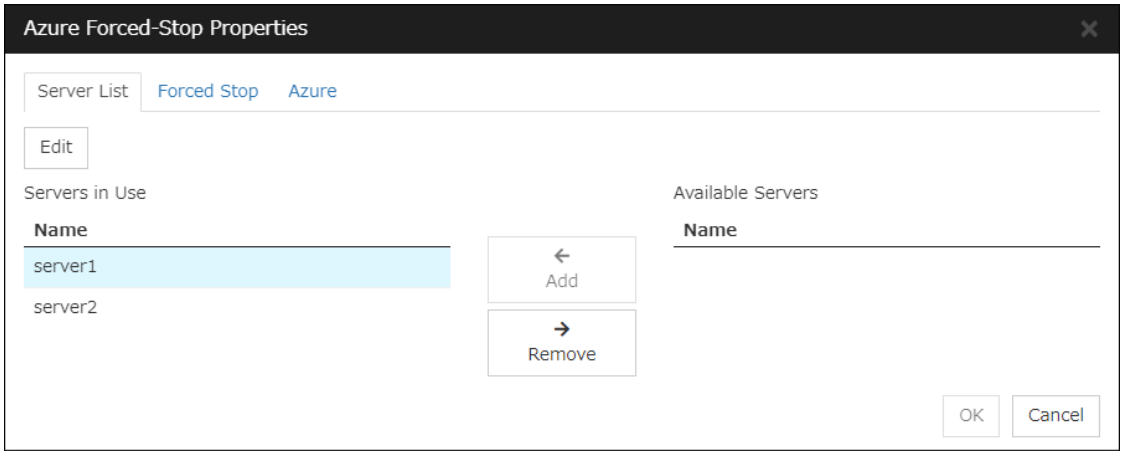
Disable Group Failover When Execution Fails

Suppresses group failover if a forced stop fails. Since the group is not started in the failover destination in this case, check the state of the failover source, then manipulate the group as needed.

Azure Forced Stop Properties

Configure the forced stop of Microsoft Azure. The **Azure Forced Stop Properties** dialog box is displayed by selecting **Azure** as a type of forced stop resource and then clicking **Properties**.

Server List tab



Add

Adds, from available servers, a server to be configured. Selecting a server and clicking **Add** displays the **Input for Virtual Machine name** dialog box.

- Virtual Machine name (Within 64 bytes)
  Specify an Azure virtual-machine name.

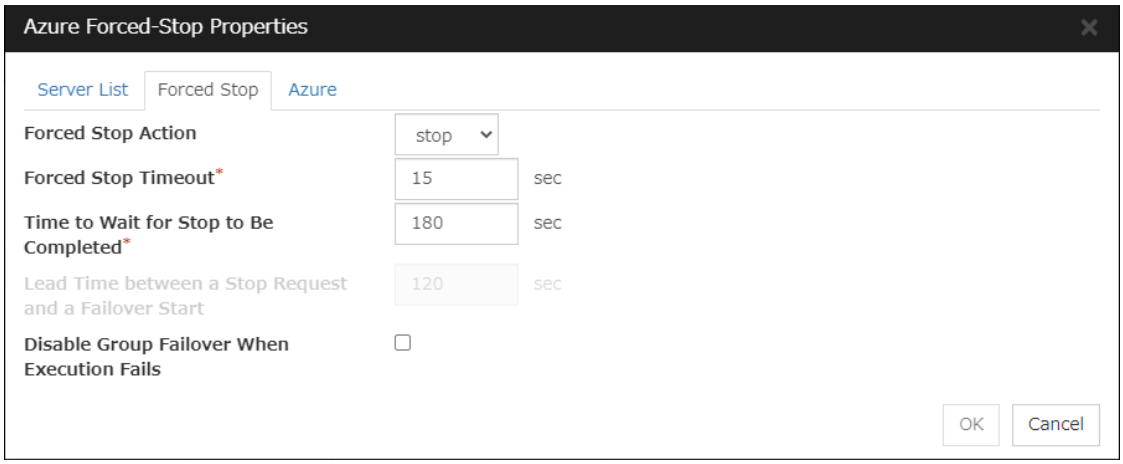
Remove

Removes a server in use. Select an unnecessary server, then click **Remove**.

Edit

Use this for changing the settings of a server. Select a desired server, then click **Edit**. This displays the **Input for Virtual Machine name** dialog box.

Forced stop tab



Forced Stop Action

Specify an action of the forced stop.

- stop
  Uses the Azure CLI to stop the instance.
- reboot
  Uses the Azure CLI to reboot the instance.

Forced Stop Timeout (0 to 999)

Specify a value for the timeout of awaiting the completion of a forced stop in action.

Time to Wait for Stop to Be Completed (0 to 999)

Specify a value for awaiting the completion of a forced stop in action. During the specified time period from the time of requesting a forced stop, whether the forced stop is completed is checked.

Specify this value with **stop** selected for **Forced Stop Action**.

Lead Time between a Stop Request and a Failover Start (0 to 999)

Specify a value for awaiting the start of a failover with a forced stop in action. The failover occurs after a forced stop is requested and the specified time passes.

Specify this value with **reboot** selected for **Forced Stop Action**.

Disable Group Failover When Execution Fails

Suppresses group failover if a forced stop fails. Since the group is not started in the failover destination in this case, check the state of the failover source, then manipulate the group as needed.

Azure tab

User URI (within 2048 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 1024 bytes)

Specify the full path (including the drive letter) to the file of a service principal (certificate) to log in to Microsoft Azure.

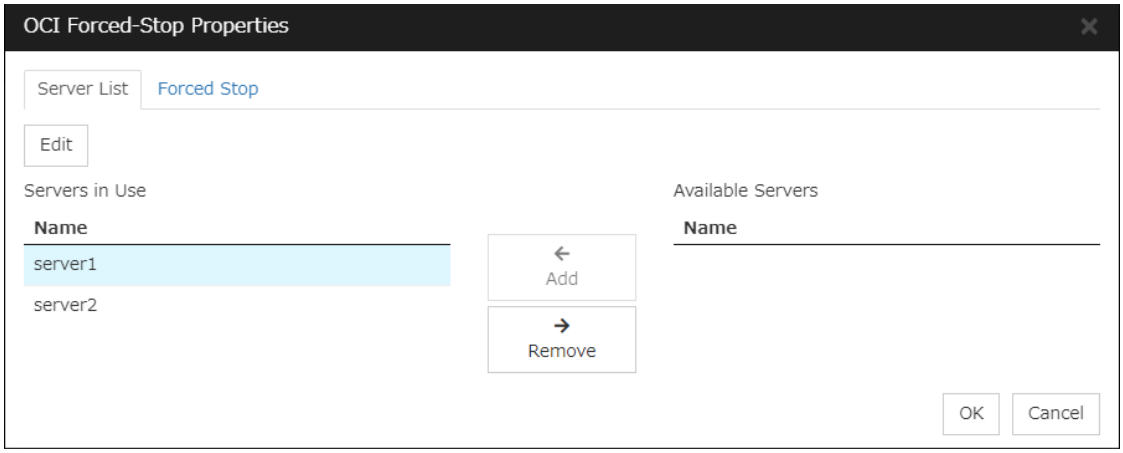
Resource Group Name (within 90 bytes)

Specify a Microsoft Azure resource group name.

OCI Forced Stop Properties

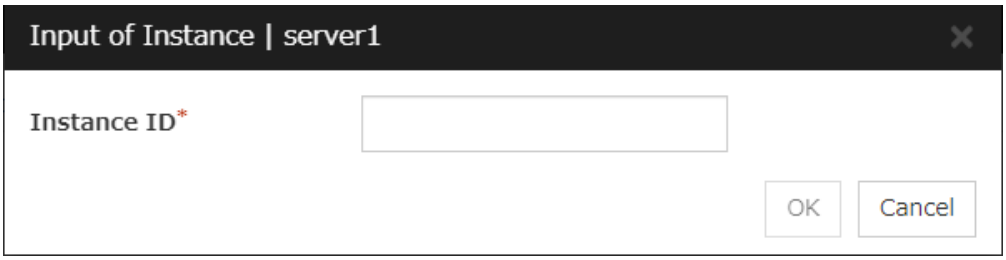
Configure the forced stop of Oracle Cloud Infrastructure. The **OCI Forced Stop Properties** dialog box is displayed by selecting **OCI** as a type of forced stop resource and then clicking **Properties**.

Server List tab



Add

Adds, from available servers, a server to be configured. Selecting a server and clicking **Add** displays the **Input of Instance** dialog box.



- Instance ID (Within 255 bytes)
  Specify the instance ID of OCI.

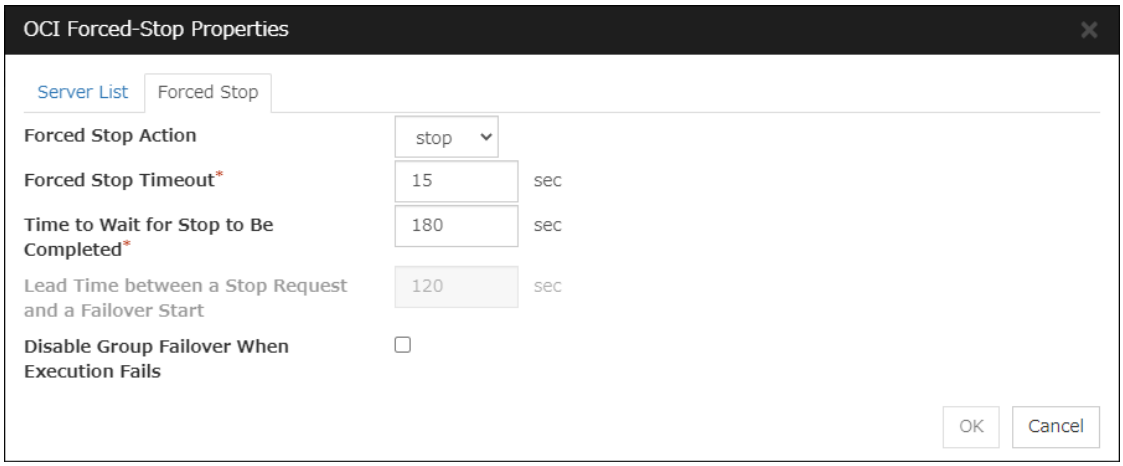
Remove

Removes a server in use. Select an unnecessary server, then click **Remove**.

Edit

Use this for changing the settings of a server. Select a desired server, then click **Edit**. This displays the **Input of Instance** dialog box.

Forced stop tab



Forced Stop Action

Specify an action of the forced stop.

- stop
  Uses the OCI CLI to stop the instance.
- reboot
  Uses the OCI CLI to reboot the instance.

Forced Stop Timeout (0 to 999)

Specify a value for the timeout of awaiting the completion of a forced stop in action.

Time to Wait for Stop to Be Completed (0 to 999)

Specify a value for awaiting the completion of a forced stop in action. During the specified time period from the time of requesting a forced stop, whether the forced stop is completed is checked.
Specify this value with **stop** selected for **Forced Stop Action**.

Lead Time between a Stop Request and a Failover Start (0 to 999)

Specify a value for awaiting the start of a failover with a forced stop in action. The failover occurs after a forced stop is requested and the specified time passes.

Specify this value with **reboot** selected for **Forced Stop Action**.

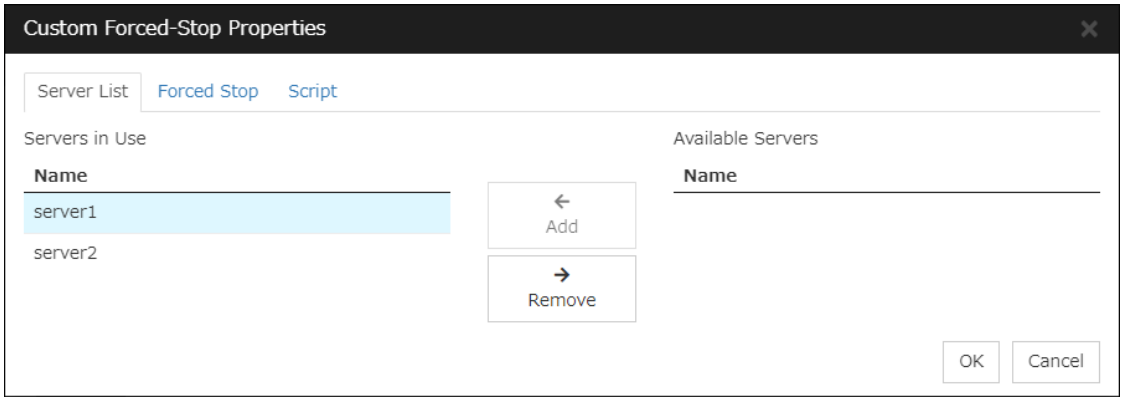
Disable Group Failover When Execution Fails

Suppresses group failover if a forced stop fails. Since the group is not started in the failover destination in this case, check the state of the failover source, then manipulate the group as needed.

Custom Forced Stop Properties

Make settings on the script for the forced stop. The **Custom Forced Stop Properties** dialog box is displayed by selecting **Custom** as a type of forced stop resource and then clicking **Properties**.

Server List tab



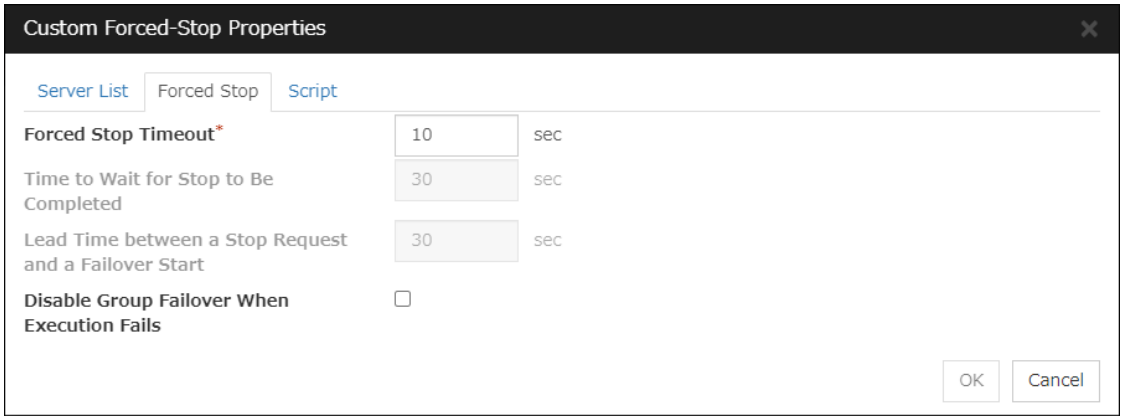
Add

Adds a server from available servers.

Remove

Removes a server in use. Select an unnecessary server, then click **Remove**.

Forced stop tab



Forced Stop Timeout (0 to 999)

Specify a value for the timeout of awaiting the completion of a forced stop in action.

Time to Wait for Stop to Be Completed (0 to 999)

Not to be specified for this function.

Lead Time between a Stop Request and a Failover Start (0 to 999)

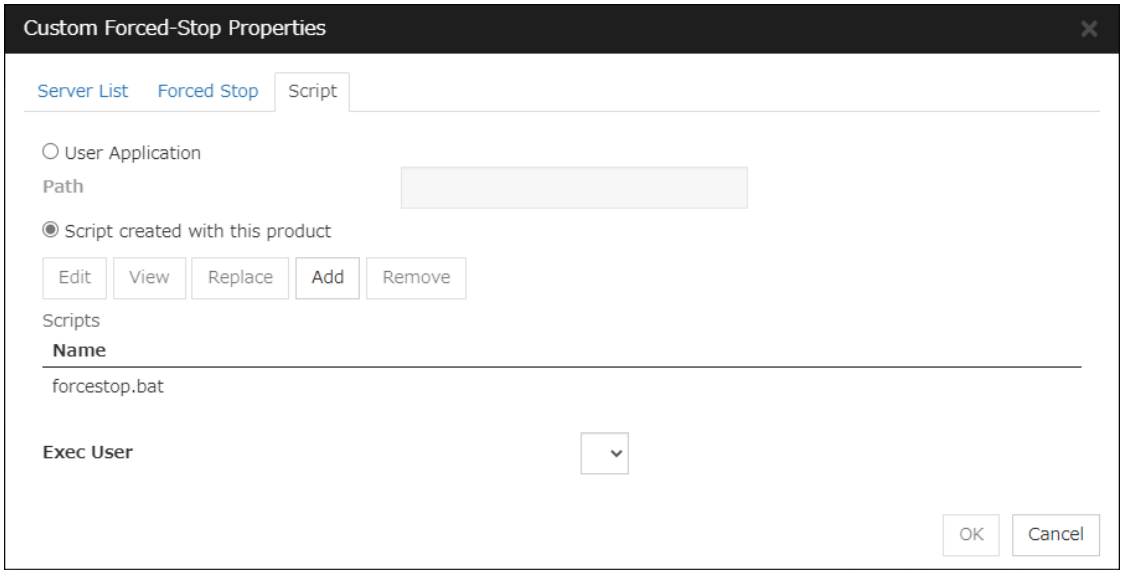
Not to be specified for this function.

Disable Group Failover When Execution Fails

Suppresses group failover if a forced stop fails. Since the group is not started in the failover destination in this case, check the state of the failover source, then manipulate the group as needed.

Script tab

The default script file names, forcestop.bat, are listed on Scripts.



User Application

Use an executable file (executable batch 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 you specify only the name of the executable file, you must configure the path with environment variable in advance. If there is any blank in the absolute path or the file name, put them in double quotation marks ("") as follows.

Example: "C:\Program Files\script.bat"

If you want to execute VBScript, enter a command and VBScript file name as follows.

Example: cscript script.vbs

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 batch 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.bat** 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.bat** 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

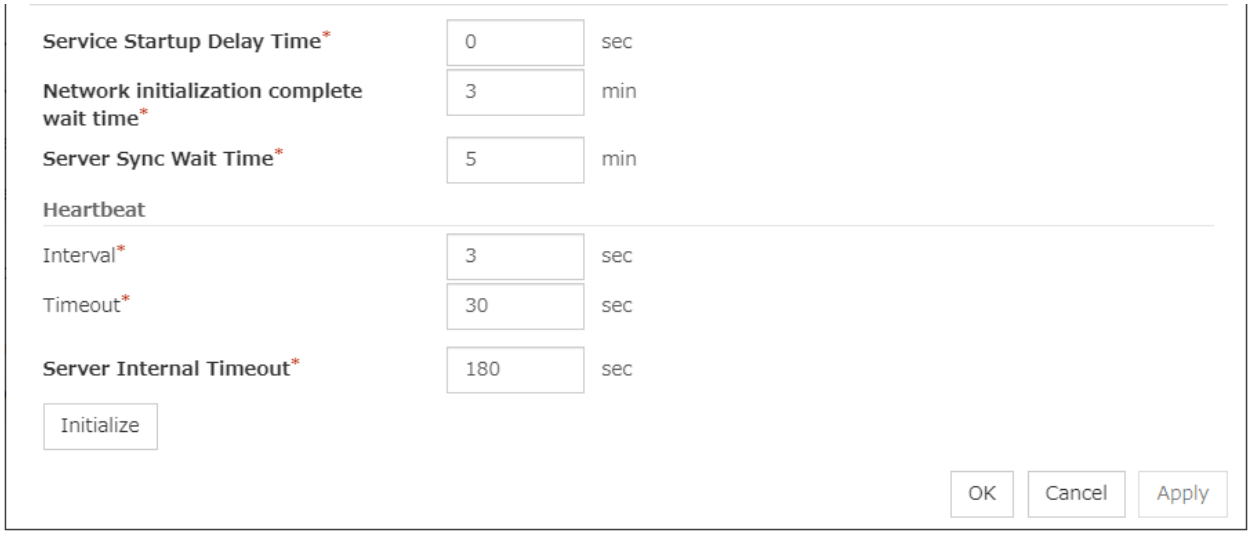
Click here to replace the contents of a script file with the contents of the script file which you selected in the file selection dialog box when you select **Script created with this product**. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not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

Exec User

Specify a user to perform a script. An exec user can be selected from **Account** tab of **Cluster properties**.
If you do not specify an exec user, the script is run by a system account.

2.2.4 Timeout tab

Specify values such as time-out on this tab.



Service Startup Delay Time (0 to 9999)

Specify how long starting the cluster service should be delayed in starting the OS.

Network initialization complete wait time (0 to 99)

This is the time the server waits until its NIC becomes valid after startup.

Server Sync Wait Time (0 to 99)

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

Heartbeat

- Interval (1 to 99)
  Interval of heartbeats
- Timeout (2 to 9999)
  A server is determined to be failed if there is no response for the time specified here.
  This time-out should be longer than the interval.

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.

Note:

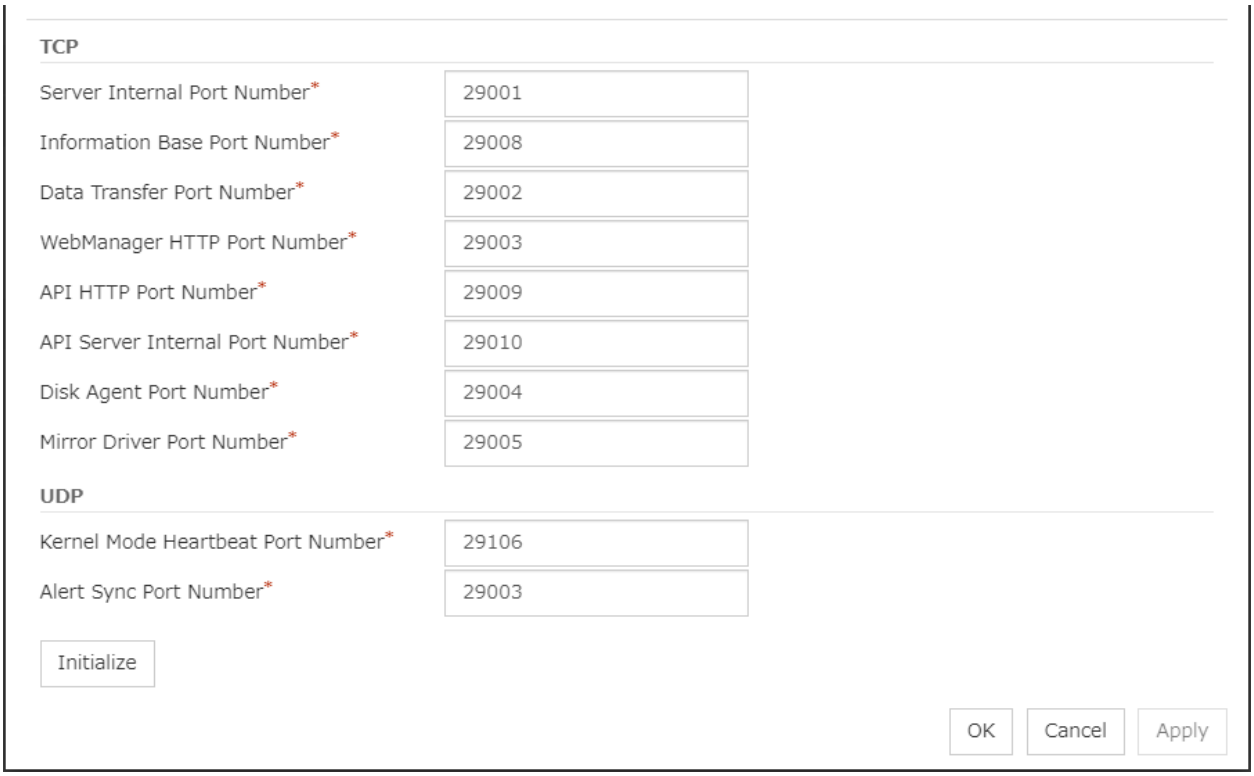
It is recommended to use the default value.
Setting this parameter to an extremely large value significantly affects, in case of a heartbeat loss, the time for executing the clpstat command or for displaying Cluster WebUI.

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/Replicator DR is used, they should not be overlapped with any mirror data port number of any mirror disk resources and hybrid disk resource.

- Server Internal Port Number (1 to 65535[2])
  This port number is used for internal communication.
- Information Base Port Number (1 to 65535[2])
  This port number is used for cluster information management.
- Data Transfer Port Number (1 to 65535[2])
  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[2])
  This port number is used for a browser to communicate with the EXPRESSCLUSTER Server.
- API HTTP Port Number (1 to 65535[2])
  This port number is used when a Restful API client communicates with the EXPRESSCLUSTER Server.
- API Server Internal Port Number (1 to 65535[2])
  This port number is used for internal communication of Restful API.
- Disk Agent Port Number (1 to 65535[2])
  This port number is used for a disk agent port number.
- Mirror Driver Port Number (1 to 65535[2])
  This port number is used for a mirror driver.

UDP

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

No UDP port numbers can be overlapped.

- Kernel Mode Heartbeat Port Number (1 to 65535[2])
  This port number is used for kernel mode heartbeat.
- Alert Sync Port Number (1 to 65535[2])
  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 the items to the default values.

2.2.6 Recovery tab

Make settings on cluster recovery.

Action When the Cluster Service Process Is Failure

Specify an action at process abnormity of the cluster service.

- Emergency shutdown
  Shutdown the server.

  Note: With a user mode monitor resource in operation: When a heartbeat timeout occurs during a shutdown, the system may perform a specified action which will be taken on a timeout occurrence in the user mode monitor resource.

- Generate an intentional stop error
  Generate a stop error (Panic) intentionally and restart the server.
- Reset the hardware[3]
  Restart the server by HW reset.

This function allows monitoring the following cluster service process:

[3] This function does not require ipmiutil, unlike the forced stop function.

- clprc.exe

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 resource, Process resource monitor resource, JVM monitor resource, and 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.

- Emergency shutdown
  Shutdown the server on which a stall occurred.
- Generate an intentional stop error
  Intentionally cause a stop error (Panic) on the server on which a stall occurred.
- 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*" , "*Resource Properties*"in "3. *Group resource details*" in this guide.

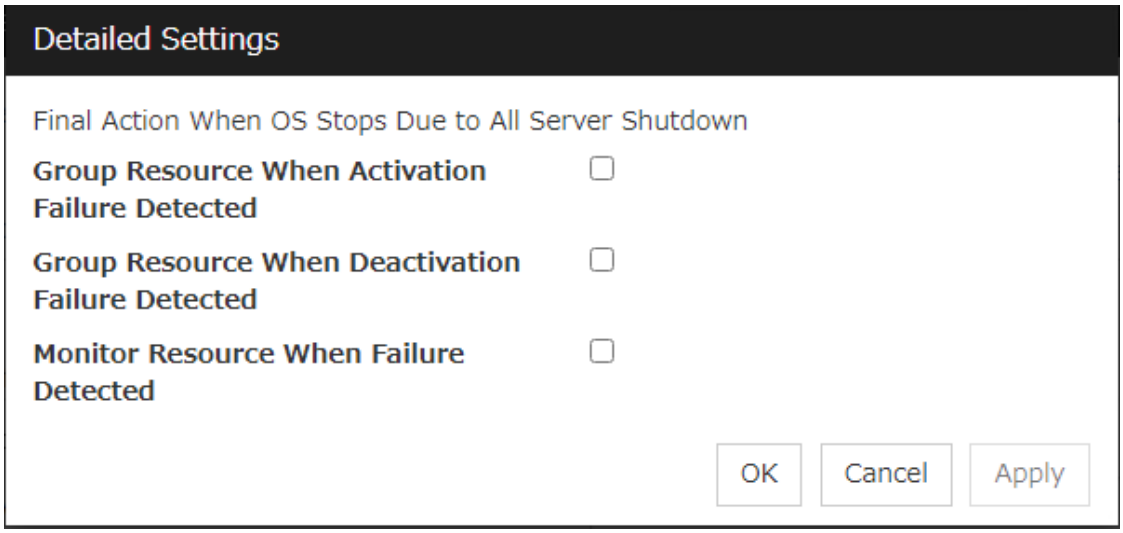
Note: If a stall occurs with "Nothing (handle a stall as an activation/deactivation failure)" specified, the effect on the group resources is undefined, so we do not recommend changing the setting to "Nothing (handle a stall as an activation/deactivation If you do specify "Nothing (handle a stall as 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 (times)
- Failover threshold: 0 (times)
- Final action: Intentionally causing a stop error

If **Stop the cluster service and shut down OS** or **Stop the cluster service and reboot OS** is specified as the final action, it takes a considerable amount of time for the cluster service to stop.

Disable the Final Action when OS Stops Due to Failure Detection

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



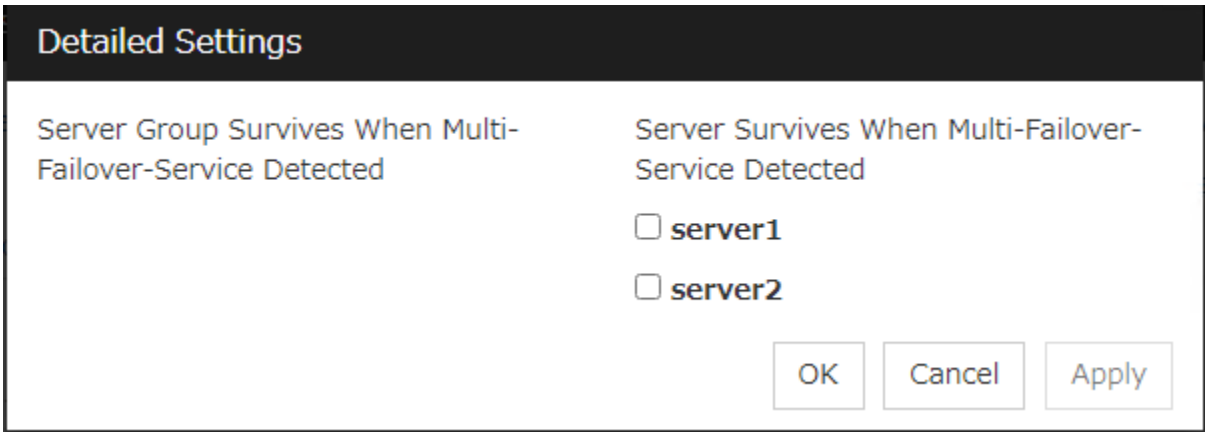
- Group Resource When Activation Failure Detected
  If the final action caused by an activation error detection in a group resource accompanies the OS stop, the final action is suppressed if all other servers are stopped.
- Group Resource When Deactivation Failure Detected
  If the final action caused 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.
  - Stop the cluster service and shutdown OS
  - Stop the cluster service and reboot OS
  - Generate an intentional stop error

Disable Shutdown When Multi-Failover-Service Detected

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



Server Group Survives When Multi-Failover-Service Detected

Select one server. 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.

Important: Suppose that shutdown is suppressed upon the detection of both-system activation in an environment in which the mirror disk resource is used for setting automatic mirror recovery. In this case, automatic mirror copying starts when the server which is shut down upon the detection of both-system activation is re-started through the OS. Care is needed since this discards one piece of data from among that updated separately on the mirror disk of each server at both-system activation.

You need to select a server for which the data is to be protected when suppressing shutdown caused by the detection of both-system activation in an environment in which the mirror disk resource is used.

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:

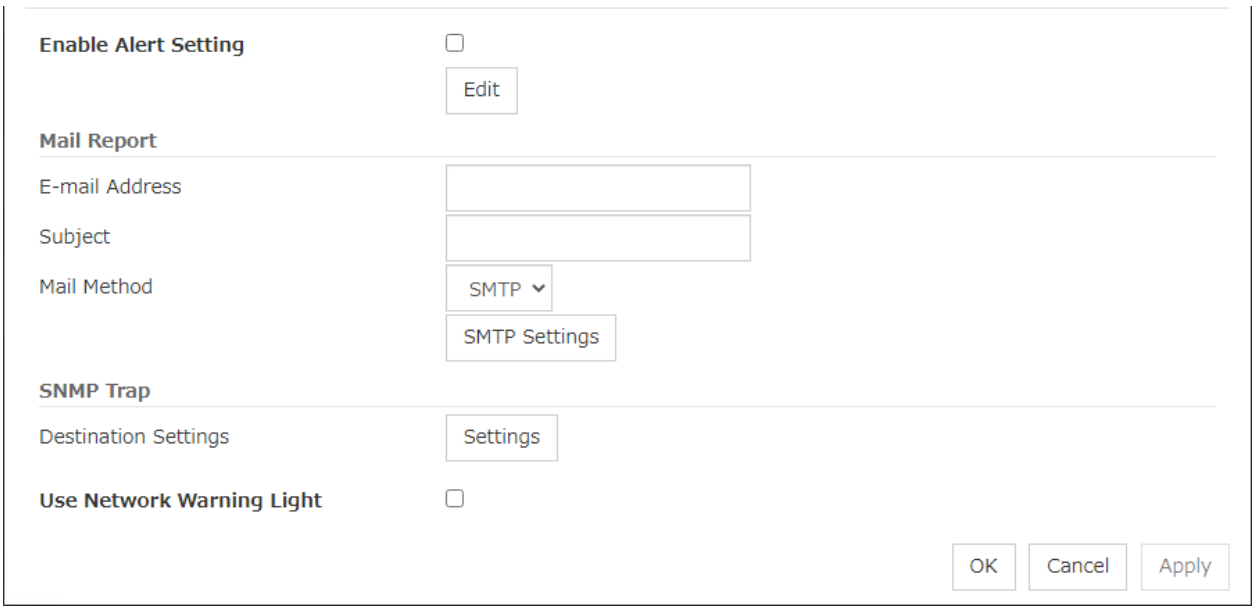
Type: Warning
Module name: rc
Event ID: 1104
Message: A mismatch in the group %1 status occurs between the servers.

To fix this problem, restart the group, execute a cluster reboot, restart all the servers on which the groups are not started, or restart the cluster services of all the servers on which the groups are not started.

2.2.7 Alert Service tab

Set up the alert service and network warning light.

Note: To use the mail alert function and network warning light, EXPRESSCLUSTER X Alert Service 5.2 for Windows is required.



Enable Alert Setting

Allows changing the alert destination from the default value. To change the destination, click **Edit**, then set a new destination in the **Change Alert Destination** dialog box.

If you clear the check box, the destination address you have modified returns to the default settings temporarily.

For the default settings for the destination address, see "*Messages reported by event log and alert*"in "*11. 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. In this version, SMTP is the only option in this.

To use SMTP as a mailing method, click **SMTP Settings**, then set the method in the **SMTP Settings** dialog box.

- SMTP
  Sends a mail by communicating directly with the SMTP server.

Destination Settings

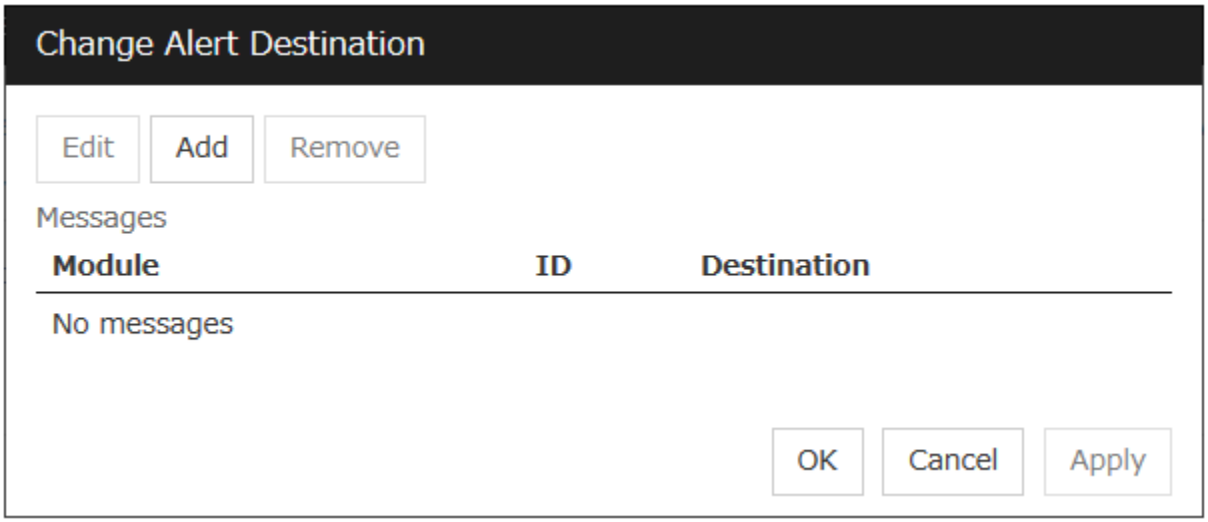
Configure the SNMP trap transmission function: Click **Settings**, then set an SNMP trap transmission destination in the **Destination Settings** dialog box.

Use Network Warning Light

Configure whether or not to use the warning light (dedicated product) controlled by network. The IP address of warning light is entered on the server property.

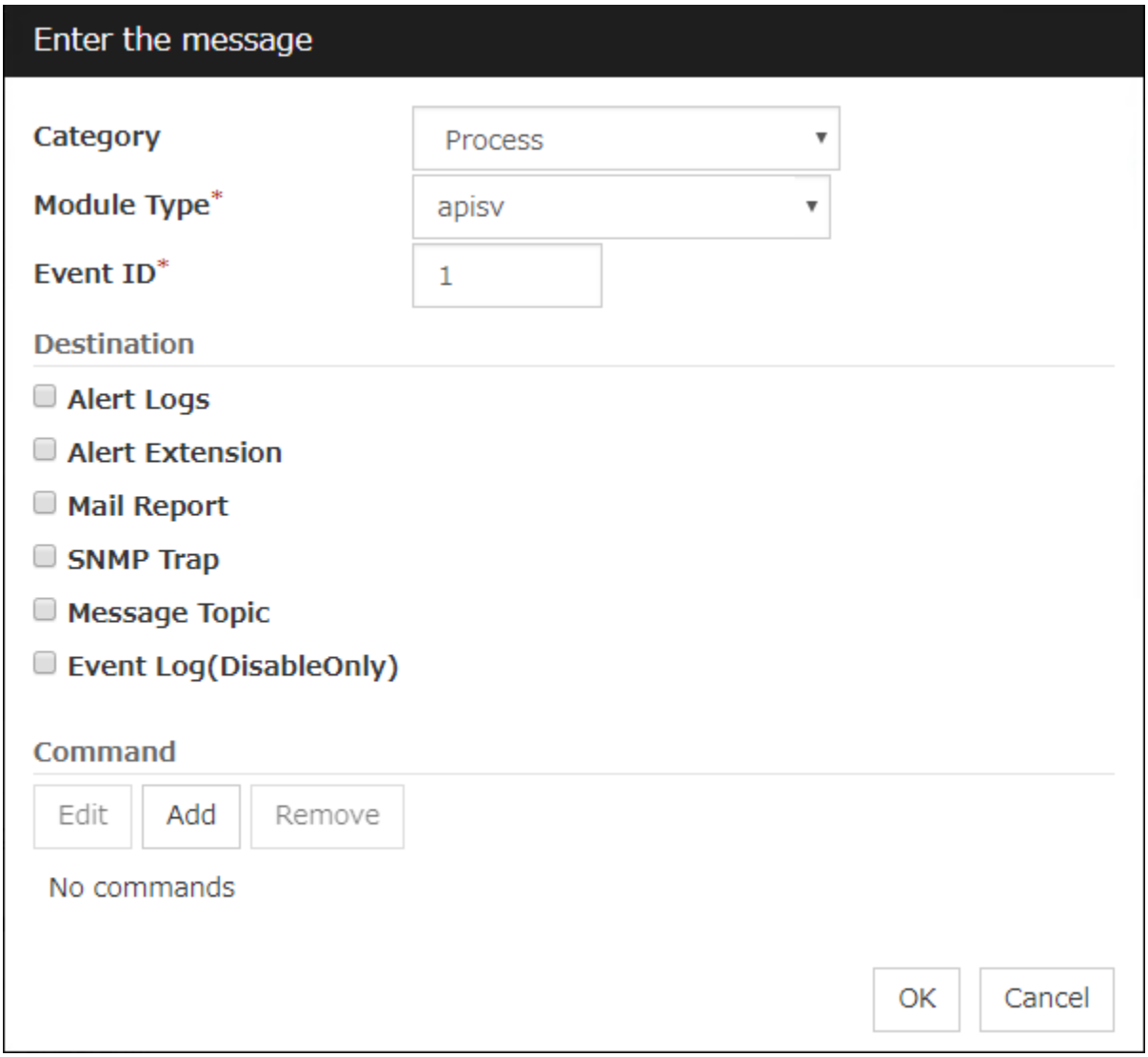
Change Alert Destination

Clicking **Edit** displays the **Change Alert Destination** dialog box.



Add

Add the alert ID of the destination which you want to customize. Clicking **Add** displays 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 message ID of the module type for which you want to change the destination. For information on the message IDs, see "*Messages reported by event log and alert*"in "11. *Error messages*" in this guide.

Destination

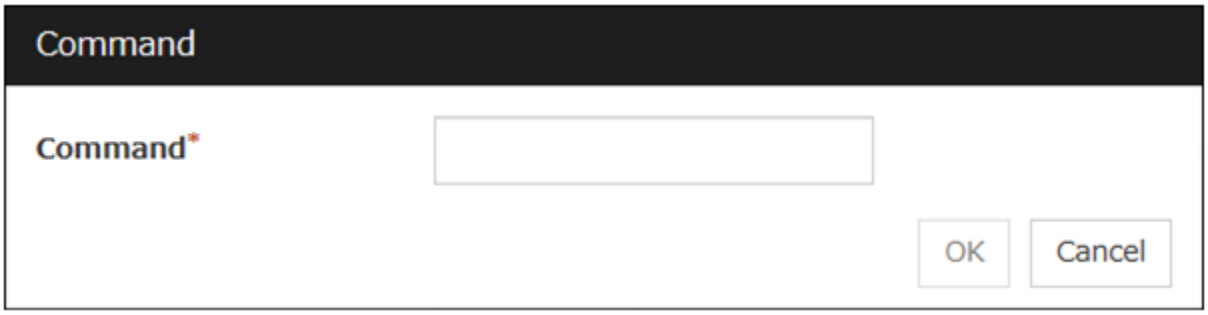
Select a message destination from the following options.

- Alert logs
  This sends messages to the alert logs.
- Alert Extension
  This executes the specified function by using the alert extension function. Modify the extension settings by using Add and/or Edit. (The command must be specified within four lines.)

- Mail Report
  Uses the mail report function.
- SNMP Trap
  Uses the SNMP trap transmission function to send messages.
- Message Topic
  This sends message to Amazon SNS.
- Event Log (Disable only)
  You can disable the settings whereby the OS reports logs to the event log by clearing this check box. (You cannot configure the settings to report messages that are not reported to event logs.)

Add

Add a command of the alert extension function. Click **Add** to display the **Enter Command** dialog box.



Command (Within 511 bytes)

Enter any command you want to use.

- Keyword
  If you specify %%MSG%%, the 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%%.
  If you set %%MSG%% as an argument for a command, you need to add backslash (\) and double quotation (") like below.
  <any command you want to use> \"%%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 used for the mail alert.

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

Clicking this displays the configured SMTP servers. No more than four SMTP servers can be configured with this version.

Add

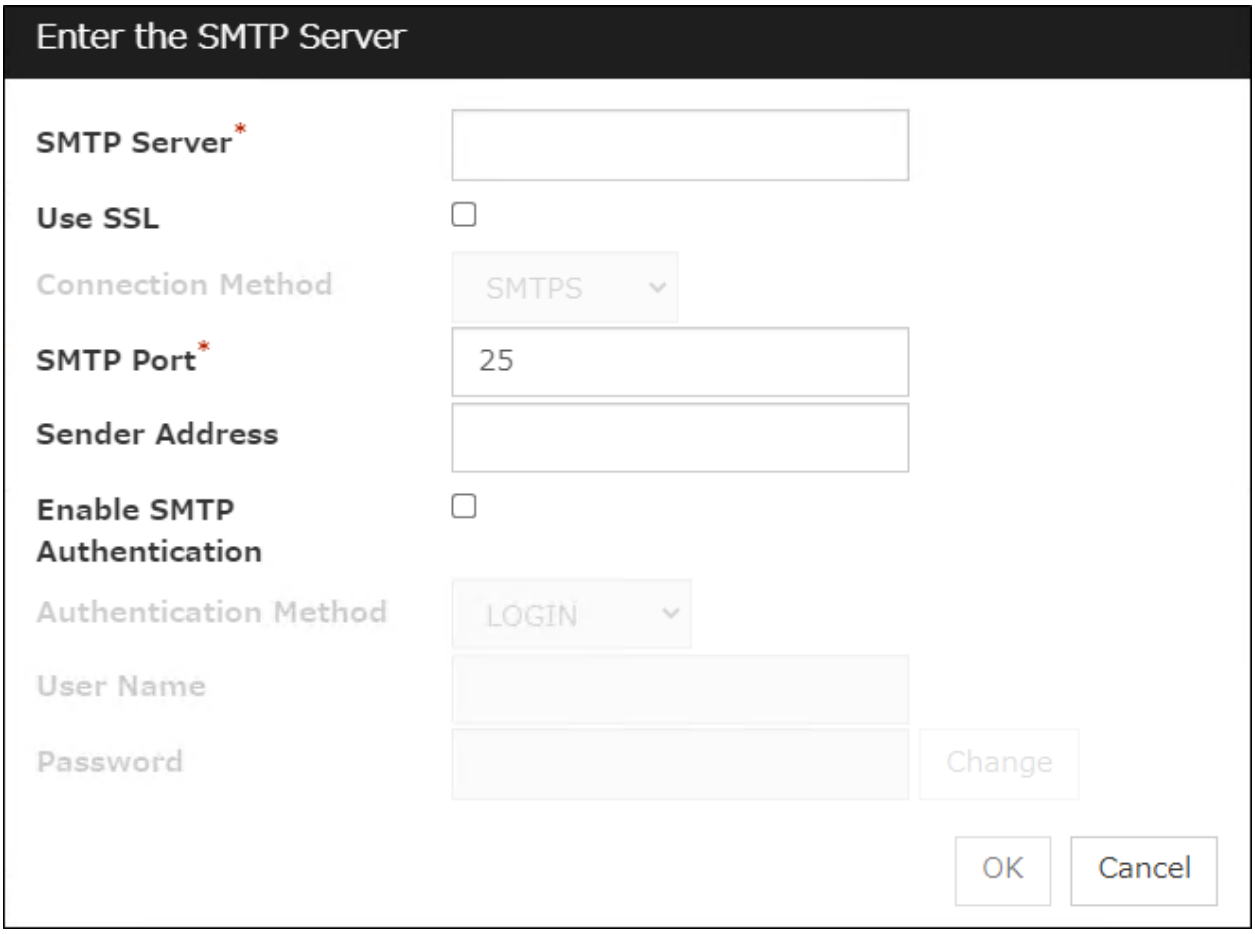
Use this button to add a SMTP server. Click **Add** to display the **Enter the SMTP Server** dialog box.

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.

Use SSL

If you use SSL for communication with the SMTP server, select the checkbox; otherwise uncheck it.

When using SSL, go to the **Encryption** tab, then set **SSL Library** and **Crypto Library**.

For OpenSSL versions supporting this, see "Getting Started Guide" -> "Installation requirements for EXPRESSCLUSTER" -> "System requirements for the EXPRESSCLUSTER Server" -> "Operation environment for enabling encryption".

Connection method

- SMTPS
  Use SMTPS for communication with the SMTP server.
- STARTTLS
  Use STARTTLS for communication with 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.

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.

SNMP Settings

Click this to display the **Destination Settings** dialog box which is used for the SNMP trap.

Destination

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

Add

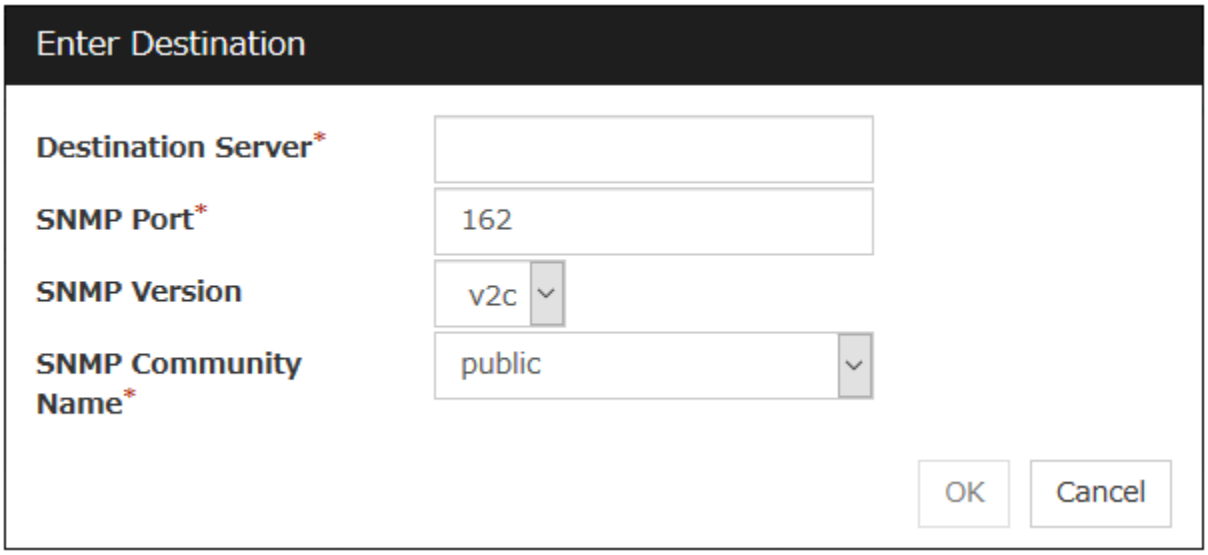
Adds an SNMP trap transmission destination. Click **Add** to display the **Change SNMP Destination** dialog box.

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

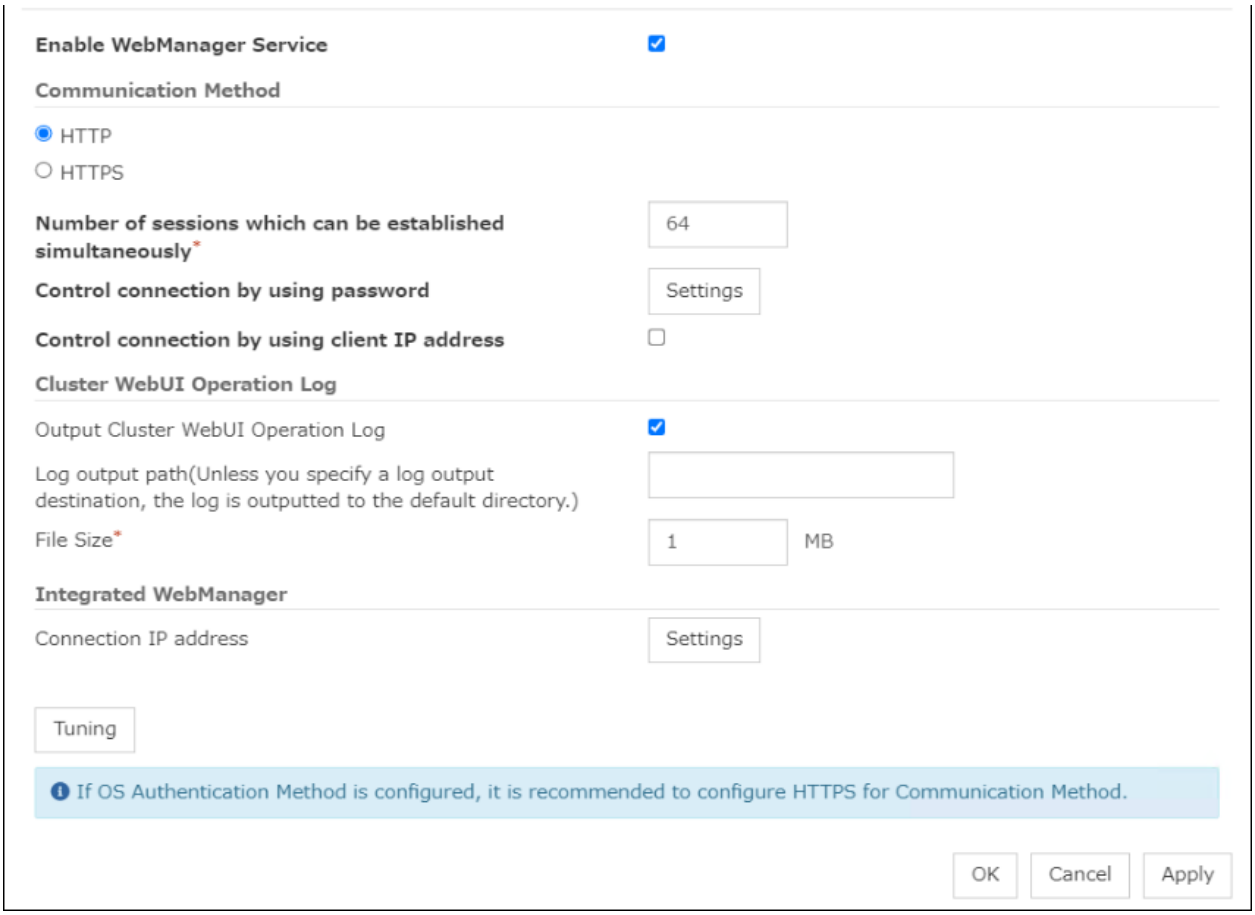
Configure the SNMP version of the SNMP trap transmission destination.

SNMP Community Name (Within 255 bytes)

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

2.2.8 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

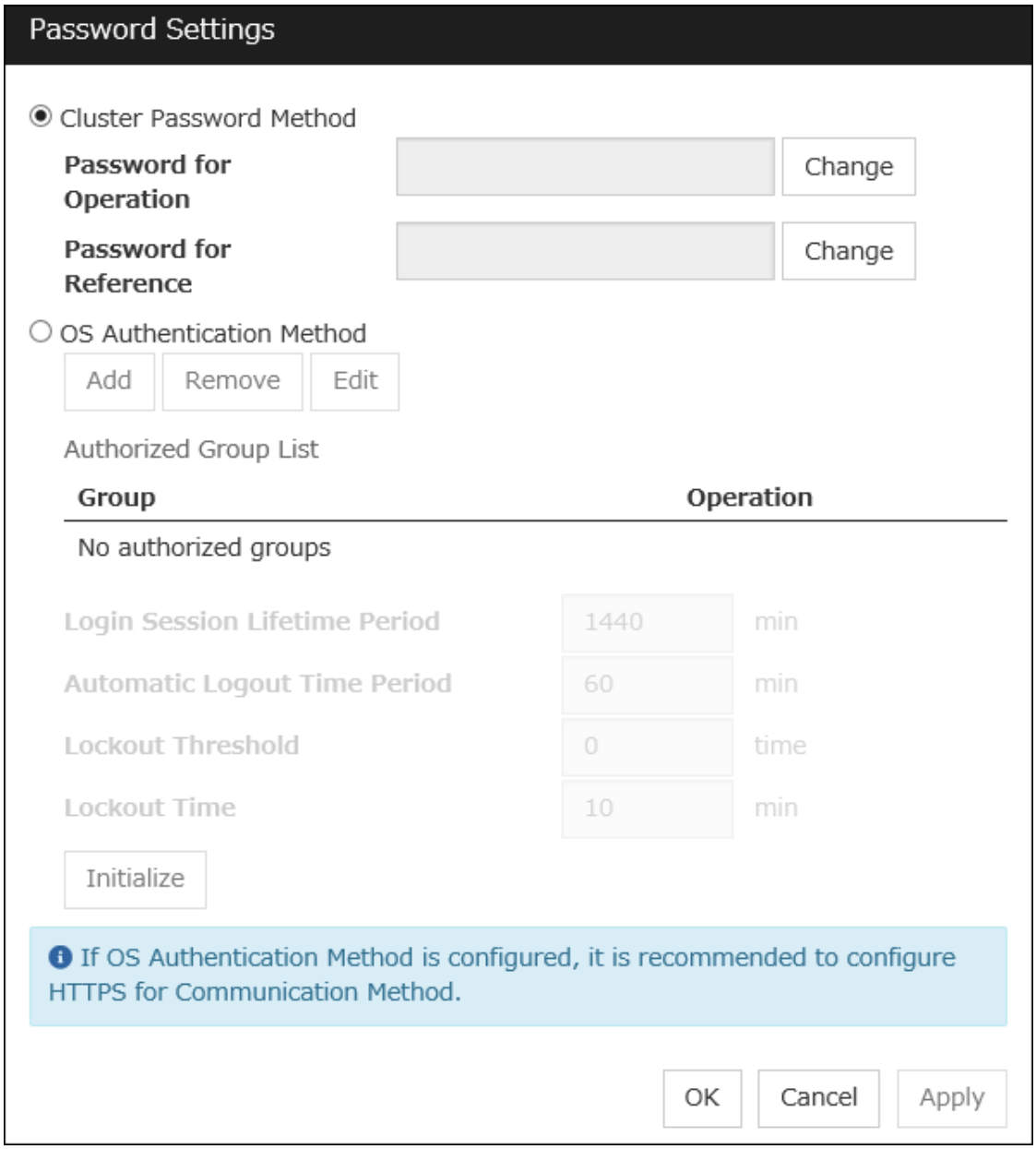
- HTTP
  No encryption is used for communicating with a client.
- HTTPS
  Encryption is used for communicating with a client.

Number of sessions which can be established simultaneously (10 to 999)

Set the number of requests that can be simultaneously received from clients. If more requests than the number set here are generated, the excess requests will be discarded.

Control connection by using password

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



Cluster Password Method / OS Authentication Method

Choose a login method for Cluster WebUI from below.

- Cluster Password Method
  Authenticates by **Password for Operation** or **Password for Reference** you set
- OS Authentication Method
  Perform authentication by 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 the operation mode, config mode, or verification 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 the 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).

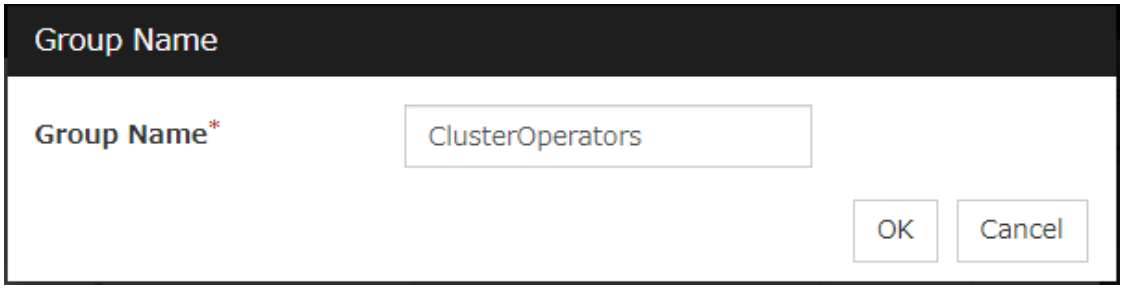
OS Authentication Method

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 control permission of a cluster is assigned per group,

- If a server belongs to a workgroup:
  Register the same user names and group names to all the servers connecting to Cluster WebUI.
- If a server belongs to a domain:
  Register users and groups to the domain.

Add

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



- Group name (Within 255 bytes)
  Enter a group name to which you want to give a 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 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 **Operation** does not change in this procedure.

Operation

Set **Operation** 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 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.

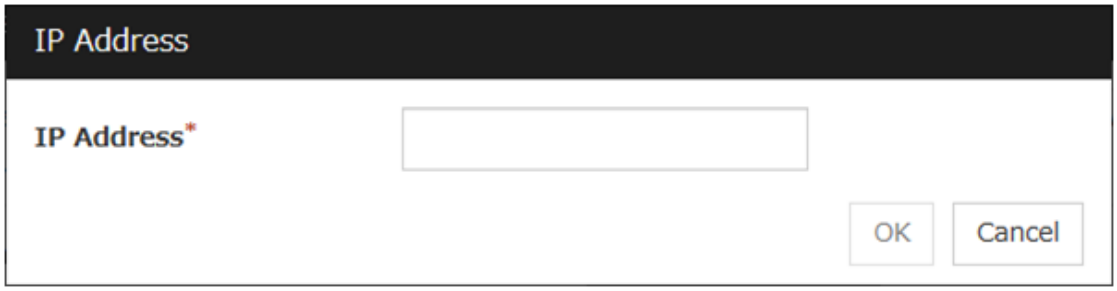
Control connection by using client IP address

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 to **Connection Permit Client IP Address List**. Click **Add to display the IP Address** dialog box is displayed. 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 you want to remove from **Connection Permit Client IP Address List** and then click **Remove**.

Edit

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

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.

Output Cluster WebUI Operation Log

Allows you to output the operation log of Cluster WebUI.

For details, see "Maintenance Guide" - "The system maintenance information" - "Function for outputting the operation log of Cluster WebUI".

- If the check box is checked:
  The operation log of Cluster WebUI is outputted.
- If the check box is not checked:
  The operation log of Cluster WebUI is not outputted.

Log output path (Within 255 bytes)

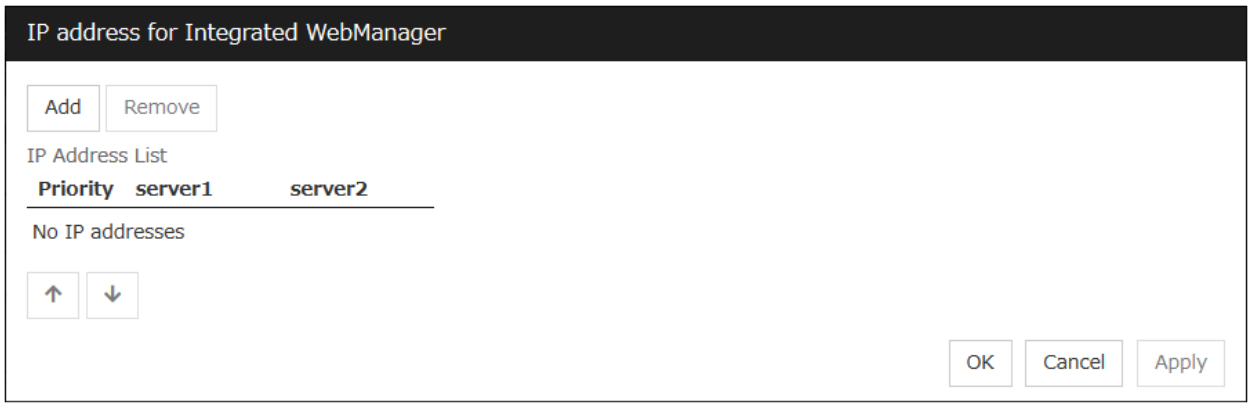
Specify the output destination directory of the Cluster WebUI operation log with an absolute path consisting of ASCII characters.
If no directory is specified, the Cluster WebUI operation log is outputted to <installation path>\log.

File Size (1 to 10)

Specify the size of Cluster WebUI operation log.
When the log data reaches the specified size, a rotation occurs. Up to five generations of the data are saved.

IP address for Integrated WebManager

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



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

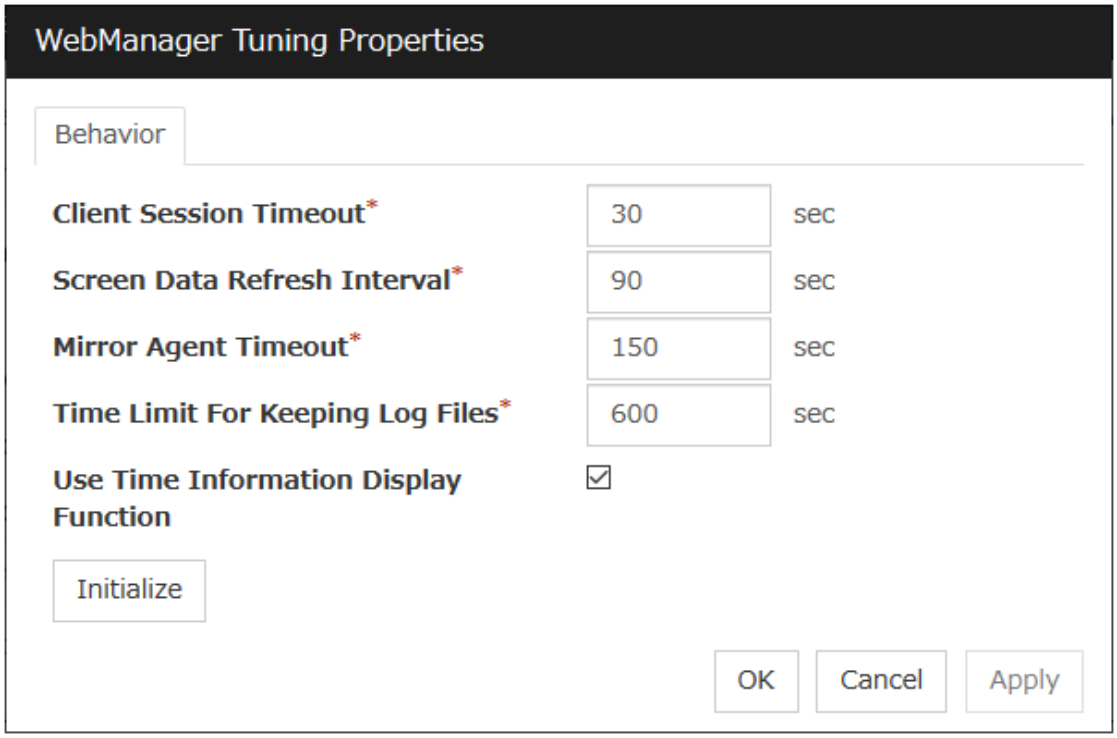
Remove the communication path. Select the communication path to be removed and click **Remove**, then the selected path is removed.

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 Properties

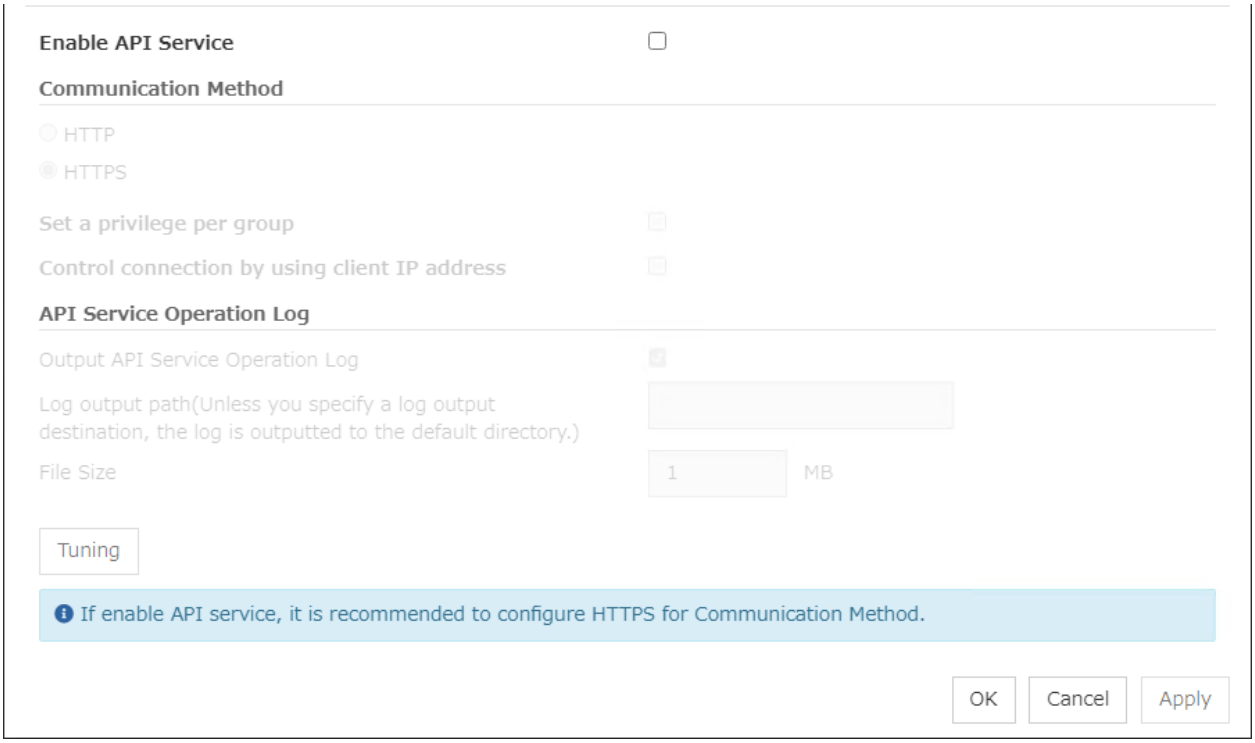
Use **Tuning** to tune the WebManager Server. Clicking **Tuning** displays the **WebManager Tuning Properties** dialog box.



- 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)
  Specify the mirror agent time-out. A time-out is determined if the time specified here elapses till the mirror disk information is acquired.
- Time Limit For Keeping Log Files (60 to 43200)
  Time limit determines when the log collection information temporarily saved on the server will be deleted. When the time specified here has elapsed, the log collection information will be deleted unless you save the file when the dialog box asking you if you save the log collection information is displayed.
- Use Time Info
  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 items to their default values.

2.2.9 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 a privilege of operating clusters per group

Allows you to set and control a privilege of operating clusters per group.

- If the check box is checked:
  Add, **Remove**, and **Edit** are displayed.
- If the check box is not checked:
  Add, **Remove**, or **Edit** is not displayed.

Login users must be registered beforehand in the server which issues the request. 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.

- If the server belongs to a work group:
  Register the same user name and group name in each of the servers which issues the request.
- If the server belongs to a domain:
  Register users and groups in the domain.

Add

Allows you to add a group to **Authorized Group List**. Clicking **Add** displays the **Group Name** dialog box. Any group added here has the **Operation** box checked.

- Group name (up to 255 bytes)
  Enter the name of a group. Users belonging to the group are to be given the permission.
  The group must be registered to a server in advance.

Remove

Use this option to delete a group from **Authorized Group List**.
From **Authorized Group List**, select a group to be deleted. Then, click **Remove**.

Edit

Use this option to edit a group. From **Authorized Group List**, select a group to be edited. Then click **Edit**. The **Group Name** dialog box appears with the selected group entered. Editing the group here does not change its operation right.

Operation

Set operation rights for any of the groups registered in **Authorized Group List**.

- If the check box is checked:
  The users of the group can operate the cluster and obtain its status.
- If the check box is not checked:
  The users of the group can only obtain the status of the cluster.

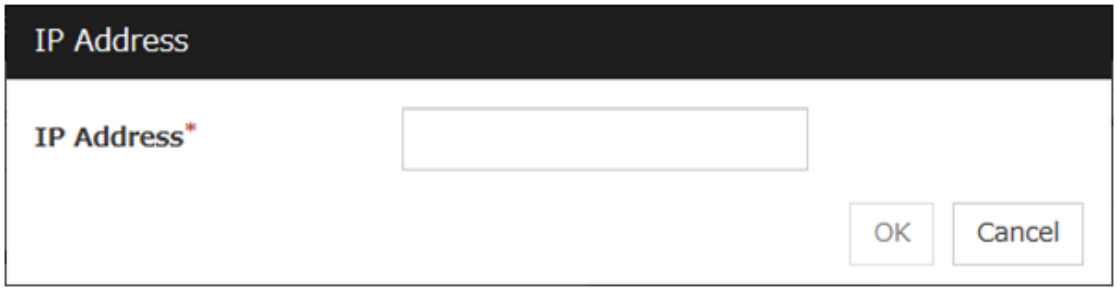
Control connection by using client IP address

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.

Operation

Set operation rights for any of the IP addresses 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.

Output API Service Operation Log

Allows you to output the operation log of API services.

For details, see "Maintenance Guide" - "The system maintenance information" - "Function for outputting an API service operation log file".

- If the check box is checked:
  The operation log of API services is outputted.
- If the check box is not checked:
  The operation log of API services is not outputted.

Log output path (Within 255 bytes)

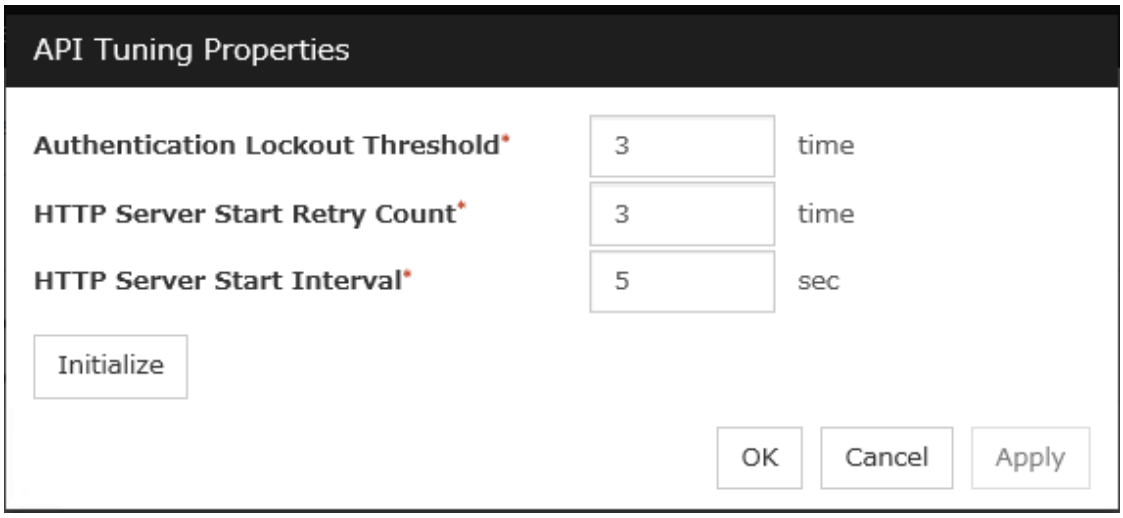
Specify the output destination directory of the API service operation log with an absolute path consisting of ASCII characters.
If no directory is specified, the API service operation log is outputted to <installation path>\log.

File Size (1 to 10)

Specify the size of API service operation log.
When the log data reaches the specified size, a rotation occurs. Up to five generations of the data are saved.

Tuning

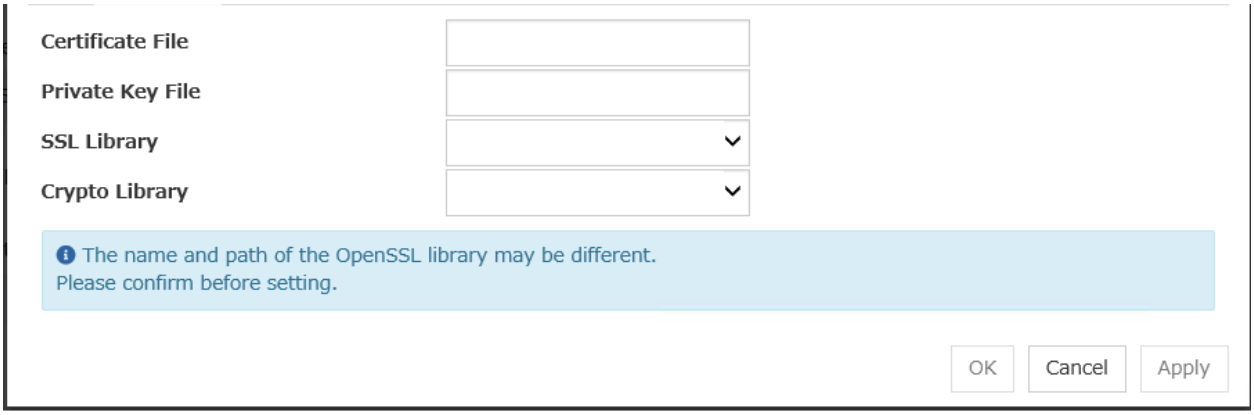
Adjusts API services. Click **Tuning** to display **API Tuning Properties** dialog box .



- 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 fail 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 by clicking **Initialize**.

2.2.10 Encryption tab

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



Certificate File

Sets the server credential file used for connecting to a client. Users need to prepare the server credential file.

Private Key File

Sets the private key file used for connecting to a client. Users need to prepare the private key file.

SSL Library

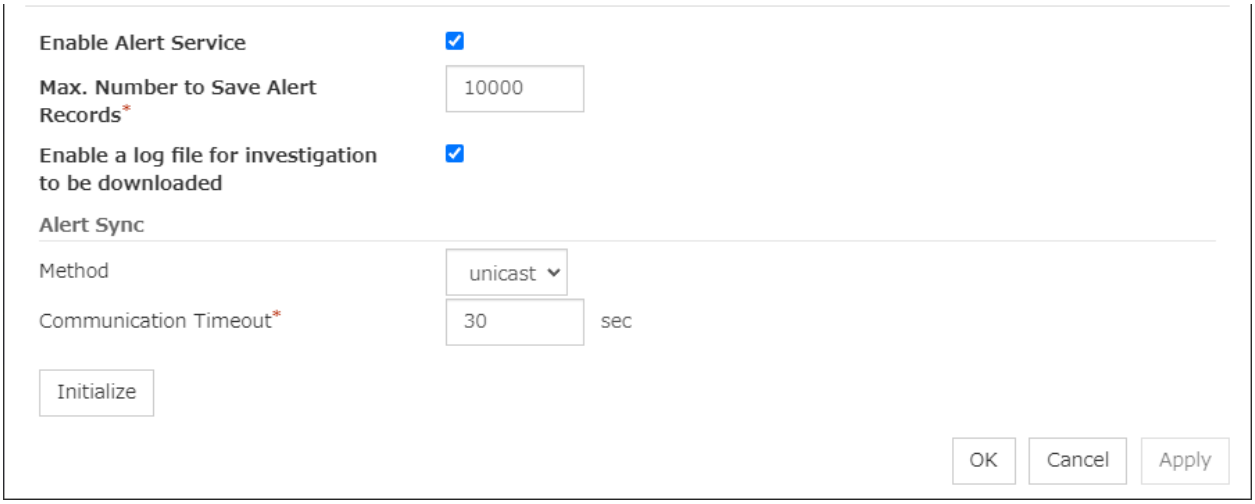
Sets the SSL library file used for encryption and selects the SSL library file included in OpenSSL. Users need to change it based on the environment, such as an installation folder.

Crypto Library

Sets the Crypto library file used for encryption and selects the Crypto library file included in OpenSSL. Users need to change it based on the environment, such as an installation folder.

2.2.11 Alert Log tab

Configure the settings for the alert log.



Enable Alert Service

Select this to start EXPRESSCLUSTER Web Alert service for the server.

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

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

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

Enable a log file for investigation to be downloaded

Enable or disable downloading a log file for investigation through Cluster WebUI in response to the occurrence of a failure. For more information on the log file, see " Function for obtaining a log file for investigation" in " The system maintenance information" in the " Maintenance Guide".

- When the check box is selected:
  The log file is downloadable through Cluster WebUI.
- When the check box is not selected:
  The log file is not downloadable through Cluster WebUI.

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)

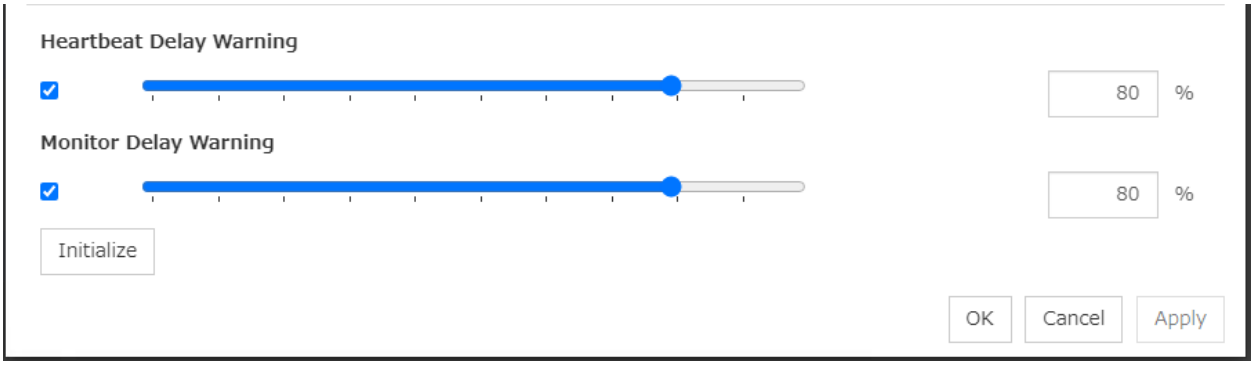
Specify a communication time-out. A communication time-out is determined if the time specified here elapses after the last communication between EXPRESSCLUSTER Web Alert service and servers.

Initialize

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

2.2.12 Delay Warning tab

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



Heartbeat Delay Warning (1 to 99)

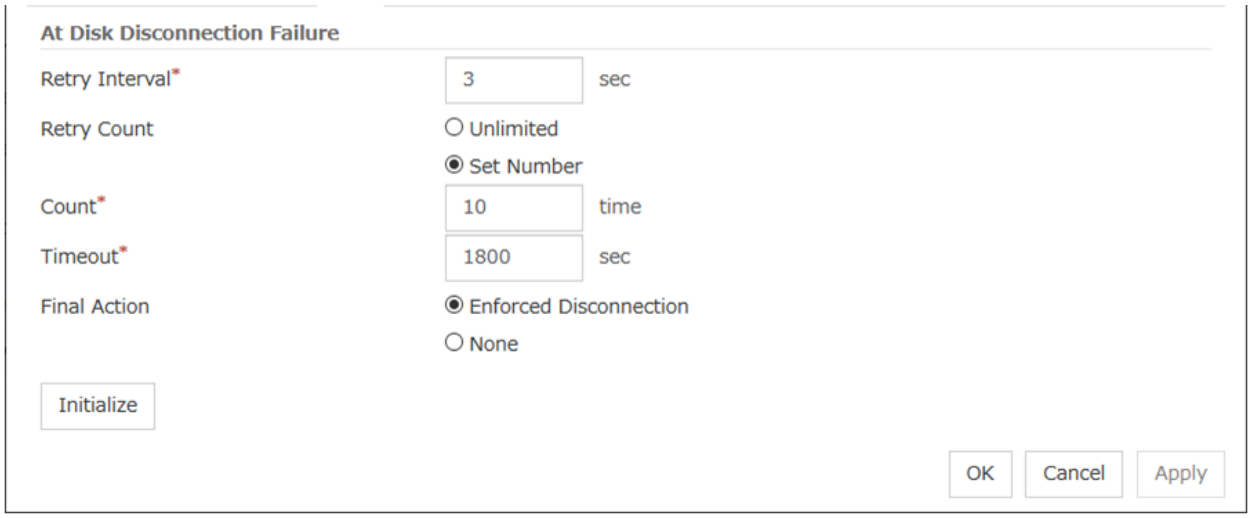
Set a percentage of heartbeat time-out at which the heartbeat delay warning is issued. If the time for the percentage passes without any heartbeat response, the warning will be produced in an alert log.

Monitor Delay Warning (1 to 99)

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.

2.2.13 Disk tab

Configure the setting for a shared disk.



At Disk Disconnection Failure: Retry Interval (1 to 10)

Set the interval time required to retry disconnecting, when disconnecting a shared disk has failed.

At Disk Disconnection Failure: Retry Count (0 to 180)

Set the count to retry disconnecting when disconnecting a shared disk has failed.

- Unlimited
  Select this to retry disconnecting a disk infinitely.
- Set Number
  Select this to specify the count to retry to disconnect a disk.

At Disk Disconnection Failure: Timeout (1 to 9999)

Set the timeout at which to disconnect a shared disk.

At Disk Disconnection Failure: Final Action

If the count to disconnect a shared disk again is specified, set the action that will be taken in the case that disconnecting is failed for the specified count.

- Enforced Disconnection
  Select this to disconnect a disk forcibly.
- None
  Select this not to disconnect a disk forcibly.

Initialize

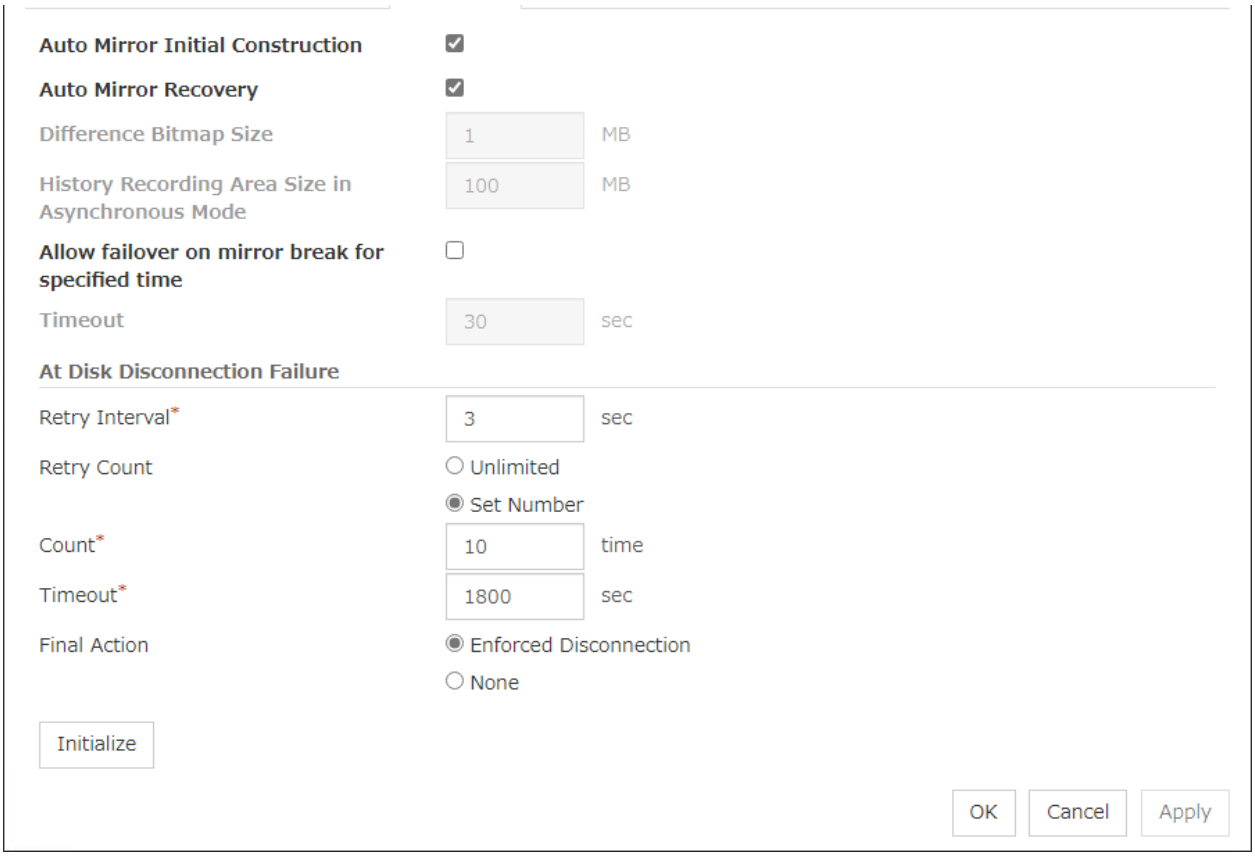
This operation is used to return the value to the default value. Click **Initialize** to set all items to their default values.

Note:

If the disk fails to be disconnected, retry or the final action is performed as many times as the value set above for each disk resource deactivation.
However, an emergency shutdown occurs if a single deactivation takes 9999 or more seconds.
To change the retry count and retry interval, set the values in consideration of the above event.

2.2.14 Mirror Disk tab

Configure the setting for a mirror disk.



Auto Mirror Initial Construction

Specify whether to perform the mirror initial construction automatically when the newly created mirror disk resource is activated for the first time.

- When selected
  Mirror initial construction is performed automatically.
- When cleared
  Auto mirror initial construction is not performed

Auto Mirror Recovery

An automatic mirror recovery is performed when any difference occurs in the data of mirror disks between both servers. There is a case that mirror recovery cannot be performed automatically even if it is selected. For details, see "*Automatically recovering from mirroring*" in "*Recovering from mirror breaks*"in "*10. Troubleshooting*" in this guide.

- When selected
  Mirror recovery is performed automatically.
- When cleared
  Mirror recovery is not performed automatically.

Difference Bitmap Size (1 to 5)

Users can set the size of an area in which the data differential information between servers is recorded, when a mirror break occurs. If the data partition is 4TB or more, data transfer for mirror recovery is optimized by enlarging the size.

This item needs to be set before establishing a mirror disk resource and a hybrid disk resource. If the mirror disk resource and the hybrid disk resource already exist in the cluster, the setting cannot be changed.

History Recording Area Size in Asynchronous Mode (1 to 100)

Users can set the size of an area in which the history of unsent data is recorded. In the asynchronous mode, a mirror break occurs if a certain amount of unsent data is stored. Larger size makes it harder for the mirror break to occur.

This item needs to be set before establishing a mirror disk resource and a hybrid disk resource. If the mirror disk resource and the hybrid disk resource already exist in the cluster, the setting cannot be changed.

Allow failover on mirror break for specified time

Allow a failover to a server, with data in the mirror disk not up to date, to succeed for a specified time since the occurrence of a mirror break.

- When selected
  Allow a failover for a specified time since the occurrence of a mirror break.
- When cleared
  Disallow a failover when a mirror break occurred.

Important: For a successful failover to a server with data in the mirror disk not up to date, the data may be rolled back even in synchronization mode.

Note:

In an environment where this option is selected, automatic mirror recovery after a mirror break is temporarily suppressed regardless of the settings for automatic mirror recovery.

This suppression persists, until the failover succeeds or the specified time elapses.

However, automatic mirror recovery may be resumed before the timeout specified for this function, if the suppression is preferentially removed by another function.

This may cause a failover to fail.

Note:

If you select this option, disable the following failover attribute settings:

- Fail over dynamically
- Failover Attribute (Advanced)

For more information, see this guide: "3. *Group resource details*" -> "*Group properties*" -> "*Attribute tab*".

Note:

If you use this feature for a hybrid disk resource, make sure that the times of servers constituting a server group synchronize with each other.
Without this synchronization, the behavior may not be as you expected.

Timeout (1 to 600)

Specify a time (since the occurrence of a mirror break) for which a failover is allowed.
It is recommended to set the value equal to or higher than that for the heartbeat timeout. For more information, see this guide: "2. *Parameter details*" -> "*Cluster properties*" -> "*Timeout tab*".
Setting the value lower than that for the heartbeat timeout may cause a failover to fail.

At Disk Disconnection Failure: Retry Interval (1 to 10)

Set the interval time required to retry disconnecting, when disconnecting a mirror disk has failed.

At Disk Disconnection Failure: Retry Count (0 to 180)

Set the count to retry disconnecting when disconnecting a mirror disk has failed.

- Unlimited
  Select this to retry disconnecting a disk infinitely.
- Set Number
  Select this to specify the count to retry to disconnect a disk.

At Disk Disconnection Failure: Timeout (1 to 9999)

Set the timeout at which to disconnect a mirror disk.

At Disk Disconnection Failure: Final Action

If a retry count is set for mirror disk disconnection, set the action when that will be taken in the case that disconnection still fails after the specified retry count exceeds.

- Enforced Disconnection
  Select this to disconnect a disk forcibly
- None
  Select this not to disconnect a disk forcibly.

Initialize

This operation is used to return the value to the default value. Click **Initialize** to set all items to their default values.

Note:

If the disk fails to be disconnected, retry or the final action is performed as many times as the value set above for each mirror disk resource deactivation.
However, an emergency shutdown occurs if a single deactivation takes 9999 or more seconds.
To change the retry count and retry interval, set the values in consideration of the above event.

2.2.15 Account tab

The **Account** tab is used to register and/or delete a user account that is used in a force-stop script. You can set up to sixteen user accounts for one cluster system. Do not set seventeen or more accounts. Accounts that have already been set on all the cluster servers are the target to be registered. **Account** lists currently registered user accounts.

Add

Use **Add** to add a user account on the Account List. Click **Add** to display the **Enter account** dialog box.

- User Name
  Enter a user account name to be registered. When specifying an account of a domain, enter, for example, "*Domain Name\Account Name*".
- Password
  Enter a password of the user account to be registered.
- Remove
  Use **Remove** to remove a user account from the Account List. Select the user account you want to remove from **Account** and then click **Remove**.

Edit

Use **Edit** to edit a user account. Select the user account you want to edit from **Account** and then click **Edit**. The **Enter account** dialog box where the selected account was entered is displayed.

2.2.16 JVM monitor tab

Configure detailed parameters for the JVM monitor.

Note: To display the **JVM monitor** tab in 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:C:\Program Files\Java\jdk1.8.0_102

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 for **Maximum Java Heap Size**. This setting becomes common for all the servers in the cluster.

Specification example: -XX:+UseSerialGC

Log Output Setting

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

Resource Measurement Setting

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

Connection Setting

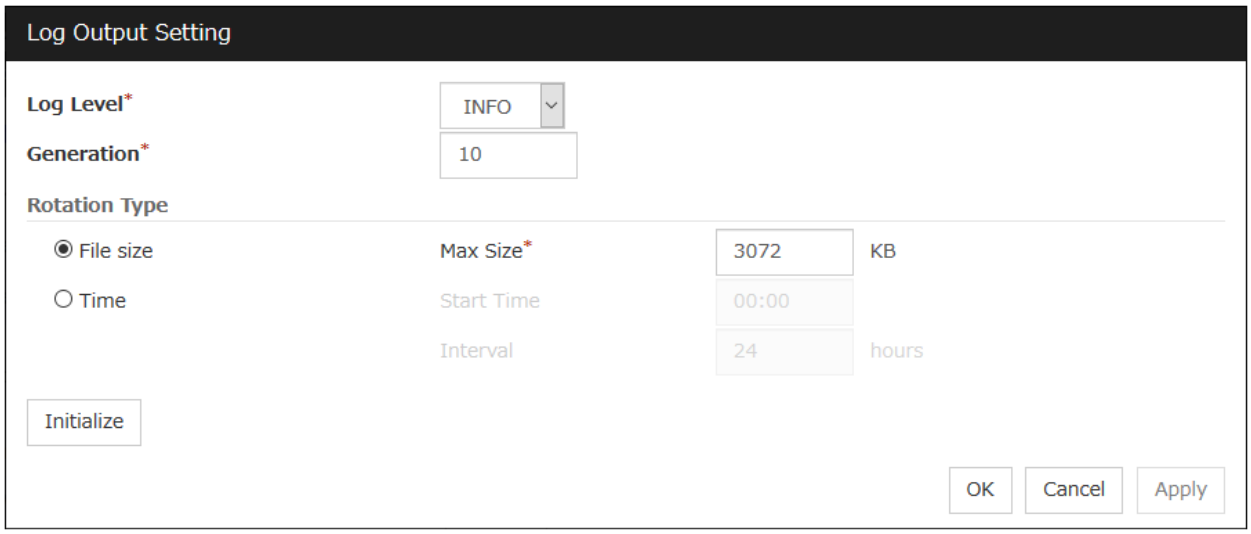
Click the **Settings** button to open the **Connection Setting** dialog box.

Action Timeout (30 to 300)

Set a timeout value for the [Command] that has been specified on each window of the JVM monitor. This setting becomes common for all of the [Commands].

Log Output Setting

Clicking **Settings** 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 the 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

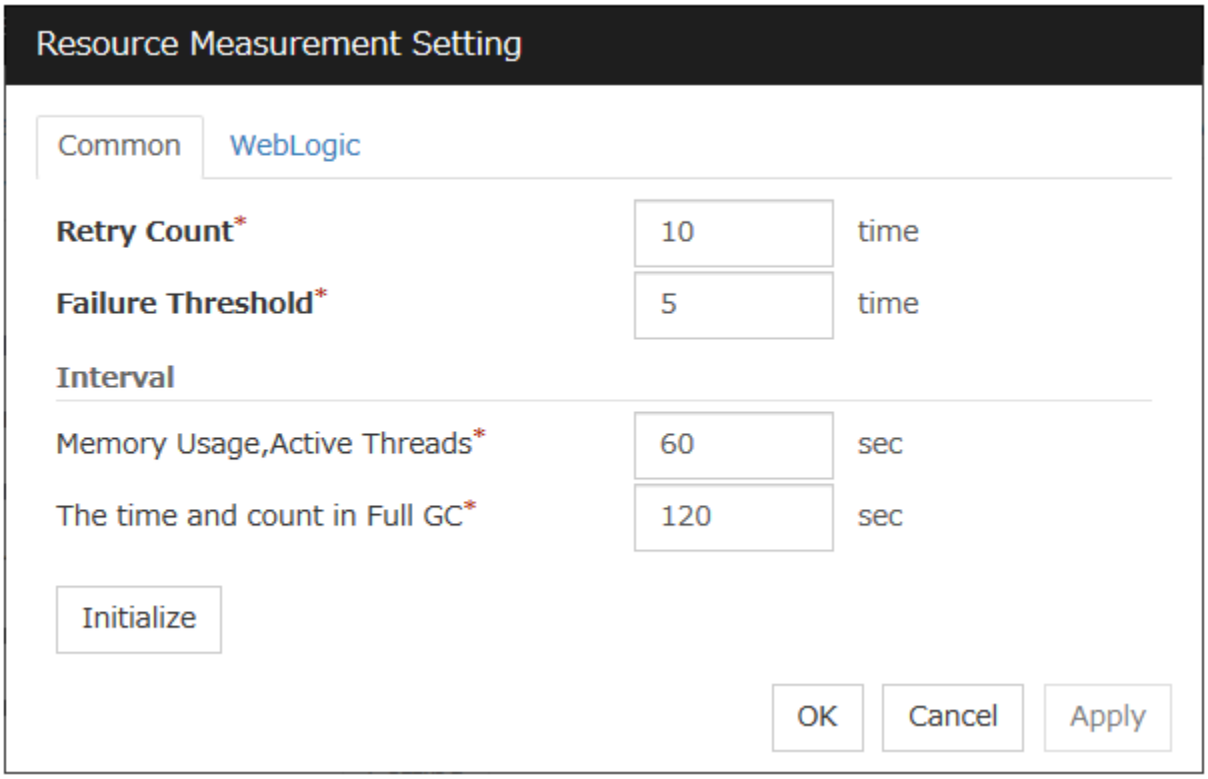
Select a rotation type for the log output by the JVM monitor. If you select **File Capacity** as the rotation type, set the maximum size (200 to 2097151), in kilobytes, for each log file such as the JVM operation log. If you select **Period** as the rotation type, set the log rotation start time in "hh:mm" 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 **Settings** displays the **Resource Measurement Setting** dialog box. For details on the scheme for error judgment by the JVM monitor, see "4. *Monitor resource details*".



Retry Count (1 to 1440)

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 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)

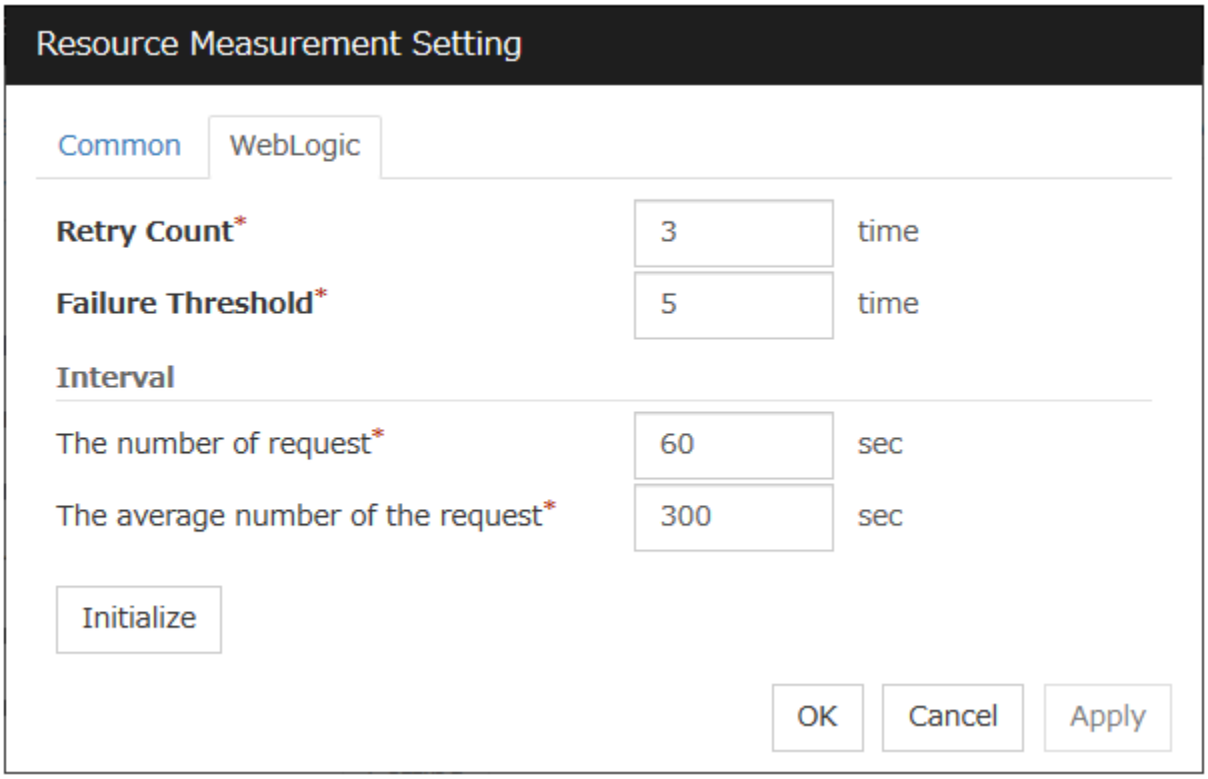
Set the interval at which the JVM monitor measures the time and count in Full GC execution.

Initialize

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

Resource Measurement Setting [WebLogic]

Clicking **Settings** displays the **Resource Measurement Setting** dialog box. For details on the scheme for error judgment by the JVM monitor, see "4. *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 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)

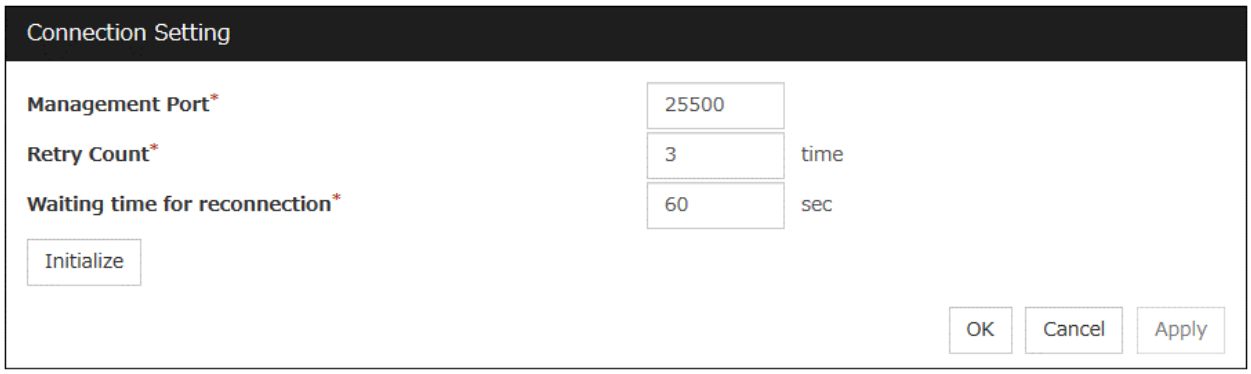
Set the interval at which the JVM monitor measures the average number of work manager or thread pool requests during WebLogic monitor. Set a value that is an integer multiple of the value set in **Interval: The number of request**.

Initialize

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

Connection Setting

Clicking **Settings** displays the **Connection Setting** 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 42424 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)

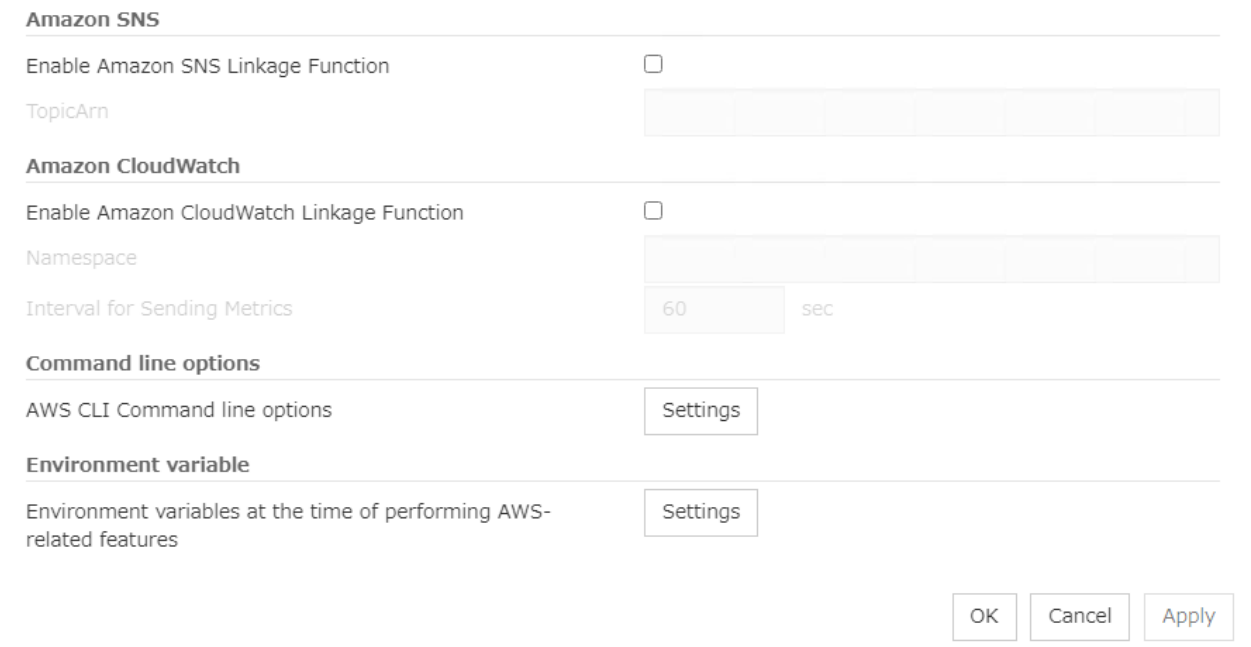
Set the interval at which the JVM monitor retries connection if it fails in Java VM connection.

Initialize

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

2.2.17 Cloud tab

Configure functions for cloud environments.



Enable Amazon SNS linkage function

Enable or disable the Amazon SNS linkage function.

- If the check box is checked:
  The Amazon SNS linkage function is enabled.
  Amazon SNS is used as a destination of EXPRESSCLUSTER messages.
  By default, the messages are sent as shown in "11. *Error messages*": the "o"-marked lines of the [8] column in the table of "11.3. *Messages reported by event log and alert*".
  To send other messages:
  Go to **Cluster Properties** -> the **Alert Service** tab -> **Change Alert Destination** -> **Destination**, and then select **Message Topic**.
- If the check box is not checked:
  The Amazon SNS linkage function is disabled.

TopicArn

Set TopicArn for the Amazon SNS linkage function.

Enable Amazon CloudWatch linkage function

Enable or disable the Amazon CloudWatch linkage function.

- If the check box is checked:
  The Amazon CloudWatch linkage function is enabled.
  Amazon CloudWatch is informed of the monitoring process time taken by the monitor resource.
- If the check box is not checked:
  The Amazon CloudWatch linkage function is disabled.

Note: Using the Amazon CloudWatch linkage function requires turning on **Enable Amazon CloudWatch linkage function**, and enabling **Send polling time metrics** of the **Monitor (common)** tab for the target monitor resource.

Namespace

Set Namespace for the Amazon CloudWatch linkage function.

Interval for Sending Metrics

Set the frequency of informing Amazon CloudWatch of the monitoring process time taken by the monitor resource.

AWS CLI command line options

Clicking **Settings** displays a text box for each AWS service.
For each AWS service, set AWS CLI command line options to be applied.

Environment variables at the time of performing AWS-related features

Clicking **Settings** displays a dialog box listing environment variables.

Environment variable List

Clicking **Edit** displays a dialog box to edit the selected environment variable.
Clicking **Add** displays a dialog box to add a new environment variable.
Clicking **Remove** deletes the selected environment variable.

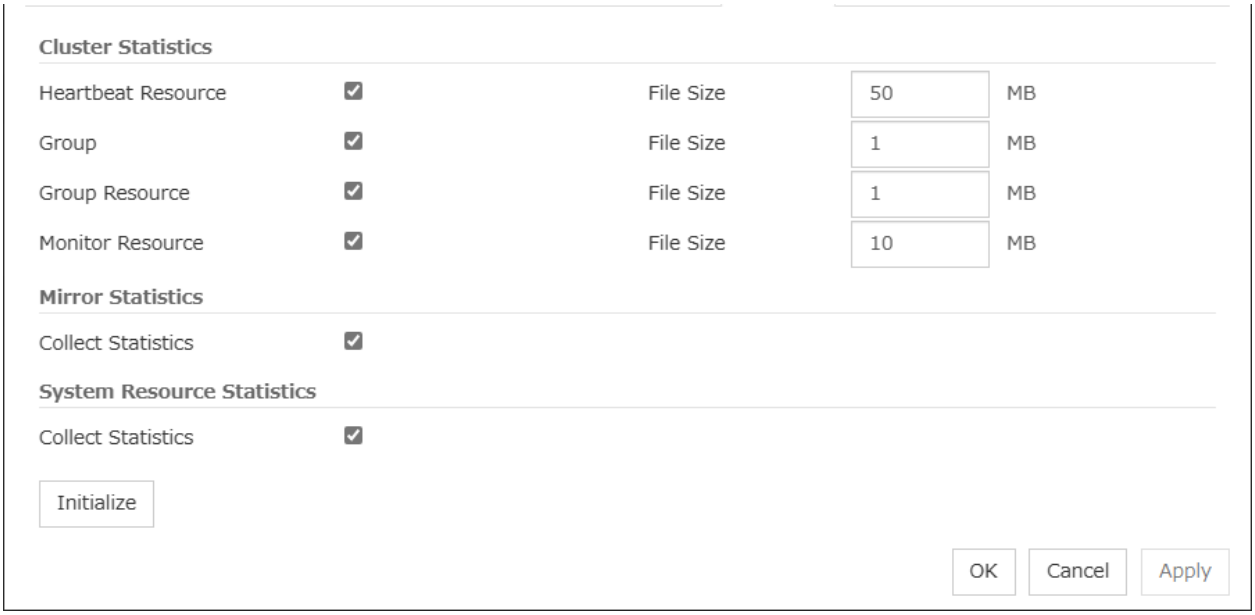
Enter environment variable

Enter the name and value of an environment variable.

- Name (within 259 bytes)
  Specify the name of an environment variable.
- Value (within 2047 bytes)
  Specify the value of the environment variable.

2.2.18 Statistics tab

Configure the settings for statistics.



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 details, 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 (whose setting range depends on the type)
    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 not selected:
  The cluster statistical information is not collected.

Note:

In **Cluster Statistics**, **File Size** can be specified as follows:

- Heartbeat resource: 1 to 50 (MB)
- Group: 1 to 5 (MB)
- Group resource: 1 to 5 (MB)

- Monitor resource: 1 to 10 (MB)

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.

System Resource Statistics

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.

For details, see " System resource statistics information collection function" and " Process resource statistics information collection function" in " The system maintenance information" in the " Maintenance Guide".

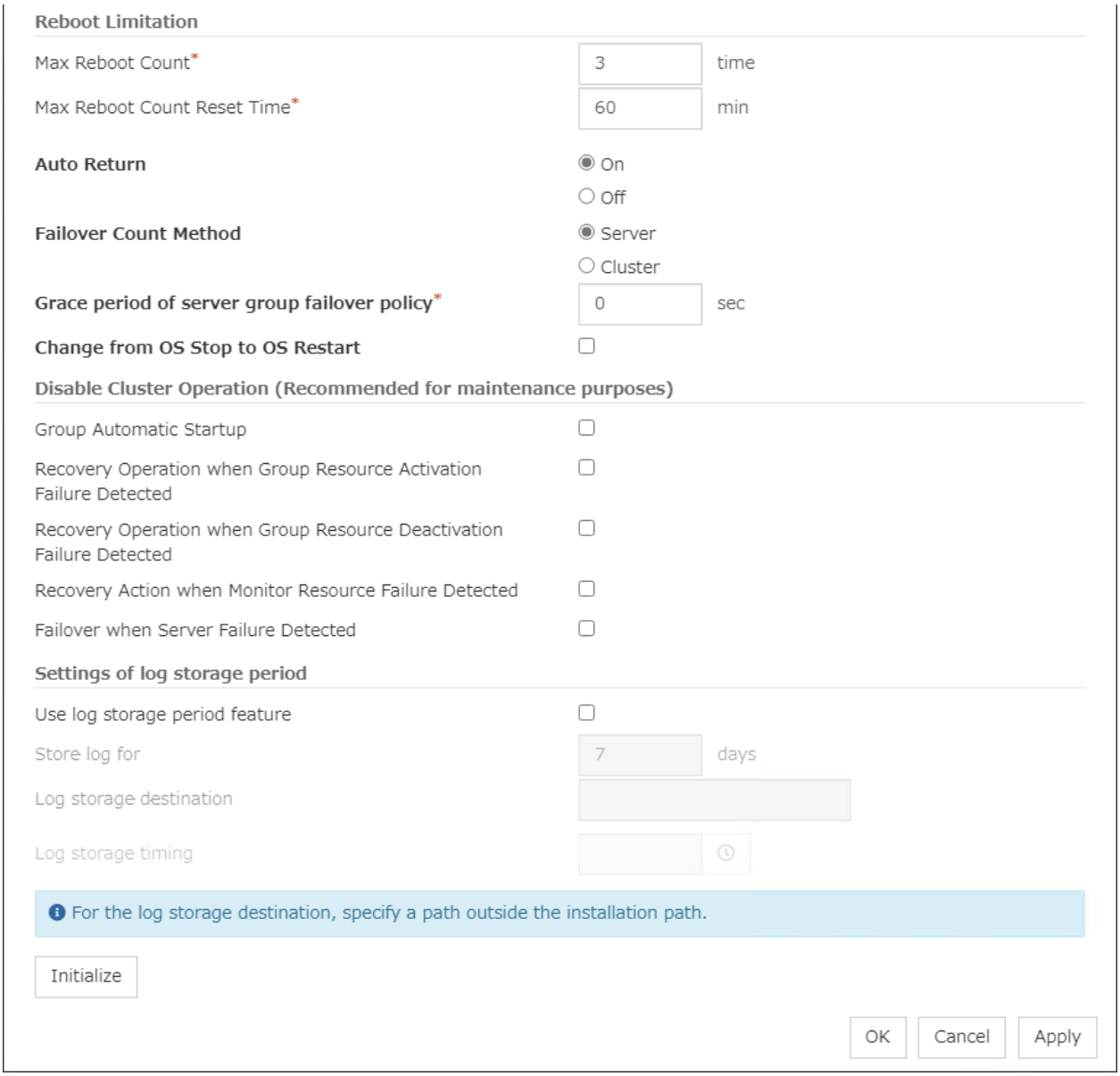
- When the check box is selected:
  System resource information related to the CPU, memory, processes, and others is collected regularly while the cluster is running.
  The collected system resource information is collected when the clplogcc command or Cluster WebUI collects logs.
  Specify type 1 to collect the log by the clplogcc command; specify Pattern 1 to collect the log by the Cluster WebUI. For details on log collection, see "*Collecting logs (clplogcc command)*"in "*9. EXPRESSCLUSTER command reference*" in this guide or 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.
- When the check box is not selected:
  No system resource information is collected.

Initialize

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

2.2.19 Extension Tab

Other cluster functions are set.



Reboot Limitation

You can specify the **Reboot OS** or **Shut down OS** as the final action at abnormality detection for group resources and monitor resources. If either of them is selected, 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.

  However, the number of reboots may not be counted with **Generate an intentional stop error** selected.

  With **Max Reboot Count** set to zero, the reboot can be unlimitedly repeated.

- 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** is set to 1 or greater, usually set **Max Reboot Count Reset Time** to 1 or greater (default: 0). If **Max Reboot Count Reset Time** is set to zero (0), the reboot count is not reset. To reset the reboot count, use the clpregctrl command.

Auto Return

For preparation against a server stop in a way other than a cluster shutdown/stop or against a failure in normally completing a cluster shutdown/stop, you can determine for the next OS startup whether to automatically recover the cluster service restarting after its crash.

- On
  Select this to perform the auto recovery.
- Off
  Select this not to perform the auto recovery.

Failover Count Method

Select the method to count the number of failovers from Server or Cluster.

- Server
  Count the number of failovers by server.
- Cluster
  Count the number of failovers by cluster.

Grace period of server group failover policy (0 to 99999)

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.

Change from OS Stop to OS Restart

Determine whether the OS stop action is collectively changed to OS restart action.

- If the check box is checked:
  The action change is made.
- If the check box is not checked:
  The action change is not made.

Note: If you want to make the action change, it is recommended to configure a network partition resolution resource or forced stop resource as well.

The changed action changes the following actions.
No actions other than those below are changed.

- Action for NP resolution
  - With **Stop cluster service and shutdown OS** selected:
    Changes to **Stop cluster service and reboot OS**.
  - With **Emergency shutdown** selected

Changes to **Reboot the OS** after the emergency shutdown.

- Action with an abnormal cluster service process
  - With **Emergency shutdown** selected
    Changes to **Reboot the OS** after the emergency shutdown.
- Action in case of an activation/deactivation stall of a group resource
  - With **Emergency shutdown** selected
    Changes to **Reboot the OS** after the emergency shutdown.
- Action in case of a split brain syndrome in a group
  - With **Emergency shutdown** selected
    Changes to **Reboot the OS** after the emergency shutdown.
- Final action with the abnormal activation/deactivation of a group resource
  - With **Stop cluster service and shutdown OS** selected:
    Changes to **Stop cluster service and reboot OS**.
- Final action with an abnormal monitor resource
  - With **Stop cluster service and shutdown OS** selected:
    Changes to **Stop cluster service and reboot OS**.

Note: The action change does not affect the following monitor resources:

- Message reception monitor resources
- User mode monitor resources
- Mirror disk monitor resources
- Hybrid disk monitor resources
- Hybrid disk TUR monitor resources

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 Group Resource Activation Failure 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 Group Resource Deactivation Failure 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 Monitor Resource Failure Detected
  - When the checkbox is selected:
    The recovery action is disabled.
  - When the checkbox is not selected:
    The recovery action is not disabled.
- Failover when server failure detected
  - When the checkbox is selected:
    The failover is disabled.
  - When the checkbox is not selected:
    The failover is not disabled.

Note: The disablement feature of **Recovery action when a monitor resource error is detected** does not support the following actions:

- Action when disk RW monitoring resources detect stall errors
- Action when timeout occurs in user mode monitor resources
- Recovery action for message receive monitor resources

Settings of log storage period

- Use log storage period feature
  Renames (not deletes) an old log file (whose name ends with 0.log, 1.log, or pre) in the following folders to <date and time when the file was last updated>_<type name>.log, when the file is rotated:
  - <installation path>/log
  - <installation path>/perf

  The log file renamed as above is compressed at a specified time, then saved as <date when the file was compressed_server name>.zip to a given log storage destination.

- Store log (1 to 9999)
  Specify a log storage period (up to 9999 days). When this period elapses, the corresponding log files are automatically removed.
- Log storage destination (within 170 characters)
  Specify an absolute path (other than the installation path) to the storage folder, in ASCII characters.
  Make sure that free space and write performance are sufficiently available.
- Log storage timing
  Specify a time at which the storage occurs every day, in the pop-up window opened by clicking the timepiece icon.

Initialize

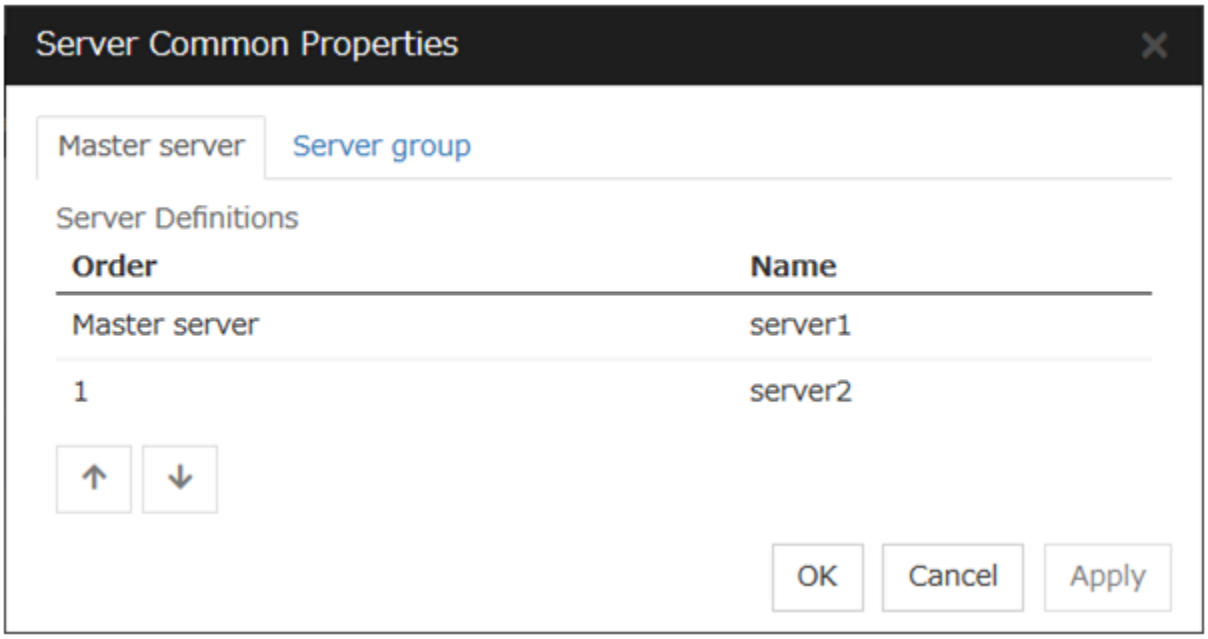
This operation is used to return the value to the default value. Click **Initialize** to set all items to their default values.

2.3 Servers 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.

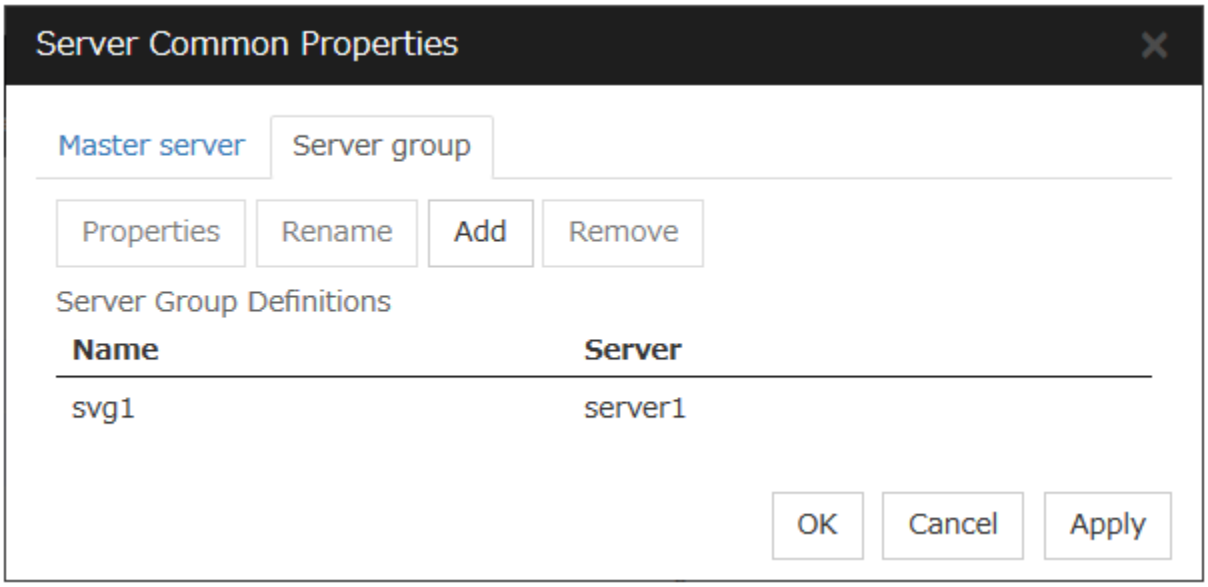


Order

Used when changing the priority order of the servers. Select the server to be changed from the server definition list, and click the arrows. The 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 details, see "Create a cluster" in " Procedure for creating the cluster configuration data" in "Creating the cluster configuration data" in the "Installation and Configuration Guide".

Remove

The selected server group is removed.

When the selected server group is used for the settings of the startup server of the failover group, the server group cannot be removed.

Rename

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

There are the following naming rules.

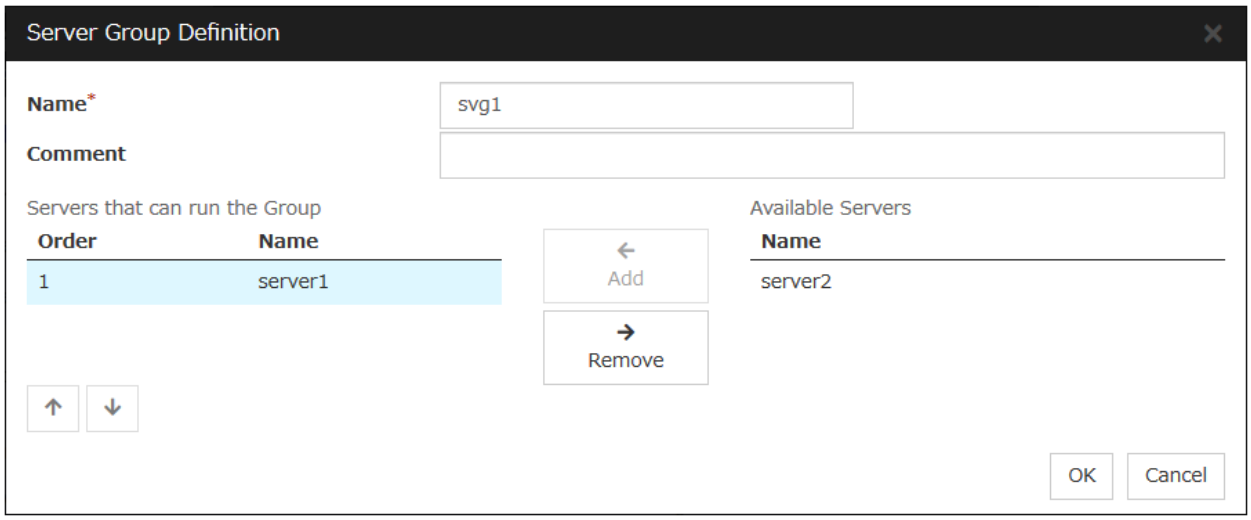
- There are naming rules that are the same as the host name of TCP/IP that can be set by the OS.
- Up to 31 characters (31 bytes).
- Names cannot start or end with a hyphen (-) or a space.
- A name consisting of only numbers is not allowed.

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

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

Remove

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

Order

Use the arrows to change the priority of a server that can run the group. Select the server whose priority you want to change, and then click the arrows. The selected row moves accordingly.

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

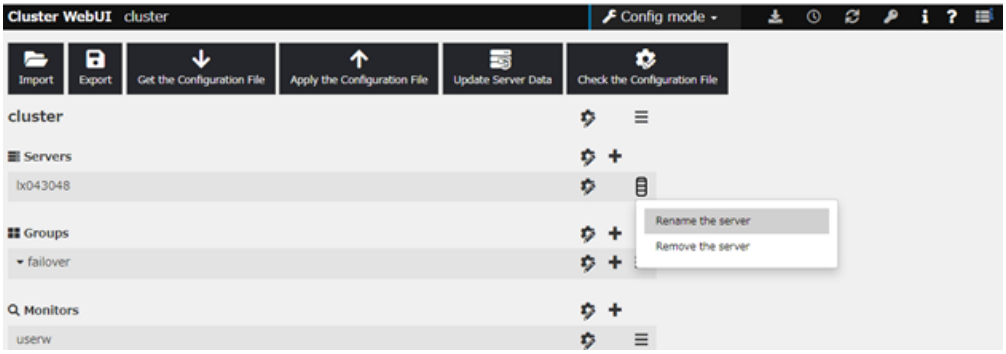
You can display the server name, and register and make a change to a comment on this tab.

Name

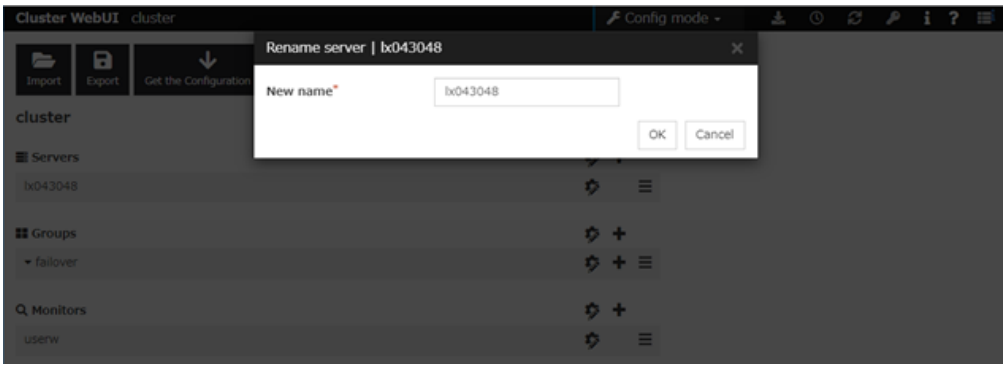
The selected server name is displayed. You cannot change the name here.

Changing the server name

1. click **others**, and then select **Rename the server**.



2. A dialog box to **rename server** is displayed.



Naming rules

- There are naming rules that are the same as the host name of TCP/IP that can be set by the OS. It should be completely the same as the name set to the server.
- Up to 63 characters (63 bytes)
- Neither hyphen (-) nor space can be the first or last letter in names.

- Underscore (_) is not allowed.
- A name consisting of only numbers is not allowed.
- Do not use "localhost" as the server name.

Comment

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

2.4.2 Warning Light tab

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

Add

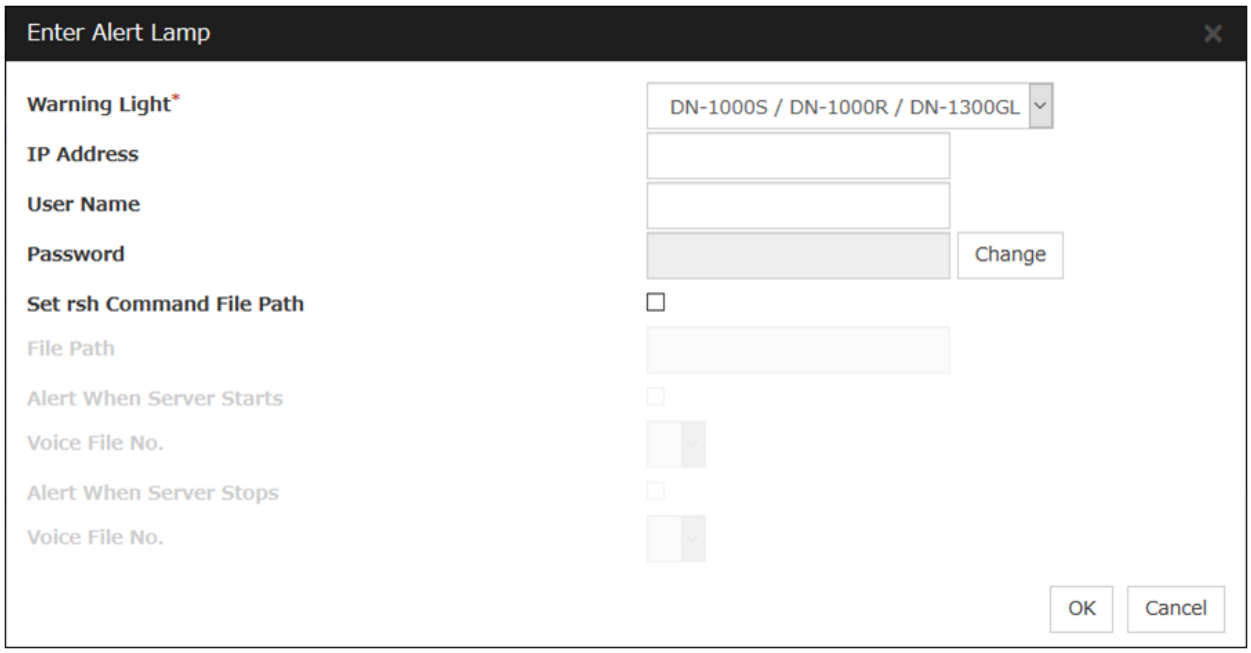
Use this button to add an IP address of warning light. Click **Add** to open the **Enter Alert Lamp** dialog box.

Remove

Use this button to remove an IP address of warning light. Select the target setting, and then, click **Remove**.

No.

The arrow can't be used because only 1 warning light can be registered at present.



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.

User Name

Enter the user name of the execution account on the server used for controlling the warning light.

Also, the user name specified here is used as the remote user name for the rsh command.

Password

Enter the password of the execution account on the server used for controlling the warning light.

Note: Enter Administrator for user name, Administrator for password.

Specify rsh command execution file path

- When the check box is selected:
  The rsh command execution file path can be specified.

- When the check box is not selected:
  The rsh command execution file path cannot be specified.

File path

Enter the full path of the rsh command to be used for controlling the warning light.
Specification example: C:\WINDOWS\system32\rsh.exe

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 reproduced at server start.

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 reproduced at server stop.

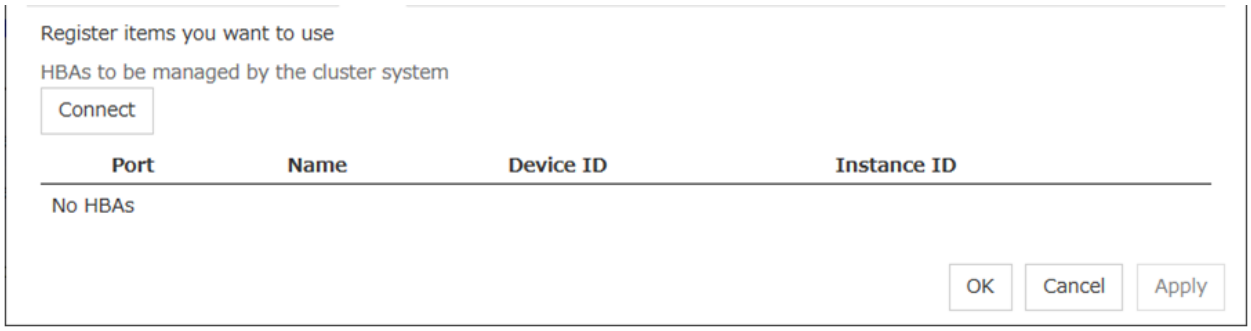
Edit

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

Note: To play 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 HBA tab

Set the HBA to which the shared disk is connected.



List of HBAs to be managed by the cluster system

Set the access to the shared disk. If the check box is selected, access to all disks connected to the HBA is controlled when starting the OS next time. To protect data, it is required to select the check box of the HBA to which the shared disk is connected.

If the HBA list is not displayed, it can be displayed by clicking the **Connect** button.

Important:

- Do not connect the shared disk to any HBA whose check box is not selected. Even though the check box is selected, do not connect to the shared disk when the OS is not started again after configuring the settings. Data on the shared disk may be corrupted.
- Do not select the check boxes other than those of HBAs to which the shared disk is connected. If access to the system partition on which the OS has been installed is restricted, the OS may not be started.
- Do not select the check boxes of HBA that connects the mirroring target internal disk if you use mirror disk resource. Starting mirror disk resource fails.

Partitions excluded from cluster management

When a disk other than the shared disk is connected to the HBA set in **HBAs to be managed by the cluster system**, register the partitions on the disk. The access to the partitions registered with this list is not restricted.

Important: In principle, do not register the partitions on the shared disk that can be accessed from multiple servers. Data on the shared disk may be corrupted.

Connect

Select this to get the HBA data by connecting to the server.

Add

Add a partition that should not be restricted in its access in **Partition excluded from cluster management**.

Remove

Remove the selected partition from **Partition excluded from cluster management.**

2.4.4 Proxy tab

Sets proxy information.

Proxy Scheme

Sets protocols you want to use.

None: Proxy is not used. HTTP: HTTP is used.

Proxy Server

Sets 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]-[9]" represents the way you apply changes of parameters on servers. Applicable method is marked with "✓."

Priority	How to change
1	Shut down and reboot cluster
2	Stop and restart the cluster daemon
3	Suspend and resume the cluster daemon
4	Stop and restart the group (Stop and restart the resource)
5	Restart the Node Manager service
6	Restart the Information Base service
7	Stop and restart the WebManager Server Stop and restart the alert log
8	Restart the API service
9	Upload only

To form a new cluster, refer to the "Installation and Configuration Guide".

Cluster

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Cluster Properties										
Info Tab										
Cluster Name	-			✓		✓				
Comment	-									✓
Language	English			✓			✓	✓	✓	
Interconnect Tab										
Priority	-			✓		✓				
Add, Remove				✓		✓				
[Type] column		✓								
[MDC] column		✓								
[Server] column: Kernel Mode	-			✓		✓	✓	✓	✓	
[Server] column: Witness HB Use				✓		✓	✓	✓	✓	
[Server] column: Mirror Communication Only		✓								
[Server] column: MDC Use		✓								
Server Down Notification	On									✓
Server Reset Notification	Off			✓		✓				
Execute Server Alive Check	Off			✓						
Timeout	1 seconds			✓						
Witness HeartBeat Properties										
Target Host						✓				
Service Port	80					✓				
Use SSL	Off					✓				
Use Proxy	Off					✓				
HTTP Timeout	10 seconds					✓				
Fencing Tab										
Add, Remove	-			✓		✓				
[Type] column	DISK			✓		✓				
Target	-			✓		✓				
[Server] column	-			✓		✓				
DISK NP Properties										
I/O Wait Time	80 seconds					✓				
Interval	60 seconds					✓				
Timeout	300 seconds					✓				
Retry Count	0 times					✓				
Ping NP Properties										
Interface Tab										
Group - No.						✓				
Group - IP Address						✓				
IP Address - IP Address						✓				
Detailed Settings - Interval	5 seconds					✓				
Detailed Settings - Timeout	3 seconds					✓				
Detailed Settings - Retry Count	3 times					✓				
HTTP NP Properties										
Use Witness HB Resource Settings	-					✓				
Target Host						✓				
Request-URI	/					✓				
Service Port	80					✓				
Use SSL	Off					✓				
Use Proxy	Off					✓				
Interval	5 seconds					✓				
Timeout	20 seconds					✓				
HTTP Timeout	10 seconds					✓				
Network Partition Resolution Tuning Properties										
Action at NP Occurrence	Emergency shutdown					✓				
Forced Stop Type	Do Not Use		✓							
BMC Forced-Stop Properties										
Server List Tab										
Servers (Add, Remove, Edit)	-		✓							
Enter BMC										
IP Address	-									✓
User Name										✓
Password										✓
Forced Stop Tab										
Forced Stop Action	BMC Power Off									✓
Forced Stop Timeout	15 seconds									✓
Time to Wait for Stop to Be Completed	15 seconds									✓
Lead Time between a Stop Request and a Failover Start	15 seconds									✓
Disable Group Failover When Execution Fails	Off									✓
vCenter Forced-Stop Properties										
Server List Tab										
Servers (Add, Remove, Edit)			✓							
Input for Virtual Machine Name										
Virtual Machine Name	-									✓
Data Center	-									✓
Forced Stop Tab										
Forced Stop Action	Power Off									✓
Forced Stop Timeout	10 seconds									✓
Time to Wait for Stop to Be Completed	10 seconds									✓
Lead Time between a Stop Request and a Failover Start	10 seconds									✓
Disable Group Failover When Execution Fails	Off									✓
vCenter Tab										
Method of performing forced stop	vSphere Automation API									✓
VMware vSphere CLI Installation Path	C:\Program Files (x86)\VMware\VMware vSphere CLI									✓
Host Name	-									✓
User Name	-									✓
Password	-									✓
Perl Path										✓

AWS Forced-Stop Properties											
Server List Tab											
Servers (Add, Remove, Edit)	-			✓							
Input of Instance											
Instance ID	-										✓
Forced Stop Tab											
Forced Stop Action	stop										✓
Forced Stop Timeout	10 seconds										✓
Time to Wait for Stop to Be Completed	180 seconds										✓
Lead Time between a Stop Request and a Failover Start	120 seconds										✓
Disable Group Failover When Execution Fails	Off										✓
Azure Forced-Stop Properties											
Server List Tab											
Servers (Add, Remove, Edit)	-			✓							
Input for Virtual Machine Name											
Virtual Machine Name	-										✓
Forced Stop Tab											
Forced Stop Action	stop and deallocate										✓
Forced Stop Timeout	10 seconds										✓
Time to Wait for Stop to Be Completed	180 seconds										✓
Lead Time between a Stop Request and a Failover Start	120 seconds										✓
Disable Group Failover When Execution Fails	Off										✓
Azure Tab											
User URI	-										✓
Tenant ID	-										✓
File Path of Service Principal	-										✓
Resource Group Name	-										✓
OCI Forced-Stop Properties											
Server List Tab											
Servers (Add, Remove, Edit)	-			✓							
Input of Instance											
Instance ID	-										✓
Forced Stop Tab											
Forced Stop Action	stop										✓
Forced Stop Timeout	15 seconds										✓
Time to Wait for Stop to Be Completed	180 seconds										✓
Lead Time between a Stop Request and a Failover Start	120 seconds										✓
Disable Group Failover When Execution Fails	Off										✓
Custom Forced-Stop Properties											
Server List Tab											
Servers (Add, Remove)	-			✓							
Forced Stop Tab											
Forced Stop Timeout	10 seconds										✓
Disable Group Failover When Execution Fails	Off										✓
Script Tab											
Select User Application Enter application path (Edit)	-										✓
Select Script created with this product Add, Remove, Edit, Replace	forcestop.bat										✓
Exec User	-										✓
Timeout Tab											
Service Startup Delay Time	0 seconds										✓
Network initialization complete wait time	3 minutes										✓
Server Sync Wait Time	5 minutes										✓
Heartbeat Interval	3 seconds				✓		✓	✓		✓	
Heartbeat Timeout	30 seconds				✓		✓				
Server Internal Timeout	180 seconds				✓				✓		
Port No. Tab											
Server Internal Port Number	29001				✓				✓		
Information Base Port Number	29008							✓		✓	
Data Transfer Port Number	29002	✓									
WebManager HTTP Port Number	29003								✓		
API HTTP Port Number	29009									✓	
API Server Internal Port Number	29010									✓	
Disk Agent Port Number	29004	✓									
Mirror Driver Port Number	29005	✓									
Kernel Mode Heartbeat Port Number	29106						✓				
Alert Sync Port Number	29003								✓		
Recovery Tab											
Action When the Cluster Service Process Is Abnormal	Emergency shutdown				✓						
Recovery Action for HA Agents											
Max Restart Count	3 times				✓						
Recovery Action over Max Restart Count	No operation				✓						
Action to apply in the event of an activation/deactivation stall of a group resource	Emergency shutdown				✓						
Disable the Final Action when OS Stops Due to Failure Detection											
Group Resource When Activation Failure Detected	Off				✓						
Group Resource When Deactivation Failure Detected	Off				✓						
Monitor Resource When Failure Detected	Off				✓						
Disable Shutdown When Multi-Failover-Service Detected											
Server Group Survives When Multi-Failover-Service Detected					✓						
Server Group When Multi-Failover-Service Detected	-				✓						

Alert Service Tab											
Enable Alert Service	Off										✓
Alert Destination Tab											
Messages (Add, Remove, Edit)	-										✓
Message Tab											
Category	Process										✓
Module Type	apisv										✓
Event ID	-										✓
Destination Alert Logs	Off										✓
Destination Mail Report	Off										✓
Destination SNMP Trap	Off										✓
Destination Alert Extension	Off										✓
Destination Message Topic	Off										✓
Destination EventLog(DisableOnly)	Off										✓
Command (Add, Remove, Edit)	-										✓
Mail Address	-										✓
Subject	-										✓
Mail Method	SMTP										✓
SMTP Settings											
Behavior Tab											
Mail Charset	-										✓
Send Mail Timeout	30 seconds										✓
Subject Encode	Off										✓
SMTP Server	-										✓
SMTP Server List (Add, Remove)	-										✓
Enter the SMTP Server											
SMTP Server	-										✓
Use SSL	Off										✓
Connection Method	SMTPS										✓
SMTP Port	25										✓
Sender Address	-										✓
Enable SMTP Authentication	Off										✓
Method	LOGIN										✓
User name	-										✓
Password	-										✓
Use Network Warning Light	Off						✓				
Behavior Tab											
Destination (Add, Remove, Edit)	-										✓
Destination Tab											
Destination Server	-										✓
SNMP Port No.	162										✓
SNMP Version	v2c										✓
SNMP Community Name	public										✓
WebManager Tab											
Enable WebManager Service	On								✓		
Communication Method	HTTP								✓		
Number of sessions which can be established simultaneously	64								✓		
Password											
Cluster Password Method / OS Authentication Method	Cluster Password Method								✓		
Cluster Password Method											
Password for Operation	-								✓		
Password for Reference	-								✓		
OS Authentication Method											
Authorized Group List(Add, Remove, Edit)									✓		
Operation	On								✓		
Login Session Lifetime Period	1440 minutes								✓		
Automatic Logout Time Period	60 minutes								✓		
Lockout Threshold	0 time								✓		
Lockout Time	10 minutes								✓		
Control connection by using client IP address	Off								✓		
IP Addresses of the Accessible Clients (Add, Remove, Edit)	-								✓		
Operation	On								✓		
Cluster WebUI Operation Log											
Output Cluster WebUI Operation Log	On								✓		
Log output path	-								✓		
File Size	1 megabyte								✓		
IP address for Integrated WebManager											
Priority	-				✓						
[Server] column	-				✓						
WebManager Tuning Properties											
Behavior Tab											
Client Session Timeout	30 seconds								✓		
Screen Data Refresh Interval	90 seconds								✓		
Mirror Agent Timeout	150 seconds								✓		
Time Limit For Keeping Log Files	600 seconds								✓		
Use Time Information Display Function	On				✓				✓		
API Tab											
Enable API Service	Off									✓	
Communication Method	HTTPS									✓	
Control connection by using client IP address	Off									✓	
IP Addresses of the Accessible Clients (Add, Remove, Edit)	-									✓	
API Service Operation Log											
Output API Service Operation Log	On									✓	
Log output path	-									✓	
File Size	1 megabyte									✓	
API Tuning Properties											
Authentication Lockout Threshold	3 times									✓	
HTTP Server Start Retry Count	3 times									✓	
HTTP Server Start Interval	5 seconds									✓	

Encryption Tab											
Certificate File	-								✓	✓	
Private Key File	-								✓	✓	
SSL Library	-			✓		✓			✓	✓	
Crypto Library	-			✓		✓			✓	✓	
Alert Log Tab											
Enable Alert Service	On								✓		
Max. Number to Save Alert Records	10000								✓		
Enable a log file for investigation to be downloaded	On								✓		
Alert Sync Method	Unicast (fixed)								✓		
Alert Sync Communication Timeout	30 seconds								✓		
Delay Warning Tab											
Heartbeat Delay Warning	On 80%			✓		✓					
Monitor Delay Warning	On 80%			✓							
Disk Tab											
At Disk Disconnection Failure: Retry Interval	3 seconds										✓
At Disk Disconnection Failure: Retry Count	Set Number										✓
At Disk Disconnection Failure: Retry Count: Set	10 times										✓
At Disk Disconnection Failure: Timeout	1800 seconds										✓
At Disk Disconnection Failure: Final Action	Enforced Disconnection										✓
Mirror Disk Tab											
Auto Mirror Initial Construction	On										✓
Auto Mirror Recovery	On										✓
Differential Bitmap Size	1		✓								
History Recording Area Size in Asynchronous Mode	100		✓								
Allow failover on mirror break for specified time	Off										✓
Timeout	30 seconds										✓
At Disk Disconnection Failure: Retry Interval	3 seconds										✓
At Disk Disconnection Failure: Retry Count	Set Number										✓
At Disk Disconnection Failure: Retry Count: Set	10 times										✓
At Disk Disconnection Failure: Timeout	1800 seconds										✓
At Disk Disconnection Failure: Final Action	Enforced Disconnection										✓
Account Tab											
Account List (Add, Remove, Edit)	-										✓
JVM monitor Tab											
Java Installation Path	-			✓							
Maximum Java Heap Size	16 megabytes			✓							
Java VM Additional Option	-			✓							
Action Timeout	60 seconds			✓							
Log Output Settings											
Log Level	INFO			✓							
Generation	10 generations			✓							
Rotation Type	File Capacity			✓							
Rotation Type, File Capacity, Max Size	3072 kilobytes			✓							
Rotation Type, Period, Start Time	0:00			✓							
Rotation Type, Period, Interval	24 hours			✓							
Resource Measurement Setting [Common]											
Retry Count	10 times			✓							
Error Threshold	5 times			✓							
Interval, Memory Usage, Active Threads	60 seconds			✓							
Interval, The time and count in Full GC	120 seconds			✓							
Resource Measurement Setting [WebLogic]											
Retry Count	3 times			✓							
Error Threshold	5 times			✓							
Interval, The number of request	60 seconds			✓							
Interval, The average number of the request	300 seconds			✓							
Connection Settings											
Management Port	25500			✓							
Retry Count	3 times			✓							
Waiting time for reconnection	60 seconds			✓							
Cloud Tab											
Enable Amazon SNS linkage function	Off										✓
TopicArn	-										✓
Enable Amazon CloudWatch linkage function	Off										✓
Namespace	-										✓
Interval for Sending Metrics	60 seconds										✓
Environment variables at the time of performing AWS-related features											
Name	-										✓
Value	-										✓
AWS CLI Command line options											
aws cloudwatch	-										✓
aws ec2	-										✓
aws route53	-										✓
aws sns	-										✓
Statistics Tab											
Cluster Statistics Heartbeat Resource	On					✓					
Cluster Statistics FileSize	50 MB					✓					
Cluster Statistics Group	On			✓							
Cluster Statistics FileSize	1 MB			✓							
Cluster Statistics Group Resource	On			✓							
Cluster Statistics FileSize	1 MB			✓							
Cluster Statistics Monitor Resource	On			✓							
Cluster Statistics FileSize	10 MB			✓							
Mirror Statistics Collect Statistics	On										✓
System Resource Statistics Collect Statistics	On			✓							

Extension Tab											
Max Reboot Count	3 times				✓						
Max Reboot Count Reset Time	60 minutes				✓						
Auto Return	On										✓
Failover Count Method	Server			✓							
Grace period of server group failover policy	0 seconds										✓
Change from OS Stop to OS Restart	Off										✓
Disable Cluster Operation											
Group Automatic Startup	Off										✓
Recovery Operation when Group Resource Activation Failure Detected	Off										✓
Recovery Operation when Group Resource Deactivation Failure Detected	Off										✓
Recovery Action when Monitor Resource Failure Detected	Off										✓
Failover when Server Failure Detected	Off										✓
Settings of log storage period											
Use log storage period feature	Off	✓									
Store log	7 days										✓
Log storage destination	-										✓
Log storage timing	-										✓

Servers

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

Server

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Add Server [1]										
Remove Server [2]										
Server Properties										
Info Tab										
Name [3]	-									
Comment										✓
Warning Light Tab										
I/F Number (Add, Remove)	The order you added I/Fs			✓		✓				
IP Address (Edit)	-			✓		✓	✓	✓	✓	
Warning Light	DN-1000S / DN-1000R / DN-1300GL			✓		✓		✓		
User Name	-			✓						
Password				✓						
Specify rsh command execution file path	Off									✓
File path	-									✓
Alert When Server Starts	Off									✓
Alert When Server Stops	Off									✓
Voice File No.	-									✓
Voice File No.	-									✓
HBA Tab										
HBAs to be managed by the cluster system	-	✓								
Partition excluded from cluster management	-			✓						
Proxy Tab										
Proxy Scheme	None					✓				
Proxy Server	-					✓				
Proxy Port	-					✓				

[1] For details about how to add or remove a server, see the Maintenance Guide.
[2] For details about how to add or remove a server, see the Maintenance Guide.
[3] 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.

Groups

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

Group

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Add Group	-			✓						
Remove Group	-			✓	✓					
Group Properties										
Info Tab										
Type	failover									
Use Server Group Settings	Off		✓							
Name	-			✓	✓					
Comment	-									✓
Startup Server Tab										
Failover is possible on all servers	On			✓						
Order	The order you added to "Servers that can run the Group."			✓						
Server (Add, Remove)	-			✓						
Attribute Tab										
Startup Attribute	Auto Startup			✓						
Execute Multi-Failover-Service Check	Off			✓						
Timeout	300 seconds			✓						
Failover Attribute	Auto Failover			✓						
Auto Failover	Use the startup server settings			✓						
Prioritize failover policy in the server group	Off			✓						
Perform a Smart Failover	Off			✓						
Enable only manual failover among the server groups	Off			✓						
Exclude Server with Error Detected by Specified Monitor Resource, from Failover Destination	Off			✓						
Failover with Error Ignored If It Is Detected in All Servers	Off			✓						
Failback Attribute	Manual Failback			✓						
Monitor Resources for Excluding Server from Failover Destination	IP monitor NIC Link Up/Down monitor			✓						
Start Dependency Tab										
Dependent Group	-			✓						
Start Wait Time	1800 seconds			✓						
Dependent Group Property										
Wait Only when on the Same Server	Off			✓						
Stop Dependency Tab										
Dependent Group	-			✓						
Stop Wait Time	1800 seconds			✓						
Wait the Dependent Groups when a Cluster Stops	On									✓
Wait the Dependent Groups when a Server Stops	Off									✓
Wait the Dependent Groups when a Group Stops	Off			✓						
If stopping a target group fails, await the timeout	Off			✓						

Group Resource (Common)

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Add Resource				✓						
Remove Resource				✓	✓					
Resource Common Properties										
Info Tab										
Name	Default value per each resource			✓	✓					
Comment										✓
Dependency Tab										
Follow the default dependence	On			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count	0			✓						
Failover Target Server	Stable server			✓						
Failover Threshold	1 time			✓						
Final Action at Activation Failure Detection	Default value per each resource			✓						
Execute Script before Final Action	Off									✓
Edit Script										
Select User Application Enter application path (Edit)										✓
Select Script created with this product Script content (Edit)										✓
File	predeactaction.bat									
Timeout	5 seconds									✓
Exec User	-									✓
Retry Count at Deactivation Failure	0			✓						
Final Action at Deactivation Failure	Default value per each resource			✓						
Execute Script before Final Action	Off									✓
Edit Script										
Select User Application Enter application path (Edit)										✓
Select Script created with this product Script content (Edit)										✓
File	predeactaction.bat									
Timeout	5 seconds									✓
Exec User	-									✓
Extention Tab										
Resource Startup Attribute	Automatic startup			✓						
Execute Script before or after Activation or Deactivation										
Execute Script before Activation	Off									✓
Execute Script after Activation	Off									✓
Execute Script before Deactivation	Off									✓
Execute Script after Deactivation	Off									✓
Edit Script										
Select User Application Enter application path (Edit)										✓
Select Script created with this product Script content (Edit)										✓
File	rscextent.bat									✓
Timeout	30 seconds									✓
Exec User	-									✓

Application resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Application Resource Properties										
Dependency Tab										
Follow the default dependence	On • CIFS resource • disk resource • floating ip resource • hybrid disk resource • mirror disk resource • registry synchronization resource • virtual computer name resource • virtual IP resource •AWS elastic ip resource •AWS virtual ip resource •AWS secondary ip resource •AWS DNS resource •Azure probe port resource •Azure DNS resource			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	0			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	0			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Resident Type	Resident				✓					
Start Path	-				✓					
Stop Path	-									✓
Application Resource Tuning Properties										
Parameter Tab										
Start Script Synchronous, Asynchronous	Synchronous									✓
Start Script Timeout	1800 seconds			✓						
Start Script Normal Return Value	-									✓
Stop Script Synchronous, Asynchronous	Synchronous									✓
Stop Script Timeout	1800 seconds			✓						
Stop Script Normal Return Value	-									✓
Target VCOM Resource Name	-				✓					
Forcibly Terminate Application When Stopping	Off									✓
Exec User	Set Up Individually				✓					
Start Tab										
Current Directory	-									✓
Option Parameter	-									✓
Window Size	Hide									✓
Exec User Domain	-				✓					
Exec User Account	-				✓					
Exec User Password	-				✓					
Execute from the Command Prompt	Off									✓
Stop Tab										
Current Directory	-									✓
Option Parameter	-									✓
Window Size	Hide									✓
Exec User Domain	-									✓
Exec User Account	-									✓
Exec User Password										✓
Execute from the Command Prompt	Off									✓

Floating IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Floating IP Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default is set)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
IP Address	-				✓					
Floating IP Resource Tuning Properties										
Parameter Tab										
Run ping	On									✓
Ping Interval	1 second			✓						
Ping Timeout	1000 milliseconds			✓						
Ping Retry Count	5 times			✓						
Forced FIP Activation	Off									✓
Judge NIC Link Down as Failure	Off			✓						
Use transmission source change feature	Off				✓					
Specification for transmission source	Specify FIP address as transmission source				✓					

Mirror Disk resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Mirror Disk Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default is set)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	3 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Mirror Disk No.	1			✓	✓					
Data Partition Drive Letter	-			✓	✓					
Cluster Partition Drive Letter	-			✓	✓					
Cluster Partition Offset Index	0			✓	✓					
Selection of Mirror Disk Connect										
Order	The order registered for the cluster	✓								
MDC (Add, Remove)	Two upper level mirror disk connects registered for the cluster	✓								
Servers that can run the group (Add, Remove)	-	✓								
Data Partition (Edit)	-			✓	✓					
Cluster Partition (Edit)	-			✓	✓					
Mirror Disk Resource Tuning Properties										
Execute the initial mirror construction	On			✓	✓					
Mirror Connect Timeout	20 seconds			✓	✓					
Request Queue Maximum Size	2048 [KB]			✓	✓					
Mode	Synchronous			✓	✓					
Kernel Queue Size	2048 [KB]			✓	✓					
Application Queue Size	2048 [KB]			✓	✓					
Thread Timeout	30 seconds			✓	✓					
Communication Band Limit	Unlimited			✓	✓					
History Files Store Folder	-			✓	✓					
History Files Size Limit	Unlimited			✓	✓					
Compress Data	Off			✓	✓					
Compress Recovery Data	Off			✓	✓					
Encrypt mirror communication	Off			✓	✓					
Key File Path	-			✓	✓					

Registry Synchronization resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Registry Synchronization Resource Properties										
Dependency Tab										
Follow the default dependence	On • CIFS resource • disk resource • floating ip resource • hybrid disk resource • mirror disk resource • virtual computer name resource • virtual IP resource •AWS elastic ip resource •AWS virtual ip resource •AWS secondary ip resource •AWS DNS resource •Azure probe port resource •Azure DNS resource			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	zero			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Registry List (Add, Remove, Edit)	1			✓	✓					
Registry Synchronization Resource Tuning										
Parameter Tab										
Delivery Interval	1 second			✓						

Script resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Script Resource Properties										
Dependency Tab										
Follow the default dependence	On • CIFS resource • disk resource • floating ip resource • hybrid disk resource • mirror disk resource • registry synchronization resource • virtual computer name resource • virtual IP resource •AWS elastic ip resource •AWS virtual ip resource •AWS secondary ip resource •AWS DNS resource •Azure probe port resource •Azure DNS resource			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	zero			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Scripts (Add, Remove, Edit, Replace)	-									✓
Script Resource Tuning Properties										
Parameter Tab										
Start Script Synchronous, Asynchronous	Synchronous									✓
Start Script Timeout	1800 seconds			✓						
Start Script Normal Return Value	When there is no value									✓
Start Script Execute on standby server	Off				✓					
Start Script Timeout (on standby server)	10 seconds			✓						
Perform recovery processing	Off									✓
Stop Script Synchronous, Asynchronous	Synchronous									✓
Stop Script Timeout	1800 seconds			✓						
Stop Script Normal Return Value	When there is no value									✓
Stop Script Execute on standby server	Off									✓
Stop Script Timeout (on standby server)	10 seconds			✓						
Target VCOM Resource Name	-									✓
Exec User	-				✓					

Disk resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Disk Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default is set)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	3 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Drive Letter				✓	✓					
Servers that can run the group (Add, Remove)				✓	✓					
GUID (Edit)				✓	✓					

Service resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Service Resource Properties										
Dependency Tab										
Follow the default dependence	On • CIFS resource • disk resource • floating ip resource • hybrid disk resource • mirror disk resource • registry synchronization resource • virtual computer name resource • virtual IP resource •AWS elastic ip resource •AWS virtual ip resource •AWS secondary ip resource •AWS DNS resource •Azure probe port resource •Azure DNS resource			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	1 time			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Service Name					✓					
Service Resource Tuning Properties										
Parameter Tab										
Start Script Synchronous, Asynchronous	Synchronous									✓
Start Script Timeout	1800 seconds			✓						
Stop Script Synchronous, Asynchronous	Synchronous									✓
Stop Script Timeout	1800 seconds			✓						
Target VCOM Resource Name	-				✓					
Service Tab										
Start Parameters	-				✓					
Do not assume it as an error when the service is already started	Off				✓					
Wait after the service is started	0 seconds									✓
Wait after the service is stopped	0 seconds									✓

Virtual Computer Name resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Virtual Computer Name Resource Properties										
Dependency Tab										
Follow the default dependence	On • floating IP resources • virtual IP resources •AWS elastic ip resource •AWS virtual ip resource •AWS secondary ip resource •Azure probe port resource			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Virtual Computer Name	-			✓	✓					
Target FIP Resource Name	-			✓	✓					
Virtual Computer Name Resource Tuning										
Parameter Tab										
Register with DNS dynamically	Off			✓	✓					
IP address to be associated	FIP			✓	✓					
edit				✓	✓					

Virtual IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Virtual IP Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default is set)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
IP Address					✓					
Net Mask	-				✓					
Destination IP Address	-				✓					
Source IP Address	-				✓					
Send Interval	30 seconds				✓					
Use Routing Protocol	RIPver1				✓					
Virtual IP Resource Tuning Properties										
Parameter Tab										
Run ping	On									✓
Interval	1 second			✓						
Timeout	1000 milliseconds			✓						
Retry Count	5 times			✓						
Forced VIP Activation	Off									✓
Judge NIC Link Down as Failure	Off			✓						
RIP Tab										
Metric	3				✓					
Port Number	520				✓					
RIPng Tab										
Metric	1				✓					
Port Number	521				✓					

CIFS resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
CIFS Resource Properties										
Dependency Tab										
Follow the default dependence	On • disk resources • Hybrid disk resources • mirror disk resources			✓	✓					
Dependent Resources (Add, Remove)				✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	Zero			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Execute the automatic saving of shared configuration of drive.	Off				✓					
Target Drive	-				✓					
Shared Configuration File	-				✓					
Errors in restoring file share setting are treated as activity failure	Off				✓					
Shared Name	-				✓					
Folder	-				✓					
Comment	-				✓					
When folder is shared not as activity failure	On				✓					
CIFS Resource Tuning Properties										
Cache Tab										
Allow Caching	On				✓					
Caching Setting	Automatic Caching				✓					
User Tab										
User Limit	No limitation				✓					
Max	-				✓					
Permission	everyone Read				✓					

Hybrid Disk resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Hybrid Disk Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default is set)			✓	✓					
Dependent Resources (Add, Remove)				✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	3 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure Detection	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Hybrid disk number	1			✓	✓					
Data partition drive letter	-			✓	✓					
Cluster partition driver letter	-			✓	✓					
Cluster partition offset index	0			✓	✓					
Selection of Mirror Disk Connect										
Order	The order registered for the cluster	✓								
MDC (Add, Remove)	Two upper level mirror disk connects registered for the cluster	✓								
Hybrid Disk Resource Tuning Properties										
Execute the initial mirror construction	On			✓	✓					
Mirror Connect Timeout	20 seconds			✓	✓					
Request Queue Maximum Size	2048 KB			✓	✓					
Mode	Synchronous			✓	✓					
Kernel Queue Size	2048 KB			✓	✓					
Application Queue Size	2048 KB			✓	✓					
Thread Timeout	30 seconds			✓	✓					
Communication Band Limit	Unlimited			✓	✓					
History Files Store Folder	-			✓	✓					
History Files Size Limit	Unlimited			✓	✓					
Compress Data When Recovering	Off			✓	✓					
Encrypt mirror communication	Off			✓	✓					
Key File Path	-			✓	✓					

Dynamic DNS resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Dynamic DNS Resource Properties										
Dependency Tab										
Follow the default dependence	On • Floating IP resource • Virtual IP resource •AWS elastic ip resource •AWS virtual ip resource •AWS secondary ip resource •Azure probe port resource			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	0 times			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Specify the count. [zero]			✓						
Final Action at Activation Failure	No operation (Do not activate the next resource.)			✓						
Execute script before final action	Off									✓
Retry Count at Deactivation Failure	0 times			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down the OS.			✓						
Execute script before final action	Off									✓
Details Tab										
Virtual Host Name	-				✓					
IP Address	-				✓					
DDNS Server					✓					
Port No.	53				✓					
Cache TTL	0 seconds				✓					
Execute Dynamic Update Periodically	On				✓					
Update Interval	60 minutes				✓					
Delete the Registered IP Address	Off				✓					
Kerberos Authentication	Off				✓					

AWS Elastic IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS elastic ip Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster daemon and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
EIP ALLOCATION ID	-				✓					
ENI ID	-				✓					
AWS elastic ip Resource Tuning Properties										
Parameter Tab										
AWS CLI Timeout	100 seconds			✓						

AWS Virtual IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS virtual ip Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
IP Address	-				✓					
VPC ID	-				✓					
ENI ID	-				✓					
AWS virtual ip Resource Tuning Properties										
Parameter Tab										
Start Timeout	300 seconds			✓						
Stop Timeout	60 seconds			✓						

AWS Secondary IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS secondary ip Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
IP Address	-				✓					
ENI ID	-				✓					
AWS secondary ip Resource Tuning Properties										
Parameter Tab										
Start Timeout	180 seconds			✓						
Stop Timeout	180 seconds			✓						

AWS DNS resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS DNS Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	0 time			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Host Zone ID	-				✓					
Resource Record Set Name	-				✓					
IP Address	-				✓					
TTL	300 seconds				✓					
Delete a resource set at deactivation	Off									✓
AWS DNS Resource Tuning Properties										
Parameter Tab										
AWS CLI Timeout	100 seconds			✓						

Azure probe port resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Azure probe port Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Probeport	-				✓					
Azure probe port Resource Tuning Properties										
Parameter Tab										
Probe wait timeout	30 seconds				✓					

Azure DNS resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Azure DNS Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	1 time			✓						
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	0 time			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Record Set Name	-				✓					
Zone Name					✓					
IP Address	-				✓					
TTL	3600 seconds				✓					
Resource Group Name	-				✓					
User URI	-				✓					
Tenant ID	-				✓					
File Path of Service Principal					✓					
Azure CLI File Path	-				✓					
Delete a record set at deactivation	On									✓
Azure DNS Resource Tuning Properties										
Parameter Tab										
Azure CLI Timeout	100 seconds			✓						

Google Cloud Virtual IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Google Cloud Virtual IP Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Port Number	-				✓					
Google Cloud Virtual IP Resource Tuning Properties										
Parameter Tab										
Health Check Timeout	30 seconds				✓					

Google Cloud DNS resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Google Cloud DNS Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	1 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Zone Name					✓					
DNS Name	-				✓					
IP Address	-				✓					
TTL	300 seconds				✓					
Delete a resource record set at deactivation	Off									✓

Oracle Cloud Virtual IP resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Oracle Cloud Virtual IP Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Port Number	-				✓					
Oracle Cloud Virtual IP Resource Tuning										
Parameter Tab										
Health Check Timeout	30 seconds				✓					

Oracle Cloud DNS resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Oracle Cloud DNS Resource Properties										
Dependency Tab										
Follow the default dependence	On (No default dependence)			✓	✓					
Dependent Resources (Add, Remove)	-			✓	✓					
Recovery Operation Tab										
Retry Count at Activation Failure	5 times			✓						
Failover Target Server	Stable operation server			✓						
When [Server] is selected for [Failover Count Method]										
Failover Threshold	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Failover Threshold	Set as much as the number of the servers			✓						
Final Action at Activation Failure	No Operation (Not activate next resources)			✓						
Execute Script before Final Action	Off									✓
Retry Count at Deactivation Failure	zero			✓						
Final Action at Deactivation Failure	Stop the cluster service and shut down OS.			✓						
Execute Script before Final Action	Off									✓
Details Tab										
Region	-				✓					
Domain (FQDN)	-				✓					
Zone OCID	-				✓					
IP Address	-				✓					
TTL	300 seconds				✓					
Delete a resource record set at deactivation	Off									✓
Use Proxy	Off									✓
How far you manage a resource record in a multi-region environment	All regions to which the cluster servers belong				✓					
Oracle Cloud DNS Resource Tuning Properties										
Parameter Tab										
OCI CLI Timeout	100 seconds			✓						

Monitor resource (common)

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Add Monitor Resource	-			✓						
Remove Monitor Resource	-			✓						
Monitor Resource Properties										
Info Tab										
Name	-			✓						
Comment	-									✓
Recovery Action Tab										
Edit Script										
When [User Application] is selected										
Enter application path (Edit)	-									✓
When [Script created with this product] is selected										
Script content (Edit)	-									✓
Timeout	5 seconds									✓
Exec User	-									✓

Application monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Application Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	3 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Final Action	No Operation			✓						
Execute Script before Final Action	Off									✓

Disk RW monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Disk RW Monitor Resource Properties										
Monitor(common) Tab										
Interval	30 seconds			✓						
Timeout	300 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	0 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Fine Name	-			✓						
I/O size	2000000 bytes			✓						
Action on Stall	Generate an intentional stop error			✓						
Action when diskfull is detected	The recovery action enabled			✓						
Use Write Through Method	Disabled			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time (if the recovery target is other than clusters)			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Floating IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Floating IP Monitor Resource Properties										
Monitor(common)Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor NIC Link Up/Down	Off									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
IP Monitor Resource Properties										
Monitor (common) tab										
Interval	60 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
IP Address (Add, Remove, Edit)	-									✓
ping Timeout	5000 milliseconds									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times (if the recovery target is other than clusters)			✓						
Execute Script before Failover	Off									✓
Failover Target Count	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Mirror Disk monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Mirror Disk Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	999 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	10 seconds			✓						
Monitor Timing	Always (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Mirror Disk Resource	-			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Destination Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

NIC Link Up/Down monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
NIC Link Up/Down Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Retry Count	1 time			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Individually Set Up Servers (Add, Remove, Edit)	-									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Multi Target monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Multi Target Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	60 seconds			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Resource List (Add, Remove)	-			✓						
Multi Target Monitor Resource Tuning										
Parameter Tab										
Error Threshold	Same as number of members									✓
Specify Number	64									✓
Warning Threshold	Off									✓
Specify Number	-									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Registry Synchronous monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Registry Synchronous Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Disk TUR monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Disk TUR Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	300 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Disk Resource	-			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Service monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Service Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	3 seconds			✓						
Monitor Timing	Active			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Service Name	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Virtual Computer Name monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Virtual Computer Name Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Recovery Action Tab										
Recovery Action	Execute only the final action			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	0 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Specify the count. [zero]			✓						
Execute Script before Final Action	Off									✓
Final Action	Stop the cluster and shut down the OS			✓						

Virtual IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Virtual IP Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Failover Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

CIFS monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
CIFS Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Access Check	Disable			✓						
Path	-			✓						
Check	Read			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Hybrid Disk monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Hybrid Disk Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	999 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	10 seconds			✓						
Monitor Timing	Always (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Hybrid Disk Resource	-			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Hybrid Disk TUR monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Hybrid Disk TUR Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	300 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) tab										
Hybrid Disk Resource	-			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Custom monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Custom Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	3 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Script Path Type	Script created with this product			✓						
File	genw.bat			✓						
Monitor Type	Synchronous			✓						
Normal Return Value	0			✓						
Warning Return Value	-			✓						
Kill the application when exit	Off			✓						
Wait for activation monitoring to stop before stopping the cluster	Off									✓
Exec User	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Message Receive monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Message Receive Monitor Resource Properties										
Monitor (common) Tab										
Retry Count	0 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Monitor (special) Tab										
Category										✓
Keyword	-									✓
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Failover Target Server	Stable Server			✓						
Execute Failover to outside the Server Group	Off			✓						
Final Action	No operation			✓						
Execute Script before Final Action	Off									✓

DB2 monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
DB2 Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Level	Level 2 (monitored by update/select)			✓						
Database Name	-			✓						
Instance Name	DB2			✓						
User Name	db2admin			✓						
Password	-			✓						
Monitor Table Name	DB2WATCH			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

FTP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
FTP Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	3 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
IP Address	127.0.0.1			✓						
Port Number	21			✓						
User Name	-			✓						
Password	-			✓						
Protocol	FTP			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target				✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Destination Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

HTTP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
HTTP Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	3 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Connecting Destination	127.0.0.1			✓						
Protocol	HTTP			✓						
Port Number	80			✓						
Monitor URI	-			✓						
Request Type	HEAD			✓						
Authentication Method	No authentication			✓						
User Name	-			✓						
Password	-			✓						
Client Authentication	Off			✓						
Client Certificate Subject Name	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

IMAP4 monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
IMAP4 Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	3 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
IP Address	127.0.0.1			✓						
Port Number	143			✓						
User Name	-			✓						
Password	-			✓						
Authentication Method	AUTHENTICATELOGIN			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target				✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

ODBC monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
ODBC Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Level	Level 2 (monitored by update/select)			✓						
Data Source Name	-			✓						
User Name	-			✓						
Password	-			✓						
Monitor Table Name	ODBCWATCH			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Oracle monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Oracle Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Collect the dump file of the monitor process at timeout occurrence	Off			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Method	listener and instance monitor			✓						
Monitor Level	Level 2 (monitored by update/select)			✓						
Connect Command	-			✓						
User Name	sys			✓						
Password	-			✓						
Authority	Off			✓						
SYSDBA/DEFAULT	SYSDBA			✓						
Monitor Table Name	ORAWATCH			✓						
ORACLE_HOME	-			✓						
Character Set	(Following the setting of the application)			✓						
Collect detailed application information at failure occurrence	Off			✓						
Collection Timeout	600 seconds			✓						
Generate the monitor error during initialization or shutdown of Oracle	Off			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

POP3 monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
POP3 Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	3 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
IP Address	127.0.0.1			✓						
Authentication Method	APOP			✓						
Port Number	110			✓						
User Name	-			✓						
Password	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target				✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

PostgreSQL monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
PostgreSQL Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Level	Level 2 (monitored by update/select)			✓						
Database Name	-			✓						
IP Address	127.0.0.1			✓						
Port Number	5432			✓						
User Name	postgres			✓						
Password	-			✓						
Monitor Table Name	PSQLWATCH			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

SMTP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
SMTP Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	3 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
IP Address	127.0.0.1			✓						
Port Number	25			✓						
User Name	-			✓						
Password	-			✓						
Authentication Method	CRAM-MD5			✓						
E-mail Address	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

SQL Server monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
SQL Server Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Level	Level 2 (monitored by update/select)			✓						
Database Name	-			✓						
Instance Name	MSSQLSERVER			✓						
User Name	SA			✓						
Password	-			✓						
Monitor Table Name	SQLWATCH			✓						
ODBC Driver Name	ODBC Driver 13 for SQL			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Tuxedo monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Tuxedo Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Application Server Name	BBL			✓						
Config File	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

WebSphere monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
WebSphere Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Application Server Name	server1			✓						
Profile Name	default			✓						
User Name	-			✓						
Password	-			✓						
Install Path	C:\Program Files\IBM\WebSphere\AppServer			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

WebLogic monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
WebLogic Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	2 times			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
IP Address	127.0.0.1			✓						
Port	7002			✓						
Monitor Method	RESTful API			✓						
Protocol	HTTP			✓						
User Name	weblogic			✓						
Password	-			✓						
Add command option	-Dwlst.offline.log=disable -Duser.language=en_US			✓						
Account Shadow	Off			✓						
On: Config File	-			✓						
On: Key File	-			✓						
Off: User Name	weblogic			✓						
Off: Password	-			✓						
Authority Method	DemoTrust			✓						
Key Store File	-			✓						
Install Path	C:\Oracle\Middleware\Oracle_Home\wlserver			✓						

Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

WebOTX monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
WebOTX Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	Off			✓						
Action at Timeout Occurrence	Recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Connecting Destination	localhost			✓						
Port Number	6212			✓						
User Name	-			✓						
Password	-			✓						
Install Path	-									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 time			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	Stop cluster service and shutdown OS			✓						

JVM monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
JVM Monitor Resource Properties										
Monitor (common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Target	-			✓						
JVM Type				✓						
Identifier	-			✓						
Connection Port	-			✓						
Process Name	-			✓						
User	-			✓						
Password				✓						
Command	-			✓						
Memory Tab(when Oracle Java is selected for JVM type)										
Monitor Heap Memory Rate	On			✓						
Total Usage	80%			✓						
Eden Space	100%			✓						
Survivor Space	100%			✓						
Tenured Gen	80%			✓						
Monitor Non-Heap Memory Rate	On			✓						
Total Usage	80%			✓						
Code Cache	100%			✓						
Perm Gen	80%			✓						
Perm Gen[shared-ro]	80%			✓						
Perm Gen[shared-rw]	80%			✓						
Command	-			✓						
Memory Tab(when Oracle Java(usage monitoring) is selected for JVM Type)										
Monitor Heap Memory Usage	Off			✓						
Total Usage	0 megabytes			✓						
Eden Space	0 megabytes			✓						
Survivor Space	0 megabytes			✓						
Tenured Gen	0 megabytes			✓						
Monitor Non-Heap Memory Usage	Off			✓						
Total Usage	0 megabytes			✓						
Code Cache	0 megabytes			✓						
CodeHeap non-nmethods	0 megabytes			✓						
CodeHeap profiled	0 megabytes			✓						
CodeHeap non- profiled	0 megabytes			✓						
Compressed Class Space	0 megabytes			✓						
Metaspace	0 megabytes			✓						
Command	-			✓						
Thread Tab										
Monitor the number of Active Threads	65535 threads			✓						
Command	-			✓						
GC Tab										
Monitor the time in Full GC	65535 milliseconds			✓						
Monitor the count of Full GC execution	1 time			✓						
Command	-			✓						
WebLogic Tab										
Monitor the requests in Work Manager	Off			✓						
Target Work Managers	-			✓						
The number	65535			✓						
Average	65535			✓						
Increment from the last	80%			✓						
Monitor the requests in Thread Pool	Off			✓						
Waiting Requests, The number	65535			✓						
Waiting Requests, Average	65535			✓						
Waiting Requests, Increment from the last	80%			✓						
Executing Requests, The number	65535			✓						
Executing Requests, Average	65535			✓						
Executing Requests, Increment from the last	80%			✓						
Command	-			✓						

Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

System monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
System Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Retry Count	0 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitoring CPU usage	ON			✓						
CPU Usage	90%			✓						
Duration Time	60 minutes			✓						
Monitoring total usage of memory	ON			✓						
Total memory usage	90%			✓						
Duration Time	60 minutes			✓						
Moitoring total usage of virtual memory	ON			✓						
Total virtual memory usage	90%			✓						
Duration Time	60 minutes			✓						
Logical drive				✓						
Utilization rate	ON			✓						
Warning level	90%			✓						
Notice level	80%			✓						
Duration	1440 minutes			✓						
Free space	ON			✓						
Warning level	500 MB			✓						
Notice level	1000 MB			✓						
Duration	1440 minutes			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	zero			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Final Action	No Operation			✓						
Execute Script before Final Action	Off									✓

Process resource monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Process Resource Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	60 seconds			✓						
Retry Count	0 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)				✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Process Name	-			✓						
Monitoring CPU usage	On			✓						
CPU usage	90%			✓						
Duration Time	1440 minutes			✓						
Monitoring usage of memory	On			✓						
Rate of Increase from the First Monitoring Point	10%			✓						
Maximum Update Count	1440 times			✓						
Monitoring number of opeing files (maximum number)	Off			✓						
Refresh Count	1440 times			✓						
Monitoring number of running threads	On			✓						
Duration Time	1440 minutes			✓						
Monitoring Processes of the Same Name	Off			✓						
Count	100			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	0			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers				✓					
Execute Script before Final Action	Off									✓
Final Action	No operation				✓					

User mode monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
User mode Monitor Resource Properties										
Monitor (common) Tab										
Interval	30 seconds			✓						
Timeout	300 seconds			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitoring Method	keepalive			✓						
Action When Timeout Occurs	Generate an intentional stop error			✓						
Create a Dummy Thread	On			✓						

Dynamic DNS monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Dynamic DNS Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitoring Timing	When active (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Check Name Resolution	On			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	0 times			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

Process Name monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Process Name Monitor Resource Properties										
Monitor(common) Tab										
Interval	5 seconds			✓						
Timeout	60 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	0 time			✓						
Wait Time to Start Monitoring	3 seconds			✓						
Monitoring Timing	Always			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Process name	-			✓						
Servers that can run the Group (Add, Remove)	1			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	0 times			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No operation			✓						

AWS Elastic IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS elastic ip Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	awseip			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

AWS Virtual IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS virtual ip Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	awsvip			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

AWS Secondary IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS secondary ip Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	3 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	awssip			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

AWS AZ monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS AZ Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Availability Zone	-			✓						
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Executing failover to the recovery target			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	0 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

AWS DNS monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
AWS DNS Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	300 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	awsdns			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Monitor Resource Record Set	On									✓
Action when AWS CLI command failed to receive response	Disable recovery action(Do nothing)									
Check Name Resolution	On									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	0 time			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Azure probe port monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Azure probe port Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	azurepp			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Action when Probe port wait timeout	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Azure load balance monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Azure load balance Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Target Resource	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	0 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Specify the count. [zero]			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Azure DNS monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Azure DNS Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	60 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	azuredns			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Check Name Resolution	On									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	azuredns			✓						
Recovery Script Execution Count	0 time			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Google Cloud Virtual IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Google Cloud Virtual IP Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	gcvip			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Health Check Timeout Operation	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Google Cloud load balance monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Google Cloud load balance Monitor Resource										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Target Resource	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	0 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Specify the count. [zero]			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Oracle Cloud Virtual IP monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Oracle Cloud Virtual IP Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	ocvip			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Health Check Timeout Operation	Disable recovery action(Do nothing)			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Google Cloud DNS monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Google Cloud DNS Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	120 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	3 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	gcdns			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	0 time			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Oracle Cloud load balance monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Oracle Cloud load balance Monitor Resource										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	0 seconds			✓						
Monitor Timing	Always (fixed)			✓						
Target Resource	-			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Target Resource	-			✓						
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	-			✓						
Recovery Script Execution Count	zero			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	0 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Specify the count. [zero]			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

Oracle Cloud DNS monitor resource

Parameters	Default	How to change								
		1	2	3	4	5	6	7	8	9
Oracle Cloud DNS Monitor Resource Properties										
Monitor(common) Tab										
Interval	60 seconds			✓						
Timeout	180 seconds			✓						
Do Not Retry at Timeout Occurrence	On			✓						
Action at Timeout Occurrence	Do not recover			✓						
Retry Count	1 time			✓						
Wait Time to Start Monitoring	300 seconds			✓						
Monitor Timing	Active (fixed)			✓						
Target Resource	ocdns			✓						
Failure Detection Server										
Failure Detection Server	All Servers			✓						
Servers that can run the Group (Add, Remove)	-			✓						
Send polling time metrics	Off									✓
Monitor (special) Tab										
Check Name Resolution	On									✓
Recovery Action Tab										
Recovery Action	Custom settings			✓						
Recovery Target	ocdns			✓						
Recovery Script Execution Count	0 time			✓						
Execute Script before Reactivation	Off									✓
Maximum Reactivation Count	3 times			✓						
Execute Script before Failover	Off									✓
Failover Target Server	Stable Server			✓						
When [Server] is selected for [Failover Count Method]										
Maximum Failover Count	1 time			✓						
When [Cluster] is selected for [Failover Count Method]										
Maximum Failover Count	Set as much as the number of the servers			✓						
Execute Script before Final Action	Off									✓
Final Action	No Operation			✓						

2.9 Upper limits of registration

	Version	You can register up to
Cluster	12.00 or later	1
Server	12.00 or later	32
Server Group	12.00 or later	9
Group	12.00 or later	128
Group resource (Per one group)	12.00 or later	512
Monitor resource	12.00 or later	384
Heartbeat resource	12.00 or later	16
Witness heartbeat resource	12.10 or later	1
Network Partition Resolution Resource	12.00 or later	64
Mirror disk resources and hybrid disk resources (Per cluster) in total	12.00 or later	22
Mirror Disk Connect	12.00 or later	16

CHAPTER

THREE

GROUP RESOURCE DETAILS

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

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

This chapter covers:

3.1 Group resources

Currently supported group resources are as follows:

Group resource name	Abbreviation	Functional overview
Application resources	appli	Refer to "*Understanding application resources*".
Floating IP resources	fip	Refer to "*Understanding floating IP resources*".
Mirror disk resources	md	Refer to "*Understanding mirror disk resources*".
Registry synchronization resources	regsync	Refer to "*Understanding registry synchronization resources*".
Script resources	script	Refer to "*Understanding script resources*".
Disk resources	sd	Refer to "*Understanding disk resources*".
Service resources	service	Refer to "*Understanding service resources*".
Virtual computer name resources	vcom	Refer to "*Understanding virtual computer name resources*".
Dynamic DNS resources	ddns	Refer to "*Understanding dynamic DNS resources*".
Virtual IP resources	vip	Refer to "*Understanding virtual IP resources*".
CIFS resources	cifs	Refer to "*Understanding CIFS resources* ".
Hybrid disk resource	hd	Refer to "*Understanding hybrid disk resources*".
AWS elastic ip resource	awseip	Refer to "*Understanding AWS elastic ip resources*".
AWS virtual ip resource	awsvip	Refer to "*Understanding AWS virtual ip resources*".
AWS secondary ip resource	awssip	Refer to "*Understanding AWS secondary ip resources*".
AWS DNS resource	awsdns	Refer to "*Understanding AWS DNS resources*".
Azure probe port resource	azurepp	Refer to "*Understanding Azure probe port resources*".
Azure DNS resource	azuredns	Refer to "*Understanding Azure DNS resources*".
Google Cloud virtual IP resource	gcvip	Refer to "*Understanding Google Cloud virtual IP resources*".
Google Cloud DNS resource	gcdns	Refer to "*Understanding Google Cloud DNS resources*".
Oracle Cloud virtual IP resource	ocvip	Refer to "*Understanding Oracle Cloud virtual IP resources*".
Oracle Cloud DNS resource	ocdns	Refer to "*Understanding Oracle Cloud DNS resources*".

3.2 What is a group?

A group is a unit to perform a failover. Rules regarding to operations at failover (failover policies) can be set per group.

3.2.1 Understanding the group types

Groups fall into the following type.

- **Failover group**
  Collects the resources required for application continuation and performs failover for each application. Up to 256 group resources can be registered with each group.

3.2.2 Understanding the group properties

The properties that can be set on each group are described below:

- **Servers that can run the Group**
  Select and set the servers that can run the group from the servers that configure a cluster. Specify the order of priority to the servers that can run the group for running the group.
- **Startup Attribute**
  Sets the startup attribute of a group to the auto startup or manual startup.
  In the case of the auto startup, when a cluster is started, a group is started up automatically on the server that has the highest priority among the servers that can run the group.
  In the case of the manual startup, a group is not started even when a server is started up. After starting the server, start up the group manually by using the Cluster WebUI or the clpgrp command. For details on the Cluster WebUI, see online manual. For details on the clpgrp command, see "Operating groups (clpgrp command)" in "EXPRESSCLUSTER command reference" in this guide.
- **Failover Attribute**
  Specify the failover method. The following failover attributes can be specified.

  Auto 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
    When failover is executed due to the error detection of the group resource or monitor resource, the failover destination settings of the resource is used (stable server/ the server that has the highest priority). Also, when failing over is executed due to the timeout detection of the heartbeat, the failover destination is determined following the priority of the server set as servers that can run the group.
    For the operation when a stable server or the server that has the highest priority is used, see "Recovery Operation tab" and "Recovery Action tab".
  - 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 critical monitor resource	Error (all servers)	When there is no failover destination, proceed to failover judgment process while ignoring errors of critical monitor resources.
	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 failover while ignoring errors of critical monitor resources	Set	Proceed to the process that ignores the status of the critical monitor resource and which compares error levels for all the activated servers.
	Not set	Failover is not performed.
Number of servers that have the lowest error level	1	The server with the lowest error level is used as the failover destination.
	Two or more	Proceed to the process that judges whether there is a server that can perform a failover in the server that has the lowest error level and that is in the same server group as the failover source.
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 a 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 3.2 – 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 operation level judgment process.
	Not set	Proceed to the operation level judgment process.
Number of servers with the lowest operation level	1	The server that has the lowest operation level is used as the failover destination.
	Two or more	The running server that has the highest priority is used as the failover destination.

Note:

Critical monitor resource
Exclude the server which is detecting the error by a monitor resource from the failover destination.
The monitor that is used can be set with the Cluster WebUI.

Error level
This is the number of monitor resources that have 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 resource must be set as the monitor resource. For details on the system resource monitor, see "Understanding system monitor resources" in "Monitor resource details" in this guide.

Operation level
This is the number of failover groups that have been started or are being started, excluding management group.

- 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. 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.
  When failover is executed due to the error detection of the group resource or monitor resource, the failover destination settings of the resource is used (stable server/ the server that has the highest priority). Also, when failing over is executed due to the timeout detection of the heartbeat, the failover destination is determined following the priority of the server set as servers that can run the group.
- 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

Failover is not automatically performed when a heartbeat is timed out. In that case, perform failover manually by using the Cluster WebUI or the clpgrp command. However, even if manual failover is specified, a failover is performed automatically when an error is detected by a group or monitor resource.

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.

- **Failover Attribute (Advanced)**

  Allows an advanced configuration of the automatic failover method specified in **Failover Attribute**.

  Available options are as follows:

  - Exclude server with error detected by specified monitor resource, from failover destination

    A server with error detected by the specified monitor resources is excluded from the failover destination.

    This option can be enabled or disabled by selecting **Use the startup server settings** or **Prioritize failover policy in the server group** in **Failover Attribute**.

    This option is automatically enabled by selecting **Fail over dynamically** in **Failover Attribute**.

  - Failover with error ignored if it is detected in all servers

    This option is selectable only with the above **Exclude server with error detected by specified monitor resource, from failover destination** selected.

    The failover destination is determined regardless of errors detected in all servers (i.e., no failover destination) by the monitor resource.

- **Failback Attribute**

  Set either auto failback 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**.

  In the case of the auto failback, failback will be automatically performed when the server that is given the highest priority is started after a failover.

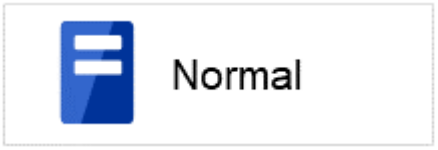
  In the case of the manual failback, a failback is not performed even if a server is started.

3.2.3 Understanding failover policy

A failover policy is a rule that determines a server to be the failover destination from multiple servers, and it is defined by the properties of a group. When you configure the failover policy, avoid making certain servers more 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
	Normal (properly working as a cluster)
	Suspended (not recovered as a cluster yet)
	Stopped (cluster is stopped)

3-node configuration:

Group	Order of server priorities		
	1st priority server	2nd priority server	3rd priority server
A	Server 1	Server 3	Server 2
B	Server 2	Server 3	Server 1

2-node configuration:

Group	Order of server priorities	
	1st priority server	2nd priority server
A	Server 1	Server 2
B	Server 2	Server 1

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. It is also assumed that the servers are configured not to recover automatically from the status of being suspended. Whether to perform auto recovery from the suspended status is set ON/OFF of **Auto Return** on the **Extension** tab in **Cluster Properties.**

- 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".

- The failover priority of the management group is determined by the server priority. You can specify server priority on the **Master Server** tab in **Cluster Properties**.

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

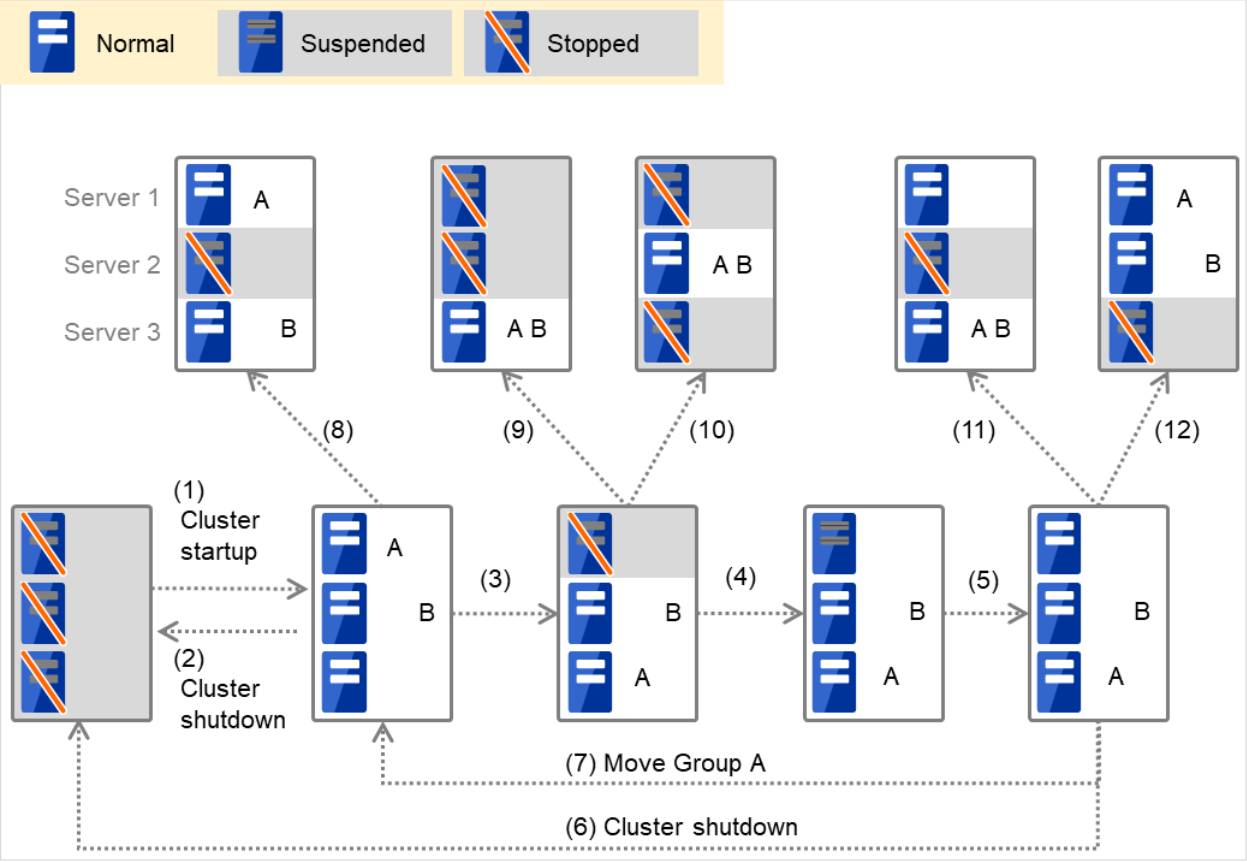


Fig. 3.1: Servers' statuses, and servers on which Groups A and B are started up

1. Cluster startup
2. Cluster shutdown
3. Failure of Server 1: Fails over to the next priority server.
4. Server1 power on
5. Server1 cluster recovery
6. Cluster shutdown
7. Move Group A
8. Failure of Server 2: Fails over to the next priority server.
9. Failure of Server 2: Fails over to the next priority server.
10. Failure of Server 3: Fails over to the next priority server
11. Failure of Server 2: Fails over to the next priority server.
12. Failure of Server 2: 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:

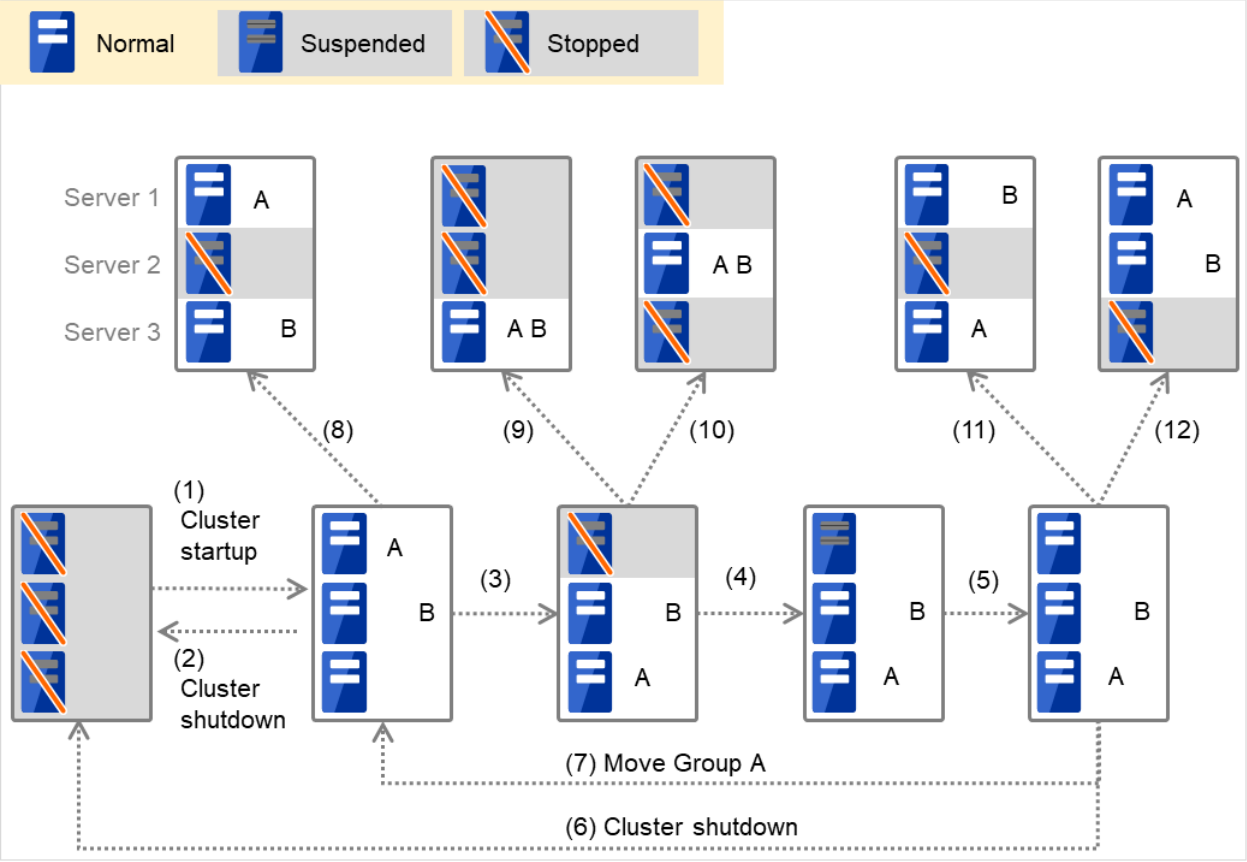


Fig. 3.2: Servers' statuses, and servers on which Groups A and B (normal exclusive groups) are started up

1. Cluster startup
2. Cluster shutdown
3. Failure of Server 1: Fails over to a server where no normal exclusive group is active.
4. Server1 power on
5. Server1 cluster recovery
6. Cluster shutdown
7. Move group A
8. Failure of Server 2: Fails over to a server where a normal exclusive group is not active.
9. Failure of Server 2: 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 Server 3: 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.
11. Failure of Server 2: Fails over to a server where a normal exclusive group is not active.
12. Failure of Server 3: 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:

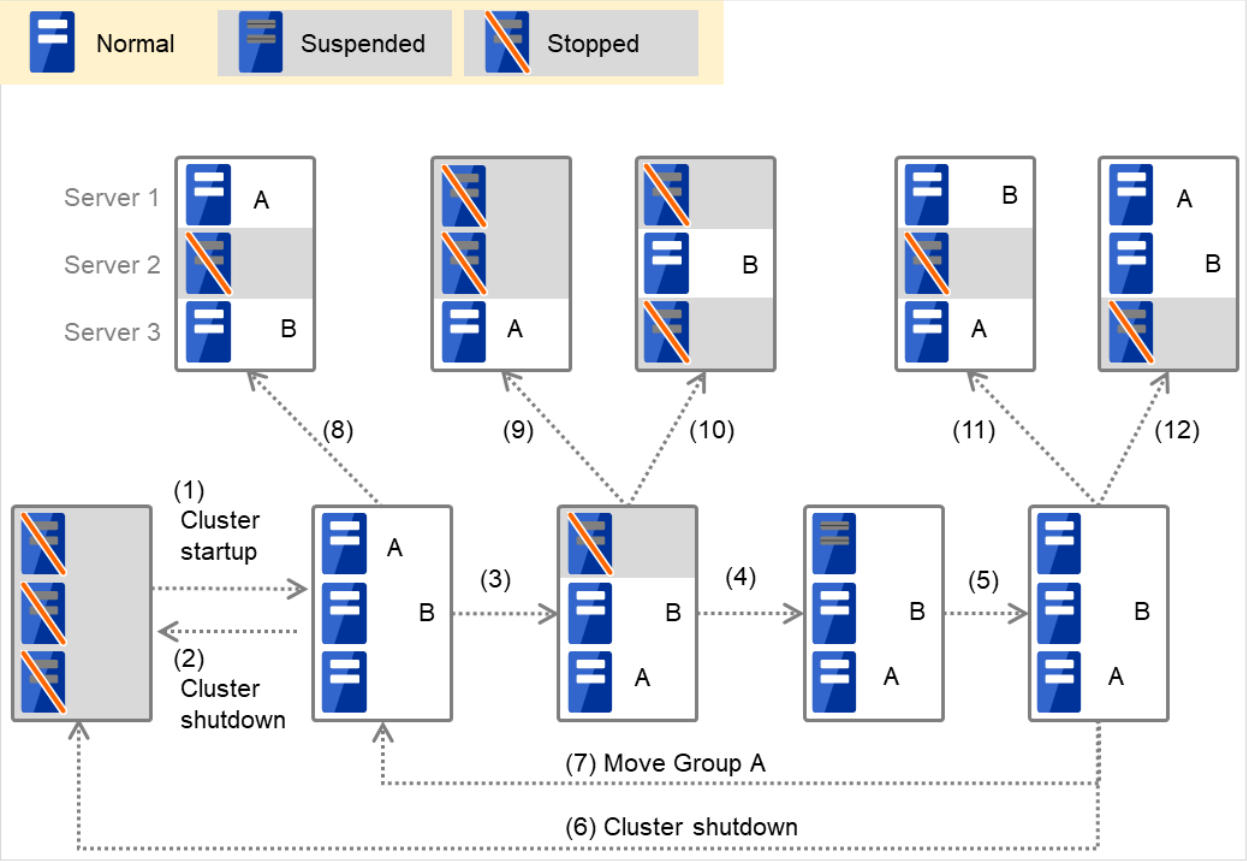


Fig. 3.3: Servers' statuses, and servers on which Groups A and B (absolute exclusive groups) are started up

1. Cluster startup
2. Cluster shutdown
3. Failure of Server 1: Fails over to the next priority server.
4. Server1 power on
5. Server1 cluster recovery
6. Cluster shutdown
7. Move group A
8. Failure of Server 2: Fails over to the next priority server.
9. Failure of Server 2: Does not failover (Group B stops).
10. Failure of Server 3: Does not failover (Group A stops).
11. Failure of Server 2: Fails over to the server where no absolute exclusive group is active.
12. Failure of Server 3: Fails over to the server where no absolute exclusive group is active.

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

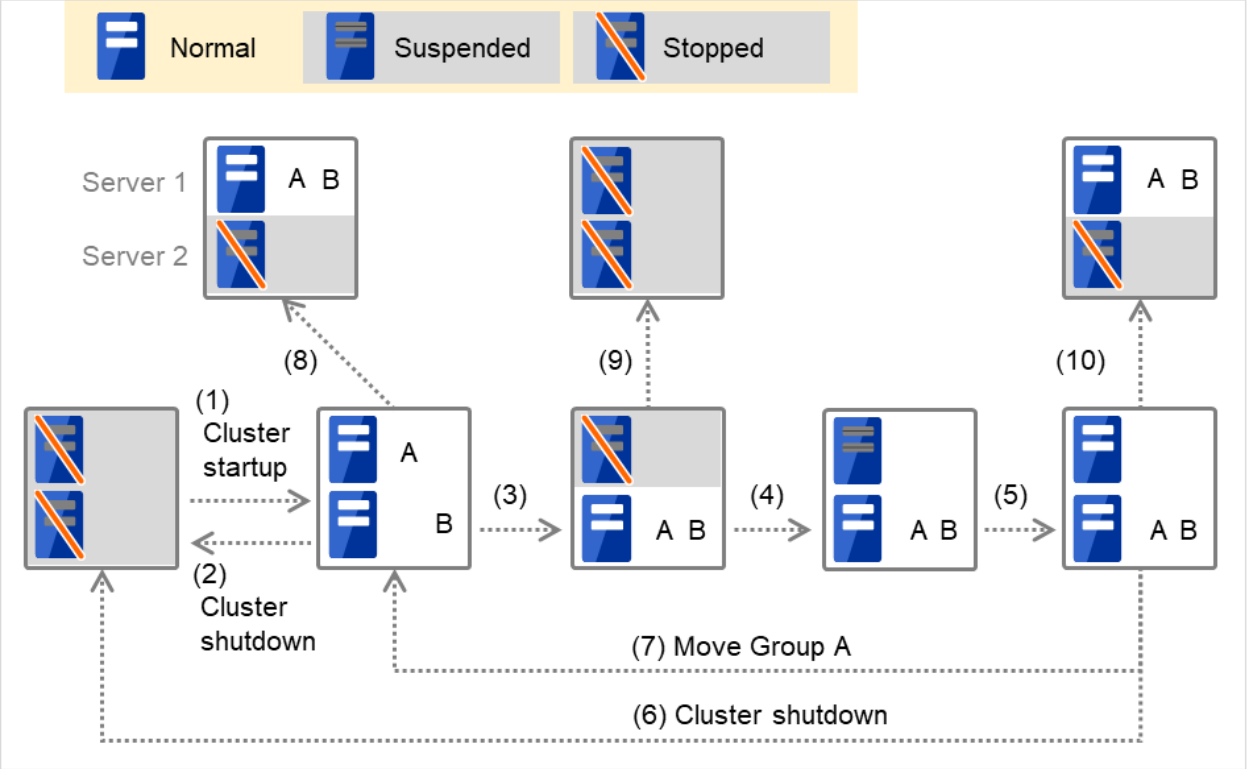


Fig. 3.4: Servers' statuses, and servers on which Groups A and B are started up (with Replicator)

1. Cluster startup
2. Cluster shutdown
3. Failure of Server 1: Fails over to the standby server of Group A.
4. Server1 power on
5. Server1 cluster recovery
6. Cluster shutdown
7. Move group A
8. Failure of Server 2: Fails over to the standby server of Group B.
9. Failure of Server 2
10. Failure of Server 2: 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.
  - W hen activation retries fail as many times as the number set to **Retry Count at Activation Failure**, a failover to the server specified in **Failover destination** takes place.
  - If the failover fails as many times as the number set to **Failover Threshold**, the action configured in **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 action configured in **Final Action** is performed.

Note:

When **Server** is selected for **Failover Count Method**:
Failover Threshold is the upper limit of failover count of a server because the number of failovers is recorded per server.
In a server in which the group activation is completed successfully, the failover count is reset.
An unsuccessful recovery action is also counted into failover count.

When **Cluster** is selected for **Failover Count Method**:
Failovers are counted on a server basis. **Failover Threshold** is the maximum failover count on a server.
The failover count is reset after the group has activated and the normal status continues for 10 minutes.
An unsuccessful recovery action is also counted into failover count.

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

When the following settings are made: (**Failover Count Method: Server**)

Retry Count at Activation Failure 3 times
Failover Threshold 1 time
Final Action Stop Group

(1) The following figure illustrates that Servers 1 and 2 are connected to the shared disk.
With Failover group A on Server 1, Disk resource 1 will start to be activated (e.g. for mounting the file system).

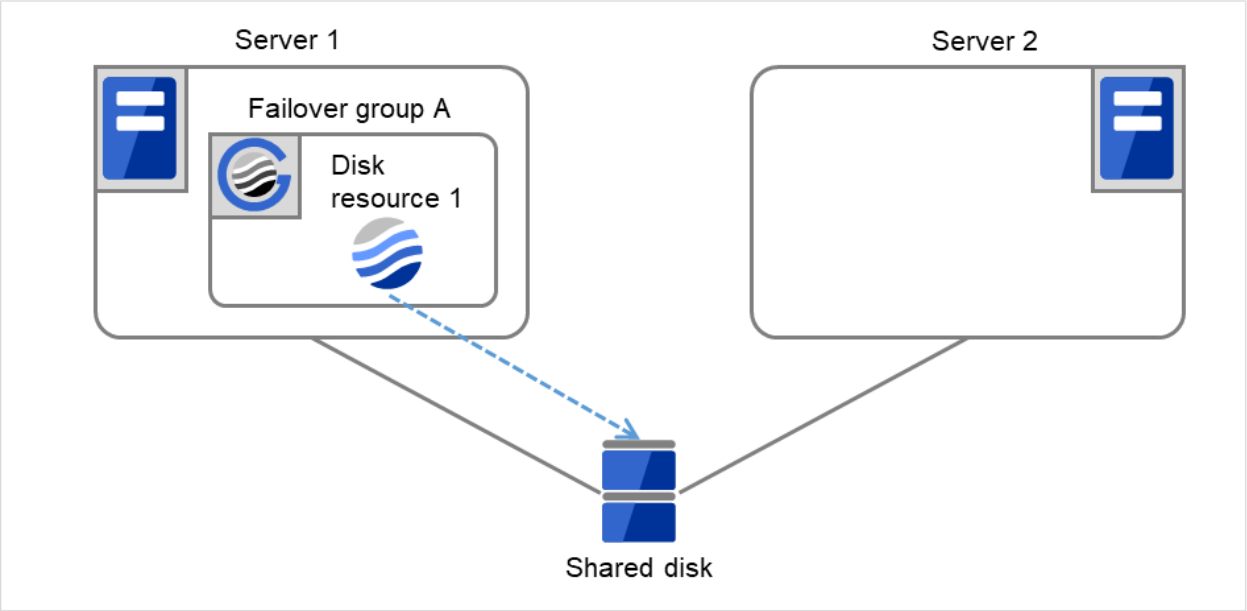


Fig. 3.5: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (1)

(2) The activation of Disk resource 1 fails due to a mounting error for a disk path failure or another cause.

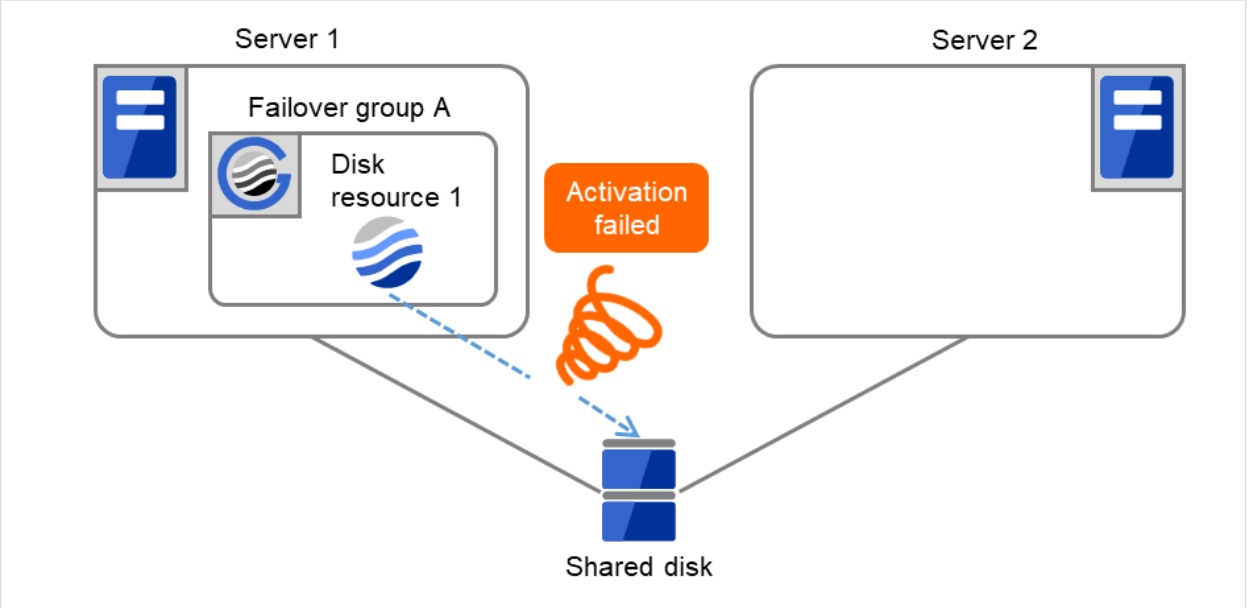


Fig. 3.6: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (2)

(3) The activation of Disk resource 1 is retried up to three times (activation retry count).

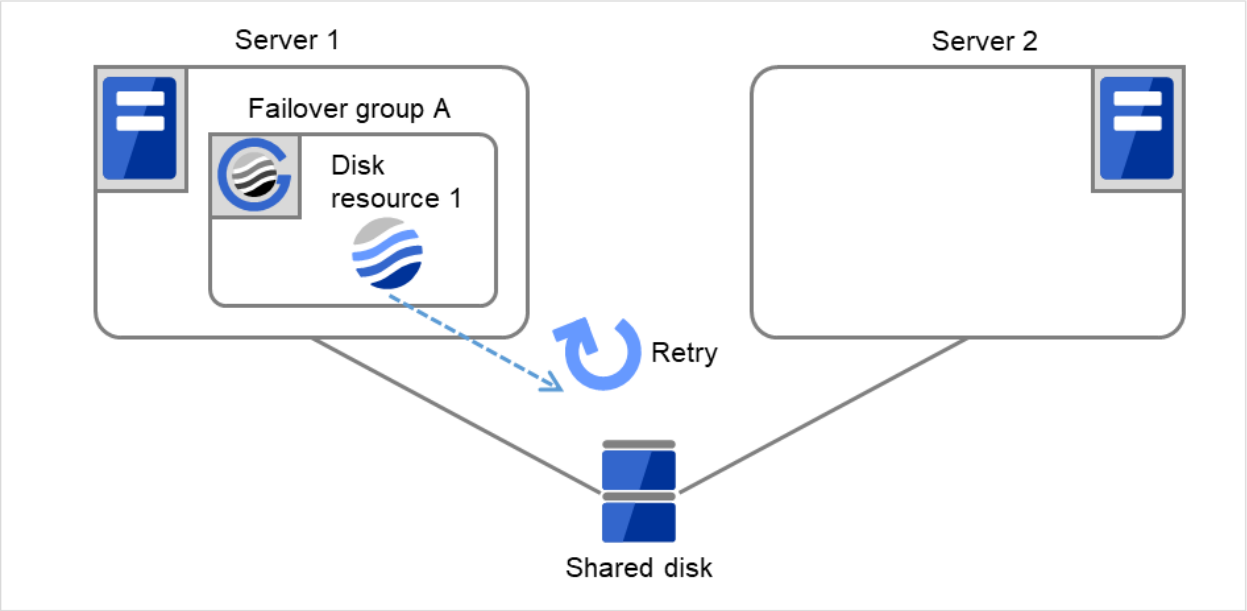


Fig. 3.7: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (3)

(4) Failover group A starts to be failed over.
Failover Threshold represents how many times failover is performed on each server.
This is the first failover on Server 1.

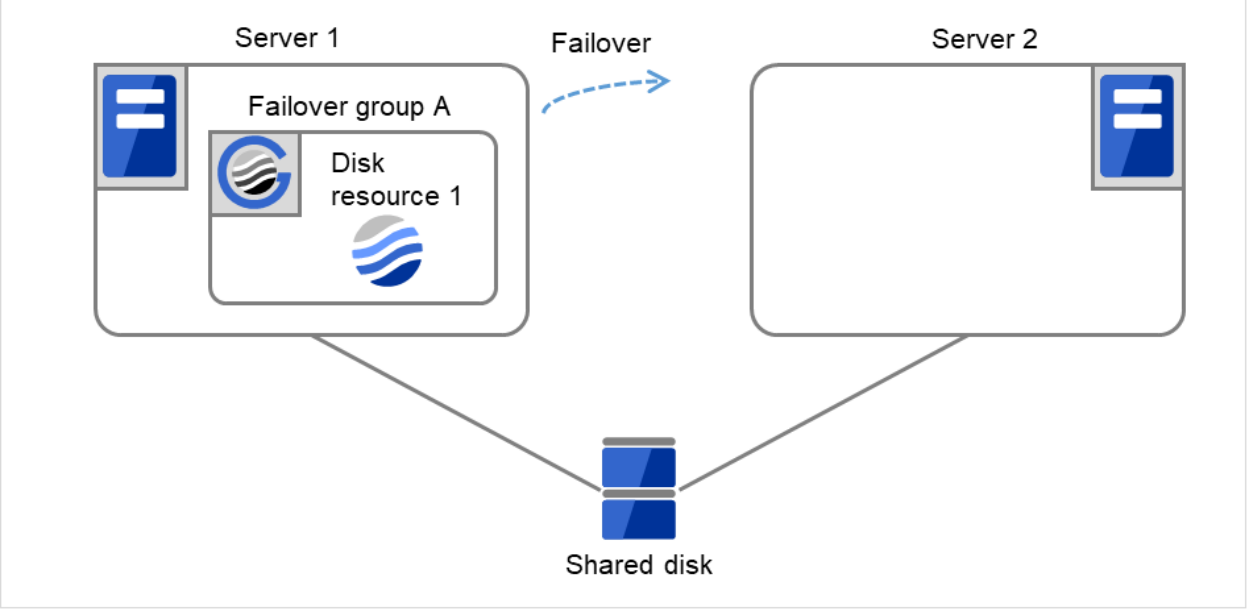


Fig. 3.8: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (4)

(5) Disk resource 1 starts to be activated (e.g. for mounting the file system).
If a failure occurs on the way, the activation is retried up to three times.

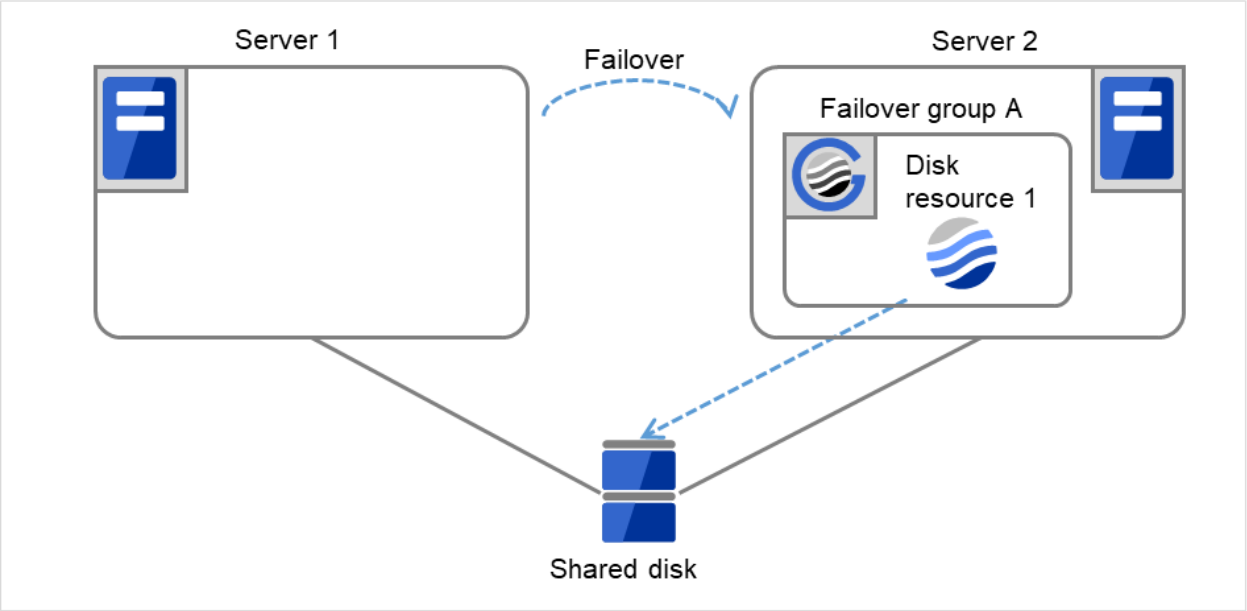


Fig. 3.9: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (5)

(6) If the specified retry count is exceeded for the activation of Disk resource 1 on Server 2 as well, Failover group A starts to be failed over.
This is the first failover on Server 2.

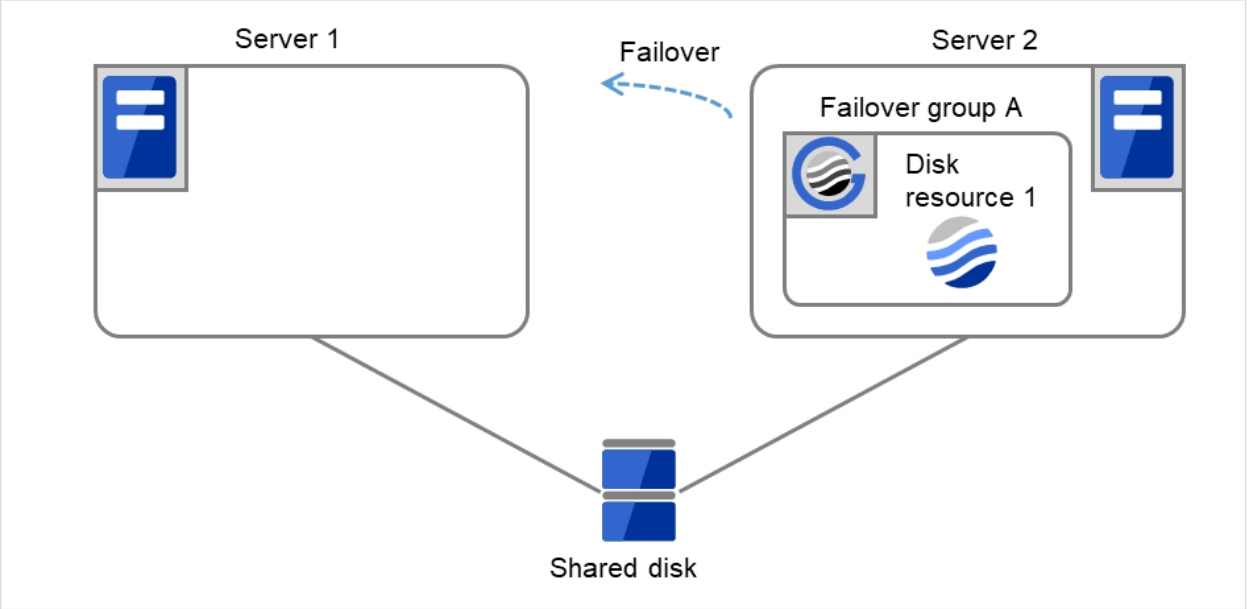


Fig. 3.10: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (6)

(7) On Server 1, Disk resource 1 starts to be activated. If a failure occurs on the way, the activation is retried up to three times.

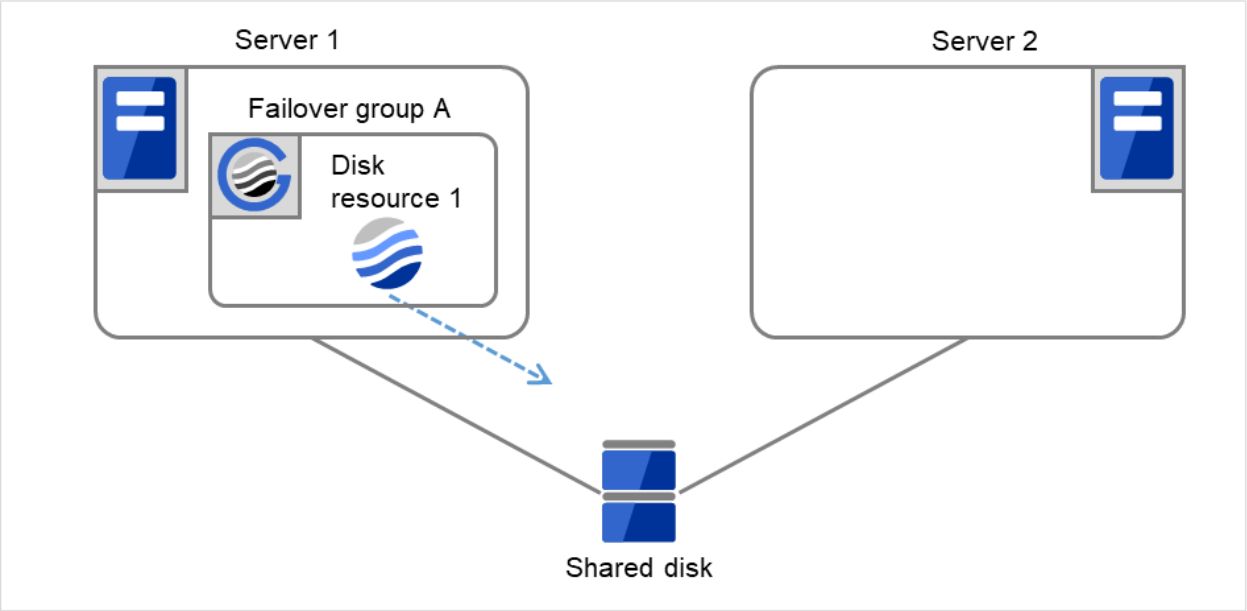


Fig. 3.11: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (7)

(8) If the specified retry count is exceeded for the activation of Disk resource 1 on Server 1 as well, the specified **Final Action** is started. No failover is performed then, because **Failover Threshold** is set at 1.
Final Action means the action to be taken after the specified failover retry count is exceeded.
Here, Failover group A starts to be stopped.

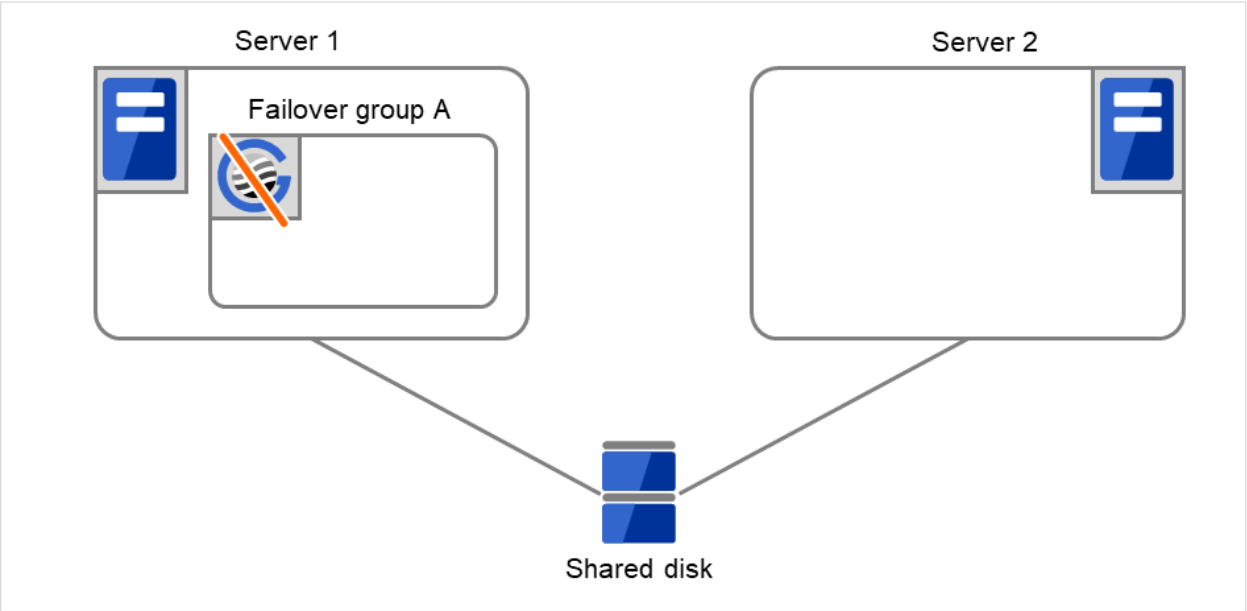


Fig. 3.12: Flow of operation on detecting a group resource activation failure (Failover Count Method: Server) (8)

When the following settings are made: (**Failover Count Method: Cluster**)

Retry Count at Activation Failure 3 times
Failover Threshold The same number as the number of servers (In the following case, 2 times)
Final Action Stop Group

(1) The following figure illustrates that Servers 1 and 2 are connected to the shared disk.
With Failover group A on Server 1, Disk resource 1 will start to be activated (e.g. for mounting the file system).

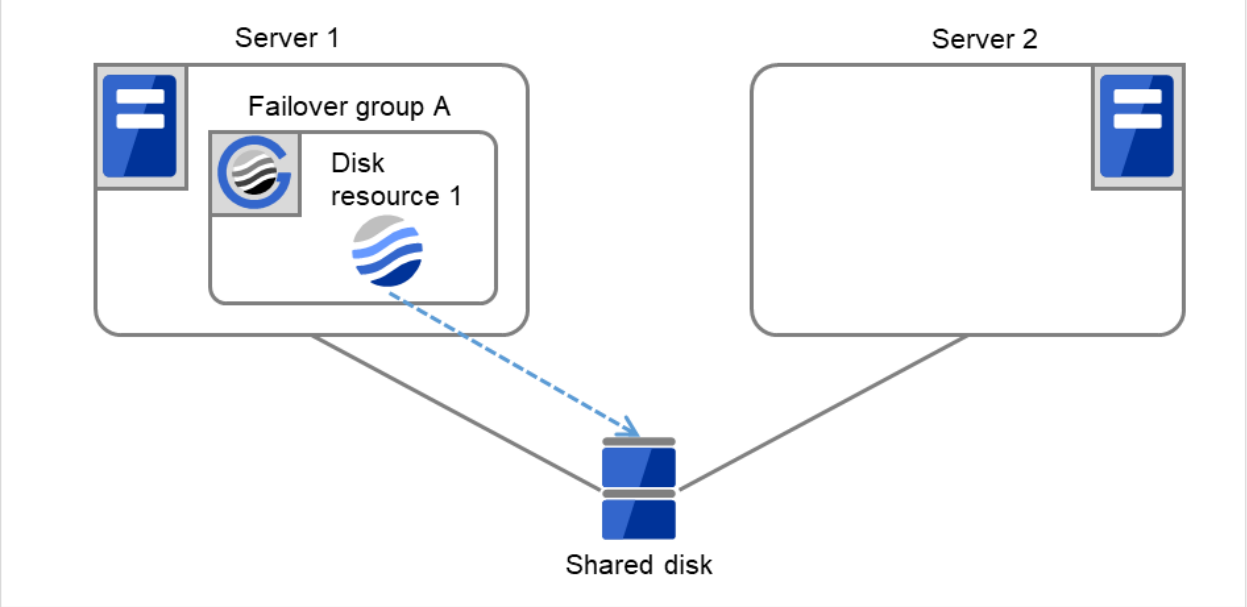


Fig. 3.13: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (1)

(2) The activation of Disk resource 1 fails due to a mounting error for a disk path failure or another cause.

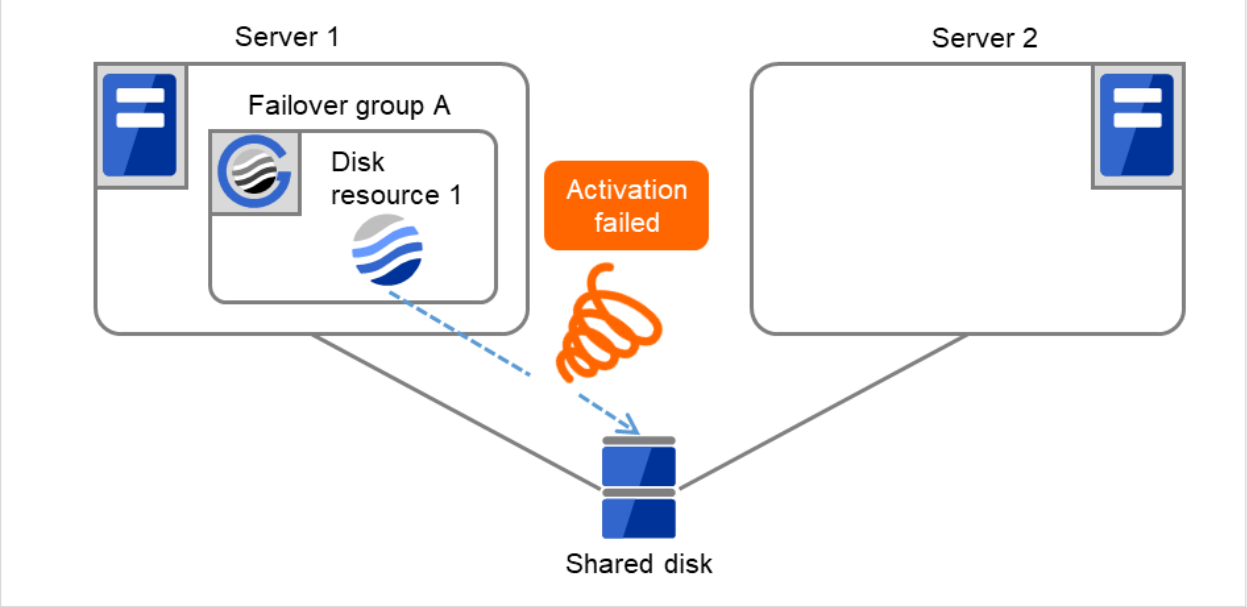


Fig. 3.14: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (2)

(3) The activation of Disk resource 1 is retried up to three times (activation retry count).

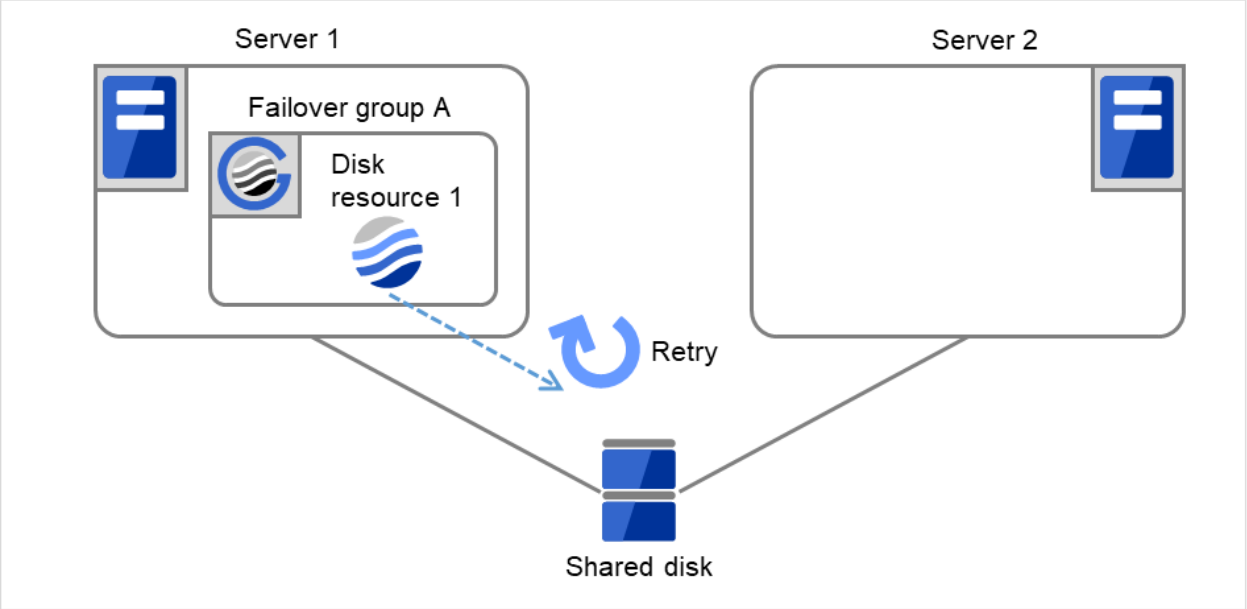


Fig. 3.15: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (3)

(4) Failover group A starts to be failed over. **Failover Threshold** represents how many times failover is performed on each server. This is the first failover on this cluster.

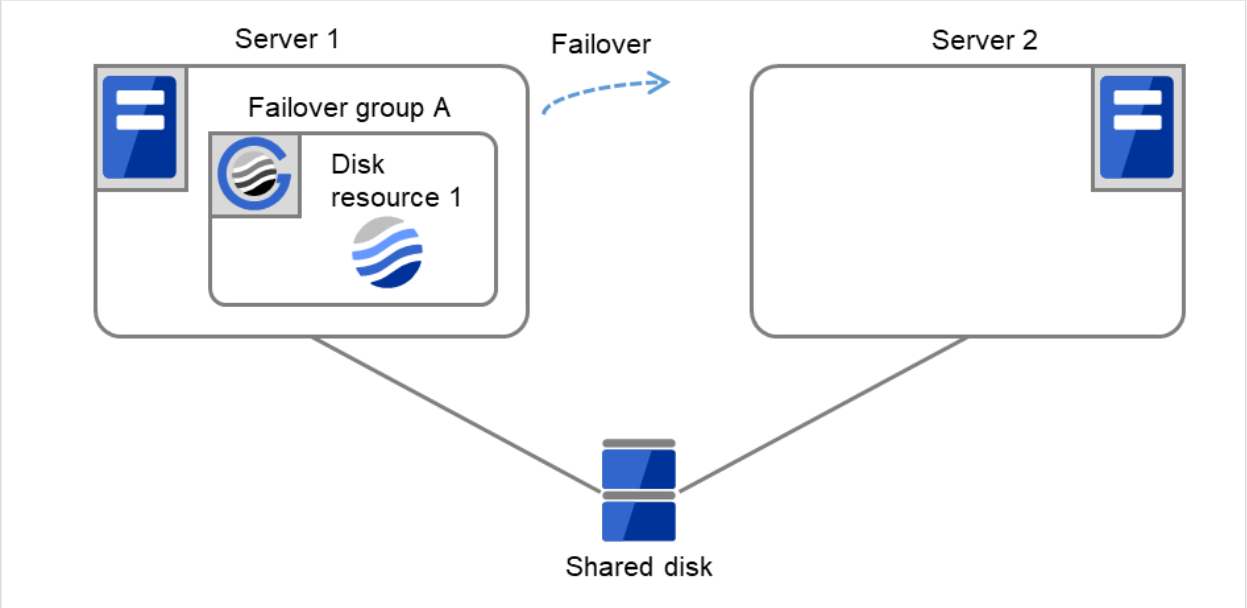


Fig. 3.16: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (4)

(5) Disk resource 1 starts to be activated (e.g. for mounting the file system). If a failure occurs on the way, the activation is retried up to three times.

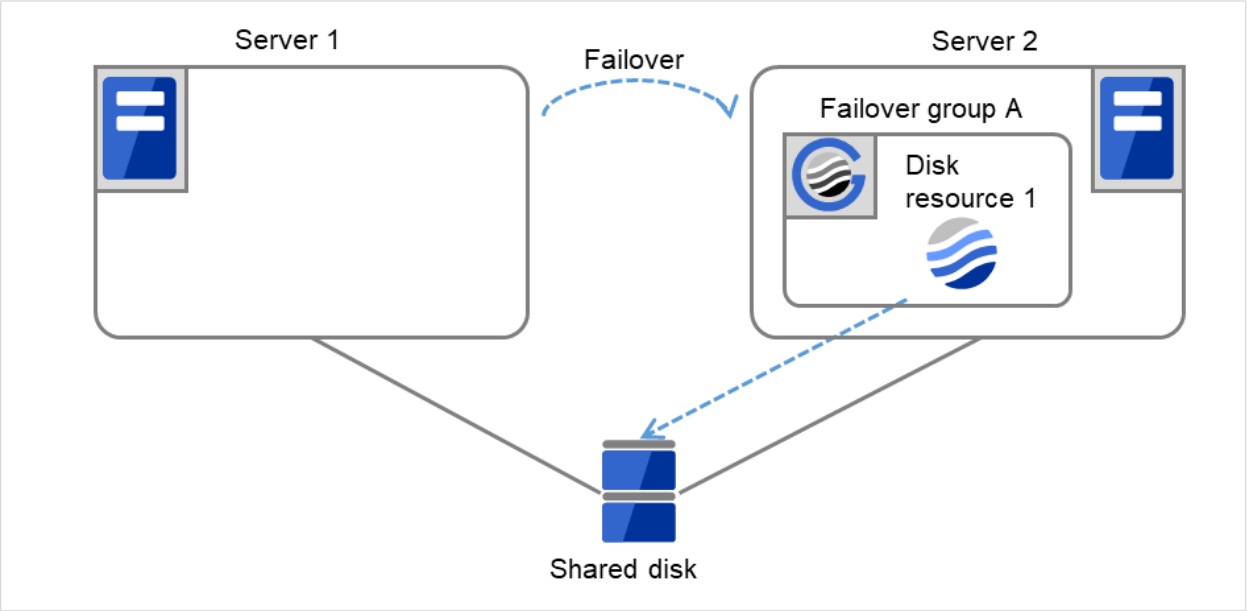


Fig. 3.17: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (5)

(6) If the specified retry count is exceeded for the activation of Disk resource 1 on Server 2 as well, Failover group A starts to be failed over. This is the second failover on this cluster.

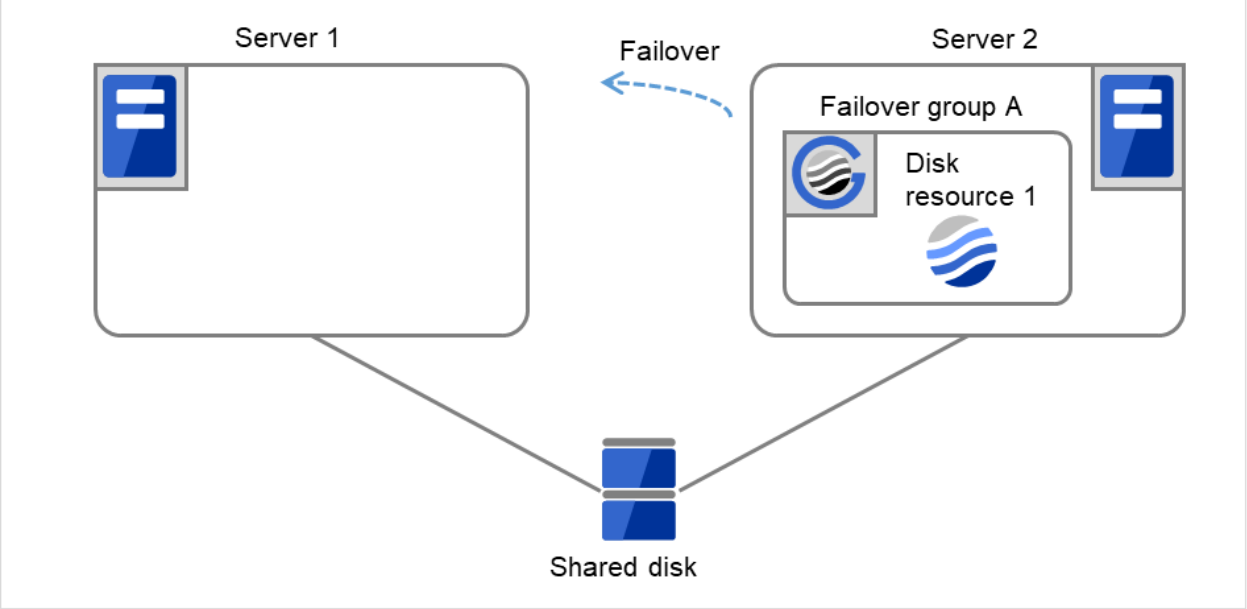


Fig. 3.18: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (6)

(7) On Server 1, Disk resource 1 starts to be activated. If a failure occurs on the way, the activation is retried up to three times.

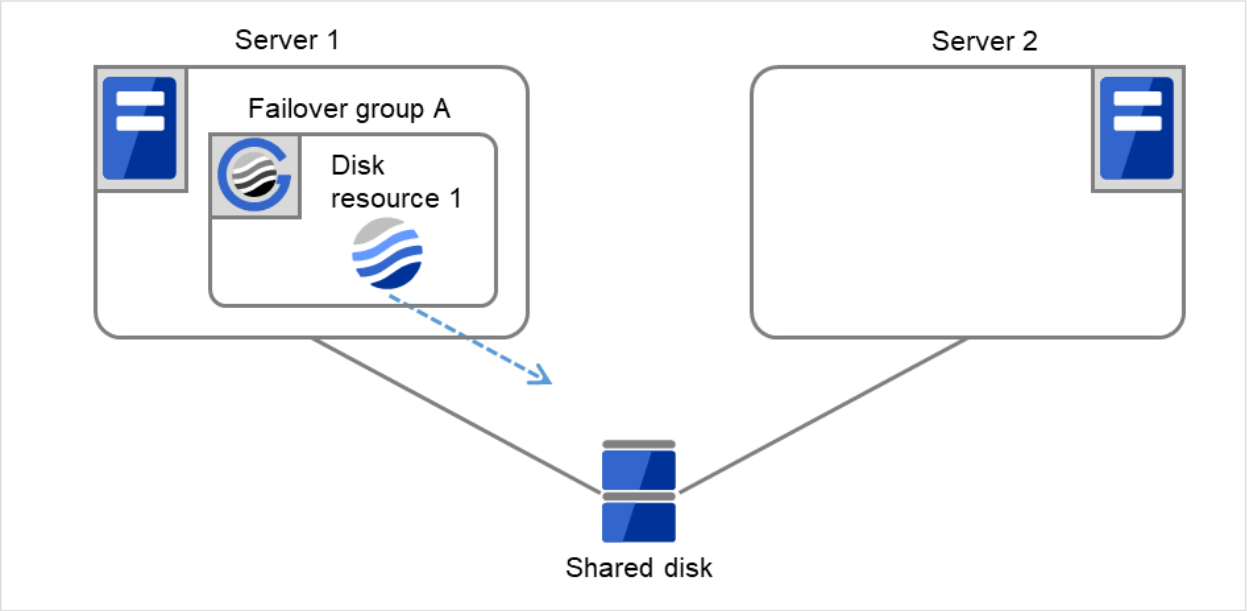


Fig. 3.19: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (7)

(8) If the specified retry count is exceeded for the activation of Disk resource 1 on Server 1 as well, the specified **Final Action** is started. No failover is performed then, because **Failover Threshold** is set at 2. **Final Action** means the action to be taken after the specified failover retry count is exceeded. Here, Failover group A starts to be stopped.

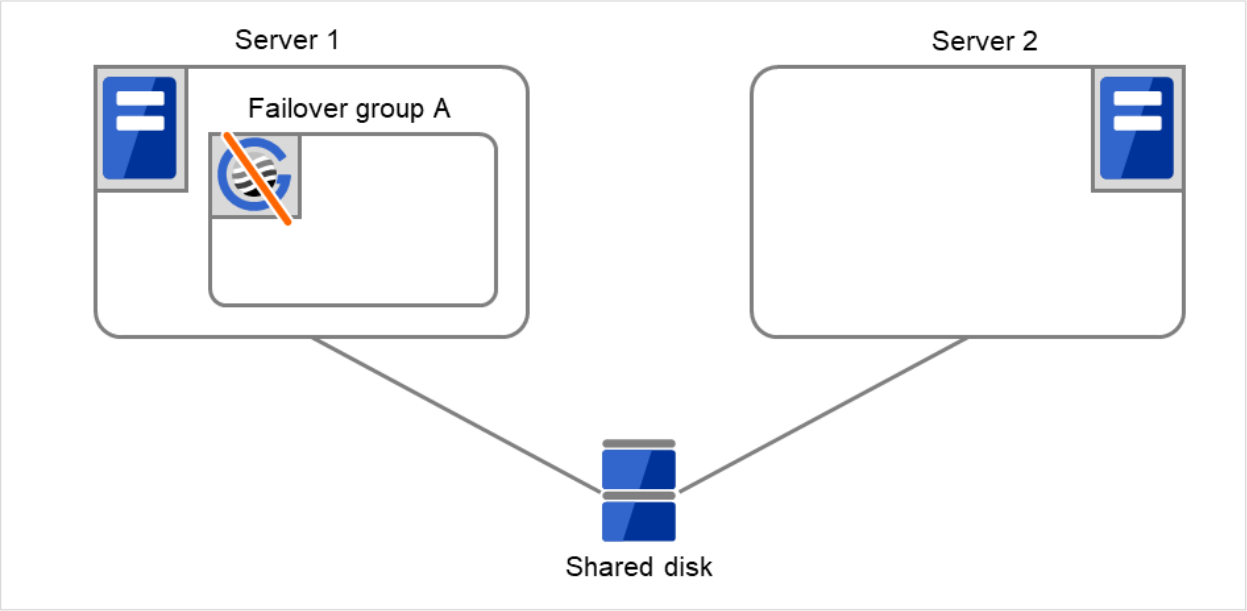


Fig. 3.20: Flow of operation on detecting a group resource activation failure (Failover Count Method: Cluster) (8)

3.2.5 Final action

When activation fails even though the failover performed as many times as the number set to **Failover Threshold**, the action configured in **Final Action** is performed. The final action can be selected from the following operations.

- **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 which the group resource that an activation error is detected belongs.
- **Stop cluster service**
  Stops the EXPRESSCLUSTER Server service of the server that an activation error is detected.
- **Stop the cluster service and shutdown OS**
  Stops the EXPRESSCLUSTER Server service of the server that an activation error is detected, and shuts down the OS.
- **Stop cluster service and reboot OS**
  Stops the EXPRESSCLUSTER Server service of the server that an activation error is detected, and reboots the OS.
- **Generating of intentional Stop Error**
  Generate a stop error intentionally on the server that an activation error is detected.

3.2.6 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.

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 deactivation error

```
rem ****************************************
rem *            predeactaction.bat            *
rem ****************************************

echo START

rem Refer to the environment variable of the script execution factor
rem to determine the subsequent process.
IF "%CLP_TIMING%"=="STOP" GOTO NORMAL

rem ****************************************
rem CLP_TIMING is not STOP (Error)
rem ****************************************
echo NO_CLP
GOTO EXIT

rem ****************************************
rem CLP_TIMING is STOP
rem ****************************************
:NORMAL
echo %CLP_GROUPNAME%
echo %CLP_RESOURCENAME%

rem Here, write a recovery process to be performed.

:EXIT
echo EXIT
```

Tips for creating a script before final action

Using clplogcmd, you can output messages to the Alert logs of Cluster WebUI.

Notes on script before final action

- 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.

3.2.7 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

```
rem ***************************************************
rem *                    rscextent.bat                *
rem ***************************************************

echo START
IF "%CLP_TIMING%"=="PRESTART" GOTO PRESTART
IF "%CLP_TIMING%"=="POSTSTART" GOTO POSTSTART
IF "%CLP_TIMING%"=="PRESTOP" GOTO PRESTOP
IF "%CLP_TIMING%"=="POSTSTOP" GOTO POSTSTOP

:PRESTART
echo %CLP_GROUPNAME%
echo %CLP_RESOURCENAME%
rem Here, write any process to be performed before the resource activation.
rem

GOTO EXIT

:POSTSTART
echo %CLP_GROUPNAME%
```

(continues on next page)

(continued from previous page)

```
echo %CLP_RESOURCENAME%
rem Here, write any process to be performed after the resource activation.
rem

GOTO EXIT

:PRESTOP
echo %CLP_GROUPNAME%
echo %CLP_RESOURCENAME%
rem Here, write any process to be performed before the resource deactivation.
rem

GOTO EXIT

:POSTSTOP
echo %CLP_GROUPNAME%
echo %CLP_RESOURCENAME%
rem Here, write any process to be performed after the resource deactivation.
rem

GOTO EXIT

:EXIT
```

Tips for creating a script before and after activation/deactivation

Using clplogcmd, you can output messages to the Alert logs of Cluster WebUI.

Notes on script before and after activation/deactivation

None.

3.2.8 Reboot count limit

If **Stop cluster service and shutdown OS** or **Stop cluster service and reboot OS** 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 monitor resources are recorded separately.
If the time to reset the maximum reboot count is set to zero (0), the reboot count is not reset. To reset the reboot count, use the clpregctrl command.

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

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

If the EXPRESSCLUSTER Server service is started successfully after rebooting OS, 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
Failover Threshold 0
Final Action Stop cluster service and reboot OS
Max Reboot Count 1
Max Reboot Count Reset Time 10 minutes

(1) The following figure illustrates that Servers 1 and 2 are connected to the shared disk.
With Failover group A on Server 1, Disk resource 1 will start to be activated (e.g. for mounting the file system).

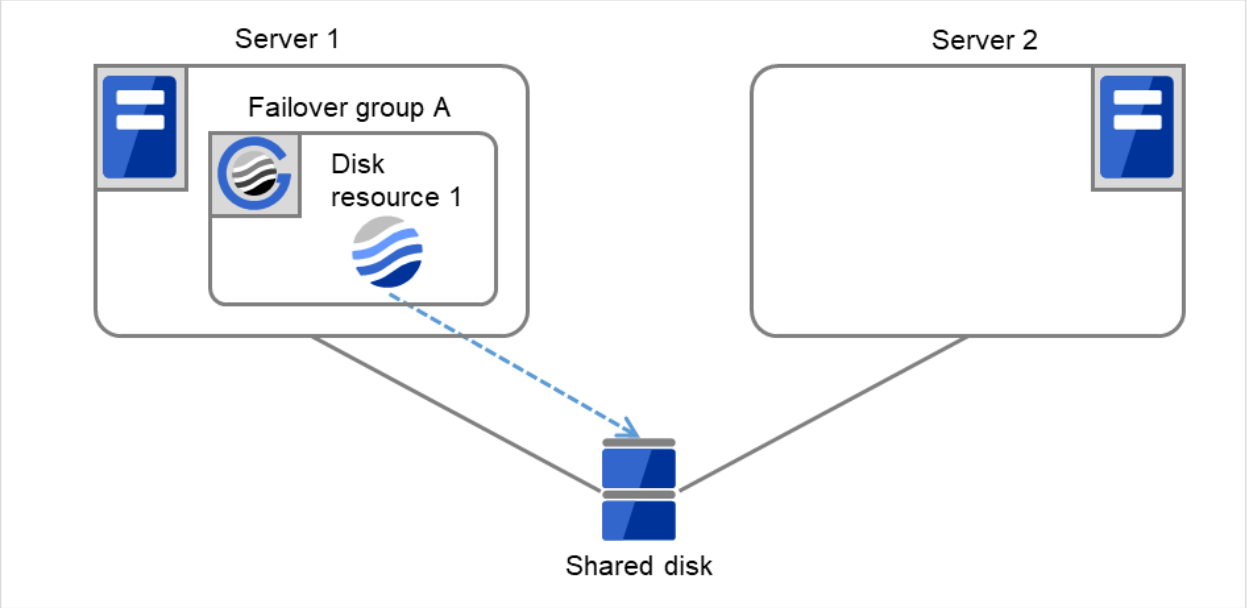


Fig. 3.21: Process with the limited number of reboots (1)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	0	0

(2) The activation of Disk resource 1 fails.

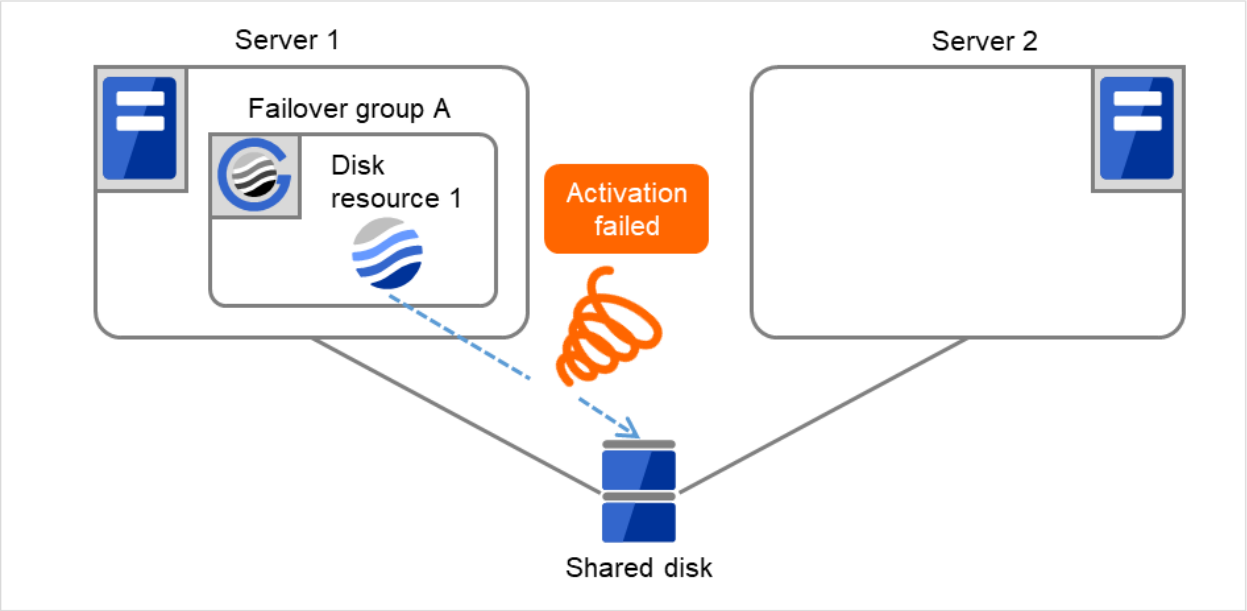


Fig. 3.22: Process with the limited number of reboots (2)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	0	0

(3) Stop the cluster service, and then reboot the OS. Since both **Retry Count at Activation Failure** and **Failover Threshold** are set at zero (0), the final action is taken.
On Server 1, the number of reboots is recorded as 1.

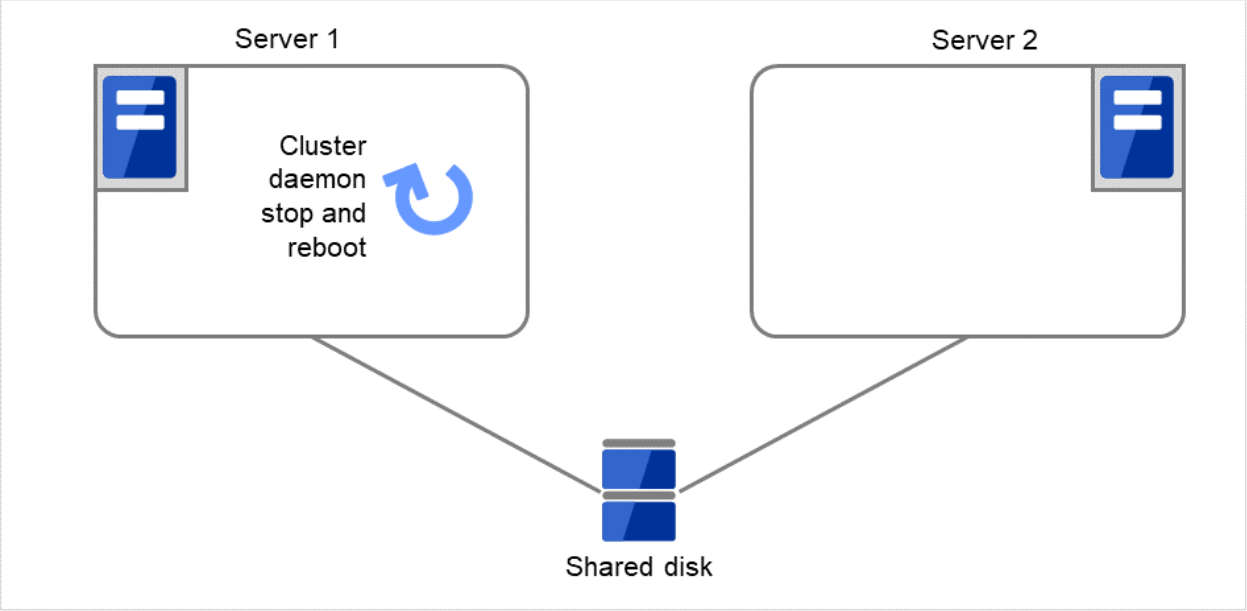


Fig. 3.23: Process with the limited number of reboots (3)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(4) Failover group A starts to be failed over.

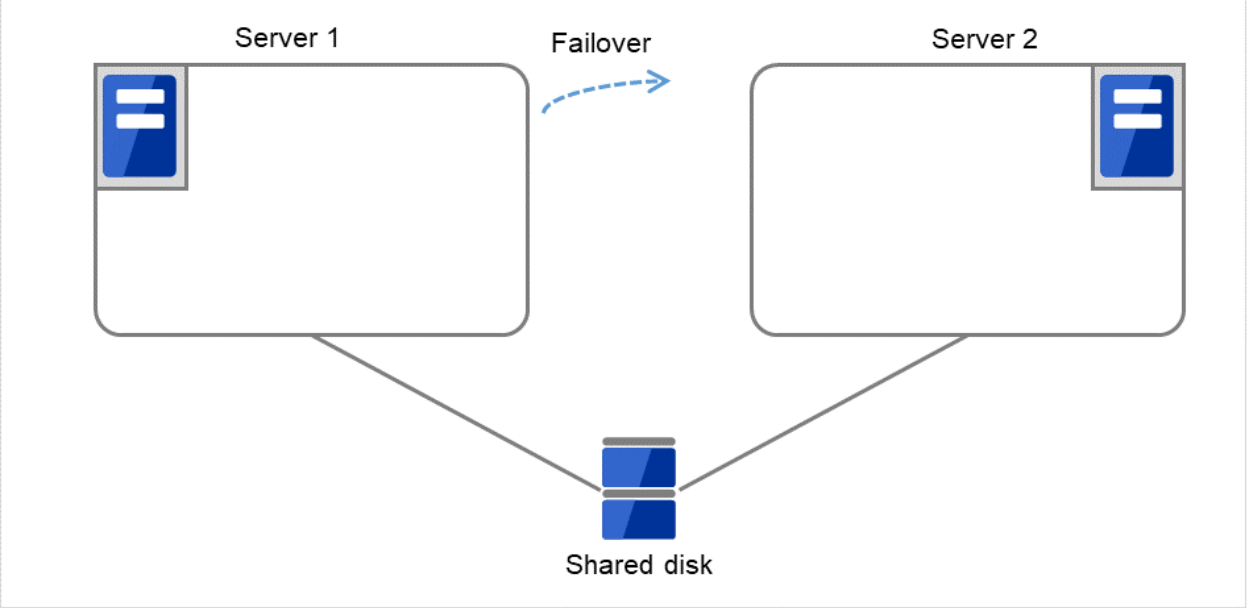


Fig. 3.24: Process with the limited number of reboots (4)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(5) Disk resource 1 starts to be activated (e.g. for mounting the file system).
The resource activation succeeds on Server 2, and the reboot is completed on Server 1.

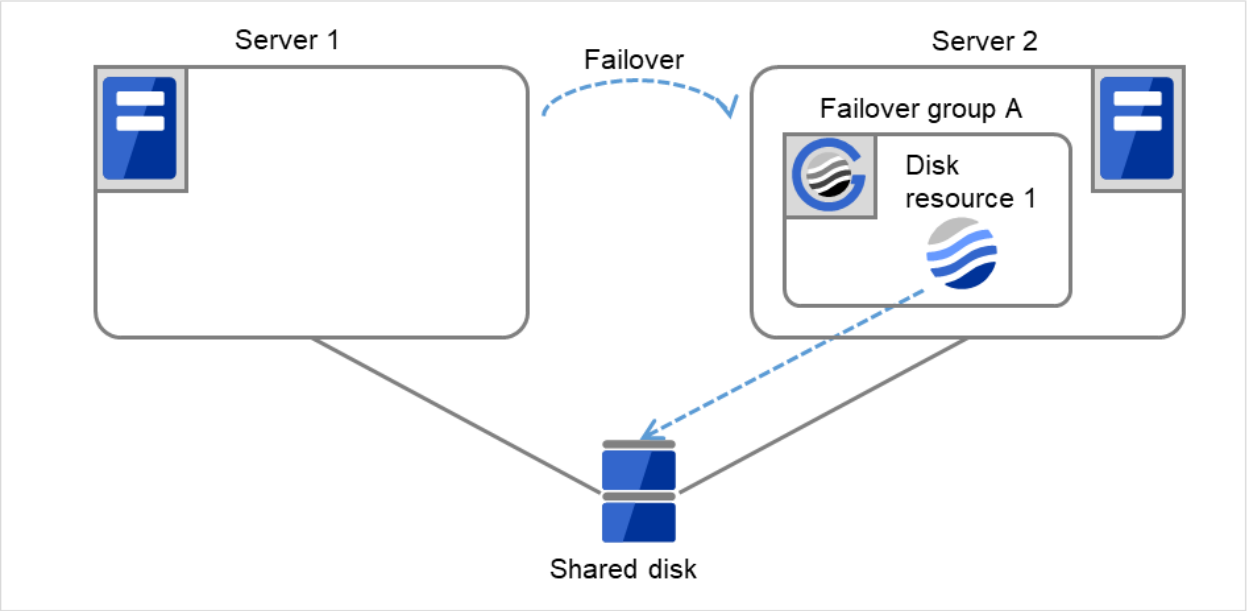


Fig. 3.25: Process with the limited number of reboots (5)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(6) Start the failover of Failover group A by using the clpgrp command or Cluster WebUI.

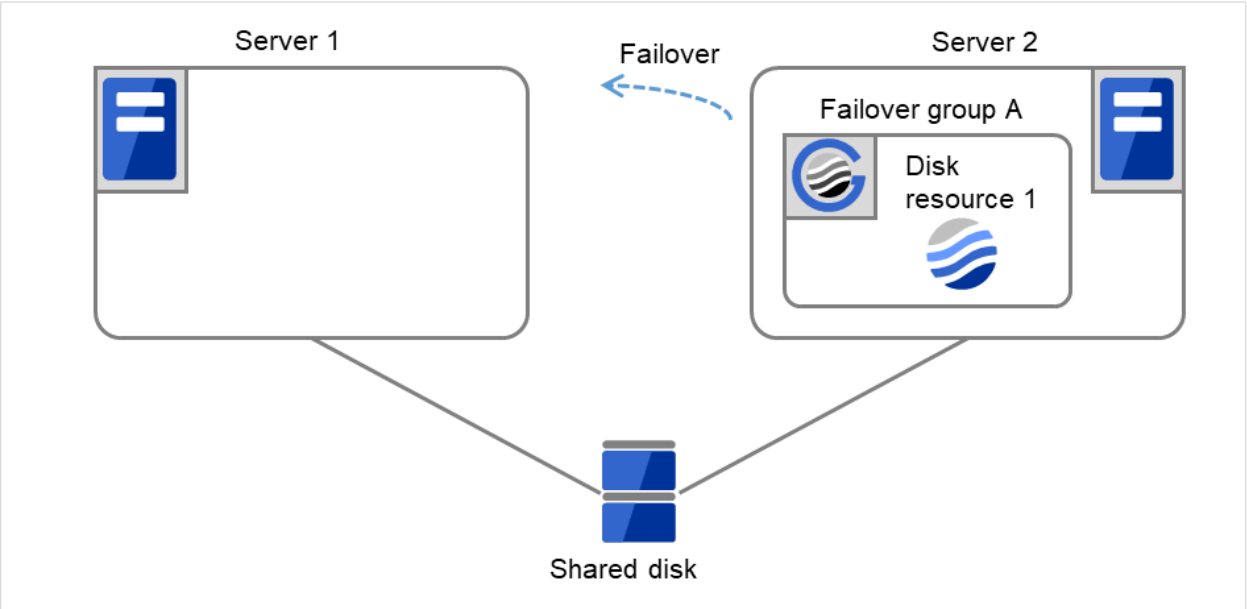


Fig. 3.26: Process with the limited number of reboots (6)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(7) Disk resource 1 starts to be activated (e.g. for mounting the file system).

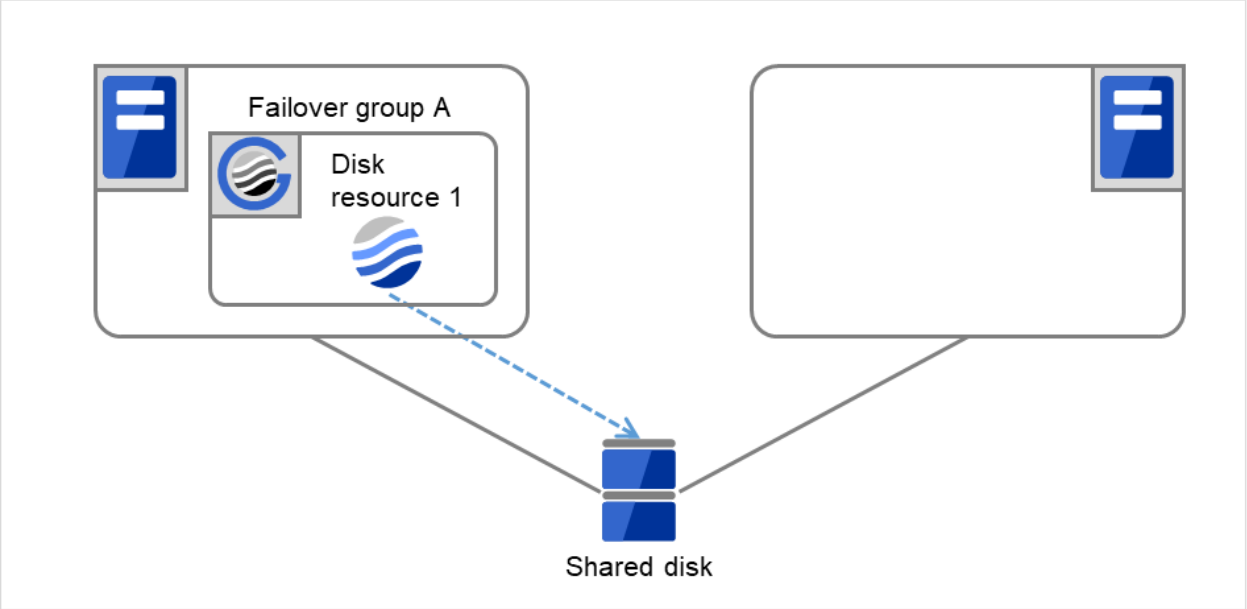


Fig. 3.27: Process with the limited number of reboots (7)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(8) The activation of Disk resource 1 fails.
The final action is not taken, because the reboot count has reached its maximum.
Even after 10 minutes pass, the reboot count is not reset.
An activation failure occurs in Failover group A.

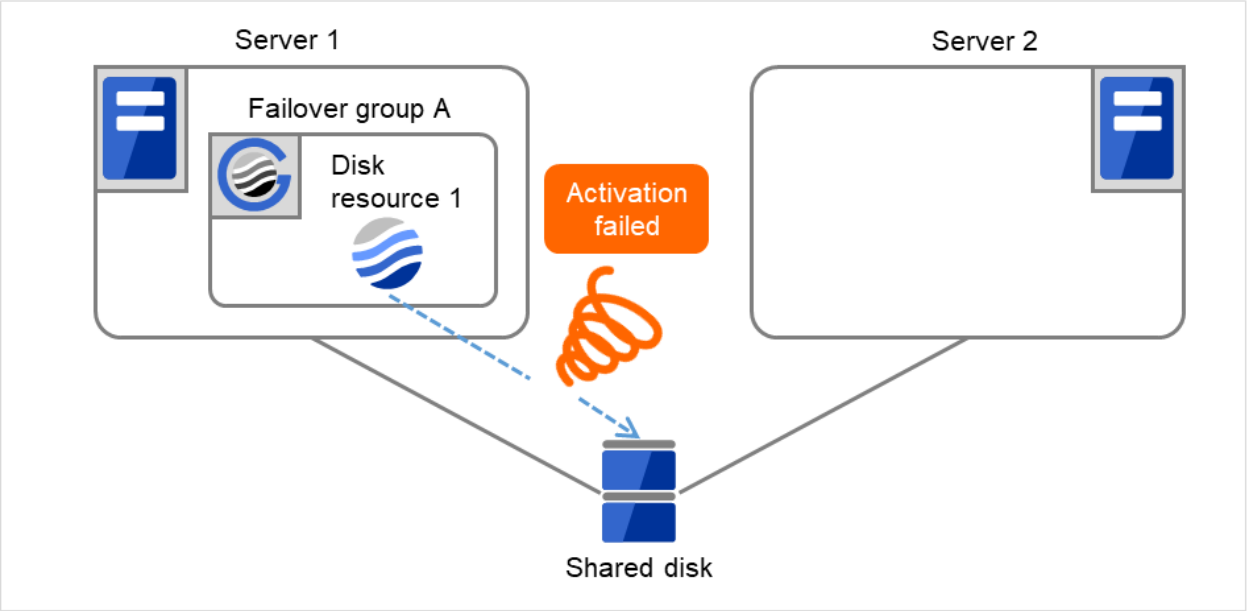


Fig. 3.28: Process with the limited number of reboots (8)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(9) Eliminate the disk error that caused the activation failure of Disk resource 1.
After that, shut down the cluster by using the clpstdn command or Cluster WebUI. Then start the reboot.

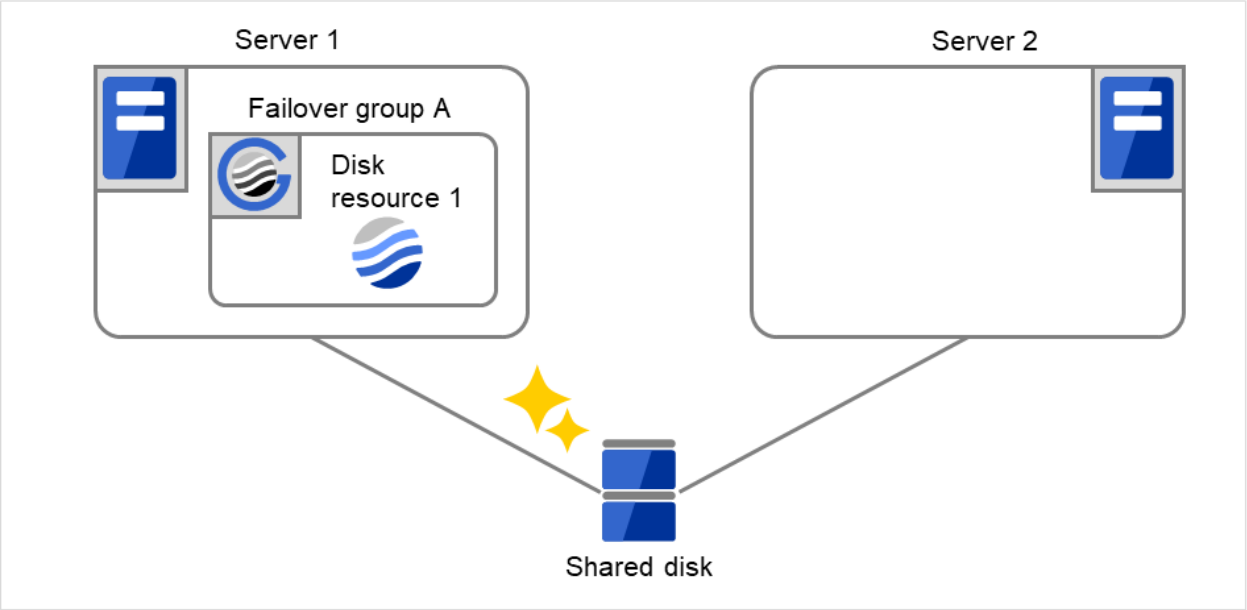


Fig. 3.29: Process with the limited number of reboots (9)

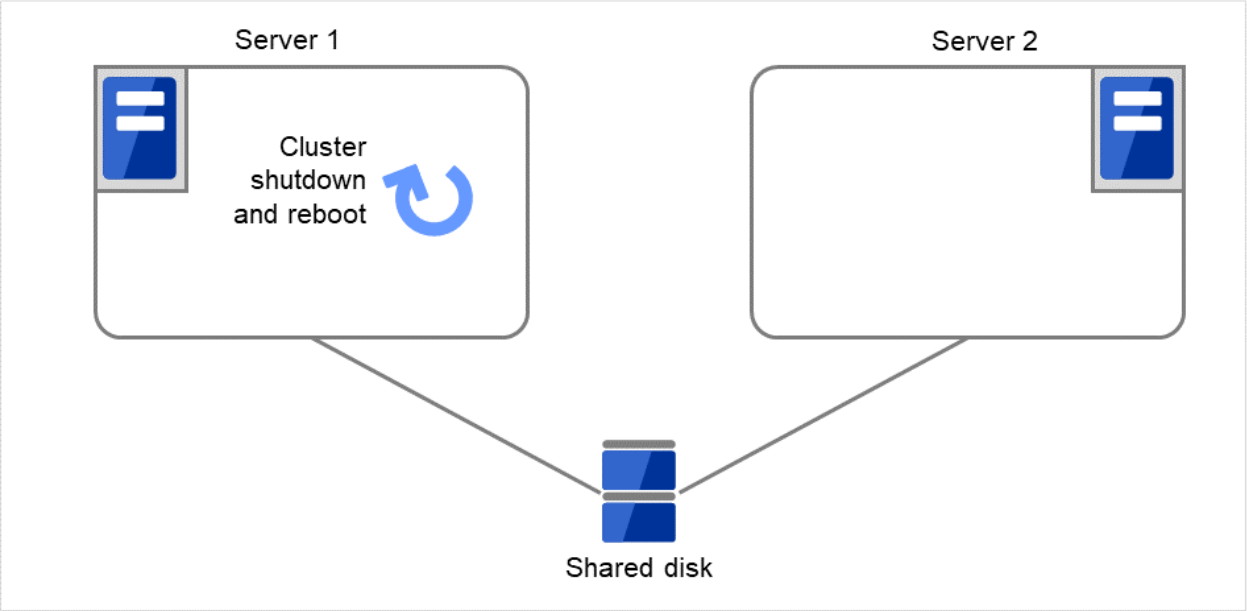


Fig. 3.30: Process with the limited number of reboots (10)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(10) Starting up Failover group A succeeds.
After 10 minutes pass, the reboot count is reset.
Next time an activation failure occurs in Disk resource 1 during a startup of Failover group A, the final action will be taken.

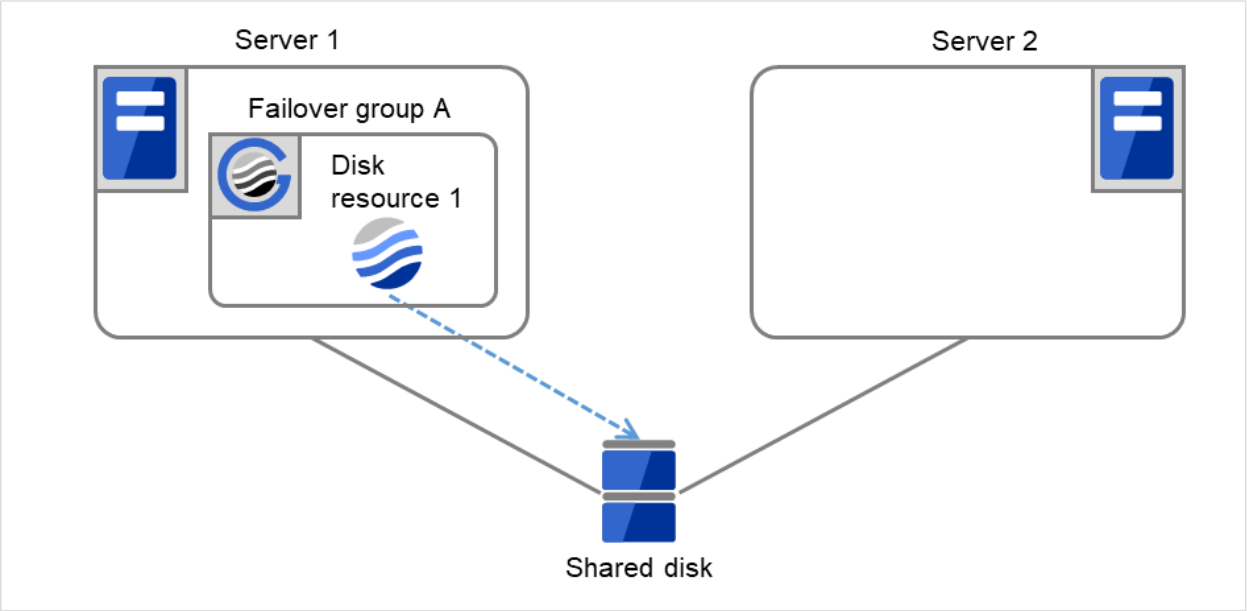


Fig. 3.31: Process with the limited number of reboots (11)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	0	0

3.2.9 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 "*9. EXPRESSCLUSTER command reference*" in this guide.

3.2.10 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 (if 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 **Execute Multi-Failover-Service Check** 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.

3.2.11 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.

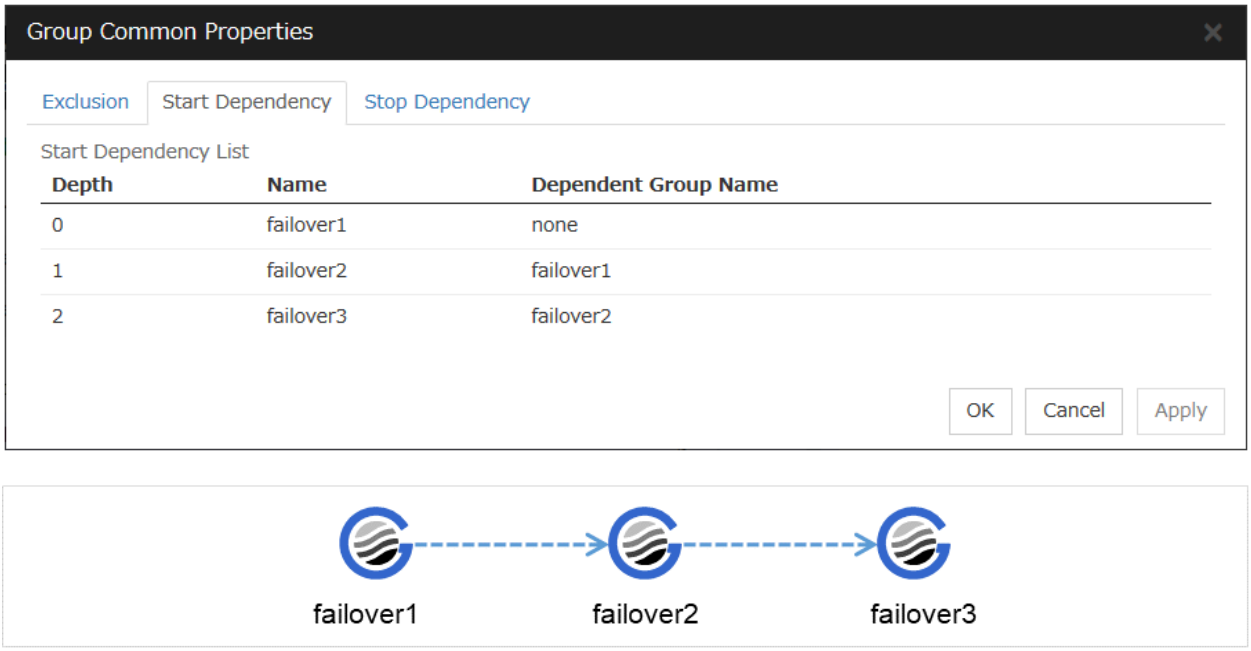


Fig. 3.32: Order of starting groups

When two servers have three groups

Group failover policy

Group A Server 1

Group B Server 2

Group C Server 1 -> Server 2

Group start dependence setting

Group A Start dependence is not set.

Group B Start dependence is not set.

Group C Group A start dependence is set.

Start dependence is set when Group C is started by the server of Group B.

1. When Server 1 starts Group A and Group C

   Server 1 starts Group C after Group A has been started normally.

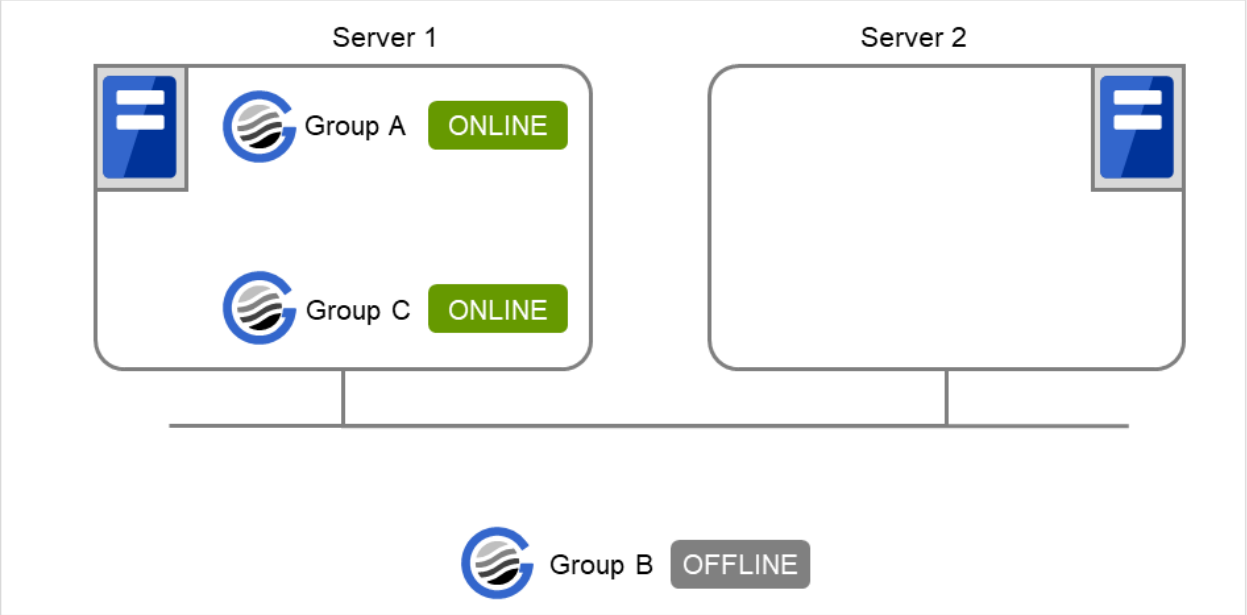


Fig. 3.33: Server 1 starts Group A and Group C

2. When Server 1 starts Group A and Server 2 starts Group C

   Server 2 starts Group C after Server 1 has started Group A normally.

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

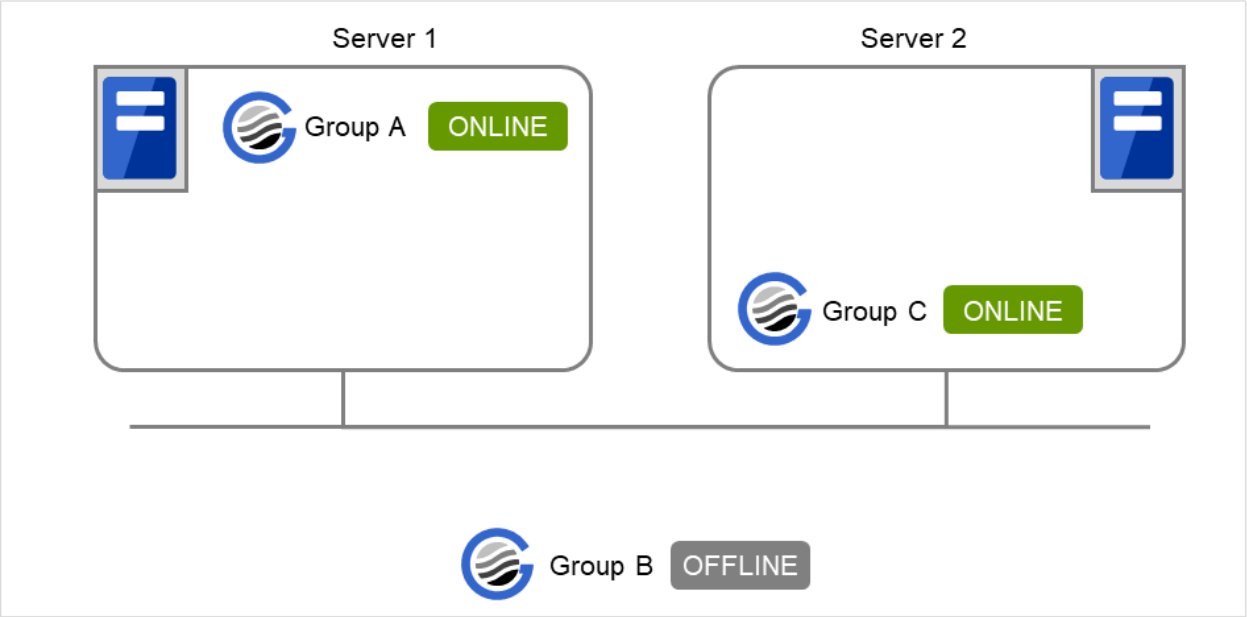


Fig. 3.34: Server 1 starts Group A and Server 2 starts Group C

3. When Server 1 starts Group C and Server 2 starts Group B

   Server 1 starts Group C without waiting for the normal start of Group B. Group C is set to wait for Group B start only when it is started by the same server. However, start dependence is not applied to Group C because Group B is set such that it is not started by Server 1.

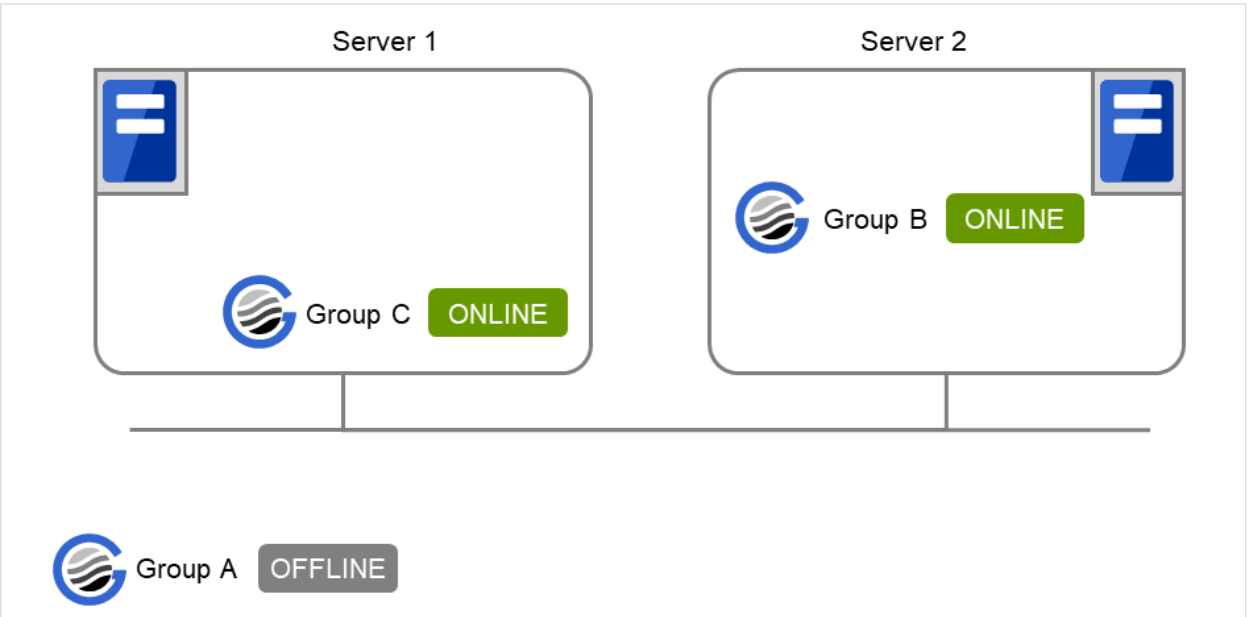


Fig. 3.35: Server 1 starts Group C and Server 2 starts Group B

4. When Server 1 starts Group A and Group C

If Server 1 fails in Group A start, Group C is not started.

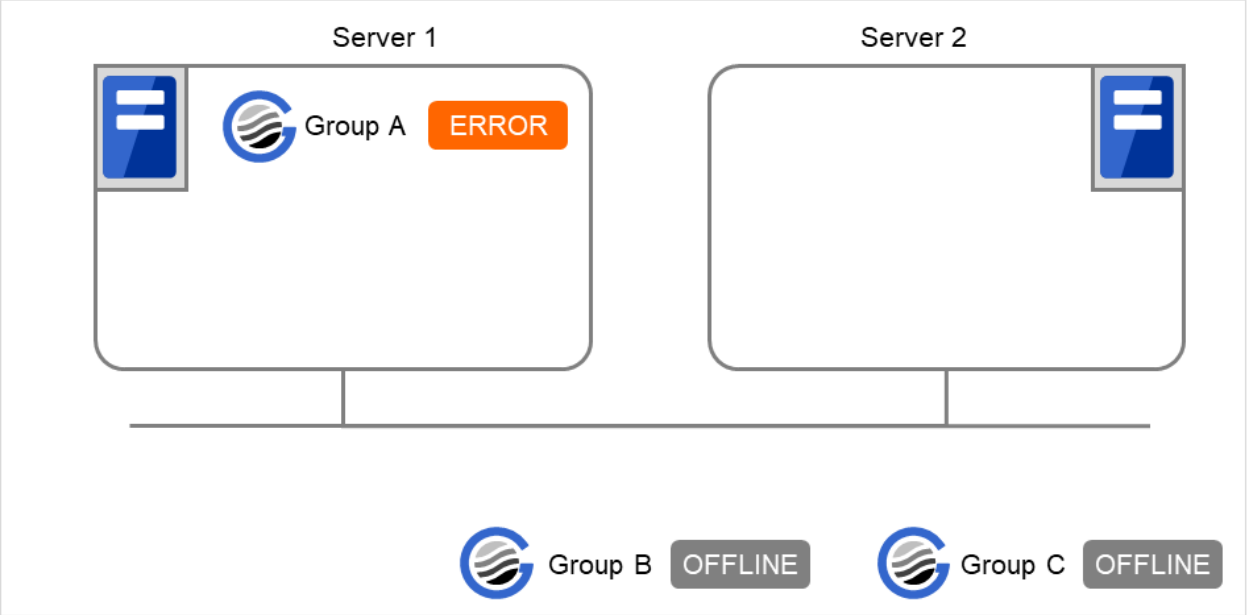


Fig. 3.36: Failing in starting Group A, Server 1 does not start Group C

5. When Server 1 starts Group A and Group C

   If Server 1 fails in Group A start and a failover occurs in Server 2 due to Group A resource recovery, Server 2 starts Group A and then Server 1 starts Group C.

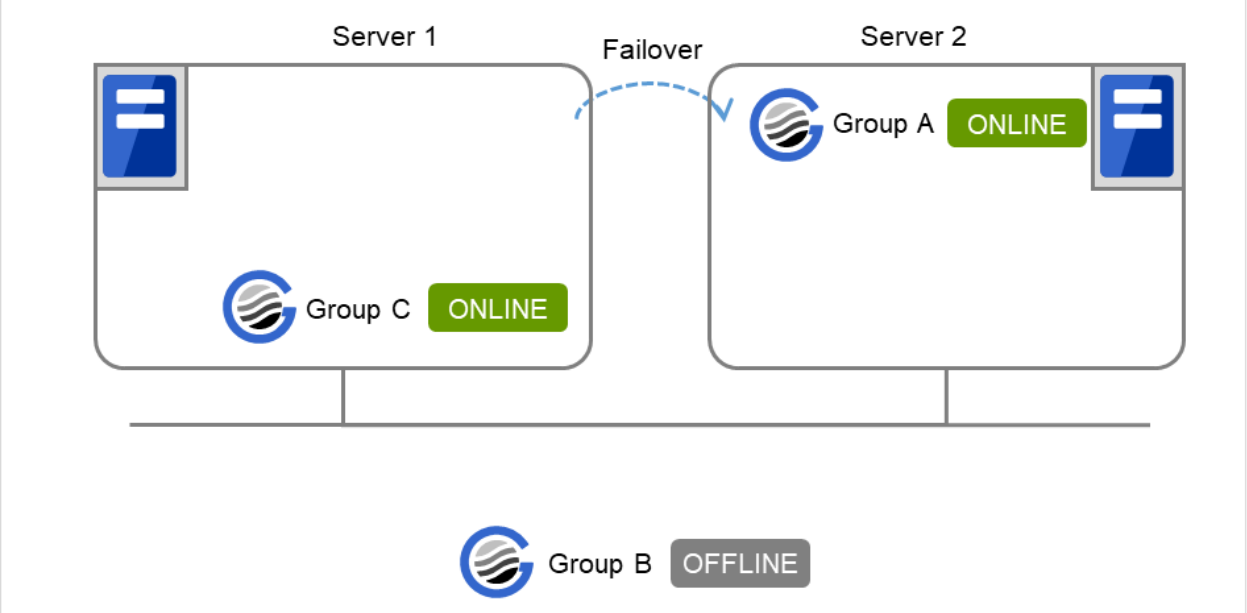


Fig. 3.37: GroupA fails over to Server 2, and Group C is started on Server 1

6. When Server 1 starts Group A and Group C

If a Group A start dependence timeout occurs on Server 1, Group C is not started.

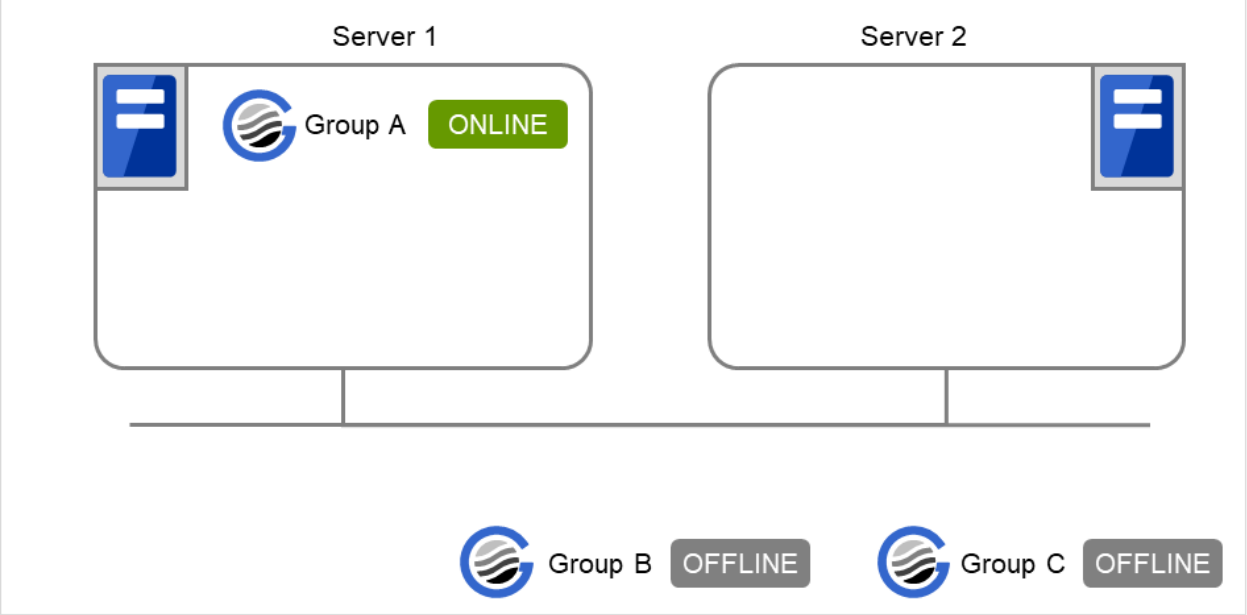


Fig. 3.38: Server 1 starts Group A

7. When Server 1 starts only Group C

   Server 1 has not started Group A, so a start dependence timeout occurs. If this timeout occurs, Group C is not started.

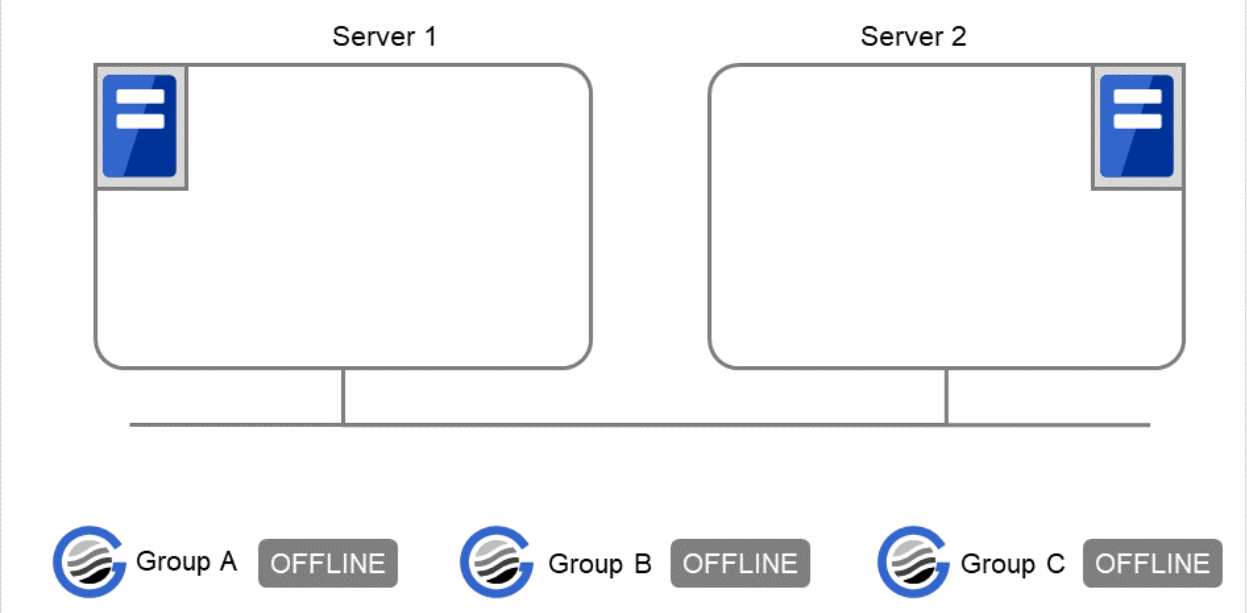


Fig. 3.39: Server 1 does not start Group A or Group C

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 has both a normally started resource and a stopped resource, the group is judged to have already been normally started.
- When a group is stopped, there is no function to automatically stop the group for which stop dependence is set.
- Group stop processing continues if a timeout occurs in a group for which stop dependence is set.
- Group stop processing continues if a 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.
- At the timing of a failover, if a start waiting timeout occurs, the failover fails

3.2.12 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:

- 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* ".

3.2.13 Understanding server groups

This section provides information 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 non-shared disk, a single server is configured as a single server group.

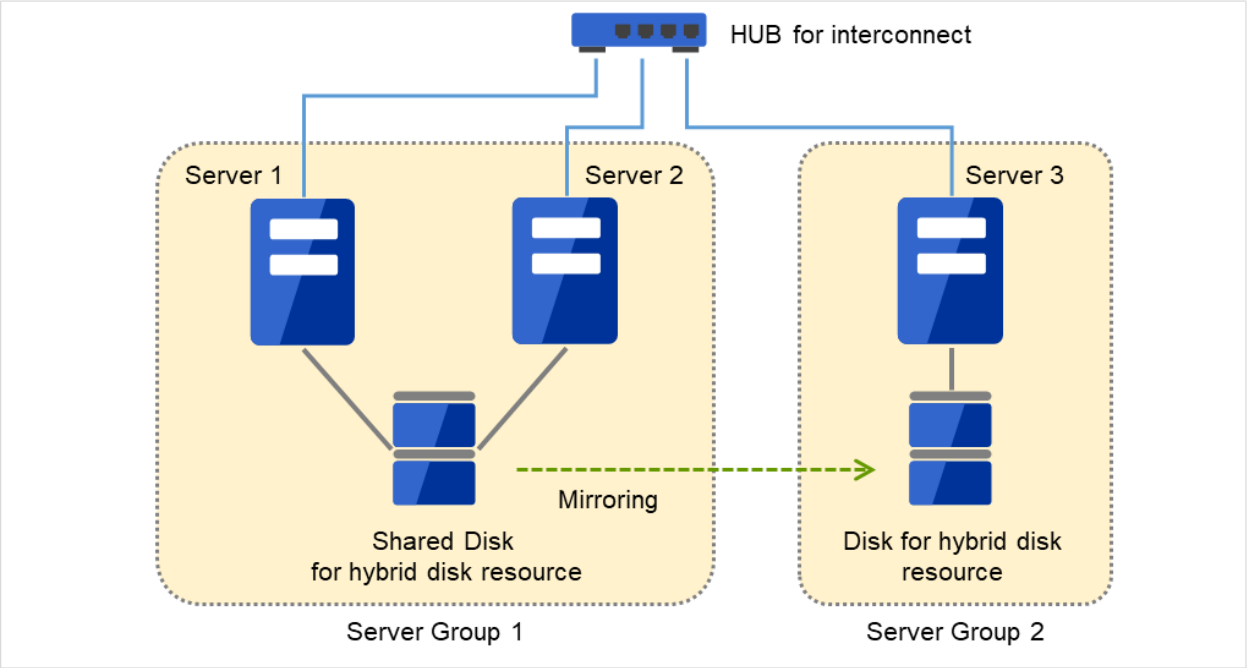


Fig. 3.40: Server groups

3.2.14 Understanding the settings of dependency among group resources

By specifying dependency among group resources, you can specify the order of activating them.

- 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.

The following shows an example of the depth of dependency of resources that belong to a group.

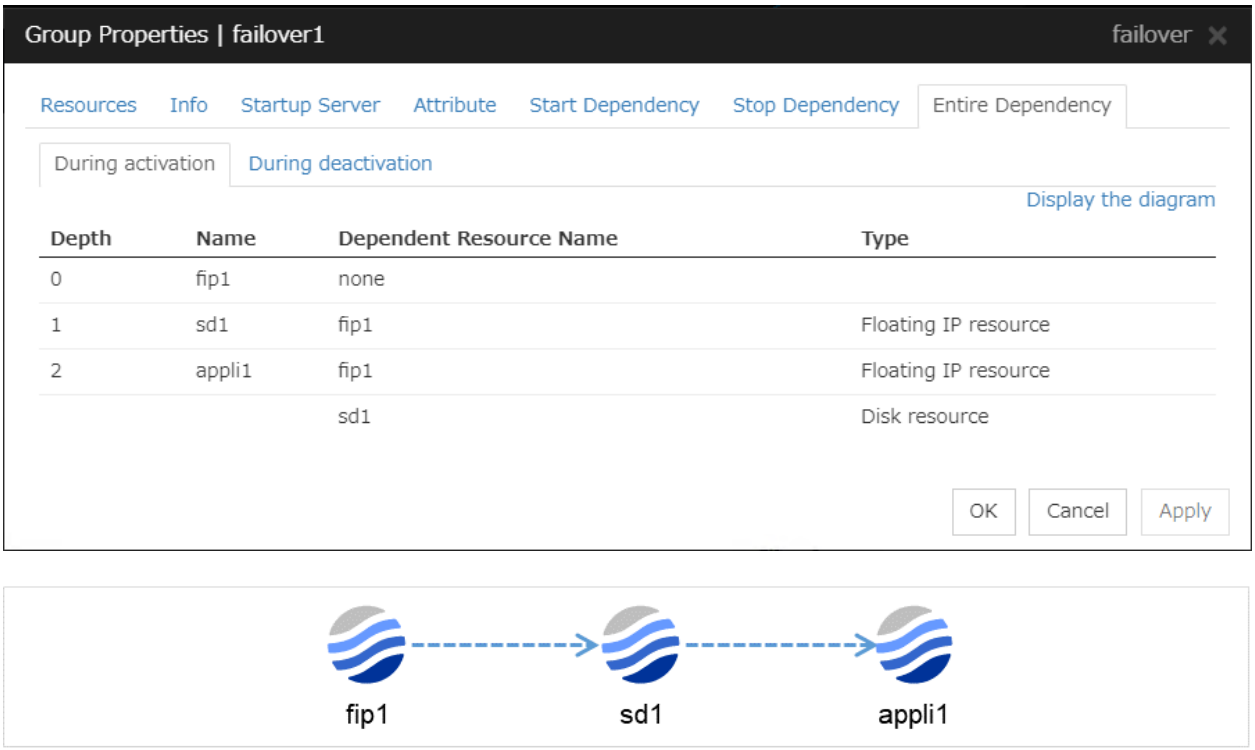
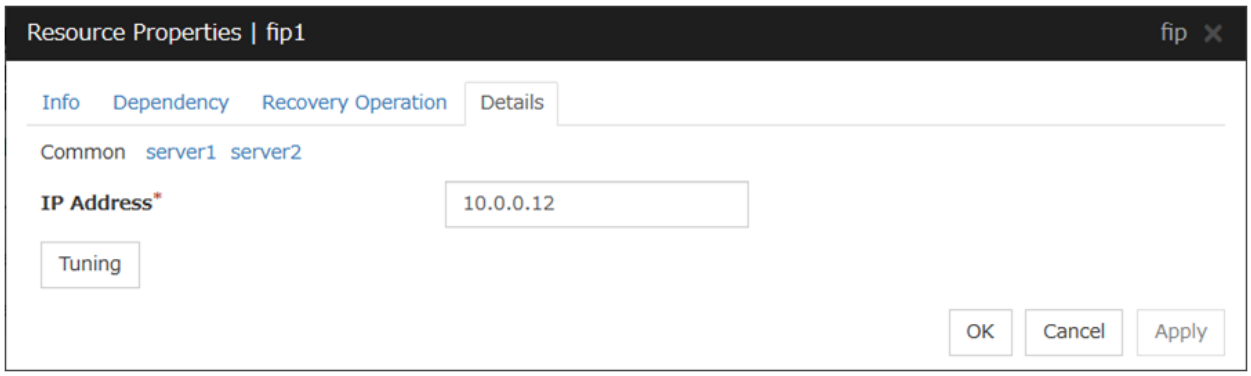


Fig. 3.41: Example of a group resource activation order

Fig. 3.42: Example of a group resource deactivation order

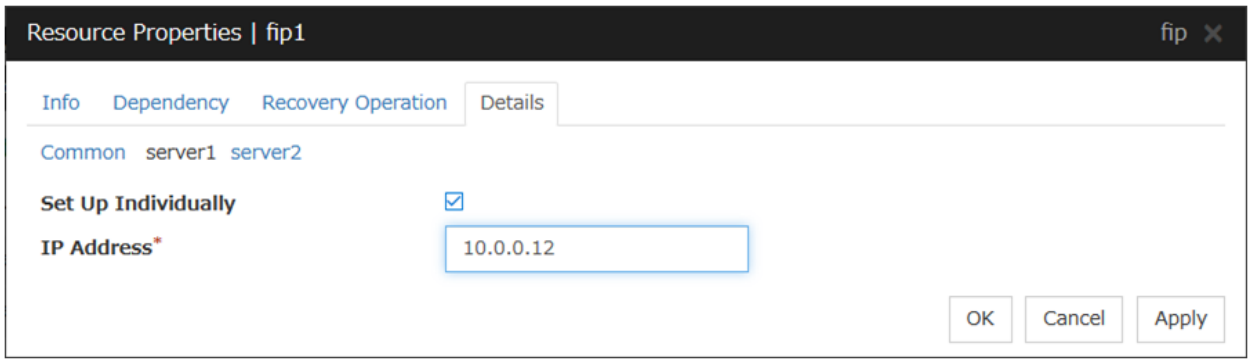
3.2.15 Setting group resources for individual server

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.
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.



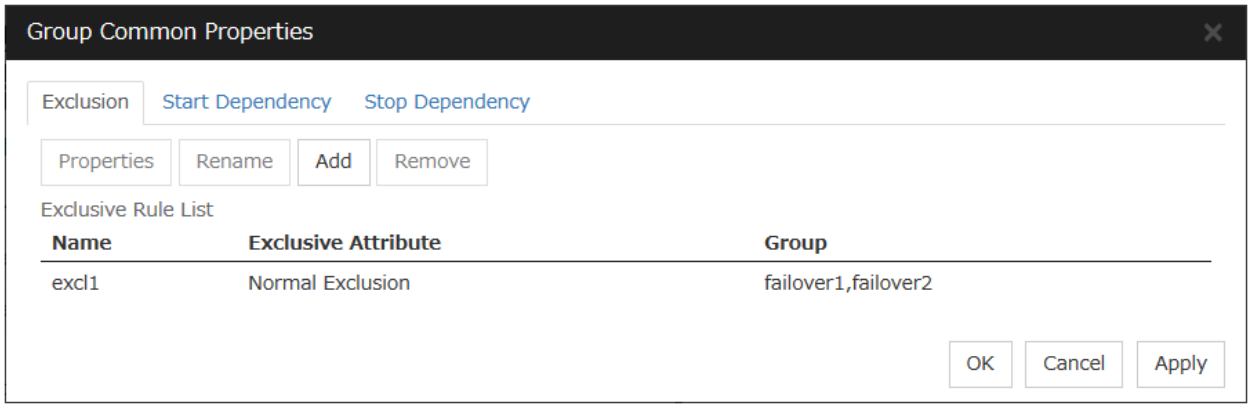
Set Up Individually

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

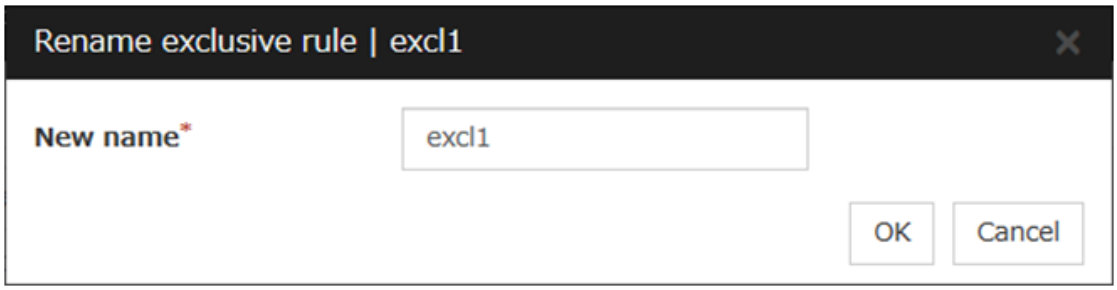
Add exclusion rules. Select Add to display the Exclusive Rule Definition dialog box.

Remove

Remove exclusion rules.

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.

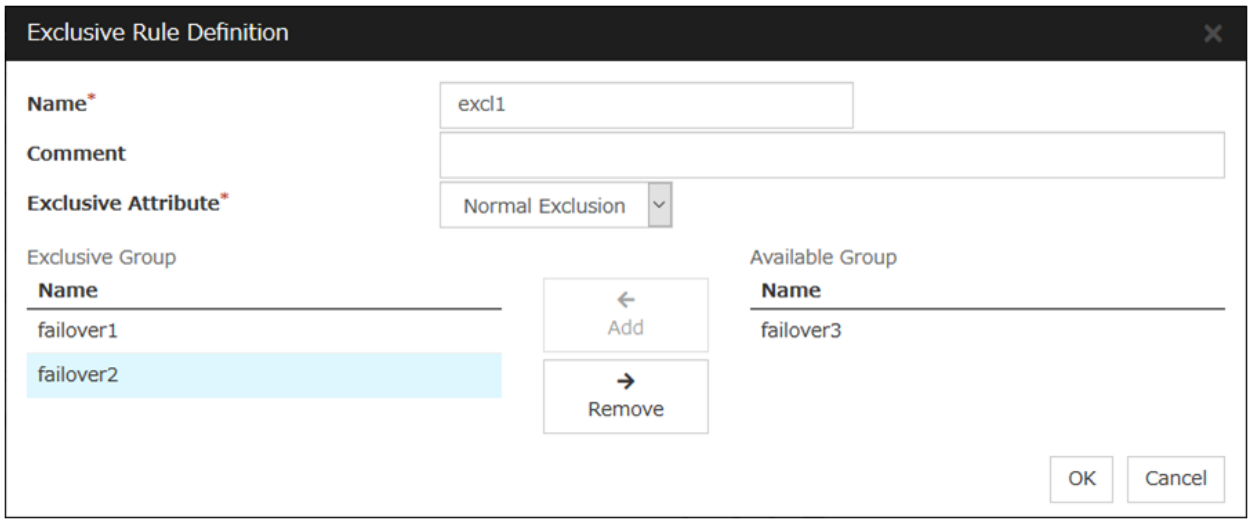
Names should be unique (case-insensitive) in the exclusion rule.

Properties

Display the properties of the selected exclusion rule.

Exclusive Rule Definition

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

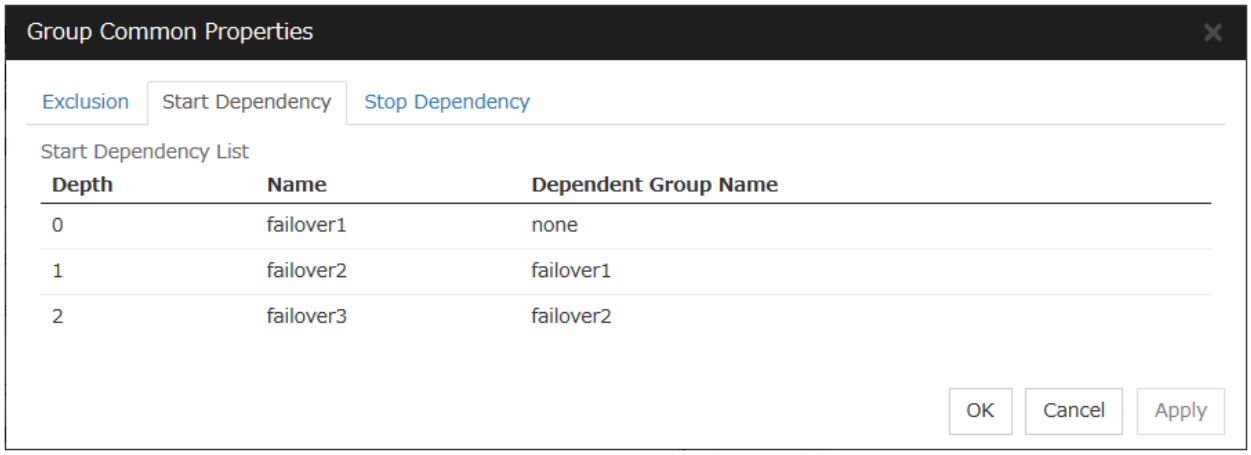
Display the list of failover group names which belong to the exclusion rule.

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**.

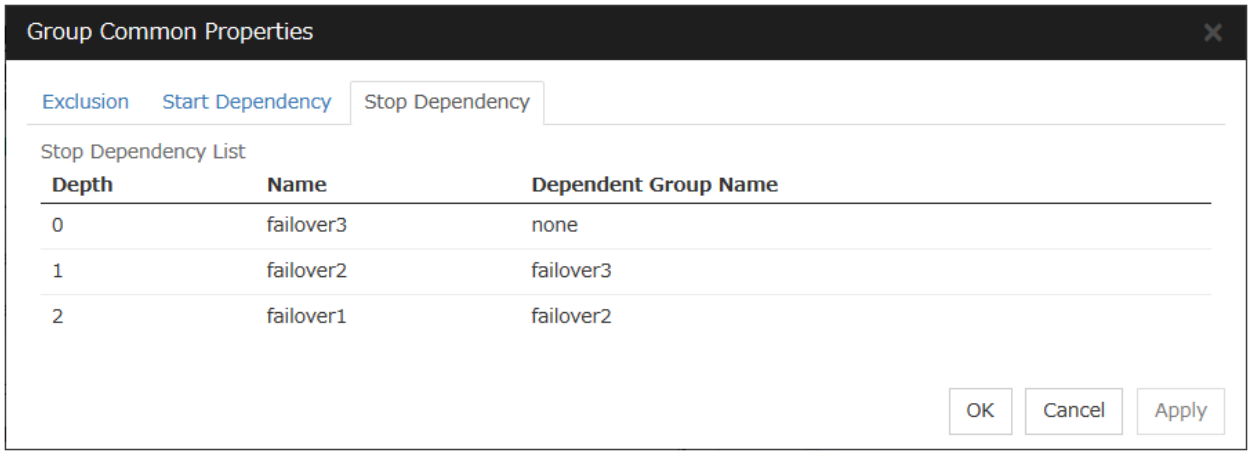
3.3.2 Start Dependency tab

Display the start dependency list.



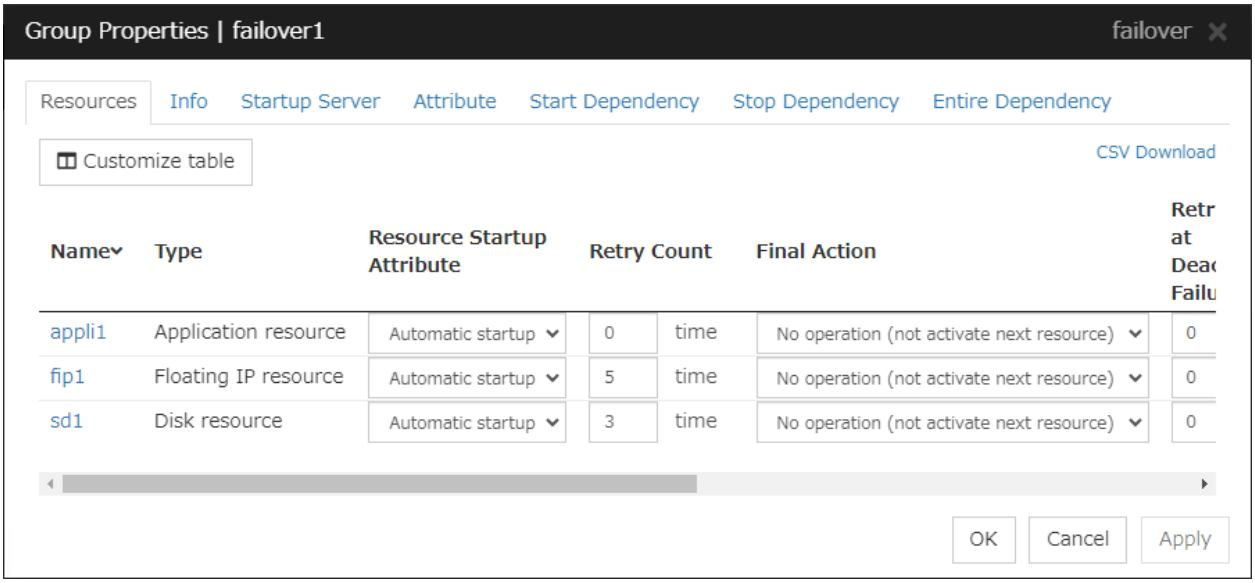
3.3.3 Stop Dependency tab

Display the stop dependency list.



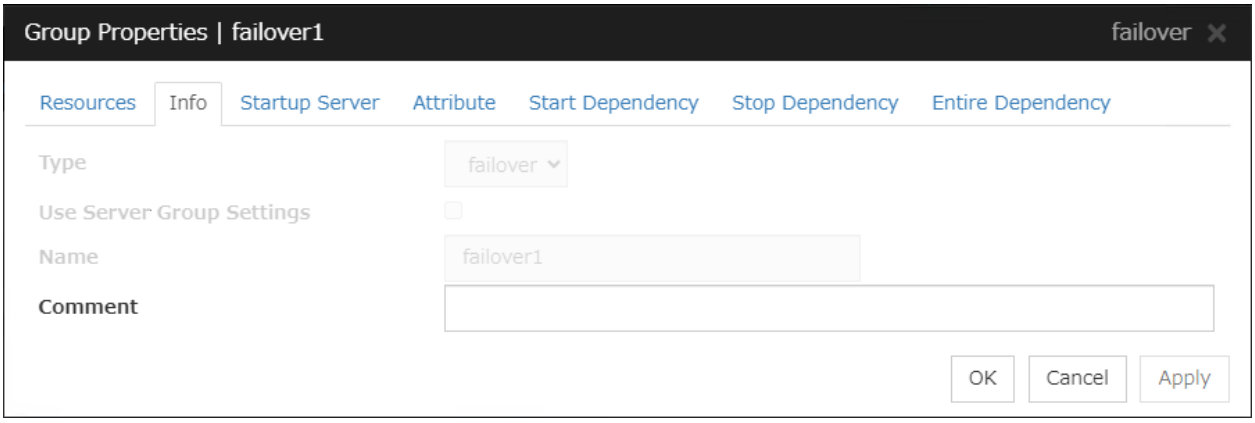
3.4 Group properties

3.4.1 Resources tab



Displays a list of group resources included in the selected group.
Allows you to change the various settings.
Clicking a name link takes you to the property screen of the corresponding resource.
Allows you to rearrange the items of the list by selecting their names or types.
Selecting **Customize table** displays the **Customize table** dialog box, where you can set which items are shown in or hidden from the list.
Clicking CSV Download downloads data, in CSV format, shown in the group resource list.
For more information on the displayed items, see " *Resource Properties* ".

3.4.2 Info tab



Type

The group type is displayed.

Use Server Group Settings

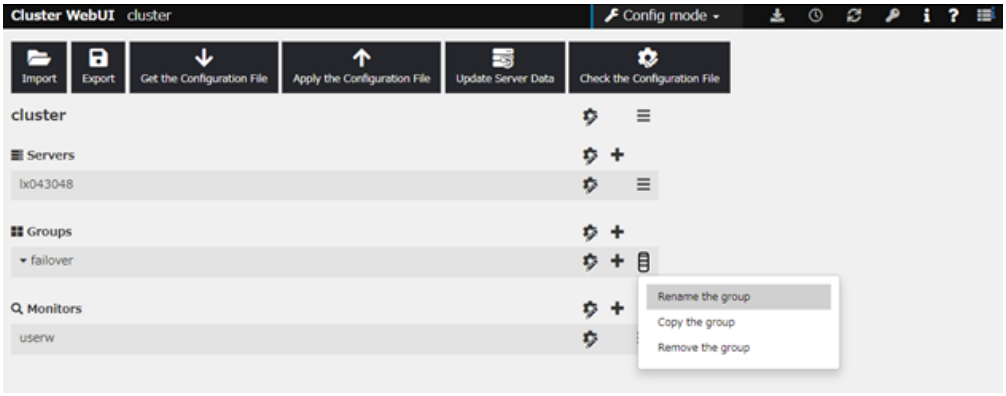
- When the check box is selected:
  Server group settings are used.
- When not selected:
  Server group settings are not used.

Name

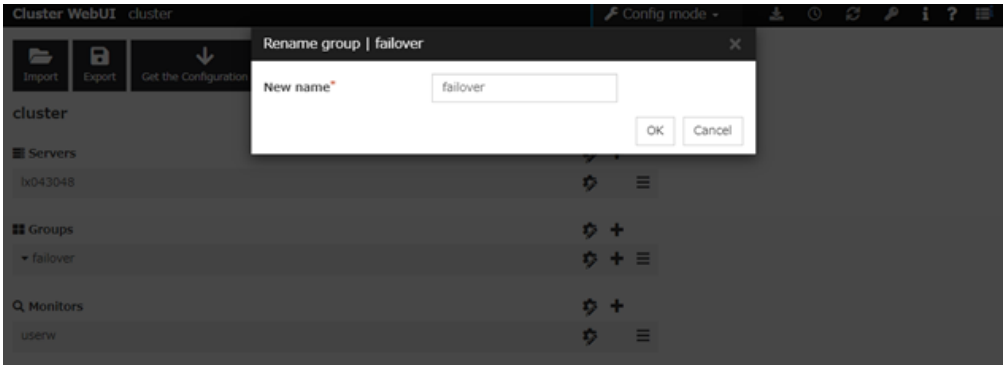
The group name is displayed.

Changing the group name

1. click **others**, and then select **Rename the group**.



2. A dialog box to **rename group** is displayed.



Naming rules

- Only alphanumeric characters, hyphen (-), underscore (_) and space are allowed for names.
- Up to 31 characters (31 bytes)
- Names cannot start or end with a hyphen (-) or space.

Comment (Within 127 bytes)

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

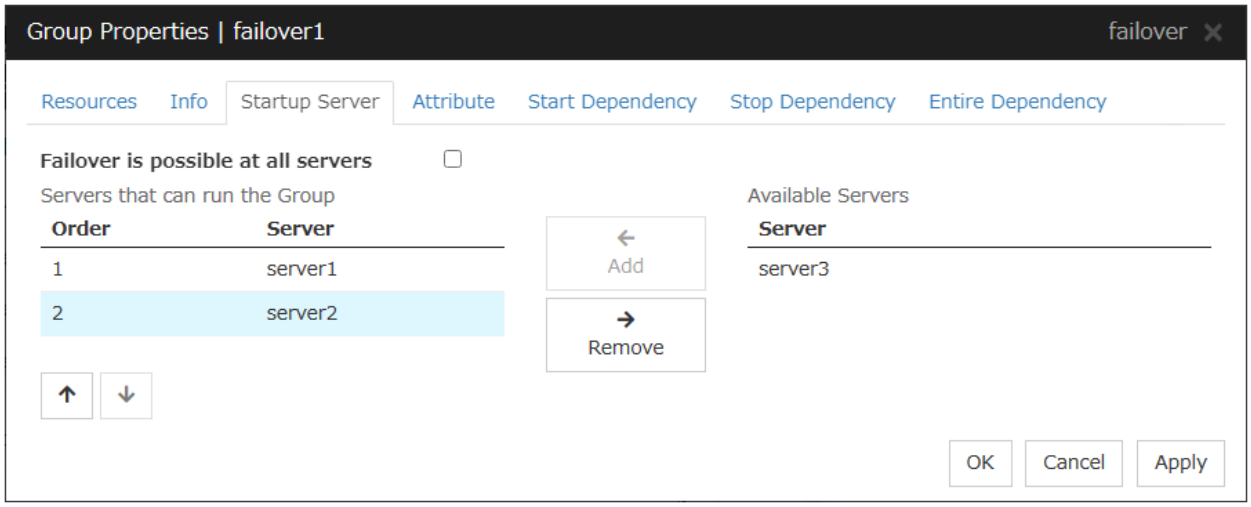
3.4.3 Startup Server tab

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 "*Servers 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 checkbox is selected:
  All servers registered to a cluster can start a group. The priority of starting up a group is the 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

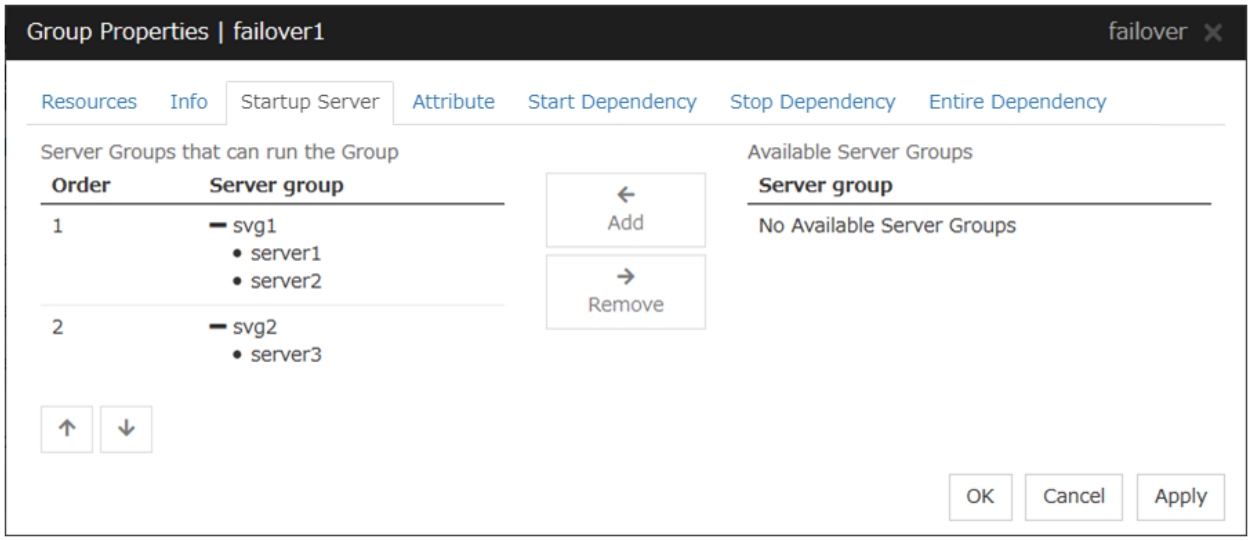
Use this button to remove a server. Select a server that you want to remove from **Servers that can run the Group**, and then click **Remove**. The server is added to **Available Servers**.

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:

In case of the group including the hybrid disk resource, it is necessary to configure the server that can run a group using the server group settings. For server group settings, see "*Server Group tab*" in "*Servers Properties*" in "*2. Parameter details*" in this guide.



Add

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

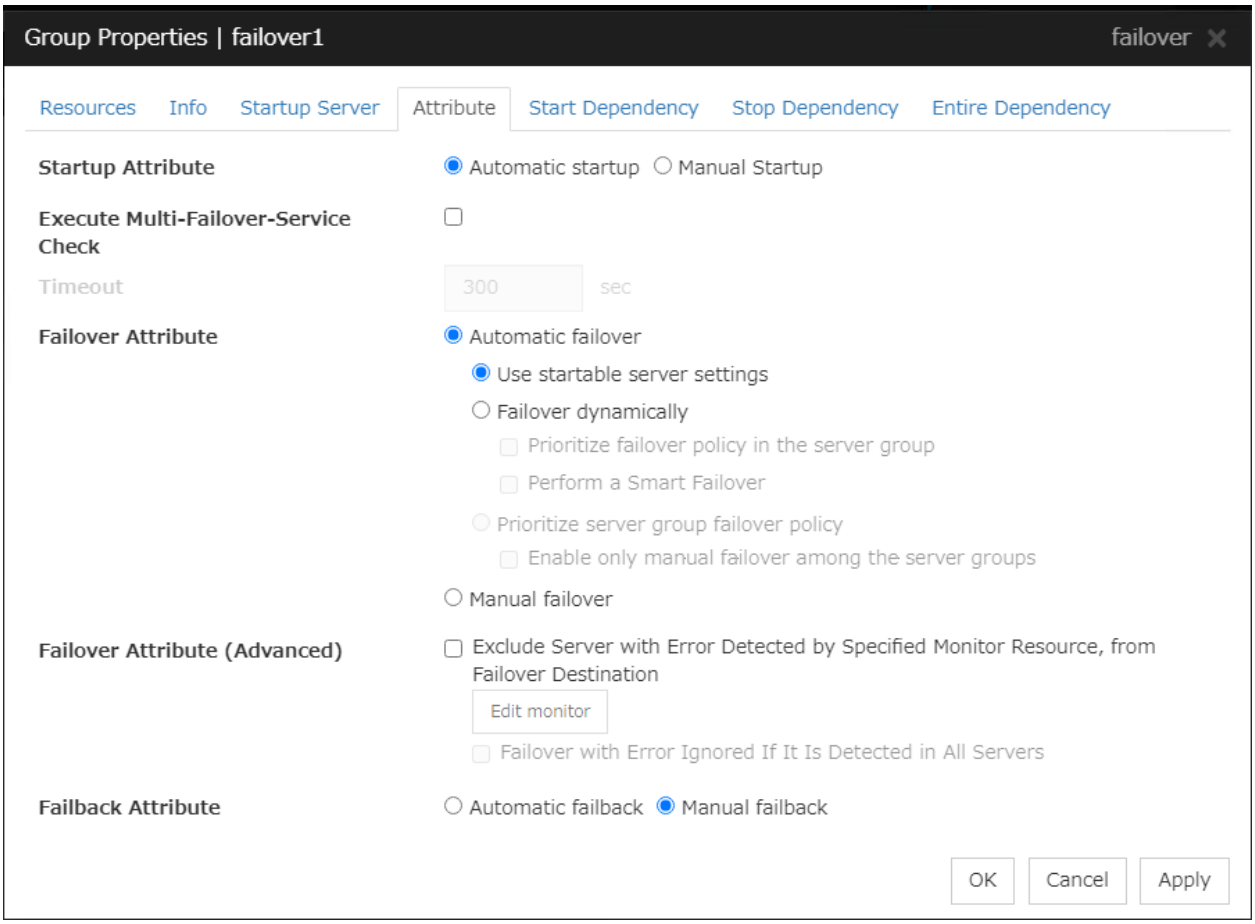
Remove

Use this button to remove a server group from server groups you use. 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 the server groups that can run a group. Select a server groups 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.

3.4.4 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.

Execute Multi-Failover-Service Check

Check whether a double activation will occur or not before a group is started.

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 performed automatically when 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.

Failover Attribute (Advanced)

Allows an advanced configuration of the automatic failover method specified in **Failover Attribute**. Refer to "*Understanding the group properties*" for the details.

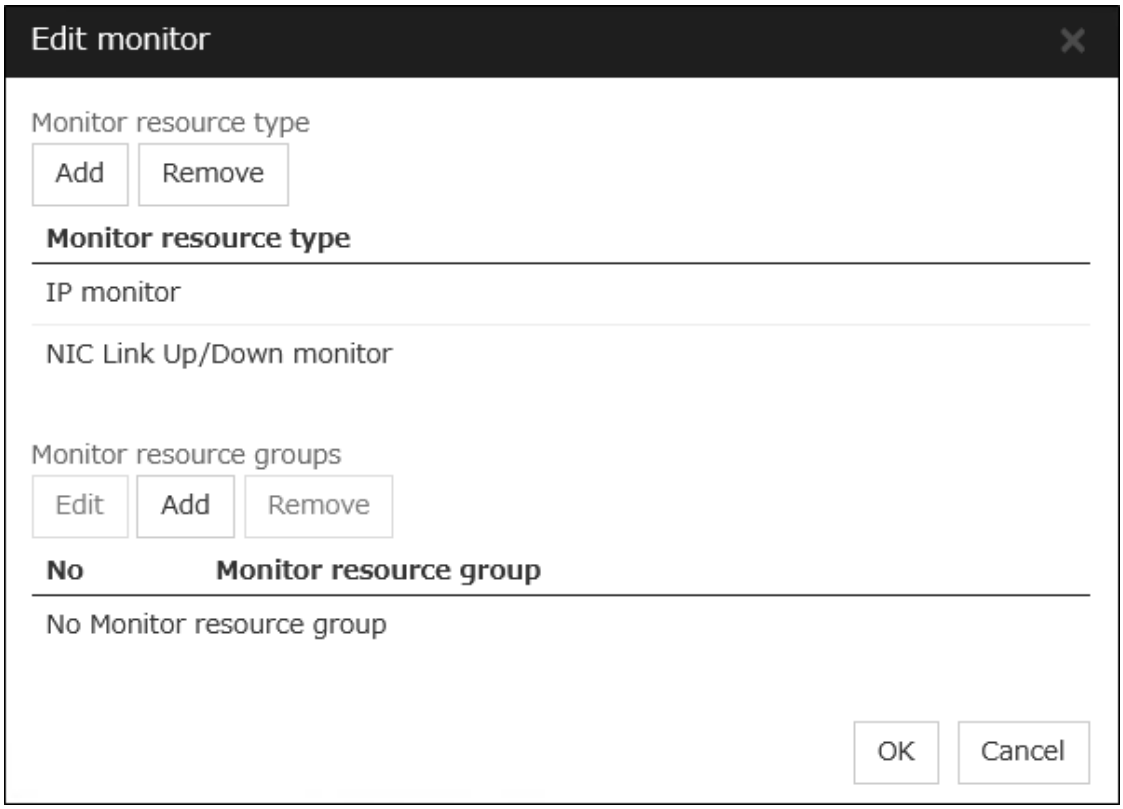
Failback Attribute

Select if the failback is performed 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.

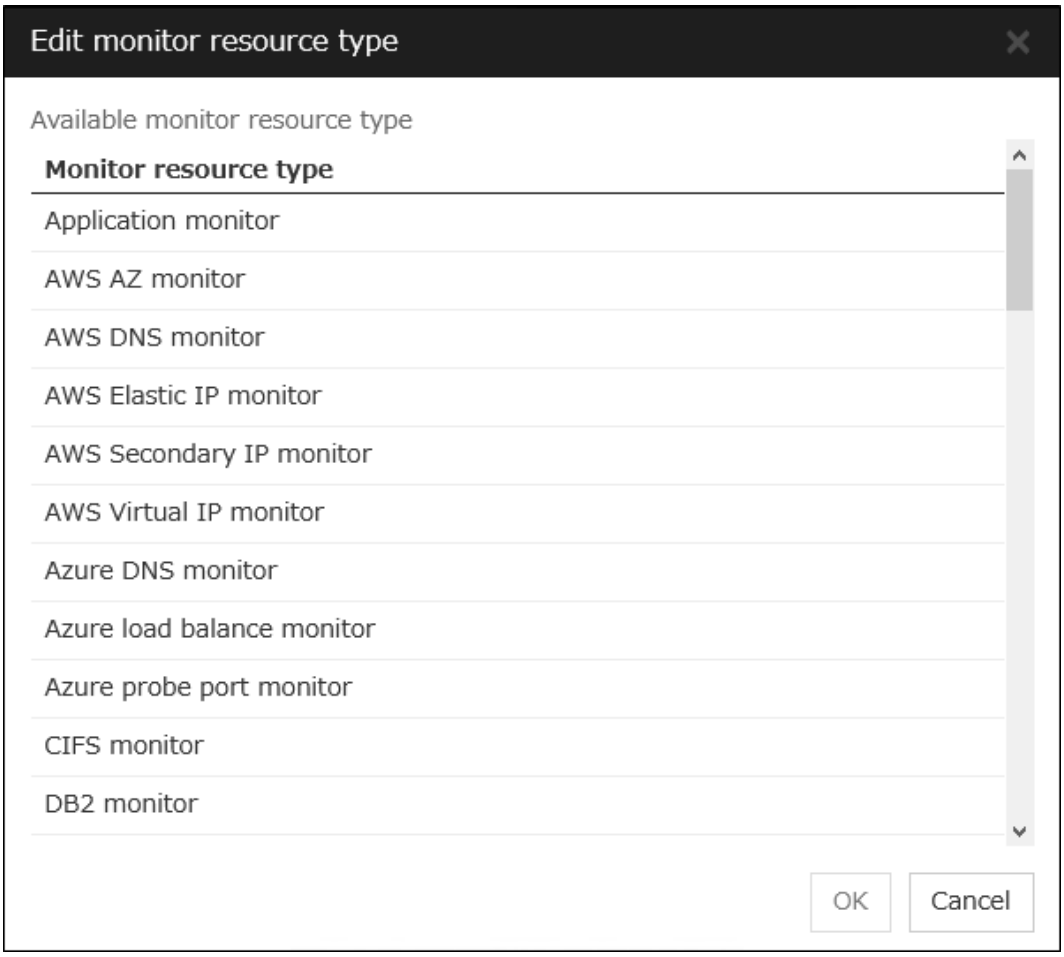
Edit Monitor

The failover process can exclude the server for which the specified monitor resource has detected an error, from the failover destinations. If **Exclude server with error detected by specified monitor resource, from failover destination** is selected in **Failover Attribute (Advanced)**, you can set the monitor resource that is used.

The monitor resource that is used can be set with the monitor resource type and monitor resource name.



- Add monitor resource type
  Adds the 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 monitor resource type
  Removes the selected monitor resource type.
- Add monitor resource group
  Adds the monitor resource group.
  The maximum number of monitor resource groups to be registered is 32.
  If multiple monitor resources are registered in a single monitor resource group, the server in which all the registered monitor resources are abnormal is excluded from the failover destinations.
  Moreover, if multiple 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 Resources list** to **Edit exclude monitor resource type**.

Remove

Removes the monitor resource selected with **Edit monitor resource type**, from the list.

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

Note: The following monitor resources cannot be registered for the monitor resource type. Moreover, a resource name of these resources cannot be registered for the monitor resource group.

- Hybrid disk monitor

Note:

The monitor resource in the warning status is not handled as being abnormal. However, the mirror disk monitor resource is excluded.

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:

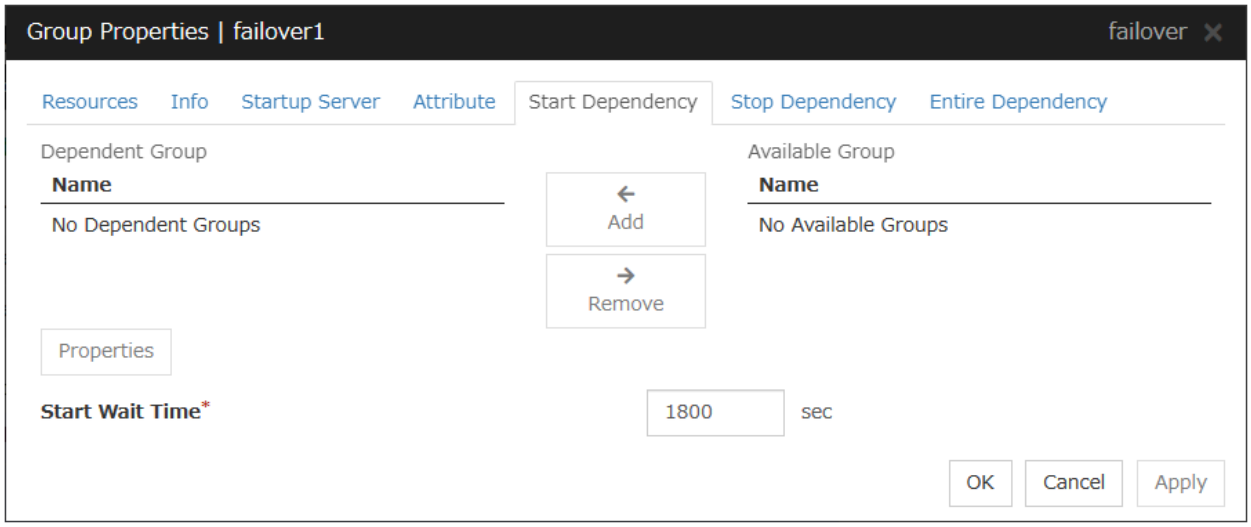
For the mirror disk monitor resource, any abnormality is determined from whether the mirror disk resource can be activated. This determination does not depend on the status of the mirror disk monitor resource.

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

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

Before the initial mirror configuration, the failover group may fail to start. It is recommended that the mirror disk monitor resource be registered in monitor resources for excluding server from failover destination after the initial mirror configuration.

3.4.5 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 to wait before a timeout occurs in the target group start processing. The default value is 1800 seconds.

Property

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

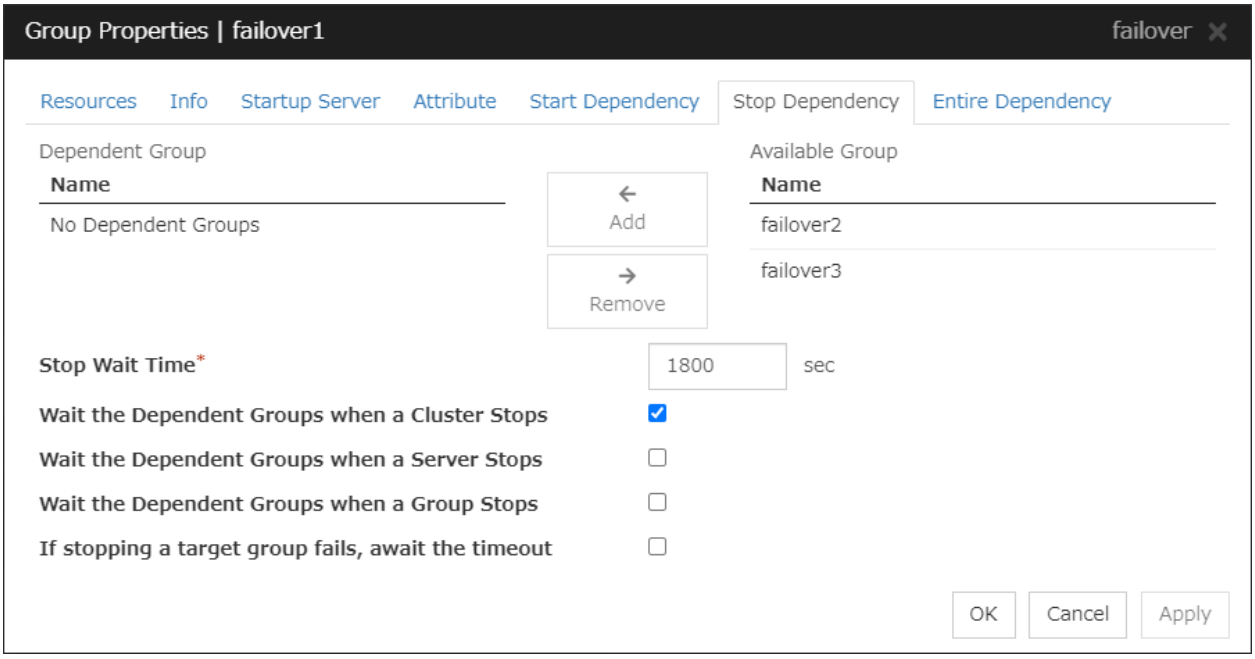
Wait Only when on the Same Server

Specify whether to wait for starting only if the group for which start waiting is specified and the target group are starting on the same server.

If the server on which the group with start waiting specified starts is not included as the Startup Server of the target group, waiting is not required.

If a target group fails to start on a server other than the server on which the group with start waiting specified is starting, waiting is not required.

3.4.6 Stop Dependency



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.

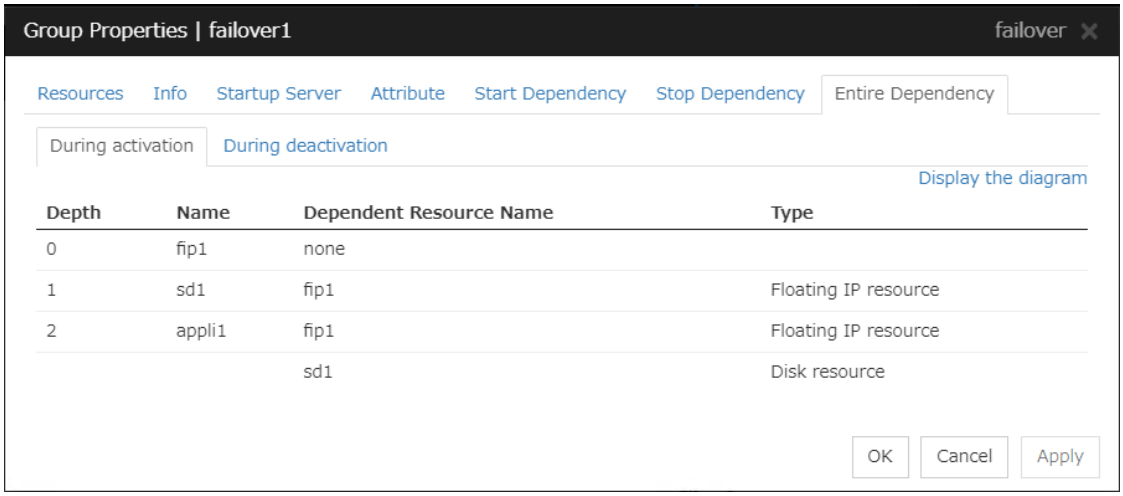
If stopping a target group fails, await the timeout

Specify whether to wait for the stop timeout following a stop failure of the target group.

- If the checkbox is checked:
  - The timeout is awaited.
- If the checkbox is not checked:
  - The timeout is not awaited; the currently selected group starts its own stop process.

3.4.7 Entire Dependency

Displays the settings of dependency among group resources.



During Activation tab

Displays dependency among group resources for failover group activation.

During Deactivation tab

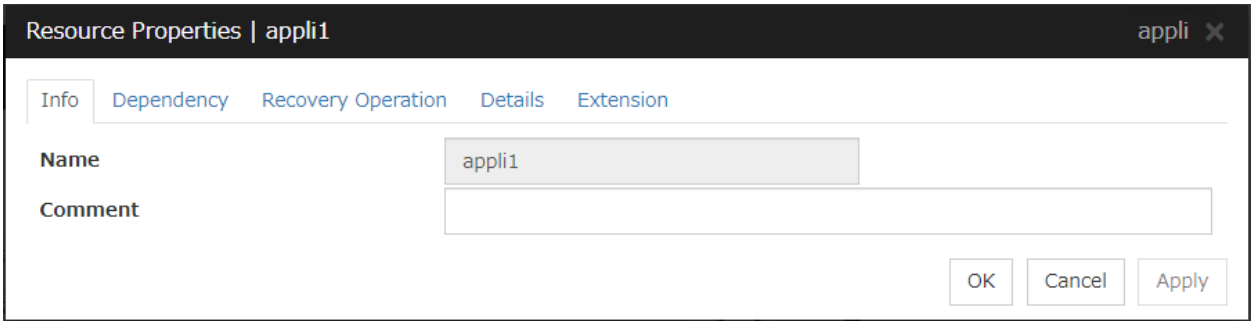
Displays dependency among group resources for failover group deactivation.

Display the diagram

Clicking the link displays the diagram of dependency among group resources.

3.5 Resource Properties

3.5.1 Info tab

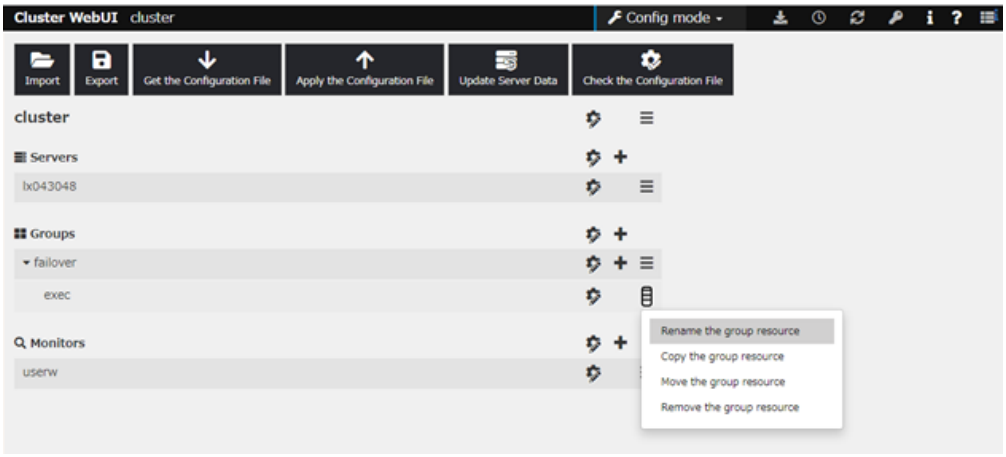


Name

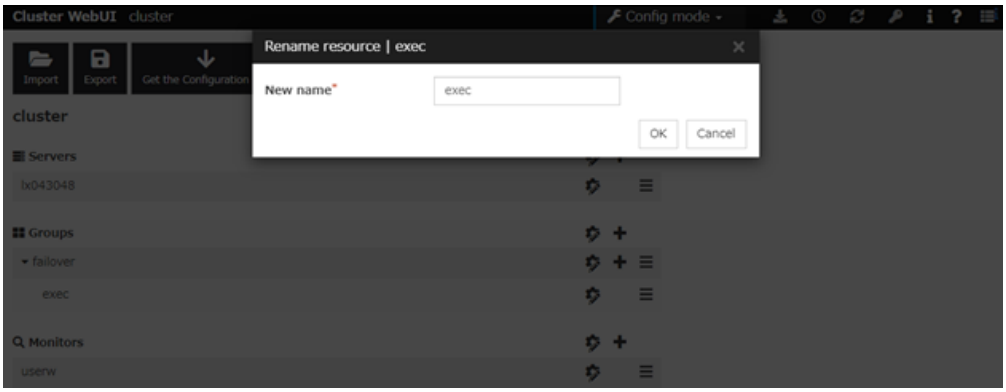
The resource name is displayed.

Changing the resource name

1. click **others**, and then select **Rename the group resource**.



2. A dialog box to **rename resource** is displayed.



Naming rules

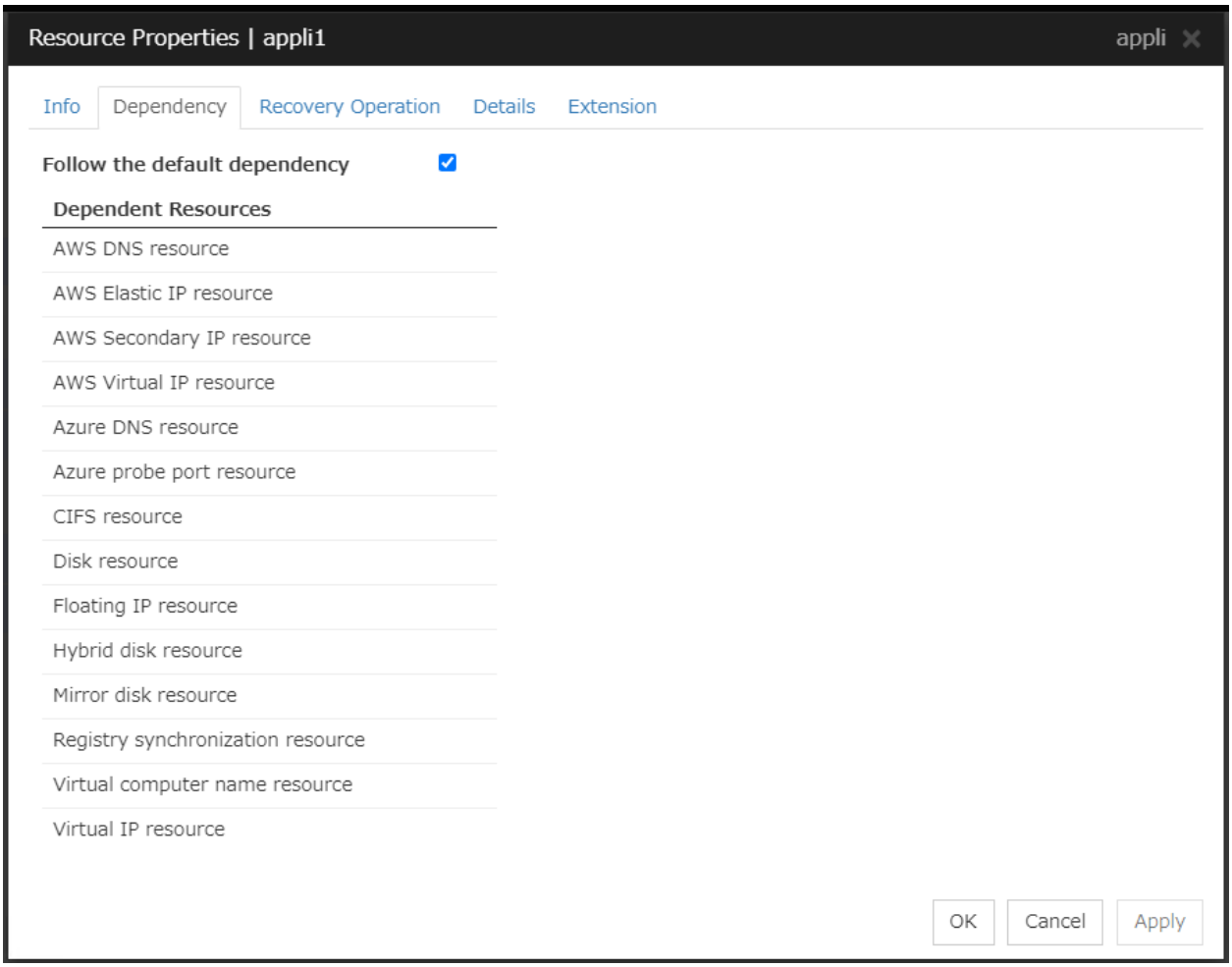
- Only alphanumeric characters, hyphen (-), underscore (_) and space are allowed for names.

- Up to 31 characters (31 bytes)
- Names cannot start or end with a hyphen (-) or space.

Comment (Within 127 bytes)

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

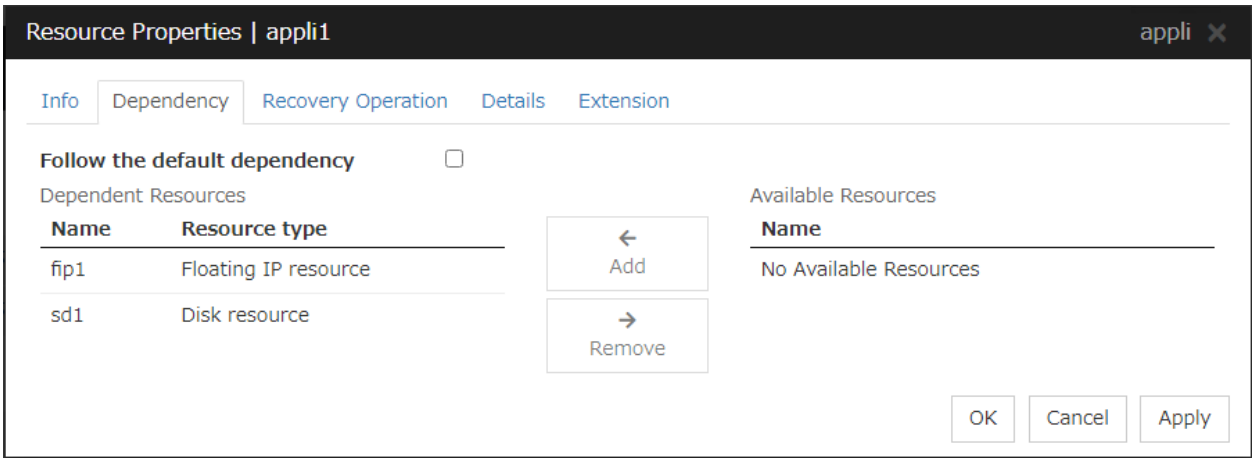
3.5.2 Dependency tab



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. For the default dependency of each resource, see "Parameters list" in "Parameter details" in this guide. 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**.

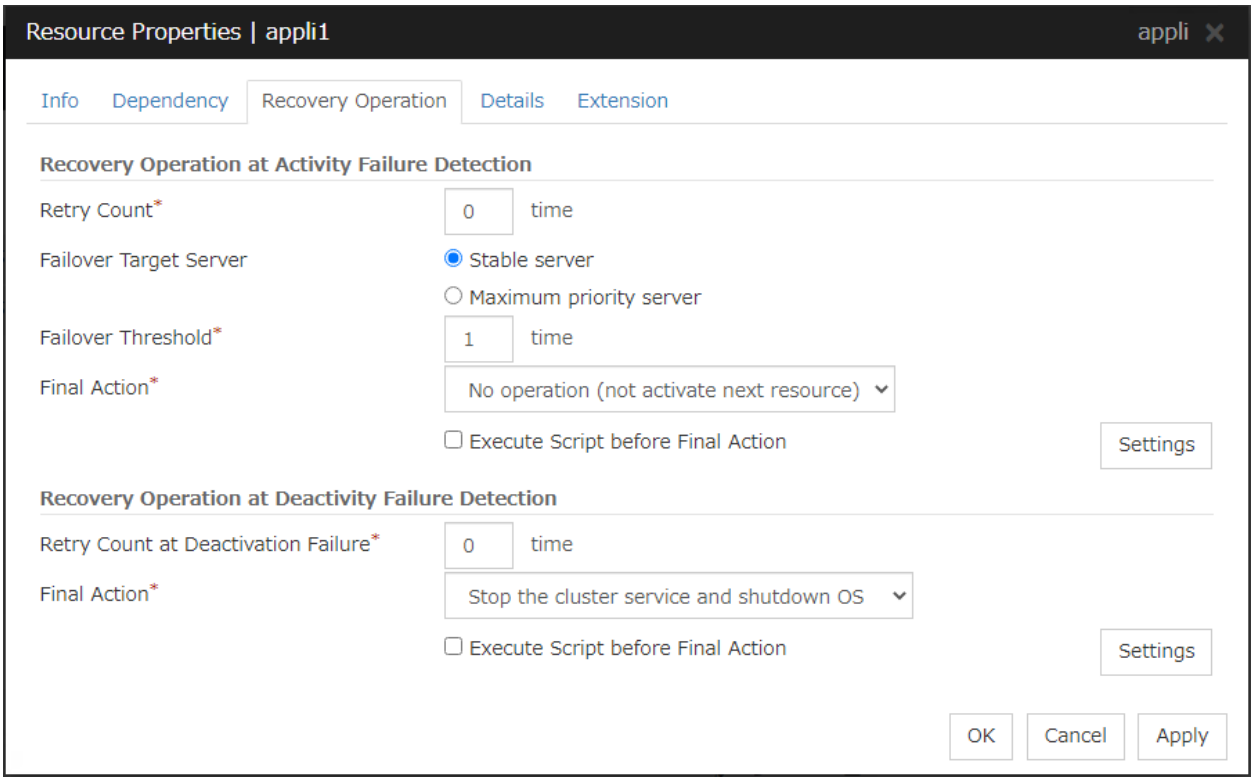
3.5.3 Recovery Operation tab

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**, failover to the server specified in the **Failover Target Server** 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.



Recovery Operation at Activation Failure Detection

Retry Count (0 to 99)

Enter how many times to retry activation when an activation error is detected. If you set this to zero (0), the activation will not be retried.

Failover Target Server

Select a Failover Target Server for the failover that takes place after activation retries upon activation error detection have failed for the number of times specified in **Retry Count**.

- Stable Server
  The failover destination is the server where least resource errors have been detected.
  If two or more servers that meet the above condition exist, failover takes place by selecting one of them according to the failover policy of the group.
- Maximum Priority Server
  Failover takes place according to the failover policy settings of the group.

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** when an error in activation is detected.

If you set this to zero (0), failover will not be executed.

When **Server** is selected for **Failover Count Method** on the **Extension** tab in the **Cluster Properties**, specify any number (0 to 99) for the failover threshold count.

When **Cluster** is selected for **Failover Count Method** on the **Extension** tab in the **Cluster Properties**, configure the following settings for the failover threshold count.

- Set as many as the number of the servers

Set the failover threshold count to the number of servers.

- Specify Number
  Specify any number for the failover threshold count.

For the settings of **Failover Count Method**, refer to "*Extension Tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

Final Action

Select an action to be taken when activation retry failed the number of times specified in **Retry Count** 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)
- No Operation (Not activate next resource)
- Stop Group
- Stop cluster service
- Stop cluster service and shutdown OS
- Stop cluster service and reboot OS
- Generating of intentional Stop Error

For details on the final action, see "*Final action*".

Execute Script before Final Action

Select whether script is run or not before executing final action when an activation failure is detected.

- When the checkbox 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 checkbox 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)
- No Operation (Not deactivate next resource)
- Stop cluster service and shutdown OS

- Stop cluster service and reboot OS
- Generating of intentional Stop Error

For details on the final action, see "*Final action*".

Note: If you select **No Operation** 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.

Execute Script before Final Action

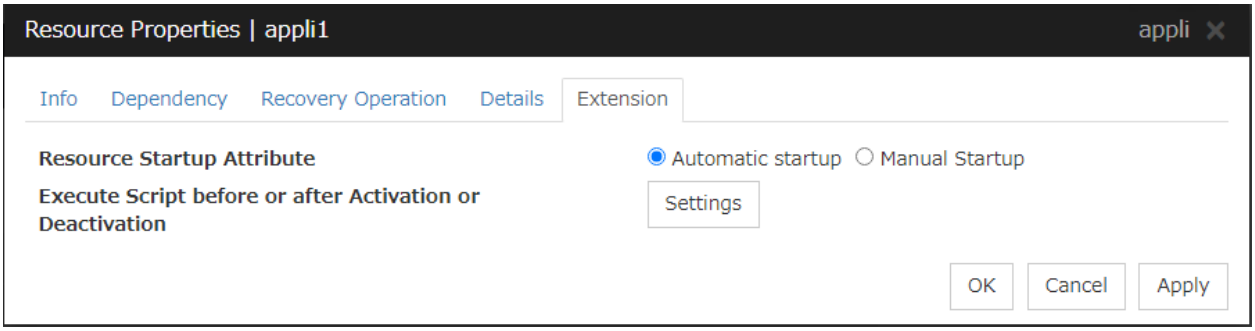
Select whether script is run or not before executing final action when a deactivation failure is detected.

- When the checkbox 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 checkbox 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.

3.5.5 Extension tab

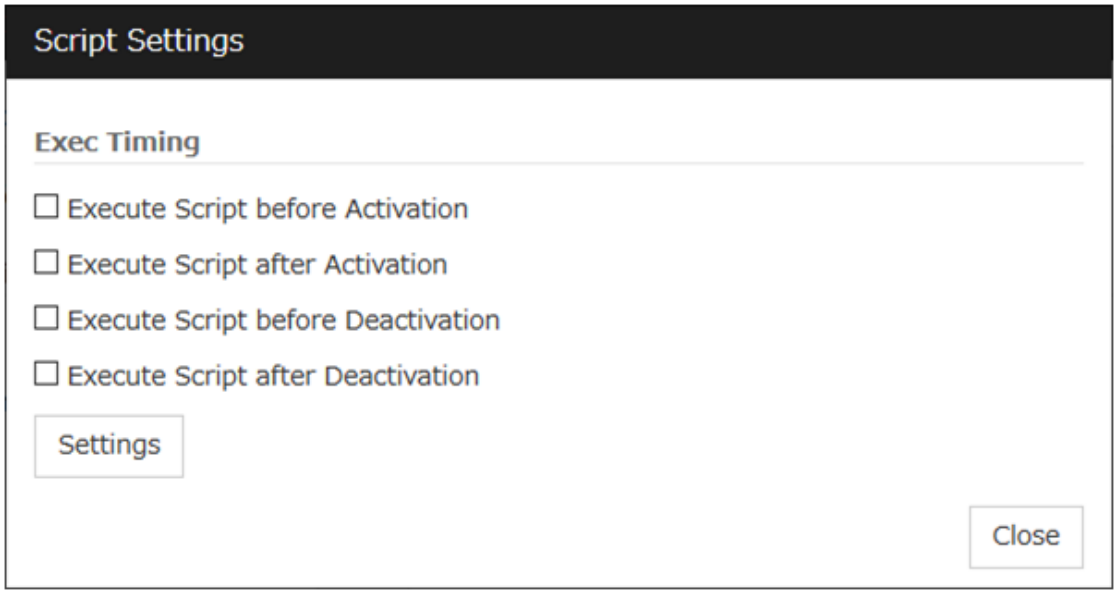


Resource Startup Attribute

Select whether to automatically start up the resource in starting up the group or manually (by using Cluster WebUI or the clprsc command).

Execute Script before or after Activation or Deactivation

Select whether script is run 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

- When the checkbox is selected
  The script is executed before the resource is activated.
- When not selected
  The script is not executed before the resource is activated.

Execute Script after Activation

- When the checkbox is selected
  The script is executed after the resource is activated.
- When not selected
  The script is not executed after the resource is activated.

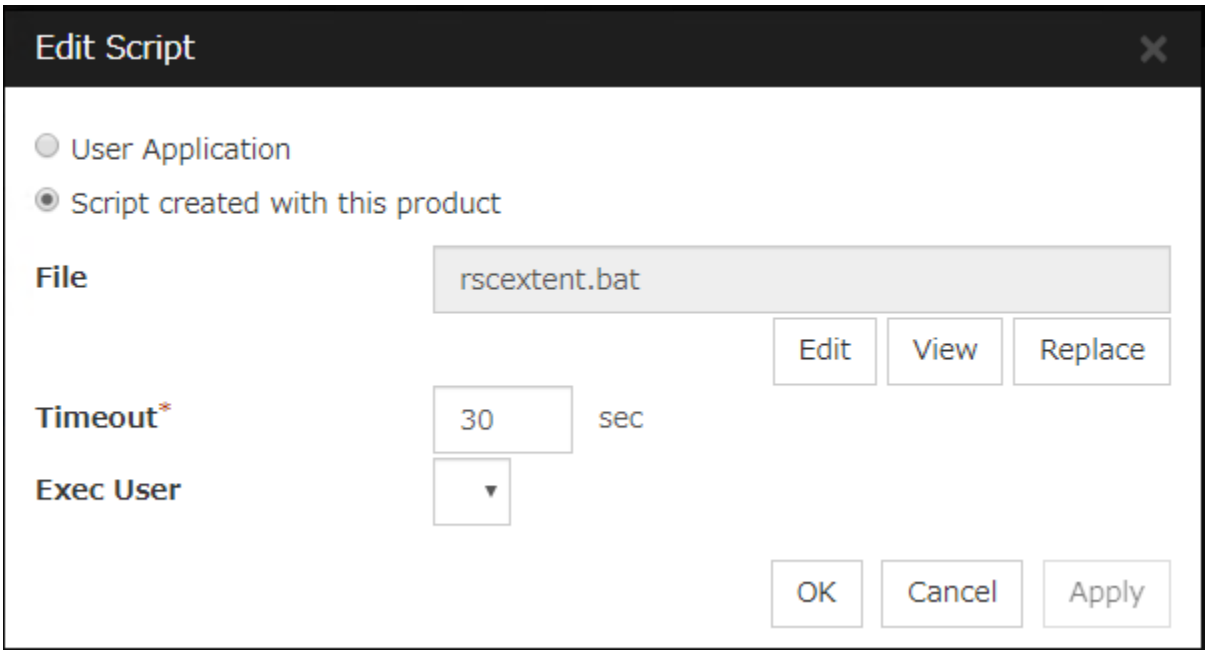
Execute Script before Deactivation

- When the checkbox is selected
  The script is executed before the resource is deactivated.
- When not selected
  The script is not executed before the resource is deactivated.

Execute Script after Deactivation

- When the checkbox is selected
  The script is executed after the resource is deactivated.
- When not selected
  The script is not executed after the resource is deactivated.

To configure the script settings, click **Settings**.



User Application

Use an executable file (executable batch 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 you specify only the name of the executable file, you must configure the path with environment variable in advance. If there is any blank in the absolute path or the file name, put them in double quotation marks ("") as follows.

Example:

"C:\Program Files\script.bat"

If you want to execute VBScript, enter a command and VBScript file name as follows.

Example:

cscript script.vbs

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 batch 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.

Exec User

Select a user by whom the script is to be executed, from users registered in the **Account** tab of **Cluster Properties**.

If no user is specified, the script is run by the local system account.

3.6 Understanding application resources

You can register applications managed by EXPRESSCLUSTER and executed when a groups in EXPRESSCLUSTER starts, stops, fails over or moves. It is also possible to register your own applications in application resources.

3.6.1 Dependency of application resources

By default, application resources depend on the following group resource types:

Group resource type
Floating IP resource
Virtual IP resource
Virtual computer name resource
Disk resource
Mirror disk resource
Hybrid disk resource
Registry synchronization resource
CIFS resource
AWS elastic ip resource
AWS virtual ip resource
AWS secondary ip resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

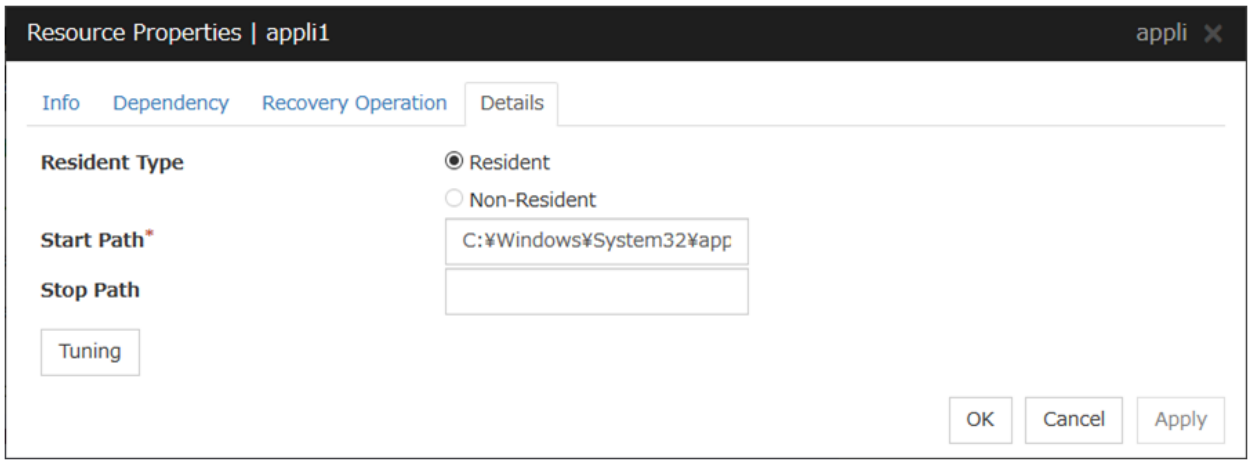
3.6.2 Application resources

Application resources are the programs that are executable from the command line by the files whose extension is exe, cmd, bat, or other.

3.6.3 Note on application resources

An application to be run from application resources must be installed on all servers in failover and must have the same version.

3.6.4 Details tab



Resident Type

Specify the type of the application. Select one of the following:

- Resident
  Select this when the application resides in EXPRESSCLUSTER.
- **Non-**Resident
  Select this when the application does not reside (Process returns right after being executed) in EXPRESSCLUSTER.

Start Path (Within 1023 bytes)

Specify the name of the file that can be run when the application resource is started.

Stop Path (Within 1023 bytes)

Specify the name of the file that can be run when the application resource is stopped. The operation is as described below if the resident type is Resident.

- If the stop path is not specified
  The application started by EXPRESSCLUSTER in the inactive state is stopped.
- If the stop path is not specified
  The application started by executing the application specified for the stop path in the inactive state is stopped.

Note: For the **Start Path** and **Stop Path**, specify an absolute path to the executable file or the name of the executable file of which the path configured with environment variable is effective. Do not specify a relative path. If it is specified, starting up the application resource may fail.

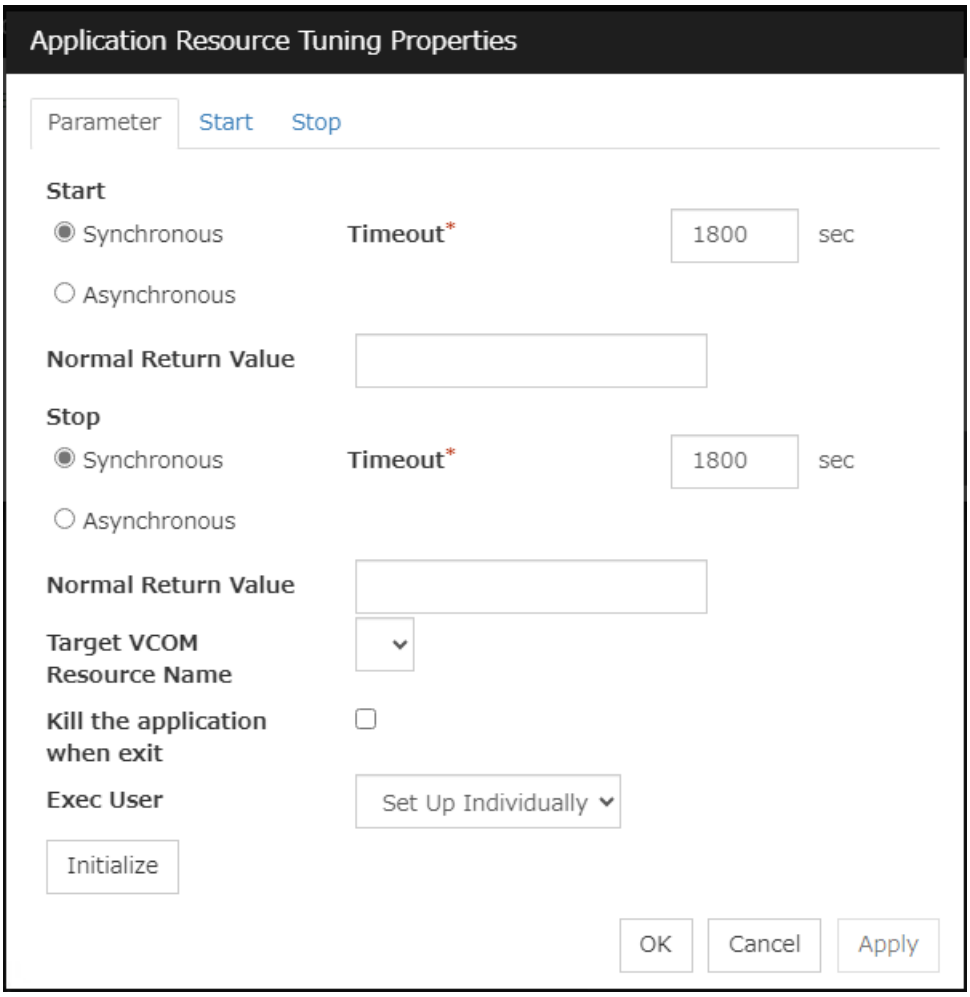
Tuning

Use this button to display the **Application Resource Tuning Properties** dialog box. Configure the detailed settings for the application resources.

Application Resource Tuning Properties

Parameter tab

Detailed parameter settings are displayed on this tab.



Synchronous (Start)

This setting is not available for a resident application.
If the application is non-resident, select this to wait for the application to stop when it is run.

Asynchronous (Start)

This setting is not available for a resident application.
If the application is non-resident, select this so as not to wait for the application to stop when it is run.

Normal Return Value (Start) (Within 1023 bytes)

This entry field cannot be entered when **Asynchronous** is selected.
Specify what error code returned from the executable file set by **Start Path** is normal when **ResidentType** is **Non-resident**.

- When there is no value
  The return value is ignored.
- When there is a value
  Observe the following input rules.
  - Values can be separated by commas (for example, 0, 2, 3).
  - Values can be specified using a hyphen (for example, 0-3).

Note: In case that a batch file is specified as the executable file, an error cannot be detected when 1 is specified as **Normal Return Value** because 1 is returned when an error occurs with cmd.exe which executes the batch file.

Synchronous (Stop)

If the application is resident, and the stop path is not specified, select this to wait for the currently running application to stop. If the application is resident, and the stop path is specified, select this to wait for the application specified for the stop path to stop.

If the application is non-resident, select this to wait for the application to stop when it is run.

Asynchronous (Stop)

If the application is resident, and the stop path is not specified, select this to wait for the currently running application to stop. If the application is resident, and the stop path is specified, select this to wait for the application specified for the stop path to stop.

If the application is non-resident, select this so as not to wait for the application to stop when it is run.

Normal Return Value (Stop) (Within 1023 bytes)

This entry field cannot be entered when **Asynchronous** is selected.

Specify what error code returned from the executable file set by **Stop Path** is normal when **Resident Type** is **Non-resident**.

- When there is no value
  The return value is ignored.
- When there is a value
  Observe the following input rules.
  - Values can be separated by commas (for example, 0, 2, 3).
  - Values can be specified using a hyphen (for example, 0-3).

Note: In case that a batch file is specified as the executable file, an error cannot be detected when 1 is specified as **Normal Return Value** because 1 is returned when an error occurs with cmd.exe which executes the batch file.

Timeout (Start) (1 to 9999)

This setting is not available for a resident application.

Configure the timeout value to wait (synchronous) for a non-resident application to stop when the application is run. A value can be entered only when **Synchronous** is selected. If the application does not stop within the timeout value set here, it is considered as an error.

Timeout (Stop) (1 to 9999)

For a resident application, configure the timeout value to wait (**Synchronous**) for the currently running application or the application specified for the stop path to stop.

The timeout value can be set only when **Synchronous** is selected. If the application does not stop within the timeout value set here, it is considered as an error.

Target VCOM Resource Name

Select a virtual computer name used as a computer name for the application resource. Virtual computer names and resource names that exist in the failover group where the application resource belong to are listed.

When you specify this parameter, add the following environment variables and then start the application:

COMPUTERNAME=<virtual computer name>
_CLUSTER_NETWORK_FQDN_=<virtual computer name>
_CLUSTER_NETWORK_HOSTNAME_=<virtual computer name>
_CLUSTER_NETWORK_NAME_=<virtual computer name>

Kill the application when exit

Specify whether or not to forcibly terminate the application as termination of deactivation. If this is selected, the application is forcibly terminated instead of normal termination. This is effective only when **Resident Type** is set to **Resident** and the stop path is not specified.

Exec User

Select a user by whom the application is to be executed, from users registered in the **Account** tab of **Cluster Properties**.

With **Set Up Individually** specified, the settings of the user in the **Start** and **Stop** tabs are applied.

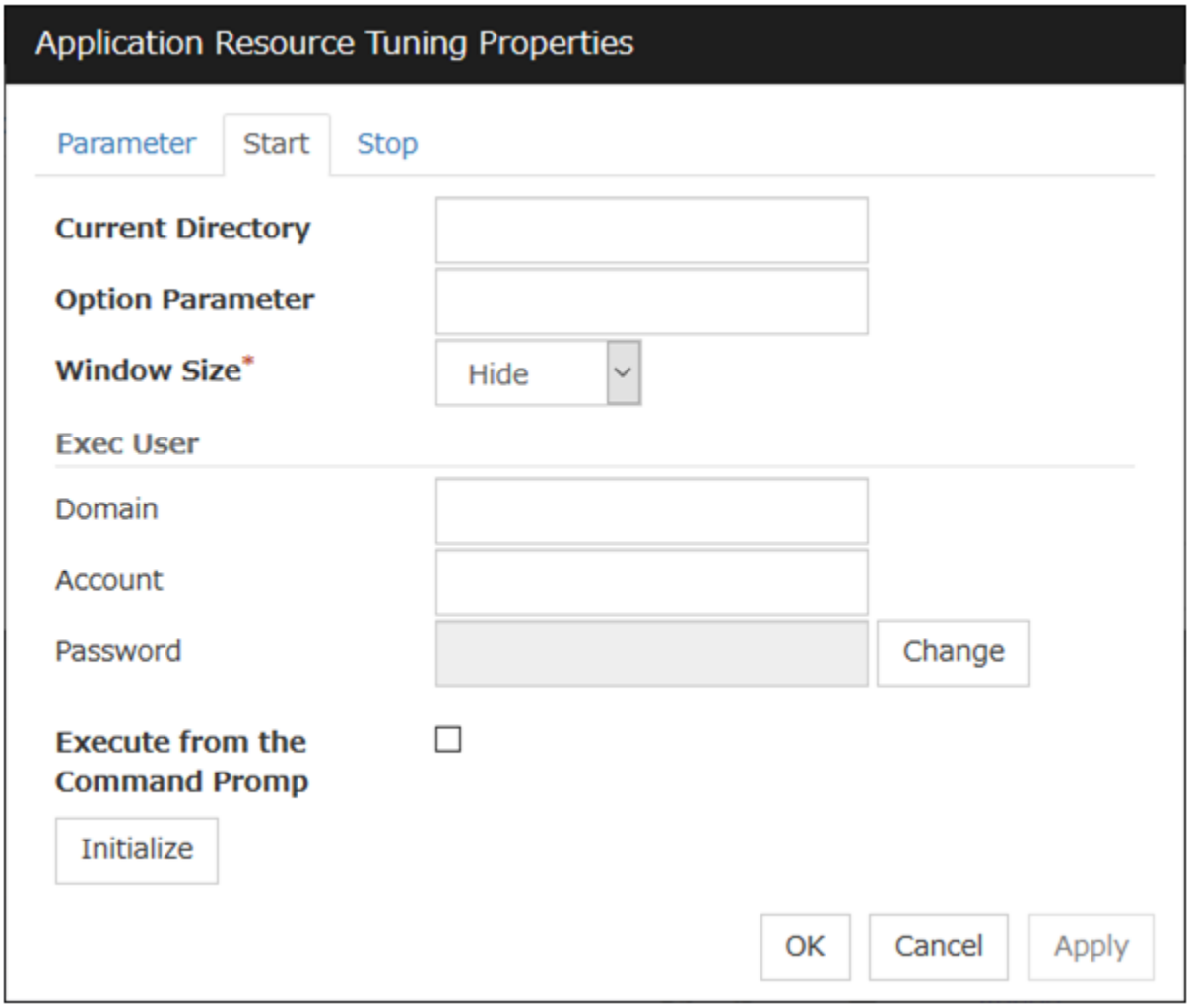
With any value other than **Set Up Individually** specified, the settings in the **Start** and **Stop** tabs are not used: Those of the user specified for this parameter are applied.

Initialize

Click **Initialize** to reset the values of all items to their default values.

Start and Stop tabs

A detailed setting for starting and stopping the application is displayed.



Current Directory (Within 1023 bytes)

Specify a directory for running the application.

Option Parameter (Within 1023 bytes)

Enter parameters to be entered for the application. If there are multiple parameters, delimit parameters with spaces. For a parameter that includes a space, enclose the parameter with double quotation marks.

Example: "param 1" param2

Window Size

Select the size of the window for running the application from the following:

- **Hide**
  The application is not displayed.
- **Normal**
  The application is displayed in a regular window size.
- **Maximize**
  The application is displayed in a maximum window size.
- **Minimize**
  The application is displayed in a minimum window size.

Exec User Domain (Within 255 bytes)

Specify the domain of a user account that runs the application.

In the case of **Stop** tab, it is unnecessary to stop and/or resume the group.

Exec User Account (Within 255 bytes)

Specify the user account that runs the application.[1]

In the case of **Stop** tab, it is unnecessary to stop and/or resume the group.

Exec User Password (Within 255 bytes)

Specify the password for the user account that runs the application.

In the case of **Stop** tab, it is unnecessary to stop and/or resume the group.

Execute from the Command Prompt

Specify whether to run the application from the command prompt (cmd.exe). Specify this when running an application (such as JavaScript and VBScript) whose extension is other than exe, cmd, or bat.

Initialize

Click **Initialize** to reset the values of all items to their default values.

[1] When Exec User Account is left blank, the application is run by the local system account.

3.7 Understanding floating IP resources

3.7.1 Dependencies of floating IP resources

By default, this function does not depend on any group resource type.

3.7.2 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.

Clients access Server 1 at its floating IP (FIP) address.

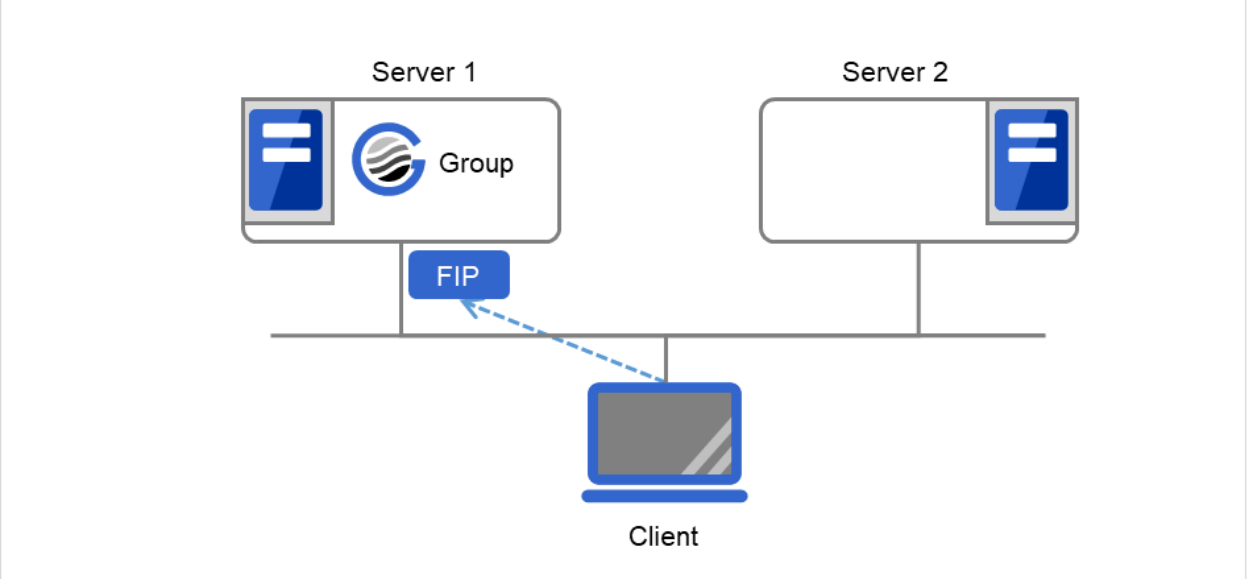


Fig. 3.43: Access to the floating IP address (1)

Even if a failover occurs from Server 1 to Server 2, clients access the FIP address without being aware of the actual, changed destination.

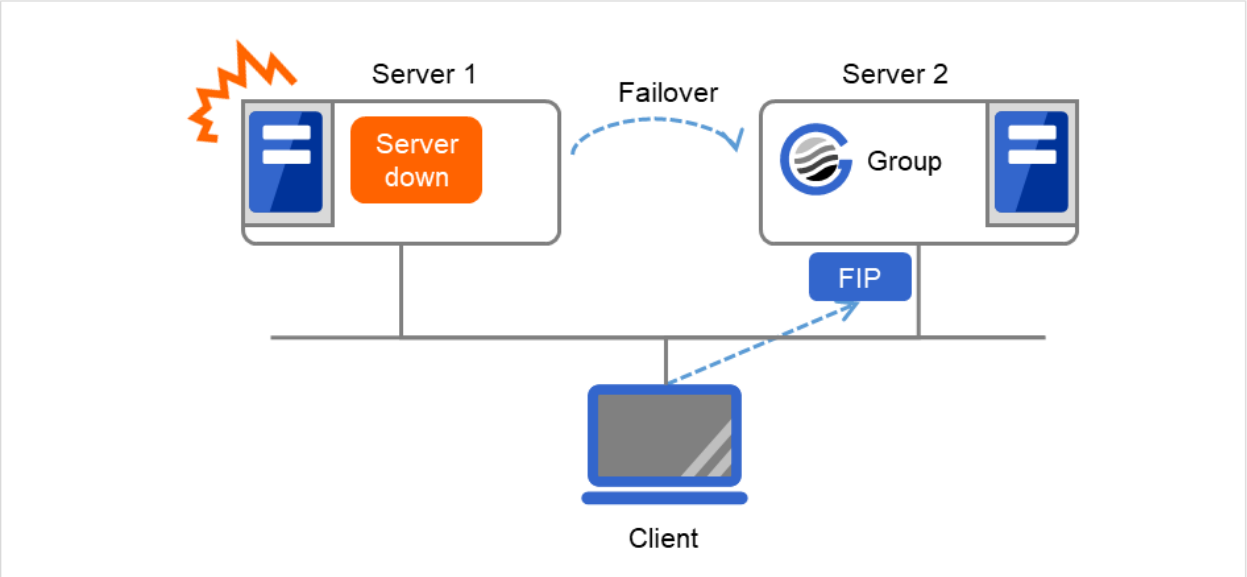


Fig. 3.44: Access to the floating IP address (2)

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, you can assign global IP addresses such as Internet.

You can also allocate IPv6addresses to floating IP addresses.

Switching method

MAC addresses on the ARP table are switched by sending ARP broadcasting packets from the server on which floating IP resources are activated.
A floating IP resource does not have the functionality to update ARP broadcasting packets periodically. Therefore, update the ARP table of a network device by using a custom monitor resource as required.

Routing

You do not need to make 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.

3.7.3 Notes on floating IP resources

If the FIP is activated forcibly when there is an IP address overlap, the NIC is invalidated due to the Windows OS specifications. Therefore, do not use **Forced FIP Activation**.

Notes on allocating floating IP addresses to IPv4 addresses

- Stopping the floating IP resource routing information may be deleted. To avoid this phenomenon, specify an interface in the IF option when registering routing information as follows:

  route -p add [destination] [Mask netmask] [gateway] [IF interface]

Notes on allocating floating IP addresses to IPv6 addresses

- IPv6 addresses should not be specified in Management Resources in Management Group.
- In the setting of virtual computer name resource, setting connection of floating IP resource assigned to IPv6 is invalid.
- When the floating IP address is set to perform to register in virtual computer name resource dynamically and it is selected to correspond to virtual computer name, the floating IP address cannot be allocated to IPv6 address.
- Stopping the floating IP resource routing information may be deleted. To avoid this phenomenon, specify an interface in the IF option when registering routing information as follows:

  route -p add [destination] [Mask netmask] [gateway] [IF interface]

When a floating IP resource is set for a physical host, Windows registers the physical host name and FIP record in the DNS (if the property of the corresponding network adapter for registering addresses to the DNS is set to ON). To convert the IP address linked by the physical host name resolution into a physical IP address, set the relevant data as follows.

- Check the setting of the network adapter to which the corresponding floating IP address is assigned, by choosing **Properties** - **Internet Protocol Version 4** - **Advanced** - **DNS** tab - **Register this connection's address in DNS**. If this check box is selected, clear it.
- Additionally, execute one of the following in order to apply this setting:
  1. Reboot the DNS Client service.
  2. Explicitly run the ipconfig/registerdns command.
- Register the physical IP address of the network adapter to which the corresponding floating IP address is assigned to the DNS server statically.

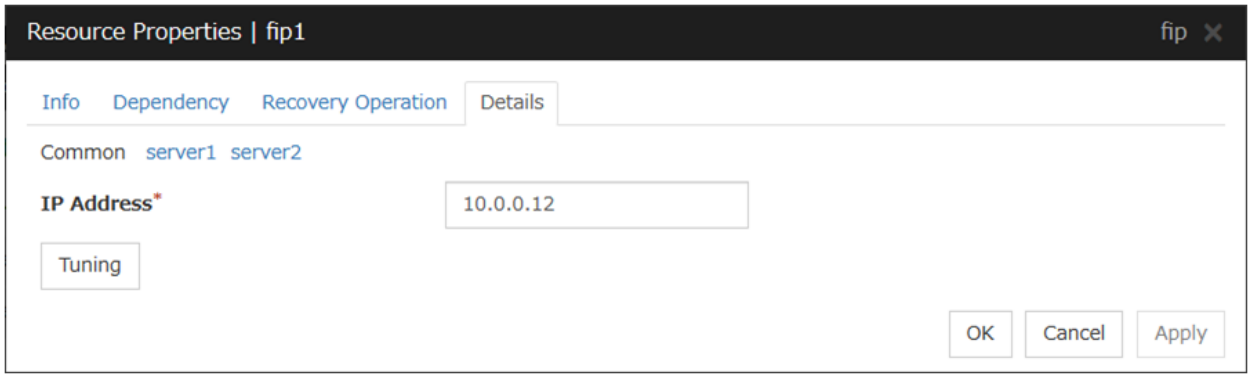
A floating IP resource adds a floating IP address to an NIC by using a Windows OS API. If the transmission source change feature is not used, the skipassource flag is not set and therefore does not take effect after the activation of a floating IP resource.

Notes on enabling the transmission source change feature of a floating IP resource

- This feature changes the existing skipassource setting.
- This feature cannot be used for any IPv6 IP address.

For the usage of the Network Load Balancing (NLB) function of OS in the servers of the cluster, see " Coexistence with the Network Load Balancing function of the OS " in " Notes when creating the cluster configuration data" in " Notes and Restrictions" in the " Getting Started Guide".

3.7.4 Details tab



IP Address

Enter the floating IP address to be used.

If you specify an IPv4 address, the number of mask bits as 24 by default, find the address of the subnet mask on the local computer to match, you can add the floating IP address to the appropriate index.

Follow the instruction below to enter an IPv6 address.

Example: fe80::1

With the default value of prefix length 64 bit, floating IP resource searches for the addresses that have matching prefix on the local computer and adds floating IP address to the matching index. When there is more than one matching address, address is added to the index that has the largest index value.

In order to specify the prefix length explicitly, specify the **prefix length** after the address.

Example: fe80::1/8

In order to specify the index explicitly, specify **%index** after the address.

Example: fe80::1%5

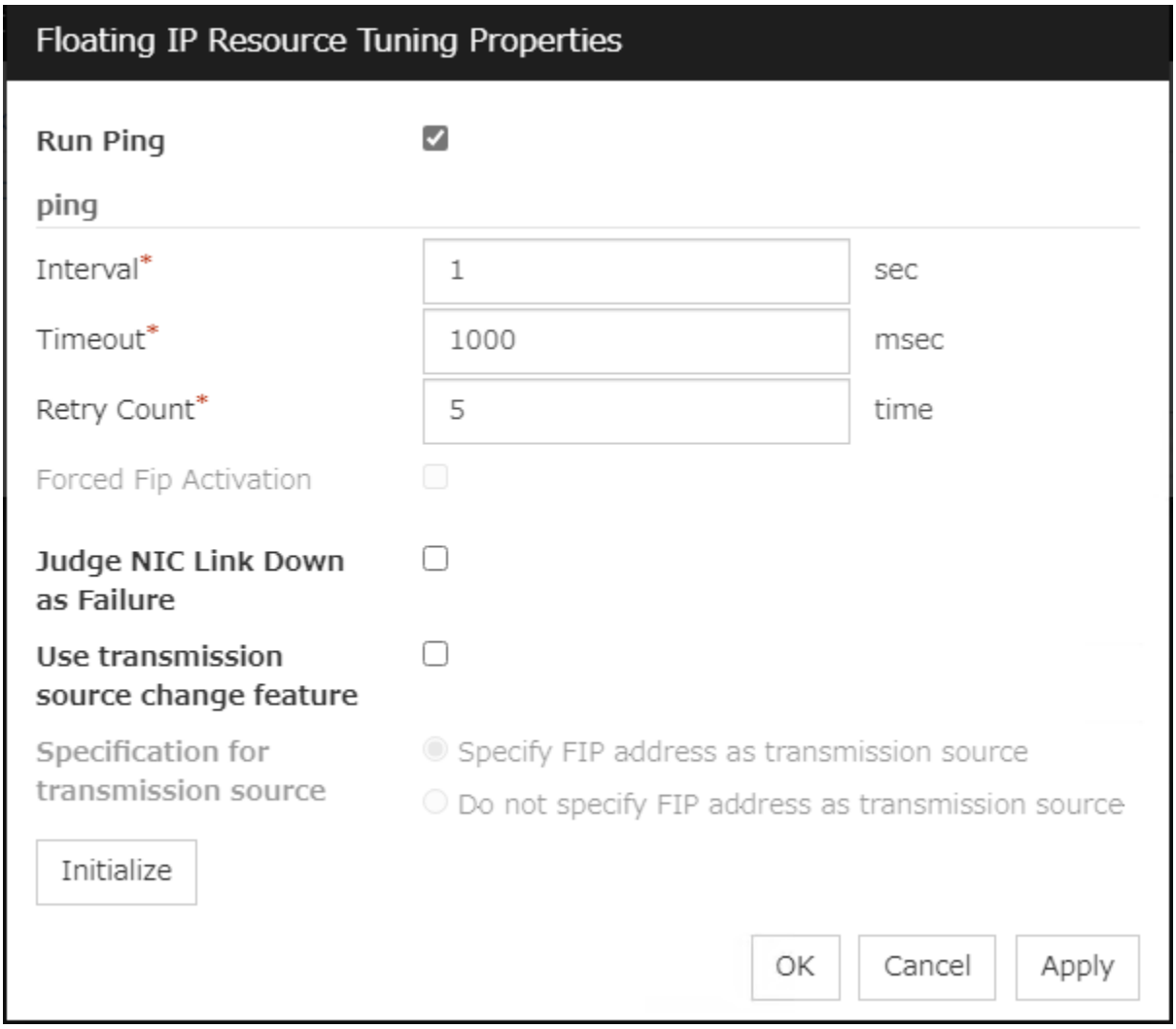
The example above shows how to add a floating IP address to the index5.

Tuning

Opens the **Floating IP Resource Tuning Properties** dialog box where you can make detailed settings for the floating IP resource.

Floating IP Resource Tuning Properties

Detailed settings on floating IP resource are displayed.



Run ping

Specify this to verify if there is any overlapped IP address before activating floating IP resource by using the ping command.

- When the checkbox is selected:
  The ping command is used.
- When the checkbox is not selected:
  The ping command is not used.

ping

These are the detailed settings of the ping command 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 in seconds.
- Timeout (1 to 999999)
  Set timeout of the ping command in milliseconds.
- 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.Be sure to set it to off.
  - When the checkbox is selected:
    Forced activation is performed.
  - When the checkbox is not selected:
    Forced activation is not performed.

Judge NIC Link Down as Failure

Specify whether to check for an NIC Link Down before the floating IP resource is activated.

- When the checkbox is selected:
  In the case of an NIC Link Down, the floating IP resource is not activated.
- When the checkbox is not selected:
  Even in the case of an NIC Link Down, the floating IP resource is activated.

Use transmission source change feature

Choose whether to change the transmission source for an NIC to which a floating IP address is given.

- When the checkbox is selected:
  The transmission source change feature is used.
- When the checkbox is not selected:
  The transmission source change feature is not used.

Specification for transmission source

Specify the transmission source.

- Specify FIP address as transmission source
  Enable the skipassource of a non-FIP address assigned to the NIC where the FIP address is given.
- Do not specify FIP address as transmission source
  Enable the skipassource of the FIP address.

Initialize

Click **Initialize** to reset the values of all items to the default values.

3.8 Understanding mirror disk resources

3.8.1 Dependencies of mirror disk resources

By default, this function does not depend on any group resource type.

3.8.2 Mirror disk

Mirror disks are a pair of disks that mirror disk data between two servers in a cluster.

Mirroring is performed by partition. It requires the RAW partition (cluster partition) to record the management data as well as the data partition that is to be mirrored. In addition, the license of EXPRESSCLUSTER X Replicator 5.2 for Windows is necessary on both servers that mirroring is performed.

- Disk type and geometry
  The size of the data partitions has to be completely the same by byte on both servers. If the disk size and geometry are different on each server, it may be unable to create partitions that are exactly the same size. Thus the geometry of disks which are used to secure data partitions needs to be the same on both servers.
  It is recommended to use disks of the same model on both servers.

  Example:

Combination	Server 1	Server 2
Correct	SCSI	SCSI
Correct	IDE	IDE
Incorrect	IDE	SCSI

Combination	Head	Sector	Cylinder
Correct and Server 1	240	63	15881
Correct and Server 2	240	63	15881
Incorrect and Server 1	240	63	15881
Incorrect and Server 2	120	63	31762

  If it is not possible to make both servers have exactly the same **disk type and geometry, check the size of data partitions in precise by using the clpvolsz command. If the disk size does not match, shrink the larger partition by using the clpvolsz command again.**

  For details on the clpvolsz command, see "*Tuning partition size (clpvolsz command)*" in "*9. EXPRESSCLUSTER command reference*" in this guide.

- Drive letter of partition
  Configure the same drive letter for a data partition and cluster partition on both servers.

  Example: Adding a SCSI disk to each server to create a pair of mirroring disks.

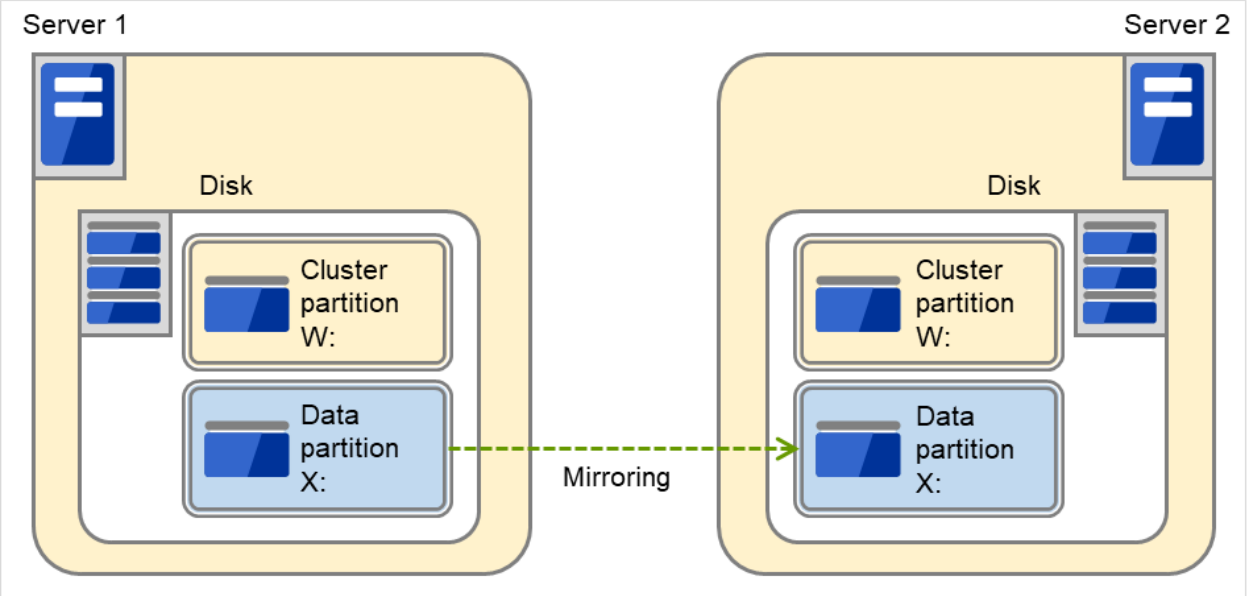


Fig. 3.45: Adding disks for a pair of mirror disks

Example: Using available area of the IDE disk on which OS of each server are stored to create a pair of mirroring disks.

The following figure illustrates using the free space of each disk as a mirror partition device (cluster partition and data partition):

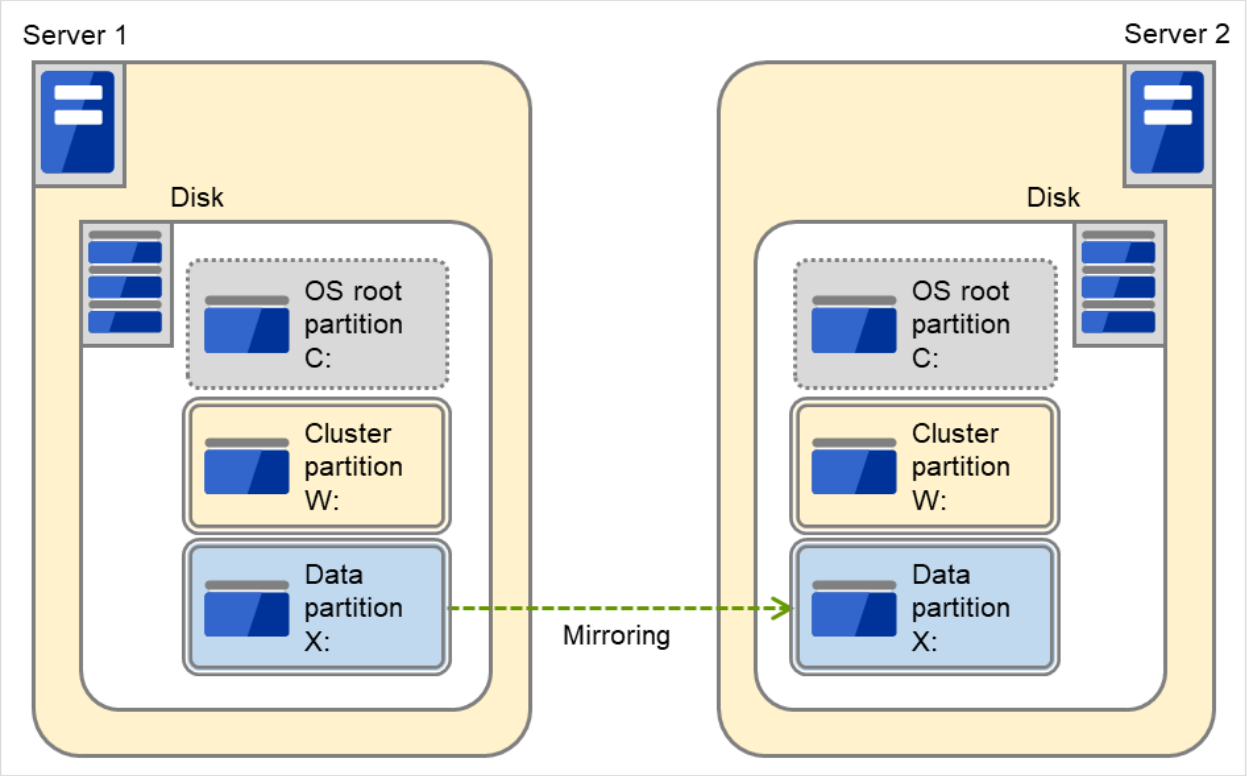


Fig. 3.46: Using the free space of each disk for a mirror partition

  - A mirror partition (cluster partition, data partition) can be allocated on the same disk as OS.
    * When the maintainability at occurrence of failure is important:
      It is recommended to have another disk for a mirror than a disk for OS in advance.
    * When a logical disk cannot be added because of the limitations of the hardware RAID specifications:
      When it is difficult to change the configuration of a logical disk because hardware RAID is pre-installed:
      A mirror partition (cluster partition, data partition) can be allocated on the same disk as OS.

- Disk allocation
  One mirror disk resource can perform mirroring to only one partition. However, multiple partitions can be mirrored by creating multiple mirror disk resources.
  It is possible to create multiple mirroring resources by allocating multiple data partitions and cluster partitions on a single disk.

  Example: Adding one SCSI disk to each server to create two pairs of mirroring disks.

  The following figure illustrates each disk on which a pair of a cluster partition and a data partition is created:

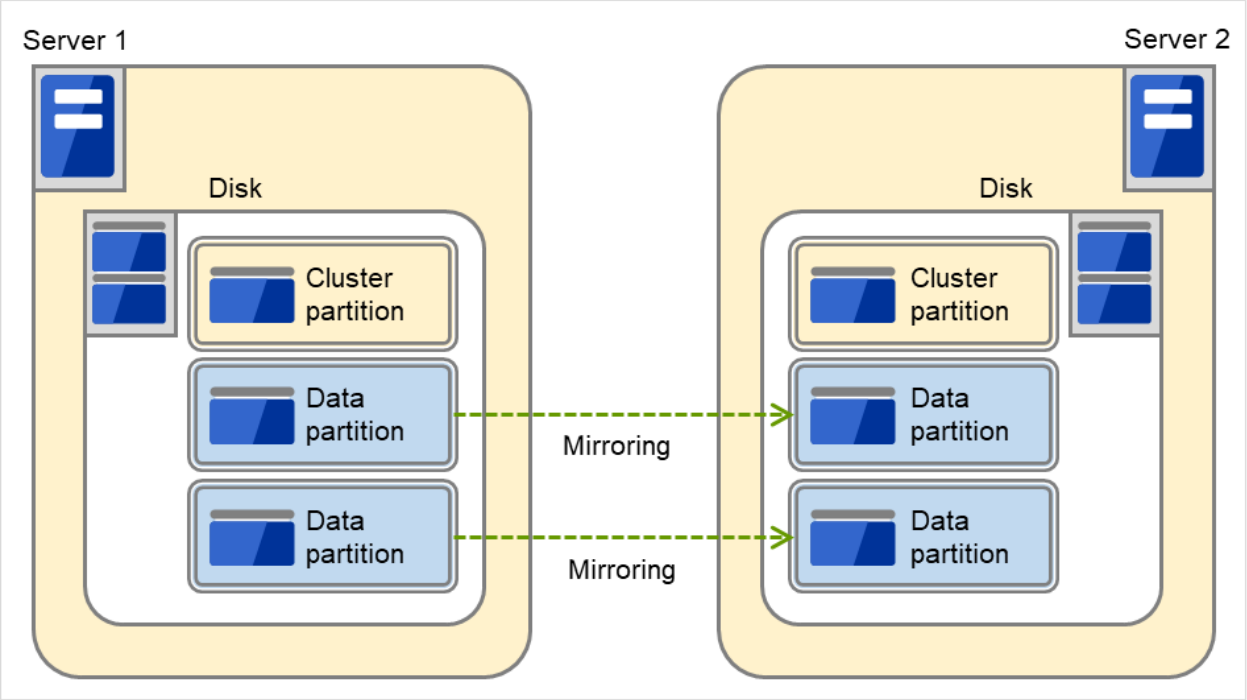


Fig. 3.47: Using multiple areas of each disk for mirror partitions

- Allocate a cluster partition and two data partitions in a pair on a single disk.
- Assign 0 and 1 for the offset index of the cluster partition management area to be used in each data partition.

Example: Adding two SCSI disks for each server to create two mirroring partitions.

The following figure illustrates using mirror partitions prepared from two pairs of disks on which partitions of the same size are created:

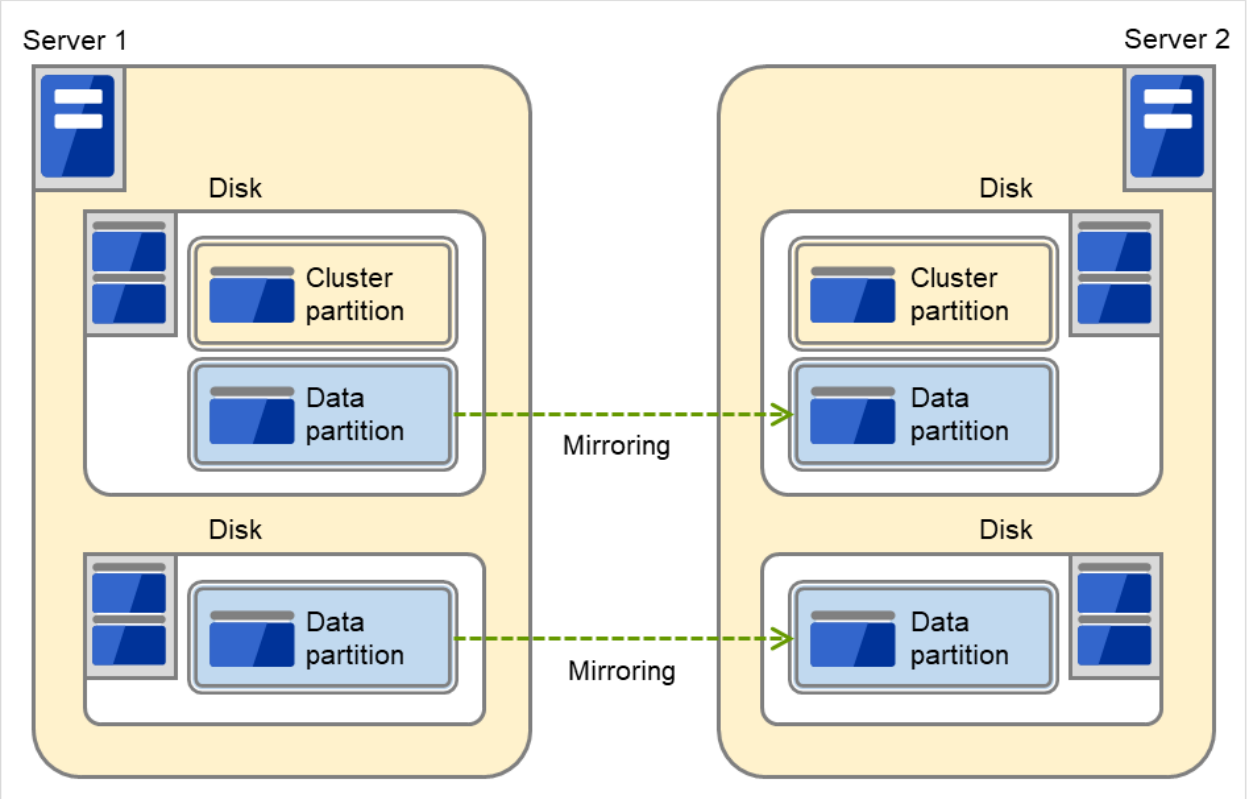


Fig. 3.48: Using two pairs of disks as mirror partitions

- Secure a cluster partition and data partition on the first disk and a data partition on the second disk.
- Routing and Remote Access Assign 0 and 1 for the offset index of the cluster partition management area to be used in each data partition.
- A cluster partition can be secured on each disk. In that case, the offset index is assigned to be 0 and 0.
- When performing mirroring in the asynchronous mode, an access to a cluster partition is generated in accordance with writing in a data partition. The access to a disk can be distributed by securing a cluster partition and data partition on separate disks.

Example: Adding one SCSI disk for three servers to create two mirroring partitions.

The following figure illustrates using data partitions between Server 1 and Server 2 and between Server 2 and Server 3, by preparing each disk for each combination of a cluster partition and two partitions of the same size:

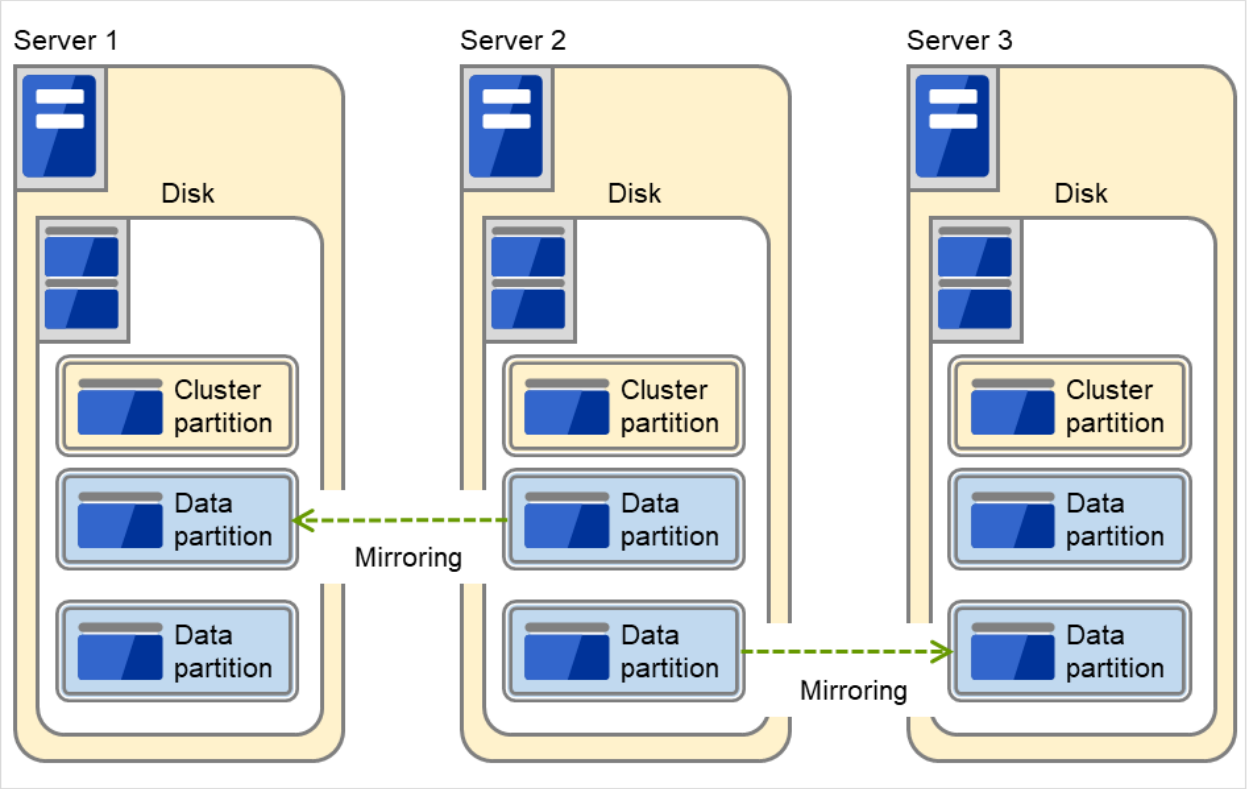


Fig. 3.49: Using multiple areas of each disk for mirror partitions (with three servers)

- Allocate a cluster partition and two data partitions on each server.
- On Server 2, the following two data partitions are required: One is used for mirroring with Server 1 while the other is used for mirroring with Server 3.
- Assign 0 and 1 as the offset index of the cluster partition management area to be used in each data partition.

Data partition

Partitions where data that is mirrored by EXPRESSCLUSTER (such as application data) is stored are referred to as data partitions.
Allocate data partitions as follows:

- Data partition size
  There is no limitation for partition size. Allocate any size of partition.
- Time required for data partition copying
  When a file is copied at initial configuration or disk replacement, the required amount of time increases in proportion to the size of the volume use area. If the volume use area cannot be specified, the required amount of time increases in proportion to the data partition size because the entire area of the volume is copied.
- File system
  Format the partition with NTFS. FAT/FAT32 is not supported.
- Allocate the partition on a basic disk. The dynamic disk is not supported.
- When making data partitions as logistical partitions on the extended partition, make sure the data partitions are logical partition on both servers. The actual size may be different even the same size

is specified on both basic partition and logical partition

- The access to the data partition is controlled by EXPRESSCLUSTER.

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
  1024MiB or more. Depending on the geometry, the size may be larger than 1024MB, but that is not a problem.
- A cluster partition and data partition for data mirroring should be allocated in a pair. If you use one cluster partition with multiple mirror disks, assign a different index number to each mirror disk so that the areas used in the cluster partition do not overlap each other.
- Do not make the file system on cluster partitions. Do not format.
- The access to a cluster partition is limited.

Access control of a data partition

The data partition to be mirrored by a mirror disk resource can be accessed only from the active server where a mirror disk resource is activated.

- EXPRESSCLUSTER is responsible for the access control of the file system. Application's accessibility to a data partition 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.
- By storing data required for applications on data partitions, the data can be automatically used after failing over or moving failover group.

The following figure illustrates mirroring disk data by a pair of Mirror disk 1 with Server 1 and Mirror disk 2 with Server 2:

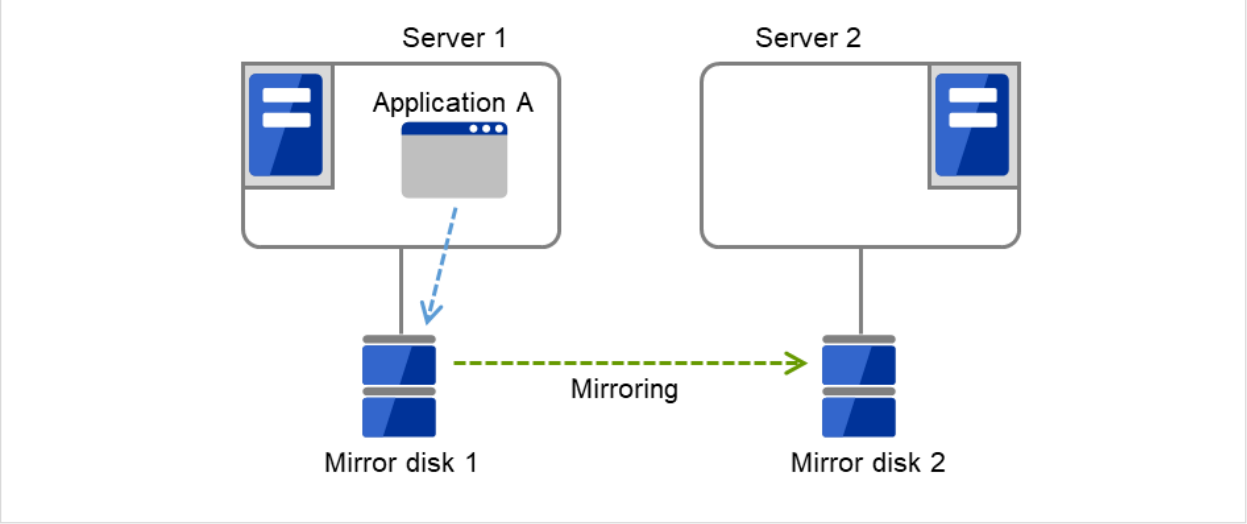


Fig. 3.50: Mirror disk configuration (1)

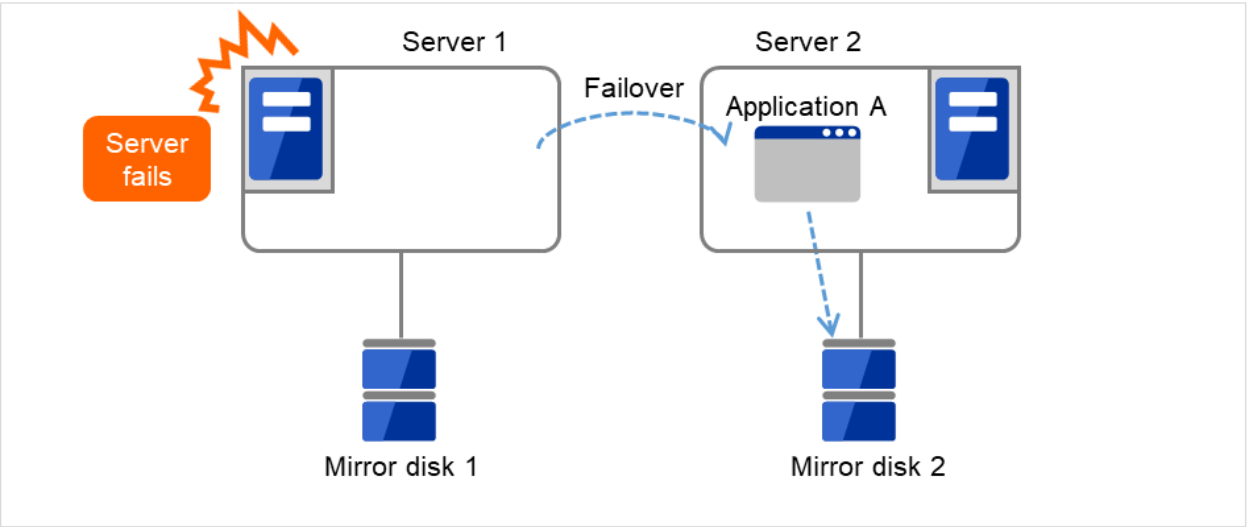


Fig. 3.51: Mirror disk configuration (2)

3.8.3 Understanding mirror parameters

The maximum size of request queues

Configure the size of queues which is used for the mirror disk driver to queue I/O requests on the communication among servers. If you select a larger value, the performance will improve but more memory will be required. If you select a smaller value, less memory will be used but the performance may be lowered.

Note the following when setting the number of queues:

- The improvement in the performance is expected when you set a larger value under the following conditions:
  - Large amount of physical memory is installed on the server and there is plenty of available memory.
  - The performance of the disk I/O is high.
- It is recommended to select a smaller value under the conditions:
  - Small amount of physical memory is installed on the server.
  - I/O performance of the disk is low.

Mirror Connect Timeout

This is the time required to cut a mirror disk connect when there is no response on the communication among servers and/or when the data synchronization has not completed at the time of mirror recovery and/or data synchronization. The time for timeout needs to be configured longer, if the line speed of the mirror disk connect is slow and/or the load to the mirror disk is high.

Adjust this parameter below the timeout value of heartbeat, based on the following calculation.

Heartbeat timeout = Mirror connect timeout + 10 seconds

* For the settings of the heartbeat timeout, see "*Timeout tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

Initial Mirror Construction

Specify if initial mirroring is configured when activating cluster for the first time after the cluster is created.

- Execute the initial mirror construction
  An initial mirroring is configured (disk images of the data partition are fully copied) when activating cluster for the first time after the cluster is created.
- Do not execute initial mirror construction
  Assume that data in the data partition has already matched among servers and do not configure initial mirroring at initial startup after constructing a cluster. When constructing a cluster, it is necessary to make the disk image of the data partition (physical data) identical without using EXPRESSCLUSTER.

Mode

Switch the synchronization mode of mirroring.

Mode	Overview	Explanation
Synchronous	Complete match of the data in the active and standby servers is guaranteed.	Writing the data to the mirrored disk is finished when writing the data to both local and remote disks is finished.
Asynchronous	The order to write in the updated data is guaranteed. However, the latest updated data may be lost, if a failover is performed in the state that a mirror disk resource cannot be deactivated as servers are down. The data is transferred to the remote disk after writing request is queued and performed on the background.	Writing the data to the mirrored disk is finished when writing the data to the local disk is finished. After queuing is kept in the kernel space memory, it is transferred to the user space memory. When the volume of data reaches a limit that the user space memory can keep, the data is sent out to a temporary file and kept there.

Kernel Queue Size

Specify the size of the request for writing to the remote disk to be kept in the kernel space memory when the mode is set to **Asynchronous**. Normally, default value is specified.

Input and output are completed, if writing data can be saved in the kernel queue.

If taking data into the application queue is delayed as the load on CPU is high, the size is set larger. However, if the size is too large, it will result in compressing the system resource.

Application Queue Size

Specify the size of the request for writing to the remote disk to be kept in the user space memory when the mode is set to **Asynchronous**. Normally, the default value is used. However, if a high-speed network is used, the frequency of creating a temporary file can be reduced and the overhead caused by input and output can be decreased by making the queue size larger.

Upper Bound of Communication Band

When the mode is **Asynchronous**, the server tries to transfer data that has been queued to the standby

server. When the channel for mirror disk connection is used for connections for other applications, the communication band may become busy. In this case, by setting the bound of communication band for the mirror disk connect communication, the impact on other communications can be reduced. If the communication band for mirror disk connect is smaller than the average amount of data to be written into the mirror disk, the queued data cannot be fully transferred to the standby server, which can result in overflow and suspension of mirroring. The bandwidth should be large enough for data to be written into the business application.

This function makes a limit to the communication band by having a maximum of one-second pause when the total amount of data to be transferred per second exceeds the configured value. If the size of data to be written into the disk at a time is greater than the configured value, expected performance may not be achieved. For example, even if you set the value of communication band limit to be 64Kbyte or smaller, the actual amount of communication during copy can be greater than the configured value because the size of data to be transferred for a copy of a mirror disk at a time is 64 Kbyte.

See also:

In addition to the limit on the communication band for each mirror disk resource, you can also set a limit on the communication band for each mirror disk connect by using a standard Windows function. For details, see "Limit on the band for mirror disk connect communication" in "The system maintenance information" in the "Maintenance Guide".

History Files Store Folder

Specify the folder that keeps the temporary file which is created when the request for writing to the remote disk in the **Asynchronous** mode cannot be recorded in the application queue. When the communication band runs short, data is recorded up to the limit of the disk space if the limit of the history file size is not specified. Thus, specifying a folder on the system disk runs out of the empty space and the system behavior may become unstable. Therefore, if you want to suspend mirroring when recording data is exceeded a certain size, create a dedicated partition or specify the limit of the history file size.

Do not specify any folder on the cluster partition and data partition to the history files store folder. Also, do not specify a folder containing a 2-byte character in the path.

Thread Timeout

This is the time that timeout is occurred when data cannot be transferred to the application queue from the kernel queue in the mode of **Asynchronous**. When it is timed out, a mirror disk connect is cut.

Timeout may occur, if the data transfer to the application queue is delayed due to high load. In this case, increase the timeout value.

Encrypt mirror communication

Choose whether to encrypt data passing through mirror disk connects.

The applied encryption algorithm is Advanced Encryption Standard (GCM), which supports up to 256-bit key length.

The encryption is recommended if the channels of mirror disk connects include external lines.

Allow failover on mirror break for specified time

Allow a failover to a server, with data in the mirror disk not up to date, to succeed for a specified time since the occurrence of a mirror break.

This enables you to give priority to business continuation even if an unexpected mirror break occurs before or after a failover.

However, carefully consider whether this setting is enabled. This is because the data in the mirror disk may be rolled back.

For more information, see this guide: "2. *Parameter details*" -> "*Cluster properties*" -> "*Mirror Disk tab*".

3.8.4 Examples of mirror disk construction

- Execute the initial mirror construction

  First, create application data to be duplicated (if available before the cluster construction) in the data partition (e.g. initial database) of Mirror disk 1 on the active server in advance. For information on the partition configuration, refer to "3.8.2. *Mirror disk*". Next, install EXPRESSCLUSTER on each of Server 1 and Server 2.

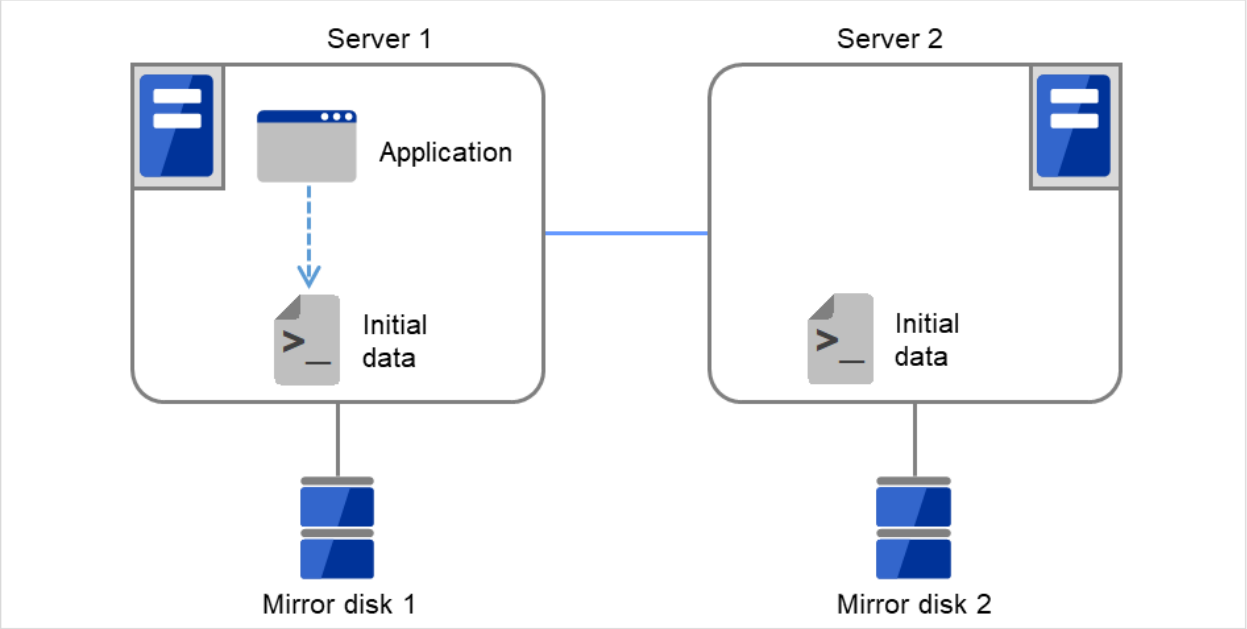


Fig. 3.52: Example of mirror disk construction: executing initial mirror construction (1)

Then start the initial mirror construction. Completely copy the content of Mirror disk 1 on Server 1 to Mirror disk 2 on Server 2.

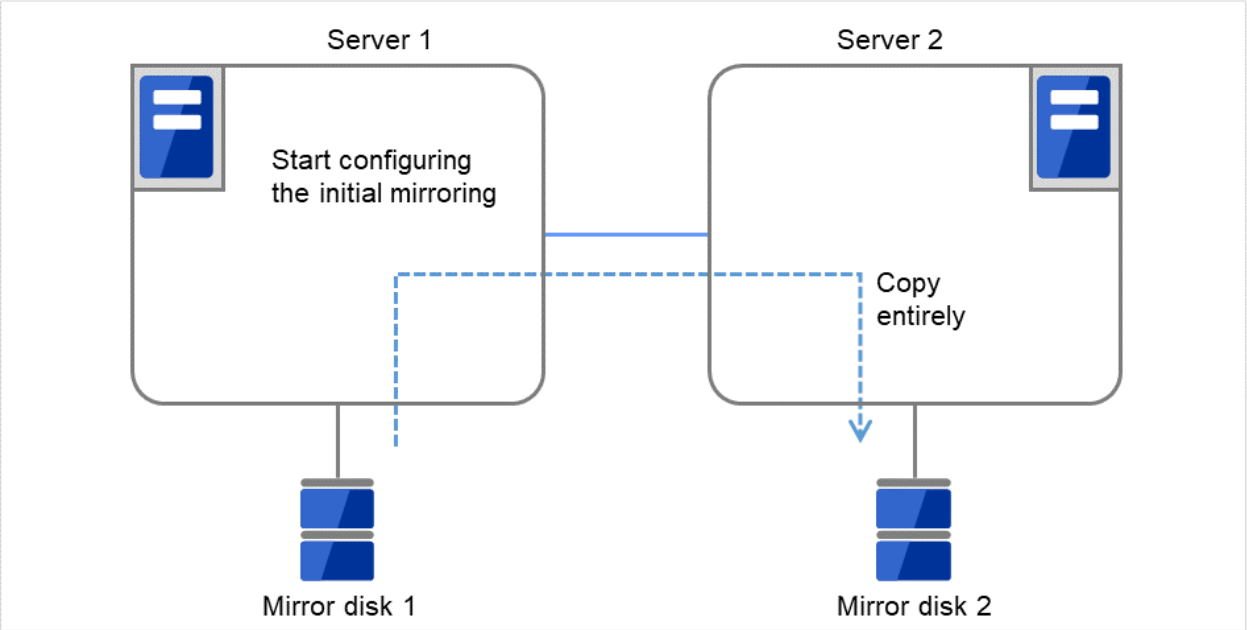


Fig. 3.53: Example of mirror disk construction: executing initial mirror construction (2)

- Do not execute the initial mirror construction

  Follow the procedures below to have identical data in the data partition on both servers:

1. If application data to be duplicated can be prepared before configuring a cluster, create it on data partition of the mirror disk on the active server in advance (ex. initial data of the database).
2. Install EXPRESSCLUSTER and configure a cluster without executing the initial mirror construction.
3. Shut down the cluster.
4. Remove disks that have data partitions on both servers, and connect to the Linux server. Then copy the data in the data partition on the active server to the data partition on the standby server by using the dd command in the state that disks are not mounted.
5. Return disks to the active and standby server and start both servers.

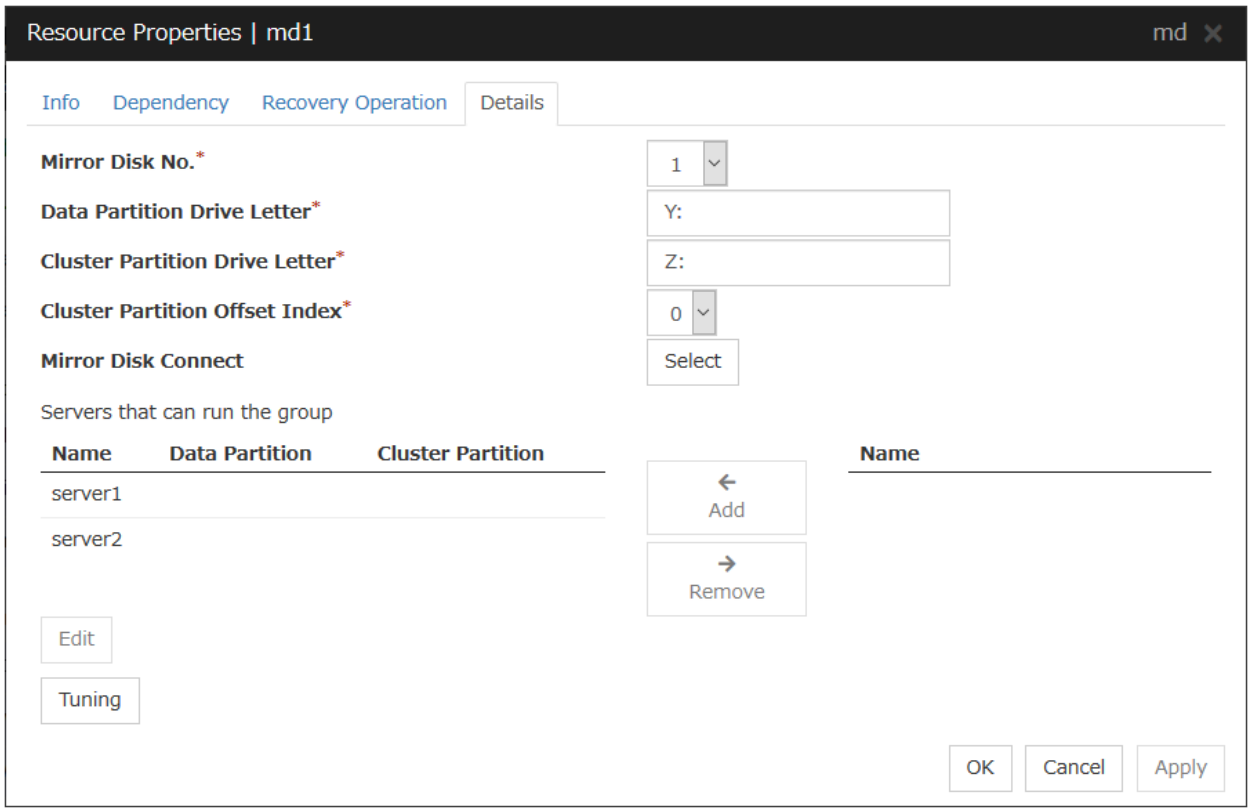
3.8.5 Notes on mirror disk resources

- Set both servers so that the identical partitions can be accessed under the identical drive letter.
- If a drive letter different from those used on partition is set, the drive letter will be changed when the mirror disk resource is started. If the drive letter is used on any other partitions, starting up the mirror disk resource will fail.
- To change the configuration so that the disk mirrored using a hybrid disk resource will be mirrored using a mirror disk resource, first delete the existing hybrid disk resource from the configuration data, and then upload the data. Next, add a mirror disk resource to the configuration data, and then upload it again.
- 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 Data partition	Server 1 Cluster partition	Server 2 Data partition	Server 2 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.

3.8.6 Details tab



Mirror Disk No.

Select the number to be allocated to the mirror partition.

Data Partition Drive Letter (Within 1023 bytes)

Specify the drive letter (A to Z) of the data partition.

Cluster Partition Drive Letter (Within 1023 bytes)

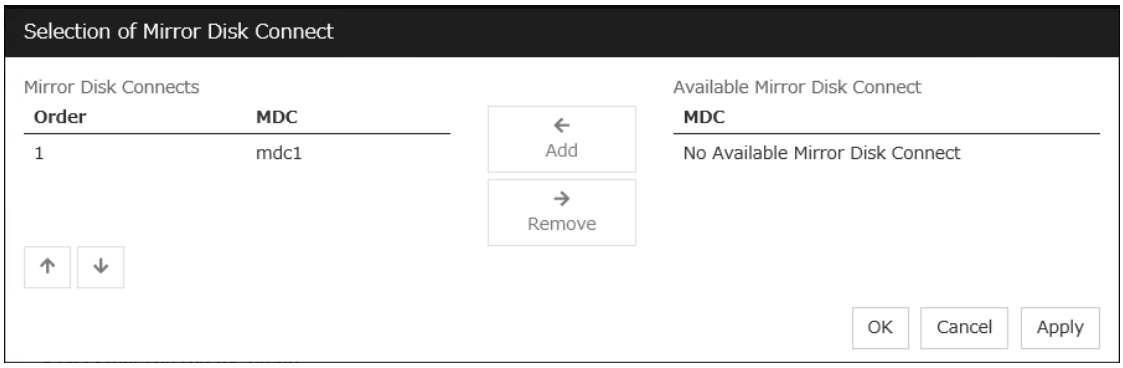
Specify the drive letter (A to Z) to the cluster partition.

Cluster Partition Offset Index

Select an index number for the area used in the cluster partition. When using the multiple mirror disks, assign different numbers for each mirror disk so that the areas to be used in the cluster partition are not overlapped.

Select

Select the communication path for the data mirroring communication (mirror disk connect). Click Select to display the **Selection of Mirror Disk Connect** dialog box.

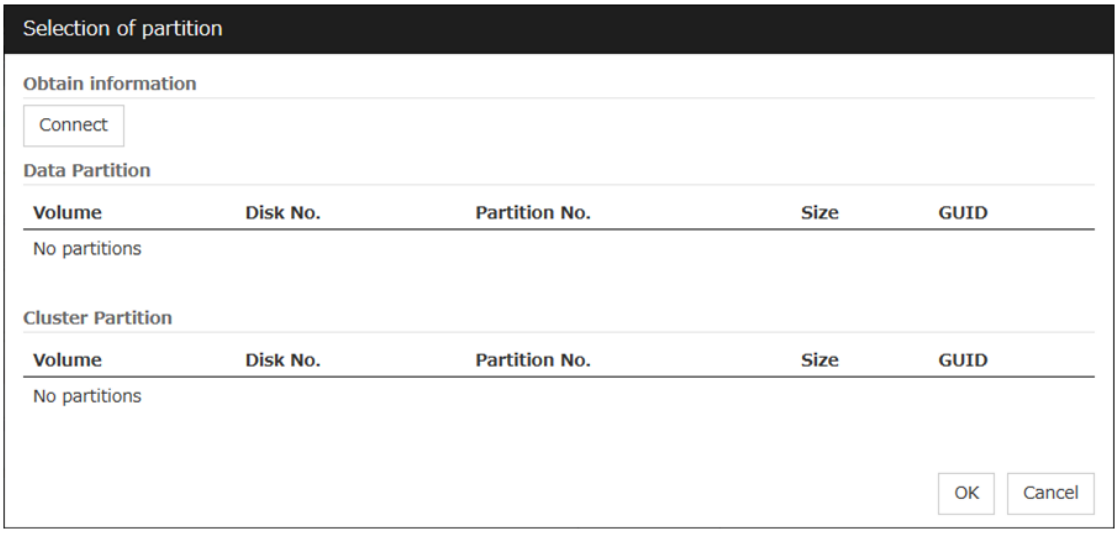


- Add
  Use **Add** to add mirror disk connects. Select the mirror disk connect you want to add from **Available Mirror Disk Connect** and then click **Add**. The selected mirror disk connect is added to the **Mirror Disk Connects**.
  Up to two lines of mirror disk connect can be set for one mirror disk resource.
- Remove
  Use Remove to remove mirror disk connects to be used. Select the mirror disk connect you want to remove from the **Mirror Disk Connects** and then click **Remove**. The selected mirror disk connect is added to **Available Mirror Disk Connect**.
- Order
  Use the arrows to change the priority of mirror disk connects to be used. Select the mirror disk connect whose priority you want to change, and then click the arrows. The selected row moves accordingly.

For mirror disk connect settings, see "*Interconnect tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

Add

Click this button to add the selected server to **Servers that can run the group**. When this button is clicked, the dialog box that allows for selection of a partition of the selected server is displayed.



- **Connect**
  Use this button to connect to the server and obtain the list of partitions.

- **Data Partition**
  Select a partition to be used as a data partition from the list. The GUID of the selected data partition is displayed.
- **Cluster Partition**
  Select a partition to be used as a cluster partition from the list. The GUID of the selected cluster partition is displayed.

Important: Specify different partitions for data partition and cluster partition. If the same partition is specified, data on the mirror disk may be corrupted. Make sure not to specify the partition on the shared disk for the data partition and cluster partition.

Remove

Use this button to delete a server from **Servers that can run the group**.

Edit

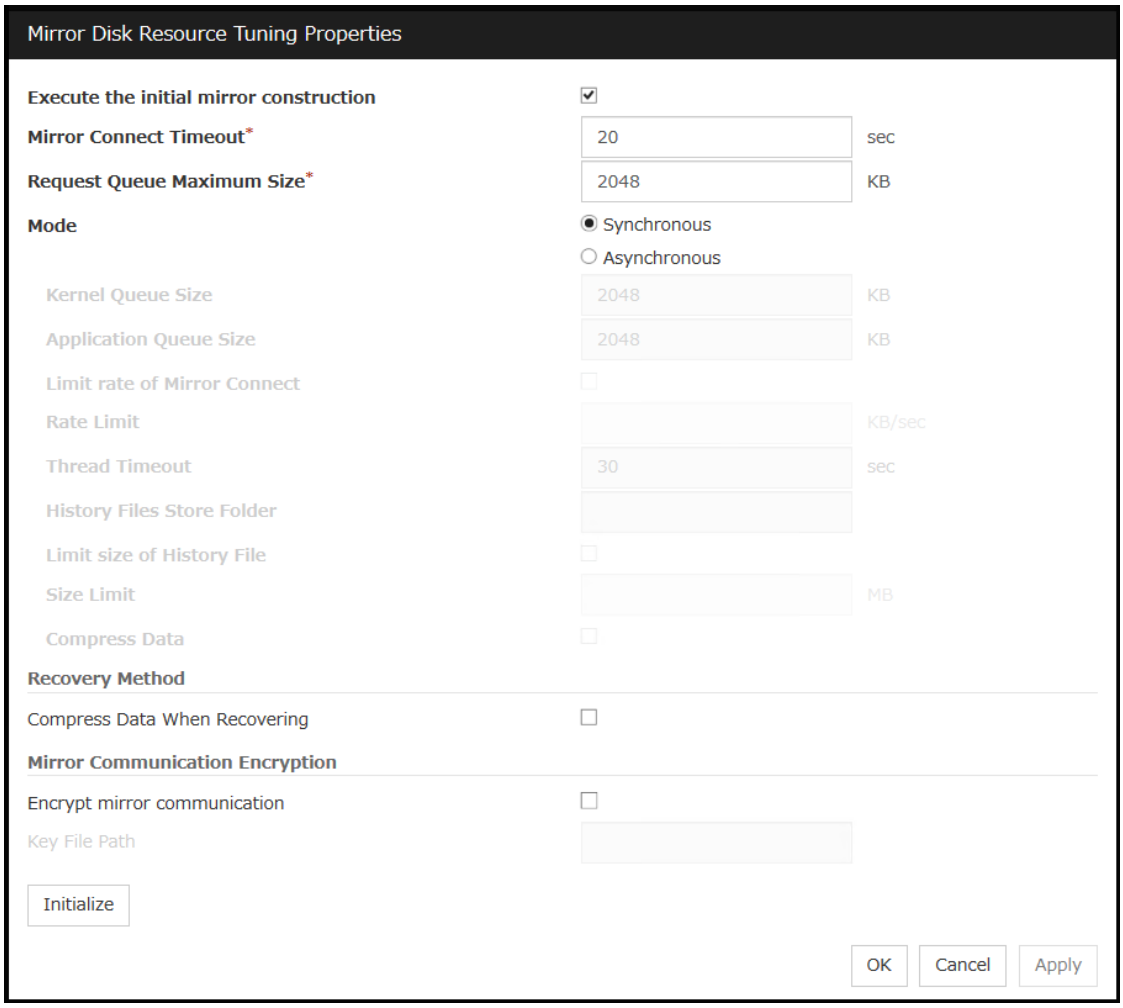
Use this button to display the dialog box to select the partition of the selected server.

Tuning

Opens the **Mirror Disk Resource Tuning Properties** dialog box. You make detailed settings for the mirror disk resource there.

Mirror DiskResource Tuning Properties

The advanced settings of mirror are displayed.



Execute the initial mirror construction

Specify whether to execute an initial mirror construction (full copy of data partition) when configuring a cluster.

- When the checkbox is selected:
  Execute an initial mirror construction. In general, specify this.
- When the checkbox is not selected:
  Handle as it is configured without executing an initial mirror construction. Specify this if the data partition contents are already the same and full copying is not required.

Mirror Connect Timeout (2 to 9999)

Specify the timeout for mirror disk connect.

Request Queue Maximum Size (512 to 65535)

Specify the size of queue that a mirror disk driver uses to queue I/O requests on the communication among servers.

Mode

Switch the mode of the mirror data synchronization.

- Synchronous

Write in the local disk and remote disk simultaneously to queue the completion.

- Asynchronous
  After writing in the local disk, write in the remote disk. Queue for the completion of writing in the local disk.

Kernel Queue Size (512 to 65535)

Specify the queue size of the kernel space to save the I/O data of the asynchronous mirror temporarily.

Application Queue Size (512 to 65535)

Specify the queue size of the user space to save the I/O data of the asynchronous mirror temporarily.

Rate limitation of Mirror Disk Connect (0 to 999999999)

Set the upper limit of the communication band used by the mirror disk connect.

Thread Timeout (2 to 9999)

Specify the timeout when it becomes unable to transfer from the kernel queue to the application queue.

History Files Store Folder (Within 1023 bytes)

Specify the destination folder to store the file when I/O data is overflowed form the application queue. It is required to specify a folder that has sufficient free space so that the remote disk and the asynchronous I/O data can be kept as a file.

Do not specify any folder in the cluster partition and data partition to the history files store folder. Additionally do not specify a folder that contains two byte characters in the path.

Also, it is recommended to set a history files store folder, in addition to the system drive of Windows (Normally, the C: drive is used.). If it is set on the system drive, due to I/O running concurrently, a failure may occur. For example, the mirror processing is delayed or the system behavior may become unstable.

Size limitation of History File (0 to 999999999)

Set the size limit of temporary files stored in the history file store folder. If the upper limit of size is specified, mirroring will stop when the total amount of the temporary files reaches the limit. The configured value is only applied to the limit of the temporary file size for the mirror disk resources, and this value does not set the total amount of the temporary files in the history file store folder.

Mirroring will also stop when the size of the area for managing the number of cases where data is yet to be sent reaches the upper limit of **History Recording Area Size in Asynchronous Mode**. This applies even if the total amount of the temporary files does not reach its upper limit. For more information, see "*Cluster properties*" -> "*Mirror Disk tab*" -> "History Recording Area Size in Asynchronous Mode".

Compress data

Specify whether to compress the mirror data flowing through the mirror disk connect.

Compress Data When Recovering

Specify whether to compress the mirror data flowing through the mirror disk connect for the purpose of mirror recovery.

Encrypt mirror communication

Choose whether to encrypt data passing through mirror disk connects. This setting affects both data for mirror synchronization and data for mirror recovery.

- If the check box is checked:
  The data is encrypted.
- If the check box is not checked:

The data is not encrypted.

Key File Path

Specify a key file to encrypt data passing through mirror disk connects.

Note: The key file to be used is generated by using the clpkeygen command. For more information on the clpkeygen command, refer to "9. *EXPRESSCLUSTER command reference*" - "*Creating a key file for encrypting communication data (clpkeygen command)*".

Important: Be sure to use the same key file on all servers which can activate mirror disk resources. Using different key files leads to unsuccessful mirroring.

Initialize

Click **Initialize** to reset the values of all items to their default values.

3.8.7 Notes on operating mirror disk resources

If mirror data was synchronized on both servers when the cluster was shut down, use one of the two orders noted below to start the servers.

- Start both servers simultaneously
- Start the first server, and then start the second server after the first server has started

Do not consecutively start and shutdown both servers[2]. The servers communicate with each other to determine whether the mirror data stored on each server is up to date. Consecutively starting and shutting down both servers prevents the servers from properly determining whether mirror data is up to date and mirror disk resources will fail to start the next time both servers are started.

[2] In other words, do not start and shut down the first server, and then start and shut down the second server.

3.9 Understanding registry synchronization resources

3.9.1 Dependencies of registry synchronization resources

By default, this function depends on the following group resource types.

Group resource type
Floating IP resource
Virtual IP resource
Virtual computer name resource
Disk resource
Mirror disk resource
Hybrid disk resource
CIFS resource
AWS elastic ip resource
AWS virtual ip resource
AWS secondary ip resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.9.2 Registry synchronization resources

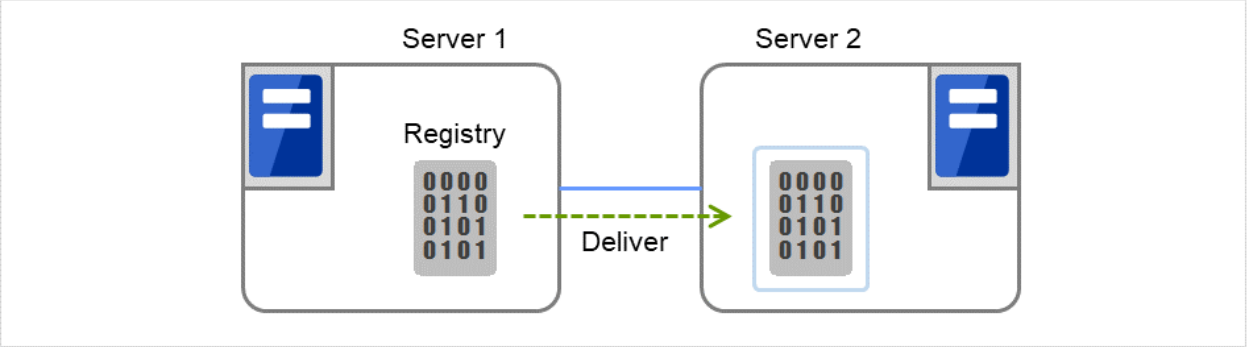


Fig. 3.54: Registry synchronization resource (1)

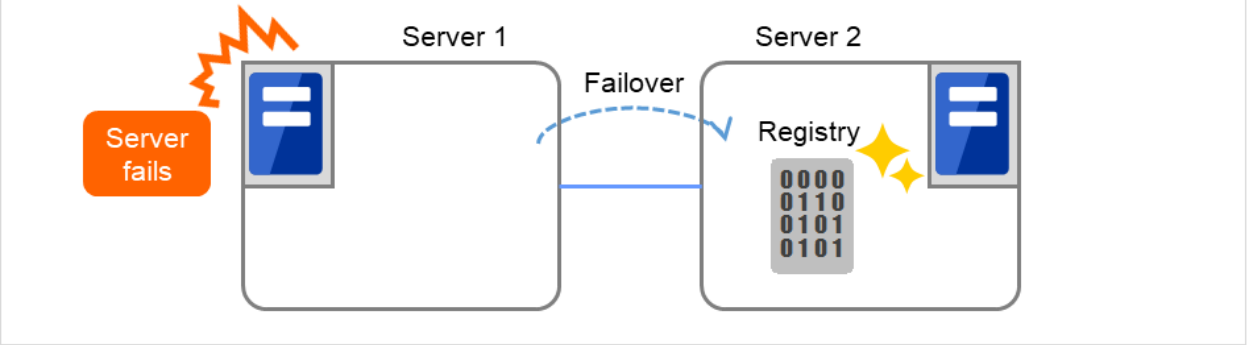


Fig. 3.55: Registry synchronization resource (2)

Registry keys to be synchronized at failover can be configured. When the content in a registry key set as synchronization target is updated while registry synchronization resource is active, the updated content is applied to the registry of the Failover Target Server.

The following describes how a registry synchronization resource synchronizes registry:

1. When there is a registry synchronization resource in a failover group, update of a registry key that has been configured is monitored when the registry synchronization resource is activated.
2. When the registry key update is detected, what is in the registry key is saved as a file in the local disk. Then the file is delivered to each Failover Target Server.
3. The servers that received the file keep it in their local disks. If a failover occurs and registry synchronization resource is activated in a server that received the file, the content of the file is restored in the corresponding registry key.

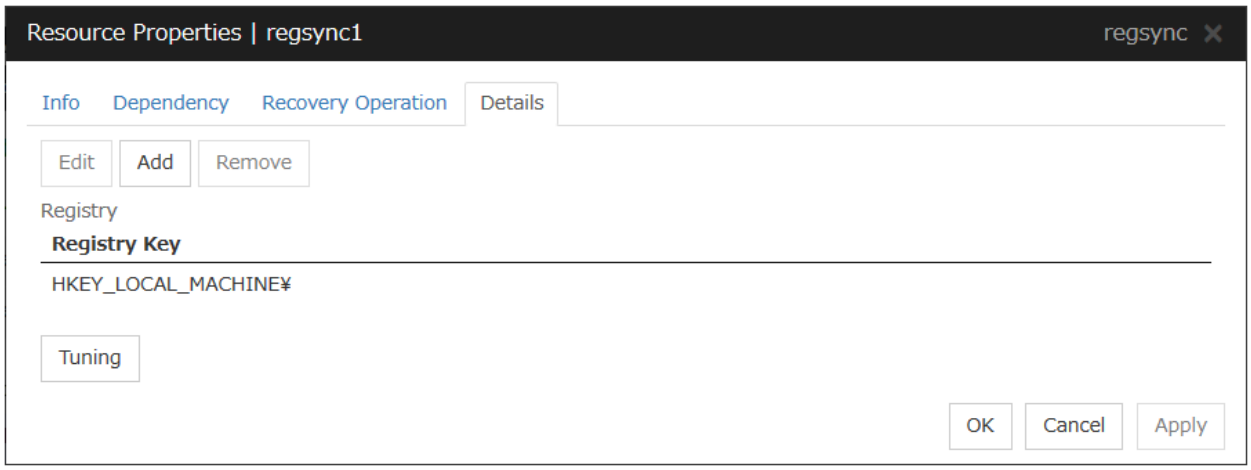
3.9.3 Notes on registry synchronization resources

- Do not open synchronization target registry keys in the standby server.
- If a synchronization target registry key is opened when a failover occurs, restoration of the registry will fail. To start and stop applications that use the synchronization target registry key, use a script resource within a control of EXPRESSCLUSTER.
- Minimize the number of synchronization target registry keys. Do not set more than needed. It is not recommended to set a registry key that is frequently updated as a synchronization target registry key.
- Saving in a file and delivering the file to other servers is done every time a synchronization target registry key is updated. The number of synchronization target registry keys and frequency of updating them can affect the system performance. Do not change or update a synchronization target registry key.
- For the synchronization target registry keys, the following can be set. The registry keys other than those listed below cannot be synchronized.
  - Any key under the HKEY_USERS
  - Any key under the HKEY_LOCAL_MACHINE

  Do not set the following keys.
  - Keys under the HKEY_LOCAL_MACHINE/SOFTWARE/NEC/EXPRESSCLUSTER
  - HKEY_LOCAL_MACHINE/SOFTWARE/NEC
  - HKEY_LOCAL_MACHINE/SOFTWARE
  - HKEY_LOCAL_MACHINE

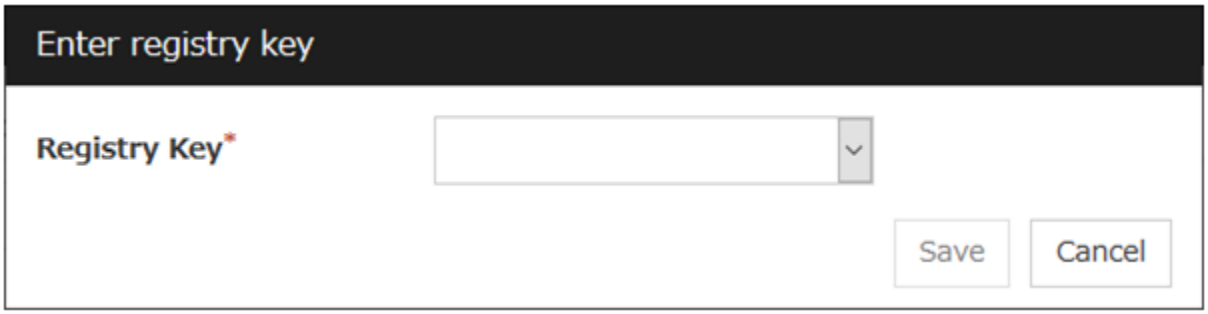
  Do not set the keys that are in parent-child relationship within the same resource.
- Up to 16 synchronization target registry keys can be set per resource.
- The following restrictions apply to names of the synchronization target registry keys:
  - The characters that can be used for registry key are determined by the OS specifications.
  - Up to 259 bytes can be used. Do not set the key name of 260 or larger bytes.

3.9.4 Details tab



Add

Use this button to add a registry key to monitor. The **Enter registry key** dialog box is displayed.



Registry Key

Enter a registry key to synchronize and click **OK**.

Remove

Click this button to delete a registry key from synchronization target listed in **Registry List**.

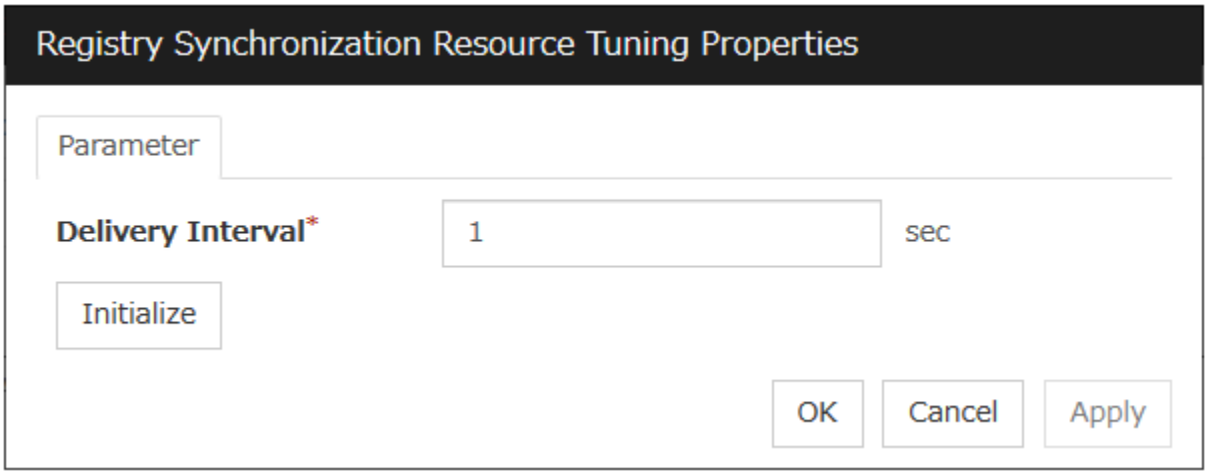
Edit

The **Enter registry key** dialog box is displayed. The selected registry keys are listed in **Registry List**. Edit a registry key and click **OK**.

Registry Synchronization Resource Tuning Properties

Parameter tab

The detailed setting for registry synchronization resource is displayed.



Delivery Interval (1 to 99)

Specify the interval to deliver the updated registry key information to other servers.

When short-time interval is set

- Updated information is immediately delivered to other servers.
- The system may get heavily loaded by frequently updating a registry key.

When long-time interval is set

- A delay in delivering updated information to other servers may occur. If a failover occurs before delivery of the updated information is not completed, it will not be delivered to the Failover Target Server.
- Increase in system load due to synchronization can be reduced when a registry key is frequently updated.

Initialize

Click **Initialize** to reset the values of all items to their default values.

3.10 Understanding script resources

You can register scripts managed by EXPRESSCLUSTER and run when starting, stopping, failing over, or moving a group in EXPRESSCLUSTER. It is also possible to register your own scripts for script resources.

Note: The same version of the application to be run from script resources must be installed on all servers in failover policy.

3.10.1 Dependencies of script resources

By default, this function depends on the following group resource types.

Group resource type
Floating IP resource
Virtual IP resource
Virtual computer name resource
Disk resource
Mirror disk resource
Hybrid disk resource
Registry synchronization resource
CIFS resource
AWS elastic ip resource
AWS virtual ip resource
AWS secondary ip resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.10.2 Scripts in script resources

Types of scripts

Start script and stop script are provided in script resources. EXPRESSCLUSTER runs a script for each script 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.

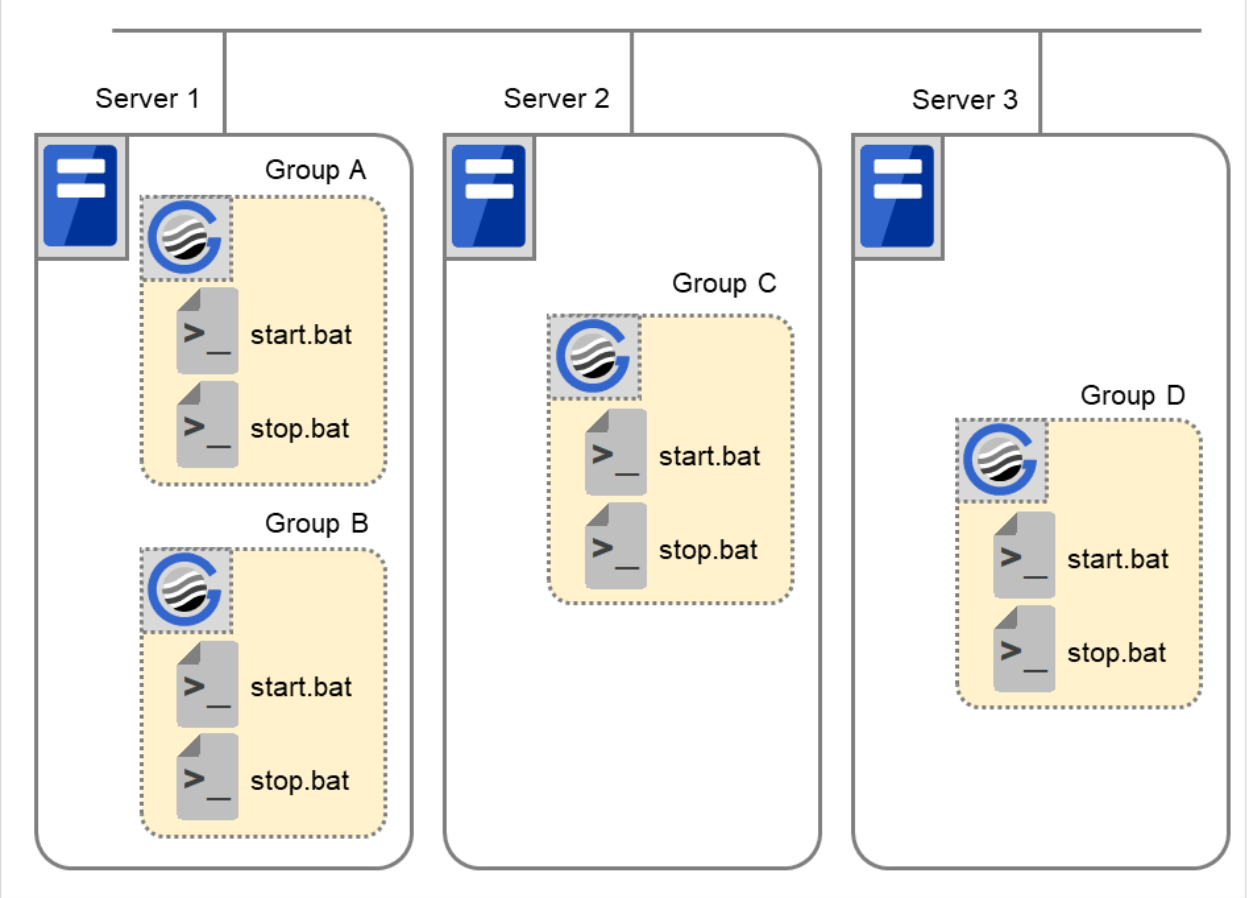


Fig. 3.56: Start script and stop script

start.bat Start script

stop.bat Stop script

3.10.3 Environment variables in script of script resource

When EXPRESSCLUSTER runs a script, it records information such as the condition when the script is run (script starting factor) in environment variables.

You can use the environment variables on the table below as branching condition to write code for your system operation.

The environment variable of a stop script returns the content of the start script that was run immediately before as a value. Start script does not set environment variables of CLP_FACTOR.

The environment variable of 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.
	FAILOVER	The script was run on the Failover Target Server: - by the server's failing; - due to the detection of a monitor resource error; or - because activation of group resources failed.
	RECOVER	- The server is recovered; - due to 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.

Continued on next page

Table 3.17 – continued from previous page

Environment Variable	Value of environment variable	Meaning
	OTHER	The script was run on a server other than the primary server of the group.
CLP_DISK[3] ...partition connection information on shared or mirror disks	SUCCESS	There was no partition with connection failure.
	FAILURE	There was one or more partition with connection failure.
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_VERSION_FULL ...EXPRESSCLUSTER full version	EXPRESSCLUSTER full version	Represents the EXPRESSCLUSTER full version. (Example) 13.20
CLP_VERSION_MAJOR ...EXPRESSCLUSTER major version	EXPRESSCLUSTER major version	Represents the EXPRESSCLUSTER major version. (Example) 13
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER installation path	Represents the path where EXPRESSCLUSTER is installed. (Example) C:\Program Files\EXPRESSCLUSTER
CLP_OSNAME ...Server OS name	Server OS name	Represents the OS name of the server where the script was executed. (Example) Windows Server 2016 Standard

Continued on next page

Table 3.17 – 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) 6.2.0.0.274.3
CLP_SERVER_PREV ...Failover source server name	Server name	Represents the failover source of the group which the script belongs to only when CLP_EVENT is FAILOVER. Indicates an indefinite value when CLP_EVENT is other than FAILOVER.

If the script is executed on the standby server, with **Execute on standby server** of **Script 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

[3] It is available for disk resource, mirror disk resource and hybrid disk resource.

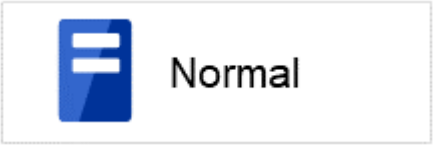
Table 3.18 – continued from previous page

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. 13.20).
CLP_VERSION_MAJOR ...Major version of EXPRESSCLUSTER	Major version of EXPRESSCLUSTER	Represents the major version of EXPRESSCLUSTER (e.g. 13).
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER installation path	Represents the EXPRESSCLUSTER installation path (e.g. C:\Program Files\EXPRESSCLUSTER).
CLP_OSNAME ...Server OS name	Server OS name	Represents the OS name of the server where the script was executed. (E.g. Windows Server 2016 Standard)
CLP_OSVER ...Server OS version	Server OS version	Represents the OS version of the server where the script was executed. (E.g. 6.2.0.0.274.3)

3.10.4 Execution timing of script resource scripts

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, a 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.

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

(Example) 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	First priority server	Second priority server
A	Server 1	Server 2
B	Server 2	Server 1
C	Server 1	Server 2

Cluster status transition diagram

This diagram illustrates a typical status transition of cluster.

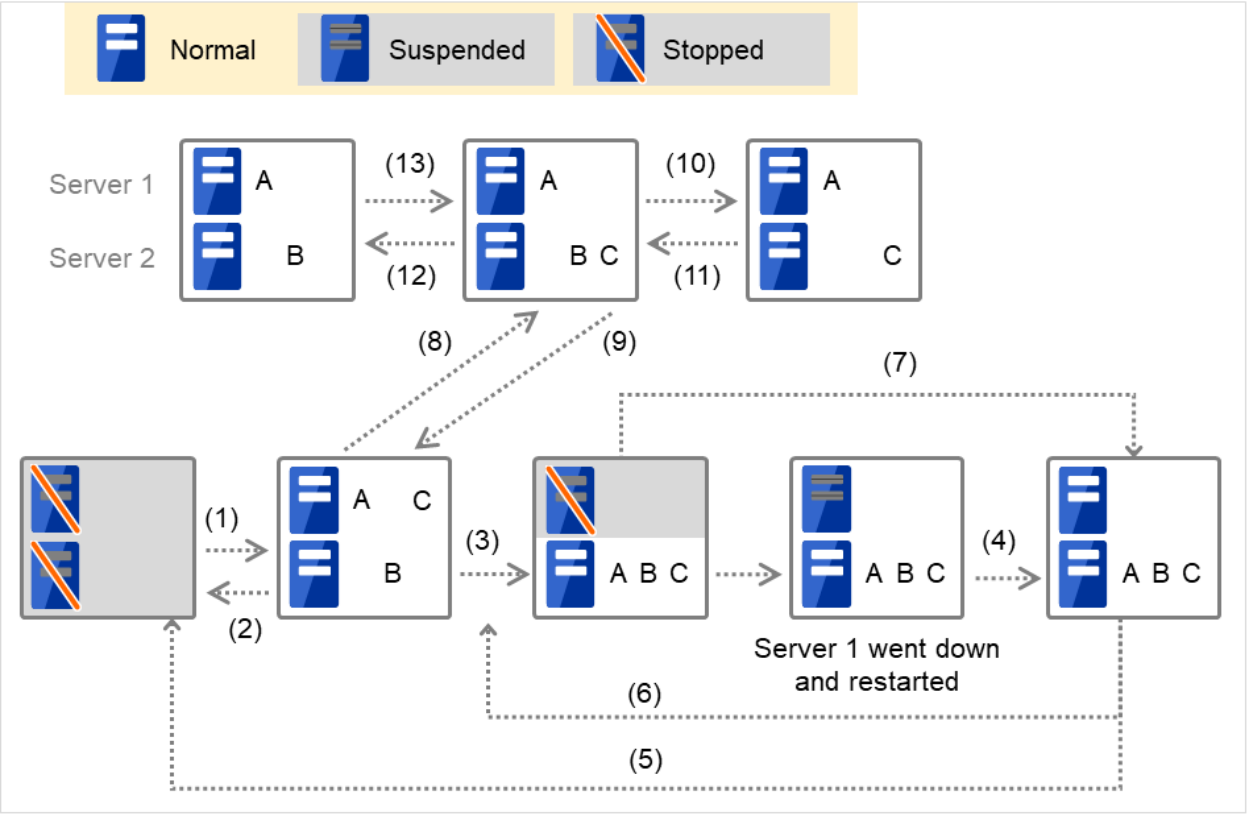


Fig. 3.57: Example of cluster status transition: overview

Numbers 1. to 13. in the diagram correspond to descriptions as follows.

1. Normal startup

Normal startup here refers to 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.

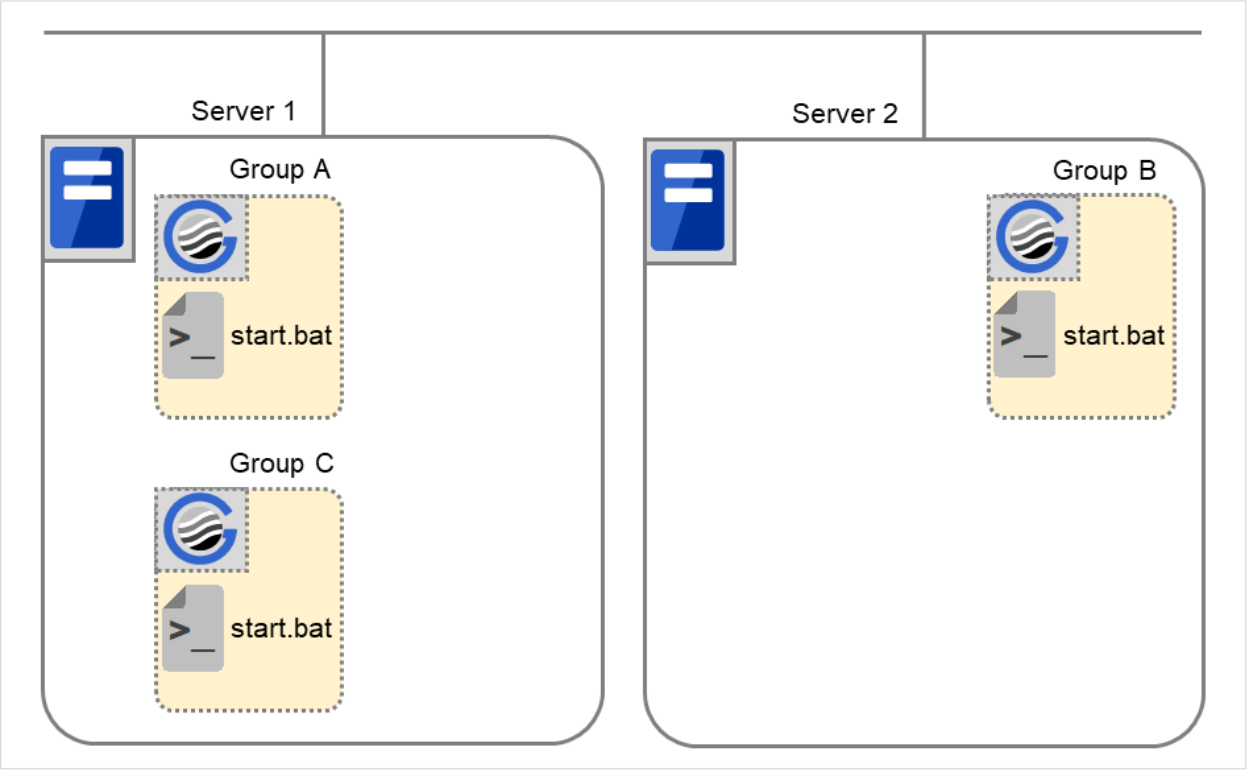


Fig. 3.58: Situation and script execution: normal startup

Environment variables for start.bat

	Group A	Group B	Group C
CLP_EVENT	START	START	START
CLP_SERVER	HOME	HOME	HOME

2. Normal shutdown

Normal shutdown here refers to a cluster shutdown immediately after the start script corresponding to a stop script was run by performing normal startup or by moving a group (online failback).

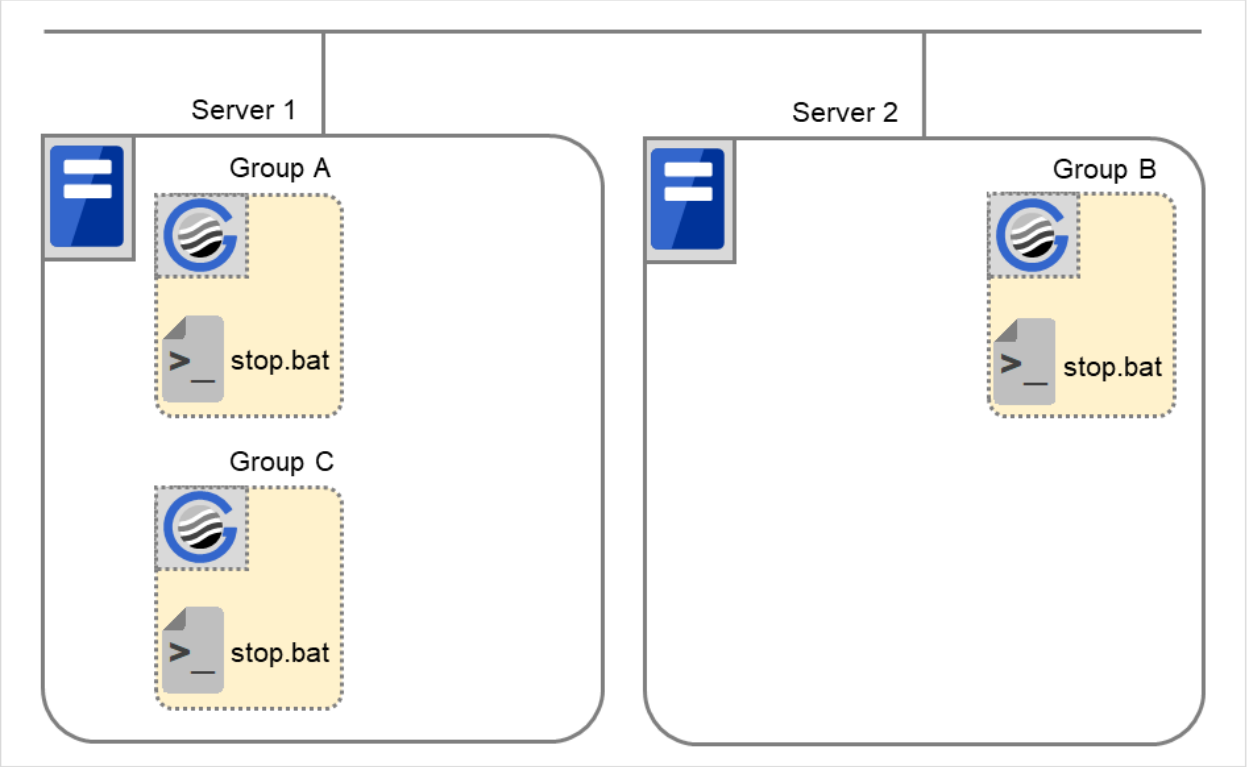


Fig. 3.59: Situation and script execution: normal shutdown

Environment variables for stop.bat

	Group A	Group B	Group C
CLP_EVENT	START	START	START
CLP_SERVER	HOME	HOME	HOME

3. Failover at the failed Server 1

The start script of a group that has Server 1 as its primary server will be run on a lower priority server (Server 2) if 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.

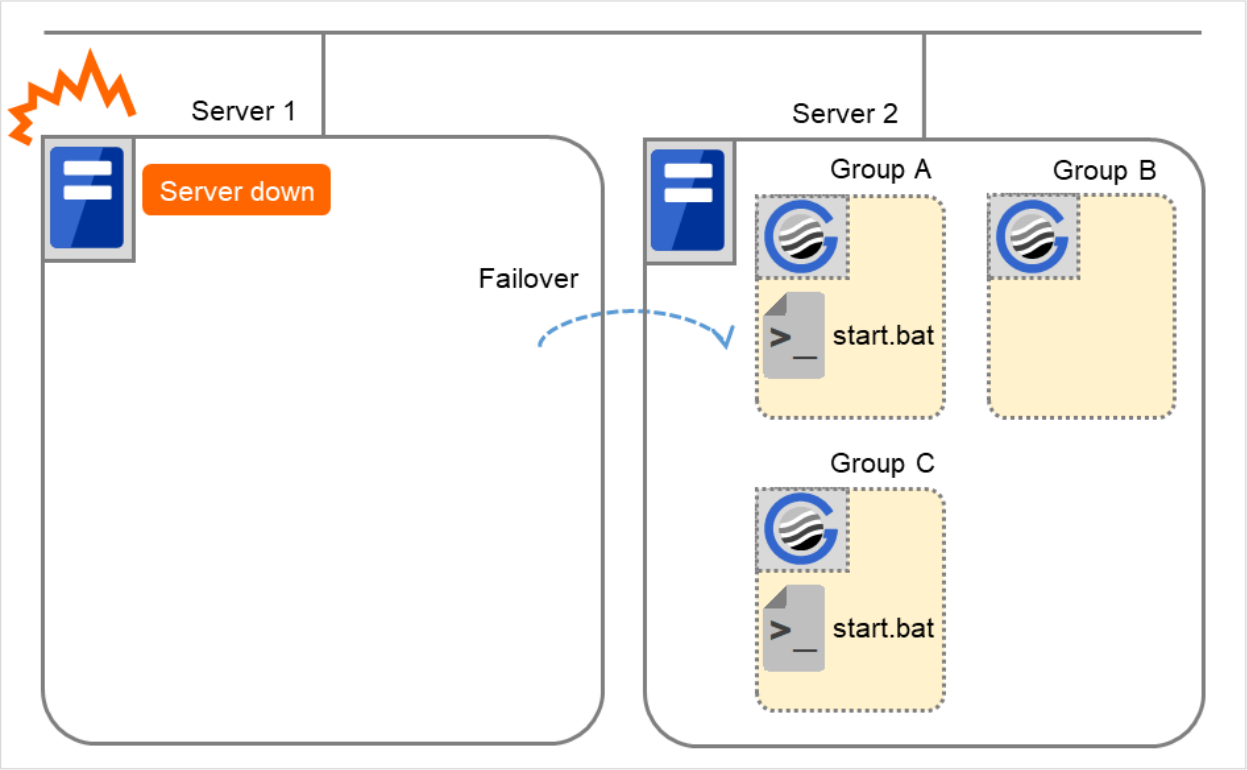


Fig. 3.60: Situation and script execution: failover due to server down

	Group A	Group C
CLP_EVENT	FAILOVER	FAILOVER
CLP_SERVER	OTHER	OTHER

4. Recovering Server 1 to cluster

When Server 1 that has been rebooted (operating as non-cluster) returns to a cluster, the start script of the failover group that was running when a failover occurred is run in Server 1. This means recovery is executed in the server where the failover has occurred.

To execute a recovery (for example, recovering database information in a local disk), you need to write CLP_EVENT(=RECOVER) as a branching condition. Even if recovery is not required, you need to write the script not to start the operation.

For data mirroring operation, data is restored (reconfiguration of mirror set) at cluster recovery.

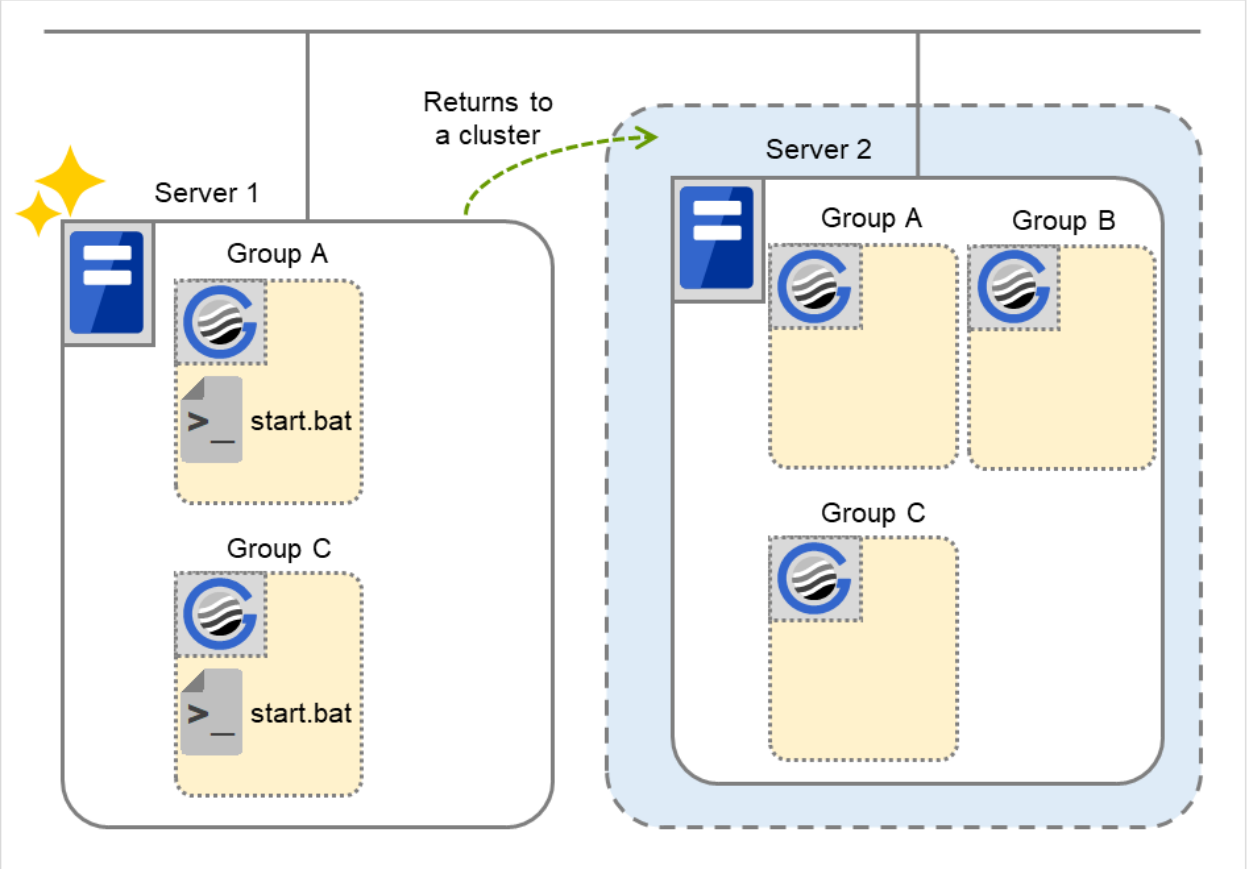


Fig. 3.61: Situation and script execution: returning a server to the cluster

Environment variables for start.bat

	Group A	Group C
CLP_EVENT	RECOVER	RECOVER
CLP_SERVER	HOME	HOME

5. Cluster shutdown after failover of Server 1

The stop scripts of the Group A and C are run on Server 2 to which the groups failed over (the stop script of Group B is run by a normal shutdown).

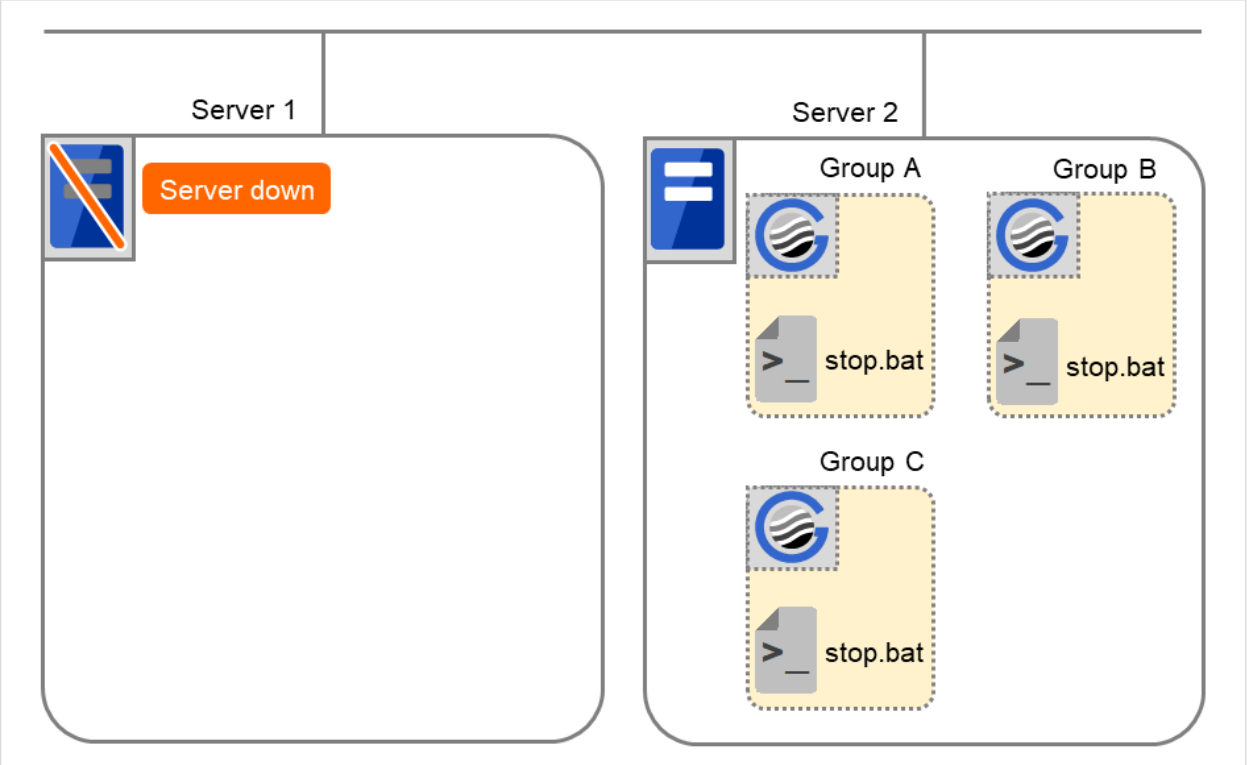


Fig. 3.62: Situation and script execution: cluster shutdown after failover

Environment variables for stop.bat

	Group A	Group B	Group C
CLP_EVENT	FAILOVER	START	FAILOVER
CLP_SERVER	OTHER	HOME	OTHER

6. Moving of Group A and C

After the stop scripts of Group A and C are run on Server 2 to which the groups failed over, their start scripts are run on Server 1.

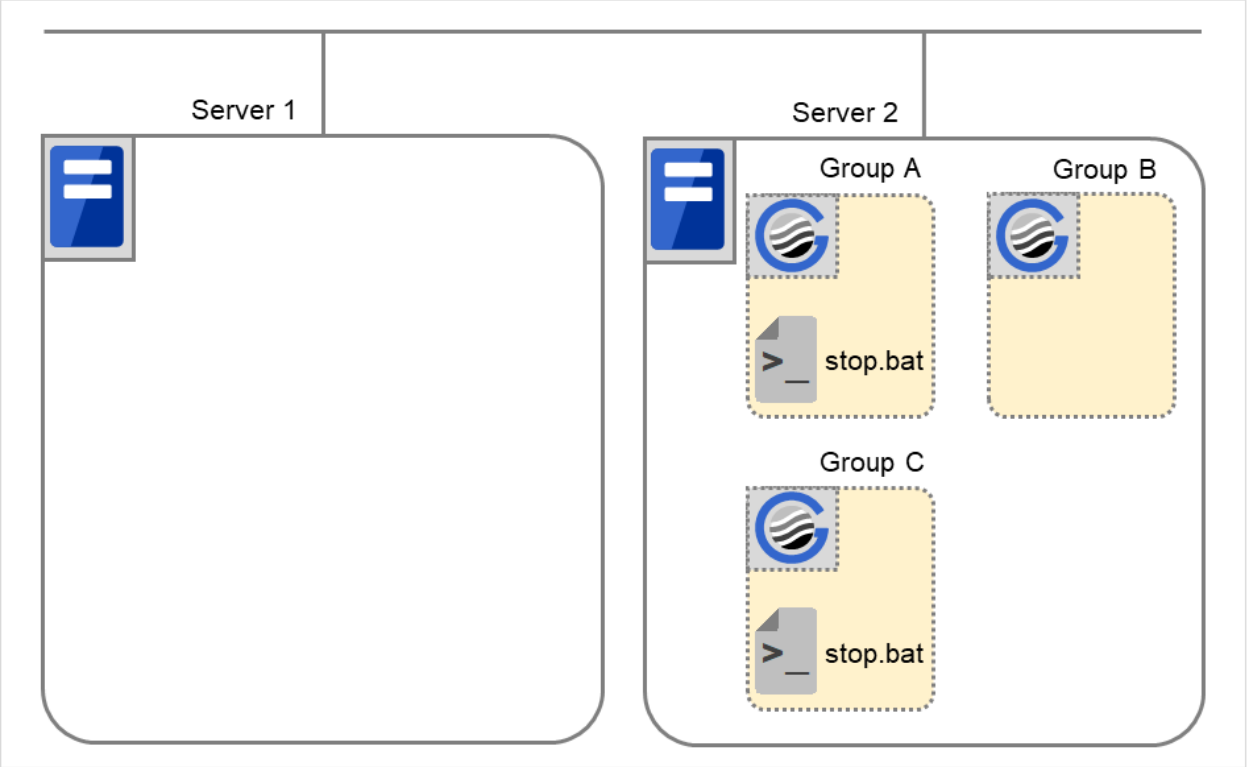


Fig. 3.63: Situation and script execution: moving Groups A and C (1)

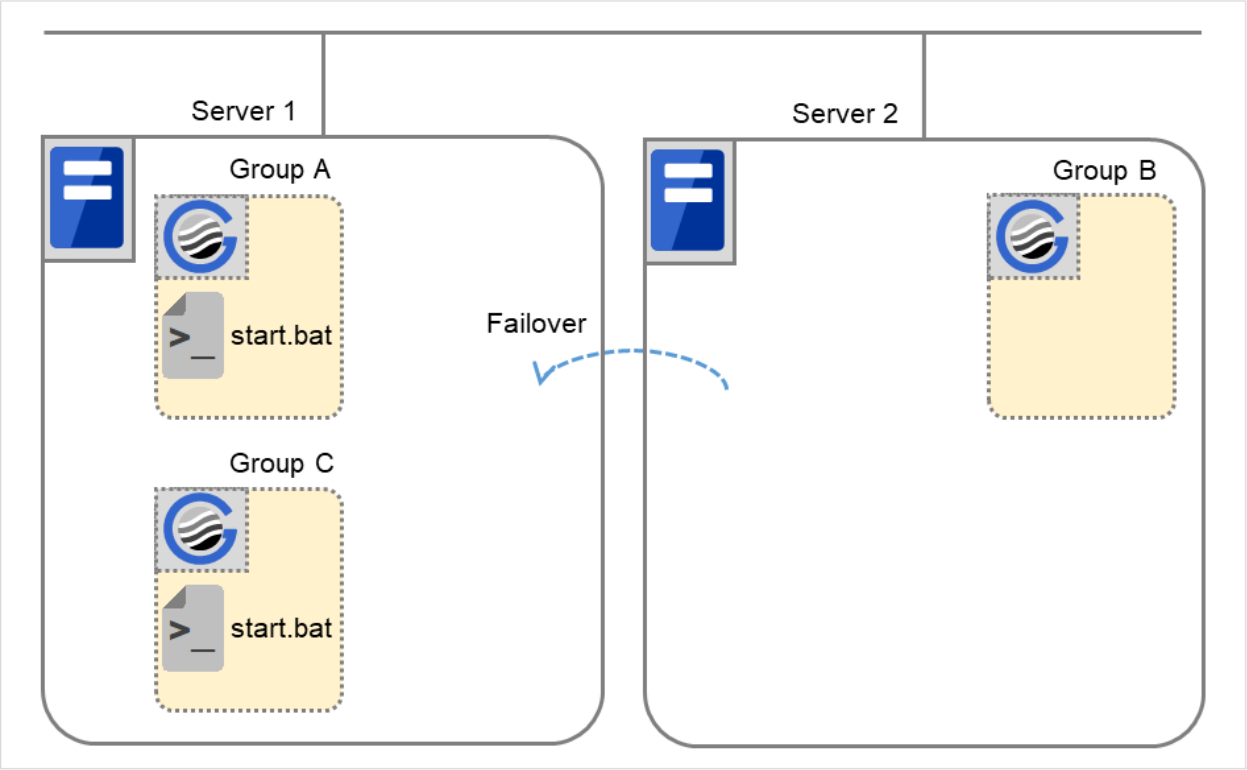


Fig. 3.64: Situation and script execution: moving Groups A and C (2)

Environment variables for stop.bat

	Group A	Group C
CLP_EVENT	FAILOVER[4]	FAILOVER
CLP_SERVER	OTHER	OTHER

Environment variables for start.bat

	Group A	Group C
CLP_EVENT	START	START
CLP_SERVER	HOME	HOME

[4] Environment variables in a stop script take those in the previous start script. For moving in "6. 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 "6. Moving of Group A and C", the environment variable is START.

7. Server 1 startup (Auto recovery mode)

Auto recovery of Server 1 is executed. The start script of the failover group operated when a failover occurred is run in Server 1. This means, recovery is executed in the server where the failover occurred. Note what is stated in "4. Recovering Server 1 to cluster". For data mirroring operation, data is restored (reconfiguration of mirror set) at cluster recovery.

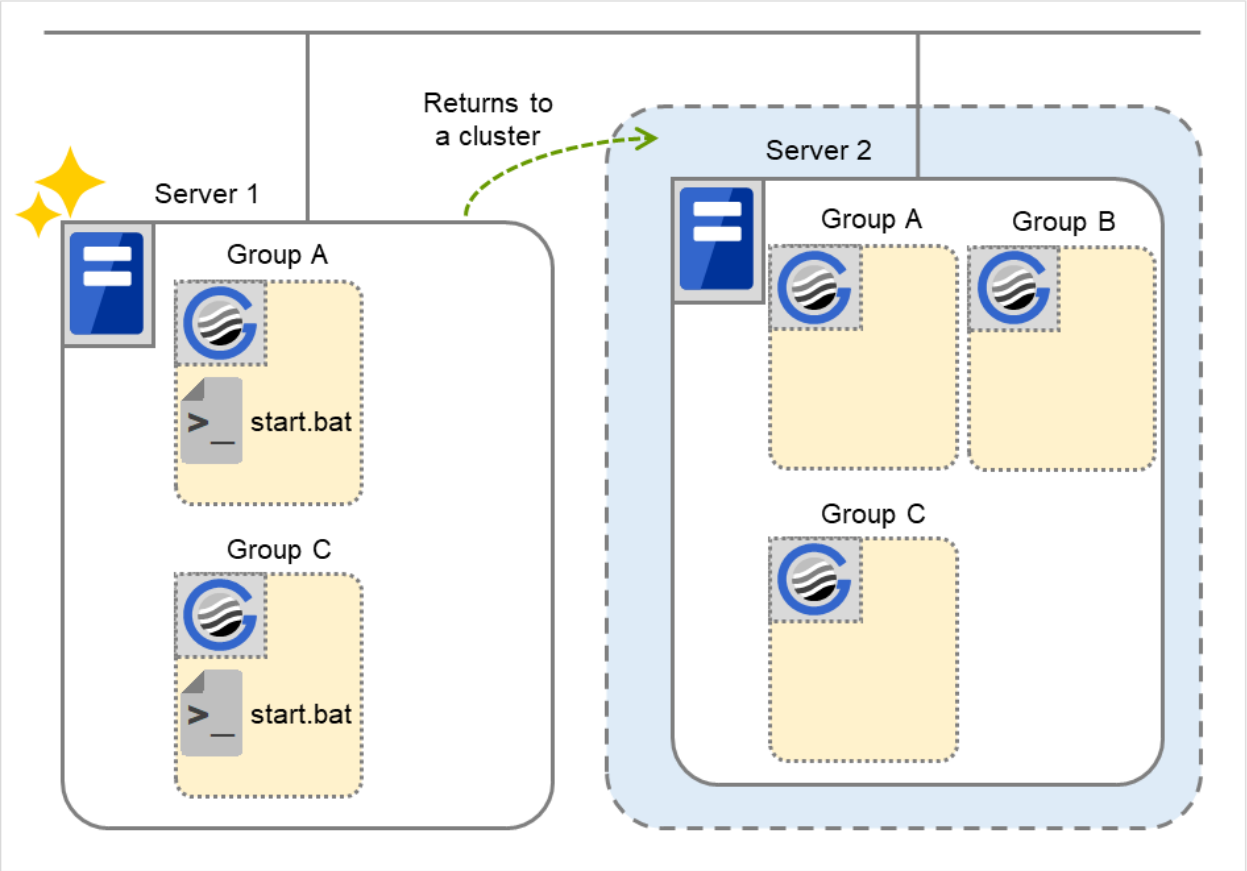


Fig. 3.65: Situation and script execution: server startup (auto recovery mode)

Environment variables for start.bat

	Group A	Group C
CLP_EVENT	RECOVER	RECOVER
CLP_SERVER	HOME	HOME

8. Error in Group C and failover

When an error occurs in Group C, its stop script is run on Server 1 and start script is run on Server 2.

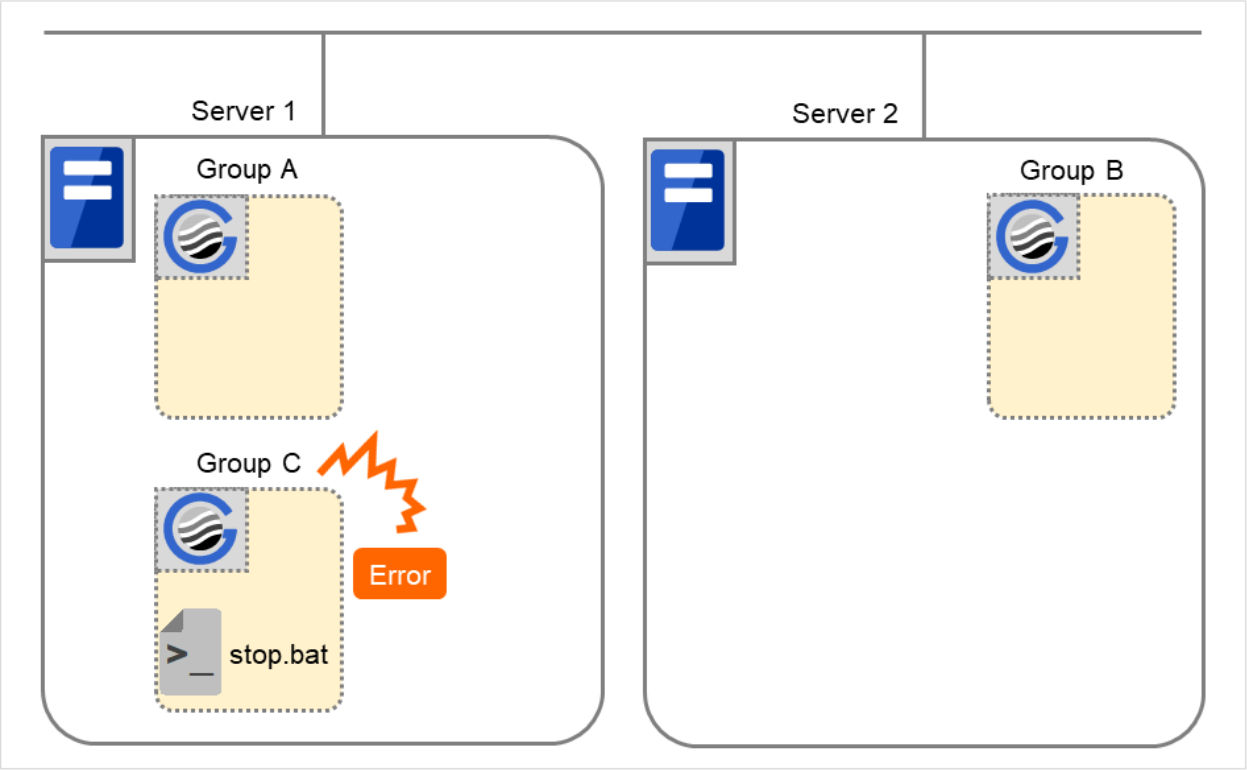


Fig. 3.66: Situation and script execution: error in Group C and failover (1)

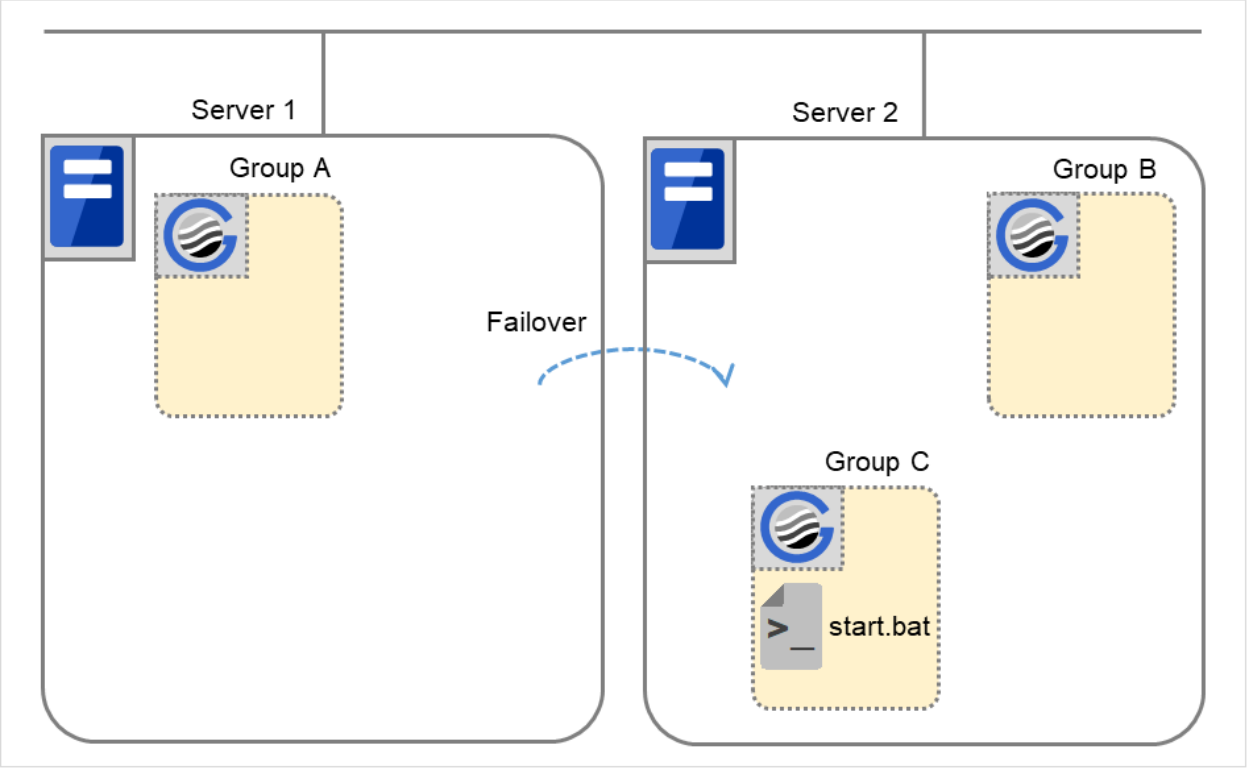


Fig. 3.67: Situation and script execution: error in Group C and failover (2)

The environment variables of Server1 for stop.bat

	Group C
CLP_EVENT	START
CLP_SERVER	HOME

Environment variables of Server 1 for start.bat

	Group C
CLP_EVENT	RECOVER

The environment variables of Server2 for start.bat

	Group C
CLP_EVENT	FAILOVER
CLP_SERVER	OTHER

9. Moving of Group C

Move the Group C that failed over to Server 2 in 8. from Server 2 to Server 1. Run the stop script on Server 2, and then run the start script on Server 1.

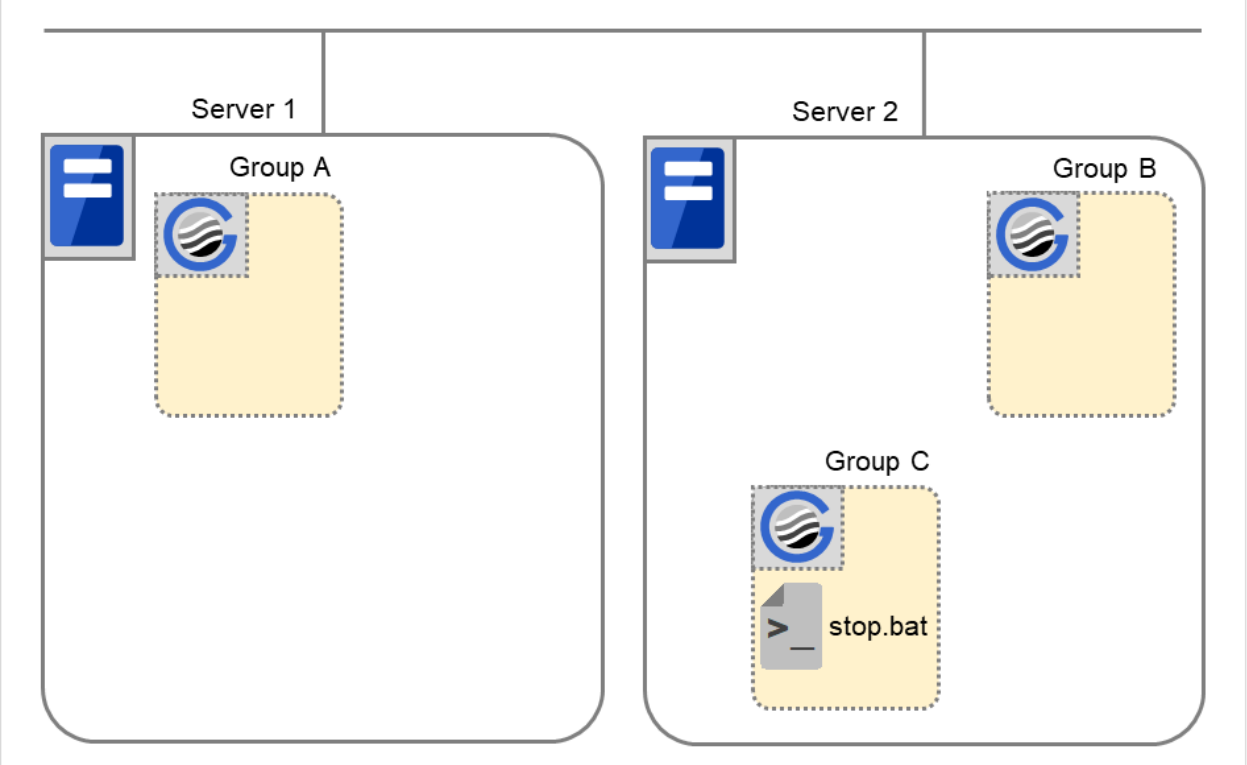


Fig. 3.68: Situation and script execution: moving Group C (1)

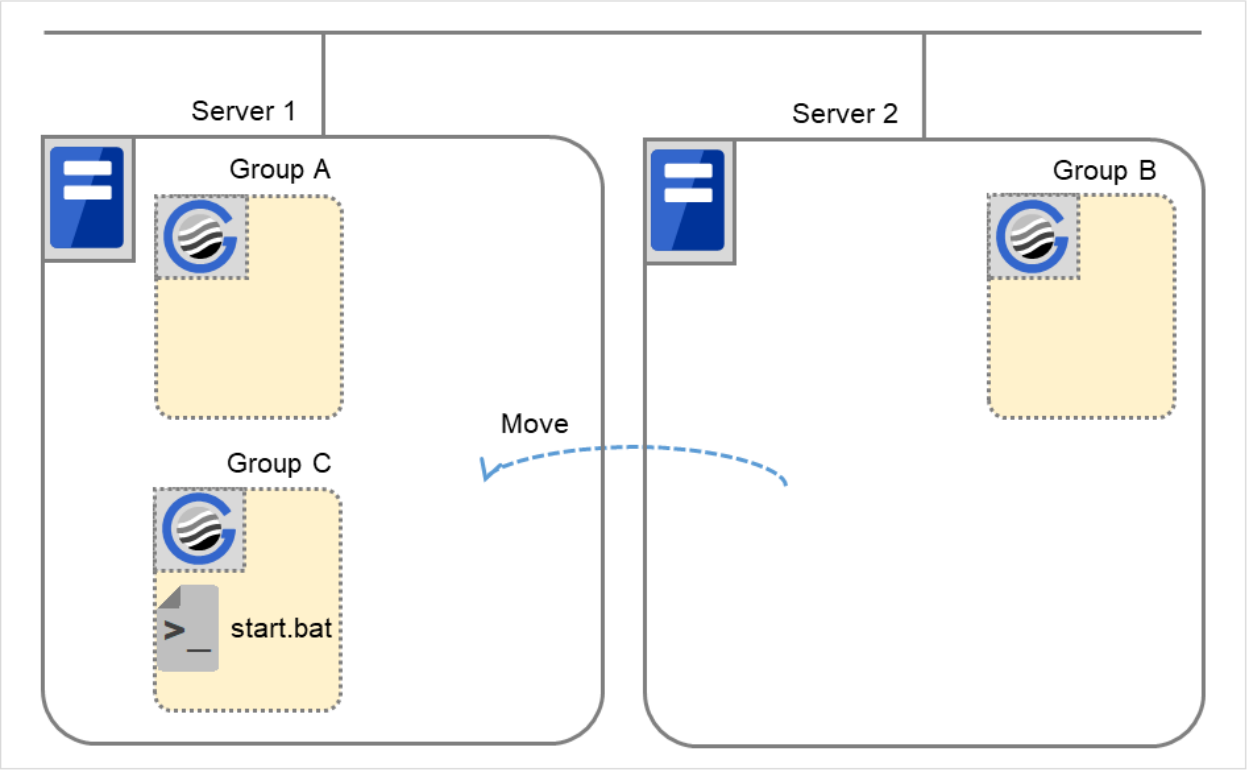


Fig. 3.69: Situation and script execution: moving Group C (2)

The environment variables for stop.bat (because of failover from 8.)

	Group C
CLP_EVENT	FAILOVER
CLP_SERVER	OTHER

The environment variables for start.bat

	Group C
CLP_EVENT	START
CLP_SERVER	HOME

10. Stopping Group B

The stop script of Group B is run on Server 2.

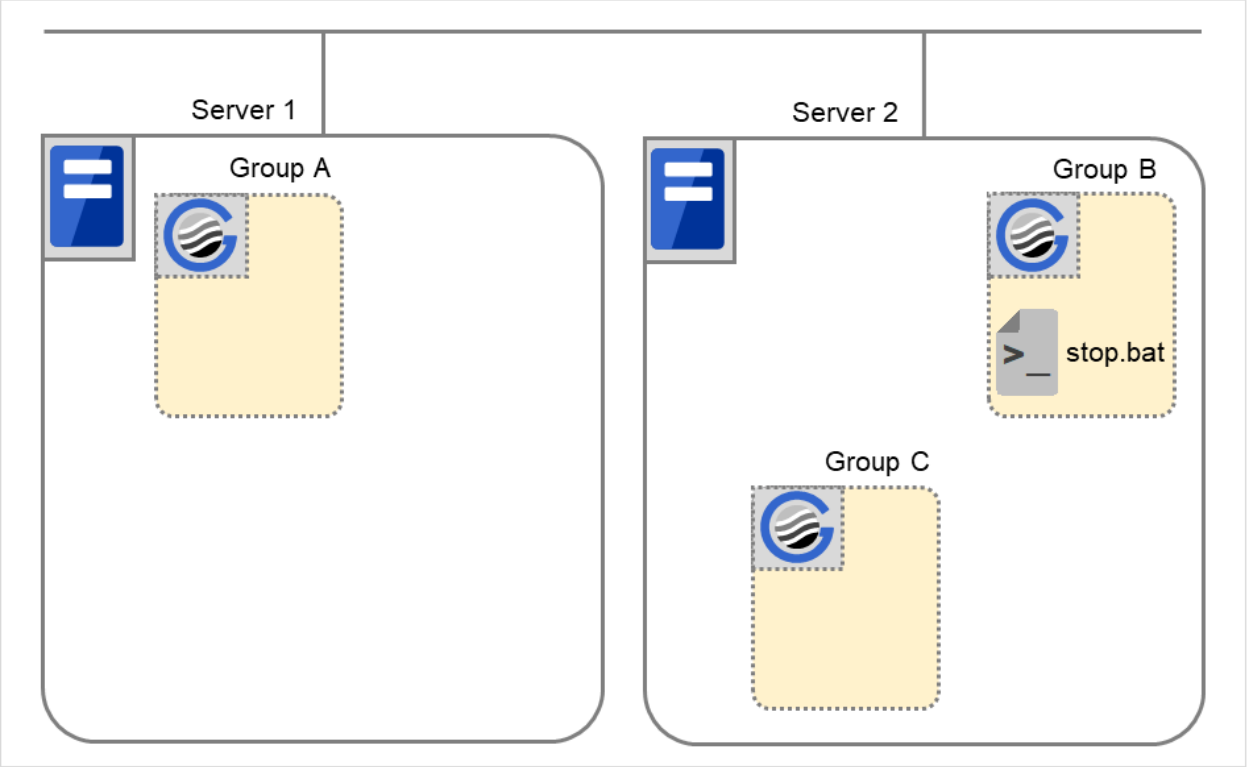


Fig. 3.70: Situation and script execution: stopping Group B

The environment variables for stop.bat

	Group B
CLP_EVENT	START
CLP_SERVER	HOME

11. Starting Group B

The start script of Group B is run on Server 2.

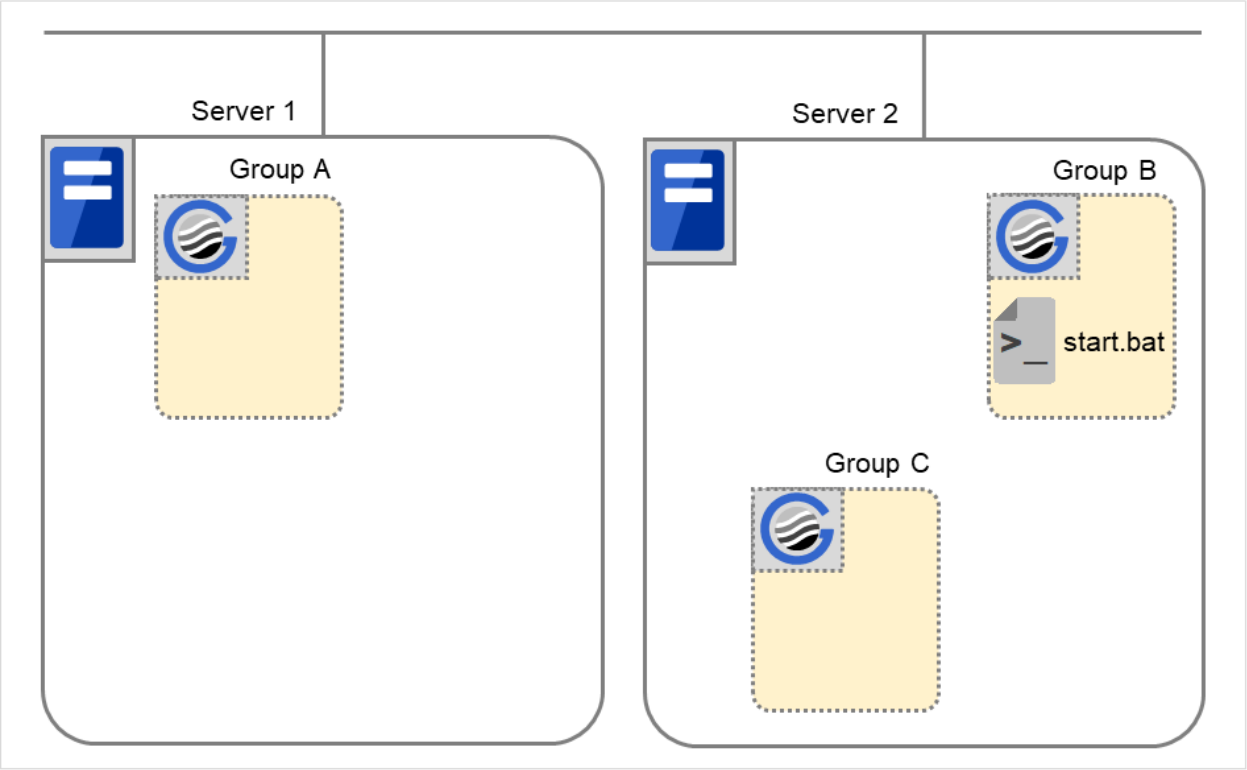


Fig. 3.71: Situation and script execution: starting Group B

The environment variables for start.bat

	Group B
CLP_EVENT	START
CLP_SERVER	HOME

12. Stopping Group C

The stop script of Group C is run on Server 2.

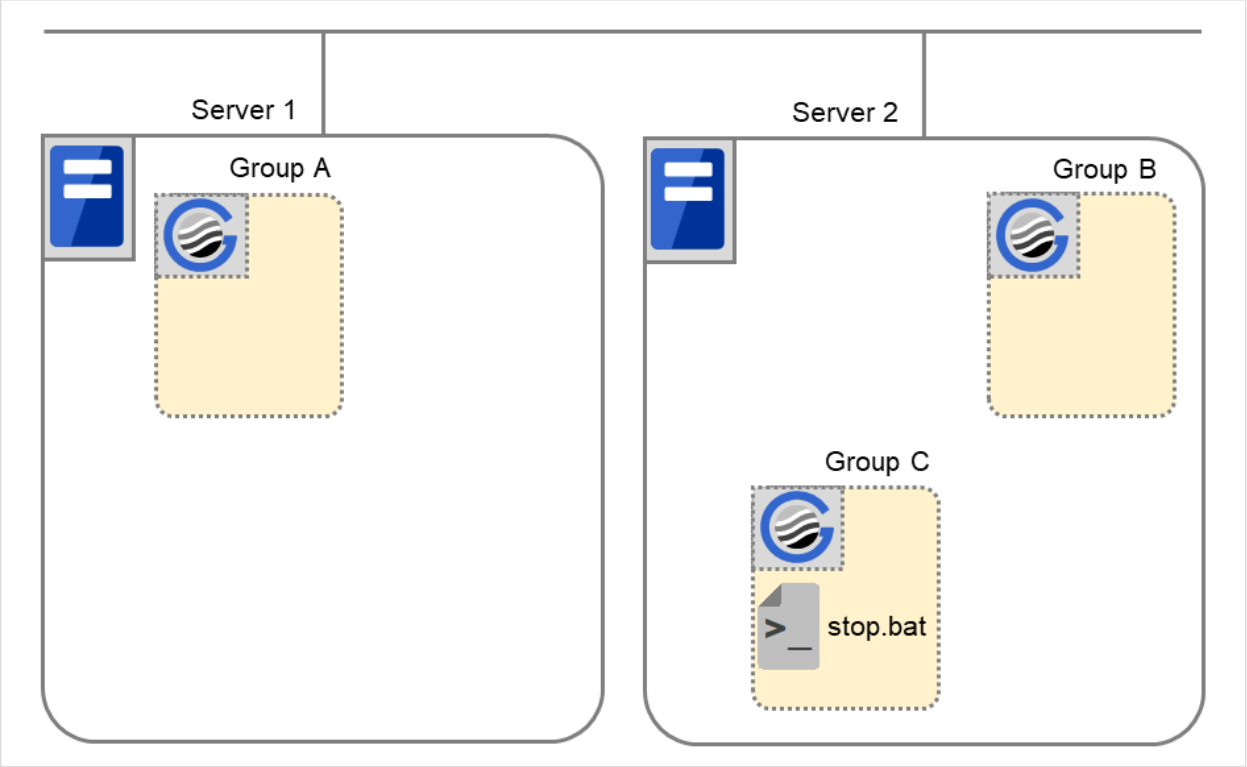


Fig. 3.72: Situation and script execution: stopping Group C

The environment variables for stop.bat

	Group C
CLP_EVENT	FAILOVER
CLP_SERVER	OTHER

13. Starting Group C

The start script of Group C is run on Server 2.

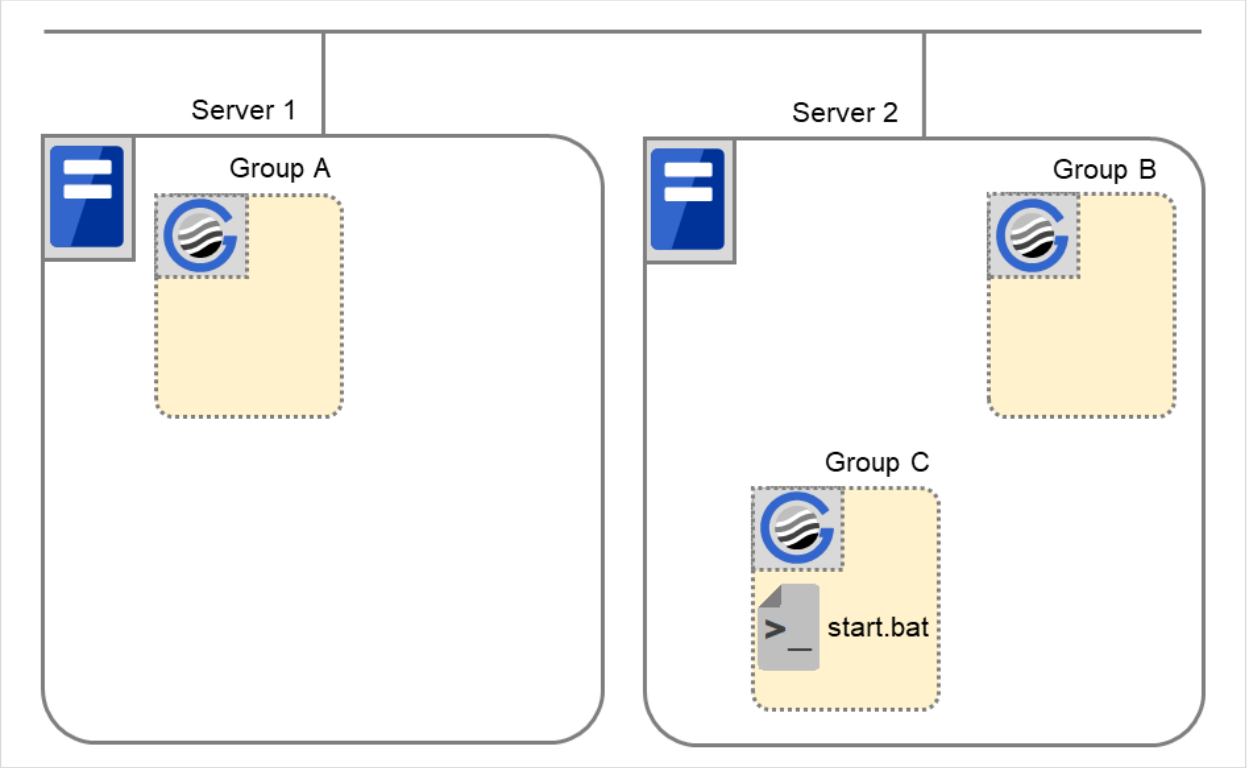


Fig. 3.73: Situation and script execution: starting Group C

The environment variables for start.bat

	Group C
CLP_EVENT	START
CLP_SERVER	OTHER

Additional 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).

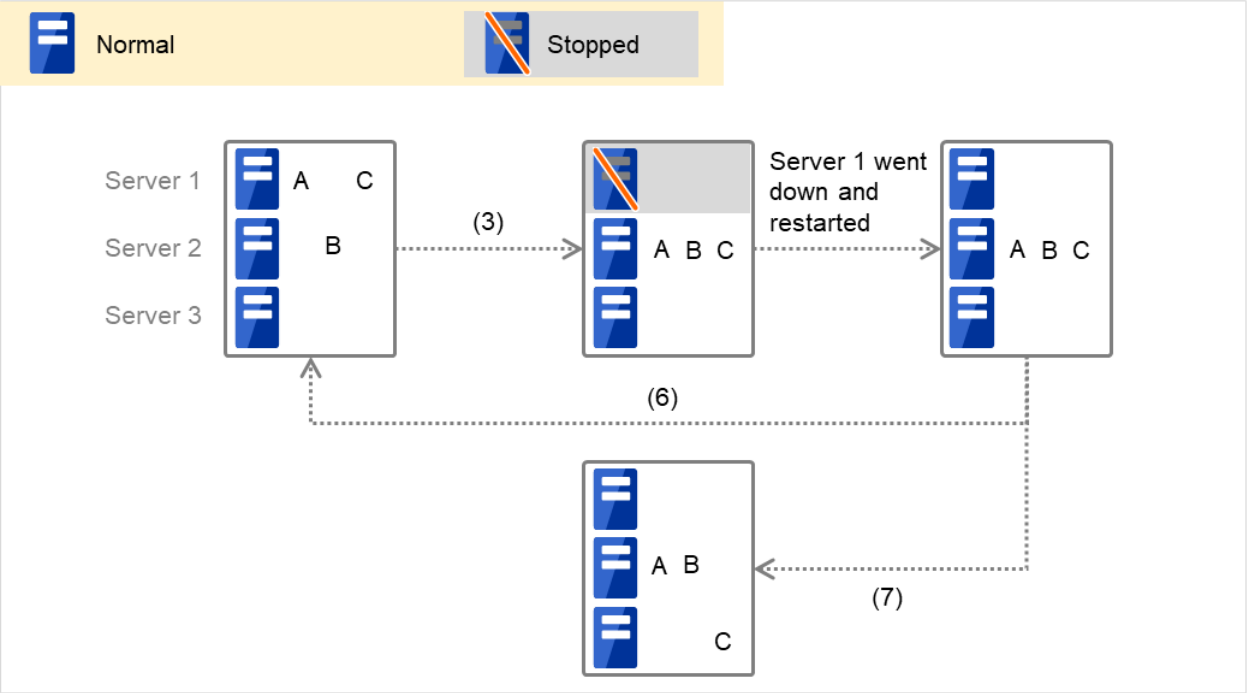


Fig. 3.74: Example of cluster status transition: failover due to server down

Example 1: "3. Failover at the failed Server 1" in the cluster status transition diagram

A group has Server 1 as its primary server. If an error occurs on Server 1, the group's start script is run on Server 2 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) in the start script in advance.

For a process to be performed only on the server that has the second highest priority failover policy, you need to write CLP_PRIORITY(=2) as the branching condition.

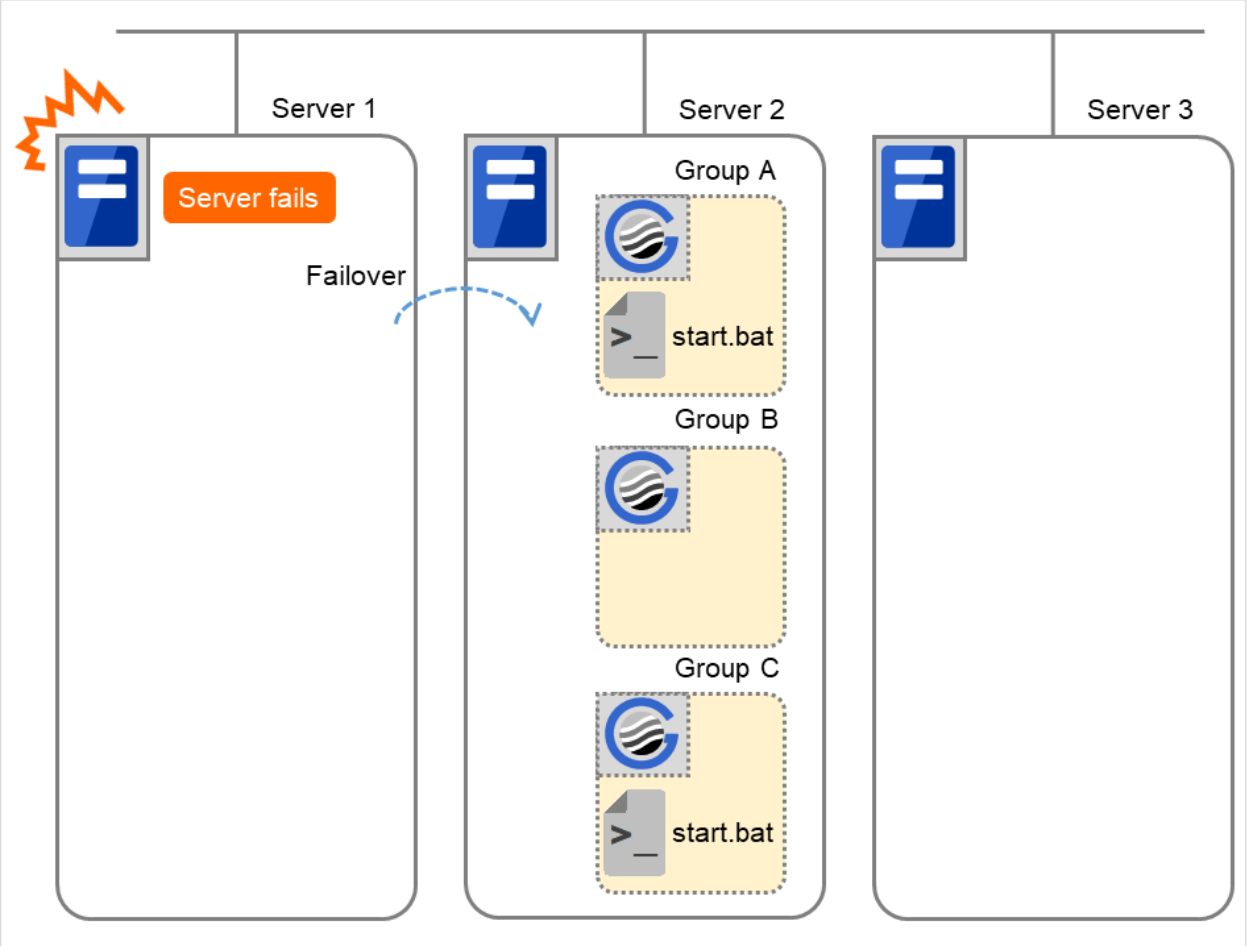


Fig. 3.75: Situation and script execution: starting Groups A and C

Environment variables for start.bat

	Group A	Group C
CLP_EVENT	FAILOVER	FAILOVER
CLP_SERVER	OTHER	OTHER
CLP_PRIORITY	2	2

Example 2: "6. Moving of Group A and C" in the cluster status transition diagram

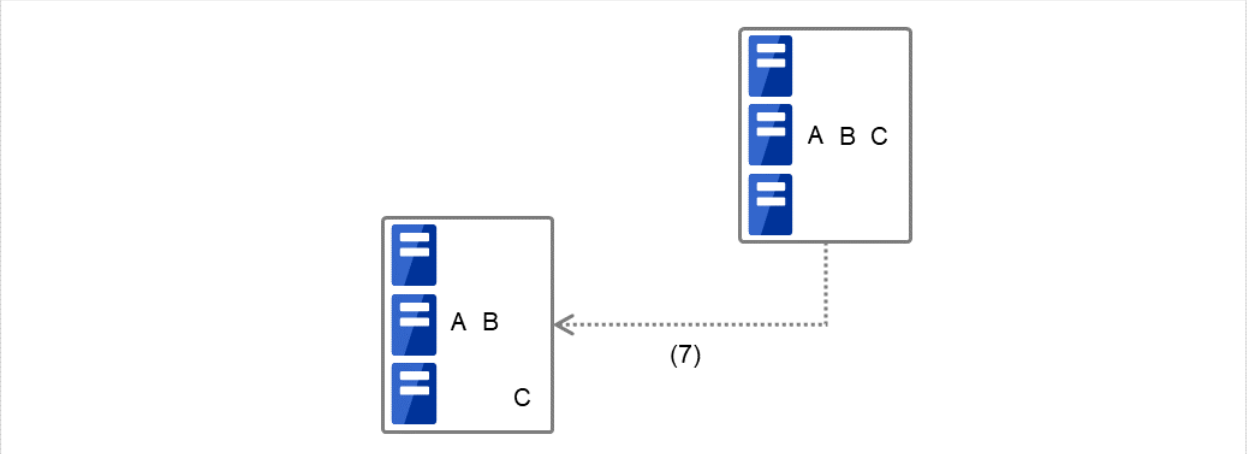


Fig. 3.76: Example of cluster status transition: moving Group C

After the stop scrip of Group C is run on Server 2 from which the group failed over, the start script is run on Server 3.

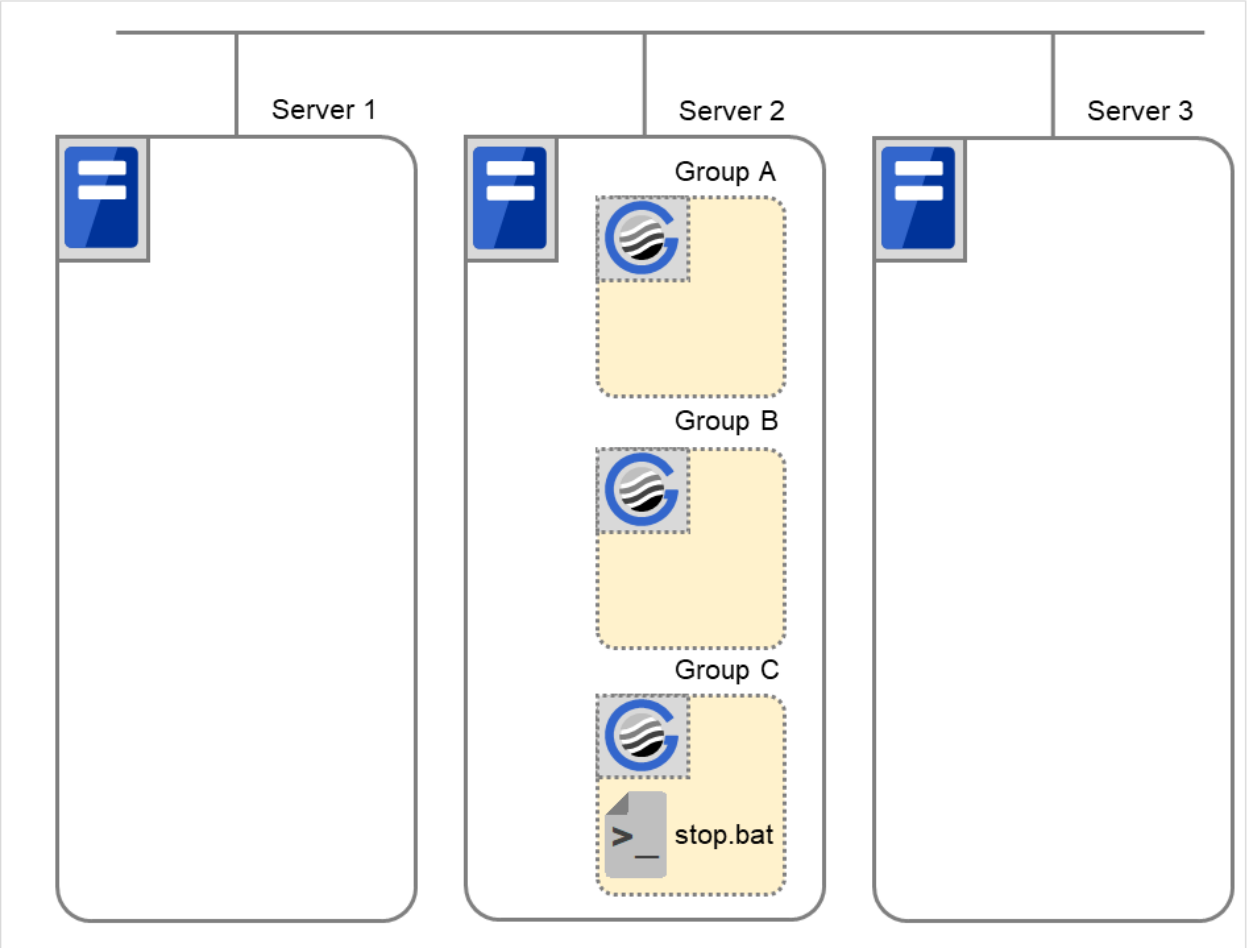


Fig. 3.77: Situation and script execution: moving Group C (1)

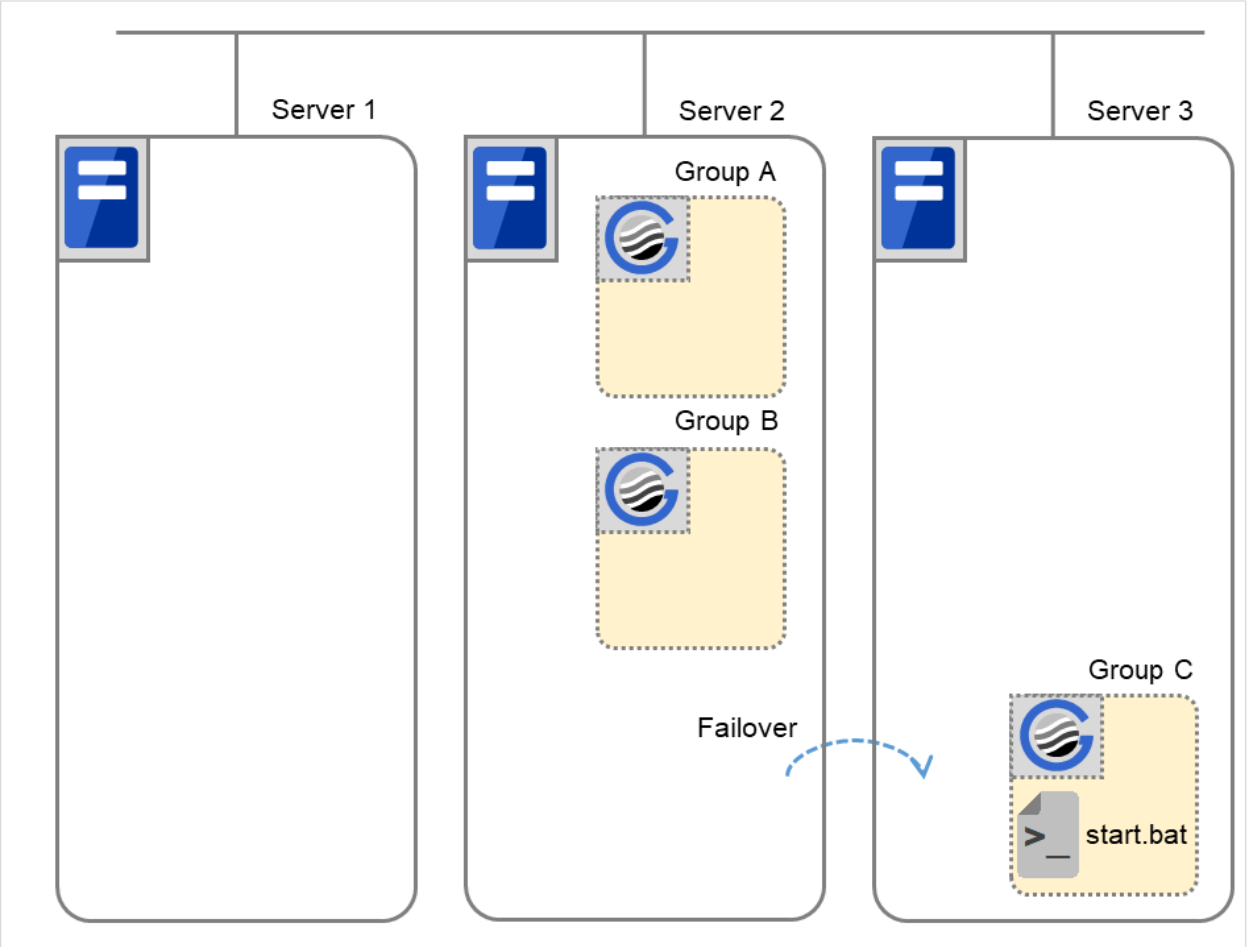


Fig. 3.78: Situation and script execution: moving Group C (2)

Environment variables for stop.bat

	Group C
CLP_EVENT	FAILOVER
CLP_SERVER	OTHER
CLP_PRIORITY	2

Environment variables for start.bat

	Group C
CLP_EVENT	START
CLP_SERVER	OTHER
CLP_PRIORITY	3

Additional information 2

When a monitor resource starts or restarts a script:

The environment variables to run a start script when a monitor resource are as follows:

Example 1: a monitor resource detected an error and restarts Group A on the Server 1.

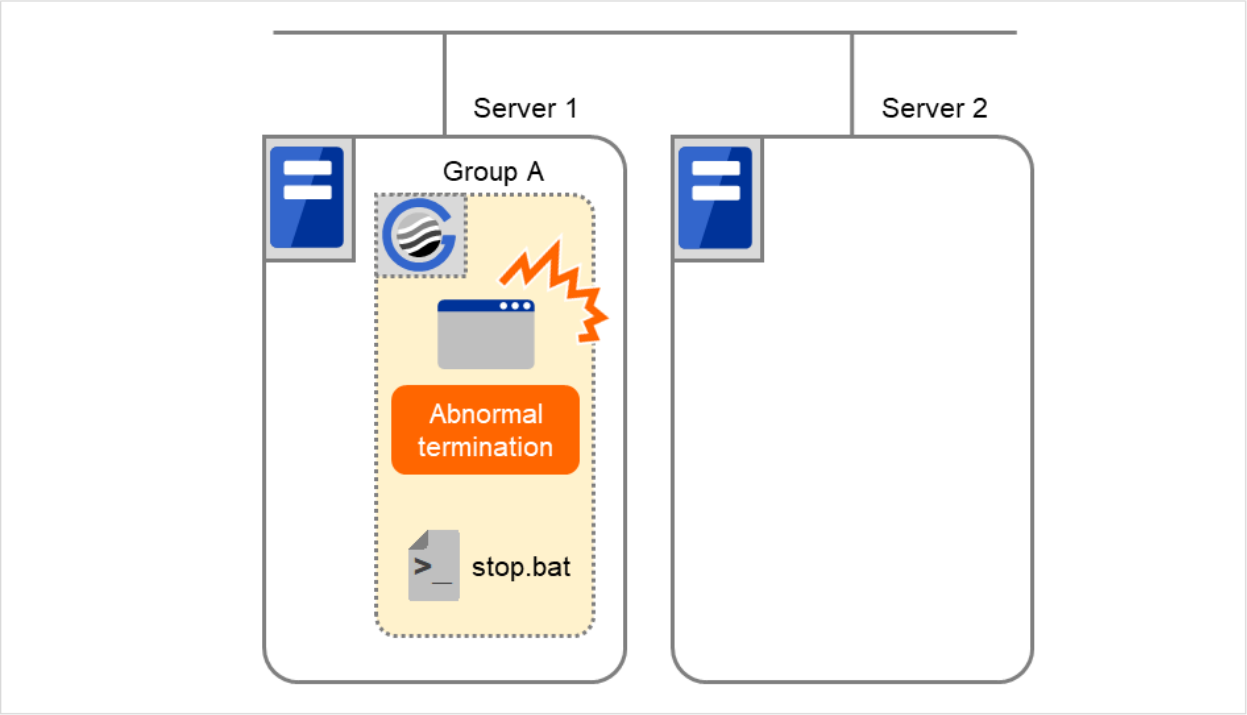


Fig. 3.79: Situation and script execution: restarting Group A (1)

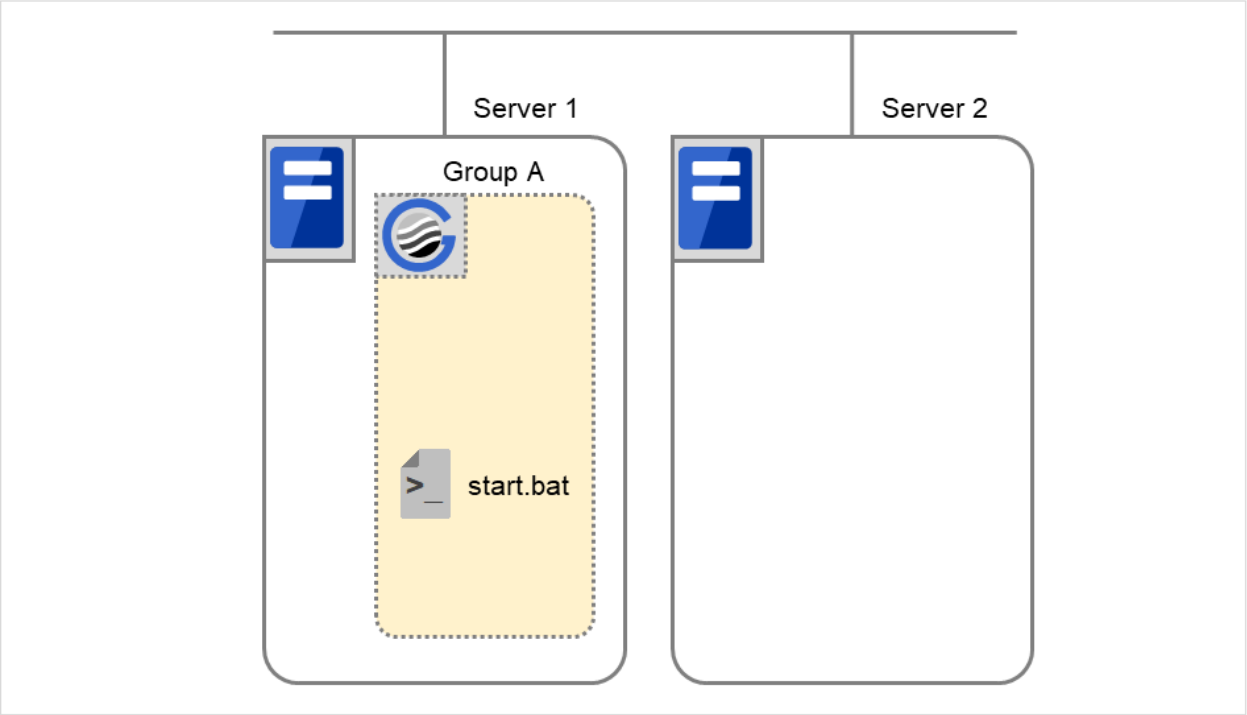


Fig. 3.80: Situation and script execution: restarting Group A (2)

Environment variable for stop.bat

	Group A
CLP_EVENT	The same value as when the start script is run

Environment variable for start.bat

		Group A
(1)	CLP_EVENT	RECOVER
(2)	CLP_EVENT	Start

* start.bat is executed twice.

Example2: a monitor resource detected an error and restarts Group A on Server 2 through failover to Server 2.

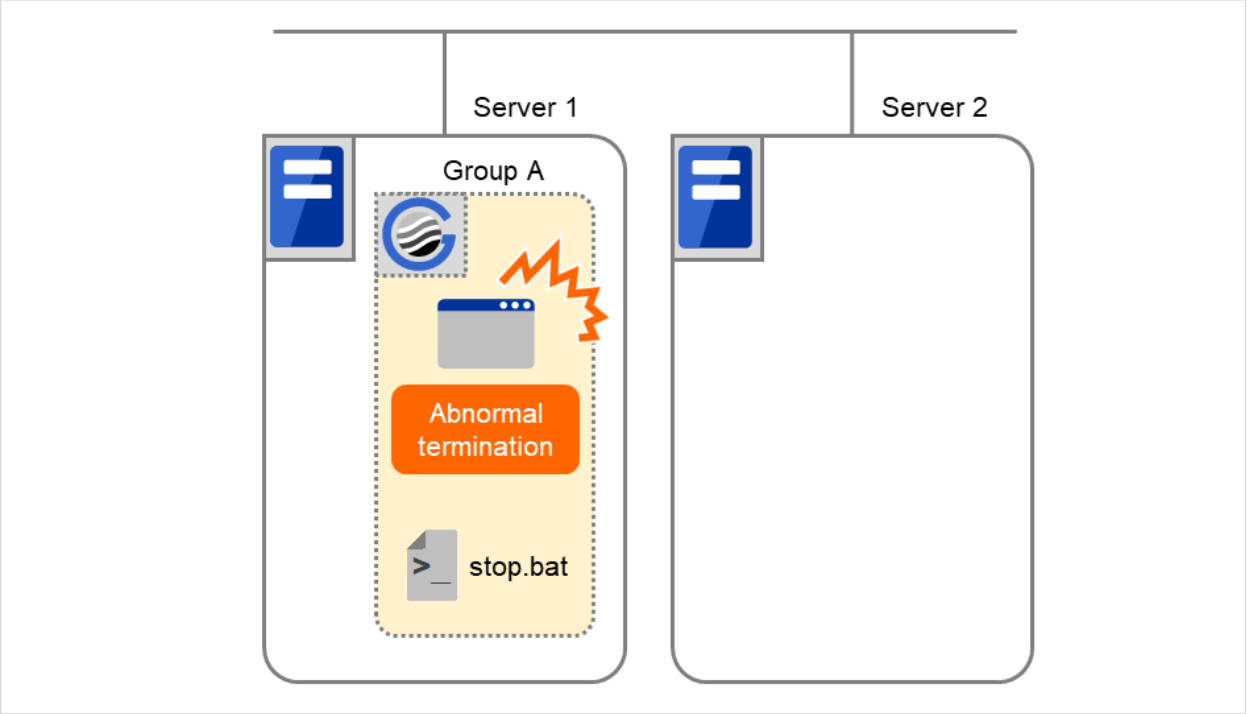


Fig. 3.81: Situation and script execution: failover of Group A (1)

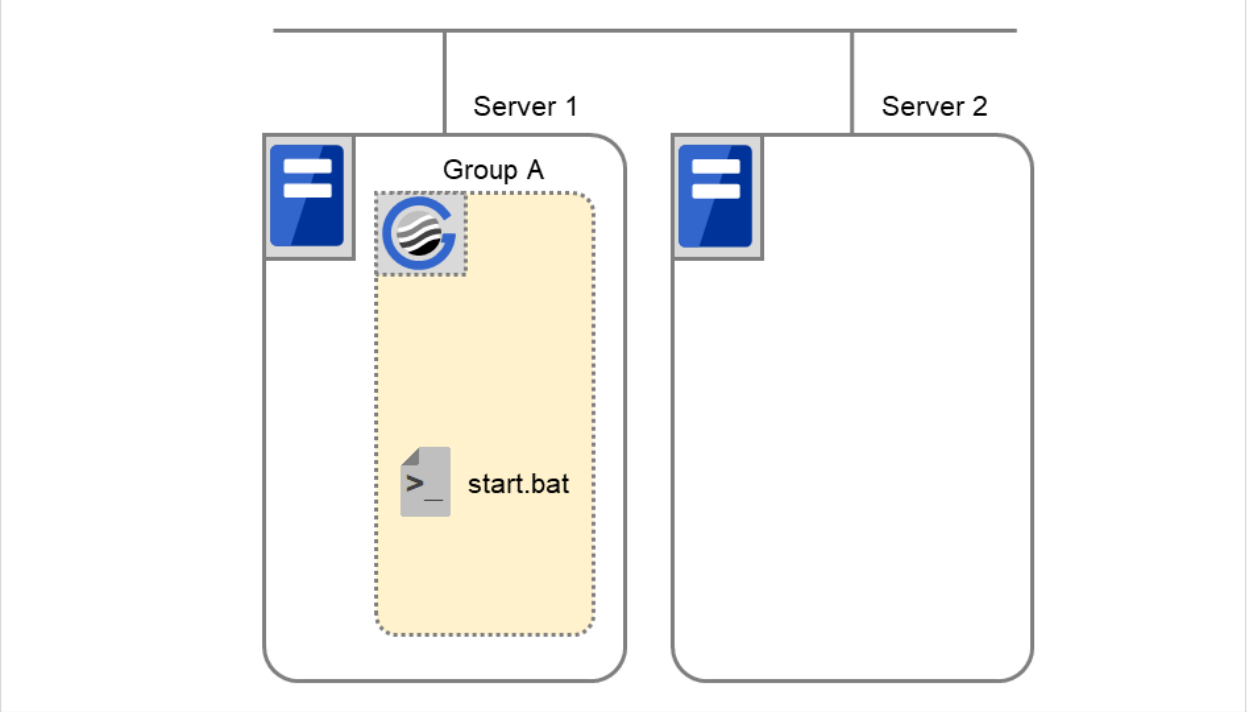


Fig. 3.82: Situation and script execution: failover of Group A (2)

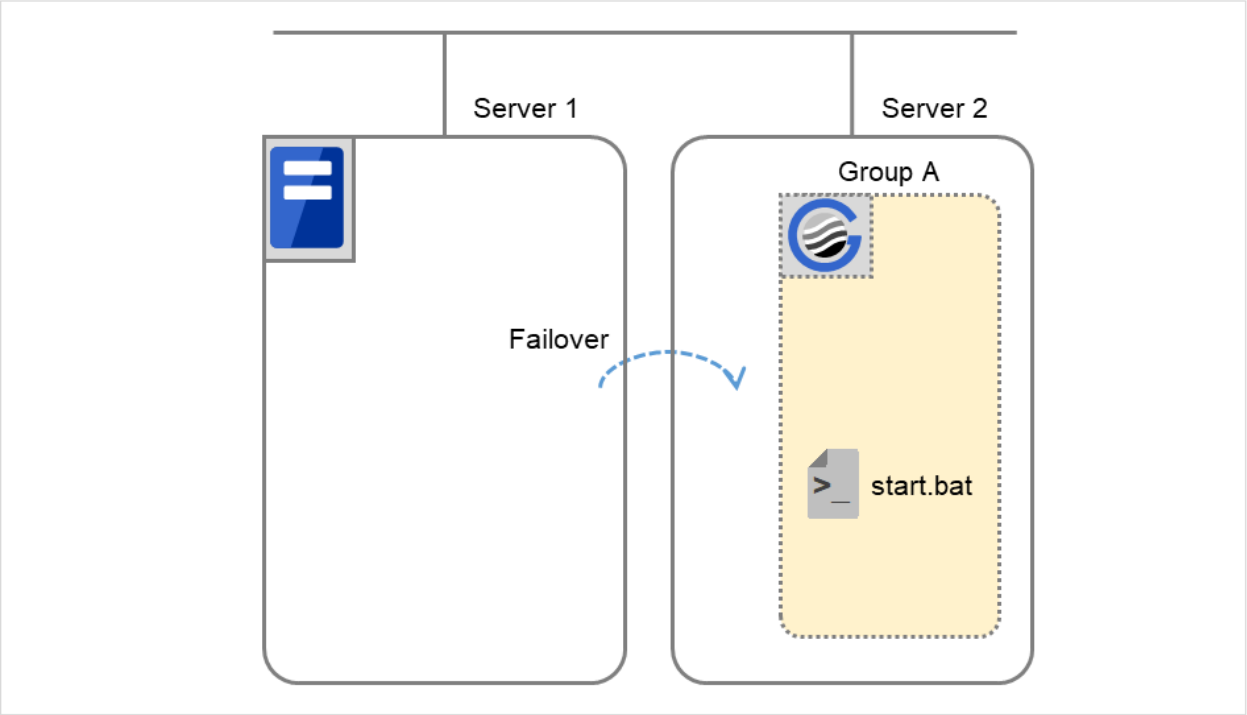


Fig. 3.83: Situation and script execution: failover of Group A (3)

Environment variable for stop.bat

	Group A
CLP_EVENT	The same value as when the start script is run

Environment variable for start.bat

		Group A
(1)	CLP_EVENT	RECOVER
(2)	CLP_EVENT	FAILOVER

Supplementary information 3

With **Execute on standby server** of **Script 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 script of script resource*" as described above.)
- No failover is performed for the cluster service stopped on the active server.

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>

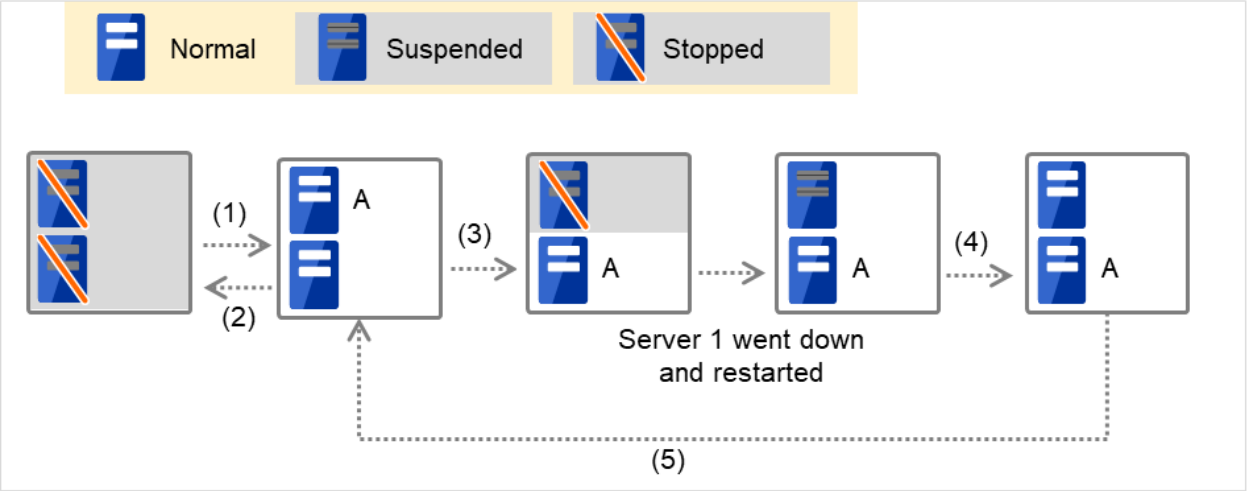


Fig. 3.84: Example of cluster status transition: failover due to server down

Numbers 1. to 5. 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.

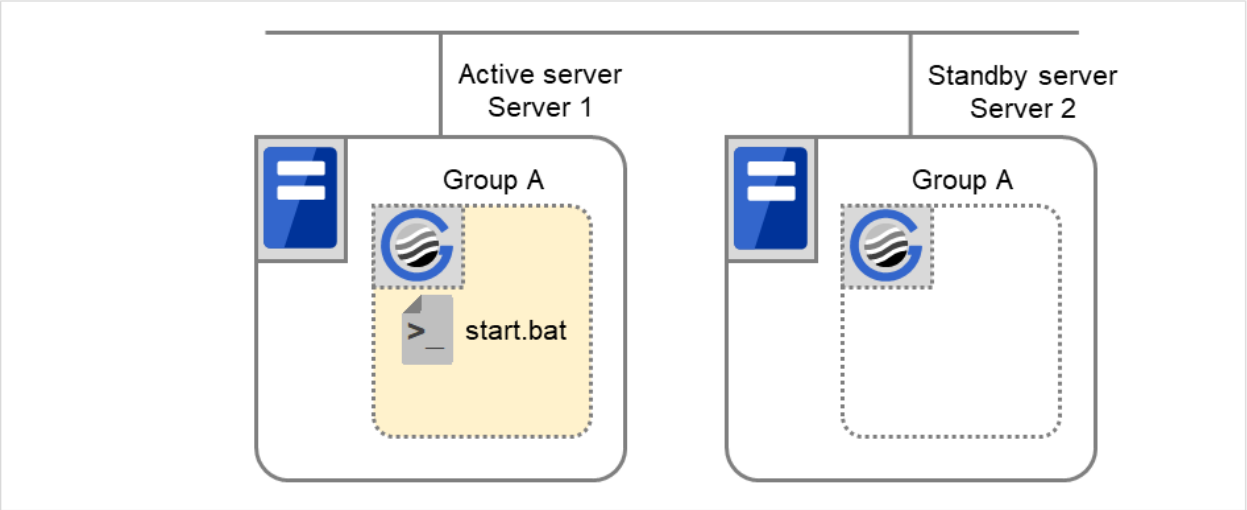


Fig. 3.85: Situation and script execution: normal startup of Group A (1)

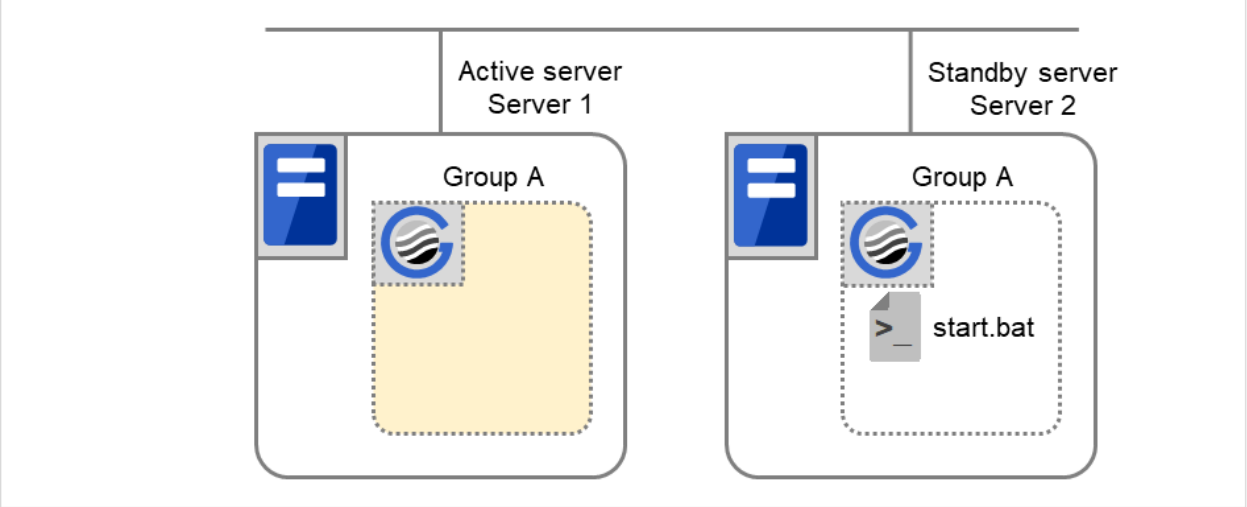


Fig. 3.86: Situation and script execution: normal startup of Group A (2)

Environment variables for start.bat

	Server 1	Server 2
CLP_EVENT	START	STANDBY
CLP_SERVER	HOME	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.

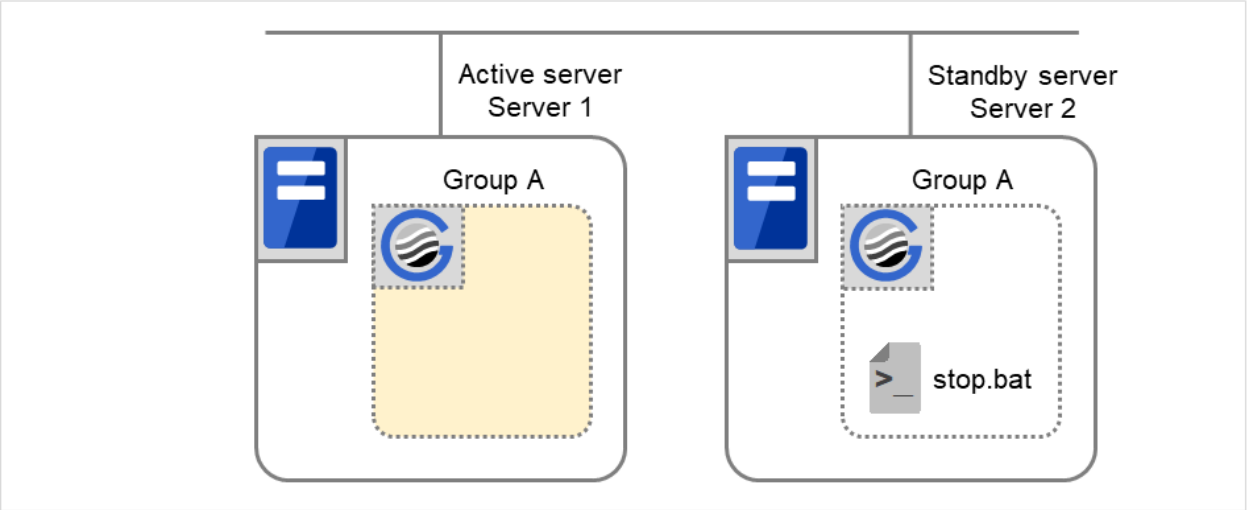


Fig. 3.87: Situation and script execution: normal shutdown of Group A (1)

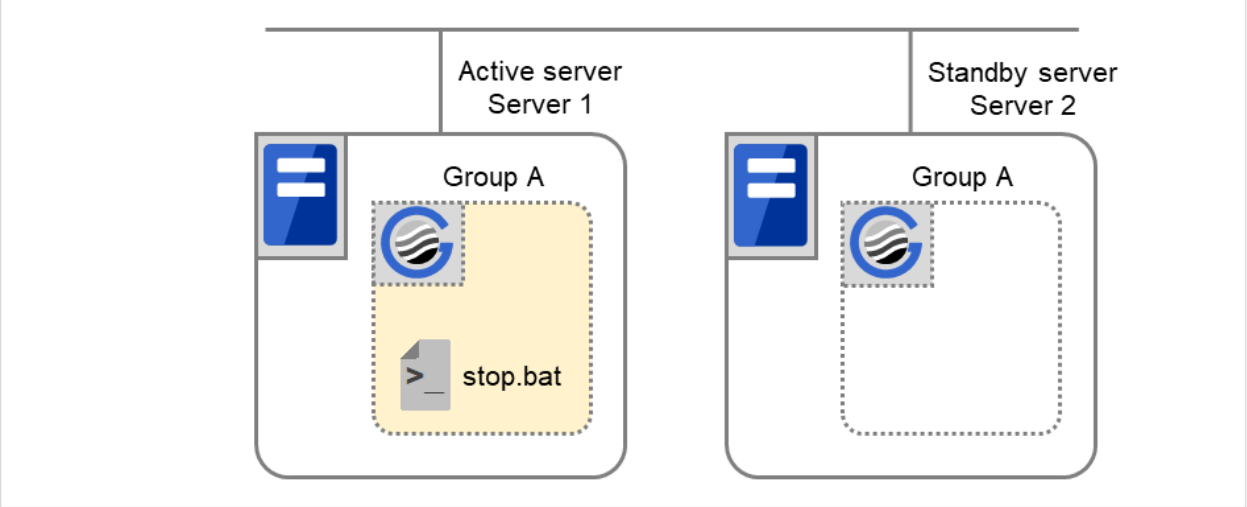


Fig. 3.88: Situation and script execution: normal shutdown of Group A (2)

Environment variables for stop.bat

	Server 1	Server 2
CLP_EVENT	START	STANDBY
CLP_SERVER	HOME	OTHER

3. **Failover at Server 1 down**

When an error occurs in Server 1, the group is failed over to Server 2, 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 Server 1 crashed, the start script is not run on it as the standby server.

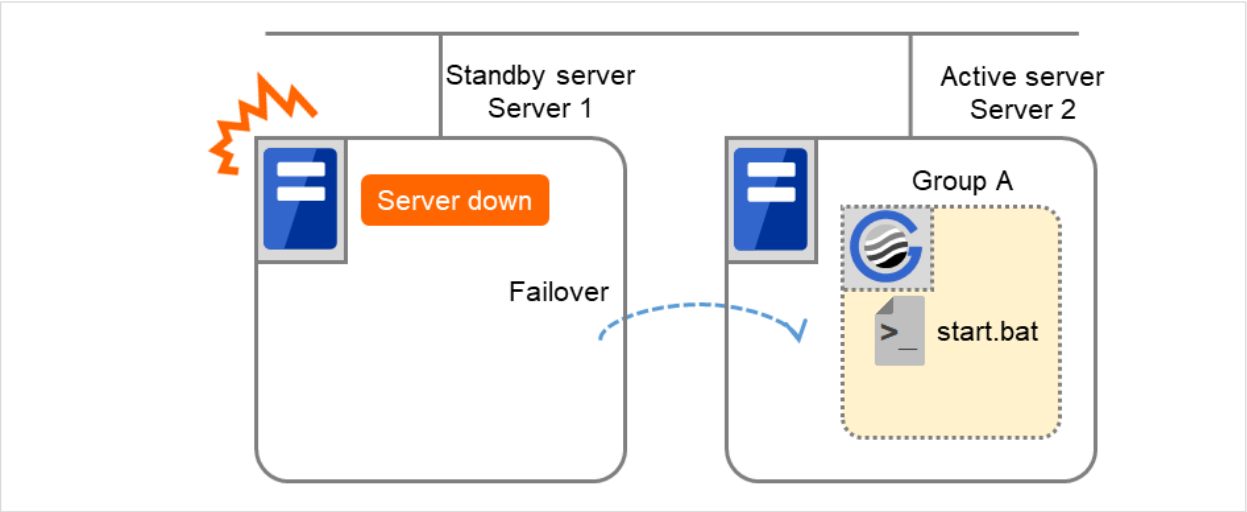


Fig. 3.89: Example of cluster status transition: failover due to server down

Environment variables for start.bat

	Server 2
CLP_EVENT	FAILOVER
CLP_SERVER	OTHER

4. **Recovering Server 1 to cluster**

When you return Server 1 that has been rebooted (operating as a non-cluster) to a cluster, the start script of the failover group that was running on the occurrence of a failover is run in Server 1. This means a recovery is made in the server where the failover has occurred.
To execute the recovery (for example, for recovering database information in a local disk), you need to write CLP_EVENT (=RECOVER) as a branch condition. Even if the recovery is not required, write the script not to start the operation.

In this case, the start script is executed in Server 1, but not in Server 2.

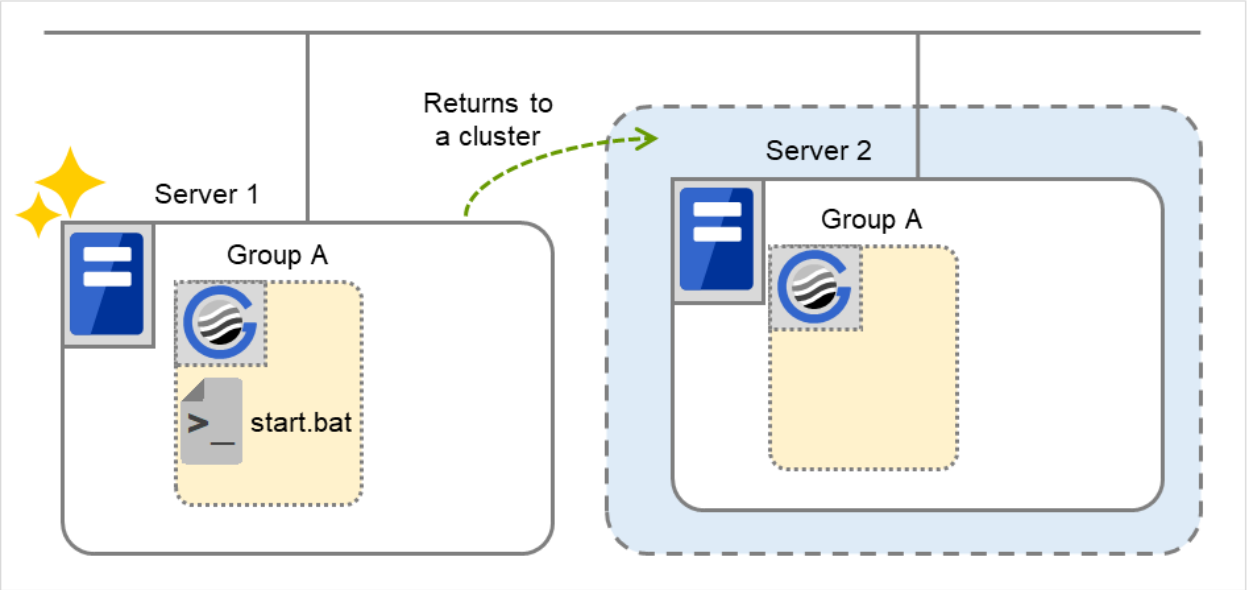


Fig. 3.90: Situation and script execution: returning a server to the cluster

Environment variables for start.bat

	Server 1
CLP_EVENT	RECOVER
CLP_SERVER	HOME

5. **Moving of Group A**

The stop script for Group A is executed on Server 1 (= standby server) and Server 2 (= active server). Then the start script is run on Server 1 (= active server) and Server 2 (= standby server).

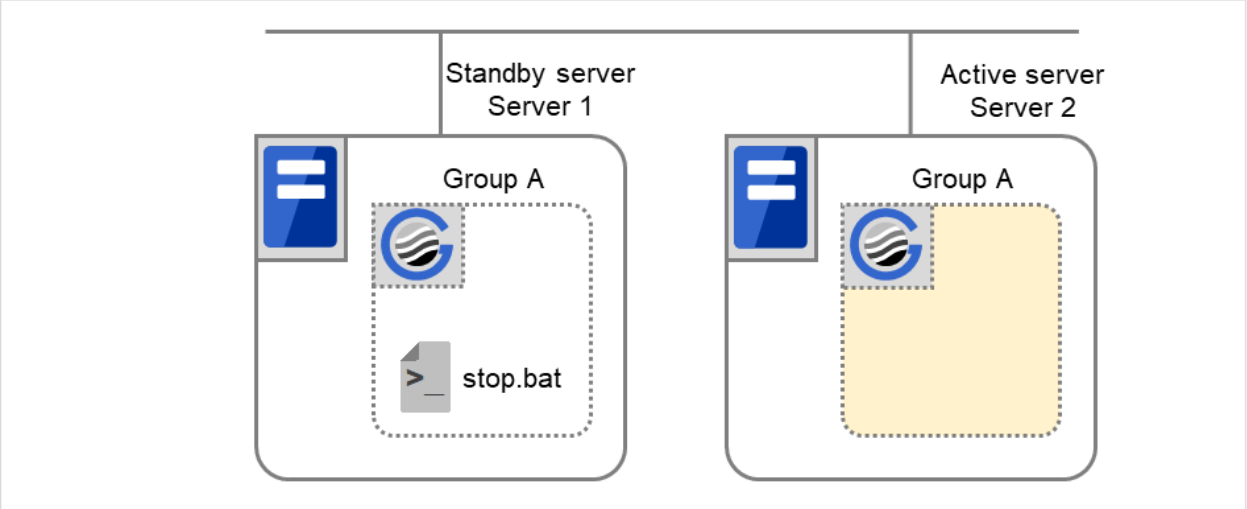


Fig. 3.91: Situation and script execution: moving Group A (1)

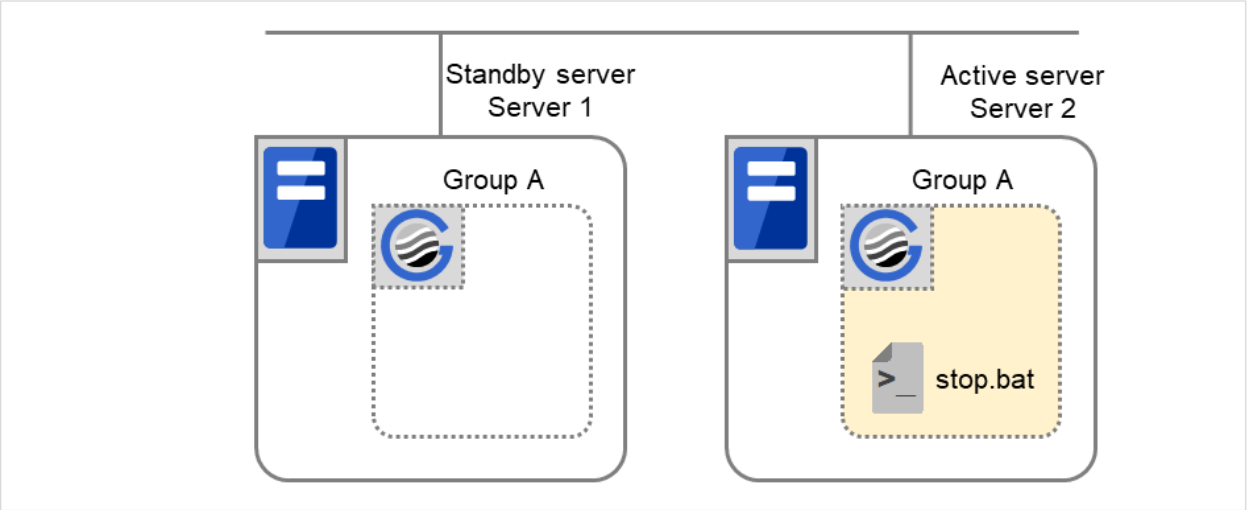


Fig. 3.92: Situation and script execution: moving Group A (2)

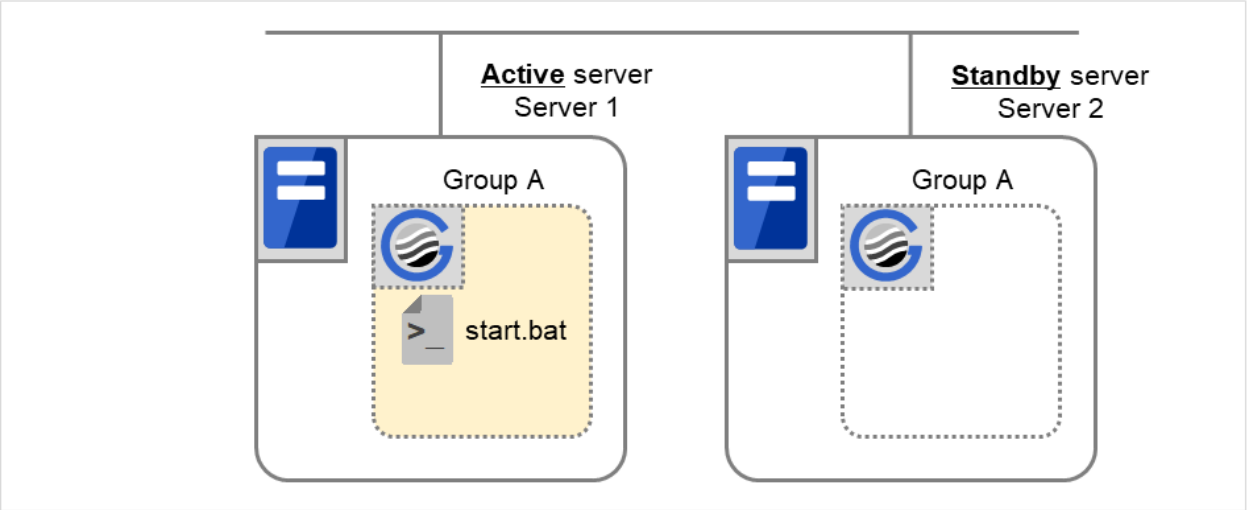


Fig. 3.93: Situation and script execution: moving Group A (3)

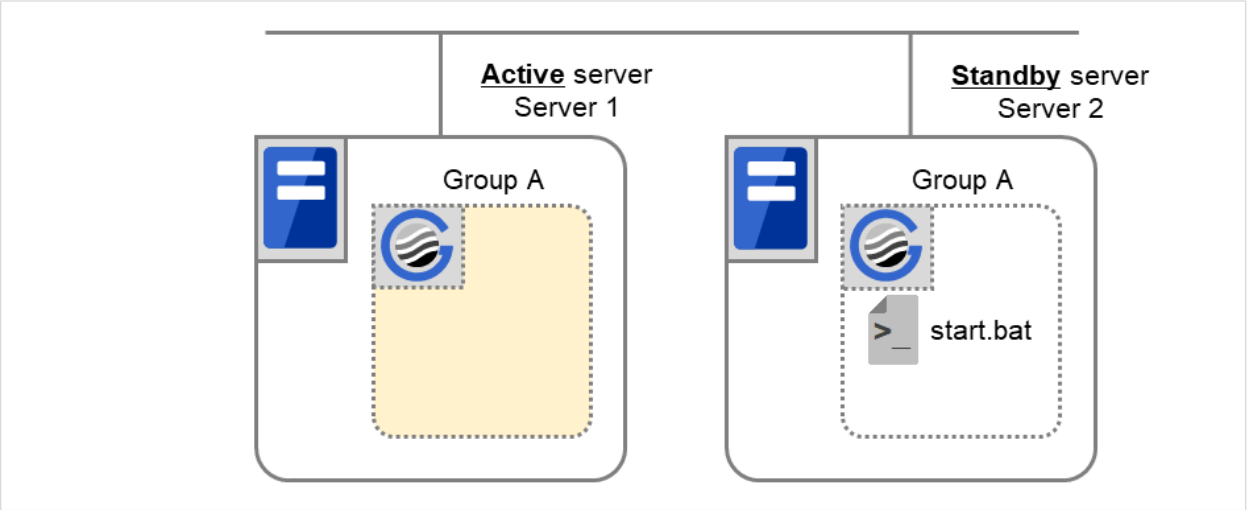


Fig. 3.94: Situation and script execution: moving Group A (4)

Environment variables for stop.bat

	Server 1	Server 2
CLP_EVENT	STANDBY	FAILOVER[5]
CLP_SERVER	HOME	OTHER

[5] 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 "5. 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 "5. Moving of Group A".

Environment variables for start.bat

	Server 1	Server 2
CLP_EVENT	START	STANDBY
CLP_SERVER	HOME	OTHER

3.10.5 Writing scripts

This section describes how you actually write script codes in association with timing to run scripts as mentioned in the previous topic.

Numbers in brackets "(*number*)" in the following example script code represent the actions described in "Execution timing of script resource scripts".

Group A start script: a sample of **start.bat**

```
rem ***************************************************************
rem *                          START.BAT                          *
rem ***************************************************************

rem Refer to the environment variable of the script execution factor to␣
↪determine the subsequent process.
IF "%CLP_EVENT%"=="START" GOTO NORMAL
IF "%CLP_EVENT%"=="FAILOVER" GOTO FAILOVER
IF "%CLP_EVENT%"=="RECOVER" GOTO RECOVER


rem EXPRESSCLUSTER is not working.
GOTO no_clp


:NORMAL
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem Here, write the normal startup process of the operation.
    rem This process is to be performed at the timing of the following:
    rem
    rem (1) Normal startup
    rem (6) Moving of Group A and C (online failback)
    rem


rem Refer to the environment variable of the execution server to determine␣
↪the subsequent process.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER1

    rem Here, write a process to be performed only for
    rem the normal startup of the operation on the primary server.
    rem This process is to be performed at the timing of the following:
    rem
    rem (1) Normal startup
    rem (6) Moving of Groups A and C (online failback)
    rem
```

(continues on next page)

(continued from previous page)

```
GOTO EXIT


:ON_OTHER1

rem Here, write a process to be performed only for
rem the normal startup of the operation on a non-primary server.


GOTO EXIT


:FAILOVER

rem Refer to the environment variable of DISK connection information to␣
↪perform error handling.
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem Write the startup process of the operation on the failover␣
↪destination server.
    rem This process is to be performed at the timing of the following:
    rem
    rem (3) Failover at the failed Server 1
    rem


rem Refer to the environment variable of the execution server to determine␣
↪the subsequent process.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER2

    rem Write a process to be performed only for the startup of
    rem the operation on the primary server after the failover.

GOTO EXIT


:ON_OTHER2

rem Write a process to be performed only for the startup of
rem the operation on a non-primary server after the failover.
rem This process is to be performed at the timing of the following:
rem
rem (3) Failover at the failed Server 1
rem

GOTO EXIT


:RECOVER

rem Write a recovery process to be performed after returning to the cluster.
rem This process is to be performed at the timing of the following:
rem
rem (4) Recovering Server 1 to cluster
rem

GOTO EXIT
```

(continues on next page)

(continued from previous page)

```
:ERROR_DISK

rem Write a disk-related error-handling process.

:no_clp

:EXIT
exit
```

Group A stop script: a sample of **stop.bat**

```
rem ************************************************************
rem *                          STOP.BAT                        *
rem ************************************************************

rem Refer to the environment variable of the script execution factor to␣
↪determine the subsequent process.
IF "%CLP_EVENT%"=="START" GOTO NORMAL
IF "%CLP_EVENT%"=="FAILOVER" GOTO FAILOVER


rem EXPRESSCLUSTER is not working.
GOTO NO_CLP


:NORMAL
rem Refer to the environment variable of DISK connection information to␣
↪perform error handling.
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem Here, write the normal end process of the operation.
    rem This process is to be performed at the timing of the following:
    rem
    rem (2) Normal shutdown
    rem


rem Refer to the environment variable of the execution server to determine␣
↪the subsequent process.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER1

    rem Here, write a process to be performed only for
    rem the normal process of the operation on the primary server.

    rem This process is to be performed at the timing of the following:
    rem
    rem (2) Normal shutdown
    rem

GOTO EXIT


:ON_OTHER1

rem Write a process to be performed only for the normal end
rem of the operation on a non-primary server.

GOTO EXIT


:FAILOVER

rem Refer to the environment variable of DISK connection information to␣
↪perform error handling.
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem Write the normal end process to be performed after the failover.
```

(continues on next page)

(continued from previous page)

```
    rem This process is to be performed at the timing of the following:
    rem
    rem (5) Cluster shutdown after failover of Server 1
    rem (6) Moving of Group A and C
    rem


rem Refer to the environment variable of the execution server to determine␣
↪the subsequent process.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER2

    rem Write a process to be performed only for the end of
    rem the operation on the primary server after the failover.

GOTO EXIT


:ON_OTHER2

rem Write a process to be performed only for the end of
rem the operation on a non-primary server after the failover.
rem This process is to be performed at the timing of the following:
rem
rem (5) Cluster shutdown after failover of Server 1
rem (6) Moving of Group A and C
rem

GOTO EXIT


:ERROR_DISK

rem Write a disk-related error-handling process.

:NO_CLP

:EXIT
exit
```

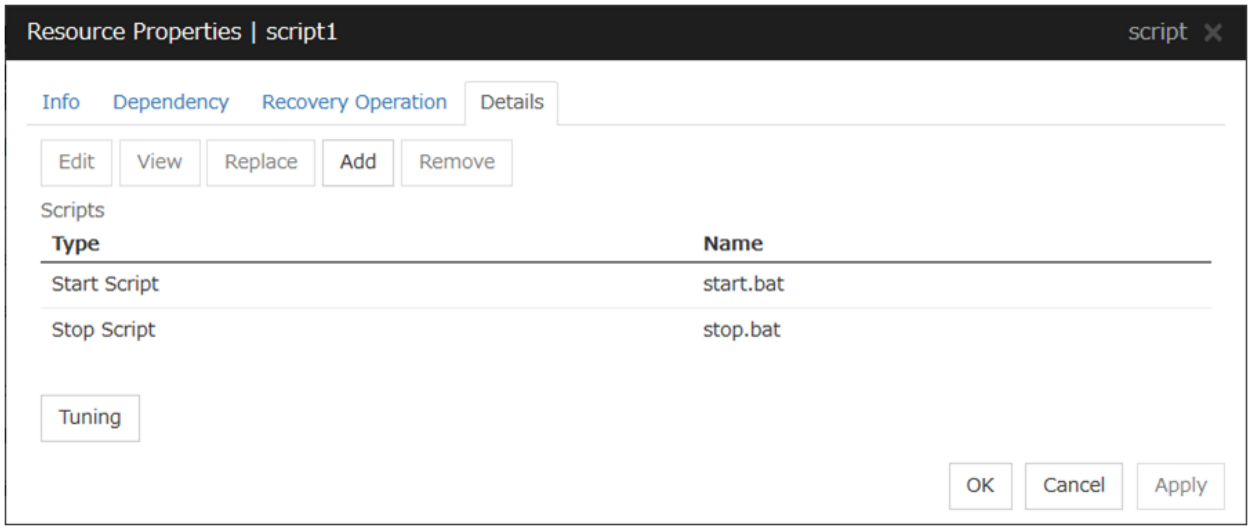
3.10.6 Tips for creating scripts

The clplogcmd command, though which message output on the alert log is possible, is available.

3.10.7 Notes on script resources

Stop the processing by using the exit command in the script activated through the start command, when the start command is used in the start/stop script.

3.10.8 Details tab



Add

Use this button to add a script other than **start.bat** script and **stop.bat** script.

Note:

Do not use 2-byte characters for the name of a script to be added.
Do not use "& (ampersand)" nor "= (equal mark)" for the name of a script to be added.

Remove

Use this button to delete a script. The **start.bat** script and **stop.bat** script cannot be deleted.

View

Use this button to display the selected script file.

Edit

Use this button to edit the selected script file. Click **Save** to apply the change. You cannot rename the script file

Replace

Opens the **Open** dialog box, where you can select a file.

Note: The file will not be deleted even if you delete a script file from the Cluster WebUI. If the cluster configuration data is reloaded by restarting the Cluster WebUI after deleting the script file, the deleted script file will be displayed in the **Scripts**.

The content of the script file selected in the **Resource Properties** is replaced with the one selected in the **Open** dialog box. If the selected script file is being viewed or edited, replacement cannot be achieved. Select a script file, not a binary file such as an application program.

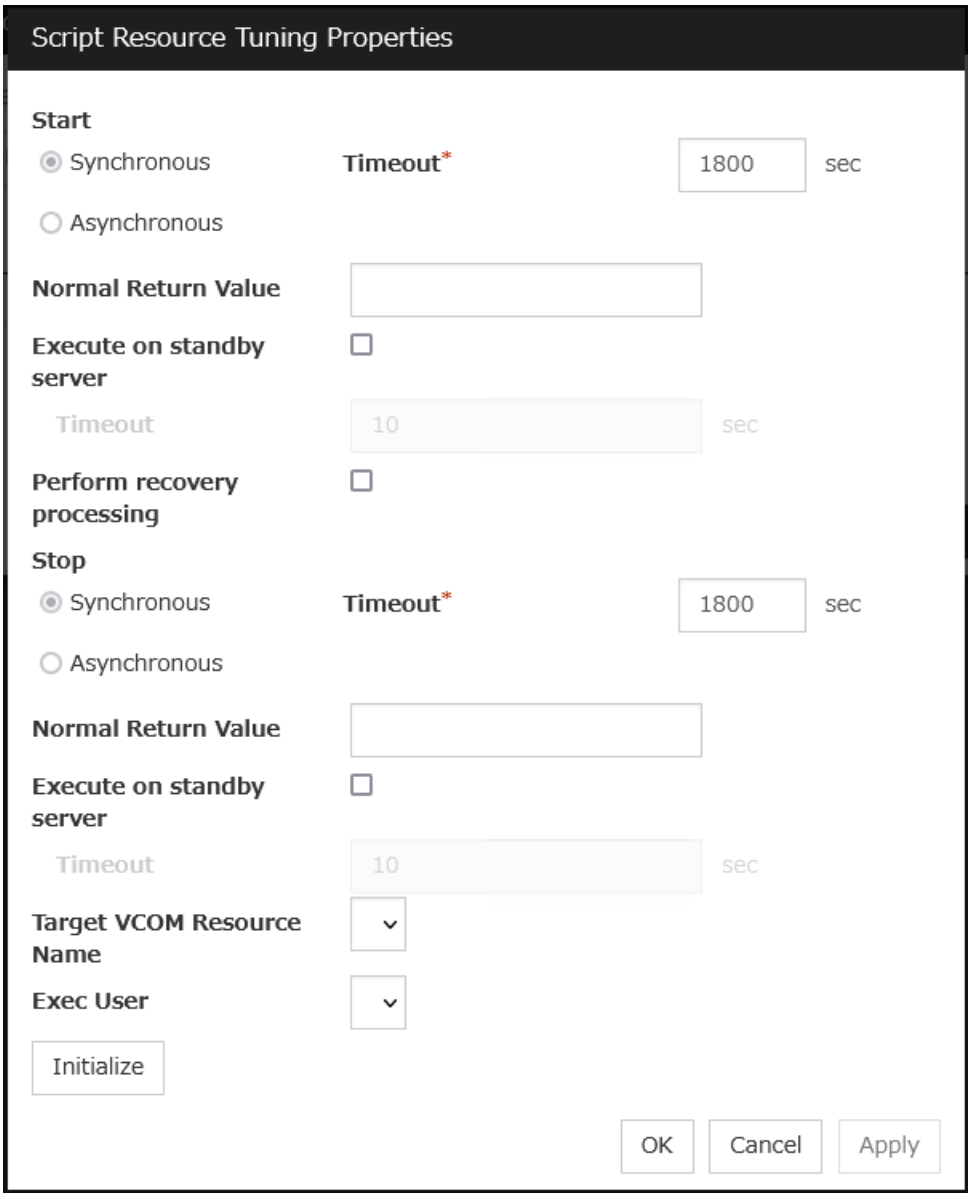
Tuning

Open the **Script Resource Tuning Properties** dialog box. You can make advanced settings for the script resource.

Script Resource Tuning Properties

Parameter tab

Display the details of setting the parameter.



Common to all start scripts and stop scripts

Synchronous

Select this button to wait for a script to end when it is run.

Asynchronous

This cannot be selected.

Normal Return Value (Within 1023 bytes)

Configure what error code from the script is normal.

- When there is no value
  The return value is ignored.
- When there is a value
  Observe the following input rules.
  - Values can be separated by commas (for example, 0, 2, 3).
  - Values can be specified using a hyphen (for example, 0-3).

Note:

When specifying a value to **Normal Return Value**, set the same value to start script and stop script.
An error cannot be detected when 1 is specified as **Normal Return Value** because 1 is returned when an error occurs with cmd.exe which executes the script.

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.

Perform recovery processing

Specify whether to run a start script or not in any of the following timings:

- When the server is recovered
- When a monitor resource error is detected
- When the group resource activation terminates due to an error

For more information, confirm with "Execution timing of script resource scripts" in this guide. When executed as the recovery operation, RECOVER is set for CLP_EVENT, the environment variable.

Timeout (1 to 9999)

When you want to wait for a script to end (when selecting **Synchronous**), specify how many seconds you want to wait before a timeout. This box is enabled when **Synchronous** is selected. If the script does not complete within the specified time, it is determined as an error.

Target VCOM Resource Name

Configure this to use a virtual computer name as a computer name used for script resources. Virtual computer names and resource names that exist in a failover group to which script resources belong are listed.
When you specify this parameter, add the following environment variables and then start the script:

COMPUTERNAME=<virtual computer name>
_CLUSTER_NETWORK_FQDN_=<virtual computer name>
_CLUSTER_NETWORK_HOSTNAME_=<virtual computer name>
_CLUSTER_NETWORK_NAME_=<virtual computer name>

Note: When **Target VCOM Resource Name** is specified, the EXPRESSCLUSTER commands cannot be used in a script.

Exec User

Select a user by whom the script is to be executed, from users registered in the **Account** tab of **Cluster Properties**.

If no user is specified, the script is run by the local system account.

Initialize

Click **Initialize** to reset the values of all items to their default values.

3.11 Understanding disk resources

3.11.1 Dependencies of disk resources

By default, this function does not depend on any group resource type.

3.11.2 Disk resources

A disk resource refers to a switching partition on a shared disk accessed by more than one server that constitutes a cluster.

- Switching partitions
  A switching partition refers to a partition on a shared disk connected to more than one server in a cluster.
  Switching is done on a failover group basis according to the failover policy. By storing data required for applications on a switching partition, the data can be automatically inherited when failover takes place or a failover group is moved.
  A switching partition should be accessible with the same drive letter in the same area on all servers.

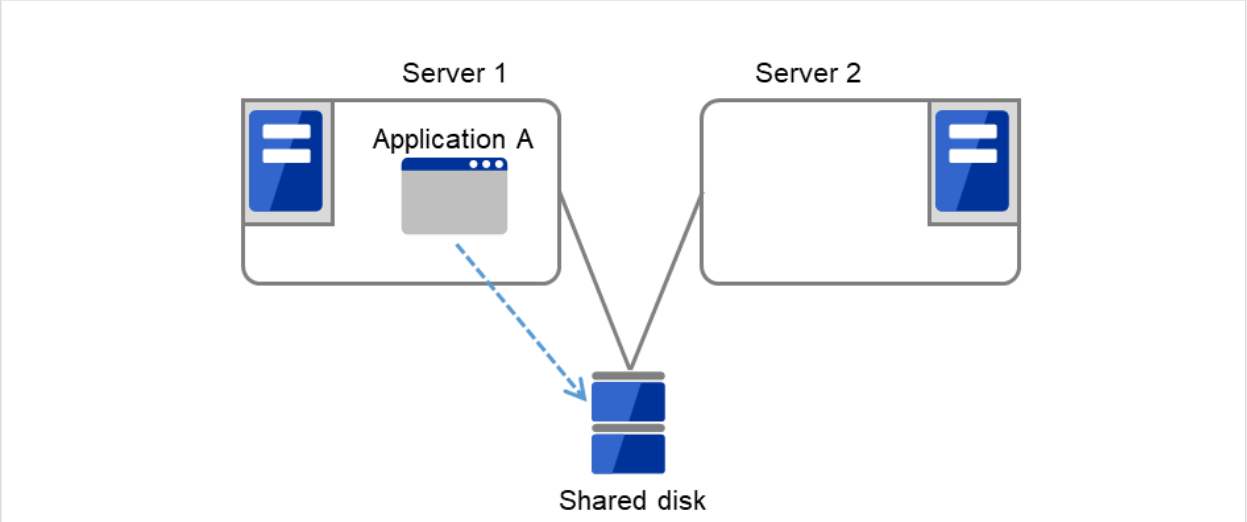


Fig. 3.95: Disk resource (1)

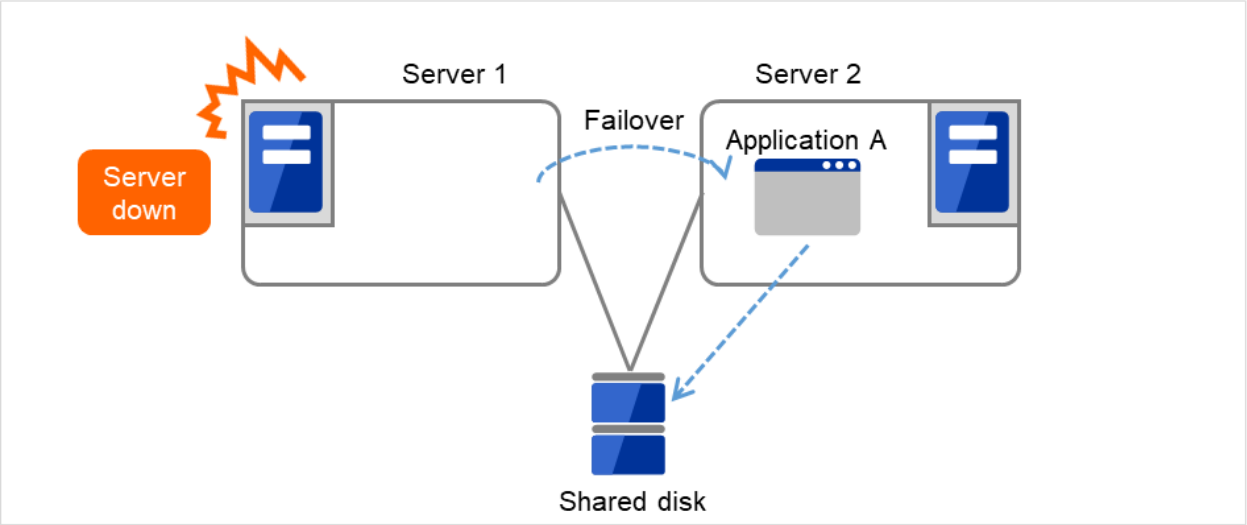


Fig. 3.96: Disk resource (2)

- Size of switching partitions
  There is no restriction on partition size. Allocate any size for partition.
- File system
  Format partitions with NTFS. FAT and FAT32 are not supported.
- Access control
  EXPRESSCLUSTER controls access to file system.
- Configuring Host Bus Adapters (HBAs)
  When more than one server is connected to a shared disk, simultaneous access from servers to the file system can corrupt the data. It is necessary to control accesses to a partition on a shared disk.
  In EXPRESSCLUSTER, accesses to a shared disk are controlled by HBA (Host Bus Adapter) settings. Configure HBAs that connect a shared disk to control accesses.
  For details, see "*HBA tab*" in "*Server Properties*" in "*2. Parameter details*" in this guide.
- Configuring DISK network partition solution resource
  When a disk resource is used, it is recommended to use DISK network partition solution resource.
  For the DISK network partition resolution resources, see "*Understanding network partition resolution by DISK method*".

3.11.3 Notes on disk resources

- Make settings so that the same partition is accessible with the same drive letter on all servers. Even if the drive letter automatically assigned by the OS is the same as the one that you want to assign, be sure to manually assign the drive letter explicitly; for example, by deleting the OS assigned drive letter and then assigning the desired drive letter.
- If a drive letter different from the one used on partition is set, the drive letter will be changed when the disk resource is started up. If the drive letter is used on other partitions, starting up the disk resource will fail.
- Dynamic disk is not supported. If a partition on dynamic disk is used for disk resource, starting up the disk resource will fail.

- Configure HBAs for a partition used for disk resource. If a partition without HBA configuration is used for disk resource, starting up resource will fail.

  When HBA configuration is changed, OS reboot is required to apply the changes. If OS is not rebooted after changing HBA configuration, starting up disk resource will fail.

  For details on HBA configuration, see "*HBA tab*" in "*Server Properties*" in "*2. Parameter details*" in this guide.

  If you try to change or delete a drive character after configuring the HBA, operation may fail. If the operation fails, configure the HBA according to the troubleshooting procedure.

- <Troubleshooting>

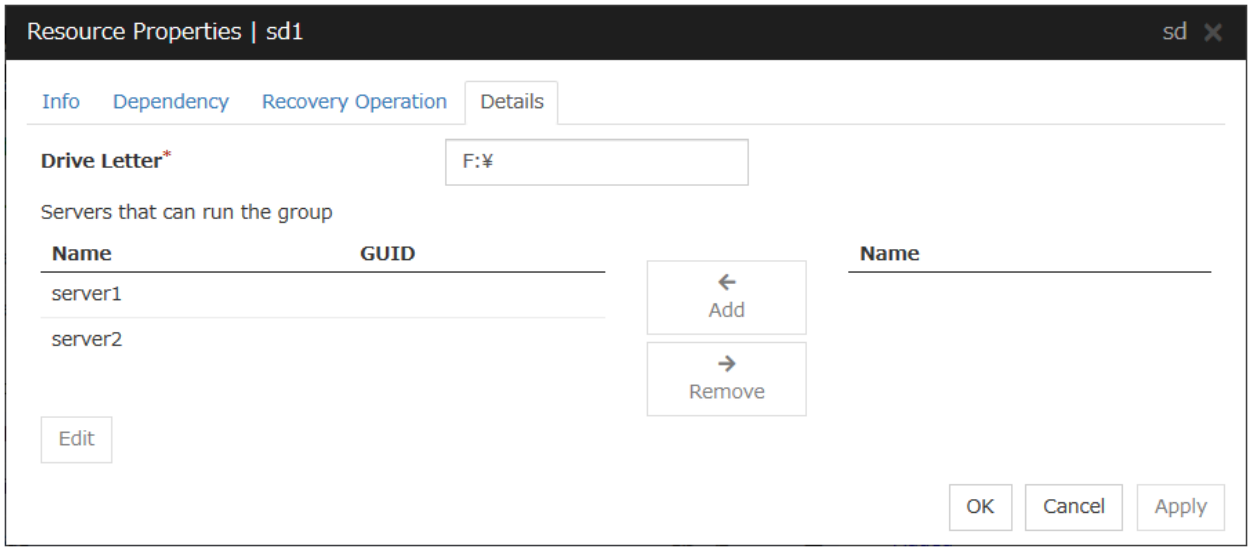
  1. Run the following command at the command prompt to remove the drive character:

     ```
     # mountvol drive_character (of_change_target): /P
     ```

  2. Check that the drive character is removed from the change target drive by using (**Control Panel > Administrative Tools > Computer Management > Disk Management**).

  3. Add the drive character from **Disk Management**.

3.11.4 Details tab



Drive Letter (Within 1023 bytes)

Specify the drive letter (A to Z) for the disk to be used.

Add

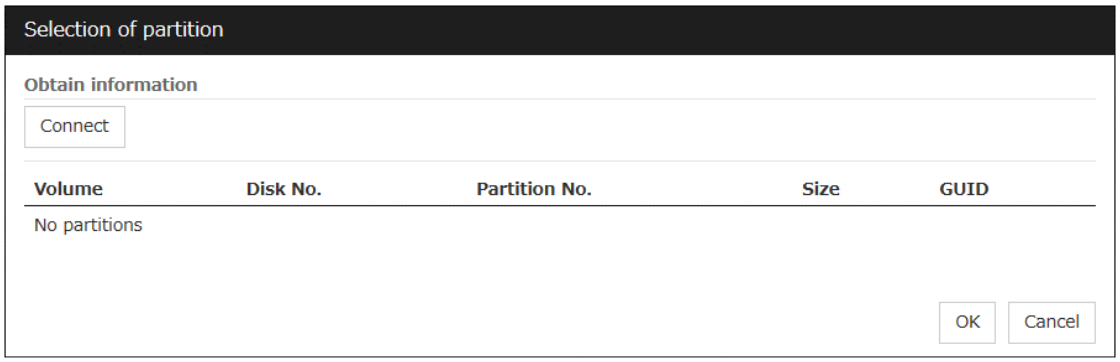
Use this button to add a server to **Servers that can run the group**. The list of added server partitions is displayed in the **Selection of Partition** dialog box.

Remove

Use this button to delete a server from **Servers that can run the group**.

Edit

The **Selection of Partition** dialog box of the selected server is displayed.



- **Selection of Partition**
  Select the partition to be used as switching partition from the list. GUID of the selected switching partition is displayed. GUID is an identifier used to uniquely identify partitions.
- **Connect**
  Connects to the server and obtain the list of partitions.

Important:

For a partition specified by disk resource, specify the partition on the shared disk that is connected to the filtering configured HBA.

Make sure not to specify a partition specified by disk resource to partition for disk heartbeat resource, or cluster partition or data partition for mirror disk resource. Data on the shared disk may be corrupted**.**

3.12 Understanding service resources

You can register services managed by EXPRESSCLUSTER and run when starting, stopping, failing over, or moving groups in EXPRESSCLUSTER. It is also possible to register your own services to service resources.

3.12.1 Dependencies of service resources

By default, this function depends on the following group resource types.

Group resource type
Floating IP resource
Virtual IP resource
Virtual computer name resource
Disk resource
Mirror disk resource
Hybrid disk resource
Registry synchronization resource
CIFS resource
AWS elastic ip resource
AWS virtual ip resource
AWS secondary ip resource
AWS DNS resource
Azure probe port resource
Azure DNS resource

3.12.2 Service resources

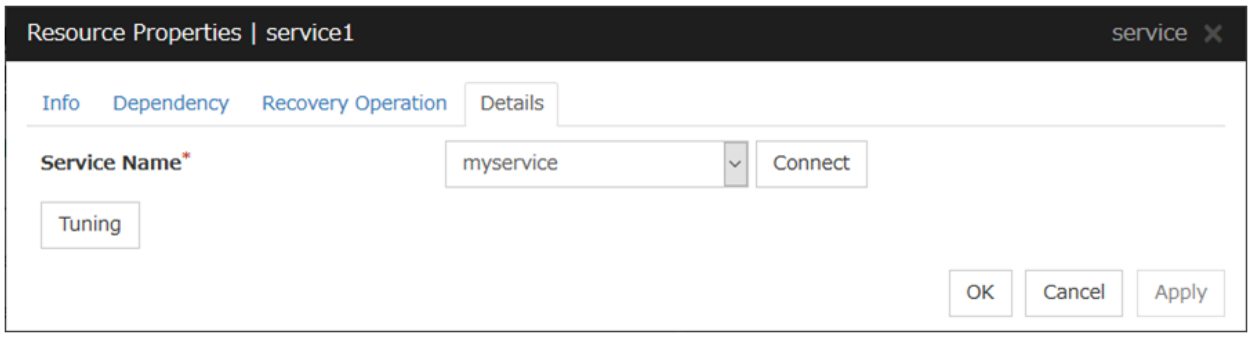
A service resource refers to a service managed by the OS service control manager.

3.12.3 Notes on service resources

- Service executed in service resource must be installed on all servers in failover policy.
- Generally, the service executed by the service resource is set to manual start. In case of the service which is executed by automatic start or the service which may be executed by other than the service resource, it is necessary to check on **Do not assume it as an error when the service is already started** which is described below in **Service** tab of **Service resource tuning properties** dialog. If this check box is off, activation fails when executing service start processing by the service resource to the service which has already been executed.
- If the **Service** tab of the **Service resource tuning properties** dialog box shows the checked **Do not assume it as an error when the service is already started** check box and the corresponding service has already been started at the service resource activation, the service is not stopped at the service resource deactivation.
- The service executed by the service resource is not controlled by applications other than EXPRESSCLUSTER. Therefore, it is recommended to set the recovery operation not to be performed by the service control manager.

  If a service is set to restart upon the recovery operation by the service control manager, an unexpected action might be performed due to duplication with the recovery operation by EXPRESSCLUSTER.

3.12.4 Details tab



Service Name (Within 1023 bytes)

Specify the service name or service display name used in the service resource.

Combo box options display the list of the service display names of the services collected from the server.

Connect

Collects the service list from all the servers and updates the service display name list to be displayed in the **Service Name** combo box.

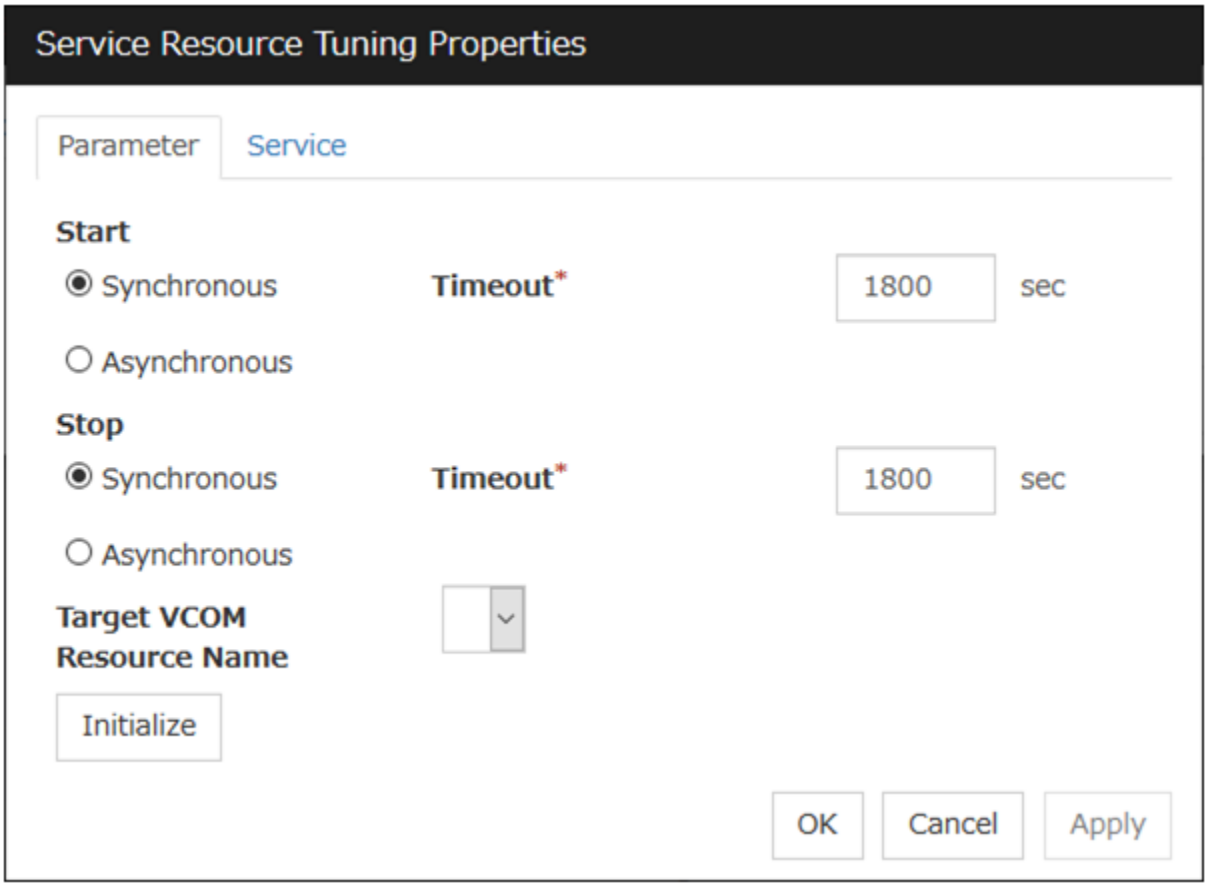
Tuning

Use this button to display the **Service Resource Tuning Properties** dialog box. You can make advanced settings for the service resource.

Service resource tuning properties

Parameter tab

The detailed setting for parameters is displayed.



Synchronous

When the service is started up, it waits for "Started". Typically, the status changes from "Stopping" to "Started" when the service is started.

When stopping the service, it waits for that the status of service becomes "Stopped". Typically, the status changes from "Stopping" to "Stopped" when the service is stopped.

Asynchronous

No synchronization is performed.

Timeout (1 to 9999)

Specify the timeout for the status of the service to become "Started" at the time starting the service. The timeout can be specified only when **Synchronous** is selected. If the status of the service does not change to "Started" within the timeout, it is determined as an error.

Specify the timeout for the stats of the service to become "Stopped" at the time stopping the service. The timeout can be specified only when **Synchronous** is selected. If the status of the service does not change to "Stopped" within the timeout, it is determined as an error.

Target VCOM Resource Name

Configure this to use a virtual computer name as a computer name used for the service resource. The virtual computer name and resource name that exist in a failover group which the service resource belongs to are listed.
When you specify this parameter, add the following registry and then start the service:

Key name

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service set by service resource>

Value

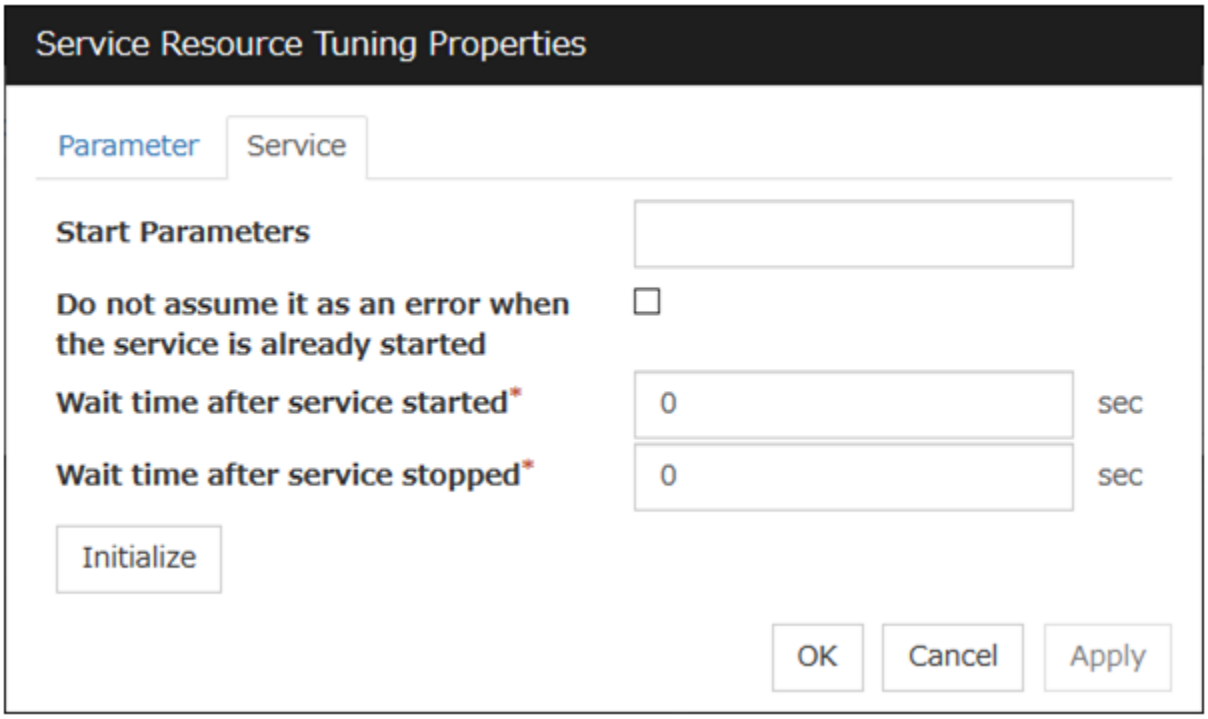
Name : Environment
Type : REG_MULTI_SZ
Data : COMPUTERNAME=<virtual computer name>
_CLUSTER_NETWORK_FQDN_=<virtual computer name>
_CLUSTER_NETWORK_HOSTNAME_=<virtual computer name>
_CLUSTER_NETWORK_NAME_=<virtual computer name>

Initialize

Click **Initialize** to reset the values of all items to their default values.

Service tab

The settings for the service are displayed.



Start Parameters (Within 1023 bytes)

Specify a parameter for the service. When there are multiple parameters, leave a space between parameters. For a parameter that includes a space, enclose the parameter by double quotation marks. Note that backslash \ cannot be used.

Example: "param 1" param2

Do not assume it as an error when the service is already started

- When the checkbox is selected:
  When the service is started, if the service is already started up, activation status is kept.
- When the checkbox is not selected:
  When the service is started, if the service is already started up, it is considered as activation error.

Wait time after service started (0 to 9999)

Specify the time to wait after the service is started.
The service resource activation will be completed after waiting for the specified time.

Wait time after service stopped (0 to 9999)

Specify the time to wait after the service is stopped.
The service resource deactivation will be completed after waiting for the specified time.

Initialize

Click **Initialize** to reset the values of all items to their default values.

3.13 Understanding virtual computer name resources

3.13.1 Dependencies of virtual computer name resources

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 secondary ip resource
Azure probe port resource

3.13.2 Virtual computer name resources

Only on Windows machines, client applications can be connected to a cluster server by using a virtual computer name. The servers can be connected to each other by using a virtual computer name. By using a virtual computer name, 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.

Virtual computer name resources use an old protocol. If you want only the name resolution of a floating IP address, do not use a virtual computer name resource, but instead register the host name and floating IP address in the DNS A record.

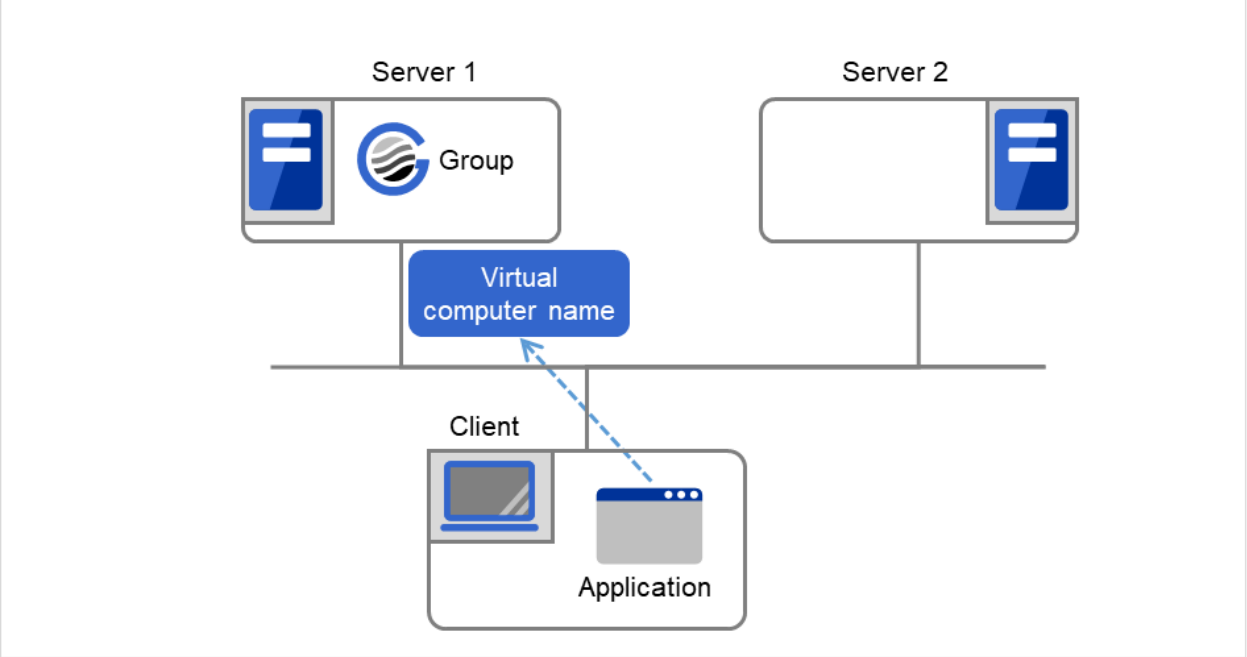


Fig. 3.97: Virtual computer name resource (1)

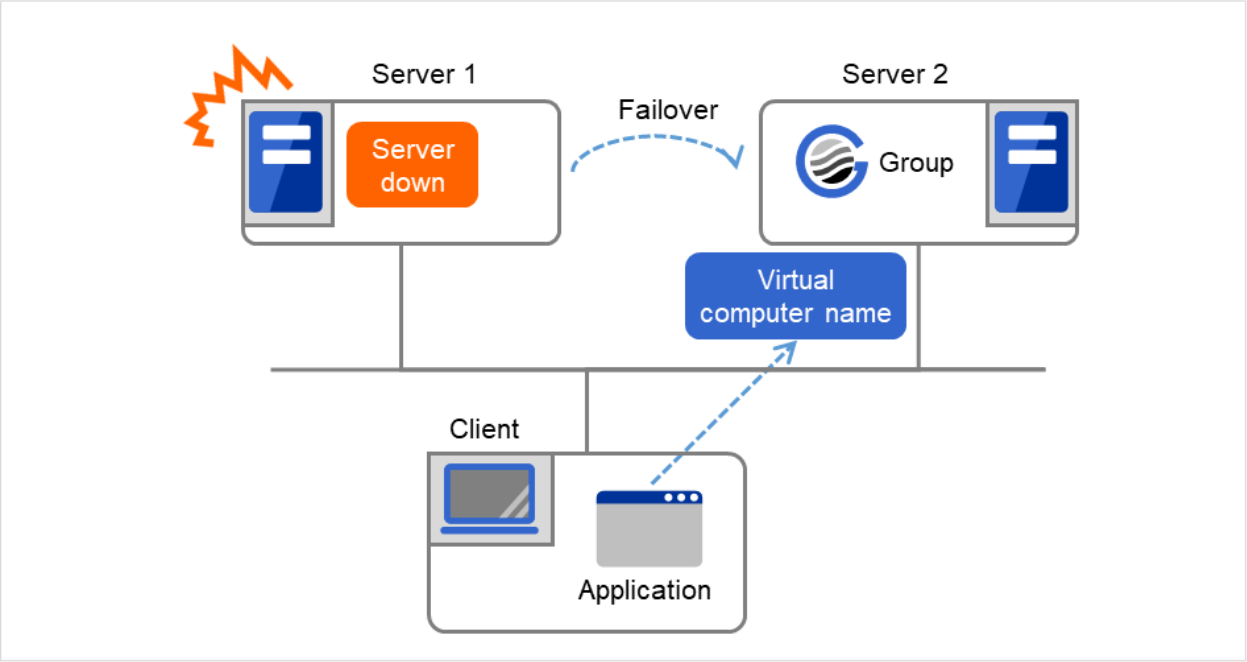


Fig. 3.98: Virtual computer name resource (2)

3.13.3 Determining virtual computer name

A computer name used as a virtual computer name should satisfy the following conditions:

- The name must be different from cluster server names.
- The name must be different from any computer names of machines connected to the same network segment.
- **The name must be within 15 characters.**
- The name must consist of only English lowercase letters (a-z), digits (0-9), and hyphens.

3.13.4 Linking virtual computer name and floating IP address

Once a virtual computer name is linked with a floating IP address, the combination of the virtual computer name and floating IP address can be written to the client's LMHOSTS file. To configure this, use the config mode of Cluster WebUI. Select **Virtual Computer Name Resource Properties**, and click **Details** tab, and then click **Target FIP Resource Name**. This configuration allows using the virtual computer name from a remote LAN.

If the virtual computer name and floating IP address are not linked, the virtual computer name cannot be used from a remote LAN by using LHMOSTS file. In this case, virtual computer name needs to be registered to DNS dynamically, or WINS needs to be set to use virtual computer names from a remote LAN. For information on how to configure WINS, refer to the next section "Configuring **WINS** server."

3.13.5 Configuring WINS server

To use a virtual computer name from a remote LAN without linking the virtual computer name to a floating IP address, set the WINS server as follows:

- When installing the WINS server to cluster servers
  1. Install the WINS server on all servers in a cluster. If you are prompted to reboot the servers after installation, click **No**.
  2. Configure the settings described from step 3 to 6 on all cluster servers.
  3. Open Control Panel and double-click Network Connections. Double-click Local Area Connection and open Local Area Connection Properties.
  4. Click Internet Protocol (TCP/IP) and click Properties.
  5. Click **Advanced** and click **WINS** tab.
  6. Add the IP addresses of public LAN in all servers in a cluster to the WINS address (The order of usage does not matter.)
  7. Shut down and reboot the cluster.
  8. Install the WINS server on the client on a remote LAN by following the same steps.
- When setting the WINS server on a server other than a cluster server
  1. Install WINS server on a server other than a cluster server.
  2. Open Control Panel and double-click Network Connections. Double-click Local Area Connection and open Local Area Connection Properties.
  3. Click Internet Protocol (TCP/IP) and click Properties.
  4. Click **Advanced** and click **WINS** tab.
  5. In **WINS addresses**, add the IP addresses of WINS server.
  6. Repeat the steps above for all servers in the cluster.
  7. Shut down and reboot the cluster.
  8. Install the WINS server to the client on a remote LAN by following the same steps.

3.13.6 Services available to the virtual computer name

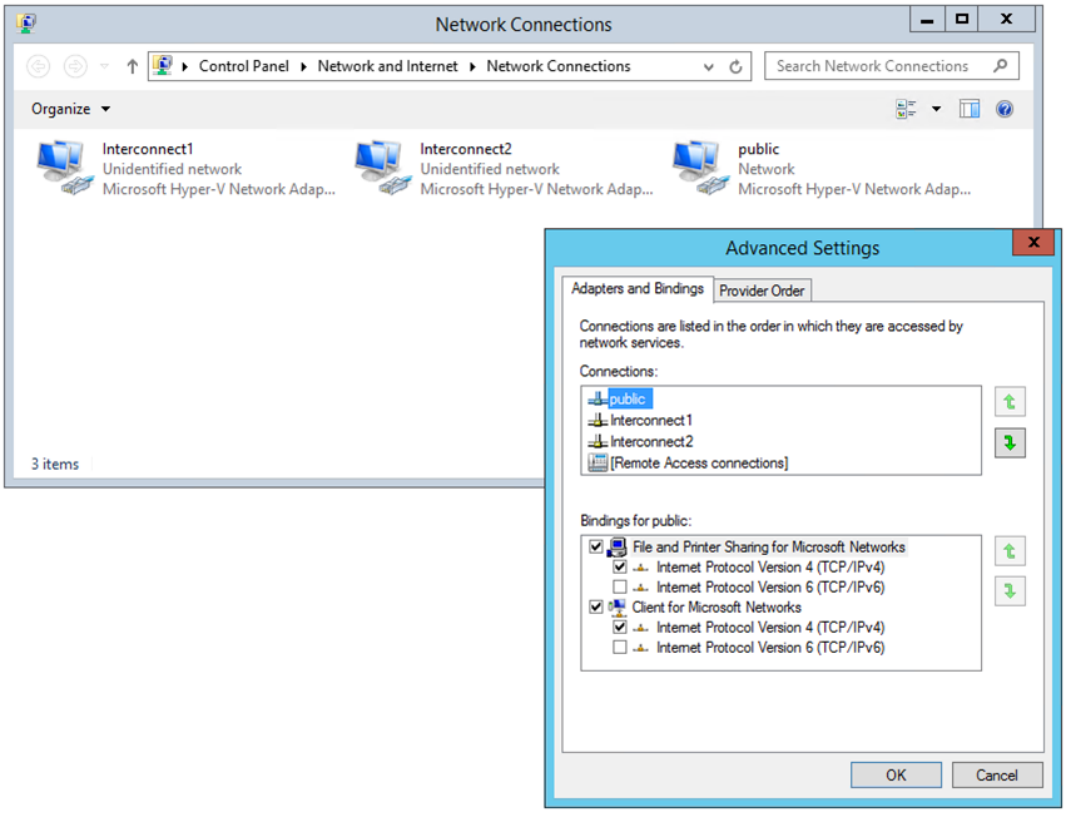
The following services are available to the virtual computer name:

Service	FIP linked	FIP n/at linked
TCP/IP name resolution (from computer name to IP address)	✓	n/a
Network drive connection	✓	✓
Network printer connection	✓	✓
Pipe with the name	✓	✓
RPC (pipe with the name)	✓	✓
RPC (TCP/IP)	✓	n/a

3.13.7 Notes on virtual computer name resources

- Create a virtual computer name control process (clpvcomp.exe) per virtual computer name resource to be activated. Make sure not to stop the process by mistake. An error of process disappearance can be detected by virtual computer name monitoring resources.
- The following services are not available to the virtual computer name:
  1. Mail slot
  2. RPC (NetBIOS)
- When the virtual computer name and floating IP address are not linked, the following needs to be considered:
  1. The following services cannot be used.
     - TCP/IP name resolution (from computer name to IP address)
     - RPC (TCP/IP)
  2. It may take a few minutes to reconnect to the cluster after failover due to a failure of the server.
  3. It may take a few minutes to display the virtual computer name in the network computer after the cluster is started.
  4. The virtual computer name cannot be written to LMHOSTS.
  5. When you have the settings to use a DNS server and the DNS server is associated with WINS, switching by failover cannot be done while cache information of the virtual computer name remaining on the DNS server. Configure the time to retain cache for WINS to approximately 1 second on the DNS server.
- If the virtual computer name and floating IP address are linked, the following need to be considered:
  1. The NetBEUI protocol cannot be used. To use the NetBEUI protocol, cancel the linkage.
  2. The virtual computer name is valid with the network address of the linked floating IP. To use the virtual computer name from a network address other than that of the linked floating IP, perform one of the following operations:
     - Register the name with DNS dynamically.
     - Enter a combination of the virtual computer name and floating IP address in LMHOSTS.
     - Configure the WINS server.
  3. **Multiple virtual computer names cannot be linked to the same floating IP.**
  4. **When different floating IPs exist on one or more public LAN, for using the same virtual computer name on each LAN, activation and deactivation processing needs to be executed sequentially by creating virtual computer name resource corresponding to each floating IP and setting dependency relation between these resources.**
- To register a virtual computer name with the WINS server on a remote network, configure the following settings in cluster servers:
  1. Open **Control Panel**, and click **Network and Sharing Center**. Then, open **Change Adapter Settings**.
  2. From the menu, click **Advanced**, and then click **Advanced Settings**. Select **Adapters and Bindings** tab.
  3. Change the order of the BindPath. The public LAN (the network adapter with which the WINS server address is registered) should be on the top.

Adapters and Bindings tab should look similar to the following:



- The communication by file sharing protocol (SMB/CIFS) using a virtual computer name owned by an activated group on the active server may fail due to an authentication error.
  (Example 1)
  The Explorer is started in the server where the group is active and the following address is entered in the address bar. However it results in causing an authentication error and cannot open the shared folder.

  <Virtual computer name>/shared name

  (Example 2)

  In a server where the group was active, started the registry editor and specified the virtual computer name in "Connect Network Registry," but failed due to authentication error.

  <Troubleshooting>

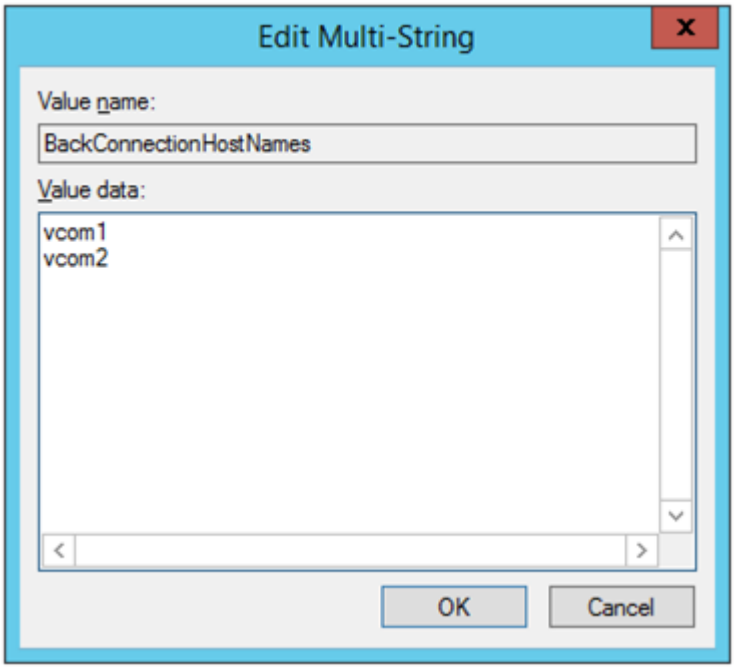
  1. Verify that the all servers are properly working from the Cluster WebUI.
  2. Execute Steps 3 to 7 below in each server in the cluster.
  3. From the **Start** menu, select **Run,** and run regedit.exe and add the following registry value:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Name (Type):
DisableStrictNameChecking (DWORD type)
Value:
0x1
```

  4. If the following value exists in the following key, delete it:

```
Key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0
Name (Type):
BackConnectionHostNames (DWORD type)
```

5. Create a new multi-line string value for the same the name in Step 4 (BackConnectionHostNames), and set a virtual computer name.
   (Example) when there are two virtual computer names: vcom1 and vcom2



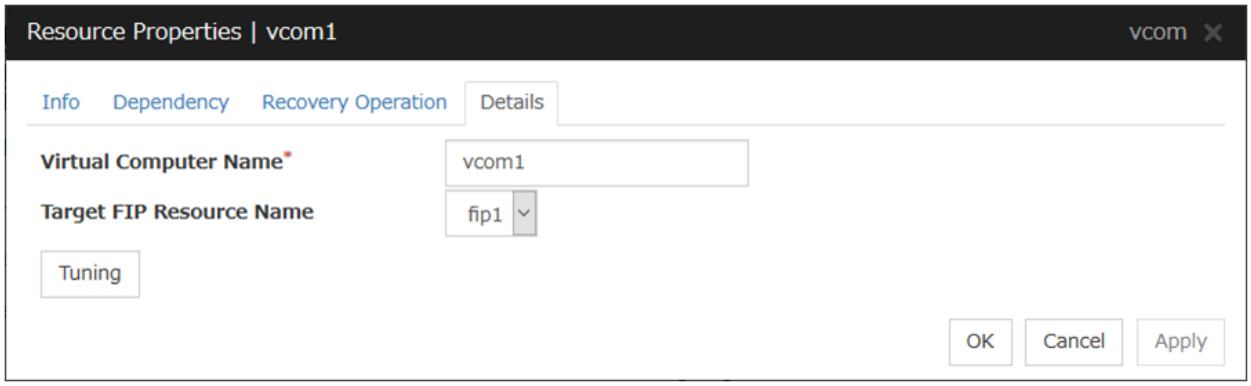
6. Close the registry editor.
7. (applicable only when the virtual computer name and the floating IP address are linked)
   In the system drive: \Windows\system32\drivers\etc\hosts, add an entry of the virtual computer name (not FQDN name but computer name only) and the linked floating IP address. When there are multiple virtual computer names linked with floating IP address, add entries for all of them.

   (Example) when the virtual computer name is "vcom1" and the linked floating IP address is "10.1.1.11":
   Add the following to the hosts file: 10.1.1.11 vcom1
8. Execute Steps 3 to 7 above in all servers. Then shut down the cluster and reboot all servers.

- Notes on registering a virtual computer name with DNS dynamically
  1. Cluster server must be assigned in the domain.
  2. DNS must be configured for the public LAN. EXPRESSCLUSTER registers virtual computer name specified by public LAN with DNS.
  3. DNS registration is performed when virtual computer name resource is activated. Failure of registration will not be recognized as an error.
  4. A virtual computer name is deleted from DNS when virtual computer name resource is deactivated. Failure of deletion will not be recognized as an error.

- **Since virtual computer name resource cannot be allocated to NIC when the LAN cable is not connected, the activation of the resource may fail.**
- **When Server service of OS is stopped, virtual computer name resource cannot be activated. If you want to use virtual computer name resource, do not disable/stop Server service.**
- If **Secure only** is specified for DNS Dynamic Updates, the **write** and the **delete subtree** permissions must be applied to computer objects in the zone to be updated by a virtual computer name resource. Apply the permissions to **This object and all descendant objects**. For how to apply the permissions, refer to the setting method for the DNS server. The settings above are not required if **Nonsecure and secure** is specified for DNS Dynamic Updates.

3.13.8 Details tab



Virtual Computer Name (Within 15 bytes)

Specify the virtual computer name.

Target FIP Resource Name

Select the floating IP resource name to be linked to the virtual computer name.

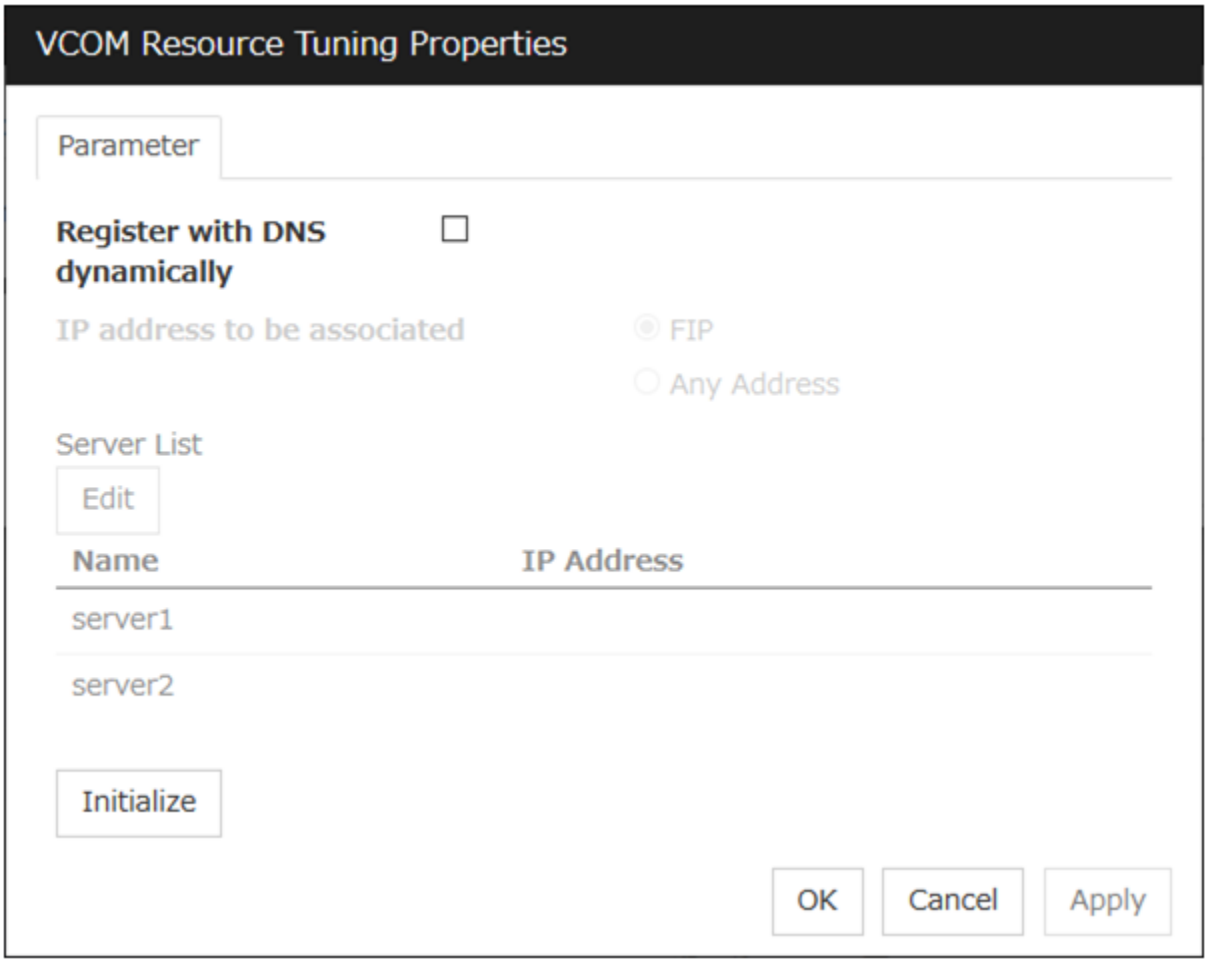
Tuning

Display the **VCOM Resource Tuning Properties** dialog box to configure the details of virtual computer name resource.

VCOM Tuning Properties

Parameter tab

Display the details of setting the parameter.



Register with DNS dynamically

Specify whether or not to register with DNS dynamically during activation of resource.

IP address to be associated

Select one of the followings as IP address for registration with DNS dynamically to associate with virtual computer name.

- FIP
  Associates the floating IP address in selected in the target FIP resources name.
- Any Address
  Associates any IP address you want on a server basis.

Edit

When **Any Address** is selected for IP address to be associated, select your target server in **Servers**. Click **Edit** to specify an IP address on a server basis..

Initialize

Click this button to configure default values for all options.

3.14 Understanding dynamic DNS resources

3.14.1 Dependency of dynamic DNS resources

By default, dynamic DNS resources depend on the following types of group resources.

Group resource type
Virtual IP resource
Floating IP resource
AWS elastic ip resource
AWS virtual ip resource
AWS secondary ip resource
Azure probe port resource

3.14.2 Dynamic DNS resources

- A dynamic DNS resource registers a virtual host name and the IP address of an activated server with the dynamic DNS server (hereafter, DDNS server). A client application can use a virtual host name to access the cluster server. Use of virtual host names allows clients to transparently switch connection from one server to another when a group is "failed over" or "moved".

The following figure shows the Dynamic DNS server (DDNS server), Servers 1 and 2, and a client. On the DDNS server, Server 1 registers the virtual host name and the IP address.

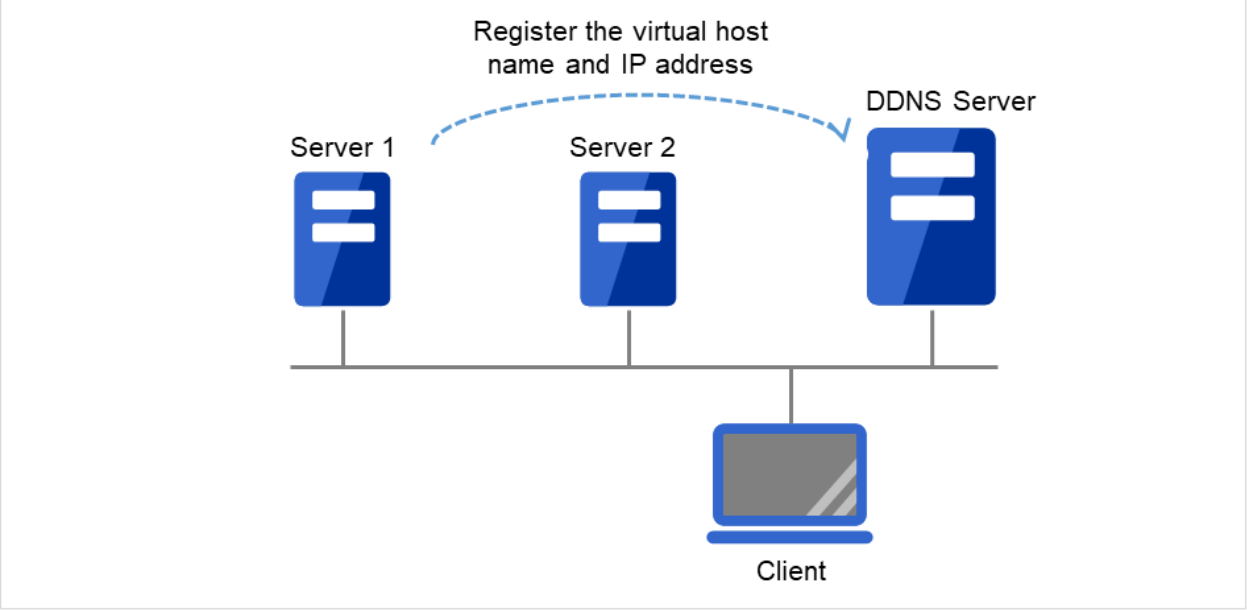


Fig. 3.99: Configuration with the DDNS server (1)

The client queries the DDNS server about the IP address (corresponding to the virtual host name) to be accessed. The DDNS server returns the IP address (corresponding to the virtual host name) of Server 1 to the client. The client then accesses the IP address of the virtual host name.

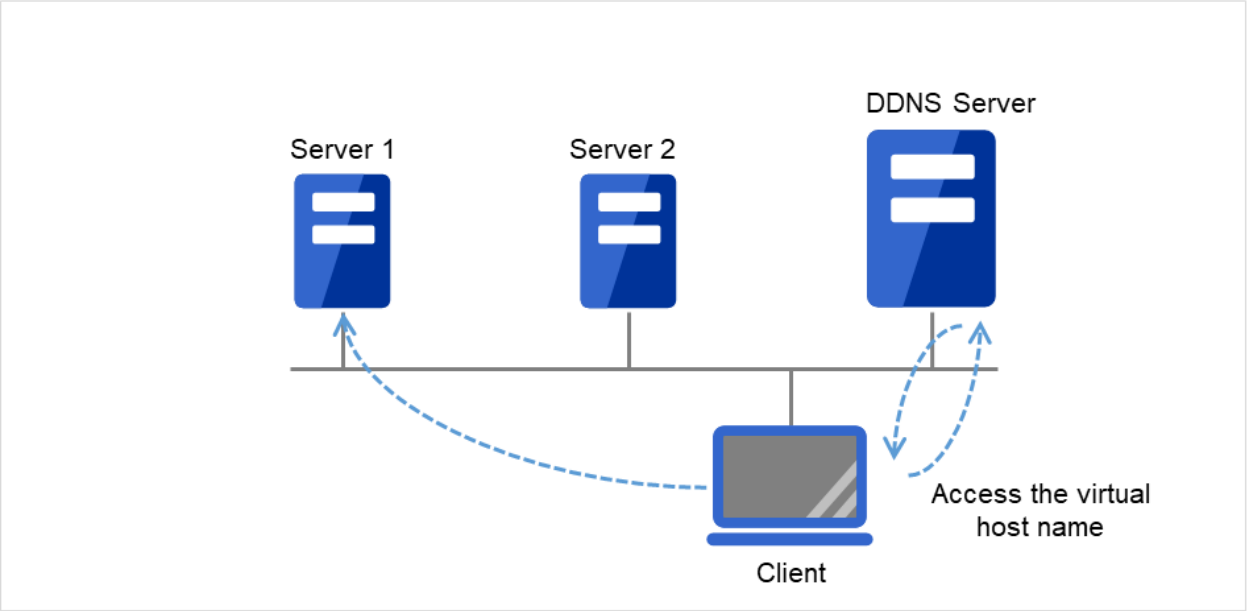


Fig. 3.100: Configuration with the DDNS server (2)

Server 1 crashes, and a failover to Server 2 occurs.

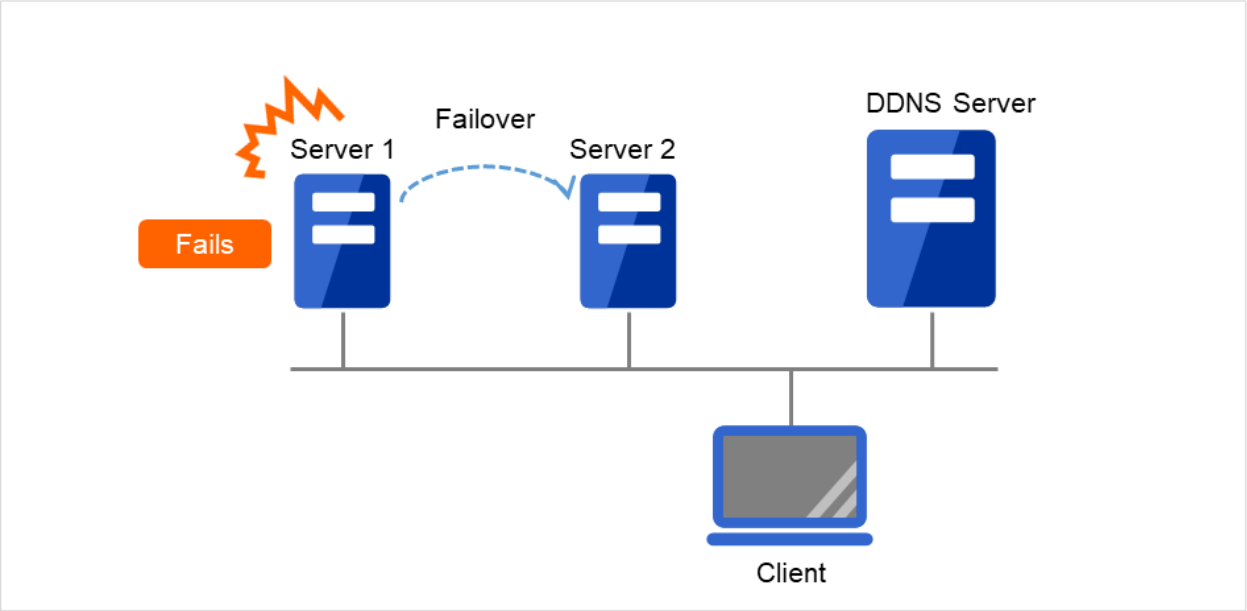


Fig. 3.101: Configuration with the DDNS server (3)

On the DDNS server, Server 2 registers the virtual host name and the IP address.

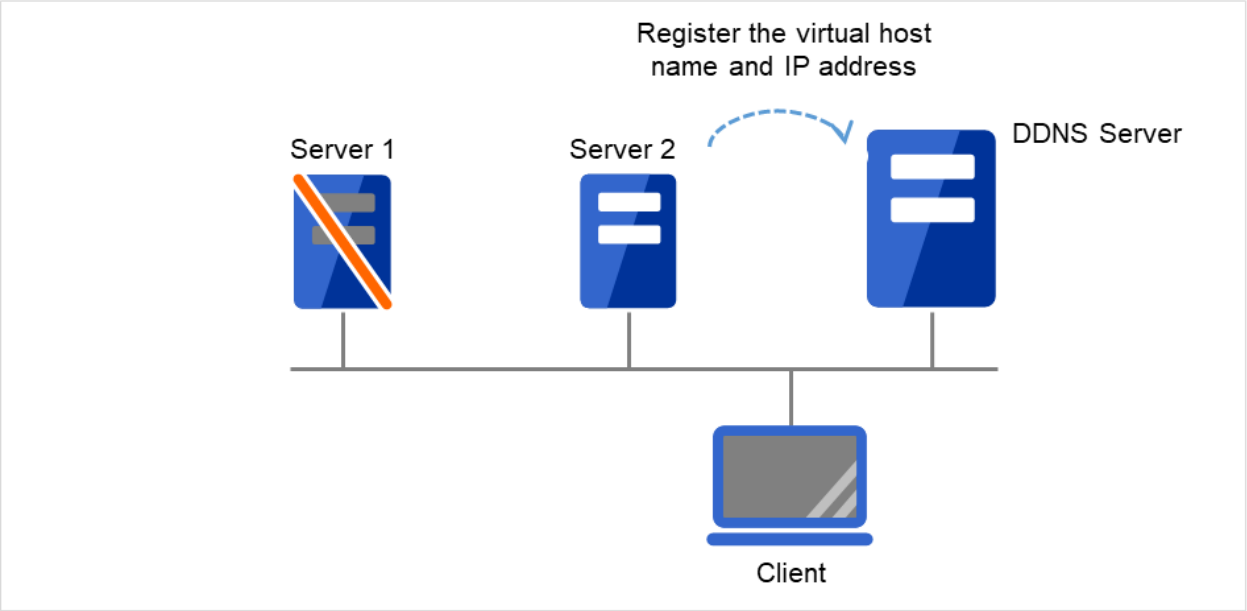


Fig. 3.102: Configuration with the DDNS server (4)

The client queries the DDNS server about the IP address (corresponding to the virtual host name) to be accessed. The DDNS server returns the IP address (corresponding to the virtual host name) of Server 2 to the client. The client then accesses the IP address of the virtual host name.

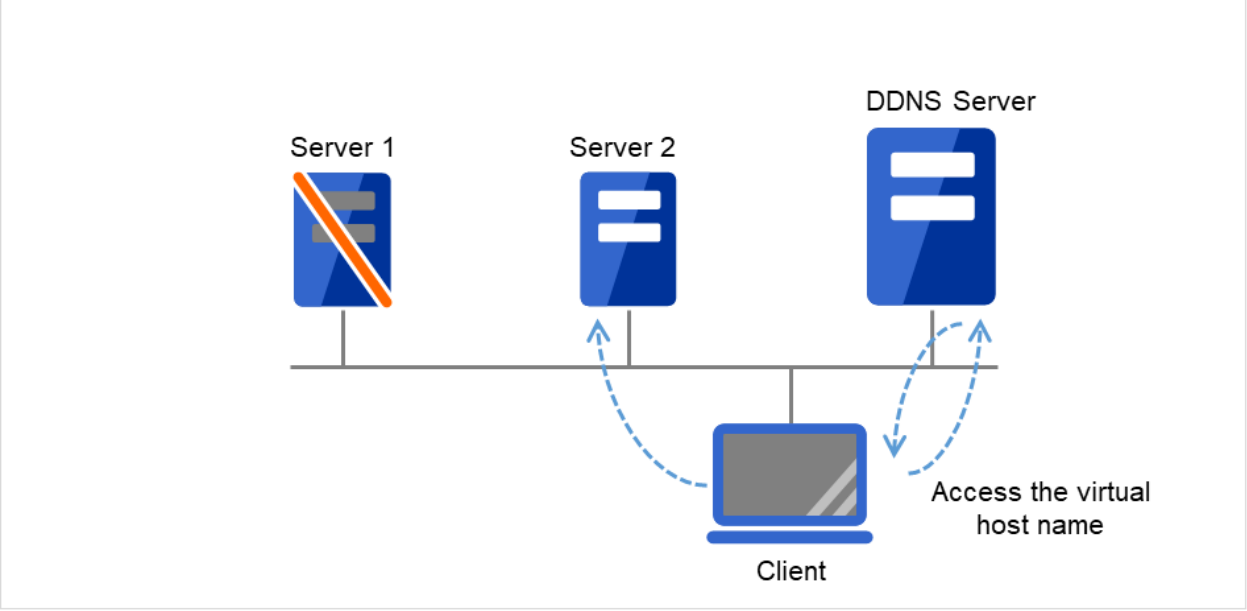


Fig. 3.103: Configuration with the DDNS server (5)

3.14.3 Preparation for use of dynamic DNS resources

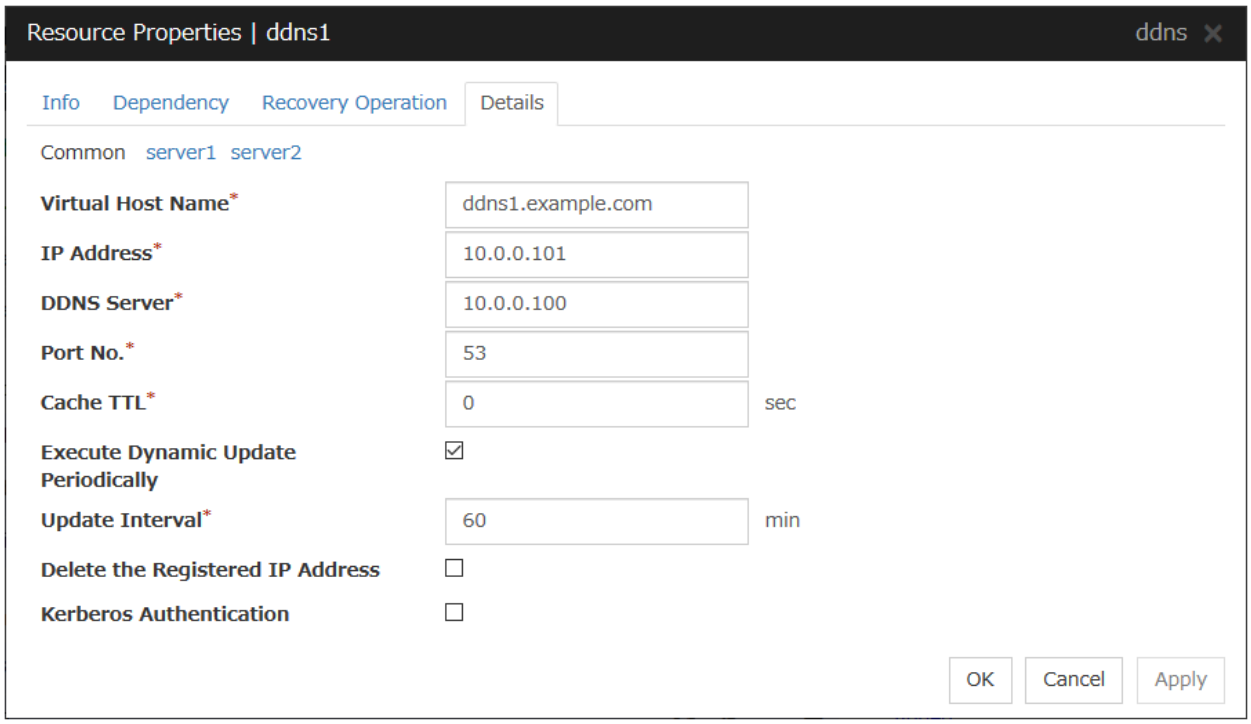
- To use dynamic DNS resources, you need to establish a DDNS server in advance. DDNS servers support only active directories.
- If using the Kerberos authentication function, you need to make the following setting for the Active Directory domain to be updated by the dynamic DNS resource.
  - Please give the following permissions to each cluster server.
    - Create All Child Objects
    - Delete All Child Objects

    Permissions will be applied to, please choose **This object and all child objects**.
- If **Secure only** is specified for DNS Dynamic Updates, the **write** and the **delete subtree** permissions must be applied to computer objects in the Active Directory and DNS domains to be updated by a dynamic DNS resource. Apply the **write** permissions to **This object and all child objects** (**This object and all descendant objects** for Windows Vista or later and Windows Server 2008 or later). For how to apply the write permissions, refer to the setting method for the DNS server.

3.14.4 Notes on dynamic DNS resources

- If **Execute Dynamic Update Periodically** is enabled, a dynamic DNS monitor resource periodically registers a virtual host name to the DDNS server.
- Create a DDNS control process (clpddnsp.exe) per dynamic DNS resource to be activated. Make sure not to stop the process by mistake. An error of process disappearance can be detected by dynamic DNS monitor resources.
- When the IP addresses of servers exist in different segments, FIP addresses cannot be specified as the IP addresses of dynamic DNS resources.
- To register the IP addresses of servers with the DDNS server, make the setting of each IP address separately for each server. Enter the IP address of any server in the **IP Address** box on the **Common** tab and then specify the IP addresses of other servers individually on each server tab.
- Regarding the settings for each server, if the same virtual host name already exists at activation, the duplicate virtual host name is temporarily deleted from the primary DNS server and the relevant virtual host name and IP address of the activated server are registered. The setting of the **Delete the Registered IP Address** option, which is a setting applied at deactivation, does not affect this behavior.
- In client access using a virtual host name, if a group having dynamic DNS resources is failed over, reconnection (e.g. restart of the browser) may be required.
- Behavior in Cluster WebUI connection using a virtual host name
  - When the IP address of each server is separately specified for dynamic DNS resources
    In client access using a virtual host name via Cluster WebUI connection, if a group having dynamic DNS resources is failed over, the Cluster WebUI connection will not be automatically switched. You need to restart the browser and to establish Cluster WebUI connection again.
  - When FIP addresses are specified for dynamic DNS resources
    In client access using a virtual host name via Cluster WebUI connection, if a group having dynamic DNS resources is failed over, the Cluster WebUI connection will be automatically switched.

3.14.5 Details tab



Virtual Host Name (Within 253 bytes)

Specify the virtual host name to be registered in the DDNS service.

IP Address (Within 79 bytes)

Specify the IP address corresponding to the virtual host name.

To use an FIP resource in parallel, specify the IP address of the FIP resource in the [Source IP Address] tab. To use the IP addresses of servers, specify each IP address in the tab of each server.

DDNS Server (Within 255 bytes)

Specify the IP address of the DDNS server. When specifying secondary DNS servers, use a comma (,) for the separator. First, specify the primary DNS server, and then specify secondary DNS servers.
Examples:
To specify only the primary DNS server: 192.168.10.180
To specify two secondary DNS servers:
192.168.10.180,192.168.10.181,192.168.10.182

Port No. (1 to 65535)

Specify the port number of the DDNS server. Its default value is 53.

Cache TTL (0 to 2147483647)

Specify the time to live (TTL) of the cache. Its default value is 0 seconds.

Execute Dynamic Update Periodically

- When the check box is selected (default):
  The virtual host name and the IP address of the active server are periodically registered to the DDNS server.
- When the check box is not selected:

The virtual host name and the IP address of the active server are not periodically registered to the DDNS server.

Update Interval (1 to 9999)

Specify the interval for periodic registration of the virtual host name and the IP address of the activated server with the DDNS server. The default value is 60 minutes.

Be sure to specify a time shorter than the update interval of the DDNS server.

Delete the Registered IP Address

- When the check box is selected (default):
  When the dynamic DNS resource is deactivated, the virtual host names and the IP addresses of the active servers that were registered to the DNS server are deleted.
- When the check box is not selected:
  When the dynamic DNS resource is deactivated, the virtual host names and the IP addresses of the active servers that were registered to the DNS server are not deleted. In this case, a client may be able to access one of these undeleted virtual host names.

Kerberos Authentication

Specify whether to enable Kerberos authentication in Active Directory. No password need to be specified because a password is automatically generated when a dynamic DNS resource registers a virtual host name in the Active Directory domain. The default is cleared.

- When the check box is selected:
  Select the check box to enable Kerberos authentication in Active Directory.
- When the check box is not selected (default):
  Clear the check box to disable Kerberos authentication in Active Directory.

3.15 Understanding virtual IP resources

3.15.1 Dependencies of virtual IP resources

By default, this function does not depend on any group resource type.

3.15.2 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.

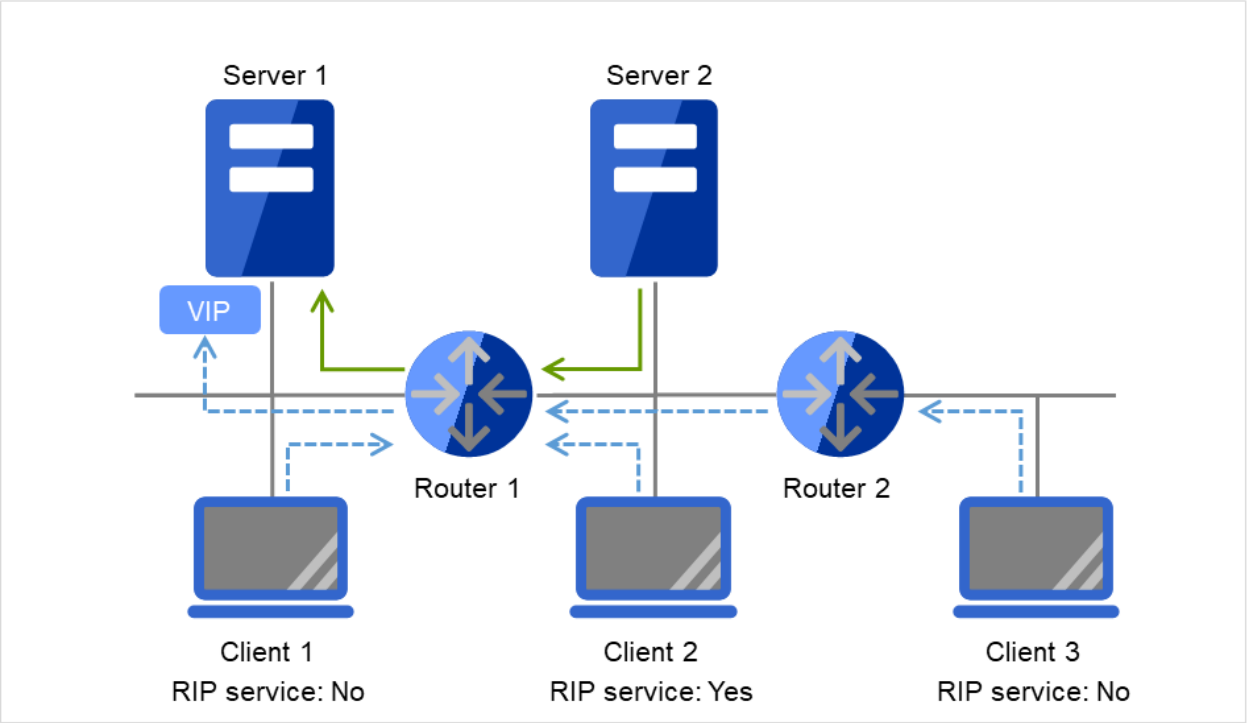


Fig. 3.104: Configuration with a virtual IP address (1)

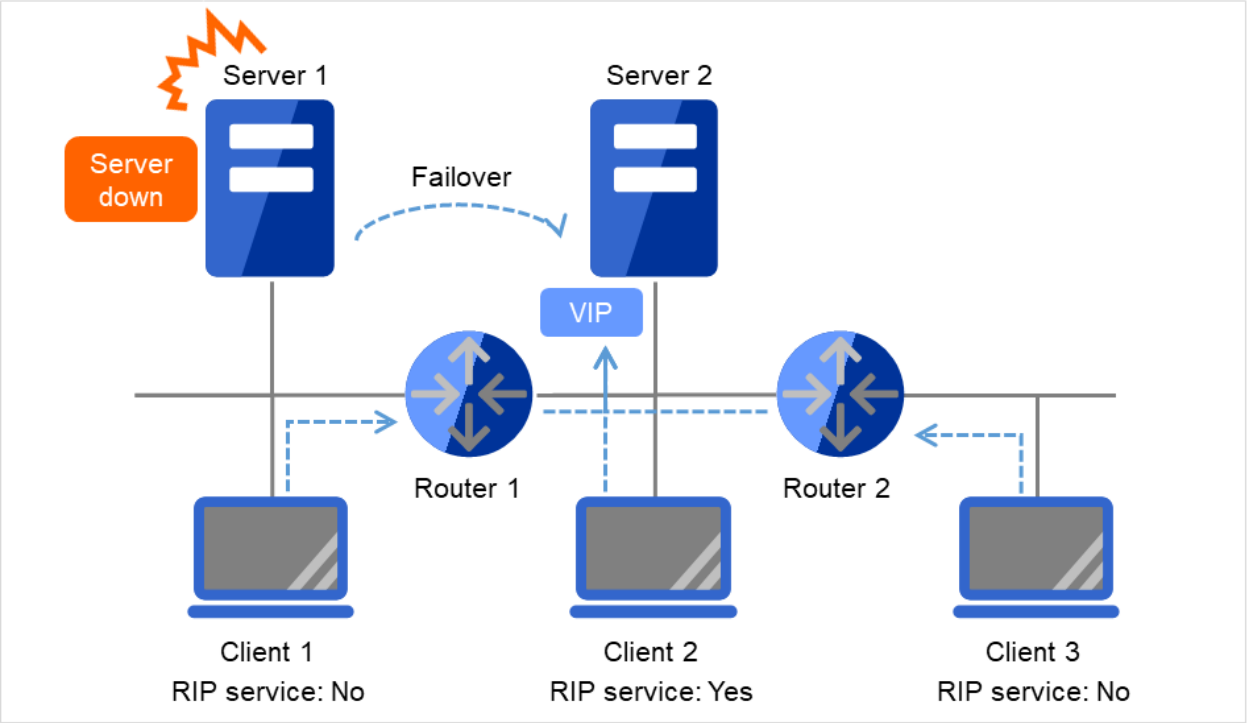


Fig. 3.105: Configuration with a virtual IP address (2)

- Note on setting servers (1)
  Each cluster server on the same LAN requires being able to change the path by receiving RIP packets, or to resolve path information on the virtual IP address by accessing a router.
- Note on setting servers (2)
  Each cluster server in a separate segment requires being able to resolve path information on the virtual IP address by accessing a router.
- Note on setting virtual IP resources (1)
  Specify an IP address outside the LAN to which the cluster servers belong, and free from a collision with existing IP addresses.
- Note on setting routers (1)
  Each router requires being able to perform dynamic routing by interpreting RIP packets, or to resolve path information on the virtual IP address as static path information.
- Note on setting virtual IP resources (2)
  Be sure to specify a sender's IP address for each of the servers in order for RIP packets to be correctly sent.
- Note on setting routers (2)
  Set the flush timer of each router at a value within the heartbeat timeout value.
- Note on setting clients (1)
  Each client on the same LAN requires being able to change the path by receiving RIP packets, or to resolve path information on the virtual IP address by accessing a router.
- Note on setting clients (2)
  Each client in a separate segment requires being able to resolve path information on the virtual IP address by accessing a router.

3.15.3 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.
- 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.

3.15.4 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.

3.15.5 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 that 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 belong to a different LAN that 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 belong to the same LAN that 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 the 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.

3.15.6 Notes on virtual IP resources

Virtual IP addresses do not support NetBIOS protocol.

- Even if you map a virtual IP address to a host name using LMHOSTS, it cannot be used for accessing and user authentication for Windows browsing, networks, and printer resources.
- Use a virtual computer name to automatically switch the connection destination with the NetBIOS protocol.

The following rule applies to virtual IP addresses.

- The number of a virtual IP resource to be registered on one cluster system is up to 64.
- To use a virtual IP resource, the names of a cluster, server and group need to be set according to the naming rules of Ver8.0 or earlier.

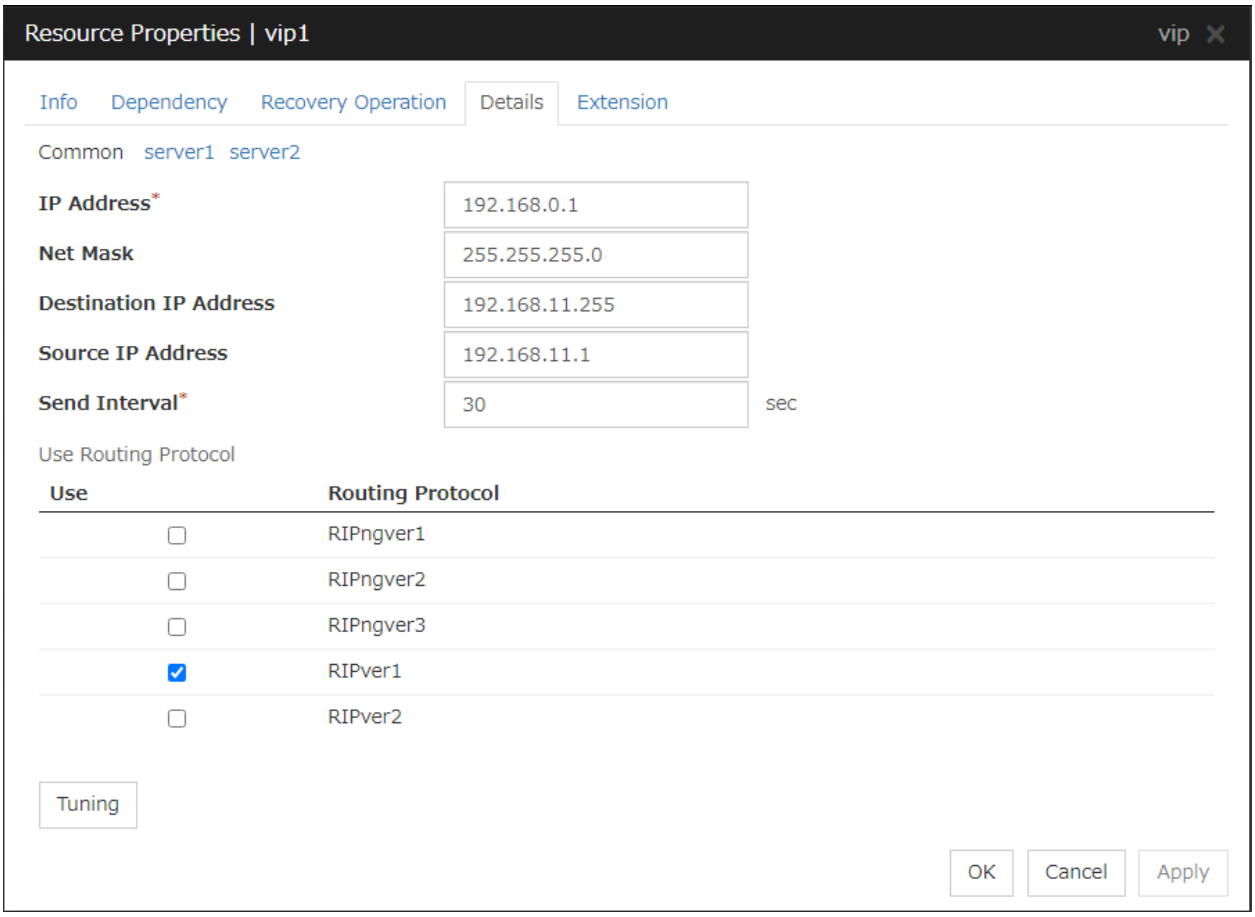
Adjust the value of the flush timer of the router within the value for heartbeat timeout. For the heartbeat timeout, see "*Timeout tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

It is necessary to add the Routing and Remote Access service to each cluster server to enable the LAN routing. This is not required when the interconnect LAN with the highest priority is common to public LAN.

When an IPv6 address is used as a virtual IP address, it is necessary to specify public LAN as the interconnect with the highest priority.

If the routing protocol is set to "RIPver2," the subnet mask for transmitted RIP packets is "255.255.255.255."

3.15.7 Details tab



IP Address (Within 45 bytes)

Enter the virtual IP address to use.

Net Mask (Within 45 bytes)

Specify the net mask of the virtual IP address to use. It is not necessary to specify it when the IPv6 address is specified as a virtual IP address.

Destination IP Address (Within 45 bytes)

Enter the destination IP address of RIP packets. The broadcast address of the LAN where the cluster server belongs is specified for IPv4 and the IPv6 address of the router of the LAN where the cluster server belongs is specified for IPv6.

Source IP Address (Within 45 bytes)

Enter the IP address to bind for sending RIP packets. Specify the actual IP address activated on NIC which activates the virtual IP address.

When using an IPv6 address, specify a link local address as the source IP address.

Note: The source IP address should be set on a server basis, 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, described the Source IP Address of any of the server, the other server, please to perform the individual settings.

Send Interval (1 to 30)

Specify the send interval of RIP packets.

Use Routing Protocol

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 one or more routing protocol.

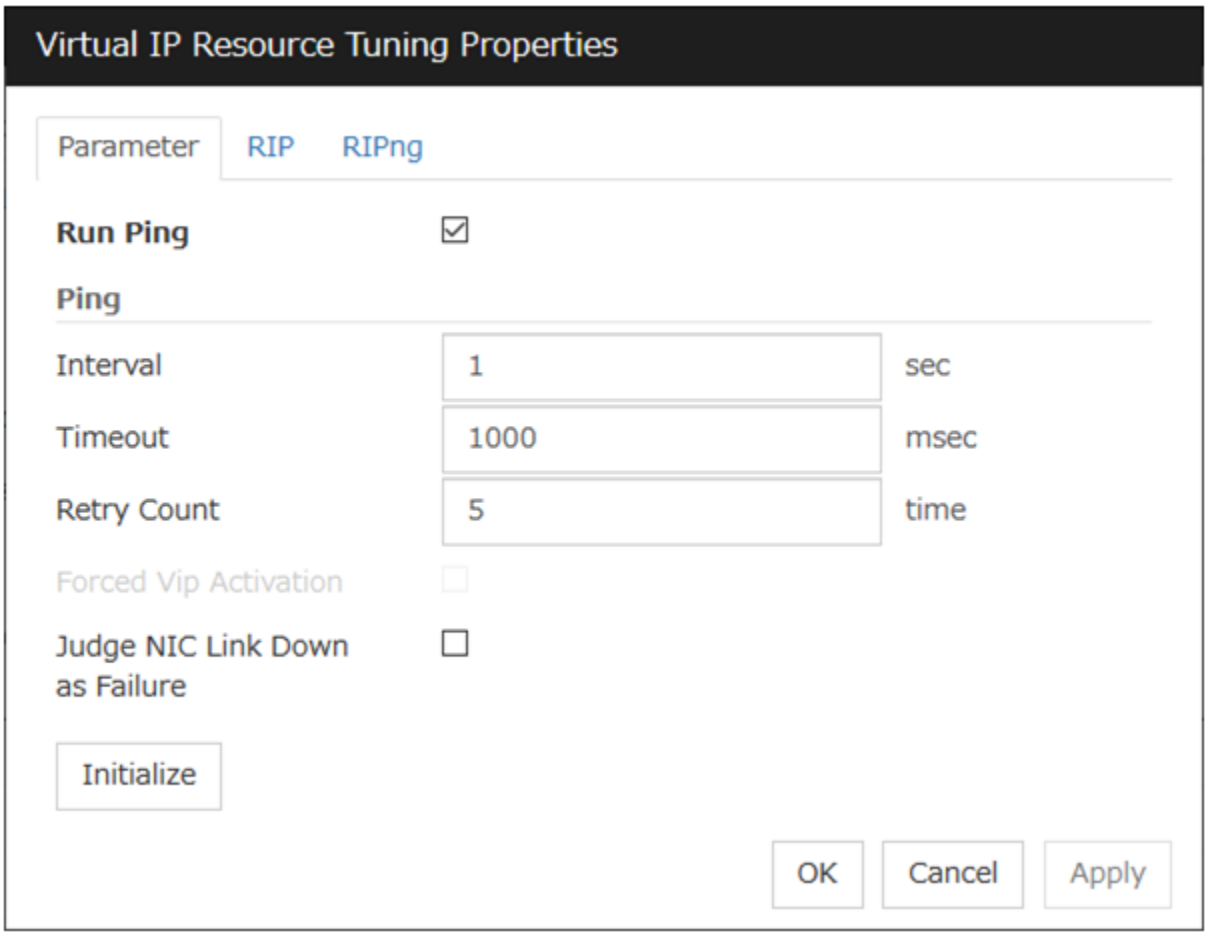
Tuning

Use this button to display the **Virtual IP Resource Tuning Properties** dialog box. You can make advanced settings for the virtual IP resource.

Virtual IP Resource Tuning Properties

Parameter tab

Detailed setting for parameter is displayed.



Run ping

Use this button to configure whether or not to check if there is any overlapped IP address by the ping command before activating the virtual IP resource.

- When the checkbox is selected:

Check by using the ping command.

- When the checkbox is not selected:
  Do not check by using the ping command.

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 (1 to 999999)
  Specify the timeout for the ping command in milliseconds.
- 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 checkbox is selected:
    Forcefully activate the virtual IP address.
  - When the checkbox is not selected:
    Do not forcefully activate the virtual IP address.

Judge NIC Link Down as Failure

Specify whether to check for an NIC Link Down before the floating IP resource is activated.

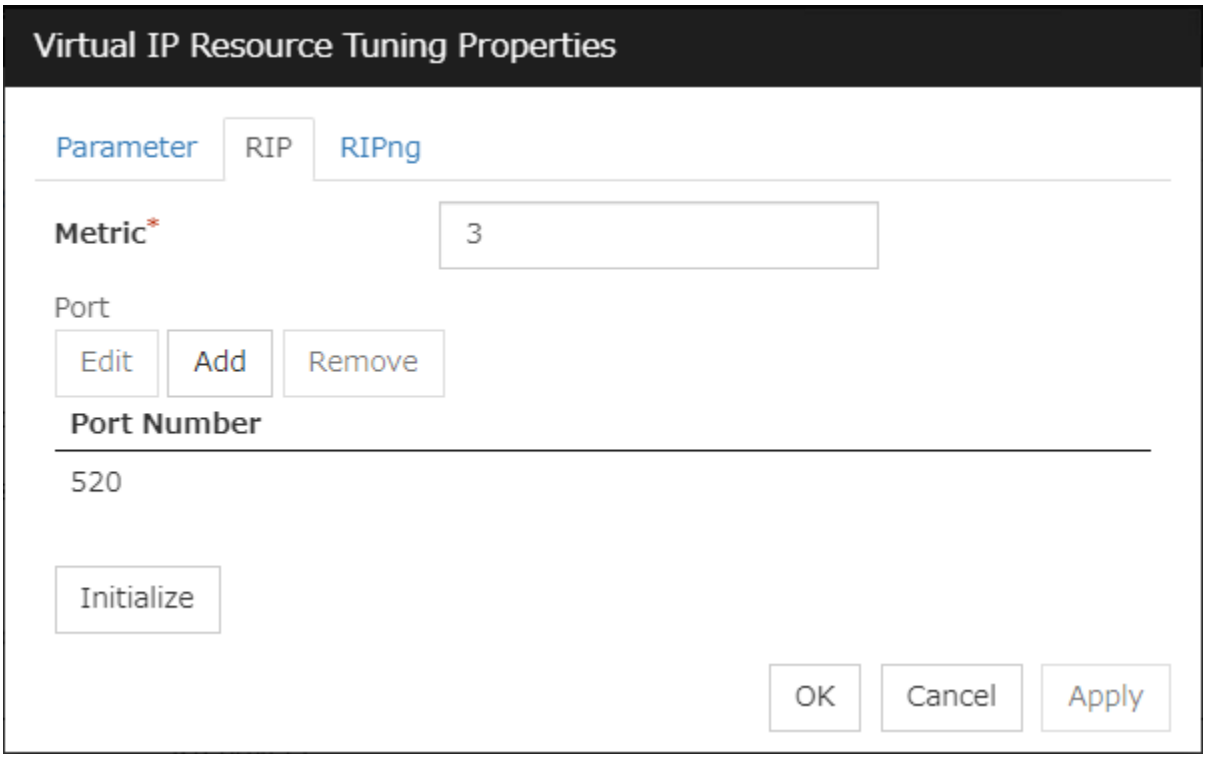
- When the checkbox is selected:
  In the case of an NIC Link Down, the floating IP resource is not activated.
- When the checkbox is not selected:
  Even in the case of an NIC Link Down, the floating IP resource is activated. This operation is the same as before.

Initialize

Clicking **Initialize** sets the values of all the items to the defaults.

RIP tab

Detailed settings on RIP of virtual IP resource are displayed.



Metric (1 to 15)

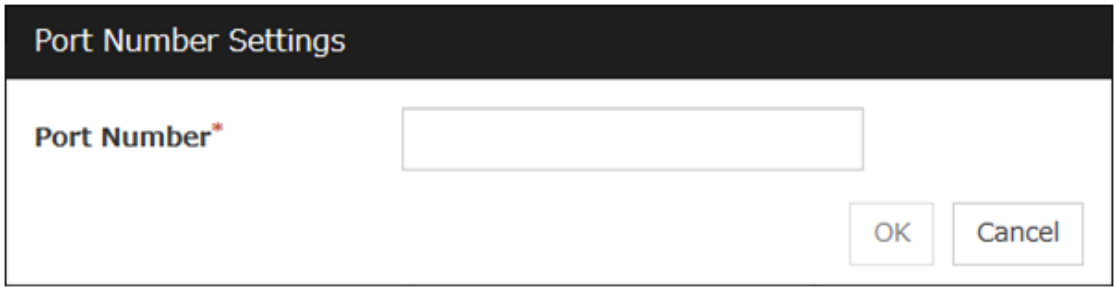
Enter a metric value of RIP. A metric is a hop count to reach the destination address.

Port

On **Port Number**, a list of communication ports used for sending RIP is displayed.

Add

Add a port number used for sending RIP. Click this button to display the dialog box to enter a port number.



Port Number

Enter a port number to be used for sending RIP, and click **OK**.

Remove

Click **Remove** to delete the selected port on the **Port Number**.

Edit

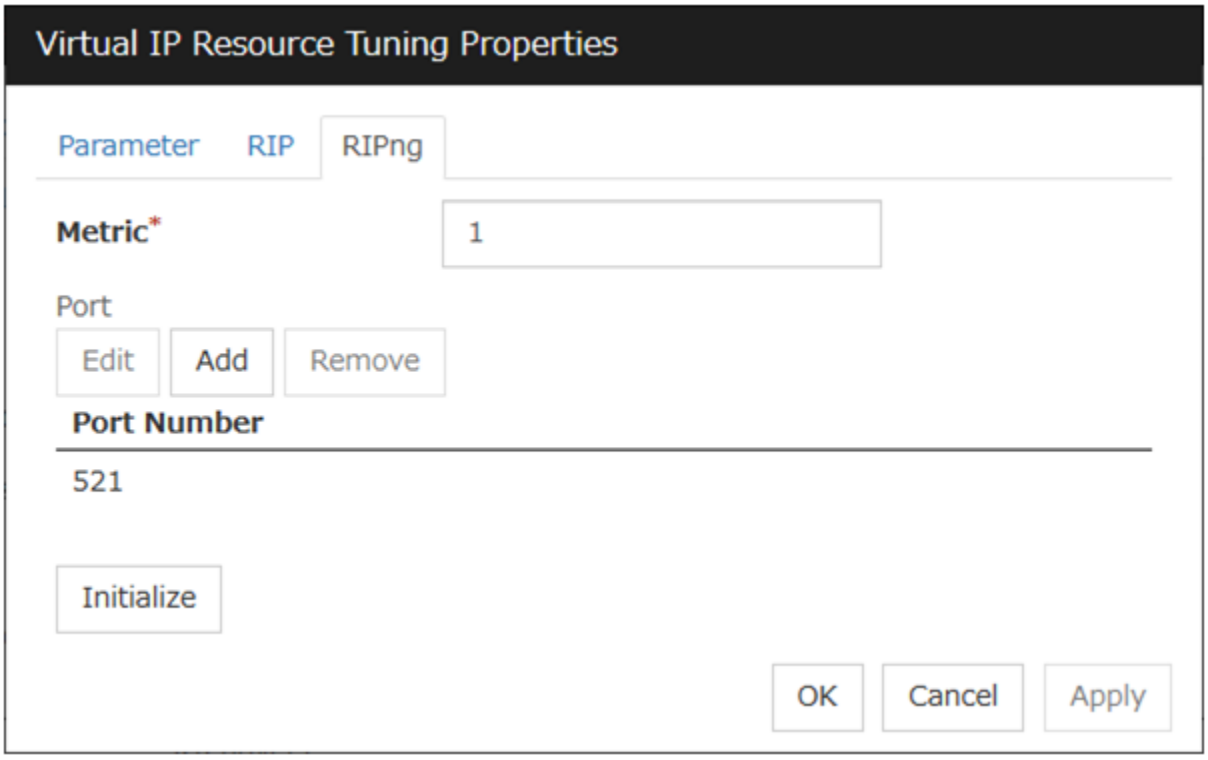
A dialog box to enter a port number is displayed. The port selected in the **Port Number** is displayed. Edit it and click **OK**.

Initialize

Clicking **Initialize** sets the values of all the items to the defaults.

RIPng tab

Detailed settings of RIPng of virtual IP resource are displayed.



Metric (1 to 15)

Enter a metric value of RIPng. A metric is a hop count of RIPng to reach the destination address.

Port

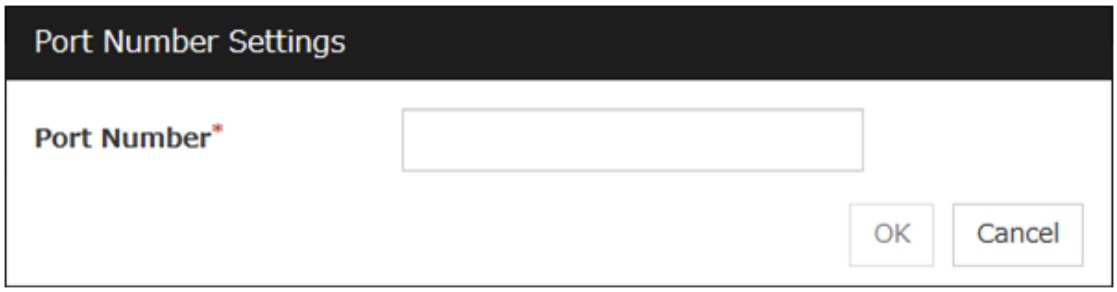
On **Port Number**, a list of ports used for sending RIPng is displayed.

Initialize

Clicking **Initialize** sets the values of all the items to the defaults.

Add

Add a port number used for sending RIPng. Click this button to display the dialog box to enter a port number.



Port Number

Enter a port number to be used for sending RIPng, and click **OK**.

Remove

Click **Remove** to delete the selected port on the **Port Number**.

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**

3.16 Understanding CIFS resources

3.16.1 Dependencies of CIFS resources

By default, CIFS resources depend on the following group resources type:

Group resource type
Disk resource
Mirror disk resource
Hybrid disk resource

3.16.2 CIFS resources

CIFS resources control publicizing and removal of shared folders. By using CIFS resources, the folders on shared disks and mirror disks are publicized as a shared file.

There are two ways of publicizing as follows:

Specify shared configuration individually

Specify shared folder configuration in advance in configuration items of CIFS resources, and then publicize shared folder with the configuration specified at resource activation. You need to create CIFS resource per shared folder to be publicized.

Auto-save shared configuration of drive

When a specified folder on shared disk/mirror disk is shared and publicized, acquire the shared configuration and save it in the configuration file of shared disk/mirror disk. The shared configuration is once released when shared disk/mirror disk is deactivated, but the shared folder is publicized again with the saved configuration.

This section describes the operation when you have checked the [**Auto-save shared configuration of drive**].

CIFS resources will automatically get the information of the shared folder on the drive, and then save it to the [**Shared Configuration File**]. Because it does not exist shared settings file during the initial start-up of CIFS resources, it scans all of the shared folder information on the drive, and then save it to the [**Shared Configuration File**].

Then you can update the shared settings file from the CIFS resources each time the set of shared folder is changed.

When CIFS resources becomes deactivation I will remove all share.

However, since the rest is shared information in the [**Shared Configuration File**], and then automatically recover the shared information at the time of activity.

The following table shows the advantage and disadvantage of the two methods.

	Advantage	Disadvantage
Specify shared configuration individually	Inconsistency does not occur in the shared configuration.	When the shared configuration is changed, it is necessary to change the CIFS resource.

Continued on next page

Table 3.50 – continued from previous page

	Advantage	Disadvantage
Auto-save shared configuration of drive	Changes made for the shared configuration are automatically saved.	When the shared configuration file is corrupted, inconsistency occurs in the shared information.

3.16.3 Notes on CIFS resources

- When files on the shared disks or the mirror disks are publicized, the sharing settings, which are configured by right-click, will be cleared by deactivation of disk resource or mirror disk resource, which will result in no inheritance to another server at a failover. In this case, use CIFS resources.
- When shared configuration of drive is automatically saved, shared configuration file configured as the saving destination is created as a hidden file. For the back up when the shared configuration file is corrupted, a file with ".bak" at the end of the specified file name is created in the same folder. Ensure not to use the same file name with the currently existing file.
- A folder that the shared configuration file is to be created must have access permission to create/update a file for the local system account (SYSTEM). Without proper access permission, creation/updating of the shared configuration file fails. If both the shared configuration file and the backup file are deleted mistakenly, configuration data may be lost. It is recommended that these files should not be deleted by other account.
- If any of the conditions mentioned below arises when publicizing and removing of the shared folders on the disk (eg. shared disk, mirror disk) managed by EXPRESSCLUSTER is controlled with CIFS resources, the activation of CIFS resources fails. Perform troubleshooting procedure 1 or 2. Troubleshooting procedure 1 is recommended.
  <Conditions>
  - The failback of the CIFS resources is executed after the server is restarted for a reason other than cluster shutdown and reboot.
  - CIFS resources are activated for the first time after a deactivation error.

  <Troubleshooting procedure 1>
  Select the **When folder is shared not as activity failure** check box.

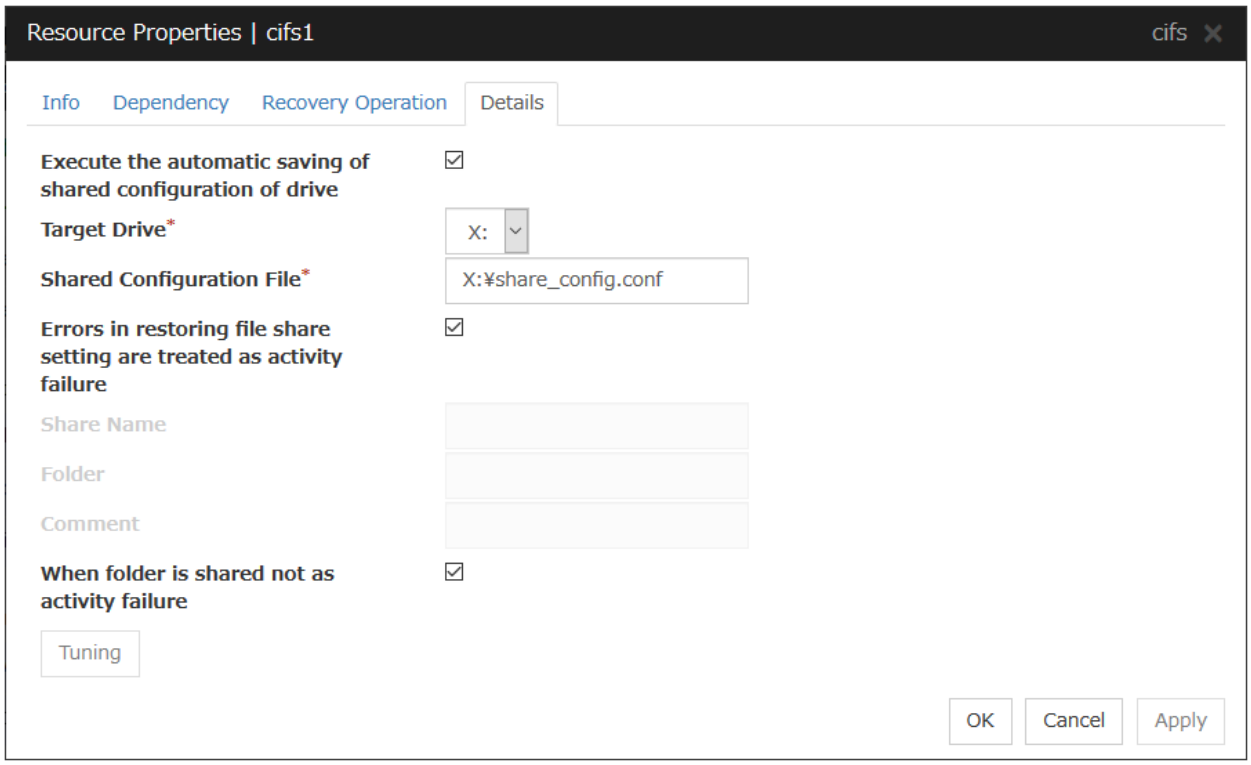
  <Troubleshooting procedure 2>
  It is necessary to delete the shared name by using a script resource before activating CIFS resources. Add a script resource and change the settings, as follows.

  1. Add a script resource, and open **Properties**. In the **Dependency** tab, clear **Follow the default dependence**, and add the corresponding disk resource to **Dependent Resources**.
  2. Open the **Details** tab of the script resource added in 1, and add the following lines of code (*) to start.bat.
     :NORMAL
     net share <*CIFS_resource_controlled_shared_name*> /delete (*Add*)
     (Omitted)
     :FAILOVER
     net share <*CIFS_resource_controlled_shared_name*> /delete (*Add*)
     To use **Auto-save shared configuration of drive** for CIFS resources, it is necessary to add all the shared names controlled with CIFS resources.

3. Open **Properties** of CIFS resources. In the Dependency tab, clear **Follow the default dependence**, and add the corresponding disk resource and the script resource added in 1 to **Dependent Resources**.

- Sharing access Please set a reference that can be user/groups from all cluster nodes. It does not set NTFS Permissions in CIFS resource
- When migrating the Active Directory server, if you configure the accounts of the migration source and destination server domains to share a shared folder with the SID history function enabled, the share setting for the accounts of the source server cannot be maintained.
- If the access permissions applied to the shared folder are either of the following, activating a CIFS resource fails. Apply the proper access permissions.
  - Among the SYSTEM access permissions, the **Read** permission is denied.
  - Among the SYSTEM access permissions, the **List of Folder Contents** permission is denied.
- When **When folder is shared not as activity failure** is enabled (selected), activating the CIFS resource fails if a user saved in the Shared Configuration File is deleted. To delete a user who is set in Permissions for the shared folder, perform either of the following:
  - Disable (clear) **When folder is shared not as activity failure**.
  - To delete a use who is set in Permissions for the shared folder, also delete the corresponding group from **Advanced Sharing > Permissions** on the **Sharing** tab of the properties of the shared folder on the drive set to the CIFS resource.
- If the Shared Configuration File is damaged, recover it by performing either of the following:
  - Among the SYSTEM access permissions, the **Read** permission is denied. Stop the CIFS resource and replace the damaged file with the backed up Shared Configuration File. Then, start the CIFS resource. This method is effective when there are many folders or there are many sharing settings required to change.
  - Stop the CIFS resource and delete the damaged Shared Configuration File. Then, start the CIFS resource and make the sharing settings again from Explorer.
- If a failover occurred, the shared folder disappears temporarily. This might disable to browse the file open before the failover occurrence or to browse files from Explorer. Therefore, it is recommended to use the shared folder offline as follows:
  - When **Execute the automatic saving of shared configuration of drive** is enabled (selected), select **All files and programs that users open from the share are automatically available offline** for the **Cache** settings of the shared folder.
  - When **Execute the automatic saving of shared configuration of drive** is disabled (not selected), select **Automatic Caching** on the **Cache** tab of the CIFS resource tuning properties.

3.16.4 Details tab



Execute the automatic saving of shared configuration of drive

Configure whether to save shared configuration of drive automatically. Check this when you want to set the auto-saving.

Target Drive

Specify the drive letter of the target disk when you want to execute auto saving of shared configuration of drive.

Shared Configuration File (Within 225 bytes)

Specify the file that saves shared configuration of drive with full path. You need to specify a path of shard disk/mirror disk/hybrid disk within the same group.

This is the file that CIFS resource creates. There is no need for you to prepare before CIFS resource activation.

Errors in restoring file share setting are treated as activity failure

When this option is selected: Activating CIFS resources fails in cases where users saved in shared configuration file does not exist or user information cannot be obtained from domain environment. When the shared folder configuration is changed, if no user is set in **Permissions** for the shared folder or if user information cannot be obtained from the domain environment, a warning message appears.

When this option is not selected (default): Activating CIFS resources is successful in above cases. The file sharing access permission is not granted to a user whose information could not be acquired. The warning message does not appear.

The following configurations are executed when specifying shared configuration individually.

Shared name (Within 79 bytes)

Specify the name of the shared folder, which is publicized by using CIFS resource. The following can not be used.

Folder (Within 255 bytes)

Specify the full path to the shared folder, which is publicized by CIFS resources.

Comment (Within 255 bytes)

Specify the comment of the shared folder, which is publicized by using CIFS resource.

When folder is shared not as activity failure

When this option is not selected: The activation of CIFS resources fails when folders are already shared. In Windows Server 2012 or later, this condition always arises because of the change in the OS specifications. It is therefore recommended to check this option.

When this option is selected (default): The activation of CIFS resources succeeds in the above case. The warning message is not output.

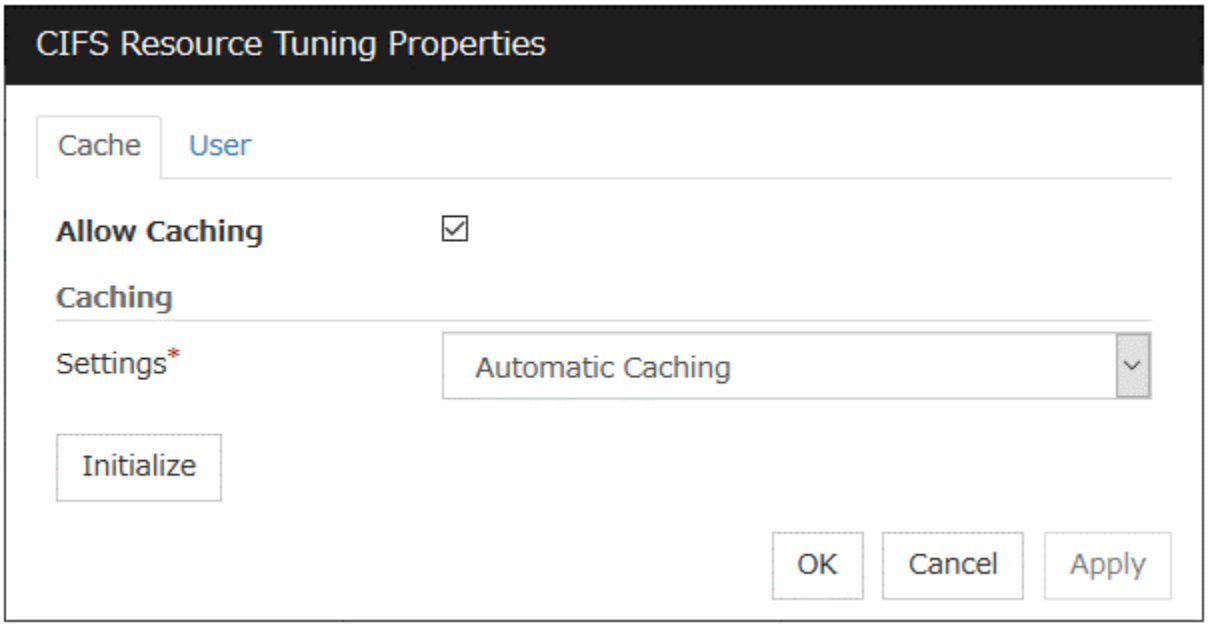
Tuning

Display CIFS resource tuning properties dialog box. You can change the settings of the detail information of the CIFS resource.

CIFS resource tuning properties

Cache tab

Display the details of cache



Allow Caching

Set to enable the caching of shared folders. By enabling this function, the files in the shared folders can be referenced in the offline status when specifying shared configuration individually, and those files can still be referenced after a failover. This function is not used when **Auto-save shared configuration of drive** method is selected.

Settings

Select the caching settings if you choose to allow caching.

Choose one of the following settings. Manual Caching (**Enable BranchCache**) is not supported.

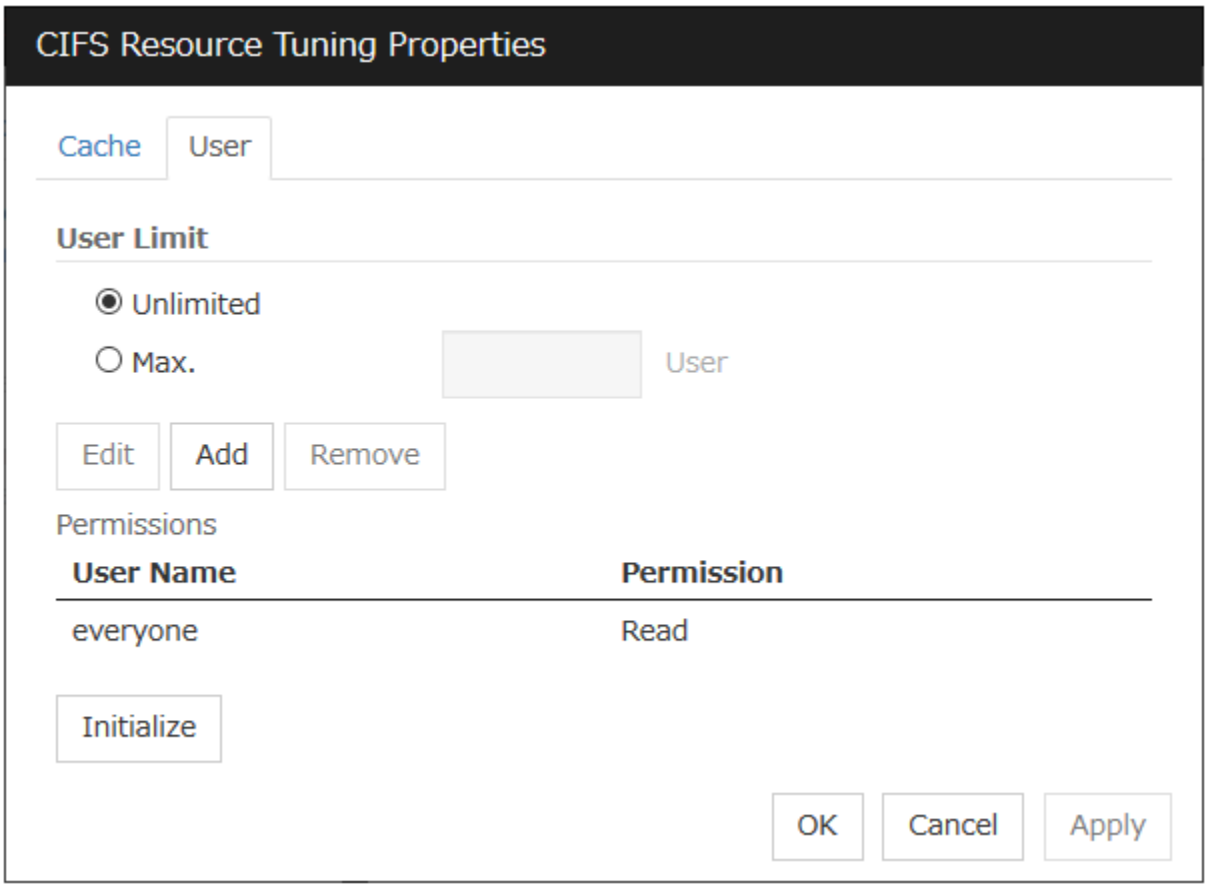
- Automatic Caching
  This setting is equivalent to the following setting in the Windows OS. The message corresponding to this setting may be different depending on the version of Windows.
  All files and programs that users open from the share will be automatically available offline.
- Manual Caching
  This setting is equivalent to the following setting in the Windows OS. The message corresponding to this setting may be different depending on the version of Windows.
  Only the files and programs that users specify will be available offline.
- Automatic Caching (Optimized for the performance)
  This setting is equivalent to the following setting in the Windows OS. The message corresponding to this setting may be different depending on the version of Windows.
  Optimize for performance

Initialize

Click **Initialize** to initialize all the items to the default value.

User tab

Display the detailed settings of restriction of the number of users and permission of access.



User Limit (1 to 9999)

Set the maximum number of users who can access the shared folder at a time.

Add

Add the settings of access permission for user account or user group to **Access Permission**. When you click this button, the **Enter user** dialog box is displayed. Specify the user name and the permission.

Remove

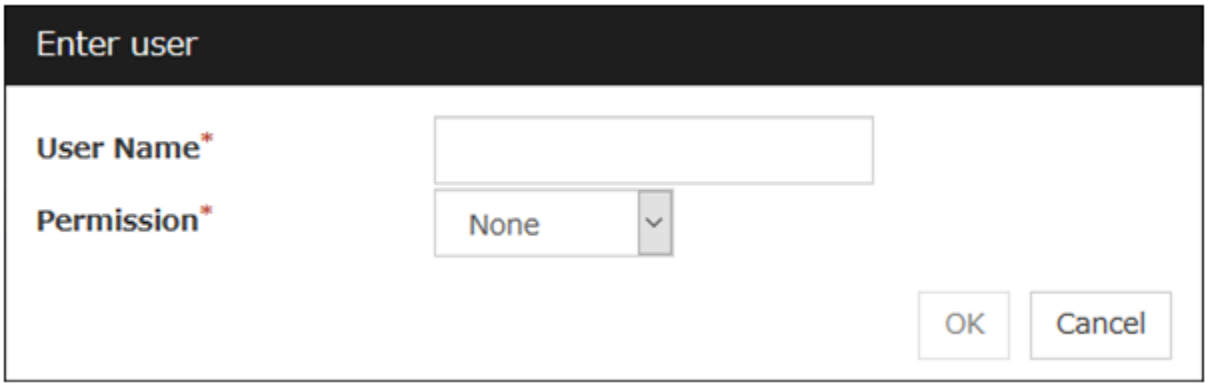
Delete the access permission selected in **Permissions**.

Edit

Modify the access permission specified in **Permissions**. The **Enter user** dialog box is displayed. The specified access permission displayed in the **Enter user** allows you to modify permission.

Initialize

Click **Initialize** to initialize all the items to the default values.



User Name (Within 255 bytes)

Enter the Window user name or a group name. When using a domain account, enter in the format of "*Domain_name\User_name*". No two-byte characters can be registered for **User Name**. A name containing a one-byte space can be registered. (Example: Domain Admins). If you want to use the double-byte characters in the Windows user name or group name, please check the **Auto-save shared configuration of drive**.

Permission

Select one of following settings for access permission of the entered user/group.

- Full control
- Change
- Read
- None

When **None** is selected**,** access is denied.

3.17 Understanding hybrid disk resources

3.17.1 Dependencies of hybrid disk resources

By default, hybrid disk resources do not depend on any group resource type.

3.17.2 Hybrid disk

A hybrid disk resource is a resource in which disk resource and mirror disk resource are combined. When you use a disk resource, a failover group can perform failover only to the cluster server connected to the same shared disk. On the other hand, in hybrid disk, by mirroring the data in the shared disk, failover can be performed to a server which is not connected to the shared disk. This enables configuring a remote cluster as in the following figure, where failover is performed in the active site upon normal failure, while failover can be performed to the stand-by site when a disaster occurs.

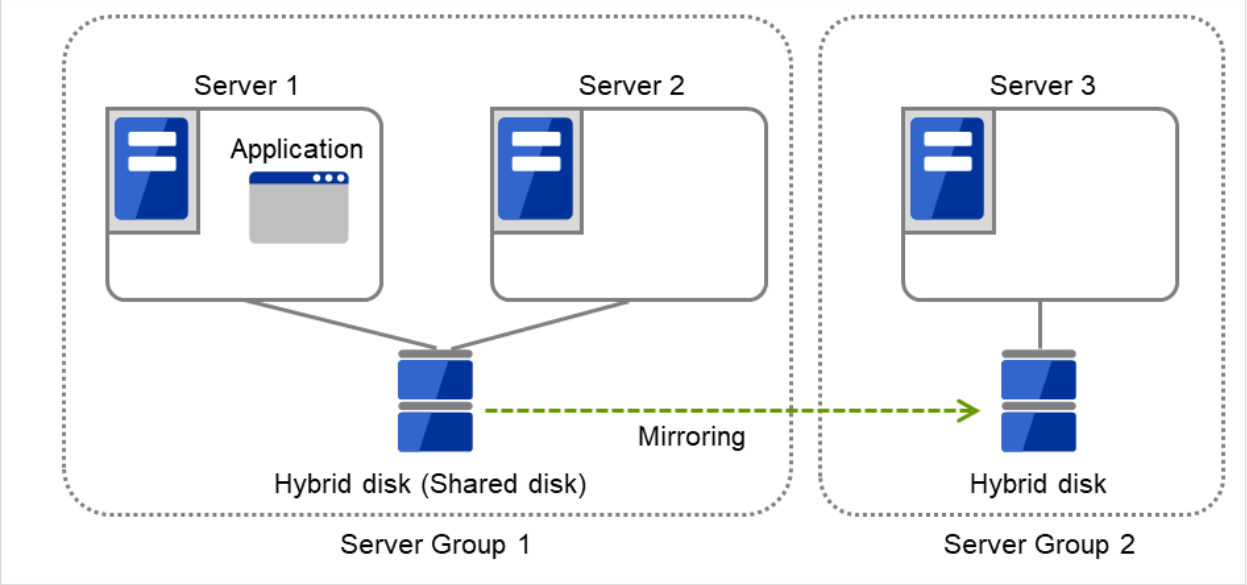


Fig. 3.106: Hybrid configuration (1): in a normal case

When Server 1 crashes, the application is failed over to Server 2.

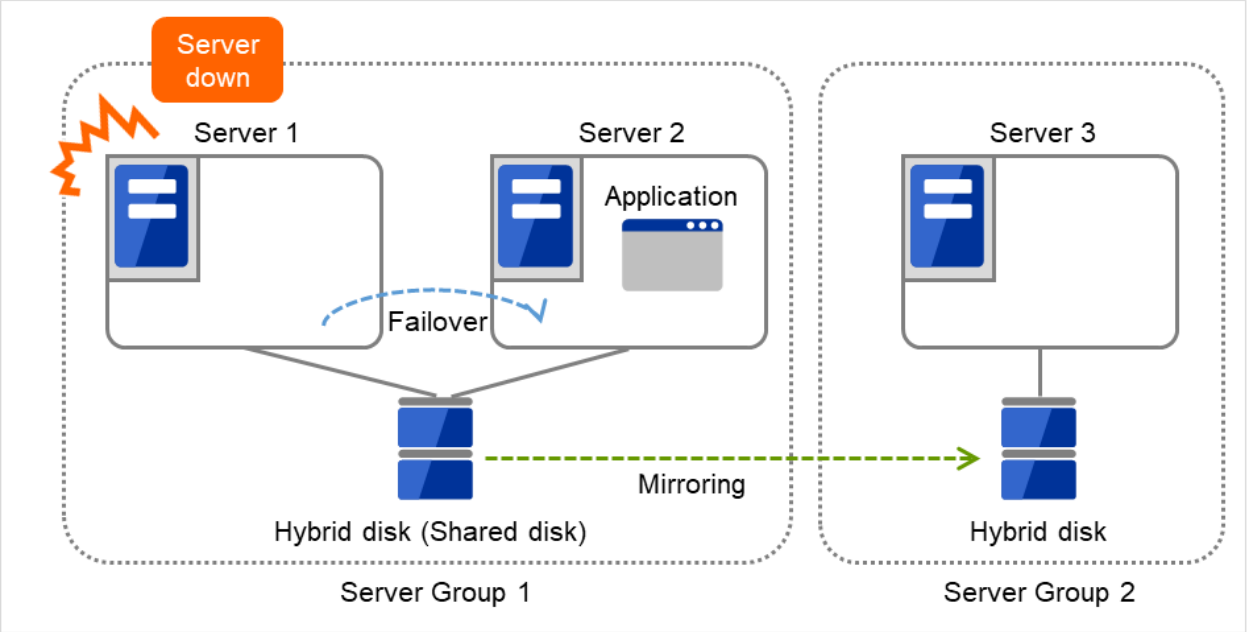


Fig. 3.107: Hybrid configuration (2): Server 1 crashes

When Server 2 crashes, the application is failed over to Server 3.

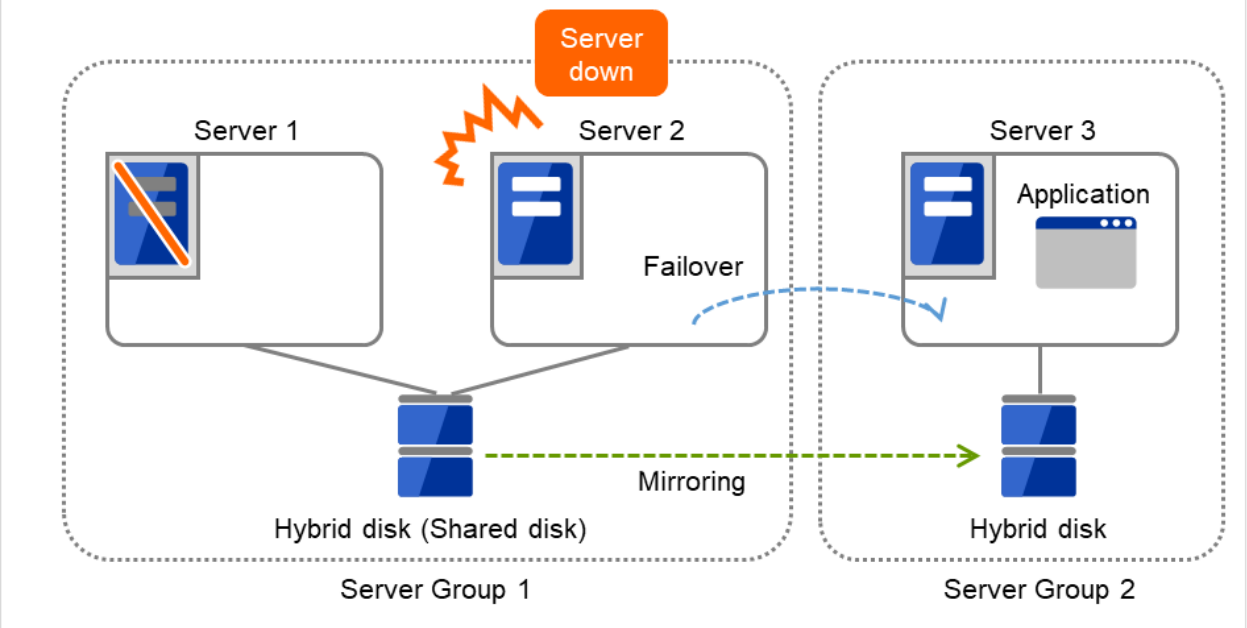


Fig. 3.108: Hybrid configuration (3): Server 2 crashes

In hybrid disk, a group of servers that is connected to the shared disk is referred to as a server group. Disk mirroring is performed between two server groups. A server which does not use the shared disk is a server group in which there is only one server.

Like mirror disk resources, mirroring takes place in each partition, where RAW partition (cluster partition) to record

management information is required as well as data partition which is the mirroring target. It is necessary that each server using hybrid disk resource has a license for EXPRESSCLUSTER X Replicator DR 5.2 for Windows.

3.17.3 Notes on hybrid disk resources

- Data partition size

  The sizes of data partitions to be mirrored need to be exactly the same by byte.

  If the type or geometry of the disks differs, you may fail to configure the same size for partitions. If this happens, check the precise size of data partitions of the servers by the clpvolsz command before configuring hybrid disk resource. If the sizes are not consistent, run the clpvolsz command again to contract the larger partition.

  For details on the clpvolsz command, see "*Tuning partition size (clpvolsz command)*" in "*9. EXPRESSCLUSTER command reference*" in this guide.

  There is no limit for data partition size.

- Time required for data partition copying

  When a file is copied at initial configuration or disk replacement, the required amount of time increases in proportion to the size of the volume use area. If the volume use area cannot be specified, the required amount of time increases in proportion to the data partition size because the entire area of the volume is copied.

- Cluster partition size

  Reserve at least 1024MiB. In some disk geometry it may be 1024MB or larger, which is not a problem.

- Partition drive letter

  Specify the same drive letters in each server for data partition and cluster partition.

  Do not change the drive letter until deleting resources after configuring hybrid disk resources. If a drive letter has been changed, restore the drive letter when hybrid disk resource is started. When the original drive letter is used by other partition, starting mirror disk resource fails.

- Partition allocation

  When a data partition on the shared disk is mirrored, the data partition and the cluster partition need to be allocated on the same shared disk (they do not have to be allocated on the same logical disk).

  Allocate the data partition and the cluster partition on a basic disk. Dynamic disk is not supported.

  When making data partitions as logical partitions on the extended partition, make sure the data partitions are logical partition on both servers. The actual size may be slightly different even the same size is specified on both basic partition and logical partition.

- Partition format

  Format a data partition by NTFS. FAT/FAT32 is not supported.

  Do not construct a file system in a cluster partition. Do not format it.

- Access control of a data partition

  The data partition to be mirrored by a hybrid disk resource can be accessed only from the active server where a hybrid disk resource is activated. Access from other servers is restricted by EXPRESSCLUSTER.

  Access to the cluster partition is also restricted by EXPRESSCLUSTER.

- Partition deletion

  When you delete a data partition or cluster partition on the hybrid disk resource, delete the hybrid disk resource in Cluster WebUI in advance.

- Server group settings

  In a failover group having hybrid disk resource, it is necessary to register two server groups which are mirrored by the hybrid disk resource in the **Server Groups** tab of **Group Properties.** Configure the settings for these server groups in **Server Groups** in the config mode of Cluster WebUI.

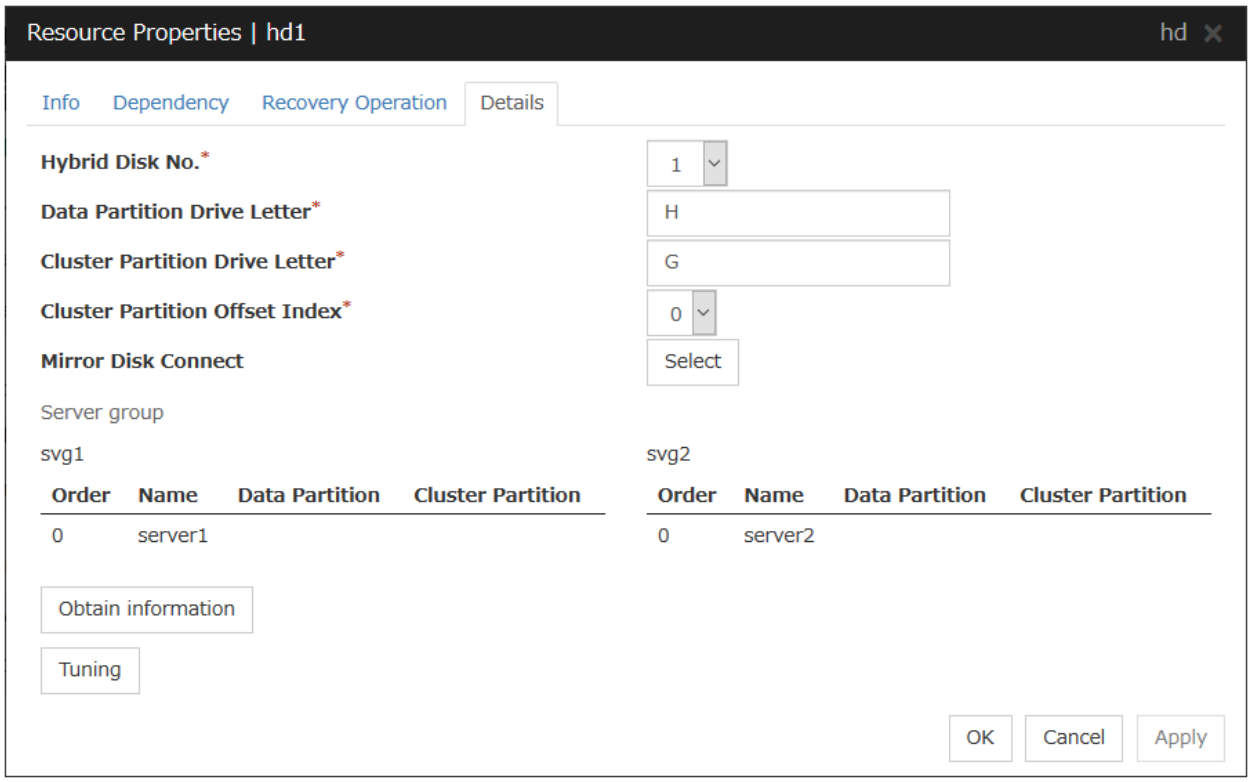
- Changing the configuration between the mirror disk and hybrid disk
  To change the configuration so that the disk mirrored using a mirror disk resource will be mirrored using a hybrid disk resource, first delete the existing mirror disk resource from the configuration data, and then upload the data. Next, add a hybrid disk resource to the configuration data, and then upload it again.
- Disk devices that configure hybrid disks
  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.

- **Auto Mirror Initial Construction** is set not to be performed
  When you use the hybrid disk resource after disabling **Auto Mirror Initial Construction** on the **Mirror Disk** tab in the **Cluster Properties**, change the icon color of the source server group to green by using Mirror Disks before starting hybrid disk resources for the first time.

3.17.4 Details tab



Hybrid Disk No.

Select a disk number to be allocated to a hybrid disk resource. This number must be different from the ones for other hybrid disk resources and mirror disk resources.

Data Partition Drive Letter (Within 1023 bytes)

Specify the drive letter (A to Z) for the data partition.

Cluster Partition Drive Letter (Within 1023 bytes)

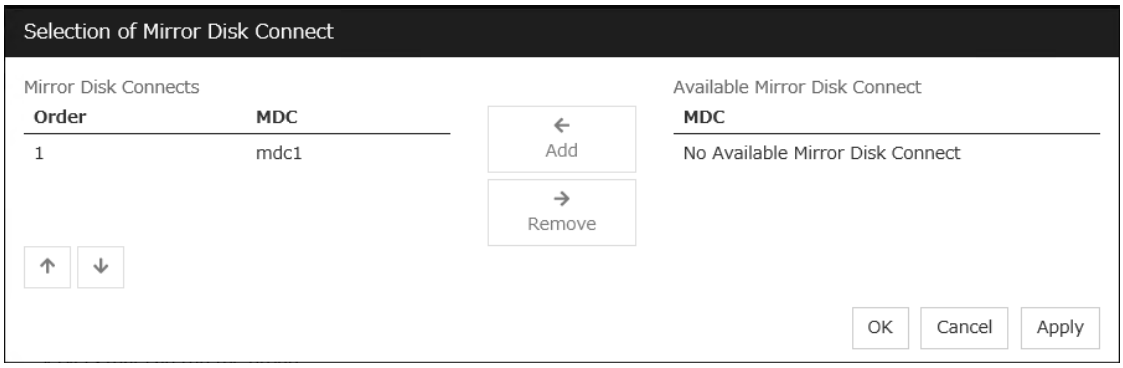
Specify the drive letter (A to Z) for the cluster partition. Multiple hybrid disks can use the same cluster partition, but it cannot be the cluster partition of the mirror disk resource.

Cluster Partition Offset Index

Select an index number for the area used in the cluster partition. When using the multiple hybrid disks, assign different numbers for hybrid disk so that the areas to be used in the cluster partition do not overlap.

Select

Select the communication path for the data mirroring communication (mirror disk connect). Click Select to display the **Selection of Mirror Disk Connect** dialog box.



- Add

  Use **Add** to add mirror disk connects. Select the mirror disk connect you want to add from **Available Mirror Disk Connect** and then click **Add**. The selected mirror disk connect is added to the **Mirror Disk Connects**.

- Remove

  Use Remove to remove mirror disk connects to be used. Select the mirror disk connect you want to remove from the **Mirror Disk Connects** and then click **Remove**. The selected mirror disk connect is added to **Available Mirror Disk Connect**.

- Order

  Use the arrows to change the priority of mirror disk connects to be used. Select the mirror disk connect whose priority you want to change, and then click the arrows. The selected row moves accordingly.

For mirror disk connect settings, see "*Interconnect tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

Server groups

Information on each member server of the two server groups selected in the **Server Groups** tab in **Properties** of failover groups is displayed.

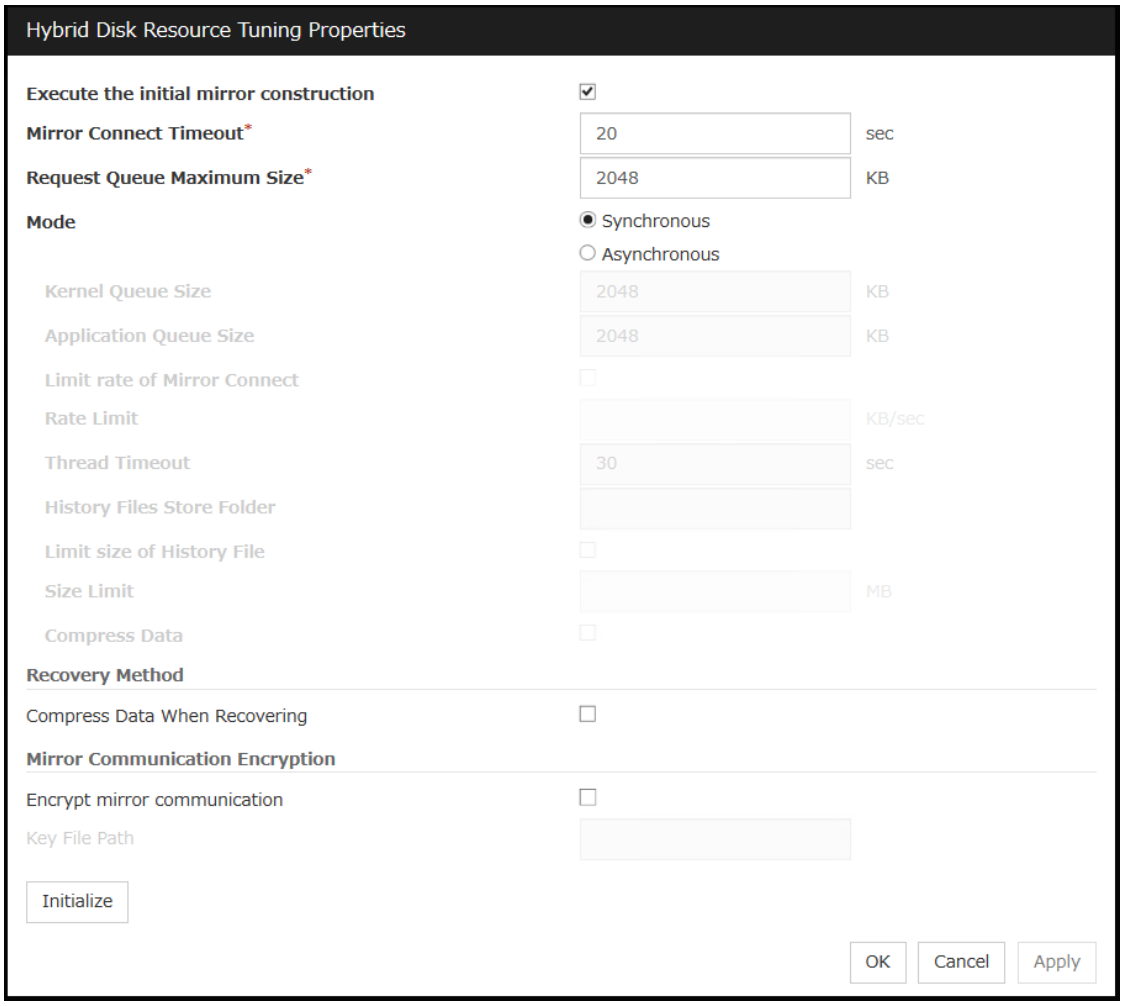
Clicking **Obtain information** on the Cluster WebUI enables you to get GUID information for the data and cluster partitions of each server.

Tuning

The **Hybrid Disk Resource Tuning Properties** dialog box is displayed. You can configure the details on hybrid disk resources.

Hybrid Disk Resource Tuning Properties

Detailed settings on mirror are displayed.



Parameters on this configuration window are the same as those of mirror disk resources.

For the meaning and setting method of each parameter, see " *Understanding mirror disk resources* ".

3.17.5 Notes on operating hybrid disk resources

If mirror data was synchronized on both server groups when the cluster was shut down, use one of the two orders noted below to start the servers.

- Simultaneously start servers belonging to both server groups at least one at a time
- Start the first server (which belongs to server group 1), and then start the second server (which belongs to server group 2) after the first server has started

Do not consecutively start and shutdown both servers[6] .The servers communicate with each other to determine whether the mirror data stored in each server group is up to date. Consecutively starting and shutting down both servers prevents the servers from properly determining whether mirror data is up to date and hybrid disk resources will fail to start the next time both server groups are started.

[6] In other words, do not start and shut down the first server, and then start and shut down the second server.

3.18 Understanding AWS elastic ip resources

3.18.1 Dependencies of AWS elastic ip resources

By default, this function does not depend on any group resource type.

3.18.2 AWS elastic ip resource

By using this resource, an HA cluster can be configured with EXPRESSCLUSTER using the Amazon Virtual Private Cloud (referred to as the VPC) in the Amazon Web Services (referred to as AWS) environment.

This makes it possible to perform more important business operations in the same environment, increasing the number of choices for the system configuration in the AWS environment. AWS is configured robustly in multiple Availability Zones (referred to as AZs) in each area (region), enabling the user to select an AZ according to his or her needs. EXPRESSCLUSTER enables an HA cluster among multiple AZs (referred to as multi-AZ), achieving high availability of business operations.

Two types of HA clusters with the data mirror method are assumed, "HA cluster with VIP control" and "HA cluster with EIP control". This section describes AWS elastic ip resources that are used for "HA cluster with EIP control".

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 AZ, and each instance can access the Internet via the Internet gateway.

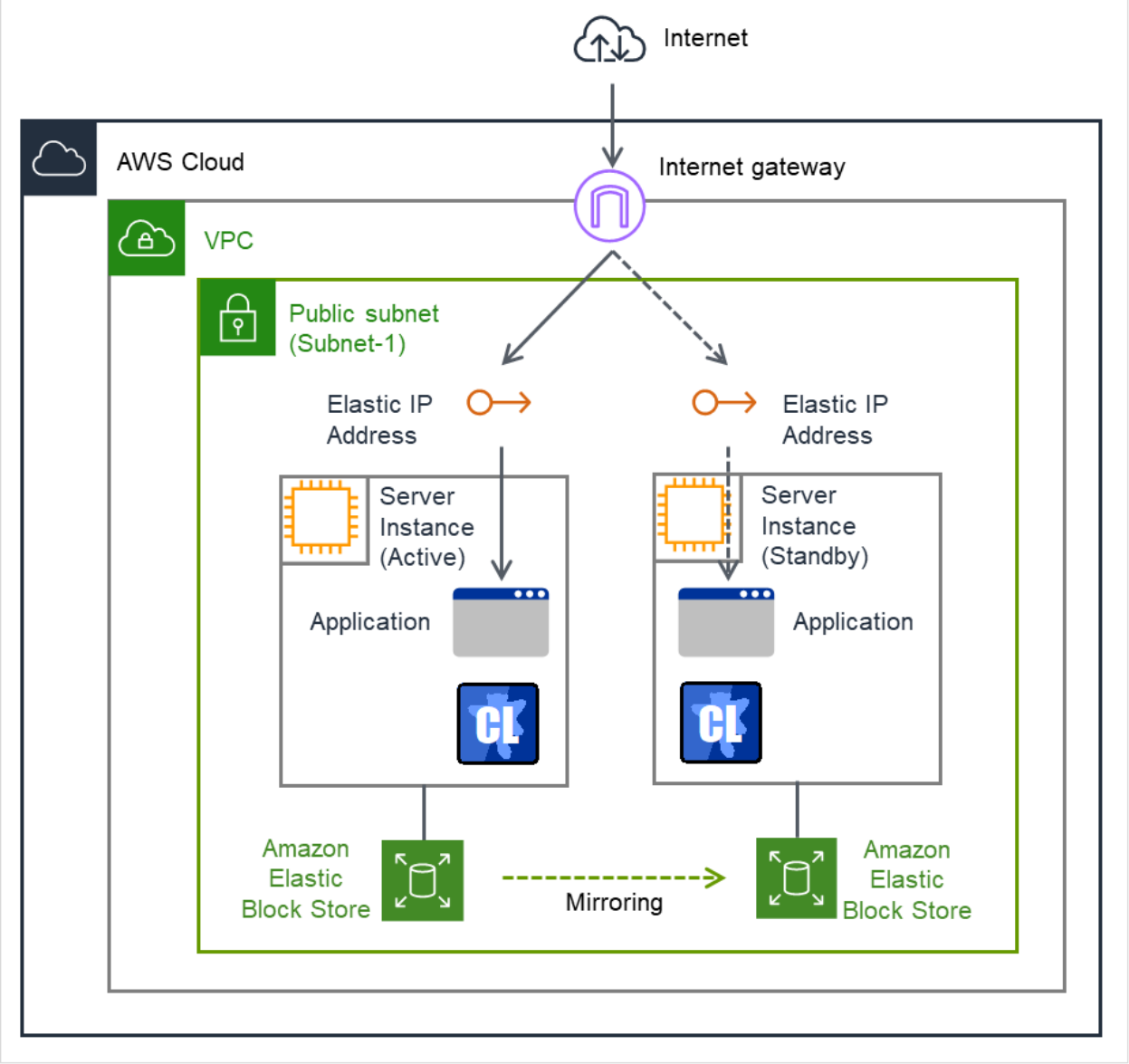


Fig. 3.109: Configuration with an AWS Elastic IP resource

3.18.3 Notes on AWS elastic ip resources

- See " Setting up AWS elastic ip resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

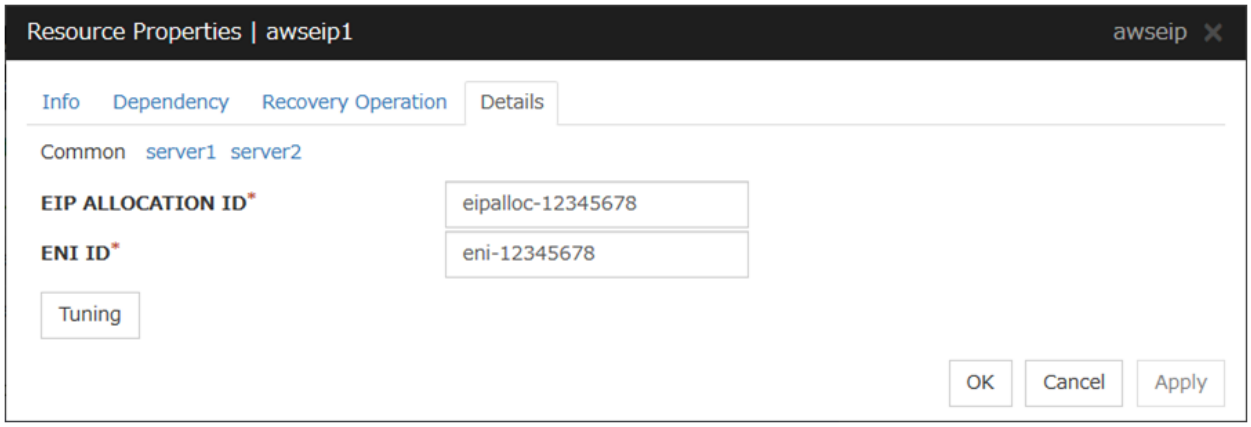
3.18.4 Applying command line options to AWS CLI run from AWS Elastic IP resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.18.5 Applying environment variables to AWS CLI run from the AWS elastic ip resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.18.6 Details tab



EIP ALLOCATION ID (Within 45 bytes)

For EIP control, specify the ID of the EIP to replace.

ENI ID (Within 45 bytes)

For EIP control, specify the ENI ID to which to allocate an EIP.

In the [common] tab, described the ENI ID of any of the server, the other server, please to perform the individual settings.

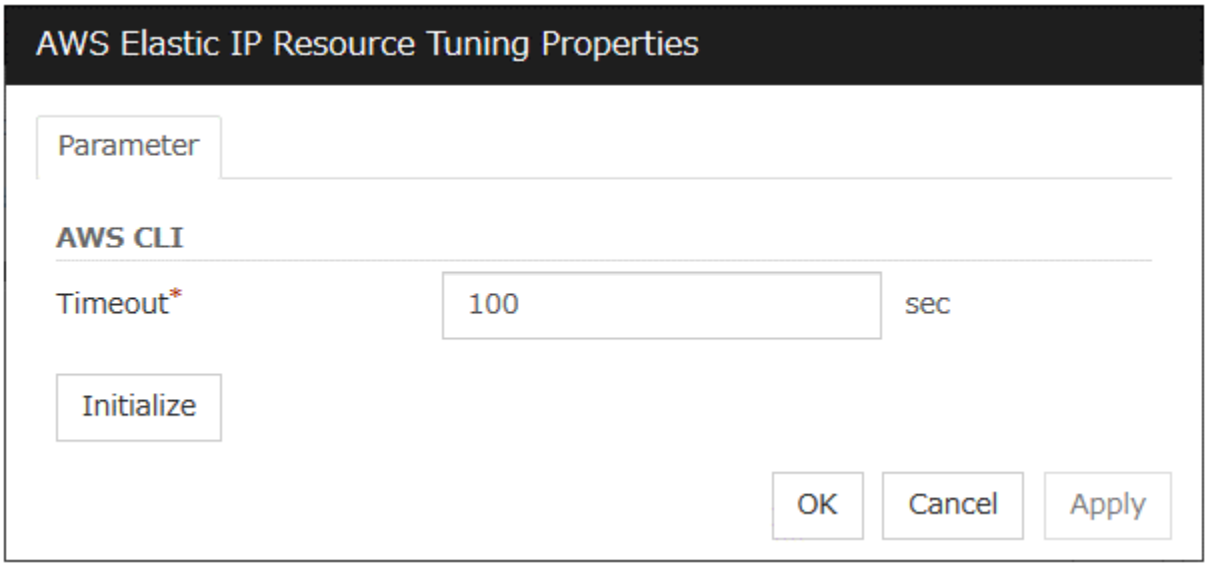
Tuning

Opens the **AWS elastic ip resource tuning properties** dialog box where the detailed settings for the AWS elastic ip resource tuning properties can be configured.

AWS Elastic IP Resource Tuning Properties

Parameter tab

Detailed setting for parameter is displayed.



Timeout (1 to 999)

Make the setting of the timeout of AWS CLI command executed for the activation and/or deactivation of the AWS elastic ip resource and AWS elastic ip monitor resource.

3.19 Understanding AWS virtual ip resources

3.19.1 Dependencies of AWS virtual ip resources

By default, this function does not depend on any group resource type.

3.19.2 AWS virtual ip resource

By using this resource, an HA cluster can be configured with EXPRESSCLUSTER using the Amazon Virtual Private Cloud (referred to as the VPC) in the Amazon Web Services (referred to as AWS) environment.

This makes it possible to perform more important business operations in the same environment, increasing the number of choices for the system configuration in the AWS environment. AWS is configured robustly in multiple Availability Zones (referred to as AZs) in each area (region), enabling the user to select an AZ according to his or her needs. EXPRESSCLUSTER enables an HA cluster among multiple AZs (referred to as multi-AZ), achieving high availability of business operations.

AWS CLI command is executed for AWS virtual ip resource when it is activated to update the route table information.

Two types of HA clusters with the data mirror method are assumed, "HA cluster with VIP control" and "HA cluster with EIP control". This section describes AWS virtual ip resources that are used for "HA cluster with VIP control"

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 AZ, and each instance can access the Internet via the NAT gateway placed on the public subnet.

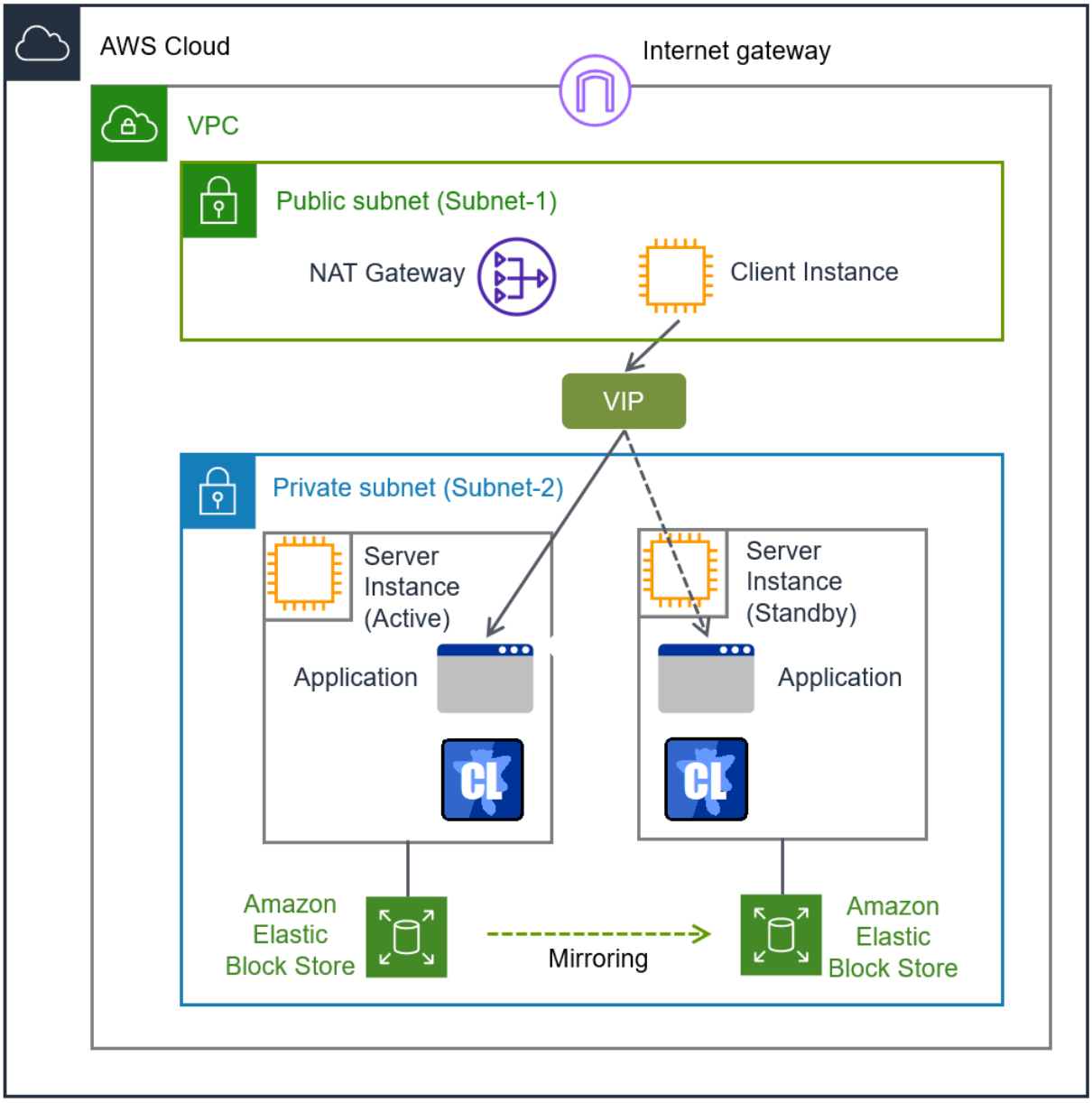


Fig. 3.110: Configuration with an AWS Virtual IP resource

3.19.3 Notes on AWS virtual ip resources

- See " Setting up AWS virtual ip resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

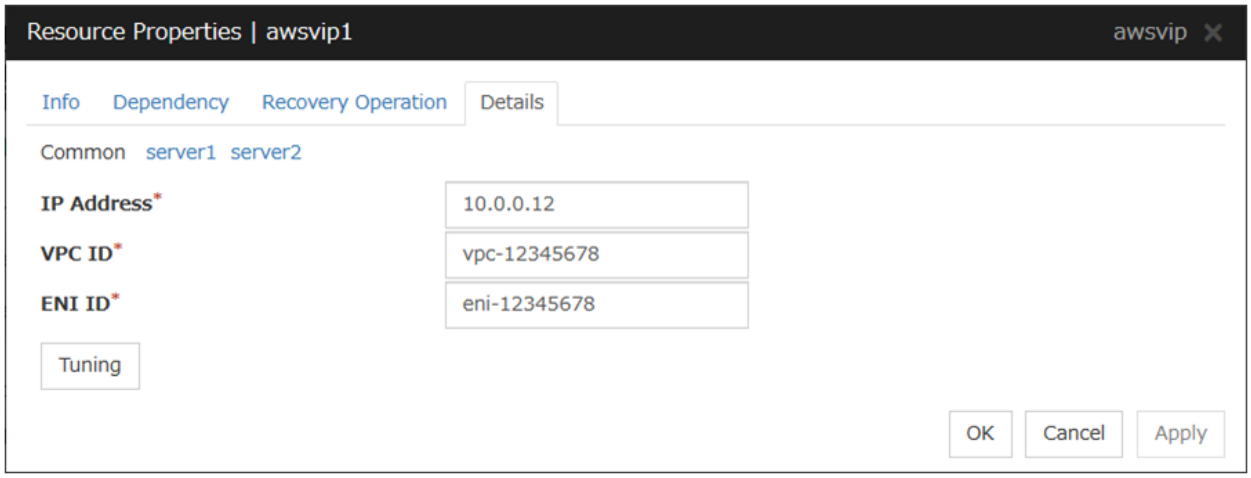
3.19.4 Applying command line options to AWS CLI run from AWS Virtual IP resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.19.5 Applying environment variables to AWS CLI run from the AWS virtual ip resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.19.6 Details tab



IP Address (Within 45 bytes)

For VIP control, specify a VIP address to be used: an IP address not belonging to VPC CIDR.

VPC ID (Within 45 bytes)

For VIP control, specify the VPC ID to which the server belongs. To specify an individual VPC ID to servers, enter a VPC ID of any server on the Common tab and specify a VPC ID for other servers individually.

ENI ID (Within 45 bytes)

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.

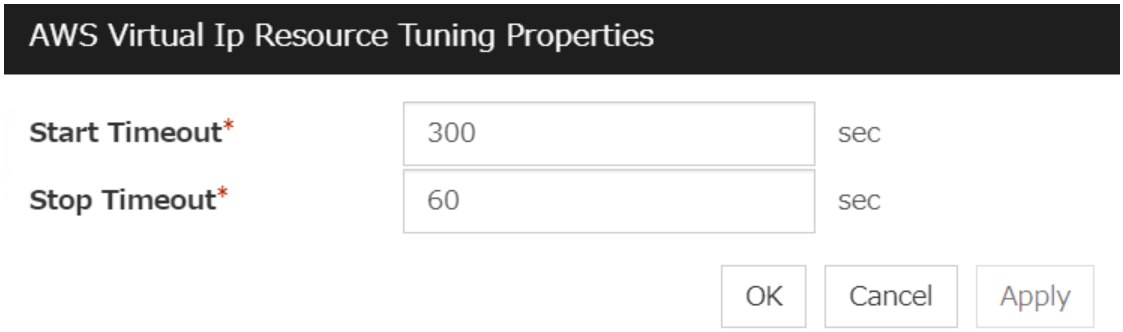
Tuning

Opens the **AWS virtual ip resource tuning properties** dialog box where the detailed settings for the AWS virtual ip resource tuning properties can be configured.

AWS Virtual Ip Resource Tuning Properties

Parameter tab

Detailed setting for parameter is displayed.



Start Timeout (1 to 9999)

Specify the timeout of the script to be used in activating AWS virtual ip resources.

Stop Timeout (1 to 9999)

Specify the timeout of the script to be used in deactivating AWS virtual ip resources.

3.20 Understanding AWS secondary ip resources

3.20.1 Dependencies of AWS secondary ip resources

By default, this function does not depend on any group resource type.

3.20.2 AWS secondary ip resource

Client applications can use Secondary IP addresses to access the VPC in AWS environment.

By using Secondary IP addresses, clients do not need to be aware of switching access destination server when a failover occurs or moving a group migration.

AWS Secondary IP resources allocate secondary IP addresses during activation, and deallocate them during deactivation.

HA cluster with Secondary IP 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 AZ, and each instance can access the Internet via the NAT gateway placed on the public subnet.

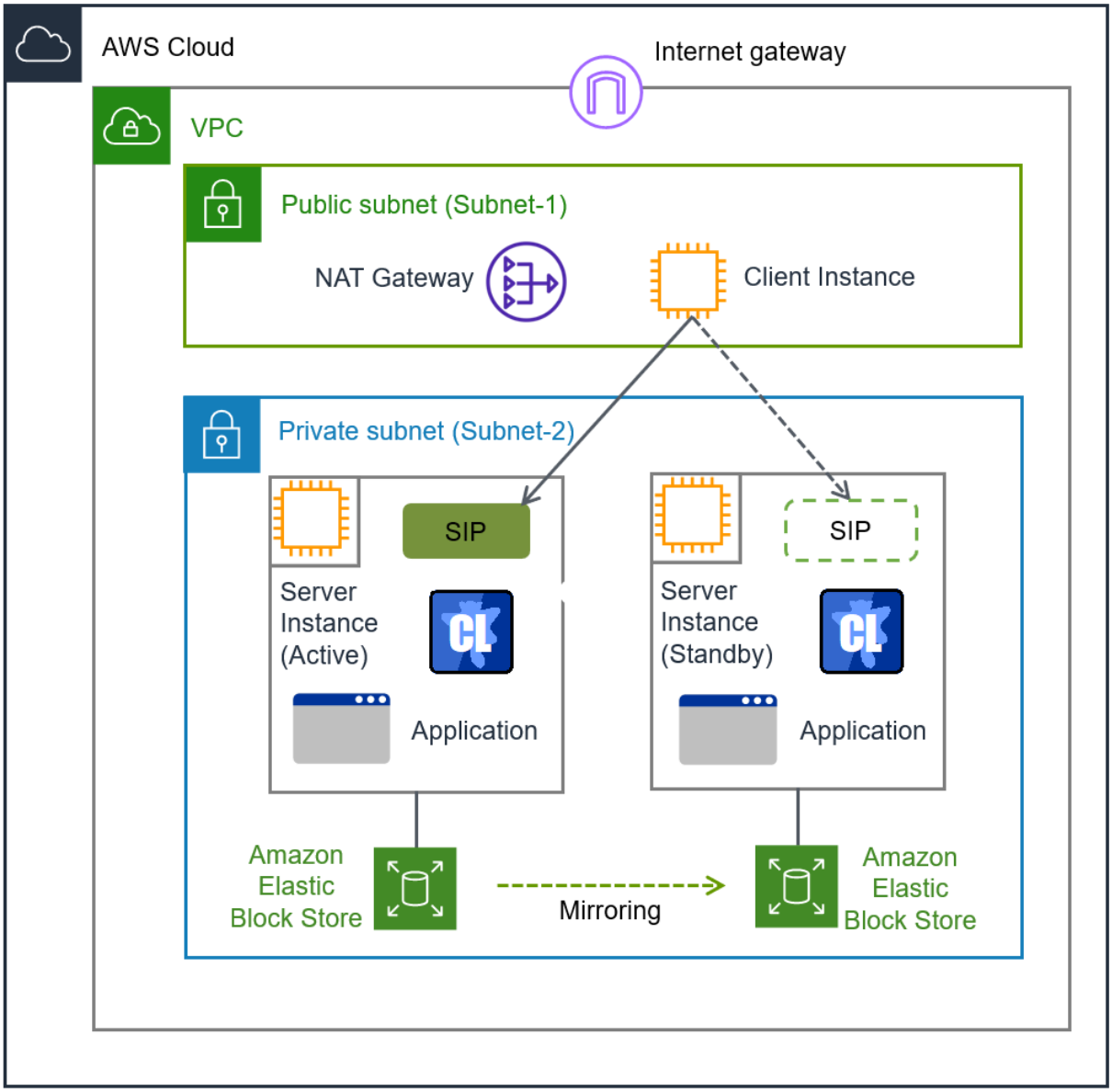


Fig. 3.111: Configuration with an AWS Secondary IP resource

Note: The term "SIP" in the above figure means a secondary IP address.

3.20.3 Notes on AWS secondary ip resources

- See " Setting up AWS secondary ip resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

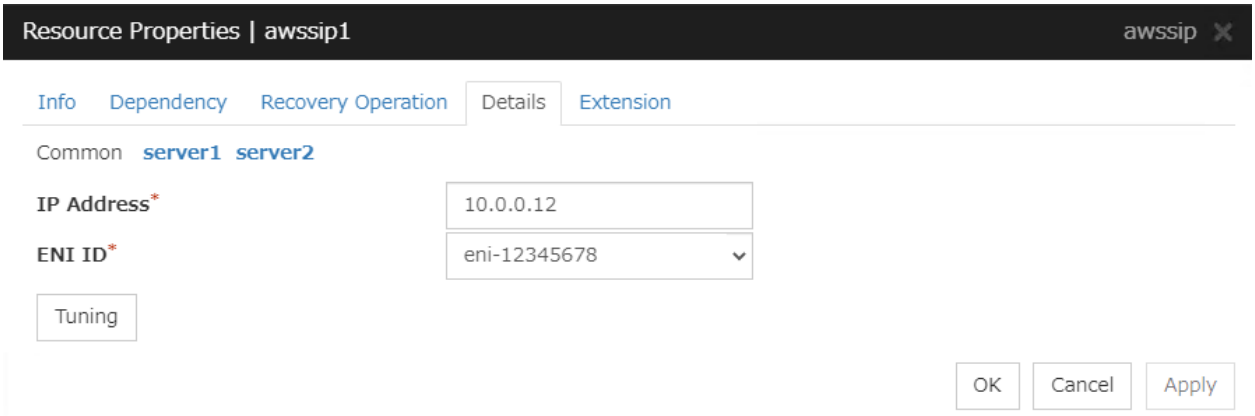
3.20.4 Applying command line options to AWS CLI run from AWS Secondary IP resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.20.5 Applying environment variables to AWS CLI run from the AWS secondary ip resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.20.6 Details tab



IP Address (Within 45 bytes)

Specify a secondary IP address existing within the subnet to which the instance belongs.
The number of the secondary IP address must be higher than that of the local server's private IPv4 address.

(Example) If the IPv4 CIDR of the subnet is 10.0.0.0/24 and the private IPv4 address of the instance is 10.0.0.11:

IP Address	NG or OK
10.0.0.10	NG
10.0.0.11	NG
10.0.0.12	OK

ENI ID (Within 45 bytes)

Specify the ENI ID of a network interface where the secondary IP address is allocated. This setting is required for each server: In the **Common** tab, enter the ENI ID of any server; in each of the other server tabs, specify the ENI ID of the corresponding server.

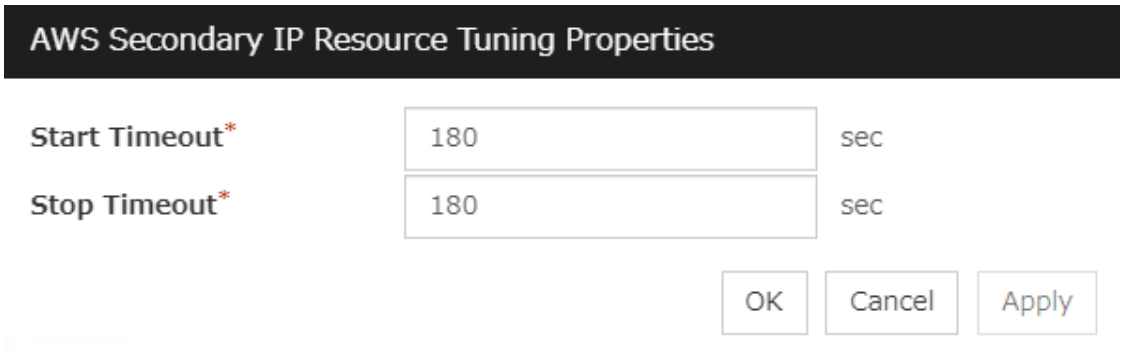
Tuning

Opens the **AWS secondary ip resource tuning properties** dialog box where the detailed settings for the AWS secondary ip resource tuning properties can be configured.

AWS Secondary Ip Resource Tuning Properties

Parameter tab

Detailed setting for parameter is displayed.



Start Timeout (1 to 9999)

Specify the timeout of the script to be used in activating AWS Secondary IP resources.

Stop Timeout (1 to 9999)

Specify the timeout of the script to be used in deactivating AWS Secondary IP resources.

3.21 Understanding AWS DNS resources

3.21.1 Dependencies of AWS DNS resources

By default, this function does not depend on any group resource type.

3.21.2 AWS DNS resource

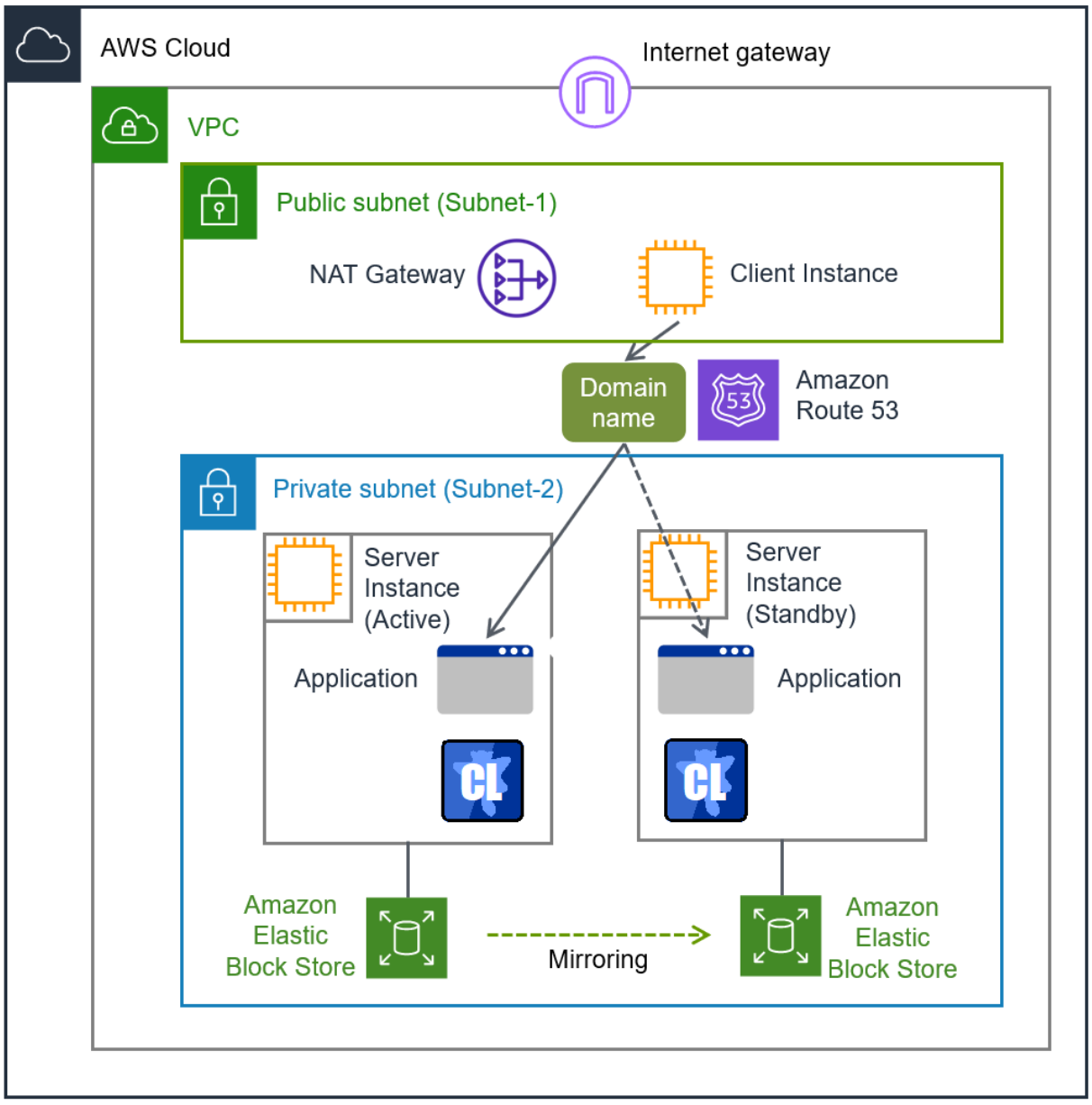


Fig. 3.112: Configuration with an AWS DNS resource

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.

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

3.21.3 Activation timing of AWS DNS resources

AWS DNS resources are activated after waiting until an update to the DNS record is applied to Amazon Route 53.

Note:

This function is available only with versions of EXPRESSCLUSTER X 5.0 or later.
To make this function with versions of EXPRESSCLUSTER X 5.0 or later upgraded from X 4.3 or lower, remove the AWS DNS resources once, add the resources again, then reconfigure them.

3.21.4 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 the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

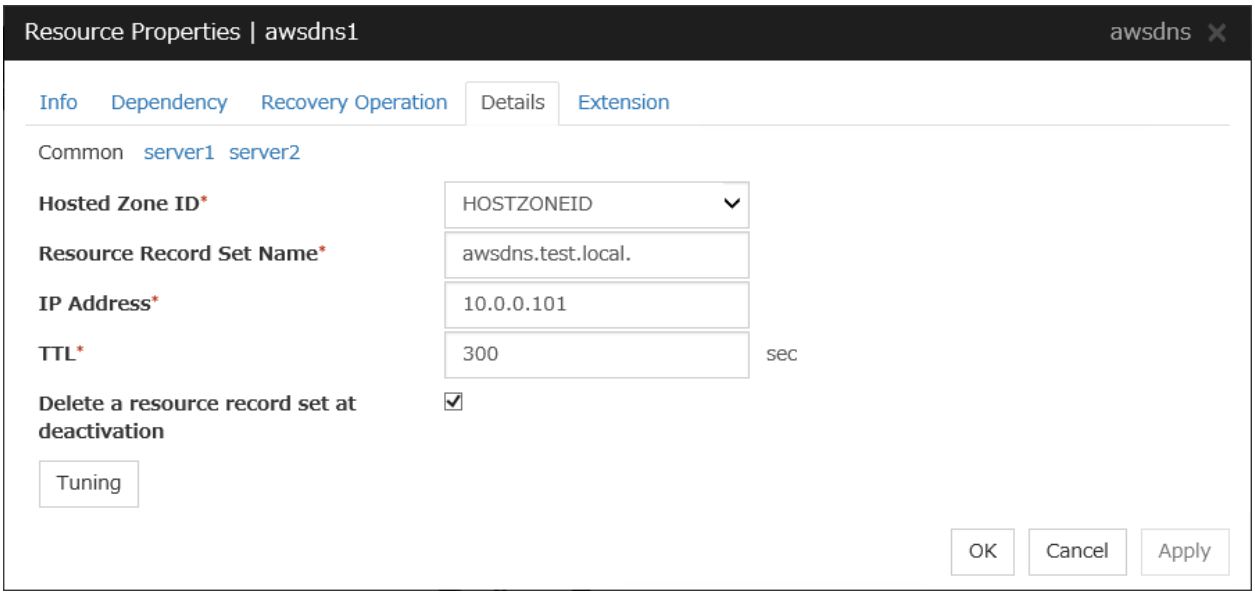
3.21.5 Applying command line options to AWS CLI run from AWS DNS resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.21.6 Applying environment variables to AWS CLI run from the AWS DNS resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.21.7 Details tab



Host 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)

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 a time-to-live (TTL) for the DNS service cache.

Delete a resource record set at deactivation

- When the check box is selected:
  The record set is delete when it is deactivated.
- When the check box is not selected (default):
  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.

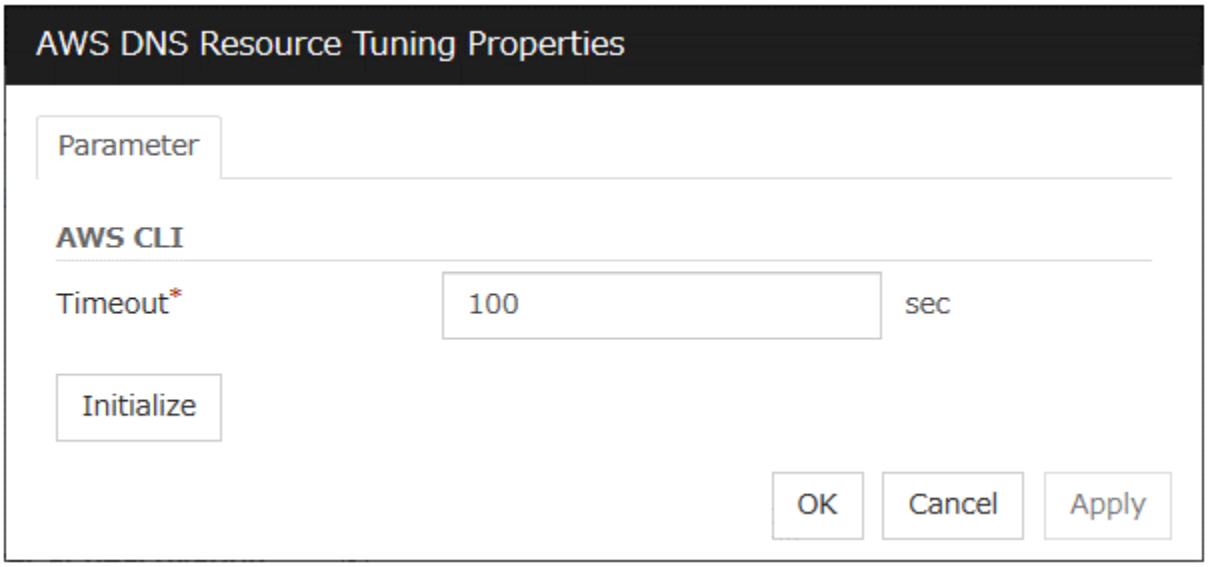
Tuning

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

Detailed setting for parameter is displayed.



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.

3.22 Understanding Azure probe port resources

3.22.1 Dependencies of Azure probe port resources

By default, this function does not depend on any group resource type.

3.22.2 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.

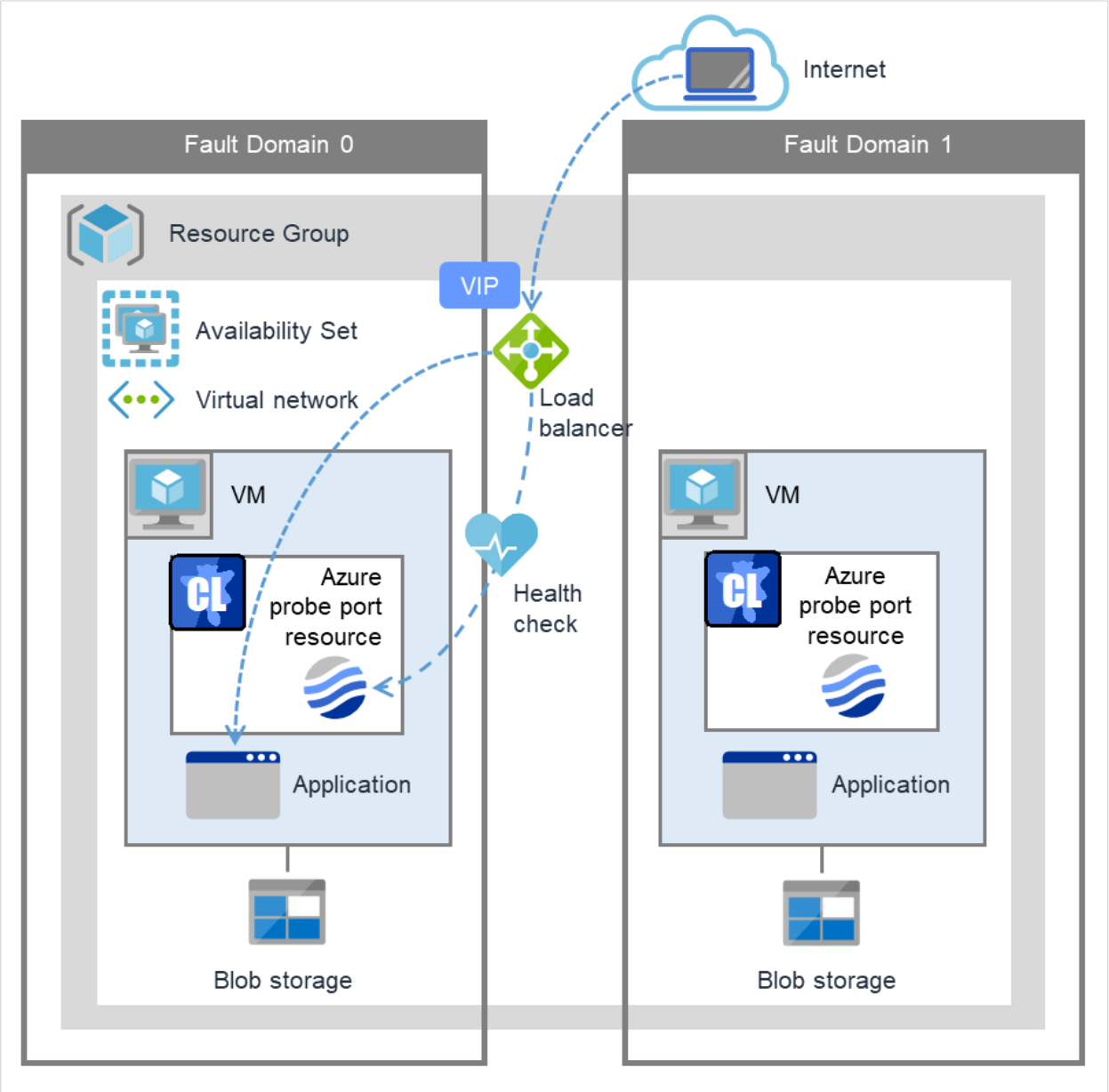


Fig. 3.113: Configuration with an Azure probe port resource

To access the cluster created on the Microsoft Azure environment, 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 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 Microsoft 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.

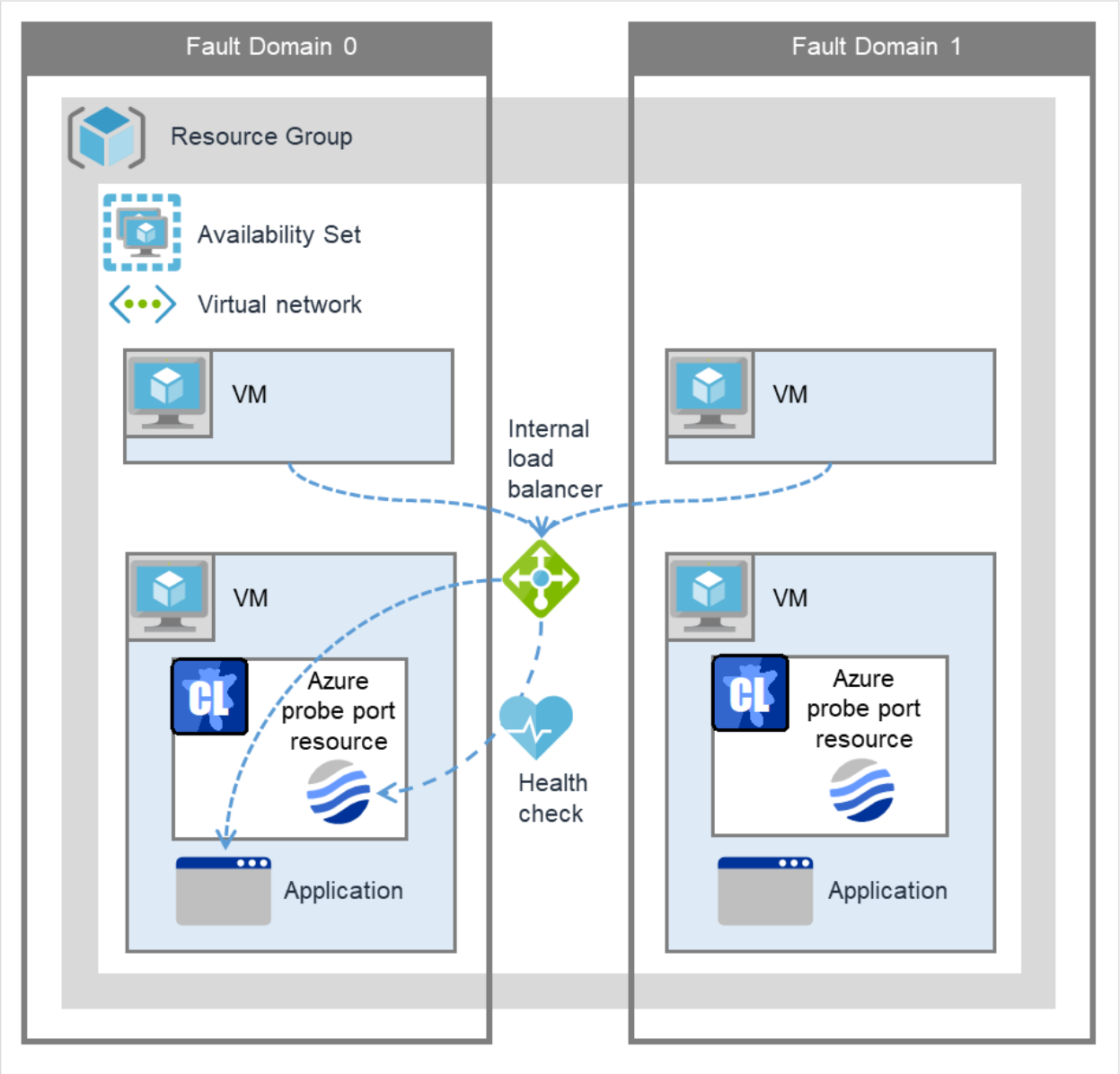
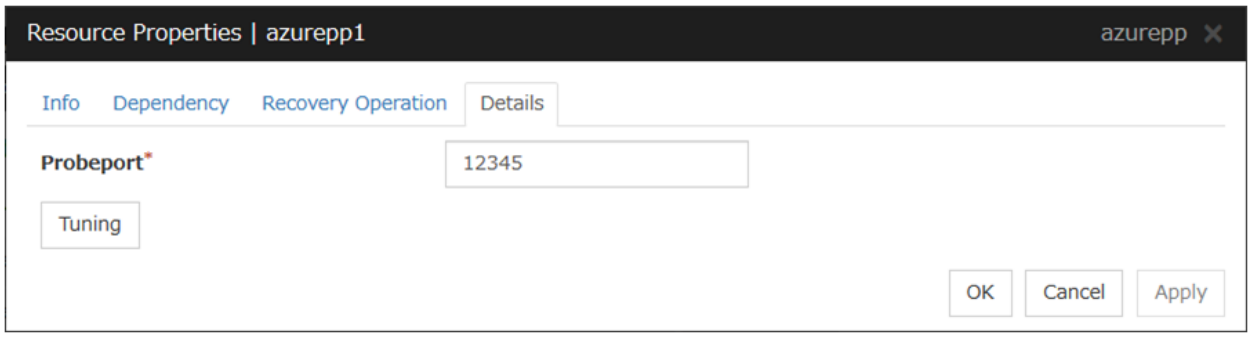


Fig. 3.114: Configuration with an Azure probe port resource (for Internal Load Balancing)

3.22.3 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.
- See " Setting up Azure probe port resources" in " Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.22.4 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.

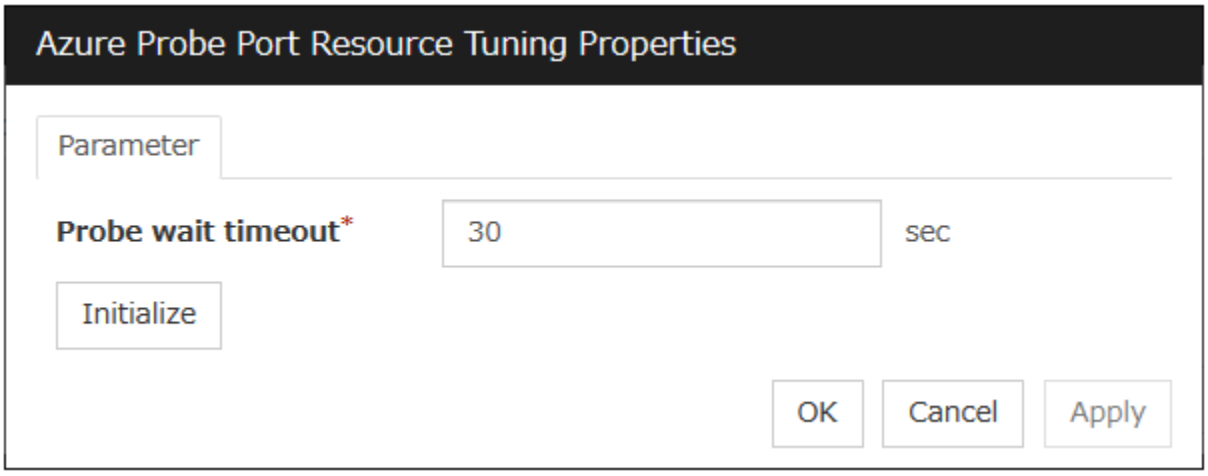
Tuning

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

Detailed setting for parameter is displayed.



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.

3.23 Understanding Azure DNS resources

3.23.1 Dependencies of Azure DNS resources

By default, this function does not depend on any group resource type.

3.23.2 Azure DNS resource

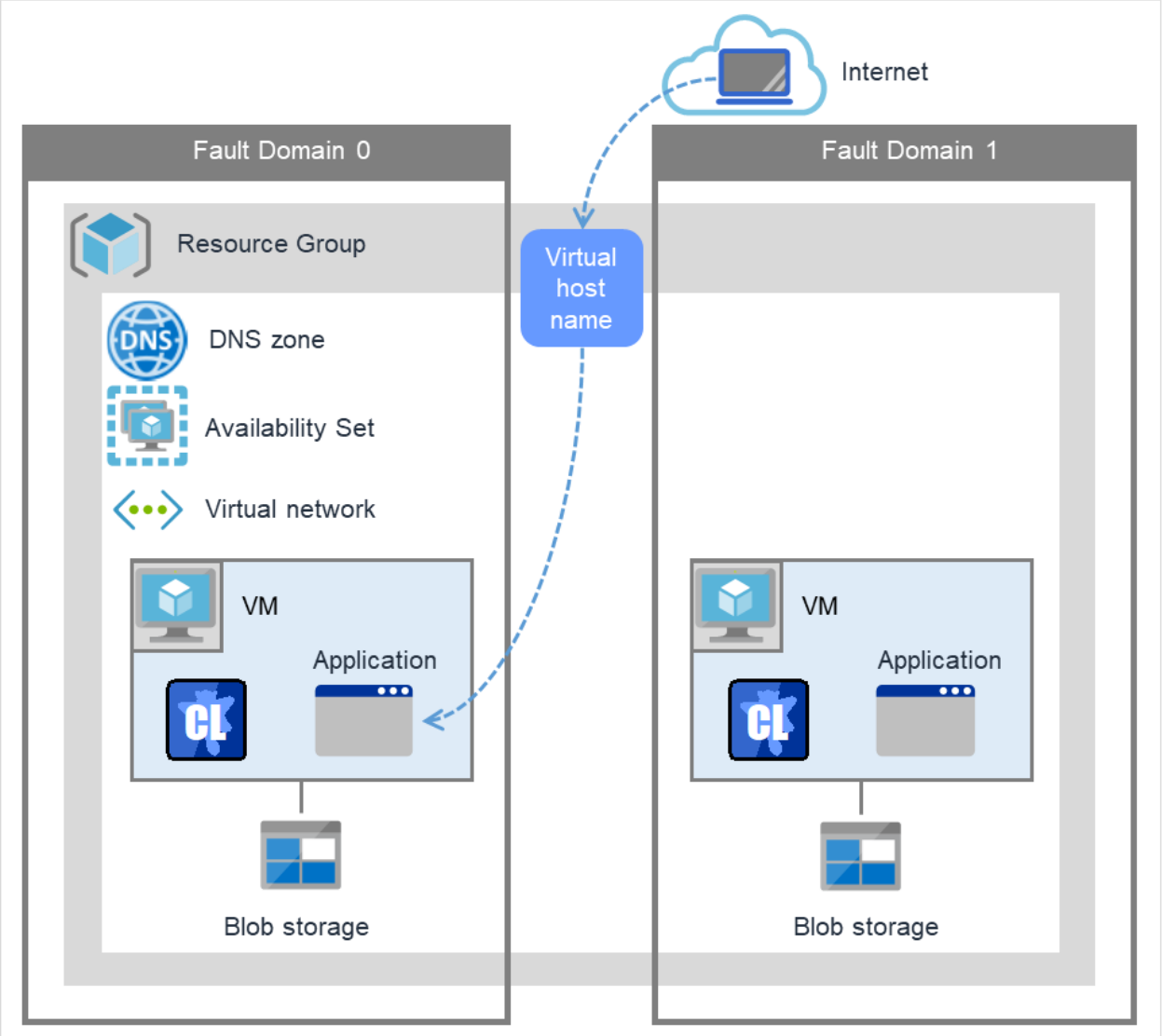


Fig. 3.115: Configuration with an Azure DNS resource

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.

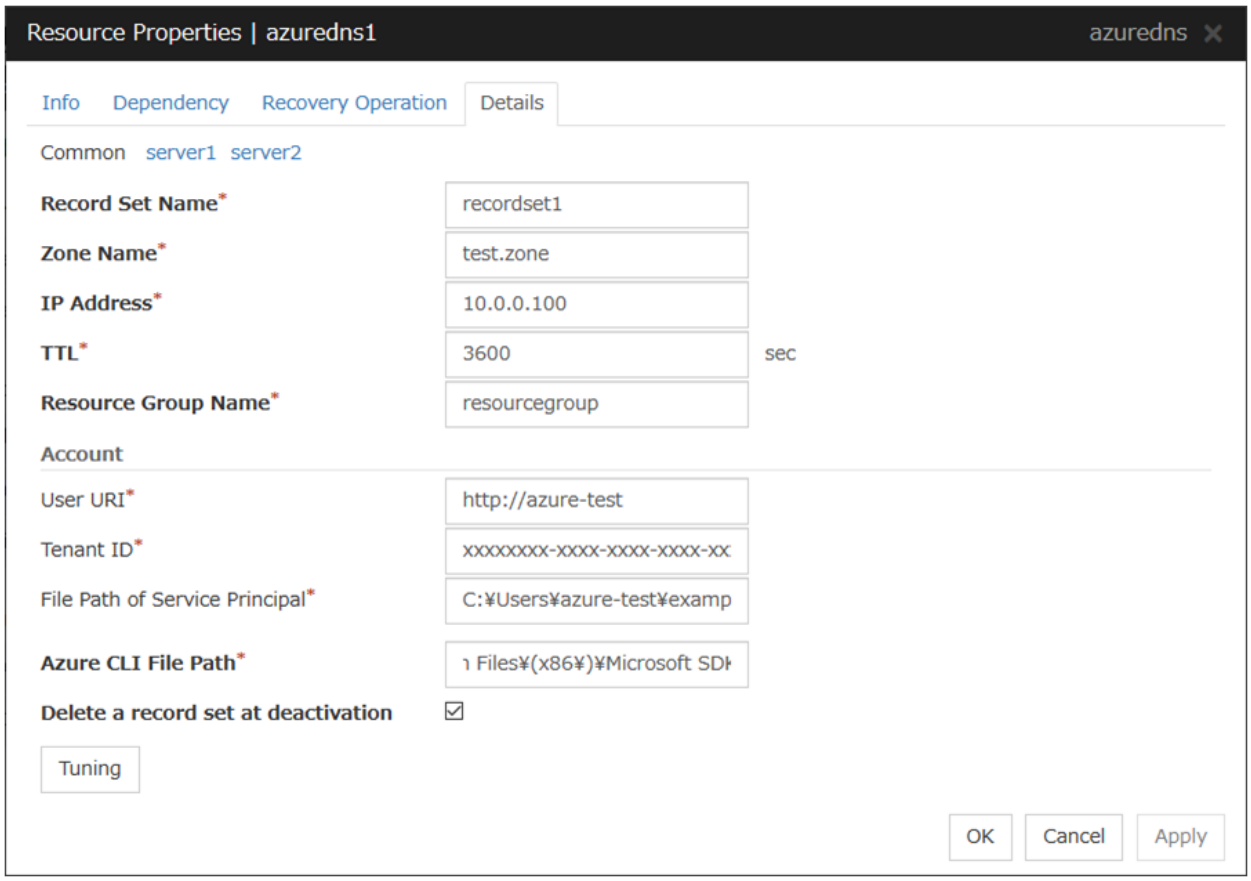
If using Azure DNS resources, you need to take the following preparations before establishing a cluster. For details, see " EXPRESSCLUSTER X HA Cluster Configuration Guide for Microsoft Azure (Windows)".

- Creating Microsoft Azure Resource Group and DNS zone
- Installing Azure CLI

3.23.3 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 "Before installing EXPRESSCLUSTER" in "Notes and Restrictions" in the "Getting Started Guide".
- See "Azure DNS resources" in " Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

3.23.4 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)

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 a time-to-live (TTL) for the DNS service 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 full path (including the drive letter) to the file of a service principal (certificate) to log in to Microsoft Azure.

Azure CLI File Path (Within 1023 bytes)

Specify the installation path of Azure CLI and the file name. Use a full path containing a drive name to specify them.

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.

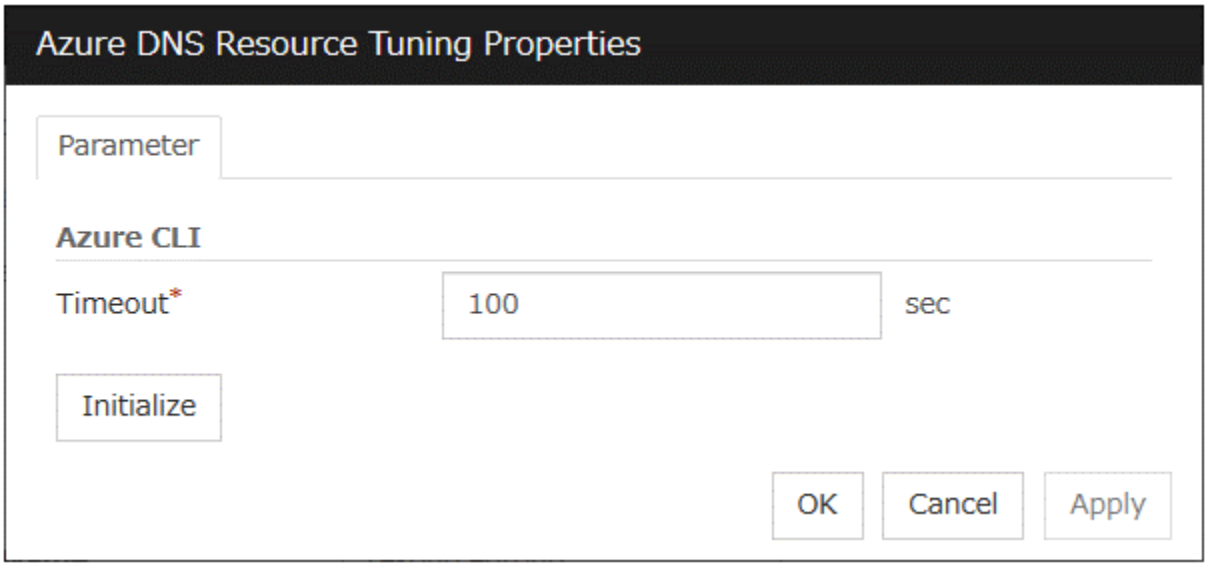
Tuning

Opens the **Azure DNS Resource Tuning Properties** dialog box where you can make detailed settings for the Azure DNS resource.

Azure DNS Resource Tuning Properties

Parameter tab

Detailed setting for parameter is displayed.



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.

3.24 Understanding Google Cloud virtual IP resources

3.24.1 Dependencies of Google Cloud virtual IP resources

By default, this function does not depend on any group resource type.

3.24.2 What is a Google Cloud virtual IP resource?

For virtual machines in the Google Cloud 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.

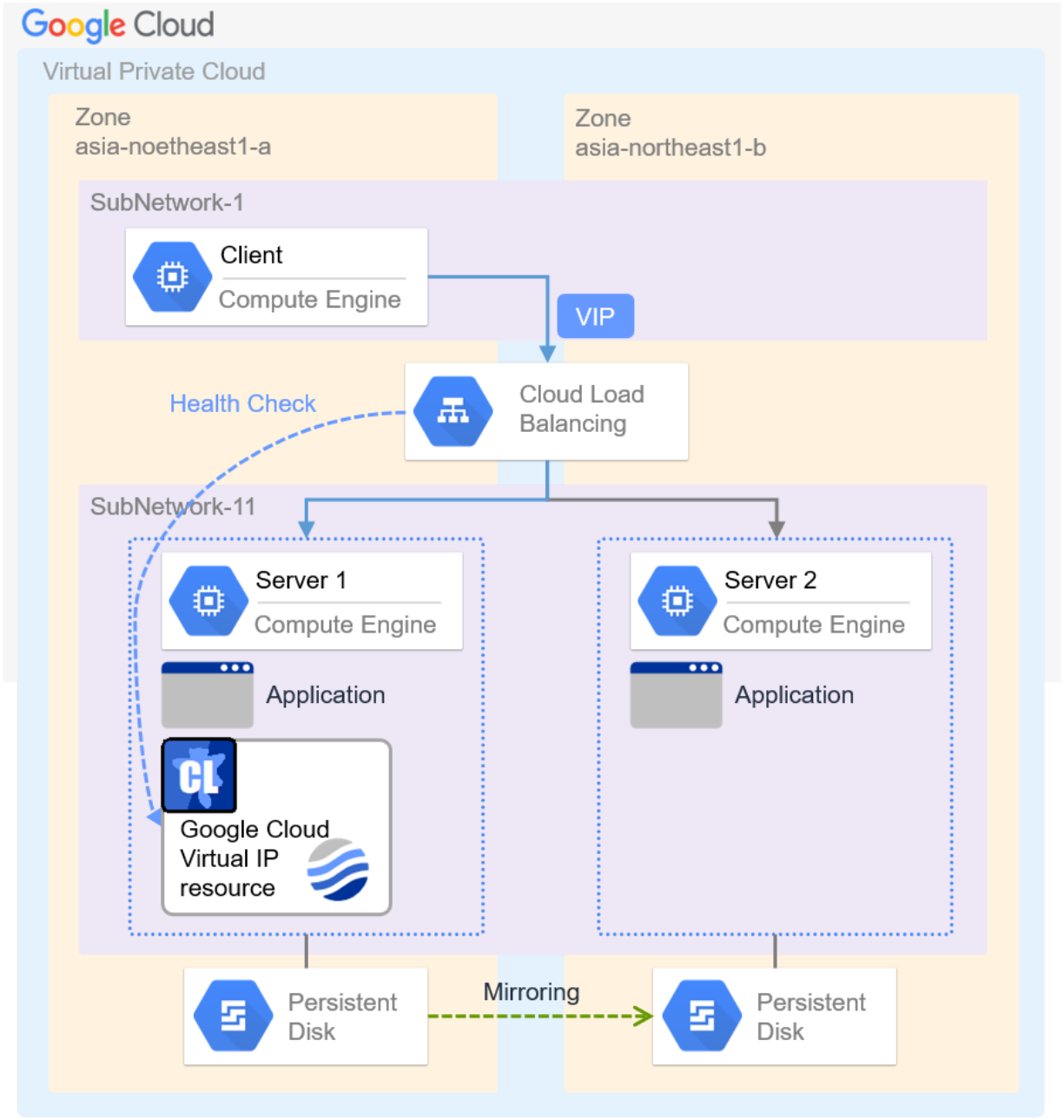


Fig. 3.116: Configuration with a Google Cloud Virtual IP resource

To access the cluster created in the Google Cloud 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 (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, and open the port specified in **Port Number**.

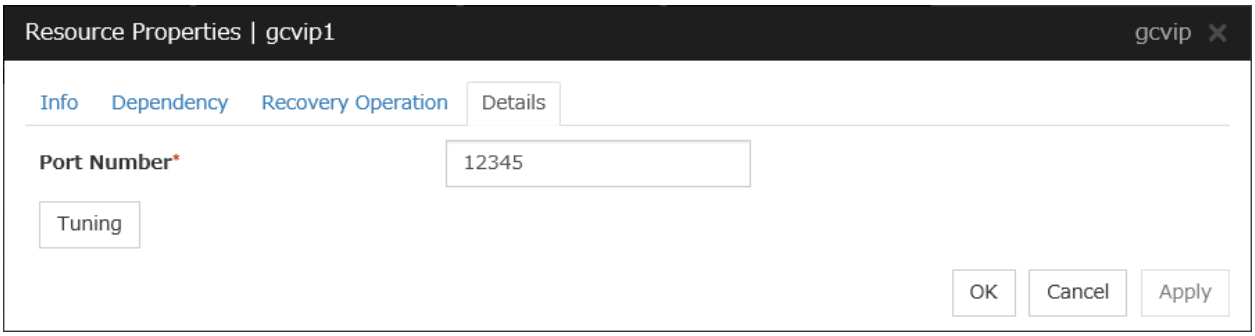
At deactivation, stop the control process for awaiting the health check, and close the port specified in **Port Number**.

Google Cloud virtual IP resources support the internal load balancing of Google Cloud.

3.24.3 Notes on Google Cloud virtual IP resources

- According to the Google Cloud 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 the cluster configuration data" -> "Setting up Google Cloud Virtual IP resources".

3.24.4 Details tab



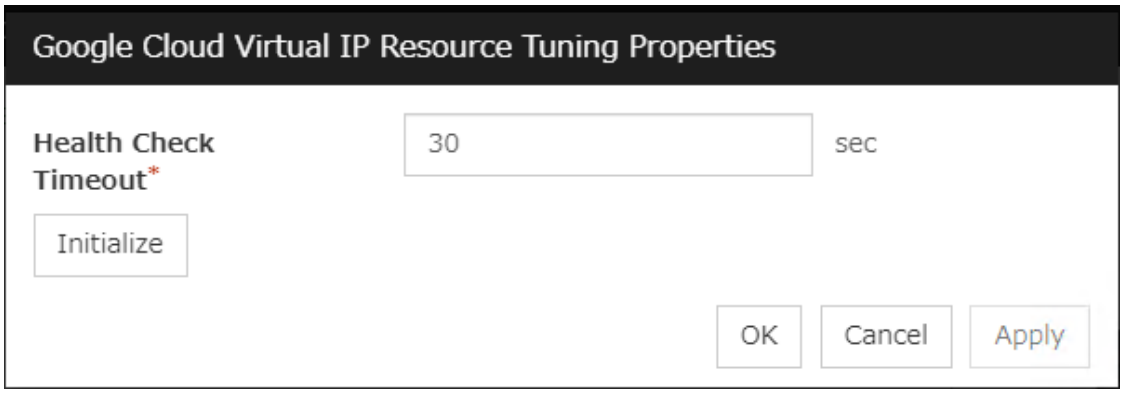
Port Number (1 to 65535)

Specify a port number to be used by the load balancer of Google Cloud 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)

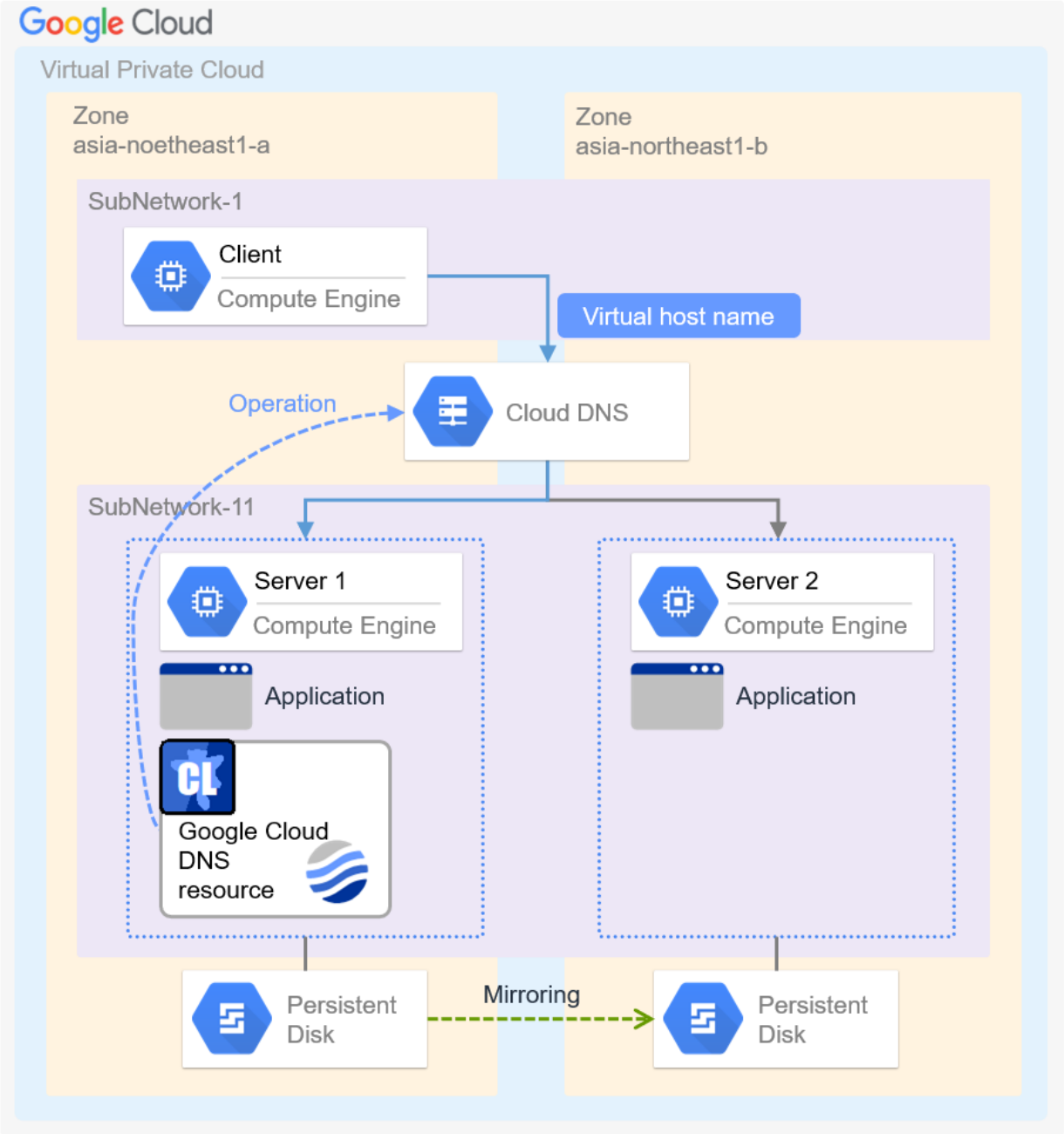
Specify a timeout value for awaiting a health check from the load balancer of Google Cloud, in order to check whether the load balancer periodically performs health checks.

3.25 Understanding Google Cloud DNS resources

3.25.1 Dependencies of Google Cloud DNS resources

By default, this function does not depend on any group resource type.

3.25.2 What is an Google Cloud DNS resource?



A Google Cloud DNS resource controls a Google Cloud DNS record set and DNS A record to obtain an IP address set from the virtual host name (DNS name).

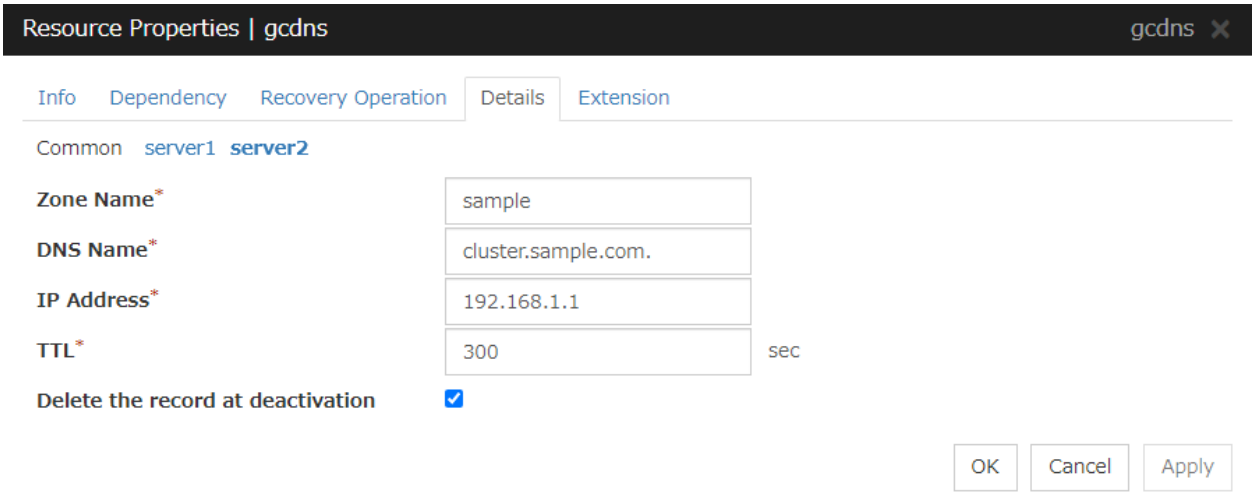
A client can access the node on which failover groups are active with the virtual host name.

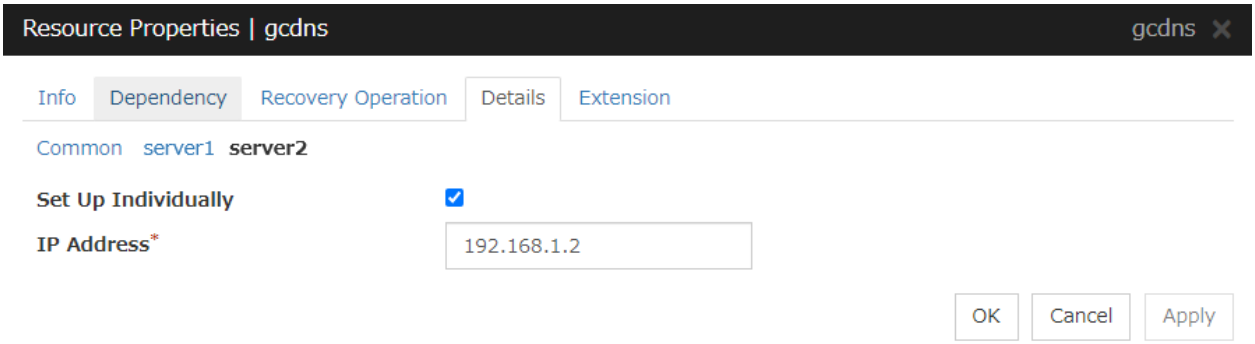
By using Google Cloud DNS resources, clients do not need to be aware of switching access destination node on Google Cloud DNS when a failover occurs or moving a group migration.

3.25.3 Notes on Google Cloud DNS resources

- See "Setting up Google Cloud DNS resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- See "Google Cloud DNS resources" in " Before installing EXPRESSCLUSTER" in "Notes and Restrictions" in the "Getting Started Guide".

3.25.4 Details tab





Zone Name (within 63 bytes)

Specify the name of the DNS zone to which the record set of Google Cloud DNS belongs.

DNS Name (within 253 bytes)

Specify the A record DNS name to be registered in Google Cloud DNS.

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 a time-to-live (TTL) for the DNS service cache.

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.

3.26 Understanding Oracle Cloud virtual IP resources

3.26.1 Dependencies of Oracle Cloud virtual IP resources

By default, this function does not depend on any group resource type.

3.26.2 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.

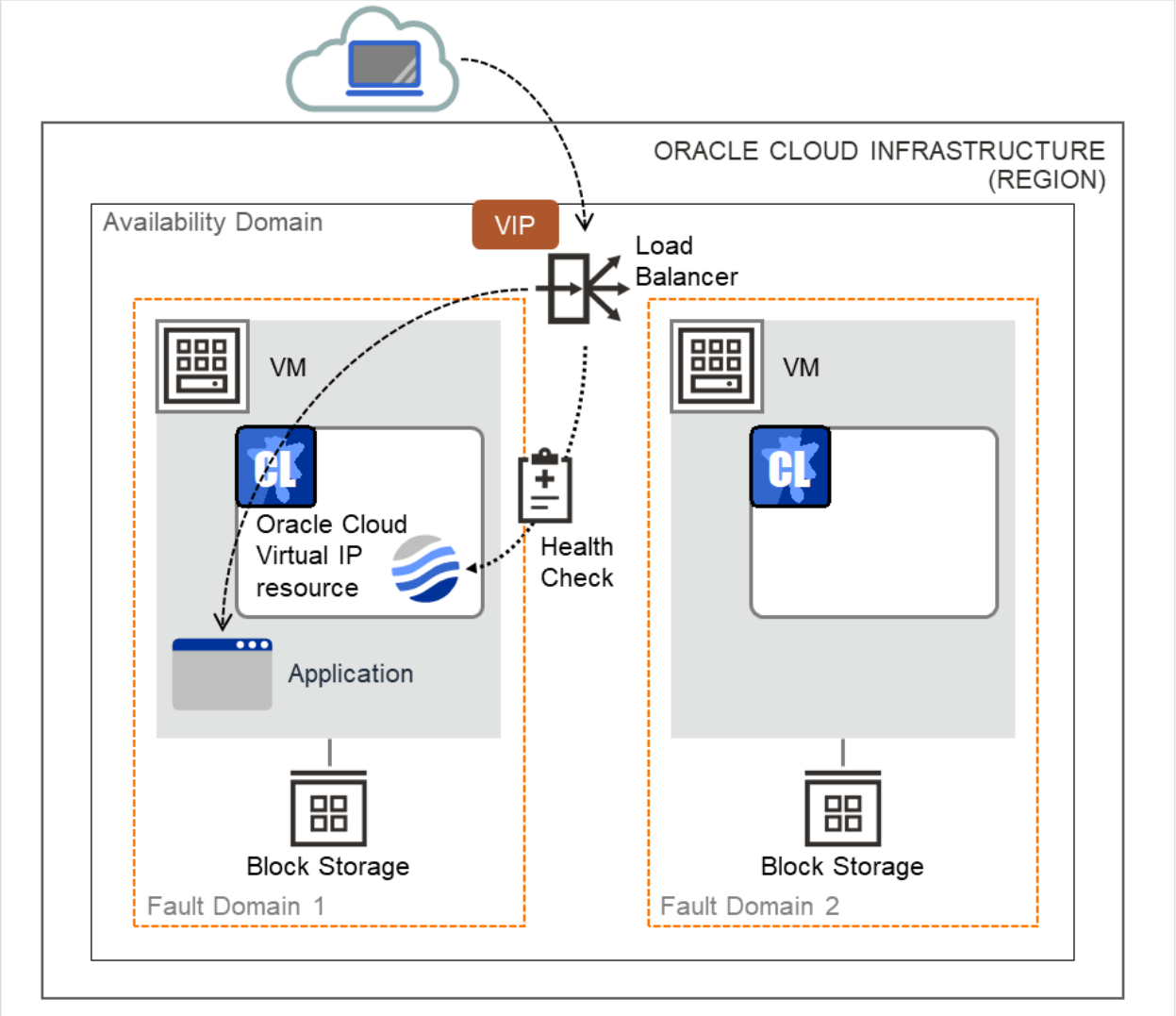


Fig. 3.117: Configuration with an Oracle Cloud Virtual IP resource

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.

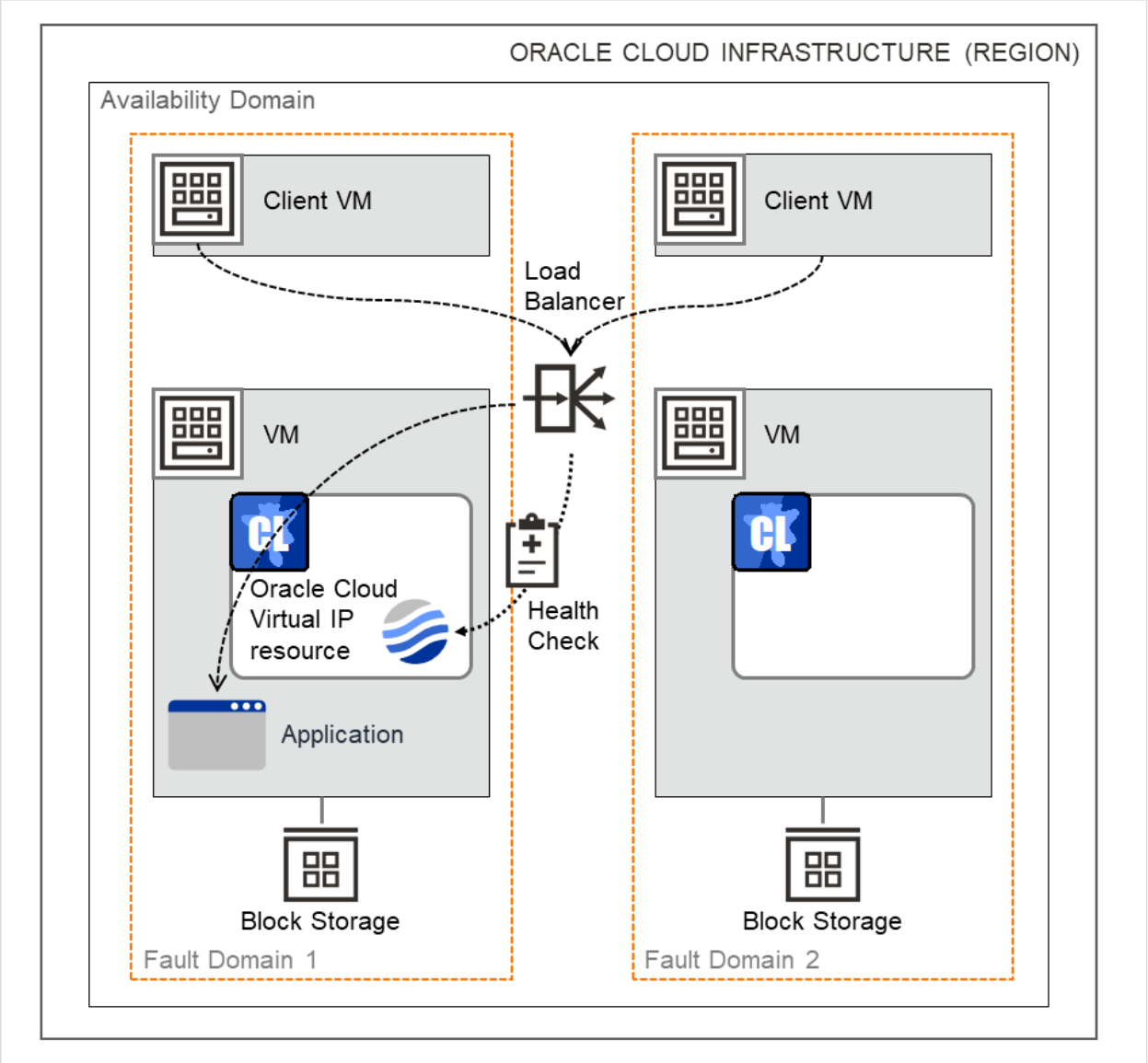
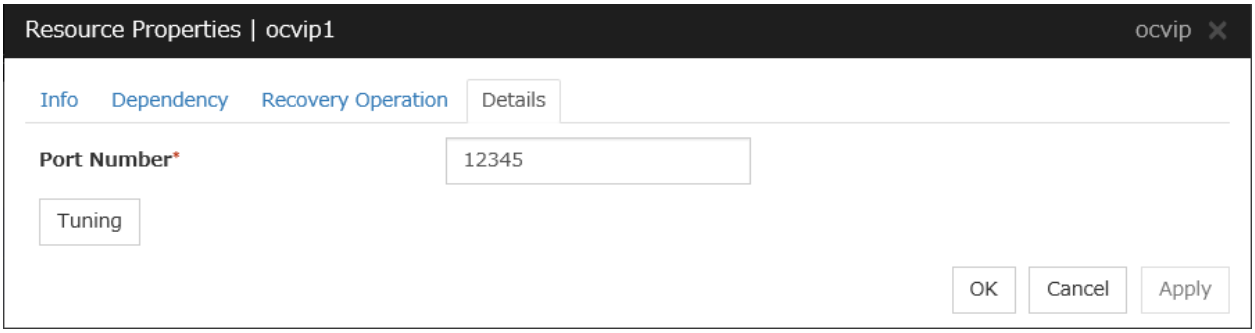


Fig. 3.118: Configuration with an Oracle Cloud Virtual IP resource (for a private load balancer)

3.26.3 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 the cluster configuration data" -> "Setting up Oracle Cloud Virtual IP resources".

3.26.4 Details tab



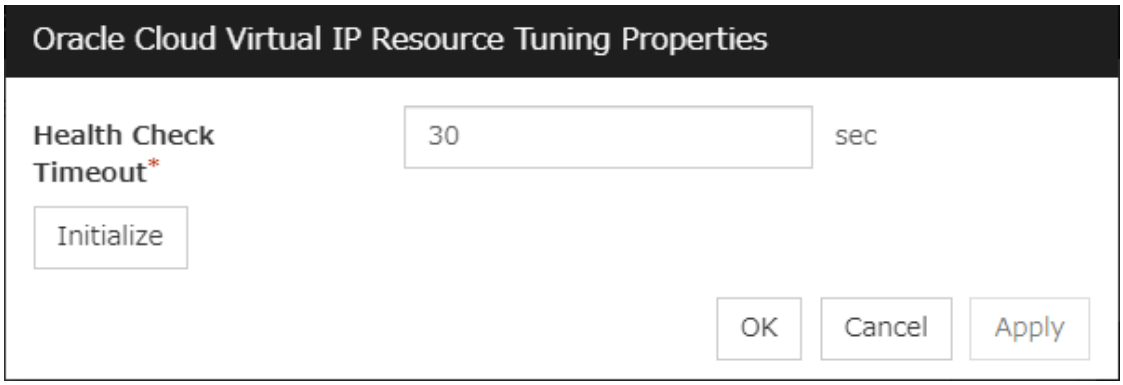
Port Number (1 to 65535)

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.

3.27 Understanding Oracle Cloud DNS resources

3.27.1 Dependencies of Oracle Cloud DNS resources

By default, this function does not depend on any group resource type.

3.27.2 What is an Oracle Cloud DNS resource?

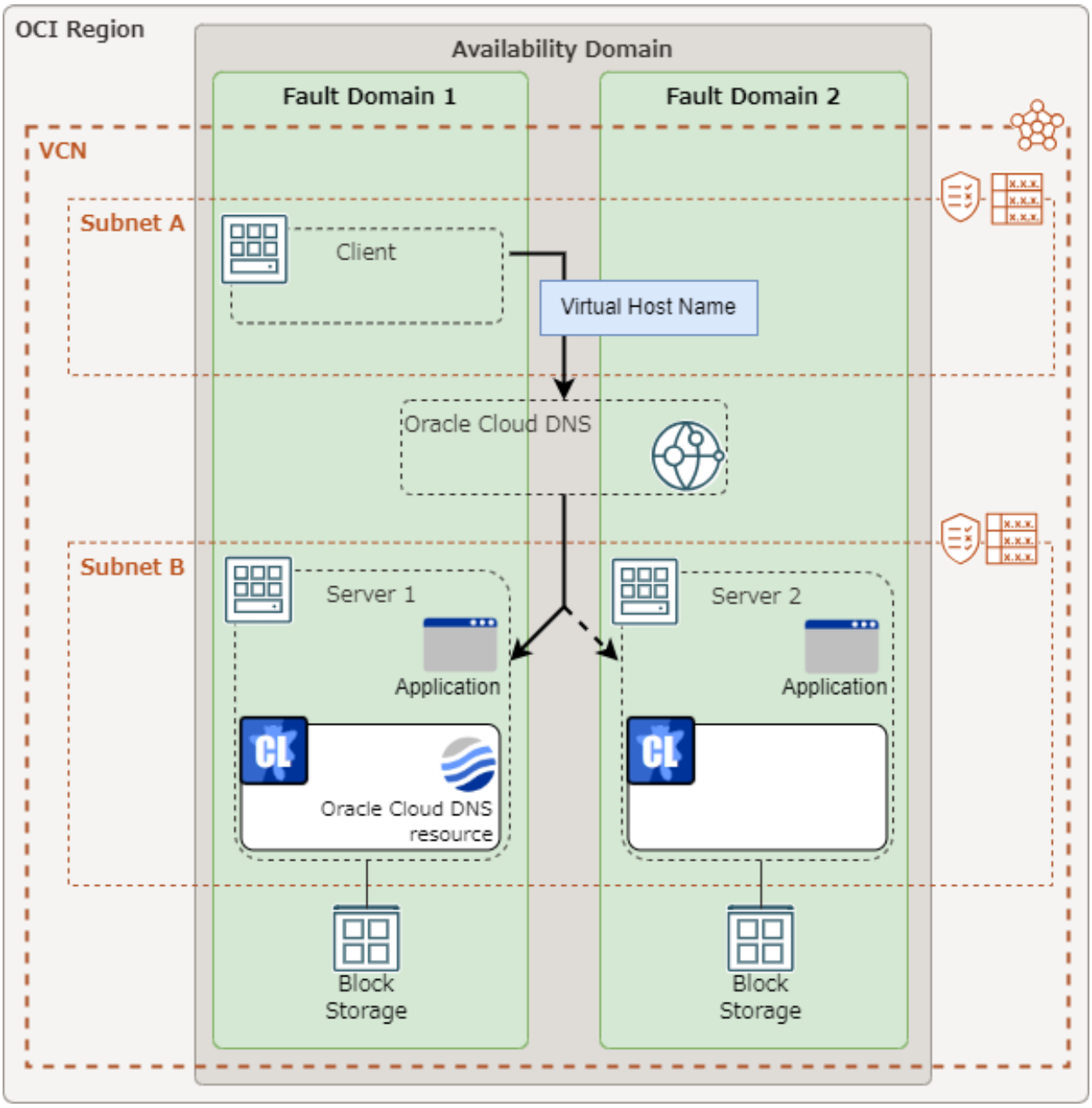


Fig. 3.119: Configuration with an Oracle Cloud DNS resource in a mono-region environment

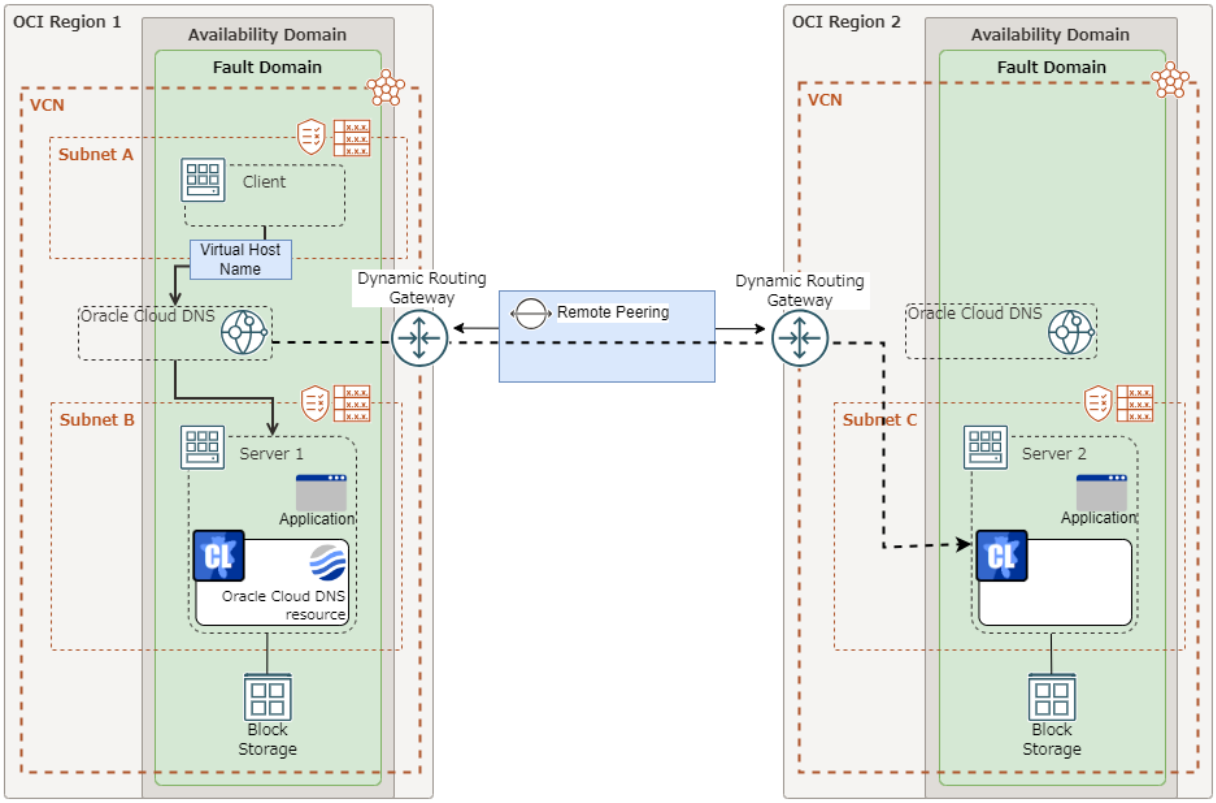


Fig. 3.120: Configuration with an Oracle Cloud DNS resource in a multi-region environment

A Oracle Cloud DNS resource controls a Oracle Cloud DNS record set and DNS A record to obtain an IP address set from the virtual host name (DNS name).

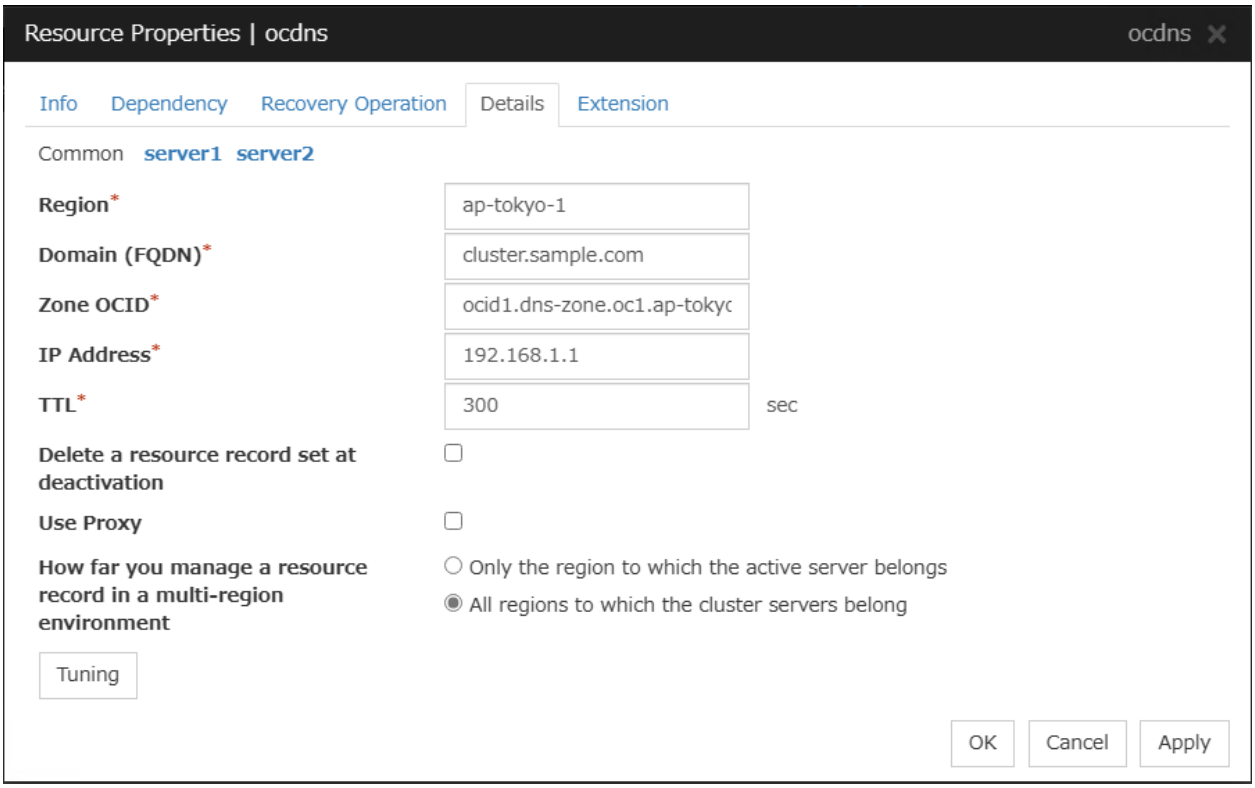
A client can access the node on which failover groups are active with the virtual host name.

By using Oracle Cloud DNS resources, clients do not need to be aware of switching access destination node on Oracle Cloud DNS when a failover occurs or moving a group migration.

3.27.3 Notes on Oracle Cloud DNS resources

- See "Setting up Oracle Cloud DNS resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- See "CLI setting in the OCI environment" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- See "Policy setting in the OCI environment" in " Before installing EXPRESSCLUSTER" in "Notes and Restrictions" in the "Getting Started Guide".

3.27.4 Details tab



Region (within 48 bytes) `Server Individual Setup`

Enter the identifier of a region to which a server belong. For a multi-region environment, enter a region identifier in each server tab. If you set this item for each server: In the **Common** tab, enter the identifier of the region to which any of the servers belong; for other servers, set the identifiers separately.

Domain (FQDN) (within 254 bytes)

Enter a domain name (FQDN) to be registered in the Oracle Cloud DNS zone.

Note: For a multi-region environment, enter the same FQDN for all the regions.

Zone OCID (within 255 bytes) `Server Individual Setup`

Enter the OCID associated with the Oracle Cloud DNS zone name. For a multi-region environment, enter the OCID in each server tab. If you set for each server: In the **Common** tab, enter the zone OCID of one of the servers; for other servers, set it separately.

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 (1 to 604800)

Specify a time-to-live (TTL) for the DNS service cache.

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.

Use Proxy

- When the check box is selected:
  Execute the OCI CLI command for activating/deactivating Oracle Cloud DNS resources, by using the proxy information (see this guide -> "*Parameter details*" -> "*Servers Properties*" -> "*Proxy tab*").
- When the check box is not selected (default):
  Execute the OCI CLI command for activating/deactivating Oracle Cloud DNS resources, without using the proxy information (see this guide -> "*Parameter details*" -> "*Servers Properties*" -> "*Proxy tab*").

How far you manage a resource record in a multi-region environment

- Only the region to which the active server belongs:
  Creates, updates, or deletes the A records of Oracle Cloud DNS in the region to which the server (with the failover group operating) belongs.
- All regions to which the cluster servers belong (default):
  Creates, updates, or deletes the A records of Oracle Cloud DNS in the regions to which all the servers registered in the cluster belong.

Note: If you selected **All regions to which the cluster servers belong**

- No activation failure is considered to have occurred even if a processing failure occurs to Oracle Cloud DNS in a region to which servers (without the failover group started) belong.
- In the region, the A records of Oracle Cloud DNS are created or updated at intervals specified in **Interval** of Oracle Cloud DNS monitor resources.

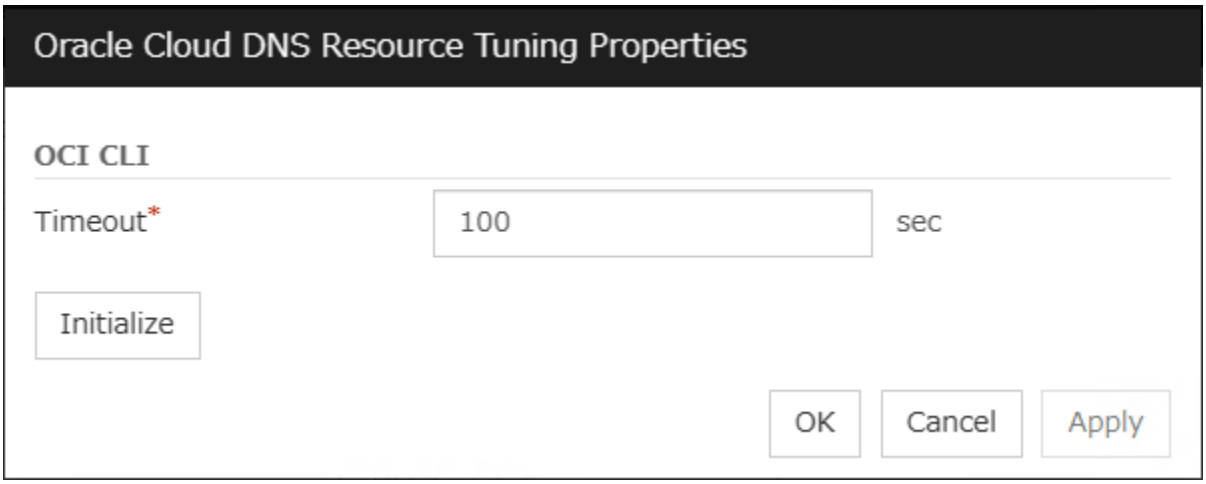
Tuning

Opens the **Oracle Cloud DNS Resource Tuning Properties** dialog box where you can make detailed settings for the Oracle Cloud DNS resource.

Oracle Cloud DNS Resource Tuning Properties

Parameter tab

Detailed setting for parameter is displayed.



Timeout (1 to 999)

Make the setting of the timeout of the OCI CLI command executed for the activation and/or deactivation of the Oracle Cloud DNS resource.

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 resources

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 resource are as follows:

Monitor resource name	Abbreviation	Functional overview
Application monitor resources	appliw	Refer to "*Understanding application monitor resources*".
Disk RW monitor resources	diskw	Refer to "*Understanding disk RW monitor resources*".
Floating IP monitor resources	fipw	Refer to "*Understanding floating IP monitor resources*".
IP monitor resources	ipw	Refer to "*Understanding IP monitor resources*".
Mirror disk monitor resources	mdw	Refer to "*Understanding mirror disk monitor resources*".
NIC Link Up/Down monitor resources	miiw	Refer to "*Understanding NIC link up/down monitor resources*".
Multi target monitor resources	mtw	Refer to "*Understanding multi target monitor resources*".
Registry synchronization monitor resources	regsyncw	Refer to "*Understanding registry synchronization monitor resources*".
Disk TUR monitor resources	sdw	Refer to "*Understanding disk TUR monitor resources*".
Service monitor resources	servicew	Refer to "*Understanding service monitor resources*".
Virtual computer name monitor resources	vcomw	Refer to "*Understanding virtual computer name monitor resources*".
Dynamic DNS monitor resources	ddnsw	Refer to "*Understanding dynamic DNS monitor resources*".
Virtual IP monitor resources	vipw	Refer to "*Understanding virtual IP monitor resources*".
CIFS monitor resources	cifsw	Refer to "*Understanding CIFS monitor resources*".
Hybrid disk monitor resources	hdw	Refer to "*Understanding hybrid disk monitor resources*".
Hybrid disk TUR monitor resources	hdtw	Refer to "*Understanding hybrid disk TUR monitor resources*".
Custom monitor resources	genw	Refer to "*Understanding custom monitor resources* ".
Message receive monitor resources	mrw	Refer to "*Understanding message receive monitor resources*".
Process name monitor resources	psw	Refer to "*Understanding process name monitor resources*".
DB2 monitor resources	db2w	Refer to "*Understanding DB2 monitor resources*".
FTP monitor resources	ftpw	Refer to "*Understanding FTP monitor resources* ".
HTTP monitor resources	httpw	Refer to "*Understanding HTTP monitor resources*".

Continued on next page

Table 4.1 – continued from previous page

Monitor resource name	Abbreviation	Functional overview
IMAP4 monitor resources	imap4w	Refer to "*Understanding IMAP4 monitor resources*".
ODBC monitor resources	odbcw	Refer to "*Understanding ODBC monitor resources*".
Oracle monitor resources	oraclew	Refer to "*Understanding Oracle monitor resources*".
POP3 monitor resources	pop3w	Refer to "*Understanding POP3 monitor resources*".
PostgreSQL monitor resources	psqlw	Refer to "*Understanding PostgreSQL monitor resources*".
SMTP monitor resources	smtpw	Refer to "*Understanding SMTP monitor resources*".
SQL Server monitor resources	sqlserverw	Refer to "*Understanding SQL Server monitor resources*".
Tuxedo monitor resources	tuxw	Refer to "*Understanding Tuxedo monitor resources*".
WebSphere monitor resources	wasw	Refer to "*Understanding WebSphere monitor resources*".
WebLogic monitor resources	wlsw	Refer to "*Understanding WebLogic monitor resources*".
WebOTX monitor resources	otxw	Refer to "*Understanding WebOTX monitor resources*".
JVM monitor resources	jraw	Refer to "*Understanding JVM monitor resources*".
Process resource monitor resources	psrw	Refer to "*Understanding process resource monitor resources*".
System monitor resources	sraw	Refer to "*Understanding system monitor resources*".
User mode monitor resources	userw	Refer to "*Understanding user mode monitor resources*".
AWS elastic ip monitor resources	awseipw	Refer to "*Understanding AWS elastic ip monitor resources*".
AWS virtual ip monitor resources	awsvipw	Refer to "*Understanding AWS virtual ip monitor resources*".
AWS secondary ip monitor resources	awssipw	Refer to "*Understanding AWS secondary ip monitor resources*".
AWS AZ monitor resources	awsazw	Refer to "*Understanding AWS AZ monitor resources*".
AWS DNS monitor resources	awsdnsw	Refer to "*Understanding AWS DNS monitor resources*".
Azure probe port monitor resources	azureppw	Refer to "*Understanding Azure probe port monitor resources*".
Azure load balance monitor resources	azurelbw	Refer to "*Understanding Azure load balance monitor resources*".
Azure DNS monitor resources	azurednsw	Refer to "*Understanding Azure DNS monitor resources*".
Google Cloud Virtual IP monitor resources	gcvipw	Refer to "*Understanding Google Cloud Virtual IP monitor resources*".
Google Cloud load balance monitor resources	gclbw	Refer to "*Understanding Google Cloud load balance monitor resources*".

Continued on next page

Table 4.1 – continued from previous page

Monitor resource name	Abbreviation	Functional overview
Google Cloud DNS monitor resources	gcdnsw	Refer to "*Understanding Google Cloud DNS monitor resources*".
Oracle Cloud Virtual IP monitor resources	ocvipw	Refer to "*Understanding Oracle Cloud Virtual IP monitor resources*".
Oracle Cloud load balance monitor resources	oclbw	Refer to "*Understanding Oracle Cloud load balance monitor resources*".
Oracle Cloud DNS monitor resources	ocdnsw	Refer to "*Understanding Oracle Cloud DNS monitor resources*".

4.1.1 Monitor timing of monitor resources

Monitoring by monitor resources are done in one of two ways: monitoring the target all the time or monitoring the target when it is activated.

Depending on the monitor resource, the configurable monitoring timing varies.

a) Always:
Monitoring is performed by the monitor resource all the time.

b) Active:
Monitoring is performed by the monitor resource while a specified group resource is active. The monitor resource does not monitor while the group resource is not activated.

(1) Cluster startup

(2) Group activation

(3) Group deactivation

(4) Cluster stop

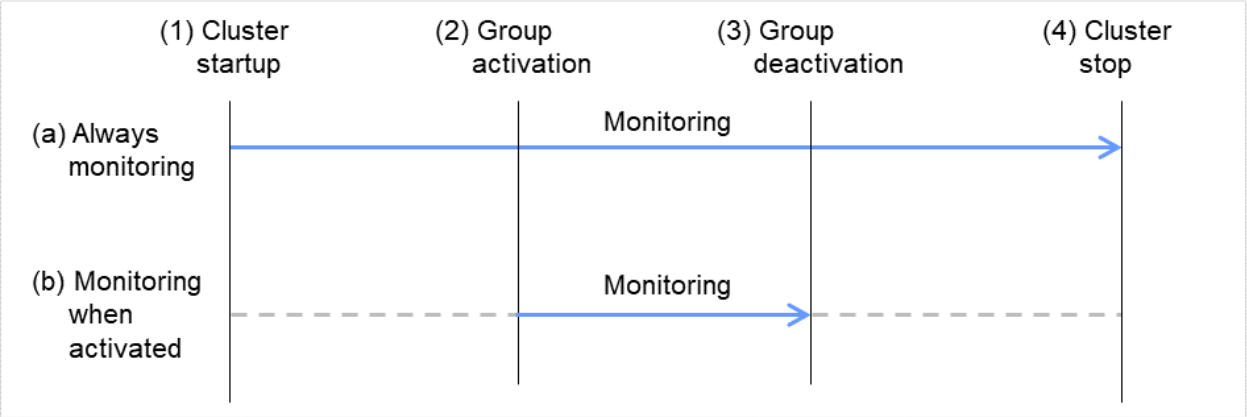


Fig. 4.1: Two types of monitoring by monitor resources: **Always** and **Active**

The initial settings for monitoring timings of each monitor resource are shown below.

The default settings are as follows.

Always monitor (From the cluster startup to the cluster stop)

- IP monitor resources
- Mirror disk monitor resources
- Hybrid disk monitor resources
- Hybrid disk TUR monitor resources
- NIC Link Up/Down monitor resources
- Disk TUR monitor resources
- Custom monitor resources
- Message receive monitor resources
- Process name monitor resources
- System monitor resources
- Process resource monitor resources
- User mode monitor resources
- AWS AZ monitor resources
- Azure load balance monitor resources
- Google Cloud load balance monitor resources
- Oracle Cloud load balance monitor resources

Monitor while a group is activated (from activation to deactivation of the group)

- Application monitor resources
- Disk RW monitor resources
- Floating IP monitor resources
- Multi target monitor resources
- Registry synchronization monitor resources
- Service monitor resources
- Virtual computer name monitor resources
- Dynamic DNS monitor resources
- Virtual IP monitor resources
- CIFS monitor resources
- DB2 monitor resources
- FTP monitor resources
- HTTP monitor resources
- IMAP4 monitor resources
- ODBC monitor resources
- Oracle monitor resources
- POP3 monitor resources
- PostgreSQL monitor resources

- SMTP monitor resources
- SQL Server monitor resources
- Tuxedo monitor resources
- WebSphere monitor resources
- WebLogic monitor resources
- WebOTX monitor resources
- JVM monitor resources
- AWS elastic ip monitor resources
- AWS virtual ip monitor resources
- AWS secondary ip monitor resources
- AWS DNS monitor resources
- Azure probe port monitor resources
- Azure DNS monitor resources
- Google Cloud Virtual IP monitor resources
- Google Cloud DNS monitor resources
- Oracle Cloud Virtual IP monitor resources
- Oracle Cloud DNS monitor resources

Monitor resource	Monitor timing	Target resource
Application monitor resources	When activated (Fixed)	appli
Disk RW monitor resources	Always or when activated	All resources
Floating IP monitor resources	When activated (Fixed)	fip
IP monitor resources	Always or when activated	All resources
Mirror disk monitor resources	Always (Fixed)	-
NIC link up/down monitor resources	Always or when activated	All resources
Multi target monitor resources	Always or when activated	All resources
Registry synchronization monitor resources	When activated (Fixed)	regsync
Disk TUR monitor resources	Always or when activated	sd
Service monitor resources	Always or when activated	All resources
Virtual computer name monitor resources	When activated (Fixed)	vcom
Dynamic DNS monitor resources	When activated (Fixed)	ddns
Virtual IP monitor resources	When activated (Fixed)	vip
CIFS monitor resources	When activated (Fixed)	cifs
Hybrid disk monitor resources	Always (Fixed)	-
Hybrid disk TUR monitor resources	Always or when activated	Hd
Custom monitor resources	Always or when activated	All resources
Message receive monitor resources	Always (Fixed)	-
Process name monitor resources	Always or when activated	All resources
DB2 monitor resources	When activated (Fixed)	All resources
FTP monitor resources	When activated (Fixed)	All resources
HTTP monitor resources	When activated (Fixed)	All resources
IMAP4 monitor resources	When activated (Fixed)	All resources
ODBC monitor resources	When activated (Fixed)	All resources
Oracle monitor resources	When activated (Fixed)	All resources

Continued on next page

Table 4.2 – continued from previous page

Monitor resource	Monitor timing	Target resource
POP3 monitor resources	When activated (Fixed)	All resources
PostgreSQL monitor resources	When activated (Fixed)	All resources
SMTP monitor resources	When activated (Fixed)	All resources
SQL Server monitor resources	When activated (Fixed)	All resources
Tuxedo monitor resources	When activated (Fixed)	All resources
WebSphere monitor resources	When activated (Fixed)	All resources
WebLogic monitor resources	When activated (Fixed)	All resources
WebOTX monitor resources	When activated (Fixed)	All resources
JVM monitor resources	Always or when activated	All resources
System monitor resources	Always (Fixed)	All resources
Process resource monitor resources	Always (Fixed)	All resources
User mode monitor resources	Always (Fixed)	-
AWS elastic ip monitor resources	When activated (Fixed)	awseip
AWS virtual ip monitor resources	When activated (Fixed)	awsvip
AWS secondary ip monitor resources	When activated (Fixed)	awssip
AWS AZ monitor resources	Always (Fixed)	-
AWS DNS monitor resources	When activated (Fixed)	awsdns
Azure probe port monitor resources	When activated (Fixed)	azurepp
Azure load balance monitor resources	Always (Fixed)	azurepp
Azure DNS monitor resources	When activated (Fixed)	azuredns
Google Cloud Virtual IP monitor resources	When activated (Fixed)	gcvip
Google Cloud load balance monitor resources	Always (Fixed)	gcvip
Google DNS monitor resources	When activated (Fixed)	azuredns
Oracle Cloud Virtual IP monitor resources	When activated (Fixed)	ocvip
Oracle Cloud load balance monitor resources	Always (Fixed)	ocvip
Oracle DNS monitor resources	When activated (Fixed)	azuredns

4.1.2 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 "*9. 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 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

4.1.3 Monitoring interval for monitor resources

All monitor resources monitor their targets at every monitoring interval.

The following describes the timeline of how a monitor resource monitors its target and finds an error with the monitoring interval settings:

When no error is detected

The following figure illustrates monitoring started/resumed after the cluster is started. When the main monitoring process receives the monitoring result, the monitoring is repeatedly started at the monitor intervals.

Examples of behavior when the following values are set:

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 0 time

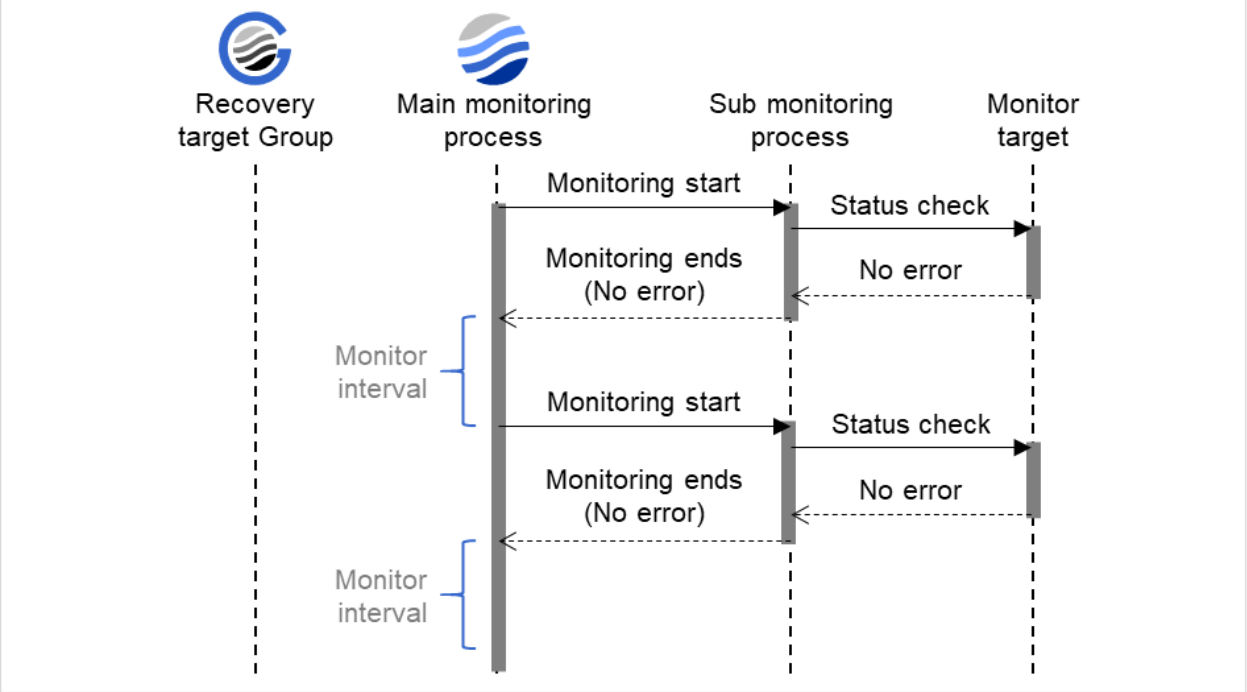


Fig. 4.2: Monitor interval (when no error is detected)

When an error is detected (without monitor retry setting)

The following figure illustrates an error occurring in the monitor target, and the operation after the error is detected. When the main monitoring process receives the monitoring result (error), a failover of the group to be recovered is performed.

When an error occurs, it is detected at the next monitoring and the recovery operation for the recovery target starts.

Examples of behavior when the following values are set:

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry count 0 time

<Error detection>
Recovery Target group
Recovery Script Execution Count 0 time
Maximum Reactivation Count 0 time
Maximum Failover Count 1 time
Final Action None

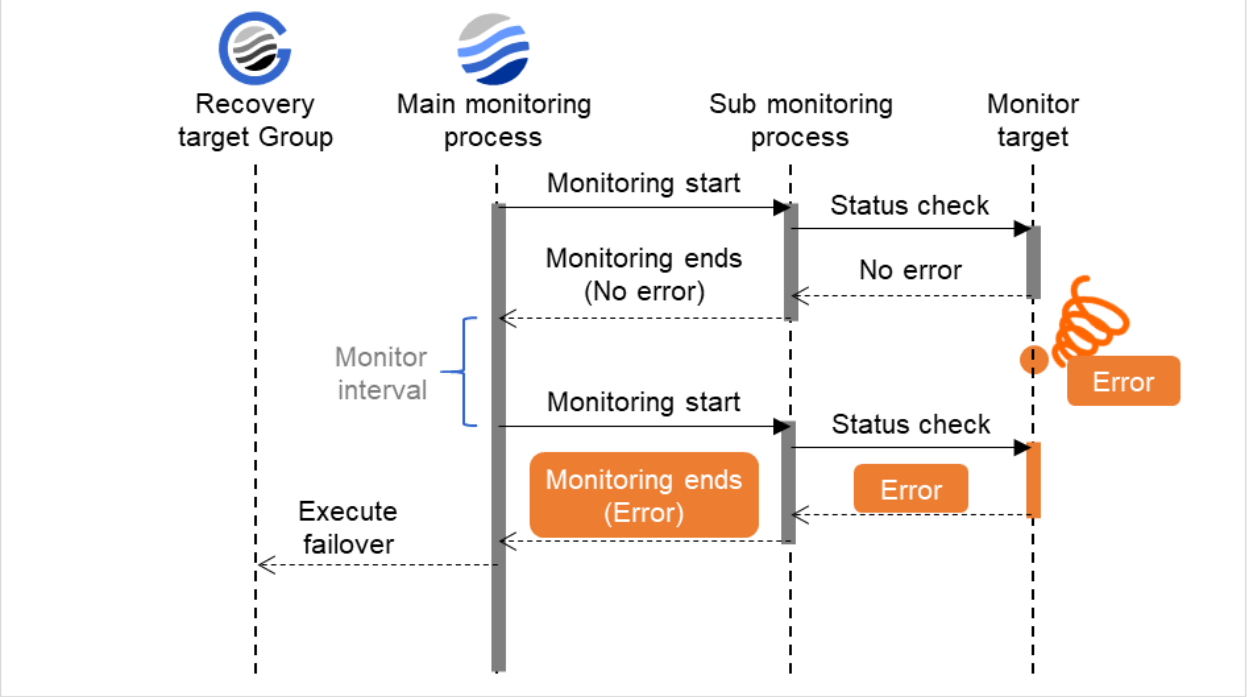


Fig. 4.3: Monitor interval (when an error is detected without monitor retry setting)

When an error is detected (with monitor retry settings)

The following figure illustrates an error occurring in the monitor target, and the operation after the error is detected. When the main monitoring process receives the monitoring result (error), the monitoring continues by its specified

count of retries. If the monitoring target is still not recovered, a failover of the group to be recovered is performed.

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.

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 time
Maximum Reactivation Count 0 time
Maximum Failover Count 1 time
Final Action None

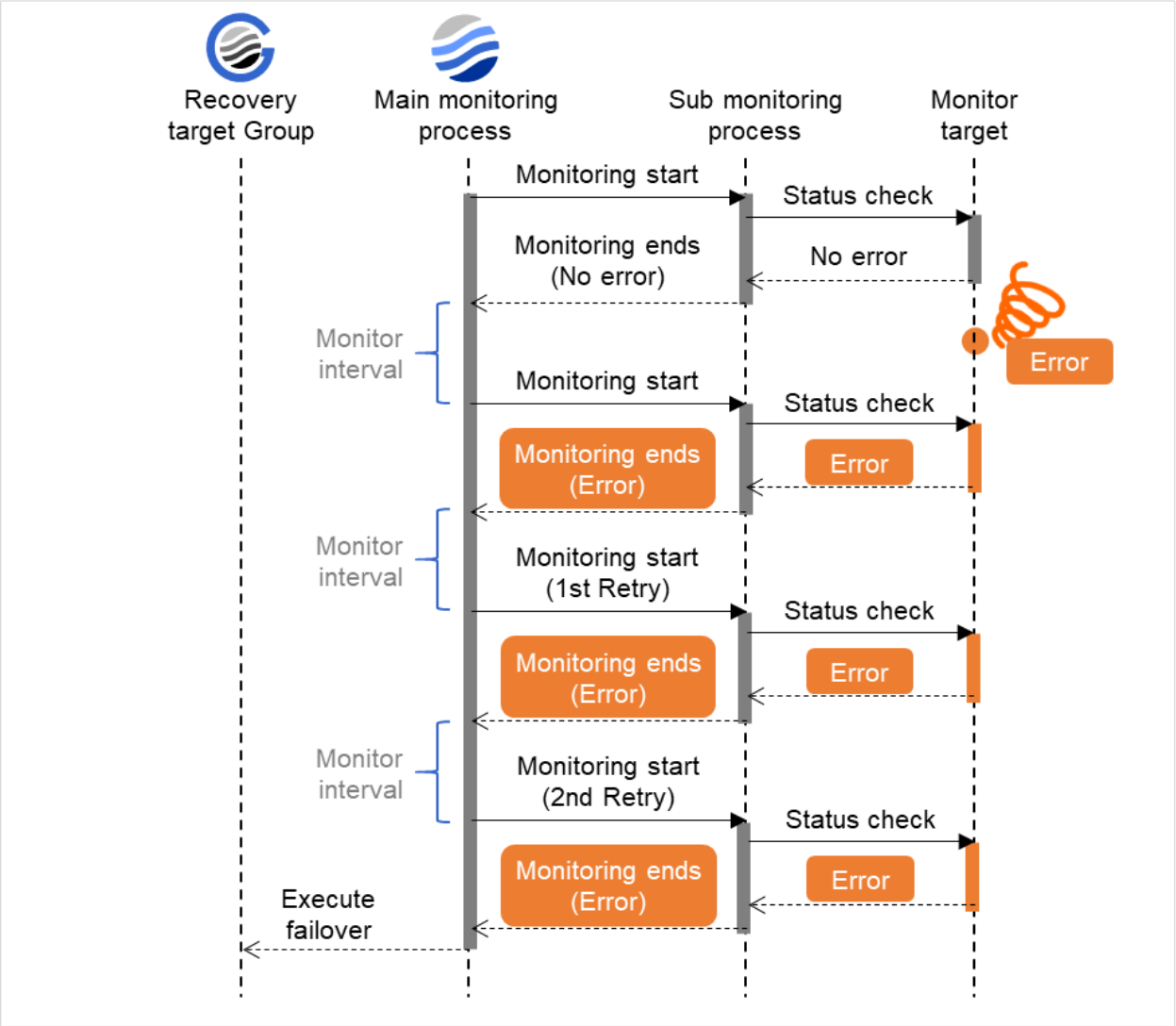


Fig. 4.4: Monitor interval (when an error is detected with monitor retry setting)

When an error is detected (without monitor retry settings)

The following figure illustrates operation in response to a monitoring process unfinished within a specified time. The main monitoring process starts the monitoring. Then, if the monitoring result cannot be obtained within a specified monitoring timeout time, a failover of the group to be recovered is performed.

Immediately after an occurrence of a monitoring timeout, the failover for the recovery target starts.

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 0 time

<Error detection>
Recovery Target group
Recovery Script Execution Count 0 time
Maximum Reactivation Count 0 time
Maximum Failover Count 1 time
Final Action None

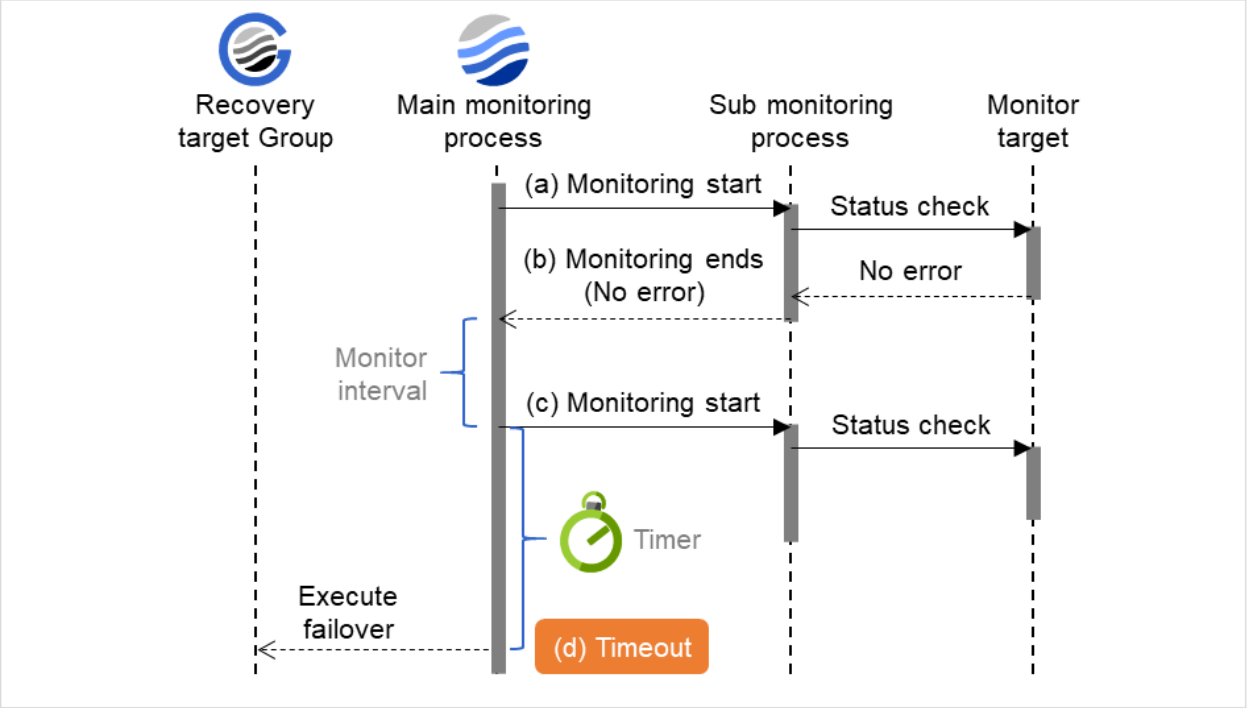


Fig. 4.5: Monitor interval (when a monitoring timeout is detected without monitor retry setting)

When a monitoring timeout is detected (with monitor retry setting)

The following figure illustrates operation in response to a monitoring process unfinished within a specified time. The main monitoring process starts the monitoring. Then, if the monitoring result cannot be obtained within a specified monitoring timeout time, the monitoring continues by its specified count of retries. If the monitoring result still cannot be obtained, a failover of the group to be recovered is performed.

When a monitoring timeout occurs, monitor retry is performed and failover is started for the recovery target.

Examples of behavior when the following values are set:

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 1 times

<Error detection>
Recovery Target group

Recovery Script Execution Count 0 time
Maximum Reactivation Count 0 time
Maximum Failover Count 1 time
Final Action none

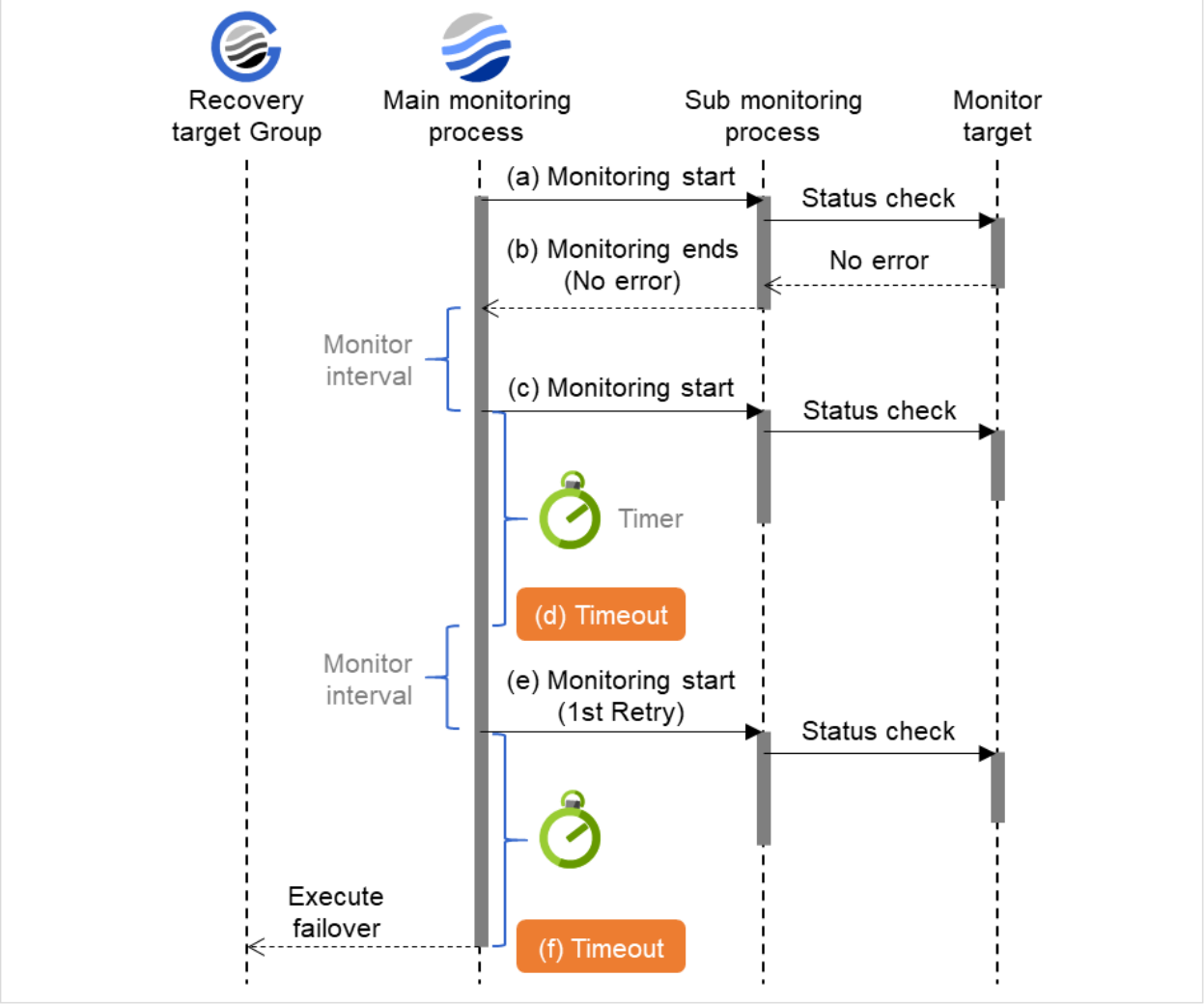


Fig. 4.6: Monitor interval (when a monitoring timeout is detected with monitor retry setting)

4.1.4 Behavior when an error is detected by a monitor resource

When an error is detected, the following recovery actions are taken against the recovery target in sequence:

- Execution of the 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 recovery target is the group resource or the failover group, the number of failover times is shared in the cluster. When the recovery target is All Groups, the number of failover times is counted by each server.). 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[1]	Failover[2]	Final action[3]
Group resource/ Failover group	Already stopped	No	No	No
	Being activated/stopped	No	No	No
	Already activated	Yes	Yes	Yes
	Error	Yes	Yes	Yes
Local Server	-	-	-	Yes

Yes: Recovery action is taken No: Recovery action is not taken

The following is an example of the progress when only one server detects an error while the gateway is specified as an IP address 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

[1] Effective only when the value for the reactivation threshold is set to 1 (one) or greater.
[2] Effective only when the value for the failover threshold is set to 1 (one) or greater.
[3] Effective only when an option other than No Operation is selected.

Note: Do not operate the following by running commands or using the Cluster WebUI when a group resource (e.g. disk resource, application 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, you can perform them when the final action is completed.

When **Server** is selected for **Failover Count Method**
When the status of the monitor resource recovers (becomes normal) from error, the reactivation count, failover count, and if the final action is executed are reset.

When **Cluster** is selected for **Failover Count Method**
When the status of the monitor resource recovers (becomes normal) from error, the reactivation count, failover count, and if the final action is executed are reset. Note that when group resource or failover group is specified as recovery target, these counters are reset only when the status of all the monitor resources in which the same recovery targets are specified are normal.
An unsuccessful recovery action is also counted into reactivation count or failover count.

<Error detection>
Recovery Target Failover Group A
Recovery Script Execution Count 3 times
Maximum Reactivation Count 3 times
Maximum Failover Count Set as much as the number of the servers
(2 times in the following case)
Final Action No Operation

(1) The following figure shows an example of monitoring by the IP monitor resource on two servers. To check for the aliveness, IP monitor resource 1 accesses the gateway's IP address at the intervals.

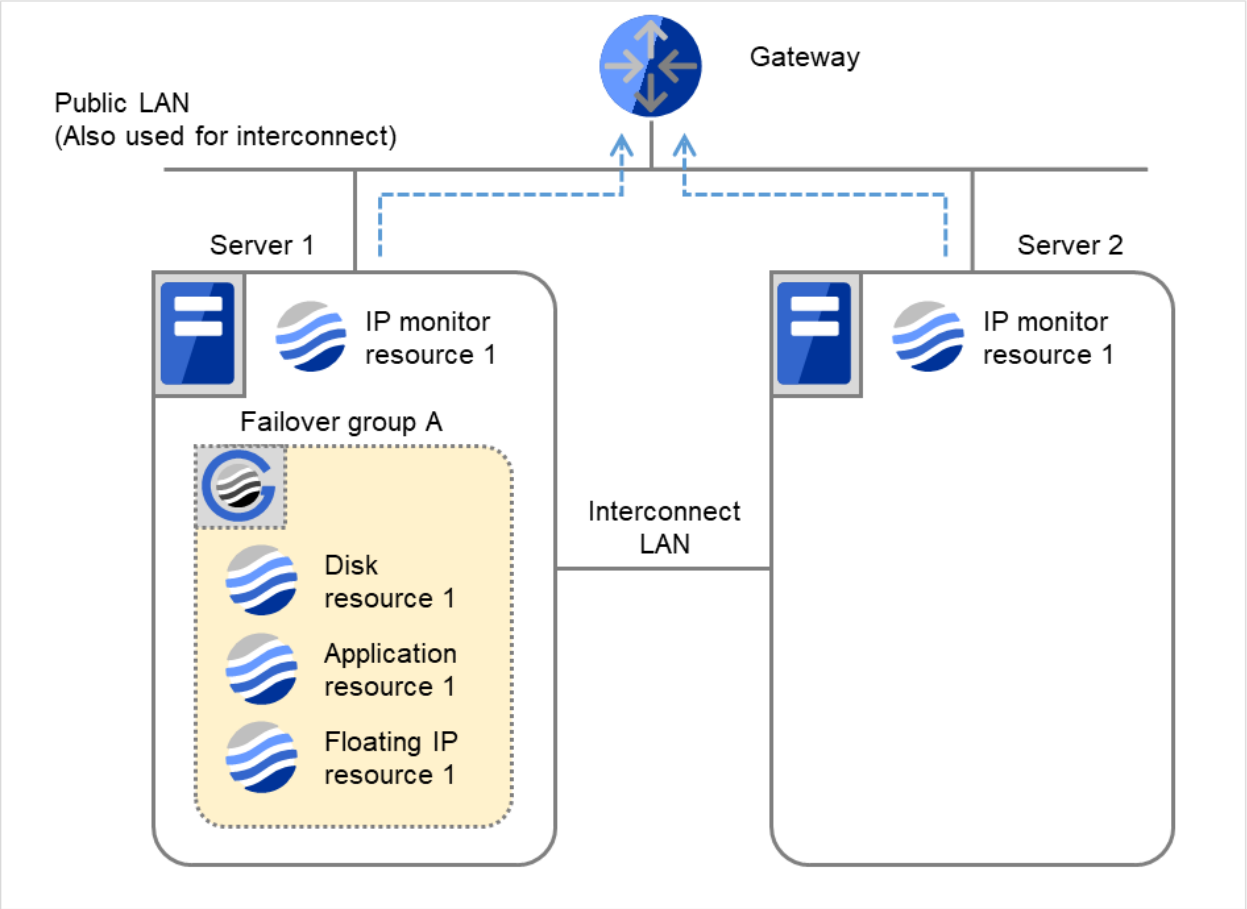


Fig. 4.7: Flow of error detection by the IP monitor resource: when only one server detects an error (1)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	0	0
Reactivation Count	0	0
Failover Count	0	0

(2) IP monitor resource 1 detects an error (such as a LAN cable disconnection and an NIC malfunction).

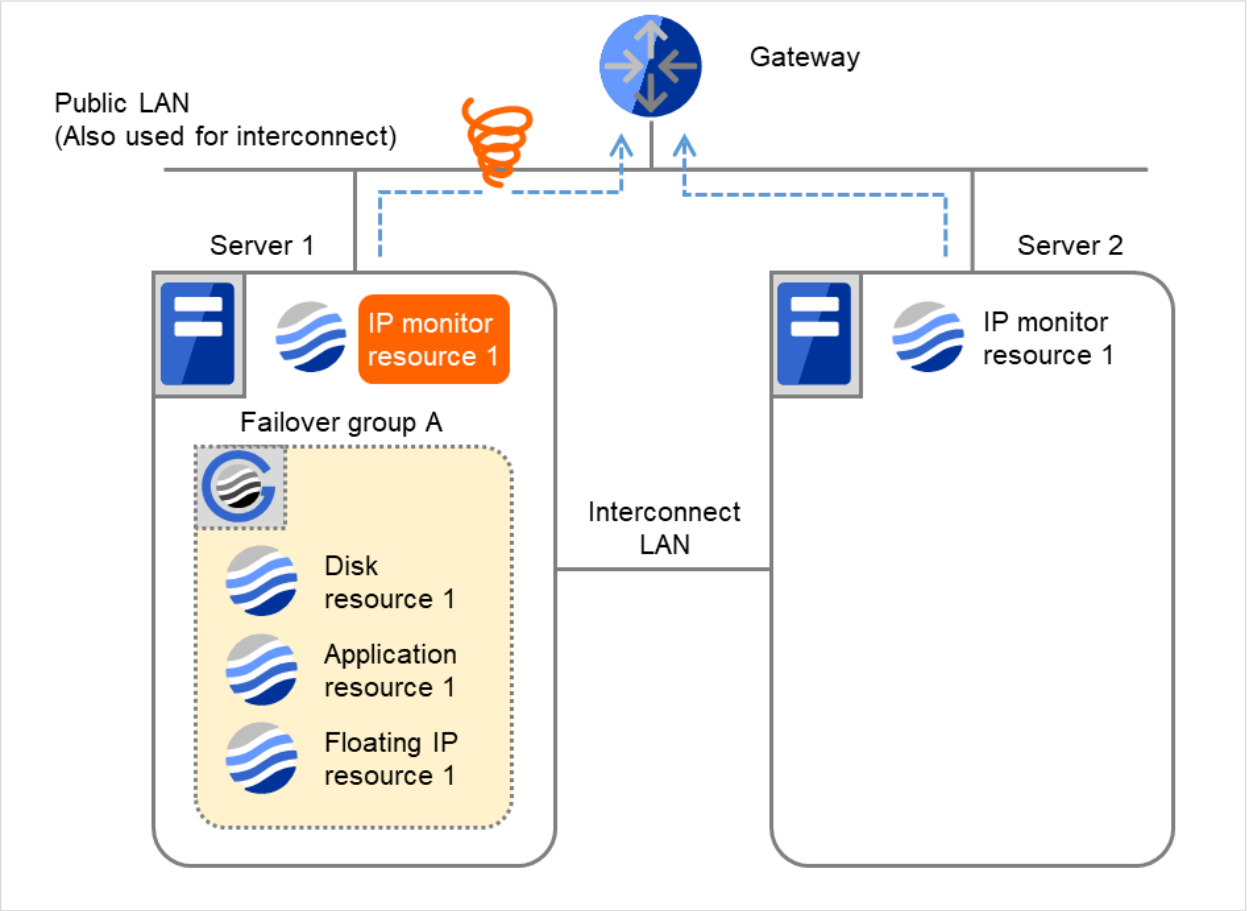


Fig. 4.8: Flow of error detection by the IP monitor resource: when only one server detects an error (2)

(3) IP monitor resource 1 retries the monitoring up to three times.

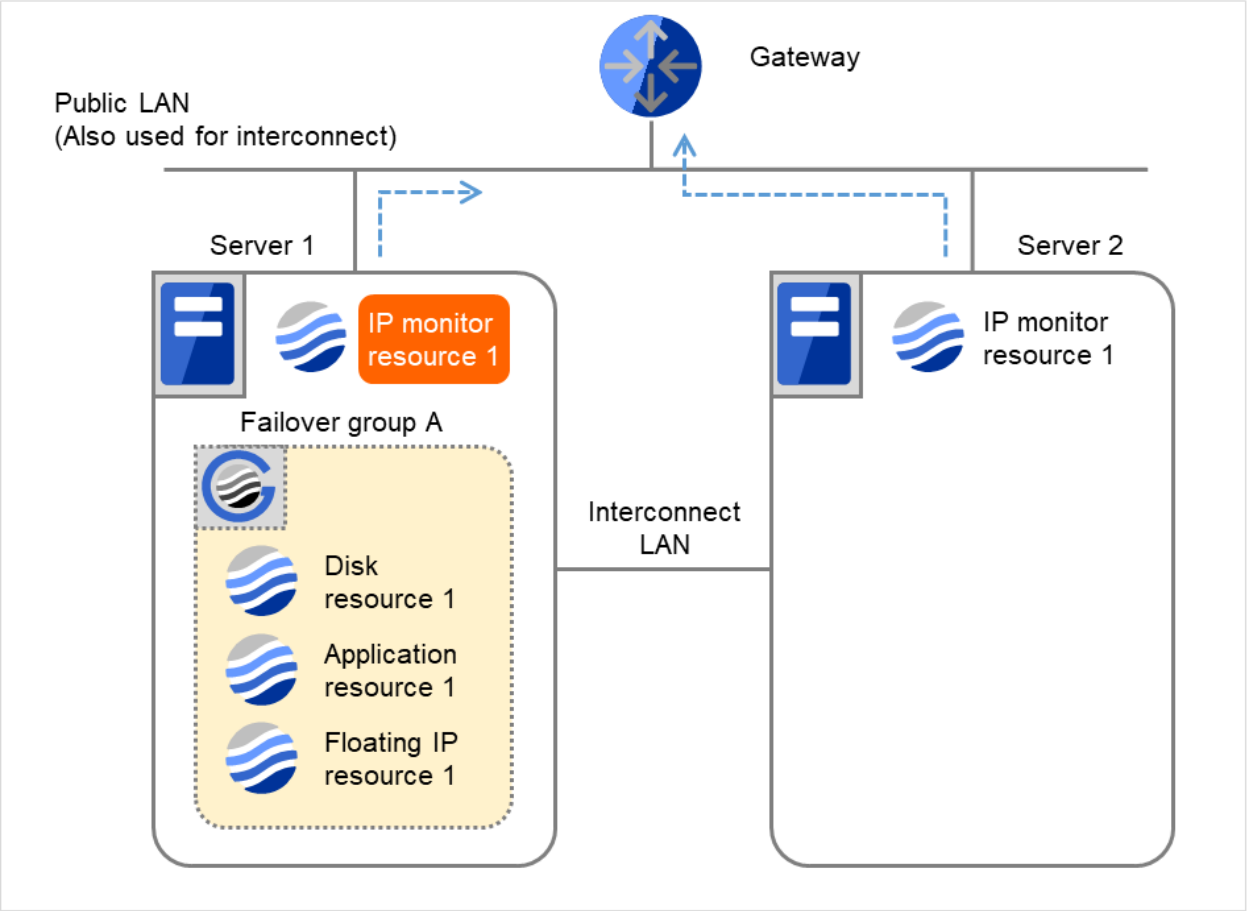


Fig. 4.9: Flow of error detection by the IP monitor resource: when only one server detects an error (3)

(4) If the specified monitor retry count is exceeded, the recovery script starts to be executed on Server 1.
Recovery Script Execution Count means how many times the recovery script is executed on each server.
This is the first execution of the recovery script on Server 1.
The recovery is not made on Server 2, because the status of Failover group A is **Already stopped**.

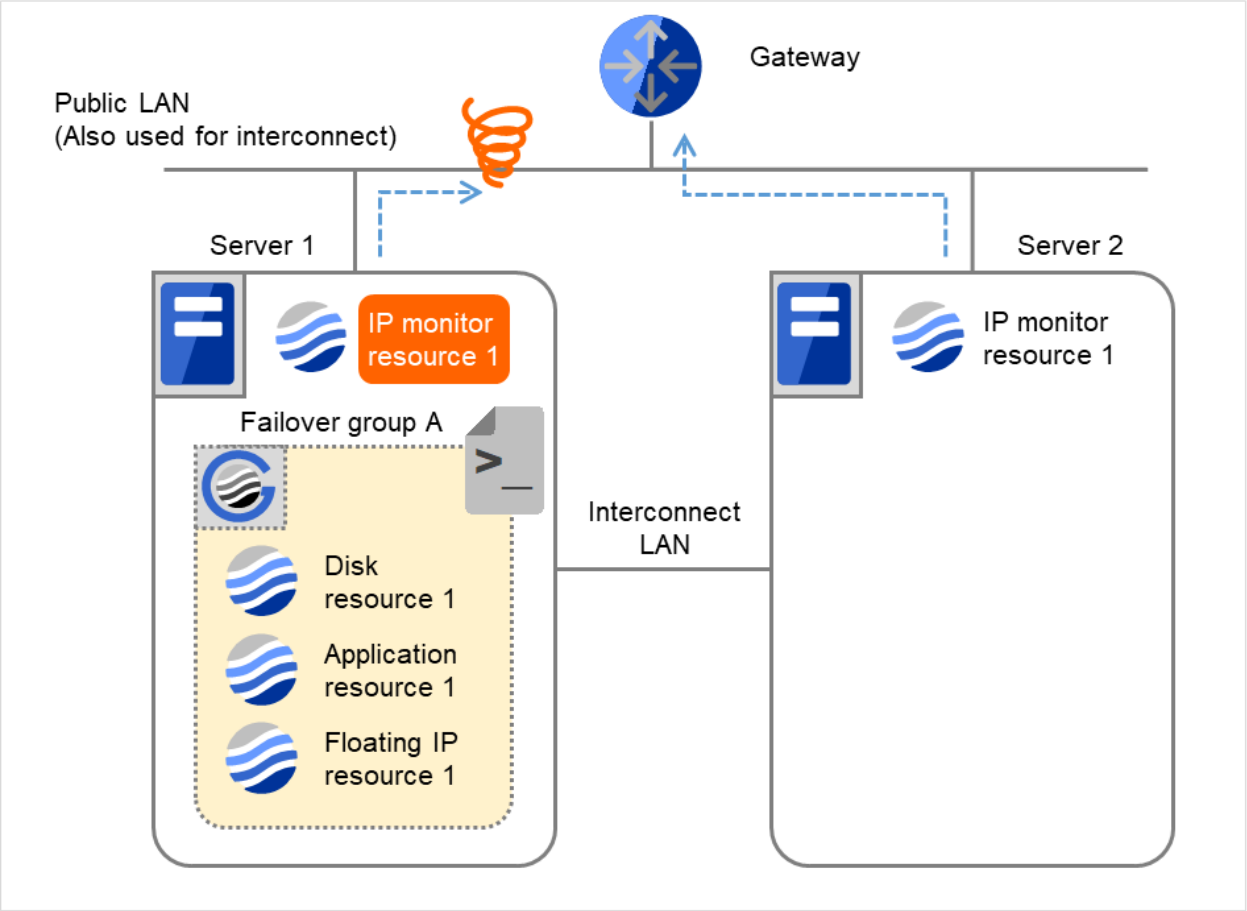


Fig. 4.10: Flow of error detection by the IP monitor resource: when only one server detects an error (4)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	0	0
Failover Count	0	0

(5) On Server 1, if the specified **Recovery Script Execution Count** is exceeded, Failover group A starts to be reactivated.

Reactivation Count represents how many times the reactivation is done on each server.

This is the first reactivation on Server 1.

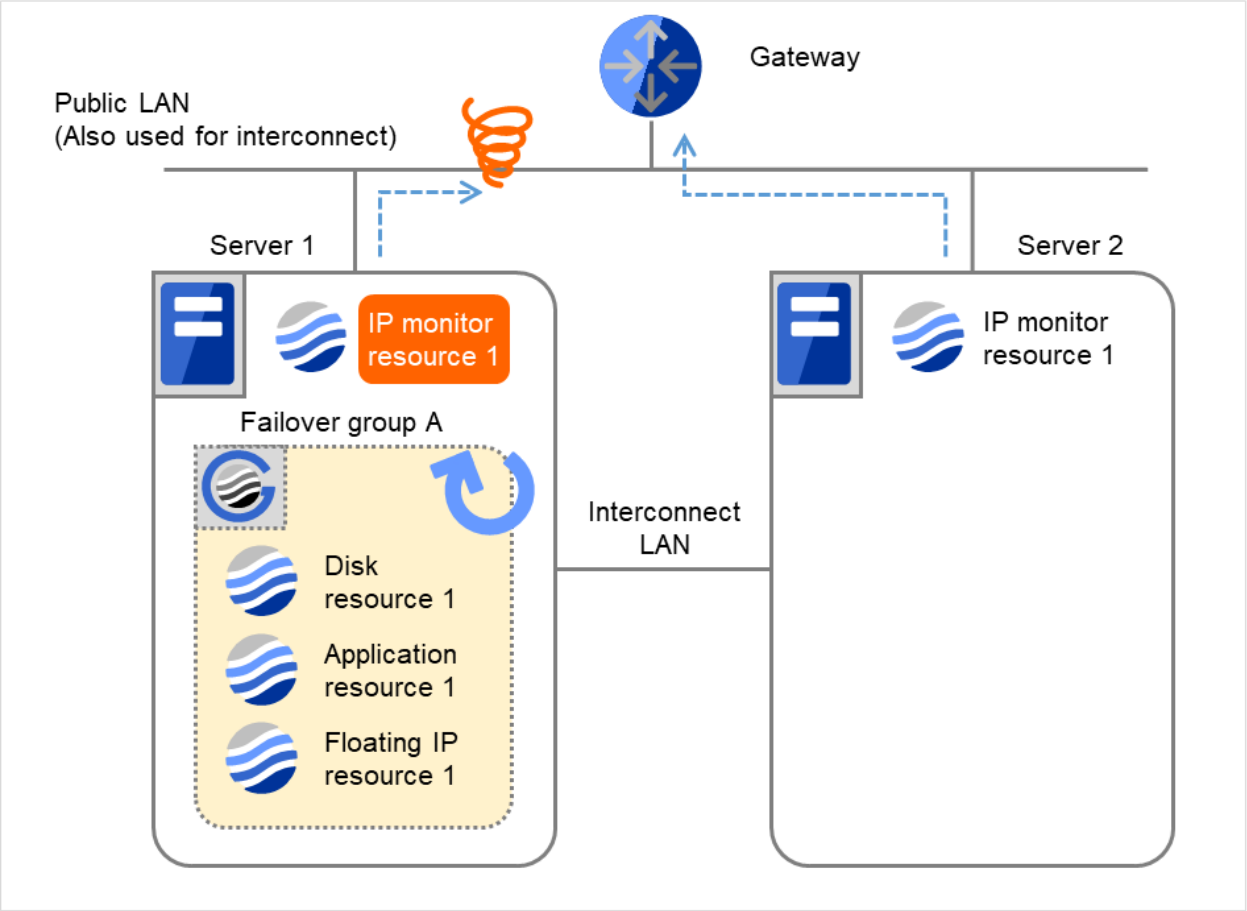


Fig. 4.11: Flow of error detection by the IP monitor resource: when only one server detects an error (5)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	3	0
Failover Count	0	0

(6) On Server 1, if the specified threshold of reactivation is exceeded, Failover group A starts to be failed over.
Failover Threshold represents how many times the failover is performed on each server.
This is the first failover on Server 1.

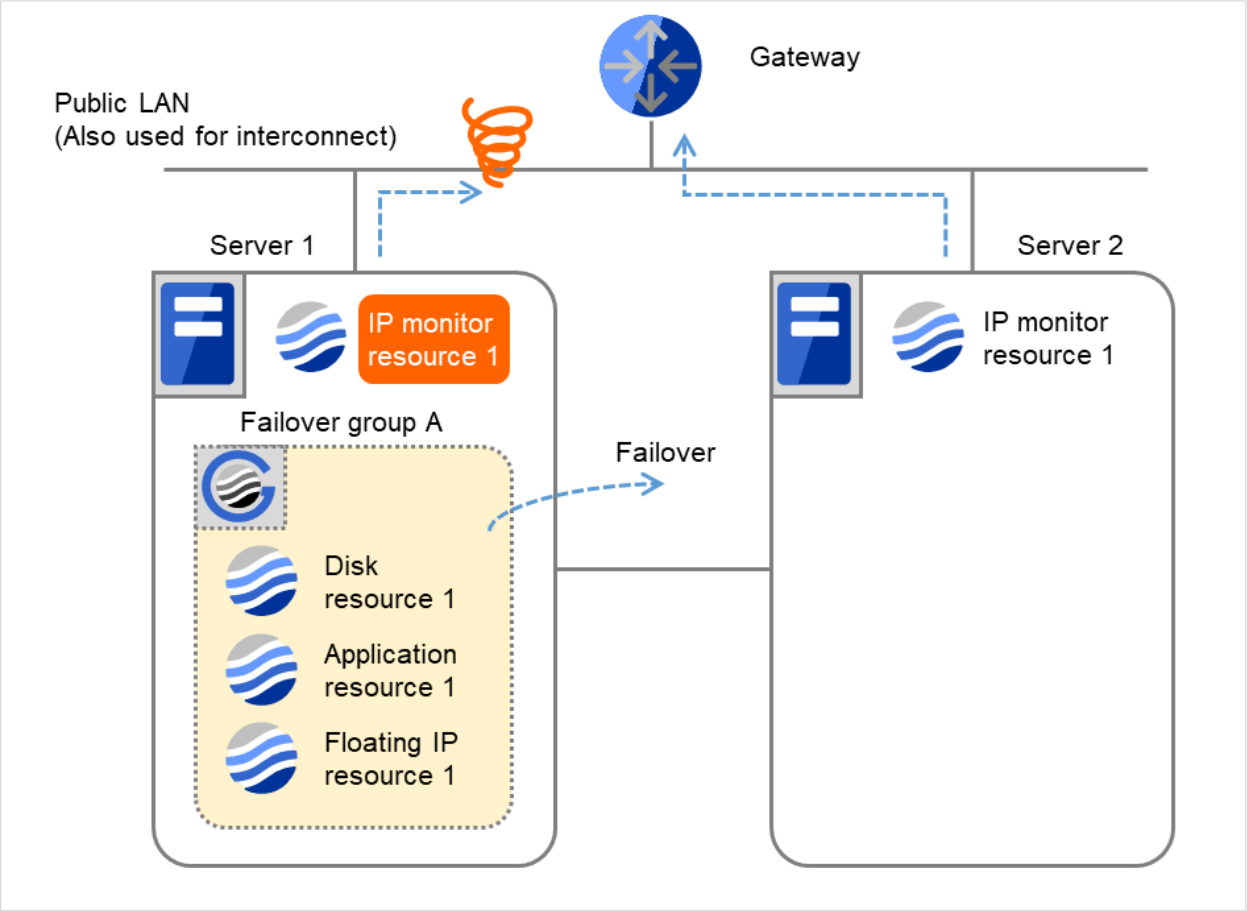


Fig. 4.12: Flow of error detection by the IP monitor resource: when only one server detects an error (6)

(7) Failover group A is failed over from Server 1 to Server 2.
On Server 2, the failover of Failover group A is completed.

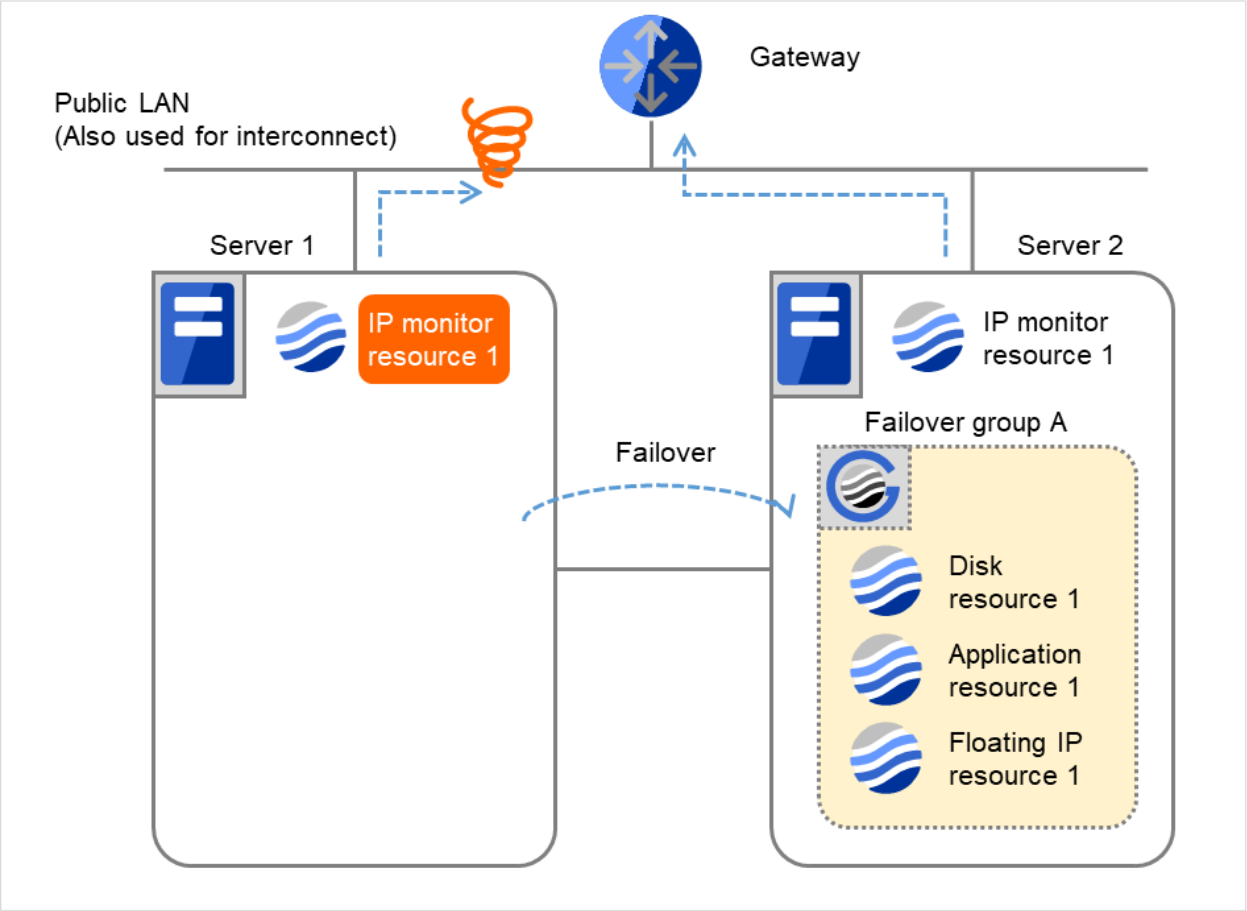


Fig. 4.13: Flow of error detection by the IP monitor resource: when only one server detects an error (7)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	3	0
Failover Count	1	1

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 IP address 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 Set as much as the number of the servers
(2 times in the following case)
Final Action No Operation

(1) The following figure shows an example of monitoring by the IP monitor resource on two servers.
To check for the aliveness, IP monitor resource 1 accesses the gateway's IP address at the intervals.

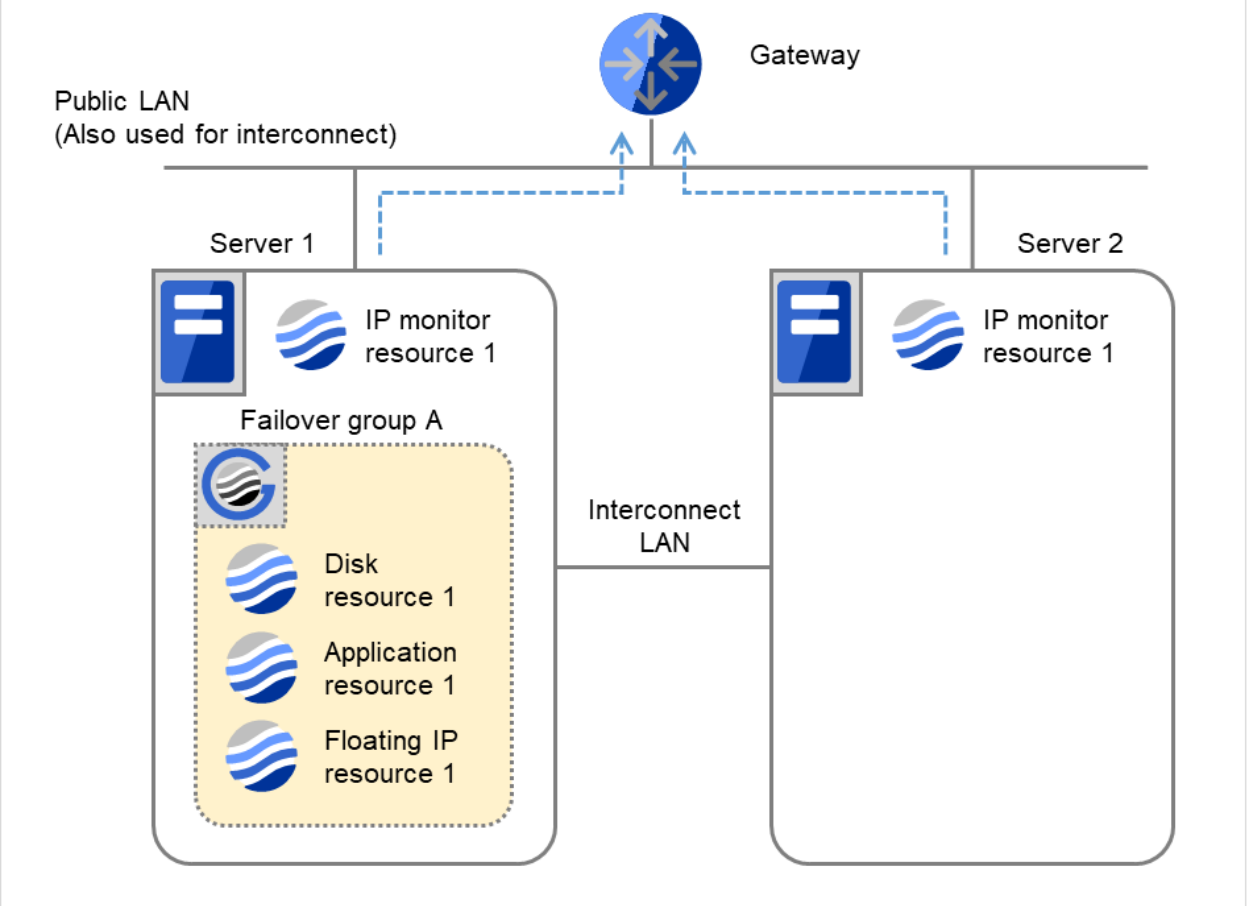


Fig. 4.14: Flow of error detection by the IP monitor resource: when both servers detect an error (1)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	0	0
Reactivation Count	0	0
Failover Count	0	0

(2) IP monitor resource 1 detects an error (such as a LAN cable disconnection and an NIC malfunction) on Servers 1 and 2.

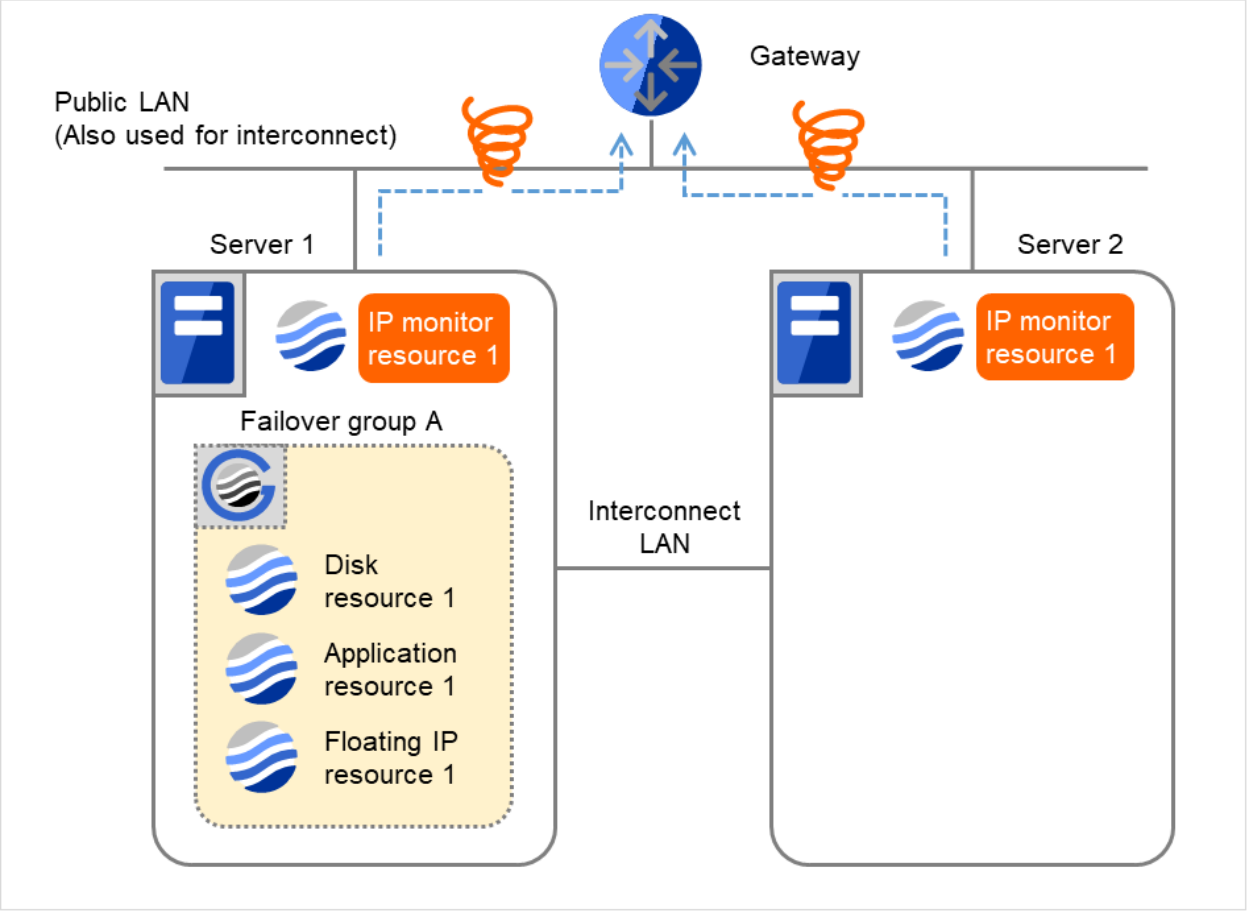


Fig. 4.15: Flow of error detection by the IP monitor resource: when both servers detect an error (2)

(3) IP monitor resource 1 retries the monitoring up to three times.

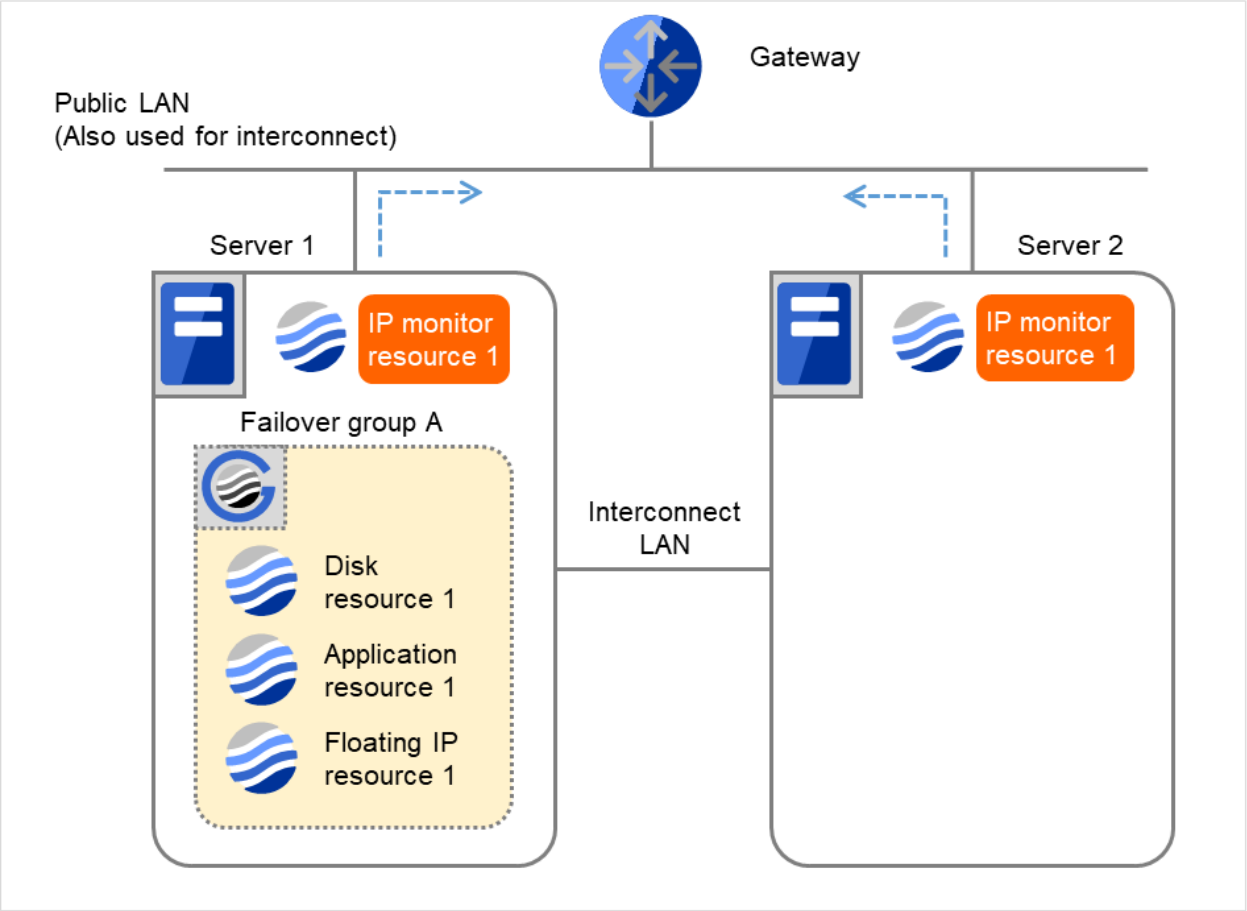


Fig. 4.16: Flow of error detection by the IP monitor resource: when both servers detect an error (3)

(4) If the specified monitor retry count is exceeded, the recovery script starts to be executed on Server 1.
Recovery Script Execution Count means how many times the recovery script is executed on each server.
This is the first execution of the recovery script on Server 1.
The recovery is not made on Server 2, because the status of Failover group A is **Already stopped**.

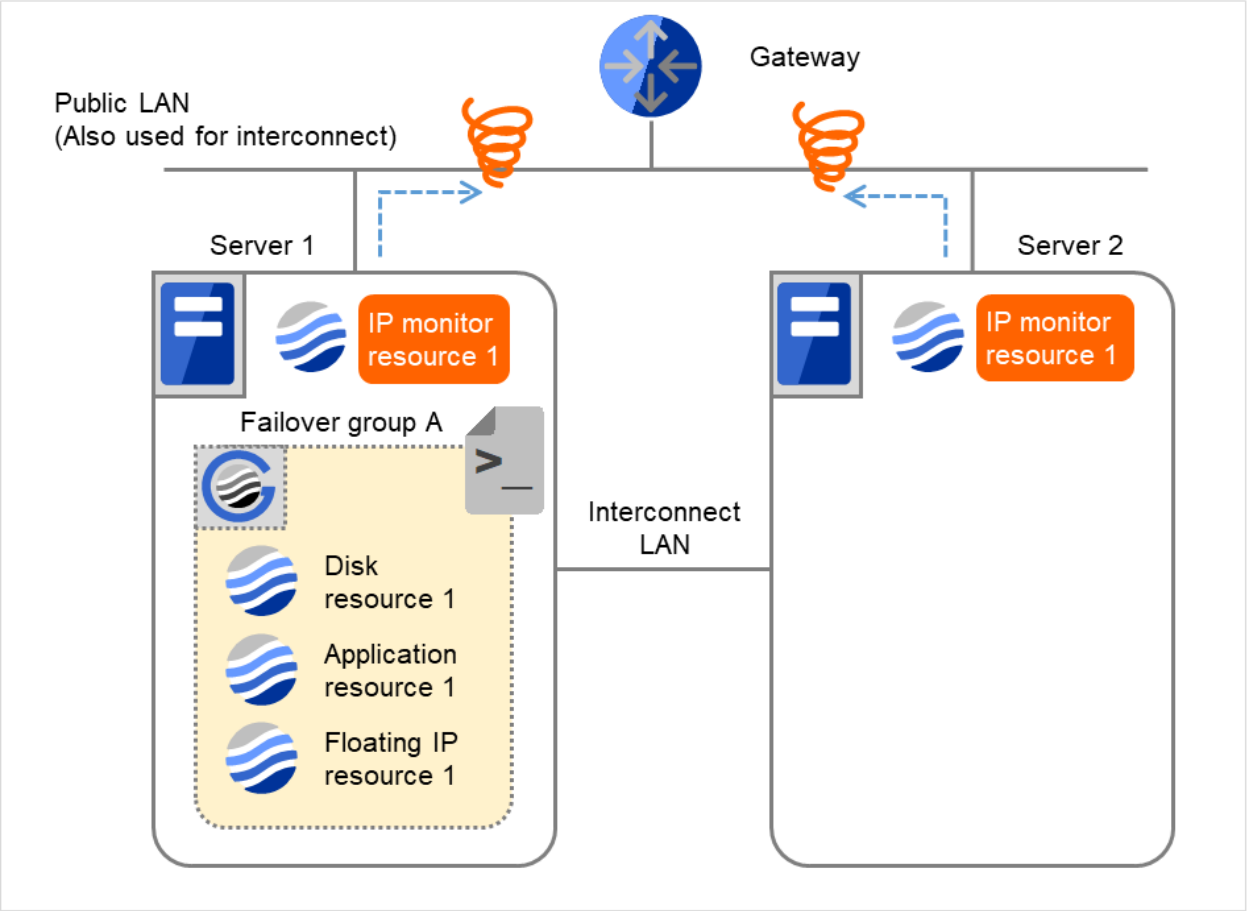


Fig. 4.17: Flow of error detection by the IP monitor resource: when both servers detect an error (4)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	0	0
Failover Count	0	0

(5) On Server 1, if the specified **Recovery Script Execution Count** is exceeded, Failover group A starts to be reactivated.

Reactivation Count represents how many times the reactivation is done on each server.

This is the first reactivation on Server 1.

The recovery is not made on Server 2, because the status of Failover group A is **Already stopped**.

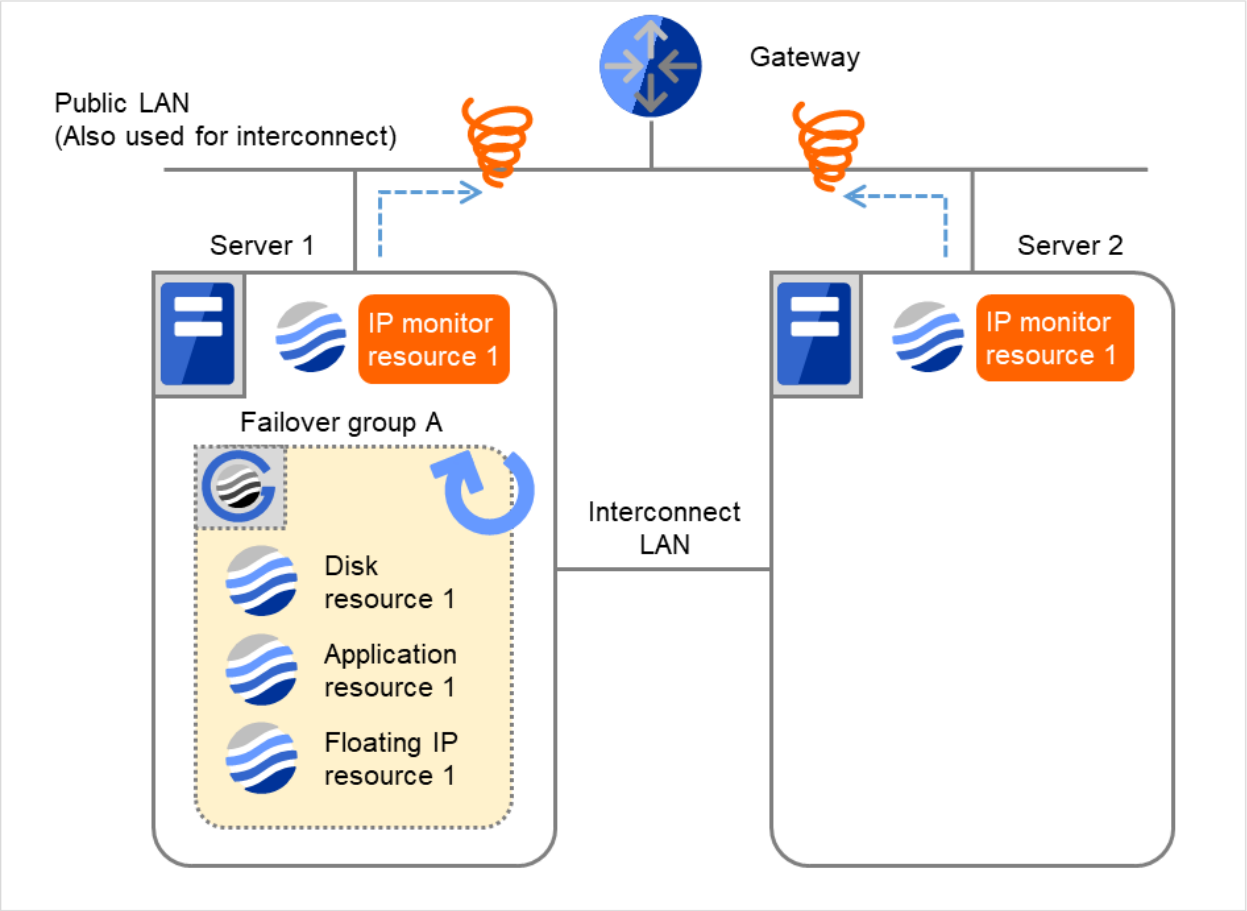


Fig. 4.18: Flow of error detection by the IP monitor resource: when both servers detect an error (5)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	3	0
Failover Count	0	0

(6) On Server 1, if the specified threshold of reactivation is exceeded, Failover group A starts to be failed over.
Failover Threshold represents how many times the failover is performed on each server.
This is the first failover on Server 1.
The recovery is not made on Server 2, because the status of Failover group A is **Already stopped**.

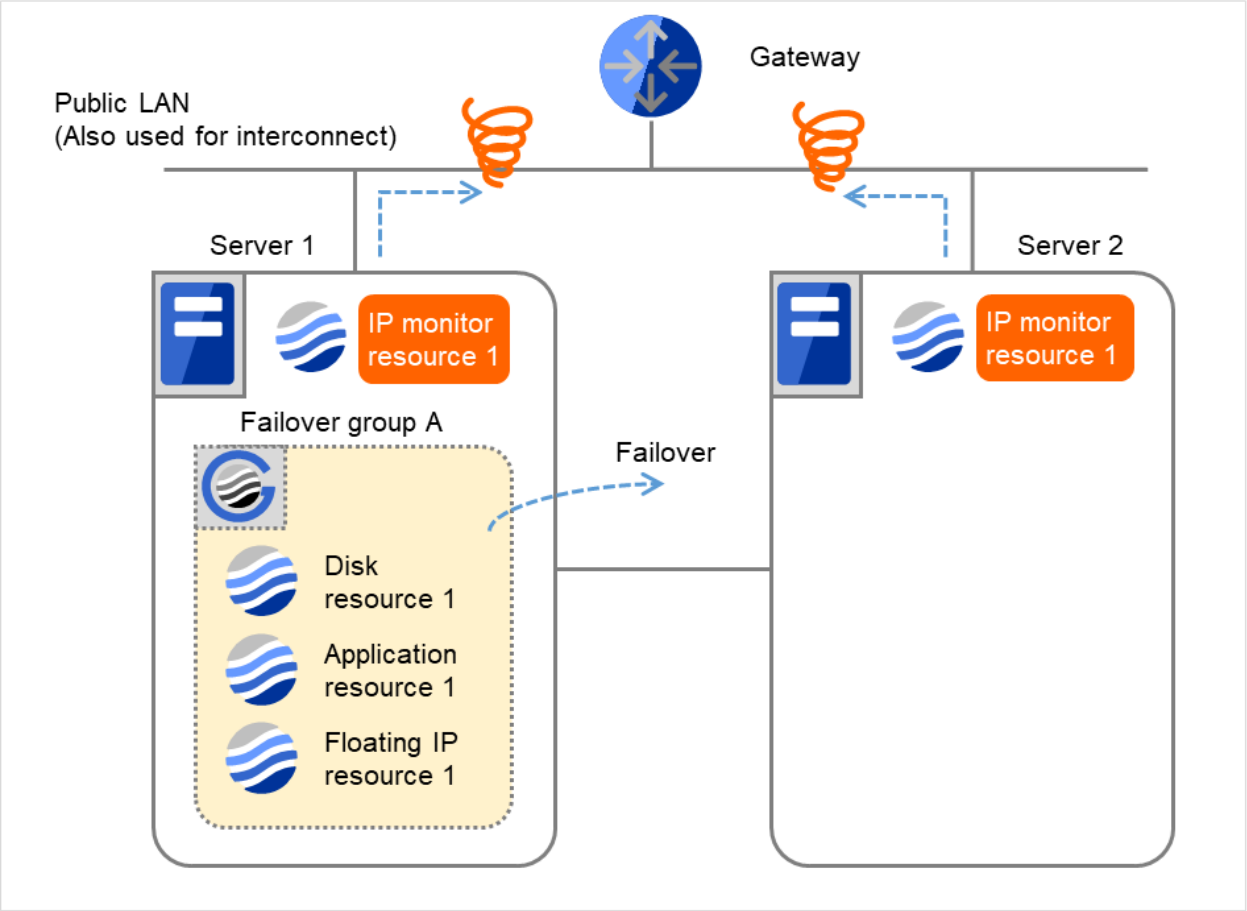


Fig. 4.19: Flow of error detection by the IP monitor resource: when both servers detect an error (6)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	3	0
Failover Count	1	1

(7) Failover group A is failed over from Server 1 to Server 2.
On Server 2, IP monitor resource 1 finds the error persisting.

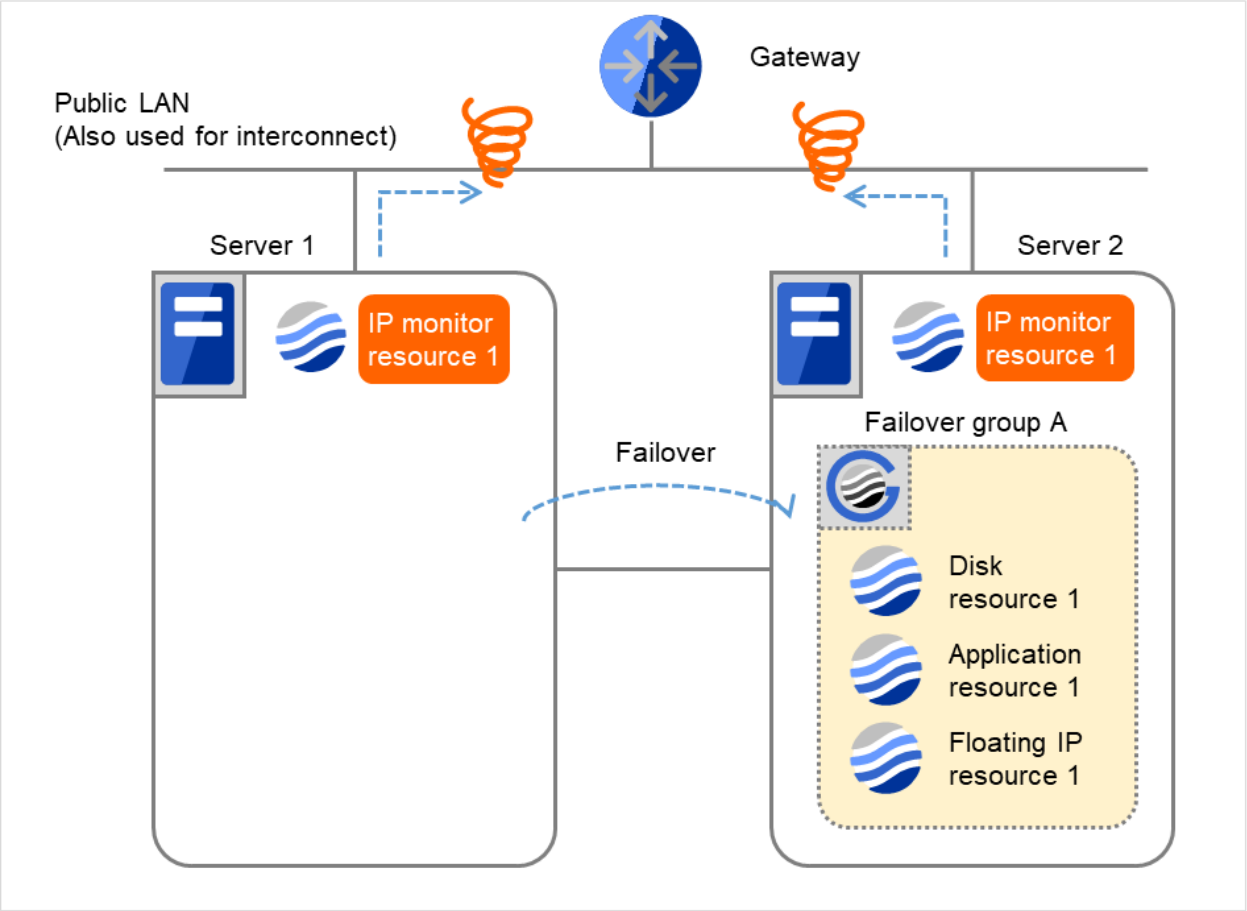


Fig. 4.20: Flow of error detection by the IP monitor resource: when both servers detect an error (7)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	3	0
Failover Count	1	1

(8) IP monitor resource 1 retries the monitoring up to three times.

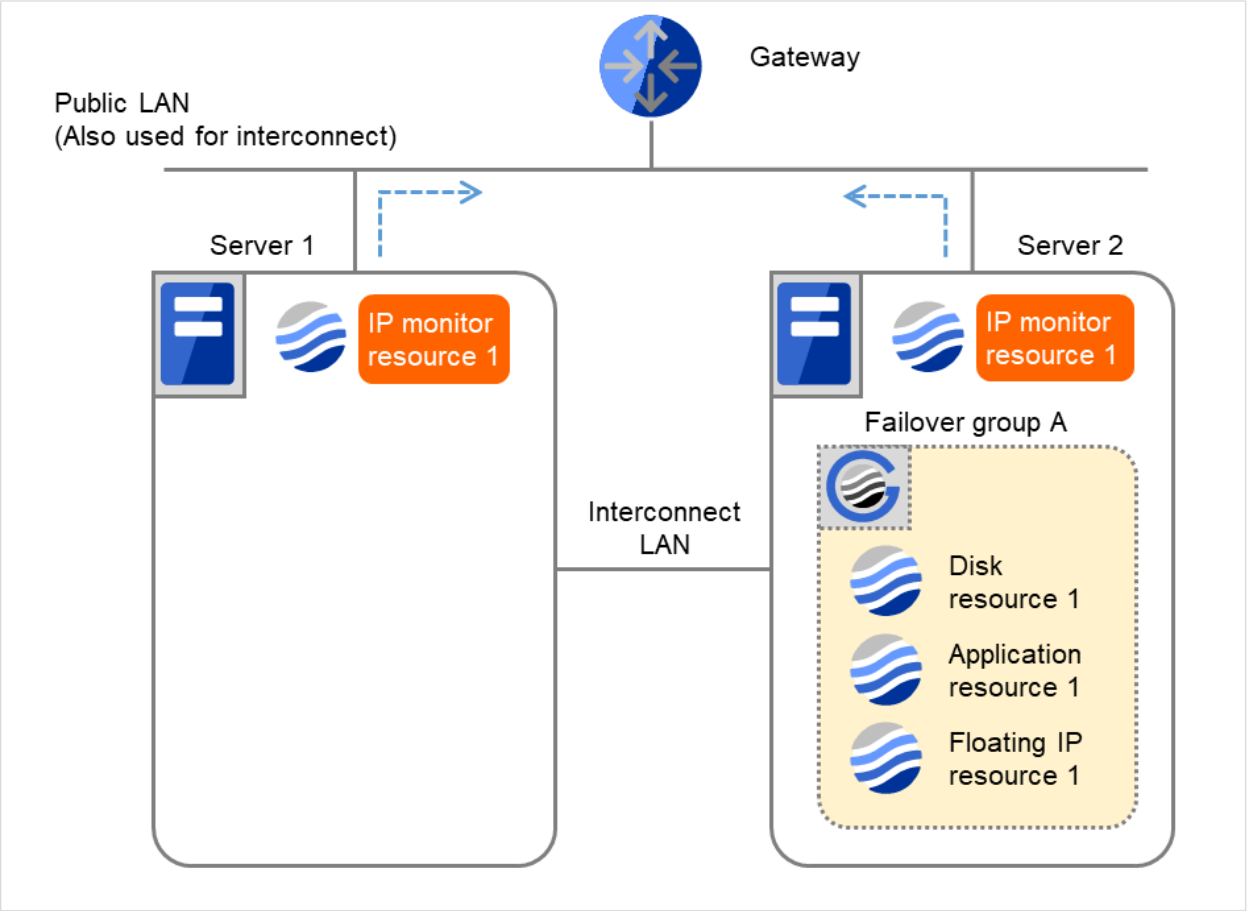


Fig. 4.21: Flow of error detection by the IP monitor resource: when both servers detect an error (8)

(9) If the specified monitor retry count is exceeded by IP monitor resource 1 and the error persists, then executing the recovery script is retried up to three times.

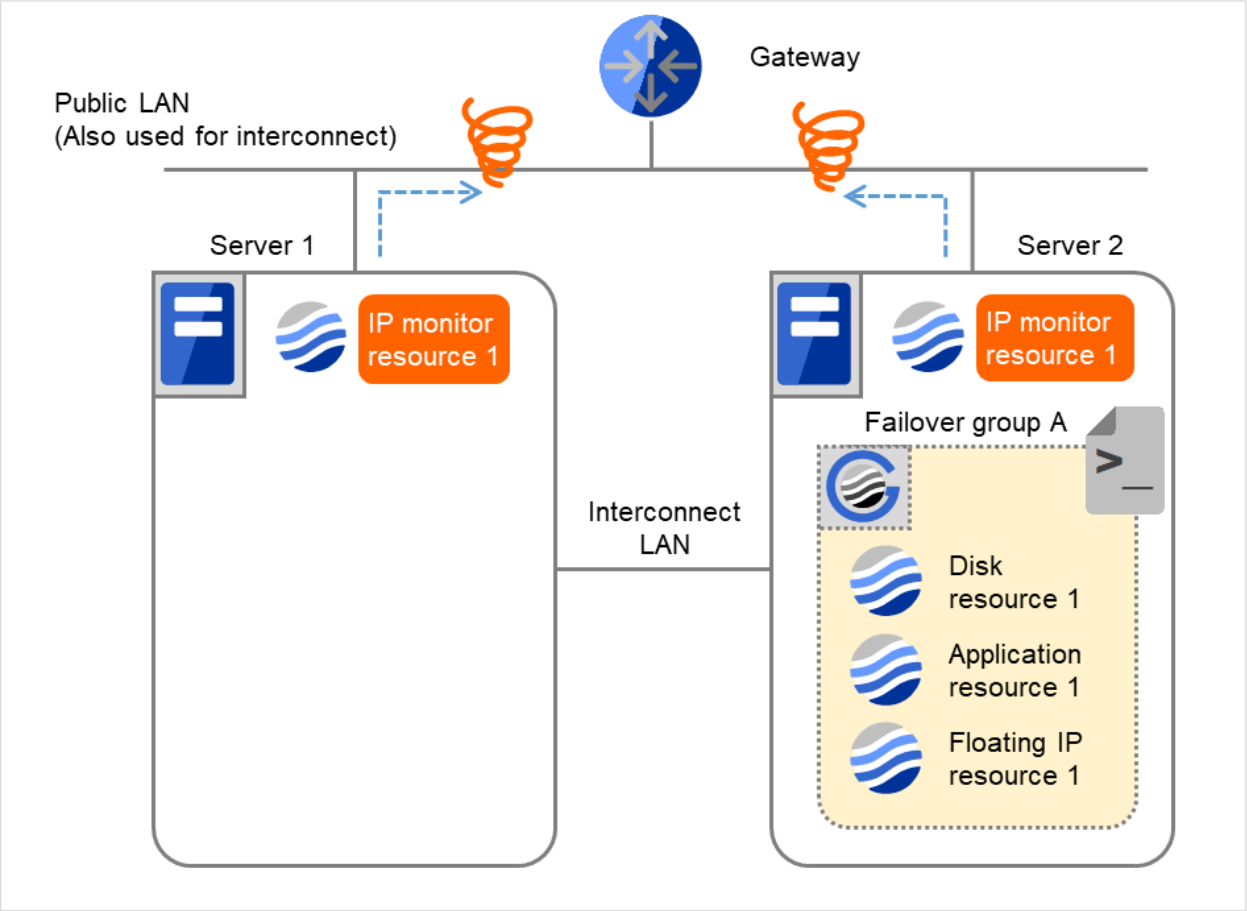


Fig. 4.22: Flow of error detection by the IP monitor resource: when both servers detect an error (9)

(10) On Server 2, if the specified retry count is exceeded for the recovery script execution and the error persists, reactivating Failover group A is retried up to three times.

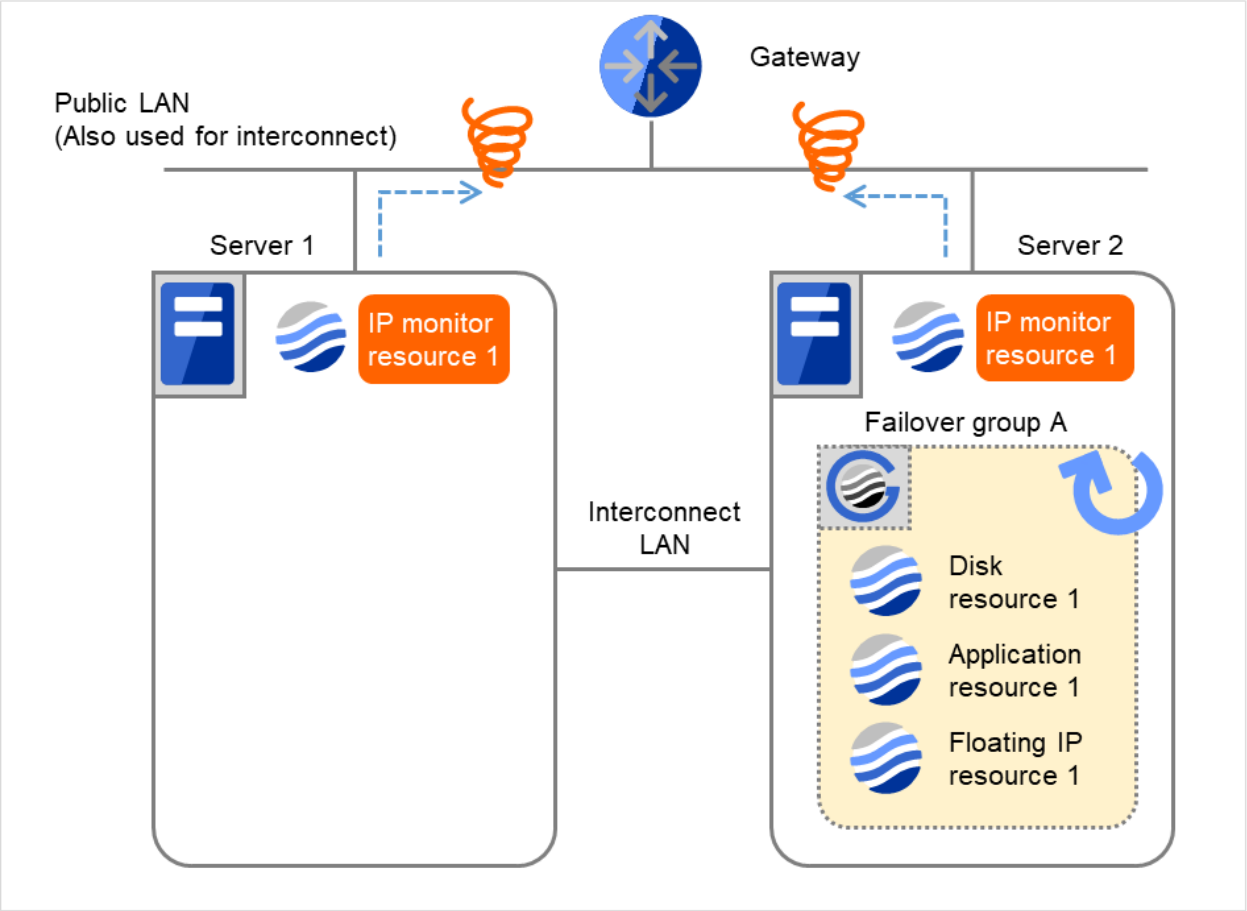


Fig. 4.23: Flow of error detection by the IP monitor resource: when both servers detect an error (10)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	3
Reactivation Count	3	3
Failover Count	1	1

(11) On Server 2, if the specified reactivation retry count is exceeded, Failover group A starts to be failed over. This is the first failover on Server 2.

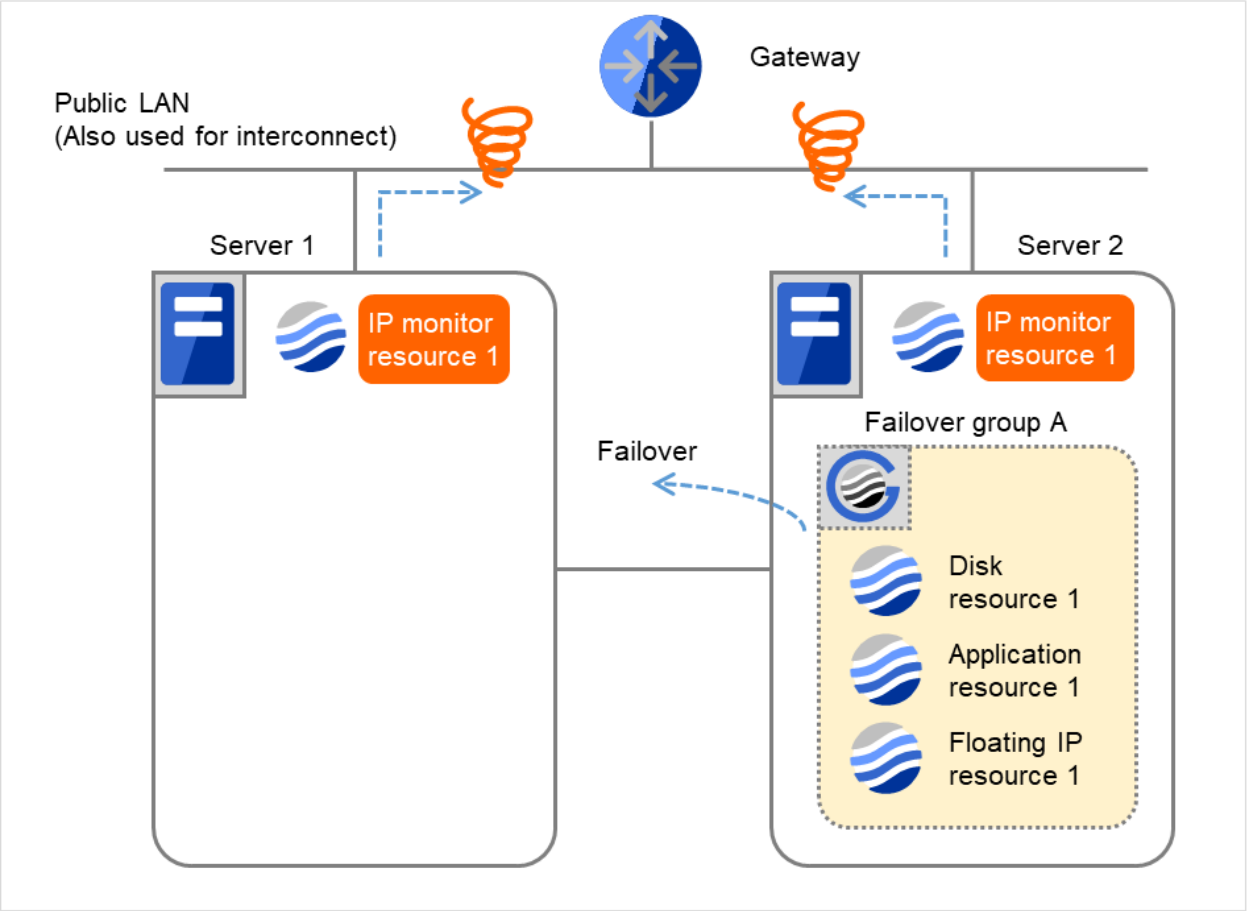


Fig. 4.24: Flow of error detection by the IP monitor resource: when both servers detect an error (11)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	3
Reactivation Count	3	3
Failover Count	2	2

(12) Failover group A is failed over from Server 2 to Server 1.
On Server 1, IP monitor resource 1 finds the error persisting.

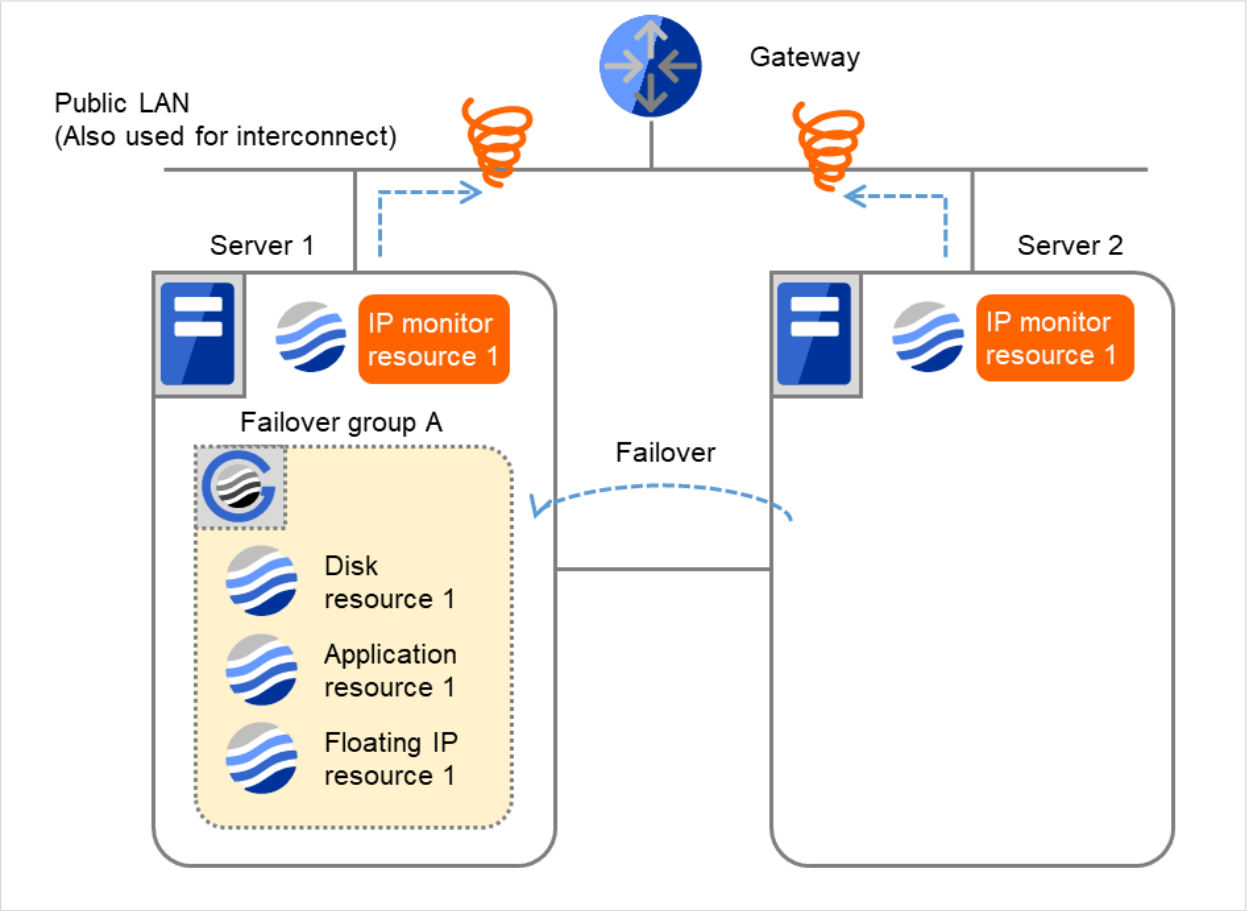


Fig. 4.25: Flow of error detection by the IP monitor resource: when both servers detect an error (12)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	3
Reactivation Count	3	3
Failover Count	2	2

(13) On Server 1, IP monitor resource 1 retries the monitoring up to three times.

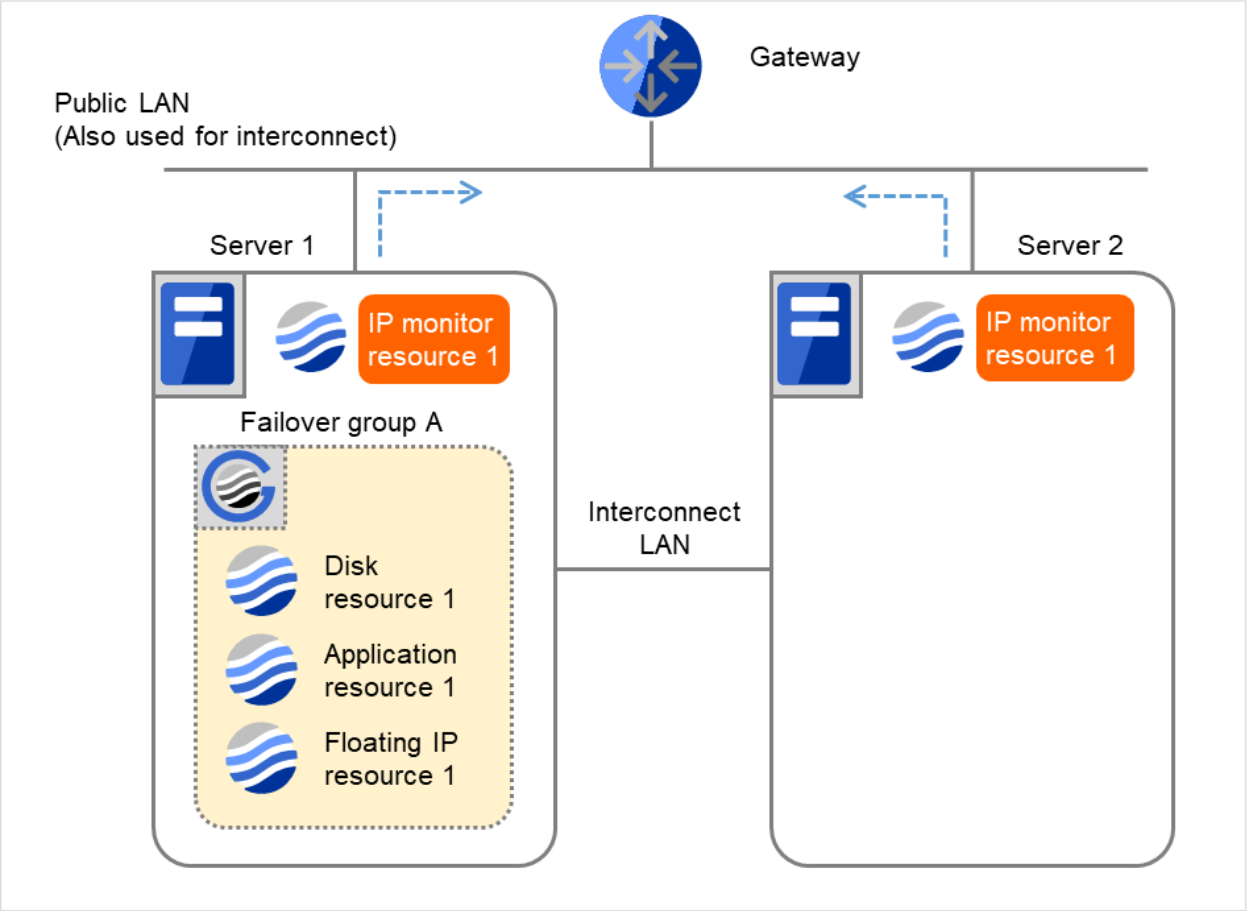


Fig. 4.26: Flow of error detection by the IP monitor resource: when both servers detect an error (13)

(14) If the specified monitor retry count is exceeded by Disk monitor resource 1 on Server 1 again, the reactivation is not performed. This is because its threshold is 3.

In addition, the specified **Final Action** is started. No failover is performed then, because **Failover Threshold** is set at 1.

On Server 1, the final action of IP monitor resource 1 is started.

Final Action means the action to be taken after the specified failover retry count is exceeded.

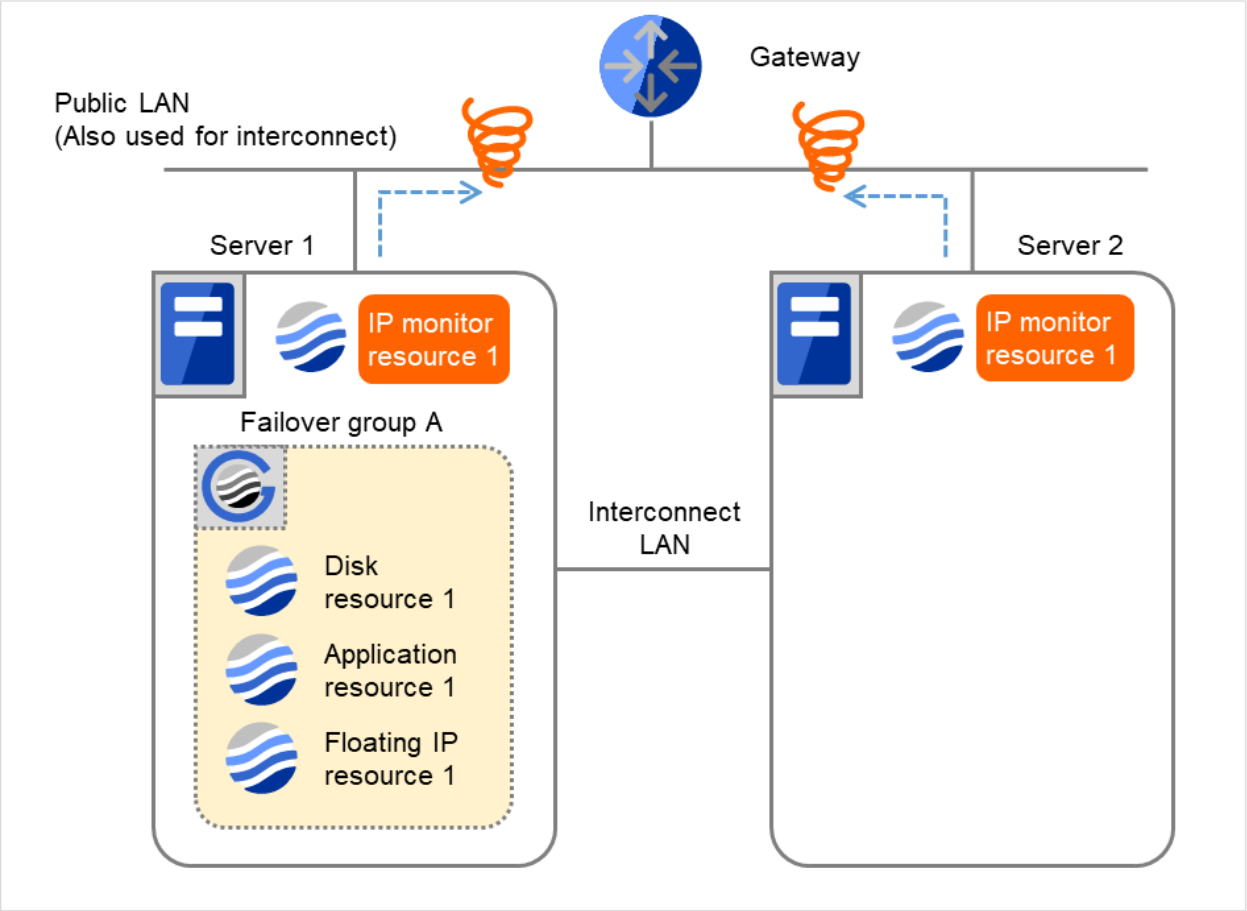


Fig. 4.27: Flow of error detection by the IP monitor resource: when both servers detect an error (14)

Additional Information

When the status of the monitor resource becomes normal from an error, the reactivation count and failover count are reset to zero (0).

4.1.5 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 following thresholds that the monitor resource keeps are reset. Note that when a group resource or failover group is specified as recovery target, these counters are reset only when the status of all the monitor resources in which the same recovery targets are specified become normal.

- Reactivation Threshold
- Failover Threshold

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 "*Behavior when an error is detected by a monitor resource*" is 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 Set as much as the number of the servers
(2 times in the following case)
Final Action No operation

(1) The following figure shows an example of monitoring by the IP monitor resource on two servers.
After all recovery actions are taken, a monitoring error persists.
On Server 1, the final action of IP monitor resource 1 was taken.

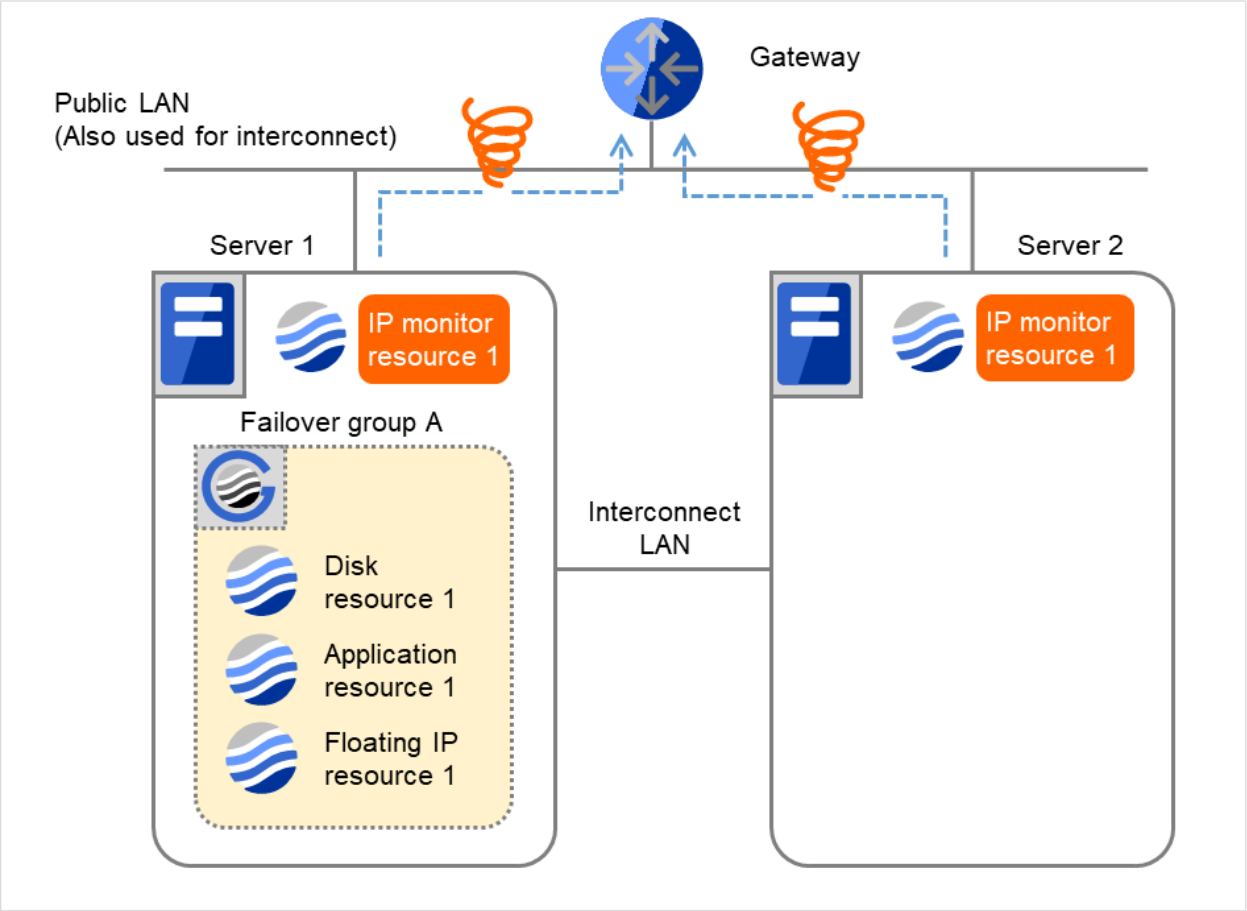


Fig. 4.28: Flow of error detection by the IP monitor resource: normally returning from a monitoring error (1)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	3
Reactivation Count	3	3
Failover Count	2	2

(2) When the gateway is restored, IP monitor resource 1 finds the situation normal.

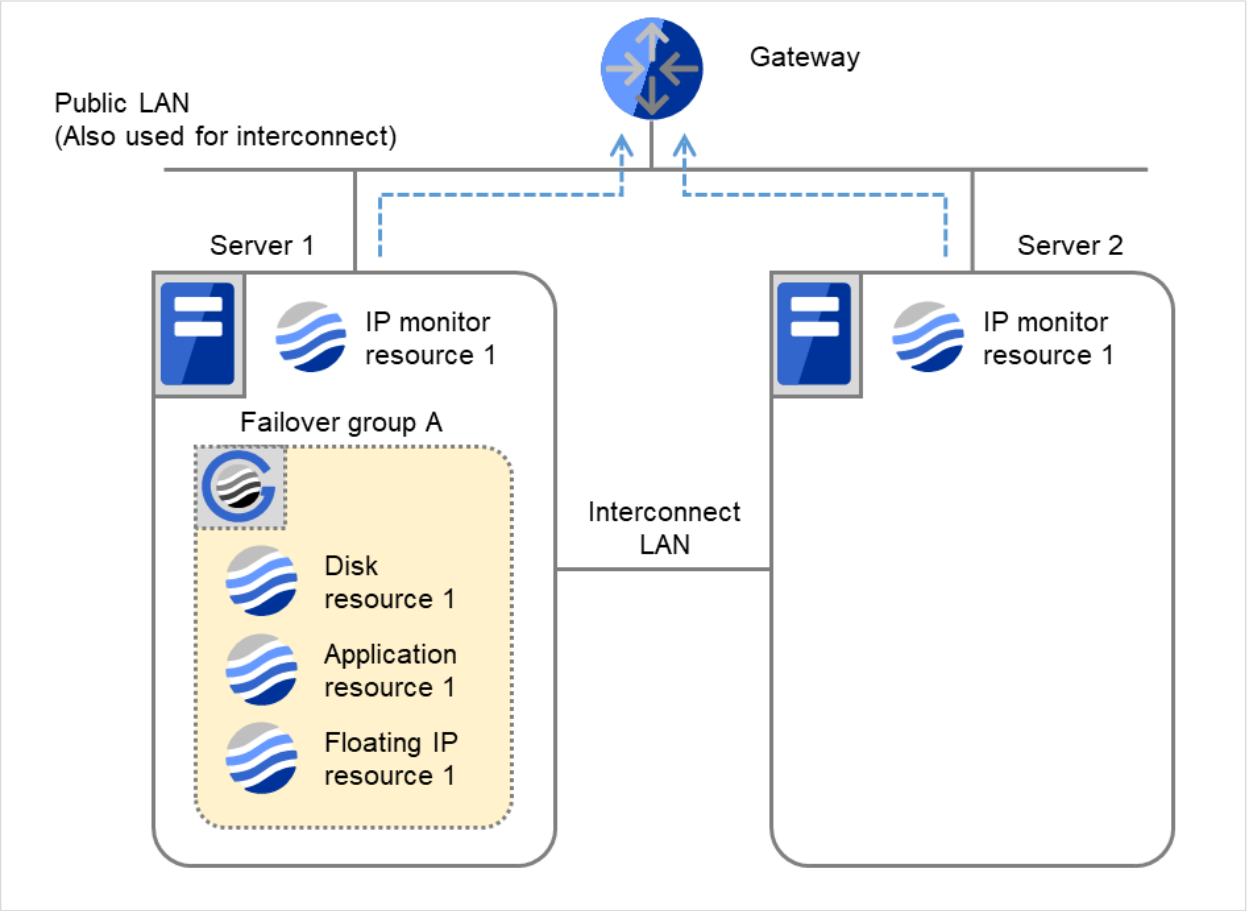


Fig. 4.29: Flow of error detection by the IP monitor resource: normally returning from a monitoring error (2)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	0	0
Reactivation Count	0	0
Failover Count	0	0

The number of reactivations and failovers are reset because it has been detected that the status of the monitor target resource became normal.

(3) IP monitor resource 1 has detected an error again.

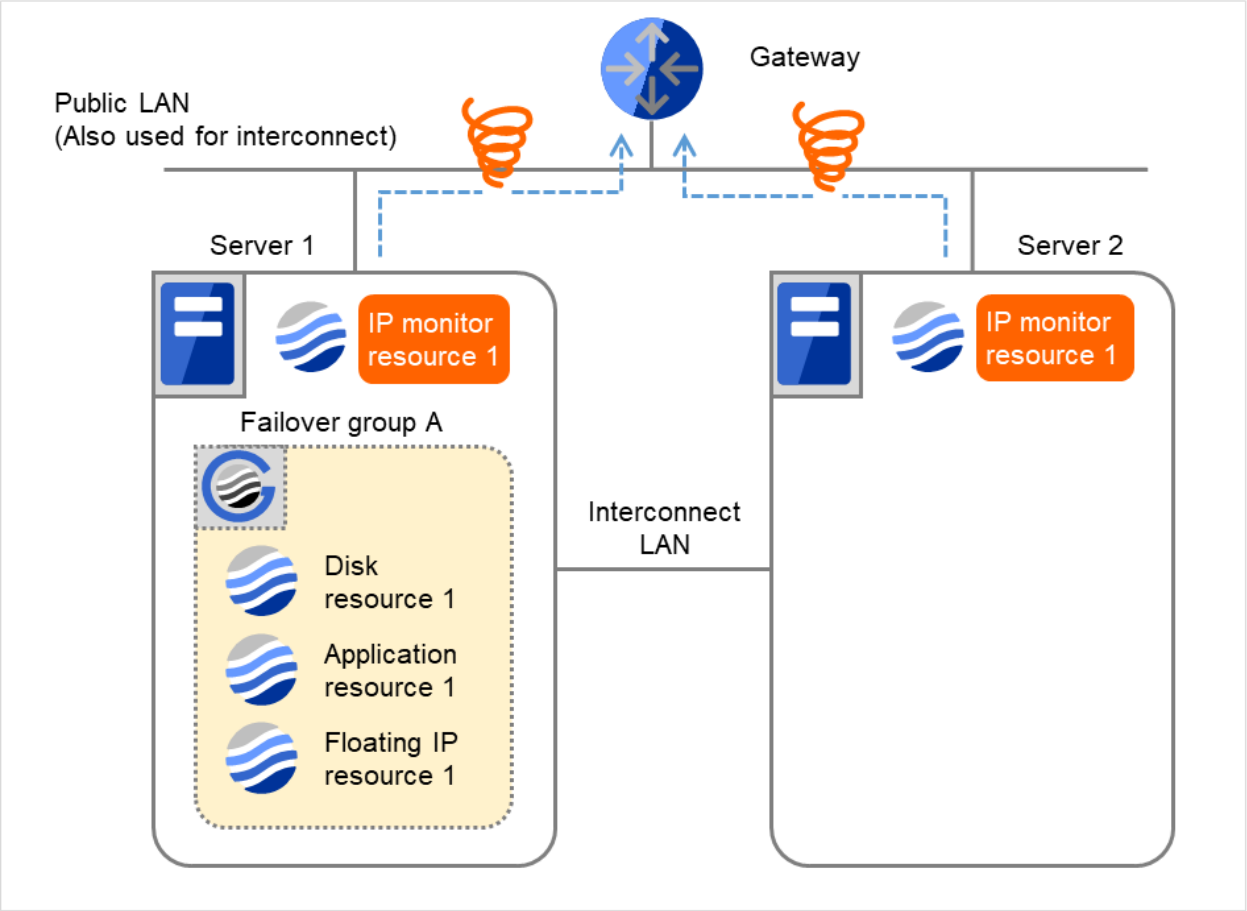


Fig. 4.30: Flow of error detection by the IP monitor resource: normally returning from a monitoring error (3)

(4) IP monitor resource 1 retries the monitoring up to three times.
Retry Count means that on this server.

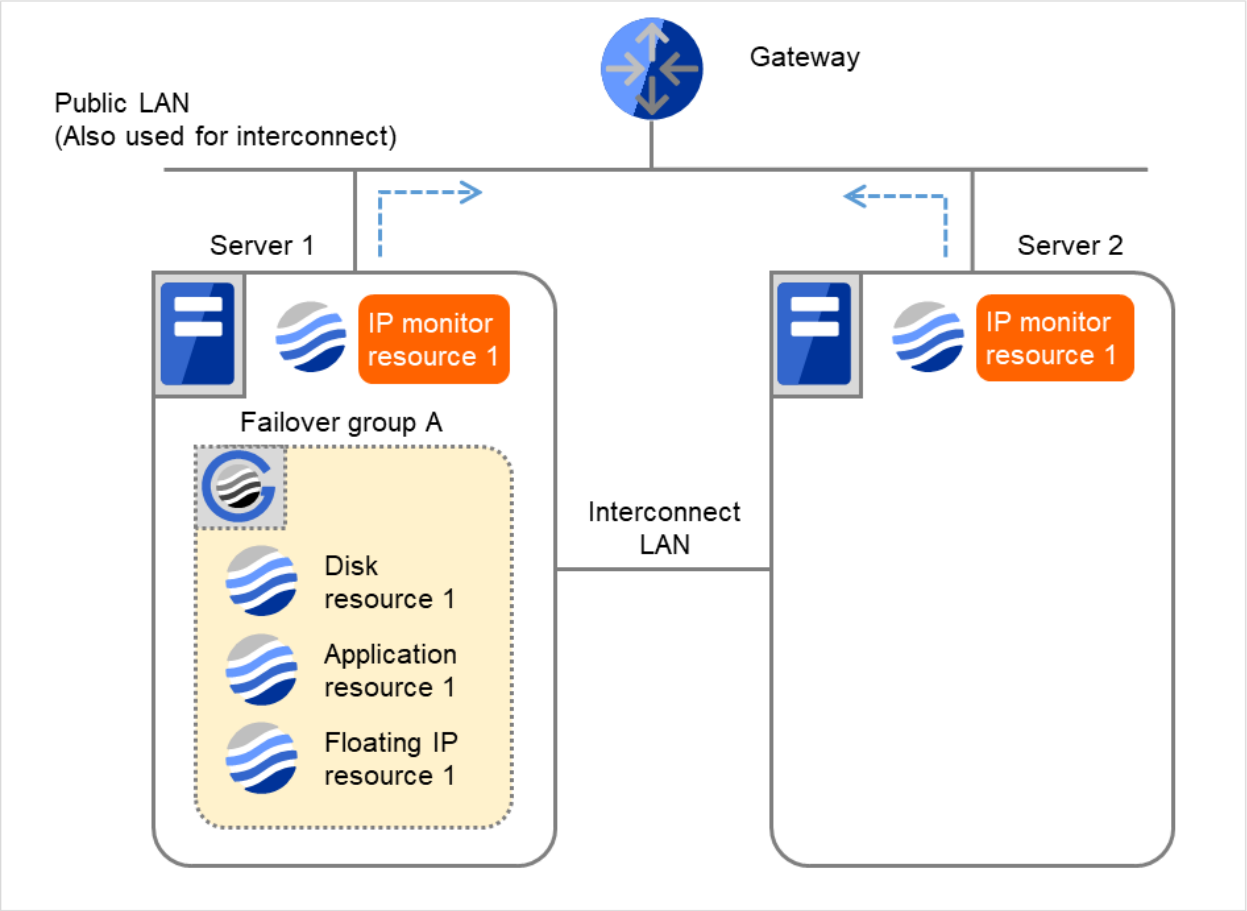


Fig. 4.31: Flow of error detection by the IP monitor resource: normally returning from a monitoring error (4)

	Server 1 IP monitor resource 1
Recovery Script Execution Count	0
Reactivation Count	0
Failover Count	0

(5) If the specified monitor retry count is exceeded, the recovery script starts to be executed on Server 1. **Recovery Script Execution Count** means how many times the recovery script is executed on each server. This is the first execution of the recovery script on Server 1. The recovery is not made on Server 2, because the status of Failover group A is **Already stopped**.

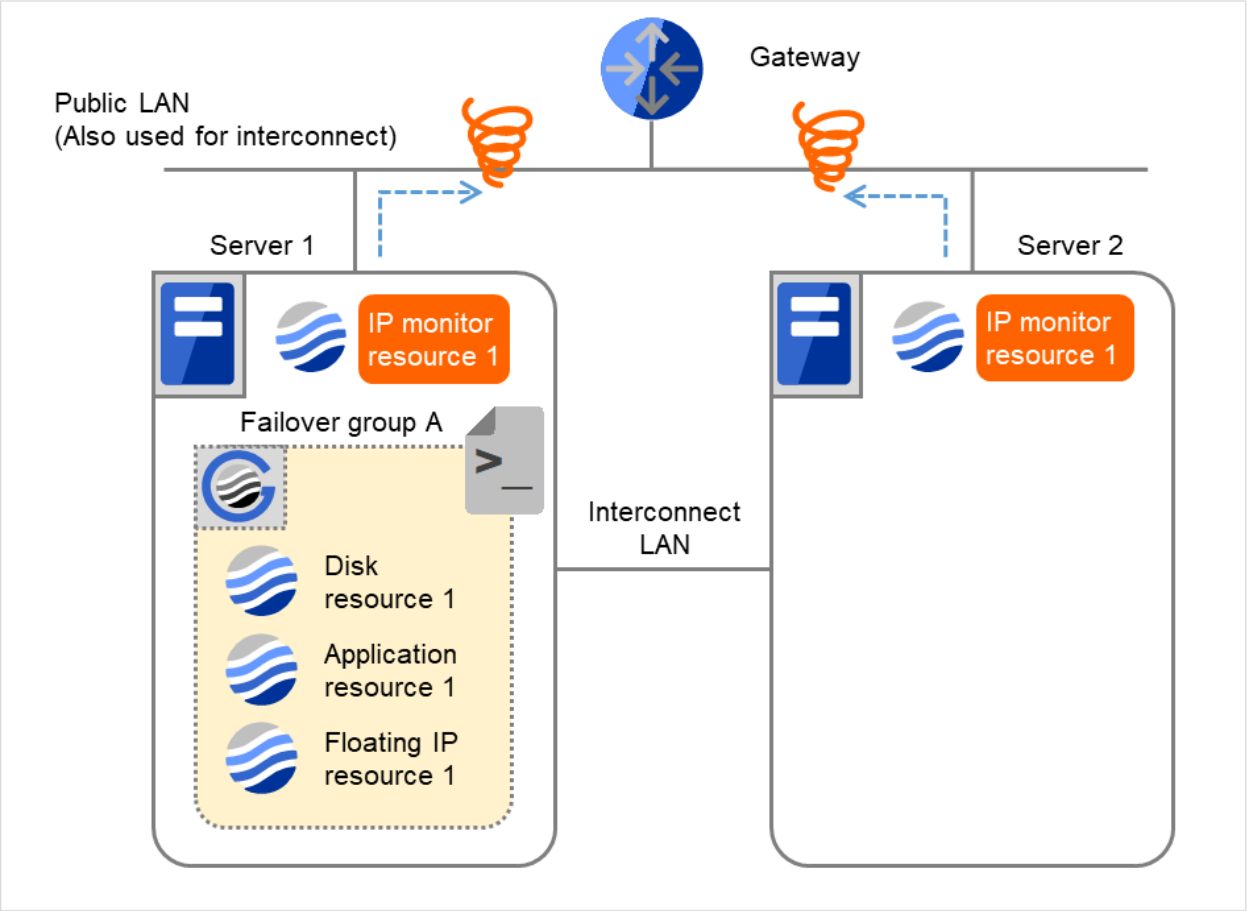


Fig. 4.32: Flow of error detection by the IP monitor resource: normally returning from a monitoring error (5)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	0	0
Failover Count	0	0

(6) On Server 1, if the specified **Recovery Script Execution Count** is exceeded, Failover group A starts to be reactivated.

Reactivation Count represents how many times the reactivation is done on each server.

This is the first reactivation on Server 1.

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.

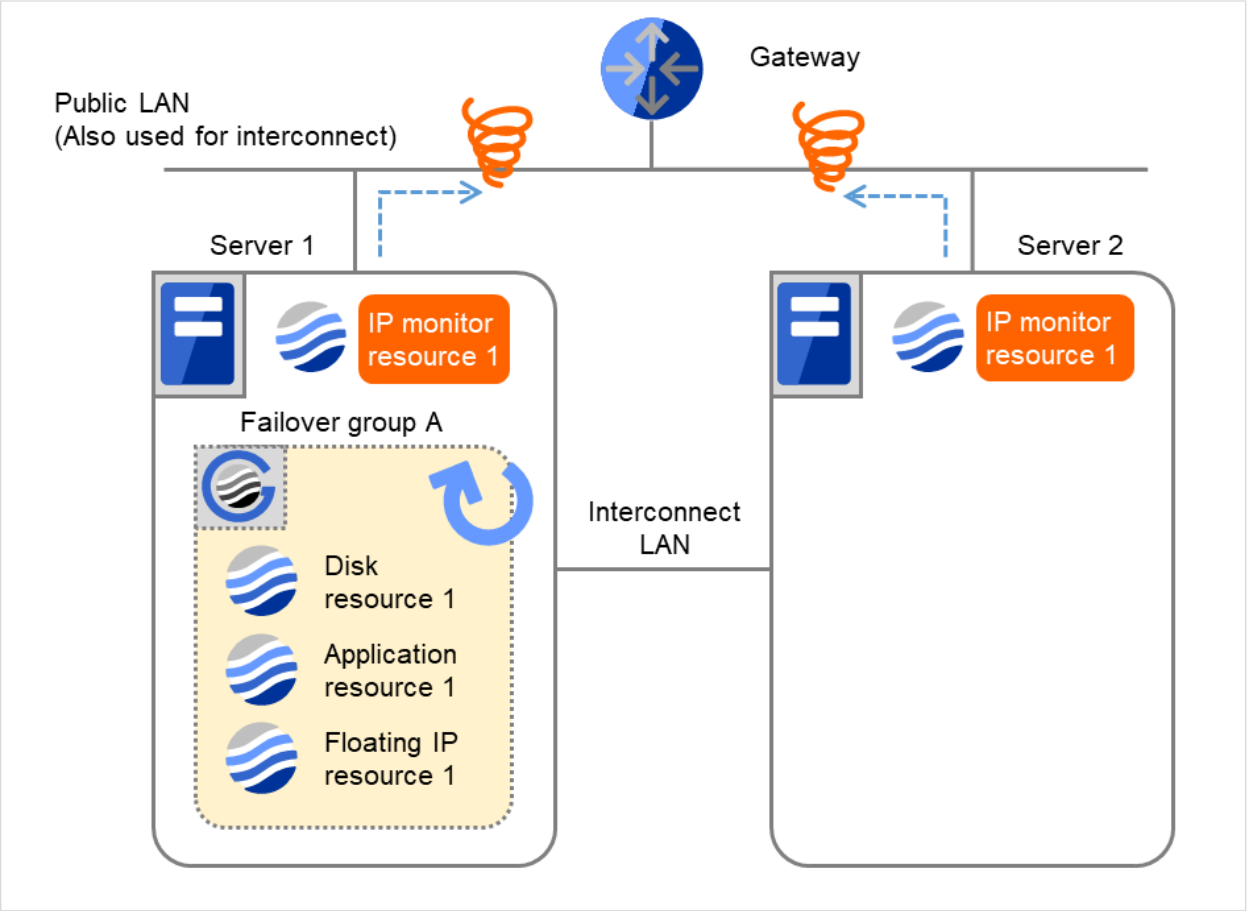


Fig. 4.33: Flow of error detection by the IP monitor resource: normally returning from a monitoring error (6)

	Server 1 IP monitor resource 1	Server 2 IP monitor resource 1
Recovery Script Execution Count	3	0
Reactivation Count	3	0
Failover Count	0	0

4.1.6 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 TUR monitor resource and the disk resource of the Failover Group A:

Configuration of the TUR monitor resource

<Monitor>
Interval 60 seconds
Timeout 120 seconds
Retry Count Zero

<Error detection>
Recovery Target Failover Group A
Recovery Script Execution Count Zero
Maximum Reactivation Count Zero
Maximum Failover Count Set as much as the number of the servers
(2 times in the following case)
Final Action Stop Failover Group

Configuration of the failover group A: disk resource

<Activation error>
Retry Count Zero
Failover Threshold Set as much as the number of the servers
(2 times in the following case)
Final Action No Operation (Next resources are not activated)

<Deactivation abnormality>
Retry Count at Deactivation Failure Zero
Final Action Stop cluster service 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).

(1) The following figure shows an example of monitoring by the disk TUR monitor resource on two servers. On Servers 1 and 2, Disk TUR monitor resource 1 and Failover group A start to be activated. At the intervals, ioctl TUR is executed on the device.

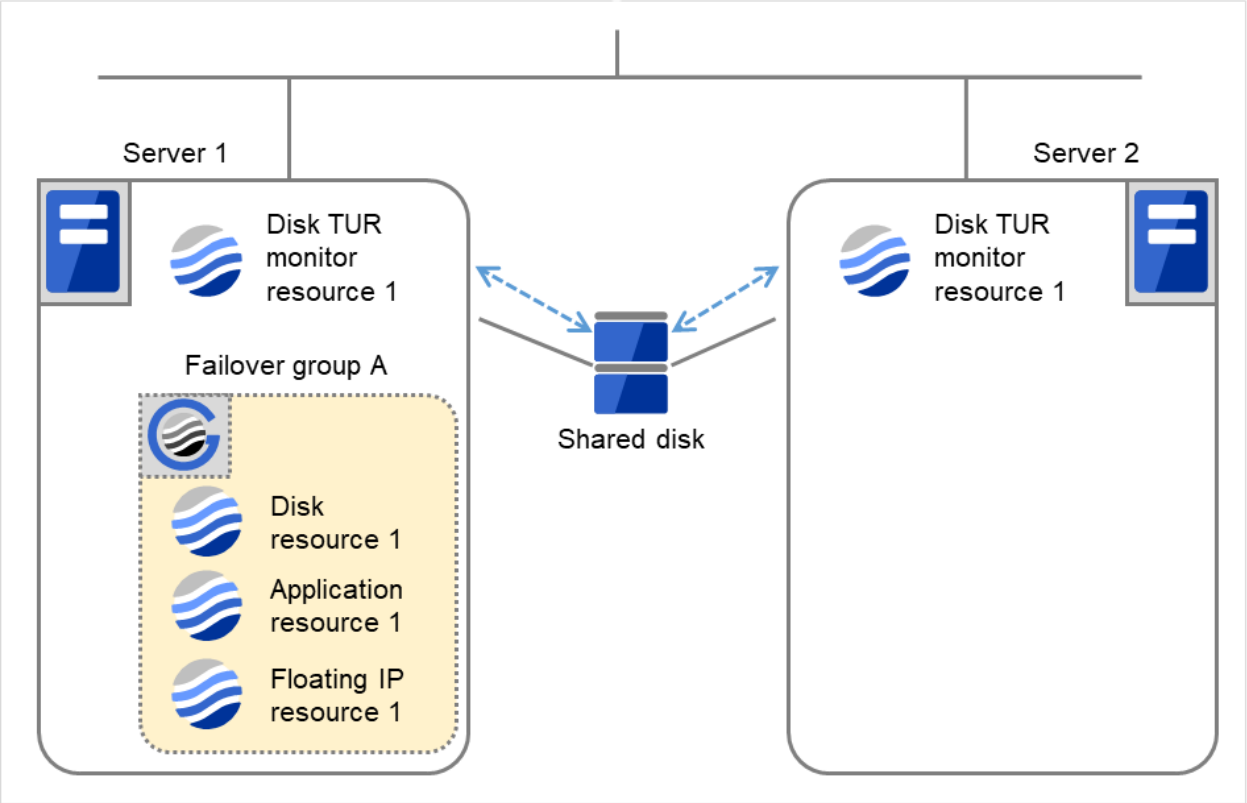


Fig. 4.34: Flow of error detection by the disk TUR monitor resource (1)

	Server 1	Server 2
Disk TUR monitor resource 1 Failover Count	0	0
Disk resource 1 Failover Count	0	0

(2) On Servers 1 and 2, Disk TUR monitor resource 1 detects an error: failure in TUR ioctl.
Depending on the error location of the disk device, the error may be detected during the deactivation of the disk resource.

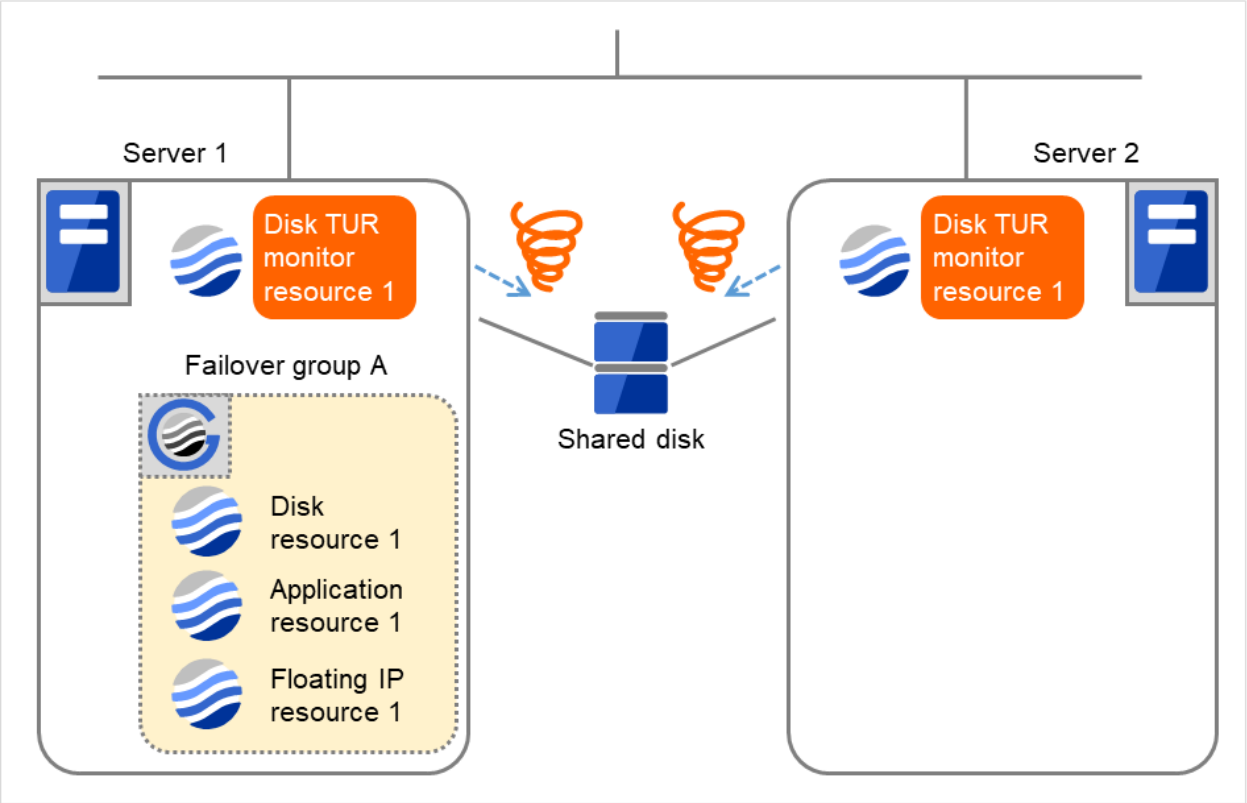


Fig. 4.35: Flow of error detection by the disk TUR monitor resource (2)

(3) Due to the error detected by Disk TUR monitor resource 1 on Server 1, Failover group A starts to be failed over. The failover threshold of the monitor resource means how many times the failover is performed on each server. This is the first failover on Server 1.

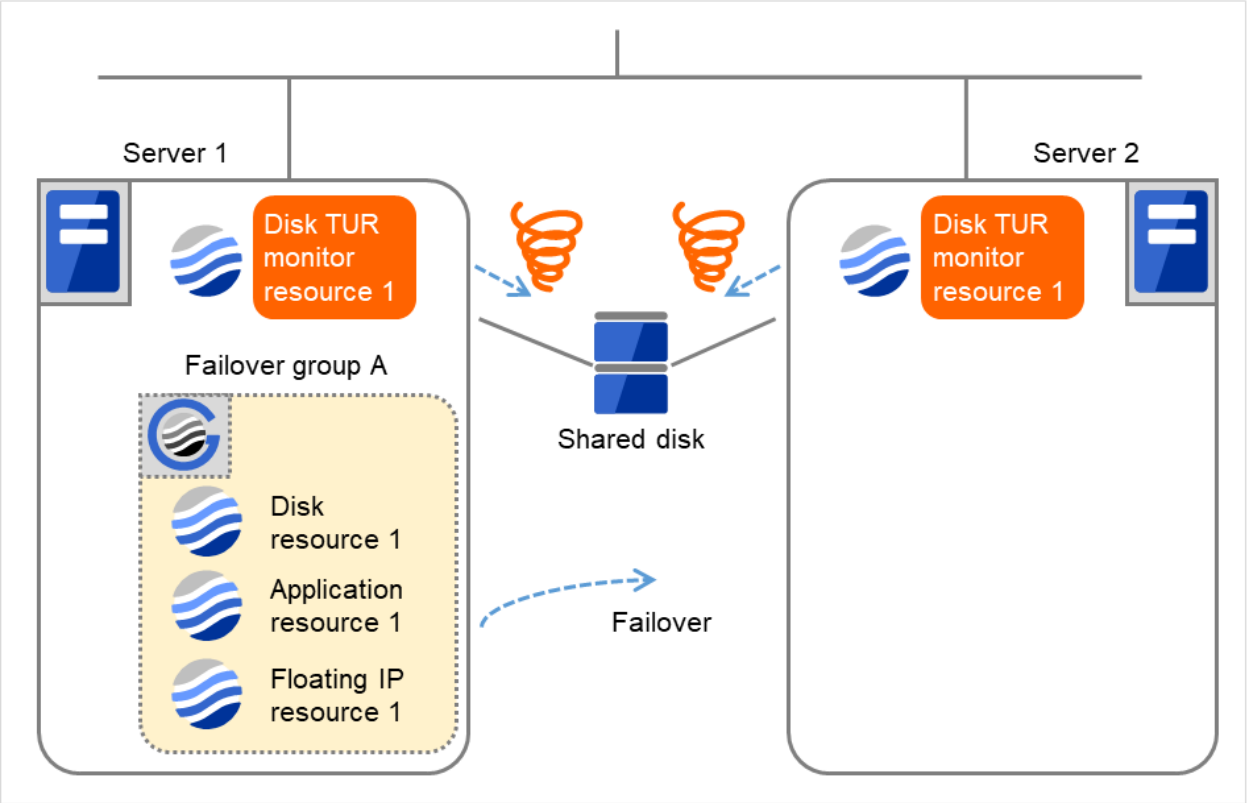


Fig. 4.36: Flow of error detection by the disk TUR monitor resource (3)

	Server 1	Server 2
Disk TUR monitor resource 1 Failover Count	1	1
Disk resource 1 Failover Count	0	0

(4) On Server 2, due to the failover, activating Disk resource 1 fails.

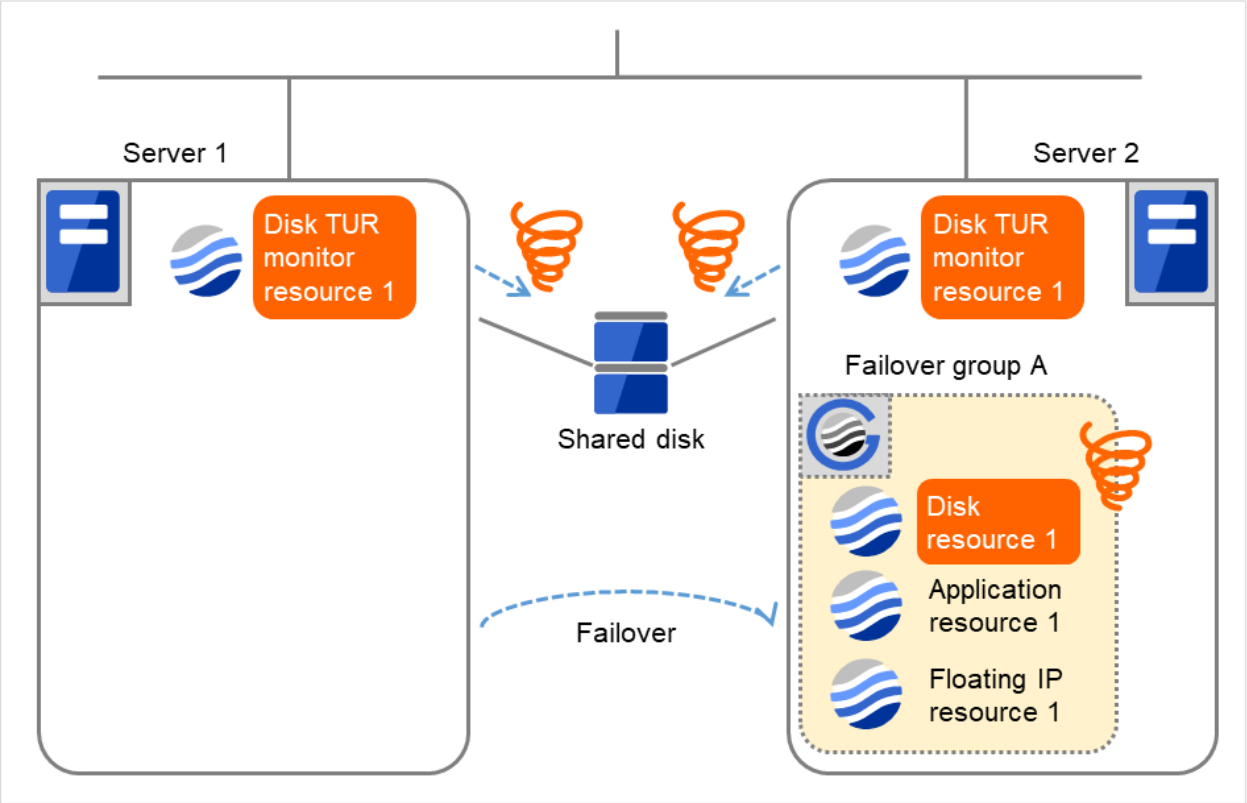


Fig. 4.37: Flow of error detection by the disk TUR monitor resource (4)

(5) Due to the activation failure of Disk resource 1 on Server 2, Failover group A starts to be failed over.
The failover threshold of the group resource means how many times the failover is performed on each server.
This is the first failover on Server 2.
Depending on the error location of the disk device, the error may be detected during the deactivation of the disk resource.

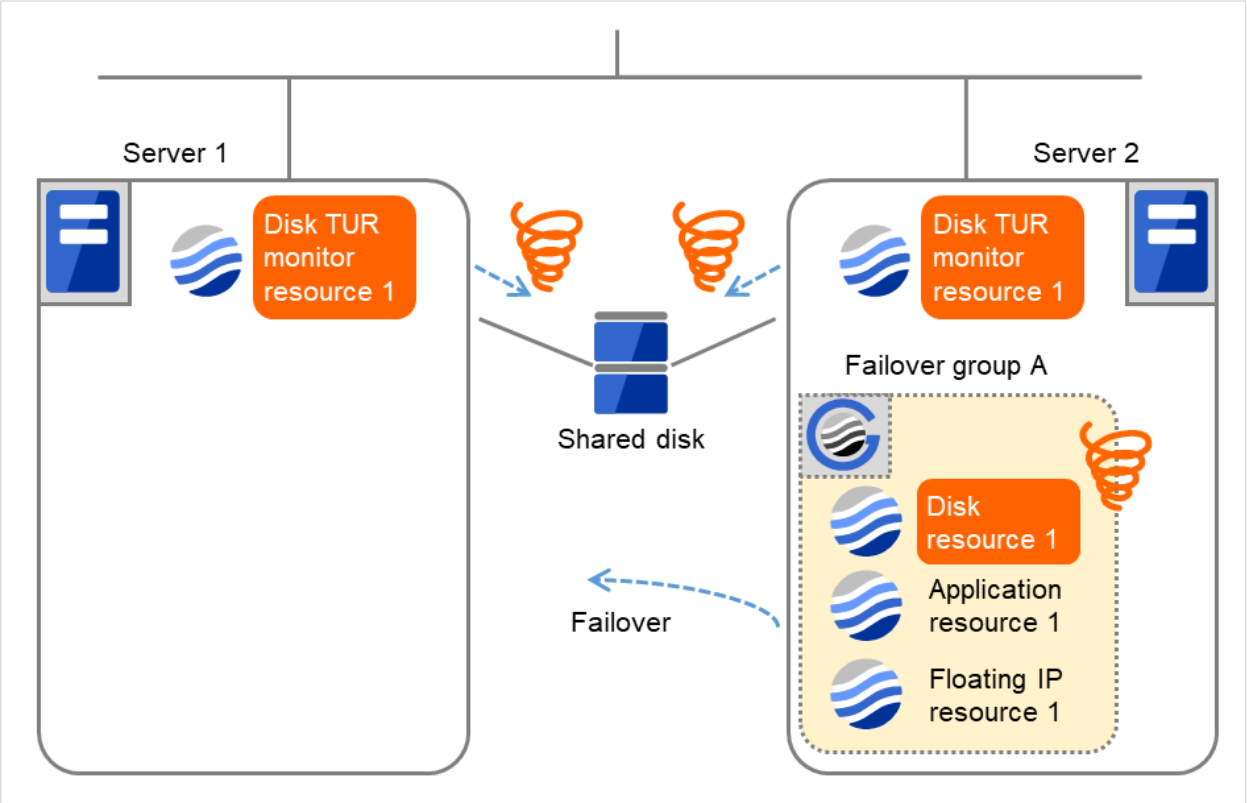


Fig. 4.38: Flow of error detection by the disk TUR monitor resource (5)

	Server 1	Server 2
Disk TUR monitor resource 1 Failover Count	1	1
Disk resource 1 Failover Count	1	1

The TUR 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 " *Behavior when an error is detected by a monitor resource* "

(6) On Server 1, due to the failover, activating Disk resource 1 fails.
Depending on the error location of the disk device, the error may be detected during the deactivation of the disk resource.

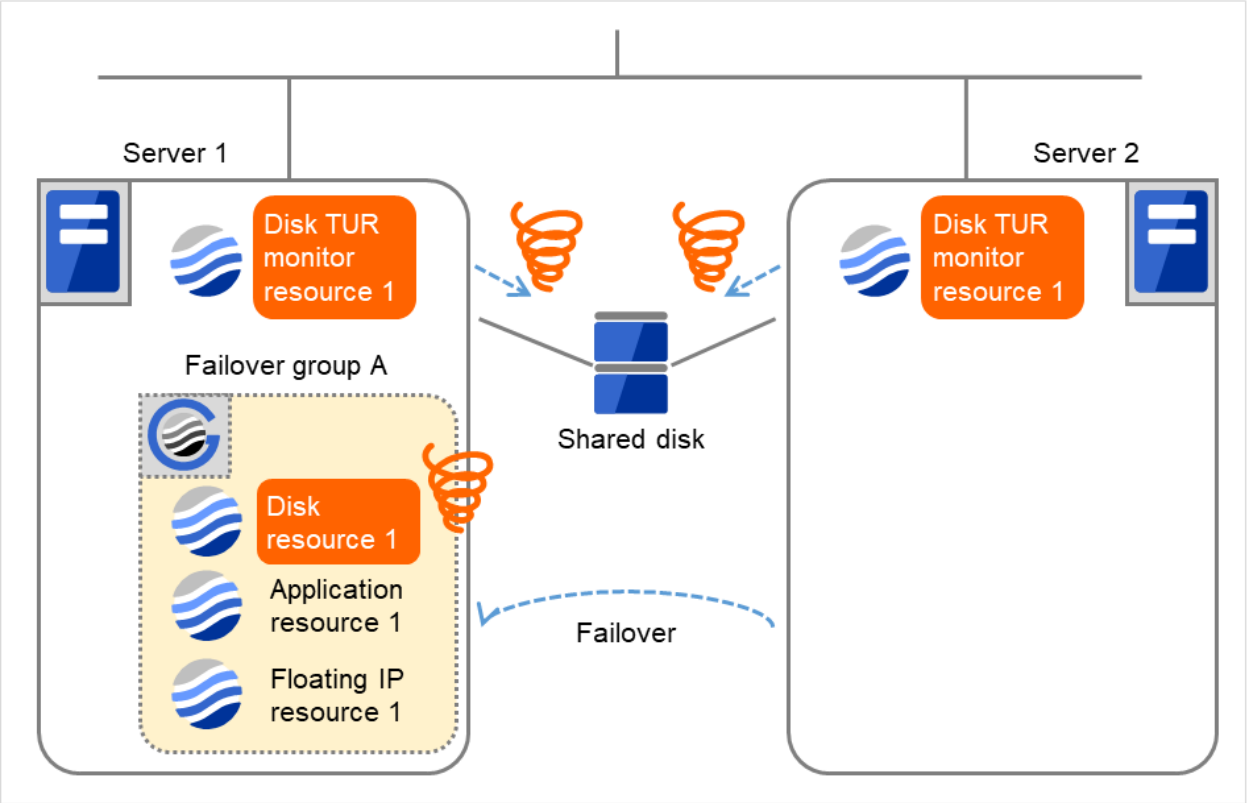


Fig. 4.39: Flow of error detection by the disk TUR monitor resource (6)

	Server 1	Server 2
Disk TUR monitor resource 1 Failover Count	1	1
Disk resource 1 Failover Count	1	1

(7) Due to the activation failure of Disk resource 1 on Server 1, Failover group A starts to be failed over. This is the first failover on Server 1.

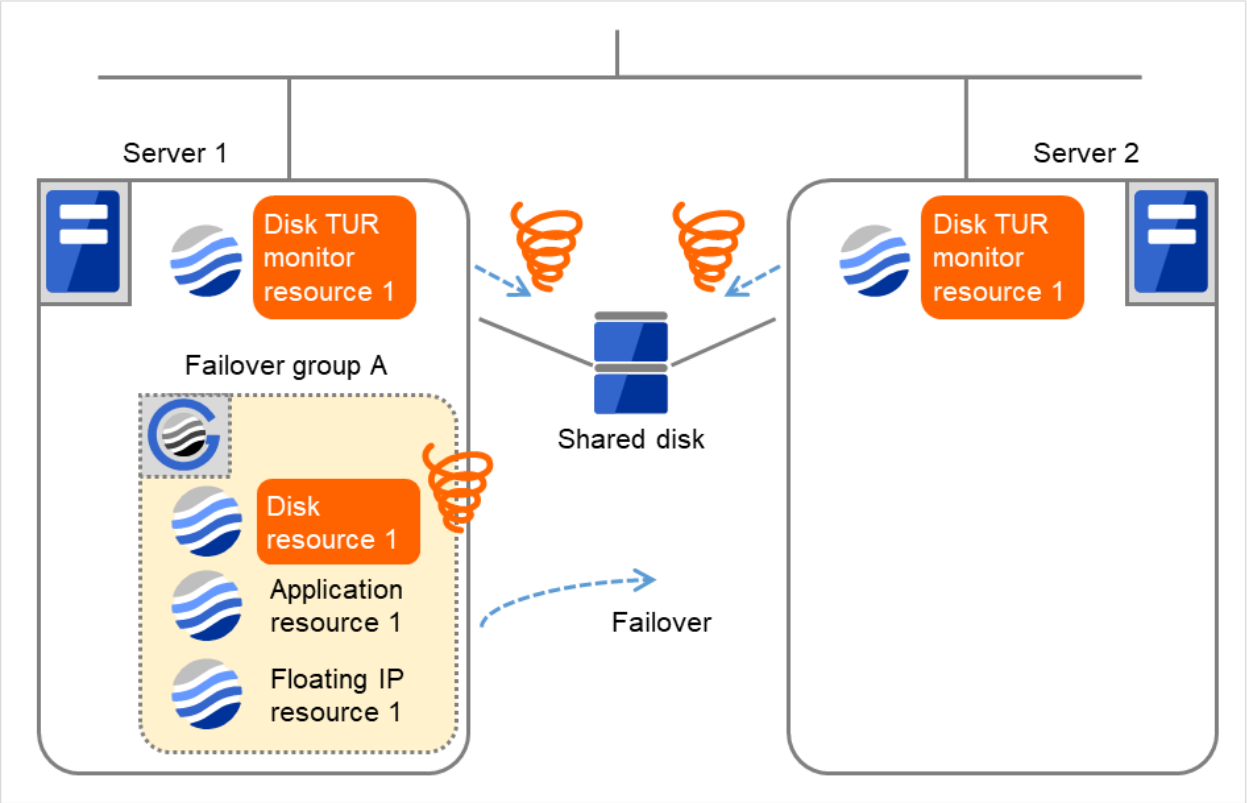


Fig. 4.40: Flow of error detection by the disk TUR monitor resource (7)

	Server 1	Server 2
Disk TUR monitor resource 1 Failover Count	1	1
Disk resource 1 Failover Count	2	2

(8) On Server 2, due to the failover, activating Disk resource 1 fails.
Depending on the error location of the disk device, the error may be detected during the deactivation of the disk resource.

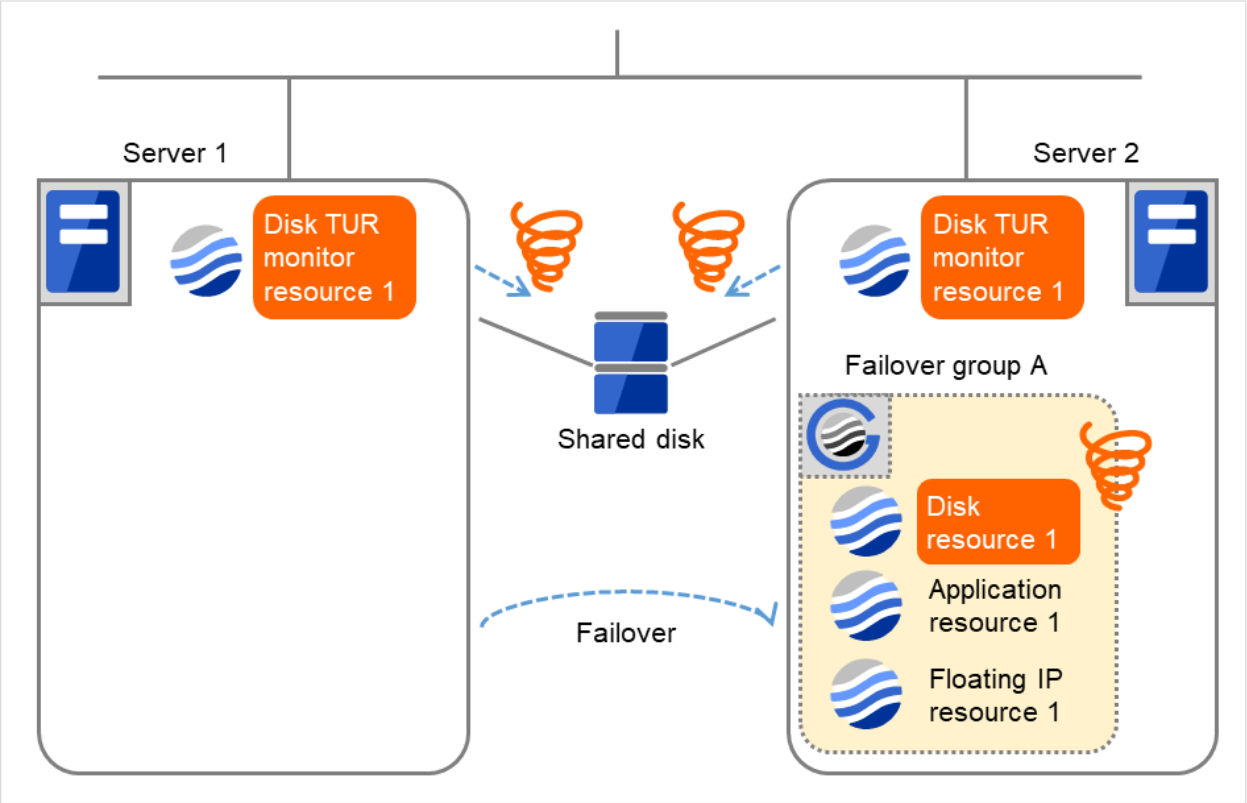


Fig. 4.41: Flow of error detection by the disk TUR monitor resource (8)

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.

(9) Due to the activation failure of Disk resource 1 on Server 2, the final action has been taken.

An activation failure occurs in Failover group A.

Depending on the error location of the disk device, the error may be detected during the deactivation of the disk resource.

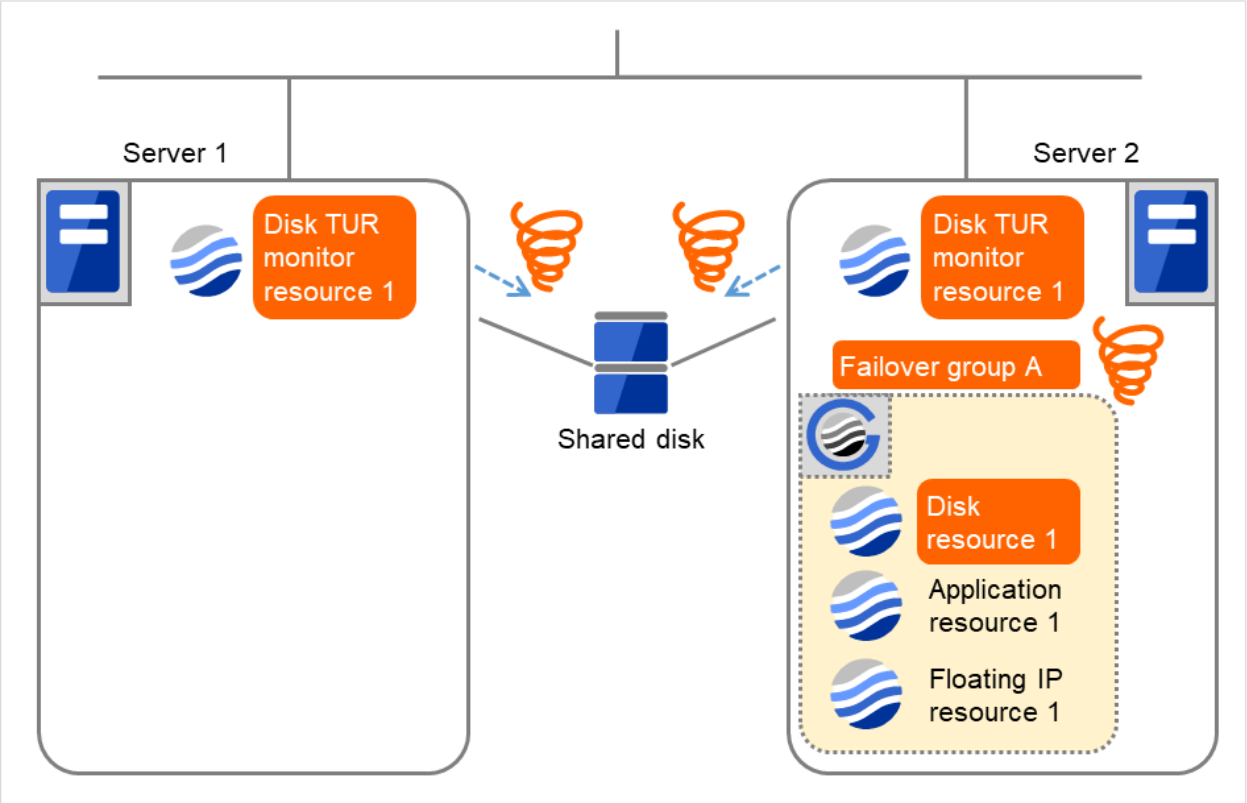


Fig. 4.42: Flow of error detection by the disk TUR monitor resource (9)

(10) Due to the error detected by Disk TUR monitor resource 1 on Server 2, Failover group A starts to be failed over. This is the first failover on Server 2.

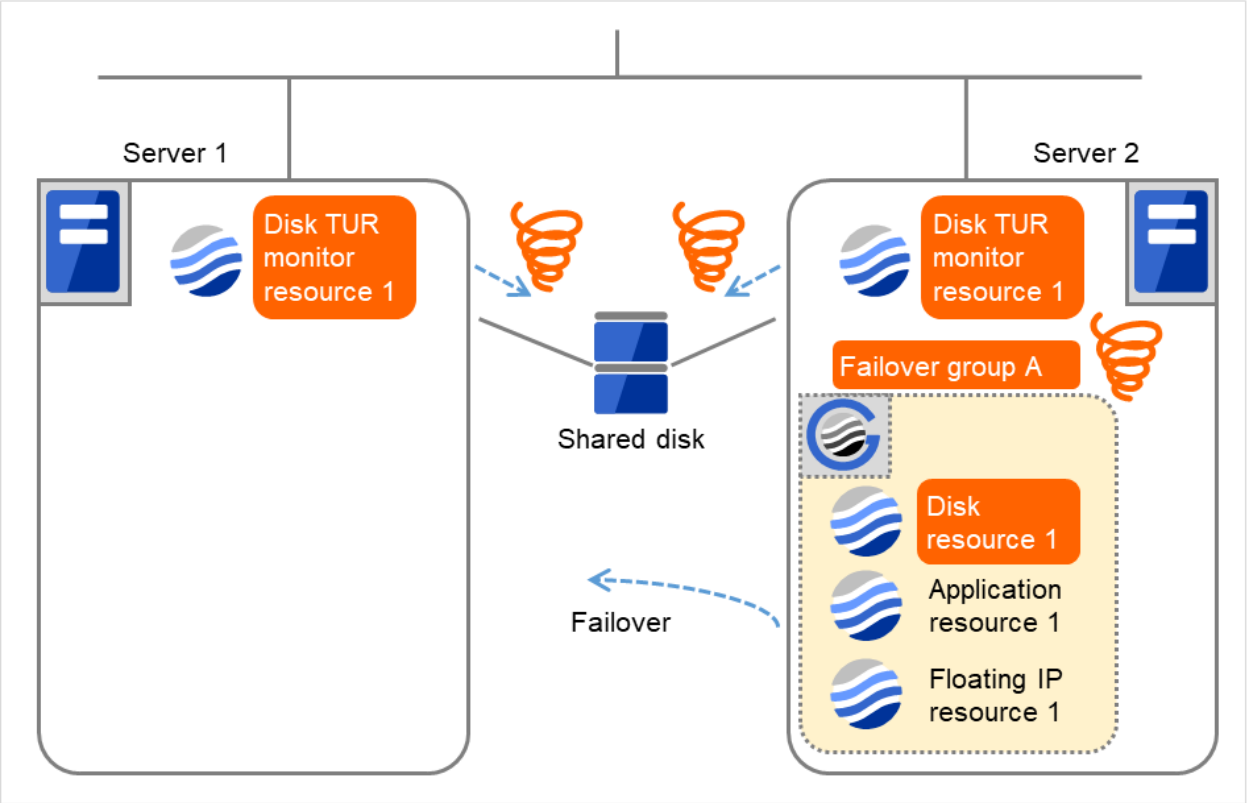


Fig. 4.43: Flow of error detection by the disk TUR monitor resource (10)

	Server 1	Server 2
Disk TUR monitor resource 1 Failover Count	2	2
Disk resource 1 Failover Count	2	2

(11) On Server 1, due to the failover, activating Disk resource 1 fails.

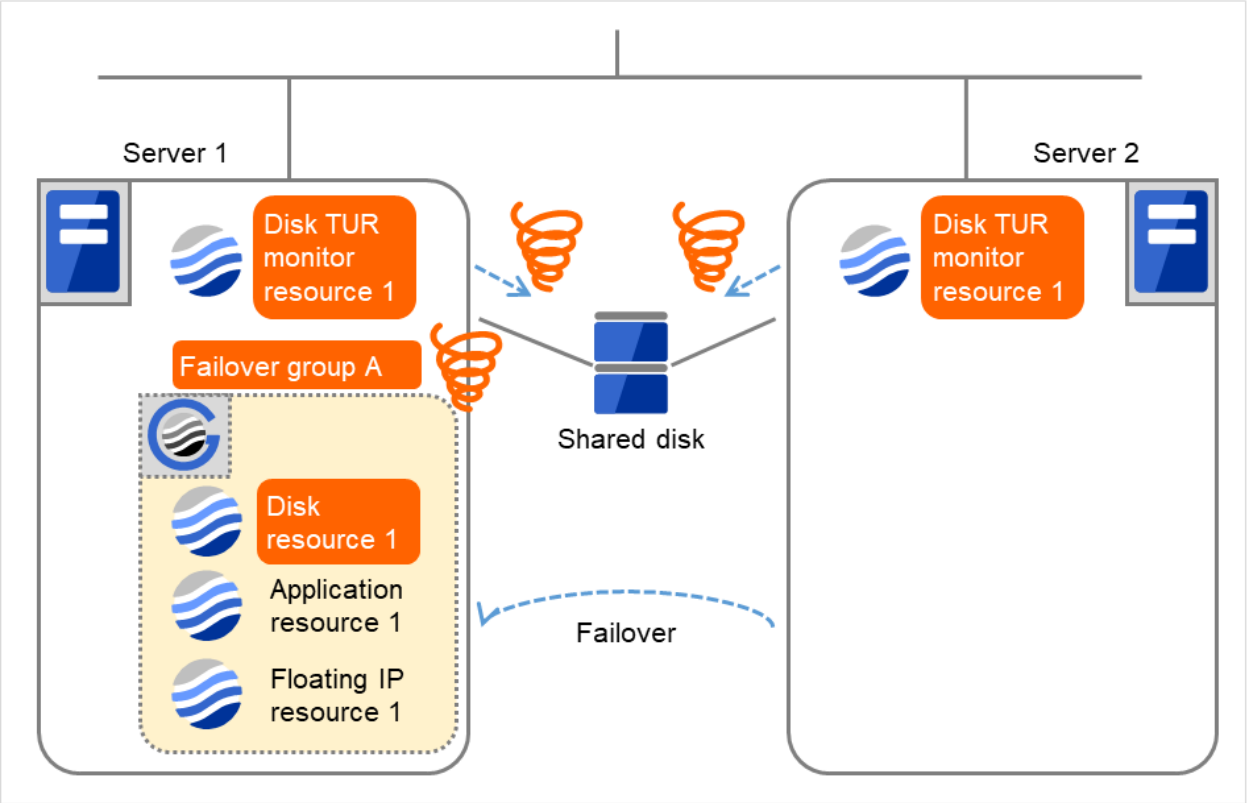


Fig. 4.44: Flow of error detection by the disk TUR monitor resource (11)

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.

(12) Due to the error detected by Disk TUR monitor resource 1 on Server 1, the final action (**Stop Failover Group**) starts to be taken for Failover group A.

The final action is executed in server1 because the number of failovers due to monitoring error detected by the disk TUR monitor resource 1 has exceeded the threshold.

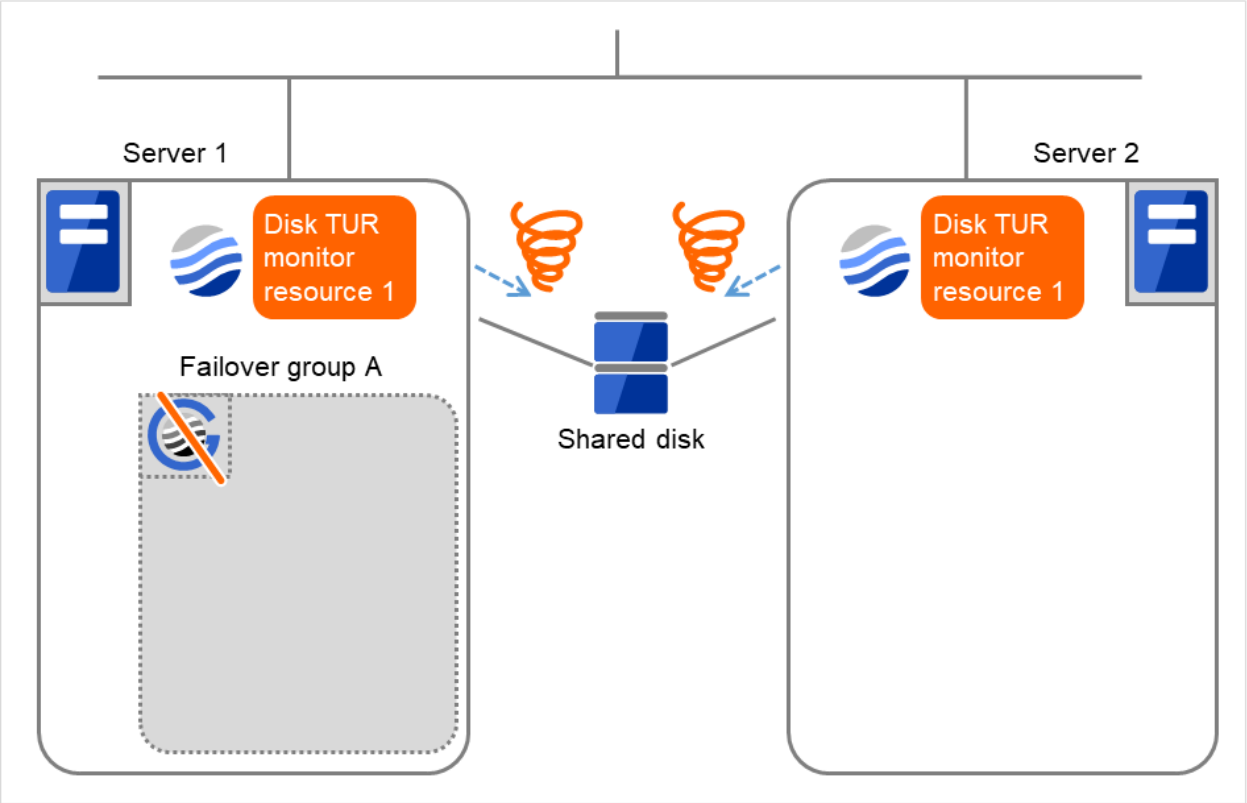


Fig. 4.45: Flow of error detection by the disk TUR monitor resource (12)

(13) After the Failover Group A is stopped due to the final action executed for the disk TUR monitor resource 1 in server1, nothing will happen even if an error is detected by the disk TUR monitor resource 1.

However, note that the final action for the disk TUR monitor resource 1 is executed in server2 if the Failover Group A is manually activated because the final action for the disk monitor TUR resource 1 is not executed yet.

4.1.7 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	EXPRESSCLUSTER full version	Represents the EXPRESSCLUSTER full version. Example: 13.20
CLP_VERSION_MAJOR ...EXPRESSCLUSTER major version	EXPRESSCLUSTER major version	Represents the EXPRESSCLUSTER major version. Example: 13
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER installation path	Represents the path where EXPRESSCLUSTER is installed. Example: `C:\Program Files\EXPRESSCLUSTER`
CLP_OSNAME ...Server OS name	Server OS name	Represents the OS name of the server where the script was executed. Example: Windows Server 2016 Standard
CLP_OSVER ...Server OS version	Server OS version	Represents the OS version of the server where the script was executed. Example: 10.0.14393
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.

Continued on next page

Table 4.27 – continued from previous page

Environment variable	Value of the environment variable	Description
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

```
rem ****************************************************
rem *                    preaction.bat                 *
rem ****************************************************

echo START

IF "%CLP_ACTION%"=="" GOTO NO_CLP

IF "%CLP_ACTION%"=="RECOVERY" GOTO RECOVERY
IF "%CLP_ACTION%"=="RESTART" GOTO RESTART
IF "%CLP_ACTION%"=="FAILOVER" GOTO FAILOVER
IF "%CLP_ACTION%"=="FINALACTION" GOTO FINALACTION


:RECOVERY
echo RECOVERY COUNT: %CLP_RECOVERYCOUNT%

rem Here, write a recovery process.
rem This process is to be performed at the timing of the following:
rem
rem  Recovery action: recovery script

GOTO EXIT


:RESTART
echo RESTART COUNT: %CLP_RESTARTCOUNT%

rem Here, write a pre-reactivation process.
rem This process is to be performed at the timing of the following:
rem
rem  Recovery action: reactivation

GOTO EXIT


:FAILOVER
```

(continues on next page)

(continued from previous page)

```
echo FAILOVER COUNT: %CLP_FAILOVERCOUNT%

rem Here, write a recovery process.
rem This process is to be performed at the timing of the following:
rem
rem  Recovery action: failover

GOTO EXIT


:FINALACTION
echo FINALACTION

rem Here, write a recovery process.
rem This process is to be performed at the timing of the following:
rem
rem  Recovery action: final action

:NO_CLP

:EXIT
echo EXIT
exit
```

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.

Note on the recovery/pre-recovery action script

- 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.

4.1.8 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 the time for monitor processing (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.

The following figure shows a case with the monitoring timeout set at 60 seconds and the delay warning rate set at 80% (48 seconds). The arrows indicate monitor polling times.

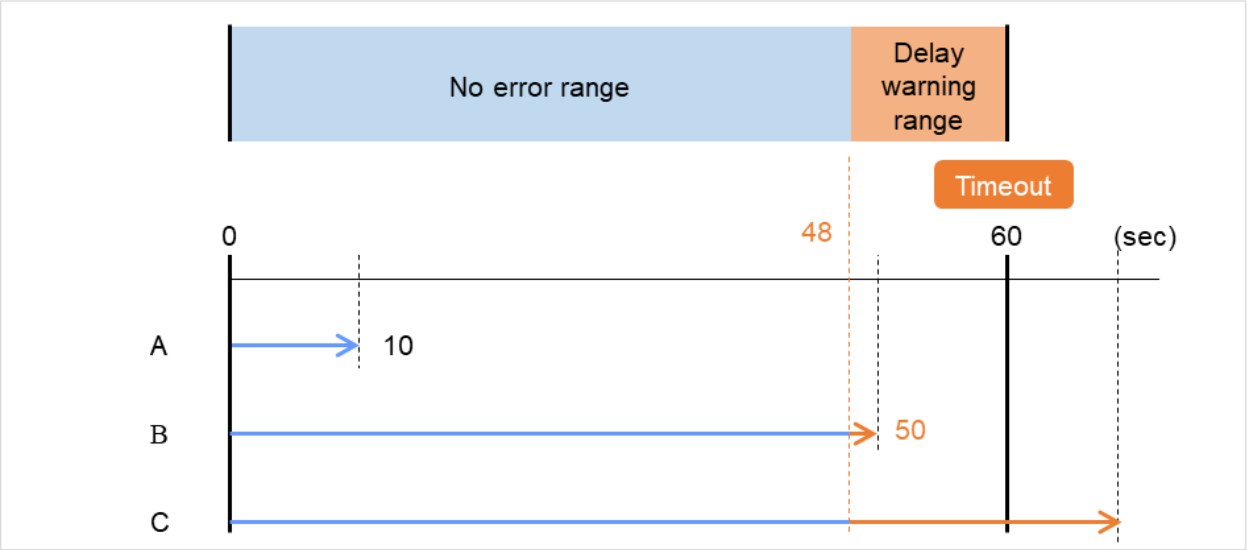


Fig. 4.46: Monitor polling times and a delay warning

A. The time for monitor processing is 10 seconds. The monitor resource is in normal status.
   In this case, no alert is used.

B. The time for monitor processing is 50 seconds and the delay of monitoring is detected during this time. 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 time for monitor processing has exceeded 60 seconds of the monitoring timeout and the delay of monitoring is detected. The monitor resource has a problem.
   In this case, no alert is used.

Alert for the delay warning is used for the heartbeat resources as well.

See also:

To configure the delay warning of monitor resources, click Cluster Properties, click Delay Warning, and select Monitor Delay Warning. For details, refer to "2. *Parameter details*" in this guide.

4.1.9 Waiting for monitor resource to start monitoring

"Wait Time to Start Monitoring" refers to start monitoring after the time period 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.

If the wait time to start monitoring is set at 0 seconds, the monitor resource polling is started after a cluster startup or a monitor resumption.

Configuration of monitor resource

<Monitor>
Interval 30 sec
Timeout 60 sec
Retry Count 0 time
Wait Time to Start Monitoring 0 sec

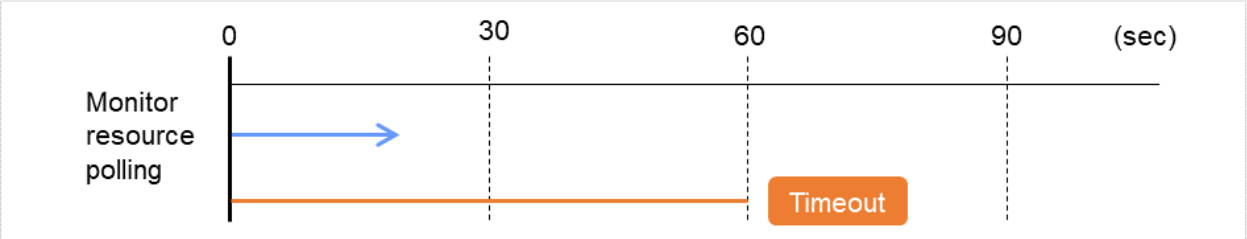


Fig. 4.47: Waiting for monitor resource to start monitoring (with its time set at 0 seconds)

If the wait time to start monitoring is set at 30 seconds, the monitor resource polling is started 30 seconds after a cluster startup or a monitor resumption.

<Monitor>
Interval 30 sec
Timeout 60 sec
Retry Count 0 time
Wait Time to Start Monitoring 30 sec

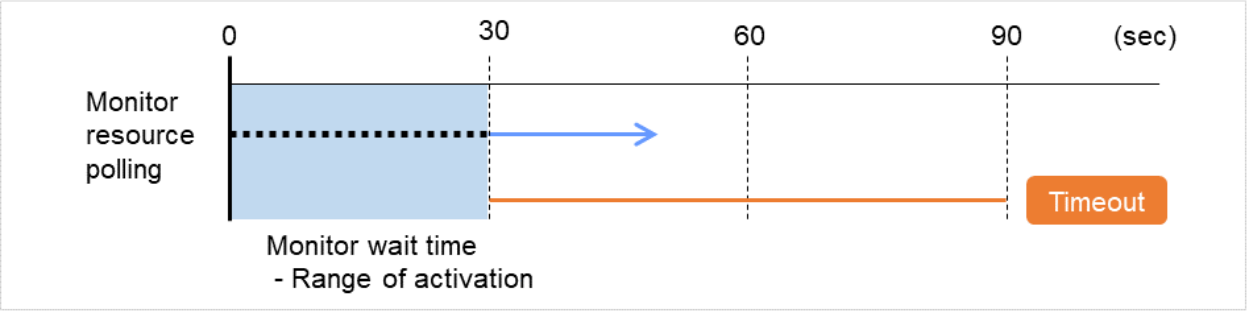


Fig. 4.48: Waiting for monitor resource to start monitoring (with its time set at 30 seconds)

Note:

Monitoring will restart 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 application resource monitored by application 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:

In this case, the application is first started. Next, the application monitor resource starts monitoring, then ends its polling. After that, however, the application abends for some reason.

Configuration of application monitor resource

<Monitor>
Interval 5 sec
Timeout 60 sec
Retry Count Zero
Wait Time to Start Monitoring 0 sec (default)

<Error Detection>
Recover Target appli1
Maximum Reactivation Count 1
Maximum Failover Count 1
Final Action Stop Group

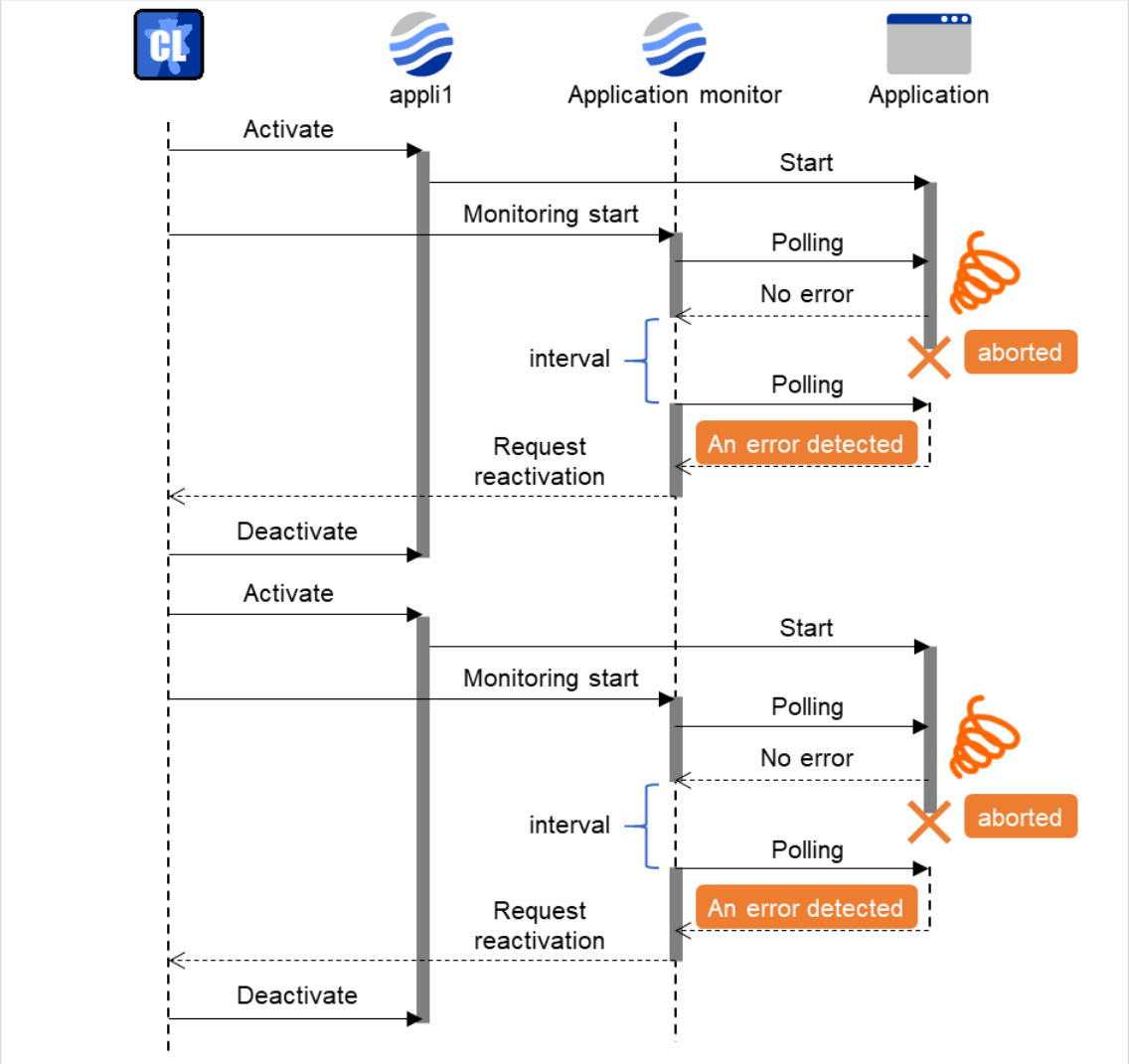


Fig. 4.49: Waiting for monitor resource to start monitoring (with its time set at 0 seconds)

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.

In this case, the application is first started. Next, through the specified wait time to start monitoring, the application monitor resource starts monitoring. After that, the application abends for some reason. However, the abend is detected with the first round of polling by the application monitor resource.

Configuration of application monitor resource

<Monitor>
Interval 5 sec
Timeout 60 sec
Retry Count Zero
Wait Time to Start Monitoring 60 sec

<Error Detection>
Recover Target appli1
Maximum Reactivation Count 1
Maximum Failover Count 1
Final Action Stop Group

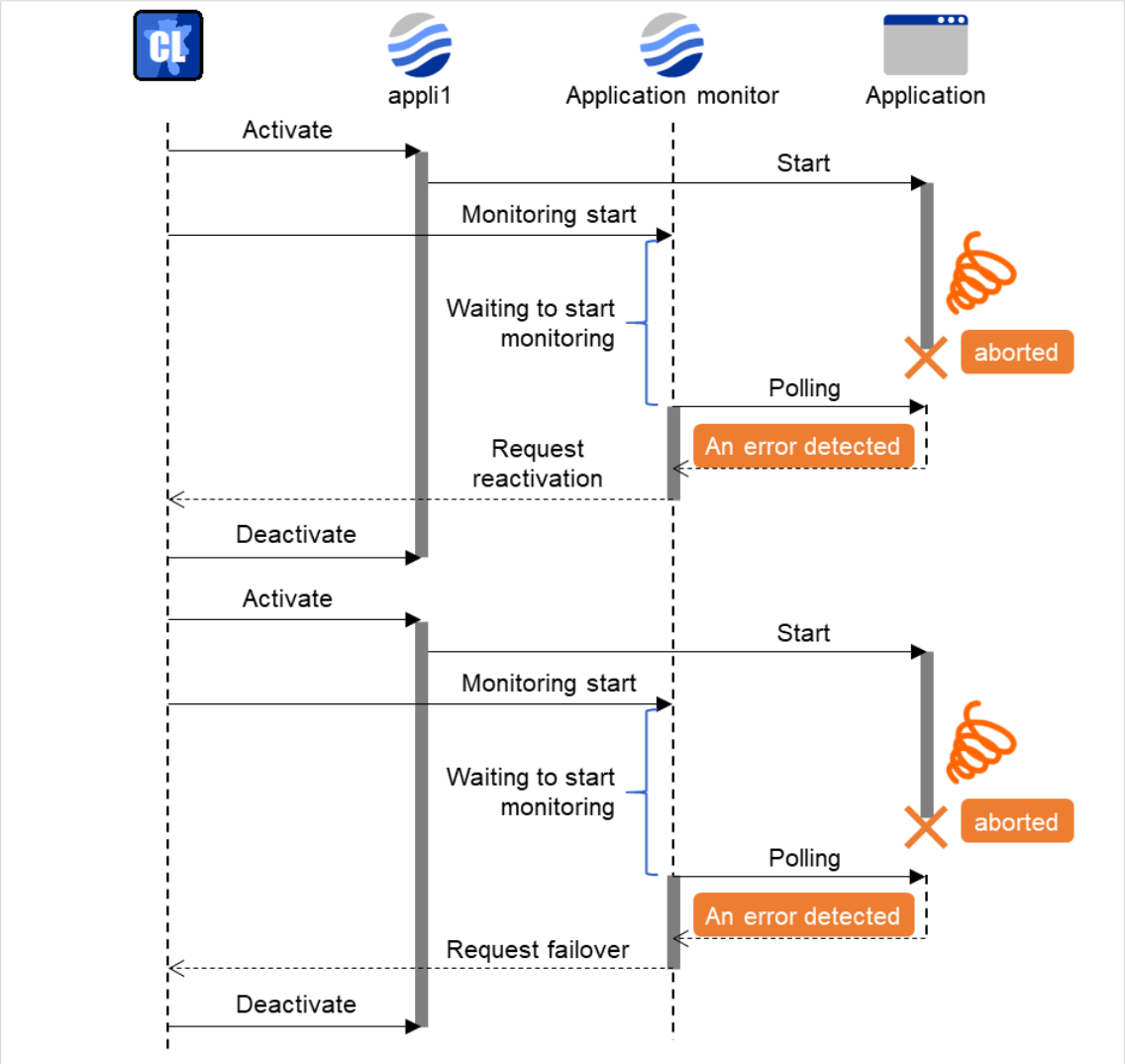


Fig. 4.50: Waiting for monitor resource to start monitoring (with its time set at 60 seconds)

If the application is abnormally terminated in the destination server of the group failover, the group stops as the final action.

4.1.10 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 daemon 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 service and reboot OS** is executed once because the maximum reboot count is set to one.

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.

Configuration example

<Monitor>
Interval 60 sec
Timeout 120 sec
Retry count 3 times

<Error Detection>
Recovery Target Failover group A
Maximum Reactivation Count zero
Maximum Failover Count zero
Final Action Stop cluster service and reboot OS

< Reboot count limit>
Maximum reboot count 1
Time to reset the maximum reboot count 10 minutes

(1) The following figure shows an example of monitoring by the disk TUR monitor resource on two servers. Disk TUR monitor resource 1 starts to be activated. At the intervals, an I/O process or other processes are executed on the device.

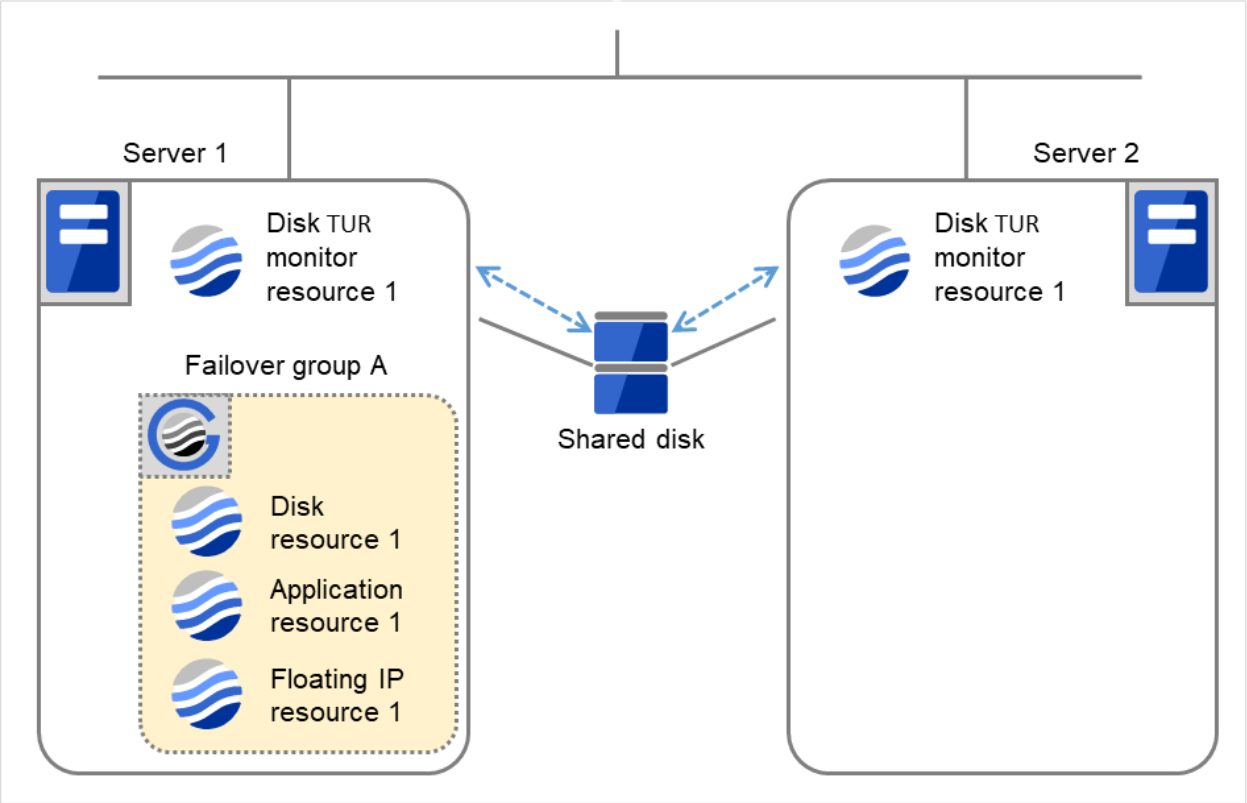


Fig. 4.51: Limiting the number of reboots (1)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	0	0

(2) Disk TUR monitor resource 1 detects an error (e.g. that of ioctl or read).

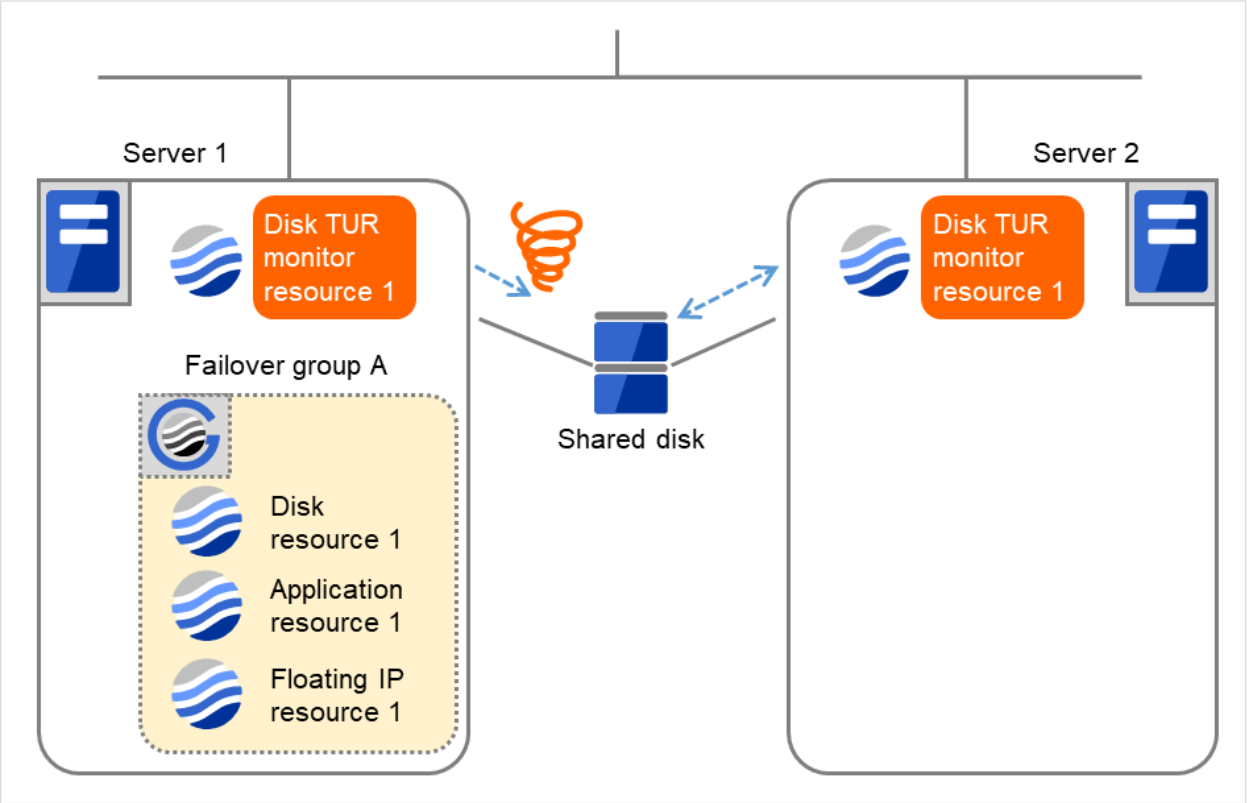


Fig. 4.52: Limiting the number of reboots (2)

(3) Stop the cluster service, and then reboot the OS. Since both **Retry Count at Activation Failure** and **Failover Threshold** are set at zero (0), the final action is taken. The number of reboots is recorded as 1. Then Failover group A starts to be failed over. **Maximum reboot count** represents the upper limit of how many times the startup is done on each server. On Server 2, the number of reboots is zero (0).

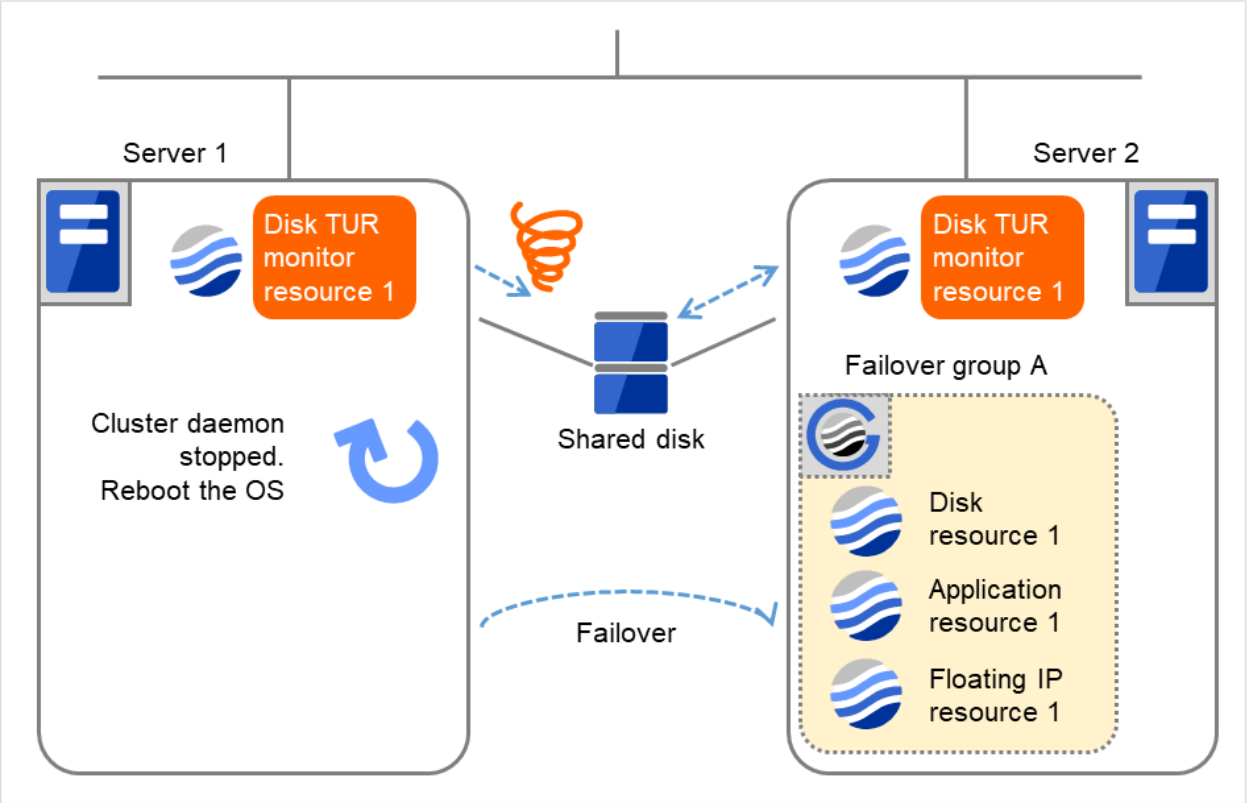


Fig. 4.53: Limiting the number of reboots (3)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(4) Server 1 completes the reboot. Move Failover group A to Server 1 by using the clpgrp command or Cluster WebUI.

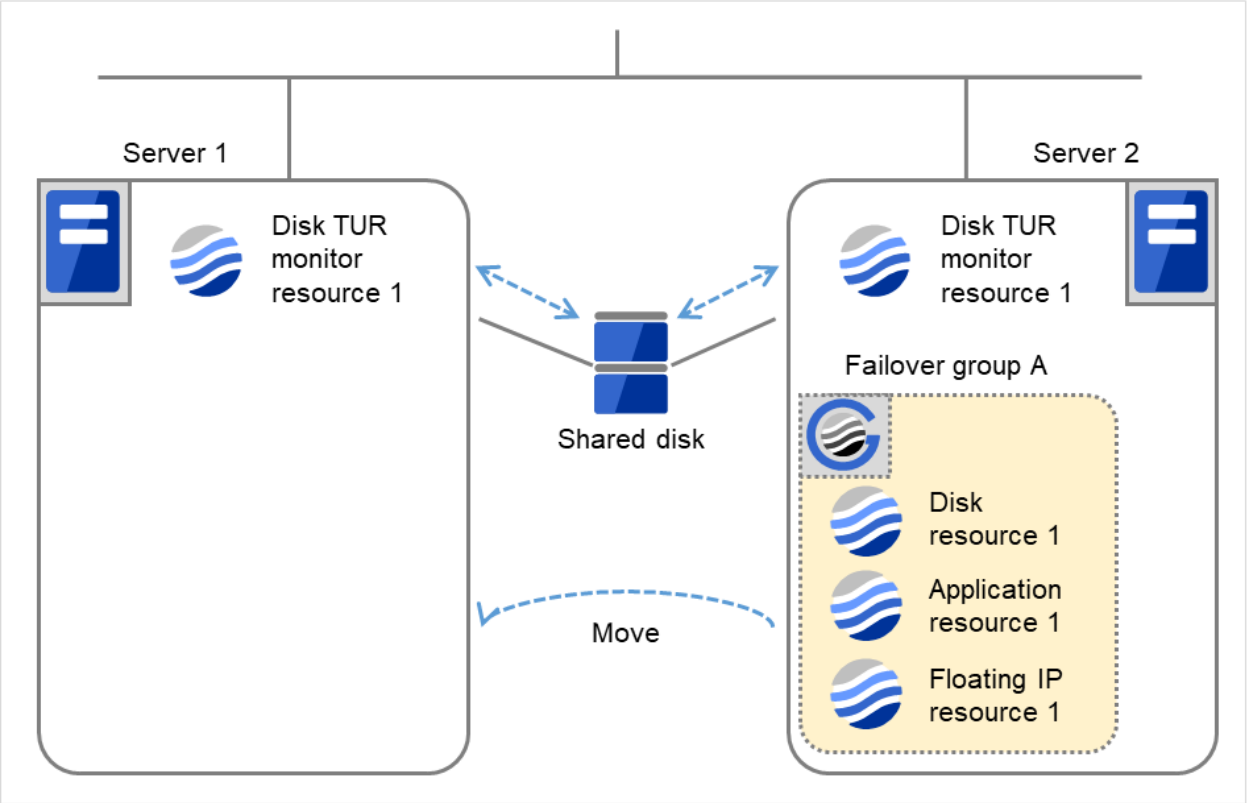


Fig. 4.54: Limiting the number of reboots (4)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(5) Disk TUR monitor resource 1 detects an error (e.g. that of ioctl or read). The final action is not taken on Server 1, because the reboot count has reached its maximum. Even after 10 minutes pass, the reboot count is not reset.

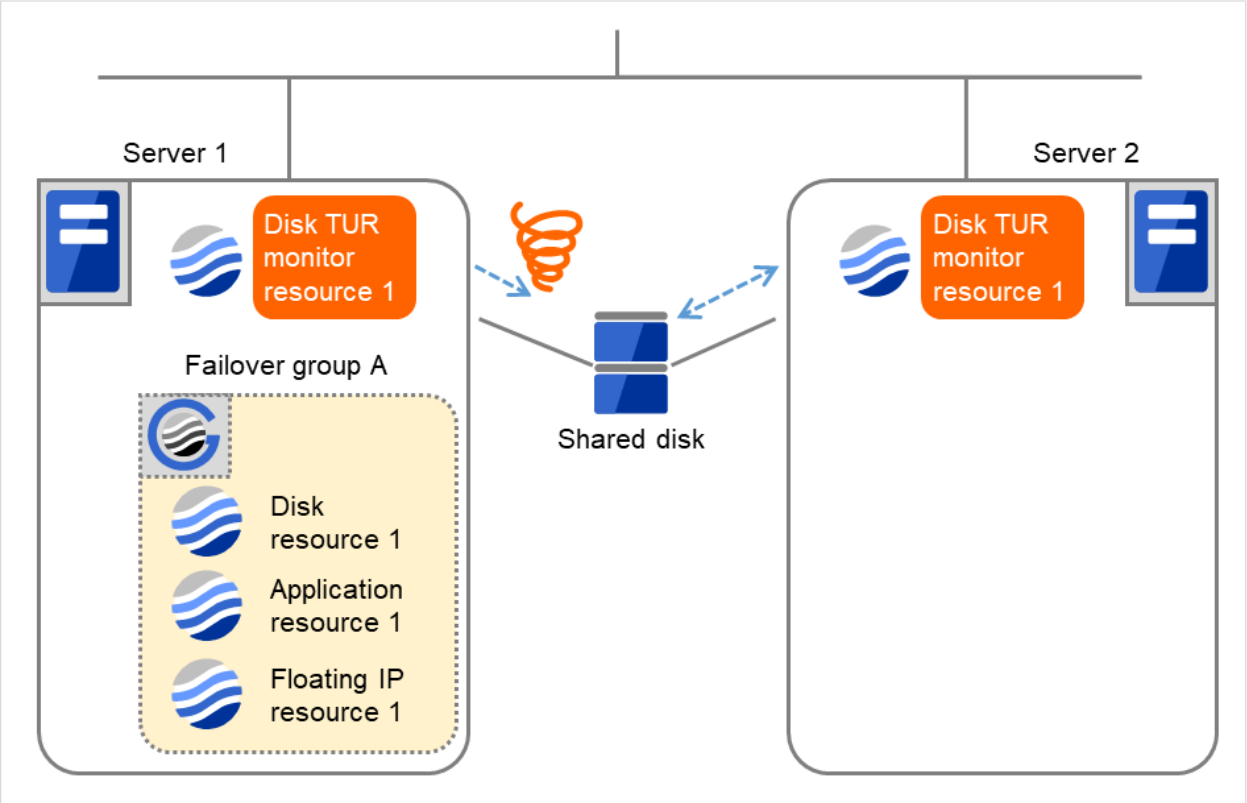


Fig. 4.55: Limiting the number of reboots (5)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(6) Remove the error from the shared disk, shut down the cluster by using the clpstdn command or Cluster WebUI, and then start the reboot.

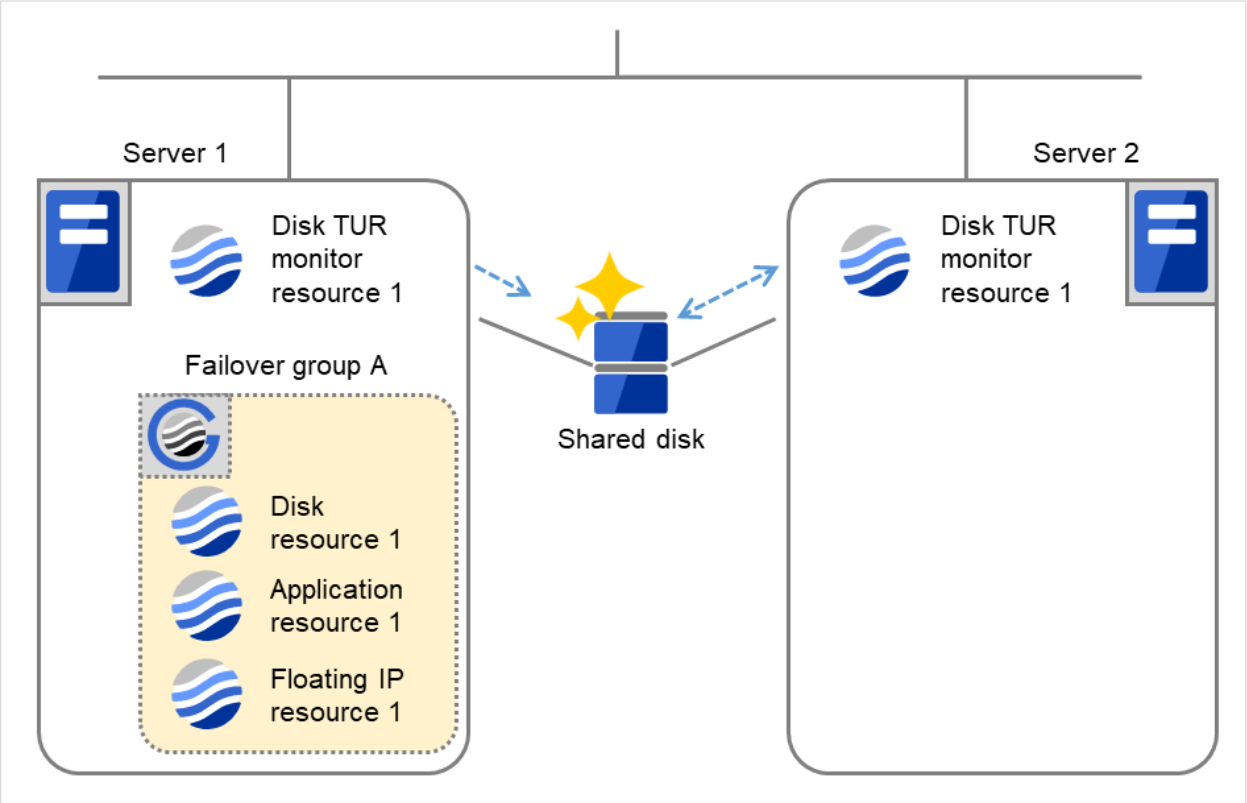


Fig. 4.56: Limiting the number of reboots (6)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	1	0

(7) On Server 1, Disk TUR monitor resource 1 returns to normal. After 10 minutes pass, the reboot count is reset. Next time Disk TUR monitor resource 1 detects an error, the final action is taken.

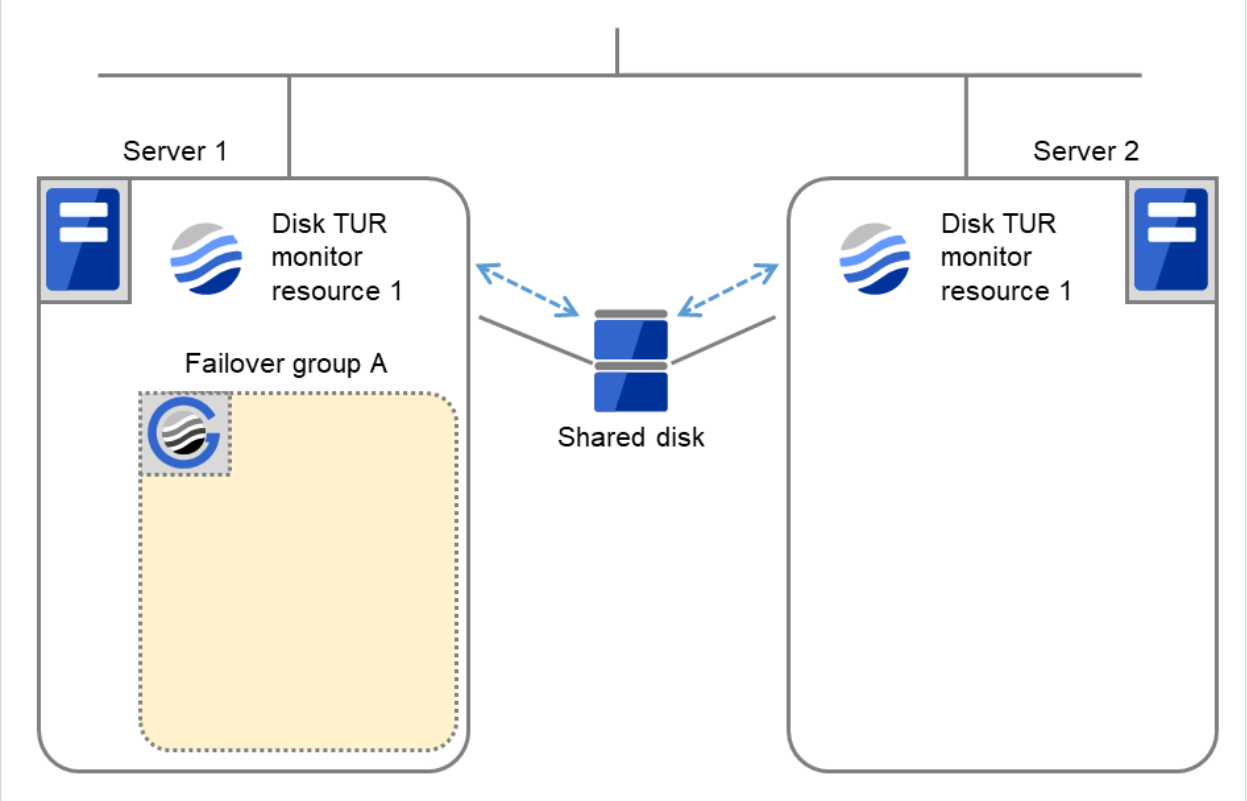


Fig. 4.57: Limiting the number of reboots (7)

	Server 1	Server 2
Maximum reboot count	1	1
Reboot count	0	0

4.1.11 Monitor resources that require a license

Monitor resources listed below require a license because they are optional products. To use these monitor resources, obtain and register a product license.

Optional product name	Monitor resource name
EXPRESSCLUSTER X Database Agent 5.2 for Windows	DB2 monitor resources
	ODBC monitor resources
	Oracle monitor resources
	PostgreSQL monitor resources
	SQL Server monitor resources
EXPRESSCLUSTER X Internet Server Agent 5.2 for Windows	FTP monitor resources
	HTTP monitor resources
	IMAP4 monitor resources
	POP3 monitor resources
	SMTP monitor resources
EXPRESSCLUSTER X Application Server Agent 5.2 for Windows	Tuxedo monitor resources

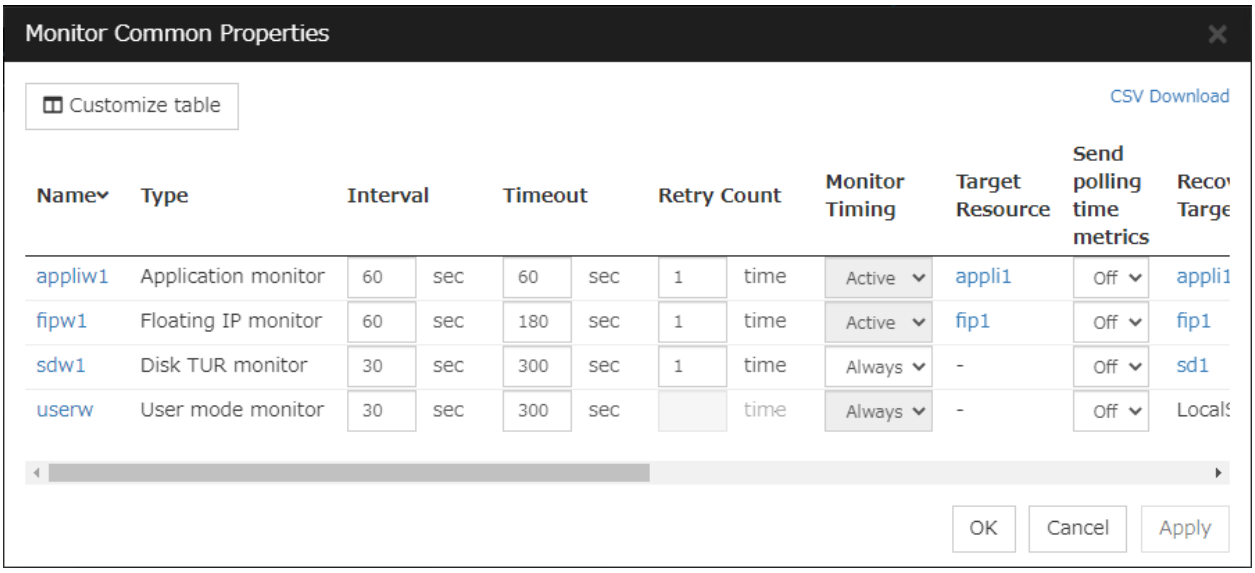
Continued on next page

Table 4.34 – continued from previous page

Optional product name	Monitor resource name
	WebSphere monitor resources
	WebLogic monitor resources
	WebOTX monitor resources
EXPRESSCLUSTER X Java Resource Agent 5.2 for Windows	JVM monitor resources
EXPRESSCLUSTER X System Resource Agent 5.2 for Windows	System monitor resources
	Process resource monitor resources

For information on how to register a license, refer to " Registering the license" in the "Installation and Configuration Guide".

4.2 Monitor Common Properties



Displays a list of monitor resources.

Allows you to change the various settings.

Clicking a name link takes you to the property screen of the corresponding monitor resource.

Allows you to rearrange the items of the list by selecting their names or types.

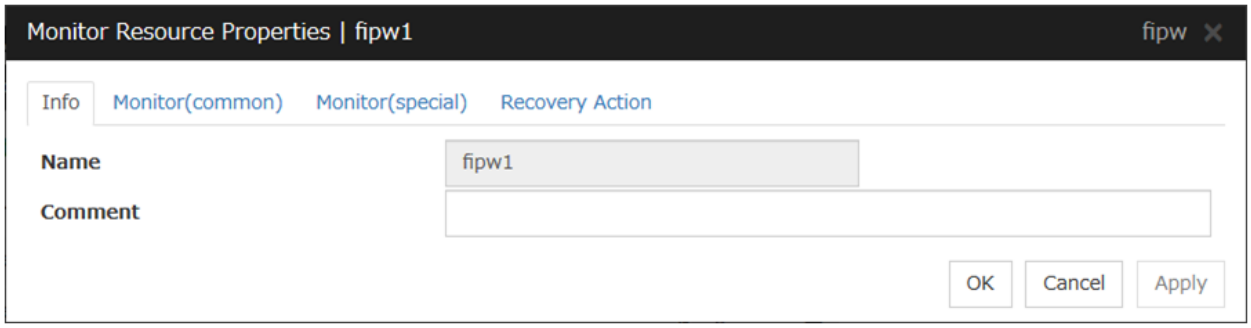
Selecting **Customize table** displays the **Customize table** dialog box, where you can set which items are shown in or hidden from the list.

Clicking CSV Download downloads data, in CSV format, shown in the monitor resource list.

For more information on the displayed items, see " *Monitor resource properties* ".

4.3 Monitor resource properties

4.3.1 Info tab

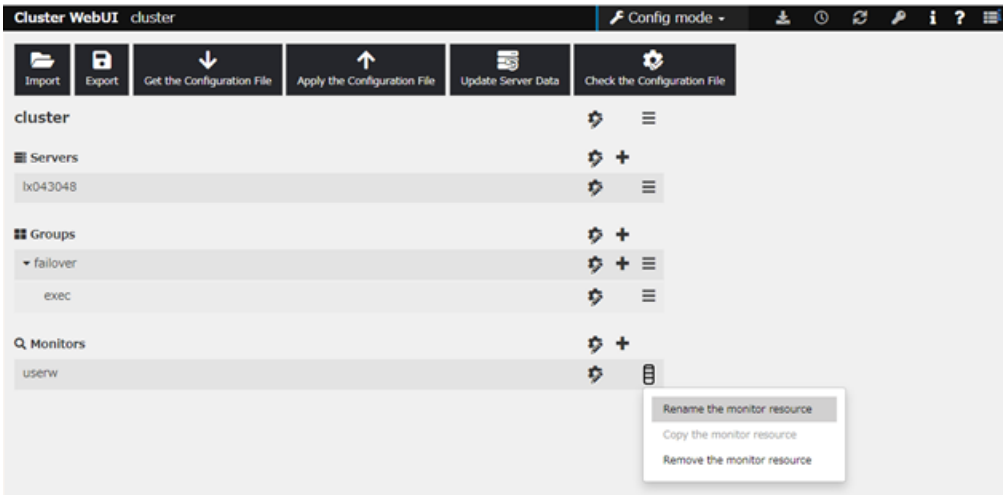


Name

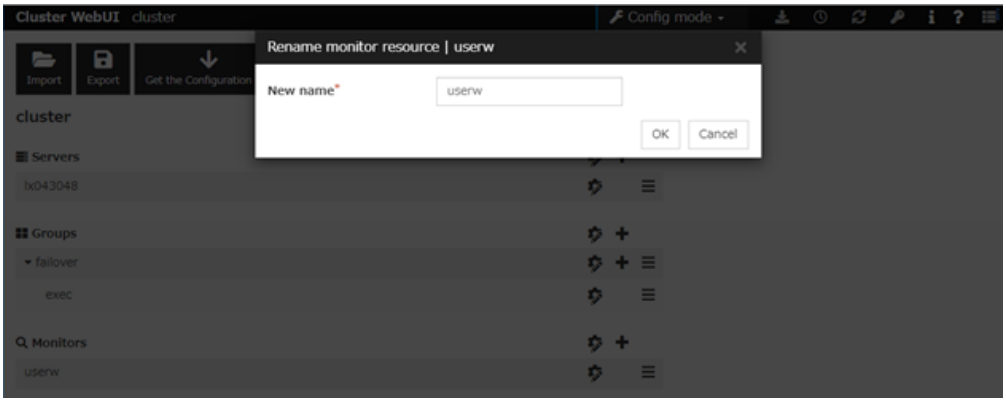
The monitor resource name is displayed.

Changing the monitor resource name

1. click **others**, and then select **Rename the monitor resource**.



2. A dialog box to **rename monitor resource** is displayed.



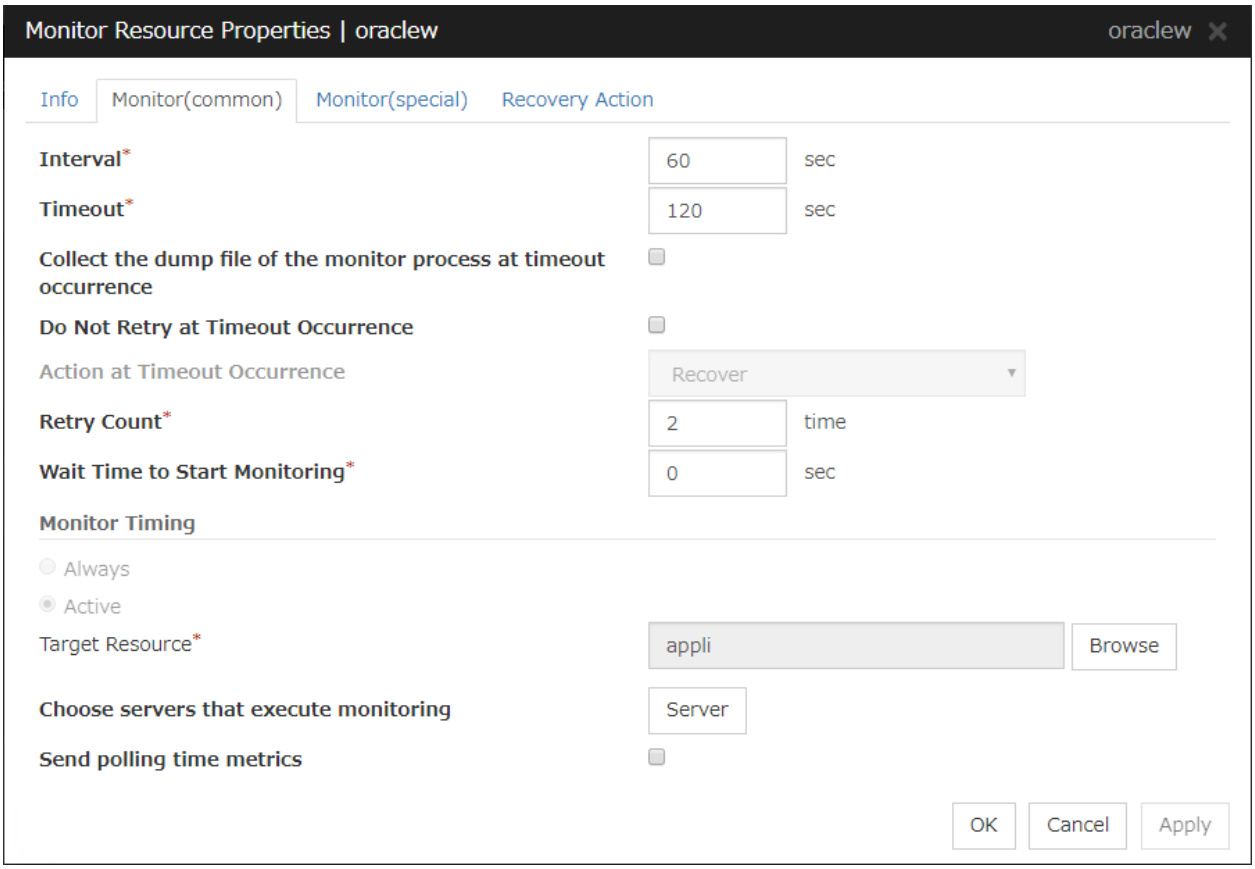
Naming rules

- Only alphanumeric characters, hyphen (-), underscore (_) and space are allowed for names.
- Up to 31 characters (31 bytes)
- Names cannot start or end with a hyphen (-) or space.

Comment (Within 127 bytes)

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

4.3.2 Monitor (common) tab



Interval (1 to 999)

Specify the interval to check the status of monitor target.

Timeout (5 to 999)

When the normal status cannot be detected within the time specified here, the status is determined to be error.

Note: It is not recommended to change the timeout value of the mirror disk monitor resource and the hybrid disk monitor resource.

Collect the dump file of the monitor process at timeout occurrence (Only for Oracle monitor resources)

Specify whether collecting the dump file of the EXPRESSCLUSTER monitoring process when time out occurs.

The collected dump file is saved in work\rm\ *resource name*\errinfo.cur folder under EXPRESSCLUSTER install folder. When collection is executed more than once, the folder names of the past collection information are renamed as errinfo.1, errinfo.2. And the folders are saved by 5 generations from the latest information.

Do Not Retry at Timeout Occurrence

If you enabled this option: Immediately after a timeout of the monitor resource, the action selected in **Action at Timeout Occurrence** is performed.

Action at Timeout Occurrence

Select an action in response to a timeout of the monitor resource. The timeout occurrence resets the retry counter.

This can be set only when the **Do Not Retry at Timeout Occurrence** function is enabled.

- **Recover**
  Performs a recovery action when the monitor resource times out.
- **Do not recover**
  Does not perform a recovery action even if the monitor resource times out.
- **Generate an intentional stop error**
  Makes an intentional stop error.

Note: For the following monitor resources, the **Do Not Retry at Timeout Occurrence** and **Action at Timeout Occurrence** functions cannot be set.

- multi target monitor resources
- Custom monitor resource (only when Monitor Type is **Asynchronous**)
- Message receive monitor resource
- JVM monitor resource
- System monitor resource
- Process resource monitor resource
- User mode 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 you set this 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:

- 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 LocalServer and the cluster are shown in a tree view. Select the target resource and click **OK**.

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.

Send polling time metrics

Enable or disable sending metrics: data on the monitoring process time taken by the monitor resource.

- If the check box is checked:
  The metrics are sent.
- If the check box is not checked:

The metrics are not sent.

Note:

For using the Amazon CloudWatch linkage function, enabling this option allows you to send data on the monitoring process time taken by any monitor resource.

Send polling time metrics cannot be set for the following monitor resources:

- Message receive monitor resource

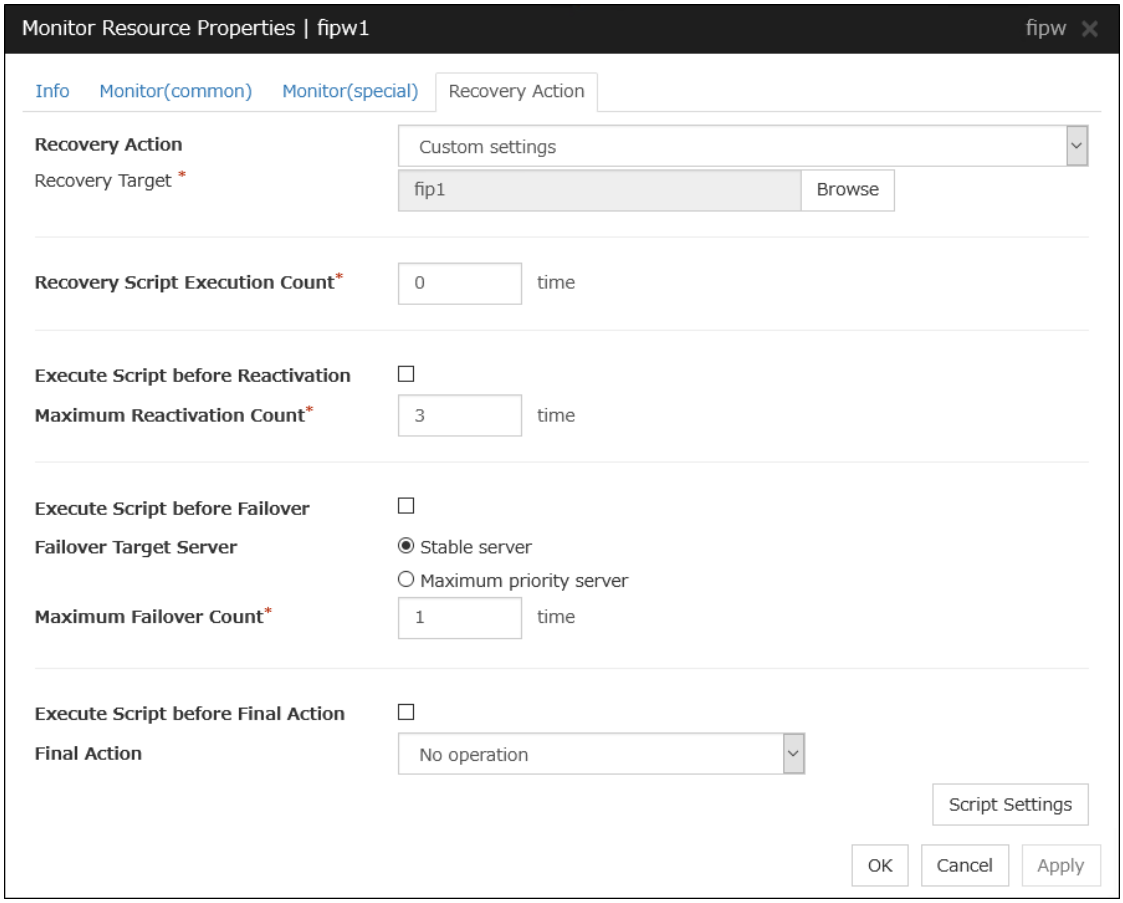
4.3.3 Monitor (special) tab

Some monitor resources require the parameters at the monitoring operation to be configured. The parameters are described in the explanation part about each resource.

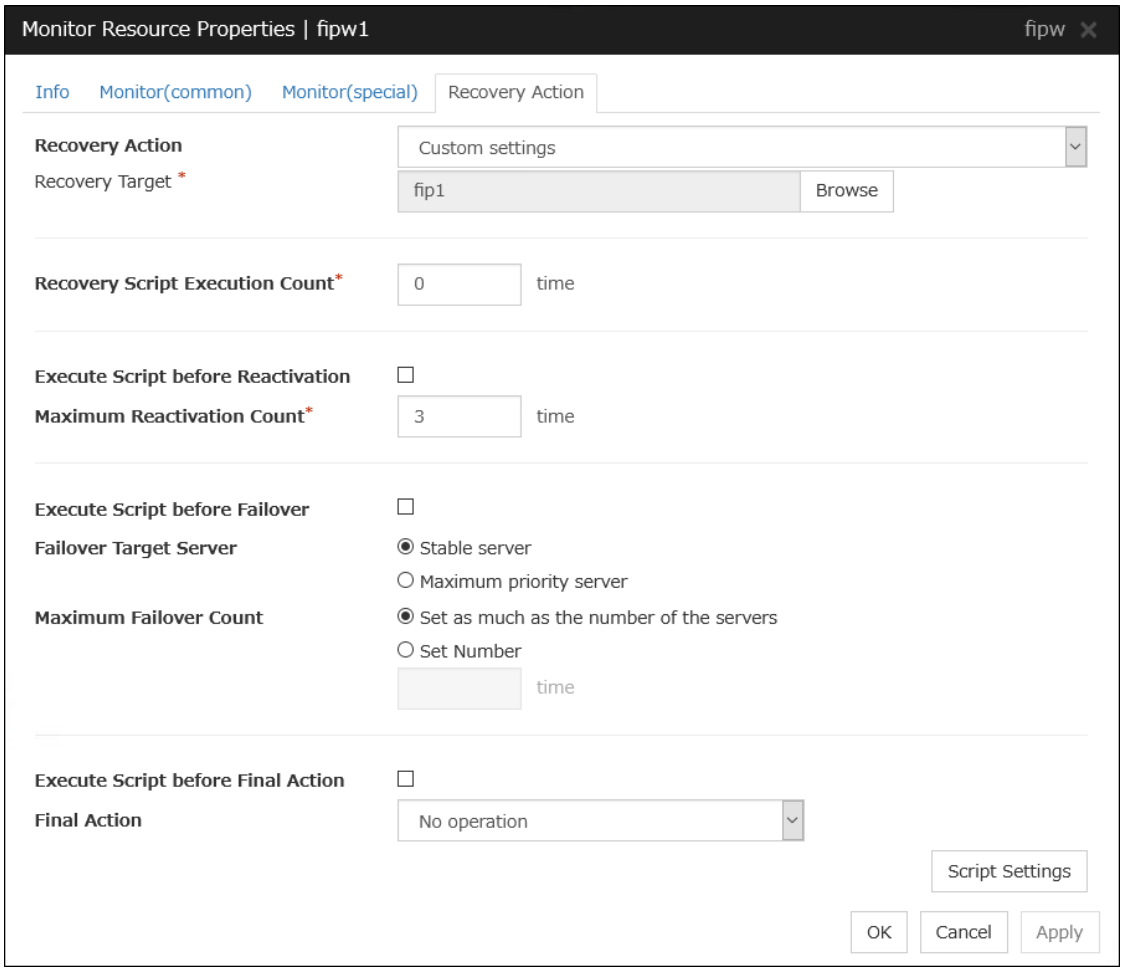
4.3.4 Recovery Action tab

Settings for monitor resources other than message receive monitor resources

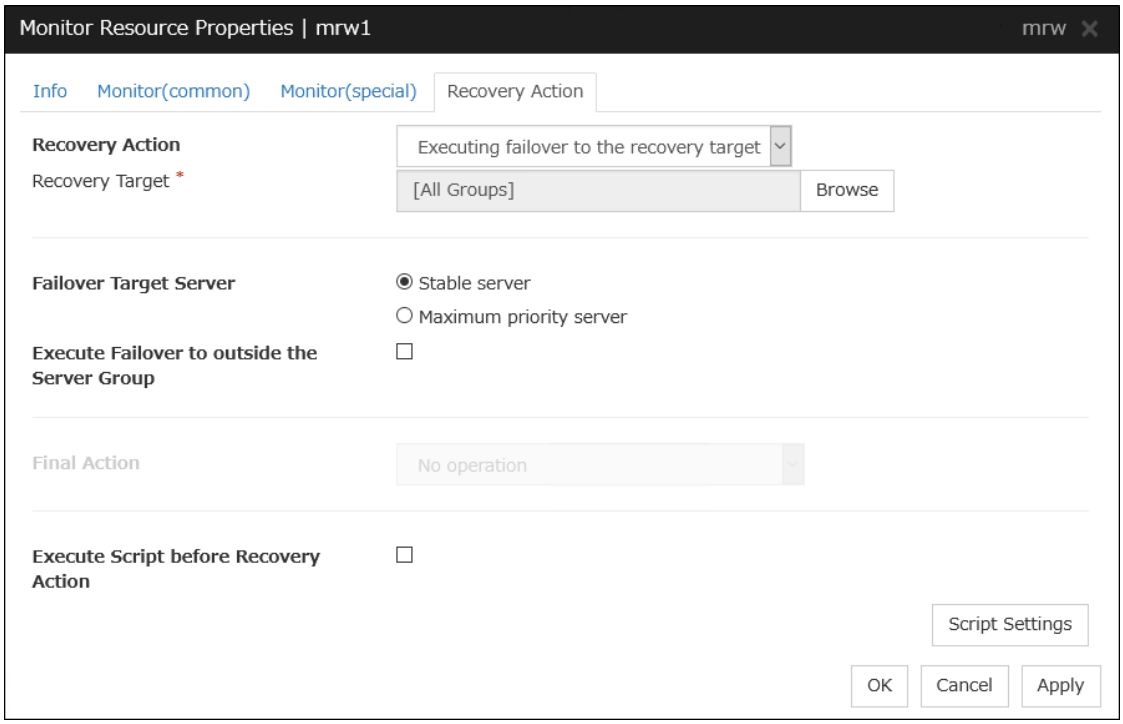
When **Server** is selected for **Failover Count Method** on the **Extension** tab in **Cluster Properties**:



When **Cluster** is selected for **Failover Count Method** on the **Extension** tab in the **Cluster Properties**:



Settings for message receive monitor resources



In this dialog box, you can configure the recovery target and an action to be taken at the time when an error is detected. 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 to 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 group or group resource selected 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 you can select the target resource. LocalServer, All Groups, and the 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

Specify whether to run the script before reactivation.

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. This cannot be set for message receive monitor resources.

If a group for which **Exclude server with error detected by specified monitor resource, from failover destination** in **Failover Attribute (Advanced)** is set or a resource that belongs to the group is set as the recovery target of an IP monitor resource or NIC Link Up/Down monitor resource, reactivation of the recovery target fails because an error is detected in the monitor resource registered as a critical monitor resource.

Execute Script before Failover

Specify whether to run the script before failover.

Failover Target Server

Select a Failover Target Server for the failover that takes place after reactivation retries upon activation error detection have failed for the number of times specified in **Retry Count at Activation Failure**.

- Stable Server

  The failover destination is the server where least resource errors have been detected.

  If two or more servers that meet the above condition exist, failover takes place by selecting one of them according to the failover policy of the group..

- Maximum Priority Server

  Failover takes place according to the failover policy settings of the group.

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.

Maximum Failover Count (0 to 99)

Specify how many times you allow failover after reactivation fails for the number of times set in **Reactivation Threshold** when an error is detected. If this is set to zero (0), no failover is executed. This is enabled when a group or group resource or All Groups is selected as a recovery target. This cannot be set for message receive monitor resources.

When **Server** is selected for **Failover Count Method** on the **Extension** tab in the **Cluster Properties**, set an arbitrary count to the maximum failover count.

When **Cluster** is selected for **Failover Count Method** on the **Extension** tab in the **Cluster Properties**, set an arbitrary count to the maximum failover count.

- Set as much as the number of the servers
  Specify the number of servers as the number of failovers to occur.
- Set Number
  Specify any number of times to a failover threshold.

For the Failover Count Method settings, refer to " *Extension Tab* " in " *Cluster properties* " in " 2. *Parameter details* " in this guide.

Execute Script before Final Action

Select whether script is run or not before executing final action.

- When the checkbox is selected:
  A script/command is run before executing final action. To configure the script/command setting, click **Script Settings**.
- When the checkbox is not selected:
  Any script/command is not run.

Execute Script before Recovery Action

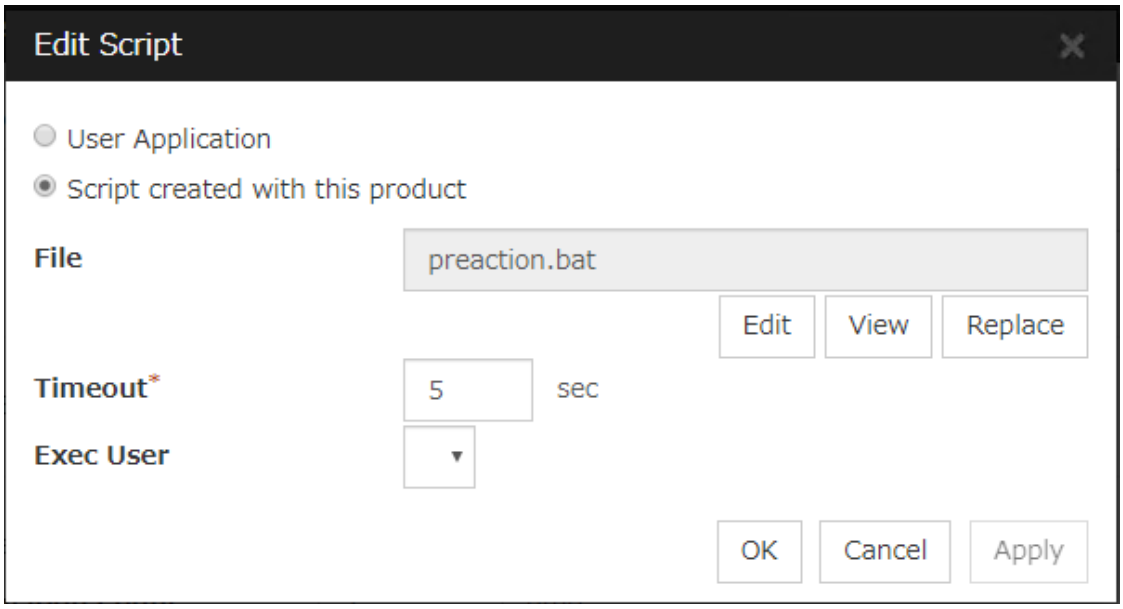
Select whether script is run or not before executing recovery action.

This can be set only for a message receive monitor resource.

- When the checkbox is selected:
  A script/command is run before executing recovery action. To configure the script/command setting, click **Script Settings**.
- When the checkbox is not selected:
  Any script/command is not run.

Script Settings

Click here to display the **Edit Script** dialog box. Set the recovery script/command.



User Application

Use an executable file (executable batch 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 you specify only the name of the executable file, you must configure the path with environment variable in advance. If there is any blank in the absolute path or the file name, put them in double quotation marks ("") as follows.

Example:

"C:\Program Files\script.bat"

If you want to execute VBScript, enter a command and VBScript file name as follows.

Example:

cscript script.vbs

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 batch 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 is set as 5.

Exec User

Specify a user to run a script. Execution users can be selected from users registered in the **Account** tab of **Cluster properties**

If you do not specify an execution user, the script is run by local system account.

Final Action

Select a final action to be taken after reactivation fails for the number of times set in **Reactivation Threshold**, and failover fails for the number of times set in **Failover Threshold** when an error is detected.

Select the final action from the options below:

- **No operation**
  No action is taken.

  Note: Use No operation to:

  - Suppress the final action temporarily
  - Show only alerts on detection of an error
  - Take the final action practically with multi-target monitor resources

  ---

- **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 or group resource is selected as a recovery target, this option stops the group or the group that the group resource belongs. When **All Groups** is selected, all the groups running on the server of which a monitor resource has detected an error are stopped. This is disabled when a LocalServer is selected as a recovery target.
- **Stop the cluster service**
  Stop the EXPRESSCLUSTER Server service of the server that detected an error.
- **Stop the cluster service and shutdown OS**
  Stop the EXPRESSCLUSTER Server service of the server that detected an error, and then shuts down the OS.
- **Stop the cluster service and reboot OS**
  Stop the EXPRESSCLUSTER Server service of the server that detected an error, and then reboots the OS.
- **Generate an intentional stop error**
  Intentionally cause stop error for the server that detected an error.

4.4 Understanding application monitor resources

Application monitor resources monitor application resources.

4.4.1 Monitoring by application monitor resources

Application monitor resources monitor application resources in a server where they are activated. They regularly monitor whether applications are active or not. When they detect that applications do not exist, it is determined to be an error.

4.4.2 Note on application monitor resources

An application monitor resource monitors a successfully activated application resource. The application resource can be monitored if it is specified as a resident type resource.

Application monitor resources are automatically registered when the resident type is set to **Resident** on addition of an application resource. Application monitor resources corresponding to an application resource are automatically registered.

Application monitor resources are initially defaulted, so configure appropriate resource settings as needed.

On addition of an application resource whose resident type is **Non-Resident**, application monitor resources cannot be added to it.

4.4.3 Monitor (special) tab

There are no monitor (special) tabs for application monitor resources.

4.5 Understanding disk RW monitor resources

Disk RW monitor resources monitor disk devices by writing dummy data to the file system.

4.5.1 Monitoring by disk RW monitor resources

Disk RW monitor resources write data to the specified file system (basic volume or dynamic volume) with the specified I/O size and evaluate the result.

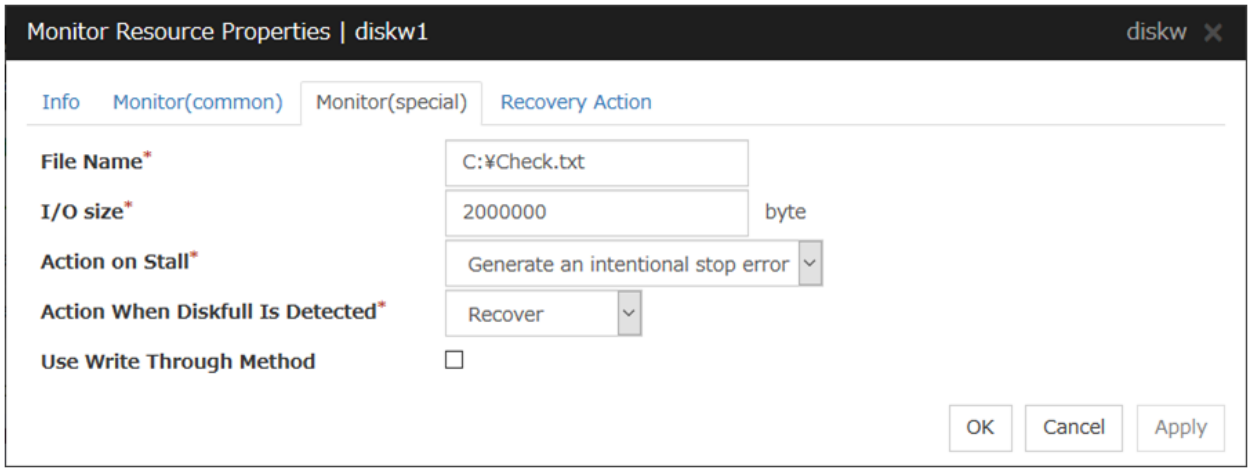
They solely evaluate whether data was written with the specified I/O size but do not evaluate validity of data. (Created file is deleted after writing)

OS and disk get highly loaded if the size of I/O is large.

Depending on disk and/or interface being used, caches for various writing are mounted. Because of this, if the size of I/O is small, a cache hit may occur and an error in writing may not get detected. Intentionally generate a disk error to confirm that the size of I/O is sufficient to detect an error.

Note: If you want multipath software to initiate path failover when disk path is not connected, you should set longer timeout for disk RW monitor resource than path failover time.

4.5.2 Monitor (special) tab



File Name (Within 1023 bytes)

Enter the file name to access. This file is created upon monitoring and deleted after I/O completes.

Note: Specify an absolute path for the file name. If a relative path is specified for the file name, the disk RW monitor resource may monitor the unexpected place.

Important: Do not specify any existing file for the file name. If an existing file is specified for the file name, the data of the file is lost.

I/O size (1 to 9999999)

Specify the I/O size for the disk to monitor.

Action on Stall

Specify the action to take when stalling is detected.

Stalling is detected if I/O control is not returned from the OS within the time specified in **Timeout** of the **Monitor (common)** tab.

- No Operation
  No action is taken.
- HW Reset[4]
  Reset the hardware.
- Generating of intentional Stop Error
  Intentionally cause a stop error.

Note: A Dummy Failure cannot be triggered by a stall.

Action When Diskfull Is Detected

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

Use Write Through Method

Applies the Write Through method to the monitor I/O method.

- If the Write Through method is enabled, the error detection precision of the disk RW monitor will improve. However, the I/O load on the system may increase.

[4] This function does not require ipmiutil, unlike the forced stop function.

4.6 Understanding floating IP monitor resources

Floating IP monitor resources monitor floating IP resources.

4.6.1 Monitoring by floating IP monitor resources

Floating IP resources monitor using WMI 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.

4.6.2 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.

4.6.3 Monitor (special) tab

Monitor NIC Link Up/Down

Specify whether to monitor NIC Link Up/Down.

4.7 Understanding IP monitor resources

IP monitor resource is a monitor resource which monitors IP addresses by using the ping command depending on whether there is a response or not.

4.7.1 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.

- 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.

  The following figure shows an example of one IP monitor resource in which all IP addresses are registered. If any of the registered IP addresses are normal, IP monitor 1 considers all of them to be normal.

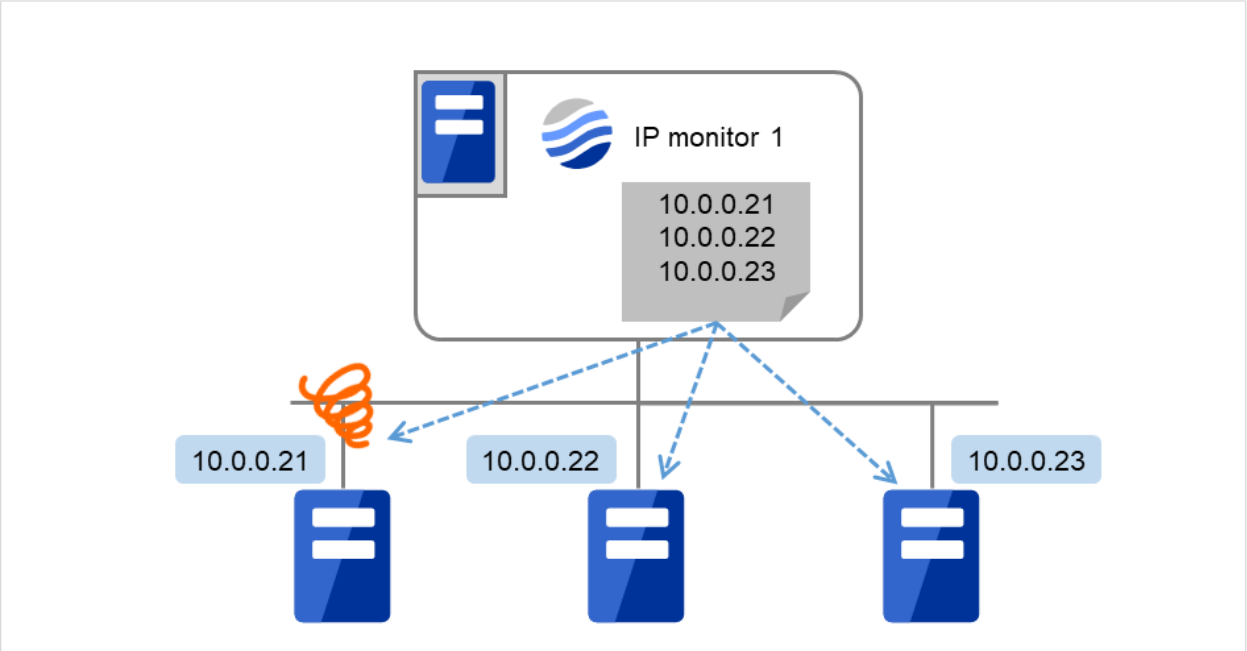


Fig. 4.58: One IP monitor resource where all IP addresses are registered (in normal cases)

The following figure shows an example of one IP monitor resource in which all IP addresses are registered. If all of the registered IP addresses are in error, IP monitor 1 considers so.

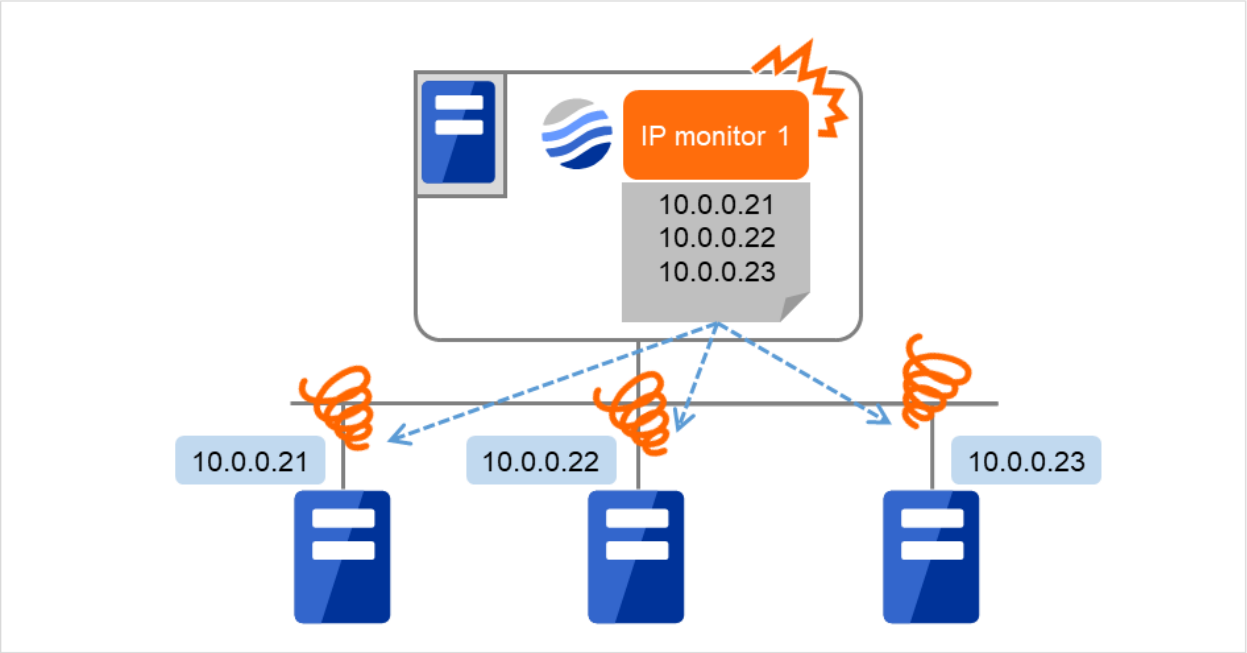


Fig. 4.59: One IP monitor resource where all IP addresses are registered (in error detection)

- If you want to establish error when any one of IP addresses has an error, create one IP monitor resource for each IP address.

  The following figure shows an example of IP monitor resources, in each of which one IP address is registered. If there is an error of the IP address registered in any of the IP monitor resources, it (IP monitor 1) considers so.

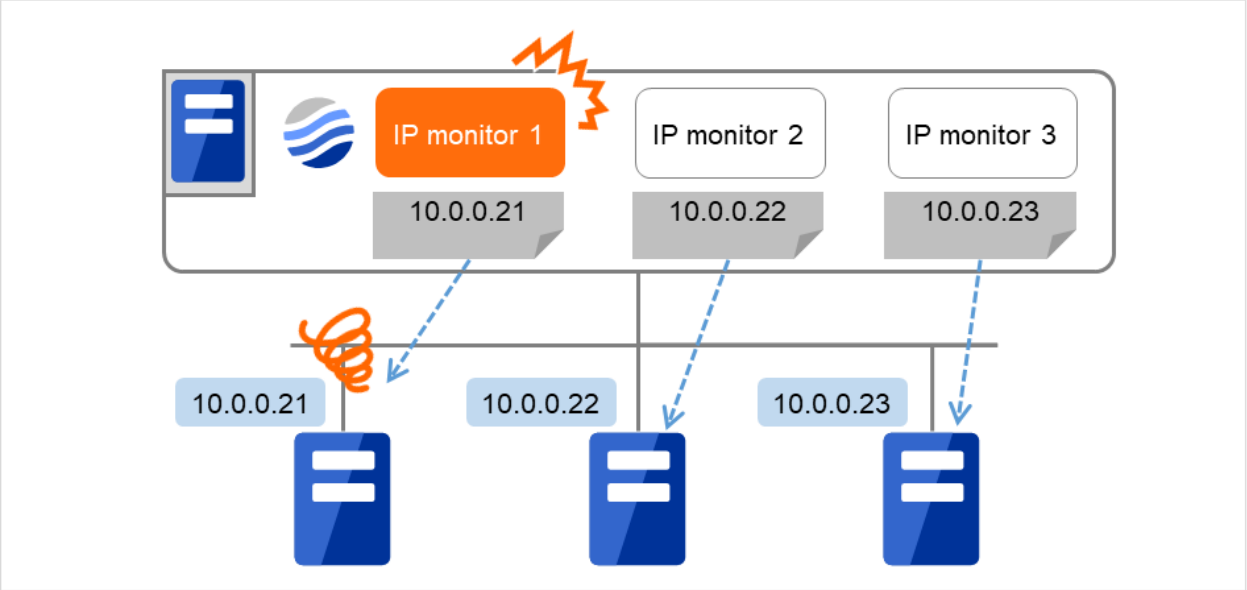
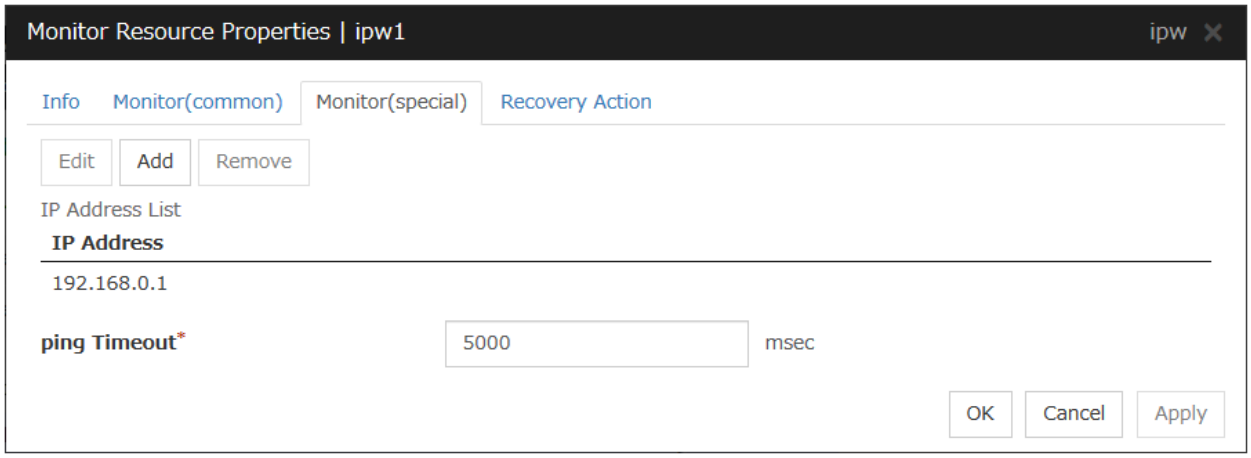


Fig. 4.60: IP monitor resources, in each of which one IP address is registered (in error detection)

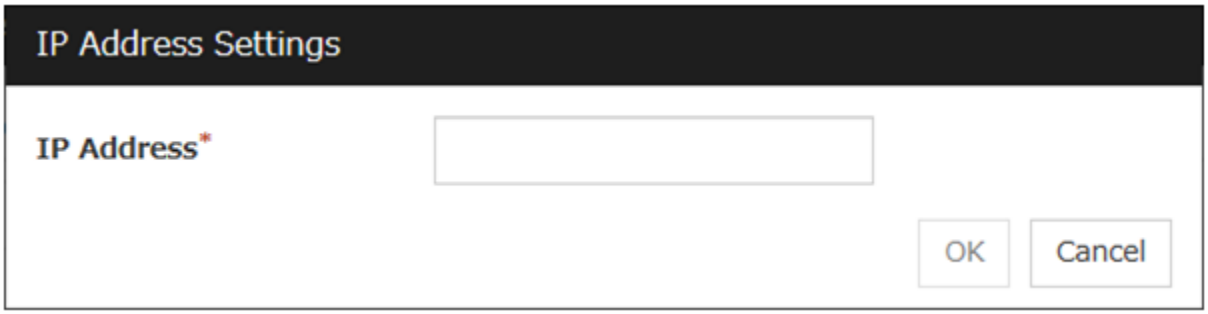
4.7.2 Monitor (spacial) tab

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 you can enter an IP address is displayed.



IP Address (Within 255 bytes)

Enter an IP address to be monitored in this field and click **OK**. The IP address to be entered here should be the one that exists on the public LAN.

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**.

ping Timeout (1 to 999999)

Specify the timeout of the ping to be sent to monitor the IP address in milliseconds.

4.8 Understanding mirror disk monitor resources

Mirror monitor resources monitor a mirror partition device or mirror driver works properly.

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 the mirror disk resource is automatically registered.

When this resource is deleted, be careful that auto mirror recovery cannot be executed.

Refer to "*Automatically recovering from mirroring*" in "*Recovering from mirror breaks*" in "10. *Troubleshooting*" in this guide for the details.

4.8.2 Monitor (special) tab

Mirror Disk Resource

The mirror disk resource to be monitored is displayed.

Browse

Click this button to display the dialog box where you can select a mirror disk resource to be monitored. Mirror disk resources registered with the cluster are displayed in a tree view. You can select only mirror disk resources in this view. Select a mirror disk resource and click OK.

4.9 Understanding NIC link up/down monitor resources

NIC Link Up/Down monitor resource obtains the information on how the specified NIC using WMI is linked and monitors the linkage is up or down.

4.9.1 Configuration and range of NIC link up/down monitoring

You can monitor an NIC dedicated to interconnect (mirror disk 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.

4.9.2 Monitor (special) tab

Add

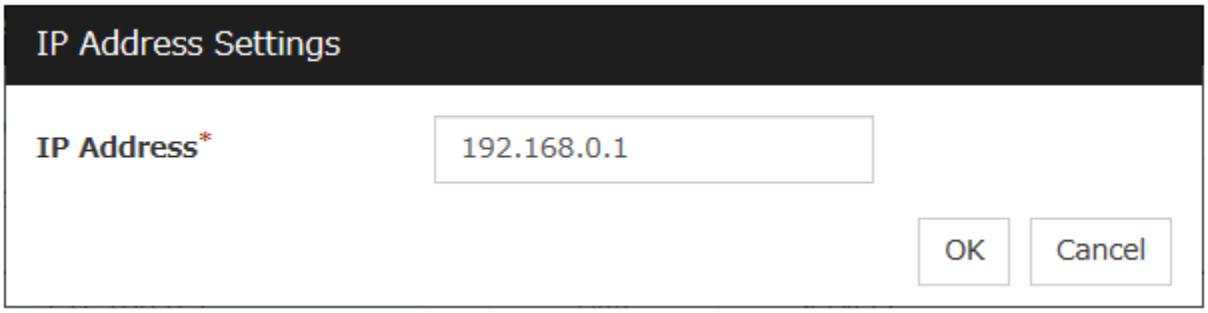
Add the IP address of the NIC to be monitored to the list of monitoring servers.

Remove

Delete the IP address of the NIC to be monitored from the list of monitoring servers.

Edit

Edit the IP address of the NIC to be monitored.



IP Address (Within 47 bytes)

Specify the IP address of the NIC to be monitored.

4.10 Understanding multi target monitor resources

The multi target monitor resource monitors more than one monitor resources.

4.10.1 Note on the multi target monitor resource

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.

4.10.2 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

The table below describes status of a multi target monitor resource:

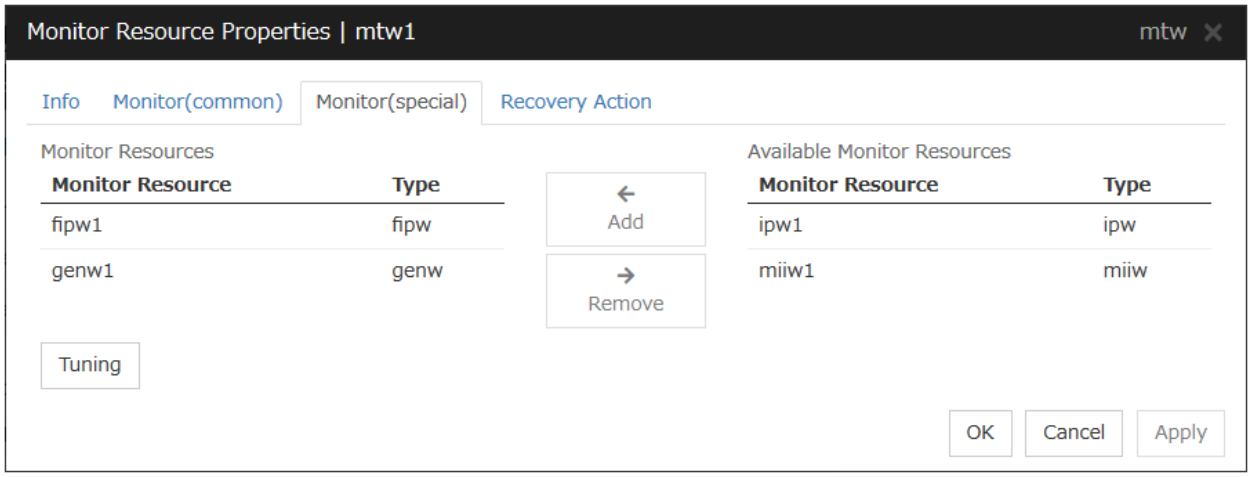
Multi target monitor resource status		**Monitor resource1 status**		
		Normal	**Error**	**Offline**
Monitor resource2 status	**Normal**	normal	caution	caution
	Error	caution	error	error
	Offline	caution	error	normal

- 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, multi target monitor resource detects an error.
  If the number of the monitor resources with the caution status exceeds the caution threshold, the status of the multi target monitor 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 monitor 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.

4.10.3 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.

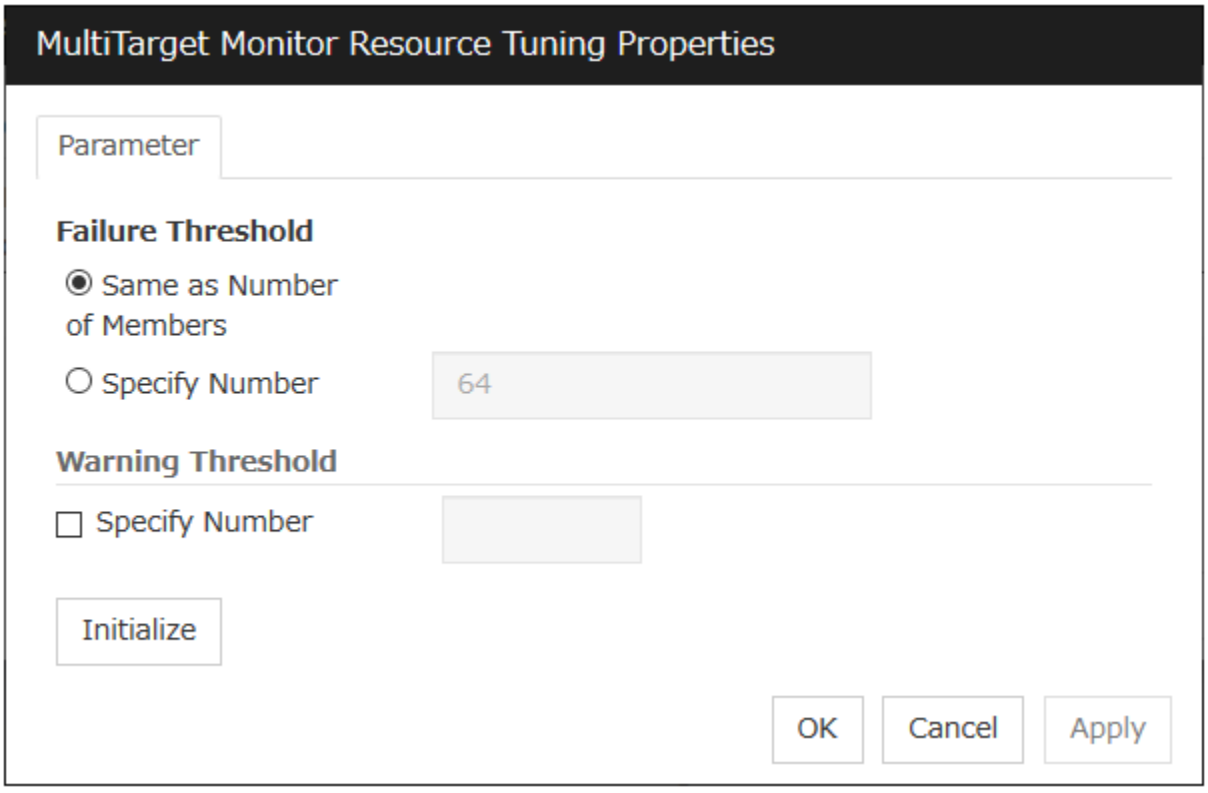
Tuning

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 checkbox 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 checkbox is not selected:
  Multi target monitor resources do not display an alert.

Initialize

Clicking **Initialize** resets all items to their default values.

4.11 Understanding registry synchronization monitor resources

Registry synchronization monitor resources monitor registry synchronization resources.

4.11.1 Note on registry synchronization monitor resources

This monitor resource is automatically registered when a registry synchronization resource is added. A registry synchronization monitor resource corresponding to a registry synchronization resource is automatically registered.
Registry synchronization monitor resources are initially defaulted, so configure appropriate resource settings as needed.

4.11.2 Monitor (special)

There are no monitor (special) tabs for registry synchronization monitor resources.

4.12 Understanding disk TUR monitor resources

Disk TUR monitor resources monitor the disk specified by disk resource.

4.12.1 Notes on disk TUR monitor resources

- You cannot run the SISI Test Unit Ready command 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.
- TUR monitor resources, compared to disk RW monitor resources, burdens OS and disks less.
- In some cases, Test Unit Ready may not be able to detect actual errors in I/O to media.
- If you want multipath software to initiate path failover when disk path is not connected, you should set longer timeout for disk RW monitor resource than path failover time.
- This monitor resource is automatically registered when a disk resource is added. A disk TUR monitor resource corresponding to a disk resource is automatically registered.
  Disk TUR monitor resources are initially defaulted, so configure appropriate resource settings as needed.

4.12.2 Monitor (special) tab

Disk Resource

Select a disk resource.

Browse

Click this button to display the disk resources that can be registered.

4.13 Understanding service monitor resources

Service monitor resources monitor service resources or services.

4.13.1 Monitoring by service monitor resources

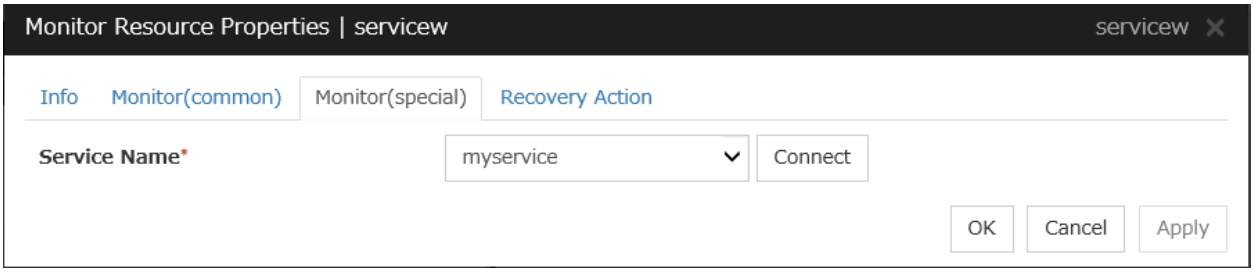
They regularly check the service status with the service control manager and if the status of the service resource becomes Stopped, it is considered as an error.

4.13.2 Note on service monitor resources

If you select **When activated** in **Monitor Timing** and specify a service resource in **Target Resource**, the **Service Name** of the service resource is applied to that of the service monitor resource.

Adding a service resource will automatically register a service monitor resource corresponding to the service resource.

4.13.3 Monitor (special) tab



Service Name (Within 1023 bytes)

Specify the service name or service display name used in the service resource.

Combo box options display the list of the service display names of the services collected from the server.

The service name cannot be changed, if you select **When activated** in **Monitor Timing** and specify a service resource in **Target Resource**.

Connect

Collects the service list from all the servers and updates the service display name list to be displayed in the **Service Name** combo box.

4.14 Understanding virtual computer name monitor resources

Virtual computer name monitor resources monitor virtual computer name resources.

4.14.1 Monitoring by virtual computer name monitor resources

Virtual computer name monitor resources monitor virtual computer name resources in a server where they are activated. Virtual computer name monitor resources regularly check the virtual computer name control process. It is considered an error if the process is not found.

4.14.2 Virtual computer name monitor resource

- This monitor resource is automatically registered when the virtual computer name resource is added.
- The effective final actions when an error in this resource is detected is set to **Stop the cluster service and shutdown OS, Stop the cluster service and reboot OS and Generating of intentional Stop Error** only.
  This is because the OS reboot is required for correctly activating virtual computer name resource when virtual computer name control process disappeared.
  The default setting is **Stop the cluster service and shutdown OS**. Do not change it to other than **Stop the cluster service and shutdown OS**, **Stop the cluster service and reboot OS**, or **Generate an intentional stop error**.
  If the virtual computer name control process is not found, the group fails over by shutting down or rebooting the server that detected an error.

4.14.3 Monitor (special) tab

There are no monitor (special) tabs for virtual computer name monitor resources.

4.15 Understanding dynamic DNS monitor resources

4.15.1 Notes on dynamic DNS monitor resources

There are no detailed settings related to dynamic DNS monitor resources.
Use them when using dynamic DNS resources of EXPRESSCLUSTER.

- Dynamic DNS monitor resources are automatically created when dynamic DNS resources are added. One dynamic DNS monitor resource is automatically created per dynamic DNS resource.
- Dynamic DNS monitor resources cannot be deleted. When dynamic DNS resources are deleted, dynamic DNS monitor resources are automatically deleted.
- Do not change the recovery target.
- Monitoring cannot be suspended or resumed using the clpmonctrl command or Cluster WebUI.
- If the target dynamic DNS resource is active when the cluster is suspended, the dynamic DNS monitor resource continues to operate without stopping.
- Alive monitoring is performed for a DDNS control process (clpddnsp.exe) periodically. If a disappearance of the process is detected, it is determined that an error has occurred. The alive monitoring interval is specified in **Interval** of the **Monitor (common)** tab. If the **Execute Dynamic Update Periodically** check box of the dynamic DNS resource **Details** tab is not selected, a DDNS control process (clpddnsp.exe) is generated, but alive monitoring is not performed.
- When the DNS server is down, a failover may start depending on the configuration. Therefore, it is recommended to use IP monitor resources together when checking the connection to the DNS server.

4.15.2 Monitor (special) tab

Check Name Resolution

- When the check box is selected (default):
  Check whether name resolution is available by sending a DNS query packet to the DNS server.
- When the check box is not selected:
  Do not check whether name resolution is available.

4.16 Understanding virtual IP monitor resources

Virtual IP monitor resources monitor virtual IP resources.

4.16.1 Monitoring by virtual IP monitor resources

Virtual IP monitor resources monitor virtual IP resources in a server where they are activated. Virtual IP monitor resources monitor whether the virtual IP address exists in the list of IP addresses. If the virtual IP address does not exist, it is considered as an error.

Floating IP resources monitor using WMI link up/down of NIC where a virtual floating IP address is active. If NIC link down is detected, it is considered as an error.

4.16.2 Notes on virtual IP monitor resources

This resource is automatically registered when virtual IP resources are added.

4.16.3 Monitor (special) tab

There are no monitor (special) tabs for virtual IP monitor resources.

4.17 Understanding CIFS monitor resources

CIFS monitor resources monitor CIFS resources.

4.17.1 Monitoring by CIFS monitor resources

CIFS resources monitor CIFS resources in a server where they are activated.

CIFS monitor resources obtain the information of shared folders publicized on a server and monitor if the shared folders publicized by CIFS resources are contained. An error is detected when the shared folders publicized by CIFS resources do not exist.

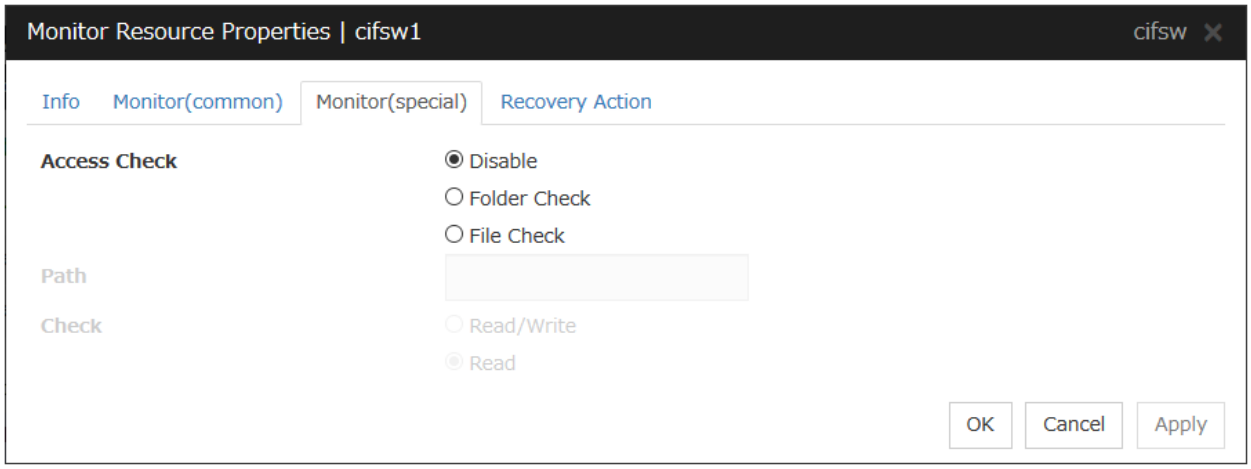
CIFS monitor resources also monitor accessibility to the shared folders.

When auto-saving of shared configuration of drive is executed, activation monitoring of the function to share and save the shared configuration is also be executed.

4.17.2 Notes on CIFS monitor resources

- When access check needs to be performed, the specified access method must be permitted for the local system account in the CIFS resources to be monitored.
- When **Execute the automatic saving of shared configuration of drive** is configured and not specify shared folder name to **path** on the monitoring target CIFS resource and the access check is executed on CIFS monitor resource, the specified access as a check method is executed on all the shared folder of the auto-saving target drive. When **Read** of folder check/file check is specified as checking method, the folder/file specified on **Path** must be on each shared folder.
- This monitor resource is automatically registered when a CIFS resource is added. A CIFS monitor resource corresponding to a CIFS resource is automatically registered.
  The default value is set for CIFS monitor resources. Change it to an appropriate value as needed.

4.17.3 Monitor (special) tab



Access Check

Specify the way to check access to the shared folders.

- Disable (default)

Access check is not performed.

- Folder Check
  Check if you can refer to the folder specified in **Path.**
- File Check
  Check if reading and writing to the file specified in **Path** can be performed.

Path (Within 255 bytes)

Specify the file/folder for access check by using a path including the shared folder or a relative path from the shared folder.

For folder check, specify the folder in the shared folder.

When **Execute the automatic saving of shared configuration of drive** is selected for the target CIFS resource, the file/folder for access check is specified by using an absolute path including the shared folder or a relative path from the shared folder. Based on which path is used, the file/folder which are created in advance for access check are different.

- If a path including shared folder is used, only specified shared name file/folder need to be created, use the format "<shared-name>\folder-name/file-name". Surround a shared name with "< >".
- If a relative path from the shared folder is used, folders with the same name need to be created in advance on all folders for which the sharing setting is configured.

When specifying shared configuration individually (when **Execute the automatic saving of shared configuration of drive** is not selected), specify the file/folder by using a relative path from the shared folder.

When **Read/Write** is selected as a file check method, the specified file is newly created. Make sure to specify a file name that does not overlap with other file names.

When **Read** is selected a file check method, specify a file in the shared folder. When **Execute the automatic saving of shared configuration of drive** is configured to the target CIFS resource, files with the same name need to be created in advance on all folders for which the sharing setting is configured.

Check

Select the way to check the access for **File Check**.

- Read/Write (default value)
  Write data to the file and check it can be read.
- Read
  Open the files and check it can be read.

4.18 Understanding hybrid disk monitor resources

Hybrid disk monitor resources monitor a mirror partition device or mirror driver works properly.

4.18.1 Note on hybrid disk monitor resources

This resource is automatically registered when a hybrid disk resource is added. A hybrid disk monitor resource corresponding to the hybrid disk resource is automatically registered.

When this resource is deleted, be careful that auto mirror recovery cannot be executed.

Refer to "*Automatically recovering from mirroring*" in "*Recovering from mirror breaks*" in "10. *Troubleshooting*" in this guide for the details.

4.18.2 Monitor (special) tab

Hybrid Disk Resource

The hybrid disk resource to be monitored is displayed.

Browse

Click this button to display the dialog box where you can select a hybrid disk resource to be monitored. Hybrid disk resources registered with the cluster are displayed in a tree view. You can select only hybrid disk resources in this view. Select a hybrid disk resource and click **OK**.

4.19 Understanding hybrid disk TUR monitor resources

Hybrid disk TUR monitor resources monitor the disk specified by hybrid disk resource.

4.19.1 Notes on hybrid disk TUR monitor resources

- This resource is automatically registered when a hybrid disk resource is added. Hybrid disk TUR monitor resources corresponding hybrid disk resources are automatically registered.
  When this resource is deleted, be careful that auto mirror recovery cannot be executed.
  Refer to "*Automatically recovering from mirroring*" in "*Recovering from mirror breaks*" in "*10. Troubleshooting*" in this guide for the details.
- You cannot run the SISI Test Unit Ready command 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.
- TUR monitor resources, compared to disk RW monitor resources, burdens OS and disks less.
- In some cases, Test Unit Ready may not be able to detect actual errors in I/O to media.

4.19.2 Monitor (special) tab

Hybrid Disk Resource

Select a hybrid disk resource.

Browse

Click this button to display the hybrid disk resources that can be registered.

4.20 Understanding custom monitor resources

Custom monitor resources monitor system by executing an arbitrary script.

4.20.1 Monitoring by custom monitor resources

Custom monitor resources monitor system by an arbitrary script.

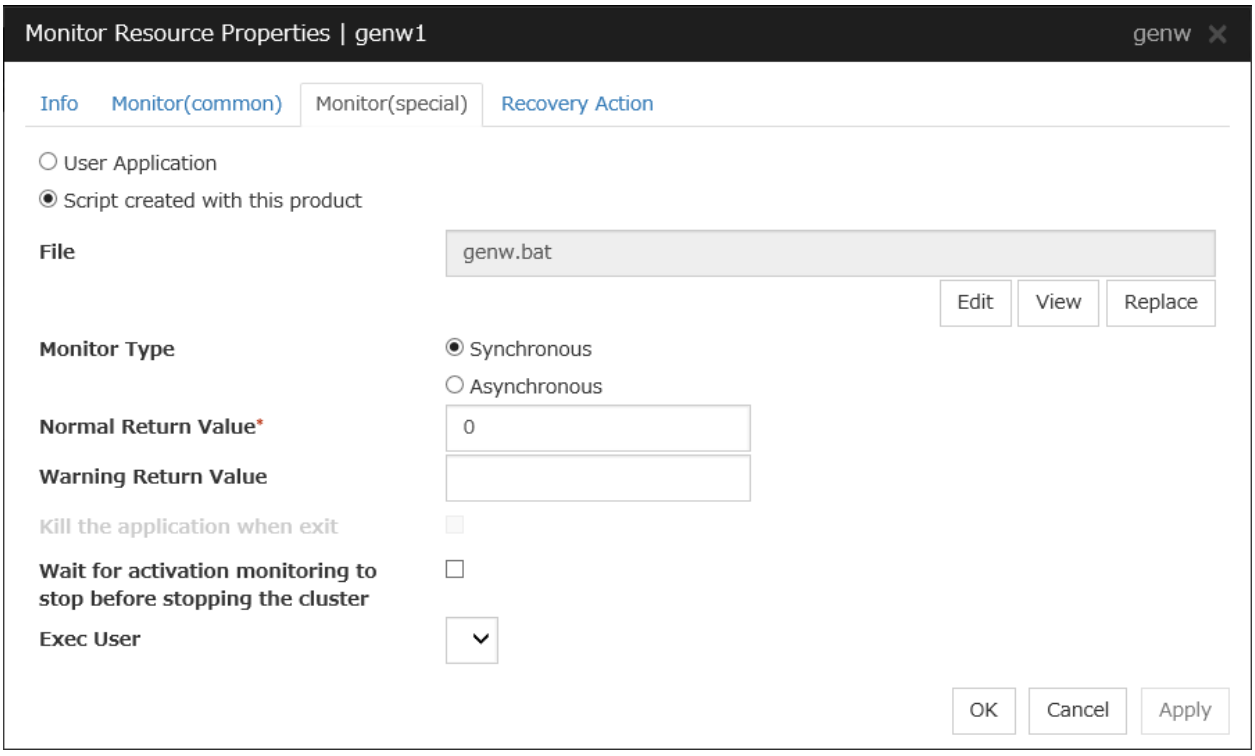
When Monitor Type is **Synchronous**, custom monitor resources regularly run a script and detect errors from its error code.

When Monitor Type is **Asynchronous**, custom monitor resources run a script upon start monitoring and detect errors if the script process disappears.

4.20.2 Note on custom monitor resources

- When a command for outputting a message (standard output, error output) in response to the prompt is executed as part of a batch file, the batch file may stop during execution of the command. Therefore, specify (perform redirection to) a file or nul as the message output destination.
- When the monitor type is set to **Asynchronous**, configure for the timeout a larger value than the waiting time for the monitor start.

4.20.3 Monitor (special) tab



User Application

Use an executable file (executable batch 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. However, no argument can be specified after the script.

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.

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.

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

Warning Return Value (Within 1023 bytes)

When **Asynchronous** is selected for **Monitor Type**, set the values of script error code to be determined as warning. 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.

If **Warning Return Value** is set to the same value as **Normal Return Value**, it is regarded as normal.

Kill the application when exit

Specify whether or not to forcibly terminate the application as termination of monitoring stop. If this is selected, the application is forcibly terminated instead of normal termination. This is effective only when **Monitor Type** is set to **Asynchronous**.

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 timing is set to **Active**.

Exec User

Specify a user to run a script. Execution users can be selected from users registered in the **Account** tab of **Cluster properties**.

If you do not specify an execution user, the script is run by local system account.

4.21 Understanding message receive monitor resources

Message receive monitor resources are passive monitors. They do not perform monitoring by themselves.
When an error message issued from a resource other than EXPRESSCLUSTER X is received from an outside source, the message receive monitor resources change their status and recover from the error.

4.21.1 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.

The following figure shows an example of a configuration with a message receive monitor resource. Receiving an error message issued by the clprexec command, the message receive monitor resource of Server 2 changes its own status and starts a recovery from the detected error.

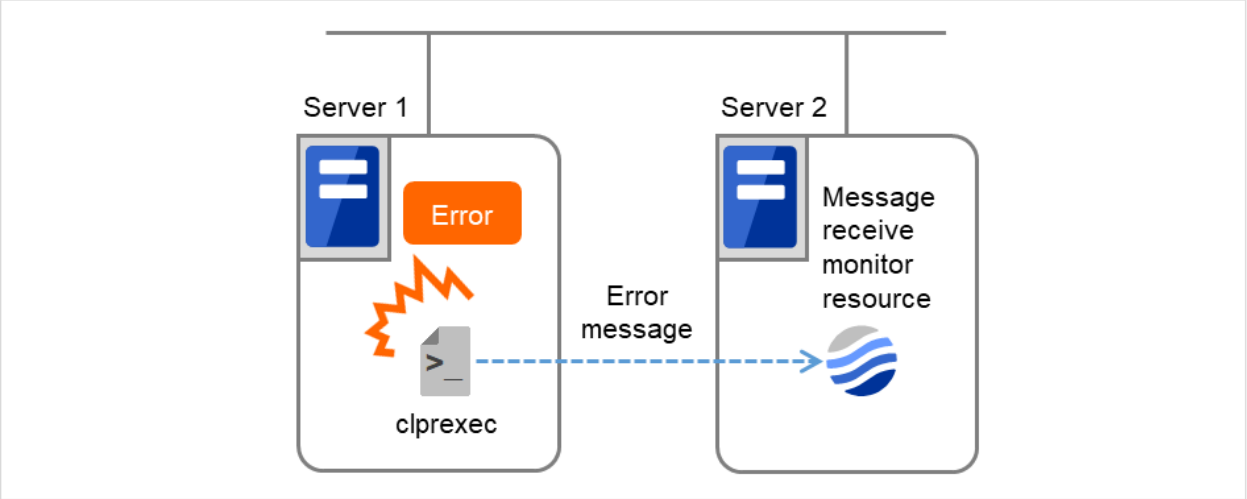


Fig. 4.61: Configuration with a message receive monitor resource

4.21.2 Failover to a server group at another site

- Upon the reception of notification of the occurrence of an error, failover from the active server group to another server group is allowed.
- The server groups and the following settings must be specified:
  - Recovery target group resource
    - Select **Use Server Group Settings**.
  - Message receive monitor
    - Select **Execute failover to the recovery target** for the recovery target.
    - Select **Execute Failover to outside the Server Group**.

- Upon the execution of server group failover to another site, 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.

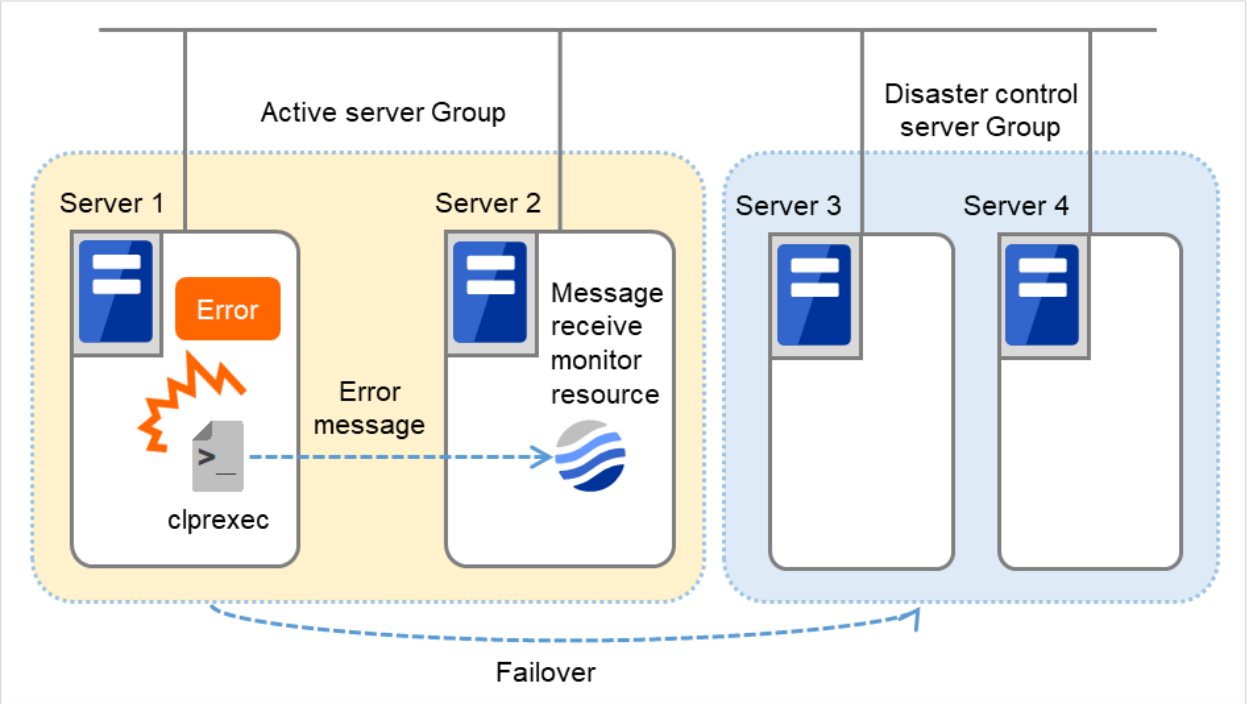


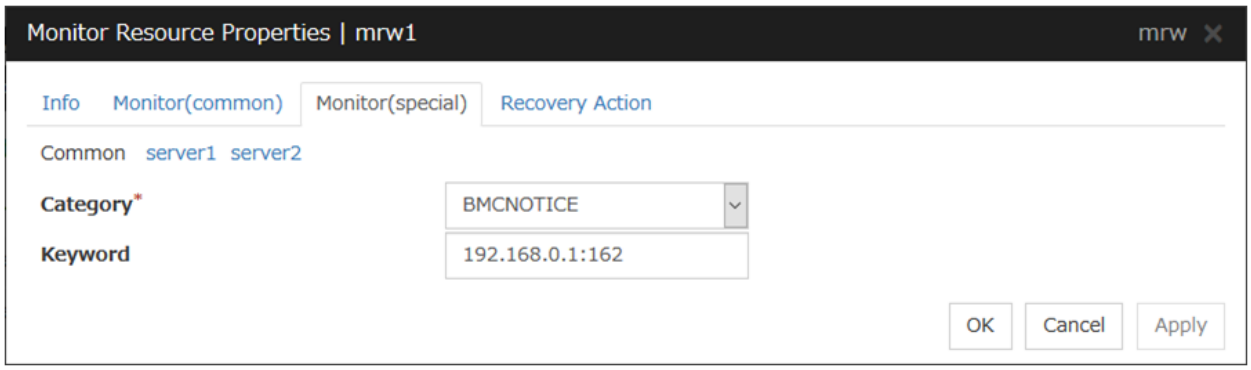
Fig. 4.62: Configuration with a message receive monitor resource (in failing over to another server group)

4.21.3 Notes on message receive monitor resources

<General 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." This error status 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 "*9. 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 the recovery target**, and if **Execute Another Server Group Failover** is selected for the recovery target, 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.

4.21.4 Monitor (special) tab



For **Category** and **Keyword**, specify a keyword passed using the -k parameter of the clprexec command. The monitor target can be omitted.

Category (Within 32 bytes)

Specify the category specified with -k argument of clprexec command.
You can select an existing character string from the list box or specify a desired character string.

Keyword (Within 1023 bytes)

Specify the keyword specified with -k argument of clprexec command.

4.22 Understanding process name monitor resources

Process name monitor resources monitor the process of arbitrary process name.

4.22.1 Notes on process name monitor resources

If you set 1 for **Minimum Process Count**, and 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.

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 (*).

If the name of the target process is 1023 bytes or longer, only the first 1023 bytes will be recognized as the process name. When specifying a process name by using a wild card (such as *), specify a character string that appears in the first 1023 bytes of the process name.

If the name of the target process is too long, the process name is output to the log file with the latter part omitted.

Use the following command to check the name of a process that is actually running and specify the name for the monitor target process name.

EXPRESSCLUSTER installation path\bin\GetProcess.vbs

When the above command is executed, GetProcess_Result.txt is output to the folder in which the command is executed. Open GetProcess_Result.txt and specify the CommandLine section of the process being displayed. If the output information includes double quotations (""), specify the section including the double quotations.

Example of output file

```
20XX/07/26 12:03:13
Caption         CommandLine
services.exe    C:\WINDOWS\system32\services.exe
svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
explorer.exe    C:\WINDOWS\Explorer.EXE
```

To monitor svchost.exe shown in the above command output information, specify C:\WINDOWS\system32\svchost -k rpcss as the monitor target process name.

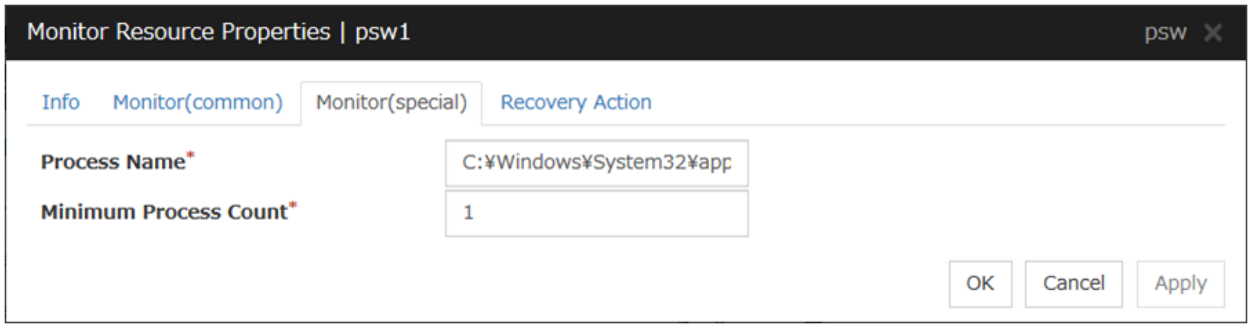
The process name specified for the name of the target process specifies the target process, using the process arguments as part of the process name. To specify the name of the target process, specify the process name containing the arguments. To monitor only the process name with the arguments excluded, specify it with the wildcard (*) using right truncation or partial match excluding the arguments.

4.22.2 Monitoring by process name monitor resources

Those processes having the specified process name are monitored. If **Minimum Process Count** is set to 1, the process ID is determined by the process name, and the error state is determined if the process ID vanishes. 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.

4.22.3 Monitor (special) tab



Process Name (Within 1023 bytes)

Specify the name of the process to be monitored. You must specify the process name.

Default value: None

Wild cards can be used to specify process names in the three patterns described below. Patterns other than these cannot be used.

prefix search : <character string included in process name>*

suffix search : *<character string included in process name>

partial search : *<character string included in 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.

4.23 Understanding DB2 monitor resources

DB2 monitor resources monitor DB2 database that runs on the server.

4.23.1 DB2 monitor resources

For the supported DB2 versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

DLL interface (DB2CLI.DLL/DB2CLI64.DLL) needs to be installed on servers where monitoring is performed because DB2 CLI is used for monitoring.

For target monitoring resources, specify a service resource or a script resource that starts DB2. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

A monitor table is created when monitoring is started and it is deleted when monitoring is stopped due to the stop of the failover group. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. It is not an error even if an alert message saying that "a monitor table exists" is displayed next time when monitoring is started.

DB2 may produce operation logs for each monitoring. Configure DB2 settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection ″Monitoring by DB2 monitor resources″, when ″Level 1″ is selected, EXPRESSCLUSTER does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.
Note that the following points about monitor levels described in the next section "Monitoring by DB2 monitor resources".
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.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional

Create a monitor table using either of the following methods:

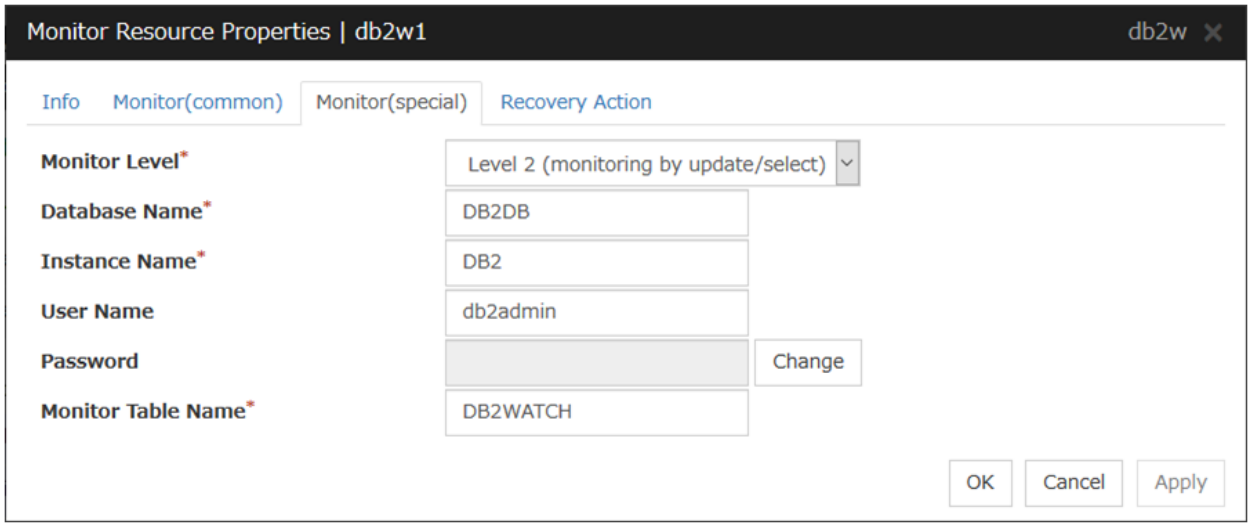
(In the following example, the monitor table is named DB2WATCH)
sql> create table DB2WATCH (num int not null primary key)
sql> insert into DB2WATCH values(0)
sql> commit

4.23.2 Monitoring by DB2 monitor resources

DB2 monitor resources perform monitoring according to the specified monitoring level.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
- 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. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
  3. 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 issued to 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 issued to the monitor table are of (create / update / select / drop) type.

Default value: 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 Name (Within 255 bytes)

Specify the instance name of the database to be monitored. You must specify the instance name.

Default value: DB2

User Name (Within 255 bytes)

Specify the user name to log on to the database.

Default value: db2admin

Password (Within 255 bytes)

Specify the password to log on to the database. Click **Change** and enter the password in the dialog box.

Default value: None

Monitor Table Name (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

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 service resources or script resources that start FTP monitor resources. Monitoring starts after target resource is activated. However, if FTP monitor resources cannot be started immediately after target resource is activated, adjust the time using **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.

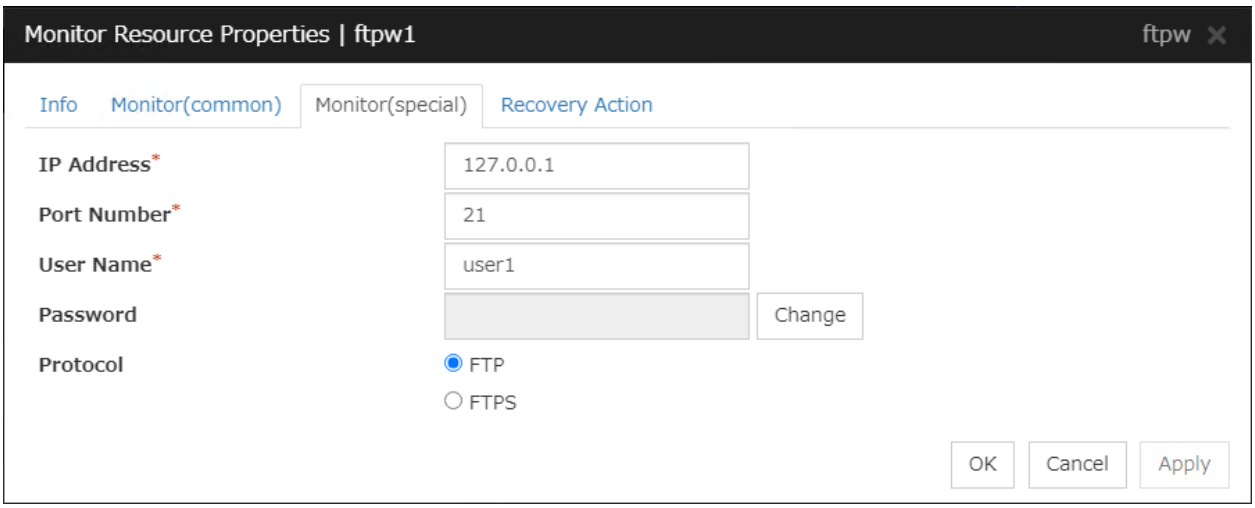
With FTPS selected in **Protocol**, you need to specify the installation path of OpenSSL libraries in the **Encryption** tab of **Cluster Properties**. The following OpenSSL library versions support FTPS: OpenSSL 3.0 and OpenSSL 1.1.1.

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 command.

4.24.3 Monitor (special) tab



IP Address (Within 255 bytes)

Specify the IP address of the FTP server to be monitored.
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).

Default value: 127.0.0.1

Port Number (1 to 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. Click **Change** and enter the password in the dialog box.

Default value: None

Protocol

Select a protocol for communication with the FTP server: **FTP** (in usual cases) or **FTPS** (with FTP over SSL/TLS connection required).

Default value: FTP

4.25 Understanding HTTP monitor resources

HTTP monitor resources monitor HTTP services that run on the server. HTTP monitor resources monitor HTTP protocol but they are not intended for monitoring specific applications. HTTP monitor resources monitor various applications that implement HTTP protocol.

4.25.1 HTTP monitor resources

For monitoring target resources, specify service resources or script resources that start HTTP services. Monitoring starts after a target resource is activated. However, if HTTP service cannot be started immediately after the target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

HTTP service may produce operation logs for each monitoring operation. Configure HTTP settings if this needs to be adjusted.

For the DIGEST authentication of HTTP monitor resources, the MD5 algorithm is used.

For the client certificate of HTTP monitor resources, IIS can be monitored.

If HTTP is specified in **Protocol**, HTTP requests of HTTP monitor resources are issued with the default port number (80).

4.25.2 Monitoring by HTTP monitor resources

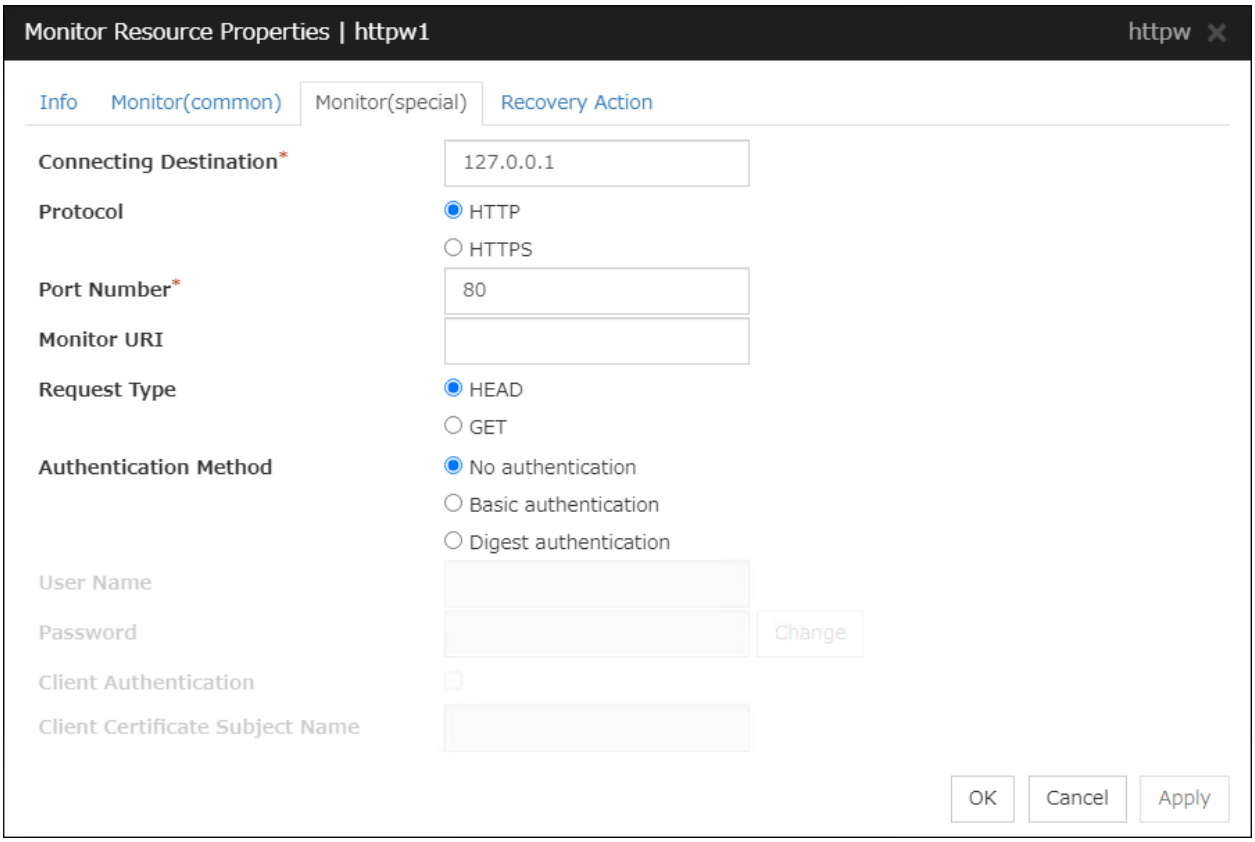
HTTP monitor resource monitors the following:

Monitors the HTTP daemon by connecting to the HTTP daemon on the server and issuing a HTTP 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 HTTP request is not started with "/HTTP"
3. the status code for the response to the HTTP request is in 400s and 500s (when URI other than the default is specified to the Monitor URI)

4.25.3 Monitor (special) tab



Connecting Destination (Within 255 bytes)

You must specify the IP address of the HTTP server to be monitored and this IP address.
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).

Default value: 127.0.0.1

Protocol

Configure protocol used for communication with HTTP server. In general, HTTP is selected. If you need to connect with HTTP over SSL, select HTTPS.

Note: If you select HTTPS, GET requests are issued regardless of which request type you choose.

Port Number (1 to 65535)

You must specify the port number of the HTTP to be monitored.

Default value:
80 (HTTP)
443 (HTTPS)

Monitor URI (Within 255 bytes)

Specify the URI of the HTTP to be monitored.

If URI is not specified, the document root is monitored. It is not necessary to create a monitoring page.

If a URI is specified, that URI is monitored. The specified URI needs to allow anonymous access.

Write the following in URI form from the DocumentRoot.

(Example) When the URI of the web page to be monitored is as follows:
*http://*WebServer:80/watch/sample.htm

/watch/sample.htm

Default value: None

Request Type

Specify a type of HTTP request for accessing the HTTP server. Setting this parameter is mandatory.

Default value: HEAD

Authentication Method

Specify an authentication method for connecting to the HTTP server.

Default value: No authentication

User Name (Within 255 bytes)

Set a user name to login to HTTP

Default value: None

Password (Within 255 bytes)

Set a password to login to HTTP

Default value: None

Client Authentication

Enabling this function, which requires selecting **HTTPS** in **Protocol**, performs client authentication.

Default value: Disabled

Note: Even if you enable this function for an HTTP server which does not perform client authentication, the operation is not affected.

Client Certificate Subject Name (Within 64 bytes)

Specify the subject name of a client certificate for client authentication. This is required when **Client Authentication** is enabled.

Note: Based on the subject name specified in **Client Certificate Subject Name**, the system retrieves the corresponding client certificate stored in **Personal** of the local computer's certificate store.

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 IMAP4 monitor resources

For monitoring target resources, specify service resources or script resources that start IMAP4 servers. Monitoring starts after 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.**

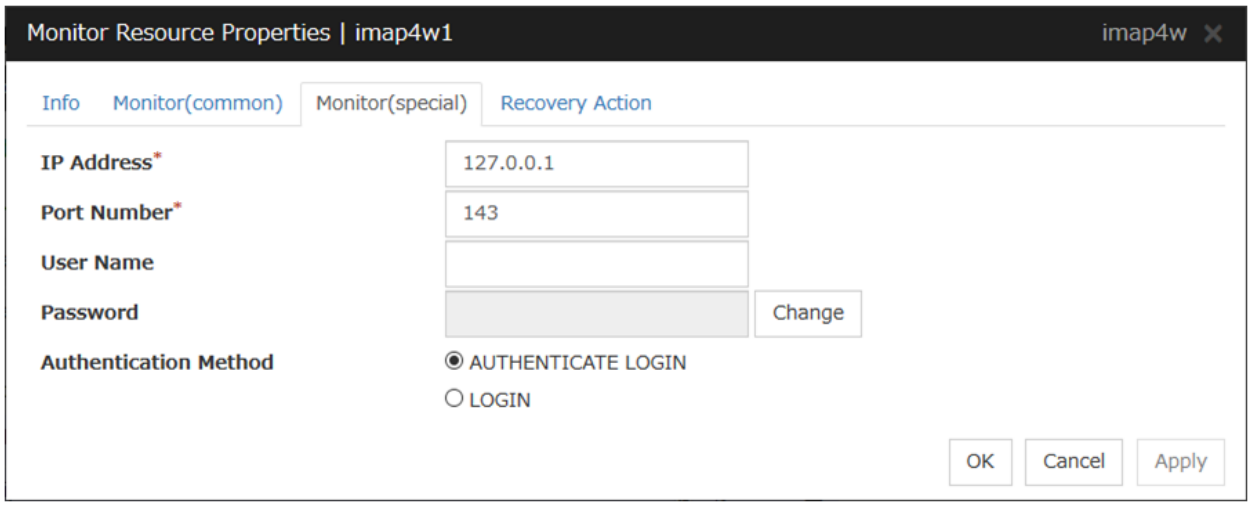
IMAP4 servers may produce operation logs for each monitoring. Configure IMAP4 servers if this needs to be adjusted.

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 255 bytes)

Specify the IP address of the IMAP4 server to be monitored.
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).

Default value: 127.0.0.1

Port Number (1 to 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. Click **Change** and enter the password in the dialog box.

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 ODBC monitor resources

ODBC monitor resources monitor ODBC database that runs on the server.

4.27.1 ODBC monitor resources

Set the data source using the ODBC data source administrator on Windows because the ODBC driver is used for monitoring. Add the data source to the system data source.

For monitoring target resources, specify service resources or script resources that start the database. Monitoring starts after target resource is activated. However, if the database cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

A monitor table is created when monitoring is started and it is deleted when monitoring is stopped due to the stop of the failover group. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. It is not an error even if an alert message saying that "a monitor table exists" is displayed next time when monitoring is started.

ODBC database may produce operation logs for each monitoring. Configure the database settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection ″Monitoring by ODBC monitor resources″, when ″Level 1″ is selected, EXPRESSCLUSTER does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

Note that the following points about monitor levels described in the next section "Monitoring by ODBC monitor resources".

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.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional

Create a monitor table using either of the following methods:

(In the following example, the monitor table is named ODBCWATCH)

sql> create table ODBCWATCH (num int not null primary key);

sql> insert into ODBCWATCH values(0);

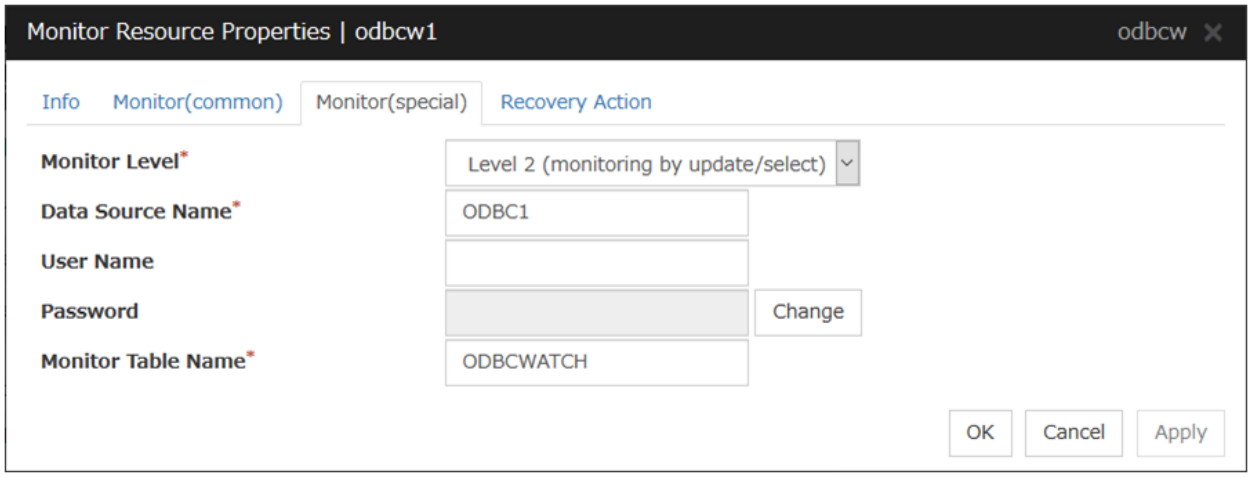
sql> commit;

4.27.2 Monitoring by ODBC monitor resources

ODBC monitor resources perform monitoring according to the specified monitoring level.

- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
- 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. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
  3. 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 issued to 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 issued to the monitor table are of (create / update / select / drop) type.

Default value: 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. You do not have to specify if the user name is specified in the data source settings.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to the database. Click **Change** and enter the password in the dialog box.

Default value: None

Monitor Table Name (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: ODBCWATCH

4.28 Understanding Oracle monitor resources

Oracle monitor resources monitor Oracle database that runs on the server.

4.28.1 Oracle monitor resources

For the supported Oracle versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

Interface DLL (OCI.DLL) needs to be installed on the server where monitoring is performed because Oracle OCI is used for monitoring.

For target a monitoring resource, specify a service resource or a script resource that can start Oracle. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

A monitor table is created when monitoring is started and it is deleted when monitoring is stopped due to the stop of the failover group. When monitoring is temporarily stopped or when the server fails before the failover group stops due to system error, the monitor table will not be deleted. It is not an error even if an alert message saying that "a monitor table exists" is displayed next time when monitoring is started.

When the OS authentication of a parameter is not selected, normally, the password authentication is used for the Oracle monitor. However, in the following conditions, The OS authentication is used for the Oracle monitor, and the user name and password specified in the parameter are ignored.

- SYSDBA is selected for the authentication method of the parameter.
- A user with Administrator privileges belongs to the ora_dba group of Windows OS.

The user specified for the user name parameter is sys by default, 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$PROCESS / SELECT permission for V$INSTANCE
Level 1 (monitoring by select)	SELECT permission for V$PROCESS / SELECT permission for a monitor table
Level 2 (monitoring by update/select)	SELECT permission for V$PROCESS / CREATE TABLE / DROP ANY TABLE / INSERT permission for a monitor table / UPDATE permission for a monitor table /SELECT permission for a monitor table

Oracle database may produce operation logs for each monitoring. Configure the Oracle settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection ″Monitoring by Oracle monitor resources″, when ″Level 1″ is selected, EXPRESSCLUSTER does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

Note that the following points about monitor levels described in the next section "*Monitoring by Oracle monitor resources*".

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.

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

Create a monitor table using either of the following methods:

(In the following example, the monitor table is named ORAWATCH)
sql> create table ORAWATCH (num int primary key);
sql> insert into ORAWATCH values(0);
sql> commit;

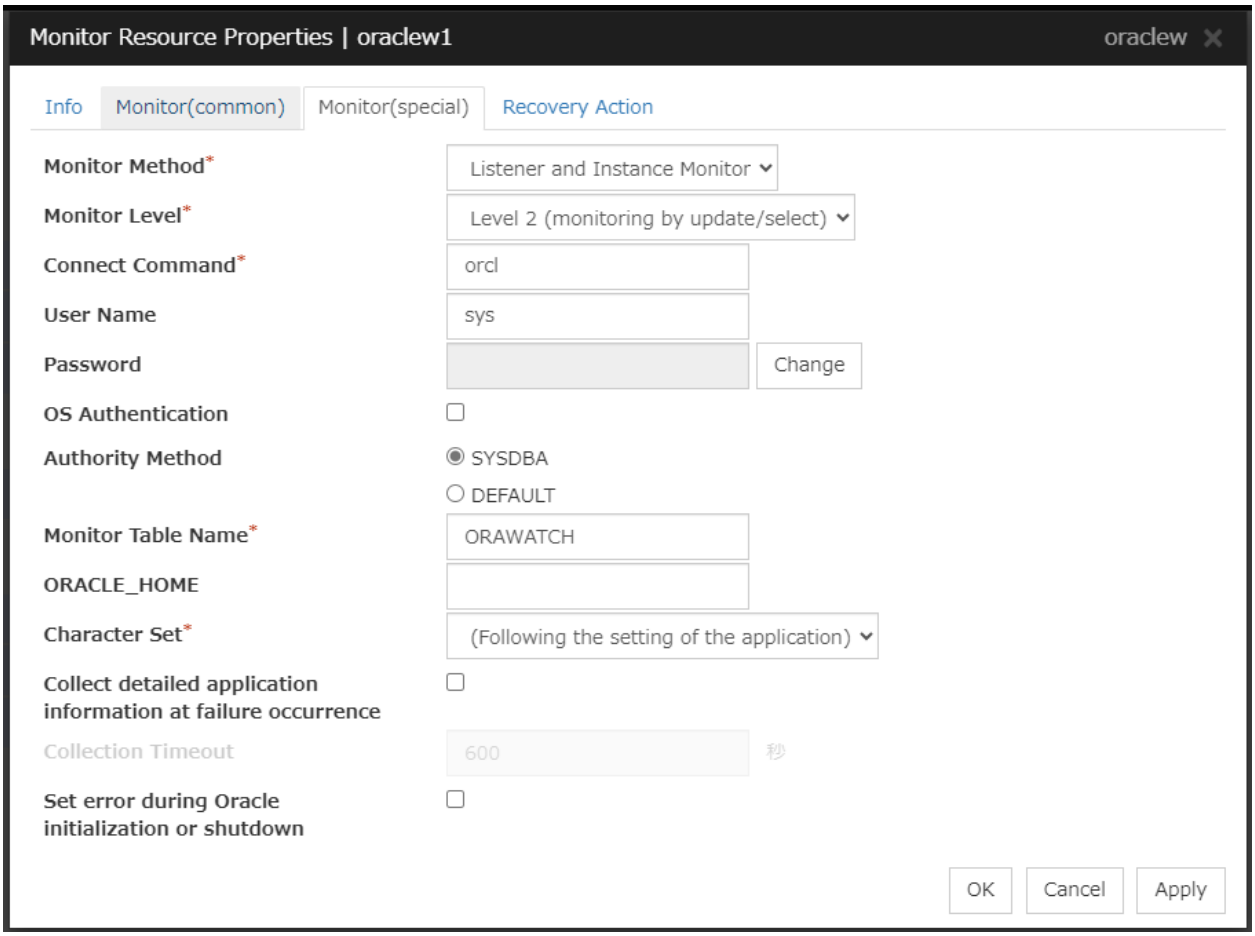
*Create this in a schema for the user specified for the user name parameter.

4.28.2 Monitoring by Oracle monitor resources

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 issued to the monitor table are of (select) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
- 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. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
  3. The written data is not the same as the read data

4.28.3 Monitor (special) tab



Monitor Method

Select the Oracle features to be monitored.

- Listener and Instance Monitor
  According to the specified monitor level, database connection, reference, and update operations are monitored.
- Listener Monitor
  To check for the listener operation, use the tnsping Oracle command. For a monitor resource property, 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.
- Instance Monitor
  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 property, ORACLE_HOME must be set. This is used for direct instance monitoring and recovery action setting without routing through the listener.
  A multi-tenant Oracle12c database cannot be monitored using a BEQ connection.
  If ORACLE_HOME is not set, only the connection specified by 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.

Default value: Listener and Instance Monitor

Monitor Level

Select one of the following levels. You cannot omit this level setting.

- 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 issued to 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 issued to the monitor table are of (create / update / select / drop) type.

Default value: Level 2 (monitoring by update/select)

Connect String (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
Listener and Instance Monitor	Need not be specified	Specify the connect string	As specified
Listener Monitor	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
Instance Monitor	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.

Default value: sys

Password (Within 255 bytes)

Specify the password to log on to the database. Click **Change** and enter the password in the dialog box.

Default value: None

OS Authentication

Specify the authentication method to log on to the Oracle monitor. It must follow the Oracle monitor settings.

- When the checkbox is selected:
  Use OS authentication.
- When the checkbox is not selected: (default value):
  Use database authentication.

Authority Method

Select the user authority to log on to the Oracle monitor. This must be set according to the authority of the specified user name.

- SYSDBA (Default value)
  Connect with SYSDBA authority.
- DEFAULT
  Connect with general user authority.

Monitor Table Name (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: 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 value: None

Character Set

Select the character set for Oracle.

- (Following the setting of the application) (default)
  The Oracle character set installed in the server is used.
- AMERICAN_AMERICA.US7ASCII
  Select this when the language for Oracle is not Japanese or English.

Collect detailed application information at failure occurrence

Specify whether to collect detailed Oracle information if an Oracle database error is detected.

- When the check box is selected
  Detailed Oracle information is collected.
- When the check box is cleared
  Detailed Oracle information is not collected.

When using this function, the local system account needs DBA authorization because the database processing for information collection is executed by the local system account. The collected information is saved in work\rm*resource name*\errinfo.cur folder under EXPRESSCLUSTER install folder. When collection is executed more than once, the folder names of the past collection information are renamed as errinfo.1, errinfo.2. And the folders are saved by 5 generations from the latest information.

Note:

When the oracle service is stopped due to cluster stop or other reasons while collecting, the correct information may not be collected.

Do not perform the manual operation such as Group stop or Group move while collecting information. Monitoring process may not work normally depending on the timing of the manual operation.

Collection Timeout (1 to 9999)

Specify the timeout time for collecting detailed information in seconds.

Default value: 600

Set error during Oracle initialization or shutdown

When this function is enabled, a monitor error occurs immediately upon the detection of Oracle initialization or shutdown in progress.

Disable this function when Oracle automatically restarts in cooperation with Oracle Clusterware or the like during operation. 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

4.29 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.

4.29.1 POP3 monitor resources

For monitoring target resources, specify service resources or script resources 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**.

POP3 services may produce operation logs for each monitoring. Configure the POP3 settings if this needs to be adjusted.

With POP3S selected in **Authentication Method**, you need to specify the installation path of OpenSSL libraries in the **Encryption** tab of **Cluster Properties**. The following OpenSSL library versions support POP3S: OpenSSL 3.1.

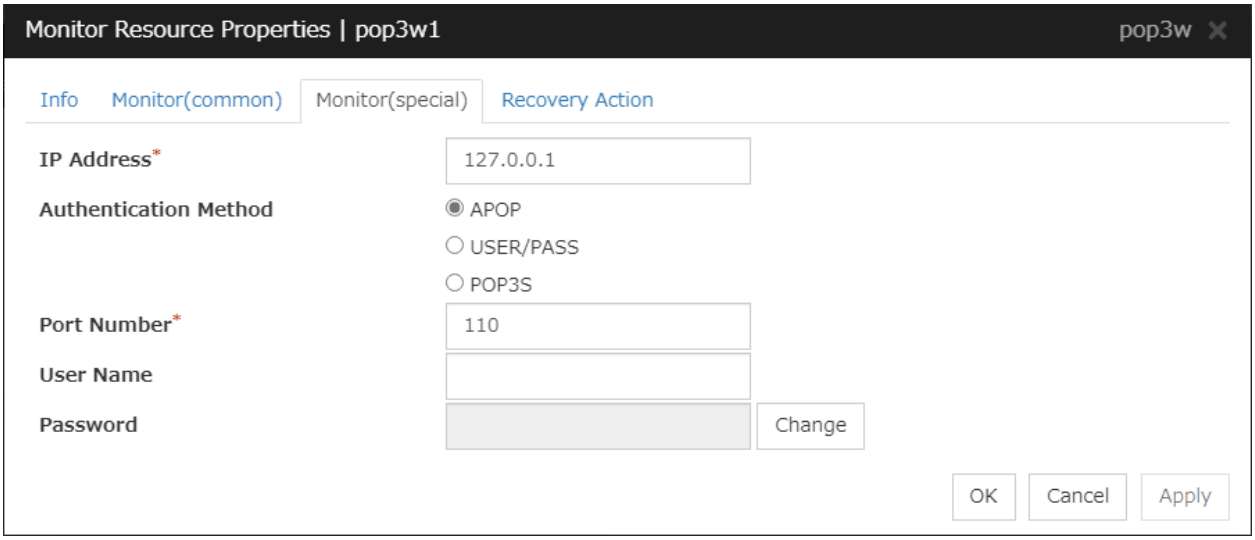
4.29.2 Monitoring by POP3 monitor resources

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.

4.29.3 Monitor (special) tab



IP Address (Within 255 bytes)

Specify the IP address of the POP3 server to be monitored.
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).

Default value: 127.0.0.1

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 plaintext method that uses the USER/PASS command.
- POP3S
  An encryption authentication method that uses SSL/TLS.

Port Number (1 to 65535)

Specify the POP3 port number to be monitored. You must specify this port number.

Default value :
110
995 (POP3S)

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

4.30 Understanding PostgreSQL monitor resources

PostgreSQL monitor resources monitor PostgreSQL database that runs on the server.

4.30.1 PostgreSQL monitor resources

For the supported PostgreSQL/PowerGres versions, see " Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

Interface DLL (LIBPQ.DLL) needs to be installed on the server where monitoring is performed because PostgreSQL/PowerGres library is used for monitoring. Specify the path of this DLL to the environmental variable when monitoring PostgreSQL.

For a target monitoring resource, specify a service resource or a script resource that can start PostgreSQL/PowerGres. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

A monitor table is created when monitoring is started and it is deleted when monitoring is stopped due to the stop of the failover group. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. It is not an error if an alert message saying that "a monitor table exists" is displayed next time when monitoring is started.

PostgreSQL/PowerGres may produce operation logs for each monitoring. Configure the PostgreSQL/PowerGres settings if this needs to be adjusted.

Because PostgreSQL is open-source software (OSS), its operation is checked but not guaranteed. Make sure to use PostgreSQL after evaluating it by yourself.

If PostgreSQL monitoring is performed, an error indicating that no library can be found may be output depending on the OS and PostgreSQL versions. In this case, add PostgreSQL bin to the PATH of the system environment variable. After that, restart the cluster.

When adding PATH to the environment variable (The following is an example of PATH of PostgreSQL9.6 bin.)

C:\Program Files\PostgreSQL\9.6\bin

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 "Monitoring by PostgreSQL monitor resources ".

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.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional

Create a monitor table using either of the following methods:

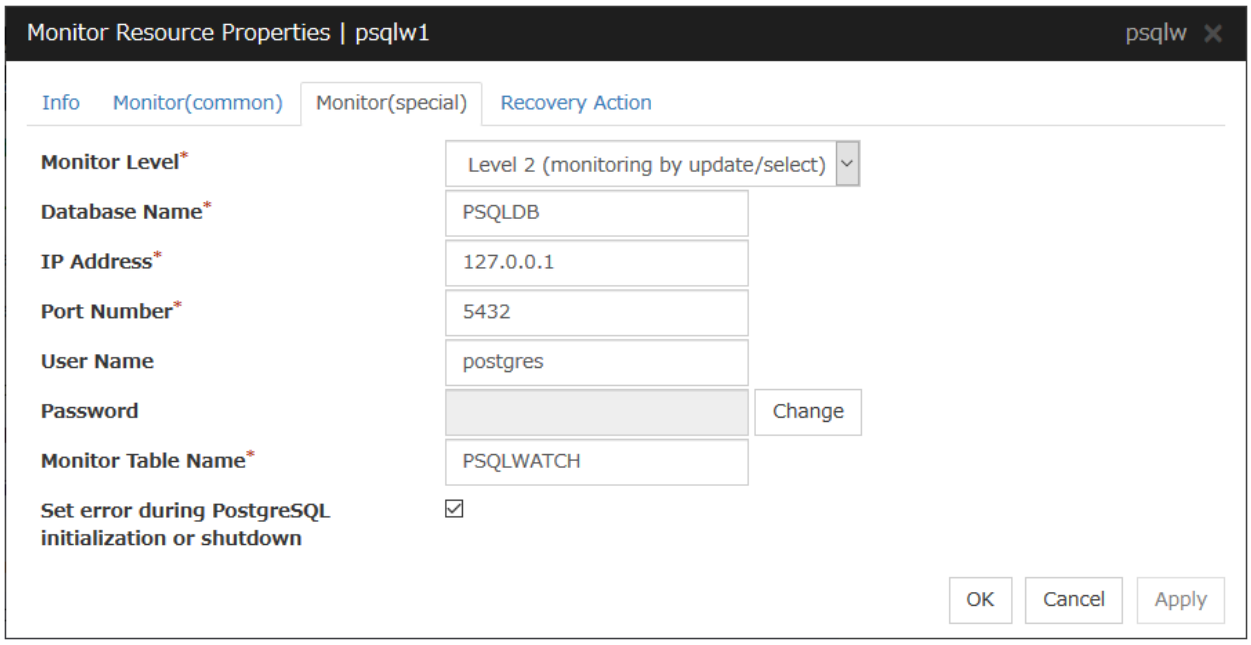
(In the following example, the monitor table is named PSQLWATCH)
sql> create table PSQLWATCH (num int not null primary key);
sql> insert into PSQLWATCH values(0);
sql> commit;

4.30.2 Monitoring by PostgreSQL monitor resources

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 issued to the monitor table are of (select) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
- 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. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / reindex / drop / vacuum) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
  3. The written data is not the same as the read data

4.30.3 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 issued to 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 issued to the monitor table are of (create / update / select / reindex / drop / vacuum) type.

Default value: 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

Specify the IP address of the database server to be monitored.

Default value: 127.0.0.1

Port Number

Specify the PostgreSQL port number to be monitored. You must specify this port number.

Default value: 5432

User Name (Within 255 bytes)

Specify the user name to log on to the database.

Default value: postgres

Password (Within 255 bytes)

Specify the password to log on to the database. Click **Change** and enter the password in the dialog box.

Default value: None

Monitor Table Name (Within 255 bytes)

You must specify the name of a monitor table created in the database. 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

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: Disabled

4.31 Understanding SMTP monitor resources

SMTP monitor resources monitor SMTP services that run on the server. SMTP monitor resources monitor SMTP protocol but they are not intended for monitoring specific applications. SMTP monitor resources monitor various applications that use SMTP protocol.

4.31.1 SMTP monitor resources

For monitoring target resources, specify service resources or script resources that start SMTP. Monitoring starts after target resource is activated. However, if the database cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring.**

SMTP services may produce operation logs for each monitoring. Configure the SMTP settings if

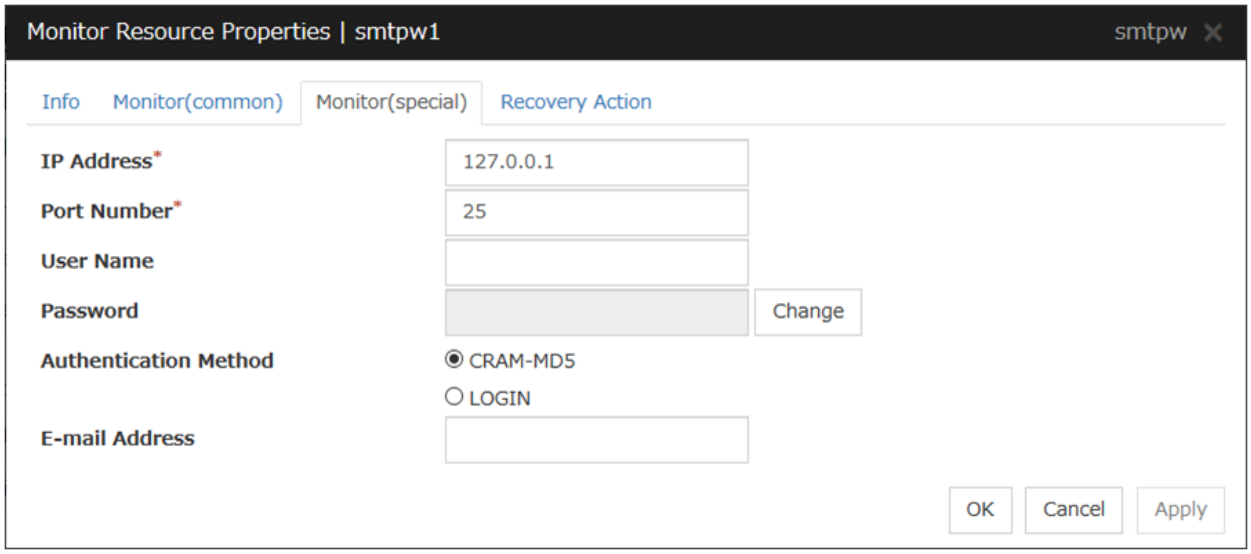
4.31.2 Monitoring by SMTP monitor resources

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 SMTP server fails.
2. When an error is notified as a response to the command.

4.31.3 Monitor (special) tab



IP Address

You must specify the IP address of the SMTP server to be monitored.

Default value: 127.0.0.1

Port Number

Specify the port number of the SMTP to be monitored. You must specify this port number.

Default value: 25

User Name (Within 255 bytes)

Specify the user name to log on to SMTP. If no user name is specified, SMTP authentication is not performed.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to SMTP. Click **Change** and enter the password in the dialog box.

Default value: None

Authentication Method

Select the authentication method to log on to the SMTP. It must follow the settings of SMTP being used:

- CRAM-MD5 (Default value)
  The encryption authentication method that uses the CRAM-MD5 command.
- LOGIN
  The plaintext method that uses the LOGIN command.

E-mail Address (Within 255 bytes)

Specify the email address used for monitoring. If nothing is specified, monitoring is performed using the command to verify the operation. The command that uses a dummy e-mail address is executed internally. If an email address is specified, monitoring is performed by running SMTP command to the specified e-mail address and verifying the result of it. It is recommended to have an e-mail address dedicated to monitoring.

Default value: None

4.32 Understanding SQL Server monitor resources

SQL Server monitor resources monitor SQL Server database that runs on the server.

4.32.1 SQL Server monitor resources

For the supported SQL Server versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

For target monitoring resource, specify a service resource that can start SQL Server. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

A monitor table is created when monitoring is started and it is deleted when monitoring is stopped due to the stop of the failover group. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. It is not an error if an alert message saying that "a monitor table exists" is displayed next time when monitoring is started.

SQL Server may produce operation logs for each monitoring. Configure the SQL Server settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection ″Monitoring by SQL Server monitor resources″, when ″Level 1″ is selected, EXPRESSCLUSTER does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

Note that the following points about monitor levels described in the next section "Monitoring by SQL Server monitor resources ".

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.

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

Create a monitor table using either of the following methods:

(In the following example, the monitor table is named SQLWATCH)

- When SET IMPLICIT_TRANSACTIONS is 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 is ON:

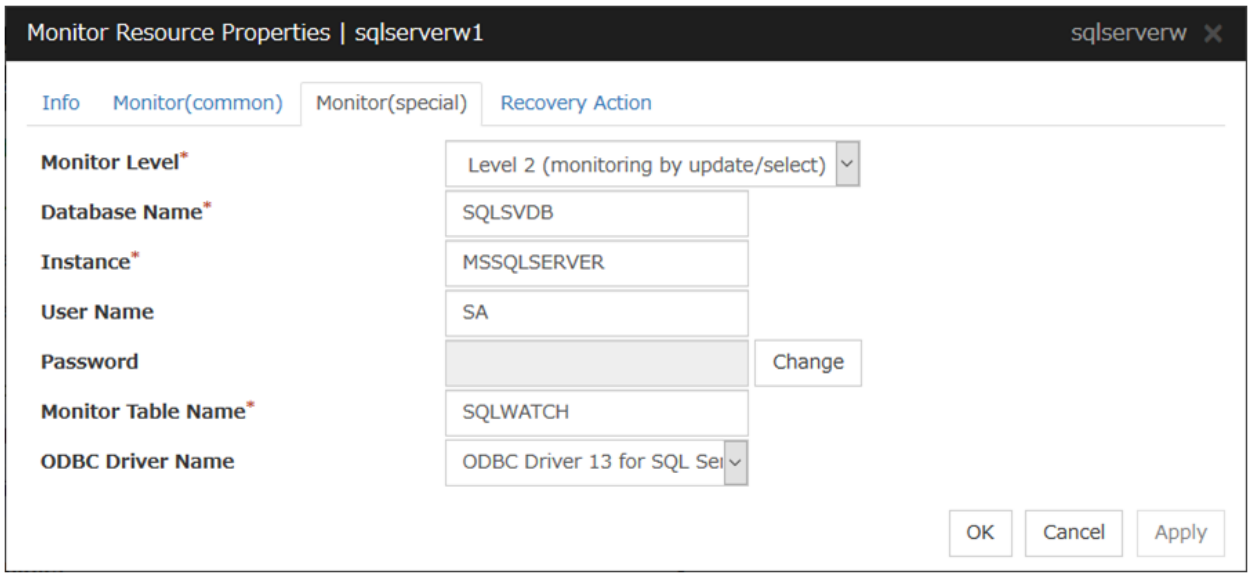
```
sql> create table SQLWATCH (num int not null primary key)
sql> go
sql> insert into SQLWATCH values(0)
sql> go
sql> commit
sql> go
```

4.32.2 Monitoring by SQL Server monitor resources

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 executed 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 issued to the monitor table are of (select) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
- 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. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.
  An error is recognized if:
  1. A database connection could not be established
  2. An error message is sent in response to an SQL statement
  3. The written data is not the same as the read data

4.32.3 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.
- Level 1 (monitoring by select)
  Monitoring with only reference to the monitor table. SQL statements issued to 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 issued to the monitor table are of (create / update / select / drop) type.

Default value: 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

Instance Name (Within 255 bytes)

Specify the database instance name. You must specify the instance name.

Default value: MSSQLSERVER

User Name (Within 255 bytes)

Specify the user name to log on to the database. If the user name is not specified, Windows authentication is used.

Default value: SA

Password (Within 255 bytes)

Specify the password to log on to the database. Click **Change** and enter the password in the dialog box.

Default value: None

Monitor Table Name (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: SQLWATCH

ODBC Driver Name (Within 255 bytes)

Specify the driver name of the target database shown in the **Driver** tab when you click **Start** -> **Administrative Tools** -> **Data Sources (ODBC)**.
Select **SQL Server Native Client 11.0** in SQL Server 2014.
Select **ODBC Driver 13 for SQL Server** in SQL Server 2016 or SQL Server 2017.
Select **ODBC Driver 17 for SQL Server** in SQL Server 2019.

Default value: ODBC Driver 13 for SQL Server

4.33 Understanding Tuxedo monitor resources

Tuxedo monitor resources monitor Tuxedo that runs on the server.

4.33.1 Tuxedo monitor resources

For the supported Tuxedo versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

For target monitoring resource, specify a script resource and application resource that can start Tuxedo. Monitoring starts after the target resource is activated; however, if Tuxedo cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

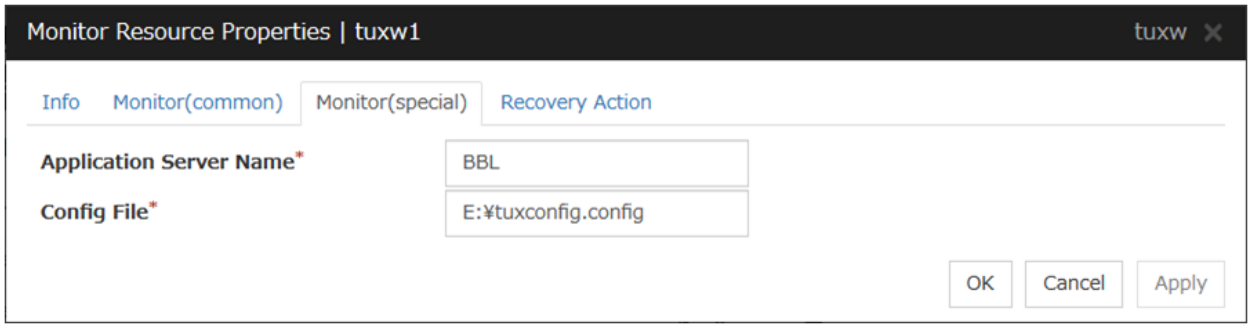
Tuxedo may produce operation logs for each monitoring. Configure the Tuxedo settings if this needs to be adjusted.

4.33.2 Monitoring by Tuxedo monitor resources

Tuxedo monitor resources connect to the Tuxedo and execute API to verify the operation. As a result of monitoring, the following is considered as an error:

1. When an error is reported during the connection to the application server and/or the acquisition of the status.

4.33.3 Monitor (special) tab



Application Server Name (Within 255 bytes)

Specify the application server name to be monitored. You must specify the name.

Default value: BBL

Config File (Within 1023 bytes)

Specify the placement file name of Tuxedo. You must specify the name.

Default value: None

4.34 Understanding WebSphere monitor resources

WebSphere monitor resources monitor WebSphere that runs on the server.

4.34.1 WebSphere monitor resources

For the supported WebSphere versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

For target monitoring resource, specify a service resource that can start WebSphere. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

A Java Runtime Environment is required to start monitoring with this command. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

WebSphere may produce operation logs for each monitoring. Configure the WebSphere settings if this needs to be adjusted.

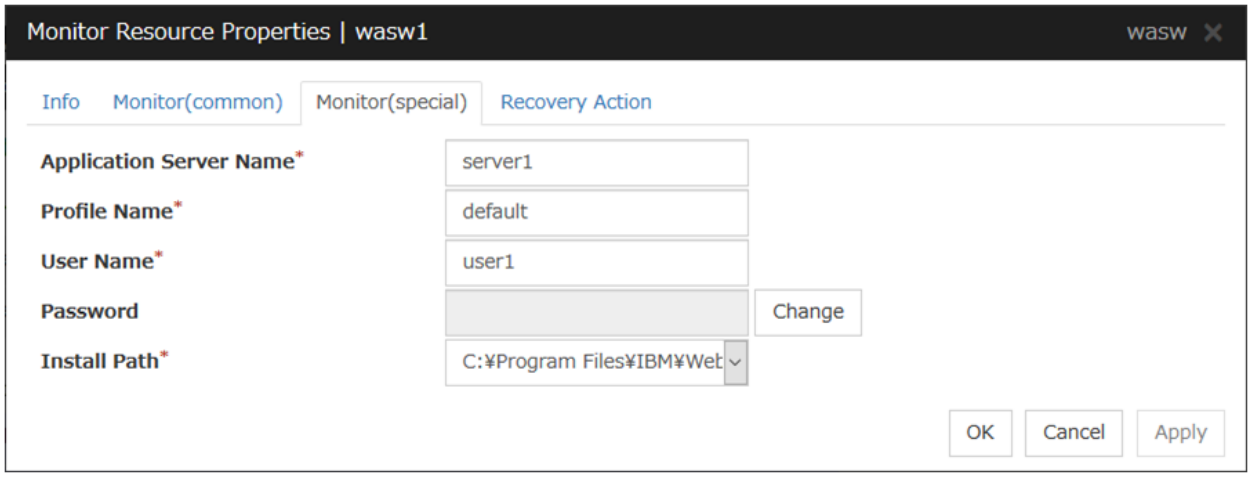
4.34.2 Monitoring by WebSphere monitor resources

WebSphere monitor resources use the serverStatus.bat command to verify the operation.

As a result of monitoring, the following is considered as an error:

1. When an error is reported with the state of the acquired application server.

4.34.3 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. You must specify the password.

Default value: None

Install Path (Within 255 bytes)

Specify the installation path of WebSphere. You must specify the path.

Default value: C:\Program Files\IBM\WebSphere\AppServer

4.35 Understanding WebLogic monitor resources

WebLogic monitor resources monitor WebLogic that runs on the server.

4.35.1 WebLogic monitor resources

For the supported WebLogic versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

If WebLogic cannot run immediately after startup, it is recognized as an error. To prevent this, adjust **Wait Time to Start Monitoring**. Or, make sure that WebLogic starts first (for example, by specifying the script resource and the application resources that start WebLogic as the monitor target resource).

If the selected monitoring method is WLST for this monitor resource, the monitoring requires a Java environment. Since the Java functions are used by the application server system, a stall of Java (if any) may be recognized as an error.

WebLogic may produce operation logs for each monitoring. Configure the WebLogic settings if this needs to be adjusted.

4.35.2 Monitoring by WebLogic monitor resources

WebLogic monitor resource monitors the following:

- Monitoring method: if RESTful API is selected

  WebLogic offers RESTful APIs called WebLogic RESTful management services.

  The RESTful APIs allow you to monitor the application server.

  As a result, an error is considered to be found if:

  1. There is an error message in response to the RESTful API.

  Note: Compared with the WLST monitoring method, RESTful API can reduce the CPU load of the application server under the monitoring.

- Monitoring method: if WLST is selected

  Monitors the application server by performing connect with the "weblogic.WLST" command.

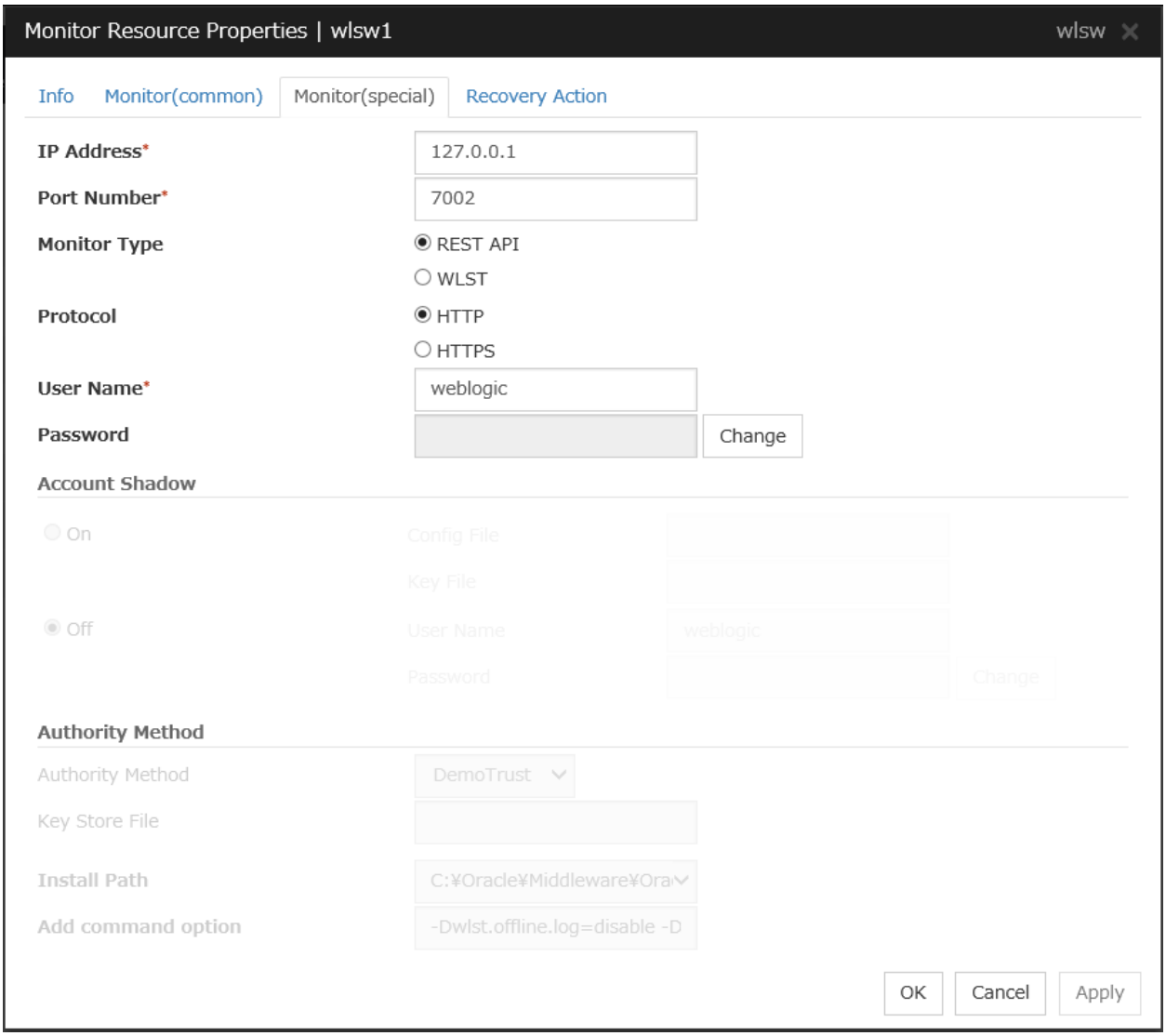
  This monitor resource determines the following results as an error:

  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.

4.35.3 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

Monitor Method

Specify the method of monitoring the server. Setting this parameter is mandatory.

Default value: RESTful API

Protocol

Specify the protocol of the server to be monitored. Setting this parameter is mandatory if RESTful API is selected in **Monitor Method**.

Default value: HTTP

User Name (Within 255 bytes)

Specify the name of the WebLogic user. Setting this parameter is mandatory if RESTful API is selected in **Monitor Method**.

Default value: weblogic

Password (Within 255 bytes)

Specify the password for WebLogic, if necessary, with RESTful API selected in **Monitor Method**.

Default value: None

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: None

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

Install Path (Within 255 bytes)

Specify the installation path of WebLogic. You must specify the path.

Default value: C:\Oracle\Middleware\Oracle_Home\wlserver

Add command option (Within 1023 bytes)

Set this value when changing the option to be passed to the webLogic.WLST command.

Default value: -Dwlst.offline.log=disable -Duser.language=en_US

4.36 Understanding WebOTX monitor resources

WebOTX monitor resources monitor WebOTX that runs on the server.

4.36.1 WebOTX monitor resources

For the supported WebOTX versions, see "Application supported by the monitoring options" in "System requirements for the EXPRESSCLUSTER Server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

For target monitoring resource, specify a script resource that can start WebOTX. Monitoring starts after the target resource is activated; however, if WebOTX cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring.**

A Java environment is required to start monitoring with this command. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

WebOTX may produce operation logs for each monitoring. Configure the WebOTX settings if this needs to be adjusted.

WebOTX monitor resource monitors application servers by using the otxadmin.bat command which Web OTX offers. ${AS_INSTALL}\bin where the otxadmin.bat command is arranged is not included in environment variable PATH any more in WebOTX V10.1 or later. When monitoring WebOTX V10.1 or later, configure either of the following settings.

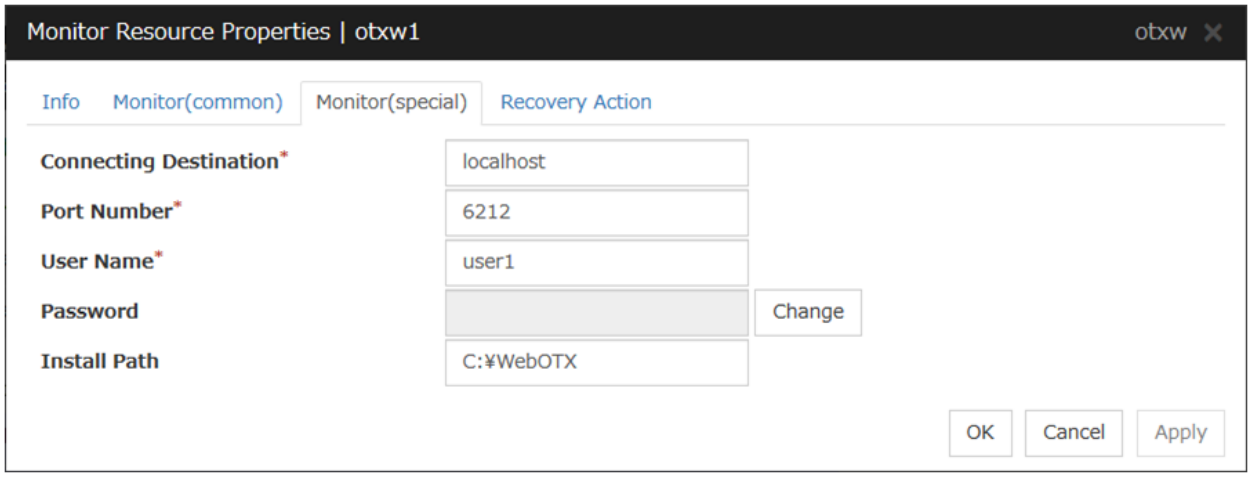
- Add the path where otxadmin.bat command is located to the system environment variable, PATH.
- Set the install path of WebOTX Application Server to Install Path. (e.g. C:\WebOTX)

4.36.2 Monitoring by WebOTX monitor resources

WebOTX monitor resources use the otxadmin.bat command to verify the operation. As a result of monitoring, the following is considered as an error:

1. When an error is reported with the state of the acquired application server.

4.36.3 Monitor (special) tab



Connecting Destination (Within 255 bytes)

Specify the server name of the server to be monitored. You must specify the name.

Default value: localhost

Port Number (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 install path of WebOTX Application Server. You must configure this setting when monitoring WebOTX Application Server V10.1 or later.

Default value: None

4.37 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.

4.37.1 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**.
- The status of the JVM monitor resource is "Warning" from when monitoring is started to when the monitoring processing is actually performed.

4.37.2 Monitoring by JVM monitor resources

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 or WebOTX).

The following figure illustrates monitoring by a JVM monitor resource.
In phase a), it starts monitoring the target Java VM.
For this monitoring, JMX (Java Management Extensions) is used.
From the Java VM via JMX, Java Resource Agent periodically obtains data on the resource usage, checking the status of the Java VM.
In phase b), when the status changes from normal to abnormal, the detected error of the Java VM is displayed on Cluster WebUI, where you can see the status and the corresponding alert.
In phase c), the failure is reported to the event log and the JVM operation log.
If the alert service is used, email notification is also available.
When the status changes from abnormal to normal after phase a), Cluster WebUI is informed in phase d) that the Java VM's returning to normal is detected.

In phase e), the restoration is reported to the event log and the JVM operation log.

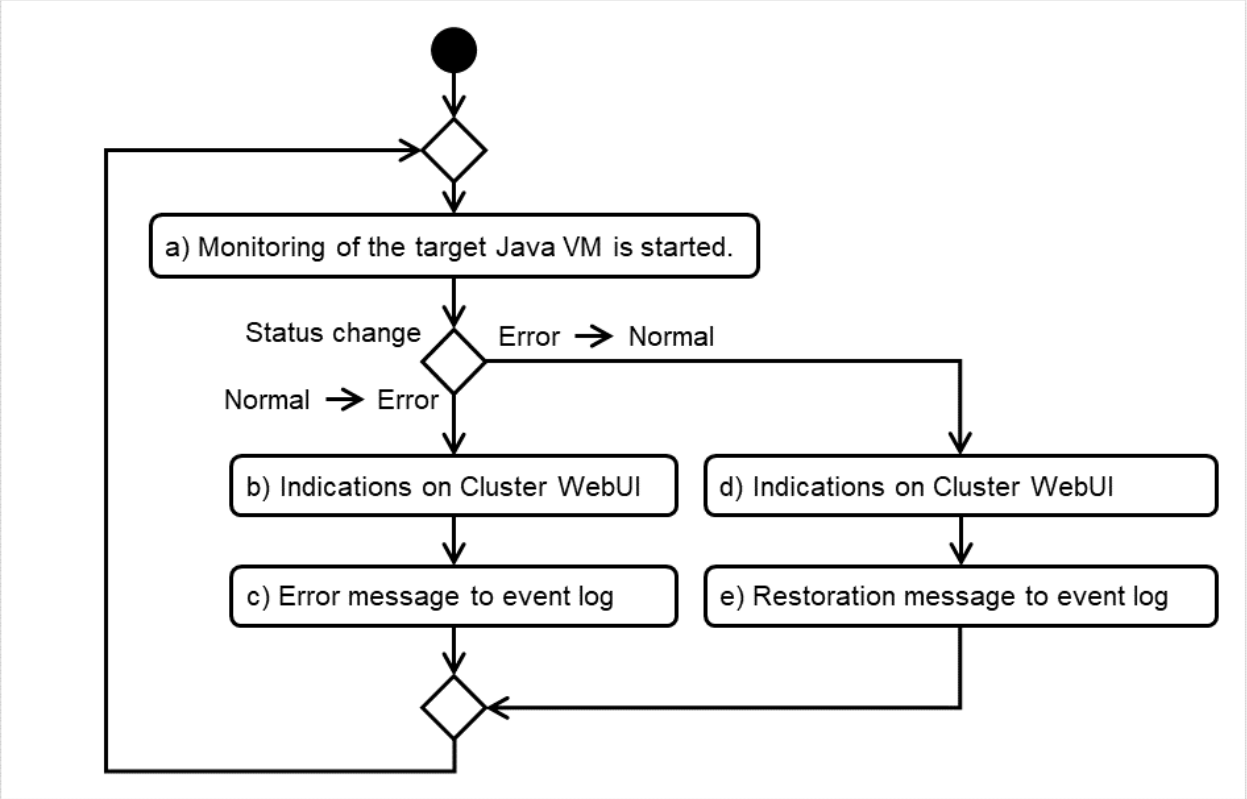


Fig. 4.63: Flow of monitoring by a JVM monitor resource

The standard operations when the threshold is exceeded are as described below.

In the following figure, the horizontal axis indicates a lapse of time; the vertical axis shows whether the monitoring threshold is exceeded or not.
If a count of consecutively exceeding the threshold reaches a specified value (five in this figure), an error is considered to occur.
After that, when the specified value is reached by a count of consecutively falling short of the threshold, the situation is considered to return to normal.

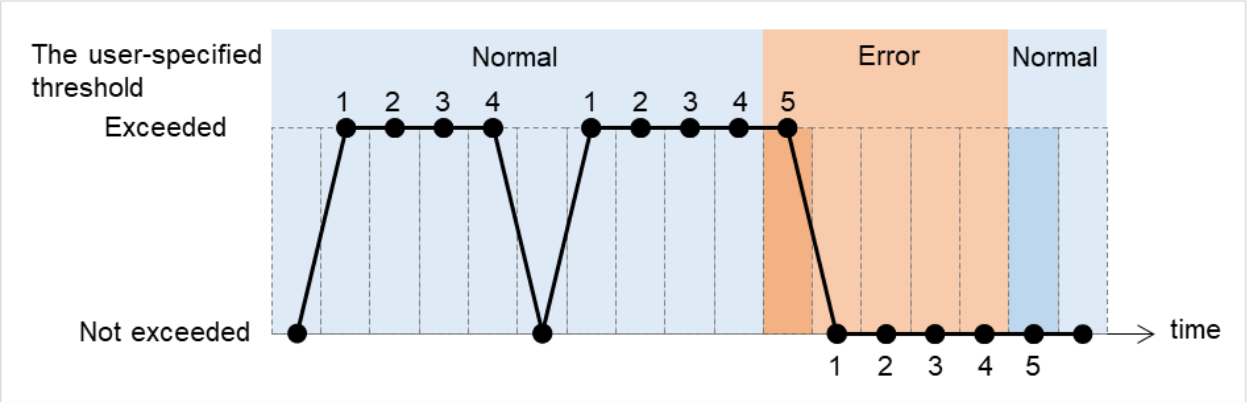


Fig. 4.64: Behavior when the threshold is exceeded

The operations performed if an error persists are as described below.

If a count of consecutively exceeding the threshold reaches a specified value, an error is considered to occur.
After that, even if the consecutive excess reoccurs by the specified count, Cluster WebUI does not alert you to it.

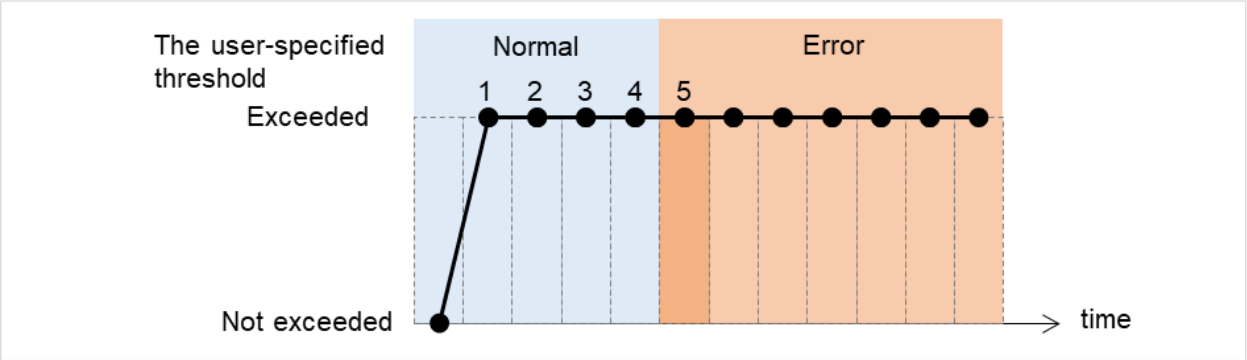


Fig. 4.65: Behavior when an error persists

The following example describes the case of monitoring Full GC (Garbage Collection).

In the following figure, the horizontal axis indicates a lapse of time.
The upper part of the figure illustrates whether the GC occurrence is detected at each timing of monitoring; the lower part shows how many times Full GC is consecutively detected at each point of time.
If a count of the consecutive Full GC occurrence reaches a specified value, the JVM monitor resource considers it as an error.
In this case, the error threshold is set at five. Therefore, when the count reaches five, an error is considered to occur.

Full GC has a significant influence on the system, thus the recommended error threshold is 1 time.

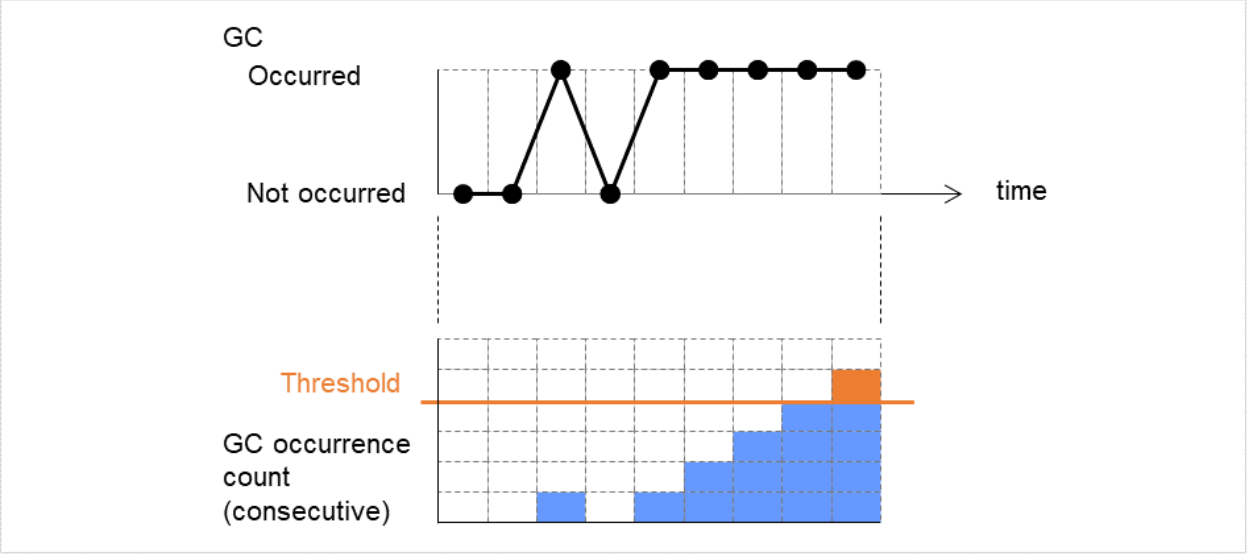


Fig. 4.66: Image of monitoring (when the error threshold is set at five)

4.37.3 JVM statistical log

JVM monitor resources collect statistical information on the monitor target Java VM. The information is stored on CSV-format files, JVM statistical logs. The file is created in the following location:

<*EXPRESSCLUSTER_install_path*>\log\ha\jra*.stat

The following "monitor items" refer to parameters in the [Monitor(special)] tab in the [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 monitor items and their corresponding JVM statistical logs.

Monitor items	Corresponding JVM statistical 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

4.37.4 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 becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: jramemory<*integer starting with 0*>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: jramemory<*YYYYMMDDhhmm*>.stat

Its data formats are 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; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] 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 the Java memory pool Heap, Non-Heap

Continued on next page

Table 4.43 – continued from previous page

No	Format	Description
5	Half-size numeric characters	Memory size that the Java VM requests from the OS at startup; it is expressed in bytes. (init) At the startup of the monitor target Java VM, the size can be specified by 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; it is expressed in bytes. (used)
7	Half-size numeric characters	Memory size guaranteed for current use in operation of the Java VM; it is expressed in bytes. (committed) This size varies depending on memory use; it is always equal to the value of "used" or larger but equal to the value of "max" or smaller.
8	Half-size numeric characters	Maximum memory size that the Java VM can use; it is expressed in bytes. (max) The size can be specified by 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, "ini" may become larger than "max". This is because "max" of HEAP is determined by subtracting half the size of Survivor Space from the area size ensured by 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). It is expressed in bytes.

Continued on next page

Table 4.43 – 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 not HEAP, it is 0.

4.37.5 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 becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: jrathread<*integer starting with 0*>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: jrathread<*YYYYMMDDhhmm*>.stat

Its data formats are 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; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	The 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; it contains the IDs of all deadlocked threads successively.
5	Half-size alphanumeric characters and symbols	Detailed information on deadlocked threads in the monitor target Java VM; it contains information on all deadlocked threads successively 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

4.37.6 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 becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type]-[File Capacity] is checked: jragc< *integer starting with 0*>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: jragc<*YYYYMMDDhhmm*>.stat

JVM monitor resources output two types of GC information: Copy GC and Full GC.

On 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

Its data formats are 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; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	GC name of the monitor target Java VM When the monitor target Java VM is Oracle Java The GC name to be indicated is one of the following. Copy MarksweepCompact MarkSweepCompact PS Scavenge PS Marksweep ParNew ConcurrentMarkSweep
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 GC executed before the JVM monitor resources starts monitoring.
5	Half-size numeric characters	Total time in GC during the period from startup of the monitor target Java VM to measurement; it is expressed in milliseconds. It includes time taken for GC executed before the JVM monitor resources starts monitoring.

4.37.7 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 becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: wlworkmanager<*integer starting with 0*>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: wlworkmanager<*YYYYMMDDhhmm*>.stat

Its data formats are 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; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] 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	Count of request execution
6	Half-size numeric characters	The number of wait requests

4.37.8 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 becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked:wlthreadpool< *integer starting with 0*>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: wlthreadpool<*YYYYMMDDhhmm*>.stat

Its data formats are 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; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size numeric characters	Total count of request execution
4	Half-size numeric characters	The number of requests queued in the WebLogic Server
5	Half-size numeric characters	Count of request execution per unit time (second)
6	Half-size numeric characters	The total number of threads for executing the application
7	Half-size numeric characters	The number of threads in an idle state
8	Half-size numeric characters	The number of executing threads
9	Half-size numeric characters	The number of threads in a stand-by state

4.37.9 Java memory pool name

This section describes the Java memory pool name outputted as memory_name in messages to the JVM operation log file. It also describes the Java memory pool name outputted to a JVM statistical log file, jramemory.stat log file.

The character strings of Java memory pool names are not determined by 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 in a version upgrade of Java VM.

Therefore, we do not recommend monitoring Java memory pool names contained in messages.

The following monitor items refer to parameters in the [Memory] tab of the [Monitor(special)] tab in the [Properties] of the JVM monitor resources.

The following memory pool names have been confirmed on actual machines operating on Oracle Java.

When **Oracle Java** is selected for **JVM Type**, and "-XX:+UseSerialGC" is specified as a startup option of the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat log file appears as follows.

Monitor item	Character string outputted 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 startup options of the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat log file appears as follows.

Monitor item	Character string outputted 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 of the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat log file appears as follows.

Monitor item	Character string outputted 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

Continued on next page

Table 4.50 – continued from previous page

Monitor item	Character string outputted as memory_name
[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]
[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 jrammemory.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 or later, 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" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.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 or later, 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 jrammemory.stat file will be as follows. For Java 9 or later, 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 Non-Heap Memory Usage]-[Tenured Gen]	Tenured Gen

Continued on next page

Table 4.53 – continued from previous page

Monitor item	Character string output as memory_name
[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 jrammemory.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 or later, 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

Java memory pool names appearing in the jrammemory.stat log file, a JVM statistical log file, correspond to the Java VM memory space as follows.

- For Oracle Java 8/Oracle Java 9/Oracle Java 11/Oracle Java 17

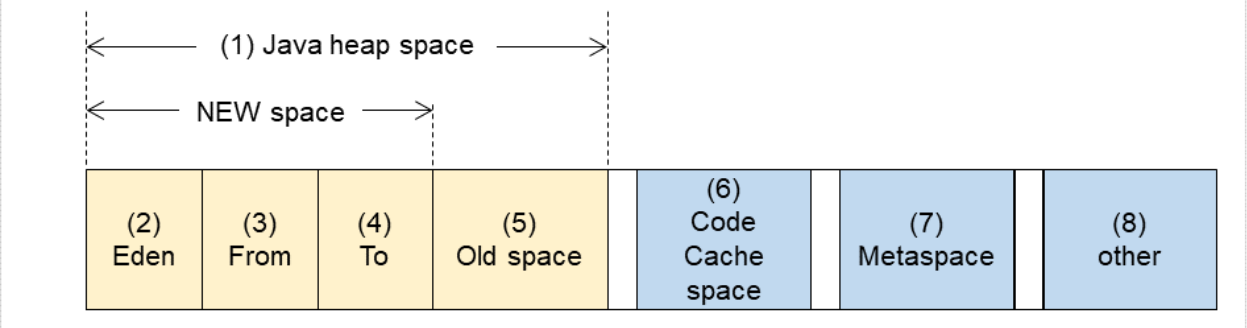


Fig. 4.67: Java VM memory space (Oracle Java 8/Oracle Java 9/Oracle Java 11/Oracle Java 17)

Number in diagram	Monitor item	Java memory pool name in jrammemory.stat log file
(1)	[Monitor Heap Memory Usage] - [Total Usage]	HEAP

Continued on next page

Table 4.55 – continued from previous page

Number in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(2)	[Monitor Heap Memory Usage] - [Eden Space]	EdenSpace PS Eden Space Par Eden Space G1 Eden Space
(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 G1 Old Gen
(6)	[Monitor Non-Heap Memory Usage] - [Code Cache]	Code Cache (For Java 9 or later, no output)
(6)	[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods (Only for Java 9 or later, it is output.)
(6)	[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods (Only for Java 9 or later, it is output.)
(6)	[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods (Only for Java 9 or later, 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

4.37.10 Executing command corresponding to cause of each detected error

EXPRESSCLUSTER does not provide means for executing specific commands according to 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 commands that will be executed according to error causes.

Error cause	Setting item
- Failure in connection to the monitor target Java VM - Failure in resource measurement	[Monitor(special)] tab - [Command]

Continued on next page

Table 4.56 – continued from previous page

Error cause	Setting item
- Heap memory rate - Non-heap memory rate - Heap memory usage - Non-heap memory usage	[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]
- The 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]

A [Command] passes the detail of an error cause as the arguments of a command with the arguments attached to the end of the [Command]. A Command further specialized for dealing with specific error causes can be defined by designing and specifying a script etc. for a [Command]. The following character strings are passed as the arguments.

When multiple character strings are stated as possible arguments, one of them will be passed according to the CG type of the monitor target Java VM. For the details of their differences, refer to "Java memory pool name".

Statements "(For Oracle Java)" suggest that different character strings are used according to the JVM type. When no such statement is contained, the same character strings will be equally used for all JVM types.

Details of error causes	Character string for 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

Continued on next page

Table 4.57 – continued from previous page

Details of error causes	Character string for argument
[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
[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

Continued on next page

Table 4.57 – continued from previous page

Details of error causes	Character string for argument
[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
[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]	c:\Program Files\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 successively as many times as specified by the Error Threshold (three times), JVM monitor resources will detect a monitor error and execute a command corresponding to "c:\Program Files\bin\downcmd Cont".

Example 2)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	"c:\Program Files\bin\downcmd" GC
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the time in Full GC]	65536
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the time in Full GC exceeds 65535 milliseconds successively as many times as specified by the Error Threshold (three times), JVM monitor resources will detect a monitor error and execute a command corresponding to "c:\Program Files\bin\downcmd GC Time".

Example 3)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]	"c:\Program Files\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% successively as many times as specified by the Error Threshold (three times), JVM monitor resources will detect a monitor error and execute a command corresponding to "c:\Program Files\bin\downcmd memory EdenSpace SurvivorSpace".

Timeout (second) for waiting for the completion of execution of the command specified by the [Command] is set by specifying the [Command Timeout] in the [JVM monitor] of the [Cluster Properties] window. The same value is applied to the timeout of the [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 needs to 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 cautions.

- No [Command] is executed when restoration of the Java VM to normal operation (error -> normal operation) is detected.
- A [Command] is executed upon detection of an error of the Java VM (when threshold crossing occurs successively as many times as specified by the error threshold). It is not executed at each threshold crossing.
- Note that specifying a [Command] on multiple tabs allows multiple commands to be executed if multiple errors occur simultaneously, causing a large system load.
- A [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 on 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 avoid this phenomenon, 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]

4.37.11 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 config mode of Cluster WebUI.
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. Open the script for starting the WebLogic Server managing server (startWebLogic.cmd).
6. Write the following instructions in the script.
   - When the target is the WebLogic Server managing server:

```
set 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.

   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.

   - When the target is a WebLogic Server managed server:

```
if "%SERVER_NAME%" == "SERVER_NAME"(
set 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 on one line.

   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%
-Dweblogic.Name=%SERVER_NAME%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy %JAVA_OPTIONS
% %PROXY_SETTINGS% %SERVER_CLASS%
```

*Write the above coding on one line.

* The contents of the above arguments may differ depending on the WebLogic version. In such a case, write JAVA_OPTIONS in the script before executing java.

7. If monitoring a request of work manager and thread pool, configure the following settings:
   Start WLST (wlst.cmd) of the target WebLogic Server.
   To do this, select Start menu-Oracle WebLogic-WebLogic Server <version number>-Tools-WebLogic Scripting Tool.
   On the prompt 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** with those for the domain environment.

8. Restart the target WebLogic Server.

4.37.12 Monitoring WebOTX

This section 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 the console" in the *WebOTX Operation (Web Administration Console)*.

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.

4.37.13 Monitoring a Java process of the WebOTX domain agent

There is no need to specify any settings.

4.37.14 Monitoring a Java process of a WebOTX process group

1. Connect to the domain by using the administration console.
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 (**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
-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 console. When making these settings by using the console, 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

4.37.15 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

4.37.16 Monitoring Tomcat

This section describes how to configure a target Tomcat to be monitored by the JVM monitor resource.

1. Stop Tomcat, and then open **Start -** (*Tomcat_Program_folder*) **- Configure Tomcat.**
2. In the Java Options of Java of the open window, 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 **(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
```

3. Save the settings, and then start Tomcat.
4. With Cluster WebUI (**JVM Monitor Resource Name - Property - Monitor(special)** tab **- Identifier**), specify a unique string that is different from those for the other monitor targets (e.g., tomcat).

4.37.17 Monitoring SVF

This section describes how to configure a target SVF to be monitored by the JVM monitor resource.

1. Select a monitor target from the following, and then use an editor to open the file.

Monitor target	File to be edited
UCX Server Service (for 9.x or later)	<SVF installation path> \launcher\UCXServer.run
Report Director EnterpriseServer	<SVF installation path> \launcher\ReportDirectorEnterpriseServer.run
Report Director Svf Server	<SVF installation path> \launcher\ReportDirectorSvfServer.run
Report Director Spool Balancer	<SVF installation path> \launcher\ReportDirectorSpoolBalancer.run
Tomcat	%FIT_PRODUCTS_BASE%\SetupUtils\setup_tomcat.bat
SVF Print Spooler services	<SVF installation path> \svfjpd\launcher\SpoolerDaemon.run

2. (When the monitor target is Tomcat:)
   Insert the additional description to --JvmOption of :install within setup_tomcat.bat in the following way. 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**).

Before the change:

```
--JvmOptions=...
```

After the change:

```
--JvmOptions=...;-Dcom.sun.management.jmxremote.port=n;-Dcom.sun.management.
↪jmxremote.ssl=false;-Dcom.sun.management.jmxremote.authenticate=false
```

3. (When the monitor target is other than Tomcat:)
   The following contents are inserted in the part where Arguments is designated just after the setting point of "-Xms". 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
```

4.37.18 Monitoring a Java application that you created

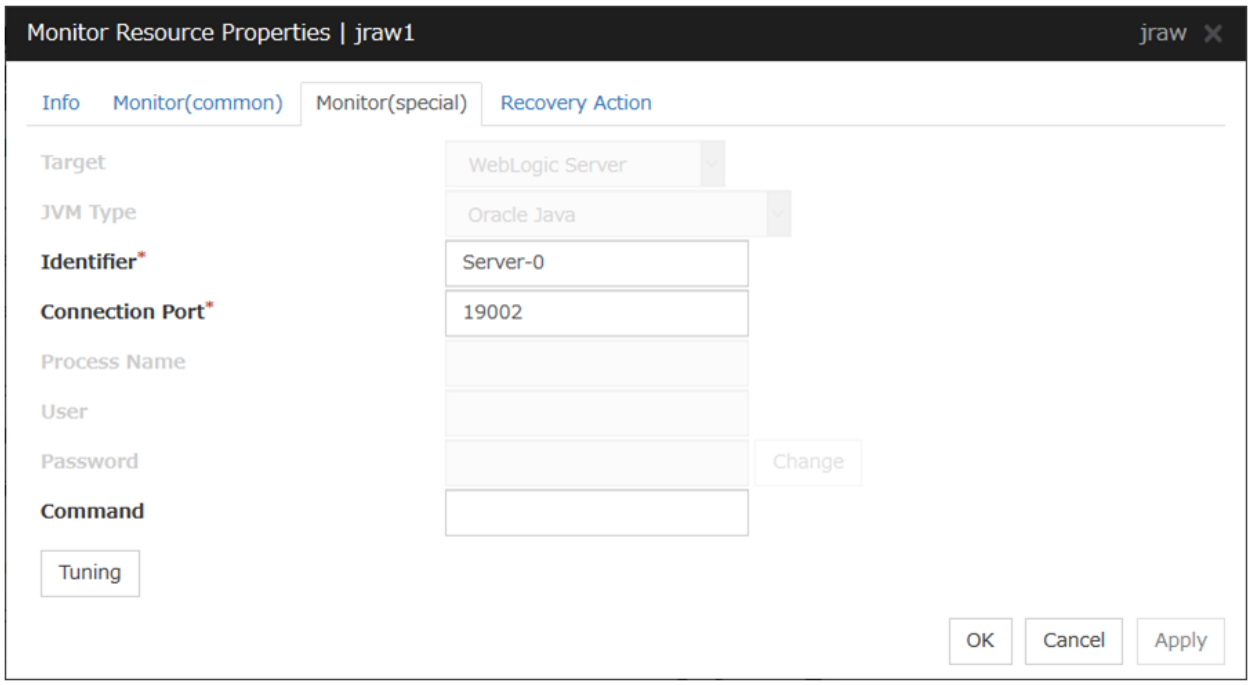
This section describes the procedure to configure Java application which is monitored by JVM monitor resource. Specify the following Java option in one row to the option for Java application startup while Java application (the monitor target) is stopped. For **n**, specify the port number. If there is 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>
```

4.37.19 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**.

Default: None

JVM Type

Select the Java VM on which the target application to be monitored is running.

For Java 8 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.

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 **WebOTX ESB**
  Same as for **WebOTX Process Group**.
- When the target is **Tomcat**
  Specify this according to "*Monitoring Tomcat*".
- When the target is **WebSAM SVF**
  Specify this according to "*Monitoring SVF*".
- When the target is **Java applications**
  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 **WebOTX ESB**
  Same as for **WebOTX Process Group**.
- When the target is **Tomcat**
  Specify as described in "*Monitoring Tomcat*".
- When the target is **WebSAM SVF**
  Specify this according to "*Monitoring SVF*".
- When the target is **Java applications**

Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

Process Name (Within 255 bytes)

This does not need to be configured because the monitor target Java VM can be identified by **Connection Port**. The internal version 11.35 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 12.00, **Monitor Virtual Memory Usage** was deleted. Therefore, it cannot be specified.

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 "(WebOTX_installation_path)\<*domain_name*>.properties".

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 "(WebOTX_installation_path)\<*domain_name*>.properties". Click **Change** and enter the password in the dialog box. The letters of the password are not displayed.

Default: None

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) "\Program Files\bin\command.bat" arg1 arg2

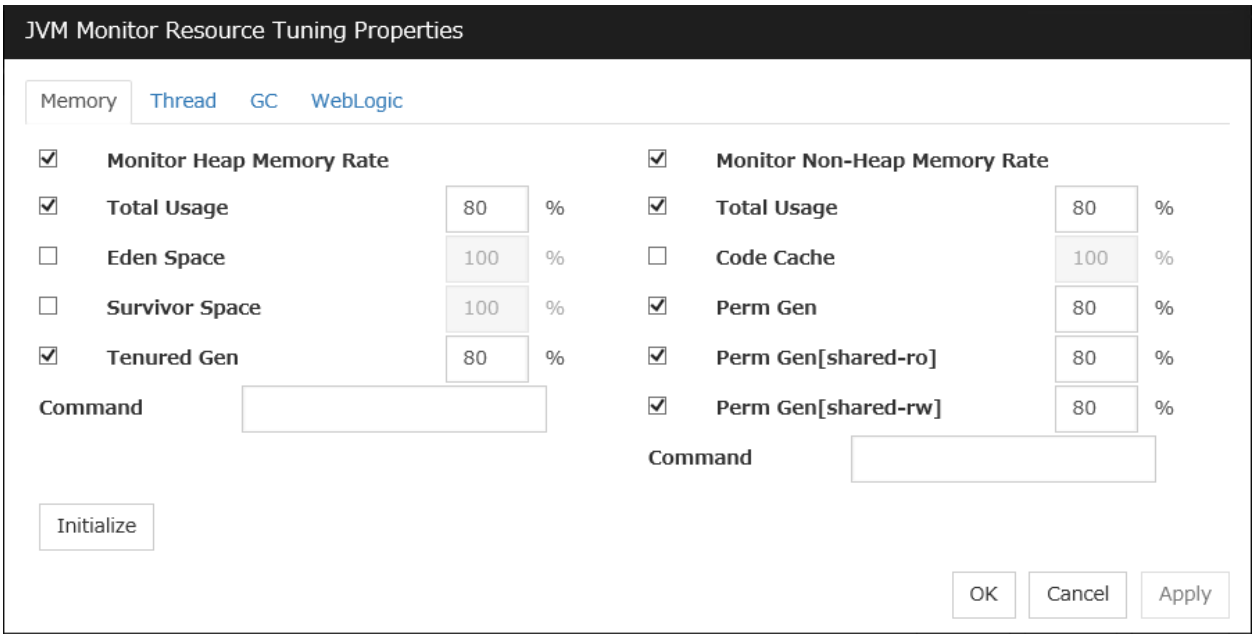
Here, specify the commands to execute if it is impossible to connect to the target Java VM and if an error is detected in acquiring the resource amount used.

See also "*Executing 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.

4.37.20 Memory tab(when Oracle Java 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 checkbox is selected (default):
  Monitoring enabled
- When the checkbox 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 of the target Java VM, 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 of the target Java VM, 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 of the target Java VM, 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 checkbox is selected (default):
  Monitoring enabled
- When the checkbox 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)

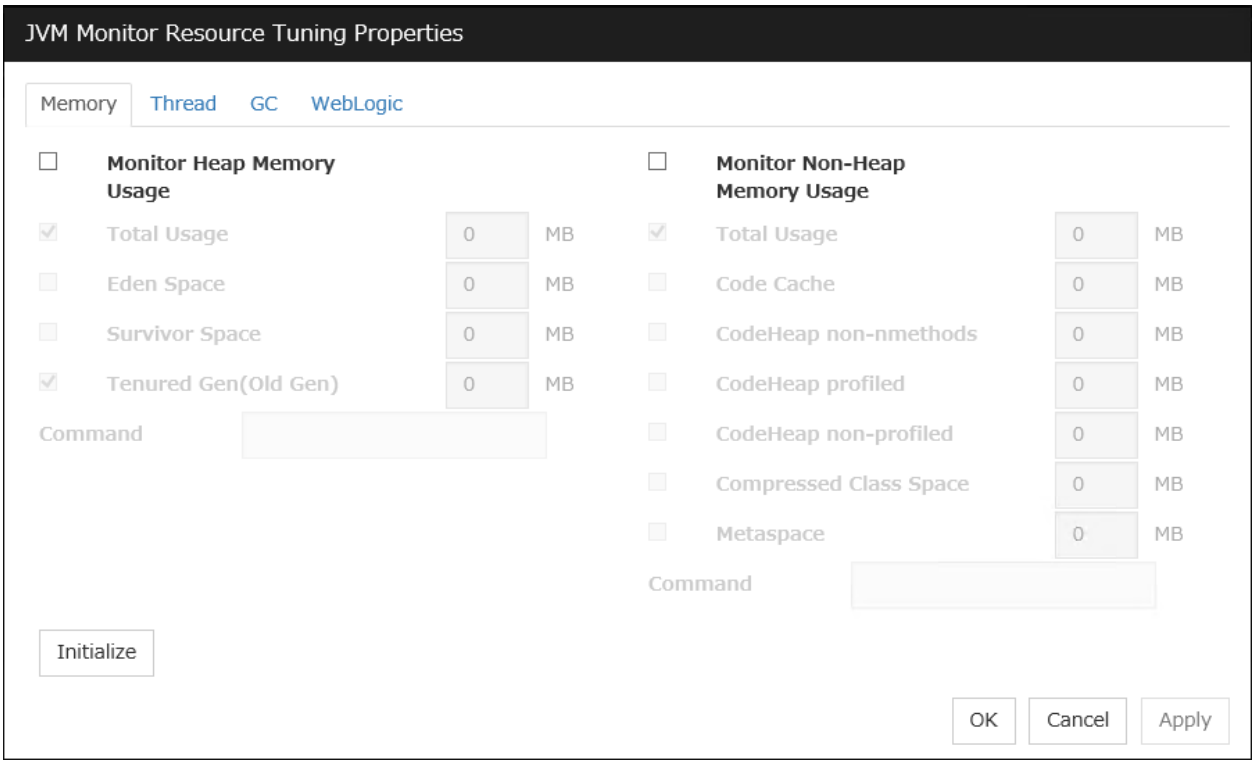
Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").
Example) "\Program Files\bin\command.bat" arg1 arg2
Here, specify the commands to execute if an error is detected in the Java heap area, and Java non-heap area of the target Java VM.
See also "*Executing command corresponding to cause of each detected error*".

Default: None

Initialize

Click the **Initialize** button to set all the items to their default values.

4.37.21 Memory tab(when Oracle Java(usage monitoring) is selected for JVM Type)



Monitor Heap Memory Usage

Enables the monitoring of the amount of the Java heap areas used by the target Java VM.

- When the checkbox is selected:
  Monitoring enabled
- When the checkbox is not selected (default):
  Monitoring disabled

Total Usage (0 to 102400)

Specify the threshold for the usage rate 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 of the target Java VM, 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 of the target Java VM, 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 of the target Java VM, 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 **Java Code Cache** 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) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the commands to execute if an error is detected in the Java heap area, and Java non-heap area of the target Java VM.

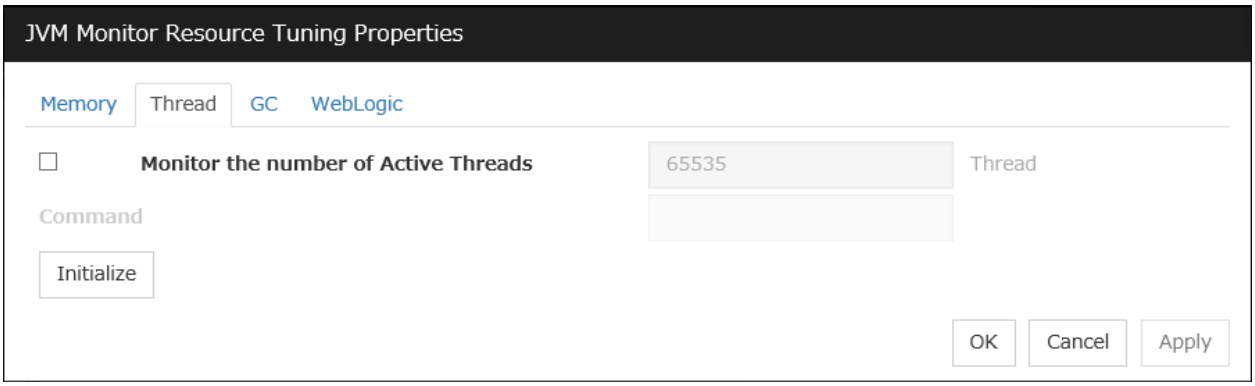
See also "*Executing command corresponding to cause of each detected error*".

Default: None

Initialize

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

4.37.22 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 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) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the command to execute if an error is detected in the number of threads currently running in the target Java VM.

See also "*Executing command corresponding to cause of each detected error*".

Default: None

Initialize

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

4.37.23 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)

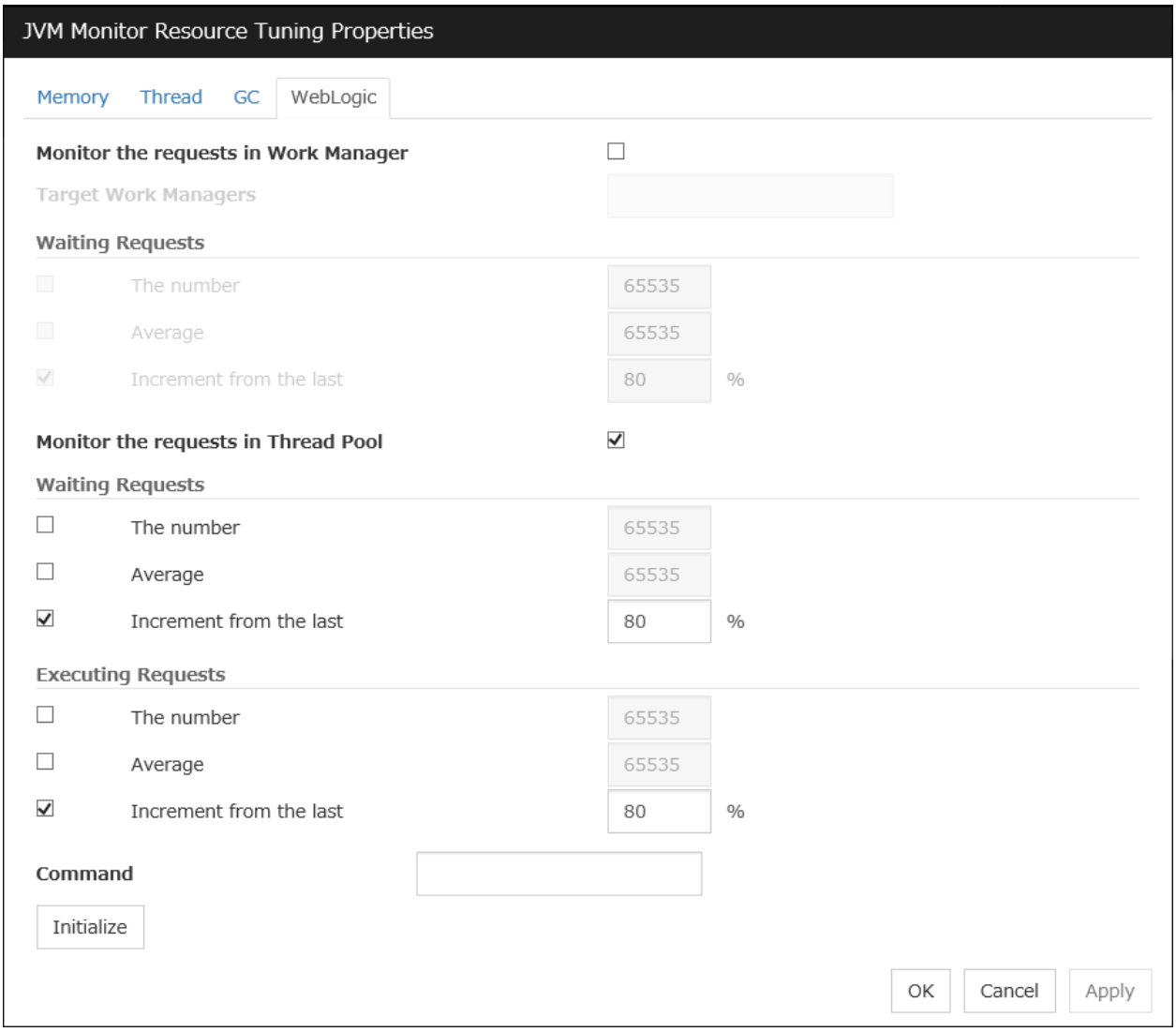
Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").
Example) "\Program Files\bin\command.bat" arg1 arg2
Here, specify the commands to execute if an error is detected in the Full GC execution time and Full GC execution count of the target Java VM.
See also "*Executing command corresponding to cause of each detected error*".

Default: None

Initialize

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

4.37.24 WebLogic tab



Monitor the requests in Work Manager

Enables the monitoring of the wait requests by Work Managers on the WebLogic Server.

- When the checkbox is selected:
  Monitoring enabled
- When the checkbox is not selected (default):
  Monitoring disabled

Target Work Managers (Within 255 bytes)

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

Enables the monitoring of the number of wait requests (number of HTTP requests queued in the WebLogic Server) and the number of executing requests (number of HTTP requests queued in the WebLogic Server) in the target WebLogic Server thread pool.

- When the checkbox is selected (default):
  Monitoring enabled
- When the checkbox 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 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) "\Program Files\bin\command.bat"

Here, specify the commands to execute if an error is detected in the requests in the thread pool or in the work manager of the WebLogic Server.

See also '"*Executing command corresponding to cause of each detected error*".

Default: None

Initialize

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

4.38 Understanding system monitor resources

System monitor resources monitor the system resources. The resources periodically collect statistical information about system resources and 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.

4.38.1 Notes on system monitor resource

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 system resource value repeatedly exceeds and then falls below a threshold.

In a case like where the system is high loaded, it may take a long time to collect statistical information and the interval of statistical information collection may be unapplied.

If date or time of OS has been changed during System Resource Agent's operation, resource monitoring may operate wrongly as follows since the timing of analyze which is normally done at 10 minute intervals may be changed at first time after changing date or time. In such case, suspend and resume cluster.

- Error is not detected after passing specified duration to detect error.
- Error is detected before passing specified duration to detect error.

Once the cluster has been suspended and resumed, the collection of information is started from that point of time.

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 smaller value than the actual disk size when specifying the disk size for free space monitoring of disk resources. If a larger value specified, a lack-of-free-space error will be detected.

If the monitored disk is exchanged, the following information analyzed up to then will be cleared if it differs from the information in the previous disk:

- Total disk capacity
- File system

For servers in which no swap areas are allocated, uncheck monitoring the total usage of virtual memory.

When monitoring disk resources, only hard disks can be monitored.

Up to 26 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.

The status of the system monitor resource is Warning from when start of monitoring is enabled to when the monitoring processing is actually performed.

Too many number of registered system monitor resources and process resource monitor resources may be detected as an error and lead to outputting the following message to the alert log.
If this message is output, review the timeout setting in the **Monitor (common)** tab.

Monitor sraw has detected an error. (99 : monitor was timeout)

4.38.2 Monitoring by system monitor resources

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.

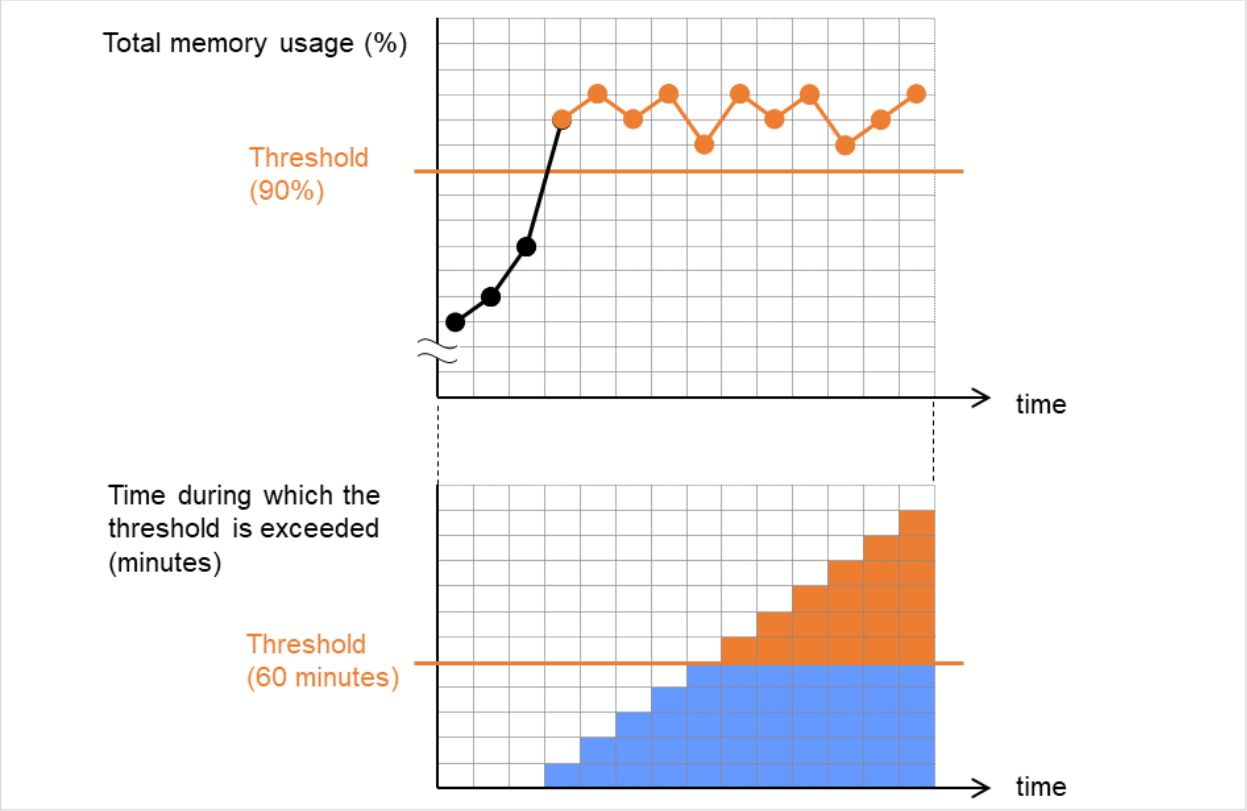


Fig. 4.68: Total memory usage at its threshold or higher for a certain time, which leads to error detection

- 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.

  In the following figure, the total memory usage temporarily reaches its threshold (90%) or higher. However, this situation does not last for the monitoring duration (60 minutes), and therefore does not lead to detecting an error in the total memory usage.

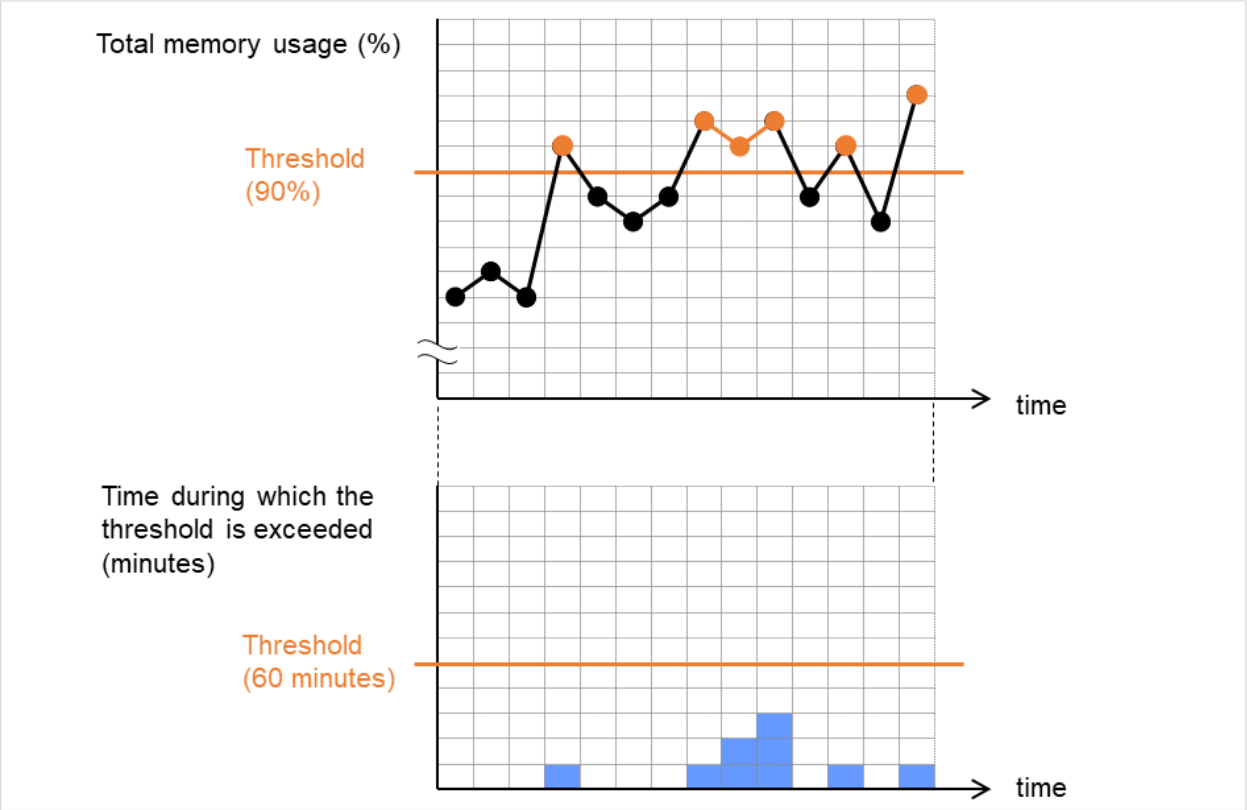


Fig. 4.69: Total memory usage at its threshold or higher for less than a certain time, which does not lead to error detection

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.

  This excess causes an error to be considered to occur in monitoring the disk usage.

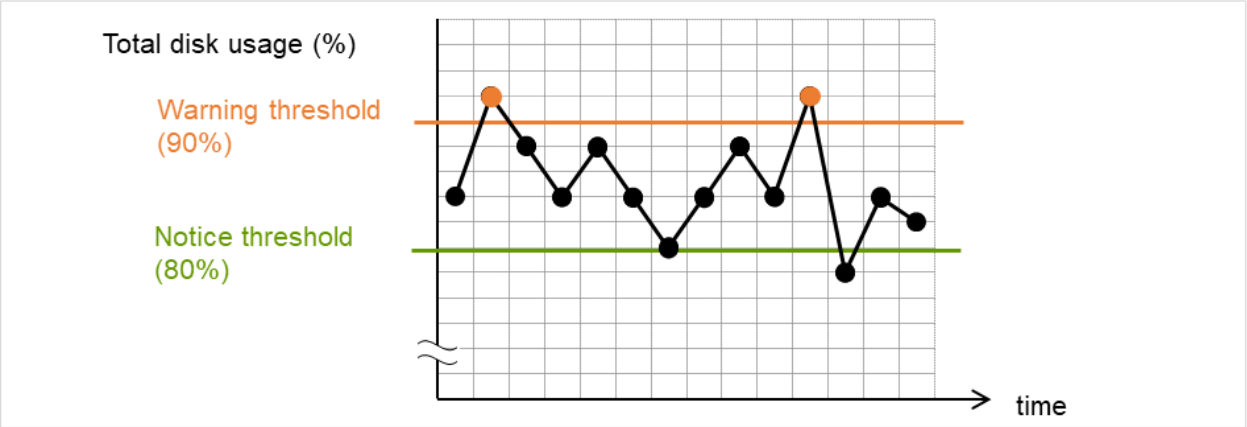


Fig. 4.70: Disk usage exceeding the upper limit of the warning level, which leads to error detection

- 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.

  Since the disk usage changes within the upper limit of the warning level, no error is considered to occur in monitoring the disk usage.

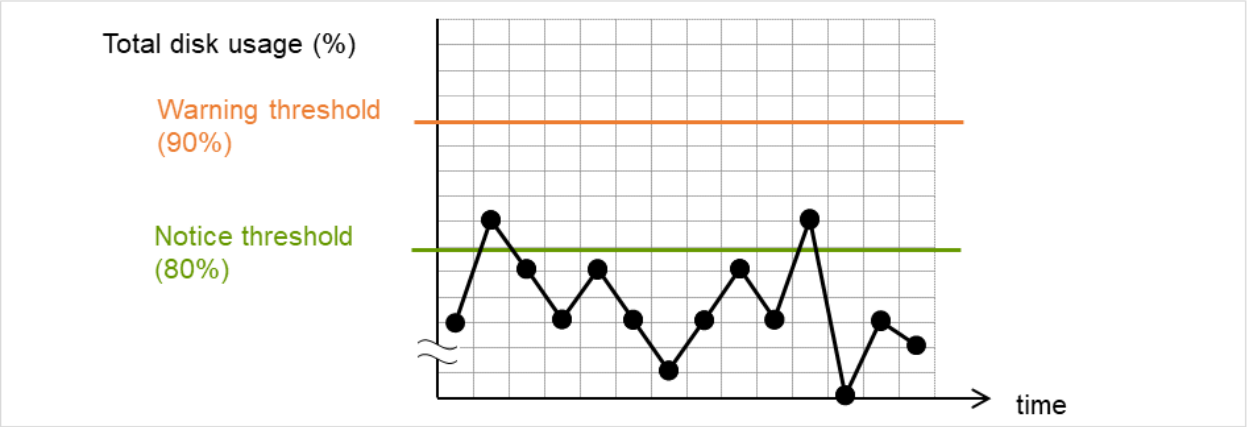


Fig. 4.71: Disk usage not exceeding the upper limit of the warning level, which does not lead to error detection

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.

  The excess of disk usage causes an error to be considered to occur in monitoring the disk usage.

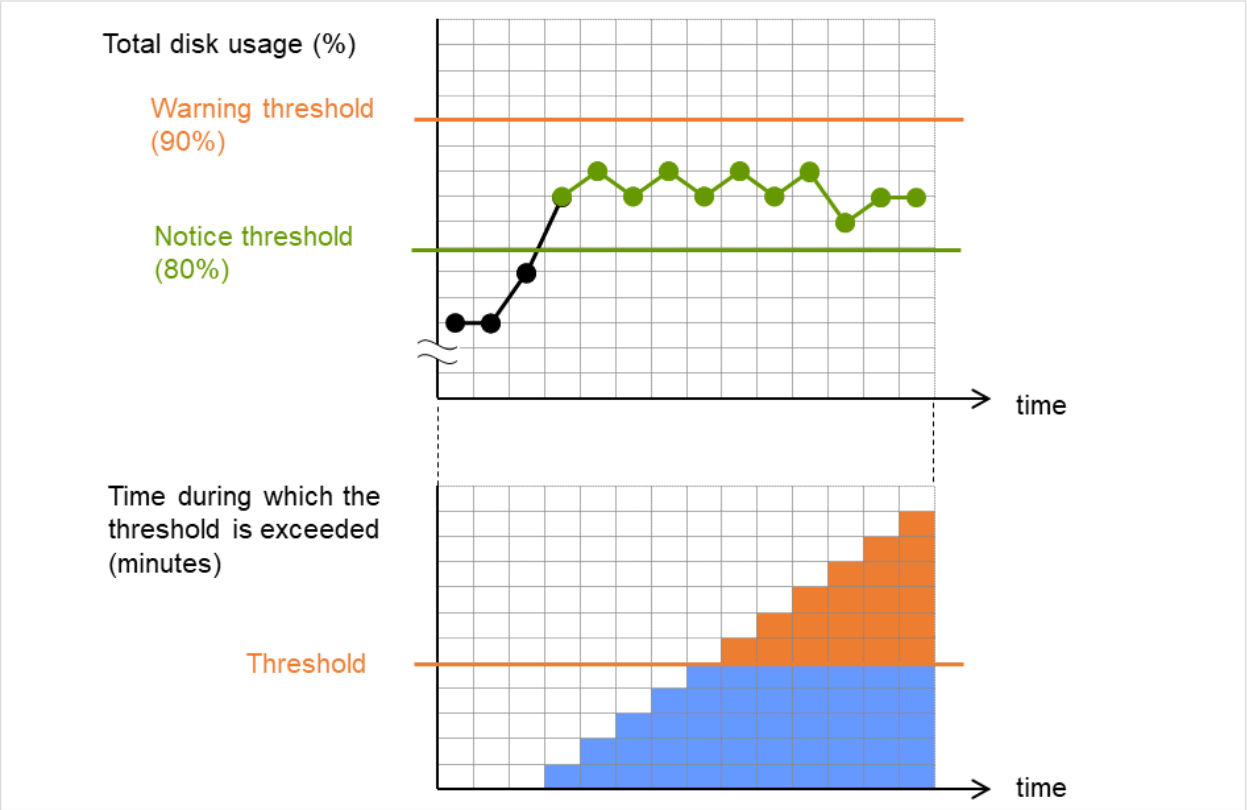


Fig. 4.72: Disk usage exceeding the upper limit of the notification level for a certain time, which leads to error detection

- 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.

  Since the excess of disk usage does not last for a certain time, no error is considered to occur in monitoring the disk usage.

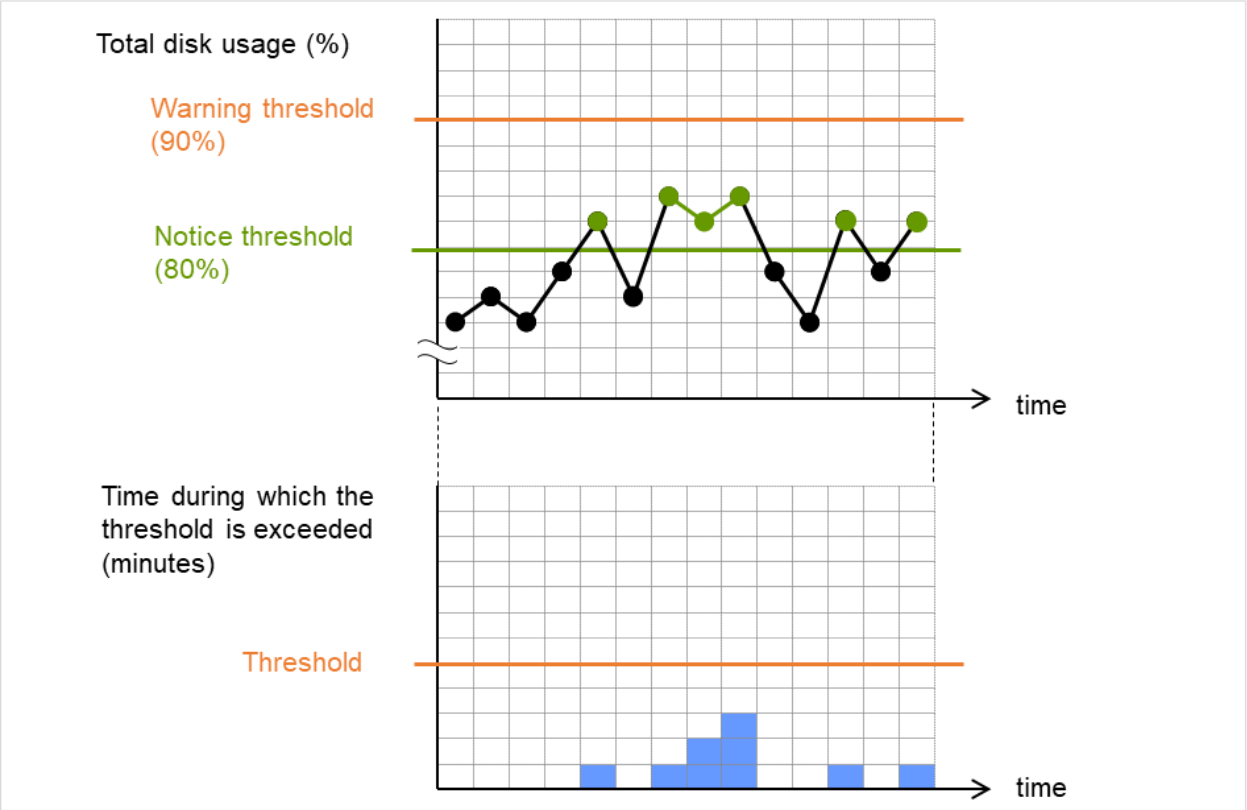
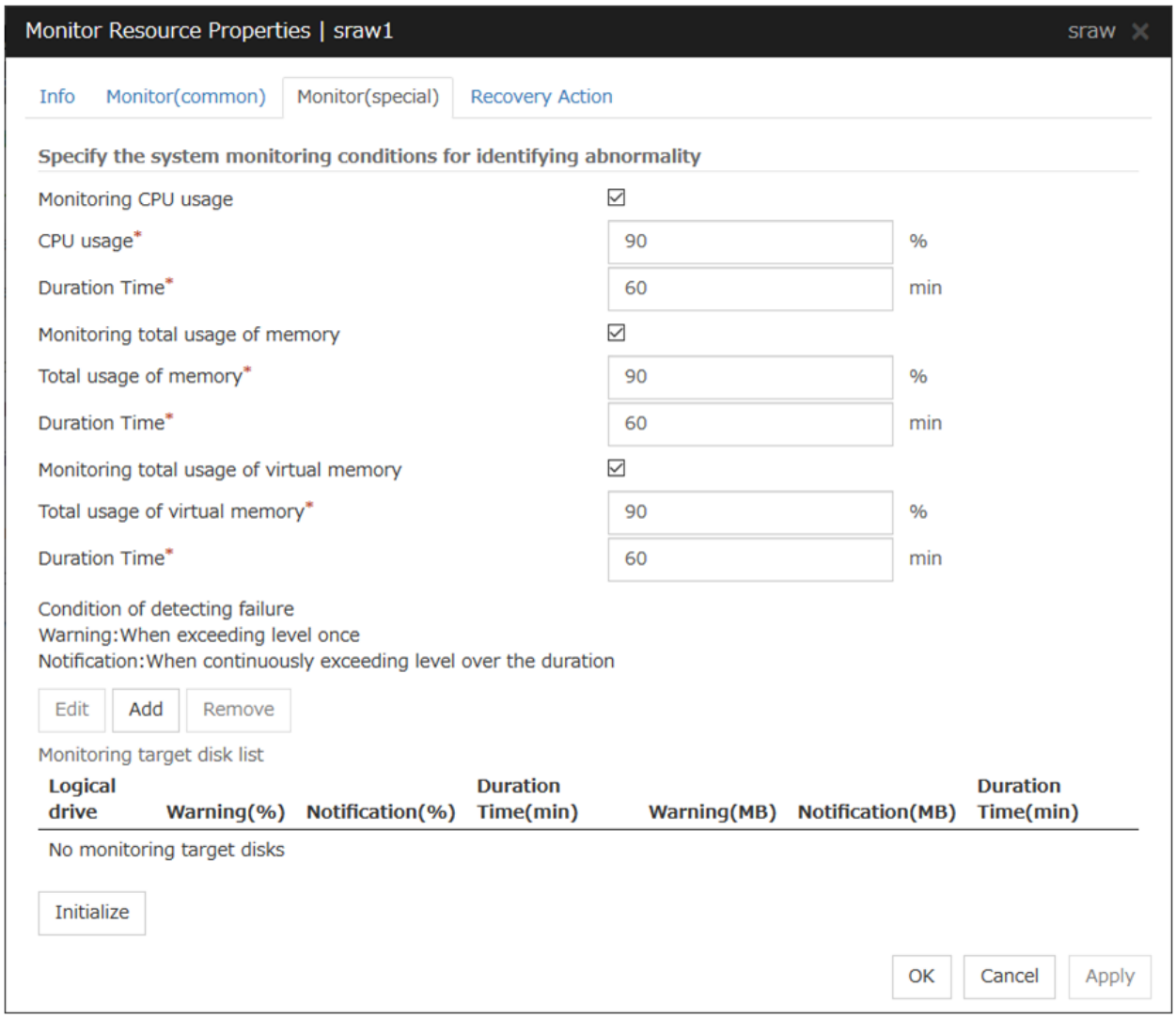


Fig. 4.73: Disk usage exceeding the upper limit of the notification level for less than a certain time, which does not lead to error detection

4.38.3 Monitor (special) tab



Monitoring CPU usage

Enables CPU usage monitoring.

- When the checkbox is selected:
  Monitoring is enabled for the CPU usage.
- When the checkbox 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 checkbox is selected:
  Monitoring is enabled for the total usage of memory.
- When the checkbox 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 checkbox is selected:
  Monitoring is enabled for the total usage of virtual memory.
- When the checkbox 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.

Add

Click this to add disks to be monitored. The **Input of watch condition** dialog box appears.

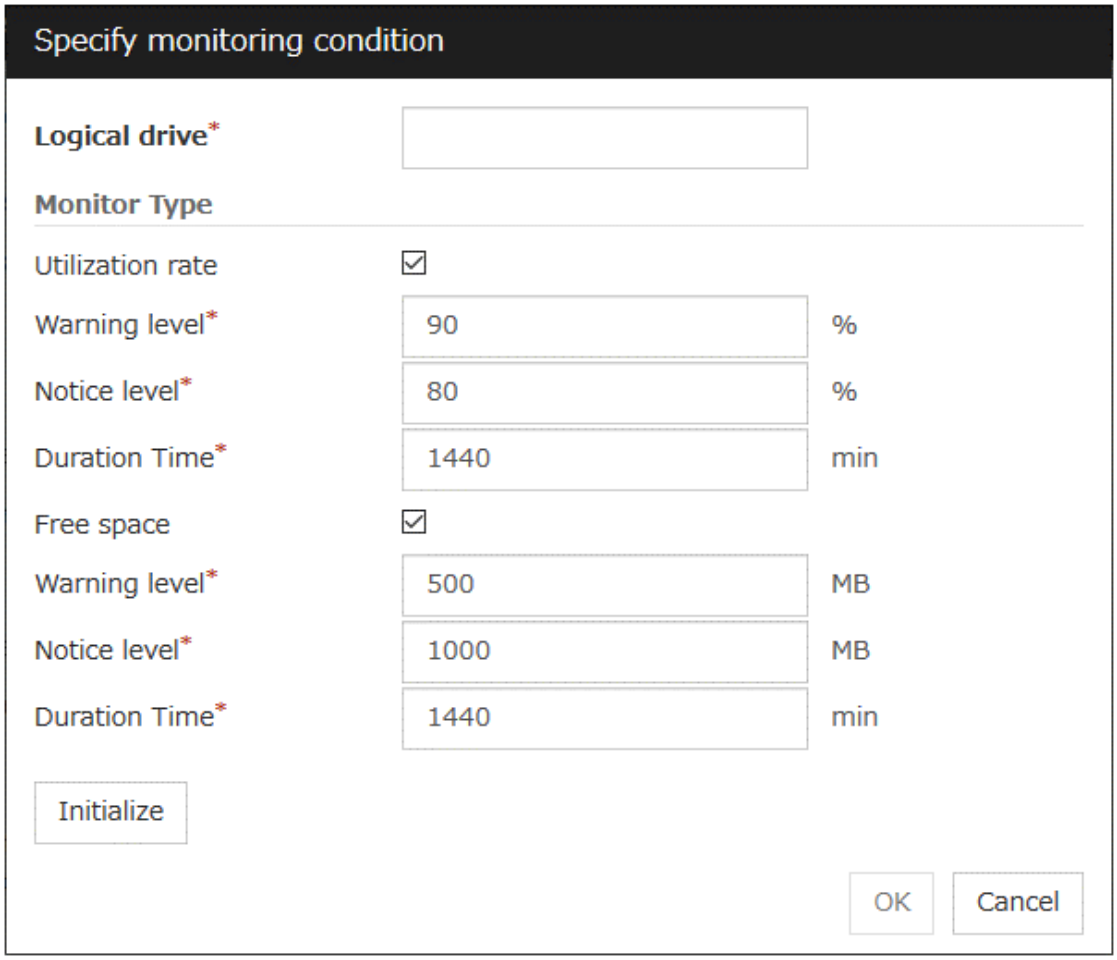
Configure the detailed monitoring conditions for error determination, according to the descriptions given in the **Input of watch condition** dialog box.

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**.



Logical drive

Set the logical drive to be monitored.

Utilization rate

Enables the monitoring of the disk usage.

- When the checkbox is selected:
  Monitoring is enabled for the disk usage.
- When the checkbox 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 checkbox is selected:
  Monitoring is enabled for the free disk space.
- When the checkbox 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.

4.39 Understanding process resource monitor resources

Process resource monitor resources monitor the resources used by processes. The 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.

4.39.1 Notes on process resource monitor resource

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 resources.

The use of the default process resource monitor resources settings is recommended.

In a case like where the system is high loaded, it may take a long time to collect statistical information and the interval of statistical information collection may be unapplied.

If date or time of OS has been changed during System Resource Agent's operation, resource monitoring may operate wrongly as follows since the timing of analyze which is normally done at 10 minute intervals may be changed at first time after changing date or time. In such case, suspend and resume cluster.

- Error is not detected after passing specified duration to detect error.
- Error is detected before passing specified duration to detect error.

Once the cluster has been suspended and resumed, the collection of information is started from that point of time.

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** is not displayed in the **Type** column on the monitor resource definition screen, select **Get License Info** and then acquire the license information.
For the license required for using the process resource monitor resources, refer to "*Monitor resources that require a license*" in "*Monitor resources* " in this chapter.

The status of the process resource monitor resource is Warning from when start of monitoring is enabled to when the monitoring processing is actually performed.

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

Use the following command to check the name of a process that is actually running and specify the name for the monitor target process name.

EXPRESSCLUSTER installation path\bin\GetProcess.vbs

When the above command is executed, GetProcess_Result.txt is output to the folder in which the command is executed. Open GetProcess_Result.txt and specify the CommandLine section of the process being displayed. If the output information includes double quotations (""), specify the section including the double quotations.

Example of output file

```
20XX/07/26 12:03:13
Caption         CommandLine
services.exe    C:\WINDOWS\system32\services.exe
svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
explorer.exe    C:\WINDOWS\Explorer.EXE
```

To monitor svchost.exe shown in the above command output information, specify C:\WINDOWS\system32\svchost -k rpcss as the monitor target process name.

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.

Too many number of registered system monitor resources and process resource monitor resources may be detected as an error and lead to outputting the following message to the alert log.

If this message is output, review the timeout setting in the **Monitor (common)** tab.

> Monitor psrw has detected an error. (99 : monitor was timeout)

4.39.2 Monitoring by process resource monitor resources

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, or number of threads) 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.

  The specified update count of the maximum value is exceeded, the increasing rate exceeds its initial value (10%), and then the default period (24 hours) elapses. This causes a memory leak to be considered to occur.

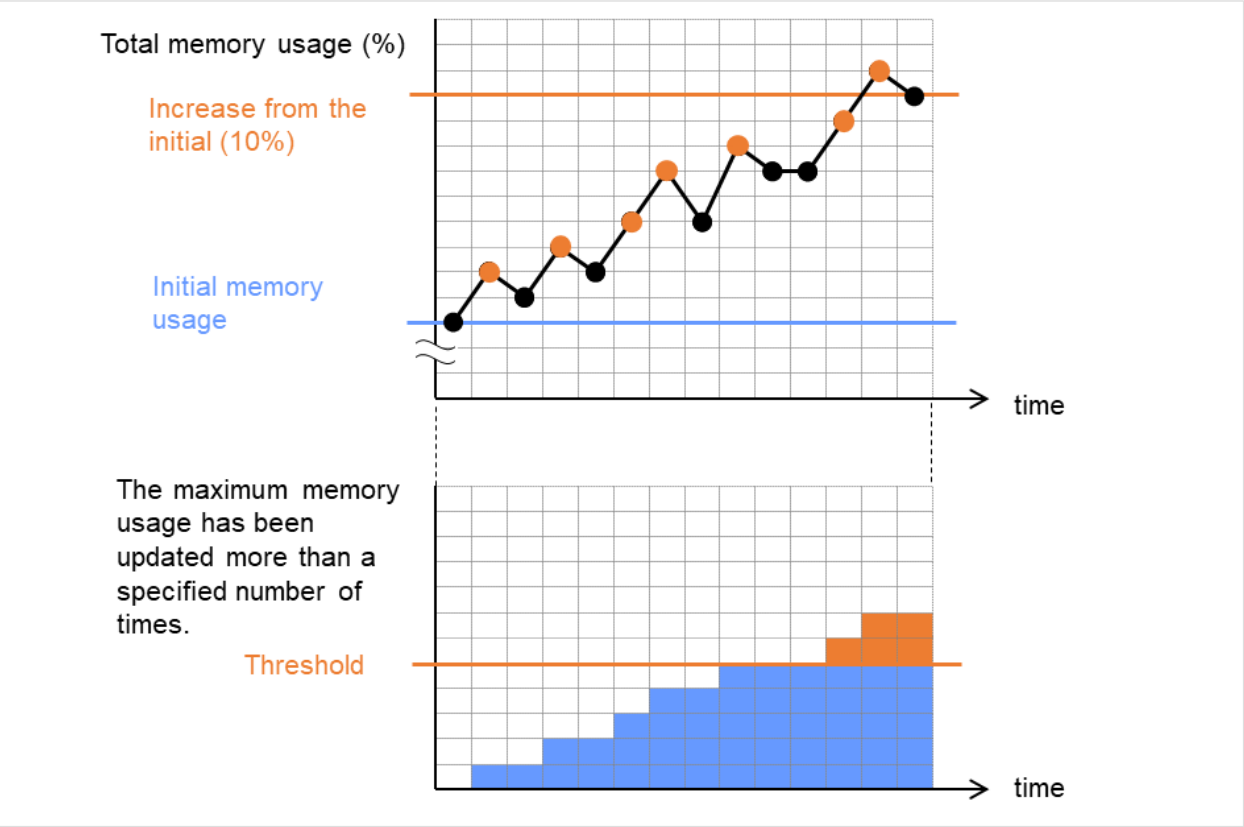


Fig. 4.74: Regarding memory usage, the maximum value is updated more times than specified, and the increasing rate exceeds its initial value (10%), which leads to error detection

- In the following example, memory usage increases and decreases, but remains within a set range.

  Since the memory usage changes below the specified level, no memory leak is considered to occur.

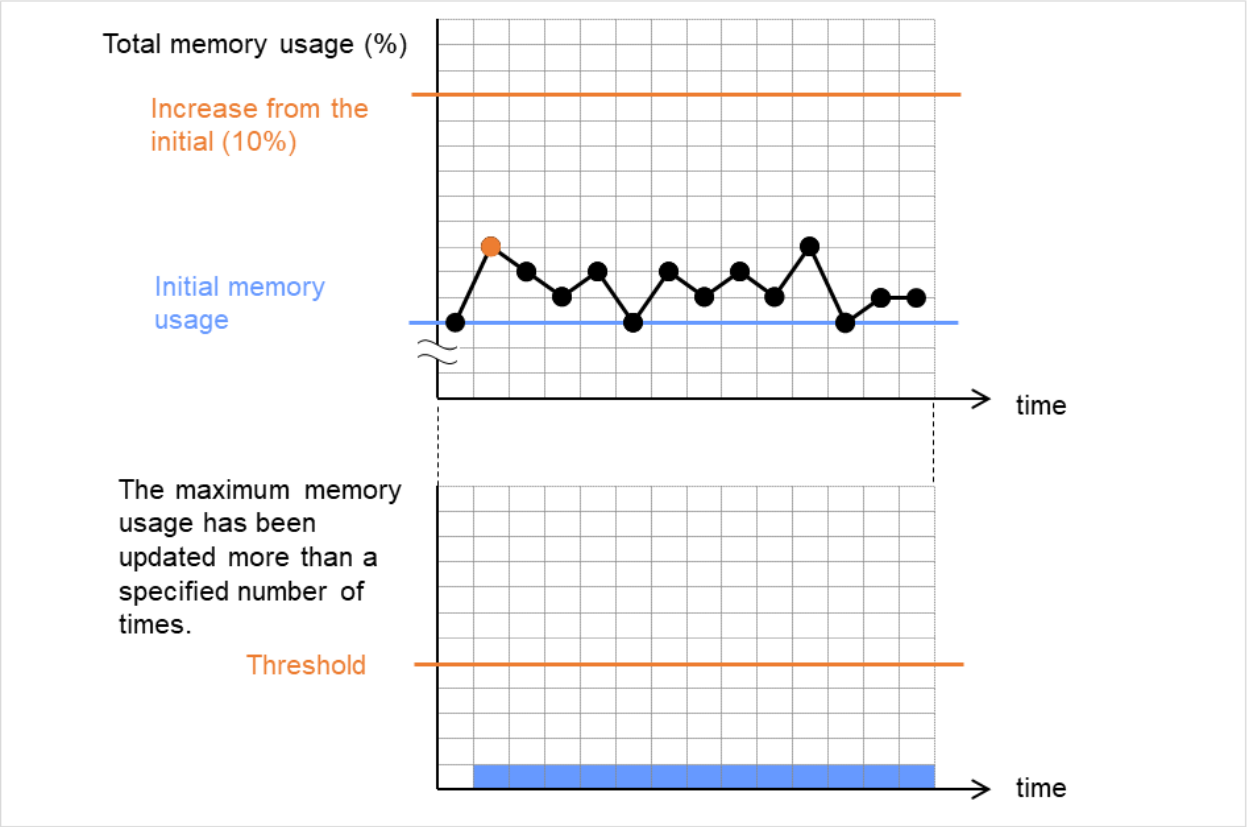
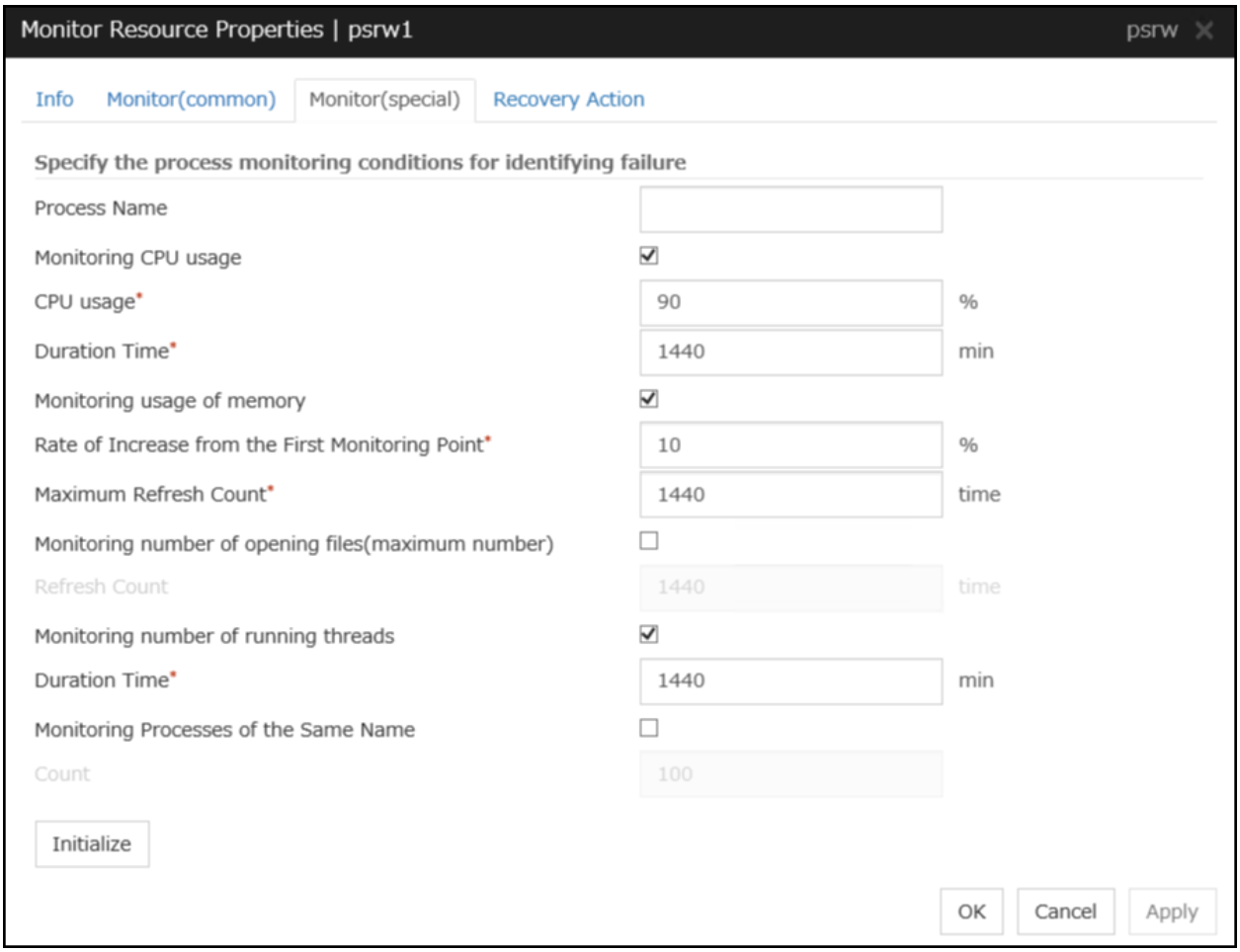


Fig. 4.75: Memory usage increasing/decreasing within a set range, which does not lead to error detection

4.39.3 Monitor (special) tab



Process Name (within 1023 bytes)

Set the name of the target process. Without setting it, all started processes are monitored.

Wild cards can be used to specify process names in the three patterns described below. Patterns other than these cannot be used.

prefix search : <character string included in process name>*

suffix search : *<character string included in process name>

partial search : *<character string included in process name>*

Monitoring CPU usage

Enables CPU usage monitoring.

- When the check box is selected:
  Monitoring is enabled for the CPU usage.
- When the checkbox 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 4320)

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 usage of memory.
- When the checkbox is not selected:
  Monitoring is disabled for the 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.

Maximum Update Count (1 to 4320)

Specify the maximum update count for the detection of a memory use amount error.
Exceeding the threshold consecutively by the specified count leads to the error detection.

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 checkbox is not selected:
  Monitoring is disabled for the number of opening files.

Refresh Count (1 to 4320)

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 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 checkbox is not selected:
  Monitoring is disabled for the number of running threads.

Duration Time (1 to 4320)

Specify the duration for detecting an error with the number of running threads.
If the processes for which the number of running threads is passed more than specified times, the detection of an error is recognized.

Monitoring Processes of the Same Name

Enables the monitoring of the processes of the same name

- When the check box is selected:
  Monitoring is enabled for the processes of the same name.

- When the checkbox 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.

4.40 Understanding user mode monitor resources

The user mode monitor resources monitor any user space stalls.

4.40.1 Monitoring by user mode monitor resources

The user mode monitor resources monitor the following:

After the start of monitoring, a user mode monitor resource starts the keepalive timer and then updates the keepalive timer at monitoring intervals. It detects an error if the timer is not updated during a set duration as a result of a user space stall.

A user mode monitor resource has a setting for extending the monitoring by creating a dummy thread. If this setting is enabled, it creates a dummy thread at monitoring intervals. If it fails to create a dummy thread, it does not update the keepalive timer.

The processing logic of the user mode monitor resources is as follows:

- Overview of processing

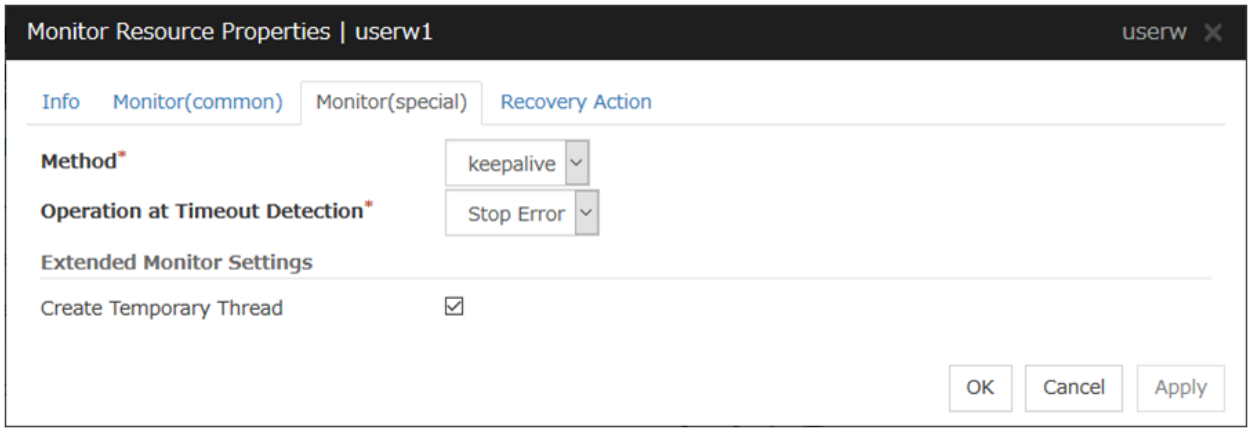
  The following steps 2 and 3 are repeated.

  1. Set the keepalive timer
  2. Create a dummy thread
  3. Update the keepalive timer

  Step 2 is a process for advanced monitor setting. If this is not set, the process is not started.

- Behavior when a timeout does not occur (steps 2 and 3,above, are processed properly)
  Recovery processing such as reset is not executed.
- Behavior when a timeout occurs (Either of steps 2 or 3, above, is stopped or delayed)
  According to the action settings, a reset or panic is generated by the clphb driver.

4.40.2 Monitor (special) tab



Method

Specify how the user space is monitored.

- keepalive

The clphb driver is used.

Operation at Timeout Detection

Specify the action to take when a timeout occurs.

- None
  No action is taken.
- HW Reset
  Reset the hardware.
- Stop Error
  Intentionally cause a stop error.

Note: A dummy failure cannot be triggered by an action when a timeout occurs.

Create Temporary Thread

Specify whether or not to create a dummy thread when monitoring.

- When the checkbox is selected (default value):
  Create a dummy thread.
- When the checkbox is not selected:
  Do not create a dummy thread.

4.41 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.

4.41.1 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 the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

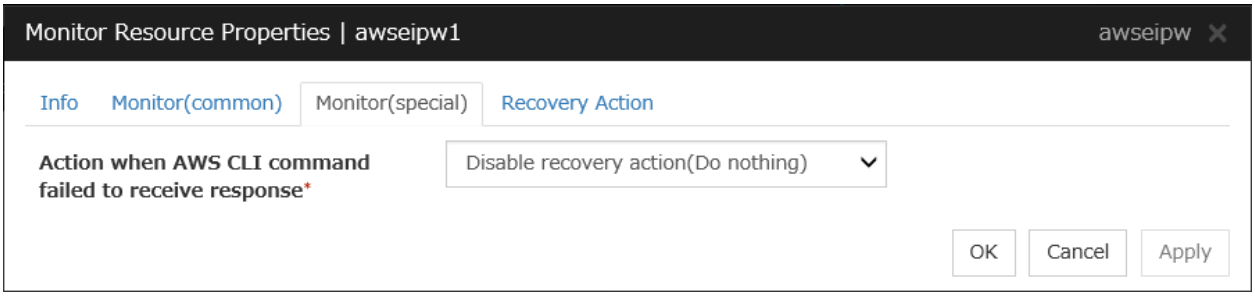
4.41.2 Applying command line options to AWS CLI run from AWS Elastic IP monitor resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.41.3 Applying environment variables to AWS CLI run from the AWS elastic ip monitor resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.41.4 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 route troubles, heavy load or delay for connecting to a region endpoint, 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).

4.42 Understanding AWS virtual ip monitor resources

For virtual IP (VIP) control, AWS Virtual IP monitor resources check the existence of VIP addresses and the soundness of VPC routing.

AWS CLI command is executed for AWS virtual ip monitor resources while monitoring to check the route table information.

4.42.1 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 the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

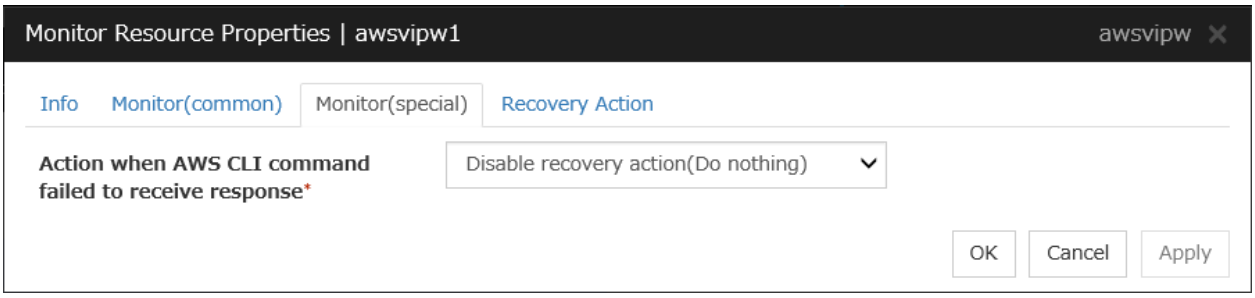
4.42.2 Applying command line options to AWS CLI run from AWS Virtual IP monitor resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.42.3 Applying environment variables to AWS CLI run from the AWS virtual ip monitor resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.42.4 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 route troubles, heavy load or delay for connecting to a region endpoint, 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.

4.43 Understanding AWS secondary ip monitor resources

AWS Secondary IP monitor resources check if secondary IP addresses exist.

4.43.1 Notes on AWS secondary ip monitor resources

- See "Setting up AWS Secondary IP resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

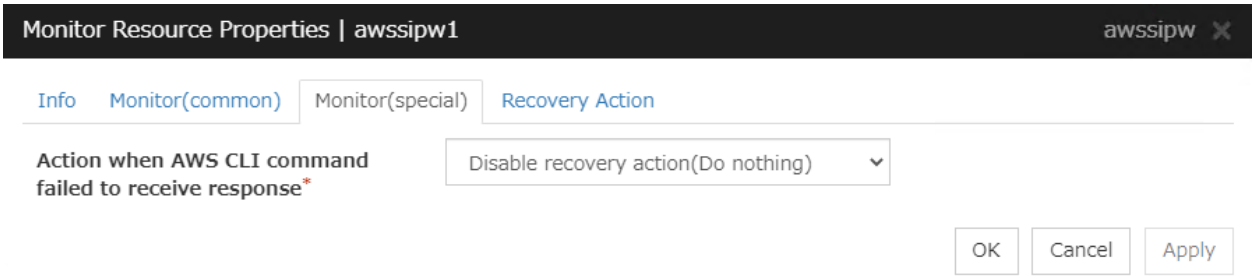
4.43.2 Applying command line options to AWS CLI run from AWS Secondary IP monitor resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.43.3 Applying environment variables to AWS CLI run from the AWS secondary ip monitor resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.43.4 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 route troubles, heavy load or delay for connecting to a region endpoint, 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.
- If no actions are to be taken, because the failure of the AWS CLI command does not mean an error in the monitoring target, it is recommended to select **Disable recovery action(Do nothing)**. Even in this case, you can detect an error in failing to check the health of a registered IP address.

4.44 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 12.20, only available represents the normal status (other results are categorized in error status).

4.44.1 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 the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

4.44.2 Applying command line options to AWS CLI run from AWS AZ monitor resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.44.3 Applying environment variables to AWS CLI run from the AWS AZ monitor resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.44.4 Monitor (special) tab

Availability Zone (Within 45 bytes)

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 route troubles, heavy load or delay for connecting to a region endpoint, 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.

4.45 Understanding AWS DNS monitor resources

AWS DNS monitor resources check the health of an IP address registered by using the AWS CLI command.

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).

4.45.1 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 the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- For information on the settings of IAM, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "IAM settings in the AWS environment".

4.45.2 Applying command line options to AWS CLI run from AWS DNS monitor resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.45.3 Applying environment variables to AWS CLI run from the AWS DNS monitor resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

4.45.4 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 route troubles, heavy load or delay for connecting to a region endpoint, 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

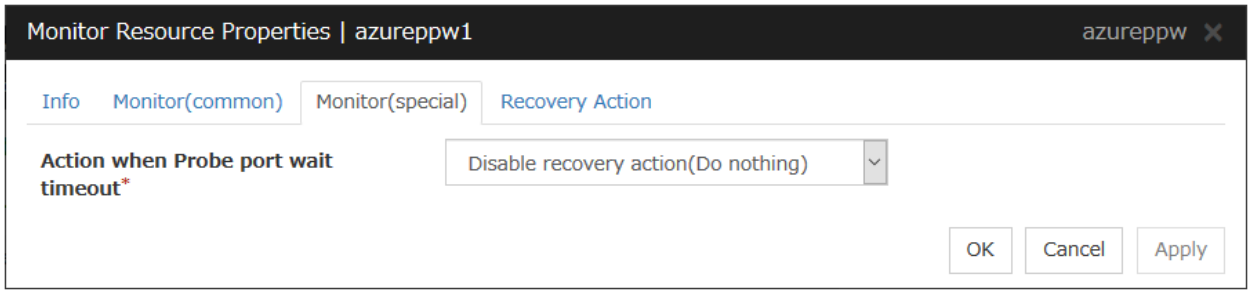
4.46 Understanding Azure probe port monitor resources

Azure probe port monitor resources perform alive monitoring on a probe port control process that starts when Azure probe port resources 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.

4.46.1 Notes on Azure probe port monitor resources

- Azure probe port 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 "Setting up Azure probe port resources"in "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.46.2 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.

4.47 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 probe port resources are not active.

4.47.1 Notes 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" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".
- See "Setting up Azure load balance monitor resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.47.2 Monitor (special) tab

Target Resource

Set Resource to be monitored.

4.48 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.

4.48.1 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 DNS resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.48.2 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.

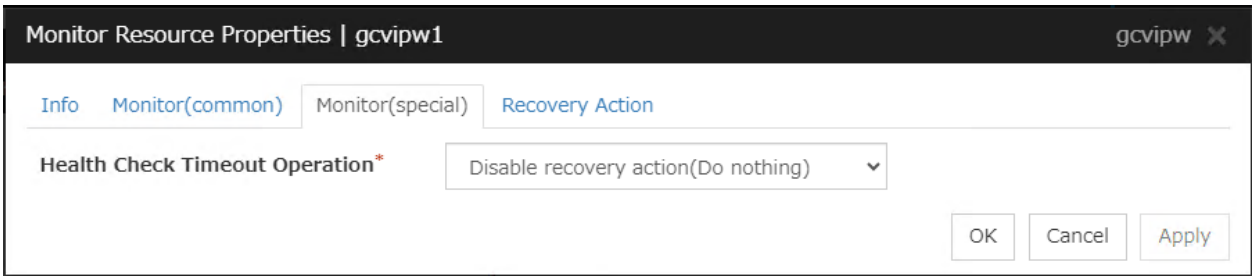
4.49 Understanding Google Cloud Virtual IP monitor resources

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 **Health Check Timeout Operation** settings.

4.49.1 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 "Setting up Google Cloud virtual IP resources" on "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.49.2 Monitor (special) tab



Health Check Timeout Operation

Specifies actions when timeout of health check wait time occurs in Google Cloud Virtual IP resources

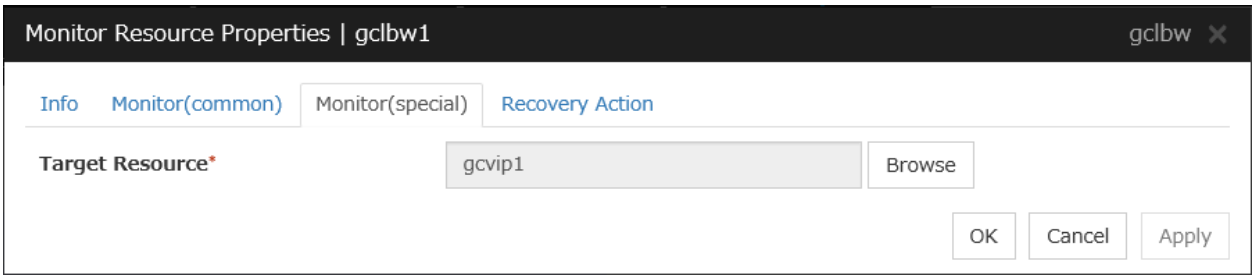
4.50 Understanding Google Cloud load balance monitor resources

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.

4.50.1 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 the cluster 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 the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.50.2 Monitor (special) tab



Target Resource

Specifies a name of the target Google Cloud Virtual IP resource.

4.51 Understanding Google Cloud DNS monitor resources

Google Cloud DNS monitor resources checks that Google Cloud DNS has the A records and record sets controlled by Google Cloud DNS resources specified as target resources for monitoring at activation.

4.51.1 Notes on Google Cloud DNS monitor resources

- See "Setting up Google Cloud DNS resources" in "Notes when creating EXPRESSCLUSTER configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.51.2 Monitor (special) tab

This tab is not available for Google Cloud DNS monitor resources.

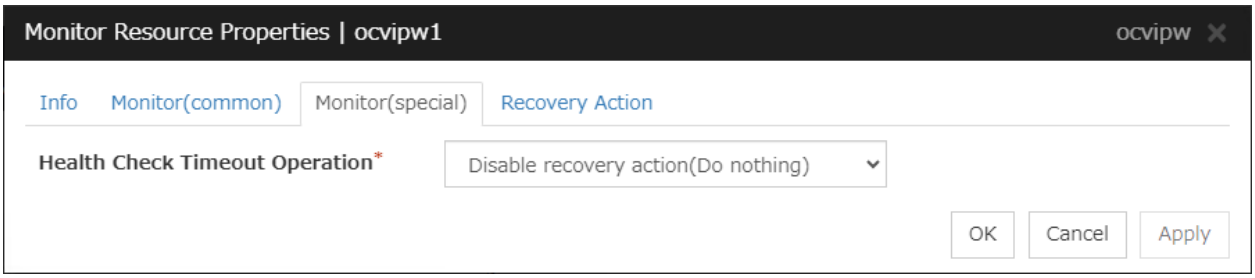
4.52 Understanding Oracle Cloud Virtual IP monitor resources

Oracle 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 **Health Check Timeout Operation** settings.

4.52.1 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 "Setting up Oracle Cloud virtual IP resources" on "Notes when creating the cluster configuration data" in "Notes and Restrictions" of the "Getting Started Guide".

4.52.2 Monitor (special) tab



Health Check Timeout Operation

Specifies actions when timeout of health check wait time occurs in Oracle Cloud Virtual IP resources.

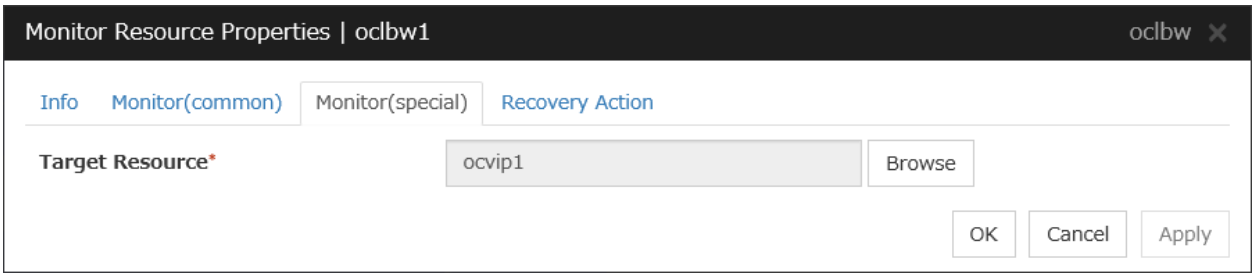
4.53 Understanding Oracle Cloud load balance monitor resources

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.

4.53.1 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 the cluster 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 the cluster 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 Oracle Cloud Virtual IP resource.

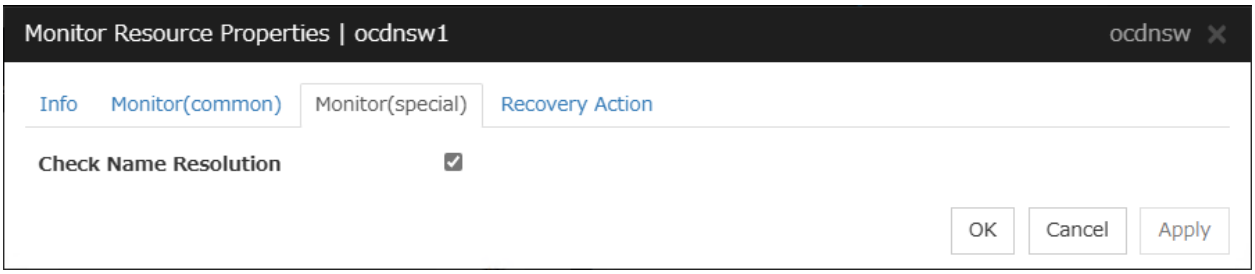
4.54 Understanding Oracle Cloud DNS monitor resources

- Oracle Cloud DNS monitor resources checks that Oracle Cloud DNS has the A records and record sets controlled by Oracle Cloud DNS resources specified as target resources for monitoring at activation.
- The record sets of Oracle Cloud DNS in a region to which servers (without the failover group started) belong are registered or updated at intervals specified in **Interval**, in the following case: For a cluster configured in a multi-region environment, the target resource is set with **All regions to which the cluster servers belong** specified in **How far you manage a resource record in a multi-region environment**.

4.54.1 Notes on Oracle Cloud DNS monitor resources

- Oracle Cloud DNS monitor resources are automatically created when Oracle Cloud DNS resources are added. A single Oracle Cloud DNS monitor resource is automatically created for a single Azure DNS resource.
- Using a public DNS zone charges you a fee of zone registration and querying. The charging occurs at intervals specified in **Interval** in the following case: With **Check Name Resolution** enabled or for a cluster configured in a multi-region environment, the target resource is set with **All regions to which the cluster servers belong** specified in **How far you manage a resource record in a multi-region environment**.
- For a cluster configured in a multi-region environment, resolving a registered IP address or DNS name may fail from a region to which the server (without its failover group started) belongs.
- See "Setting up Oracle Cloud DNS resources" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- See "CLI setting in the OCI environment" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".
- See "Policy setting in the OCI environment" in " Before installing EXPRESSCLUSTER" in "Notes and Restrictions" in the "Getting Started Guide".

4.54.2 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.

CHAPTER

FIVE

HEARTBEAT RESOURCES

This chapter provides detailed information on heartbeat resources.

This chapter covers:

5.1 Heartbeat resources

Servers in a cluster monitor if other servers in the cluster are activated. For this monitoring, heartbeat resources are used.

1. kernel mode LAN heartbeat (primary interconnect)

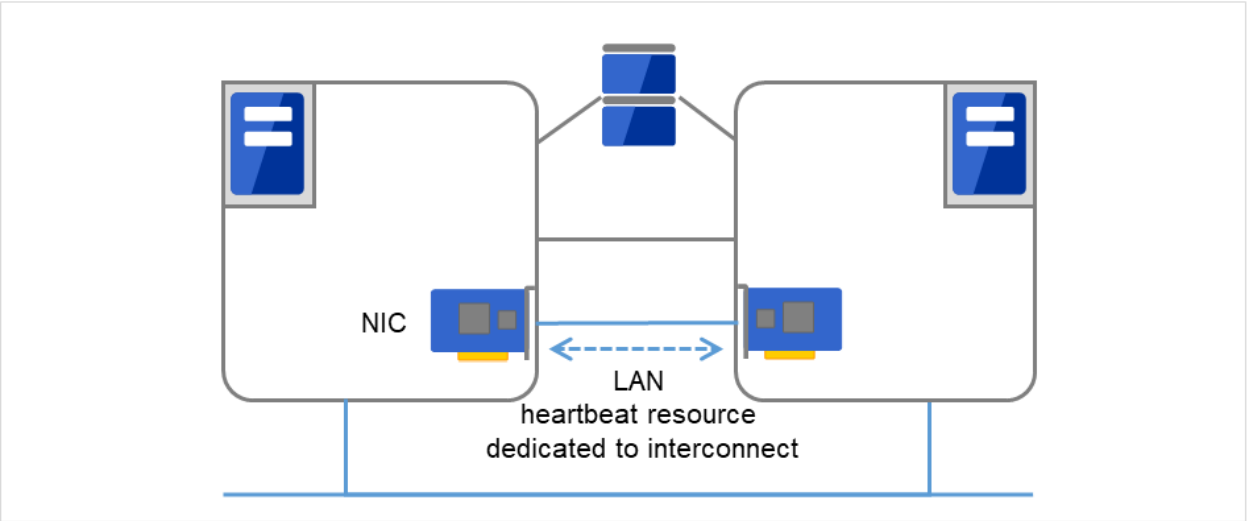


Fig. 5.1: kernel mode LAN heartbeat (primary interconnect)

2. kernel mode LAN heartbeat (secondary interconnect)

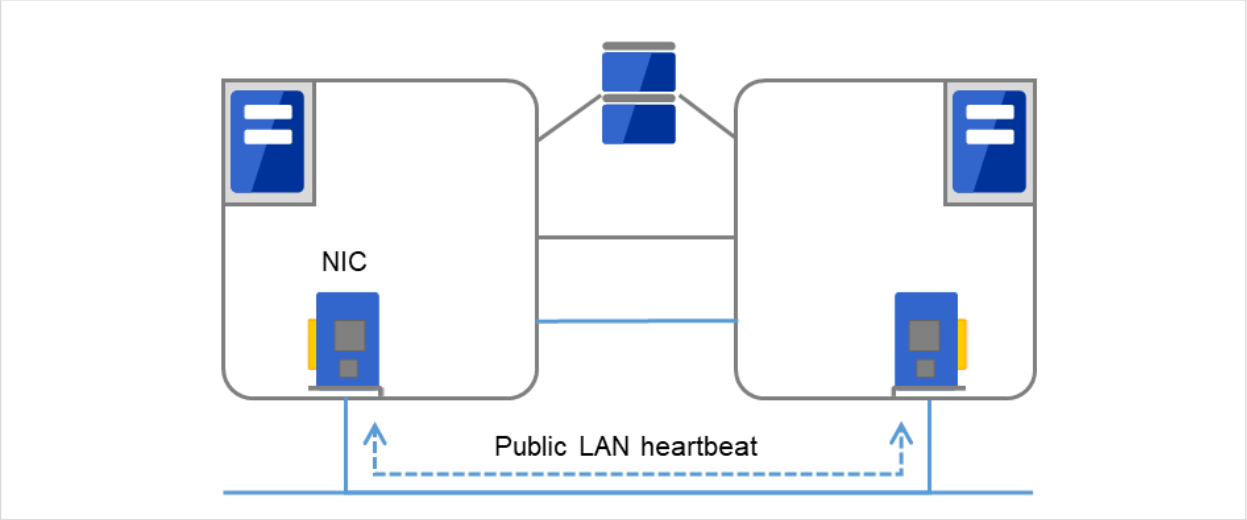


Fig. 5.2: kernel mode LAN heartbeat (secondary interconnect)

3. Witness heartbeat

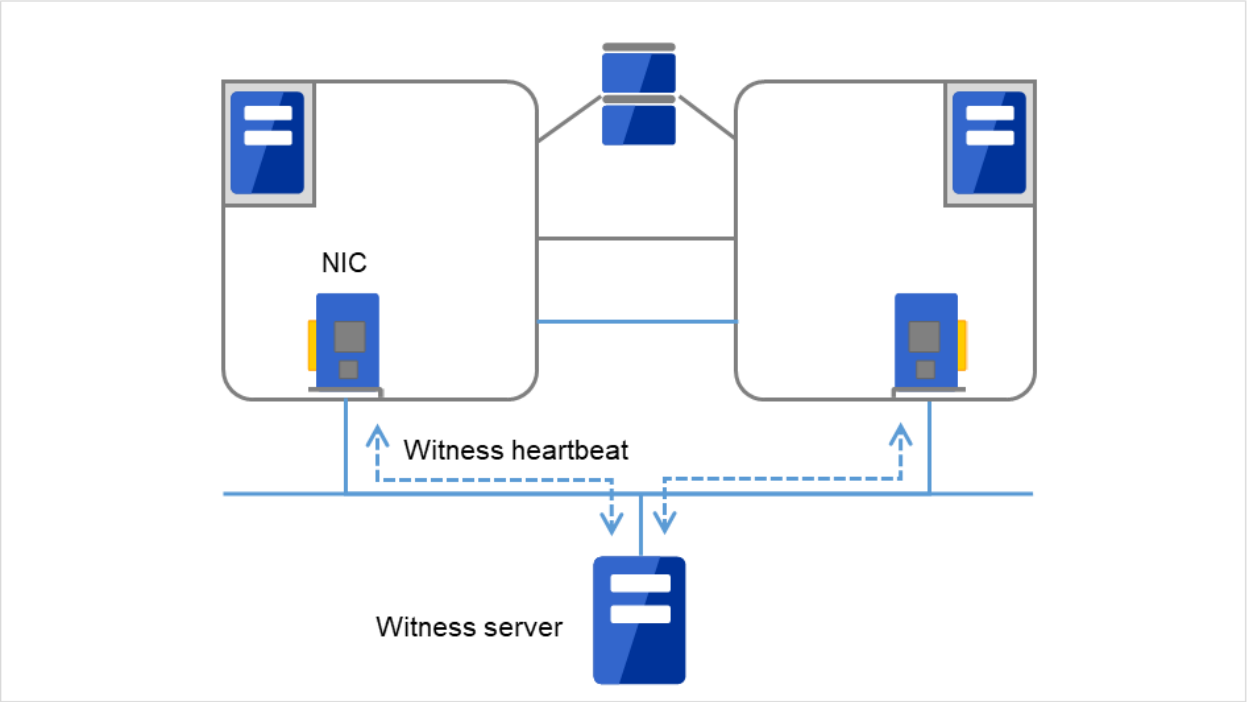


Fig. 5.3: Witness heartbeat

Type of Heartbeat resource	Abbreviation	Functional overview
Kernel mode LAN heartbeat resource (1), (2)	lankhb	A kernel mode module uses a LAN to monitor if servers are activated.
Witness heartbeat resource (3)	witnesshb	A module uses the Witness server to monitor whether or not servers are active.

- For an interconnect with the highest priority, configure kernel mode LAN heartbeat resources which can be exchanged between all servers.
- Configuring at least two kernel mode LAN heartbeat resources is recommended unless it is difficult to add a network to an environment such as the cloud or a remote cluster.
- It is recommended to register both an interconnect-dedicated LAN and a public LAN as LAN heartbeat resources.

5.2 Understanding kernel mode LAN heartbeat resources

5.2.1 Kernel mode LAN heartbeat resources

Kernel mode LAN heartbeat resources achieve heartbeat functions using the kernel mode driver module. Kernel mode LAN heartbeat resources are less burdened and help to reduce misidentification of disconnection of interconnect by using the kernel mode driver.

5.2.2 Settings of the kernel mode LAN heartbeat resources

For details on settings of the kernel mode LAN heartbeat resources, see "*Interconnect tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

5.2.3 Notes on the 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.

5.3 Understanding Witness heartbeat resources

5.3.1 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 "8. *Information on other settings*".

The Witness heartbeat resources allow to regularly check the server alive information which the Witness server retains. 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.

5.3.2 Notes on the Witness heartbeat resources

- In the communication with the Witness server, NIC and a source address are selected according to the OS settings.

CHAPTER

SIX

DETAILS ON NETWORK PARTITION RESOLUTION RESOURCES

This chapter provides detailed information on network partition resolution resources.

This chapter covers:

6.1 Network partitions

Network partitioning, or 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 "Status," 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 "Status" 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 Status, the selected "action at NP occurrence"[1] is executed because protecting data has higher priority over continuity of the operation.

6.1.1 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 four types of network partition resolution resources are provided.

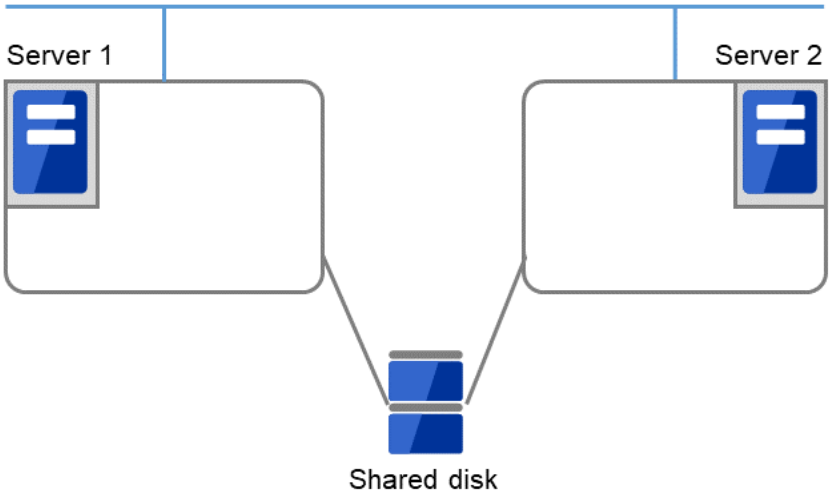


Fig. 6.1: Servers connected via LAN, and a shared disk

Network partition resolution resources	Abbreviation	Function Overview
DISK network partition resolution resource (DISK method)	disknp	A network partition is solved by using a dedicated disk partition on the shared disk.

Continued on next page

[1] The action can be changed in the config mode Cluster WebUI by selecting Cluster Properties->NP Resolution tab->Tuning button->Network Partition Resolution Tuning Properties window->Action at NP Occurrence.

Table 6.1 – continued from previous page

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.
Majority network partition resolution resource (Majority method)	majonp	A network partition is solved by the number of servers that can make connection among three or more servers.

A network partition resolution resource that can be selected is different depending on a server configuration in a cluster. Select one of the following network partition resolution methods:

Cluster server configuration	Network partition resolution method (Listed in the order of our recommendation)
Mirror disk resource exists	Number of servers: 2 • PING method and DISK method • DISK method Number of servers: 3 or more servers • PING method and DISK method • DISK method • Majority method
Mirror disk resource exists but disk resource does not exist	Number of servers: 2 • HTTP method • PING method • No network partition resolution Number of servers: 3 or more servers • HTTP method • PING method • Majority method • No network partition resolution
Neither disk resource nor mirror disk resource does not exist	Number of servers: 2 • HTTP method • PING method • No network partition resolution Number of servers: 3 or more servers • HTTP method • PING method • Majority method • No network partition resolution

- For example, if both server1 and server2 use disk resource and mirror disk resource, the combination of DISK method and PING method, or a DISK method can be selected as a network partition resolution resource.

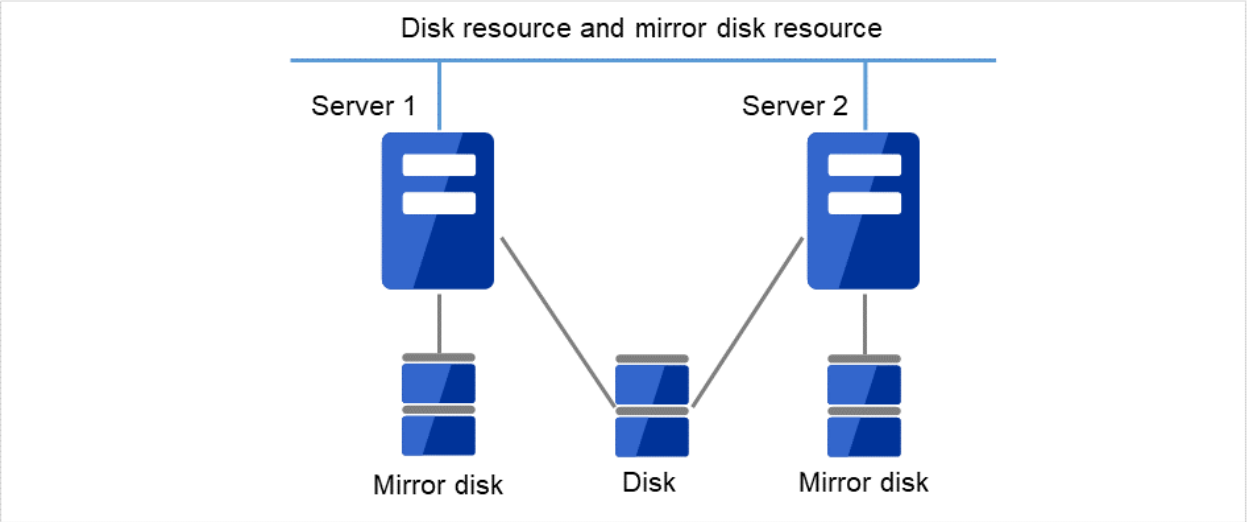


Fig. 6.2: Both servers using a disk resource and a mirror disk resource

- When servers that can be started by disk resource and mirror disk resource differ, the network partition resolution resource needs to be set in each server. For example, if server1 and server2 use a shared disk, and server2 and server3 use a mirror disk, the combination of COM method and DISK method, PING method and DISK method, DISK method can be selected as network partition resolution resource for server1 and server2. PING method or COM method can be selected for server2 and server3.

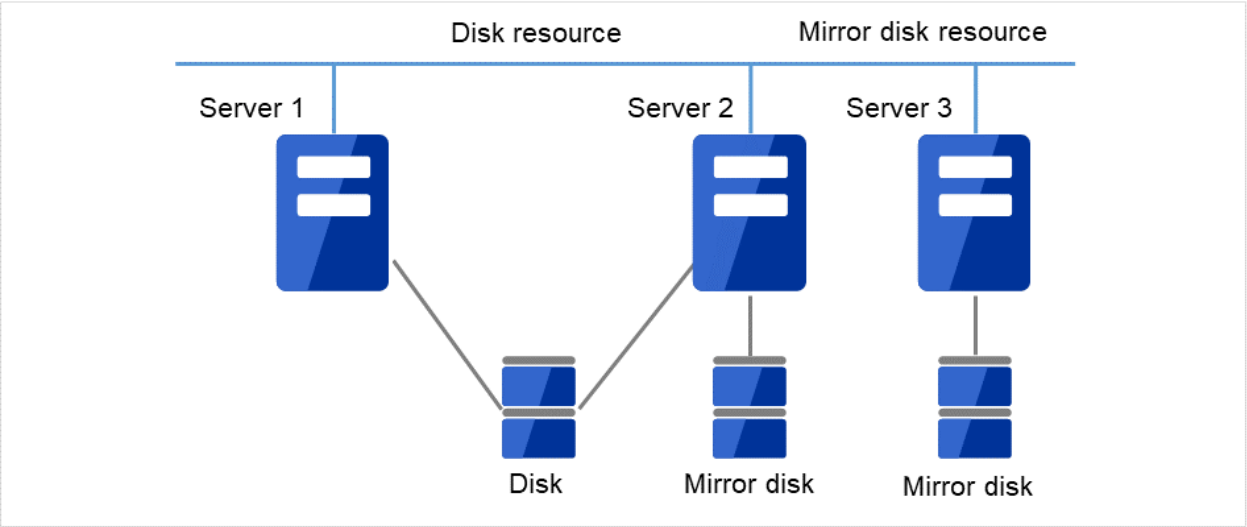


Fig. 6.3: A server enable to be activated by a disk resource and a server enabled to be activated by a mirror disk resource are different

- A combination of two or more types of network partition resolution resources can be registered. When two or more types of resources are registered, they are used for solving an NP in the following order:
  1. PING method and DISK method
  2. HTTP method
  3. PING method
  4. DISK method

5. Majority method

6.1.2 Network partition resolution during cluster service start

When cluster services are started but all heartbeat routes to other servers are found cut off, resolving the network partitions takes place. In this case, the cluster services are stopped on the servers with the detected network partitions. Check the statuses of the heartbeat routes, then manually start the cluster services.

6.2 Understanding network partition resolution by DISK method

6.2.1 Settings of the DISK network partition resolution resources

The following settings are required to use DISK network partition resolution resource:

- Allocate a dedicated disk partition for disk heartbeat resource on the shared disk. It is not necessary to format the partition.
- Allocate driver letters for the disk partition on the shared disk. The drive letters must be the same for all the servers.

DISK network partition resolution resources cause the "action at NP occurrence" in servers that cannot communicate with the first priority server or the cluster service to stop when a network partition is detected.

(1) Two servers, which share a disk, are connected by two LANs.

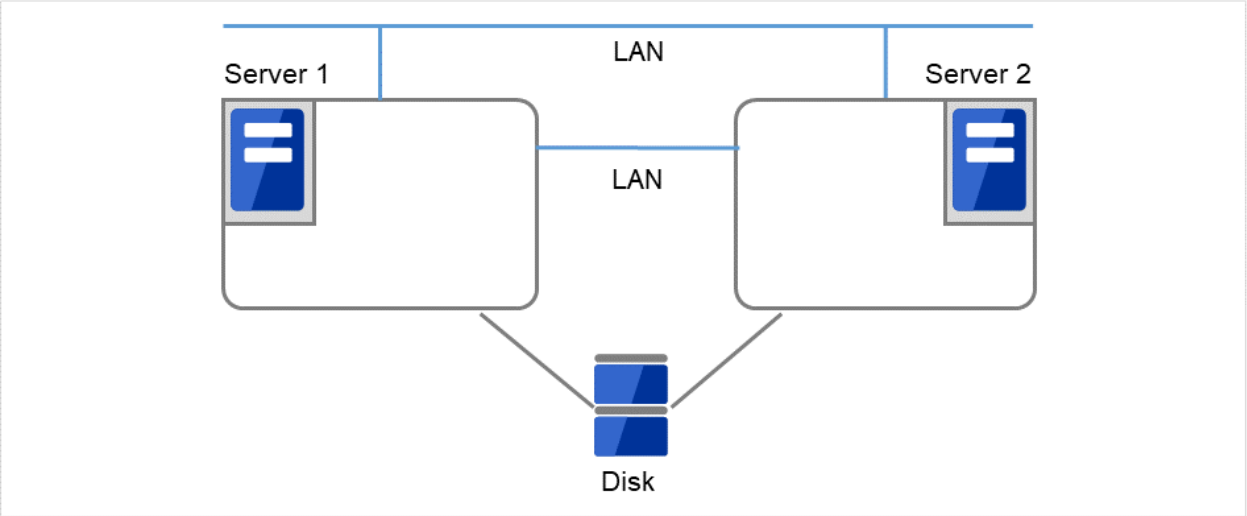


Fig. 6.4: DISK network partition resolution resources (1)

(2) If all the networks are disconnected, the DISK network partition resolution resources cause one server to shut down. This prevents a split brain syndrome in the same group of both the active and standby servers.

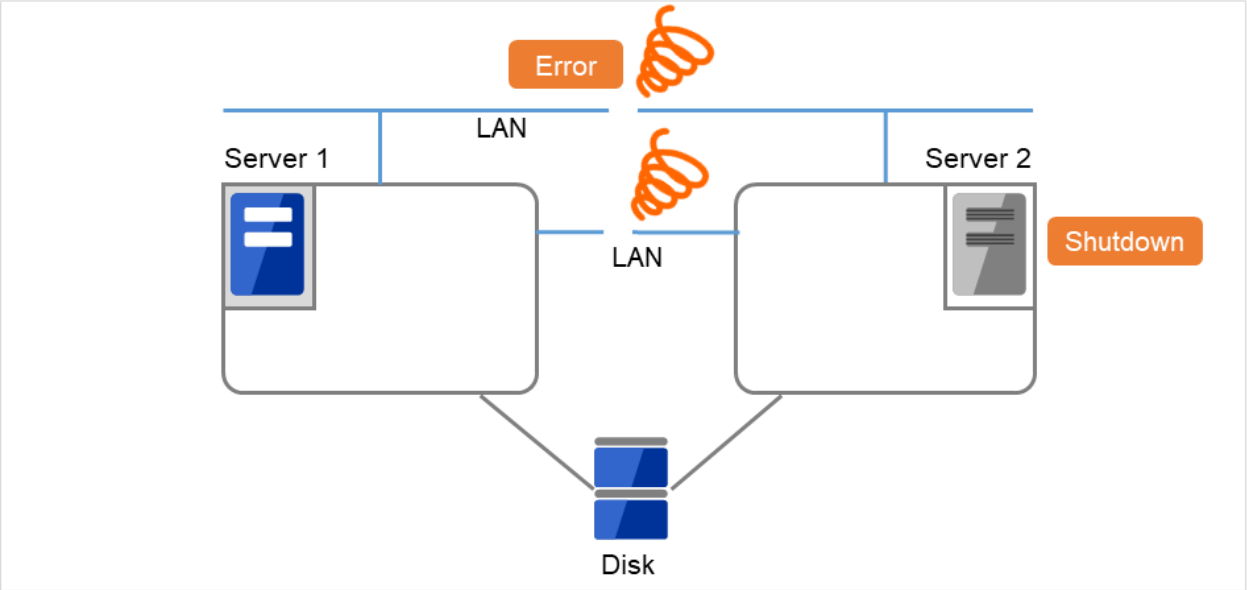


Fig. 6.5: DISK network partition resolution resources (2)

When a cluster is configured with two or more servers, DISK network partition resolution resources can be used as described below. DISK network partition resolution resources can be set to be used by servers that use the shared disk in a cluster.

For more information, refer to "*Fencing tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

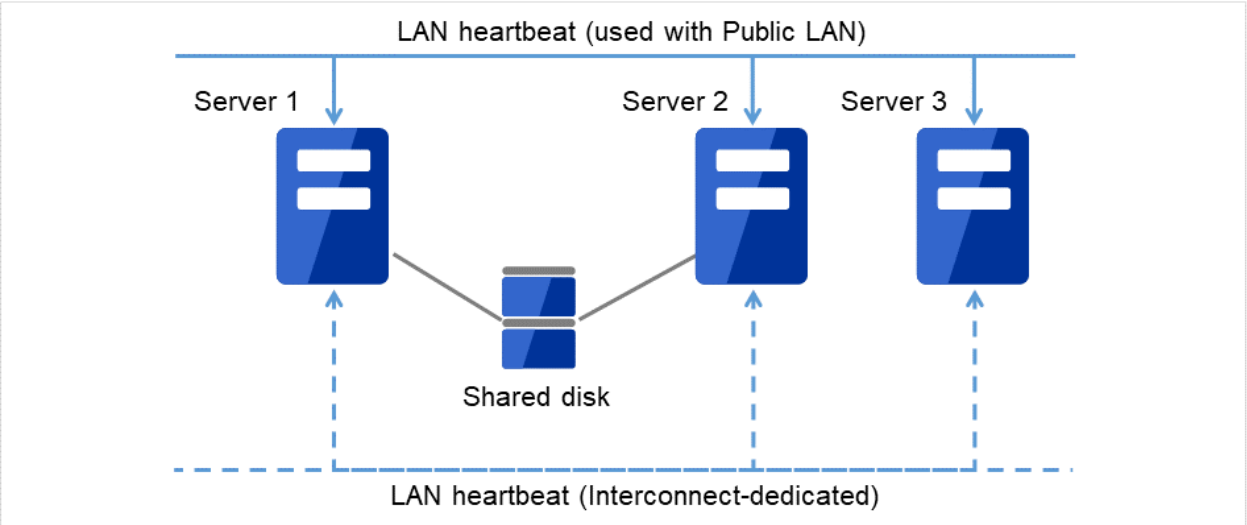


Fig. 6.6: A cluster configured with two or more servers

6.2.2 DISK network partition resolution resources

- It is recommended to use DISK network partition resolution resources when a shared disk is used.
- Configure DISK network partition resolution resources considering burden on the disk because they regularly perform read/write operations to the disk.
- For disk heartbeat partitions to be used in DISK network partition resolution resources, use partitions that are configured to be managed in cluster in the HBA settings.
- If a failure has occurred on all network channels while all disk heartbeat partitions can be accessed normally, a network partition is detected. Then failover takes place in the master server and a server that can communicate with the master server. The selected "action at NP occurrence" takes place in the rest of servers.
- If the heartbeat is lost while some disk heartbeat partitions cannot be accessed normally, the network partitions cannot be solved and a failover cannot be performed. In this case, the selected "action at NP occurrence" is performed for those servers for which the disk heartbeat partition cannot be accessed normally.
- When the I/O time to the shared disk takes longer than I/O Wait Time of DiskNP resource configured in cluster properties, a failover may not be performed due to timeout of solving a network partition.
- Solving a network partition with this method takes longer compared to other methods because delay in disk I/O needs to be taken into account. The time required to solve a network partition takes twice as long as the longer time of the heartbeat timeout and Disk I/O Wait Time configured in cluster properties.
- When DISK network partition resolution resources are used, all servers on which a cluster is started periodically access the dedicated disk partition on the shared disk. The servers on which the cluster is stopped or suspended do not access the dedicated partition.

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 "Status," and the selected "action at NP occurrence" takes place.

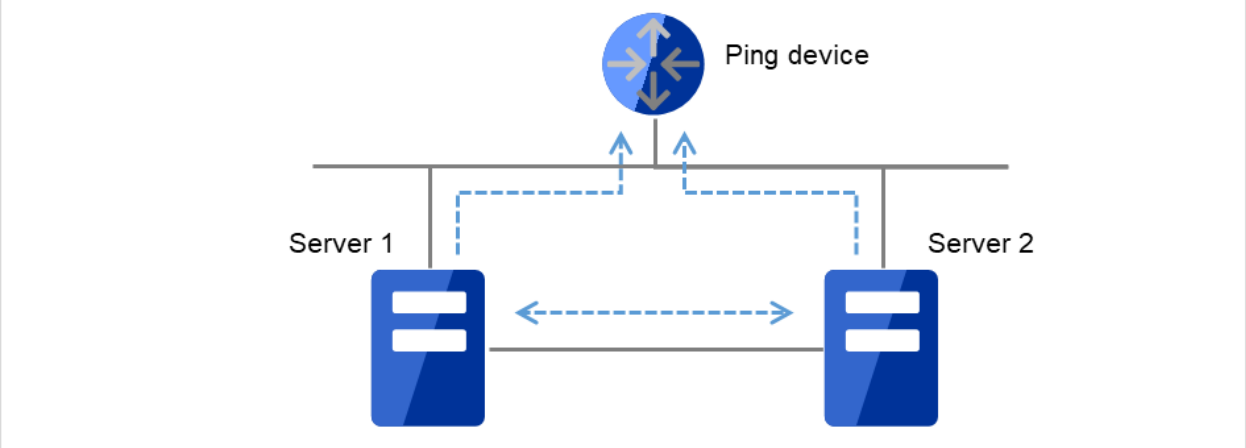


Fig. 6.7: PING network partition resolution resources (1)

When the heartbeat from the other server is found lost and the ping device does not respond to the ping command, the server is shut down. This prevents a split brain syndrome in the same group of both the active and standby servers.

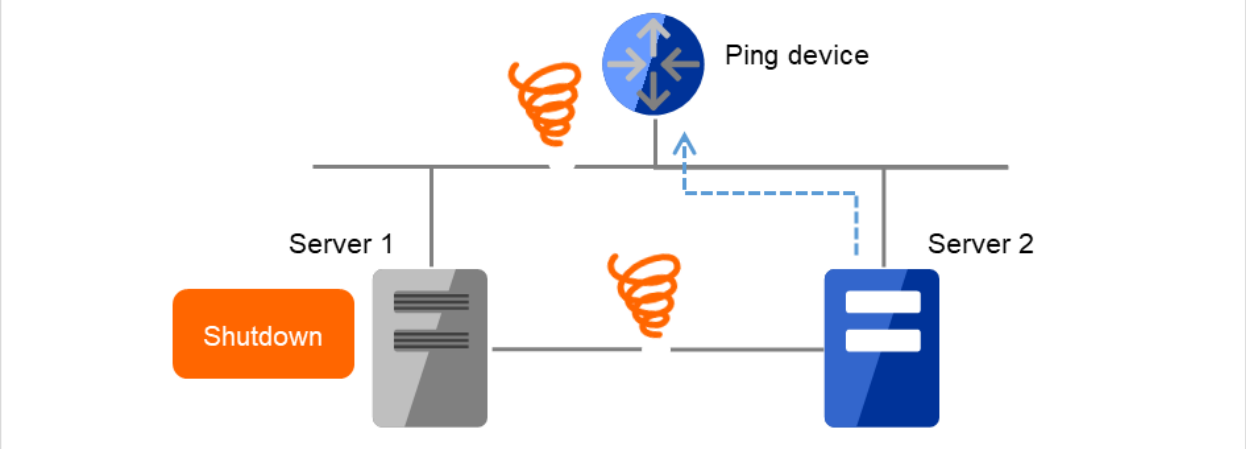


Fig. 6.8: PING network partition resolution resources (2)

For more information, refer to "*Fencing tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

6.3.2 Notes on PING network partition resolution resource

To use the ping network partition resolution resource, specify an address that allows transmission and reception via the interconnect LAN registered in the configuration data.

When the status where no response is returned to the ping command on all servers continues before the heartbeat is lost, which is caused by a failure in the ping device, if a network partition occurs under such situation, "action at NP occurrence" is not executed.

When shared disk is used, it is recommended to use not only PING Network Partition Resolution resource, but also DISK Network Partition Resolution resource at the same time.

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.

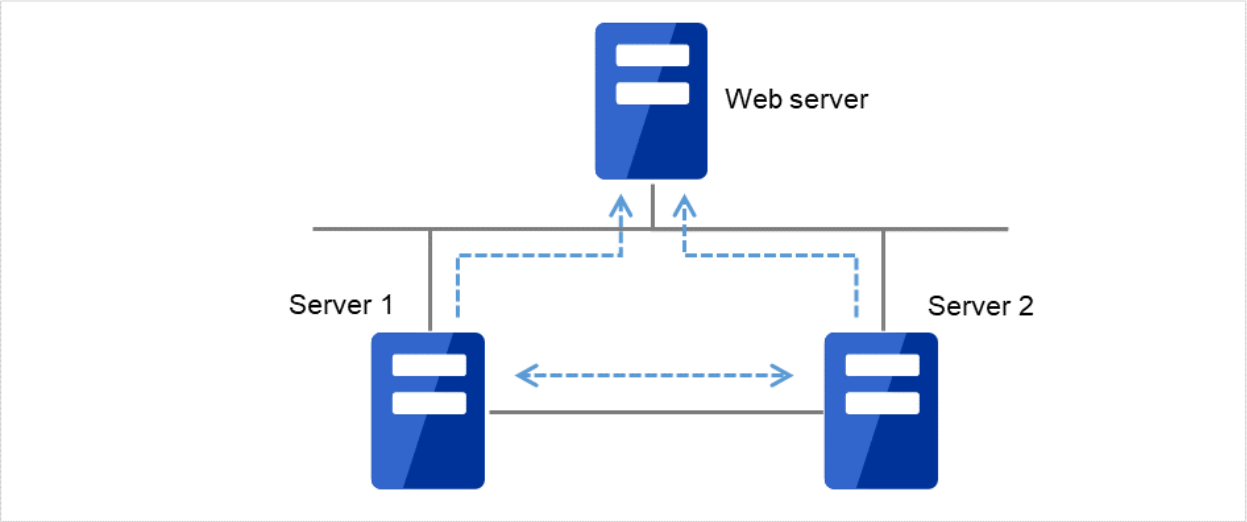


Fig. 6.9: HTTP network partition resolution resources (1)

When the heartbeat from the other server is found lost and there is no response from the Web server, the server is shut down. This prevents a split brain syndrome in the same group of both the active and standby servers.

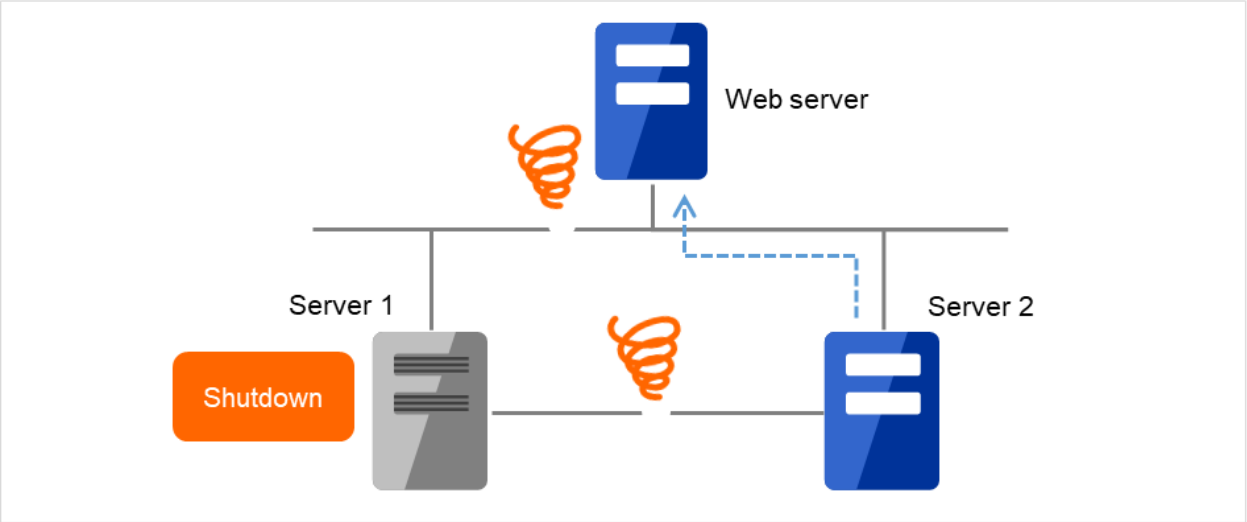


Fig. 6.10: HTTP network partition resolution resources (2)

For more information, refer to "*Fencing tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

6.4.2 Notes on HTTP network partition resolution resource

- To use the HTTP network partition resolution resource, specify an address that allows transmission and reception via the interconnect LAN registered in the configuration data.
- Specify a device which responds to HTTP HEAD requests.
  Responding to a HEAD request with a status code 200 or 301, the target is considered normal.
  Responding with a status code other than 200 and 301 or not responding, the target is considered abnormal.
- In the communication with Web server, NIC and a source address are selected according to the OS settings.

6.5 Understanding network partition resolution by majority method

6.5.1 Settings of the majority network partition resolution resources

This method prevents data corruption caused by "Split Brain Syndrome" by executes the selected "action at NP occurrence" in the server that can no longer communicate with the majority of the servers in the entire cluster because of network failure or stopping the cluster service.

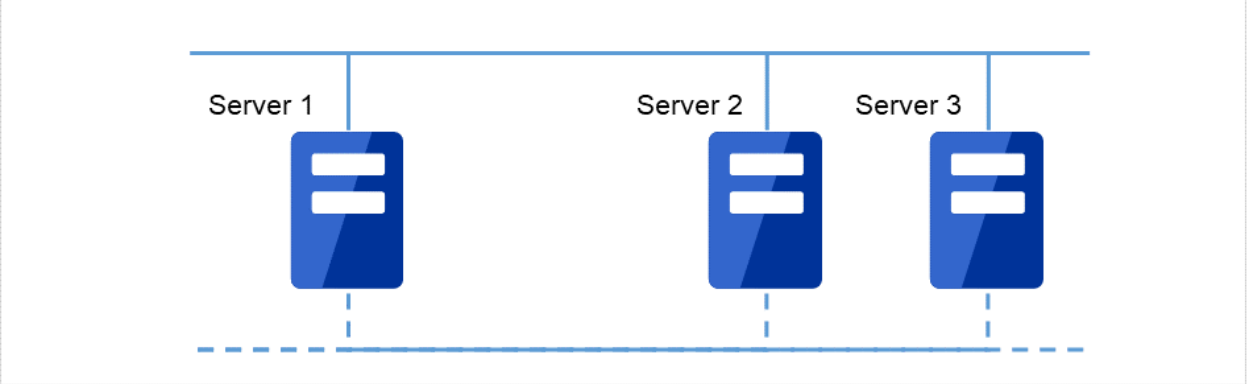


Fig. 6.11: Majority network partition resolution resources (1)

When the heartbeat from the other server is found lost and there is no response from the Web server, the server is shut down. This prevents a split brain syndrome in the same group of both the active and standby servers.

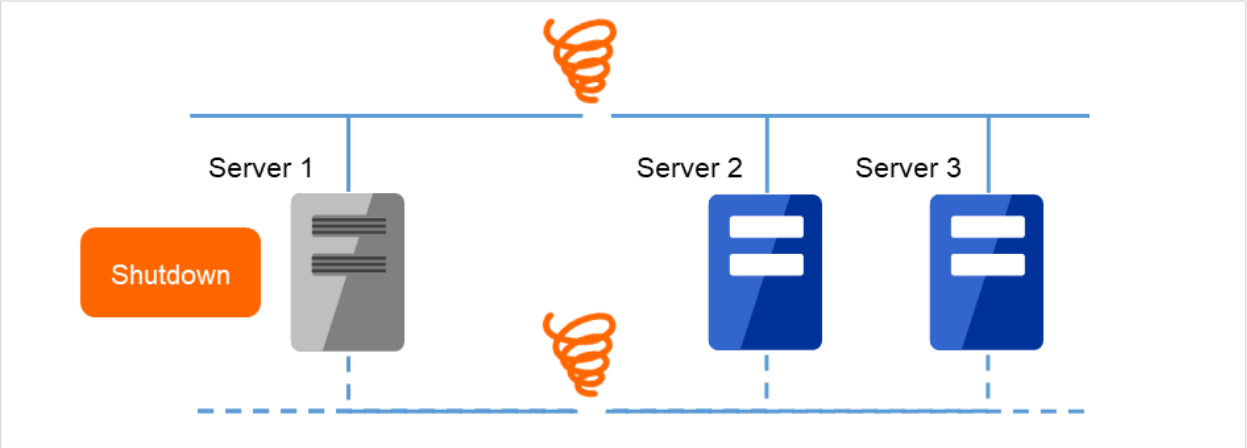


Fig. 6.12: Majority network partition resolution resources (2)

For more information, refer to "*Fencing tab*" in "*Cluster properties*" in "*2. Parameter details*" in this guide.

6.5.2 Majority network partition resolution resources

- This method can be used in a cluster with three or more nodes.
- If majority of the servers are down, the selected "action at NP occurrence" takes place in rest of the servers working properly. When communication with exactly half of the servers in the entire cluster is failing, the selected "action at NP occurrence" takes place in a server that cannot communicate with the top priority server.
- If all servers are isolated form the network due to a hub error, the selected "action at NP occurrence" takes place in all servers.

6.6 Understanding network partition resolution by PING method and DISK method

A network partition is solved by combining PING network partition resolution resources and DISK network partition resolution resources.

When the communication with all servers and ping device is not working properly due to the failure of ping device[2], this method works in the same way as the DISK method. This mechanism allows for higher availability than using the PING method alone. The method also solves network partition faster than using only the disk method.

This method works as PING + DISK method when the server which uses PING network partition resolution resources and the server which uses DISK network partition resolution resources are identical. For example, in the clusters of hybrid disk configuration, when DISK network partition resolution resources used by a particular server group and PING network resolution resources used by the whole clusters are configured, these resources work independently. In such a case, to configure the resources to work in PING+DISK method, it is required to add PING network resolution resources to be used only by the same server group as DISK network partition resolution resources.

[2] Status where no response is returned to the ping command on all servers before the heartbeat is lost.

6.7 Not resolving network partition

- This method can be selected in a cluster that does not use a shared disk.
- If a failure occurs on all network channels between servers in a cluster, all servers failover.

6.8 Notes on network partition resolution resource settings

In X2.1 or earlier, if any combination of network partition resolution resources other than those shown above is specified, network partitions are not resolved. In X3.0 or later, network partitions are resolved in the following order according to the specified resources, even for a combination of network partition resolution resources other than those shown above.

1. PING method and DISK method
2. HTTP method (added in X4.1 version or later)
3. PING method (not applied if network partition resolution processing is performed in 1.)
4. DISK method (not applied if network partition resolution processing is performed in 1 or 2.)
5. Majority method

CHAPTER

SEVEN

FORCED STOP RESOURCE DETAILS

This chapter provides the detailed information on forced stop resources.

7.1 What is the forced stop function?

When a server crash is recognized due to a heartbeat loss, the forced stop function makes the remaining servers (operating properly) forcibly stop the down server.
Suppose the recognized server crash is actually a temporary inability to operate due to the server's stall. In this case, the forced stop function surely stops the down server before its application is failed over to a healthy server. This reduces the risk of the corruption of data in the same resource accessed from multiple servers.

The method for forcibly stopping the failing server varies depending on the type of environment where the cluster was created: physical machines, virtual machines, or the cloud. When using the forced stop function, configure a **forced stop resource** corresponding to the environment type.

Moreover, you can execute a script in which the procedure for stopping the failing server is written. For details, refer to "7.7. *Understanding forced stop with script*" in this guide.

A forced stop resource operates in two ways: performing a forced stop and periodically checking if the target can be forcibly stopped. The following explains what these are and when they are done:

- Performing a forced stop
  - Forcibly stops a down server by using a device or infrastructure system as a server status manager.
  - Done by recognizing the server crash. For more information on the conditions, see "7.1.1. *Conditions for performing forced stop*".
- Periodically checking if the target can be forcibly stopped
  - Checks whether a forced stop can be performed, by communicating with a device or infrastructure system for forcibly stopping a server. Depending on the result, the forced stop resource shows whether the server can be forcibly stopped: "Normal" (yes) or "Error" (no).
  - Done on a regular basis while the cluster service is running.

7.1.1 Conditions for performing forced stop

- Forced stop is not performed when:
  - The failover group successfully stops before the server fails
  - The server is shut down by the clpdown 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)
- Forced stop is performed when:
  - The server is failing and there is a failover group to perform failover from the failing server to another server

7.2 Understanding forced stop on physical environment

7.2.1 Settings of BMC forced stop resource

When you use the ipmiutil command, it is necessary to install ipmiutil in each cluster server. For information on how to get ipmiutil and how to install it, refer to "Setup of BMC and ipmiutil" in "Settings after configuring hardware" in "Determining a system configuration" in the "Installation and Configuration Guide".

Commands for BMC forced stop resource

For forcibly stopping a physical machine, use the [ipmiutil reset] command of IPMI Management Utilities.

For periodically checking the status of the forced stop resource and for checking whether a forced stop succeeds, use the [ipmiutil health] command.

When executing either of the commands, specify the following option values:

command option	item to be set in **BMC Forced-Stop Properties** -> **Server List** -> **Edit** -> **Enter BMC**
-N ip_address	IP address
-U username	User name
-P password	Password

The following table shows commands to be executed for forced stop actions by the BMC forced stop resource:

Forced Stop Action	Parameters
BMC Power Off	ipmiutil reset -d -N *ip_address* -U *username* -P *password*
BMC Reset	ipmiutil reset -r -N *ip_address* -U *username* -P *password*
BMC Power Cycle	ipmiutil reset -c -N *ip_address* -U *username* -P *password*
BMC NMI	ipmiutil reset -n -N *ip_address* -U *username* -P *password*

If the above commands fail to be executed, perform the following commands:

Forced Stop Action	Parameters
BMC Power Off	ipmiutil reset -d -N *ip_address* -U *username* -P *password* -J 3
BMC Reset	ipmiutil reset -r -N *ip_address* -U *username* -P *password* -J 3
BMC Power Cycle	ipmiutil reset -c -N *ip_address* -U *username* -P *password* -J 3
BMC NMI	ipmiutil reset -n -N *ip_address* -U *username* -P *password* -J 3

The following table shows commands to be executed for periodically checking the status of the BMC forced stop resource and for checking whether a forced stop succeeds:

Command to periodically check the status Command to check a forced stop
ipmiutil health -N *ip_address* -U *username* -P *password*

If the above command fails to be executed, perform the following command:

Command to periodically check the status Command to check a forced stop
ipmiutil health -N *ip_address* -U *username* -P *password* -J 3

Editing commands for BMC forced stop resource

For forced stop resources, you can also specify a command line for a forced stop by editing a script file for the command execution.

The following file can be edited:

<EXPRESSCLUSTER_install_path>\bin\clpbmcforcestop.bat

For the BMC forced stop resource, set environment variable values necessary for commands to be executed with the script.

The following table shows environment variables written in the script:

Environment variable	Setting value	Description
CLP_BMC_ACTION ...Forced Stop Action	-d : BMC Power Off -r : BMC Reset -c : BMC Power Cycle -n : BMC NMI	Specifies the Forced Stop Action set in the BMC Forced-Stop Properties.
CLP_BMC_HOST ...IP address for BMC	IP Address	Specifies the IP address set in the BMC Forced-Stop Properties.
CLP_BMC_USER ...User name for BMC	User name	Specifies the user name set in the BMC Forced-Stop Properties.
CLP_BMC_PASSWORD ...Password for BMC	Password	Specifies the password set in the BMC Forced-Stop Properties.

For more information on configuring the BMC forced stop resource, see this guide: "2. *Parameter details*" -> "*Cluster properties*" -> "*Fencing tab*" -> "Forced stop" -> "BMC Forced-Stop Properties".

7.2.2 Notes on BMC forced stop resource

- Impacts on 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

    Because 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 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

  When using the BMC forced stop resource, disable the iLO shared network port.

  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 when BMC is not installed in the server, or in the environment where the network for the BMC management is blocked.

  Navigate **BMC Forced-Stop Properties** -> **Server List** -> **Edit** -> **Enter BMC**, then enter the IP address assigned to the LAN port for BMC management.

  See the server's manuals etc. for information on how to configure the IP address of the LAN port for the BMC management etc.

- Power Options settings of the OS

  Conducting a power-off or power cycle by BMC may perform an action selected in **Power Options** of the OS, such as **Sleep**, **Hibernate**, or **Shutdown**.

  The settings can be referred to and configured by the following instruction:

  Open **Power Options** in **Control Panel** and select **Choose what the power button does**, **Power button settings** and **When I press the power button:**.

  When Forced stop is used in EXPRESSCLUSTER, it is recommended that this setting is configured as **No Operation**.

7.3 Understanding forced stop on vCenter environment

7.3.1 Settings of vCenter forced stop resource

The vCenter forced stop resource can be used with vSphere Automation APIs or with the VMware vSphere Command Line Interface (vCLI).

In an environment with VMware vSphere 7.0 Update 3 or higher, the vCLI cannot be used. In an environment with VMware vSphere earlier than 7.0 Update 2, vSphere Automation APIs cannot be used.

Setting parameters of vCenter forced stop resource

For the vCenter forced stop resource, set parameters listed below.
With vSphere Automation APIs, these parameters are specified for requests.
With the vCLI, these parameters are specified for command options.

Parameter	Item to be set in **vCenter Forced-Stop Properties** -> the **vCenter** tab	Item to be set in **vCenter Forced-Stop Properties** -> **Server List** -> **Edit** -> **Input for Virtual Machine name**
ip_address	IP address	-
username	User name	-
password	Password	-
virtualmachine	-	Virtual machine name
datacenter	-	Datacenter name

APIs for vCenter forced stop resource

When the vCenter forced stop resource is used with vSphere Automation APIs, the following APIs are executed:

Creating a session to obtain the session ID (api_session_id)

Creating a session
curl -k -X POST -u {*username*}:{*password*} https://{*ip_address*}/api/session

Retrieving data center information to obtain the data center ID (datacenter_id)

Retrieving data center information
curl -k -X GET https://{*ip_address*}/api/vcenter/datacenter?names={*datacenter*} -H "vmware-api-session-id: {api_session_id}"

Retrieving virtual-machine information to check the power-supply state and obtain the virtual-machine ID (vm_id)
The data on the power-supply state is used for periodical checks and for stop checks after forced-stop executions, by the vCenter forced stop resource.

Retrieving virtual-machine information
curl -k -X GET https://{*ip_address*}/api/vcenter/vm?names={*virtualmachine*}&datacenters={datacenter_id} -H "vmware-api-session-id: {api_session_id}"

Forcibly stopping the guest OS on the virtual machine

Forced stop	
poweroff	curl -k -X POST https://{*ip_address*}/api/vcenter/vm/{vm_id}/power?action=stop -H "vmware-api-session-id: {api_session_id}"
reset	curl -k -X POST https://{*ip_address*}/api/vcenter/vm/{vm_id}/power?action=reset -H "vmware-api-session-id: {api_session_id}"

Deleting the created session

Deleting the session
curl -k -X DELETE https://{*ip_address*}/api/session -H "vmware-api-session-id: {api_session_id}"

vCLI commands for vCenter forced stop resource

For forcibly stopping the guest OS on a virtual machine, use the [vmcontrol] command of the vCLI. For periodically checking the status of the forced stop resource and for checking whether a forced stop succeeds, use the [vminfo] command.

Using the vCLI requires installing the package.

Note:

If the version of vCLI is 6.5 or later, Perl execution environment is required to be installed. For the information on the versions of Perl necessary to execute vCLI, refer to the website of VMware, Inc.

Perform the following procedure after installing the Perl execution environment.

- Set the Perl path

  Select **Cluster Properties** -> **Fencing tab** -> **Forced stop** -> **vCenter Forced-Stop Properties** -> **vCenter tab**, specify the path to the Perl execution module for Perl Path. This is common to all the servers in the cluster.

  For more information about the Perl path, refer to "*Extension Tab*" in "*Cluster properties*" in "2.2.3. *Fencing tab*" in "*Forced stop*" in "*vCenter Forced-Stop Properties*" in this guide.

- Add the system environment variable

  Add the following variable for the system environment variable. Then restart the OS.

  Variable name: PERL5LIB

  Variable value: vCLI Perl module path (Example: C:\Program Files (x86)\VMware\VMware vSphere CLI\Perl\lib

The following table shows commands to be executed for forced stop actions by the vCenter forced stop resource:

Forced-stop commands	
poweroff	vmcontrol.pl --server *ip_address* --username *username* --password *password* --vmname *virtualmachine* --datacenter *datacenter* --operation poweroff
reset	vmcontrol.pl --server *ip_address* --username *username* --password *password* --vmname *virtualmachine* --datacenter *datacenter* --operation reset

The following table shows commands to be executed for periodically checking the status of the vCenter forced stop resource:

Command to periodically check the status
vminfo.pl --server *ip_address* --username *username* --password *password* --vmname *virtualmachine* --datacenter *datacenter*

The following table shows commands to be executed for checking whether a forced stop succeeds:

Command to check a forced stop
vminfo.pl --server *ip_address* --username *username* --password *password* --vmname *virtualmachine* --datacenter *datacenter* --powerstatus "poweredOff"

Editing commands for vCenter forced stop resource

For forced stop resources, you can also specify a command line for a forced stop by editing a script file for the command execution.

When using the vCenter forced stop resource with vSphere Automation APIs, you can edit the following file:

<EXPRESSCLUSTER_installation_path>\bin\clpvcenterrestapiforcestop.bat

When using the vCenter forced stop resource with the vCLI, you can edit the following file:

<EXPRESSCLUSTER_installation_path>\bin\clpvcentercliforcestop.bat

For the vCenter forced stop resource, set environment variable values necessary for commands to be executed with the script.

The following table shows environment variables written in the script:

Environment variable	Setting value	Description
CLP_VCLI_PATH ...vCLI install path	Install path	Specifies the VMware vSphere CLI install path set in the vCenter Forced-Stop Properties.

Continued on next page

Table 7.8 – continued from previous page

Environment variable	Setting value	Description
CLP_VCENTER_ACTION ...Forced Stop Action	poweroff : power off reset : reset	Specifies the Forced Stop Action set in the vCenter Forced-Stop Properties.
CLP_VCENTER_HOST ...Host name for vCenter	Host name	Specifies the host name set in the vCenter Forced-Stop Properties.
CLP_VCENTER_USER ...User name for vCenter	User name	Specifies the user name set in the vCenter Forced-Stop Properties.
CLP_VCENTER_PASSWORD ...Password for vCenter	Password	Specifies the password set in the vCenter Forced-Stop Properties.
CLP_VMNAME ...Virtual machine name	Virtual machine name	Specifies the virtual machine name set in the vCenter Forced-Stop Properties.
CLP_DATACENTER_NAME ...Data center name	Data center name	Specifies the data center name set in the vCenter Forced-Stop Properties.
CLP_PERL_PATH ...Perl path	Perl path	Specifies the perl path set in the vCenter Forced-Stop Properties.

For more information on configuring the vCenter forced stop resource, see this guide: "2. *Parameter details*" -> "*Cluster properties*" -> "*Fencing tab*" -> "Forced stop" -> "vCenter Forced-Stop Properties".

7.3.2 Notes on vCenter forced stop resource

- Forcibly stopping the guest OS on a virtual machine
  Only power off operation can be performed. Moreover, this function cannot be used in the following cases:

  - vSphere infrastructure: Communication with VMware vCenter Server is not possible.

- Impacts on forced stop
  When you use the forced stop function, the following functions are influenced because power off, reset is forcibly performed regardless of the OS or server status.

  – Dump collection
  Because it is not recognized that dump files are being collected, power off, reset is performed even though dump collection is being performed, so dump collection does not complete.

  – Power on within heartbeat timeout
  When the server is powered on again for the purpose of maintenance etc. within heartbeat timeout, power off, reset may occur after heartbeat timeout has elapsed.

- Power Options settings of the OS

  Conducting a power-off of the guest OS on a virtual machine with the vCLI may perform an action selected in **Power Options** of the OS, such as **Sleep**, **Hibernate**, or **Shutdown**.

  The settings can be referred to and configured by the following instruction:

  Open **Power Options** in **Control Panel** and select **Choose what the power button does**, **Power button settings** and **When I press the power button:**.

  When Forced stop is used in EXPRESSCLUSTER, it is recommended that this setting is configured as **No Operation**.

7.4 Understanding forced stop on AWS environment

7.4.1 Settings of AWS forced stop resource

Using the AWS forced stop resource requires installing the AWS Command Line Interface (AWS CLI).

For information on how to obtain and install the AWS CLI, see "Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "Time synchronization in the AWS environment" and "IAM settings in the AWS environment".

Commands for AWS forced stop resource

For forcibly stopping an AWS instance, for periodically checking the status of the forced stop resource, and for checking whether a forced stop succeeds, use the command of the AWS CLI.

When executing either of the commands, specify the following option values:

command option	item to be set in **AWS Forced-Stop Properties** -> **Server List** -> **Edit** -> **Input of Instance**
--instance-ids *instance-ids*	InstanceID

The following table shows commands to be executed for forced stop actions by the AWS forced stop resource:

Forced Stop Action	Parameters
stop	aws ec2 stop-instances --instance-ids *instance-ids* --force
reboot	aws ec2 reboot-instances --instance-ids *instance-ids*

The following table shows commands to be executed for periodically checking the status of the AWS forced stop resource:

Forced Stop Action	Command to periodically check the status
stop	aws ec2 stop-instances --instance-ids *instance-ids* --dry-run aws ec2 describe-instances --instance-ids *instance-ids* aws ec2 describe-instance-attribute --instance-ids *instance-ids* --attribute disableApiStop
reboot	aws ec2 reboot-instances --instance-ids *instance-ids* --dry-run aws ec2 describe-instances --instance-ids *instance-ids*

The following table shows commands to be executed for checking whether a forced stop succeeds:

Command to periodically check the status
aws ec2 describe-instances --instance-ids *instance-ids* --filters \"Name=instance-state-name,Values=stopped\"

7.4.2 Applying command line options to AWS CLI run from AWS forced stop resource

- See "AWS CLI command line options" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

7.4.3 Applying environment variables to AWS CLI run from the AWS forced stop resource

- See "Environment variables for running AWS-related features" in "Notes when creating the cluster configuration data" in "Notes and Restrictions" in the "Getting Started Guide".

7.4.4 Notes on AWS forced stop resource

- For forcibly stopping instance
  You can perform only the following actions: stop and reboot.
- Impacts on forced stop
  When you use the forced stop function, the following functions are influenced because stop, reboot is forcibly performed regardless of the OS or server status.
  - Dump collection
    Because it is not recognized that dump files are being collected, stop, reboot is performed even though dump collection is being performed, so dump collection does not complete.
  - Power on within heartbeat timeout
    When the server is powered on again for the purpose of maintenance etc. within heartbeat timeout, stop, reboot may occur after heartbeat timeout has elapsed.
- Power Options settings of the OS
  Conducting the action (stop or reboot) with the AWS CLI may perform an action selected in **Power Options** of the OS, such as **Sleep**, **Hibernate**, or **Shutdown**.
  The settings can be referred to and configured by the following instruction:
  Open **Power Options** in **Control Panel** and select **Choose what the power button does**, **Power button settings** and **When I press the power button:**.
  When Forced stop is used in EXPRESSCLUSTER, it is recommended that this setting is configured as **No Operation**.
- **stop protection** setting for AWS
  With **stop protection** of **Instance settings** enabled, setting **Forced Stop Action** to **stop** leads to a failure in forced stopping and a periodical checking.
  Avoid enabling **stop protection** if you use the forced-stop function of EXPRESSCLUSTER and set **Forced Stop Action** to **stop**.
- Cluster configuration
  For a cluster configured in a multi-region environment, you cannot use the forced-stop function.

7.5 Understanding forced stop on Azure environment

7.5.1 Settings of Azure forced stop resource

Using the Azure forced stop resource requires installing the Azure CLI.

Commands for Azure forced stop resource

For forcibly stopping an Azure instance, for periodically checking the status of the forced stop resource, and for checking whether a forced stop succeeds, use the command of the Azure CLI.

When executing either of the commands, specify the following option values:

command option	item to be set in **Azure Forced-Stop Properties** -> the **Azure** tab	item to be set in **Azure Forced-Stop Properties** -> **Server List** -> **Edit** -> **Input for Virtual Machine name**
--name/-n	-	Virtual Machine Name
--username/-u	User URI	-
--tenant/-t	Tenant ID	-
--password/-p	File Path of Service Principal	-
--resource-group/-g	Resource Group Name	-

For the use of Azure CLI commands, the following command is executed:

Logging in to the Azure CLI
az login --service-principal -u *MyUserUri* -p *MyCertfile.pem* --tenant *MyTenantId*

The following table shows commands to be executed for forced stop actions by the Azure forced stop resource:

Forced Stop Action	Parameters
stop and deallocate[1]	az vm deallocate -g *MyResourceGroup* -n *MyVm* --no-wait
stop only[2]	az vm stop -g *MyResourceGroup* -n *MyVm* --no-wait --skip-shutdown
reboot	az vm restart -g *MyResourceGroup* -n *MyVm* --no-wait

The following table shows commands to be executed for periodically checking the status of the Azure forced stop resource:

Command to periodically check the status
az vm update -g *MyResourceGroup* -n *MyVm* --no-wait
az vm get-instance-view -g *MyResourceGroup* -n *MyVm*

The following table shows commands to be executed for checking whether a forced stop succeeds:

Command to periodically check the status
az vm get-instance-view -g *MyResourceGroup* -n *MyVm* --query instanceView.statuses[1].displayStatus --output tsv

[1] Stops the instance through the shutdown sequence. Since allocated resources (e.g., public IP address) are also released, no charging occurs.
[2] Stops the instance not through the shutdown sequence. Since allocated resources are maintained, the charging continues.

7.5.2 Notes on Azure forced stop resource

- For forcibly stopping instance
  Any of the following actions can be performed: stop and deallocate, stop only, or reboot.
- Impacts on forced stop
  When you use the forced stop function, the following functions are influenced because stop, reboot is forcibly performed regardless of the OS or server status.
  - Dump collection
    Because it is not recognized that dump files are being collected, stop, reboot is performed even though dump collection is being performed, so dump collection does not complete.
  - Power on within heartbeat timeout
    When the server is powered on again for the purpose of maintenance etc. within heartbeat timeout, stop, reboot may occur after heartbeat timeout has elapsed.
- Power Options settings of the OS
  Conducting the action (stop or reboot) with the OCI CLI may perform an action selected in **Power Options** of the OS, such as **Sleep**, **Hibernate**, or **Shutdown**.
  The settings can be referred to and configured by the following instruction:
  Open **Power Options** in **Control Panel** and select **Choose what the power button does**, **Power button settings** and **When I press the power button:**.
  When Forced stop is used in EXPRESSCLUSTER, it is recommended that this setting is configured as **No Operation**.
- Cluster configuration
  For a cluster configured in a multi-region environment, you cannot use the forced-stop function.

7.6 Understanding forced stop on OCI environment

7.6.1 Settings of OCI forced stop resource

Using the OCI forced stop resource requires installing the Oracle Cloud Infrastructure CLI (OCI CLI).

For information on how to obtain and install the OCI CLI, see "Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "CLI settings in the OCI environment".

Commands for OCI forced stop resource

For forcibly stopping an OCI instance, for periodically checking the status of the forced stop resource, and for checking whether a forced stop succeeds, use the command of the OCI CLI.

When executing either of the commands, specify the following option values:

command option	item to be set in **OCI Forced-Stop Properties** -> **Server List** -> **Edit** -> **Input of Instance**
--instance-ids *instance-ids*	InstanceID

The following table shows commands to be executed for forced stop actions by the OCI forced stop resource:

Forced Stop Action	Parameters
stop	oci compute instance action --action STOP --instance-id *instance-ids*
reboot	oci compute instance action --action RESET --instance-id *instance-ids*

The following table shows commands to be executed for periodically checking the status of the OCI forced stop resource:

Command to periodically check the status
oci compute instance update --instance-id *instance-ids* --wait-for-state RUNNING --max-wait-seconds 1

The following table shows commands to be executed for checking whether a forced stop succeeds:

Command to periodically check the status
oci compute instance get --instance-id *instance-ids* | grep lifecycle-state | awk -F" '{print $4}'

7.6.2 Notes on OCI forced stop resource

- For forcibly stopping instance
  You can perform only the following actions: stop and reboot.
- Impacts on forced stop
  When you use the forced stop function, the following functions are influenced because stop, reboot is forcibly performed regardless of the OS or server status.
  - Dump collection
    Because it is not recognized that dump files are being collected, stop, reboot is performed even though dump collection is being performed, so dump collection does not complete.
  - Power on within heartbeat timeout
    When the server is powered on again for the purpose of maintenance etc. within heartbeat timeout, stop,

reboot may occur after heartbeat timeout has elapsed.

- Power Options settings of the OS
  Conducting the action (stop or reboot) with the OCI CLI may perform an action selected in **Power Options** of the OS, such as **Sleep**, **Hibernate**, or **Shutdown**.
  The settings can be referred to and configured by the following instruction:
  Open **Power Options** in **Control Panel** and select **Choose what the power button does**, **Power button settings** and **When I press the power button:**.
  When Forced stop is used in EXPRESSCLUSTER, it is recommended that this setting is configured as **No Operation**.
- Cluster configuration
  For a cluster configured in a multi-region environment, you cannot use the forced-stop function.

7.7 Understanding forced stop with script

7.7.1 Settings of custom forced stop resource

You can create a script for a forced stop. When a server crash is recognized, using the script on the remaining servers (operating properly) allows you to forcibly stop the down server.

The script is executed in both of the following modes: performing a forced stop and periodically checking if the target can be forcibly stopped. For appropriate processing based on each of the modes, write conditional branches by using environment variables described later.

Environment variables for script

When executing the script, EXPRESSCLUSTER sets environment variable values such as which mode (a periodical status check or a forced stop) to be performed and what server has crashed.

In the script, you can use the following environment variables:

Environment variable	Setting value	Description
CLP_FORCESTOP_MODE ...Mode	0 : When periodically checking the status 1 : When performing a forced stop	Means a mode to be performed. Can be used for process branches for each of the modes.
CLP_SERVER_DOWN ...Down server name	Server name	Means the name of a down server. For periodically checking the status, "" is set.
CLP_SERVER_LOCAL ...Local server name	Server name	Means the name of a server to execute the script.

Returned value of script

Return 0 when the script terminates normally.

For more information on configuring the custom forced stop resource, see this guide: "2. *Parameter details*" -> "*Cluster properties*" -> "*Fencing tab*" -> "Forced stop" -> "Custom Forced-Stop Properties".

7.7.2 Notes on custom forced stop resource

- Describe the customer-defined process in the script to stop the server.
- If there is nothing to be done as periodically checking the status, write the process as such (so that the value 0 can be returned).

7.8 Notes on settings of forced stop resource

- You can configure only one forced stop resource for one cluster.
- If you want to configure a forced stop resource, it is recommended to configure a network partition resolution resource as well.
- In configuring a forced stop resource, all the cluster servers must be set to use the forced stop resource.
- To prevent a split-brain syndrome in a failover group with a forced-stop resource operating, set the service startup delay time as follows:
  - When setting up DISK network partition resolution resources
    Service startup delay time >= forced-stop timeout of forced-stop resource + time to wait for stop to be completed of forced-stop resource + heartbeat timeout + heartbeat interval + IO Wait Time of DISK network partition resolution resources + 10 seconds
  - When not setting up DISK network partition resolution resources
    Service startup delay time >= forced-stop timeout of forced-stop resource + time to wait for stop to be completed of forced-stop resource + heartbeat timeout + heartbeat interval

  For more information on the service startup delay time, see "Adjustment of time for EXPRESSCLUSTER services to start up (Required)".

CHAPTER

EIGHT

INFORMATION ON OTHER SETTINGS

This chapter provides the information on the other monitor or notification settings.

This chapter covers:

8.1 Alert Service

8.1.1 Alert Service

EXPRESSCLUSTER Alert Service is a function to report failures found in operations on EXPRESSCLUSTER 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. Warning light
   The warning light is a visual display of the status of the server. When the server shuts down successfully, the warning light goes off.
   The e-mail report and the 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.

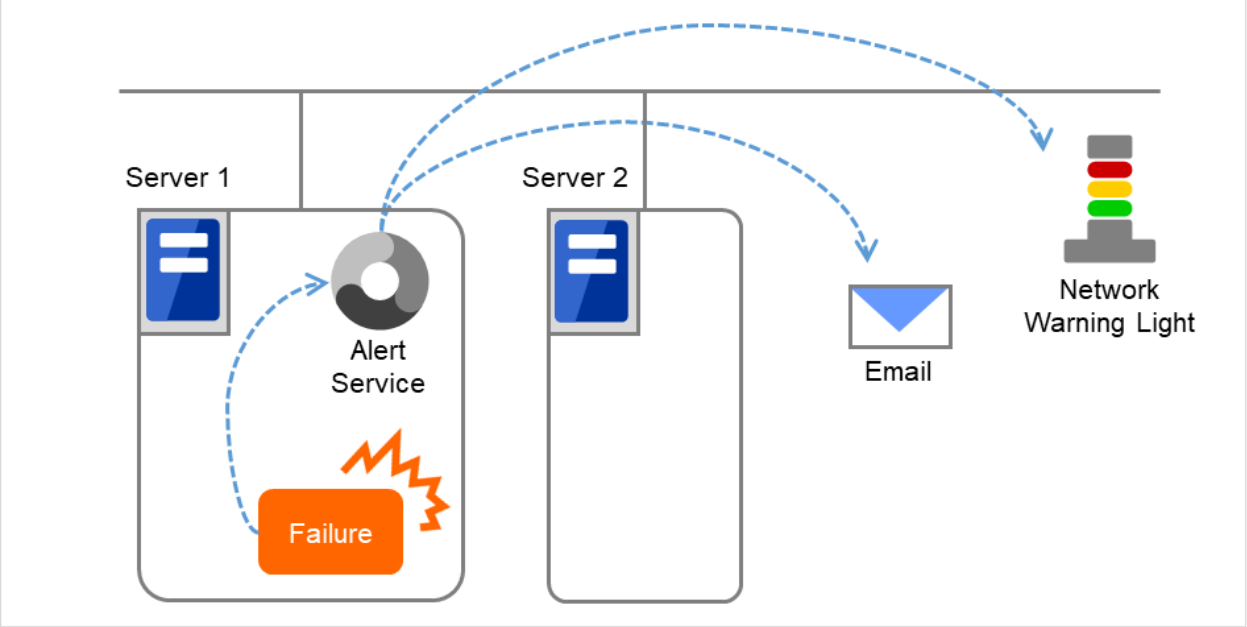


Fig. 8.1: Alert service

Alert Service allows you to:

- Receive information about failures while not physically located in the place where management PC is. This is achieved via e-mail reporting function.
- Receive e-mail messages on your mobile phone.
- Visually be alerted of failures by viewing a 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]
```

8.1.2 Notes on Alert Service

- To use the mail report and warning light function, the EXPRESSCLUSTER X Alert Service 5.2 license must be applied to the system.
- 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.
- When the warning light function is used, it is necessary to set up the command such as rsh that is supported by the warning light manufacturer.

8.1.3 Mail report actions

- Alert Service sends the same messages as the Cluster WebUI. For the alert messages to be reported by e-mail, see "*Messages reported by event log and alert*" in "11. *Error messages*" in this guide.
- You can change the alerts that are reported by e-mail. For more information, see "*Alert Service tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.

8.1.4 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 warning light is controlled by a normal server that monitors other servers.

Once a 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 "*Switching off network warning light (clplamp command)*" in "9. *EXPRESSCLUSTER command reference*" 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.

8.1.5 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 event log and alert*" in "11. *Error messages*" in this guide.
- The alerts subject to SNMP trap sending can be changed. For more information, see "*Alert Service tab*" in "*Cluster properties*" in "2. *Parameter details*" in this guide.
- For details on the SNMP trap, see "*SNMP trap sending*".

8.2 SNMP linkage

8.2.1 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.

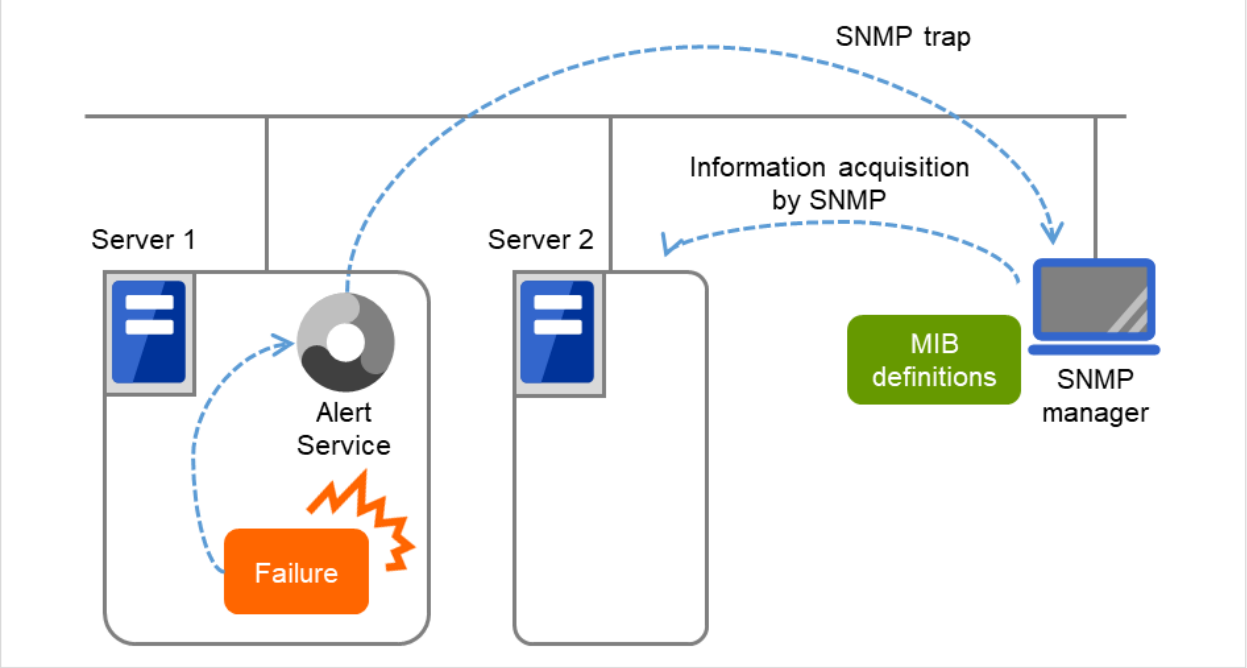


Fig. 8.2: SNMP linkage

8.2.2 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 DVD-ROM.

<EXPRESSCLUSTER_X_DVD-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 get information by SNMP:

1. NEC-CLUSTER-SMI.mib 3. NEC-CLUSTER-MANAGEMENT-MIB.mib

8.2.3 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.
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.

8.2.4 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, Windows SNMP Service 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:

If Windows SNMP Service has been installed when EXPRESSCLUSTER Server is installed, the SNMP linkage function is automatically registered. Otherwise, it is not automatically registered.

It needs to be manually registered; for details on how to manually register it, refer to "Setting up the SNMP linkage function manually" in "Installing the EXPRESSCLUSTER Server" in "Installing EXPRESSCLUSTER" in the "Installation and Configuration Guide".

8.2.5 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 status 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 8.5 – 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  status`
		`----------`
		`online  Online`
		`caution  Suspension (Network Partition Unsolved)`
		`isolated  Suspension (Isolated)`
		`offline  Offline`
		`unknown  Unknown`

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. If the return value is other than an ASCII character, the data might be corrupt.
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.

Continued on next page

Table 8.6 – continued from previous page

No.	SNMP OID	Description
5.	clusterGroupComment	Indicates a comment for the group.
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
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). If the group has been deactivated, the return value is -1

8.3 Grace period dependence at the automatic failover between server groups

8.3.1 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.

8.3.2 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 tab
  - **Prioritize failover policy in the server group** is selected and **Enable only manual failover among the server groups** is not selected for **Automatic 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 forced stop is successfully executed while the type of forced stop is selected for other than **Do Not Use**, or the condition not to execute the forced stop is met.
  - The NP resolution resource is configured.

8.3.3 Displaying and changing the grace period dependence

Specify the waiting time for **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

8.3.4 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 canceled 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 canceled and the failover is not executed.

If the failover target server goes down, the failover may start later than when the grace period ends.

8.4 Witness server service

8.4.1 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.

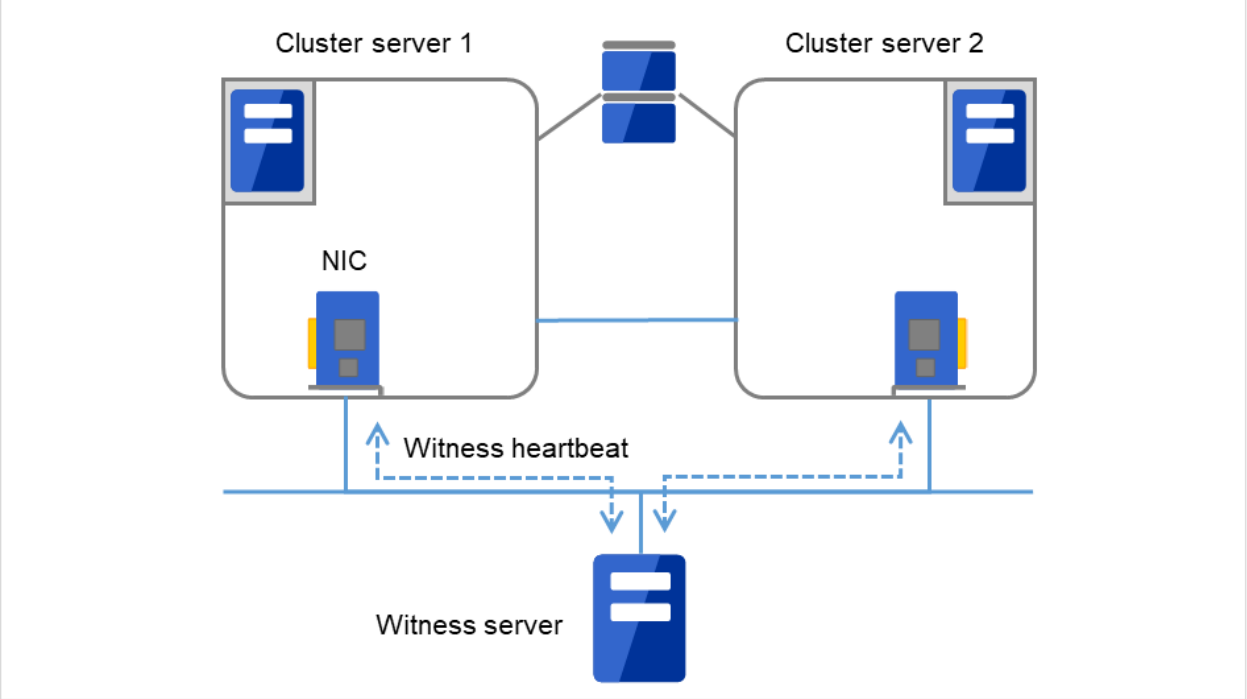


Fig. 8.3: Witness server service

8.4.2 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.
- See "System requirements for the Witness server" in "Installation requirements for EXPRESSCLUSTER" in the "Getting Started Guide".

8.4.3 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
```

Obtain the Witness server service module in the following path of the DVD-ROM for installation:

```
Common\<version>\common\tools\witnessd\clpwitnessd-<version>.tgz
```

8.4.4 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.
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.

8.4.5 How to execute Witness server service

Execute 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

8.4.6 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 manager

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 package.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)

2. Create the unit file of the Witness server service in /etc/systemd/system.
   (ex. clpwitnessd.service)

```
[Unit]
Description=EXPRESSCLUSTER 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

NINE

EXPRESSCLUSTER COMMAND REFERENCE

This chapter describes commands that are used on EXPRESSCLUSTER.

9.1 Operating the cluster from the command line

EXPRESSCLUSTER provides various commands to operate a cluster by the command prompt. These commands are useful for things like constructing a cluster or when you cannot use the WebManager. 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 application 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.

9.2 EXPRESSCLUSTER commands

Commands for configuring a cluster

Command	Description	Page
clpcfctrl.exe	Distributes configuration data created by the Cluster WebUI to servers. Cluster WebUI up the cluster configuration data to be used by the Cluster WebUI.	9.9.
clplcnsc.exe	Manages the product or trial version license of this product.	9.12.
clpcfchk.exe	Checks the cluster configuration information.	9.28.
clpcfconv.bat	Converts an old version of a cluster configuration data file into the current version.	9.29.
clpfwctrl.bat	Adds a firewall rule.	9.30.

Commands for displaying status

Command	Description	Page
clpstat.exe	Displays the cluster status and configuration information.	9.3.
clphealthchk.exe	Check the process health.	9.21.

Commands for cluster operation

Command	Description	Page
clpcl.exe	Starts, stops, suspends, or resumes the EXPRESSCLUSTER service.	9.4.
clpdown.exe	Stops the EXPRESSCLUSTER service and shuts down the server.	9.5.
clpstdn.exe	Stops the EXPRESSCLUSTER service across the whole cluster and shuts down all servers.	9.6.
clpgrp.exe	Starts, stops, or moves groups.	9.7.
clptoratio.exe	Extends or displays the various time-out values of all servers in the cluster.	9.10.
clpmonctrl.exe	Controls monitor resources.	9.15.
clprsc.exe	Stops or resumes group resources	9.16.
clprexec.exe	Requests that an EXPRESSCLUSTER server execute a process from external monitoring.	9.18.
clpbwctrl.exe	Controls the cluster activation synchronization wait processing.	9.19.
clpregctrl.exe	Displays and/or initializes reboot count on a single server	9.20.
clpstdncnf.exe	Setting Operations for Shutting Down OS from Outside Clusters	9.22.

Log-related commands

Command	Description	Page
clplogcc.exe	Collects logs and OS information.	9.8.
clplogcf.exe	Modifies and displays a configuration of log level and the file size of log output.	9.11.
clpperfc.exe	Displays the cluster statistics data about groups and monitor resources.	9.27.

Script-related commands

Command	Description	Page
clplogcmd.exe	Writes texts in the script resource script to create a desired message to the output destination.	9.14.

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.

Mirror-related commands (when the Replicator/Replicator DR is used)

Command	Description	Page
clpmdstat.exe	Displays the status and configuration information on mirror disk.	9.13.1.
clpmdctrl.exe	Allows operations such as mirror recovery and activating/deactivating a mirror disk resource.	9.13.2.
clphdstat.exe	Displays the status and configuration information on hybrid disk.	9.13.7.
clphdctrl.exe	Allows operations such as mirror recovery and activating/deactivating a hybrid disk resource.	9.13.8.
clpvolsz.exe	Checks and adjusts the size of partitions to be mirrored.	9.13.3.
clpvolctrl.exe	Accesses a volume not registered as a resource.	9.13.4.
clpkeygen.exe	Creates an encryption key file for encrypting mirror data communication.	9.13.5.
clphdsnapshot.exe	Controls the access restriction or alike when snap shot backups of data partition in the hybrid disk resource are collected	9.13.6.
clpbackup.bat	Allows a partition to be mirrored to be backed up to a disk image.	9.13.9.
clprestore.bat	Allows a restored mirror disk image to be enabled.	9.13.10.

Warning-related commands (when the Alert Service is used)

Command	Description	Page
clplamp.exe	Lights off the network warning light.	9.17.

DB rest point-related commands

Command	Description	Page
clpdb2still	Controls the securing/release of a rest point of DB2.	9.23.
clporclstill	Controls the securing/release of a rest point of Oracle.	9.24.
clppsqlstill	Controls the securing/release of a rest point of PostgreSQL.	9.25.
clpmssqlstill	Controls the securing/release of a rest point of SQL Server.	9.26.

9.3 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 -f [-h <*hostname*>]
clpstat -i [--detail] [-h <*hostname*>]
clpstat --cl [--detail] [-h <*hostname*>]
clpstat --sv [<*srvname*>] [--detail] [-h <*hostname*>]
clpstat --hb [<*hbname*>] [--detail] [-h *host_name*]
clpstat --fnc [<*fncname*>] [--detail] [-h <*hostname*>]
clpstat --svg [<*svgname*>] [-h <*hostname*>]
clpstat --grp [<*grpname*>] [--detail] [-h <*hostname*>]
clpstat --rsc [<*rscname*>] [--detail] [-h <*hostname*>]
clpstat --mon [<*monname*>] [--detail] [-h <*hostname*>]
clpstat --xcl [<*xclname*>] [--detail] [-h <*hostname*>]
clpstat --local

Description

This command line displays a cluster status and configuration data.

-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.

-f
Displays the status of fencing function (network partition resolution and forced stop 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.

--fnc [fnc_name]
Displays the configuration information on the fencing function (the network partition resolution resource and the forced stop resource). By specifying the resource name, you can display only the information on the specified network partition resolution resource or the specified forced stop resource.

--grp [group_name]
Displays group configuration information. By specifying the name of a group, you can display only the information on the specified group.

--svg [svgname]
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 monitor 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 host_name
Acquires information from the server specified with *host_name*. 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

0	Success
Other than the above	Failure

Remarks
According to the combination of options, configuration information shows information in various forms.

"*" alongside the server name, displayed after executing this command, represents the server that executed this command.

Notes
Run this command as a user with Administrator privileges.

When you specify the name of a server for the -h option, the server should be in the cluster.

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 section.

Error Messages

Message	Cause/Solution
Log in as administrator.	Log in as a user with Administrator privileges.
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 service is active.	Check if the EXPRESSCLUSTER Information Base service is started.
Invalid server status.	Check if the EXPRESSCLUSTER service is operating.
Server is not active. Check if the cluster service is active.	Check if the EXPRESSCLUSTER service is operating.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid server name in the cluster.
Invalid heartbeat resource name. Specify a valid heartbeat resource name in the cluster.	Specify the valid heart beat resource name in the cluster.
Invalid network partition resource name. Specify a valid network partition resource name in the cluster.	Specify the valid network partition resolution resource name 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 service is stopped in the cluster.	Check if there is any server on which the EXPRESSCLUSTER service has stopped in the cluster.
Invalid parameter.	An invalid value may be specified to command argument.
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set the 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 if the memory or OS resource is sufficient.
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 started.

Continued on next page

Table 9.9 – continued from previous page

Message	Cause/Solution
Cluster is suspended. To display the cluster status, use --local option.	Cluster is suspended. To display the cluster status, use --local option.

Common entry examples

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
  lankhb1           : Normal LAN Heartbeat
  lankhb2           : Normal LAN Heartbeat
  witnesshb1        : Normal Witness Heartbeat
  pingnp1           : Normal ping resolution
  httpnp1           : Normal http resolution
  forcestop1        : Normal Forced stop
server2 ........... : Online server2
  lankhb1           : Normal LAN Heartbeat
  lankhb2           : Normal LAN Heartbeat
  witnesshb1        : Normal Witness Heartbeat
  pingnp1           : Normal ping resolution
  httpnp1           : Normal http resolution
  forcestop1        : Normal Forced stop

<group>
ManagementGroup     : Online Management Group
  current           : server1
  ManagementIP      : Online 10.0.0.10
failover1.......... : Online failover group1
current             : server1
  fip1              : Online 10.0.0.11
  md1               : Online I:
  script1           : Online script resource1
failover2 ......... : Online failover group2
  current           : server2
  fip2              : Online 10.0.0.12
  md2               : Online J:
  script1           : Online script resource2
<monitor>
fipw1               : Normal fip1
fipw2               : Normal fip2
ipw1                : Normal ip monitor1
mdw1                : Normal md1
mdw2                : Normal md2
============================================================
```

Information on each status is provided in " *Status Descriptions* ".

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* ".

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 [fipw1 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Offline

 Monitor1 [fipw2 : Normal]
-------------------------------------------------------------
  server0 [o] : Offline
  server1 [o] : Online

 Monitor2 [ipw1 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online

 Monitor3 [mdw1 : Normal]
-------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
```

(continues on next page)

(continued from previous page)

```
 Monitor4 [mdw2 : Normal]
-----------------------------------------------------------------
  server0 [o] : Online
  server1 [o] : Online
=================================================================
```

Information on each status is provided in " *Status Descriptions* ".

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 : lankhb1
    HB1 : lankhb2
    HB2 : witnesshb1

    [on server0 : Online]
           HB 0 1 2
-----------------------------------------------------------------
    server0 : o o o
    server1 : o x o

     on server1 : Online]
           HB 0 1 2
-----------------------------------------------------------------
    server0 : o x o
    server1 : 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 kernel-mode LAN heartbeat resource that has the second-highest priority is disconnected.

Because kernel-mode LAN heartbeat resource lankhb1 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.

Displaying the status of fencing function (-f option)

Specify the -f option to the clpstat command and execute the command to display the status of the fencing function (network partition resolution resources or a forced stop resource).

Example of a command entry

```
# clpstat -f
```

Example of the display after running the command:

```
======================== FENCING STATUS ========================
  Cluster : cluster
    *server0 : server1
     server1 : server2

    NP0 : disknp1
    NP1 : pingnp1
    NP2 : httpnp1
    FST : forcestop1

    [on server0 : Online]
     NP/FST   0 1 2 F
-----------------------------------------------------------------
    server0 : o o o o
    server1 : o o o -

    [on server1 : Online]
     NP/FST   0 1 2 F
-----------------------------------------------------------------
    server0 : o o o -
    server1 : o o o o
=================================================================
```

Detailed information on each status is provided in " *Status Descriptions* ".

Displaying the cluster configuration data (clpstat command, --cl option)

To display the configuration data of a cluster, run the clpstat command with the -i, --cl, --sv, --hb, --fnc, --svg, --grp, --rsc, or --mon option. You can see more detailed information by specifying the --detail option. See a separate section, "2. *Parameter details*" in this guide for details of each item of the list.

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 Name: cluster]
Comment                          : failover cluster
===========================================================
```

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. To see the details, specify the -- detail option. When the server name is not specified, cluster configuration data of all the servers is displayed.

Example of a command entry

```
# clpstat --sv server1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ====================
[Server0 : server1]
Comment                      : server1
Virtual Infrastructure       : vSphere
Product                      : EXPRESSCLUSTER X 5.2 for Windows
Internal Version             : 13.20
Install Path                 : C:\Program Files\EXPRESSCLUSTER
=============================================================
```

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. When the heartbeat resource is not specified, the cluster configuration data of all the heartbeat resources is displayed.

Example of a command entry

For a kernel-mode LAN heartbeat resource

```
# clpstat --hb lankhb1
```

Example of the display after running the command:

```
=================== CLUSTER INFORMATION ===================
[HB0 : lanhb1]
Type                        : lankhb
Comment                     : LAN 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 5.2 for Windows
  Internal Version           : 13.20
  Install Path               : C:\Program Files\EXPRESSCLUSTER
 [HB0 : lankhb1]
  Type                       : lankhb
  Comment                    : LAN Heartbeat
 [HB1 : lanhb2]
  Type                       : lankhb
  Comment                    : LAN Heartbeat
 [Server1 : server2]
  Comment                    : server2
  Virtual Infrastructure     :
  Product                    : EXPRESSCLUSTER X 5.2 for Windows
  Internal Version           : 13.20
  Install Path               : C:\Program Files\EXPRESSCLUSTER
  [HB0 : lankhb1]
```

(continues on next page)

(continued from previous page)

```
  Type                          : lankhb
  Comment                       : LAN Heartbeat
 [HB1 : lankhb2]
  Type                          : lankhb
  Comment                       : LAN Heartbeat
================================================================
```

Displaying only the resource information of certain fencing function (--fnc option)

When you want to display only the cluster configuration data on a specified fencing function (network partition resolution resource and forced stop resource), specify the name of the network partition resolution resource or the forced stop resource after the --fnc option in the clpstat command. If you want to see the details, specify the --detail option. If the network partition name or the forced stop resource name is not specified, the cluster configuration data on all the fencing function is displayed.

Example of a command entry

For a DISK network partition resolution resource:

```
# clpstat --fnc disknp1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ======================
[NP0 : disknp1]
Type                          : disknp
Comment                       : disk resolution
================================================================
```

Example of a command entry

For a PING network partition resolution resource:

```
# clpstat --fnc pingnp1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ======================
[NP0 : pingnp1]
Type                          : pingnp
Comment                       : ping resolution
================================================================
```

Example of a command entry

For an HTTP network partition resolution resource:

```
# clpstat --fnc httpnp1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ======================
[NP0 : httpnp1]
Type                          : httpnp
Comment                       : http resolution
================================================================
```

Example of a command entry

For a majority network partition resolution resource:

```
# clpstat --fnc majonp1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ======================
[NP0 : majonp1]
Type                        : majonp
Comment                     : majority resolution
===============================================================
```

Example of a command entry

For a forced stop resource:

```
# clpstat --fnc forcestop1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ======================
[FST : forcestop1]
Type                        : bmc
Comment                     : Forced stop
===============================================================
```

Displaying only the configuration data of certain server groups (--svg option)

When you want to display only the cluster configuration data on a specified server group, specify the name of the server group after the --svg option in the clpstat command. When a server group name is not specified, the cluster configuration data on all the server groups is displayed.

Example of a command entry

```
# clpstat -- svg servergroup1
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ====================
   [Server group 0 : servergroup1]
      Server0 : server1
      Server1 : server2
      Server2 : server3
=============================================================
```

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 the group name is not specified, the cluster configuration data on all the groups is displayed.

Example of a command entry

```
# clpstat --grp
```

Example of the display after running the command:

```
==================== CLUSTER INFORMATION ==================
[Group0 : ManagementGroup]
   Type : cluster
   Comment :
[Group1 : failover1]
   Type : failover
```

(continues on next page)

(continued from previous page)

```
   Comment : failover group1
[Group2 : failover2]
   Type : failover
   Comment : failover group2
[Group3 : virtualmachine1]
   Type : virtualmachine
   Comment :
================================================================
```

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 the group resource name is not specified, the cluster configuration data on 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 ==================
[Resource0 : 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 : ManagementGroup]
 Type                          : cluster
 Comment                       :
 [Resource0                    : ManagementIP]
  Type                         : fip
  Comment                      :
  IP Address                   : 10.0.0.10
[Group1 : failover1]
Type                           : failover
Comment                        : failover group1
 [Resource0 : fip1]
  Type                         : fip
  Comment                      : 10.0.0.11
  IP Address                   : 10.0.0.11
 [Resource1 : md1]
  Type                         : md
  Comment                      : I:
  Mirror Disk No.              : 1
  Drive Letter                 : I:
```

(continues on next page)

(continued from previous page)

```
  Mirror Disk Connect           : mdc1
[Group2 : failover2]
 Type                           : failover
 Comment                        : failover group2
 [Resource0 : fip2]
  Type                          : fip
  Comment                       : 10.0.0.12
  IP Address                    : 10.0.0.12
 [Resource1 : md2]
  Type : md
  Comment                       : J:
  Mirror Disk No.               : 2
  Drive Letter                  : J:
  Mirror Disk Connect           : mdc1
================================================================
```

Displaying only the 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 a monitor resource name is not specified, the configuration data of all the 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 ==================
[Monitor0 : fipw1]
Type : fipw
Comment : fip1
================================================================
```

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
================================================================
```

Displaying all cluster configuration data (-i option)

By specifying the -i option, you can display the configuration information that is shown when --cl, --sv, --hb, --fnc, --svg, --grp, --rsc, and --mon 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 more command, and pipe, or redirect the output in a file for the output.

Example of a command entry:

```
# clpstat -i
```

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, --fnc, --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
```

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 display after running the command:

```
==================== CLUSTER STATUS ======================
Cluster : cluster
  cluster           : Start cluster
<server>
 *server1...........: Online server1
   lankhb1          : Normal LAN Heartbeat
   lankhb2          : Normal LAN Heartbeat
   pingnp1          : Normal ping resolution
   forcestop1       : Normal Forced stop
  server2...........: Online server2
   lankhb1          : - LAN Heartbeat
   lankhb2          : - LAN Heartbeat
   pingnp1          : - ping resolution
   forcestop1       : - Forced stop
<group>
 ManagementGroup : Online Management Group
   current          : server1
   ManagementIP     : Online 10.0.0.10
 failover1..........: Online failover group1
   current          : server1
   fip1             : Online 10.0.0.11
   md1              : Online I:
   script1          : Online script resource1
 failover2..........: - failover group2
   current          : server2
   fip2             : - 10.0.0.12
   md2              : - J:
   script2          : - script resource2
<monitor>
   fipw1            : Online fip1
```

(continues on next page)

(continued from previous page)

```
   fipw2            : Online fip2
   ipw1             : Online ip monitor1
   mdw1             : Online md1
   mdw2             : Online md2
==========================================================
```

Information on each status is provided in "*Status Descriptions*".

9.3.1 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
	Caution	Heartbeat resource failure
	Isolated	Suspension (isolated)
	Online Pending	Now being started
	Offline Pending	Now being stopped
	Pending	Suspension (Network partition unsolved)
	Unknown	Status unknown
	-	Status unknown
Group map display Monitor resource status display	o	Starting
	s	Suspension (isolated)
	p	Now being started/stopped Network partition unsolved
	x	Offline Pending
	-	Status unknown

Heartbeat Resource

Function	Status	Description
Status display	Normal	Normal
	Caution	Failure (Some)
	Error	Failure (All)
	Not used	Not used
	Unknown	Status unknown
	-	Status unknown
Heartbeat resource status display	o	Able to communicate
	x	Unable to communicate
	-	Not used or status unknown

Network Partition Resolution Resource and Forced Stop Resource

Function	Status	Description
Status display	Normal	Normal
	Caution	Failure (Some)
	Error	Failure (All)
	Unused	Not used
	Unknown	Status unknown
	-	Status unknown
Network partition resolution resource / Forced stop resource 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

Continued on next page

Table 9.15 – continued from previous page

Function	Status	Description
	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)
	Unused	Not Used
	Unknown	Status unknown
	Normal (Dummy failure)	Normal (Dummy Failure)
	Caution (Dummy failure)	Error (Some) (Dummy Failure)
	Error (Dummy failure)	Error (All) (Dummy Failure)
Status display (--local) Monitor resource status display	Online	Started and normal
	Offline	Stopped
	Caution	Warning
	Suspend	Stopped temporarily
	Online Pending	Now being started
	Offline Pending	Now being stopped
	Online Failure	Error
	Offline Failure	Stopping failed
	Unused	Not used
	Unknown	Status unknown
	Online (Dummy failure)	Started (Dummy Failure)
	Offline (Dummy failure)	Stopped (Dummy Failure)
	Caution (Dummy failure)	Warning (Dummy Failure)
	Suspend (Dummy failure)	Stopped temporarily (Dummy Failure)
	Online Pending (Dummy failure)	Now being started (Dummy Failure)
	Offline Pending (Dummy failure)	Now being stopped (Dummy Failure)
	Online Failure (Dummy failure)	Starting failed (Dummy Failure)
	Offline Failure (Dummy failure)	Stopping failed (Dummy Failure)
	-	Status unknown

9.4 Operating the cluster (clpcl command)

The clpcl command operates a cluster

Command line:

clpcl -s [-a] [-h *hostname*]
clpcl -t [-a] [-h *hostname*] [-w *time-out*] [--apito *time-out*]
clpcl -r [-a] [-h *hostname*] [-w *time-out*] [--apito *time-out*]
clpcl --return [-h *hostname*] [--apito *time-out*]
clpcl --suspend [--force] [-w *time-out*] [--apito *time-out*]
clpcl --resume

Description
This command starts, stops, return, suspends, or resumes the EXPRESSCLUSTER service.

Option

-s
Starts the EXPRESSCLUSTER service.

-t
Stops the EXPRESSCLUSTER service.

-r
Restarts the EXPRESSCLUSTER service.

--return
Restores a server that is in the suspension (isolated) status to the normal status.

--suspend
Suspends the entire cluster

--resume
Resumes the entire cluster

-a
Executed the command on all servers

-h<host_name>
Makes a request to run the command to the server specified in *host_name*. Makes a processing request to the server on which this command runs (local server) if the -h option is omitted.

-w<time-out>

When -t, -r, or --suspend option is used, specify the wait time in seconds that the clpcl command waits for the EXPRESSCLUSTER service to be completely stopped or suspended.
When a time-out is not specified, it waits for unlimited time.
When "0 (zero)" is specified, it does not wait.
When the -w option is not specified, it waits for twice the heartbeat time-out (in seconds).

--force
When used with the --suspend option, forcefully suspends the cluster regardless of the status of all the servers in the cluster.

--apito <time-out>

Specify the time in seconds to wait for the EXPRESSCLUSTER service to be stopped, restarted, or suspended (internal communication timeout). A value between 1 to 9999 can be specified.

When the --apito option is not specified, the command waits for 3600 seconds.

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 a user with Administrator privileges.

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 that allows name resolution.

When you suspend the cluster, the EXPRESSCLUSTER service 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.

In starting and resuming the cluster, the IP addresses of cluster servers are tried to be connected in order of interconnect priority, then a successful route is used.

When you resume the cluster, use the clpstat command to see there is no activated server in the cluster.

Example of a command entry

Example 1: Activating the EXPRESSCLUSTER service in the local server

```
# clpcl -s
Command succeeded
```

Example 2: Activating the EXPRESSCLUSTER service 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 *server_name* : *Execution result*

Example 3: Activating the EXPRESSCLUSTER service in all servers

```
# clpcl -s -a
Start server0 : Command succeeded.
Start server1 : Performed startup processing to the active cluster␣
↪service.
```

When all the servers are activated, the display after running the command should look similar to above.

Start *server_name* : *Execution result*

Example 4: Stopping the EXPRESSCLUSTER service in all servers

```
# clpcl -t -a
Stop server0 : Command succeeded.
Stop server1 : Command succeeded.
```

When all the servers are stopped, the display after running the command should look similar to above. Stop *server_name* : *Execution result*.

When the stopping process fails, the display may be different from the example above depending on the process.

Wait for the stopping of all servers of the EXPRESSCLUSTER service.

`Error Messages`

Message	Cause/Solution
Log in as administrator.	Log in as a user with Administrator privileges.
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 service.	The stopping process has been executed to the stopped EXPRESSCLUSTER service.
Performed startup processing to the active cluster service.	The startup process has been executed to the activated EXPRESSCLUSTER service.
Command timeout.	The command timed out.
Failed to return the server. Check the status of failed server.	Failed to return the server. Check the status of the failed server.
Could not connect to the server. Check if the cluster service is active.	Check if the EXPRESSCLUSTER service 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.
Failed to obtain the service name.	Failed to obtain the service name.
Failed to operate the service.	Failed to operate the service.
Resumed the cluster service that is not suspended.	Resumed the EXPRESSCLUSTER service that is not suspended.
invalid server status.	Check if the EXPRESSCLUSTER service is activated.
Server is busy. Check if this command is already run.	This command may be run already. Check it.
Server is not active. Check if the cluster service is active.	Check if the EXPRESSCLUSTER service is activated.
There is one or more servers of which cluster service is active. If you want to perform resume, check if there is any server whose cluster service is active in the cluster.	When you execute the command to resume, check if there is no server in the cluster on which the EXPRESSCLUSTER service is activated.
All servers must be activated. When suspending the server, the cluster service need to be active on all servers in the cluster.	When you execute the command to suspend, the EXPRESSCLUSTER service 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 suspended.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid name of a server 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 on which the EXPRESSCLUSTER service has stopped in the cluster.
invalid parameter.	The value specified as a command parameter may be invalid.

Continued on next page

Table 9.17 – continued from previous page

Message	Cause/Solution
Internal communication timeout has occurred in the cluster server. If it occurs frequently, set the longer timeout.	A timeout occurred in the EXPRESSCLUSTER 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 process is executed to all servers, there is one or 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 if the memory or OS resource is sufficient.
Failed to shutdown the server.	Shutting down or rebooting the server failed.
Failed to get privilege.	Obtaining the privilege to shut down or reboot the server failed.

9.5 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 EXPRESSCLUSTER service and shuts down a server.

Option

None
Shuts down a server.

-r
Reboots the server.

-h `<host_name>`
Makes a processing request to the server specified in *host_name*. 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.

This command shuts down the server even when the EXPRESSCLUSTER service is stopped.

Notes
Run this command as a user with Administrator privileges.

This command cannot be executed while a group is being started or stopped.

Do not use this command while a cluster is suspended.

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 EXPRESSCLUSTER service 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)* ".

9.6 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 EXPRESSCLUSTER service in the entire cluster and shuts down all servers.

Option

None
Executes cluster shutdown.

-r
Executes cluster shutdown reboot.

-h <host_name>
Makes a processing request to the server specified in *host_name*. 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 a user with Administrator privileges.

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.

Error Message
See "*Operating the cluster (clpcl command)*".

9.7 Operating groups (clpgrp command)

The clpgrp command operates groups

Command line

clpgrp -s [*grpname*] [-h *hostname*] [-f] [--apito *time-out*]
clpgrp -t [*grpname*] [-h *hostname*] [-f] [--apito *time-out*]
clpgrp -m [*grpname]* [-h *hostname*] [-a *hostname*] [--apito *time-out*]
clpgrp -n <*grpname*>

Description

This command starts, deactivates or moves groups.

Option

-s [grpname]
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 [grpname]
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 [grpname]
Moves groups. When you specify the name of a group, only the specified group is moved. If no group name is specified, all the groups are moved.

-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 <grpname>
Displays the name of the server on which the group has been started.

--apito <time-out>

Specify the time in seconds to wait for groups to be started, stopped, or moved(internal communication timeout). A value between 1 to 9999 can be specified.
When the --apito option is not specified, the command waits for 3600 seconds.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as a user with Administrator privileges.

The EXPRESSCLUSTER service 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.

Moving a group by using the -m option is considered to have succeeded (the value 0 is returned), with the group start process started on the destination server; even so, be careful of a possible failure in resource activation there.

To judge from a returned value the result of the group start process on the destination server, move the group by executing the following command:

```
# 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 -> serve

1. Both groups are stopped.

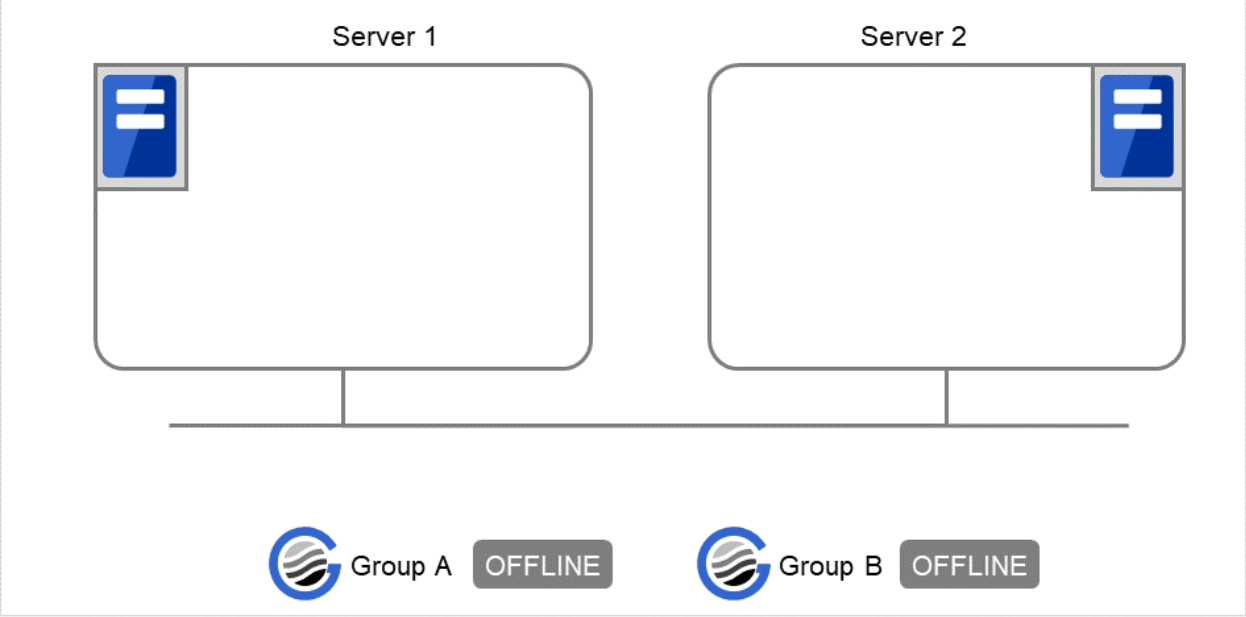


Fig. 9.1: Run-time state of the clpgrp command (1)

2. Run the following command on server1.

   ```
   # clpgrp -s groupA
   ```

   GroupA starts in server1.

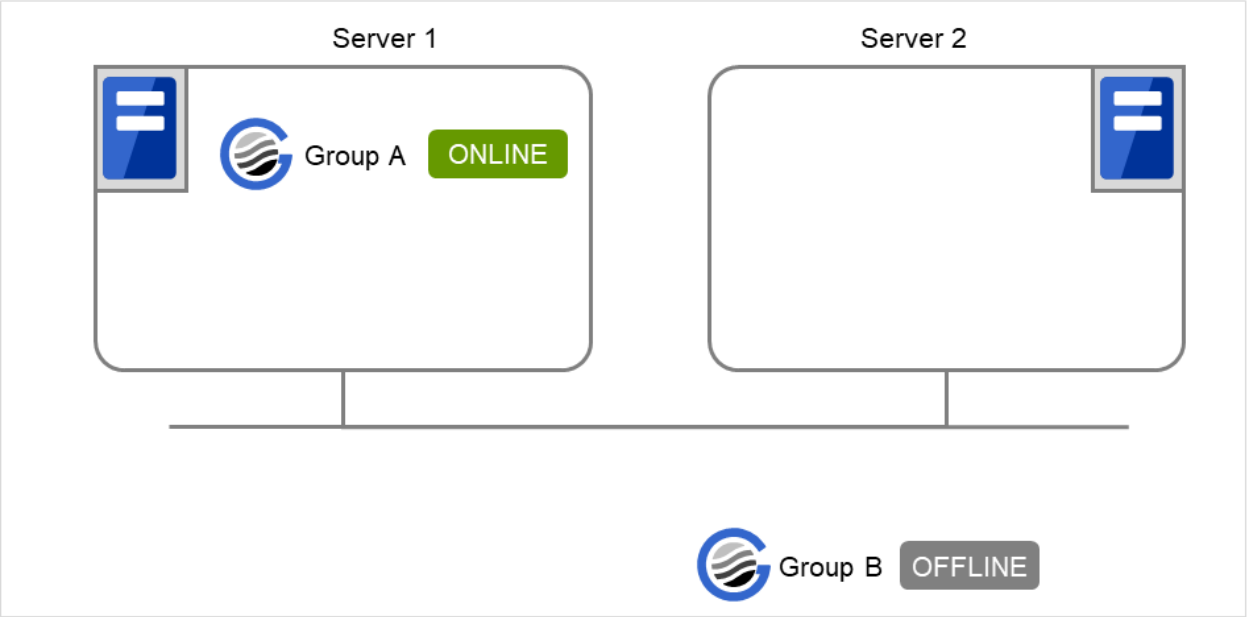


Fig. 9.2: Run-time state of the clpgrp command (2)

3. Run the following command in server1.

   ```
   # clpgrp -n groupA
   server1
   ```

   When the command is executed, groupA is running on server1. So, "server1" appears.

4. Run the following command in server2.

   ```
   # clpgrp -s
   ```

   All groups that are currently stopped but can be started start in server2.

Fig. 9.3: Run-time state of the clpgrp command (3)

5. Run the following command in server1

   ```
   # clpgrp -m groupA
   ```

   GroupA moves to server2.

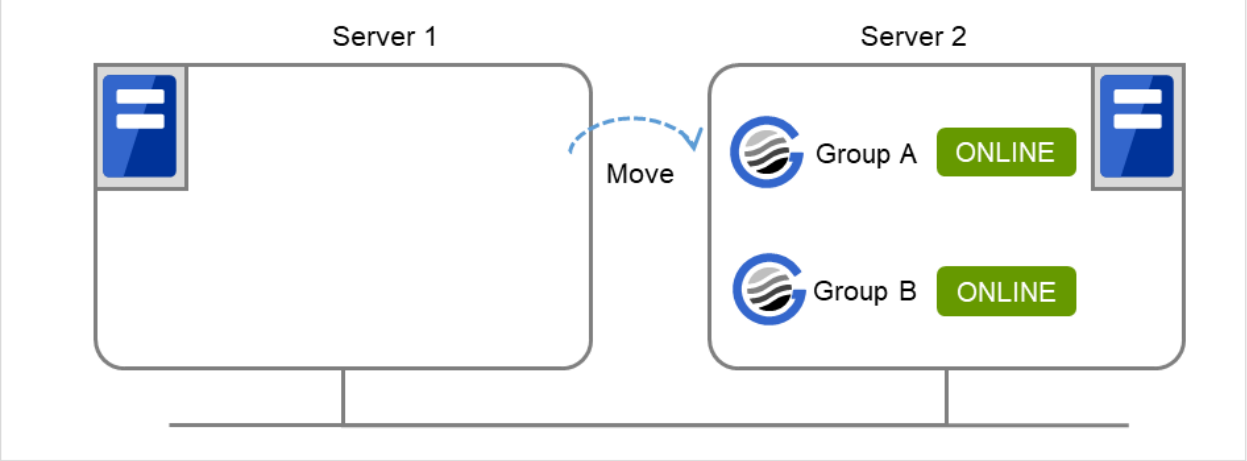


Fig. 9.4: Run-time state of the clpgrp command (4)

6. Run the following command in server1

   ```
   # clpgrp -t groupA -h server2
   ```

   GroupA stops.

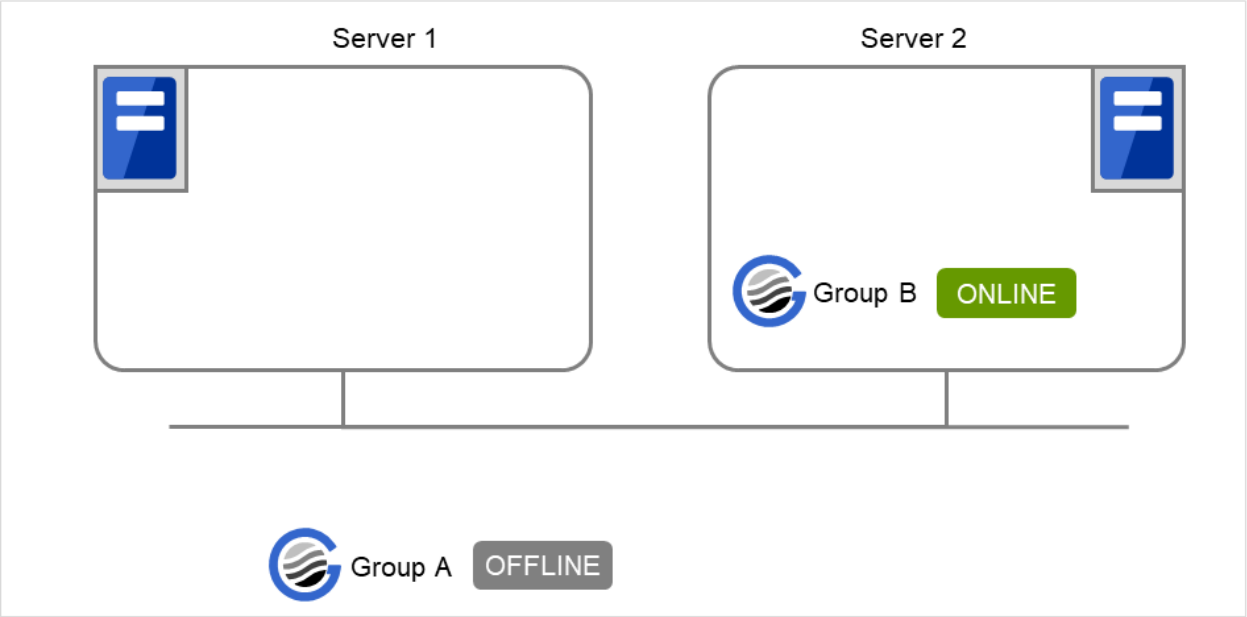


Fig. 9.5: Run-time state of the clpgrp command (5)

7. 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.

8. Add -f to the command you have run in Step 7 and execute it on server1.

   ```
   # clpgrp -t -f
   ```

   Groups which were started in server2 can be forcefully deactivated from server1.

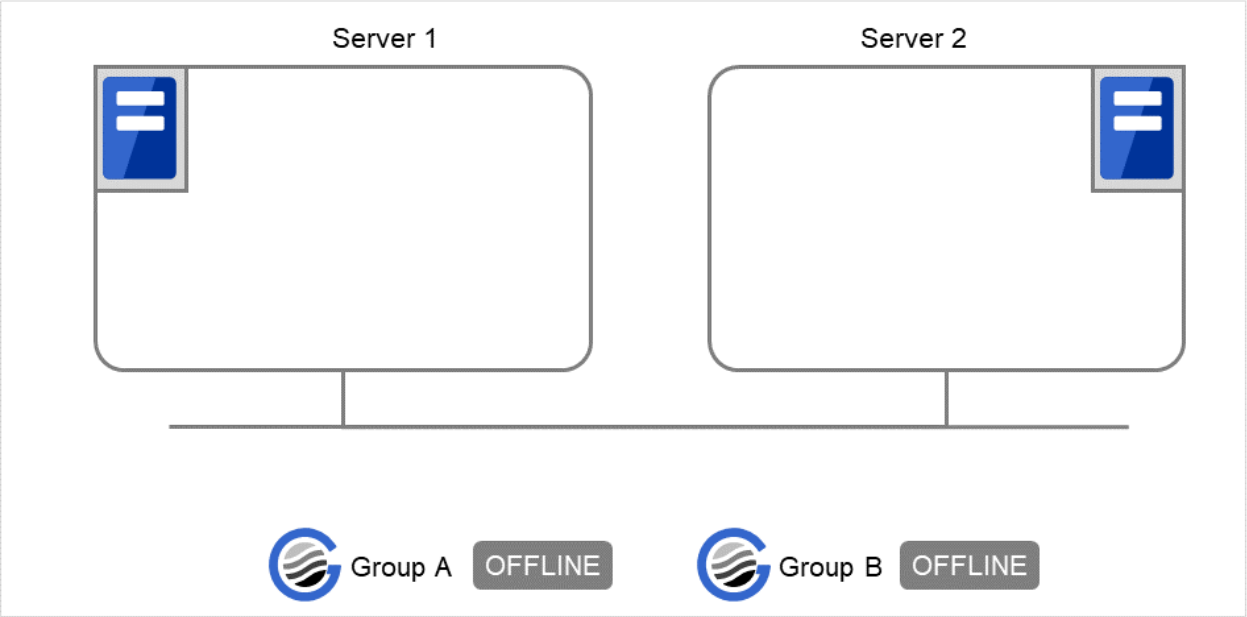


Fig. 9.6: Run-time state of the clpgrp command (6)

Error message

Message	Cause/Solution
Log in as administrator.	Log in as a user with Administrator privileges.
Invalid configuration data. 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 service is active.	Check if the EXPRESSCLUSTER service is operating.
Invalid server status. Check if the cluster service is active.	Check if the EXPRESSCLUSTER service is operating.
Server is not active. Check if the cluster service is active.	Check if the EXPRESSCLUSTER service is operating.
Invalid server name. Specify a valid server name in the cluster.	Specify the valid 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 on which the EXPRESSCLUSTER service 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 the longer timeout.	A time-out occurred in the EXPRESSCLUSTER internal communication. If time-out keeps occurring, set the internal communication time-out longer.

Continued on next page

Table 9.18 – continued from previous page

Message	Cause/Solution
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.	Server that starts and 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 timeout 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 stopped.	Check the status of the group by using the Cluster WebUI or the clpstat command.
Failed to start one or more resources. Check the status of group.	Check the status of group by using the Cluster WebUI or the clpstat command.
Failed to stop one or more 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.	The group is now being started or stopped. Wait for a while and try again.
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 isolated.	The server has been suspended. The server is rebooted after it went down.
Some invalid status. Check the status of cluster.	The status is invalid. Check the status of the cluster.
Log in as administrator.	Check if the memory or OS resource is sufficient.
Server is not in a condition to start group. 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. 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.

9.8 Collecting logs (clplogcc command)

The clplogcc command collects logs.

Command line

clplogcc [[-n *targetnode1* -n *targetnode2* .....]] [-t *collect_type*] [-o *path*] [--local] [--evt event_type ...]

Description

This command collects information including logs and the OS information by accessing the data transfer server.

Option

None

Collects logs in the cluster.

-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 "Specifying a event log type to collect (--evt option)".

-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

Collects logs on the local server without going through the data transfer server. The -n option cannot be specified at the same time.

--local

Collects logs on the local server without going through the data transfer server. The -n option cannot be specified at the same time.

--evt event_type

Specifies the type of the event log to be collected.

When this option is skipped, application logs, system logs and security logs will be collected.

If none is specified, the event log is not collected.

This option is enabled only when --local option is specified.

For details, see "Specifying a event log type to collect (--evt option)".

Return Value

0	Success
Other than 0	Failure

Remarks

Since log files are compressed by zip, decompress them using an appropriate application.

Notes

Run this command as a user with Administrator privileges.

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.

In executing this command, the IP addresses of cluster servers are tried to be connected in order of interconnect priority, then a successful route is used.

If this command times out, wait for a while and then execute it again.

Example of command execution

Example 1: Collecting logs from all servers in the cluster

```
# clplogcc

Please wait, now collecting..

server status result
------------------------------
server0 Completion Normal
server1 Completion Normal
```

The execution results of the server that collected logs are displayed.

Server name Progress Result

Execution Result

For this command, the following processes are displayed.

Steps in Process	Meaning
Preparing	Initializing
Connecting	Connecting to the server
Compressing	Compressing log files
Transmitting	Sending log files
Disconnecting	Disconnecting from the server
Completion	Finished collecting logs

The following results (server status) are displayed:

Result (server status)	Meaning
Normal	Completed successfully
Canceled	Canceled by the user
Invalid Parameters	Parameters are invalid
Compression Error	There was an error while compressing files
Timeout	Time-out occurred.
Busy	The server is busy.
No Free Space	No free space on the disk.
File I/O Error	There was a file I/O error.
Unknown Error	Failure caused by other errors

Error Message

Message	Cause/Solution
Log in as administrator.	Log in as a user with Administrator privileges.
Invalid option.	Specify a valid option.
Collect type must be specified 'type1' or 'type2' or 'type3' or 'type4' or 'type5' or 'type6'. Incorrect collection type is specified.	Invalid collection type is specified.

Continued on next page

Table 9.21 – continued from previous page

Message	Cause/Solution
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.
Failed to obtain properties.	Failed to obtain the properties.
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 name. Specify a valid server name in the cluster.	Specify the invalid server name in the cluster.
Failed to collect log.	Failed to collect logs.
Server is busy. Check if this command is already run.	This command may be run already. Check it.
Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resource is sufficient.

9.8.1 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	✓	✓	✓	n/a	n/a	n/a
2. event log	✓	✓	✓	✓	n/a	n/a
3. Windows error report	✓	✓	✓	✓	n/a	n/a
4. user dump	✓	✓	n/a	n/a	n/a	n/a
5. Diagnostics Report	✓	✓	n/a	n/a	n/a	n/a
6. Registry	✓	✓	✓	n/a	n/a	n/a
7. Script	✓	✓	✓	n/a	n/a	n/a
8. ESMPRO/AC and ESMPRO/UPSC Logs	✓	✓	✓	n/a	n/a	n/a
9. HA Logs	n/a	✓	n/a	n/a	n/a	n/a

Continued on next page

Table 9.22 – continued from previous page

	type1	type2	type3	type4	type5	type6
10. Mirror statistics information	n/a	n/a	n/a	n/a	✓	n/a
11. Cluster statistics information	n/a	n/a	n/a	n/a	n/a	✓
12. System statistics information	✓	✓	✓	n/a	n/a	✓

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.

Information to be collected by default

- Logs of each module in the EXPRESSCLUSTER Server
- Attribute information on each module (dir) in the EXPRESSCLUSTER Server
  - In bin
  - In cloud
  - In alert/bin, webmgr/bin
  - In %SystemRoot%\system32\drivers
- EXPRESSCLUSTER version information
- OS information
- update log
- License information
- Configuration file
- Policy file
- Cloud environment configuration directory
- Shared memory dump
- Local node status of EXPRESSCLUSTER (clpstat --local execution result)
- Host name and domain name information (hostname execution result)
- Network information (netstat execution result)
- IP routing table information (route print execution result)
- Process existing status (tasklist execution result)
- ipconfig (ipconfig execution result)
- Shared configuration of files (net share execution result)
- Session information (net session execution result)
- Windows firewall settings (netsh execution result)

- SNP (Scalable Networking Pack) setting (netsh execution result)
- Task scheduler settings (schtasks execution result)
- Usage status of the VSS shadow copy area (execution result of vssadmin list shadowstorage)
- Operation log of Cluster WebUI (see "Maintenance Guide" -> "The system maintenance information" -> "Function for outputting the operation log of Cluster WebUI")
- Operation log of API services (see "Maintenance Guide" -> "The system maintenance information" -> "Function for outputting an API service operation log file")
- AWS-related information

  Results of executing the following commands:

  - where aws
  - aws --version
  - aws configure list
  - aws ec2 describe-network-interfaces
  - aws ec2 describe-instance-attribute --attribute disableApiStop

  The following instance metadata:

  - ami-id
  - instance-type
  - availability-zone
  - region
- OCI-related information

  The following instance metadata:

  - image
  - shape
  - availabilityDomain
  - region
- Google Cloud-related information

  The following instance metadata:

  - image
  - vmSize
  - zone
- Azure-related information

  The following instance metadata:

  - imageReference
  - location
  - vmSize
  - zone

event log

- application log (Application.evtx)
- system log (System.evtx)
- security log (Security.evtx)

Windows error report

- ***.wer

User dump

- ***.*dmp

Diagnostics Report

- the result of running msinfo32.exe

Registry

- Registry information of the EXPRESSCLUSTER Server
  - HKLM\SOFTWARE\NEC\EXPRESSCLUSTER\Alert
  - HKLM\SOFTWARE\NEC\EXPRESSCLUSTER\MirrorList
  - HKLM \SOFTWARE\NEC\EXPRESSCLUSTER\RC
  - HKLM \SOFTWARE\NEC\EXPRESSCLUSTER\VCOM
  - registry information of diskfltr
- Registry information of OS
  - HKLM\SYSTEM\CurrentControlSet\Services\Disk
  - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\DOS Devices
  - HKLM\SYSTEM\MountedDevices
  - HKLM\SYSTEM\CurrentControlSet\Enum\SCSI
  - HKLM\SYSTEM\CurrentControlSet\Enum\STORAGE
  - HKLM\SYSTEM\CurrentControlSet\Services\symc8xx
  - HKLM\SYSTEM\CurrentControlSet\Control\FileSystem

Script

Start/stop script for a group that was created with the Cluster WebUI.

If you specify a user-defined script, it is not included in the log collection information. It must be collected separately.

ESMPRO/AC and ESMPRO/UPSC logs

Files collected by running the acupslog.exe command.

HA logs

- System resource information
- JVM monitor log
- System monitor log

Mirror statistics information

- Mirror statistics information

- In perf\disk

Cluster statistics information

- Cluster statistics information
  - In perf\cluster

System Resource statistics information

- System statistics information
  - In perf\system

9.8.2 Output paths of log files (-o option)

- Log file is named and be saved as "*server_name*-log.zip"
- Since log files are compressed by zip, decompress them by using an appropriate application.

If not specifying -o option

Logs are output in tmp of installation path.

When the -o option is specified:

If you run the command as follows, logs are located in the specified c:\tmp.

```
# clplogcc -o C:\tmp
```

9.8.3 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.

9.8.4 Specifying a event log type to collect (--evt option)

You can specify the type of the event log included in the information obtained at the log collection.

Specify one or more text strings that represent event log types as shown in the following table after --evt option.

Event log type	Character string to specify
Application log	app
System log	sys
Security log	sec
Not collected	none

Example) Collecting the system log and the security log

```
# clplogcc --local --evt sys sec
```

- This option is enabled only when the --local option is specified.

9.8.5 Collecting information when a failure occurs

When the following failure occurs, the information for analyzing the failure is collected.

- When the cluster service that forms the cluster fails due to termination by an internal status error.
- 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
- Information created by running a command
  - Host name and domain name information (hostname execution result)
  - Network information (netstat execution result)
  - Process existing status (tasklist execution result)
  - ipconfig (ipconfig execution result)
  - Shared configuration of files (net share execution result)
  - Session information (net session execution result)
  - Routing table information (route print execution result)
  - Service information (execution result of sc query type=service)
  - Shadow copy information (execution result of vssadmin list shadowstorage)

These are collected by default in the log collection. You do not need to collect them separately.

9.9 Creating a cluster and backing up configuration data (clpcfctrl command)

9.9.1 Creating a cluster (clpcfctrl --push)

The clpcfctrl --push command delivers cluster configuration data to servers.

Command line

clpcfctrl --push [-w] [-x <*path*>] [-h <*hostname*>|<*IP*>]
[-p <*portnumber*>] [--force]

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.

-x

Specify this option to deliver the configuration data that is in the specified directory.

-w

Displays that the graphic character code of the cluster configuration data file to be delivered is SJIS.
In general, it is not necessary to specify this option
You cannot specify -l and -w together. Specify either -l or -w.

-h

Specifies a server to which configuration data is delivered. Specify host name or IP address.
When this option is omitted, the default value will be used.
In general, it is not necessary to specify this option.

-p

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.

--force

Even if there is a server that has not started, the configuration data is delivered forcefully.

--nocheck

The configuration data is delivered without the checking operation that is required when applying a settings change to the cluster. To apply the delivered configuration data to the cluster, therefore, execute the required operation manually.

Return Value

0	Success
Other than 0	Failure

Remarks

To deliver the cluster configuration data file exported from Cluster WebUI, to cluster servers by executing the clpcfctrl --push command, follow these steps:

1. Start Cluster WebUI, then switch to **Config Mode**.
2. If necessary, change the cluster configuration in Cluster WebUI.
3. In Cluster WebUI, select **Export**, then export the cluster configuration data file (in zip format) to any folder.
4. In any folder accessible from the cluster servers, unzip the exported zip file.
5. On any of the cluster servers, start Command Prompt, then execute the clpcfctrl --push command.

Notes

Run this command as a user with Administrative authority.

In executing this command, the IP addresses of cluster servers are tried to be connected in order of interconnect priority, then a successful route is used.

Before uploading cluster configuration data with one or more servers removed, uninstall the EXPRESSCLUSTER Server on the servers that will be removed from the cluster configuration.

When delivering the cluster configuration data, the current cluster configuration data and the configuration data to be delivered are compared.

If there is any change in the configuration data, the following message output. Follow the instructions of the message to complete the delivery.

Message	Solution
Please stop the EXPRESSCLUSTER.	Stop the server.
Please suspend the EXPRESSCLUSTER	Suspend the server.
Please stop the following groups.	Stop the group of which setting has been changed.
Reboot of a cluster is necessary to reflect setting.	Shut down and reboot the cluster to apply the change of settings.
To apply the changes you made, restart the EXPRESSCLUSTER Web Alert service.	Restart the EXPRESSCLUSTER Web Alert service to apply the change of settings.
To apply the changes you made, restart the EXPRESSCLUSTER Manager service.	Restart the EXPRESSCLUSTER Manager service to apply the change of settings.
To apply the changes you made, restart the EXPRESSCLUSTER Information Base service.	Restart the EXPRESSCLUSTER Information Base service to apply the change of settings.
To apply the changes you made, restart the EXPRESSCLUSTER API service.	Restart the EXPRESSCLUSTER API service to apply the change of settings.
To apply the changes you made, restart the EXPRESSCLUSTER Node Manager service.	Restart the EXPRESSCLUSTER Node Manager service to apply the change of settings.
Start of a cluster is necessary to reflect setting.	This is the message displayed at the initial cluster configuration. Start the cluster.

The --nocheck option is used only for special purposes including a maintenance procedure. Do not use the --nocheck option for normal operations.

Example of command execution

Example 1: Generating a cluster from the floppy disk with the data saved by Cluster WebUI

```
# clpcfctrl --push -x C:\tmp\config
```

```
file delivery to server 10.0.0.11 success.
file delivery to server 10.0.0.12 success.

Command succeeded.(code:0)
```

Example 2: Delivering configuration data that was saved on the file system using Cluster WebUI

```
# clpcfctrl --push -x C:\tmp\config -h 10.0.0.11
Command succeeded.(code:0)
```

Error Message

Message	Cause/Solution
Command succeeded.	The command ran successfully.
Log in as administrator.	Log in as a user with Administrator privileges.
This command is already run.	This command has already been run.
invalid option.	This option is invalid. Check the option.
Invalid mode. Check if --push or --pull option is specified.	Check if --push is specified.
The target directory does not exist.	The specified directory is not found. Check if the specified directory is valid.
Invalid host name. Server specified by -h option is not included in the configuration	The server specified with -h is not included in configuration data. Check if the specified server name or IP address is correct.
Invalid type of file.	Check that the character code used for the configuration data is correct.
Failed to initialize the xml library. Check if memory or OS resources are sufficient. or Failed to load the configuration file. Check if memory or OS resources are sufficient. or Failed to change the configuration file. Check if memory or OS resources are sufficient.	Check if the memory or OS resources are sufficient.
Failed to load the all.pol file. Reinstall the RPM cluster.	Reinstall the EXPRESSCLUSTER Server.
Failed to load the cfctrl.pol file. Reinstall the RPM cluster.	Reinstall the EXPRESSCLUSTER Server.
Failed to get the install path. Reinstall the RPM cluster.	Reinstall the EXPRESSCLUSTER Server.
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 resources are sufficient.
Failed to connect to trnsv. Check if the other server is active.	Accessing the server has failed. Check if the other server has been started up.
Failed to get the list of node. Check if the server name or ip addresses are correct.	Check if the server name and the IP address of the configuration information are correctly set.

Continued on next page

Table 9.25 – continued from previous page

Message	Cause/Solution
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.
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 upload the configuration file. 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
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.
Canceled to deliver the configuration file since it failed to connect to one or more server. If you want to deliver the configuration file to servers that can be connected, run the command again with "-force" option.	Canceled the delivery of the configuration data. There are some servers that failed to connect. If you want to deliver the configuration data only to the server that can be connected, run the command again by using the --force option.
The directory "work" is not found. Reinstall the RPM.	Reinstall the EXPRESSCLUSTER Server.
Failed to make a working directory.	Check if the memory or OS resources are sufficient.
The directory does not exist. or This is not a directory. or The source file does not exist. or The source file is a directory. or The source directory does not exist. or The source file is not a directory.	Check if the path to the cluster configuration data file is correct.

Continued on next page

Table 9.25 – continued from previous page

Message	Cause/Solution
Failed to change the character code set (EUC to SJIS). or Failed to change the character code set (SJIS to EUC).	Check if the memory or OS resources are sufficient.
Failed to allocate memory. or Failed to change the directory. or Failed to make a directory. or Failed to remove the directory. or Failed to remove the file.	Check if the memory or OS resources are sufficient.
Failed to open the file.	Check if the path to the cluster configuration data file is correct.
Failed to read the file. or Failed to copy the file. or Failed to create the mutex. Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resources are sufficient.
Failed to check server property. Check if the server name or ip addresses are correct.	Check if the server name and the IP address of the configuration information are correctly set.
Please stop the following resources.	Stop the resource of which the configuration has been changed.
Failed to get server status.	Failed to acquire the server status. Check that the server is operating normally.
target does not exist.	The specified directory does not exist. Check that the directory is specified correctly.
connect to server succeeded.	Connected to the server successfully.
connect to server failed.	Failed to connect to the server. Check that the server has started.
connect to server failed. (please retry later)	Failed to connect to the server. Check that the server has started. Wait a short while and then retry.
clp.conf delivered.	Configuration data has already been delivered.
To apply the changes you made, reboot the cluster.	To apply the changes you made, restart the cluster.
To apply the changes you made, start the cluster service.	To apply the changes you made, start the cluster.

Continued on next page

Table 9.25 – continued from previous page

Message	Cause/Solution
Failed to deliver the configuration file. 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 apply the setting due to ongoing mirror recovery. After the mirror recovery is completed, execute the command again.	Failed to apply the setting due to ongoing mirror recovery. After the mirror recovery is completed, execute the command again.

9.9.2 Backing up the cluster configuration data

The clpcfctrl --pull command backups cluster configuration data.

Command line

clpcfctrl --pull [-w] [-x <*path*>] [-h <*hostname*>|<*IP*>]
[-p <portnumber>]

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.

-x

Specify this option when backing up configuration data in the specified directory.

-w

Save the configuration data with graphic character code, SJIS.

-h

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

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.

Return Value

0	Success
Other than 0	Failure

Remarks

To deliver the cluster configuration data file obtained by executing the clpcfctrl --pull command, from Cluster WebUI to cluster servers, follow these steps:

1. Execute the clpcfctrl --pull command to save the cluster configuration data file (in zip format) to any folder.
2. Unzip the zip file, select the clp.conf file and the scripts folder, and then create a zipped file (named freely).
3. Start Cluster WebUI, switch to **Config Mode**, and then click **Import** to import the file created in Step 2.
4. If necessary, change the cluster configuration in Cluster WebUI, then click **Apply the Configuration File**.

Notes

Run this command as a user with Administrator privileges.

In executing this command, the IP addresses of cluster servers are tried to be connected in order of interconnect priority, then a successful route is used.

Example of command execution

Example 1: Backing up configuration data into the specified directory

```
# clpcfctrl --pull -x C:\tmp\config
Command succeeded.(code:0)
```

Example 2: Backing up configuration data of the specified server into the specified directory

```
# clpcfctrl --pull -x C:\tmp\config -h 10.0.0.11
Command succeeded.(code:0)
```

Error Message

Message	Cause/Solution
Log in as administrator.	Log on as a user with Administrator privileges.
This command is already run.	This command has already been run.
invalid option.	The option is invalid. Check the option.
Invalid mode. Check if --push or --pull option is specified.	Check if --pull is specified.
Failed to initialize the xml library. Check if memory or OS resources are sufficient. or Failed to load the configuration file. Check if memory or OS resources are sufficient. or Failed to change the configuration file. Check if memory or OS resources are sufficient.	Check if the memory or OS resources are sufficient.
Failed to load the all.pol file. Reinstall the cluster.	Reinstall the EXPRESSCLUSTER Server.
Failed to load the cfctrl.pol file. Reinstall the cluster.	Reinstall the EXPRESSCLUSTER Server.
Failed to get the install path. Reinstall the cluster.	Reinstall the EXPRESSCLUSTER Server.
Failed to initialize the trncl library. Check if memory or OS resources are sufficient	Check if the memory or OS resources are sufficient.
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.
The directory "work" is not found. Reinstall the cluster.	Reinstall the EXPRESSCLUSTER Server.

Continued on next page

Table 9.26 – continued from previous page

Message	Cause/Solution
Failed to make a working directory. or The directory does not exist. or This is not a directory. or The source file does not exist. or The source file is a directory. or The source directory does not exist. or The source file is not a directory. or Failed to change the character code set (EUC to SJIS). or Failed to change the character code set (SJIS to EUC).	Check if the memory or OS resources are sufficient.

Continued on next page

Table 9.26 – continued from previous page

Message	Cause/Solution
Failed to allocate memory. or Failed to change the directory. or Failed to make a directory. or Failed to remove the directory. or Failed to remove the file. or Failed to open the file. or Failed to read the file. or Failed to write the file. or Failed to copy the file. or Failed to create the mutex. or Failed to copy the file. or Failed to create the mutex. or Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resources are sufficient.

9.10 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 the current time-out ratio or temporarily extends the various time-out values of the following on all servers in the cluster.

- Monitor resource
- Heartbeat resource
- Disk Agent
- Alert synchronous service
- WebManager service

Note that the following value is not supported.

- Kernel mode LAN heartbeat resources

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 shut down, 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 a user with Administrator privileges.

Make sure that the EXPRESSCLUSTER service 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.

This command does not support the time-out values of forced stop resources.

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 administrator.	Log on as a user with Administrator privileges.
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. ex) 2m, 3h, 4d	Set a valid extension period.
Set the extension period in a range less than the maximum extension period.	Set the extension period which does not exceed the maximum extension period.
Could not connect to the server. Check if the cluster service is active.	Check that the EXPRESSCLUSTER service is operating.

Continued on next page

Table 9.27 – continued from previous page

Message	Cause/Solution
Server is not active. Check if the cluster service is active.	Check that the EXPRESSCLUSTER service is operating.
Connection was lost. Check if there is a server where the cluster service is stopped in the cluster.	Check if there is any server in the cluster that the EXPRESSCLUSTER service stopped.
Invalid parameter.	The value specified as the 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 EXPRESSCLUSTER 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.	There is a server in which the processing has failed. Check the statuses of servers in the cluster. Run the command with all servers in the cluster activated.
Internal error. Check if memory or OS resources are sufficient.	Check if the memory or OS resources are sufficient.

9.11 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

Specifies a module type whose settings will be changed.

For types which can be specified, see the Type column, which shows information outputted by executing the command with no options specified.

-l

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.

-s

Specifies the size of a file for log output.

The unit is byte.

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 two log files. Therefore, it is necessary to have the disk space that is twice larger than what is specified by -s.

Notes

Run this command as a user with Administrator privileges.

To run this command, the EXPRESSCLUSTER Event service must be started.

Configuration change is effective only to servers on which this command was run.

Rebooting the server restores the settings to their pre-change values.

Displaying or changing the settings of the following hybrid-disk-related modules requires specifying the types of corresponding mirror-disk-related modules.

For more information, see the table of "Types that can be specified to the -t option".

- clphd.dll
- clphdctrl.exe
- clphdstat.exe
- clphdw.dll

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 administrator.	Log on as a user with Administrator privileges.
invalid option.	The option is invalid. Check the option.
Failed to change configuration. Check if the event service is running.	clpevent may not have been started.
invalid level	The specified level is invalid.
invalid size	The specified size is invalid.
Failed to initialize the xml library.Check if memory of OS resources are sufficient.	Check if the memory or OS resources are sufficient.
Failed to print current configuration.Check if the event service is running.	clpevent may not be started yet.

9.12 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.

Option

-i `[licensefile...]`
When a license file is specified, license information is acquired from the file for registration. You can specify multiple licenses. You can also specify a wildcard. 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[1][2]
End date	End date of valid period[1][2]
Status	Status of the license

Status	Explanation
valid	valid
invalid	invalid
unknown	unknown
inactive	Before valid period[1][2]
expired	After valid period[1][2]

When -a option not specified, 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.

[1] Displayed in the case of the fixed term license
[2] Displayed in the case of the license of 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...
This option, usually not used, is for reinstalling only some servers of a cluster in an environment where a fixed-term license is used.

Return Value

0	Normal termination
1	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 "Licensing" in "troubleshooting" in the "Installation and Configuration Guide".
2	Initialization error
4	Invalid option
7	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
```

(continues on next page)

(continued from previous page)

```
    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 deleting 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 Administrator user.

When you register a license, verify that the data transfer server is started up and a cluster has been generated for license synchronization.

In license synchronization, the IP addresses of cluster servers are tried to be connected in order of interconnect priority, then a successful route is used.

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	The number of processed licenses (success: %d, error: %d)
(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" in "the Installation and Configuration Guide" for information on cluster generation.
Log in as administrator.	Log on as the Administrator 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.
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.

Continued on next page

Table 9.32 – continued from previous page

Message	Cause/Solution
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. or Could not read 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.
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. or Failed to open the license. Check if the entered license information is correct.	Check to see if the entered license information is correct.
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.

9.13 Mirror-related commands

9.13.1 Displaying the mirror disk status (clpmdstat command)

The clpmdstat command displays the status and configuration information on mirror disk.

Command line

clpmdstat {-m|--mirror} *mirrordisk-alias*

clpmdstat {-a|--active} *mirrordisk-alias*

clpmdstat {-l|--config}

clpmdstat {-c|--connect} *mirrordisk-alias*

Description

This command displays various status on mirror disk and the configuration information on mirror disk resource.

Option

-m,--mirror
Displays mirror disk resource status.

-a,--active
Displays status of mirror disk resource activation.

-l,--config
Displays the configuration information on mirror disk resource.

-c,--connect
Displays the mirror disk connect status.

Parameter

mirrordisk-alias
Specifies a mirror disk resource name.

Return value

-m,--mirror

Return value	Classification	Status of mirror disk[3] on server with 1 specified as startup order[4]	Status of mirror disk[3] on server with 2 specified as startup order[4]
17	Success	GREEN	GREEN
20		GREEN	RED
22		GREEN	GRAY
34		YELLOW	YELLOW
51		ORANGE	ORANGE
54		ORANGE	GRAY
65		RED	GREEN
68		RED	RED
70		RED	GRAY
85		BLUE	BLUE
97		GRAY	GREEN

Continued on next page

Table 9.33 – continued from previous page

Return value	Classification	Status of mirror disk[3] on server with 1 specified as startup order[4]	Status of mirror disk[3] on server with 2 specified as startup order[4]
99		GRAY	ORANGE
100		GRAY	RED
102		GRAY	GRAY
Other than the above	Failure	-	-

-a,--active

Return value	Classification	Active status of mirror disk resource[5] on server with 1 specified as startup order[6]	Active status of mirror disk resource[5] on server with 2 specified as startup order[6]
17	Success	Inactive	Inactive
18		Inactive	Active
19		Inactive	Force Active
20		Inactive	Being stopped, communication error
33		Active	Inactive
34		Active	Active
35		Active	Force Active
36		Active	Being stopped, communication error
49		Force Active	Inactive
50		Force Active	Active
51		Force Active	Force Active
52		Force Active	Being stopped, communication error
65		Being stopped, communication error	Inactive
66		Being stopped, communication error	Active
67		Being stopped, communication error	Force Active
Other than the above	Failure	-	-

-l,--config

[3] See "*Display examples*" -> "Displaying the status of mirror disk resource" -> "Explanation of each item".
[4] Order of servers ready to be started. (See "*3. Group resource details*" -> "*Group properties*" -> "*Startup Server tab*".)
[5] See "*Display examples*" -> "Displaying active status of mirror disk resource" -> "Explanation of each item".
[6] Order of servers ready to be started. (See "*3. Group resource details*" -> "*Group properties*" -> "*Startup Server tab*".)

Return value	Classification
0	Success
Other than the above	Failure

-c,--connect

Return value	Classification	Status of the mirror disk connect
0	Success	Available for communication (all mirror disk connects are normal)[7]
1		Available for communication (some mirror disk connects are abnormal)[7]
2		Not available for communication
Other than the above	Failure	-

Notes

Run this command as a user with Administrator privileges.

In the case where the mirror disk resource is deactivated in the server on which the command is run, a warning message "Trying again to disconnect mirror disk" appears when the command is executed in the environment where processes other than EXPRESSCLUSTER access to the volume. (The command is executed successfully.)

Example of command display

Example of information display after running these commands are provided in the next section.

Error messages

Message	Cause/Solution
Invalid parameter.	The parameter is invalid. Check if there is any error in its format or parameter.
All servers are down.	Check that at least one server having the target mirror disk resource is operating, and then execute the command again.
Internal error. The error code is [error code].	Restart the local server.

[7] The return value does not reflect the usage status of any mirror disk connect.
To know the usage status, check the display.

Display examples

- Displaying the status of mirror disk resource

  When the -m or --mirror option is specified, the status of the specified mirror disk resource is displayed.

  There are two types of mirror disk resource status display depending on the mirror disk resource status.

  – When the mirror disk resource status is other than Recovering

```
Status: Abnormal

md1                     server1              server2
-------------------------------------------------------------
Mirror Color            GREEN                RED
Fast Copy               OK                   OK
Lastupdate Time         2021/08/16 18:24:10  --
Break Time              2021/08/16 18:24:01  --
Needed Copy Percent     1%                   0%
Volume Used Percent     64%                  --%
Volume Size             10240MB              10240MB

Server Name             DP Error             CP Error
-------------------------------------------------------------
server1                 NO ERROR             ERROR
server2                 NO ERROR             ERROR
```

Explanation of each item

Item	Description

Status	Status of mirror disk resource
	`Status Description`
	`Normal Normal`
	`Recovering Mirror is recovering`
	`Abnormal Abnormal`
	`No Construction Initial mirror construction is not done`
	`Uncertain Unknown status or undefined of new/old`

Mirror Color	Status of mirror disk on each server
	`Status Description`
	`GREEN Normal`
	`YELLOW Mirror is recovering`
	`ORANGE Undefined of new/old`
	`RED Abnormal`
	`BLUE Both disks are active`
	`GRAY Being stopped, Unknown status`

Continued on next page

Table 9.38 – continued from previous page

Item	Description

Fast Copy	Indicates whether differential copy is enabled
	`Status  Description`
	`----------------------------------`
	`OK      Differential copy is enabled`
	`NG      Differential copy is disabled`
	`UNKNOWN Status is unknown`
	`--      Differential copy is unnecessary`

Lastupdate Time	Time when the data was last updated on the server
Break Time	Time when mirror break occurred
Needed Copy Percent	Percentage of the amount of the volume to be copied again
Volume Used Percent	Percentage of volume usage
Volume size	The size of the volume

DP Error	Whether or not there is data partition I/O error in servers
	`Status   Description`
	`--------------------------------`
	`NO ERROR Normal`
	`ERROR    Abnormal (Unable to I/O)`
	`--       Unknown`

CP Error	Whether or not there is cluster partition I/O error in servers (Refer to "DP Error")

– When the mirror disk resource status is Recovering

```
Status: Recovering

md1                server1            server2
----------------------------------------------------------------
Mirror Color       YELLOW      ->     YELLOW
                              15%

Recovery Status
----------------------------------------------------------------
Used Time          00:00:21
Remain Time        00:01:59
```

Explanation of each item

Item	Description
Status	Status of mirror disk resource[8]

Continued on next page

Table 9.39 – continued from previous page

Item	Description
Mirror Color	Mirror disk status in servers[8] Copy direction of mirror recovery is shown with an arrow. -> : Copy from the left server to the right server Or <- : Copy from the right server to the left server Progress of copying is shown as xx%.
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.

- Displaying active status of mirror disk resource

  When the -a or --active option is specified, active status of the specified mirror disk resource is displayed.

```
Resource Name: md1

Server Name       Active Status
----------------------------------------
server1           Active
server2           Inactive
```

Explanation of each item

Item	Description
Resource Name	Mirror disk resource name
Active Status	Active Status Status Description Inactive Inactive Active Active Force Active Forced activation -- Unknown

- Displaying the configuration information on mirror disk resources

  When the -l or --config option is specified, configuration information on all mirror disk resources are displayed.

```
Resource Name: md1
Syncmode     : Sync

Config               server1           server2
-------------------------------------------------------------
Drive Letter         z                 z
Disk Size            10240MB           10240MB
```

Explanation of each item

[8] See "When the mirror disk resource status is other than Recovering" -> "Explanation of each item".

Item	Description
Resource Name	Mirror disk resource name
Syncmode	Synchronization mode
Drive Letter	Drive letter of the data partition
Disk Size	Data partition size

- Displaying the mirror disk connect status

  When the -c or --connect option is specified, the mirror disk connect status is displayed.

  An example of a two-node mirror disk resource is given below.

  – The resource is active on server1. (The currently used mirror disk connect has Priority1, and the next mirror disk connect to be connected has Priority2.)

```
Resource Name       : md1
Number of Connection: 2

Mirror Disk Connect    Priority1         Priority2
-------------------------------------------------------------
server1
  Address              10.0.10.11        10.0.20.11
  Status               Active            Standby
server2
  Address              10.0.10.12        10.0.20.12
  Status               Active            Standby
```

  – The resource is in the standby status on both servers. (There is no currently used mirror disk connect, and the next mirror disk connect to be connected has Priority1.)

```
Resource Name       : md1
Number of Connection: 2

Mirror Disk Connect    Priority1         Priority2
-------------------------------------------------------------
server1
  Address              10.0.10.11        10.0.20.11
  Status               Standby           Standby
server2
  Address              10.0.10.12        10.0.20.12
  Status               Standby           Standby
```

  – Only one mirror disk connect is set up. (The resource is active on server1.)

```
Resource Name       : md1
Number of Connection: 1

Mirror Disk Connect    Priority1         Priority2
-------------------------------------------------------------
server1
  Address              10.0.10.11        --
  Status               Active            --
server2
  Address              10.0.10.12        --
  Status               Active            --
```

  – server2 is in the error status. (The mirror disk connect status of server2 cannot be acquired, and the resource is active on server1.)

```
Resource Name       : md1
Number of Connection: 2

Mirror Disk Connect    Priority1          Priority2
-----------------------------------------------------------
server1
  Address              10.0.10.11         10.0.20.11
  Status               Error              Error
server2
  Address              10.0.10.12         10.0.20.12
  Status               Unknown            Unknown
```

Explanation of each item

Item	Description
Resource Name	Mirror disk resource name
Number of Connection	Number of mirror disk connects
Address	IP address of the mirror disk connect (primary and secondary) The values specified in the Cluster WebUI are referenced.
Status	Status of the mirror disk connect (primary and secondary) (Operation status and presence of any error such as a disconnection or connection error) String Status of the mirror disk connect Active Being used Standby Not used and on standby (There is no error and the connect is available for communication.) Error Not used and disconnected (There is an error and the connect is not available for communication.) Unknown Unknown -- No configuration data

9.13.2 Operating mirror disk resource (clpmdctrl command)

The clpmdctrl command operates mirror disk resources.

Command line

clpmdctrl {-a|--active} *mirrordisk-alias* [-n or -f]
clpmdctrl {-d|--deactive} *mirrordisk-alias*
clpmdctrl {-b|--break} *mirrordisk-alias* [-n or -f]
clpmdctrl {-f|--force} *mirrordisk-alias*
clpmdctrl {-r|--recovery} *mirrordisk-alias* [-a or -f or -vf]
clpmdctrl {-c|--cancel} *mirrordisk-alias*
clpmdctrl {-w|--rwait} *mirrordisk-alias* [-timeout *time*] [-rcancel]

clpmdctrl {-s|--mdcswitch} *mirrordisk-alias* [*priority-number*]
clpmdctrl {-p|--compress} [*mirrordisk-alias*]
clpmdctrl {-n|--nocompress} [*mirrordisk-alias*]
clpmdctrl {-z|--resize} *mirrordisk-alias partition-size* [-force]
clpmdctrl --updatekey *mirrordisk-alias*

Note: Make sure that the EXPRESSCLUSTER service has been stopped when you use the --active or --deactive option.

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" -> "Increasing the mirror disk size" .

Note: When you extend the data partition of the mirror disk resource by using --resize option, a sufficient amount of free space is required right after the data partition area.

Note: In updating an encryption key with the --updatekey option, follow the procedures specified in "Maintenance Guide" -> "The system maintenance information" -> "Updating data encryption key file of mirror/hybrid disk resources".

Description

This command allows operations such as mirror recovery and activating/deactivating a mirror disk resource.

Option

-a,--active

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.
When neither -n or -f is specified, the command behaves in the same way as when -n is specified.

-n(-a,--active)

Specifies normal activation for activation mode.
This option can be omitted.
This cannot be specified when -f is specified.

-f(-a,--active)

Specifies forced activation for activation mode.
This option can be omitted.
This cannot be specified when -n is specified.

-d,--deactive

Deactivates the activated mirror disk resource on the local server.

-b,--break

Stops mirroring of the mirror disk resource and makes the data status not to be the latest on the server where the command is executed.

The data is not synchronized until mirror recovery is completed even if writing on the mirror disk takes place.

When neither -n or -f is specified, the command behaves in the same way as when -n is specified.

-n(-b,--break)

Specifies the degeneration mode as normal degeneration.

In the case of normal degeneration, mirroring is intermitted and the server becomes not the latest status only when the mirroring is executed normally on the mirror disk.

This option can be omitted.

This cannot be specified when -f is specified.

-f(-b,--break)

Specifies the degeneration mode as forced degeneration mode.

In the case of forced degeneration, mirroring is intermitted and the server becomes not the latest status even if the mirroring target server status is abnormal or unknown.

This option can be omitted.

This cannot be specified when -n is specified.

-f,--force

Performs forced mirror recovery on the specified mirror disk resource.

-r,--recovery

Performs either full mirror recovery or differential mirror recovery for the specified mirror disk resource with the local server as the copy source.

If none of -a, -f, or -vf is specified, the command behaves in the same way as when -a is specified.

-a(-r,--recovery)

Automatically selects the recovery mode.

If the difference can be identified, differential copying is performed.

If differences cannot be identified, the command behaves in the same way as when -f is specified.

This option can be omitted.

This cannot be specified when -f or -vf is specified.

-f(-r,--recovery)

Copies all the used area of a volume if the used area can be identified.

Copies the entire area of a volume if the used area cannot be identified.

This option can be omitted.

This cannot be specified when -a or -vf is specified.

-vf(-r,--recovery)

Copies the entire area of a volume regardless of differences and the used area.

This option can be omitted.
This cannot be specified when -a or -f is specified.

-c,--cancel
Cancels mirror recovery.

-w,--rwait
Waits for the completion of the specified mirror disk resource mirror recovery.

-timeout(-w,--rwait)

Specifies the time of mirror recovery completion timeout (second).
This option can be omitted.
When this option is omitted, timeout is not executed and waits for the completion of mirror recovery.

-rcancel(-w,--rwait)

Intermits mirror recovery when waiting for the mirror recovery completion is timed out.
This option can be set when -timeout option is set.
When this option is omitted, the mirror recovery continues even after the timeout takes place.

-s,--mdcswitch

Switches between the primary and secondary mirror disk connects of the user-specified mirror disk resource.
If the priority number is omitted, the secondary mirror disk connect is switched to when the primary mirror disk connect is used at the time of command execution. When the secondary mirror disk connect is used, the primary mirror disk connect is switched to.
If the priority numbers are specified, the mirror disk connect that has the appropriate priority number is switched to.

-p,--compress

Temporarily enables mirror data compression for the specified mirror disk resource.
If the mirror disk resource name is omitted, mirror data compression is temporarily enabled for all mirror disk resources.

-n,--nocompress

Temporarily disables mirror data compression for the specified mirror disk resource.
If the mirror disk resource name is omitted, mirror data compression is temporarily disabled for all mirror disk resources.

-z,--resize

Extends the data partition size of mirror disk resource.
The extension is available only when the status of mirror disk resource is normal.

-force(-z,--resize)

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.

--updatekey

Updates the encryption key without stopping the resource.

The execution of this option, after completing the update of the encryption key files for both of the servers, updates the key for the encryption.

At this time, mirroring in progress is suspended. As required, execute mirror recovery after the execution.

Parameter

mirrordisk-alias
Specifies the mirror disk resource name.

time
Specifies the time of mirror recovery completion timeout (second).

priority-number
Specify the priority number (1 or 2).

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
Other than 0	Failure
101	Invalid parameter
102	Invalid status including the case when -w or --rwait option is specified and mirror recovery is intermitted by -rcancel.
103	Operations for the same resource are executed simultaneously from another server.
104	Operations for the same resource were executed simultaneously from the own server.
105	The copy destination server is down.
106	The server that command is executed does not have the target resource.
107	I/O error occurred on the cluster partition or on the data partition.
109	Waiting for the completion of mirror recovery of the target mirror disk is timed out (only when -w or --rwait -timeout option is specified).
110	Other errors
111	Failed in extending a mirror disk (only when the -z or --resize option is specified).
112	Failed in updating an encryption key (only when the --updatekey option is specified).
113	The encryption function is disabled (only when the --updatekey option is specified).
114	The encryption key file has not been updated (only when the --updatekey option is specified).
201	The status of the destination mirror disk connect is invalid (only when the -m or --mdcswitch option is specified).
202	Only one mirror disk connect is set up (only when the -m or --mdcswitch option is specified).
203	The remote server is down.

Remarks

This command returns control when the specified processing starts. Run the clpmdstat command to check the processing status.

Notes

This command must be executed by the user with administrator privilege.

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 mirror recovery that was suspended by selecting **Cancel**, use this command for forced mirror recovery.

Example of command execution

Example 1: When activating mirror disk resource md1

```
# clpmdctrl --active md1
Command succeeded.
```

Example 2: When deactivating mirror disk resource md1

```
# clpmdctrl --deactive md1
Command succeeded.
```

Example 3: When recovering mirror for mirror disk resource md1

```
# clpmdctrl --recovery md1
Command succeeded.
```

Error messages

Message	Cause/Solution
Invalid parameter.	The parameter is invalid. Check if there is any error in its format or parameter.
The status of [mirror disk resource name] is invalid.	Check the status and execute the command again.

Continued on next page

Table 9.43 – continued from previous page

Message	Cause/Solution
This command is already run in another server.	After finishing the command which is currently executed, execute the command again.
This command is already run in the local server.	After finishing the command which is currently executed, execute the command again.
[copy destination server name] is down.	Start the copy destination server to execute the command again.
[local server name] is not included in Servers that can run the Group of [mirror disk resource name].	Execute the command from the server where the target mirror disk resource can be started.
Disk error.	Check if there is not HW failure in the disk or disk path where cluster partition or data partition exists.
Mirror recovery of [mirror disk resource name] is timed out.	Check if the specified timeout time is appropriate, or if the disk I/O or communication delay is not occurring due to heavy load.
Internal error. The error code is [error code].	Restart the local server.
Standby mirror disk connect has invalid status.	Check the connection status of the mirror disk connect.
[mirror disk resource name] has only one mirror disk connect.	Make sure that more than one mirror disk connect is registered.
Other server downed.	Check the server operating status.
Resize the mirror disk([mirror disk resource name]) is failed.	Check that the status of mirror disk resource is normal. Check that there is a sufficient amount of free space right after the current data partition area.
Failed to update the encryption key.	Check if the key file exists in the configured key file full path on each server.
The encryption function is disabled.	The encryption key cannot be updated due to **Encrypt mirror communication** disabled on the specified mirror disk resource.
The same encryption key is already used.	Update the key file of each server to a new one and try again.
Automatic mirror recovery is disabled. Its manual resumption is required to resume mirroring.	The encryption key has been updated. The mirroring, however, is suspended. Mirror recovery must be performed manually due to disabled automatic mirror recovery.
Failed to resume the automatic mirror recovery. Its manual resumption is required to resume mirroring.	The encryption key has been updated. The mirroring, however, is suspended. Mirror recovery must be performed manually due to disabled automatic mirror recovery.

9.13.3 Tuning partition size (clpvolsz command)

The clpvolsz command enlarges and shrinks the disk partition size.

Command line

clpvolsz *drive-letter [size]*

Description

This command checks the sizes of data partitions mirrored by mirror disk resource. If the partitions are not of the same size, the command adjusts the sizes.

Parameter

drive-letter

Specify the drive letter of the target partition drive.

size

Specify the partition size by byte. If nothing is specified, the current size is displayed.

Return value

0	succeeded in displaying the size
1	succeeded in changing the size
2 or greater	abnormal

Notes

Run this command as a user with Administrator privileges.

You cannot extend the partition size by this command.

Shrinking the partition size by using this command may cause the change of the drive latter. After shrinking the partition size, make sure to use Disk Management. (Navigate from Control Panel to Administrative Tools, Computer Management , Disk Management) to rescan the disk and check the drive letter and configure as necessary.

When the target partition has been registered as data partition/cluster partition in the cluster configuration information of the mirror disk resource, delete the mirror disk resource before shrinking the partition size and register again after shrinking and reconfiguration of drive letter.

The partition size is coordinated by MBR. Typically, it is a multiple of 512 bytes .

Example of command execution

Example 1 : When checking the Z drive size

```
# clpvolsz z:
Drive <z:> 8,587,160,064
```

Example 2: When shrinking the Z drive size to 8,587,159,552Byte

```
# clpvolsz z: 8587159552
Drive <z:> 8,587,160,064 -> 8,587,159,552
Execute it? [Y/N] ->y
SUCCESS
```

Error messages

Message	Causes/Solution
ERROR:invalid parameter.	The parameter is incorrect. Check the number of arguments and formats are set correctly.
ERROR:larger than partition size.	The value larger than the current partition size is set. Specify a smaller value.
ERROR:drive not found.	The specified drive is not found. Check if you have specified the right drive.
ERROR:drive open failed.	The specified drive cannot be opened. Check if the drive can be accessed.
ERROR:partition not found.	The partition number on the specified drive cannot be found. Check if you have checked the right driver.
ERROR:partition size zero.	The partition size of the specified server is 0. Check if the target partition is a basic volume.
ERROR:device layout info.	Acquiring disk partition configuration information has failed. Check if the target partition is a basic volume.
ERROR:device geometry info.	Acquiring the disk geometry information has failed. Check if the disk device is working properly.
ERROR:device no info.	Acquiring Device No. / Partition No has failed. Check the target partition is a basic volume.
ERROR:set device info.	Configuration of partition information has failed on the disk. Check if writing to disks is not prohibited.
ERROR:memory alloc error.	Reserving the resource has failed. Check if the memory or OS resource is enough.

9.13.4 Controlling disk access (clpvolctrl command)

Accesses a volume.

Command line

clpvolctrl {-ol--open} *drive_name*
clpvolctrl {-cl--close} *drive_name*
clpvolctrl {-vl--view} [*drive_name]*
clpvolctrl --view

Description

Accesses a disk volume under an HBA for which filtering is set up.

Note: The operation and display by this command does not apply to a volume registered as a mirror disk resource or a hybrid disk resource.

Option

-o, --open

Permits access to a volume.
Specify the drive name of the volume to which you want to permit access.

-c, --close

Restricts access to a volume.

Specify the drive name of the volume to which you want to restrict access.

-v, --view

Displays the status of access to a volume.

Specify the drive letter of the volume whose access status you want to display.

- When a drive letter is specified

  The status of access to the specified volume is displayed.

- When a drive letter is not specified (default)

  The command displays the access status of all volumes not registered as resources on a disk that belongs to the server executing the command and that is connected to an HBA for which filtering is set up.

Parameter

drive_name

Specify the drive letter of the target volume.

Return value

0	The command is successfully executed.
101	Invalid Parameters
102	The target volume is already registered as a resource.
103	Access to the target volume is already permitted (only when the -o or --open option is used).
104	Access to the target volume is already restricted (only when the -c or --close option is used).
200	Other errors

Notes

This command must be executed by a user with the administrator privilege.

Example of command execution

Example 1: This example shows how to permit access to a volume:

```
#clpvolctrl --open z:
Command succeeded.
```

Example 2: This example shows how to restrict access to a volume:

```
# clpvolctrl --close z:
Command succeeded.
```

Example 3: The examples below show how to display the status of access to a volume.

a) When a drive letter is specified:

```
# clpvolctrl --view z:
Drive Name Access Status
---------------------------------------
z open
```

b) When a drive letter is not specified:

```
# clpvolctrl --view:
Drive Name Access Status
-------------------------------------
w open
x close
y close
```

```
z open
```

Error messages

Message	Causes/Solution
Invalid parameter.	Check if there is any error in its format or parameter.
[drive name]: is a volume registered as a resource.	Check whether a group resource is using the specified drive.
Access to [drive name]: is already permitted.	The command has been executed with the ?o or --open option for a drive to which access is already permitted.
Access to [drive name]: is already restricted.	The command has been executed with the ?c or --close option for a drive to which access is already prohibited.
Internal error. The error code is [error code].	Restart the local server.

9.13.5 Creating a key file for encrypting communication data (clpkeygen command)

Creates a key file for encrypting communication data.

Command line

clpkeygen *key-bit-length file-name*

Description

Creates a key file for encrypting the data passing through mirror disk connects.

Option

None

Parameter

key-bit-length

Specifies a bit length for an encryption key. Only 128, 192, or 256 bits can be specified for a length of an encryption key.

file-name

Specifies a file name created for the encryption.

Return value

0	Command succeeded.
1	Invalid parameter
2 to 12	Failed in creating an encryption key.
13, 14	Failed in writing an encryption key to a file.

Notes

This command randomly creates a different key file for each execution.

When using a key file for the encryption, copy the file, which is created by the single execution, to each server.

Example of command execution

E.g., creating a key file of 256 bits in length:

```
# clpkeygen 256 keyfile.bin
```

Error messages

Message	Cause/Solution
Invalid option.	The parameter is invalid. Check if the number of arguments or formats are set correctly.
Internal error.(code=[error code]): Check if memory or OS resources are sufficient.	Check if the memory or OS resources are sufficient.
Internal error.(code=[error code] status=[NTSTATUS]) Internal error.(code=[error code])	An error occurs in the OS. Restart the server, or execute on another server.
Failed to open file.(code=[error code] status=[NTSTATUS]): Move or delete file, or Check access right is valid.	Check if you have the privilege of writing to a directory where a key file is created.
Failed to write file.(code=[error code] status=[NTSTATUS]): Check if disk space is sufficient.	Check if there is sufficient free space in a directory where a key file is created.

9.13.6 Operating snapshot backup of hybrid disk resource (clphdsnapshot command)

The clphdsnapshot is used for operating hybrid disk resource snapshot.

Command line

clphdsnapshot {-o|--open} *hybriddisk-alias*
clphdsnapshot {-c|--close} *hybriddisk-alias*

Description

This command interrupts the mirroring of hybrid disk resource and cancels the data partition access restriction to allow collection of snapshot backup, and then resumes ordinary status by resuming mirroring.

Option

-o, --open
Interrupts mirroring and allows collecting the snapshot backups on the server on which the command is executed by canceling the data partition access restriction, and then resumes mirroring. When the auto mirror recovery is set to be enabled, this setting is made to disable temporarily.

-c, --close
Restricts access to the data partition. If the auto mirror recovery is set to be enabled, the disablement is canceled and then, mirroring is resumed.

Parameter

hybriddisk-alias
Specifies the hybrid disk resource name.

Return Value

0	The command is successfully executed.
1	Invalid parameter.
2	The target resource is not mirrored (only when using the -o or --open option).
3	The target resource is already in the snapshot status on other server, or forcibly activated (only when using the -o or --open option.).
4	The target resource is already in the snapshot status (only when using the -o or --open option).
5	The target resource is not in the snapshot status (only when using the -c or --close option).
6	The target resource is now on mirror recovery.
7	The target resource does not exist in local server.
8	The command is executed on the active server group.
9	Other errors

Notes

This command must be executed by the user with administrator privilege.

This command should be executed on one of the standby server group which works as a copy destination of mirroring for the active hybrid disk resource that is properly mirrored. This command cannot be executed on a server in active server group (i.e., server in the same group as the server whose resources are activated).

When mirroring is interrupted using this command, note that the data at the mirroring copy destination does not necessarily have integrity as NTFS or application data, depending on the timing of the mirroring.

Example of command execution

The following shows how backup of the Z drive which is mirrored at the hybrid disk resource hd_Z is collected.

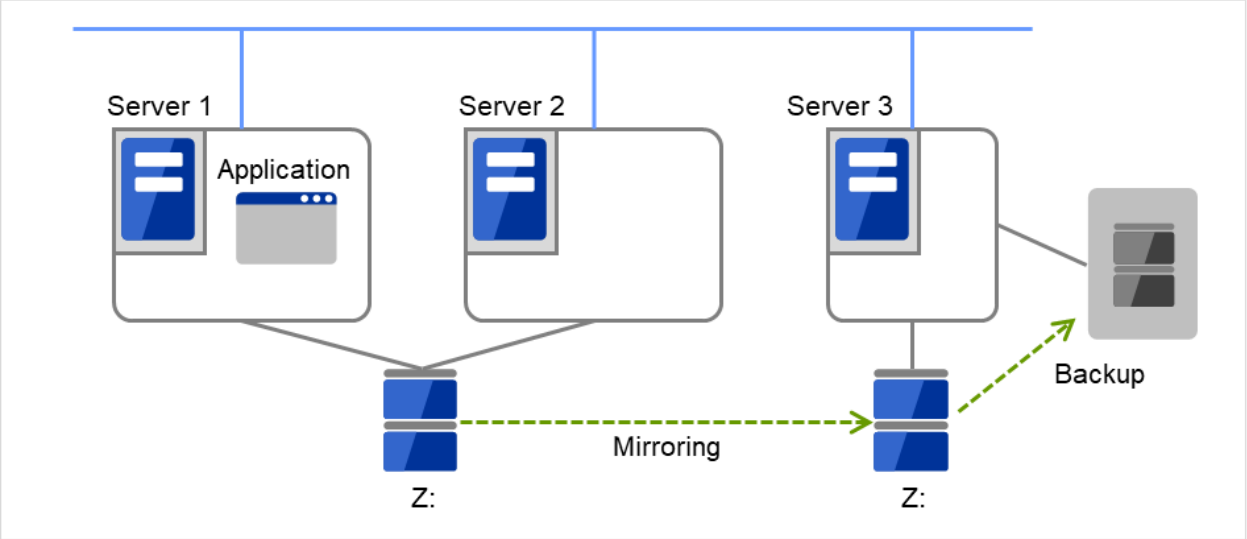


Fig. 9.7: Backup with a hybrid configuration

1. Execute the command below on the server 3 in the standby server group.

```
# clphdsnapshot --open hd_Z
Command succeeded.
```

2. Collect backup of the Z drive at the server 3 by using the backup tool.
3. Execute the command below on the server 3.

```
# clphdsnapshot --close hd_Z
Command succeeded.
```

4. When the auto mirror recovery is set to be disabled, run the mirror recovery manually.

Error messages

Message	Cause/Solution
Invalid parameter.	The parameter is invalid. Check if there is any error in its format or parameter.
[hybrid disk resource name] is not mirroring, or not active.	Snapshot backup cannot be performed on a hybrid disk resource which is deactivated or is not mirrored. Try again after activating the resource on another server group and while the mirroring is performed.
[hybrid disk resource name] is busy on [server name].	Check that the target resource is already in the snapshot status on another server in the same server group, or is not forcefully activated.
[hybrid disk resource name] has already opened.	The command is executed by specifying the -o or --open option for the resource that is already been in the snapshot status. Check the execution procedures.
[hybrid disk resource name] is not open.	The command is executed with the -c or --close option for the resource that is not in snapshot status by the -o or --open option. Make sure that the command with the -o or --open option has been executed successfully.
[hybrid disk resource name] is copying.	A snapshot backup cannot be performed for the hybrid disk resource in the process of mirror recovery. Try again after the mirror recovery has been completed.
[server name] is not available to [hybrid disk resource name].	Snapshot backups cannot be collected on a server on which the target resource cannot be activated. Execute it on a server on which the failover group containing this resource can be started.
Don't execute at active server group.	Snap shot back cannot be performed on a hybrid disk resource that is already activated in another server in the same server group. Execute it on a server in the standby server group.
Internal error. The error code is [error code].	Check the status of the cluster partition/data partition of the target resource. Make sure that memory or OS resource is sufficient.

9.13.7 Displaying the hybrid disk status (clphdstat command)

The clphdstat command displays the status and configuration information on hybrid disk.

Command line

clphdstat {-m|--mirror} *hybriddisk-alias*
clphdstat {-a|--active} *hybriddisk-alias*
clphdstat {-l|--config}
clphdstat {-c|--connect} *hybriddisk -alias*

Description

This command displays various status on hybrid disk and the configuration information on hybrid disk resource.

Option

-m, --mirror
Displays the status of hybrid disk resource.

-a, --active
Displays the activation status of hybrid disk resource.

-l, --config
Displays the configuration information on hybrid disk resource.

-c, --connect
Displays the mirror disk connect status.

Parameter

hybriddisk-alias
Specifies the hybrid disk resource name.

Return Value

-m, --mirror

Return value	Classification	Status of hybrid disk[9] on server group with 1 specified as startup order[10]	Status of hybrid disk[9] on server group with 2 specified as startup order[10]
17	Success	GREEN	GREEN
20		GREEN	RED
22		GREEN	GRAY
34		YELLOW	YELLOW
51		ORANGE	ORANGE
54		ORANGE	GRAY
65		RED	GREEN
68		RED	RED
70		RED	GRAY
85		BLUE	BLUE
97		GRAY	GREEN
99		GRAY	ORANGE
100		GRAY	RED
102		GRAY	GRAY
Other than the above	Failure	-	-

-a,--active

[9] See "*Display examples*" -> "Displaying the status of hybrid disk resource" -> "Explanation of each item".
[10] Order of server groups ready to be started. (See "*3. Group resource details*" -> "*Group properties*" -> "*Startup Server tab*".)

Return value	Classification	Active status of hybrid disk resource[11] on server group with 1 specified as startup order[12]	Active status of hybrid disk resource[11] on server group with 2 specified as startup order[12]
17	Success	Inactive	Inactive
18		Inactive	Active
19		Inactive	Force Active
20		Inactive	Being stopped, communication error
33		Active	Inactive
34		Active	Active
35		Active	Force Active
36		Active	Being stopped, communication error
49		Force Active	Inactive
50		Force Active	Active
51		Force Active	Force Active
52		Force Active	Being stopped, communication error
65		Being stopped, communication error	Inactive
66		Being stopped, communication error	Active
67		Being stopped, communication error	Force Active
Other than the above	Failure	-	-

For details on return values other than the above, see "*Displaying the mirror disk status (clpmdstat command)*" -> "Return value".

Notes

This command must be executed by the user with administrator privilege.

In the case where the hybrid disk resource is deactivated in the server on which the command is run, a warning message "Trying again to disconnect hybrid disk" appears when the command is executed in the environment where processes other than EXPRESSCLUSTER access to the volume. (The command is executed successfully.)

Example of command display

Examples of information displayed after running these commands are provided in the next section.

Error messages

[11] See "*Display examples*" -> "Displaying active status of hybrid disk resource" -> "Explanation of each item".
[12] Order of server groups ready to be started. (See "*3. Group resource details*" -> "*Group properties*" -> "*Startup Server tab*".)

Message	Cause/Solution
Invalid parameter.	The parameter is invalid. Check if there is any error in its format or parameter.
All servers are down.	Check that at least one server having the target hybrid disk resource is operating, and then execute the command again.
Internal error. The error code is [error code].	Restart the local server.

Display examples

- Displaying the status of hybrid disk resource

  When the -m or --mirror option is specified, the status of the specified hybrid disk resource is displayed.

  There are two types of hybrid disk resource status display depending on the hybrid disk resource status.

  - When the hybrid disk resource status is other than Recovering

```
Status: Abnormal

hd1                 svg01                svg02
-------------------------------------------------------
Mirror Color        GREEN                RED
Fast Copy           OK                   OK
Lastupdate Time     2021/08/17 15:50:27  --
Break Time          2021/08/17 15:44:35  --
Needed Copy Percent 1%                   0%
Volume Used Percent 67%                  --%
Volume Size         10240MB              10240MB
Disk Error          NO ERROR             ERROR

Server Name         DP Error             CP Error
-------------------------------------------------------
server1             NO ERROR             NO ERROR
server2             NO ERROR             NO ERROR
server3             NO ERROR             ERROR
server4             NO ERROR             ERROR
```

Explanation of each item

Item	Description

Status	Hybrid disk resource status
	`Status Description`
	`---------- ----------`
	`Normal Normal`
	`Recovering Mirror is being recovered`
	`Abnormal Abnormal`
	`No Construction Mirror initial construction has not been performed`
	`Uncertain Unknown status or undefined of new/old`

Continued on next page

Table 9.52 – continued from previous page

Item	Description

Mirror Color	Hybrid disk status in each server
	`Status Description`
	`------------------------------`
	`GREEN  Normal`
	`YELLOW Mirror is being recovered`
	`ORANGE Undefined of new/old`
	`RED    Abnormal`
	`BLUE   Both systems are active`
	`GRAY   Stopped or Unknown`

Fast Copy	Indicates whether differential copy is enabled
	`Status  Description`
	`-----------------------------------`
	`OK      Differential copy is enabled`
	`NG      Differential copy is disabled`
	`UNKNOWN Status is unknown`
	`--      Differential copy is unnecessary`

Lastupdate Time	Time when the data was last updated on the server
Break Time	Time when mirror break occurred
Needed Copy Percent	Percentage of the amount of the volume to be copied again
Volume Used Percent	Percentage of volume usage
Volume Size	The size of the volume

Disk Error	Disk I/O status
	`Status   Description`
	`---------------------------------`
	`NO ERROR Normal`
	`ERROR    Abnormal (Unable to I/O)`
	`--       Unknown`

DP Error	Whether or not there is data partition I/O error in servers (See "Disk Error")
CP Error	Whether or not there is cluster partition I/O error in servers (See "Disk Error")

– When the hybrid disk resource status is Recovering

```
Status: Recovering

hd1                svg01              svg02
-------------------------------------------------------------
Mirror Color       YELLOW      ->     YELLOW
                              15%

Recovery Status
-------------------------------------------------------------
```

(continues on next page)

(continued from previous page)

```
Source Server      server1
Destination Server server3
Used Time          00:00:21
Remain Time        00:01:59
```

Explanation of each item

Item	Description
Status	Hybrid disk resource status[13]
Mirror Color	Hybrid disk status in servers[13] Copy direction of mirror recovery is shown with an arrow. -> : Copy from the left server group to the right server group Or <- : Copy from the right server group to the left server group Progress of copying is shown as xx%.
Source Server	Copy source server name
Destination Server	Copy destination server name
Used Time	Time passed since copying started
Remain Time	Estimated time required to complete copying Because it is estimated from the copy rate of the finished part, the value may vary due to load status of the servers or other factors.

- Displaying active status of hybrid disk resource

  When the -a or --active option is specified, active status of the specified hybrid disk resource is displayed.

```
Resource Name: hd1

Server Name       Active Status      Current Server
------------------------------------------------------------
svg01
  server1         Active             CURRENT
  server2         Inactive           --
svg02
  server3         Force Active       CURRENT
  server4         Inactive           --
```

Explanation of each item

Item	Description
Resource Name	Hybrid disk resource name

Continued on next page

[13] See "When the hybrid disk resource status is other than Recovering" -> "Explanation of each item".

Table 9.54 – continued from previous page

Item	Description

Active Status	Active Status
	`Status Description`
	`------ -----------`
	`Inactive Inactive`
	`Active Active`
	`Force Active Forced activation`
	`-- Unknown`

Current Server	Current Server
	`Status Description`
	`------ -----------`
	`CURRENT Current server`
	`-- Non-current server`

- Displaying the configuration information on hybrid disk resources

  When the -l or --config option is specified, configuration information on all hybrid disk resources are displayed.

```
Resource Name: hd1
Syncmode     : Sync

Config              svg01           svg02
-------------------------------------------------------------
Drive Letter        z               z
Disk Size           10240MB         10240MB
Server Name         server1         server3
                    server2         server4
```

Explanation of each item

Item	Description
Resource Name	Hybrid disk resource name
Syncmode	Synchronization mode
Drive Letter	Drive letter of the data partition
Disk Size	Data partition size
Server Name	Member server of each server group

- Displaying the mirror disk connect status

  When the -c or --connect option is specified, the mirror disk connect status is displayed.

  An example of a four-node hybrid disk resource is given below.

  [Cluster configuration]

  Four servers (server1 - server4)
  Two server groups (svg01 and svg02)
  Servers registered for svg01: server1 and server2
  Servers registered for svg02: server3 and server4
  One hybrid disk resource (hd1)

[Cluster status]

- Hybrid disk resource hd1 is active on server1.
- Server group svg01 is using a priority 1 mirror disk connect.
- Server group svg02 is using a priority 2 mirror disk connect.

```
Resource Name       : hd1
Number of Connection: 2

Mirror Disk Connect    Priority1        Priority2
-------------------------------------------------------------
<svg01>
server1
  Address              10.0.10.11       10.0.20.11
  Status               Active           Standby
server2
  Address              10.0.10.12       10.0.20.12
  Status               Error            Standby

<svg02>
server3
  Address              10.0.10.21       10.0.20.21
  Status               Standby          Active
server4
  Address              10.0.10.22       10.0.20.22
  Status               Standby          Standby
```

Explanation of each item

Item	Description
Resource Name	Hybrid disk resource name
Number of Connection	Number of mirror disk connects
Address	IP address of the mirror disk connect (primary and secondary) The values set in the Cluster WebUI are referenced.

Continued on next page

Table 9.56 – continued from previous page

Item	Description
Status	Status of the mirror disk connect (primary and secondary) (Operation status and presence of any error such as disconnection or connection error) String Status of mirror disk connect ---------- Active Being used Standby Not used and on standby (There is no error and the connect is available for communication.) Error Not used and disconnected (There is an error and the connect is not available for communication.) Unknown Unknown -- No configuration data

9.13.8 Operating hybrid disk resource (clphdctrl command)

The clphdctrl command operates hybrid disk resource.

Command line

clphdctrl {-a|--active} *hybriddisk-alias* [-n or -f]
clphdctrl {-d|--deactive} *hybriddisk-alias*
clphdctrl {-b|--break} *hybriddisk-alias* [-n or -f]
clphdctrl {-f|--force} *hybriddisk-alias*
clphdctrl {-r|--recovery} *hybriddisk-alias* [-a or -f or -vf] [*dest-servername*]
clphdctrl {-c|--cancel} *hybriddisk-alias*
clphdctrl {-w|--rwait} *hybriddisk-alias* [-timeout *time*] [-rcancel]
clphdctrl {-s|--mdcswitch} *hybriddisk-alias* [*priority-number*]
clphdctrl {-p|--compress} [*hybriddisk-alias*]
clphdctrl {-n|--nocompress} [*hybriddisk-alias*]
clphdctrl {-z|--resize} *hybriddisk-alias partition-size* [-force]
clphdctrl --updatekey *hybriddisk-alias*

Note: Make sure that the EXPRESSCLUSTER service has been stopped when you use the --active or --deactive option.

Note: When you extend the data partition of the hybrid disk resource by using --resize option, extend both servers by following "Maintenance Guide" -> "The system maintenance information" -> "Increasing the hybrid disk size" .

Note: When you extend the data partition of the hybrid disk resource by using --resize option, a sufficient

amount of free space is required right after the data partition area.

Note: In updating an encryption key with the --updatekey option, follow the procedures specified in "Maintenance Guide" -> "The system maintenance information" -> "Updating data encryption key file of mirror/hybrid disk resources".

Description

This command allows operations such as mirror recovery and activating/deactivating a hybrid disk resource.

Option

-a,--active

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.
When neither -n or -f is specified, the command behaves in the same way as when -n is specified.

-n(-a,--active)

Specifies normal activation for activation mode.
This option can be omitted.
This cannot be specified when -f is specified.

-f(-a,--active)

Specifies forced activation for activation mode.
This option can be omitted.
This cannot be specified when -n is specified.

-d,--deactive

Deactivates the activated hybrid disk resource on the local server.

-b,--break

Stops mirroring of the hybrid disk resource and makes the data status not to be the latest on the server where the command is executed.
The data is not synchronized until mirror recovery is completed even if writing on the hybrid disk takes place.
When neither -n or -f is specified, the command behaves in the same way as when -n is specified.

-n(-b,--break)

Specifies the degeneration mode as normal degeneration.
In the case of normal degeneration, mirroring is intermitted and the server becomes not the latest status only when the mirroring is executed normally on the hybrid disk.
This option can be omitted.
This cannot be specified when -f is specified.

-f(-b,--break)

Specifies the degeneration mode as forced degeneration mode.
In the case of forced degeneration, mirroring is intermitted and the server becomes not the latest status even if the mirroring target server/server group status is abnormal or unknown.
This option can be omitted.
This cannot be specified when -n is specified.

-f,--force
Performs forced mirror recovery on the specified hybrid disk resource.

-r,--recovery

Performs either full mirror recovery or differential mirror recovery for the specified hybrid disk resource with the local server as the copy source.
If none of -a, -f, or -vf is specified, the command behaves in the same way as when -a is specified.

-a(-r,--recovery)

Automatically selects the recovery mode.
If the difference can be identified, differential copying is performed.
If differences cannot be identified, the command behaves in the same way as when -f is specified.
This option can be omitted.
This cannot be specified when -f or -vf is specified.

-f(-r,--recovery)

Copies all the used area of a volume if the used area can be identified.
Copies the entire area of a volume if the used area cannot be identified.
This option can be omitted.
This cannot be specified when -a or -vf is specified.

-vf(-r,--recovery)

Copies the entire area of a volume regardless of differences and the used area.
This option can be omitted.
This cannot be specified when -a or -f is specified.

-c,--cancel
Cancels mirror recovery.

-w,--rwait
Waits for the completion of the specified hybrid disk resource mirror recovery.

-timeout(-w,--rwait)

Specifies the time of mirror recovery completion timeout (second).
This option can be omitted.
When this option is omitted, timeout is not executed and waits for the completion of mirror recovery.

-rcancel(-w,--rwait)

Intermits mirror recovery when waiting for the mirror recovery completion is timed out.
This option can be set when -timeout option is set.
When this option is omitted, the mirror recovery continues even after the timeout takes place.

-s,--mdcswitch

Switches between the primary and secondary mirror disk connects of the user-specified hybrid disk resource.

If the priority number is omitted, the secondary mirror disk connect is switched to when the primary mirror disk connect is used at the time of command execution. When the secondary mirror disk connect is used, the primary mirror disk connect is switched to.

If the priority numbers are specified, the mirror disk connect that has the appropriate priority number is switched to.

-p,--compress

Temporarily enables mirror data compression for the specified hybrid disk resource.

If the hybrid disk resource name is omitted, mirror data compression is temporarily enabled for all hybrid disk resources.

-n,--nocompress

Temporarily disables mirror data compression for the specified hybrid disk resource.

If the hybrid disk resource name is omitted, mirror data compression is temporarily disabled for all hybrid disk resources.

-z,--resize

Extends the data partition size of hybrid disk resource.

The extension is available only when the status of hybrid disk resource is normal.

-force(-z,--resize)

Forcibly executes the extension regardless of the status of hybrid disk resource.

If this option is used, full copy of the hybrid disk will be executed for the next time.

In addition, even if this option is used, the extension is unavailable during the mirror recovery.

--updatekey

Updates the encryption key without stopping the resource.

The execution of this option, after completing the update of the encryption key files for both of the servers, updates the key for the encryption.

At this time, mirroring in progress is suspended. As required, execute mirror recovery after the execution.

Parameter

hybriddisk-alias
Specifies the hybrid disk resource name.

dest-servername

Specifies the copy destination server name.

When you omit this, the copy destination server is automatically determined from another server group.

time
Specifies the time of mirror recovery completion timeout (second).

priority-number
Specify the priority number (1 or 2).

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
Other than 0	Failure
101	Invalid parameter
102	Invalid status including the case when -w or --rwait option is specified and mirror recovery is intermitted by -rcancel.
103	Operations for the same resource are executed simultaneously from other servers.
104	Operations for the same resource were executed simultaneously from the own server.
105	The copy destination server is down.
106	The server that command is executed does not have the target resource.
107	I/O error occurred on the cluster partition or on the data partition.
109	Waiting for the completion of mirror recovery of the target hybrid disk is timed out (only when -w or --rwait -timeout option is specified).
110	Other errors
111	Failed in extending a hybrid disk (only when the -z or --resize option is specified).
112	Failed in updating an encryption key (only when the --updatekey option is specified).
113	The encryption function is disabled (only when the --updatekey option is specified).
114	The encryption key file has not been updated (only when the --updatekey option is specified).
201	The status of the destination mirror disk connect is invalid (only when the -m or --mdcswitch option is specified).
202	Only one mirror disk connect is set up (only when the -m or --mdcswitch option is specified).
203	All the servers in the remote server group are down.

Remarks
This command returns control when the specified processing starts. Run the clphdstat command to check the processing status.

Notes
This command must be executed by the user with administrator privilege.

When performing mirror recovery again after mirror recovery failed, specify the same server you used last time for mirror recovery or another server in the same server group which this server belongs to as a copy source.

To resume mirror recovery that was suspended by selecting **Cancel**, use this command for forced mirror recovery.

Example of command execution

Example 1: When activating hybrid disk resource hd1

```
# clphdctrl --active hd1
Command succeeded.
```

Example 2: When deactivating hybrid disk resource hd1

```
# clphdctrl --deactive hd1
Command succeeded.
```

Example 3: When recovering mirror for hybrid disk resource hd1

```
# clphdctrl --recovery hd1
Command succeeded.
```

Error messages

Message	Cause/Solution
Invalid parameter.	The parameter is invalid. Check if there is any error in its format or parameter.
The status of [hybrid disk resource name] is invalid.	Check the status and execute the command again.
This command is already run in another server.	After finishing the command which is currently executed, execute the command again.
This command is already run in the local server.	After finishing the command which is currently executed, execute the command again.
[copy destination server name] is down.	Start the server which has been specified as copy destination, or specify another server as copy destination to execute the command again.
[local server name] is not included in Servers that can run the Group of [hybrid disk resource name].	Execute the command from the server where the target hybrid disk resource can be started.
Disk error.	Check if there is not HW failure in the disk or disk path where cluster partition or data partition exists.
Mirror recovery of [hybrid disk resource name] is timed out.	Check if the specified timeout time is appropriate, or if the disk I/O or communication delay is not occurring due to heavy load.
Internal error. The error code is [error code].	Restart the local server.
Standby mirror disk connect has invalid status.	Check the connection status of the mirror disk connect.
[hybrid disk resource name] has only one mirror disk connect.	Make sure that more than one mirror disk connect is registered.
All of other server group downed.	Check the server operating status.
Resize the hybrid disk([hybrid disk resource name]) is failed.	Check that the status of hybrid disk resource is normal. Check that there is a sufficient amount of free space right after the current data partition area.
Failed to update the encryption key.	Check if the key file exists in the configured key file full path on each server.
The encryption function is disabled.	The encryption key cannot be updated due to **Encrypt mirror communication** disabled on the specified mirror disk resource.
The same encryption key is already used.	Update the key file of each server to a new one and try again.

Continued on next page

Table 9.57 – continued from previous page

Message	Cause/Solution
Automatic mirror recovery is disabled. Its manual resumption is required to resume mirroring.	The encryption key has been updated. The mirroring, however, is suspended. Mirror recovery must be performed manually due to disabled automatic mirror recovery.
Failed to resume the automatic mirror recovery. Its manual resumption is required to resume mirroring.	The encryption key has been updated. The mirroring, however, is suspended. Mirror recovery must be performed manually due to disabled automatic mirror recovery.

9.13.9 Preparing for backup to a disk image (clpbackup command)

Allows a partition to be mirrored to be backed up to its disk image.

Command line

clpbackup --pre
clpbackup --pre --no-shutdown
clpbackup --pre --only-shutdown
clpbackup --post
clpbackup --post --no-reboot
clpbackup --post --only-reboot
clpbackup --help

Description

Execute this command when backing up the disks for mirroring on a server (i.e., the cluster partition and the data partition) to its disk image, or the system disk on the server containing those to its disk image.

Execute this command as follows:

1. Run the clpbackup --pre command, which places the mirror into a backup mode and the server shuts down.
2. Back up a disk to its disk image.
3. Run the clpbackup --post command, which returns the mirror to a normal mode and the server restarts.
4. After the server is restarted, perform mirror recovery to synchronize differences generated during the backup.

In restoring from the disk image backed up, use the clprestore command.

For the procedure of backing up disks to their disk images with this command, see "Maintenance Guide" -> "The system maintenance information" -> "How to back up a mirror/hybrid disk to its disk image".

Option

--pre

Use this option for backing up partitions to be mirrored fully to its disk image, or backing up a system disk on a server containing those to its disk image.

Execute the command with this option immediately before the backup.

Executing the command with this option places all the cluster partitions and the data partitions (i.e., the partitions to be mirrored) into a backup mode and the server shuts down.

After shutting down and then starting the server, the EXPRESSCLUSTER service is not automatically started at the next startup of the server.

The status of the mirror in a backup mode is not of the latest (status: red) and the mirror recovery by full-copy needs to be performed. Automatic mirror recovery is not performed.

--post

Executing the command with this option clears the backup mode, which was set by the --pre option, to return to a normal mode, and the server restarts.

After the completion of the restart, the EXPRESSCLUSTER service automatically starts.

Execute the command with this option after the completion of backup to the disk image.

--no-shutdown

Executing the command with this option completes the command with no server shutdown.

No server shutdown occurs, but the EXPRESSCLUSTER service is stopped instead.

Use this option to prevent a server shutdown.

--no-reboot

Executing the command with this option skips a server reboot.

No server reboot occurs, but the EXPRESSCLUSTER service is started instead.

Use this option to prevent a server reboot or to save the reboot time.

--only-shutdown

Use this option if there are multiple servers in the server group with hybrid disk resources.

After the completion of executing the clpbackup --pre command on the first server in the server group, execute the clpbackup --pre --only-shutdown command on the remaining servers in the server group.

--only-reboot

Use this option if there are multiple servers in the server group with hybrid disk resources.

After the completion of executing the clpbackup --post command on the first server in the server group, execute the clpbackup --post --only-reboot command on the remaining servers in the server group.

--help

Displays the usage.

Return Value

0	Success
1	Failure

Remarks

In a backup mode, the status of the mirror is not of the latest (status: red) and the automatic mirror recovery is not performed. Not differential copy but full copy is executed at the mirror recovery.

This command applies not to the backup and restoration of files, but to those of disk images.
The procedure of using this command is different from that for backing up files from activated mirror disks/hybrid disks or backing up files from standby mirror disks/hybrid disks by canceling the access restriction.

Notes

Run this command as a user with Administrator privileges.

The execution of this command applies all the mirror disk resources and hybrid disk resources on the server.

Back up/restore both of the cluster partition and the data partition.

Executing this command causes the server to shut down or to restart.

This function does not apply to a cluster environment including a server with a version earlier than 4.3 of EXPRESSCLUSTER installed.

Error messages

Message	Cause/Solution
Invalid option.	Specify a valid option.
Log in as administrator.	Run this command as a user with Administrator privileges.
Internal error.	Check to see if the memory or OS resource is sufficient.
Internal error (setlocal command).	Check to see if the memory or OS resource is sufficient.
Log directory is not found.	Installation is not correctly performed or you do not have the administrator privilege.
Command failed.	This command failed. Check for any error message displayed immediately before this error message appears.

Example of command execution

Example 1: Causing mirror disk resources and hybrid disk resources to enter a backup mode prior to the execution of the backup:

```
C:\> clpbackup --pre
clpbackup.bat : Beginning backup-mode.
Command succeeded.
clpbackup.bat : Changing the setting of cluster services to Manual␣
↪Startup.
clpbackup.bat : Shutting down...
Command succeeded.
clpbackup.bat : Command succeeded.
```

Example 2: Ending the backup mode after the completion of the backup:

```
C:\> clpbackup --post
clpbackup.bat : Ending backup-mode.
Command succeeded.
clpbackup.bat : Changing the setting of cluster services to Auto Startup.
clpbackup.bat : Rebooting...
Command succeeded.
clpbackup.bat : Command succeeded.
```

9.13.10 Perform the processing after restoring from a disk image (clprestore command)

Allows a restored mirror disk image to be available.

Command line

clprestore --pre
clprestore --pre --only-shutdown
clprestore --post
clprestore --post --only-reboot
clprestore --post --skip-copy
clprestore --help

Description

Execute this command in restoring the cluster partition and the data partition from its disk image, or the system disk on the server containing those from its disk image.

Execute this command as follows:

1. Run the clprestore --pre command, which disables the automatic startup of the EXPRESSCLUSTER service and the server shuts down.
2. Restore from the disk image.
3. Start Cluster WebUI and change the mode to **Config mode**. After confirming or modifying the settings of each of the mirror disk resource and hybrid disk resource, execute **Apply the Configuration File**.
4. Run the clprestore --post command, which enables the automatic startup of the EXPRESSCLUSTER service and the server restarts.
5. After the restart of the server, perform the mirror recovery in Cluster WebUI or with the command. The data is fully copied and the mirror becomes synchronized. (Full copy is not required when --skip-copy is specified.)

For backing up the disk image, run the clpbackup command.

For the procedure of restoring from disk image with this command, see "Maintenance Guide" -> "The system maintenance information" -> "How to restore the mirror/hybrid disk from the disk image".

Option

--pre

Running the command with this option disables the automatic startup of the EXPRESSCLUSTER service and the server shuts down.
The EXPRESSCLUSTER service is therefore not automatically started at the next startup of the server.
Before restoring from the disk image, run this command at the time of shutting down the server.
When not starting the server, or restoring the system disk as well, this command does not need to be executed before the restoration.

--post

Running the command with this option enables the automatic startup of the EXPRESSCLUSTER service and the server restarts.

Execute this command after restoring from the disk image.

--skip-copy

Specify this option with the --post option.

This option can be specified only when the same disk image is restored to both of the active server and the standby server.

Full copy is not necessary at the time of mirror recovery.

In running the command with this option, **Execute the initial mirror construction** needs to be disabled in advance in the settings of mirror disk resources and hybrid disk resources.

--only-shutdown

Use this option if there are multiple servers in the server group with hybrid disk resources.

After the completion of executing the clprestore --pre command on the first server in the server group, execute the clprestore --pre --only-shutdown command on the remaining servers in the server group.

This option can be omitted.

--only-reboot

Use this option if there are multiple servers in the server group with hybrid disk resources.

After the completion of executing the clprestore --post command or the clprestore --post --skip-copy command on the first server in the server group, execute the clprestore --post --only-reboot command on the remaining servers in the server group.

--help

Displays the usage.

Return Value

0	Success
1	Failure

Remarks

This command applies not to the backup and restoration of files, but to those of disk images.

The procedure of using this command is different from that for backing up files from activated mirror disks/hybrid disks or backing up files from standby mirror disks/hybrid disks by canceling the access restriction.

Notes

Run this command as a user with Administrator privileges.

The execution of this command applies all the mirror disk resources and hybrid disk resources on the server.

Back up/restore both of the cluster partition and the data partition.

Executing this command causes the server to shut down or to restart.

This function does not apply to a cluster environment including a server with a version earlier than 4.3 of EXPRESSCLUSTER installed.

Error messages

Message	Cause/Solution
Invalid option.	Specify a valid option.
Log in as administrator.	Run this command as a user with Administrator privileges.
Internal error.	Check to see if the memory or OS resource is sufficient.
Internal error (setlocal command).	Check to see if the memory or OS resource is sufficient.
Set "Initial Mirror Construction" parameter of md/hd resource to off by using Cluster WebUI.	In specifying the --skip-copy option, **Execute the initial mirror construction** must be disabled in the settings of the md/hd resources. Before running the command, disable **Execute the initial mirror construction** in the config mode of Cluster WebUI.
Log directory is not found.	Installation is not correctly performed or you do not have the administrator privilege.
Command failed.	This command failed. Check for any error message displayed immediately before this error message appears.

Example of command execution

Example 1: Shutting down before the restoration:

```
C:\> clprestore --pre
clprestore.bat : Changing the setting of cluster services to Manual␣
↪Startup.
clprestore.bat : Shutting down...
Command succeeded.
clprestore.bat : Command succeeded.
```

Example 2: Starting a cluster after the restoration is performed and the configuration data is applied again:

```
C:\> clprestore --post
clprestore.bat : Beginning backup-mode.
Command succeeded.
clprestore.bat : Changing the setting of cluster services to Auto Startup.
clprestore.bat : Rebooting...
Command succeeded.
clprestore.bat : Command succeeded.
```

Example 3: Starting a cluster after the same image is restored to both of the servers and the configuration data is applied again:

```
C:\> clprestore --post --skip-copy
Command succeeded.
clprestore.bat : Changing the setting of cluster services to Auto Startup.
clprestore.bat : Rebooting...
Command succeeded.
clprestore.bat : Command succeeded.
```

9.14 Outputting messages (clplogcmd command)

The clplogcmd command registers the specified message with Alert logs.

Command line

clplogcmd -m *message* [--alert] [--mail] [-i *ID*] [-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 script resource script.

Description

Write this command in the script resource script and output messages **you want to send to the destination.**

Messages are produced in the following format:

[ID] message

Options

-m message

Specifies a message. This option cannot be omitted. The maximum size of message is 498 bytes.
You may use alphabets, numbers, and symbols. See below[14] for notes on them.

--alert

Specify the output destination from alert, mail.(Multiple destinations can be specified.)

--mail

This parameter can be omitted. The 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".

-i ID

Specify event ID.
This parameter can be omitted. The default value 1 is set for the event ID when the parameter is omitted.

-l level

Select a level of alert output from ERR, WARN, or INFO. The icon on the alert view of the Cluster WebUI is determined according to the level you select here.
This parameter can be omitted. The default value INFO is set to level when the parameter is omitted.
For more information, see the online manual.

[14] 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.)
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**.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as a user with Administrator privileges.

The specification of the -i option is different from that of the Linux version. The event ID that is displayed in alert is fixed and unchangeable in the Windows version.

Example of command execution

Example 1: When specifying message, message ID, and level:

When the following is written in the script resource script, the message is displayed in the Alert logs.

```
clplogcmd -m test1 -i 100 -l ERR
```

Example 2: When specifying message, output destination, event ID, and level (output destination is mail):

When the following is written in the script 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: 2019/04/10 10:00:00
```

9.15 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.

If you want to suspend/resume the monitor resources on all the servers in the clusters, it is recommended to use Cluster WebUI.

When [Cluster] is selected for [Failover Counting Method], -c and --clear options are applied only to several servers, the number of recovery operation count may be inconsistent among the servers and the recovery operations may fail.

Description

This command suspends and/or resumes the monitor resources, displays and/or initializes the recovery operation count, and enable and/or disable dummy failure.

Option

-s, --suspend
Suspends monitoring

-r, --resume
Resumes monitoring

-c, --clear
Initializes the recovery operation count.

-v, --view
Displays the recovery operation count.

-e
Enables dummy failure. Be sure to specify a monitor resource name with the -m option.

-n
Disables 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, --monitor

Specifies a monitor resource to be controlled.
This option can be omitted. All monitor resources are controlled when the option is omitted.

-w, --wait

Waits for control monitoring on a monitor resource basis (in seconds).

This option can be omitted. The default value of 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 EXPRESSCLUSTER service 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 successfully without changing the status of the monitor resource. If you suspend a monitor resource that is already suspended or resume the one that is already resumed, this command terminates with error, without changing the status of the monitor resource.

Notes

Run this command as a user with Administrator privileges.

Check the status of monitor resource by using the status display 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.
You are not authorized to run the command. Log in as Administrator.	You are not authorized to run this command. Log in as a user with Administrator privileges.
Initialization error. Check if memory or OS resources are sufficient.	Check 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 service by using the command such as ps command.	The cluster has been stopped. Check the activation status of the EXPRESSCLUSTER service by using the ps command.
The cluster has been suspended. The cluster service has been suspended. Check activation status of the cluster service by using a command such as the ps command.	The EXPRESSCLUSTER service has been suspended. Check the activation status of the EXPRESSCLUSTER service 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 synchronization of the cluster is completed.
Monitor %1 was unregistered, ignored. The specified monitor resources %1is not registered, but continues 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
The command is already executed. Check the execution state by using the "ps" command or some other command.	The command has already been run. Check the status by using the ps command.
Internal error. Check if memory or OS resources are sufficient.	Check 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.

Continued on next page

Table 9.60 – continued from previous page

Message	Causes/Solution
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 (y=yes, n=no)

Type	Suspending/Resume	Reset Recovery Count	Dummy Failure Possibility
appliw	✓	✓	✓
diskw	✓	✓	✓
fipw	✓	✓	✓
ipw	✓	✓	✓
mdw	✓	✓	n/a
miiw	✓	✓	✓
mtw	✓	✓	✓
regsyncw	✓	✓	✓
sdw	✓	✓	✓
servicew	✓	✓	✓
vcomw	✓	✓	✓
vipw	n/a	✓	✓
cifsw	✓	✓	✓
hdw	✓	✓	n/a
hdtw	✓	✓	✓
genw	✓	✓	✓
mrw	✓	✓	n/a
db2w	✓	✓	✓
ftpw	✓	✓	✓
httpw	✓	✓	✓
imap4w	✓	✓	✓
odbcw	✓	✓	✓
oraclew	✓	✓	✓
pop3w	✓	✓	✓
psqlw	✓	✓	✓
smtpw	✓	✓	✓
sqlserverw	✓	✓	✓
tuxw	✓	✓	✓
userw	✓	✓	✓
wasw	✓	✓	✓
wlsw	✓	✓	✓
otxw	✓	✓	✓
jraw	✓	✓	✓
sraw	✓	✓	✓
psrw	✓	✓	✓
psw	✓	✓	✓
ddnsw	n/a	✓	n/a
awsazw	✓	✓	✓
awsdnsw	✓	✓	✓
awseipw	✓	✓	✓
awssipw	✓	✓	✓
awsvipw	✓	✓	✓

Continued on next page

Table 9.61 – continued from previous page

Type	Suspending/Resume	Reset Recovery Count	Dummy Failure Possibility
azurednsw	✓	✓	✓
azurelbw	✓	✓	✓
azureppw	✓	✓	✓
gcdnsw	✓	✓	✓
gclbw	✓	✓	✓
gcvipw	✓	✓	✓
oclbw	✓	✓	✓
ocvipw	✓	✓	✓

9.16 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 time in seconds to wait for group resources to be started or stopped (internal communication timeout). A value between 1 to 9999 can be specified.
When the --apito option is not specified, the command waits for 3600 seconds.

-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
      lankhb1          : Normal
      lankhb2          : Normal
      pingnp1          : Normal
   server2.............: Online
      lankhb1          : Normal
      lankhb2          : Normal
      pingnp1          : Normal
<group>
    ManagementGroup.....: Online
      current          : server1
      ManagementIP     : Online
    failover1...........: Online
      current          : server1
      fip1             : Online
      md1              : Online
      script1          : Online
    failover2...........: Online
      current          : server2
      fip2             : Online
      md2              : Online
      script1          : Online
<monitor>
    fipw1              : Normal
    fipw2              : Normal
    ipw1               : 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
     script1           : Online
    failover2...........: Online
     current           : server2
     fip2              : Online
     md2               : Online
     script1           : 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
     script1                 : Online
    failover2...............: Online
     current                 : server2
     fip2                    : Online
     md2                     : Online
     script1                 : Online
  <Abbreviation>
```

Notes

Run this command as a user with Administrator 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 Administrator.	Run this command as a user with Administrator 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 9.62 – 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 till the other server starts or the wait time times out, 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. To start the group resource on the local server, stop the group resource.	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.
Depending 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 isolated.	The server is suspended. (Rebooting after down)
Internal error. Check if memory or OS resources are sufficient.	Not enough memory space or OS resource. Check if there is enough space.
Server is not in a condition to start resource. 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.

9.17 Switching off network warning light (clplamp command)

The clplamp command switches off network warning light.

Command line

clplamp -h *host_name*

Description

This command switches off the network warning light corresponding to the specified server.

If the reproduction of audio file is set, audio file reproduction is stopped.

Option

-h host_name

Specify the target server whose network warning light you want to switch off.

This must be configured.

Return value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Example

Example 1: When turning off the warning light and audio alert associated with server1

```
# clplamp -h server1
Command succeeded.(code:0)
```

Notes

This command must be executed by a user with the administrator privilege.

9.18 Requesting processing to cluster servers (clprexec command)

The clprexec 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

The command issues the request to execute specified process to the server in another cluster.

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 batch file or executable file).
The script must be created in the work/rexec folder, which is in the folder where EXPRESSCLUSTER is installed, on each server specified using -h.

--notice

Sends an error message to the EXPRESSCLUSTER server.
Specify a message reception monitor resource name for mrw_name.
When not specifying the monitor resource name, specify the monitor type and monitor target of the message reception monitor resource by using the -k option.

--clear

Requests changing the status of the message reception monitor resource from "Abnormal" to "Normal."
Specify a message reception monitor resource name for mrw_name.
When not specifying the monitor resource name, specify the monitor type and monitor target of the message reception 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 period 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 999 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 reception monitor resources for which executing an action when an error occurs is specified in EXPRESSCLUSTER server must be registered and started.

The server that has the IP address specified for the -h option must satisfy the following conditions:
= EXPRESSCLUSTER X 3.0 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 Limiting the access by using client IP addresses is enabled, add the IP address of the device to execute the clprexec command.
For details of the Limiting the access by using client IP addresses function, see "*WebManager tab*" of "*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.bat) on EXPRESSCLUSTER server 1 (10.0.0.1):

```
# clprexec --script script1.bat -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 reception monitor resource name:

```
# clprexec --notice mrw1 -h 10.0.0.1 -w 30 -o /tmp/clprexec/ clprexec.
↪log
```

- This example shows how to specify the *category* and *keyword* specified for the message reception monitor resource:

```
# clprexec --notice -h 10.0.0.1 -k earthquake.scale3 -w 30 -o /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 reception 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 reception monitor resource:

```
# clprexec --clear -h 10.0.0.1 -k earthquake.scale3
```

Error messages

Message	Cause/solution
Success	-
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.
Could not connect to all data transfer server.	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.
Group(%s) is offline.	Check the processing result on the server that received the request.
Group that specified resource(%s) belongs to is offline.	Check the group status.
Specified script(%s) does not exist.	Check if the specified script exist.

Continued on next page

Table 9.63 – continued from previous page

Message	Cause/solution
Specified resource(%s) is not exist.	Check the resource name or monitor resource name.
Specified resource(Category:%s, Keyword:%s) is not exist.	Check the resource name or monitor resource name.
Specified group(%s) does not exist.	Check the group name.
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 failed in execute.	Check the status of the EXPRESSCLUSTER server that received the request.

9.19 Controlling cluster activation synchronization wait processing (clpbwctrl command)

The clpbwctrl command controls the cluster activation synchronization wait processing.

Command line

clpbwctrl -c
clpbwctrl --np [on|off]
clpbwctrl -h

Note: The command with the --np option must be executed on all the servers that control the processing because the command controls the processing on a single server.

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.
Specifies whether to execute the NP resolution process when the cluster is started on a single server.

Option

-c, --cancel
Cancels the cluster activation synchronization wait processing.

--np [on|off]

Specifies whether to execute the NP resolution process when the cluster is started. When "on" is specified, the NP resolution process is executed. When "off" is specified, it is not executed.
[on|off] is optional. When omitted, the current setting is displayed.

-h, --help
Displays the usage.

Return Value

0	Completed successfully.
Other than 0	Terminated due to a failure.

Notes
Run this command as a user with Administrator privileges.

Examples
This example shows how to cancel the cluster activation synchronization wait processing:

```
#clpbwctrl -c
Command succeeded.
```

The NP resolution process is not performed at the cluster startup:

```
#clpbwctrl --np off
Command succeeded.

#clpbwctrl --np
Resolve network partition on startup : off
```

Error messages

Message	Cause/solution
Log in as Administrator	Log in as a user with administrator privileges.
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.

9.20 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	Completed successfully.
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.

Examples

Display of reboot count information

```
# clpregctrl -g

*************************
-------------------------
type : rc
registry : haltcount
comment : halt count
kind : int
value : 0
```

```
default : 0
-------------------------
type : rm
registry : haltcount
comment : halt count
kind : int
value : 3
default : 0

**************************
success.(code:0)
#
```

The reboot count is initialized in the following examples.

Run this command on the server which actually control the reboot count, because the reboot count is recorded on each server.

Example1: When initializing the count of reboots caused by group resource error:

```
# clpregctrl -c -t rc -r haltcount
success.(code:0)
#
```

Example2: When initializing the count of reboots caused by monitor resource error:

```
# clpregctrl -c -t rm -r haltcount
success.(code:0)
#
```

Notes

See "*What is a group?*" "*Reboot count limit*" in "*3. Group resource details*" in this guide for information on reboot count limit.

Examples

Run this command as a user with Administrator privileges.

Error messages

Message	Cause/solution
Command succeeded.	The command ran successfully.
Log in as Administrator.	You are not authorized to run this command. Run this command as a user with Administrator privileges.
The command is already executed.	The command is already running.
Invalid option.	Specify a valid option.
Internal error. Check if memory or OS resources are sufficient.	Not enough memory space or OS resource.

9.21 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 clppm, clprc, clprm, and clpnm.

-t <process>

<process>

pm Checks the health of clppm.

rc Checks the health of clprc.

rm Checks the health of clprm.

nm Checks the health of clpnm.

-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 OK
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 a user with Administrator privileges.

Error Messages

Message	Cause/Solution
Log in as Administrator.	Log in as a user with Administrator privileges.
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.
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.
Internal error. Check if memory or OS resources are sufficient.	Check to see if the memory or OS resource is sufficient.

9.22 Setting an action for OS shutdown initiated by other than cluster service (clpstdncnf command)

The clpstdncnf command sets an action for OS shutdown initiated by other than cluster service.

Command line

clpstdncnf -e [*time*]
clpstdncnf -d
clpstdncnf -v

Note: This command sets an action for OS shutdown initiated by other than cluster service on a single server. The command must be executed on all of the servers in which you want to set.

Description

This command sets an action for OS shutdown initiated by other than cluster service on a single server.

Option

-e [time]

Waits for cluster services to be stopped when OS shutdown is initiated by other than cluster service.
You can specify a timeout value in minutes (A value between 1 to 1440 can be specified).
It is necessary to specify the timeout value at first execution.
From the second execution on, if you don't specify the timeout value, the current value is used.

-d

Does not wait for cluster services to be stopped when OS shutdown is initiated by other than cluster service.

-v

shows the current setting.

Return Value

0	Success
Other than 0	Failure

Notes

Run this command as a user with Administrator privileges.

In case of a virtual environment, such as cloud environment, when OS shutdown is initiated from the virtual infrastructure, power-off may be executed depending on the virtual infrastructure.

Example of command execution

Example 1: Waits for cluster service to be stopped (timeout = 30 minutes)

```
# clpstdncnf -e 30
Command succeeded.

# clpstdncnf -v
Mode : wait
Timeout: 30 min
```

Example 2: Does not wait for cluster service to be stopped

```
# clpstdncnf -d
Command succeeded.

# clpstdncnf -v
Mode : no wait
Timeout: 30 min
```

9.23 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
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.

Notes

Run this command as a user with Administrator privileges.

Set the user name and password specified in the -u option in advance from the **Account** tab in **Properties** of the cluster in the config mode of EXPRESSCLUSTER.

A user specified in the -u option needs to have the privilege to run the SET WRITE command of DB2.

Examples

```
# clpdb2still -d sample -u db2inst1 -s

Database Connection Information

Database server = DB2/NT64 11.1.0
SQL authorization ID = DB2ADMIN
Local database alias = SAMPLE
DB20000I The SET WRITE command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL DISCONNECT command completed successfully.
Command succeed

# clpdb2still -d sample -u db2inst1 -r
```

```
Database Connection Information

Database server = DB2/NT64 11.1.0
SQL authorization ID = DB2ADMIN
Local database alias = SAMPLE
DB20000I The SET WRITE command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL DISCONNECT command completed successfully.
Command succeed.
```

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.

9.24 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

Notes

Run this command as a user with Administrator privileges.

If OS authentication is used without specifying the -u option, a user who runs his command needs to belong to the dba group, in order to gain administrative privileges for Oracle.

Set the user name and password specified in the -u option in advance from the Account tab in Properties of the cluster in the config mode of EXPRESSCLUSTER.

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.

Examples

```
# clporclstill -d orcl -u oracle -s
Command succeeded.

# clporclstill -d orcl -r
Command succeeded.
```

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.

9.25 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

Notes

Run this command as a user with Administrator privileges.

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.

A user specified in the -u option needs to have superuser privileges for PostgreSQL.

Enable WAL archive of PostgreSQL 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.

Examples

```
# clppsqlstill -d postgres -u postgres -s
Command succeeded.

# clppsqlstill -d postgres -r
Command succeeded.
```

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.

9.26 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 vdiusername -r

Description

Controls the securing/release of the rest point of SQL Server.

Option

-d databasename
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	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

Notes

Run this command as a user with Administrator privileges.

The user needs to have administrator privileges for SQL Server to run this command if the OS authentication is used without specifying the -u option.

Set the user name and password specified in the -u option in advance from the Account tab in Properties of the cluster in the config mode of EXPRESSCLUSTER.

A user specified in the -u option needs to have the privilege to run the BACKUP DATABASE statement of 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.

Examples

```
# clpmssqlstill -d userdb -u sa -v mssql -s
Command succeeded.

# clpmssqlstill -d userdb -v mssql -r
Command succeeded.
```

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.

9.27 Displaying the cluster statistics information (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

Displays the median values (millisecond) of the group start time and group stop time.

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 Administrator.

Error Messages

Message	Cause/Solution
Log in as Administrator.	Execute this command as Administrator.
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.

9.28 Checking the cluster configuration information (clpcfchk command)

Checks the cluster configuration information.

Command line

clpcfchk -o *path* [-i *conf_path*]

Description

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

Execute this command as Administrator.

When checking the configuration information exported through Cluster WebUI, decompress it in advance.

Error Messages

Message	Cause/Solution
Log in as Administrator.	Execute this command as Administrator.
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.	Check if the memory or OS resource is sufficient.

9.29 Converting a cluster configuration data file (clpcfconv command)

Converts a cluster configuration data file.

Command line

clpcfconv -i <*input-path*> [-o <*output-path*>]

Description

Converts an old version of a cluster configuration data file into the current version.

Option

-i <input-path>

Specifies a directory where an old version of a cluster configuration data file exists.

-o <output-path>

Specifies a directory where the converted cluster configuration data file is outputted.

If this option is omitted, the converted cluster configuration data file is outputted to the current directory.

Return value

0	Normal termination
Other	than 0 Termination with an error

Notes

Execute this command as Administrator.

This command converts only clp.conf among cluster configuration data files.

This command cannot be executed right under <installation destination directory>\etc.

This command does not support any cluster configuration data file created with a version older than EXPRESSCLUSTER X 3.3 for Windows (internal version: 11.35).

If a password was set on the cluster password method with a version older than EXPRESSCLUSTER X 5.0 for Windows, executing this command clears the password.

After applying the converted cluster configuration data, set the password again by using Cluster WebUI.

For information on how to set a password, see this guide: "2. *Parameter details*" -> "*Cluster properties*" -> "*WebManager tab*".

Example of Execution

When the conversion succeeds

```
# clpcfconv -i C:\temp\config_x430 -o C:\temp\config_new
Command succeeded.
```

When the conversion succeeds and the password is cleared

```
# clpcfconv -i C:\temp\config_x430 -o C:\temp\config_new
Command succeeded.

Password for Operation has been initialized.
```

```
Password for Reference has been initialized.
Please set the password again by using Cluster WebUI.
```

Error Messages

Message	Cause/Solution
Command succeeded.	The command ran successfully.
Password for Operation has been initialized.	The operation password set on the cluster password method has been cleared.
Password for Reference has been initialized.	The reference password set on the cluster password method has been cleared.
Please set the password again by using Cluster WebUI.	Set the cleared password again by using Cluster WebUI.
Log in as administrator.	Execute this command as Administrator.
Failed to get etc directory path.	Installation is not correctly performed or you do not have the administrator privilege.
Not available in this directory.	This command cannot be executed right under <installation destination directory>\etc. Change the current directory to a different directory (other than <installation destination directory>\etc).
Could not opened the configuration file. Check if the configuration file exists on the specified path.	The cluster configuration data file (clp.conf) does not exist on the path specified with the -i option. Check if the cluster configuration data file exists on the specified path.
The specified output-path does not exist.	The path specified with the -o option does not exist. Specify the right path.
Invalid configuration file.	The cluster configuration data file is invalid. Check the cluster configuration data file.
The version of this configuration data file is not supported. Convert it with Builder for offline use (internal version 11.35), then retry.	The version of the cluster configuration data file is not supported by this command. Convert it with Builder for offline use (internal version: 11.35), then retry.
%1 : Command failed. code:%2	The command (%1) failed. Check the returned value (%2) of the command, or the error message displayed just before this error message.

Continued on next page

Table 9.75 – continued from previous page

Message	Cause/Solution
Command failed.	This command failed. Check for any error message displayed immediately before this error message appears.

9.30 Adding a firewall rule (clpfwctrl command)

Adds or deletes an inbound firewall rule on servers for EXPRESSCLUSTER.

Command line

clpfwctrl --add [--profile public | private | domain]
clpfwctrl --remove
clpfwctrl --help

Description

Note: Before executing this command, enable the server firewall.

Note: This command adds or deletes an inbound firewall rule on a single server, and therefore must be executed on every server for which you want the rule to be added or deleted.

Note: Execute this command immediately after installing EXPRESSCLUSTER and directly after applying configuration data.

An inbound firewall rule can be added for accessing port numbers for EXPRESSCLUSTER, and the added rule can be deleted.
For more information on port numbers to be specified with this command, and for that on protocols, see "Getting Started Guide" -> "Notes and Restrictions" -> "Before installing EXPRESSCLUSTER" -> "Communication port number".
Add an inbound firewall rule with the following group name and names. If the group name is already used, first delete it, then add it again. Do not change the group name.

- Group name
  - EXPRESSCLUSTER
- Names
  - EXPRESSCLUSTER (TCP-In)
  - EXPRESSCLUSTER (UDP-In)
  - EXPRESSCLUSTER (ICMPv4-In)
  - EXPRESSCLUSTER (ICMPv6-In)

Option

--add [--profile public | private | domain]
Adds an inbound firewall rule, and its profile name (if specified) as well. The profile name can be omitted.

--remove
Deletes the added inbound firewall rule.

--help
Displays the usage.

Return value

0	Success
Other than 0	Failure

Notes

Execute this command as Administrator.

This command does not add an outbound firewall rule. Adding it requires a separate procedure.

Once a JVM monitor resource is registered, this command always allows the port number for managing the resource.

Example of Execution

Adding an inbound firewall rule without the --profile option:

```
# clpfwctrl.bat --add
Command succeeded.
```

Example of Execution

Adding an inbound firewall rule with domain and private (the --profile option) specified:

```
# clpfwctrl.bat --profile domain private
Command succeeded.
```

Example of Execution

Deleting the added inbound firewall rule:

```
# clpfwctrl.bat --remove
Command succeeded.
```

Error Messages

Message	Cause/Solution
Log in as Administrator.	Log in as a user with Administrator privileges.
Invalid option.	Specify the right option.
Log directory is not found.	Installation is not correctly performed or you do not have the administrator privilege.
Failed to register rule(CLUSTERPRO). Invalid port.	Check the configuration data, which includes an invalid port number.
Unsupported environment.	The OS is unsupported.
Could not read xmlpath. Check if xmlpath exists on the specified path. (%1)	Check if the xml path exists in the configuration data. %1: xml path
Could not opened the configuration file. Check if the configuration file exists on the specified path. (%1)	Check if the configuration data exists. %1: xml path

Continued on next page

Table 9.76 – continued from previous page

Message	Cause/Solution
Could not read type. Check if type exists on the policy file. (%1)	Check if the policy file exists. %1: xml path
not exist xmlpath. (%1)	Check if the xml path exists in the configuration data. %1: xml path
Failed to obtain properties. (%1)	Check if the xml path exists in the configuration data. %1: xml path
Not exist java install path. (%1)	Check if the Java installation path exists. %1: Java installation path
Internal error. Check if memory or OS resources are sufficient. (%1)	The possible cause is insufficient memory or insufficient OS resources. Check if these two are sufficient. %1: xml path

CHAPTER

TEN

TROUBLESHOOTING

This chapter provides instructions for troubleshooting problems with EXPRESSCLUSTER.

This chapter covers:

10.1 Troubleshooting

The following provides instructions for troubleshooting problems you experience in operating the EXPRESSCLUSTER system.

10.1.1 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. Make sure that the cluster configuration data is uploaded on all the servers.
   For details, 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,>ipconfig....)
3. License registration
   The license may not be registered yet. Run the license manager on all servers in the cluster to confirm that the license is registered:
   If you are using the trial version license or fixed term license, confirm if it is not expired yet.
   To run the license manager, select **EXPRESSCLUSTER Server** from the **Start** menu, and then **License Manager**.
4. EXPRESSCLUSTER service
   Start the service control manager of the OS, and make sure that the following EXPRESSCLUSTER services have been started. If all of them have been started, EXPRESSCLUSTER is running normally. To run the service control manager, from **Control Panel,** select **Administrative Tools** and select **Services**.
   - EXPRESSCLUSTER
   - EXPRESSCLUSTER API
   - EXPRESSCLUSTER Disk Agent
   - EXPRESSCLUSTER Event
   - EXPRESSCLUSTER Information Base
   - EXPRESSCLUSTER Manager
   - EXPRESSCLUSTER Node Manager
   - EXPRESSCLUSTER Server
   - EXPRESSCLUSTER Transaction
   - EXPRESSCLUSTER Web Alert
5. Free disk space
   Run [Disk Management] to check the size of the free disk space in the drive that contains *<EXPRESSCLUSTER_installation_path>*. For details on the disk space to be used by EXPRESSCLUSTER, see "Installation requirements for EXPRESSCLUSTER" in "Getting Started Guide". To run Disk Management, select **Control Panel**, select **Administrative Tools**, and select **Computer Management**. Then from the icon tree, select **Services** under **Services and Applications**.
6. Usage of memory or OS resource
   Run Task Manager of the OS to check the OS memory usage and CPU usage rate.

10.1.2 When activating or deactivating network partition resolution resource fails

1. Majority method
   Memory or OS resources may not be sufficient. Check them.
2. PING method
   Memory or OS resources may not be sufficient. Check them.
3. DISK method
   The settings of the Cluster WebUI are invalid. Check that the disk heartbeat partition is set to be filtered on the **HBA** tab of **Server Properties** of the server that failed to be activated or deactivated. Check that the disk heartbeat partition is not used by other resource (disk resource, mirror disk resource).

10.1.3 When a network partition resolution resource error is detected

1. Majority method
   Memory or OS resources may not be sufficient. Check them.
2. PING method
   There is no PING command response from the PING destination device. Check that there is no problem in the communication path from the cluster server to the PING destination device.
3. DISK method
   Timeout occurred in accessing the disk heartbeat partition, or disconnection of the cable to the shared disk was detected.
   If a timeout has occurred, select **Cluster Properties -> disk network partition resolution resource** in which the error occurred from the **NP Resolution** tab, and then open **Properties**. Adjust **IO Wait Time** in the **Disk NP Properties** dialog.
   If cable disconnection is detected, check the cable connection status.

10.1.4 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 event log. See " *Detailed information in activating and deactivating group resources* " and examine the logs to find the cause of the error and take appropriate action for it.

10.1.5 When a monitor resource error occurs

If a monitor resource detects any error, detailed information on error is logged in the alert and event logs. From the information, see " *Detailed information of monitor resource errors* " and examine the logs to find the cause of the error and take appropriate action for it.

10.1.6 When a heartbeat timeout occurs

Possible causes of heartbeat timeout between servers are listed below:

Cause	Solution
Disconnection of LAN cables	Check that you can send packets with the ping command.

10.1.7 Recovering from failure of one server

If the automatic recovery mode is not set in **Cluster Properties**, the server that you have removed errors and restarted is in the **Suspension (Isolated)** status. To recover the server to the normally functioning cluster from this status, use the Cluster WebUI or the clpcl command.

If the Replicator is used, data between the disks that form a mirror set becomes inconsistent. However, by recovering the server, the mirror will be automatically rebuilt, and the data will become consistent.

To recover the server by using the Cluster WebUI, see the online manual.

To recover the server by using the clpcl command, see "*Operating the cluster (clpcl command)*" in "*9. EXPRESSCLUSTER command reference*" in this guide.

10.1.8 Recovering from failure of both servers

When **Off** is selected for **Auto Return** on the **Extension** tab in **Cluster Properties**, when all the servers shut down by failures such as a hardware failure, after starting them up, they are removed from the cluster. Recover all the servers by using the Cluster WebUI or the clpcl command.

Right after recovering the servers, all the groups are stopped. Start all the groups. If the Replicator is used, the mirror will be automatically built again by starting the groups, and the data will become consistent.

10.1.9 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 when the network partition resolution resource is not registered. The following examples assume that you have registered kernel mode LAN heartbeat resources 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 : lankhb1
  HB1 : lankhb2

[on server0 : Online]
        HB 0 1
---------------------------------------------------------------
```

```
  server0 : o o
  server1 : o o

[on server1 : Online]
        HB 0 1
----------------------------------------------------------------
  server0 : o o
   server1 : o o
================================================================
```

When you run the command on server2

```
# clpstat -n
==================== HEARTBEAT RESOURCE STATUS =================
Cluster : cluster
  server0 : server1
  *server1 : server2

  HB0 : lankhb1
  HB1 : lankhb2

[on server0 : Online]
        HB 0 1
----------------------------------------------------------------
  server0 : o o
  server1 : o o

[on server1 : Online]
        HB 0 1
----------------------------------------------------------------
  server0 : o o
  server1 : 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 : lankhb1
  HB1 : lankhb2

[on server0 : Caution]
        HB 0 1
----------------------------------------------------------------
  server0 : o o
  server1 : x x

[on server1 : Offline]
        HB 0 1
```

```
----------------------------------------------------------------
  server0 : - -
  server1 : - -
================================================================
```

When you run the command on server2

```
# clpstat -n
=================== HEARTBEAT RESOURCE STATUS ================
Cluster : cluster
  server0 : server1
  *server1 : server2

  HB0 : lankhb1
  HB1 : lankhb2

[on server0 : Offline]
         HB 0 1
----------------------------------------------------------------
  server0 : - -
  server1 : - -

[on server1 : Caution]
         HB 0 1 2
----------------------------------------------------------------
  server0 : x x
  server1 : o o
================================================================
```

Shut down both servers immediately if the network is partitioned. Check the following for heartbeat resources.

1. Kernel mode LAN heartbeat resource
   - LAN cable status
   - Network interface 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.

10.1.10 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 Server service.	Other servers cannot be operated, suspended or resumed.
clpdown	Stops the EXPRESSCLUSTER service and shuts down a server registered in the configuration information.	Other servers cannot be operated.
clpstdn	Stops the EXPRESSCLUSTER service in the entire cluster, and shuts down all servers.	Other servers cannot be operated.
clpgrp	Starts, stops and moves groups.	Only groups on the local server can be stopped.
clptoratio	Extends and displays timeout values of all servers in the cluster.	Timeout 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 / Replicator DR)

Command	Description	Remarks
clpmdstat	Displays the status and configuration information on mirror disk.	The mirror disk status of the other servers cannot be retrieved.
clpmdctrl	Allows operations such as mirror recovery and activating/deactivating a mirror disk resource.	No operation relating to mirror disk resources can be performed for other servers.
clphdsnapshot	Controls snapshot backup of hybrid disk resource.	This command cannot be used unless mirroring is successfully performed.

Continued on next page

Table 10.6 – continued from previous page

Command	Description	Remarks
clphdstat	Displays the status and configuration information on hybrid disk.	The hybrid disk status of the other servers cannot be retrieved.
clphdctrl	Allows operations such as mirror recovery and activating/deactivating a hybrid disk resource.	No operation relating to hybrid disk resources can be performed for other server groups.

10.2 Connecting mirror disks/hybrid disks manually

This section describes how to cancel the access restriction for the data partition of mirror disk resource or hybrid disk resource when you cannot start EXPRESSCLUSTER due to some sort of failure.

10.2.1 Normally connecting mirror disk when mirroring is available

When the EXPRESSCLUSTER Server service can be activated while the EXPRESSCLUSTER X Disk Agent service cannot be, access restriction can be canceled by following the steps below.

1. Run the following command on the server where you want to connect disks.
   - For mirror disks:

     ```
     clpmdctrl --active <mirror_disk_resource_name (Example: md1)>
     ```

   - For hybrid disks:

     ```
     clphdctrl --active <hybrid_disk_resource_name (Example: hd1)>
     ```

2. The mirror disk resource or hybrid disk resource becomes accessible. Written data is mirrored to the other server.

10.2.2 Forcibly connecting mirror disk when mirroring is not available

Follow the steps below to save data on mirror disks when both the EXPRESSCLUSTER Server service and the EXPRESSCLUSTER X Disk Agent service cannot be activated.

However, the mirroring status up to the moment just before both the EXPRESSCLUSTER Server service and the EXPRESSCLUSTER X Disk Agent service became unable to be activated must be normal, or you must know which server has the latest data.

1. The EXPRESSCLUSTER service cannot be started on Server 1 or Server 2. Server 1 has the latest data. Uninstall EXPRESSCLUSTER on the server which has the latest data and restart the server.

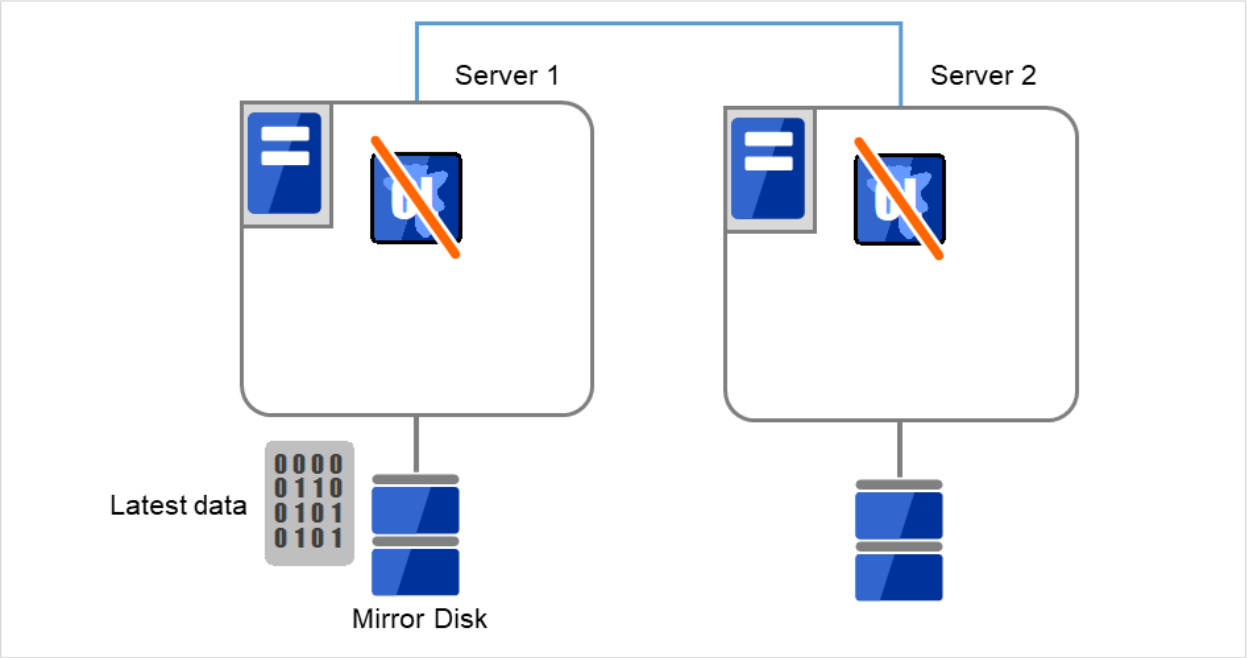


Fig. 10.1: Saving the data on the mirror disk (1)

2. Connect the backup device to Server 1, and back up the data in the data partition by using the backup command.

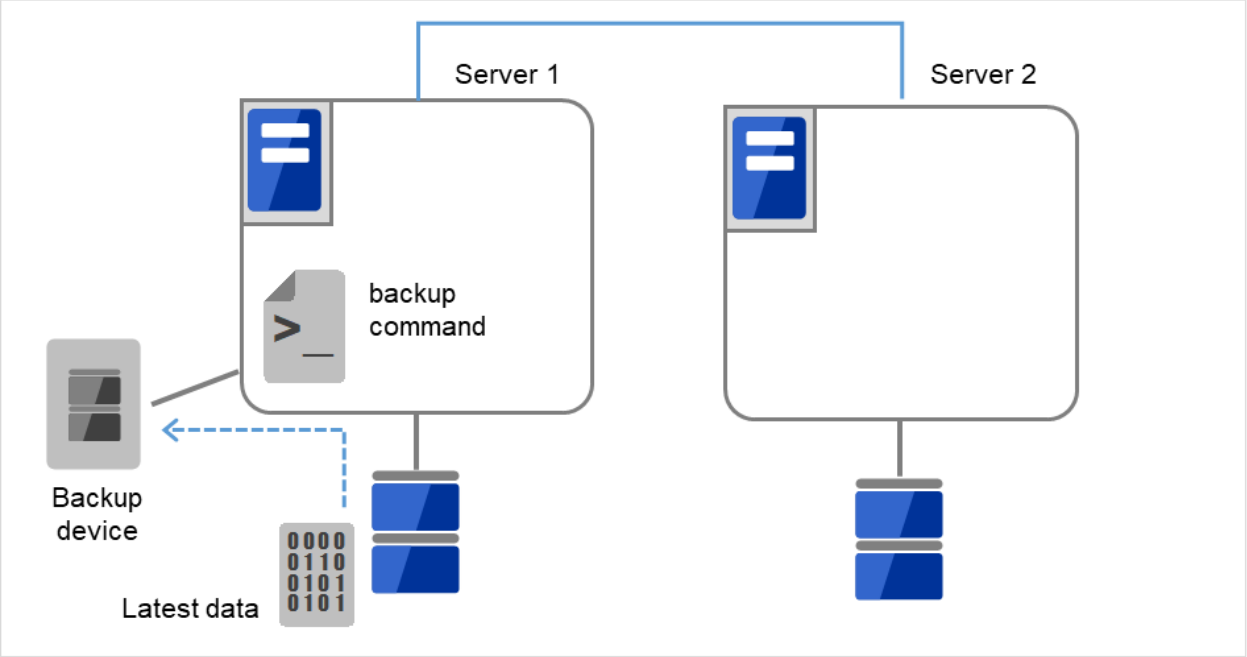


Fig. 10.2: Saving the data on the mirror disk (2)

As for hybrid disk resources, if the above is performed while another server in the same server group is using the shared disk, the data on the shared disk may be destroyed. Make sure to stop the other server or disconnect the disk

cable of the other server when you perform the above.

10.3 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.

If the auto-mirror recovery is disabled, you have to recover mirroring by executing a command or using the Cluster WebUI.

The difference mirror recovery function is disabled and full copy is performed in the following cases:

- When the partition configuration for mirror disk resource or hybrid disk has been changed due to disk replacement etc.
- When both servers fail at the same time while mirror disk resource is normally activated
- When the current servers (servers updating and managing the disk in the server group) in the both server groups fail at the same time when the hybrid disk resource is normally activated
- When difference information could not be written successfully due to disk failure etc.

10.3.1 Automatically recovering from mirroring

When the auto-mirror recovery is enabled, mirroring is automatically recovered under the following conditions:

1. Mirror disk resource or hybrid disk resource is active.
2. The server where mirror disk resource or hybrid disk resource is activated 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.
5. In case of mirror disk, both the mirror disk monitor resource must operate normally on all the registered servers.
   In case of hybrid disk, hybrid disk monitor resource must operate normally on a server that monitor target resource is activated.
6. Resource is not activated on a server/server group that does not store the latest data.
7. **Auto Mirror Recovery Setting** in the cluster's properties must be checked.
   However, if the initial mirror configuration is yet to be set, the initial auto mirror configuration must be checked in accordance with the above indicated.
8. Failures such as disk errors on the target disk of the mirror disk or hybrid disk are not occurring

The auto-mirror recovery is not performed if any of the following applies.

1. One of the servers (for hybrid disk resource, all servers in one of the server groups) is not started.
2. You cannot confirm the mirroring status of the other server.
3. There is no server whose mirror status is normal.
4. Mirror disk monitor resource or hybrid disk monitor resource is not registered.
5. Monitor resource is suspended or stopped in a server or server group that stores the latest data.
6. Resource is forcibly activated in other server or server group, including when snap shot backup is being executed.

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".

10.3.2 Checking the mirror break status with a command

For mirror disk resources, run the following command to view the mirror break statuses.

`clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>`

You can view the mirror disk resource statuses by running the clpmdstat command.

1. When normal:

```
Status: Normal

md1                     server1              server2
-------------------------------------------------------------
Mirror Color            GREEN                GREEN
Fast Copy               --                   --
Lastupdate Time         --                   --
Break Time              --                   --
Needed Copy Percent     0%                   0%
Volume Used Percent     64%                  64%
Volume Size             10240MB              10240MB

Server Name             DP Error             CP Error
-------------------------------------------------------------
server1                 NO ERROR             NO ERROR
server2                 NO ERROR             NO ERROR
```

2. When the mirror recovery is required:

```
Status: Abnormal

md1                     server1              server2
-------------------------------------------------------------
Mirror Color            GREEN                RED
Fast Copy               OK                   OK
Lastupdate Time         2021/08/16 18:24:10  --
Break Time              2021/08/16 18:24:01  --
Needed Copy Percent     1%                   0%
Volume Used Percent     64%                  --%
Volume Size             10240MB              10240MB

Server Name             DP Error             CP Error
-------------------------------------------------------------
server1                 NO ERROR             NO ERROR
server2                 NO ERROR             NO ERROR
```

3. When the forcible mirror recovery is required:

```
Status: Abnormal

md1                     server1              server2
-------------------------------------------------------------
Mirror Color            RED                  RED
Fast Copy               NG                   NG
Lastupdate Time         2021/08/16 18:24:10  2021/08/16 18:50:33
Break Time              2021/08/16 18:24:01  2021/08/16 18:24:01
Needed Copy Percent     1%                   1%
Volume Used Percent     64%                  --%
Volume Size             10240MB              10240MB
```

(continues on next page)

(continued from previous page)

```
Server Name            DP Error             CP Error
-------------------------------------------------------------
server1                NO ERROR             NO ERROR
server2                NO ERROR             NO ERROR
```

4. While the mirroring is being recovered:

See " *Checking the mirror recovery progress with a command* ".

For hybrid disk, execute the following command to check the mirror break status.

```
clphdstat --mirror <hybrid_disk_resource_name (Example: hd1)>
```

For details, see "*Displaying the hybrid disk status (clphdstat command)*" in "*9. EXPRESSCLUSTER command reference*" in this guide.

10.3.3 Checking the mirror recovery progress with a command

For mirror disk resources, run the following command to view the progress of recovering mirroring.

```
clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>
```

You will see the following data while mirroring is being recovered.

```
Status: Recovering

md1                server1            server2
-------------------------------------------------------------
Mirror Color       YELLOW      ->     YELLOW
                              15%

Recovery Status
-------------------------------------------------------------
Used Time          00:00:21
Remain Time        00:01:59
```

You will see the following information when the mirror recovery is successfully completed.

```
Status: Normal

md1                    server1              server2
-------------------------------------------------------------
Mirror Color           GREEN                GREEN
Fast Copy              --                   --
Lastupdate Time        --                   --
Break Time             --                   --
Needed Copy Percent    0%                   0%
Volume Used Percent    64%                  64%
Volume Size            10240MB              10240MB

Server Name            DP Error             CP Error
-------------------------------------------------------------
server1                NO ERROR             NO ERROR
server2                NO ERROR             NO ERROR
```

For hybrid disks, execute the following command to check the mirror break status.

```
clphdstat --mirror <hybrid_disk_resource_name (Example: hd1)>
```

For details, see "*Displaying the hybrid disk status (clphdstat command)*" in "*9. EXPRESSCLUSTER command reference*" in this guide.

10.3.4 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: md1)>
  ```

When the difference mirror recovery can be performed, the difference data is used to recover the mirror (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 from the Cluster WebUI*".

10.3.5 Running the forcible mirror recovery with a command

If EXPRESSCLUSTER cannot automatically 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.

Note: The difference mirror recovery function is disabled in the forcible mirror recover, and the data may be fully copied.

Identify the server that holds the latest data by any of the following means:

Using Mirror disks of the Cluster WebUI

1. In the mirror disks of Cluster WebUI, click the mirror disk resource or hybrid disk resource you want to check.
2. Click the **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 / clphdstat command

You can identify the server which has the latest data by using the following commands.

1. Run the following command.
   - For mirror disks:

     ```
     clpmdstat --mirror <mirror_disk_resource_name (Example: md1)>
     ```

   - For hybrid disks:

     ```
     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 disks

Note: This method is not recommended because the data may be damaged if anything goes wrong in the procedure. Use the procedure described in "Using Mirror disks of the Cluster WebUI" or "Using the clpmdstat/clphdstat command" above when possible.

- For mirror disks:

1. Confirm all groups are stopped.
2. Run the following command to connect the mirror disk resource.

   ```
   clpmdctrl --active <mirror_disk_resource_name (Example: md1)> -f
   ```

3. Logically examine the data on the connection destination.
4. Run the following command to disconnect the mirror disk resource.

   ```
   clpmdctrl --deactive <mirror_disk_resource_name (Example: md1)>
   ```

- For hybrid disks:

1. Confirm all groups are stopped.
2. Run the following command to connect the hybrid disk resource.

   ```
   clphdctrl --active <hybrid_disk_resource_name (Example: hd1)> -f
   ```

3. Logically examine the data on the connection destination.
4. Run the following command to disconnect the hybrid disk resource.

   ```
   clphdctrl --deactive <hybrid_disk_resource_name (Example: hd1)>
   ```

When you have identified the server holding the latest data, run the following command to start the forcible mirror recovery.

- For mirror disks (conducted on the server having the latest data):

  ```
  clpmdctrl --force <mirror_disk_resource_name (Example: md1)>
  ```

- For hybrid disks (conducted on the server having the latest data):

  ```
  clphdctrl --force <hybrid_disk_resource_name (Example: hd1)>
  ```

Note: The clpmdctrl --force command and the clphdctrl --force command update data in the server where they are executed. If automatic mirror recovery does not work through this step, perform manual mirror recovery.

The clpmdctrl / clphdctrl command immediately returns the control once the forcible mirror recovery starts. 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".

When the forcible mirror recovery is successfully completed, activate the groups. The mirror disks become available.

10.3.6 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.

Execute the following command on the target server to start forcible mirror recovery.

- For mirror disk resources:

  ```
  clpmdctrl --force <mirror_disk_resource_name (Example: md1)>
  ```

- For mirror disk resources:

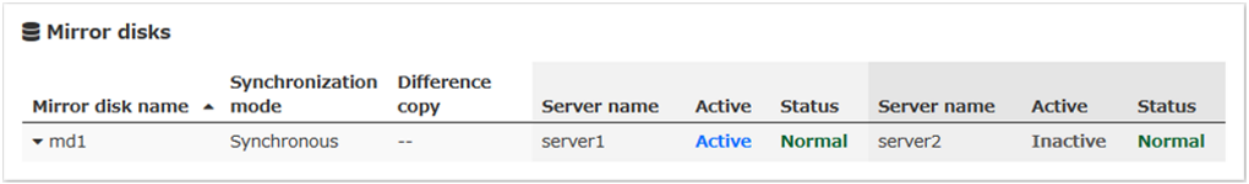
  ```
  clphdctrl --force <hybrid_disk_resource_name (Example: hd1)>
  ```

After executing the command, it becomes possible to start the group to use the resource.

10.3.7 Checking the mirror break status from the Cluster WebUI

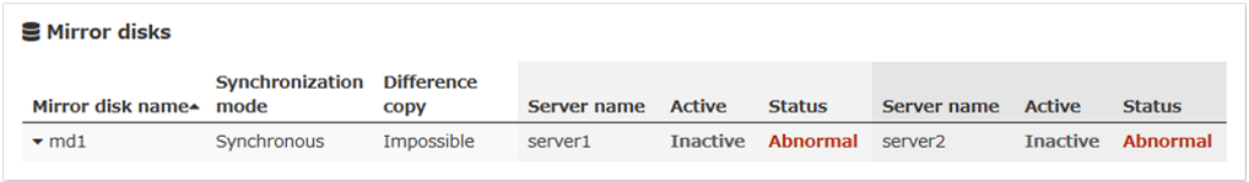
You can see the mirror break status by starting Mirror disks from the Cluster WebUI.

When normal:



When mirror recovery is required:

When forcible mirror recovery is required:



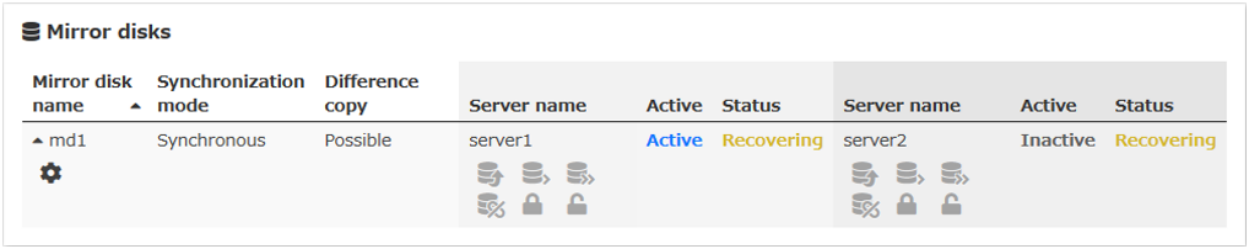
While mirror recovery is in progress:

See " *Checking the mirror recovery progress from the Cluster WebUI* ".

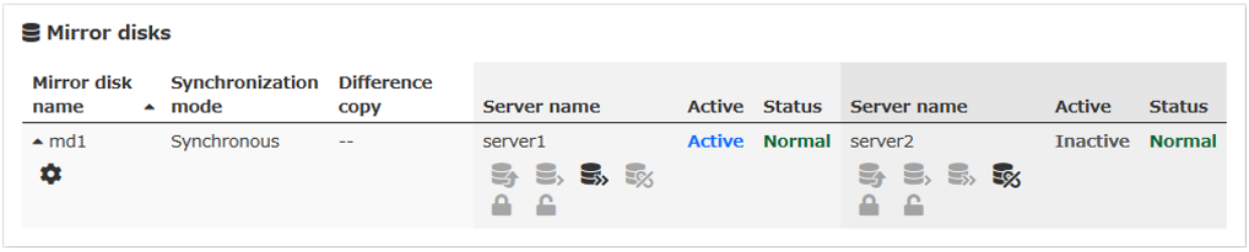
10.3.8 Checking the mirror recovery progress from the Cluster WebUI

From the mirror disks of Cluster WebUI to view the mirror recovery progress.

You will see the following screen during the mirror recovery.



You will see the following screen when the mirror recovery is successfully completed.

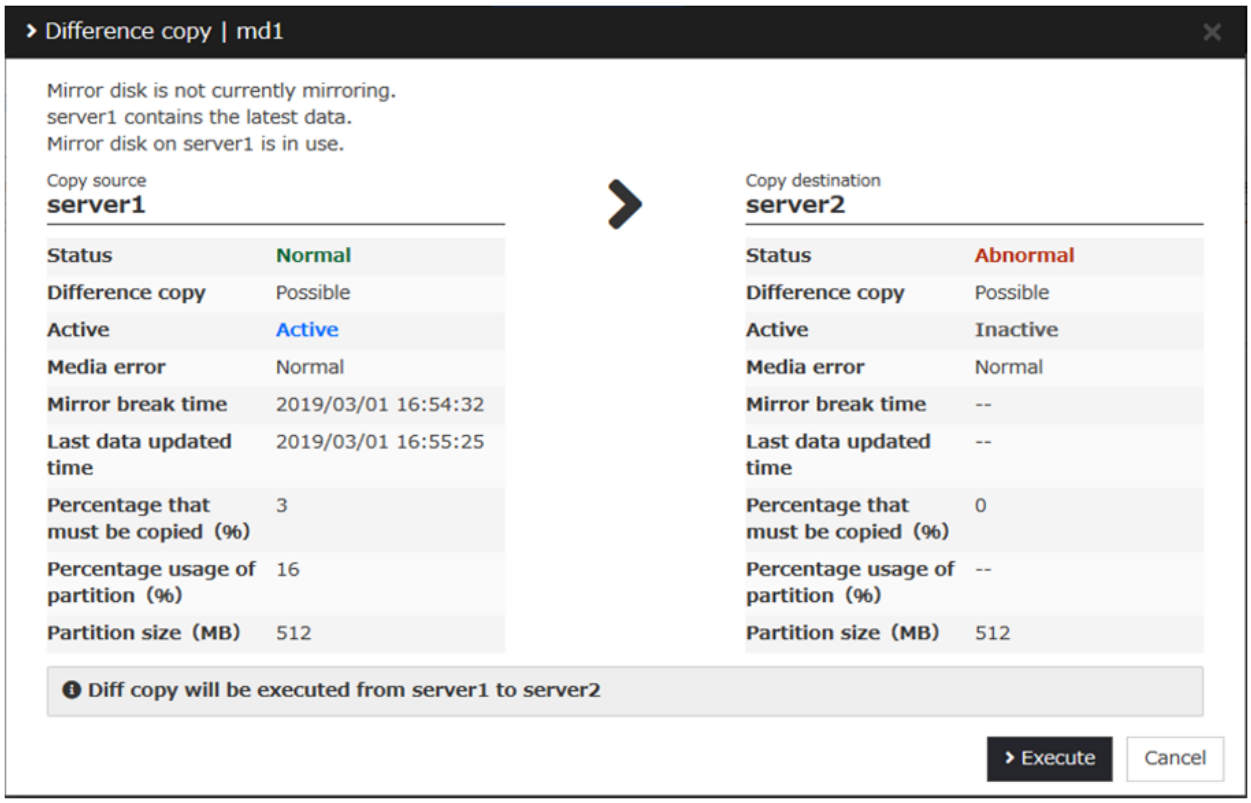


10.3.9 Recovering mirror using the Cluster WebUI

From the mirrors disks of Cluster WebUI, click the name of the mirror disk that needs to be recovered. The window below will be displayed.

Click **Difference Copy** or **Full Copy** of the server that needs to be recovered. Click **Execute** to start the mirror recovery processing.

When the difference mirror recovery can be performed, the recovery is done using the difference data. (FastSync technology)The difference mirror recovery takes less time than the forcible mirror recovery.



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*".

10.3.10 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.

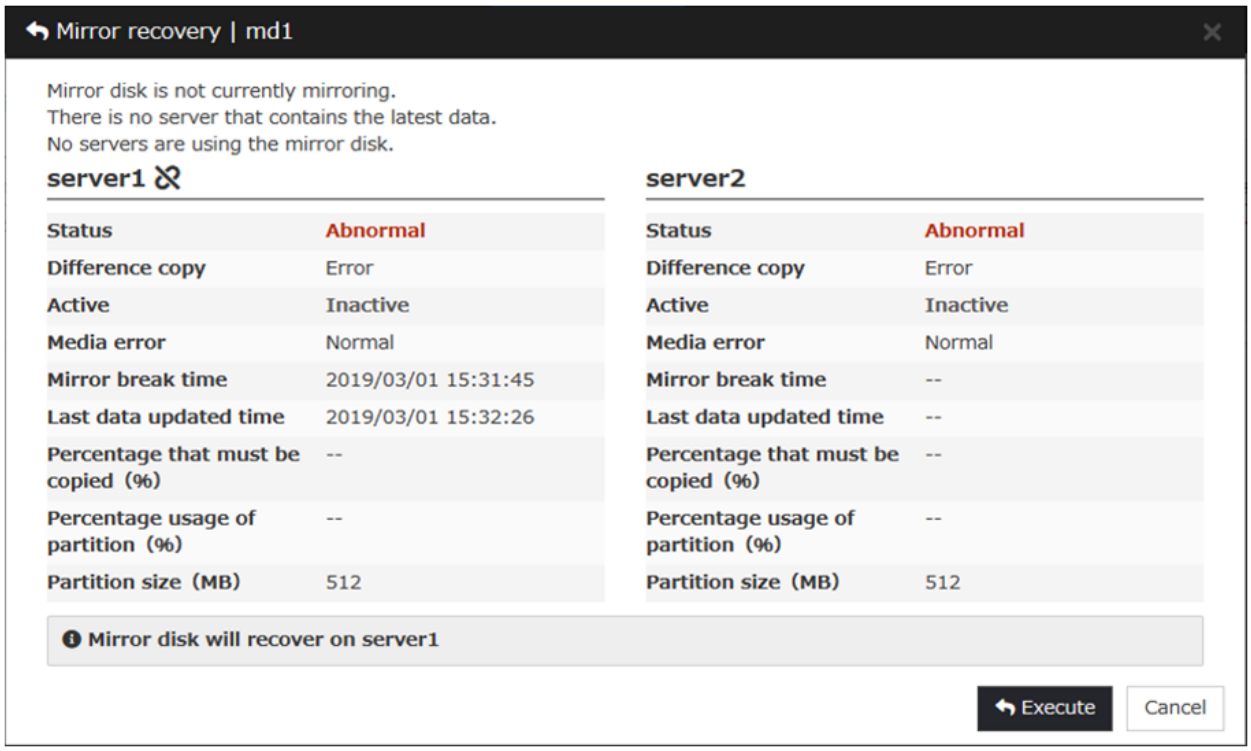
The difference mirror recovery function is disabled in the forcible mirror recovery and the data may be fully copied.

Identify the server that has the latest data by any of the following methods:

Using Mirror disks of the Cluster WebUI

1. From the mirror disks of Cluster WebUI, display the detailed data of the mirror disk resources you want to see.
2. Click the **Details** icon.
3. See the last update time stamp to identify the server which has the latest data. However, this Last Data Updated Time depends on the operating system's clock.

Click **Mirror Recovery** of the server containing the latest data to display the following window. Click **Execute** to start the mirror recovery processing.



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*".

When the forcible mirror recovery is successfully completed, you can activate the groups and use the mirror disks.

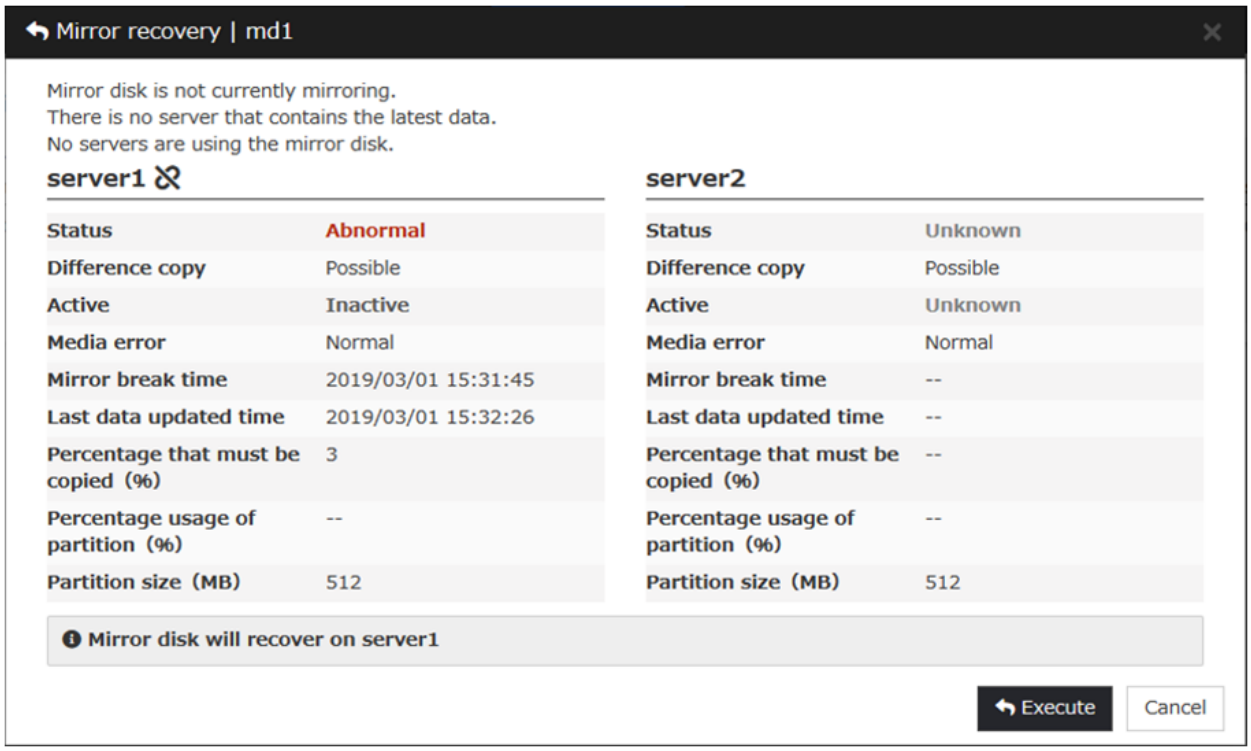
10.3.11 Running the forcible mirror recovery from the Cluster WebUI only on one server

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 no matter which server actually has it. 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.

From the mirror disks of Cluster WebUI, execute the forcible mirror recovery. Click **Mirror Recovery** of the server to which you want to perform the forcible mirror recovery, and then the following window appears. Click **Execute** to perform the forcible mirror recovery processing.

When the forcible mirror recovery is successfully completed, you can activate the groups and use the mirror disks.


Mirror recovery | md1
Mirror disk is not currently mirroring.
There is no server that contains the latest data.
No servers are using the mirror disk.
server1
Status
Abnormal
Difference copy
Possible
Active
Inactive
Media error
Normal
Mirror break time
2019/03/01 15:31:45
Last data updated time
2019/03/01 15:32:26
Percentage that must be copied (%)
3
Percentage usage of partition (%)
--
Partition size (MB)
512
server2
Status
Unknown
Difference copy
Possible
Active
Unknown
Media error
Normal
Mirror break time
--
Last data updated time
--
Percentage that must be copied (%)
--
Percentage usage of partition (%)
--
Partition size (MB)
512
Mirror disk will recover on server1
Execute
Cancel

10.4 Media sense function becomes invalid

Media sense function is the OS function that detects disconnection of network cable. When disconnection is detected, TCP/IP receives a notification from the media sense function and renders the information such as an IP address assigned to the disconnected network card unavailable while it is disconnected. EXPRESSCLUSTER cannot be operated properly if the information such as IP address becomes invalid during its operation, so the media sense function is rendered invalid when installing EXPRESSCLUSTER.

CHAPTER

ELEVEN

ERROR MESSAGES

This chapter provides information on error messages you might encounter in operating EXPRESSCLUSTER.

This chapter covers:

11.1 Messages

11.2 Messages during setup

Module Type	Error Message	Solution
setup	Previous version of EXPRESSCLUSTER is installed. Upgrading from this version is not supported. Install after uninstalling the previous version of EXPRESSCLUSTER.	Uninstall the previous version of EXPRESSCLUSTER, and then try installing again.
setup	The SNMP service is running. You need to stop the SNMP service before you perform uninstallation. Do you want to stop the SNMP service now?	Select Yes to stop the SNMP service automatically and continue the installation. Or, select No to cancel the installation, manually stop the SNMP service and then perform installation again.
setup	Setup has failed. Error code : xxx	- Check the system requirements, setup procedures and notes described in the manual, and make sure they are followed. - If other application is running, terminate it. - Install again after restarting the OS.
setup	Setup has failed(xxx). Error code : xxx Please reboot the system and try again.	- Check the system requirements, setup procedures and notes described in the manual, and make sure these requirements are followed. - If other application is running, terminate it. - Install again after starting the OS again.
setup	Unsupported environment.	Install in the environment where the system requirements are met.
setup	Cannot perform uninstallation because there is one or more EXPRESSCLUSTER services still running. Stop all EXPRESSCLUSTER services before you restart uninstallation.	Stop all EXPRESSCLUSTER services, and then perform uninstallation.
setup	Failed to start the installer. (ercode: xxx)	- Check the system requirements, setup procedures and notes described in the manual, and make sure they are followed. - If other application is running, terminate it. - The installer file may be corrupted or missing. Check it.

Continued on next page

Table 11.1 – continued from previous page

Module Type	Error Message	Solution
setup	Internal error. (xxx)	- Check the system requirements, setup procedures and notes described in the manual, and make sure they are followed. - If other application is running, terminate it.

11.3 Messages reported by event log and alert

These are the messages reported by applications, event logs, and alert logs of the Cluster WebUI. Messages with o in the columns of Alert, Eventlog and Userlog are recorded in each log. The following shows how to refer the logs:

Log Name	How to refer	File Name
Alert	Output to the Alert Logs of the Cluster WebUI. Logs can be collected by using the log collection tool.	alertlog.alt
Event log	Output to the Event Viewer (application log) of the OS. Collect logs by using the log collection tool. The source of the event is "EXPRESSCLUSTER X." Logs can be collected by using the log collection tool. Note because they are collected in the binary format with the file names in the right column, it is necessary to open the files using Event Viewer in the environment where EXPRESSCLUSTER is set up to refer to the information.	Application.evtx System.evtx
User log	These are the logs with text format, in which detail information is recorded. They are output in the "userlog.{00 - 02}.log" file in the log folder of the logs collected by using the log collection tool.	userlog.{00 - 02}.log

Messages with "o" in the Mail Report column will be sent as e-mail by EXPRESSCLUSTER X Alert Service.

Messages with "o" in the SNMP Trap column will be sent as SNMP trap.

"Report Settings" are settings of when linking to the ESMPRO Agent. In "Alive," the ESMPRO Agent performs the Alert report. In "Manager," alerts are output to the ESMPRO Agent. For details, see the manual of the ESMPRO Agent**.**

For Mail Alert and SNMP Trap sending, refer to "*Alert Service tab*" of "*Cluster properties*" in "2. *Parameter details*" and "*Alert Service*" in "8. *Information on other settings*"

The report settings in "*Alert Service tab*" of "2. *Parameter details*" cannot be configured for any message marked with x.

If the "o" mark is shown in the Message Topic column, the message on that row is reported when Amazon SNS linkage function is enabled.

For details of Amazon SNS linkage function, see "2. *Parameter details*" - "2.2. *Cluster properties*" - "2.2.17. *Cloud tab*".

In the table below, each number indicates the following:

[1]Alert, [2]Eventlog, [3]Userlog, [4]Mail Report, [5]SNMP Trap, [6]Alive, [7]Manager, [8]Message Topic

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
nm	Information	1	The server %1 has been started.	Server up	-	o	o						
nm	Information	2	The server %1 has been stopped.	Server down	Server down was detected. Remove the failures of the server and then return the server to the cluster.	o	o		o	o	o	o	o
nm	Information	3	The resource %2 of the server %1 has been started.	Resource up	-			o					
nm	Error	4	The resource %2 of the server %1 has an error.	Resource abnormally	An error of the resource was detected. Refer to the event logs of the appropriate resource.			o					
nm	Information	5	The resource %2 of the server %1 has been recovered to the normal status.	Resource recover	-			o					
nm	Error	6	The resource %2 of the server %1 is unknown.	Resource unknown	Check the cluster configuration data.	o	o					o	
nm	Error	7	Network partition was detected. Shut down the server %1 to protect data.	Network partition detected	No heartbeat resources can be used. Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o			o	o	
nm	Error	8	An error occurred while confirming the network partition. Shut down the server %1.	It was not possible to check for a network partition.	Refer to the event logs to check whether an error has occurred in a resource.	o	o	o			o	o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
nm	Error	9	An error occurred in confirming the network partition. To avoid failover on multiple servers, the server %1 suspended failover.	Failover hold	Refer to the event logs to check whether an error has occurred in a resource.	o	o	o			o	o	
nm	Information	10	The server %1 canceled the pending failover.	Failover hold cancel	-	o	o	o					
nm	Error	11	Shut down the server %1. (reason:%2)	Server shut-down	No heartbeat resources can be used. Make sure there is no error in the network adapter and the network is correctly connected.	o	o				o	o	
nm	Error	12	Cluster service will be stopped. (reason:%1)	Cluster service stopping	Check the cause following the message.	o	o					o	
nm	Warning	13	The combination of the network partition resources is invalid. (server name:%1)	NP resource combination error	Check the cluster configuration data.	o	o					o	
nm	Error	14	The status of heartbeat %1 is abnormal.	Heartbeat abnormally	Make sure there is no error in the network adapter and the network is correctly connected.	o	o				o	o	
nm	Information	15	The heartbeat %1 has been recovered to the normal status.	Heartbeat recovered	-	o	o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
nm	Error	16	The network partition %2 of the server %1 has an error.	Network partition abnormally	Refer to the event logs to check whether an error has occurred in a resource.	o	o				o	o	
nm	Information	17	The network partition %2 of the server %1 has been recovered to the normal status.	Network partition recovered	-	o	o						
nm	Error	18	Failed to start the resource %1. Server name:%2	Resource start failed	Refer to the event logs to check whether an error has occurred in a resource.	o	o				o	o	
nm	Information	19	Waiting for servers to start up has been canceled.	Waiting for servers to start up has been canceled.	-	o	o						
nm	Error	20	Network partition was detected. Shut down the server %1 for the cluster service to protect data.	Network partition detected	No heartbeat resources can be used. Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o					
nm	Error	21	An error occurred when checking for a network partition. Shut down the server %1 for the cluster service to protect data.	It was not possible to check for a network partition.	Refer to the event logs to check whether an error has occurred in a resource.	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
nm	Error	22	Network partition was detected. Execute action(%1) on the server %2 for the cluster service to protect data.	Network partition	No heartbeat resources can be used. Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o					
nm	Error	23	An error occurred when checking for a network partition. Execute action(%1) on the server %2 for the cluster service to protect data.	Can not network partition resolution	Refer to the event logs to check whether an error has occurred in a resource.	o	o	o					
nm	Error	24	Execute action(%1) on the server %2. (reason:%3)	Can not network partition resolution	No heartbeat resources can be used. Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o					
nm	Warning	25	The NP resolution process at the cluster startup is disabled.	Network partition resolution disabled	The NP resolution process at the cluster startup is disabled.	o	o	o					
nm	Error	102	The server %1 has been stopped.	Server down	Server down was detected. Remove the failures of the server and then return the server to the cluster.	o	o		o	o	o	o	o
pm	Information	501	Cluster service has been started properly.	Cluster service started	-	o	o	o					
pm	Information	502	Cluster service is shutting down.	Cluster service shutting down	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
pm	Error	510	Cluster service has already been started.	Cluster service already started	Check the status of cluster service.	o	o	o				o	
pm	Error	511	Fatal error has occurred in the cluster service.	Critical error in cluster service	The service is not run by a user with required privilege or the system may not be able to operate properly.	o	o	o	o	o		o	o
pm	Error	512	An error is detected in xml library.	problem detected in xml library	The system may not be able to operate properly.	o	o	o				o	
pm	Error	513	An error is detected in configuration file.	problem detected in configuration file	Check the cluster configuration data.	o	o	o	o	o		o	o
pm	Error	514	Configuration file does not exist.	Configuration file not exists	Upload the cluster configuration data.	o	o	o				o	
pm	Error	515	My host name is not found in configuration file.	my name not found in configuration file	Check the cluster configuration data.	o	o	o				o	
pm	Warning	516	The recovery action is configured to change from an OS stop to an OS restart.	Checking the configuration of cluster properties.	-	o	o	o					
pm	Error	520	%1 process terminated abnormally.	process exit abnormally	The system may not be able to operate properly.	o	o	o	o	o		o	o
pm	Error	521	The cluster service process returned an error. (halting system)	Rc process exit with error	Deactivation of group resources may be failed. Take appropriate action by following the group resource message.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
pm	Error	522	An error has occurred while initializing %1 process. (return code:%2)	process init error	Check the cause of an initialization error and troubleshoot it.	o	o	o	o	o		o	o
pm	Information	523	The system will be shut down.	system halting	-	o	o	o					
pm	Information	524	Cluster service will be stopped.	Cluster service stopping	-	o	o	o					
pm	Information	525	System will be rebooted.	System rebooting	-	o	o	o					
pm	Information	526	%1 process will be restarted.	Process restarting	-	o	o	o					
pm	Information	527	Emergency shutdown is in progress.	Emergency shutdown	-	o	o	o					
pm	Information	528	Generating STOP error.	Stop Error	-	o	o	o					
pm	Information	529	Generating hardware reset.	HW reset	-	o	o	o					
pm	Information	530	There was a request to shut down the system from the %1.	request of system halt	-	o	o	o					
pm	Information	531	There was a request to stop cluster service from the %1.	request of cluster service stop	-	o	o	o					
pm	Information	532	There was a request to reboot system from the %1.	request of system reboot	-	o	o	o					
pm	Information	533	There was a request to restart cluster service from the %1.	request of cluster service restart	-	o	o	o					
pm	Information	534	There was a request to resume cluster service from the %1.	request of cluster service resume	•	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
pm	Information	535	There was a request to suspend cluster service from the %1.	request of cluster service suspend	-	o	o	o					
pm	Information	536	There was a request of emergency shutdown from the %1.	request of emergency shutdown	-	o	o	o					
pm	Information	537	There was a request to generate STOP error from the %1.	request of STOP error	-	o	o	o					
pm	Information	538	There was a request to generate hardware reset from the %1.	request of HW reset	-	o	o	o					
pm	Information	540	Requesting shutdown to the automatic running control software.	shutdown request to the automatic running control software start	-	o	o	o					
pm	Information	541	Requesting shutdown (reboot) to the automatic running control software.	shutdown (reboot) request to the automatic running control software	-	o	o	o					
pm	Information	542	Shutdown request to the automatic running control software is completed.	shutdown request to the automatic running control software complete	-	o	o	o					
pm	Error	543	The automatic running control software returned an error to the shutdown request.	shutdown by ESMPRO/AC fail	The automatic operating settings may be incorrect. Check the settings.	o	o	o				o	
pm	Error	544	Communications with the automatic running control software failed.	Communications with ESMPRO/AC fail	The system may not be able to operate properly.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
pmsvc	Error	801	The system will be shutdown because cluster resume was failed.	Failed to resume the cluster daemon	-	o	o	o					
pmsvc	Error	802	An attempt to shutdown the system failed.	Failed to shutdown the system	The system may not be able to operate properly.	o	o	o					
pmsvc	Information	810	The system shutdown was initiated by other than cluster service. Stopping cluster service. (timeout=%1 min).	Stopping cluster service.	-	o	o	o					
pmsvc	Information	811	Stopping cluster service has been completed.	Stopping cluster service has been completed.	-	o	o	o					
pmsvc	Error	812	Stopping cluster service has timed out.	Stopping cluster service has timed out.	-	o	o	o					
pmsvc	Warning	813	Stopping cluster service has been canceled.	Stopping cluster service has been canceled.	-	o	o	o					
rc	Information	1010	The group %1 is starting.	group-start started	-	o	o	o					
rc	Information	1011	The group %1 has been started.	group-start ended	-	o	o	o					
rc	Error	1012	Failed to start the group %1.	group-start failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Information	1015	Waiting for group %1 to start has started.	waiting for group to start has started.	-	o	o	o					
rc	Information	1016	Waiting for group %1 to start has been completed.	waiting for group to start has been completed.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Error	1017	Group start was canceled because waiting for group %1 to start was timed out. (%2)	waiting for 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	o					
rc	Warning	1018	Waiting for group %1 to start has timed out. However, group start continues. (%2)	group start continues.	-	o	o	o					
rc	Warning	1019	Server %1 is not in a condition to start group %2.	cannot-start-group	Perform server recovery if the target server is suspended (Isolated). If it is suspended (Network Partition Unsolved), recover network partition resources to the normal status.	o							
rc	Information	1020	The group %1 is stopping.	group-stop started	-	o	o	o					
rc	Information	1021	The group %1 has been stopped.	group-stop ended	-	o	o	o					
rc	Error	1022	Failed to stop the group %1.	group-stop failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Information	1025	Waiting for group %1 to stop has started.	waiting for group to stop has started.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1026	Waiting for group %1 to stop has started.	waiting for group to stop has been completed.	-	o	o	o					
rc	Error	1027	Group stop has been canceled because waiting for group %1 to stop has timed out. (%2)	waiting for 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	o					
rc	Warning	1028	Waiting for group %1 to stop has timed out. However, group stop continues. (%2)	group stop continues.	-	o	o	o					
rc	Information	1030	The resource %1 is starting.	resource-start started	-		o	o					
rc	Information	1031	The resource %1 has been started.	resource-start ended	-		o	o					
rc	Error	1032	Failed to start the resource %1. (%2 : %3)	resource-start failed	Check the cause for failing to start the resource. If a stall occurs during start processing, "Failed to start the resource %1. (99 : command is timeout)" is output.	o	o	o	o	o		o	o

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Error	1033	Failed to start the recovery script of resource %1. (%2 : %3)	recoverscript-start failed	Check the cause for failing to start the recovery script.	o	o	o				o	
rc	Information	1034	A request to activate %1 resource on server %2 has been started.	Resource start request to the standby server	-	o	o	o					
rc	Information	1035	A request to activate %1 resource on server %2 has been completed.	Resource start request to the standby server completed.	-	o	o	o					
rc	Error	1036	A request to activate %1 resource on server %2 has been failed.	Resource activation request to the standby server failed.	Check if there is an error with the network or with the remote server.	o	o	o					
rc	Information	1037	Since the startup attribute is set to manual, the activation of resource %1 was suppressed.	Resource activation suppressed	-	o	o	o					
rc	Information	1040	The resource %1 is stopping.	resource-stop started	-		o	o					
rc	Information	1041	The resource %1 has been stopped.	resource-stop ended	-		o	o					
rc	Error	1042	Failed to stop the resource %1. (%2 : %3)	resource-stop failed	Check the cause for failing to stop the resource. If a stall occurs during stop processing, "Failed to stop the resource %1. (99 : command is timeout)" is output.	o	o	o	o	o		o	o

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1043	Waiting for resource %1 to stop has canceled. However, resource stop continues.	waiting for resource to stop has canceled	-		o	o					
rc	Information	1044	A request to stop %1 resource on server %2 has been started.	Resource stop request to the standby server	-	o	o	o					
rc	Information	1045	A request to stop %1 resource on server %2 has been completed.	Resource stop request to the standby server completed.	-	o	o	o					
rc	Error	1046	A request to stop %1 resource on server %2 has been failed.	Resource stop request to the standby server failed.	Check if there is an error with the network or with the remote server.	o	o	o					
rc	Information	1050	Moving the group %1.	group-move started	-	o	o	o					
rc	Information	1051	The group %1 has been moved.	group-move ended	-	o	o	o					
rc	Error	1052	Failed to move the group %1.	group-move failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Warning	1059	Server %1 is not in a condition to move group %2.	cannot-move-group	Perform server recovery if the target server is suspended (Isolated). If it is suspended (Network Partition Unsolved), recover network partition resources to the normal status.	o							
rc	Information	1060	Failing over the group %1.	group-failover started	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1061	The group %1 has been failed over.	group-failover ended	-	o	o	o					
rc	Error	1062	Failed to fail over the group %1.	group-failover failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Information	1070	Restarting the group %1.	group-restart started	-	o	o	o					
rc	Information	1071	The group %1 has been restarted.	group-restart ended	-	o	o	o					
rc	Error	1072	Failed to restart the group %1.	group-restart failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Error	1077	Group failover has failed because there is a server incapable of internal communication.	group-failover failed (internal communication disabled)	Check the LAN heartbeat status in kernel mode. Start the group after recovering internal communication.	o	o	o					
rc	Information	1080	Restarting the resource %1.	resource-restart started	-	o	o	o					
rc	Information	1081	The resource %1 has been restarted.	resource-restart ended	-	o	o	o					
rc	Error	1082	Failed to restart the resource %1.	resource-restart failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Information	1090	Shutting down the cluster.	cluster shutdown	-	o	o	o					
rc	Information	1091	Shutting down the server.	server shutdown	-	o	o	o					
rc	Error	1092	Group %1 is started on more than one server.	group double start	Server will automatically be shut down. Check the cause for the group to be started in more than one server.	o	o	o	o	o		o	o

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Error	1093	The system shutdown was performed by other than the cluster service.	system shutdown by other than cluster service	It is considered as an error if the system shuts down by other than cluster service. Follow the appropriate steps to shut down the system.	o	o	o				o	
rc	Warning	1100	Shutdown count is reached the maximum number (%1). Final action of resource %2 was ignored.	shutdown count reached the limit	-	o	o	o	o	o		o	o
rc	Warning	1101	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	o					
rc	Warning	1102	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	o					
rc	Warning	1103	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	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Warning	1104	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	o					
rc	Information	1105	Since server %1 is not specified as that which suppresses shutdown at both-system activation detection, it executed the shutdown request.	Shutdown caused by both-system	-	o	o	o					
rc	Information	1106	The number of reboots due to group resource errors has been reset.	Resetting the reboot count (group resource)	-	o	o	o					
rc	Information	1110	Server %1 is returned to the cluster.	server returned	-	o	o	o					
rc	Information	1111	Server %1 is isolated from the cluster.	server isolated	-	o	o	o					
rc	Information	1112	Server %1 started to return to the cluster.	server return start	-	o	o	o					
rc	Error	1113	Server %1 failed to return to the cluster.	server return fail	The system may not be able to operate properly.	o	o	o				o	
rc	Information	1120	Server %1 will notify the automatic running control software of shutdown start.	shutdown notification start	-	o	o	o					
rc	Error	1121	The automatic running control software returned an error to the shutdown start notification in server %1.	shutdown notification fail	The automatic operating settings may be incorrect. Check the settings.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1122	Server %1 notified the automatic running control software of shutdown start.	shutdown notification finish	-	o	o	o					
rc	Information	1123	The automatic running control software is checking the power status of shared disks. A server will be restarted after the power status is checked.	waiting for disk power-on	-	o	o	o					
rc	Error	1124	An error was returned from the automatic running control software. Failed to check the power status of shared disks.	disk power-on confirmation failed	The automatic operating settings may be incorrect. Check the settings. An error may have occurred in the automatic power control unit. Check the automatic power control unit.	o	o	o				o	
rc	Error	1125	Server %1 failed to communicate with the automatic running control software.	communications with the automatic running control software failed	The system may not be able to operate properly.	o	o	o				o	
rc	Information	1130	Starting a single resource %1.	single-resource-start started	-	o	o	o					
rc	Information	1131	A single resource %1 has been started.	single-resource-start ended	-	o	o	o					
rc	Error	1132	Failed to start a single resource %1.	single-resource-start failed	Take appropriate action by following the group resource message.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Warning	1139	Server %1 is not in a condition to start a single resource %2.	cannot-start-single-resource	Perform server recovery if the target server is suspended (Isolated). If it is suspended (Network Partition Unsolved), recover network partition resources to the normal status.	o							
rc	Information	1140	Stopping a single resource %1.	single-resource-stop started	-	o	o	o					
rc	Information	1141	A single resource %1 has been stopped.	single-resource-stop ended	-	o	o	o					
rc	Error	1142	Failed to stop a single resource %1.	single-resource-stop failed	Take appropriate action by following the group resource message.	o	o	o				o	
rc	Information	1150	The group %1 is being migrated.	The group is being migrated.	-	o	o	o					
rc	Information	1151	The group %1 has been migrated.	The group has been migrated.	-	o	o	o					
rc	Error	1152	Failed to migrate the group %1.	Migrating the group has failed.	Take appropriate action by following the group resource message.	o	o	o					
rc	Warning	1159	Server %1 is not in a condition to migrate group %2.	The group cannot be migrated.	Perform server recovery if the target server is suspended (isolated). If it is suspended (due to an unresolved network partition), recover network partition resources to the normal status.	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1170	Server %1 in the same server group (%2) has been set as the destination for the group %3.	The destination found in the same server group	-	o	o	o					
rc	Information	1171	Server %1 not in the same server group (%2) has been set as the destination for the group %3.	The destination found in the other server group	-	o	o	o					
rc	Warning	1179	Can not fail over the group %1 because there is no appropriate destination in the same server group %2.	The destination not found in the same server group	Check if other servers in the same server group are stopped or isolated. If so, start the servers or return the servers to the cluster.	o	o	o					
rc	Information	1200	The resource %1 will be restarted since starting the resource %2 failed.	resource-restart by resource-acterr	-	o	o	o					
rc	Information	1201	The group %1 will be failed over to server %2 since starting the resource %3 failed.	group-failover by resource-acterr	-	o	o	o					
rc	Information	1202	The group %1 will be stopped since starting the resource %2 failed.	group-stop by resource-acterr	-	o	o	o					
rc	Information	1203	The cluster service will be stopped since starting the resource %1 failed.	service-stop by resource-acterr	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1204	The system will be shut down since starting the resource %1 failed.	shutdown-system by resource-acterr	-	o	o	o					
rc	Information	1205	The system will be re-booted since starting the resource %1 failed.	reboot-system by resource-acterr	-	o	o	o					
rc	Information	1220	The resource %1 will be stopped again since stopping the resource %2 failed.	resource-stop retry by resource-deacterr	-	o	o	o					
rc	Information	1223	The cluster service will be stopped since stopping the resource %1 failed.	service-stop by resource-deacterr	-	o	o	o					
rc	Information	1224	The system will be shut down since stopping the resource %1 failed.	shutdown-system by resource-deacterr	-	o	o	o					
rc	Information	1225	The system will be re-booted since stopping the resource %1 failed.	reboot-system by resource-deacterr	-	o	o	o					
rc	Information	1241	Hardware reset will be generated since starting the resource %1 failed.	hw-reset by resource-acterr	-	o	o	o					
rc	Information	1242	STOP error will be generated since starting the resource %1 failed.	stop-error by resource-acterr	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1281	Hardware reset will be generated since stopping the resource %1 failed.	hw-reset by resource-deacterr	-	o	o	o					
rc	Information	1282	STOP error will be generated since stopping the resource %1 failed.	stop-error by resource-deacterr	-	o	o	o					
rc	Information	1300	Script before final action upon activation failure in resource %1 started.	Script before final action upon resource activation failure started.	-	o	o	o					
rc	Information	1301	Script before final action upon activation failure in resource %1 completed.	Script before final action upon resource activation failure completed.	-	o	o	o					
rc	Information	1302	Script before final action upon deactivation failure in resource %1 started.	Script before final action upon resource deactivation failure started.	-	o	o	o					
rc	Information	1303	Script before final action upon deactivation failure in resource %1 completed.	Script before final action upon resource deactivation failure completed.	-	o	o	o					
rc	Information	1304	Script before activation in resource %1 started.	Script before resource activation started.	-	o	o	o					
rc	Information	1305	Script before activation in resource %1 completed.	Script before resource activation completed.	-	o	o	o					
rc	Information	1306	Script after activation in resource %1 started.	Script after resource activation started.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1307	Script after activation in resource %1 completed.	Script after resource activation completed.	-	o	o	o					
rc	Information	1308	Script before deactivation in resource %1 started.	Script before resource deactivation started.	-	o	o	o					
rc	Information	1309	Script before deactivation in resource %1 completed.	Script before resource deactivation completed.	-	o	o	o					
rc	Information	1310	Script after deactivation in resource %1 started.	Script after resource deactivation started.	-	o	o	o					
rc	Information	1311	Script after deactivation in resource %1 completed.	Script after resource deactivation completed.	-	o	o	o					
rc	Error	1340	Script before final action upon activation failure in resource %1 failed.	Script before final action upon resource activation failure failed.	Check the cause of the script failure and take measures.	o	o	o				o	
rc	Error	1341	Script before final action upon deactivation failure in resource %1 failed.	Script before final action upon resource deactivation failure failed.	Check the cause of the script failure and take measures.	o	o	o				o	
rc	Error	1342	Failed to execute script before activation in resource %1.	Script before resource activation failed.	Check the cause of the script failure and take measures.	o	o	o				o	
rc	Error	1343	Failed to execute script after activation in resource %1.	Script after resource activation has failed.	Check the cause of the script failure and take measures.	o	o	o				o	
rc	Error	1344	Failed to execute script before deactivation in resource %1.	Script before resource deactivation failed.	Check the cause of the script failure and take measures.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Error	1345	Failed to execute script after deactivation in resource %1.	Script after resource deactivation failed.	Check the cause of the script failure and take measures.	o	o	o				o	
rc	Error	1346	Failed to log on as a user.	Logon as a user failed	Check if the domain, account and password of the execution user are correctly set.	o	o	o					
rc	Information	1400	The status of the regular check for a forced stop returned to normal.	Normal status for a forced stop	-	o	o	o					
rc	Error	1401	The regular check for a forced stop detected an abnormality.	Abnormal status for a forced stop	The forced-stop function may not be working normally. Identify the cause.	o	o	o					
rc	Error	1402	The request for forcibly stopping the server has been timed out.	Timeout of the forced-stop request	Identify the cause of the timeout and take measures.	o	o	o					
rc	Information	1403	The request for forcibly stopping the server will be retried.	Retrying the forced-stop request	-	o	o	o					
rc	Error	1404	The check of forcibly stopping the server has been timed out.	Timeout of the forced-stop check	Identify the cause of the timeout and take measures.	o	o	o					
rc	Information	1405	The check of forcibly stopping the server will be retried.	Retrying the forced-stop check	-	o	o	o					
rc	Error	1411	The regular check for a forced stop detected an abnormality. (%1)	Abnormal status for a forced stop	The forced-stop function may not be working normally. Identify the cause.	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1415	The check of forcibly stopping the server will be retried. (%1)	Retrying the forced-stop check	-	o	o	o					
rc	Warning	1427	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 failure and take measures.	o	o	o					
rc	Warning	1430	The group %1 which were activated on the server %2 will be activated on the same server because its reboot has been completed within the heartbeat timeout.	Server rebooted before the heartbeat timeout occurs.	Adjust the OS startup time so that the server reboot is not completed before the heartbeat timeout occurs.	o	o	o					
rc	Warning	1450	Cluster operation is disabled.	Cluster operation is disabled.	-	o	o	o					
rc	Warning	1451	Ignored the automatic start of groups because automatic group startup is disabled.	Automatic group startup is not executed.	-	o	o	o					
rc	Warning	1452	Ignored the recovery action in resource activation because recovery action caused by group resource activation error is disabled.	Resource recovery action is not executed.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Warning	1453	Ignored the recovery action in resource deactivation because recovery action caused by group resource deactivation error is disabled.	Resource recovery action is not executed.	-	o	o	o					
rc	Information	1454	Cluster operation is set disabled.	Cluster operation is disabled.	-	o	o	o					
rc	Information	1455	Cluster operation is set enabled.	Cluster operation is enabled.	-	o	o	o					
rc	Warning	1456	Cluster operation is forcibly disabled since a valid license has not been registered.	Cluster operation is forcibly disabled (License disabled).	Register the license. Canceling the forcible disablement of cluster operation requires up to 1 hour after the license is registered. To cancel it immediately, suspend and resume the cluster after the license registration.	o	o	o					
rc	Information	1457	The forcible disablement of cluster operation was canceled since the valid licenses are registered.	Forcible disablement of cluster operation is canceled.	-	o	o	o					
rc	Warning	1458	Ignored the group failover because failover for a server failure is disabled.	Group failover is not executed.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Information	1470	Server %1 has been set as the destination for the group %2 (reason: %3).	destination found	-	o	o	o					
rc	Warning	1471	There is no appropriate destination for the group %1 (reason: %2).	destination not found	Check if any monitor resources detects an error on the other servers.	o	o	o				o	
rc	Warning	1472	Server %1 is not in a condition to start group %2 (reason: %3).	not in a condition to start group	Check if any monitor resources detects an error on the server.	o	o	o					
rc	Error	1480	Group start has been canceled because waiting for group %1 to start has failed. (%2)	waiting for group to start failed	-	o	o	o					
rc	Warning	1481	Waiting for group %1 to start has failed. However, group start continues. (%2)	waiting for group to start failed	-	o	o	o					
rc	Error	1482	Group start has been canceled because waiting for group %1 to start has canceled.	waiting for group to start canceled	-	o	o	o					
rc	Warning	1483	Waiting for group %1 to start has canceled. However, group start continues.	waiting for group to start canceled	-	o	o	o					
rc	Error	1484	Group stop has been canceled because waiting for group %1 to stop has failed. (%2)	waiting for group to stop failed	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rc	Warning	1485	Waiting for group %1 to stop has failed. However, group stop continues. (%2)	waiting for group to stop failed	-	o	o	o					
rc	Error	1486	Group stop has been canceled because waiting for group %1 to stop has canceled.	waiting for group to stop canceled	-	o	o	o					
rc	Warning	1487	Waiting for group %1 to stop has canceled. However, group stop continues.	waiting for group to stop canceled	-	o	o	o					
rc	Information	1490	Group %1 started to check the double activation.	check the double activation started	-			o					
rc	Information	1491	Group %1 completed to check the double activation.	check the double activation ended	-			o					
rc	Error	1492	Group %1 failed to check the double activation.	check the double activation failed	Check the status of the group.	o	o	o				o	
rc	Information	1493	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	o					
rm	Information	1501	Monitor %1 has been started.	Monitor start	-	o	o	o					
rm	Information	1502	Monitor %1 has been stopped.	Monitor stop	-	o	o	o					
rm	Information	1503	Monitor %1 does not monitor in this server.	Not target server	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Warning	1504	Monitor %1 is in the warning status. (%2 : %3)	Monitor warn	Check the cause of Warning.	o	o	o				o	
rm	Warning	1505	The number of monitor resources reached the maximum number. (registered resource: %1)	invalid number of monitor resource	Check the cluster configuration data.	o	o	o				o	
rm	Warning	1506	Configuration of %1 is invalid. (%2 : %3)	invalid monitor resource	Check the cluster configuration data.	o	o	o				o	
rm	Error	1507	Failed to start monitor %1.	monitor starting failed	The system may not be able to operate properly.	o	o	o	o	o		o	o
rm	Error	1508	Failed to stop monitor %1.	monitor stopping failed	The system may not be able to operate properly.	o	o	o				o	
rm	Error	1509	Monitor %1 detected an error. (%2 : %3)	monitor failed	Check the cause for monitor error.	o	o	o	o	o		o	o
rm	Information	1510	Monitor %1 is not monitored.	not monitored	-	o	o	o					
rm	Information	1511	Monitor resource has not been registered.	unregistered monitor resource	-	o	o	o					
rm	Information	1512	%1 was stopped for failure in monitor %2.	relation stop	-	o	o	o					
rm	Information	1513	%1 was restarted for failure in monitor %2.	relation restart	-	o	o	o					
rm	Information	1514	%1 was failed over for failure in monitor %2.	relation group failover	-	o	o	o					
rm	Information	1515	There was a request to stop cluster for failure in monitor %1.	cluster stop	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Information	1516	There was a request to shut down the system for failure in monitor %1.	system shutdown	-	o	o	o					
rm	Information	1517	There was a request to restart the system for failure in monitor %1.	system reboot	-	o	o	o					
rm	Error	1518	Failed to stop %1 due to error detection of %2.	relation stop failure	Check the status of resources.	o	o	o				o	
rm	Error	1519	Failed to restart %1 due to error detection of %2.	relation restart failure	Check the status of resources.	o	o	o				o	
rm	Error	1520	Failed to fail over %1 due to error detection of %2.	relation group failover failure	Check the status of resources.	o	o	o				o	
rm	Error	1521	Failed to stop the cluster due to error detection of %1.	cluster stop failure	The system may not be able to operate properly.	o	o	o				o	
rm	Error	1522	Failed to shut down the system due to error detection of %1.	os shutdown failure	The system may not be able to operate properly.	o	o	o				o	
rm	Error	1523	Failed to restart the system due to error detection of %1.	os reboot failure	The system may not be able to operate properly.	o	o	o				o	
rm	Error	1524	The group of monitor %1 is unknown.	unknown group	Check the cluster configuration data.	o	o	o				o	
rm	Warning	1525	No action is taken because %1 is not online.	not perform failure action	-	o	o	o				o	
rm	Information	1526	Status of monitor %1 was returned to normal.	status changed into normal	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Information	1527	Status of monitor %1 was changed into unknown.	status changed into unknown	The system may not be able to operate properly.	o	o	o					
rm	Error	1528	Initialization error has occurred (%1 : %2)	process initialize error	The system may not be able to operate properly.	o	o	o				o	
rm	Information	1529	Monitor %1 was suspended.	suspend (single monitor)	-	o	o	o					
rm	Information	1530	Monitor %1 was resumed.	resume (single monitor)	-	o	o	o					
rm	Information	1531	All monitors were suspended.	suspend (all monitors)	-	o	o	o					
rm	Information	1532	All monitors were resumed.	resume (all monitors)	-	o	o	o					
rm	Information	1533	The polling interval of monitor %1 was changed into %2*%3.	change polling interval (single monitor)	-	o	o	o					
rm	Information	1534	The polling interval ratio of all monitors were changed into %1.	change polling interval (all monitors)	-	o	o	o					
rm	Information	1535	Causing intentional stop error was required because an error is detected by %1.	intentional panic	-	o	o	o					
rm	Error	1536	Causing intentional stop error has failed because an error is detected by %1.	intentional panic failure	The system may not be able to operate properly.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Warning	1537	Recovery will not be executed since server is suspending.	not recovery(server suspending)	Monitor resource is not recovered if the server is suspended (Network Partition Unsolved). Check the cause for being suspended (Network Partition Unsolved) and recover network partition resources to the normal status.	o	o	o				o	
rm	Warning	1538	No action is taken because any recovery target is not online.	not recovery (all groups)	-	o	o	o					
rm	Warning	1539	No action is taken because the group is set for the recovery target %1 is not online.	not recovery (group)	-	o	o	o					
rm	Warning	1571	Monitor %1 was delayed. (timeout=%2, response time=%3, rate=%4)	monitor delayed	Check the load on the server where monitoring delay was detected and reduce the load. Set longer timeout if the monitoring timeout is detected.	o	o	o				o	
rm	Warning	1572	Monitor %1 could not perform monitoring.	Delay in internal processing	The system may not be able to operate properly.	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Warning	1600	Shutdown count reached the maximum number (%1). Final action of monitor %2 was ignored.	reached OS shutdown limit	-	o	o	o	o	o		o	o
rm	Warning	1601	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	o					
rm	Info	1602	The number of reboots due to monitor resource errors has been reset.	Resetting the reboot count (monitor resource)	-	o	o	o					
rm	Information	1700	Script before action(%1) upon failure in %2 monitor resource started.	Script before final action upon monitor resource failure started.	-	o	o	o					
rm	Information	1701	Script before action(%1) upon failure in %2 monitor resource completed.	Script before final action upon monitor resource failure completed.	-	o	o	o					
rm	Information	1720	Script before action(%1) upon failure in %2 monitor resource failed.	Script before final action upon monitor resource failure has failed.	-	o	o	o					
rm	Information	1750	The collecting of detailed information triggered by monitoring %1 error has been started (timeout=%2).	The collecting of detailed information has been started.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Information	1751	The collection of detailed information triggered by monitoring %1 error has been completed.	The collection of detailed information has been completed.	-	o	o	o					
rm	Information	1752	The collection of detailed information triggered by monitoring %1 error has been failed (%2).	The collection of detailed information has been failed.	-	o	o	o					
rm	Information	1800	The %1 service will be started by cluster system.	start service	-	o	o	o					
rm	Information	1801	The %1 service will be started again because the service has been stopped by cluster system. (retry: %2/%3)	start service (retry)	-	o	o	o					
rm	Information	1802	The %1 service will be resumed by cluster system.	resume service	-	o	o	o					
rm	Information	1803	The %1 service will be resumed again because the service has been suspended by cluster system. (retry: %2/%3)	resume service (retry)	-	o	o	o					
rm	Information	1804	The %1 service will be stopped by cluster system.	stop service	-	o	o	o					
rm	Information	1805	The %1 service entered the running state.	service running	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Information	1806	The %1 service entered the stopped state.	service stopped	-	o	o	o					
rm	Warning	1811	Start request of the %1 service failed. Check the service status.	failed to start service	Check the service status.	o	o	o					
rm	Warning	1812	Resume request of the %1 service failed. Check the service status.	failed to resume service	Check the service status.	o	o	o					
rm	Warning	1813	Stop request of the %1 service failed. Check the service status.	failed to stop the service	Check the service status.	o	o	o					
rm	Warning	1816	The %1 service has been stopped by other than cluster system.	service stopped (error)	Check the cause of the service stopped.	o	o	o					
rm	Warning	1817	The %1 service has been suspended by other than cluster system.	service suspended (error)	Check the cause of the service suspended.	o	o	o					
rm	Warning	1819	Start or resume retry count for the %1 service exceeded the threshold (%2).	start or resume retry count exceeded the threshold	-	o	o	o					
rm	Information	1820	The cluster will be stopped because there was a failure in %1 service monitoring.	cluster stop (failure in service monitoring)	-	o	o	o					
rm	Information	1821	The system will be shut down because there was a failure in %1 service monitoring.	system shut down (failure in service monitoring)	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Information	1822	The cluster will be rebooted because there was a failure in %1 service monitoring.	system reboot (failure in service monitoring)	-	o	o	o					
rm	Error	1870	Monitor resource %1 can not be controlled because the license is invalid.	cannot control monitor (invalid license)	Check if the license is registered or the license is valid.	o	o	o					
rm	Information	1890	Recovery script has executed because an error was detected in monitoring %1.	Recovery script upon monitor resource failure executed		o	o	o					
rm	Error	1891	Attempted to execute recovery script due to the error detected in monitoring %1, but failed.	failed to execute recovery script	Check the cause of the recovery script failure and take measures.	o	o	o					
rm	Error	1892	Failed to log on as a user.	Logon as a user failed	Check if the domain, account and password of the execution user are correctly set.	o	o	o					
rm	Information	1910	Dummy Failure of monitor resource %1 is enabled.	enable dummy failure	-	o	o	o					
rm	Information	1911	Dummy Failure of monitor resource %1 is disabled.	disable dummy failure	-	o	o	o					
rm	Information	1912	Dummy Failure of all monitors will be enabled.	enable dummy failure (all monitors)	-	o	o	o					
rm	Information	1913	Dummy Failure of all monitors will be disabled.	disable dummy failure (all monitors)	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
rm	Warning	1914	An attempt was made to enable Dummy Failure of monitor resource %1, but failed.	failed to enable dummy failure	-	o	o	o					
rm	Warning	1915	An attempt was made to disable Dummy Failure of monitor resource %1, but failed.	failed to disable dummy failure	-	o	o	o					
rm	Information	1930	Recovery action caused by monitor resource error is disabled.	disable recovery action caused by monitor resource error	-	o	o	o					
rm	Information	1931	Recovery action caused by monitor resource error is enabled.	enable recovery action caused by monitor resource error	-	o	o	o					
rm	Warning	1932	Ignored the recovery action in monitoring %1 because recovery action caused by monitor resource error is disabled.	not recovery (recovery action caused by monitor resource error has disabled)	-	o	o	o					
rm	Warning	1933	Recovery action at timeout occurrence was disabled, so the recovery action of monitor %1 was not executed.	disable recovery action caused by monitor resource timeout	-	o	o	o					
diskagent	Information	2001	%1 service was started.	Start service	-		o	o					
diskagent	Information	2002	%1 service was stopped.	Stop service	-		o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
diskagent	Warning	2030	%1 service was not stopped successfully due to stop timeout or other errors of the internal threads.	Fail to stop service	The system may not be able to operate properly.	o	o	o				o	
diskagent	Error	2050	%1 service was not started successfully because the specified parameter was invalid. Confirm the cluster configuration data.	Fail to start service	Check the cluster configuration data.	o	o	o				o	
diskagent	Error	2051	%1 service was not started because obtaining the policy data failed. Check the data.	Fail to start service	Check the policy file.	o	o	o				o	
diskagent	Error	2052	%1 service was not started successfully because dispatching to service manager failed. System may be unable to operate correctly.	Fail to start service	The system may not be able to operate properly.	o	o	o				o	
diskagent	Error	2053	%1 service was not started successfully because creating and loading internal resources failed. System may be unable to operate correctly.	Fail to start service	System may be unable to operate correctly.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
diskagent	Error	2054	%1 service was not started successfully because initialization of shared disk or mirror disk library failed at exit code %2. System may be unable to operate correctly.	Fail to start service	The system may not be able to operate properly.	o	o	o				o	
diskagent	Error	2055	%1 service was not started successfully because creating communication socket failed. System may be unable to operate correctly.	Fail to start service	The system may not be able to operate properly.	o	o	o				o	
diskagent	Error	2056	%1 service was not started successfully because creating internal threads failed. System may be unable to operate successfully.	Fail to start service	The system may not be able to operate properly.	o	o	o				o	
diskagent	Error	2057	%1 service was not started because it may be stopped or forcibly stopped last time when it was started. Reboot the server.	Fail to start service	Reboot the server.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
diskagent	Error	2090	%1 service failed to reload cluster configuration data. System may be unable to operate correctly. The own server will be shut down.	Server shutdown	The system may not be able to operate properly.	o	o	o				o	
diskagent	Error	2099	%1 service was not started successfully because the other internal error occurred. System may be unable to operate correctly.	Fail to start service	The system may not be able to operate properly.	o	o	o				o	
event	Information	2101	%1 service has been started.	Start service	-		o						
event	Information	2102	%1 service has been stopped.	Stop service	-		o						
event	Warning	2130	Timeout or other error has occurred while waiting for internal threads to stop. Detected internal error %1.	Threads were timeout	The system may not be able to operate properly.	o	o					o	
event	Error	2150	The specified parameters are invalid. Check the cluster configuration data.	Invalid configuration	Check the cluster configuration data.	o	o					o	
event	Error	2151	Failed to obtain the policy data. Check the data.	Invalid configuration	Check the policy file.	o	o					o	
event	Error	2152	Failed to obtain the registry data. System may be unable to operate correctly.	Failed to read registry	The system may not be able to operate properly.	o	o					o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
event	Error	2153	Failed to dispatch to the service manager. System may be unable to operate correctly.	Dispatch failed	The system may not be able to operate properly.	o	o					o	
event	Error	2154	Failed to create an internal resource. System may be unable to operate correctly.	failed to resource creation	The system may not be able to operate properly.	o	o					o	
event	Error	2155	Failed to create communication sockets. System may be unable to operate correctly.	failed to socket creation	The system may not be able to operate properly.	o	o					o	
event	Error	2156	Failed to control the shared memory. System may be unable to operate correctly.	failed to shared memory control	The system may not be able to operate properly.	o	o					o	
event	Error	2157	Failed to generate internal threads. System may be unable to operate correctly.	failed to thread creation	The system may not be able to operate properly.	o	o					o	
event	Error	2158	Failed to initialize the settings of the log storage period. With the settings invalid, the system will be started.	failed to initialize the settings of the log storage period	The system may not be able to operate properly.	o	o					o	
event	Error	2199	Other internal error has occurred. System may be unable to operate correctly.	Internal Error	The system may not be able to operate properly.	o	o					o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
trnsv	Error	2301	There was a notification from external (IP=%1), but it was denied.	Connection limit by client IP address	Check the client IP address from which the connection is permitted.	o	o	o					
trnsv	Information	2310	There was a notification (%1) from external (IP=%2).	Received an abnormity occurrence notification from outside	-	o	o	o					
trnsv	Information	2320	Recovery action (%1) of monitoring %2 has been executed because a notification arrived from external.	Executed the recovery action at abnormity occurrence	-	o	o	o					
trnsv	Information	2321	Recovery action (%1) of monitoring %2 has been completed.	Completed the recovery action at abnormity occurrence	-	o	o	o					
trnsv	Error	2322	Attempted to recovery action (%1) of monitoring %2 due to the notification from external, but failed.	Failed to execute the recovery action at abnormity occurrence	Make sure that the recovery action on the environment is executable.	o	o	o					
trnsv	Information	2330	Action (%1) has been completed.	The requested action completed	-	o	o	o					
trnsv	Error	2331	Attempted to execute action (%1), but it failed.	The requested action Failed	Make sure that the recovery action is an executable environment.	o	o	o					
trnsv	Information	2340	Script before action of monitoring %1 has been executed.	Script execution started	-	o	o	o					
trnsv	Information	2341	Script before action of monitoring %1 has been completed.	Script execution completed	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
trnsv	Error	2342	Attempted to execute script before action of monitoring %1, but it failed.	Script execution failed	Handle the problem after making sure the cause of script failure.	o	o	o					
trnsv	Error	2350	The system will be shutdown because cluster resume was failed.	Failed to resume the cluster daemon	-	o	o	o					
trnsv	Error	2351	An attempt to shutdown the system failed.	Failed to shutdown the system	The system may not be able to operate properly.	o	o	o					
trnsv	Error	2360	The log storage destination (%1) is not found.	Finding the log storage destination failed.	Check if the specified log storage destination exists.	o	o	o					
trnsv	Error	2361	A path under the installation path is specified for the log storage destination.	The log storage destination is incorrect.	For the log storage destination, avoid specifying a path under the installation path.	o	o	o					
trnsv	Error	2370	Failed to execute the Amazon CloudWatch linkage function. (%1)	%1:The user is not permitted to execute the function.	Check the permission for the cloud service.	o	o	o					
				%1:An internal error has occurred.	Check the configuration of the Amazon CloudWatch linkage function.	o	o	o					
lankhb	Error	2851	Keep-alive timeout was detected on the server %1.	Keep-alive timeout	There is a server where keep-alive timeout is detected. Check the server error.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
lankhb	Error	2852	STOP error was detected on the server %1. (source:%2, exit code:%3)	STOP error	There is a server where STOP error is detected. Remove the failure of the server.	o	o	o				o	
lankhb	Error	2853	Hardware reset was detected on the server %1. (source:%2, exit code:%3)	Hardware reset	There is a server where hardware reset is detected. Remove the failure of the server.	o	o	o				o	
fip	Error	2901	IP address already exists. (IP=%1)	address duplication	-	o	o	o					
fip	Information	2902	IP address will be activated forcibly. (IP=%1)	address force activation	-	o	o	o					
vip	Error	3051	IP address already exists. (IP=%1)	address duplication	-	o	o	o					
vip	Information	3052	IP address will be activated forcibly. (IP=%1)	address force activation	-	o	o	o					
sdfunc	Warning	3201	Trying again to disconnect disk %1. Check if the disk is being used.	Retry disk disconnection	Check if the disk is being used.	o	o	o				o	
sdfunc	Information	3202	Disk %1 was forcibly disconnected.	Disconnect disk forcibly	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sdfunc	Warning	3203	Updated configuration data was not reflected properly. Update the configuration data again after modifying the configuration settings.	Fail to update configuration	Check whether the cluster configuration information, specifically the HBA setting and the letter of the drive and GUID data for the disk NP resolution resource and disk resources for each server, matches the current disk configuration of each server.	o	o	o				o	
sdfunc	Warning	3204	The server %1 is not found in the configuration data. Check the server name of the configuration data.	Fail to detect server name	Check the cluster configuration data.	o	o	o				o	
sdfunc	Information	3205	Detected disk resources that have not been identified. Disk reidentification will be executed.	Execute disk reconfirmation	-	o	o	o					
sdfunc	Information	3206	Reidentification of the disk has finished.	Finish disk reconfirmation	-	o	o	o					
sdfunc	Error	3207	Connecting disk %1 has failed.	Fail to connect disk	Check if the partition is allocated and the disk is being recognized by operating system.		o				o	o	
sdfunc	Error	3208	Disconnecting disk %1 has failed.	Fail to disconnect disk	Check if the disk is being used.		o					o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
disknp	Warning	3251	Timeout has occurred in read/write to the partition for disk heart-beat. Check the connection status of partition for disk heartbeat.	Disk heart beat timeout	Make sure there is no error in the disk and it is correctly connected .	o	o	o			o	o	
disknp	Information	3252	Recovered from the time-out occurred in read/write to the partition for disk heartbeat.	Recover from disk heartbeat timeout	-	o	o	o					
disknp	Error	3257	Disconnection monitoring(%1) among the shared disk and the servers could not be started. The system may not be able to operate properly.	Fail to start monitoring	The system may not be able to operate properly.	o	o	o				o	
ptun	Warning	3301	The parameter (%1) exceeded the threshold (%2 p.c.). Timeout value=%3(sec) Data=%4(sec)	Delay warning	The parameter exceeded the threshold. Set an appropriate value to the parameter.	o	o	o				o	
ptun	Warning	3302	The parameter (%1) exceeded the threshold (%2 p.c.). Timeout value=%3 Data=%4 Server=%5 Resource=%6	Delay warning	The parameter exceeded the threshold. Set an appropriate value to the parameter.	o	o	o				o	
lcns	Information	3551	The trial license is valid until %1. (Product name:%2)	Trial version license (normal)	-	o	o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
lcns	Error	3552	The trial license has expired in %1. (Product name:%2)	Trial version license (expired)	Register the license.	o	o	o				o	
lcns	Warning	3553	The number of licenses is insufficient. The number of insufficient licenses is %1. (Product name:%2)	Insufficient	Register the license.	o	o					o	
lcns	Error	3554	The license is not registered. (Product name:%1)	Not registered	Register the license.	o	o	o				o	
lcns	Error	3555	The same license is registered with other servers. (Product name:%1)	Repetition registered	Delete the overlapping license.	o	o	o				o	
lcns	Error	3556	Manufacturer or model of this server is invalid.	Invalid manufacturer or model	Confirm the manufacturer or model.	o	o	o				o	
lcns	Error	3558	The registered license is invalid. (Product name:%1, Serial No:%2)	The license is invalid.	Register the valid license.	o	o	o				o	
lcns	Information	3559	The fixed term license is effective until %1. (Product name:%2)	Fixed term license (normal)	-	o	o						
lcns	Error	3560	The fixed term license has expired in %1. (Product name:%2)	Fixed term license (expired)	Register the license.	o	o	o				o	
logcmd	Information	3601		log command	-	o	x	x	x	x	x	x	x
sdw/hdtw	Warning	3651	Monitor %1 was delayed. (timeout=%2 response time=%3 rate=%4)	Monitoring is delayed		o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sdw/hdtw	Error	3652	Cannot access the disk (%1).	Disconnection is detected.	Make sure there is no error in the disk and the shared disk is correctly connected.		o				o	o	
sdw/hdtw	Information	3653	Recovered the status where access to the disk (%1) is possible.	Recovery from disconnection has been done.	-		o						
diskw	Warning	3701	Monitor %1 was delayed. (timeout=%2 response time=%3 rate=%4)	monitor delayed	-	o	o	o				o	
userw	Warning	3711	Monitor %1 was delayed. (timeout=%2 response time=%3 rate=%4)	monitor delayed	-	o	o	o				o	
vcom	Error	3751	Failed to register the virtual computer name (%1) to the DNS server.	Failed to register the virtual computer name	Make sure there is no error on the DNS server, or a trouble occurred in communicating with the DNS server.	o	o						
vcom	Error	3752	Failed to delete the virtual computer name (%1) from the DNS server.	Failed to delete the virtual computer name	Make sure there is no error on the DNS server, or a trouble occurred in communicating with the DNS server.	o	o						
mdadmn	Information	3851	Full Recovery of mirror disk %1 started.	Full Recovery of mirror disk started	-	o	o	o					
			Full Recovery of hybrid disk %1 started.	Full Recovery of hybrid disk started	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mdadmn	Information	3852	Full Recovery of mirror disk %1 finished successfully.	Full Recovery of mirror disk succeeded	-	o	o	o					
			Full Recovery of hybrid disk %1 finished successfully.	Full Recovery of hybrid disk succeeded	-	o	o	o					
mdadmn	Information	3853	Full Recovery of mirror disk %1 was canceled.	Full Recovery of mirror disk was canceled	-	o	o	o					
			Full Recovery of hybrid disk %1 was canceled.	Full Recovery of hybrid disk was canceled	-	o	o	o					
mdadmn	Error	3854	Full Recovery of mirror disk %1 failed.	Full Recovery of mirror disk failed	Make sure there is no error in the disk and network adapter and the network is correctly connected.	o	o	o			o	o	
			Full Recovery of hybrid disk %1 failed.	Full Recovery of hybrid disk failed	Make sure there is no error in the disk and network adapter and the network is correctly connected.	o	o	o			o	o	
mdadmn	Information	3855	Fast Recovery of mirror disk %1 started.	Fast Recovery of mirror disk started	-	o	o	o					
			Fast Recovery of hybrid disk %1 started.	Fast Recovery of hybrid disk started	-	o	o	o					
mdadmn	Information	3856	Fast Recovery of mirror disk %1 finished successfully.	Fast Recovery of mirror disk succeeded	-	o	o	o					
			Fast Recovery of hybrid disk %1 finished successfully.	Fast Recovery of hybrid disk succeeded	-	o	o	o					
mdadmn	Information	3857	Fast Recovery of mirror disk %1 was canceled.	Fast Recovery of mirror disk was canceled	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
			Fast Recovery of hybrid disk %1 was canceled.	Fast Recovery of hybrid disk was canceled	-	o	o	o					
mdadmn	Error	3858	Fast Recovery of mirror disk %1 failed.	Fast Recovery of mirror disk failed	Make sure there is no error in the disk and network adapter and the network is correctly connected.	o	o	o			o	o	
			Fast Recovery of hybrid disk %1 failed.	Fast Recovery of hybrid disk failed	Make sure there is no error in the disk and network adapter and the network is correctly connected.	o	o	o			o	o	
mdfunc	Warning	3859	Trying again to disconnect mirror disk %1. Check if the mirror disk is being used.	Disconnection of mirror disk is being retried	Check if the mirror disk is being used.	o	o	o				o	
			Trying again to disconnect hybrid disk %1. Check if the hybrid disk is being used.	Disconnection of hybrid disk is being retried	Check if the hybrid disk is being used.	o	o	o				o	
mdfunc	Information	3860	Mirror disk %1 was forcibly disconnected.	Mirror disk was forcibly disconnected.	-	o	o	o					
			Hybrid disk %1 was forcibly disconnected.	Hybrid disk was forcibly disconnected.	-	o	o	o					
mdadmn	Error	3862	A data partition error occurred in the mirror disk %1.	disk error	Replace the server disk.	o	o	o			o	o	
			A data partition error occurred in the hybrid disk %1.	disk error	Replace the server disk.	o	o	o			o	o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mdadmn	Error	3863	A cluster partition error occurred in the mirror disk %1.	disk error	Replace the server disk.	o	o	o			o	o	
			A cluster partition error occurred in the hybrid disk %1.	disk error	Replace the server disk.	o	o	o			o	o	
mdadmn	Error	3864	Failed to initialize the mirror disk connect.	Mirror disk connection initialization failed	Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o			o	o	
mdadmn	Error	3865	Failed to initialize the mirror disk %1.	Mirror disk initialization failed	Check the partition exists and the disk is recognized by the operating system.	o	o	o			o	o	
			Failed to initialize the hybrid disk %1.	Hybrid disk initialization failed	Check the partition exists and the disk is recognized by the operating system.	o	o	o			o	o	
mdadmn	Error	3866	Failed to initialize the mirror disk %1. The cluster partition and the data partition must be different partitions.	Mirror disk initialization failed	Check the cluster configuration data.	o	o	o				o	
			Failed to initialize the hybrid disk %1. The cluster partition and the data partition must be different partitions.	Hybrid disk initialization failed	Check the cluster configuration data.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mdadmn	Error	3867	Failed to initialize the mirror disk %1. The area in the cluster partition has been used by another mirror disk.	Mirror disk initialization failed	Check the cluster configuration data.	o	o	o				o	
			Failed to initialize the hybrid disk %1. The area in the cluster partition has been used by another hybrid disk.	Hybrid disk initialization failed	Check the cluster configuration data.	o	o	o				o	
mdadmn	Error	3868	Failed to initialize the mirror disk %1. The partition specified for the cluster partition has been used as the data partition of another mirror disk.	Mirror disk initialization failed	Check the cluster configuration data.	o	o	o				o	
			Failed to initialize the hybrid disk %1. The partition specified for the cluster partition has been used as the data partition of another hybrid disk.	Hybrid disk initialization failed	Check the cluster configuration data.	o	o	o				o	
mdadmn	Error	3869	Failed to initialize the mirror disk %1. The partition specified for the data partition has been used by another mirror disk.	Mirror disk initialization failed	Check the cluster configuration data.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
			Failed to initialize the hybrid disk %1. The partition specified for the data partition has been used by another hybrid disk.	Hybrid disk initialization failed	Check the cluster configuration data.	o	o	o				o	
mdadmn	Error	3874	A fatal error has occurred during control mirror disk %1. Shutdown the server.	Fatal error has occurred	Make sure there is no error in the disk and network adapter and the network is correctly connected.	o	o	o			o	o	
			A fatal error has occurred during control hybrid disk %1. Shutdown the server.	Fatal error has occurred	Make sure there is no error in the disk and network adapter and the network is correctly connected.	o	o	o			o	o	
mdadmn	Warning	3875	The mirror disk connect of mirror disk %1 has been changed. (Priority %2 -> %3)	The mirror disk connect has been switched due to disconnection of the active mirror disk connect.	Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o				o	
			The mirror disk connect of hybrid disk %1 has been changed. (Priority %2 -> %3)	The mirror disk connect has been switched due to disconnection of the active mirror disk connect.	Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mdadmn	Error	3876	Disconnecting mirror disk %1 has failed while it is being copied. The server is shut down to protect data.	Failed sending server closing due to process access Execution of emergency shutdown by process access	The mirror disk may be in use. Check the mirror disk.	o	o	o			o	o	
			Disconnecting hybrid disk %1 has failed while it is being copied. The server is shut down to protect data.	Failed sending server closing due to process access Execution of emergency shutdown by process access	The hybrid disk may be in use. Check the hybrid disk.	o	o	o			o	o	
mdadmn	Warning	3880	The mirror disk connect of mirror disk %1 has been disconnected.	An error occurred in the mirror disk connect.	Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o					
			The mirror disk connect of hybrid disk %1 has been disconnected.	An error occurred in the mirror disk connect.	Make sure there is no error in the network adapter and the network is correctly connected.	o	o	o					
mdadmn	Warning	3881	The Auto mirror recovery check box is not selected. It is necessary to recover the mirror manually, in order to resume mirroring (%1).	It is necessary to recover the mirror manually, in order to resume mirroring.	Recover a mirror from the command or Mirror disks.	o	o	o	o				o

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mdadmn	Information	3882	Extend the mirror disk(%1) finished successfully. (size:%2 Bytes)	Mirror disk extend succeeded	-	o	o	o					
			Extend the hybrid disk(%1) finished successfully. (size:%2 Bytes)	Hybrid disk extend succeeded	-	o	o	o					
mdadmn	Error	3883	Extend the mirror disk(%1) has failed.	Mirror disk extend failed	Check that there is enough free disk space and there is no error in disk and network adapter and the network is correctly connected.	o	o	o			o	o	
			Extend the hybrid disk(%1) has failed.	Hybrid disk extend failed	Check that there is enough free disk space and there is no error in disk and network adapter and the network is correctly connected.	o	o	o			o	o	
mdadmn	Information	3885	Updated the encryption key of mirror disk %1 successfully.	Updating the encryption key succeeded.	-	o	o	o					
			Updated the encryption key of hybrid disk %1 successfully.	Updating the encryption key succeeded.	-	o	o	o					
mdadmn	Error	3886	Failed to update the encryption key of mirror disk %1.	Updating the encryption key failed.	Check if the key file exists in the configured key file full path on each server.	o	o	o			o	o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
			Failed to update the encryption key of hybrid disk %1.	Updating the encryption key failed.	Check if the key file exists in the configured key file full path on each server.	o	o	o			o	o	
mdadmn	Error	3887	Update the encryption key of mirror disk %1.	Notification of necessary update of the encryption key.	Update the encryption key.	o	o	o			o	o	
			Update the encryption key of hybrid disk %1.	Notification of necessary update of the encryption key.	Update the encryption key.	o	o	o			o	o	
mdadmn	Information	3888	The mirror disk(%1) is activated, but the data is not up-to-date. (Elapsed time since the mirror break occurred: %2 seconds)	The mirror disk is activated with the data not up-to-date.	-	o	o	o					
			The hybrid disk(%1) is activated, but the data is not up-to-date. (Elapsed time since the mirror break occurred: %2 seconds)	The hybrid disk is activated with the data not up-to-date.	-	o	o	o					
hdtw	Warning	4001	Monitor %1 was delayed. (timeout=%2 response time=%3 rate=%4)	Monitoring is delayed	-	o	o	o				o	
hdtw	Error	4002	Cannot access the disk (%1).	Disconnection is detected.	Make sure there is no error in the disk and the shared disk is correctly connected.		o				o	o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
hdtw	Information	4003	Recovered the status where access to the disk (%1) is possible.	Recovery from disconnection has been done.	-		o						
mail	Error	4101	mail failed(%1).(SMTP server: %2)	Mail failed	Make sure there is no error in the SMTP server and no problem communicating with the SMTP server.	o	o	o				o	
mail	Information	4102	mail succeed.(SMTP server: %1)	Mail succeeded	-		o	o					
lamp	Information	4151	Notice by the network warming light succeeded.	Network warning light succeeded	-	o	o	o					
lamp	Error	4152	Error in network warning light notice command.(%1)	Network warning light failed	Take appropriate action by following the error code.	o	o	o				o	
lamp	Error	4153	Failed to execute warning light command.(%1)	Network warning light failed	The system may not be able to operate properly.	o	o	o				o	
cifs	Information	4201	Created new shared configuration file.	Created new shared configuration file.	-	o	o	o					
cifs	Warning	4202	Failed to read in shared configuration file. File may be corrupted.	Reading shared configuration file failed.	Check if the shared configuration file is corrupted.	o	o	o					
cifs	Information	4203	Recovered shared configuration file from backup file.	Shared configuration file is restored.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
cifs	Warning	4204	Recreated shared configuration file since it cannot be found.	Shared configuration file is created again.	This is a normal action at first activation. In other cases, check if the shared configuration file is not deleted.	o	o	o					
cifs	Warning	4205	There are differences between share settings stored in shared configuration file and the current configuration settings.	Sharing target folder is lost.	Check if the shared folder is not deleted while CIFS resource is deactivated.	o	o	o					
cifs	Information	4206	Failed to get shared folder account information	Failed to get shared folder account information	Check if a deleted group or user is set in Permissions for the shared folder.	o	o	o					
apisv	Information	4301	There was a request to stop cluster from the %1(IP=%2).	Cluster stop	-	o		o					
apisv	Information	4302	There was a request to shutdown cluster from the %1(IP=%2).	Cluster shutdown	-	o		o					
apisv	Information	4303	There was a request to reboot cluster from the %1(IP=%2).	Cluster restart	-	o		o					
apisv	Information	4304	There was a request to suspend cluster from the %1(IP=%2).	Cluster suspend	-	o		o					
apisv	Information	4310	There was a request to stop server from the %1(IP=%2).	Cluster service stop	-	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Information	4311	There was a request to shutdown server from the %1(IP=%2).	Shutdown	-	o		o					
apisv	Information	4312	There was a request to reboot server from the %1(IP=%2).	Restart	-	o		o					
apisv	Information	4330	There was a request to start group(%1) from the %2(IP=%3).	Group start	-	o		o					
apisv	Information	4331	There was a request to start all groups from the %1(IP=%2).	All group start	-	o		o					
apisv	Information	4332	There was a request to stop group(%1) from the %2(IP=%3).	Group stop		o		o					
apisv	Information	4333	There was a request to stop all groups from the %1(IP=%2).	All group stop	-	o		o					
apisv	Information	4334	There was a request to restart group(%1) from the %2(IP=%3).	Group restart	-	o		o					
apisv	Information	4335	There was a request to restart all groups from the %1(IP=%2).	All group restart	-	o		o					
apisv	Information	4336	There was a request to move group(%1) from the %2(IP=%3).	Group move	-	o		o					
apisv	Information	4337	There was a request to move all groups from the %1(IP=%2).	All group move	-	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Information	4338	There was a request to failover group(%1) from the %2(IP=%3).	Group failover	-	o		o					
apisv	Information	4339	There was a request to failover all groups from the %1(IP=%2).	All group failover	-	o		o					
apisv	Information	4340	There was a request to migrate group(%1) from the %2(IP=%3).	Group migration	-	o		o					
apisv	Information	4341	There was a request to migrate all groups from the %1(IP=%2).	All group migration	-	o		o					
apisv	Information	4342	There was a request to failover all groups from the %1(IP=%2).	All group failover	-	o		o					
apisv	Information	4343	There was a request to cancel waiting for the dependence destination group of group %1 was issued from the %2.	Cancel waiting	-	o		o					
apisv	Information	4350	There was a request to start resource(%1) from the %2(IP=%3).	Resource start	-	o		o					
apisv	Information	4351	There was a request to start all resources from the %1(IP=%2).	All resource start	-	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Information	4352	There was a request to stop resource(%1) from the %2(IP=%3).	Resource stop	-	o		o					
apisv	Information	4353	There was a request to stop all resources from the %1(IP=%2).	All resource stop	-	o		o					
apisv	Information	4354	There was a request to restart resource(%1) from the %2(IP=%3).	Resource restart	-	o		o					
apisv	Information	4355	There was a request to restart all resources from the %1(IP=%2).	All resource restart	-	o		o					
apisv	Information	4360	There was a request to suspend monitor resources from the %1(IP=%2).	Monitor temporary stop	-	o		o					
apisv	Information	4361	There was a request to resume monitor resources from the %1(IP=%2).	Monitor restart	-	o		o					
apisv	Information	4362	There was a request to enable Dummy Failure of monitor resource(%1) from the %2(IP=%3).	Dummy Failure enabled	-	o		o					
apisv	Information	4363	There was a request to disable Dummy Failure of monitor resource(%1) from the %2(IP=%3).	Dummy Failure disabled	-	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Information	4364	There was a request to disable Dummy Failure of all monitor resources from the %1(IP=%2).	All Dummy Failure disabled	-	o		o					
apisv	Error	4401	A request to stop cluster was failed(%1).	Cluster stop failure	Check the cluster status.	o		o					
apisv	Error	4402	A request to shutdown cluster was failed(%1).	Cluster shutdown failure	Check the cluster status.	o		o					
apisv	Error	4403	A request to reboot cluster was failed(%1).	Cluster restart failure	Check the cluster status.	o		o					
apisv	Error	4404	A request to suspend cluster was failed(%1).	Cluster suspend failure	Check the cluster status.	o		o					
apisv	Error	4410	A request to stop server was failed(%1).	Cluster service stop failure	Check the cluster status.	o		o					
apisv	Error	4411	A request to shutdown server was failed(%1).	Server shutdown failure	Check the server status.	o		o					
apisv	Error	4412	A request to reboot server was failed(%1).	Server restart failure	Check the server status.	o		o					
apisv	Error	4430	A request to start group(%1) was failed(%2).	Group start failure	Check the group status.	o		o					
apisv	Error	4431	A request to start all groups was failed(%1).	All group start failure	Check the group status.	o		o					
apisv	Error	4432	A request to stop group(%1) was failed(%2).	Group stop failure	Check the group status.	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Error	4433	A request to stop all groups was failed(%1).	All group stop failure	Check the group status.	o		o					
apisv	Error	4434	A request to restart group(%1) was failed(%2).	Group restart failure	Check the group status.	o		o					
apisv	Error	4435	A request to restart all groups was failed(%1).	All group restart failure	Check the group status.	o		o					
apisv	Error	4436	A request to move group(%1) was failed(%2).	Group move failure	Check the group status.	o		o					
apisv	Error	4437	A request to move all groups was failed(%1).	All group move failure	Check the group status.	o		o					
apisv	Error	4438	A request to failover group(%1) was failed(%2).	Group failover failure	Check the group status.	o		o					
apisv	Error	4439	A request to failover all groups was failed(%1).	All group failover failure	Check the group status.	o		o					
apisv	Error	4440	A request to migrate group(%1) was failed(%2).	Group migration failure	Check the group status.	o		o					
apisv	Error	4441	A request to migrate all groups was failed(%1).	All group migration failure	Check the group status.	o		o					
apisv	Error	4442	A request to failover all groups was failed(%1).	All group failover failure	Check the group status.	o		o					
apisv	Error	4443	A request to cancel waiting for the dependency destination group of group %s has failed(%1).	Cancel waiting failure	Check the group status.	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Error	4450	A request to start resource(%1) was failed(%2).	Resource start failure	Check the resource status.	o		o					
apisv	Error	4451	A request to start all resources was failed(%1).	All resource start failure	Check the resource status.	o		o					
apisv	Error	4452	A request to stop resource(%1) was failed(%2).	Resource stop failure	Check the resource status.	o		o					
apisv	Error	4453	A request to stop all resources was failed(%1).	All resource stop failure	Check the resource status.	o		o					
apisv	Error	4454	A request to restart resource(%1) was failed(%2).	Resource restart failure	Check the resource status.	o		o					
apisv	Error	4455	A request to restart all resources was failed(%1).	All resource restart failure	Check the resource status.	o		o					
apisv	Error	4460	A request to suspend monitor resource was failed(%1).	Monitor temporary stop failure	Check the monitor resource status.	o		o					
apisv	Error	4461	A request to resume monitor resource was failed(%1).	Monitor restart failure	Check the monitor resource status.	o		o					
apisv	Error	4462	A request to enable Dummy Failure of monitor resource(%1) was failed(%2).	Dummy Failure enabled	Check the monitor resource status.	o		o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
apisv	Error	4463	A request to disable Dummy Failure of monitor resource(%1) was failed(%2).	Dummy Failure disabled	Check the monitor resource status.	o		o					
apisv	Error	4464	A request to disable Dummy Failure of all monitor resource was failed(%1).	All Dummy Failure disabled	Check the monitor resource status.	o		o					
apisv	Error	4480	Initializing internal communication (%1) failed (port=%2).	Initializing internal communication failed.	Check if an application other than EXPRESSCLUSTER uses the port.	o		o					
diskperf	Warning	4801	An internal error occurred in clpdiskperf.dll There is a possibility that certain Cluster Disk Resource Performance Data can't be collected	An internal error occurred in clpdiskperf.dll.	There may be insufficient memory or OS resources. Check whether there are sufficient resources available.	o	o	o					
diskperf	Information	4802	clpdiskperf.dll internal problem has gone.	The internal error in clpdiskperf.dll has been resolved.	-	o	o	o					
diskperf	Warning	4803	An error occurred by writing in Cluster Disk Resource Performance Data log. Please confirm the state of the disk.	An error occurred when writing the Cluster Disk Resource Performance Data log.	Check whether there is sufficient free disk space.	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
diskperf	Information	4804	Write error of Cluster Disk Resource Performance Data log was recovered.	The write error in the Cluster Disk Resource Performance Data log has been resolved.	-	o	o	o					
diskperf	Error	4805	An internal error occurred in clpdiskperf.dll Cluster Disk Resource Performance Data can't be collected until a server restart.	An internal error occurred in clpdiskperf.dll	Reboot the server.		o	o					
diskperf	Error	4806	Cluster Disk Resource Performance Data can't be collected because a performance monitor is too numerous.	The number of processes that load clpdiskperf.dll exceeded 32.	Refer to the following topic in the "Getting Started Guide": "Notes and Restrictions" -> " After starting operating EXPRESSCLUSTER" -> " Event log output relating to linkage between mirror statistical information collection function and OS standard function"								
userw	Warning	5001	Monitor %1 was delayed. (timeout=%2 response time=%3 rate=%4)	Monitor delayed	-	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
genw	Warning	5151	The script(%1) was re-activated because it was disappeared.(%2)	The target script was rebooted. %1:Script name %2:Monitor resource name	-	o	o						
db2 ftp http imap4 odbc oracle otx pop3 psql smtp sqlserver tux was wls	Warning	10001	%1	Error message for each monitored application.	Take appropriate action for the application failure by following the error message.	o	x	x	x	x	x	x	x

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
db2w ftpw httpw imap4w odbcw oraclew otxw pop3w psqlw smtpw sqlserverw tuxw wasw wlsw db2 ftp http imap4 odbc oracle otx pop3 psql smtp sqlserver tux was wls	Warning	10002	The API Error of Windows occurred.%1	API error of Windows has occurred. %1 is API error code.	Take appropriate action for the OS failure by following the error code.	o	x	x	x	x	x	x	x
mrw	Warning	4901	Monitor %1 is in the warning status. (%2 : %3)	Monitor warn	Check the cause of Warning.	o	o	o				o	
mrw	Warning	4902	Configuration of %1 is invalid. (%2 : %3)	invalid monitor resource	Check the cluster configuration data.	o	o	o				o	
mrw	Error	4903	Failed to start monitor %1.	monitor starting failed	The system may not be able to operate properly.	o	o	o	o	o		o	o

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mrw	Error	4904	Failed to stop monitor %1.	monitor stopping failed	The system may not be able to operate properly.	o	o	o				o	
mrw	Error	4905	Monitor %1 detected an error. (%2 : %3)	monitor failed	Check the cause for monitor error.	o	o	o	o	o		o	o
mrw	Information	4906	Monitor resource has not been registered.	unregistered monitor resource	-	o	o	o					
mrw	Information	4907	%1 was stopped for failure in monitor %2.	relation stop	-	o	o	o					
mrw	Information	4908	%1 was restarted for failure in monitor %2.	relation restart	-	o	o	o					
mrw	Information	4909	%1 was failed over for failure in monitor %2.	relation group failover	-	o	o	o					
mrw	Information	4910	There was a request to stop cluster for failure in monitor %1.	cluster stop	-	o	o	o					
mrw	Information	4911	There was a request to shut down the system for failure in monitor %1.	system shutdown	-	o	o	o					
mrw	Information	4912	There was a request to restart the system for failure in monitor %1.	system reboot	-	o	o	o					
mrw	Information	4913	Failed to stop %1 due to error detection of %2.	relation stop failure	Check the status of resources.	o	o	o				o	
mrw	Error	4914	Failed to restart %1 due to error detection of %2.	relation restart failure	Check the status of resources.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mrw	Error	4915	Failed to fail over %1 due to error detection of %2.	relation group failover failure	Check the status of resources.	o	o	o				o	
mrw	Error	4916	Failed to stop the cluster due to error detection of %1.	cluster stop failure	The system may not be able to operate properly.	o	o	o				o	
mrw	Error	4917	Failed to shut down the system due to error detection of %1.	os shutdown failure	The system may not be able to operate properly.	o	o	o				o	
mrw	Error	4918	Failed to restart the system due to error detection of %1.	os reboot failure	The system may not be able to operate properly.	o	o	o				o	
mrw	Error	4919	The group of monitor %1 is unknown.	unknown group	Check the cluster configuration data.	o	o	o				o	
mrw	Warning	4920	No action is taken because %1 is not online.	not perform failure action	-	o	o	o				o	
mrw	Information	4921	Status of monitor %1 was returned to normal.	status changed into normal	-	o	o	o					
mrw	Information	4922	Status of monitor %1 was changed into unknown.	status changed into unknown	The system may not be able to operate properly.	o	o	o					
mrw	Error	4923	Initialization error has occurred (%1 : %2)	process initialize error	The system may not be able to operate properly.	o	o	o				o	
mrw	Information	4924	Causing intentional stop error was required because an error is detected by %1.	intentional panic	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mrw	Error	4925	Causing intentional stop error has failed because an error is detected by %1.	intentional panic failure	The system may not be able to operate properly.	o	o	o				o	
mrw	Warning	4926	Recovery will not be executed since server is suspending.	not recovery(server suspending)	Monitor resource is not recovered if the server is suspended (Network Partition Unsolved). Check the cause for being suspended (Network Partition Unsolved) and recover network partition resources to the normal status.	o	o	o				o	
mrw	Warning	4927	Shutdown count reached the maximum number (%1). Final action of monitor %2 was ignored.	reached OS shutdown limit	-	o	o	o	o	o		o	o
mrw	Information	4928	Script before action(%1) upon failure in %2 monitor resource started.	Script before final action upon monitor resource failure started.	-	o	o	o					
mrw	Information	4929	Script before action(%1) upon failure in %2 monitor resource completed.	Script before final action upon monitor resource failure completed.	-	o	o	o					
mrw	Information	4930	Script before action(%1) upon failure in %2 monitor resource failed.	Script before final action upon monitor resource failure has failed.	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
mrw	Information	4931	Recovery script has executed because an error was detected in monitoring %1.	Recovery script upon monitor resource failure executed		o	o	o					
mrw	Error	4932	Attempted to execute recovery script due to the error detected in monitoring %1, but failed.	failed to execute recovery script	Check the cause of the recovery script failure and take measures.	o	o	o					
mrw	Warning	4933	Ignored the recovery action in monitoring %1 because recovery action caused by monitor resource error is disabled.	not recovery (recovery action caused by monitor resource error has disabled)	-	o	o	o					
mrw	Information	4934	There was a notification (%1) from external. (detail: %2)	An error notification from external was received.	-	o	o	o					
tuxw	Warning	10004	The API Error of Application occurred.%1	API error of application has occurred. %1 is API error code.	Take appropriate action for the application failure by following the error code.	o							
jra	Error	20251	Internal processing has failed. (%1)	An internal error occurred. %1: Internal error code	Check if JVM monitor resource is running. If not, restart the server.		o						
jra	Error	20252	Startup has failed due to an error of the setting value. (%1)	Specified setting value is invalid. %1: Internal error code	Check if the Java installation path is correct.		o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Error	20301	Service was terminated because reading an SG file failed.	An error occurred in reading the setting file.	Check the message separately issued.		o						
sra	Error	20302	The installation folder name could not be acquired.	The installation folder name could not be acquired.	Restart the cluster, or execute the suspend and resume.		o						
sra	Error	20305	No IModules could be loaded.	Some files required to execute this product do not exist. So, this product failed to start.	Install this product again.		o						
sra	Error	20306	An unexpected error occurred.	An attempt was made to start this product, but failed for some reason or another.	Restart the cluster, or execute the suspend and resume.		o						
sra	Error	20307	Internal error occurred.	This product has terminated abnormally.	See the system log message issued last.		o						
sra	Error	20308	An error has occurred in issuing WMI. %1(ErrorID:0x%2 class:%3) %1: Message %2: Error code %3: Information that could not be acquired	Statistics information could not be acquired. %1: Message %2: Error code %3: Information that could not be acquired	Restart the cluster, or execute the suspend and resume.		o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Warning	20336	Script is timeout. (%1 %2) %1: Script file name %2: Argument	An internal error has occurred.	Check the load status of the server and remove the load.		o						
sra	Information	20346	%1 event succeeded. %1: Event type (Boot, Shutdown, Stop, Start, or Flush)	The operation management command has been executed. The executed event type %1 (boot, shutdown, stop, start, or flush) is output.	-		o						
sra	Warning	20347	%1 was smaller than %2, it changed to minimum value(%3).	The configuration value of the monitoring is not correct. %1:Variable name %2:Variable name %3:configured value	Check the configured value on the Cluster WebUI.		o						
sra	Warning	20348	%1 was too long compared with %2, it changed to %1(%3).	The configuration value of the monitoring is not correct. %1:Variable name %2:Variable name %3:configured value	Check the configured value on the Cluster WebUI.		o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Warning	20349	%1 was smaller than %2, it changed to %2 value(%3).(%4)	The configuration value of the monitoring is not correct. %1:Variable name %2:Variable name %3:configured value %4:Monitor resource name	Check the configured value on the Cluster WebUI.		o						
sra	Warning	20350	%1 was larger than %2, it changed to %2 value(%3).(%4)	The configuration value of the monitoring is not correct. %1:Variable name %2:Variable name %3:configured value %4:Monitor resource name	Check the configured value on the Cluster WebUI.		o						
sra	Warning	20351	%1 was over than Total disk size, (%2 %3).	The configuration value of the monitoring is not correct. %1:Variable name %2:Monitor resource name %3:configured value	Check the configured value on the Cluster WebUI.		o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Warning	20352	%1 was over than Total disk size, (%2 %3).	The configuration value of the monitoring is not correct. %1:Variable name %2:Monitor resource name %3:configured value	Check the configured value on the Cluster WebUI.		o						
sra	Warning	20353	Delete MOUNT[%1] in DiskCapacity list.(%2)	The configuration value of the monitoring is not correct. %1:configured value %2:Monitor resource name	Check the configured value on the Cluster WebUI.		o						
sra	Warning	20354	%1 was illegal value (%2).(%3)	The configuration value of the monitoring is not correct. %1:Variable name %2:configured value %3:Monitor resource name	Check the configured value on the Cluster WebUI.		o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Warning	20355	The DriveLetter of %1 is not ready, or Drive type was not fixed.(%2 DriveLetter = %3)	The configuration value of the monitoring is not correct. %1:Variable name %2:Monitor resource name %3:configured value	Check the configured value on the Cluster WebUI.		o						
sra	Error	20358	A process resource error was detected. (%1 type = cpu, pid = %2, %3)	An error was detected in monitoring the CPU usage rate of the specific process. %1:Monitor resource name %2:Process ID %3:Process name	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20358	A process resource error was detected. (%1 type = memory leak, pid = %2, %3)	An error was detected in monitoring the memory usage of the specific process. %1:Monitor resource name %2:Process ID %3:Process name	Check the possible causes of the monitoring failure.	o	o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Error	20358	A process resource error was detected. (%1 type = file leak, pid = %2, %3)	An error was detected in monitoring the number of the open files of the specific process. %1:Monitor resource name %2:Process ID %3:Process name	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20358	A process resource error was detected. (%1 type = thread leak, pid = %2, %3)	An error was detected in monitoring the number of the threads of the specific process. %1:Monitor resource name %2:Process ID %3:Process name	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20358	A process resource error was detected. (%1 type = same name process, pid = %2, %3)	An error was detected in monitoring a process with the same name. %1:Monitor resource name %2:Process ID %3:Process name	Check the possible causes of the monitoring failure.	o	o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Error	20359	A system resource error was detected. (%1 type = cpu)	An error was detected in monitoring the CPU usage rate of the system. %1:Monitor resource name	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20359	A system resource error was detected. (%1 type = memory)	An error was detected in monitoring the usage amount of the total memories of the system. %1:Monitor resource name	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20359	A system resource error was detected. (%1 type = swap)	An error was detected in monitoring the usage amount of the total virtual memories of the system. %1:Monitor resource name	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20360	A disk resource error was detected. (%1 type = used rate, level = NOTICE, %2)	A notice-level error was detected in monitoring the disk usage rate. %1:Monitor resource name %2:Logical drive	Check the possible causes of the monitoring failure.	o	o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
sra	Error	20360	A disk resource error was detected. (%1 type = used rate, level = WARNING, %2)	A warning-level error was detected in monitoring the disk usage rate. %1:Monitor resource name %2:Logical drive	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20360	A disk resource error was detected. (%1 type = free space, level = NOTICE, %2)	A notice-level error was detected in monitoring the free space of disks. %1:Monitor resource name %2:Logical drive	Check the possible causes of the monitoring failure.	o	o						
sra	Error	20360	A disk resource error was detected. (%1 type = free space, level = WARNING, %2)	A warning-level error was detected in monitoring the free space of disks. %1:Monitor resource name %2:Logical drive	Check the possible causes of the monitoring failure.	o	o						
ddns	Error	5051	Failed to register the virtual host name (%1) to the DNS server.	DNS registration failure %1: Virtual host name	Check whether an error occurred in the DNS server, or whether an error occurred in communication with the DNS server.	o	o						

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
ddns	Error	5052	Failed to delete the virtual host name (%1) from the DNS server.	Failure of deletion of DNS registration %1: Virtual host name	Check whether an error occurred in the DNS server, or whether an error occurred in communication with the DNS server.	o	o						
ddns	Error	5053	Failed to disable the Kerberos Authentication (virtual host name: %1).	Failure of disabling Kerberos Authentication %1: Virtual host name	Check if there is an error in Kerberos Authentication server (KDC) or a problem of communications with Kerberos Authentication server (KDC). You can ignore this error if the settings have been made for each server.	o	o						
webmgr	Warning	5121	HTTPS configuration isn't correct, HTTPS mode doesn't work. Please access WebManager by HTTP mode.	Invalid HTTPS setting	-	o	o	o					
forcestop	Information	5201	Forced stop of server %1 has been requested.(%2, %3)	forced-stop requested	-	o	o	o					
forcestop	Information	5202	Forced stop of server %1 has completed.(%2, %3)	forced-stop completed	-	o	o	o					

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
forcestop	Error	5203	The previous forced-stop request has not yet been completed on server %1. (%2, %3, pid=%4)	Uncompleted forced-stop request	Check the started processes.	o	o	o				o	
forcestop	Error	5204	A request to Forced stop of server %1 has been failed.(%2, %3)	Failure of the forced-stop request	Check whether the command can be used.	o	o	o				o	
forcestop	Error	5205	The previous forced-stop check request has not yet been completed on server %1. (%2, %3, pid=%4)	Uncompleted forced-stop check request	Check the started processes.	o	o	o				o	
forcestop	Error	5206	Forced stop of server %1 failed.(%2, %3)	forced-stop failed	Check whether the command can be used.	o	o	o				o	
httpnp	Error	5251	In %1, communication with the target failed.	Communication with the target failed. %1:Resource name	Check if an error occurred in the network adapter or if the network connection is normal.	o	o	o				o	
httpnp	Error	5252	In %1, communication with the target timed out.	Communication with the target timed out. %1:Resource name	Check if an error occurred in the network adapter or if the network connection is normal.	o	o	o				o	
httpnp	Error	5253	In %1, the target returned a status code of %2.	The status code from the target is invalid. %1:Resource name %2:Status code	Check the target's status.	o	o	o				o	

Continued on next page

Table 11.3 – continued from previous page

Module Type	Event Type	Event ID	Messages	Description	Solution	1	2	3	4	5	6	7	8
witnesshb	Error	5301	In %1, communication with the target failed.	Communication with the target failed. %1:Resource name	Check if an error occurred in the network adapter or if the network connection is normal.	o	o	o				o	
witnesshb	Error	5302	In %1, communication with the target timed out.	Communication with the target timed out. %1:Resource name	Check if an error occurred in the network adapter or if the network connection is normal.	o	o	o				o	
witnesshb	Error	5303	In %1, the target returned a status code of %2.	The status code from the target is invalid. %1:Resource name %2:Status code	Check the target's status.	o	o	o				o	
witnesshb	Error	5304	In %1, an invalid response was received from the target.	An invalid response was received from the target. %1:Resource name	Check the status of the target, which may not be a Witness server.	o	o	o				o	
log	Error	5351	Failed to initialize the settings of the log storage period. The log may be missing. (type=%1)	Failed to initialize the settings of the log storage period	The system may not be able to operate properly.	o	o					o	

11.4 Driver event log messages

11.4.1 Disk filter driver

The following events are recorded in system event log as the source "clpdiskfltr".

Event Type	Event ID	Message	Description	Solution
Info	1001	Mirror disk resource activated without mirroring achieved.(%1)	Mirror disk resource has been activated without connecting to the mirror disk connect. %1: mirror disk number	Mirror disk resource has been activated while the other server is not in normal state such as in failover or access restriction release. Make sure there is no error in the other server.
Info	1002	The mirror disk connect of mirror disk %1 is available. (Priority %2)	The standby mirror disk connect has been recovered. The degenerated state has changed to the redundant state. %1: Mirror disk number %2: Priority number	-
Info	1003	The mirror disk connect used for mirror data communication of mirror disk %1 has been changed due to a user request. (Priority %2 -> %3)	The active mirror disk connect has been changed due to a manual change request. %1: Mirror disk number %2: Priority number before switching %3: Priority number after switching	-
Info	1004	The mirror disk connect used for mirror data communication of mirror disk %1 has been changed due to a request from the sending server. (Priority %2 -> %3)	The active mirror disk connect has been changed due to a request from the sending server. %1: Mirror disk number %2: Priority number before switching %3: Priority number after switching	Make sure there is no error in the network.

Continued on next page

Table 11.4 – continued from previous page

Event Type	Event ID	Message	Description	Solution
Info	1005	The operation of compressing mirror communication data of mirror disk %1 has been changed (%2).	The mirror communication data compression method has been changed to one different from the specified method.	-
Info	1006	The mirror disk has been activated in compatible mode. The version of the driver is different from that of the mirror destination server (%1).	The version of the EXPRESSCLUSTER on the destination server is old. %1: Mirror disk number	Make sure the version of the installed EXPRESSCLUSTER is the same.
Info	1007	An error occurred when the mirror disk connect was initialized. (%1)	Because an error occurred during initialization of the mirror disk connect, the target mirror disk connect is not available. %1: IP address of the mirror disk connect	Make sure there is no error in the network.
Error	2001	Mirror disk connect error.(%1)	Disconnected: Disconnection has been detected in the mirror disk connect.	Make sure there is no error in the network.
			Timeout - HealthCheck: There was no response from the other server.	Same as above.
			Timeout - 1stAck: There was no response from the other server.	Make sure there is no error in the network or the other server.
			Timeout - 2ndAck: There was no response from the other server.	Same as above.
			refused by other: The other server is in an invalid status (like being activated).	The same as above
			Mirror DP Not Found: The data partition of the other server cannot be found.	Make sure there is no error in the data partition of the other server.

Continued on next page

Table 11.4 – continued from previous page

Event Type	Event ID	Message	Description	Solution
Error	2002	Asynchronized transfer error.(%1)	Timeout - GetKernelQueue: Timeout occurred in asynchronized transfer.	An error occurred in the user process of asynchronized transfer. Check that the clpdiskagent process is running normally, and that there is no error in I/O to the local disk.
			History Overflow: The number of the items to be recorded as history (default 6553500 I/O) was exceeded, so mirroring was interrupted.	Consider to decrease the process to write asynchronized transfer or improve the speed of circuit.
Error	2003	Mirror disk access error(DP).(%1)	Accessing the mirror disk failed. %1: mirror disk number	Make sure there is no error in the data partition of the mirror disk. In case of an error, exchange the disk for the one without an error.
Error	2004	Mirror disk access error(CP).(%1)	Failed to record the difference information on the cluster partition. %1: mirror disk number	Make sure there is no error in the cluster partition of the mirror disk. In case of an error, exchange the disk for the one without an error.
Error	2005	Cluster partition access error.	Accessing the cluster portion failed.	Make sure there is no error in the cluster partition of the mirror disk. In case of an error, exchange the disk for the one without an error.
Error	2006	Mirror disk activation error.(%1)	Standby: Mirror disk is already being operated as the standby system.	An error in operation is considered to have caused this error. Check the cause of this error.
			Already opened: Mirror disk is already being operated as the active system.	Same as above.
			Refused by other: The status of the other server is wrong. (It is being activated now.)	Same as above.
Error	2007	Failed to initialize the encryption. (%1)	The initialization of the encryption failed. %1: nmp_index=Mirror disk number	Kernel memory or OS resource may not be sufficient. Check with performance monitor.

Continued on next page

Table 11.4 – continued from previous page

Event Type	Event ID	Message	Description	Solution
Error	2008	The encryption key is invalid. (%1)	Invalid encryption key. %2: nmp_index=Mirror disk number	Check if the correct encryption key is used.
Error	2009	Failed to encrypt the mirror data. (%1)	The encryption of the mirror data failed. %1: nmp_index=Mirror disk number	Kernel memory or OS resource may not be sufficient. Check with performance monitor.
		Failed to encrypt the mirror data. (%1, Encryption serial no overflow.)	Overflow of encryption serial number. %1: nmp_index=Mirror disk number	Update the encryption key.
Error	2010	Failed to decrypt the mirror data. (%1)	The decryption of mirror data failed. %1: nmp_index=Mirror disk number	Kernel memory or OS resource may not be sufficient. Check with performance monitor.
		Failed to decrypt the mirror data. (%1, Encryption serial no overflow.)	Overflow of encryption serial number. %1: nmp_index=Mirror disk number	Update the encryption key.
Error	2099	Internal error.	An internal error occurred.	Insufficient kernel memory or OS resource is considered to have caused this error. Check this error with the performance monitor.
Warning	3001	The mirror disk connect used for mirror data communication of mirror disk %1 has been changed due to a communication error. (Priority %2 -> %3)	Disconnection of the active mirror disk connect has been detected. The mirror disk connect will be switched and mirror disk connect %3 will be used. %1: Mirror disk number %2: Priority number before switching %3: Priority number after switching	Make sure there is no error in the network.
Warning	3002	The mirror disk connect of mirror disk %1 is unavailable. (Priority %2)	Disconnection of the standby mirror disk connect has been detected. %1: Mirror disk number %2: Priority number	Make sure there is no error in the network.

Continued on next page

Table 11.4 – continued from previous page

Event Type	Event ID	Message	Description	Solution
Error	5001	Connection error on mirror disk connect.(%1)	Connecting to the mirror disk connect failed.	Make sure there is no error in the network or the mirror disk connect settings.
Error	5002	Communication error on mirror disk connect.(%1)	Because the network has an error or is highly loaded, the mirror disk connect is disconnected.	Make sure there is no error in the network.
Error	5003	History file access error.(%1)	Failed to write or read the history file.	Make sure there is no error in the hard disk. In case of an error, exchange the disk for the one without an error.
Error	5004	Mirror disk virtual device access error.(%1)	Failed to obtain the data from the mirror disk virtual driver.	The mirror disk virtual driver is not running normally or has an error. Check that EXPRESSCLUSTER has been set up correctly.
Error	5005	Mirror disk connect timeout.(%1)	The network has an error or is highly loaded, the mirror disk connect is disconnected.	Make sure there is no error in the network or the other server.
Error	5006	History file disk overflow.(%1)	Failed to output the history file because of insufficient disk capacity.	The folder to store the history file does not have enough. Set the folder with enough capacity.
Error	5007	Queue buffer allocation error.(%1)	Failed to allocate the buffer for asynchronized transfer.	Insufficient memory or OS resource is considered to have caused this error. Check the cause.
Error	5099	Internal error.(%1)	An internal error occurred.	Insufficient memory or OS resource is considered to have caused this error. Check the cause.

11.4.2 Kernel mode LAN heartbeat driver

The following events are recorded in system event log as the source "clphb".

Event Type	Event ID	Message	Description	Solution
Error	3001	Fatal error occurred in the driver.	Fatal error occurred in the driver.	Kernel memory or OS resource may not be sufficient. Check with performance monitor.

Continued on next page

Table 11.5 – continued from previous page

Event Type	Event ID	Message	Description	Solution
Info	1001	Signal has been set to the shutdown event due to the keep alive timeout.	User space is stalled.	Kernel memory or OS resource may not be sufficient. Check with performance monitor.
Info	1002	Signal has been set to the shutdown event due to the FILTER closing action.	Received FILTER closing action.	Kernel memory or OS resource may not be sufficient. Check with performance monitor.

11.5 Detailed information in activating and deactivating group resources

The following information is displayed in the messages recorded in event logs or alert logs as detail information when the resource activation/deactivation fails.

11.5.1 Application resource

Module Type	Type	Return Value	Message	Description	Solution
appli	Error	5	The application path is invalid.	The application path is invalid.	Check if the application path is correct.
appli	Error	7	Failed to start application.	Failed to start application.	Memory or OS resources may not be sufficient. Check them.
appli	Error	8	Failed to stop application.	Failed to stop application.	Memory or OS resources may not be sufficient. Check them.
appli	Error	10	Timeout occurred.	Timeout occurred.	Check if the application terminates within the timeout period.
appli	Error	11	Failed to log on as a user.	Failed to log on as a user.	Check if a domain, an account and a password of the logon user are set properly.
appli	Error	12	Returned exit code %1.	The non-resident type application returned abnormal error code.	Check the cause for the abnormal error code.
appli	Error	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.2 CIFS Resource

Module Type	Type	Return Value	Message	Description	Solution
cifs	Error	2	The specified path is invalid.	The specified path is invalid.	Correct the setting of target folder.
cifs	Error	3	Access denied.	Access denied.	Check if local system account has the appropriate access right to the target folder.
cifs	Error	4	The share name is already in use on this server.	The specified name of the shared folder is already in use on this server.	Correct the setting of shared name.
cifs	Error	5	The specified path does not exist.	The specified path does not exist.	Correct the setting of target folder.

Continued on next page

Table 11.7 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
cifs	Error	6	Insufficient memory is available.	Insufficient memory is available.	Memory or OS resources may not be sufficient. Check them.
cifs	Error	7	The specified folder can not be found.	The specified folder can not be found.	Correct the setting of target folder.
cifs	Error	8	The specified shared name cannot be found.	The shared folder to be monitored does not exist.	Check if the shared configuration has not been released.
cifs	Error	10	Failed to set the caching.	Failed to set the caching.	Check if local system account has the appropriate access right to the target folder.
cifs	Error	11	Failed to set security information.	Failed to set security information.	Check if local system account has the appropriate access right to the target folder.
cifs	Error	15	The shared configuration file path is wrong.	Specified path does not exist, or invalid character strings are used in the absolute path.	Correct the configuration value.
cifs	Error	17	Failed to write the shared configuration file.	Failed to save the shared configuration in the file.	Check if the writing to the shared configuration file is available with the local system account.
cifs	Error	18	Failed to read the shared configuration file.	Failed to read the shared configuration form the file.	Check if the reading from the shared configuration file is available with the local system account.
cifs	Error	20	Failed to start up CIFS control process.	Failed to start up the process (clpcifsp.exe) that monitors the change of shared configuration	There may be corruption of the execution file, lack of memory capacity or lack of OS resource. Check these issues.
cifs	Error	25	Failed to set comments for the shared folder.	Failed to set comments for the shared folder.	Check the access right for the local system account and the shared name of the shared folder.
cifs	Error	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.3 Floating IP resource

Module Type	Type	Return Value	Message	Description	Solution
fip	Error	5	IP address already exists.	IP address already exists.	Check if the IP address is already used on the network. Set the IP address that is not used.
fip	Error	8	Available adapter does not exist.	Available adapter does not exist.	Check if the FIP address network is the same as the server's real IP address.
fip	Error	9	Failed to add IP address.	Failed to add IP address.	Check the result of the ipconfig command. If 0.0.0.0 address exists, restart NIC.
fip	Error	10	Failed to delete IP address.	Failed to delete IP address.	Memory or OS resources may not be sufficient. Check them.
fip	Error	99	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.4 Mirror disk resource/Hybrid disk resource

Module Type	Type	Return Value	Message	Description	Solution
md/hd	Error	2	An internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.
md/hd	Error	2	The resource is busy.	The resource is busy.	The partition may be in use. Wait for a while, and retry the operation.
md/hd	Error	2	This operation has been canceled due to timeout.	This operation has been canceled due to timeout.	Memory or OS resources may not be sufficient. Check them.
md/hd	Error	2	The operation was canceled.	The operation was canceled.	Memory or OS resources may not be sufficient. Check them.
md/hd	Error	2	A network error occurred.	A network error occurred.	Check the status of the interconnect connection.
md/hd	Error	2	Cannot establish the mirror disk connection.	Cannot establish the mirror disk connection.	Check if the cluster configuration data is correct.
md/hd	Error	2	The resource name is invalid.	The resource name is invalid.	Check if the cluster configuration data is correct.
md/hd	Error	2	The status is invalid.	The status is invalid.	You need to perform the mirror recovery.

Continued on next page

Table 11.9 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
md/hd	Error	2	The resource is not initialized.	The resource is not initialized.	Check if the partition is allocated and OS recognizes the disk. Check if the cluster configuration data is correct.
md/hd	Error	2	The resource is not performed first mirror construction.	The resource is not performed first mirror construction.	You need to perform the initial mirror construction.
md/hd	Error	2	The license is not registered.	The license is not registered.	Register the license.
md/hd	Error	2	The trial version has expired.	The trial version has expired.	Register the license.
md/hd	Error	2	The license authentication failed.	The license authentication failed.	Register the license.
md/hd	Error	2	Cannot find the history folder.	Cannot find the history folder.	Check if the cluster configuration data is correct.
md/hd	Error	2	The mirror disk connect is not initialized.	The mirror disk connect is not initialized.	Check the status of the mirror disk connect. Check if the cluster configuration data is correct.
md/hd	Error	2	The server name is invalid.	The server name is invalid.	Check if the cluster configuration data is correct.
hd	Error	2	The server group name is invalid.	The server group name is invalid.	Check if the cluster configuration data is correct.

11.5.5 Registry synchronization resource

Module Type	Type	Return Value	Message	Description	Solution
regsync	Error	2	Timeout has occurred while waiting for completion of synchronization processing at startup.	The resource cannot be activated because synchronization of registry files between servers has not been completed.	Activate the resource again after a while. If the error persists, OS may have errors. Check the status of the system.
regsync	Error	2	Timeout occurred when waiting for completing initialization of resource thread.	Activating the resource failed because initialization process of the thread has not been completed.	OS may have errors. Check the status of the system.
regsync	Error	2	Timeout occurred when waiting for completing termination of resource thread.	Deactivating the resource failed because termination process of the thread has not been completed.	OS may have errors. Check the status of the system.

Continued on next page

Table 11.10 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
regsync	Error	4	Specified resource does not exist in cluster configuration data.	Activating or deactivating the resource failed because it does not exist on the cluster configuration data.	Check if the resource name is consistent with the information in the cluster configuration data.
regsync	Error	5	Failed to allocate memory.	Activating the resource failed because the memory cannot be allocated.	Memory or OS resources may not be sufficient. Check the status of the system.
regsync	Error	6	Failed to get OS resource.	Activating the resource failed because OS resource cannot be obtained.	Memory or OS resources may not be sufficient. Check the status of the system.
regsync	Error	6	Failed to create thread.	Activating the resource failed because the thread cannot be created.	Memory or OS resources may not be sufficient. Check the status of the system.
regsync	Error	7	Failed to open registry.	Opening the registry failed because invalid registry key is registered to the resource.	Check the value set on the Cluster WebUI (Details on Resource Properties), and change to a correct registry key.
regsync	Error	7	Failed to restore registry.	Restoring the registry failed because invalid registry key is registered to the resource.	Check the value set on the Cluster WebUI (Details on Resource Properties), and change to a correct registry key.
regsync	Error	8	Failed to open registry.	Opening the registry failed because the registry key registered to the resource does not exist on the registry, or Win32 API error occurred.	Check if the registry key exists on the registry. If it does not exist, create it. If it exists, OS may have errors. Check the status of the system.
regsync	Error	8	Failed to restore registry.	Opening the registry failed because the registry key registered to the resource does not exist on the registry, other process opens the registry key, or the system call for registry operation returned an error.	Check if the registry key exists on the registry. If it does not exist, create it. If it exists, check if a process other than EXPRESSCLUSTER opens the registry key. If the registry key exists and no other process opens it, OS may have errors. Check the status of the system.
regsync	Error	9	Failed to lock file.	Locking a file failed when operating the registry storage file.	Check if the process other than EXPRESSCLUSTER opens the registry storage file.

Continued on next page

Table 11.10 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
regsync	Error	9	Failed to input/output the file.	The input/output process of the file failed when operating the registry storage file.	Check if the process other than EXPRESSCLUSTER opens the registry storage file. OS may have errors. Check the status of the system.
regsync	Error	12	Synchronization processing at startup has failed.	The resource cannot be activated because synchronization process of the registry storage file between servers failed.	OS may have errors. Check the status of the system.

11.5.6 Script resource

Module Type	Type	Return Value	Message	Description	Solution
script	Error	6	Failed to execute start script.	Failed to execute start script.	Memory or OS resources may not be sufficient. Check them.
script	Error	7	Failed to execute stop script.	Failed to execute stop script.	Memory or OS resources may not be sufficient. Check them.
script	Error	8	Returned exit code %1.	The synchronous type script returned abnormal error code.	Check the cause for the abnormal error code.
script	Error	9	Timeout occurred.	Timeout occurred.	Check if the script terminates within the timeout period.
script	Error	10	Failed to log on as a user.	Logon as a user failed	Check if the domain, account and password of the execution user are correctly set.
script	Error	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.7 Disk resource

Module Type	Type	Return Value	Message	Description	Solution
sd	Error	-1	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
sd	Error	-1	Failed to load cluster configuration data.	Failed to load cluster configuration data.	Check if the cluster configuration data is stored on a proper location.
sd	Error	-1	Failed to unload cluster configuration data.	Failed to unload cluster configuration data.	Check if the cluster configuration data is stored on a proper location.
sd	Error	-1	Failed to get cluster configuration data.	Failed to get cluster configuration data.	Check if the cluster configuration data is correct.
sd	Error	-1	Failed to allocate memory.	Failed to allocate memory.	Memory or OS resources may not be sufficient. Check them.
sd	Error	-1	Failed to activate resource.	Failed to activate resource.	Check if the HBA settings are correct. The partition may be in use. Check it.
sd	Error	-1	Failed to create thread.	Failed to create thread.	Memory or OS resources may not be sufficient. Check them.
sd	Error	-1	Timeout occurred on thread.	Timeout occurred on thread.	Memory or OS resources may not be sufficient. Check them.
sd	Error	-1	Failed to dismount the partition specified by the resource.	Failed to dismount the partition specified by the resource.	The partition may be in use. Check it.
sd	Error	-1	Failed to lock the partition specified by the resource.	Failed to lock the partition specified by the resource.	The partition may be in use. Check it.
sd	Error	-1	Failed to deactivate resource.	Failed to deactivate resource.	Check if the HBA settings are correct.
sd	Error	-1	Server does not exist in cluster configuration data.	Server does not exist in cluster configuration data.	Check if the server exists in the cluster configuration data.
sd	Error	-1	Resource does not exist in cluster configuration data.	Resource does not exist in cluster configuration data.	Check if the resource exists in the cluster configuration data.
sd	Error	-1	Cannot find the specified partition.	Cannot find the specified partition.	Check if OS recognizes the specified partition.
sd	Error	-1	Cannot change the drive letter.	Cannot change the drive letter.	Check if the specified drive letter is used for another partition.

11.5.8 Service resource

Module Type	Type	Return Value	Message	Description	Solution
service	Error	5	Failed to get service control right.	Failed to get service control right.	Check if the service name is correct.
service	Error	6	Failed to start service.	Failed to start service.	Check the status of the service.
service	Error	7	Failed to stop service.	Failed to stop service.	Check the status of the service.
service	Error	8	Service has already been running.	Service has already been running.	Check the status of the service. It is possible to configure settings not to make it an error when the service is already running.
service	Error	10	Timeout occurred.	Timeout occurred.	Check if the service starts or stops within the timeout period.
service	Error	13	Computer name related to service that is running is different from virtual computer name of target VCOM resource.	Computer name related to service that is running is different from virtual computer name of target VCOM resource.	When you set the same service to more than one service, do not set the target VCOM resource name.
service	Error	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.9 Virtual computer name resource

Module Type	Type	Return Value	Message	Description	Solution
vcom	Error	5	VCOM control process has already been started.	VCOM control process has already been started.	Memory or OS resources may not be sufficient. Check them. Restart the OS.
vcom	Error	6	VCOM control process has not been started.	VCOM control process has not been started.	Memory or OS resources may not be sufficient. Check them. Restart the OS.

Continued on next page

Table 11.14 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
vcom	Error	8	VCOM control process does not exist.	VCOM control process does not exist.	Memory or OS resources may not be sufficient. Check them. Restart the OS.
vcom	Error	9	Failed to get IP address table.	Failed to get IP address table.	Memory or OS resources may not be sufficient. Check them.
vcom	Error	10	Target FIP address does not exist.	Target FIP address does not exist.	Check if the IP address of the target FIP resource exists.
vcom	Error	11	Virtual computer name is the same as local host-name.	Virtual computer name is the same as local host-name.	Do not set existing host names for a virtual com-puter name.
vcom	Error	12	Failed to start VCOM control process.	Failed to start VCOM control process.	Check if all conditions for using a virtual com-puter are met.
vcom	Error	13	Failed to stop VCOM control process.	Failed to stop VCOM control process.	An error occurred when stopping the virtual computer. Restart the OS.
vcom	Error	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.10 Virtual IP resource

Module Type	Type	Return Value	Message	Description	Solution
vip	Error	5	IP address already exists.	IP address already exists.	Check if the IP address is already used on the network. Set the IP address that is not used.
vip	Error	8	Available adapter does not exist.	Available adapter does not exist.	Check if the IP address set on the interconnect exists on the server. Set a proper IP address.
vip	Error	9	Failed to add IP address.	Failed to add IP address.	Check the result of the ipconfig command. If 0.0.0.0 address exists, restart NIC.

Continued on next page

Table 11.15 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
vip	Error	10	Failed to delete IP address.	Failed to delete IP address.	Memory or OS resources may not be sufficient. Check them.
vip	Error	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.11 Dynamic DNS resource

Module Type	Type	Return Value	Message	Description	Solution
ddns	Error	1	Parameter is invalid.	The dynamic DNS resource or dynamic DNS monitoring resource parameter is invalid.	Check the cluster configuration data.
ddns	Error	2	Group does not exist in cluster configuration data.	Group does not exist in cluster configuration data.	Check the cluster configuration data.
ddns	Error	3	Resource does not exist in cluster configuration data.	Resource does not exist in cluster configuration data.	Check the cluster configuration data.
ddns	Error	4	Failed to get the value from cluster configuration data.	Failed to get the value from cluster configuration data.	Check the cluster configuration data.
ddns	Error	5	Query to DNS has failed.	Query to DNS has failed.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddns	Error	6	Failed to delete DNS.	Failed to delete DNS.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddns	Error	7	Failed to update DNS.	Failed to update DNS.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddns	Error	8	A reception timeout occurred.	A reception timeout occurred.	Memory or OS resources may not be sufficient. Check them.
ddns	Error	9	Failed to send to the DNS server.	Failed to send to the DNS server.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddns	Error	10	Failed to receive from the DNS server.	Failed to receive from the DNS server.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.

Continued on next page

Table 11.16 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
ddns	Error	13	DDNS control process has already started.	DDNS control process has already started.	Memory or OS resources may not be sufficient. Check them. Or, the previous activation might fail. In this case, stop the cluster and kill the DDNS control process (clpddnsp.exe) manually.
ddns	Error	14	DDNS control process is not running.	DDNS control process is not running.	Check the DNS server setting. Make sure that communication with the DNS server is enabled. Or, memory or OS resources are shortage. Check them.
ddns	Error	16	Failed to start DDNS control process.	Failed to start DDNS control process.	Check the DNS server setting. Make sure that communication with the DNS server is enabled. Or, memory or OS resources are shortage. Check them.
ddns	Error	17	Failed to stop DDNS control process.	Failed to stop DDNS control process.	Check the DNS server setting. Make sure that communication with the DNS server is enabled. Or, memory or OS resources may not be sufficient. Check them.
ddns	Error	18	DDNS control process path is invalid.	DDNS control process path is invalid.	The executable file is damaged, or memory or OS resources are shortage. Check them.
ddns	Error	99	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.12 AWS elastic ip resources

Module type	Type	Return value	Message	Description	Solution
awseip	Error	50	The AWS CLI command failed.	The AWS CLI command failed.	Check if the settings in the AWS CLI file are correct.
awseip	Error	50	* Any other message	* An error message of the AWS CLI command.	-
awseip	Error	51	The AWS CLI command was not found.	The AWS CLI command was not found.	Check if AWS CLI is installed correctly.
awseip	Error	52	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS elastic ip resource.
awseip	Error	53	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awseip	Error	54	Failed to obtain a primary private IP address.	Failed to obtain a primary private IP address.	Check the settings of AWS Elastic ip resource. Check if the settings in the AWS CLI file are correct.
awseip	Error	55	ENI ID is invalid.	The ENI ID is invalid.	Check if the value of ENI ID is correct. Check if ENI ID of other instance is specified mistakenly.
awseip	Error	79	Internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.13 AWS virtual ip resources

Module type	Type	Return value	Message	Description	Solution
awsvip	Error	50	The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsvip	Error	50	* Any other message	* An error message of the AWS CLI command.	-
awsvip	Error	51	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awsvip	Error	52	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS virtual ip resource.

Continued on next page

Table 11.18 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsvip	Error	53	The VIP address belongs to a VPC subnet.	The VIP address 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	54	Failed to add the VIP address.	Failed to add the VIP address.	Check the VIP settings. Memory or OS resources may not be sufficient. Check them.
awsvip	Error	55	Failed to delete the VIP address.	Failed to delete the VIP address.	Memory or OS resources may not be sufficient. Check them.
awsvip	Error	56	Failed to obtain a NIC name.	Failed to obtain a NIC name.	Check the settings of AWS virtual ip resource. Memory or OS resources may not be sufficient. Check them.
awsvip	Error	57	Failed to obtain a network adapter index.	Failed to obtain a network adapter index.	Check the settings of AWS virtual ip resource. Memory or OS resources may not be sufficient. Check them.
awsvip	Error	63	Failed to obtain a primary private IP address.	Failed to obtain a primary private IP address.	Check the settings of AWS virtual ip resource. Check if the settings in the AWS CLI file are correct.
awsvip	Error	64	ENI ID is invalid.	The ENI ID is invalid.	Check if the value of ENI ID is correct. Check if ENI ID of other instance is specified mistakenly.
awsvip	Error	79	Internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.14 AWS secondary ip resources

Module type	Type	Return value	Message	Description	Solution
awssip	Error	50	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awssip	Error	52	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS secondary ip resource.
awssip	Error	54	Failed to process checking DHCP.	Failed to process checking DHCP.	Check the DHCP settings.
awssip	Error	55	Failed to assign the secondary IP address on the AWS side.(%1)	Failed to assign the secondary IP address on the AWS side. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssip	Error	56	Failed to release the assigned secondary IP address on the AWS side.(%1)	Failed to release the assigned secondary IP address on the AWS side. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssip	Error	57	Failed to process checking the secondary IP address on the AWS side.(%1)	Failed to process checking the secondary IP address on the AWS side. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssip	Error	58	Failed to assign the secondary IP address on the OS side.	Failed to assign the secondary IP address on the OS side.	Check the settings of AWS secondary ip resource. Memory or OS resources may not be sufficient. Check them.
awssip	Error	59	Failed to release the assigned secondary IP address on the OS side.	Failed to release the assigned secondary IP address on the OS side.	Check the settings of AWS secondary ip resource. Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.19 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awssip	Error	61	Failed to process checking the secondary IP address on the OS side.	Failed to process checking the secondary IP address on the OS side.	Check the settings of AWS secondary ip resource. Memory or OS resources may not be sufficient. Check them.
awssip	Error	62	Failed to obtain a MAC address.(%1)	Failed to obtain a MAC address. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssip	Error	63	Failed to obtain a NIC name.	Failed to obtain a NIC name.	Check the settings of AWS secondary ip resource. Memory or OS resources may not be sufficient. Check them.
awssip	Error	64	Failed to obtain a subnet ID.(%1)	Failed to obtain a subnet ID. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssip	Error	65	Failed to obtain a CIDR block.(%1)	Failed to obtain a CIDR block. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssip	Error	68	Failed to obtain a primary private IP address.(%1)	Failed to obtain a primary private IP address. %1:Cause of error	Check the settings of AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.

Continued on next page

Table 11.19 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awssip	Error	69	ENI ID is invalid.	The ENI ID is invalid.	Check if the value of ENI ID is correct. Check if ENI ID of other instance is specified mistakenly.
awssip	Error	79	Internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.15 AWS DNS resource

Module type	Type	Return value	Message	Description	Solution
awsdns	Error	50	The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsdns	Error	50	* Any other message	* An error message of the AWS CLI command.	-
awsdns	Error	51	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsdns	Error	52	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awsdns	Error	53	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS DNS resource.
awsdns	Error	54	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.
awsdns	Error	55	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.
awsdns	Error	79	Internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.16 Azure probe port resources

Module type	Type	Return value	Message	Description	Solution
azurepp	Error	5	Probe port is already used.	The Probe port is already used.	Check if the probe port is already opened on the local server.
azurepp	Error	6	Failed to open the probe port.	Failed to open the probe port.	Memory or OS resources may not be sufficient. Check them.
azurepp	Error	7	Failed to close the probe port.	Failed to close the probe port.	Memory or OS resources may not be sufficient. Check them.
azurepp	Error	8	Failed to stop the probe port control process.	Failed to stop the probe port control process.	Memory or OS resources may not be sufficient. Check them. Reboot the OS.
azurepp	Error	9	The probe port control process has already started.	The probe port 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 probe port control process (clpazureppp.exe) manually.
azurepp	Error	10	Failed to start the robe port control process.	Failed to start the probe port control process.	Memory or OS resources may not be sufficient. Check them.
azurepp	Error	99	Internal error has occurred.	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.17 Azure DNS resource

Module type	Type	Return value	Message	Description	Solution
azuredns	Error	41	Timeout has occurred when executing the Azure CLI command.	The Azure CLI command did not end within Azure CLI Timeout.	Make sure that the Azure CLI command can be executed properly in EXPRESSCLUSTER server. Check the load status of the server and remove the load. Check the value of Azure CLI Timeout.
azuredns	Error	42	The Azure CLI command failed. (%1)	The Azure CLI command was executed. However, an error was returned. %1:Cause of error	Make sure that the settings of resources are correct.
azuredns	Error	43	The Azure CLI command was not found.	The Azure CLI command was not found.	Make sure that the settings of Azure CLI File Path are correct and that Azure CLI is installed properly.
azuredns	Error	99	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.18 Google Cloud virtual IP resource

Module type	Type	Return value	Message	Description	Solution
gcvip	Error	5	Port is already used.	Port is already used.	Check if the port specified for **Port Number** on the local server has already been used.
gcvip	Error	6	Failed to open the port.	Opening the port failed.	Check if memory or OS resources are sufficient.
gcvip	Error	7	Failed to close the port.	Closing the port failed.	Check if memory or OS resources are sufficient.
gcvip	Error	8	Failed to stop the port control process.	Stopping the port control process failed.	Check if memory or OS resources are sufficient. Restart the OS.

Continued on next page

Table 11.23 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
gcvip	Error	9	The port control process has already started.	The port control process has already started.	Check if memory or OS resources are sufficient. Or, the immediately preceding deactivation may have failed. In that case, stop the cluster and forcibly terminate the port control process (clpgcvipp.exe) manually.
gcvip	Error	10	Failed to start the port control process.	Starting the port control process failed.	Check if memory or OS resources are sufficient.
gcvip	Error	99	Internal error.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.5.19 Google Cloud DNS resources

Module Type	Type	Return Value	Message	Description	Solution
gcdns	Error	50	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of Google Cloud DNS resource.
gcdns	Error	51	Failed to obtain the record set.(%1)	Failed to obtain the record set of Cloud DNS. %1:Cause of error	Check the setting value of Google Cloud DNS resource and the privilege of the account which permitted Cloud SDK.
gcdns	Error	52	Failed to start the transaction.(%1)	Failed to start the transaction. %1:Cause of error	Check the privilege of the account which permitted Cloud SDK.
gcdns	Error	53	Failed to delete the record set.(%1)	Failed to add the record set deletion processing to the transaction. %1:Cause of error	Check the privilege of the account which permitted Cloud SDK.
gcdns	Error	54	Failed to add the record set.(%1)	Failed to add the record set addition processing to the transaction. %1:Cause of error	Check the privilege of the account which permitted Cloud SDK.

Continued on next page

Table 11.24 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
gcdns	Error	55	Failed to execute the transaction.(%1)	Failed to execute the transaction. %1:Cause of error	Check the privilege of the account which permitted Cloud SDK.
gcdns	Error	56	Detected an invalid parameter.	An internal error occurred.	-
gcdns	Error	57	The gcloud CLI command is not found.	The gcloud CLI command is not found.	Check if gcloud CLI is installed correctly.
gcdns	Error	79	Internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.5.20 Oracle Cloud virtual IP resource

Module type	Type	Return value	Message	Description	Solution
ocvip	Error	5	Port is already used.	Port is already used.	Check if the port specified for **Port Number** on the local server has already been used.
ocvip	Error	6	Failed to open the port.	Opening the port failed.	Check if memory or OS resources are sufficient.
ocvip	Error	7	Failed to close the port.	Closing the port failed.	Check if memory or OS resources are sufficient.
ocvip	Error	8	Failed to stop the port control process.	Stopping the port control process failed.	Check if memory or OS resources are sufficient. Restart the OS.
ocvip	Error	9	The port control process has already started.	The port control process has already started.	Check if memory or OS resources are sufficient. Or, the immediately preceding deactivation may have failed. In that case, stop the cluster and forcibly terminate the port control process (clpocvipp.exe) manually.
ocvip	Error	10	Failed to start the port control process.	Starting the port control process failed.	Check if memory or OS resources are sufficient.
ocvip	Error	99	Internal error.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.5.21 Oracle Cloud DNS resources

Module type	Type	Return value	Message	Description	Solution
ocdns	Error	50	The OCI CLI command failed. (%1)	The OCI CLI command failed. %1:Cause of error	Check the settings of Oracle Cloud DNS resources.
ocdns	Error	51	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
ocdns	Error	52	The OCI CLI command is not found.	The OCI CLI command is not found.	Check if OCI CLI is installed correctly.
ocdns	Error	79	Internal error occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.6 Detailed information of monitor resource errors

The following information is displayed in the message recorded in event logs or alert logs as detail information when monitor resource detects an error.

11.6.1 Application monitor resource

Module Type	Type	Return Value	Message	Description	Solution
appliw	Error	9	Process did not exist. (Stop code : %1)	Process did not exist. (The stop code is displayed only if it can be acquired.)	Process of the monitoring target application resource was cleared due to some error. Check it.
appliw	Error	11	Failed to log on as a user.	Failed to log on as a user.	Check if a domain, an account and a password of the logon user are set properly.
appliw	Warning	Others	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.2 CIFS monitor resource

Module Type	Type	Return Value	Message	Description	Solution
cifsw	Error	8	The specified share name can not be found.	The specified share name can not be found.	Check if the setting of file sharing has been canceled.
cifsw	Error	13	Error occurred while doing file check.	Error occurred while doing file check.	Check if local system account has the appropriate access right for executing specified method of monitoring.
cifsw	Error	14	Error occurred while doing folder check.	Error occurred while doing folder check.	Check if local system account has the appropriate access right for executing specified method of monitoring.
cifsw	Error	19	Failed to check the shared configuration file.	Failed to execute checking the configuration data saved in the shared configuration file.	Check if the shared configuration file is corrupted.
cifsw	Warning	21	CIFS control process does not exist.	Failed to start up the process (clpcifsp.exe) that monitors the change of shared configuration.	Activate CIFS resource again.

Continued on next page

Table 11.28 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
cifsw	Warning	101	Setting has been changed.	Setting of file sharing has been changed.	Check if the user limit setting or the target folder of file sharing has been changed.
cifsw	Warning	103	Access denied.	Local system account doesn't have the appropriate access right to the shared folder.	Set an access privilege for the local system account.
cifsw	Warning	106	Insufficient memory is available.	Insufficient memory is available.	Memory or OS resources may not be sufficient. Check them.
cifsw	Warning	189	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.3 DB2 monitor resource

Module Type	Type	Return Value	Message	Description	Solution
db2w	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure. Information on the initialization may be displayed on %1.	OS itself may have errors. Restart the server or take other actions.
db2w	Warning	102	The configured value is not correct.	The configured value of the monitoring is not correct.	Check the configured value on the Cluster WebUI because they may not be correct.
db2w	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
db2w	Error	11	An error was detected in accessing the monitor target.	Accessing the database failed.	Check configured values on the Cluster WebUI (such as a database name). If there is no error, check the database has errors.
db2w	Warning	112	An error was detected in user authentication.	Accessing the database failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check the database has errors.

Continued on next page

Table 11.29 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
db2w	Warning	113	An application error was detected.	A database error was detected.	Refer to error messages for database described separately to fix errors.
db2w	Error	14	An error was detected in executing SQL statement [%1].	Executing SQL statement failed. The executed SQL statement is displayed on %1.	Refer to error messages for database described separately to fix errors.
db2w	Error	15	A data error was detected.	A value on the table of database has an error.	Database may be corrupt. Stop the database operation and investigate it. This error may occur when more than one monitoring is performed with the same monitor table name concurrently. Check if the values set in the multi-directional environment are appropriate.
db2w	Warning	140	No license is registered.	The license has not been registered.	Register the license.
db2w	Warning	160	Failed to obtain the configuration data.	The configured value could not be obtained.	OS may have errors. Restart the server or take other actions.
db2w	Warning	190	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.4 Disk RW monitor resource

Module Type	Type	Return Value	Message	Description	Solution
diskw	Error	5	Failed to open the file.	Failed to open the file.	Check if the disk driver of the monitoring target disk is loaded, the disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.30 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
diskw	Error	6	Failed to write in the file.	Failed to write in the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. Memory or OS resources may not be sufficient. Check them.
diskw	Error	7	Failed to synchronize the disk of the file.	Failed to synchronize the disk of the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. Memory or OS resources may not be sufficient. Check them.
diskw	Error	8	Failed to close the file.	Failed to close the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. Memory or OS resources may not be sufficient. Check them.
diskw	Error	71	Timeout has occurred when opening the file.	Timeout has occurred when opening the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. The system may be under high load, or memory or OS resources may not be sufficient. Check them.
diskw	Error	72	Timeout has occurred when writing in the file.	Timeout has occurred when writing in the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. The system may be under high load, or memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.30 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
diskw	Error	73	Timeout has occurred when synchronizing the disk of the file.	Timeout has occurred when synchronizing the disk of the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. The system may be under high load, or memory or OS resources may not be sufficient. Check them.
diskw	Error	74	Timeout has occurred when closing the file.	Timeout has occurred when closing the file.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. The system may be under high load, or memory or OS resources may not be sufficient. Check them.
diskw	Warning	100	Failed to add keep alive drive when initializing keep alive driver.	Failed to add keep alive drive when initializing keep alive driver.	Memory or OS resources may not be sufficient. Check them.
diskw	Warning	101	There is not enough disk space.	There is not enough disk space.	Secure free space on the monitoring target disk.
diskw	Warning	102	Timeout has occurred when initializing internal resources.	Timeout has occurred when initializing internal resources.	Memory or OS resources may not be sufficient. Check them.
diskw	Warning	103	Timeout has occurred when other timing.	Timeout has occurred when other timing.	The system may be under high load, or memory or OS resources may not be sufficient. Check them.
diskw	Warning	104	Failed to allocate memory.	Failed to allocate memory.	Memory or OS resources may not be sufficient. Check them.
diskw	Warning	105	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
diskw	Warning	190	Initialization error has occurred in internal resource.	Initialization error has occurred in internal resource.	Memory or OS resources may not be sufficient. Check them.

11.6.5 Floating IP monitor resource

Module Type	Type	Return Value	Message	Description	Solution
fipw	Error	6	IP address does not exist.	IP address does not exist.	NIC may have been disabled. Check if the FIP address exists by the ipconfig command.
fipw	Error	11	Adapter Index is different.	Adapter Index is different.	NIC may have been disabled. Check if the FIP address exists by the ipconfig command.
fipw	Error	15	Detected NIC Link Down.	Detected NIC Link Down.	Check if the LAN cable is connected properly.
fipw	Warning	112	Failed to get the IP address list.	Failed to get the IP address list.	Memory or OS resources may not be sufficient. Check them.
fipw	Warning	113	Failed to get the NIC interface name.	Failed to get the NIC interface name.	Memory or OS resources may not be sufficient. Check them.
fipw	Warning	114	Failed to get the NIC status.	Failed to get the NIC status.	Check if the NIC device is supported by the device I/O controller.
fipw	Warning	189	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.6 FTP monitor resource

Module Type	Type	Return Value	Message	Description	Solution
ftpw	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address). If there is no error, check if the monitor application has errors.
ftpw	Error	12	An error was detected in user authentication.	The user authentication failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors
ftpw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.

Continued on next page

Table 11.32 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
ftpw	Warning	113	An application error was detected.	A monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
ftpw	Warning	115	A data error was detected.	A value of the response data has an error.	Refer to error messages for monitor applications described separately to fix errors.
ftpw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
ftpw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
ftpw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions

11.6.7 Custom monitor resource

Module Type	Type	Return Value	Message	Description	Solution
genw	Error	5	Failed to start script.	Failed to start script.	Check if the script can be executed.
genw	Error	6	Script did not exist.	The asynchronous type script terminated abnormally.	Check the cause of the termination of the script.
genw	Error	8	Returned exit code %1.	The synchronous type script returned abnormal error code.	Check the cause for the abnormal error code.
genw	Error	9	Failed to log on as a user.	Logon as a user failed	Check if the domain, account and password of the execution user are correctly set.
genw	Warning	100	Timeout occurred.	The synchronous type script did not terminate within the timeout period.	Check the cause of the delay of the script.
genw	Warning	100	Returned exit code %1.	The synchronous type script returned abnormal error code.	Check the cause for the abnormal error code.

Continued on next page

Table 11.33 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
genw	Warning	110	Returned warning value (%1).	The synchronous type script returned a warning value.	Check the cause of the warning value returned by the script.
genw	Warning	100 190	Script path is invalid.	The configured value of the script path is not correct.	Check the configured value on the Cluster WebUI.
genw	Warning	100 190	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
genw	Warning	190	Parameter is invalid.	The configured value of the monitoring is not correct.	Check the configured value on the Cluster WebUI.
genw	Warning	190	Resource does not exist in cluster configuration data.	The cluster configuration data is not correct.	Check the cluster configuration data on the Cluster WebUI.
genw	Warning	190	Failed to get the value from cluster configuration data.	The cluster configuration data is not correct.	Check the cluster configuration data on the Cluster WebUI.
genw	Warning	190	Script did not exist.	The asynchronous type script terminated abnormally.	Check the cause of the termination of the script.
genw	Error	200	Failed to start script.	Failed to start script.	Check if the script can be executed.

11.6.8 Hybrid disk TUR monitor resource

Module Type	Type	Return Value	Message	Description	Solution
hdtw	Error	4	Failed to open device. Check the disk status of monitor destination volume.	Failed to open device. Check the disk status of monitor destination volume.	Check if the disk driver of the monitoring target disk is loaded, the device exists, the disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. Memory or OS resources may not be sufficient. Check them.
hdtw	Error	5	Failed to control device. Check the disk status of monitor destination volume.	Failed to control device. Check the disk status of monitor destination volume.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk.

Continued on next page

Table 11.34 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
hdtw	Warning	100	Other internal error has occurred. Check the system resource.	Other internal error has occurred. Check the system resource.	Memory or OS resources may not be sufficient. Check them.
hdtw	Warning	190	Initialization has failed. Check the cluster configuration data or system resources.	Initialization has failed. Check the cluster configuration data or system resources.	Memory or OS resources may not be sufficient. Check them.

11.6.9 Mirror disk monitor resource/Hybrid disk monitor resource

Module Type	Type	Return Value	Message	Description	Solution
mdw/hdw	Error	3	Mirror disk %1 has old data.	The information in the activated mirror disk %1 is not updated.	Check the status of the mirror disk with Mirror disks.
			Hybrid disk %1 has old data.	The information in the activated hybrid disk %1 is not updated.	Check the status of the hybrid disk with Mirror disks.
mdw/hdw	Error	4	A disk error is detected in mirror disk %1.	A disk error has been detected in mirror disk %1.	Make sure there is no HW failure in the disk or disk path where cluster partition or data partition exists.
			A disk error is detected in hybrid disk %1.	A disk error has been detected in hybrid disk %1.	Make sure there is no HW failure in the disk or disk path where cluster partition or data partition exists.
mdw/hdw	Error	5	The status of mirror disk %1 is invalid.	The status of the mirror disk %1 is invalid.	Restart the cluster.
			The status of hybrid disk %1 is invalid.	The status of the hybrid disk %1 is invalid.	Restart the cluster.
mdw/hdw	Warning	101	Mirror disk %1 recovery is in progress.	Mirror disk %1 is being copied.	Wait for a while until mirror recovery completes.
			Hybrid disk %1 recovery is in progress.	Hybrid disk %1 is being copied.	Wait for a while until mirror recovery completes.
mdw/hdw	Warning	102	Mirror disk %1 is not being mirrored.	Mirror disk %1 has not been mirrored.	Check the status of the mirror disk with Mirror disks.
			Hybrid disk %1 is not being mirrored.	Hybrid disk %1 has not been mirrored.	Check the status of the hybrid disk with Mirror disks.
mdw/hdw	Warning	103	Mirror disk %1 is activated on more than one server.	Mirror disk %1 is activated on both servers.	Deactivate the mirror disk on one of the servers.

Continued on next page

Table 11.35 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
			Hybrid disk %1 is activated on more than one server.	Hybrid disk %1 is activated on both server groups.	Deactivate the hybrid disk on one of the server groups.
mdw/hdw	Warning	104	The status of mirror disk %1 is unknown.	Mirror disk to be monitored is stopped.	Stop the monitor resource or start the mirror disk to be monitored.
			The status of hybrid disk %1 is unknown.	Hybrid disk to be monitored is stopped.	Stop the monitor resource or start the hybrid disk to be monitored.
mdw/hdw	Warning	105	Whether mirror disk %1 data is old/new is not determined.	Whether the data in mirror disk %1 is old or new has not been determined.	Activate the mirror disk on one of the servers.
			Whether hybrid disk %1 data is old/new is not determined.	Whether the data in hybrid disk %1 is old or new has not been determined.	Activate the hybrid disk on one of the servers.
mdw/hdw	Warning	106	Internal error.	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.10 HTTP monitor resource

Module Type	Type	Return Value	Message	Description	Solution
httpw	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address). If there is no error, check if the monitor application has errors.
httpw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
httpw	Warning	113	An application error was detected.	A monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
httpw	Warning	115	A data error was detected.	A value of the response data has an error.	Refer to error messages for monitor applications described separately to fix errors.
httpw	Warning	116	The algorithm is not supported. (%1)	The algorithm is not supported. %1 represents the algorithm.	-

Continued on next page

Table 11.36 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
httpw	Warning	117	Client authentication error.	Client authentication error.	Check if the client certificate subject name is correctly set.
httpw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
httpw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
httpw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.11 IMAP4 monitor resource

Module Type	Type	Return Value	Message	Description	Solution
imap4w	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address). If there is no error, check if the monitor application has errors.
imap4w	Error	12	An error was detected in user authentication.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors.
imap4w	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
imap4w	Warning	113	An application error was detected.	A monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.

Continued on next page

Table 11.37 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
imap4w	Warning	115	A data error was detected.	A value of the response data has an error.	Refer to error messages for monitor applications described separately to fix errors.
imap4w	Warning	140	No license is registered.	The license has not been registered.	Register the license.
imap4w	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
imap4w	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions

11.6.12 IP monitor resource

Module Type	Type	Return Value	Message	Description	Solution
ipw	Error	4	Ping could not reach.	Ping could not reach.	Check if the ping command to the corresponding IP address succeeds. When the command fails, check the status of the device that has the IP address and the network interface.
ipw	Warning	105	Timeout occurred.	Timeout occurred.	Memory or OS resources may not be sufficient. Check them.
ipw	Warning	189	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.13 NIC Link Up/Down monitor resource

Module Type	Type	Return Value	Message	Description	Solution
miiw	Error	4	IP address does not exist.	IP address does not exist.	NIC may have been disabled. Check if the IP address of the specified NIC exists by the ipconfig command.
miiw	Error	8	Detected NIC Link Down.	Detected NIC Link Down.	Check if the LAN cable is connected properly.
miiw	Warning	105	Failed to get the IP address list.	Failed to get the IP address list.	Memory or OS resources may not be sufficient. Check them.
miiw	Warning	106	Failed to get the NIC interface name.	Failed to get the NIC interface name.	Memory or OS resources may not be sufficient. Check them.
miiw	Warning	107	Failed to get the NIC status.	Failed to get the NIC status.	Check if the NIC device is supported by the device I/O controller.
miiw	Warning	189	An internal error has occurred.	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.14 Multi target monitor resource

Module Type	Type	Return Value	Message	Description	Solution
mtw	Error	Other	Internal error occurred.(status:%1)	Internal error occurred.(status:%1)	Memory or OS resources may not be sufficient. Check them.
mtw	Error	5	Status of resources is abnormal.	Status of resources is abnormal.	Check the status of the monitor resources listed on the monitor resources list.
mtw	Error	1	This option is invalid.	This option is invalid.	Memory or OS resources may not be sufficient. Check them.

11.6.15 Process name monitor resource

Module Type	Type	Return Value	Message	Description	Solution
psw	Error	4	Process [%1, pid=%2] down.	Loss of the process to be monitored has been detected.	Check whether the process to be monitored is running properly.

Continued on next page

Table 11.41 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
psw	Error	5	The number of processes is less than the specified minimum process count. %1/%2 (%3)	The number of running processes to be monitored does not reach the specified lower limit.	Check whether the process to be monitored is running properly.
psw	Warning	100	Internal error occurred.	An internal error has occurred.	Check the following possible causes: memory shortage or OS resource insufficiency. Check it.
psw	Warning	190	Parameter is invalid.	The monitor setting value is incorrect.	The setting value for the Cluster WebUI may be incorrect. Check it.

11.6.16 ODBC monitor resource

Module Type	Type	Return Value	Message	Description	Solution
odbcw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure. Information on the initialization may be displayed on %1.	OS itself may have errors. Restart the server or take other actions.
odbcw	Warning	102	The configured value is not correct.	The configured value of the monitoring is not correct.	Check the configured value on the Cluster WebUI because it may not be correct.
odbcw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
odbcw	Error	11	An error was detected in accessing the monitor target.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a database name). If there is no error, check the database has errors.
odbcw	Warning	112	An error was detected in user authentication.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the database has errors.
odbcw	Warning	113	An application error was detected.	The database error was detected.	Refer to error messages for database described separately to fix errors.

Continued on next page

Table 11.42 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
odbcw	Error	14	An error was detected in executing SQL statement [%1].	Executing SQL statement failed. The executed SQL statement is displayed on %1.	Refer to error messages for database described separately to fix errors.
odbcw	Error	15	A data error was detected.	A value on the table of database has an error.	Database may be corrupt. Stop the database operation and investigate it. This error may occur when more than one monitoring is performed with the same monitor table name concurrently. Check if the values set in the multi-directional environment are appropriate.
odbcw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
odbcw	Warning	160	Failed to obtain the configuration data.	The configured value could not be obtained.	OS may have errors. Restart the server or take other actions
odbcw	Warning	190	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.17 Oracle monitor resource

Module Type	Type	Return Value	Message	Description	Solution
oraclew	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure. Information on the initialization may be displayed on %1.	OS itself may have errors. Restart the server or take other actions
oraclew	Warning	102	The configured value is not correct.	The configured value of the monitoring is not correct.	Check the configured value on the Cluster WebUI because it may not be correct.

Continued on next page

Table 11.43 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
oraclew	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
oraclew	Error	11	An error was detected in accessing the monitor target.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a database name). If there is no error, check the database has errors.
oraclew	Warning	112	An error was detected in user authentication.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the database has errors.
oraclew	Warning	113	An application error was detected.	The database error was detected.	Refer to error messages for database described separately to fix errors.
oraclew	Error	14	An error was detected in executing SQL statement [%1].	Executing SQL statement failed. The executed SQL statement is displayed on %1.	Refer to error messages for database described separately to fix errors.
oraclew	Error	15	A data error was detected.	A value on the table of database has an error.	Database may be corrupt. Stop the database operation and investigate it. This error may occur when more than one monitoring is performed with the same monitor table name concurrently. Check if the values set in the multi-directional environment are appropriate.
oraclew	Warning	140	No license is registered.	The license has not been registered.	Register the license.
oraclew	Warning	160	Failed to obtain the configuration data.	The configured value could not be obtained.	OS may have errors. Restart the server or take other actions.
oraclew	Warning	190	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.18 POP3 monitor resource

Module Type	Type	Return Value	Message	Description	Solution
pop3w	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address). If there is no error, check if the monitor application has errors.
pop3w	Error	12	An error was detected in user authentication.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors.
pop3w	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
pop3w	Warning	113	An application error was detected.	The monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
pop3w	Warning	115	A data error was detected.	A value of the response data has an error.	Refer to error messages for monitor applications described separately to fix errors.
pop3w	Warning	140	No license is registered.	The license has not been registered.	Register the license.
pop3w	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
pop3w	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.19 PostgreSQL monitor resource

Module Type	Type	Return Value	Message	Description	Solution
psqlw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure. Information on the initialization may be displayed on %1.	OS itself may have errors. Restart the server or take other actions.
psqlw	Warning	102	The configured value is not correct.	The configured value of the monitoring is not correct.	Check the configured value on the Cluster WebUI because it may not be correct.
psqlw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
psqlw	Error	11	An error was detected in accessing the monitor target.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a database name). If there is no error, check the database has errors.
psqlw	Warning	112	An error was detected in user authentication.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the database has errors.
psqlw	Warning	113	An application error was detected.	The database error was detected.	Refer to error messages for database described separately to fix errors.
psqlw	Error	14	An error was detected in executing SQL statement [%1].	Executing SQL statement failed. The executed SQL statement is displayed on %1.	Refer to error messages for database described separately to fix errors.

Continued on next page

Table 11.45 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
psqlw	Error	15	A data error was detected.	A value on the table of database has an error.	Database may be corrupt. Stop the database operation and investigate it. This error may occur when more than one monitoring is performed with the same monitor table name concurrently. Check if the values set in the multi-directional environment are appropriate.
psqlw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
psqlw	Warning	160	Failed to obtain the configuration data.	The configured value could not be obtained.	OS may have errors. Restart the server or take other actions.
psqlw	Warning	190	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.20 Registry synchronization monitor resource

Module Type	Type	Return Value	Message	Description	Solution
regsyncw	Error	50	Failed to save registry.	The process of storing to a file at detection of registry update failed.	Check if the process other than EXPRESSCLUSTER opens the registry storage file. Memory or OS resources may not be sufficient. Check the status of the system.
regsyncw	Warning	100	Delivery processing to other nodes has failed.	Registry storage files cannot be delivered to other nodes.	There may be an error on the connection to the other node. Check the status of the network. OS of the local or other server may have an error. Check the status of the system.
regsyncw	Warning	101	Setting of registry keys is invalid.	An invalid registry key is registered to the resource.	Check the value set on the Cluster WebUI (Details on Resource Properties), and change to a correct registry key.

11.6.21 Disk TUR monitor resource

Module Type	Type	Return Value	Message	Description	Solution
sdw	Error	4	Failed to open device. Check the disk status of monitor destination volume.	Failed to open device. Check the disk status of monitor destination volume.	Check if the disk driver of the monitoring target disk is loaded, the device exists, the disk is connected properly, the disk is powered on, or no other errors are occurred on the disk. Memory or OS resources may not be sufficient. Check them.
sdw	Error	5	Failed to control device. Check the disk status of monitor destination volume.	Failed to control device. Check the disk status of monitor destination volume.	Check if the monitoring target disk is connected properly, the disk is powered on, or no other errors are occurred on the disk.
sdw	Warning	100	Other internal error has occurred. Check the system resource.	Other internal error has occurred. Check the system resource.	Memory or OS resources may not be sufficient. Check them.
sdw	Warning	190	Initialization has failed. Check the cluster configuration data or system resources.	Initialization has failed. Check the cluster configuration data or system resources.	Memory or OS resources may not be sufficient. Check them.

11.6.22 Service monitor resource

Module Type	Type	Return Value	Message	Description	Solution
servicew	Error	9	Service has been stopped.	Service has been stopped.	Check the status of the service.
servicew	Warning	100	Failed to obtain the service control right.	Failed to obtain the service control right.	Check if the service name is correct.
servicew	Warning	Others	An internal error has occurred.	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.23 SMTP monitor resource

Module Type	Type	Return Value	Message	Description	Solution
smtpw	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address). If there is no error, check if the monitor application has errors.
smtpw	Error	12	An error was detected in user authentication.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors.
smtpw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
smtpw	Warning	113	An application error was detected.	The monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
smtpw	Warning	115	A data error was detected.	A value of the response data has an error.	Refer to error messages for monitor applications described separately to fix errors.
smtpw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
smtpw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
smtpw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.24 SQL Server monitor resource

Module Type	Type	Return Value	Message	Description	Solution
sqlserverw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure. Information on the initialization may be displayed on %1.	OS itself may have errors. Restart the server or take other actions.
sqlserverw	Warning	102	The configured value is not correct.	The configured value of the monitoring is not correct.	Check the configured value on the Cluster WebUI because it may not be correct.
sqlserverw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
sqlserverw	Error	11	An error was detected in accessing the monitor target.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a database name). If there is no error, check the database has errors.
sqlserverw	Warning	112	An error was detected in user authentication.	The access to the database failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the database has errors.
sqlserverw	Warning	113	An application error was detected.	The database error was detected.	Refer to error messages for database described separately to fix errors.
sqlserverw	Error	14	An error was detected in executing SQL statement [%1].	Executing SQL statement failed. The executed SQL statement is displayed on %1.	Refer to error messages for database described separately to fix errors.

Continued on next page

Table 11.50 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
sqlserverw	Error	15	A data error was detected.	A value on the table of database has an error.	Database may be corrupt. Stop the database operation and investigate it. This error may occur when more than one monitoring is performed with the same monitor table name concurrently. Check if the values set in the multi-directional environment are appropriate.
sqlserverw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
sqlserverw	Warning	160	Failed to obtain the configuration data.	The configured value could not be obtained.	OS may have errors. Restart the server or take other actions.
sqlserverw	Warning	190	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.25 Tuxedo monitor resource

Module Type	Type	Return Value	Message	Description	Solution
tuxw	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an application config file). If there is no error, check if the monitor application has errors.
tuxw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
tuxw	Warning	113	An application error was detected.	The monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
tuxw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
tuxw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.51 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
tuxw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.26 Virtual computer name monitor resource

Module Type	Type	Return Value	Message	Description	Solution
vcomw	Error	5	VCOM control process has already been started.	VCOM control process has already been started.	Memory or OS resources may not be sufficient. Check them. Restart the OS.
vcomw	Error	6	VCOM control process has not been started.	VCOM control process has not been started.	Memory or OS resources may not be sufficient. Check them. Restart the OS.
vcomw	Error	8	VCOM control process does not exist.	VCOM control process does not exist.	The VCOM control process ID does not exist. Restart the OS.
vcomw	Warning	189	An internal error has occurred.	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.27 Virtual IP monitor resource

Module Type	Type	Return Value	Message	Description	Solution
vipw	Error	6	IP address does not exist.	IP address does not exist.	NIC may have been disabled. Check if the VIP address exists by the ipconfig command.
vipw	Error	11	Adapter Index is different.	Adapter Index is different.	NIC may have been disabled. Check if the VIP address exists by the ipconfig command.
vipw	Warning	189	An internal error has occurred.	An internal error has occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.28 WebSphere monitor resource

Module Type	Type	Return Value	Message	Description	Solution
wasw	Error	12	An error was detected in user authentication.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors.
wasw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
wasw	Warning	113	An application error was detected.	The monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
wasw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
wasw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.54 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
wasw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.29 WebLogic monitor resource

Module Type	Type	Return Value	Message	Description	Solution
wlsw	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address). If there is no error, check if the monitor application has errors.
wlsw	Error	12	An error was detected in user authentication.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors.
wlsw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
wlsw	Warning	113	An application error was detected.	The monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
wlsw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
wlsw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.55 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
wlsw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.30 WebOTX monitor resource

Module Type	Type	Return Value	Message	Description	Solution
otxw	Error	11	An error was detected in accessing the monitor target.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as an IP address or an application server name). If there is no error, check if the monitor application has errors.
otxw	Error	12	An error was detected in user authentication.	The access to the monitor application failed.	Check configured values on the Cluster WebUI (such as a user name or a password). If there is no error, check if the monitor application has errors.
otxw	Warning	110	A function error was detected.	A function error occurred.	Monitor applications or OS may have errors. Check the status of the system.
otxw	Warning	113	An application error was detected.	The monitor application error was detected.	Refer to error messages for monitor applications described separately to fix errors.
otxw	Warning	140	No license is registered.	The license has not been registered.	Register the license.
otxw	Warning	188	Internal error.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

Continued on next page

Table 11.56 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
otxw	Warning	190	Initialization has failed[%1].	Initialization process has failed. It may be due to memory allocation failure or a failure in obtaining the configured value. Information on the initialization may be displayed on %1.	The configured value of the Cluster WebUI may be incorrect. Check the value. If there is no problem with the value, OS itself may have errors. Restart the server or take other actions.

11.6.31 JVM monitor resource

Module Type	Type	Return Value	Message	Description	Solution
jraw	Error	11	An error was detected in accessing the monitor target.	Connection to the target to be monitored has failed.	Check that the Java VM to be monitored is running.
jraw	Error	12	%1 to be monitored has become abnormal. %1:Error generation cause	An error in the target to be monitored has been detected.	Based on the message, check the Java application that is running on Java VM to be monitored.
jraw	Warning	192	Internal error occurred.	An internal error has occurred.	Execute cluster suspend and cluster resume.

11.6.32 System monitor resource

Module Type	Type	Return Value	Message	Description	Solution
sraw	Error	11	Monitor sraw has detected an 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.

11.6.33 Process resource monitor resource

Module Type	Type	Return Value	Message	Description	Solution
psrw	Error	11	Monitor psrw has detected an 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.

11.6.34 User mode monitoring resource

Module Type	Type	Return Value	Message	Description	Solution
userw	Error	71	Timeout has occurred when creating dummy thread.	Timeout has occurred when creating dummy thread.	The system may be under high load, or memory or OS resources may not be sufficient. Check them.
userw	Warning	100	A timeout occurred when initializing internal resources.	A timeout occurred when initializing internal resources.	Memory or OS resources may not be sufficient. Check them.
userw	Warning	101	Timeout has occurred when closing dummy thread handle.	Timeout has occurred when closing dummy thread handle.	The system may be under high load, or memory or OS resources may not be sufficient. Check them.
userw	Warning	102	Timeout has occurred when other timing.	Timeout has occurred when other timing.	The system may be under high load, or memory or OS resources may not be sufficient. Check them.
userw	Warning	190	An initialization error has occurred in an internal resource.	An initialization error has occurred in an internal resource.	Memory or OS resources may not be sufficient. Check them.

11.6.35 Dynamic DNS monitoring resource

Module Type	Type	Return Value	Message	Description	Solution
ddnsw	Error	5	Query to DNS has failed.	Query to DNS has failed.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.

Continued on next page

Table 11.61 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
ddnsw	Warning	13	DDNS control process has already started.	DDNS control process has already started.	Memory or OS resources may not be sufficient. Check them. Or, the previous activation might fail. In this case, stop the cluster and kill the DDNS control process (clpddnsp.exe) manually.
ddnsw	Warning	14	DDNS control process is not running.	DDNS control process is not running.	Check the DNS server setting. Make sure that communication with the DNS server is enabled. Or, memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	16	Failed to start DDNS control process.	Failed to start DDNS control process.	Check the DNS server setting. Make sure that communication with the DNS server is enabled. Or, memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	17	Failed to stop DDNS control process.	Failed to stop DDNS control process.	Check the DNS server setting. Make sure that communication with the DNS server is enabled. Or, memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	18	DDNS control process path is invalid.	DDNS control process path is invalid.	The executable file is damaged, or memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	106	Failed to delete DNS.	Failed to delete DNS.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.

Continued on next page

Table 11.61 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
ddnsw	Warning	107	Failed to update DNS.	Failed to update DNS.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddnsw	Warning	108	A reception timeout occurred.	A reception timeout occurred.	Memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	109	Failed to send to the DNS server.	Failed to send to the DNS server.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddnsw	Warning	110	Failed to receive from the DNS server.	Failed to receive from the DNS server.	Check the DNS server setting. Make sure that communication with the DNS server is enabled.
ddnsw	Warning	111	Ping has not reached.	Ping has not reached.	Check whether the ping command is successfully executed for the target IP address. If the ping command failed, check the status of the device that uses the target IP address, or the network interface status.
ddnsw	Warning	112	Ping timeout occurred.	Ping timeout occurred.	Memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	189	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
ddnsw	Warning	190	Initialization has failed.	Initialization process has failed. A failure in obtaining the configuration data might occur.	Check the cluster configuration data.

11.6.36 AWS elastic ip monitor resources

Module type	Type	Return value	Message	Description	Solution
awseipw	Error	50	The AWS CLI command failed.	The AWS CLI command failed.	Check if the settings in the AWS CLI file are correct.
awseipw	Error	50	* Any other message	* An error message of the AWS CLI command.	-

Continued on next page

Table 11.62 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awseipw	Error	51	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awseipw	Error	52	The EIP address does not exist.	The EIP address does not exist.	The EIP may have been detached. Check it.
awseipw	Warning	150	The AWS CLI command failed.	The AWS CLI command failed.	Check if the settings in the AWS CLI file are correct.
awseipw	Warning	150	* Any other message	* An error message of the AWS CLI command.	-
awseipw	Warning	151	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awseipw	Warning	153	The AWS CLI command was not found.	The AWS CLI command was not found.	Check if AWS CLI is installed correctly.
awseipw	Warning	154	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS elastic ip monitor resources.
awseipw	Warning	155	Failed to obtain the environment variables.	Failed to obtain the environment variables.	Check if the given environment variables at the time of performing AWS-related features are correct.
awseipw	Warning	156	Failed to obtain the AWS CLI command line options.	Failed to obtain the AWS CLI command line options.	Check if the given AWS CLI command line options are correct.
awseipw	Warning	179	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.37 AWS virtual ip monitor resources

Module type	Type	Return value	Message	Description	Solution
awsvipw	Error	50	The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsvipw	Error	50	* Any other message	* An error message of the AWS CLI command.	-
awsvipw	Error	56	The routing for VIP was changed.	The routing for VIP was changed.	The VIP routing may have been changed. Check the Route Tables of the VPC.

Continued on next page

Table 11.63 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsvipw	Error	57	The VIP address does not exist.	The VIP address does not exist.	NIC may have been disabled. Check if the VIP address exists with the ipconfig command.
awsvipw	Error	79	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
awsvipw	Warning	150	The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsvipw	Warning	150	* Any other message	* An error message of the AWS CLI command.	-
awsvipw	Warning	151	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awsvipw	Warning	152	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS virtual ip monitor resources.
awsvipw	Warning	153	Failed to obtain the VIP address.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS virtual ip monitor resources and AWS virtual ip resource.
awsvipw	Warning	154	Failed to obtain the VPC ID.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS virtual ip monitor resources and AWS virtual ip resource.
awsvipw	Warning	155	Failed to obtain the ENI ID.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS virtual ip monitor resources and AWS virtual ip resource.
awsvipw	Warning	158	Failed to obtain the environment variables.	Failed to obtain the environment variables.	Check if the given environment variables at the time of performing AWS-related features are correct.
awsvipw	Warning	160	Failed to obtain the AWS CLI command line options.	Failed to obtain the AWS CLI command line options.	Check if the given AWS CLI command line options are correct.
awsvipw	Warning	179	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.38 AWS secondary ip monitor resources

Module type	Type	Return value	Message	Description	Solution
awssipw	Error	57	Failed to process checking the secondary IP address on the AWS side.(%1)	Failed to process checking the secondary IP address on the AWS side. %1:Cause of error	Check the settings of AWS secondary ip monitor resources and AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssipw	Error	58	Failed to process checking the secondary IP address on the OS side.	Failed to process checking the secondary IP address on the OS side.	Check the settings of AWS secondary ip monitor resources and AWS secondary ip resource. Memory or OS resources may not be sufficient. Check them.
awssipw	Error	79	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
awssipw	Warning	150	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awssipw	Warning	151	Failed to obtain the environment variables.	Failed to obtain the environment variables.	Check if the given environment variables at the time of performing AWS-related features are correct.
awssipw	Warning	152	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS secondary ip monitor resources.
awssipw	Warning	154	Failed to obtain the secondary IP address.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS secondary ip monitor resources and AWS secondary ip resource.
awssipw	Warning	155	Failed to obtain the ENI ID.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS secondary ip monitor resources and AWS secondary ip resource.

Continued on next page

Table 11.64 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awssipw	Warning	157	Failed to process checking the secondary IP address on the AWS side.(%1)	Failed to process checking the secondary IP address on the AWS side. %1:Cause of error	Check the settings of AWS secondary ip monitor resources and AWS secondary ip resource. Check if the settings in the AWS CLI file are correct.
awssipw	Warning	159	Failed to obtain the AWS CLI command line options.	Failed to obtain the AWS CLI command line options.	Check if the given AWS CLI command line options are correct.
awssipw	Warning	179	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.39 AWS AZ monitor resources

Module type	Type	Return value	Message	Description	Solution
awsazw	Error	50	The AWS CLI command failed.	The AWS CLI command failed.	Check if the settings in the AWS CLI file are correct.
awsazw	Error	50	* Any other message	* An error message of the AWS CLI command.	-
awsazw	Error	51	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsazw	Error	52	Failed to monitor the availability zone.	Failed to monitor the availability zone.	The availability zone to which the server belongs may have a problem. Check it.
awsazw	Error	79	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
awsazw	Warning	150	The AWS CLI command failed.	The AWS CLI command failed.	Check if the settings in the AWS CLI file are correct.
awsazw	Warning	150	* Any other message	* An error message of the AWS CLI command.	-
awsazw	Warning	151	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.

Continued on next page

Table 11.65 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsazw	Warning	152	Failed to monitor the availability zone.	Failed to monitor the availability zone.	The availability zone to which the server belongs may have a problem. Check it.
awsazw	Warning	153	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awsazw	Warning	154	Failed to obtain the environment variables.	Failed to obtain the environment variables.	Check if the given environment variables at the time of performing AWS-related features are correct.
awsazw	Warning	155	Failed to obtain the AWS CLI command line options.	Failed to obtain the AWS CLI command line options.	Check if the given AWS CLI command line options are correct.
awsazw	Warning	178	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
awsazw	Warning	179	Initialize error occurred.	Initialize error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.40 AWS DNS monitor resource

Module type	Type	Return value	Message	Description	Solution
awsdnsw	Error	50	The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsdnsw	Error	50	* Any other message	* An error message of the AWS CLI command.	-
awsdnsw	Error	51	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsdnsw	Error	52	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.
awsdnsw	Error	53	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.

Continued on next page

Table 11.66 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsdnsw	Error	54	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	55	IP address which is resolved domain name from the DNS resolver is defferent 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	Error	79	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
awsdnsw	Warning	150	The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
awsdnsw	Warning	150	* Any other message	* An error message of the AWS CLI command.	-
awsdnsw	Warning	151	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
awsdnsw	Warning	156	The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
awsdnsw	Warning	157	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of AWS DNS monitor resource.
awsdnsw	Warning	158	Failed to obtain the environment variables.	Failed to obtain the environment variables.	Check if the given environment variables at the time of performing AWS-related features are correct.
awsdnsw	Warning	159	Failed to obtain the AWS CLI command line options.	Failed to obtain the AWS CLI command line options.	Check if the given AWS CLI command line options are correct.
awsdnsw	Warning	160	Failed to obtain the Hosted Zone ID.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS DNS monitor resources and AWS DNS resource.

Continued on next page

Table 11.66 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
awsdnsw	Warning	161	Failed to obtain the Resource Record Set Name.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS DNS monitor resources and AWS DNS resource.
awsdnsw	Warning	162	Failed to obtain the IP Address.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of AWS DNS monitor resources and AWS DNS resource.
awsdnsw	Warning	179	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.41 Azure probe port monitor resource

Module type	Type	Return value	Message	Description	Solution
azureppw	Error	4	Probe port is closed.	Probe port is closed.	The probe port is closed. Check the network settings on the server.
azureppw	Error	5	Timeout of waiting probe port occurred.	Timeout of waiting probe port occurred.	The server could not receive the probe from the Azure load balancer in the probe wait timeout. Check if an error does not occur with a network adaptor. Check if the server is connected to the network correctly.
azureppw	Warning	105	Timeout of waiting probe port occurred.	Timeout of waiting probe port occurred.	The server could not receive the probe from the Azure load balancer in the probe wait timeout. Check if an error does not occur with a network adaptor. Check if the server is connected to the network correctly.

Continued on next page

Table 11.67 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
azureppw	Warning	189	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.42 Azure load balance monitor resource

Module type	Type	Return value	Message	Description	Solution
azurelbw	Error	4	Probe port is opened.	Probe port is opened.	The probe has been opened on the standby server. Make sure that the probe port is not opened on the standby server.
azurelbw	Warning	189	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.43 Azure DNS monitor resource

Module type	Type	Return value	Message	Description	Solution
azurednsw	Error	11	Query to DNS server has failed.	Query for name resolution was executed to DNS server of Microsoft Azure. However, it failed.	Make sure that EXPRESSCLUSTER server can communicate with DNS server of Microsoft Azure. From DNS zone of Microsoft Azure portal, check if DNS zone and the record set are registered.
azurednsw	Error	12	An IP address different from the setting value is registered in the record set of Azure DNS zone.	The record set of DNS server might be deleted or rewritten from external.	From DNS zone of Microsoft Azure portal, check the record set.
azurednsw	Warning	189	Internal error occurred.	An internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.44 Google Cloud virtual IP monitor resource

Module type	Type	Return value	Message	Description	Solution
gcvipw	Error	4	Port is closed.	Port is closed.	The port specified for **Port Number** is closed. Check the network settings of the server.
gcvipw	Error	5	Timeout of waiting port 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 failed.	Monitoring port failed.	Check if memory or OS resources are sufficient.
gcvipw	Error	7	Monitoring port is frozen.	Monitoring port is frozen.	Check if memory or OS resources are sufficient.
gcvipw	Error	99	Internal error.	Internal error occurred.	Check if memory or OS resources are sufficient.
gcvipw	Warning	105	Timeout of waiting port 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 occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.6.45 Google Cloud load balance monitor resource

Module type	Type	Return value	Message	Description	Solution
gclbw	Error	4	Port is opened.	Port 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 failed.	Monitoring port failed.	Check if memory or OS resources are sufficient.
gclbw	Error	99	Internal error.	Internal error occurred.	Check if memory or OS resources are sufficient.
gclbw	Warning	189	Internal error occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.6.46 Google Cloud DNS monitor resources

Module Type	Type	Return Value	Message	Description	Solution
gcdnsw	Error	56	Failed to obtain the record set.(%1)	Failed to obtain the record set of Cloud DNS. %1:Cause of error	Check the setting value of Google Cloud DNS monitor resource and the privilege of the account which permitted Cloud SDK.
gcdnsw	Error	57	No record set to be monitored.(%1)	A monitoring failure was detected. %1:Cause of error	-
gcdnsw	Error	79	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.
gcdnsw	Warning	150	Failed to obtain the setting value.	Failed to obtain the setting value.	Check the settings of Google Cloud DNS monitor resource.
gcdnsw	Warning	151	Failed to obtain the zone name.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of Google Cloud DNS monitor resource and Google Cloud DNS resource.

Continued on next page

Table 11.72 – continued from previous page

Module Type	Type	Return Value	Message	Description	Solution
gcdnsw	Warning	152	Failed to obtain the DNS name.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of Google Cloud DNS monitor resource and Google Cloud DNS resource.
gcdnsw	Warning	153	Failed to obtain the record type.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of Google Cloud DNS monitor resource and Google Cloud DNS resource.
gcdnsw	Warning	154	Failed to obtain the TTL.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of Google Cloud DNS monitor resource and Google Cloud DNS resource.
gcdnsw	Warning	155	Failed to obtain the IP address.	Failed to obtain the setting value of the resource to be monitored at activation.	Check the settings of Google Cloud DNS monitor resource and Google Cloud DNS resource.
gcdnsw	Warning	158	The gcloud CLI command is not found.	The gcloud CLI command is not found.	Check if gcloud CLI is installed correctly.
gcdnsw	Warning	179	Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.6.47 Oracle Cloud virtual IP monitor resource

Module type	Type	Return value	Message	Description	Solution
ocvipw	Error	4	Port is closed.	Port is closed.	The port specified for **Port Number** is closed. Check the network settings of the server.

Continued on next page

Table 11.73 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
ocvipw	Error	5	Timeout of waiting port 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 failed.	Monitoring port failed.	Check if memory or OS resources are sufficient.
ocvipw	Error	7	Monitoring port is frozen.	Monitoring port is frozen.	Check if memory or OS resources are sufficient.
ocvipw	Error	99	Internal error.	Internal error occurred.	Check if memory or OS resources are sufficient.
ocvipw	Warning	105	Timeout of waiting port 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 occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.6.48 Oracle Cloud load balance monitor resource

Module type	Type	Return value	Message	Description	Solution
oclbw	Error	4	Port is opened.	Port 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.

Continued on next page

Table 11.74 – continued from previous page

Module type	Type	Return value	Message	Description	Solution
oclbw	Error	5	Monitoring port failed.	Monitoring port failed.	Check if memory or OS resources are sufficient.
oclbw	Error	99	Internal error.	Internal error occurred.	Check if memory or OS resources are sufficient.
oclbw	Warning	189	Internal error occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.6.49 Oracle Cloud DNS monitor resources

Module type	Type	Return value	Message	Description	Solution
ocdnsw	Error	50	The OCI CLI command failed. (%1)	The OCI CLI command failed. %1:Cause of error	Check the settings of Oracle Cloud DNS resources.
ocdnsw	Error	51	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
ocdnsw	Error	52	Name resolution has failed.	Failed to check name resolution of the resource record set.	Set a resolver, or make sure that there is no problem with the network.
ocdnsw	Error	53	The IP address of the result of name resolution is different from the setting value.	The IP address of the result of name resolution is different from the setting value.	Make sure that the settings of DNS resolver are correct and that there is no unintended entry in the hosts file.
ocdnsw	Error	79	Internal error occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.
ocdnsw	Warning	150	The OCI CLI command failed. (%1)	The OCI CLI command failed. %1:Cause of error	Check the settings of Oracle Cloud DNS resources.
ocdnsw	Warning	151	Timeout occurred.	Timeout occurred.	Check the load status of the server and remove the load.
ocdnsw	Warning	152	The OCI CLI command is not found.	The OCI CLI command is not found.	Check if OCI CLI is installed correctly.
ocdnsw	Warning	153	Failed to get the value from cluster configuration data.	Failed to get the value from cluster configuration data.	Check the cluster configuration data.
ocdnsw	Warning	179	Internal error occurred.	Internal error occurred.	Check if memory or OS resources are sufficient.

11.7 Detailed information on forced stop resource errors

The following information is displayed as details in the messages recorded in event logs or alert logs when forced stop resources detect errors.

11.7.1 AWS forced stop resource

Message	Description	Solution
Protection against stopping instances is enabled.	Protection against stopping instances is enabled.	Check the configuration of protection against stopping instances.
The AWS CLI command is not found.	The AWS CLI command is not found.	Check if AWS CLI is installed correctly.
The AWS CLI command failed.	Failed in the AWS CLI command.	Check if the settings in the AWS CLI file are correct.
Stopping instances failed to be completed.	Stopping instances failed to be completed.	Check the configuration of the AWS forced stop resource.
Internal error occurred.	Internal error occurred.	Check the configuration of the AWS forced stop resource.
* Any other message	* An error message of the AWS CLI command.	Check the configuration of the AWS forced stop resource.

11.7.2 Azure forced stop resource

Message	Description	Solution
The Azure CLI command is not found.	The Azure CLI command is not found.	Check if Azure CLI is installed correctly.
Failed to log in to the Azure.	Failed to log in to the Azure.	Check the configuration of the Azure forced stop resource.
The Azure CLI command failed. (%1)	The Azure CLI command failed. %1:Cause of error	Check the configuration of the Azure forced stop resource.
Stopping instances failed to be completed.	Stopping instances failed to be completed.	Check the configuration of the Azure forced stop resource.
Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.7.3 OCI forced stop resource

Message	Description	Solution
The OCI CLI command is not found.	The OCI CLI command is not found.	Check if OCI CLI is installed correctly.
The OCI CLI command failed. (%1)	The OCI CLI command failed. %1:Cause of error	Check the configuration of the OCI forced stop resource.

Continued on next page

Table 11.78 – continued from previous page

Message	Description	Solution
Stopping instances failed to be completed.	Stopping instances failed to be completed.	Check the configuration of the OCI forced stop resource.
Internal error occurred.	Internal error occurred.	Memory or OS resources may not be sufficient. Check them.

11.8 STOP codes list of disk RW monitor resources

The following information is the STOP codes list which are generated when selecting **Generating of intentional Stop Error** on **Action when stalling is detected** of disk RW monitor resource.

STOP code	Description
0xE0000000	The STOP error which was generated as the Final action at detection of an error of the monitor resource at activation or deactivation failure of the group resource.
0xE000FF**	The STOP error which was generated by keep alive timeout (the timeout of disk RW monitor). The lower 8 bits (the part of "**") shows the following checkpoint (The chances are high that it was being executed during timeout).
0xE000FF00	The internal processing of EXPRESSCLUSTER
0xE000FF01	free(), SetWaitableTimer(), GetTickCount(), WaitForMultipleObjects()
0xE000FF02	CreateFile(), _beginthreadex()
0xE000FF03	malloc(), WriteFile()
0xE000FF04	FlushFileBuffers()
0xE000FF05	CloseHandle()
0xE000FF06	The internal processing of EXPRESSCLUSTER

11.9 Filter driver STOP code list

The following lists the STOP codes generated by the EXPRESSCLUSTER filter driver (clpdiskfltr.sys).

STOP code	Description
0xE000FD00	A fatal internal error has occurred in the filter driver.
0xE000FD01	A timeout has occurred during monitoring of the CLUSTER partitions (monitoring by reading and writing for partitions).
0xE000FD02	It is not possible to access the data partition for mirror disk resources or hybrid disk resources.
0xE000FD03	It is not possible to access the cluster partition for mirror disk resources or hybrid disk resources.

11.10 JVM monitor resource log output messages

The following messages belong to the JVM operation 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.)

11.10.1 JVM operation log

Message	Cause of generation	Action
Failed to write the %1.stat.	Writing to the JVM statistics log has failed. %1 .stat: JVM statistics log file name	Check whether there is sufficient free disk space.
%1: analyze finish[%4]. state = %2, cause = %3	(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: Name of the Java VM to be monitored %2: Status of Java VM to be monitored (1=normal, 0=abnormal) %3: Error generation location at abnormality occurrence %4: 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: monitor thread can't connect to JVM.	The Java VM to be monitored could not be connected. %1: Name of the Java VM to be monitored	Check that the Java VM to be monitored is running.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: monitor thread can't get the JVM state.	The resource use amount could not be acquired from Java VM to be monitored. %1: Name of the Java VM to be monitored	Check that the Java VM to be monitored is running.
%1: JVM state is changed [abnormal -> normal].	The status of the Java VM to be monitored has changed from abnormal to normal. %1: Name of the Java VM to be monitored	-
%1: JVM state is changed [normal -> abnormal].	The status of the Java VM to be monitored has changed from normal to abnormal. %1: Name of the Java VM to be monitored	Review the Java application that runs on the Java VM to be monitored.
%1: Failed to connect to JVM. retry = %2 / %3.	The Java VM to be monitored could not be connected. %1: Name of the Java VM to be monitored %2: Number of times the connection consecutively failed %3: Retry Count * **retry = %2$s / %3$s** is not shown after the former value exceeds the latter.	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.
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.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: GARBAGE_COLLECTOR _MXBEAN_DOMAIN_TYPE is invalid.	GC information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: GarbageCollectorMXBean is invalid.	GC information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: Failed to measure the GC stat.	GC information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: GC stat is invalid. last.getCount = %2, last.getTime = %3, now.getCount = %4, now.getTime = %5.	The GC generation count and GC execution time could not be measured for the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: GC generation count at last measurement %3: Total GC execution time at last measurement %4: GC generation count at this measurement %5: 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 11.81 – continued from previous page

Message	Cause of generation	Action
%1: GC average time is too long. av = %6, last.getCount = %2, last.getTime = %3, now.getCount = %4, now.getTime = %5, error_count = %7 / %8.	The average GC execution time has exceeded the threshold in the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: GC generation count at last measurement %3: Total GC execution time at last measurement %4: GC generation count at this measurement %5: Total GC execution time at this measurement %6: Average of the GC execution time used from the last measurement to this measurement %7: Number of times the threshold was consecutively exceeded %8: Error Threshold * **error_count = %7$s / %8$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the Java VM to be monitored.
%1: GC count is too frequently. count = %4 last.getCount = %2, now.getCount = %3, error_count = %5 / %6.	The GC generation count has exceeded the threshold in the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: GC generation count at last measurement %3: GC generation count at this measurement %4: GC generation count from the last measurement to this measurement %5: Number of times the threshold was consecutively exceeded %6: Error Threshold * **error_count = %5$s / %6$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: RuntimeMXBean is invalid.	Information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: Failed to measure the runtime stat.	Information could not be acquired from the Java VM to be monitored. %1: 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: MEMORY_MXBEAN_NAME is invalid. %2, %3.	Memory information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: Memory pool name %3: Memory name	Check whether the operating environment of the Java VM to be monitored is correct.
%1: MemoryMXBean is invalid.	Memory information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: Failed to measure the memory stat.	Memory information could not be acquired from the Java VM to be monitored. %1: 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: MemoryPool name is undefined. memory_name = %2.	Memory information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: Name of the Java memory pool to be measured	Check whether the operating environment of the Java VM to be monitored is correct.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: MemoryPool capacity is too little. memory_name = %2, used = %3, max = %4, ratio = %5, error_count = %6 / %7.	The Java memory pool free space has fallen below the threshold in the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: Name of the Java memory pool to be measured %3: Use amount of the Java memory pool %4: Maximum usable amount of the Java memory pool %5: Use rate of the Java memory pool %6: Number of times the threshold was consecutively exceeded %7: Error Threshold * **error_count = %6$s / %7$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the Java VM to be monitored.
%1: THREAD_MXBEAN_NAME is invalid.	Thread information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: ThreadMXBean is invalid.	Thread information could not be acquired from the Java VM to be monitored.	Check whether the operating environment of the Java VM to be monitored is correct. %1: Name of the Java VM to be monitored
%1: Failed to measure the thread stat.	Thread information could not be acquired from Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: Detect Deadlock. threads = %2.	Thread deadlock has occurred in the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: ID of the deadlock thread	Review the Java application that runs on the Java VM to be monitored.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: Thread count is too much(%2). error_count = %3 / %4.	The number of activated threads has exceeded the threshold in the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: Number of activated threads at measurement %3: Number of times the threshold was consecutively exceeded %4: Error Threshold * **error_count = %3$s / %4$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the Java VM to be monitored.
%1: ThreadInfo is null.Thread count = %2.	Thread information could not be acquired in the Java VM to be monitored. %1: Name of the Java VM to be monitored %2: Number of activated threads at measurement	Check whether the operating environment of the version of the Java VM to be monitored is correct.
%1: Failed to disconnect.	Disconnection from the Java VM to be monitored has failed. %1: Name of the Java VM to be monitored	-
%1: Failed to connect to WebLogic-Server.	WebLogic Server to be monitored could not be connected. %1: Name of the Java VM to be monitored	Review the Java application that runs on the WebLogic Server to be monitored.
%1: Failed to connect to Sun JVM.	Java VM and WebOTX to be monitored could not be connected. %1: 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.	The JVM statistics log could not be output. %1: 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.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: Can't find monitor file.	No monitoring %1: Name of the Java VM to be monitored	-
%1: Can't find monitor file, monitor stopped[thread:%2].	Monitoring stops. %1: Name of the Java VM to be monitored %2: Type of the measurement thread	-
%1: Failed to create monitor status file.	An internal file could not be created. %1: Name of the Java VM to be monitored	Check whether the disk free space and the maximum number of volume files are sufficient.
%1: Failed to delete monitor status file.	An internal file could not be deleted.	Check whether there is a problem with the hard disk.
%1: com.bea:Type=ServerRuntime is invalid.	Information could not be acquired from the Java VM to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the Java VM to be monitored is correct.
%1: WorkManagerRuntimeMBean or ThreadPoolRuntimeMBean is invalid.	Information could not be acquired from the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the WebLogic Server to be monitored is correct.
%1: Failed to measure the WorkManager or ThreadPool stat.	Information could not be acquired from the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored	Check whether the operating environment of the WebLogic Server to be monitored is correct.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: ThreadPool stat is invalid. last.pending = %2, now.pending = %3.	The number of waiting requests could not be measured in the thread pool of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Number of waiting requests at last measurement %3: 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: WorkManager stat is invalid. last.pending = %2, now.pending = %3.	The number of waiting requests could not be measured in the work manager of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Number of waiting requests at last measurement %3: 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: PendingRequest count is too much. count = %2, error_count = %3 / %4.	The number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Number of waiting requests at this measurement %3: Number of times the threshold was consecutively exceeded %4: Error Threshold * **error_count = %3$s / %4$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: PendingRequest increment is too much. increment = %4, last.pending = %2, now.pending = %3, error_count = %5 / %6.	The increment of the number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Number of waiting requests at last measurement %3: Number of waiting requests at this measurement %4: Increment of the number of waiting requests from the last measurement to this measurement %5: Number of times the threshold was consecutively exceeded %6: Error Threshold * **error_count = %5$s / %6$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the WebLogic Server to be monitored.
%1: Throughput count is too much. count = %2, error_count = %3 / %4.	The number of requests executed per unit time has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Number of requests executed per unit time at this measurement %3: Number of times the threshold was consecutively exceeded %4: Error Threshold * **error_count = %3$s / %4$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: Throughput increment is too much. increment = %4, last.throughput = %2, now.throughput = %3, error_count = %5 / %6.	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: Name of the Java VM to be monitored %2: Number of requests executed per unit time at last measurement %3: Number of requests executed per unit time at this measurement %4: Increment of the number of requests executed per unit time from the last measurement to this measurement %5: Number of times the threshold was consecutively exceeded %6: Error Threshold * **error_count = %5$s / %6$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the WebLogic Server to be monitored.
%1: PendingRequest count is too much. appName = %2, name = %3, count = %4, error_count = %5 / %6.	The number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Application name %3: Work manager name %4: Number of waiting requests %5: Number of times the threshold was consecutively exceeded %6: Error Threshold * **error_count = %5$s / %6$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the WebLogic Server to be monitored.

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: PendingRequest increment is too much. appName = %2, name = %3, increment = %6, last.pending = %4, now.pending = %5, error_count = %7 / %8.	The increment of the number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Application name %3: Work manager name %4: Number of waiting requests at last measurement %5: Number of waiting requests at this measurement %6: Increment of the number of waiting requests from the last measurement to this measurement %7: Number of times the threshold was consecutively exceeded %8: Error Threshold * **error_count = %7$s / %8$s** is not shown after the former value exceeds the latter.	Review the Java application that runs on the WebLogic Server to be monitored.
%1: Can't find WorkManager. appName = %2, name = %3.	The work manager which was set could not be acquired from the WebLogic Server. %1: Name of the Java VM to be monitored %2: Application name %3: Work manager name	Review the setting of Target WebLogic Work Managers.
%1: analyze of average start[%2].	Analyzing of the average value has started. %1: Name of the Java VM to be monitored %2: Thread name	-

Continued on next page

Table 11.81 – continued from previous page

Message	Cause of generation	Action
%1: analyze of average finish[%2].state = %3.	Analyzing of the average value has been completed. %1: Name of the Java VM to be monitored %2: Thread name %3: Status of the target to be monitored	-
%1: Average of PendingRequest count is too much. count = %2.	The average of the number of waiting requests has exceeded the threshold in the thread pool of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Number of waiting requests at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.
%1: Average of Throughput count is too high. count = %2.	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: Name of the Java VM to be monitored %2: Number of requests executed per unit time at this measurement	Review the Java application that runs on the WebLogic Server to be monitored.
%1: Average of PendingRequest count is too high. AppName = %2, Name = %3, count = %4.	The average of the number of waiting requests has exceeded the threshold in the work manager of the WebLogic Server to be monitored. %1: Name of the Java VM to be monitored %2: Application name %3: Work manager name %4: 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]	%1: Error code	Review the setting.

11.11 STOP codes list of user mode monitor resources

The following information is a list of the STOP codes which are generated upon the selection of **Generate an intentional stop error** for **Action When Timeout Occurs** of the user mode monitor resource.

STOP code	Description
0xE0000000	The STOP error which was generated as the final action upon the detection of an error of the monitor resource
0xE000FF**	The STOP error which was generated by keep alive timeout (the timeout of user mode monitor) The lower 8 bits (the part of "**") shows the following checkpoint (The chances are high that it was being executed during timeout).
0xE000FF00	The internal processing of EXPRESSCLUSTER
0xE000FF01	SetWaitableTimer(), GetTickCount(), WaitForMultipleObjects()
0xE000FF02	_beginthreadex(),WaitForMultipleObjects()
0xE000FF05	CloseHandle()
0xE000FF06	The internal processing of EXPRESSCLUSTER

11.12 Details on checking cluster configuration data

11.12.1 Cluster Properties

Check item	ID	Message	Action
Ping check on pingnp	1001	Ping could not reach to %1.	Check if an IP address reachable with a ping is set.
Partition presence check for disknp	1021	Failed.	Check if the Get-WmiObject commandlet is available.
	1022	%1 does not exist.	Specify an existing drive letter.
Port No. tab : port number check	1011	Failed.	Check if the netsh command is available.
	1012	The port number %1 is within the range of automatically assigned port numbers.	Specify a port number which is not automatically assigned.

11.12.2 Group Resources

Check item	ID	Message	Action
Ping check on fip	2001	%1 is used already.	Specify an unused IP address in the LAN to which the cluster servers belong.
Ping check on vip	2011	%1 is used already.	Specify an unused IP address in the LAN to which the cluster servers belong.
Partition presence check for sd	2021	Failed.	Check if the Get-WmiObject commandlet is available.
	2022	%1 does not exist.	Specify an existing drive letter.
Partition presence check for md	2031	Failed.	Check if the Get-WmiObject commandlet is available.
	2032	%1 does not exist.	Specify an existing drive letter.
Partition presence check for hd	2041	Failed.	Check if the Get-WmiObject commandlet is available.
	2042	%1 does not exist.	Specify an existing drive letter.
Cluster partition size check for md	2051	Failed.	Check if the Get-WmiObject commandlet is available.
	2052	Failed.	Check if the specified drive letter is for a drive whose disk type is other than a basic disk.
	2053	In %1, the size is less than 1 GB.	Set the disk size to 1 GB or more.
Cluster partition size check for hd	2061	Failed.	Check if the Get-WmiObject commandlet is available.

Continued on next page

Table 11.84 – continued from previous page

Check item	ID	Message	Action
	2062	Failed.	Check if the specified drive letter is for a drive whose disk type is other than a basic disk.
	2063	In %1, the size is less than 1 GB.	Set the disk size to 1 GB or more.
Port number check for azurepp	2071	Failed.	Check if the netsh command is available.
	2072	The port number %1 is within the range of automatically assigned port numbers.	Specify a port number which is not automatically assigned.

11.12.3 Heartbeat Resources

Check item	ID	Message	Action
Ping check on khb	4001	Ping could not reach to %1.	Check if an IP address reachable with a ping is set.

11.12.4 Others

Check item	ID	Message	Action
AWSCLI command execution check	5001	AWSCLI command execution failed.	Check if the AWSCLI execution environment is correctly configured.
OS start time check	5011	OS start time has not been adjusted. Please adjust the OS start time.	Adjust the OS start time. For the procedure, see "Installation and Configuration Guide" - "Adjustment of time for EXPRESSCLUSTER services to start up (Required)".

11.12.5 Unrecommended settings check

Check item	ID	Message	Action
Recovery action check for deactivation failure(%1)	6001	"No operation" is set for Recovery Operation at Deactivation Failure Detection. It is recommended to select any other value.	It is recommended to select a value other than "No operation" for the final action on deactivation failure detection.

CHAPTER

TWELVE

GLOSSARY

Active server server that is running for an application set.

(Related term: Standby server)

Cluster partition A partition on a mirror disk. Used for managing mirror disks.

(Related term: Disk heartbeat partition)

Cluster shutdown To shut down an entire cluster system (all servers that configure a cluster system).

Cluster system Multiple computers are connected via a LAN (or other network) and behave as if it were a single system.

Data partition A local disk that can be used as a shared disk for switchable partition. Data partition for mirror disks.

(Related term: Cluster partition)

Disk heartbeat partition A partition used for heartbeat communication in a shared disk type cluster.

Failback A process of returning an application back to an active server after an application fails over to another server.

Failover The process of a standby server taking over the group of resources that the active server previously was handling due to error detection.

Failover group A group of cluster resources and attributes required to execute an application.

Failover policy A priority list of servers that a group can fail over to.

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.

GC Abbreviation for garbage collection

Heartbeat Signals that servers in a cluster send to each other to detect a failure in a cluster.

(Related terms: Interconnect, Network partition)

Interconnect A dedicated communication path for server-to-server communication in a cluster.

(Related terms: Private LAN, Public LAN)

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 monitoring 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 monitoring. The file is created in the following location:

<EXPRESSCLUSTER_install_path>\log\ha\jra*.stat

Management client Any machine that uses the Cluster WebUI to access and manage a cluster system.

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 a data mirror type cluster. Mirror disk 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.

Moving failover group Moving an application from an active server to a standby server by a user.

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.

Primary (server) A server that is the main server for a failover group.

(Related term: Secondary server)

Private LAN LAN in which only servers configured in a clustered system are connected.

(Related terms: Interconnect, Public LAN)

Public LAN A communication channel between clients and servers.

(Related terms: Interconnect, Private LAN)

Secondary server A destination server where a failover group fails over to during normal operations.

(Related term: Primary server)

Server Group A group of servers connected to the same network or the shared disk device

Shared disk A disk that multiple servers can access.

Shared disk type cluster A cluster system that uses one or more shared disks.

Standby server A server that is not an active server.

(Related term: Active server)

Startup attribute A failover group attribute that determines whether a failover group should be started up automatically or manually when a cluster is started.

Switchable partition A disk partition connected to multiple computers and is switchable among computers.

(Related terms: Disk heartbeat partition)

Virtual IP address IP address used to configure a remote cluster.

CHAPTER

THIRTEEN

LEGAL NOTICE

13.1 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.

13.2 Trademark Information

- EXPRESSCLUSTER® is a registered trademark of NEC Corporation.
- FastSync™ is a trademark of NEC Corporation.
- Microsoft, Windows, Windows Server, Internet Explorer, Azure, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- 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.
- VMware, vCenter Server, and vSphere is registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- Python is a registered trademark of the Python Software Foundation.
- SVF is a registered trademark of WingArc Technologies, Inc.
- 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.
- PowerGres is a registered trademark of SRA OSS, Inc.
- 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 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

FOURTEEN

REVISION HISTORY

Edition	Revised Date	Description
1st	Apr 15, 2024	New manual
2nd	Apr 26, 2024	Corrected typographical errors.