EXPRESSCLUSTER® X SingleServerSafe 3.3 *for Linux*

Configuration Guide

10/02/2017
6th Edition

Revision History

Edition	Revised Date	Description
1st	02/09/2015	New manual
2nd	06/30/2015	Corresponds to the internal version 3.3.1-1.
3rd	01/29/2016	Corresponds to the internal version 3.3.2-1.
4th	10/03/2016	Corresponds to the internal version 3.3.3-1.
5th	04/10/2017	Corresponds to the internal version 3.3.4-1.
6th	10/02/2017	Corresponds to the internal version 3.3.5-1.

Disclaimer

Information in this document is subject to change without notice.
NEC Corporation is not liable for technical or editorial errors or omissions in the information in this document.
You are completely liable for all risks associated with installing or using the product as described in this manual to obtain expected results and the effects of such usage.
The information in this document is copyrighted by NEC Corporation.
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.

Trademark Information

EXPRESSCLUSTER® is a registered trademark of NEC Corporation.
FastSync® is a registered trademark of NEC Corporation.
Linux is a registered trademark and trademark of Linus Torvalds in the United State and other countries.
RPM is a trademark of Red Hat, Inc.
Intel, Pentium, and Xeon are registered trademarks or trademarks of Intel Corporation.
Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
Turbolinux is a registered trademark of Turbolinux. Inc.
VERITAS, VERITAS Logo, and all other VERITAS product names and slogans are trademarks and registered trademarks of VERITAS Software Corporation.
Oracle, Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and other countries.
Novell is a registered trademark of Novell, Inc. in the United States and Japan.
SUSE is a registered trademark of SUSE LINUX AG, a group company of U.S. Novell.
Citrix, Citrix XenServer, and Citrix Essentials are registered trademarks or trademarks of Citrix Systems, Inc. in the United State and other countries.
WebOTX is a registered trademark of NEC Corporation.
JBoss is a registered trademark of Red Hat, Inc. in the United States and its subsidiaries.
Apache Tomcat, Tomcat, and Apache are registered trademarks or trademarks of Apache Software Foundation.
Android is a trademark or registered trademark of Google, Inc.
Other product names and slogans written in this manual are trademarks or registered trademarks of their respective companies.

Table of Contents

Preface

Who Should Use This Guide

The *Configuration Guide* is intended for system engineers who intend to introduce a system and system administrators who will operate and maintain the introduced system. It describes how to set up EXPRESSCLUSTER X SingleServerSafe. The guide consists of five sections: I to V.

How This Guide Is Organized

Section I Overview of EXPRESSCLUSTER X SingleServerSafe

Chapter 1 "EXPRESSCLUSTER X SingleServerSafe": Provides a product overview of EXPRESSCLUSTER X SingleServerSafe.

Section II Configuration of EXPRESSCLUSTER X SingleServerSafe

Chapter 2 "Creating configuration data": Describes how to start the WebManager and the procedures to create the configuration data by using the Builder with a sample configuration.
Chapter 3 "Checking the cluster system" : Verify if the system that you have configured operates successfully.

Section III Resource details

Chapter 4 "Group resource details": Provides details on group resources, which are used as a unit for controlling an application by using EXPRESSCLUSTER X SingleServerSafe.
Chapter 5 "Monitor resource details": Provides details on monitor resources, which are used as a unit when EXPRESSCLUSTER X SingleServerSafe executes monitoring.
Chapter 6 "Heartbeat resources": Provides details on the heartbeat resource.
Chapter 7 Chapter 7 "Details of other settings: Provides details on other settings of EXPRESSCLUSTER X SingleServerSafe.

Section IV How monitoring works

Chapter 8 Chapter 8 "Monitoring details": Provides details on how several types of errors are detected.

Section V Release Notes

Chapter 9 Chapter 9 "Notes and restrictions": Describes known problems and how to prevent them.

Appendix

Appendix A "Index"

Terms Used in This Guide

EXPRESSCLUSTER X SingleServerSafe, which is described in this guide, uses windows and commands common to those of the clustering software EXPRESSCLUSTER X to ensure high compatibility with EXPRESSCLUSTER X in terms of operation and other aspects. Therefore, cluster-related terms are used in parts of the guide.
The terms used in this guide are defined below.

Term	Explanation
Cluster, cluster system	A single server system using EXPRESSCLUSTER X SingleServerSafe
Cluster shutdown, reboot	Shutdown or reboot of a system using EXPRESSCLUSTER X SingleServerSafe
Cluster resource	A resource used in EXPRESSCLUSTER X SingleServerSafe
Cluster object	A resource object used in EXPRESSCLUSTER X SingleServerSafe
Failover group	A group of group resources (such as applications and services) used in EXPRESSCLUSTER X SingleServerSafe

EXPRESSCLUSTER X SingleServerSafe Documentation Set

The EXPRESSCLUSTER X SingleServerSafe documentation consists of the five guides below. The title and purpose of each guide is described below:

EXPRESSCLUSTER X SingleServerSafe Installation Guide
This guide is intended for system engineers who intend to introduce a system using EXPRESSCLUSTER X SingleServerSafe and describes how to install EXPRESSCLUSTER X SingleServerSafe.

EXPRESSCLUSTER X SingleServerSafe Configuration Guide
This guide is intended for system engineers who intend to introduce a system using EXPRESSCLUSTER X SingleServerSafe and system administrators who will operate and maintain the introduced system. It describes how to set up EXPRESSCLUSTER X SingleServerSafe.

EXPRESSCLUSTER X SingleServerSafe Operation Guide
This guide is intended for system administrators who will operate and maintain an introduced system that uses EXPRESSCLUSTER X SingleServerSafe. It describes how to operate EXPRESSCLUSTER X SingleServerSafe.

EXPRESSCLUSTER X Integrated WebManager Administrator's Guide
This guide is intended for system administrators who manage a cluster system using EXPRESSCLUSTER with EXPRESSCLUSTER Integrated WebManager and for system engineers who are introducing the Integrated WebManager. Details about items required when introducing a cluster system are described in accordance with actual procedures.

EXPRESSCLUSTER X WebManager Mobile Administrator's Guide
This guide is intended for system administrators who manage cluster systems using EXPRESSCLUSTER with EXPRESSCLUSTER WebManager Mobile and for system engineers who are installing the WebManager Mobile. In this guide, details on those items required for installing the cluster system using the WebManager Mobile are explained in accordance with the actual procedures.

Conventions

In this guide, **Note**, **Important**, and **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.

Related Information:
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]`
#	Prompt to indicate that a Linux user has logged in as root user.	`# clpcl -s -a`
Monospace `(courier)`	Indicates path names, commands, system output (message, prompt, etc), directory, file names, functions and parameters.	`/Linux/3.3/en/server/`
Monospace bold `(courier)`	Indicates the value that a user actually enters from a command line.	Enter the following: **`clpcl -s -a`**
Monospace italic `(courier)`	Indicates that users should replace italicized part with values that they are actually working with.	`rpm -i expressclssss-<version_number>-<release_number>.i686.rpm`

Contacting NEC

For the latest product information, visit our website below:

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

Section I Overview of EXPRESSCLUSTER X SingleServerSafe

This section provides a product overview of EXPRESSCLUSTER X SingleServerSafe and outlines its monitoring function.

Chapter 1 EXPRESSCLUSTER X SingleServerSafe

Chapter 1 EXPRESSCLUSTER X SingleServerSafe

This chapter outlines the functions of EXPRESSCLUSTER X SingleServerSafe and describes the types of errors that can be monitored.

This chapter covers:

EXPRESSCLUSTER X SingleServerSafe

EXPRESSCLUSTER X SingleServerSafe is set up on a server. It monitors for application errors and hardware failures on the server and, upon detecting an error or failure, automatically restarts the failed application or reboots the server so as to ensure greater server availability.

With an ordinary server, if an application has ended abnormally, you need to restart it when you realize that it has ended abnormally.

There are also cases in which an application is not running stably but has not ended abnormally. Usually, such an error condition is not easy to identify.

For a hardware error, rebooting the server might achieve recovery if the error is temporary. However, hardware errors are difficult to notice. The abnormal behavior of an application often turns out to be due to a hardware error when the application is checked.

With EXPRESSCLUSTER X SingleServerSafe, specify the applications and hardware components to be monitored for automatic error detection. Upon detecting an error, EXPRESSCLUSTER X SingleServerSafe automatically restarts the application or server that caused the error to recover from the error.

Note:
As indicated above, in many cases, a physical hardware failure cannot be recovered from just by rebooting the server. To protect against physical hardware failure, consider implementing hardware redundancy or introducing clustering software.

How an error is detected in EXPRESSCLUSTER X SingleServerSafe

EXPRESSCLUSTER X SingleServerSafe performs several different types of monitoring to ensure quick and reliable error detection. The details of the monitoring functions are described below.

- Monitoring activation status of applications

An error can be detected by starting up an application by using an application-starting resource (called application resource and service resource) of EXPRESSCLUSTER and regularly checking whether the process is active or not by using application-monitoring resource (called application monitor resource and service monitor resource). It is effective when the factor for application to stop is due to error termination of an application.

Note 1:
If an application started directly by EXPRESSCLUSTER X SingleServerSafe starts and then ends a resident process to be monitored, EXPRESSCLUSTER X SingleServerSafe cannot detect an error in that resident process.
Note 2:
An internal application error (for example, application stalling and result error) cannot be detected.

- Monitoring applications and/or protocols to see if they are stalled or failed by using the monitoring option.

You can monitor for the stalling and failure of applications including specific databases (such as Oracle, DB2), protocols (such as FTP, HTTP), and application servers (such as WebSphere, WebLogic) by introducing optional monitoring products of EXPRESSCLUSTER X SingleServerSafe. For details, see Chapter 5, "Monitor resource details."

- Resource monitoring

An error can be detected by monitoring the resources (applications, services, etc.) and LAN status by using the monitor resources of EXPRESSCLUSTER X SingleServerSafe. It is effective when the factor for application to stop is due to an error of a resource that is necessary for an application to operate.

Errors that can and cannot be monitored for

For EXPRESSCLUSTER X SingleServerSafe, some errors can be monitored for, and others cannot. It is important to know what can or cannot be monitored when building and operating a cluster system.

Errors that can be detected and those that cannot through application monitoring

Monitoring conditions: Termination of application with errors, continuous resource errors, disconnection of a path to the network devices.

◆ Example of errors that can be monitored:

- Abnormal termination of an application
- LAN NIC problem

◆ Example of errors that cannot be monitored:

- Application stalling and resulting in error.

  EXPRESSCLUSTER X SingleServerSafe cannot directly monitor for application stalling or resulting errors. However, it is possible to make EXPRESSCLUSTER X restart by creating an application monitoring program to make EXPRESSCLUSTER X terminate if an error is detected, running the program by using the EXEC resource, and monitoring by using a PID monitor resourc

Section II Configuration of EXPRESSCLUSTER X SingleServerSafe

This section describes how to set up EXPRESSCLUSTER X SingleServerSafe. As configuration examples, it deals with the typical cases of configuration related to application control and IP monitoring.

Chapter 2 Creating configuration data
Chapter 3 Checking the cluster system

Chapter 2 Creating configuration data

In EXPRESSCLUSTER X SingleServerSafe, data describing how a system is set up is called configuration data. Generally, configuration data is created using the Builder, which is started in the WebManager. This chapter describes how to start the WebManager and the procedure for creating configuration data by using the Builder with a sample cluster configuration.

This chapter covers:

Checking the values to be specified

Before creating configuration data by using the Builder (the config mode of the WebManager), check the values you are going to specify as the configuration data. Write down the values to make sure there is no missing information.

Sample environment

Sample configuration data values are shown below. The following sections describe step-by-step procedures for creating configuration data based on these conditions. When actually specifying the values, you might need to modify them according to the cluster you intend to create. For details about how to decide on the values, see Chapter 4, "Group resource details " and Chapter 5, "Monitor resource details."

Sample values of configuration data

Target	Parameter	Value
Server information	Server Name	server1
	Monitor Resource Count	3
Group	Type	Failover
	Group Name	failover1
	Startup Server	server1
First group resource	Type	EXEC resource
	Group Resource Name	exec1
	Resident Type	Resident
	Start Path	Path of execution file
First monitor resource (created by default)	Type	User mode monitor (User Space Monitor)
	Monitor Resource Name	userw1
Second monitor resources	Type	IP monitor
	Monitor Resource Name	ipw1
	Monitor IP Address	192.168.0.254 (gateway)
	Recovery Target	LocalServer
	Reactivation Threshold	-
	Final Action	Stop service and reboot OS
Third monitor resources	Type	PID monitor
	Monitor Resource Name	Pidw1
	Target Resource	Exec1
	Recovery Target	failover1
	Reactivation Threshold	3
	Final Action	Stop service and reboot OS

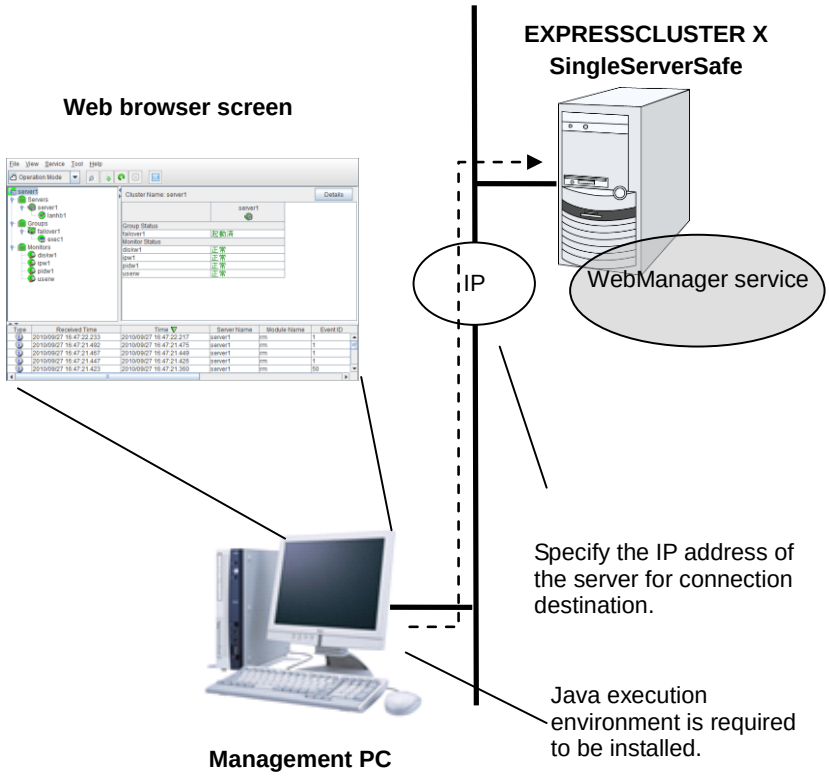
Note:
”User Space Monitor” is automatically specified for the first monitor resource.

Starting up the WebManager

Accessing the WebManager is necessary to create configuration data. This section provides an overview of the WebManager and how to access the WebManager and create configuration data.

What is the WebManager?

The WebManager is a function for switching to the Builder (the config mode of the WebManager), monitoring the server status, starting and stopping servers and groups, and collecting operation logs through a Web browser. The overview of the WebManager is shown in the following figures.



The WebManager service on the EXPRESSCLUSTER X SingleServerSafe Server is set up to start up when the operating system starts up.

Setting up Java runtime environment to a management PC

To access the WebManager, a Java Plug-in (Java™ Runtime Environment Version 6.0 Update 21(1.6.0_21) or later, Java™ Runtime Environment Version 7.0 Update 2 (1.7.0_2) or later, or Java™ Runtime Environment Version 8.0 Update 5(1.8.0_5) or later) must be installed in a browser on a management PC.

When the version of Java Plug-in is older than the version written above, the browser might prompt you to install Java. In this case, install the Java Plug-in of the version of which the operation is verified on EXPRESSCLUSTER WebManager.

To install Java Plug-in on a browser, refer to the browser's help and the JavaVM installation guide.

Starting up the WebManager

The procedure for starting the WebManager is described below.

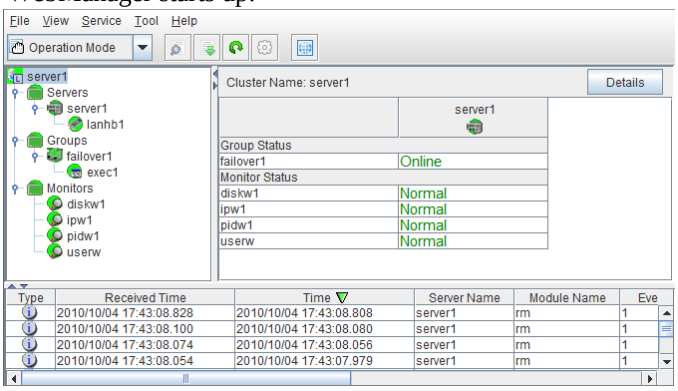
1. Start your Web browser.
Enter the IP address and port number of the server where EXPRESSCLUSTER X SingleServerSafe is installed in the browser address bar.

http://192.168.0.3:29003/

The port number for the WebManager specified at installation. (Default value 29003).

The IP address of the server where the EXPRESSCLUSTER X SingleServerSafe is installed. If the local server is used, localhost can be specified.

2. WebManager starts up.



3. Click Config mode on the **View** menu to switch to the config mode (Builder (online version)).

Creating the configuration data

Creating configuration data involves three steps: setting up the server, creating groups, and creating monitor resources. Use the cluster creation wizard to create new configuration data. The procedure is described below.

Note:
Most of the created configuration data can be modified later by using the rename function or property viewing function.

1 Setting up the server

Set up the server on which to run EXPRESSCLUSTER X SingleServerSafe.

1-1 Setting up the server

Specify the server name to be configured.

2 Setting up groups

Set up groups. Starting and stopping an application is controlled by a group. Create as many groups as necessary. Generally, you need as many groups as the number of applications you want to control. However, when you use script resources, you can combine more than one application into a single group.

2-1 Adding a group

Add a group.

2-2 Adding a group resource

Add a resource that can start and stop an application.

3 Setting up monitor resources

Add a monitor resource that monitors the specified target.
Create a monitor resource for each monitoring target.

3-1 Adding a monitor resource

Add a monitor resource that performs monitoring.

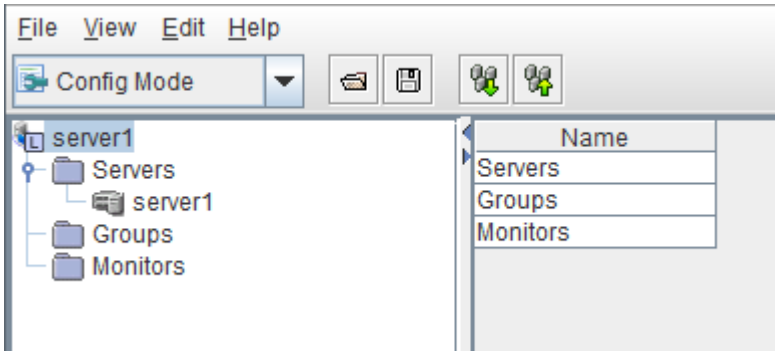
1. Setting up the server

Set up the server.

1-1 Setting up the server

The server settings are automatically created when you reboot the OS after installing EXPRESSCLUSTER X SingleServerSafe. When you switch from the WebManager's operation mode window to the config mode (the online version of the Builder) window, you will see the created data.

The table view is as follows:



2. Setting up groups

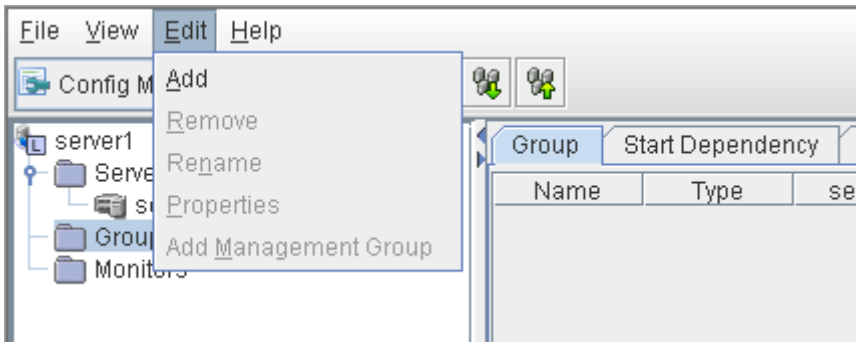
A group is a set of services and processes necessary to perform an independent operation in the system.

The procedure for adding a group is described below.

2-1 Adding a group

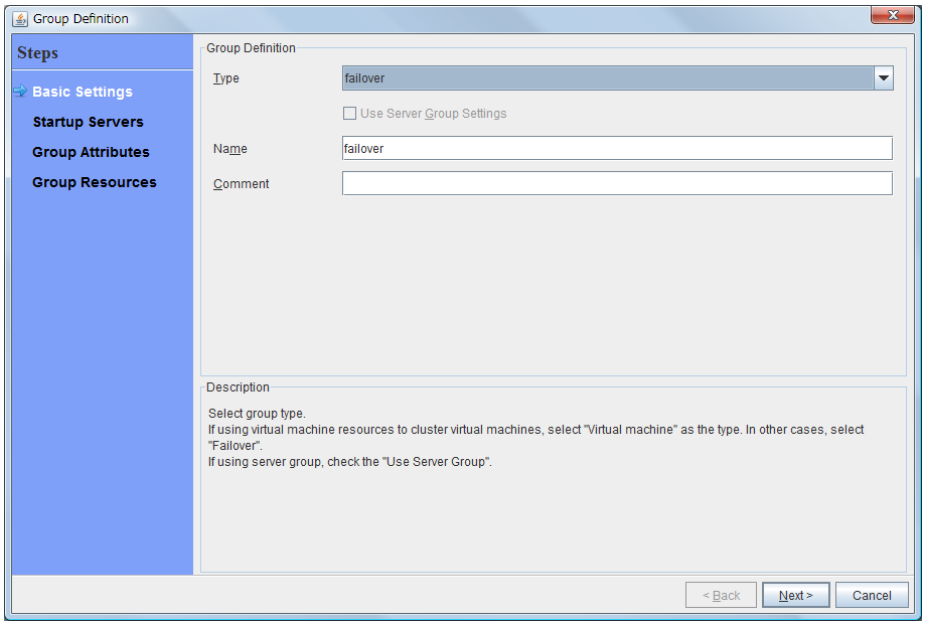
Set up a group.

1. Click **Groups** in the tree view, and click **Add** on the **Edit** menu.

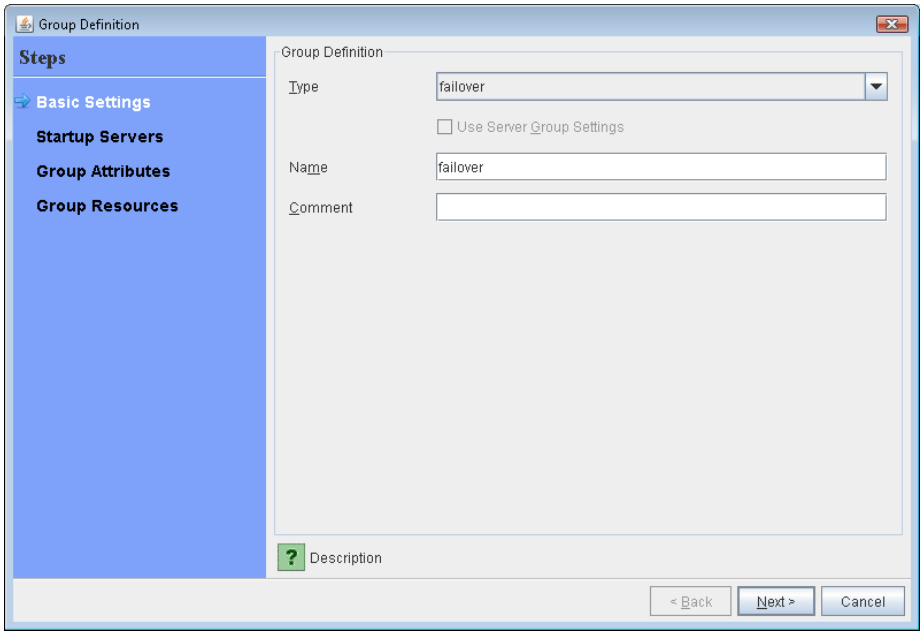


2. The **Group Definition** dialog box is displayed.
   Choose one of the types below.
   Type:
   - Failover
     In general, specify this.
   - Virtual machine
     When using a virtual machine resource, specify this.

3. Enter the group name (failover1) in the **Name** box, and click **Next**.

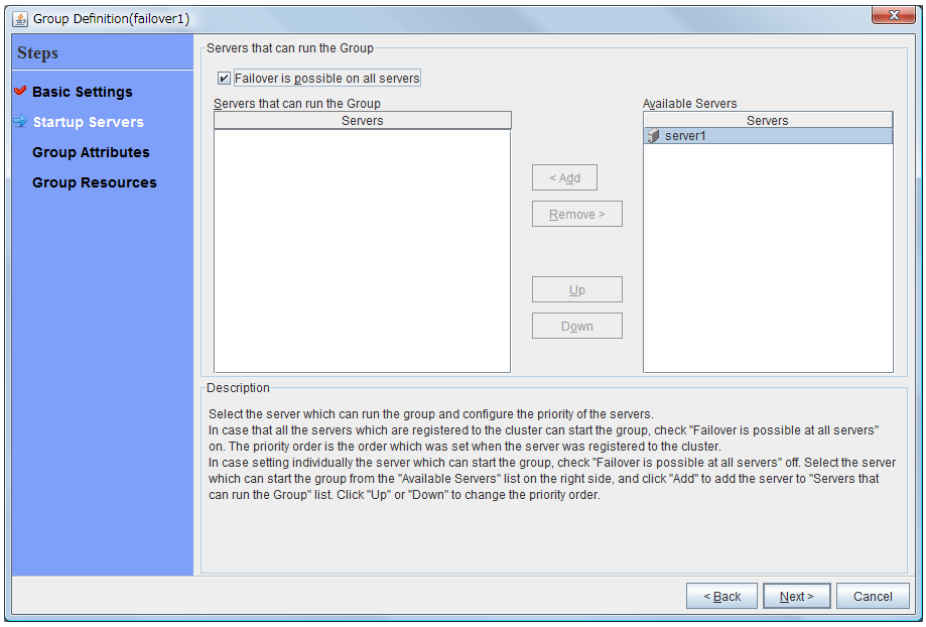


If the screen resolution is 800 x 600 pixels or less, the **Description** field will be displayed as a tool tip.

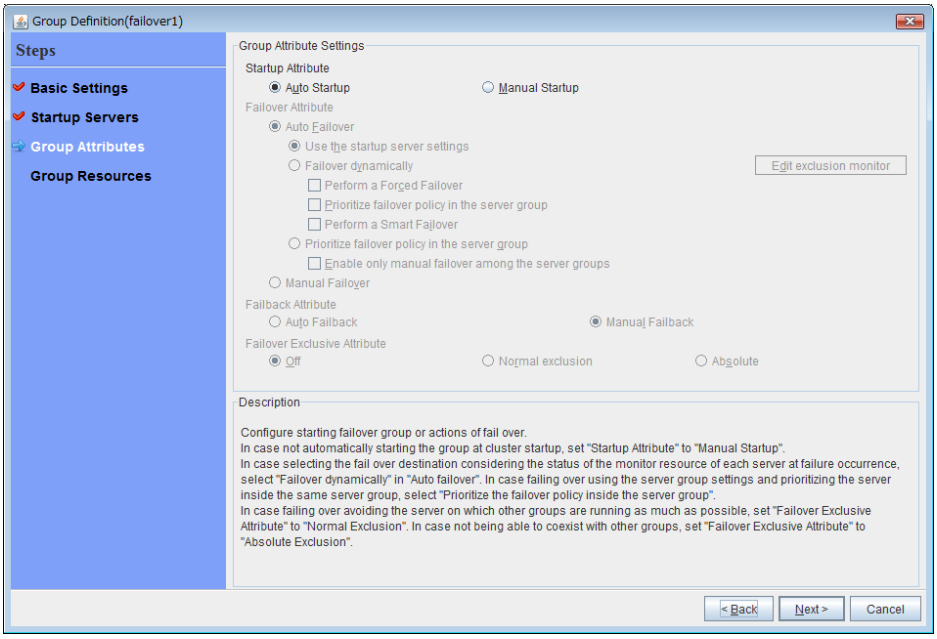


Positioning the mouse cursor to the **?** icon displays a tool tip with the full description.

4. Make sure that the **Failover is possible on all servers** check box is selected, and then click **Next**.

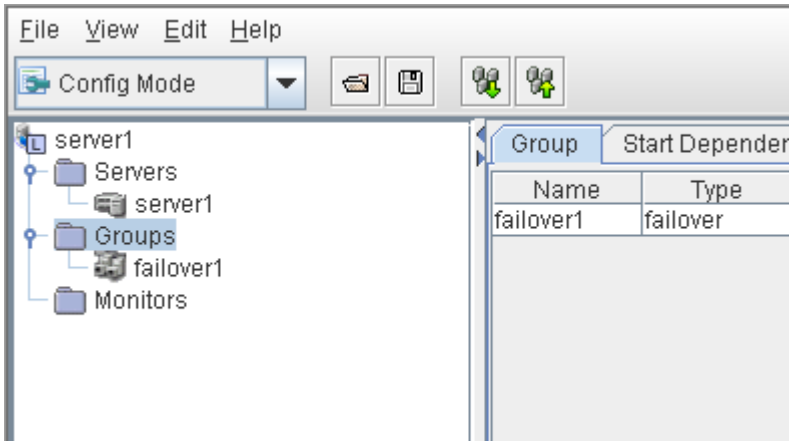


5. This dialog box is used to specify the values of the group attributes. Click **Next** without specifying anything.



6. The **Group Resource Definitions** is displayed. Click **Finish** without specifying anything.

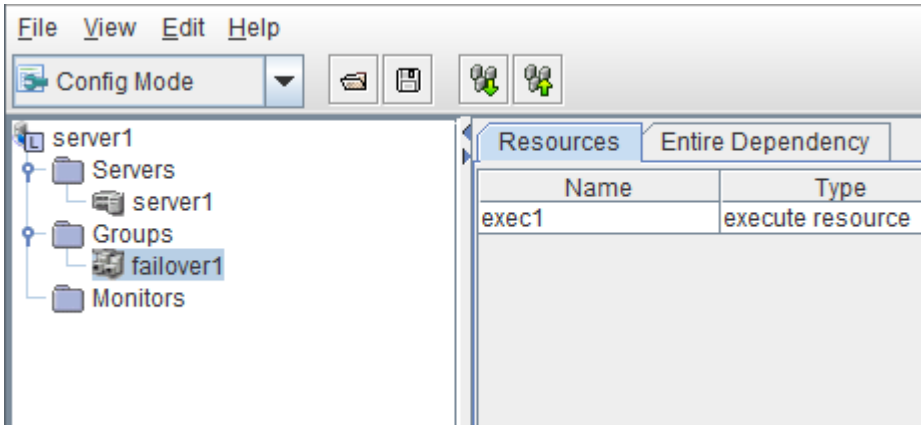
The table view is as follows:



2-2 Adding a group resource (EXEC resource)

Add EXEC resource to start or stop the application by script.

1. Click failover1 in the tree view, and then click **Add** in the **Edit** menu.
2. The **Resource Definition** dialog box is displayed.
   Select the group resource type execute resource in the **Type** box, and then enter the group resource name exec1 in the **Name** box. Click **Next**.
3. A page for setting up a dependency is displayed. Click **Next**.
4. A page for setting up a recovery operation is displayed. Click **Next**.
5. Select **User Application**. Specify the path of the execution file for **Start Path**.
6. Click **Tuning** to open the dialog box. Next, click **Asynchronous** for **Start Script**, and then click **OK**.
7. Click **Finish**.
   The table view is as follows:

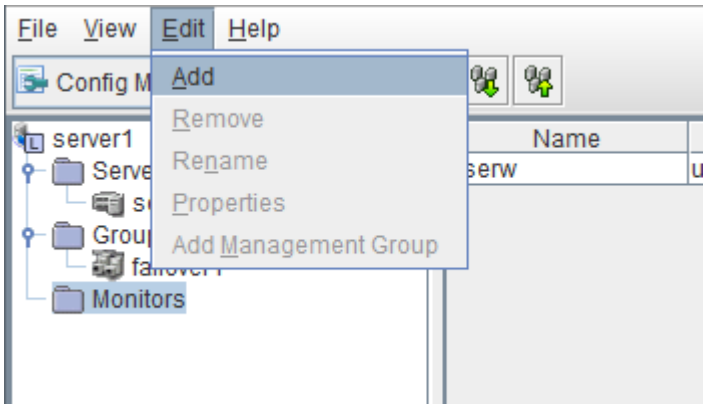


3. Setting up monitor resources

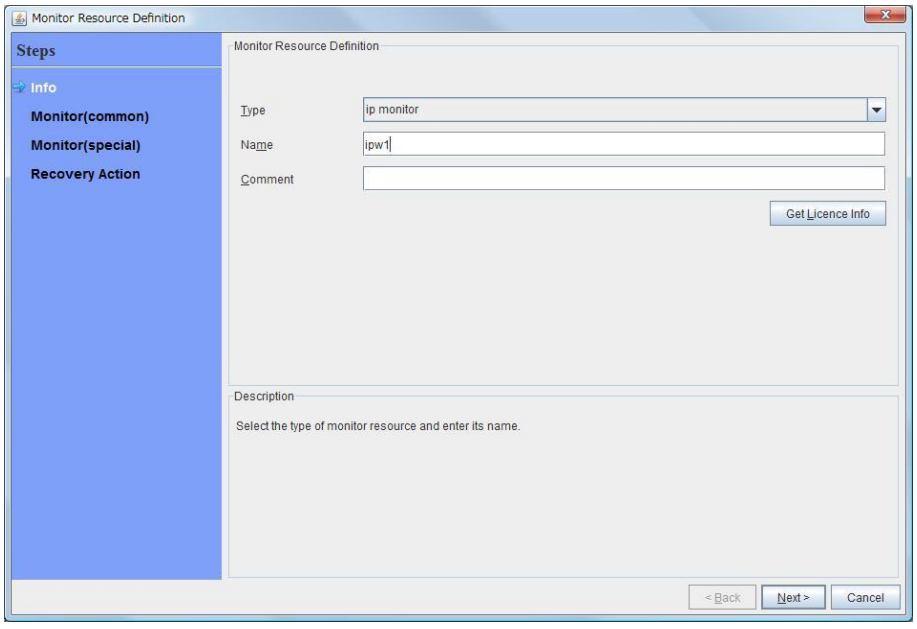
Add a monitor resource that monitors the specified target.

3-1 Adding a monitor resource (IP monitor resource)

1. Click the **Monitors object** in the tree view, and then click **Add** in the **Edit** menu. The **Monitor Resource Definition**s is displayed.

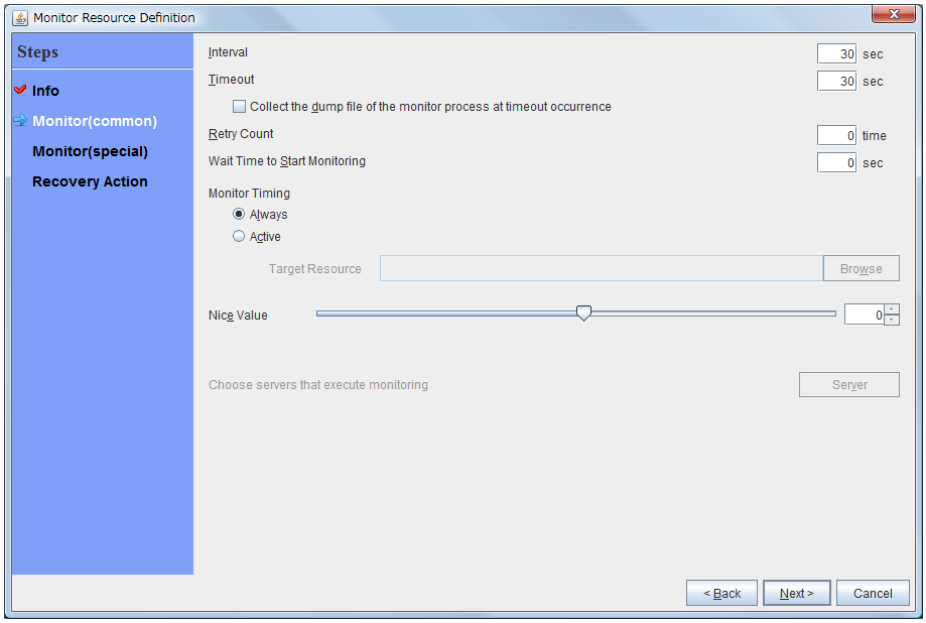


2. Select the monitor resource type **ip monitor** in the **Type** box, and enter the monitor resource name **ipw1** in the **Name** box. Click **Next**.

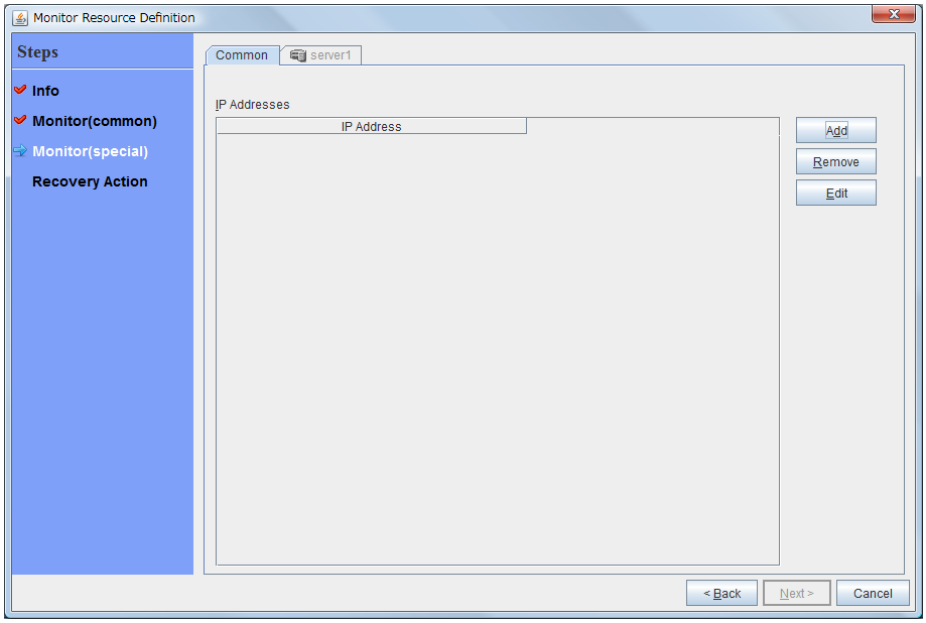


Note:
Monitor resources are displayed in **Type**. Select the resource you want to monitor.
If the licenses for optional products have not been installed, the resources and monitor resources corresponding to those licenses are not shown in the list on the Builder (online version).

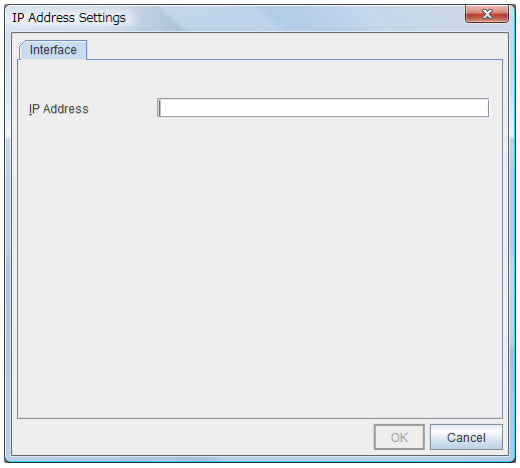
3. Enter the monitoring settings. Click **Next** without changing the default value.



4. The **IP Addresses** is displayed. Click **Add**.

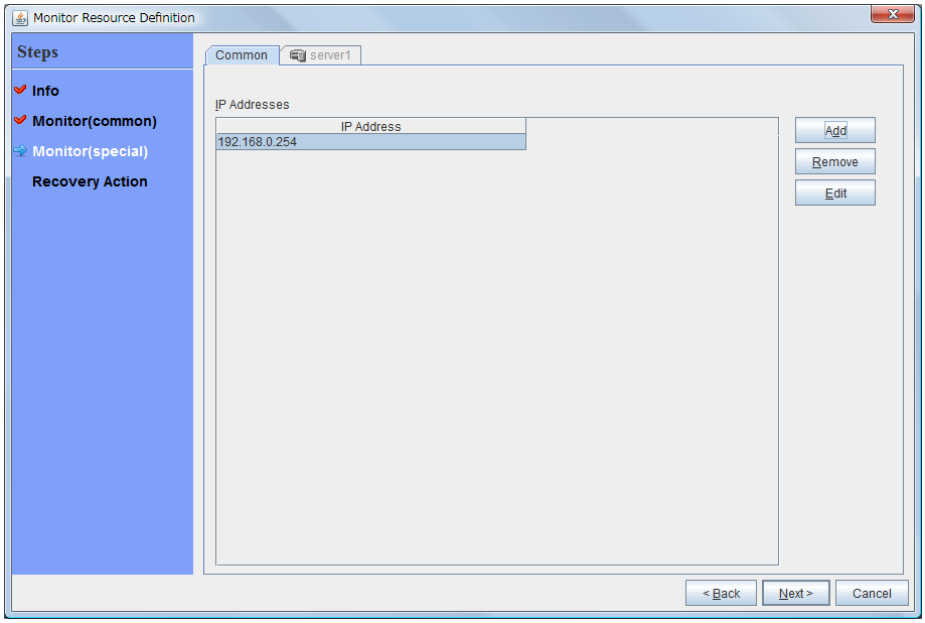


5. Enter the IP address to be monitored 192.168.0.254 in the **IP Address** box, and then click **OK**.

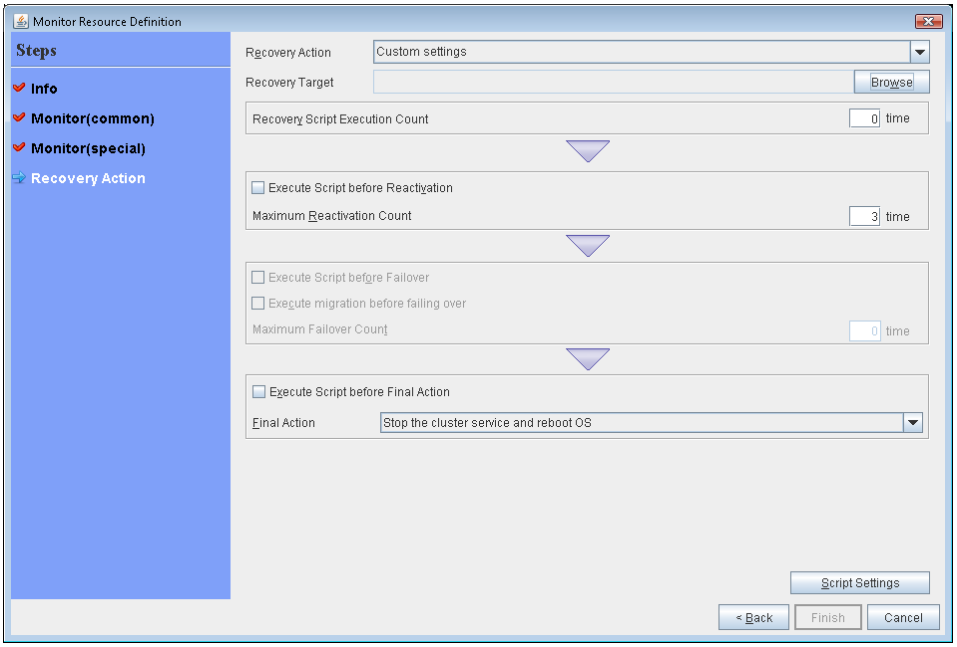


Note:
For the monitoring target of the IP monitor resource, specify the IP address of a device (such as a gateway) that is assumed to always be active on the LAN.

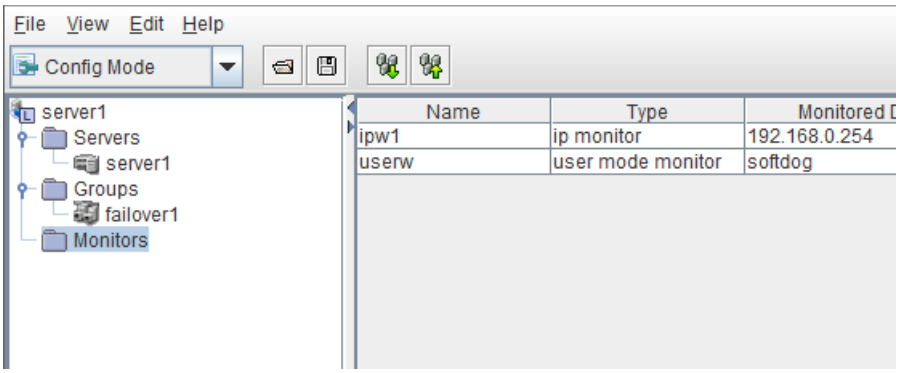
6. The entered IP address is set in the **IP Addresses**. Click **Next**.



7. Set **Recovery Target**. Select **LocalServer** on the tree view being displayed, and click **OK**. **LocalServer** is set to **Recovery Target**.Click **Browse**. click **Finish** without changing the default values.



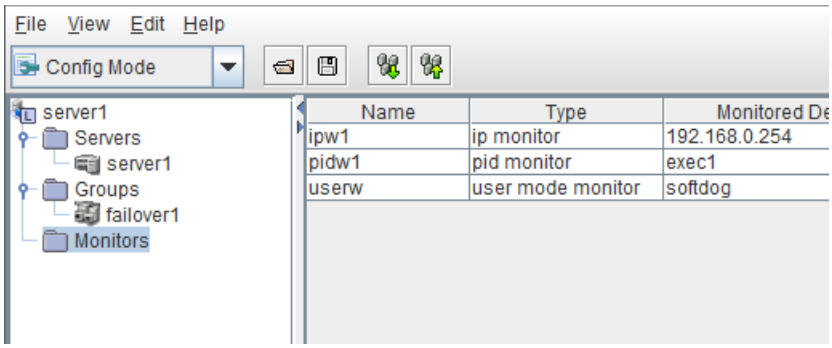
After the settings are specified, the window appears as follows.



3-2 Adding a monitor resource (PID monitor resource)

1. A monitor resource can be set up when the EXEC resource activation script type is set to **Asynchronous**.
2. Click the **Monitors object** in the tree view, and then click **Add** in the **Edit** menu. Select the monitor resource type **pid monitor** in the **Type** box, and then enter the monitor resource name pidw1 in the **Name** box. Click **Next**.
3. Enter the monitoring settings. Click **Browse**.
4. Click **exec1** in the displayed tree view, and then click **OK**. Exec1 is specified for **Target Resource**. Click **Next**.
5. Set the recovery target. Click **Browse**.
6. Click **failover1** in the displayed tree view. Click **OK**. failover1 is set in the **Recovery Target**.
7. Click **Finish**.

The table view will look similar to the following.



This concludes creating the configuration data. Proceed to the next section, “Saving configuration data.”

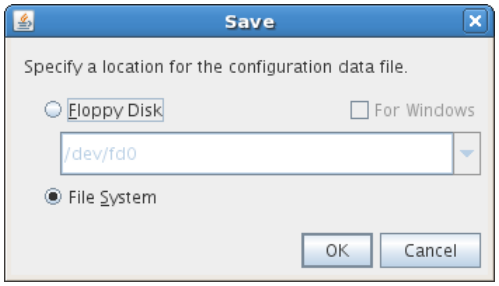
Saving configuration data

The configuration data can be saved to a file system or to media such as a floppy disk. When the Builder has been activated through the WebManager, you can apply the saved configuration data to the servers for which the EXPRESSCLUSTER Server has been installed from the WebManager.

Saving the configuration data to the file system (Linux)

Perform the procedure below to save the configuration data to the file system when using a Linux machine.

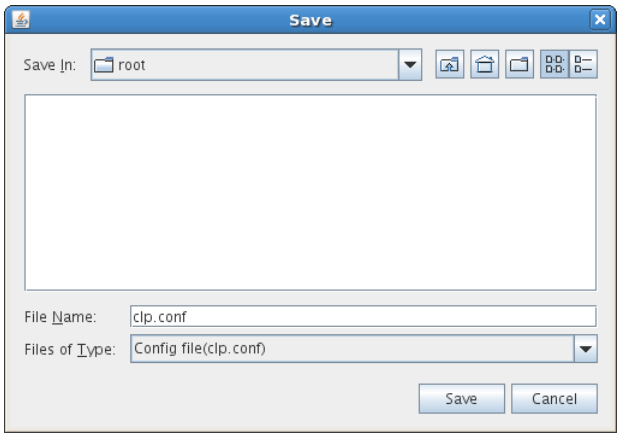
1. Select **Export** on the **File** menu of the Builder.
2. Click **File System** in the following dialog box, and click **OK**.



3. The following dialog box is displayed. Select a location to save the data in the following dialog box, and click **Save**.

Note:

- One file (clp.conf) and one directory (scripts) are saved. If any of these are missing, the command does not run successfully. Make sure to treat these two as a set when moving the files. When new configuration data is edited, clp.conf.bak is created in addition to these two.
- The file and directory can be seen only when For Windows or File System is selected.

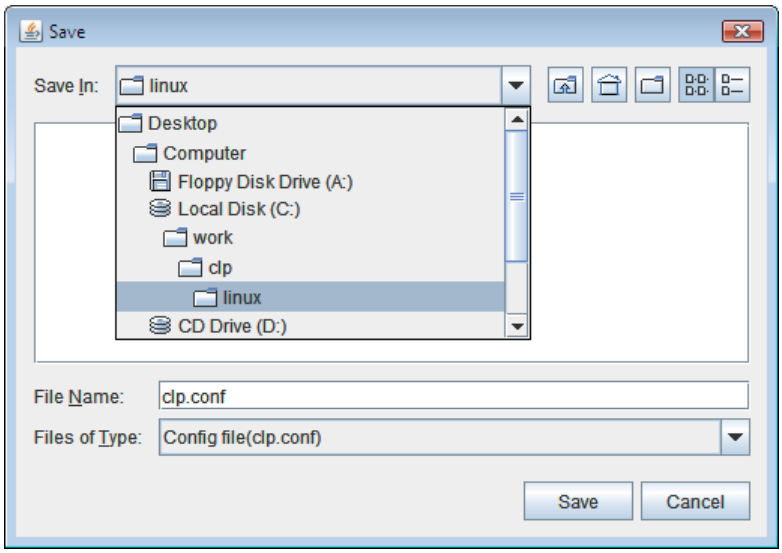


4. Check the file system and verify if the file (clp.conf) and the directory (scripts) are located in a directory to be saved.

Saving the configuration data to the file system (Windows)

Perform the procedure below to save the configuration data to the file system when using a Windows machine.

1. Select **Export** on the **File** menu of the Builder.
2. Select a location to save the data in the following dialog box, and click **Save**.



3. Select a location to save the data in the following dialog box, and click **Save**.

Note:
One file (clp.conf) and one directory (scripts) are saved. If any of these are missing, the attempt to apply the configuration data will fail. Make sure to treat these two as a set. When new configuration data is edited, clp.conf.bak is created in addition to these two.

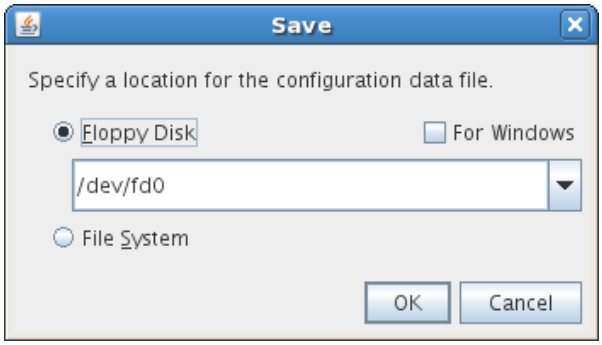
4. Check the file system and verify if the file (clp.conf) and the directory (scripts) are located in a directory to be saved.

Saving the configuration data to a floppy disk (Linux)

Perform the procedure below to save the configuration data created using the Builder on a Linux machine to a floppy disk.

1. Insert a floppy disk into the floppy disk drive. Click **Export** on the **File** menu.

2. The following dialog box is displayed. Select the floppy disk drive name and click **OK**. Click **Save** on the **File** menu. Generally, the data is saved directly under the FD without creating a directory inside the FD.



Note:

To make the configuration data editable with the Builder that runs in a Windows browser as well, select For Windows. In this case, you need to prepare a Windows FAT (VFAT) formatted 1.44-MB floppy disk.

One file (clp.conf) and one directory (scripts) are saved. If any of these are missing, the command does not run successfully. Make sure to treat these two as a set when moving the files. When new configuration data is edited, clp.conf.bak is created in addition to these two.

3. Check the floppy disk and verify if the file (clp.conf) and the directory (scripts) are saved directly to the floppy disk.

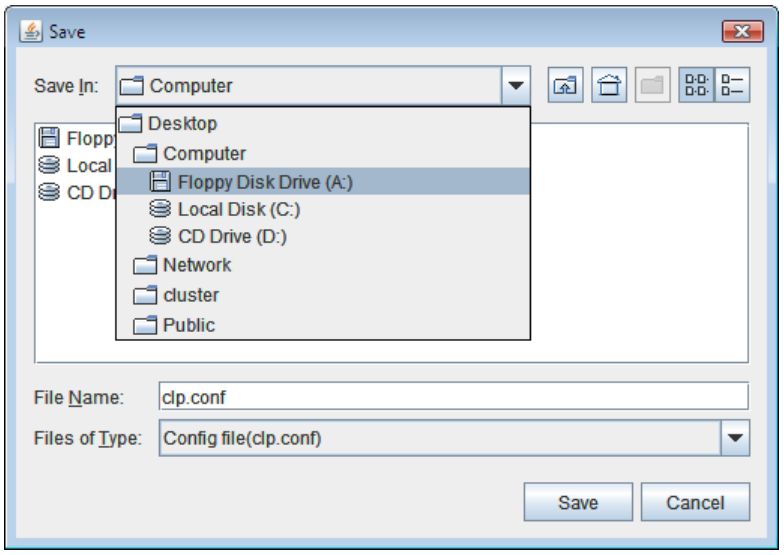
Saving the configuration data to a floppy disk (Windows)

Perform the procedure below to save the configuration data created using the Builder on a Windows machine to a floppy disk.

1. Prepare a formatted 1.44-MB floppy disk.

2. Insert the floppy disk into the floppy disk drive. Select the floppy disk drive in the **Save** box and click **Save**. Click **Export** on the **File** menu. Generally, the data is saved directly under the FD without creating a directory inside the FD.

3. The following dialog box is displayed. Select the FD drive in the **Save** dialog box, and then click **Save**.



Note:

- To make the configuration data editable with the Builder that runs in a Windows browser as well, select For Windows. In this case, you need to prepare a Windows FAT (VFAT) formatted 1.44-MB floppy disk. For details, refer to the Operation Guide.
- One file (clp.conf) and one directory (scripts) are saved. If any of these are missing, the command does not run successfully. Make sure to treat these two as a set when moving the files. When new configuration data is edited, clp.conf.bak is created in addition to these two.

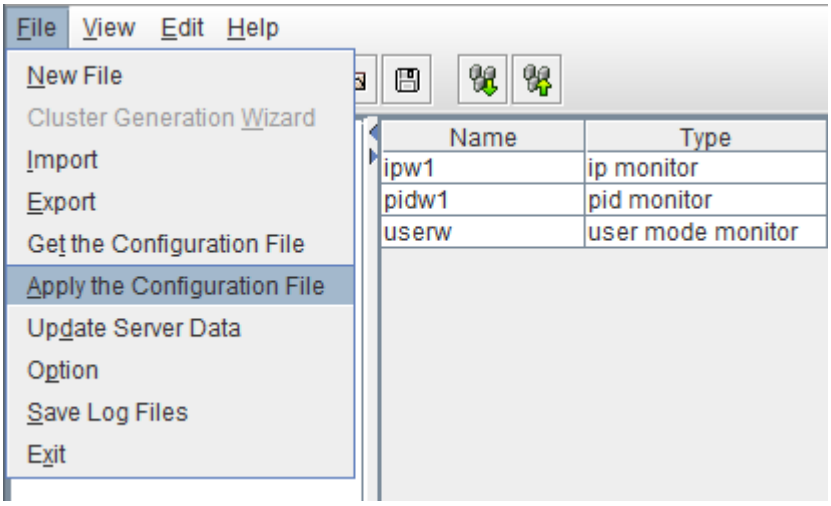
4. Check the floppy disk and verify if the file (clp.conf) and the directory (scripts) are saved directly to the floppy disk.

Applying configuration data

After creating configuration data by using the Builder (the WebManager config mode), apply the configuration data to the server.

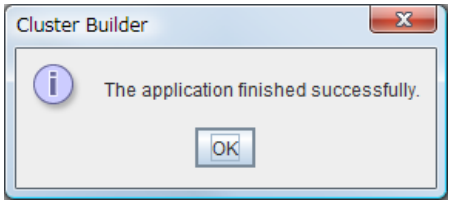
To apply the configuration data, follow the procedure below.

1. Click **Apply the Configuration File** on the **File** menu in the WebManager config mode (the online version of the Builder) window.



2. Depending on the difference between the existing configuration data and the configuration data you are applying, a pop-up window might be displayed to prompt you to check the operation necessary to apply the data.
If there is no problem with the operation, click **OK**.

3. If the application succeeds, the following dialog box is displayed:



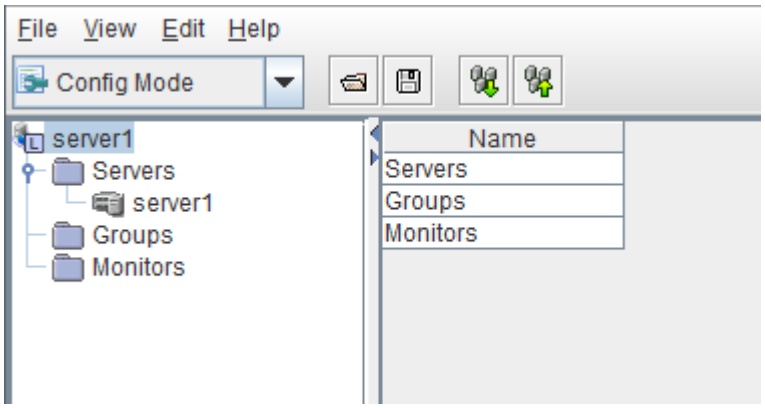
Note:
If the application fails, perform the operations by following the displayed message.

Differences regarding the use of the offline version of the Builder

When using the offline version of the Builder, you need to use different procedures for creating configuration data initially and having the data applied.

1. Setting up the server

1. On the **File** menu, click **Cluster Generation Wizard**. The **Cluster Generation Wizard** is displayed. In the **Language** field, select a language that is used on the machine that the WebManager works. Click **Next**.
2. Enter the server name **server1** in the **Name** box. Click **Next**.
The table view is as follows:



2. Applying the configuration data

1. Activate the EXPRESSCLUSTER Builder by using a Web browser.
(The path for installation) /clptrek.htm
2. Open the saved configuration data.
3. The configuration data is displayed. Modify it.
4. Save the modified configuration data.
5. Apply the saved configuration data at the command prompt to a server EXPRESSCLUSTER Server is installed on.
clpcfctrl –push -w –x <path on which the configuration data is saved>
At this time, some servers might have to be suspended or stopped, or restarted upon server shutdown depending on the modified configuration. In such a case, applying is cancelled once and the required operation is displayed. Follow the displayed message and do as instructed to perform apply again.

Chapter 3 Checking the cluster system

This chapter describes how you verify that the created system runs normally.

This chapter covers:

Checking the operation by using the WebManager

The WebManager or command line can be used to check the set up system operation. This section describes how to check the system operation by using the WebManager. The WebManager is installed at the time of the EXPRESSCLUSTER Server installation. Therefore, it is not necessary to install it separately. This section first provides a summary of the WebManager, and then describes how to access the WebManager and check the server status.

Related Information:
For details about the WebManager system requirements, refer to Chapter 1, "Checking the EXPRESSCLUSTER X SingleServerSafe system requirements (software)" in the *Installation Guide*.

Follow the steps below to check the operation after creation and connecting to the WebManager.

Related Information:
For details about how to use the WebManager, refer to Chapter 1, "Functions of the WebManager" in the *Operation Guide*.

1. Check heartbeat resources

Make sure that the status of the server is online in the WebManager.
Make sure that the heartbeat resource status of the server is normal.

2. Check monitor resources

Verify that the status of each monitor resource is normal on the WebManager.

3. Start a group

Starts a group.
Verify that the status of the group is online on the WebManager.

4. EXEC resource

Verify that an application is working on the server where the group having an EXEC resource is active.

5. Stop Group

Stops a group.
Verify that the status of the group is offline on the WebManager.

6. Start a group

Starts a group.
Verify on the WebManager that the group has been started.

7. Shut down the servers

Shuts down the server. Make sure that all the servers successfully shut down.

Checking the server operation by using commands

After creation, perform the following procedure to check the system status by using commands from a server.

Related Information:
For details about how to use commands, refer to Chapter 2, "EXPRESSCLUSTER X SingleServerSafe command reference" in the *Operation Guide*.

1. Check monitor resources

Verify that the status of each monitor resource is normal by using the clpstat command.

2. Start a group

Start a group by using the clpgrp command.
Verify that the status of the group is online by using the clpstat command.

3. EXEC resource

Verify that an application is working on the server where the group having an EXEC resource is active.

4. Stop Group

Stop a group by using the clpgrp command.
Verify that the status of the group is offline by using the clpstat command.

5. Start a group

Start a group by using the clpgrp command.
Verify that the status of the group is online by using the clpstat command.

6. Shut down

Shut down the server by using the clpstdn command. Make sure that the server successfully shut down.

Section III Resource details

This section provides details about resources. EXPRESSCLUSTER X SingleServerSafe uses windows common to those of the clustering software EXPRESSCLUSTER X to ensure high compatibility with EXPRESSCLUSTER X in terms of operation and other aspects. Because the information contained herein is specific to EXPRESSCLUSTER X SingleServerSafe, see the *Reference Guide* for EXPRESSCLUSTER X to obtain an overall understanding of the settings.

Chapter 4 Group resource details

This chapter provides details about group resources.

This chapter covers:

Group resources

The following resources can be defined as group resources.

Group resource name	Function	Abbreviation
EXEC resource	Register applications and shell scripts executed upon activation or deactivation of the group.	exec
VM resource	Starts and stops a virtual machine.	vm

System requirements for VM resources

The versions of the virtualization platform that support VM resources are listed below.

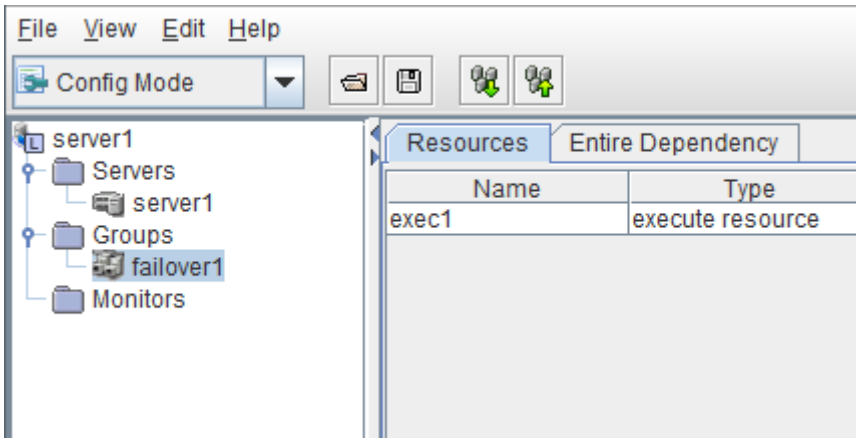
Virtual Machine	Version	EXPRESSCLUSTER version	Remarks
vSphere	4.0 update1	3.0.0-1 or later	x86_64
	4.0 update2	3.0.0-1 or later	x86_64
	4.1	3.0.0-1 or later	x86_64
	5	3.1.0-1 or later	VM
	5.1	3.1.0-1 or later	VM
	5.5	3.2.0-1 or later	VM
XenServer	5.5	3.0.0-1 or later	IA32
	5.6	3.0.0-1 or later	IA32
KVM	Redhat Enterprise Linux 5.5	3.0.0-1 or later	x86_64
	Redhat Enterprise Linux 5.6	3.0.0-1 or later	x86_64
	Redhat Enterprise Linux 5.7	3.2.0-1 or later	x86_64
	Redhat Enterprise Linux 5.8	3.2.0-1 or later	x86_64
	Redhat Enterprise Linux 5.9	3.2.0-1 or later	x86_64
	Redhat Enterprise Linux 6.0	3.1.0-1 or later	x86_64
	Redhat Enterprise Linux 6.1	3.1.0-1 or later	x86_64
	Redhat Enterprise Linux 6.2	3.2.0-1 or later	x86_64
	Redhat Enterprise Linux 6.3	3.2.0-1 or later	x86_64
	Redhat Enterprise Linux 6.4	3.2.0-1 or later	x86_64
	Redhat Enterprise Linux 6.5	3.2.0-1 or later	x86_64

Setting up an EXEC resource

EXPRESSCLUSTER allows registration of applications and shell scripts that are managed by EXPRESSCLUSTER and executed upon activation or deactivation of the group. You can also possible to register your own programs and shell scripts in EXEC resources. You can write codes as required for respective application because shell scripts are in the same format as sh shell script.

1. Click **failover1** in the tree view, and then click **Add** on the **Edit** menu.
2. The **Resource Definition** dialog box is opened. Select the group resource type execute resource in the **Type** box, and then enter the group resource name exec1 in the **Name** box. Click **Next**.
3. A page for setting up a dependency is displayed. Click **Next**.
4. A page for setting up a recovery operation is displayed. Click **Next**.
5. Select **User Application**. Specify the path of the execution file for **Start Path**. Click **Finish** .

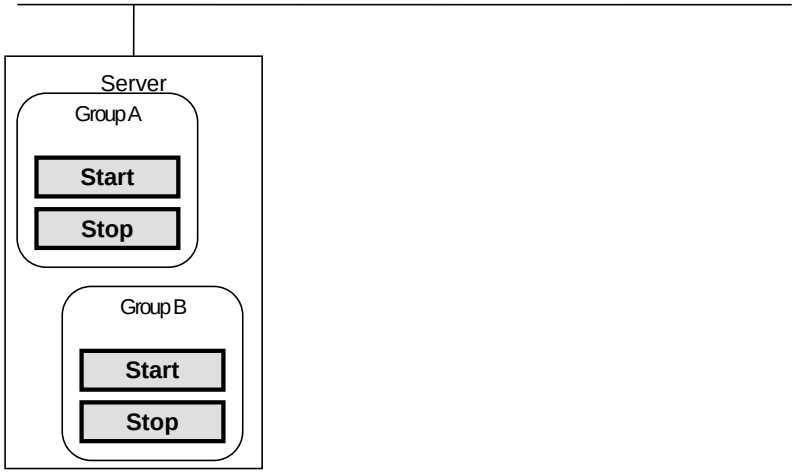
The table view is as follows:



Scripts used for the EXEC resource

Types of scripts

Start script and stop script are provided in EXEC resources. EXPRESSCLUSTER runs a script for each EXEC resource when the server needs to change its status. Activation, deactivation, and restoration procedures must be written in the scripts.



Start: Start script
Stop: Stop script

Environment variables used in EXEC resource scripts

When EXPRESSCLUSTER runs a script, it records information such as condition when the script was 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 and CLP_PID.

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	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	Not used.
CLP_FACTOR …group stopping factor	CLUSTERSHUTDOWN	The group was stopped by stopping the server.
	SERVERSHUTDOWN	The group was stopped by stopping the server.
	GROUPSTOP	The group was stopped by stopping the group.
	GROUPMOVE	Not used.
	GROUPFAILOVER	Not used.
	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 …processing after stopping	REBOOT	In case of rebooting OS.
	HALT	In case of halting OS.
	NONE	No action was taken.
CLP_SERVER	HOME	Not used.
	OTHER	Not used.
CLP_DISK	SUCCESS	Not used.
	FAILURE	Not used.
CLP_PRIORITY	1 to the number of servers in the cluster	Not used.

Environment variable	Value of environment variable	Meaning
CLP_GROUPNAME …Group name	Group name	Represents the name of the group to which the script belongs.
CLP_RESOURCENAME …Resource name	Resource Name:	Represents the name of the resource to which the script belongs.
CLP_PID …Process ID	Process ID	Represents the process ID of the start script when the properties of the start script are set to asynchronous. This environment variable is null when the start script is set to synchronous.
CLP_VERSION_FULL …EXPRESSCLUSTER full version	EXPRESSCLUSTER X SnigleServerSafe full version	Represents the EXPRESSCLUSTER X SingleServerSafe full version. (Example) 3.3.0-1
CLP_VERSION_MAJOR …EXPRESSCLUSTER major version	EXPRESSCLUSTER X SingleServerSafe major version	Represents the EXPRESSCLUSTER X SingleServerSafe major version. (Example) 3
CLP_PATH …EXPRESSCLUSTER install path	EXPRESSCLUSTER X SingleServerSafe install path	Represents the path where EXPRESSCLUSTER X SingleServerSafe is installed. (Example) `/opt/nec/clusterpro`
CLP_OSNAME …Server OS name	Server OS name	Represents the OS name of the server where the script was executed. (Example) 1) When the OS name could be acquired: Red Hat Enterprise Linux Server release 6.0 (Santiago) 2) When the OS name could not be acquired: Linux
CLP_OSVER …Server OS version	Server OS version	Represents the OS version of the server where the script was executed. (Example) 1) When the OS version could be acquired: 6.0 2) When the OS version could not be acquired: *Blank

Execution timing of EXEC resource scripts

The timings at which the start script and stop script are executed and how the environment variables are associated with the execution are described below with diagrams of status transitions.

◆ O and × in the diagrams represent the server status.

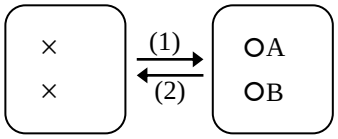
Server	Server status
O	Normal
×	Stopped

(Example) OA: Group A is working on a normally running server.

◆ Group A and Group B are defined.

Status transitions

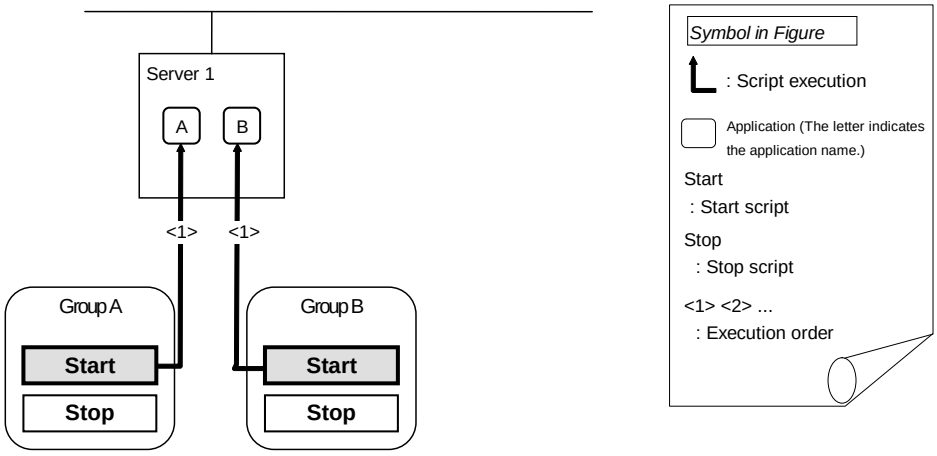
This diagram shows possible status transitions.



Numbers (1) and (2) in the diagram correspond to descriptions as follows.

(1) Normal startup

The normal startup in this context indicates when the start script is normally executed on the server.

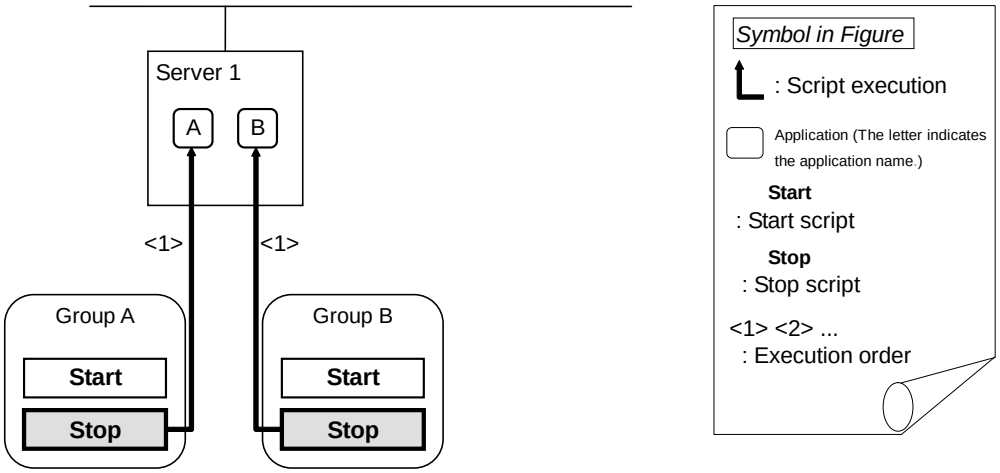


Environment variable for Start

group	Environment variable	Value
A	CLP_EVENT	START
B	CLP_EVENT	START

(2) Normal shutdown

The normal shutdown in this context indicates the shutdown immediately after the start script corresponding to the stop script is executed for normal startup.



Environment variable for Stop

group	Environment variable	Value
A	CLP_EVENT	START
B	CLP_EVENT	START

Writing EXEC resource 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 EXEC resource scripts" on page 61.

Group A start script: A sample of start.sh

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

if [ "$CLP_EVENT" = "START" ]
then
```

The environment variable for script execution is referenced to distribute processing.

Processing overview:
Application's normal startup processing
When to start the processing:
(1) Upon normal startup

```
else
        #NO_CLP

fi
#EXIT

exit 0
```

EXPRESSCLUSTER is not running.

Group A stop script: A sample of stop.sh

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

if [ "$CLP_EVENT" = "START" ]
then

        Process overview:
                Application's normal stop processing
        When to execute the processing:
                (2) Upon normal shutdown

else
        #NO_CLP

fi
#EXIT
exit 0
```

The environment variable for script execution is referenced to distribute processing.

EXPRESSCLUSTER is not running.

Tips for creating EXEC resource scripts

Note the following points when creating EXEC resource script.

- If your script has a command that requires some time to complete, it is recommended to configure command completion messages to be always produced. This message can be used to determine the error when a problem occurs. There are two ways to produce the message:
- Specify the EXEC resource log output path by writing the `echo` command in the script.

  Trace results can be output to the standard output by using the `echo` command. Specify the log output path in the resource properties that contain the script.

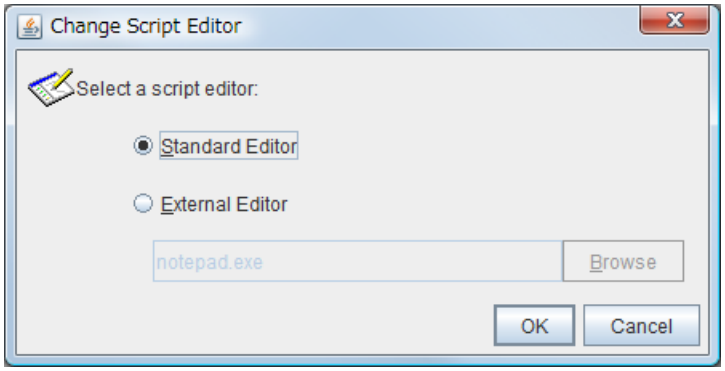
  The message is not logged by default. For the log output path setting, see "Tuning an EXEC resource" on page 74. If the **Rotate Log** check box is not selected, pay attention to the available disk space of a file system because messages are sent to the file specified as the log output destination file regardless of the size of available disk space.

  (Example: Sample script)
  ```
  echo "appstart.."
  appstart
  echo "OK"
  ```
- Writing `clplogcmd` in the script
  `clplogcmd` outputs messages to the alert view of the WebManager or OS syslog. For details about the `clplogcmd` command, refer to "Message output command" in Chapter 2, "EXPRESSCLUSTER SingleServerSafe command reference" in the *Operation Guide*.

  (Example: Sample script)
  ```
  clplogcmd -m "appstart.."
  appstart
  clplogcmd -m "OK"
  ```

Change

Click here to display the **Change Script Editor** dialog box. You can change editor for displaying or editing a script to an arbitrary editor.



Standard Editor

Select this option to use the standard editor for editing scripts.

- Linux: vi (vi which is detected by the user's search path)
- Windows: Notepad (notepad.exe which is detected by the user's search path)

External Editor

Select here to specify an arbitrary script editor. Click Browse to specify the editor to be used

To specify a CUI-based external editor on Linux, create a shell script.

The following is a sample shell script to run vi:

```
xterm -name clpedit -title "Cluster Builder" -n "Cluster Builder" -e
vi "$1"
```

Tuning

Opens the EXEC resource tuning properties dialog box. You can make advanced settings for the EXEC resource. If you want the PID monitor resource to monitor the EXEC resources, you have to set the start script to asynchronous.

Notes on EXEC resources

- About the rotate log function of the script

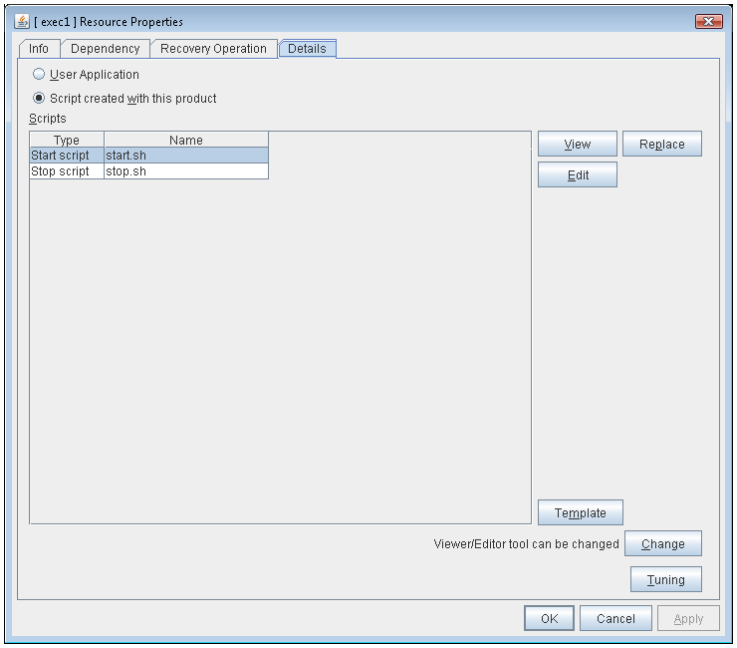
  If the rotate log function of the script is enabled, it's written in a specified file when the script finishes. If the start script is set to **Asynchronous**, the script does not finish and the logs are not written. Therefore, it is recommended that you disable Script Log Rotate. If the start script is set to **Synchronous**, redirect the standard output of the resident process started in the start script to /dev/null.

  If a start script is set to Asynchronous, it is recommend that you disable the rotate log function.

- The start script and the stop script are executed by root user.
- To start an application dependent on an environment variable, the script must set the environment variable as needed.

Displaying and changing EXEC resource details

1. From the tree view displayed on the left pane of the Builder, click the icon of the group to which the EXEC resource whose detail information you want to display and change belongs.
2. The list of group resources is displayed on the table view in the right pane of the screen. Right-click the EXEC resource name. Then click **Properties** and select the **Details** tab.
3. Display and/or change the settings by following the description below.



User Application

Select this option to use executable files (executable shell scripts and binary files) on your server as scripts. Specify the local disk path on the server for each executable file name.

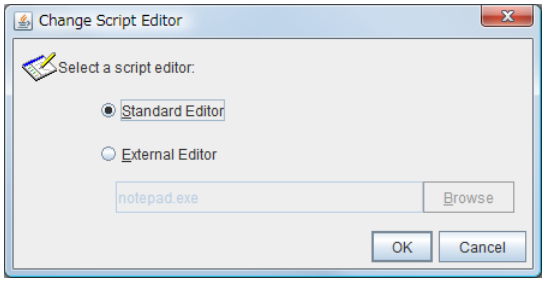
The configuration data created by the Builder does not contain these files. You cannot edit the script files using the Builder.

Script created with this product

Use a script file which is prepared by the Builder as a script. You can edit the script file with the Builder if you need. The script file is included in the configuration data.

Change

Click here to display the **Change Script Editor** dialog box. You can change editor for displaying or editing a script to an arbitrary editor.



Standard Editor

Select this option to use the standard editor for editing scripts.

- Linux: vi (vi which is detected by the user's search path)
- Windows: Notepad (notepad.exe which is detected by the user's search path)

External Editor

Select here to specify an arbitrary script editor. Click **Browse** to specify the editor to be used.

To specify a CUI-based external editor on Linux, create a shell script.

The following is a sample shell script to run vi:

```
xterm -name clpedit -title "Cluster Builder" -n "Cluster Builder" -e
vi "$1"
```

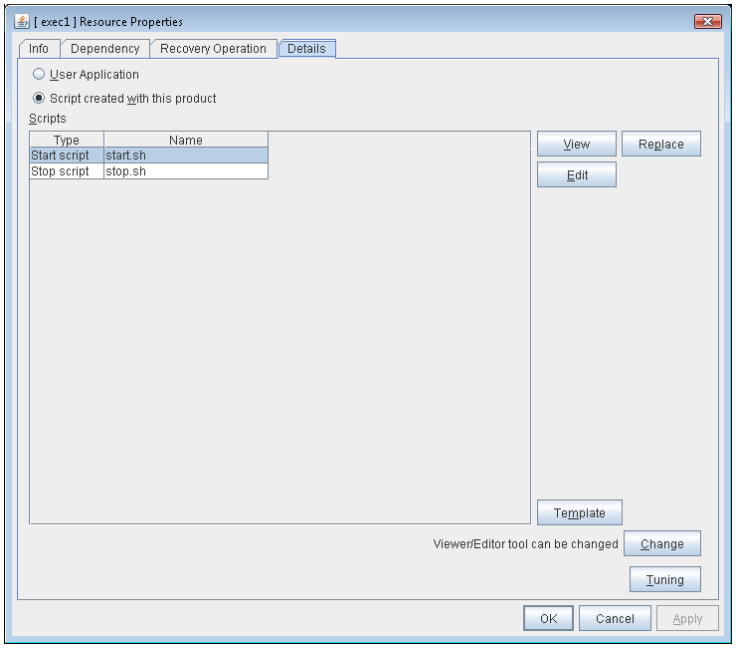
Tuning

Opens the EXEC resource tuning properties dialog box. You can make advanced settings for the EXEC resource. If you want the PID monitor resource to monitor the EXEC resources, you have to set the start script to asynchronous.

Displaying and changing EXEC resource scripts created by the Builder

1. From the tree view displayed on the left pane of the Builder, click the icon of the group to which the EXEC resource whose detail information you want to display and change belongs.
2. The list of group resources is displayed on the table view in the right pane of the screen. Right-click the EXEC resource name. Then click **Properties** and select the **Details** tab.
3. Click **Script Created by the Builder** in the **Details** tab.
4. The settings of multi target monitor resource can be displayed and changed by following the description below.

   The default script file names, start.sh and stop.sh, are listed on **Scripts**.



View

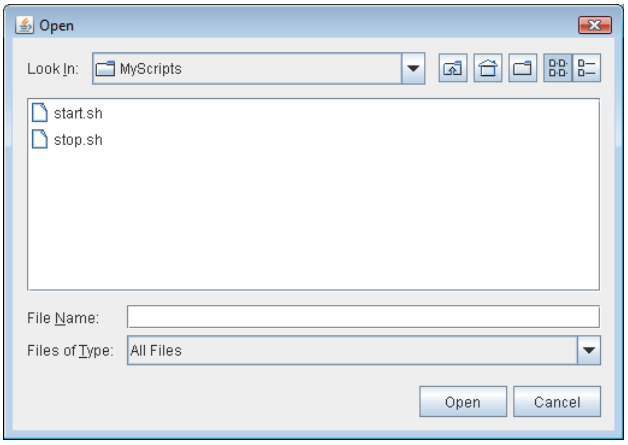
Use this button to display the selected script file on the script editor. The information edited and stored with the editor is not applied. You cannot display the script file if it is currently displayed or edited.

Edit

Use this button to edit the selected script file on the script editor. Overwrite the script file to apply the change. If the selected script file is being viewed or edited, you cannot edit it. You cannot modify the name of the script file.

Replace

Opens the **Open** dialog box, where you can select a file.



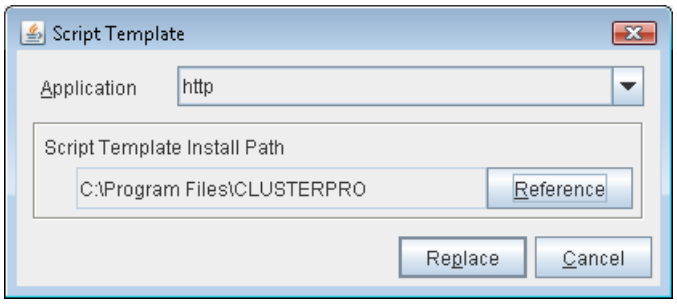
The content of the script file selected in the **Resource Property** is replaced with the one selected in the **Open** dialog box. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not select binary files (applications), and so on.

Using the simple selection function of a script template

Selecting an application from the EXEC resource enables you to automatically replace the necessary script template. You can simply create a script by editing the template script.

Note: To use this function, you must install the script template in advance. For how to obtain the script template.

1. From the tree view displayed in the left pane of the Builder, click the icon of the group containing the EXEC resource for which you want to replace the script template.
2. A group resource list is displayed in the table view to the right of the window. Right-click the target EXEC resource name and then click the **Details** tab of **Properties**.
3. On the **Details** tab, click **Script created with this product.**
4. Click **Template**.
5. The **Script Template** dialog box is displayed.



Application

Clicking **Application** displays the replaceable script template applications in a list box.

Note:
If the script template is not installed, nothing is displayed in the application list.

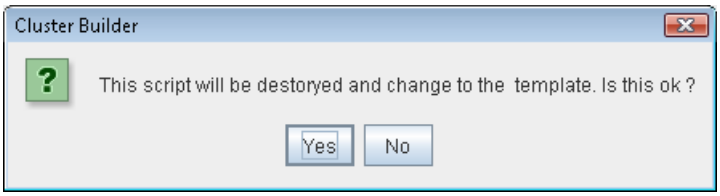
Browse

Clicking **Browse** browses to the folder path where the script template is installed.

Note:
If the script template is not installed in the default folder path, a warning message appears. If the script template is installed, specify the correct install path.

Replace

Clicking **Replace** displays the script replacement confirmation dialog box.



Clicking **OK** replaces the script.

Note:

You must edit the replaced script to suit your environment. For how to edit the script, see “Displaying and changing EXEC resource scripts created by the Builder”.

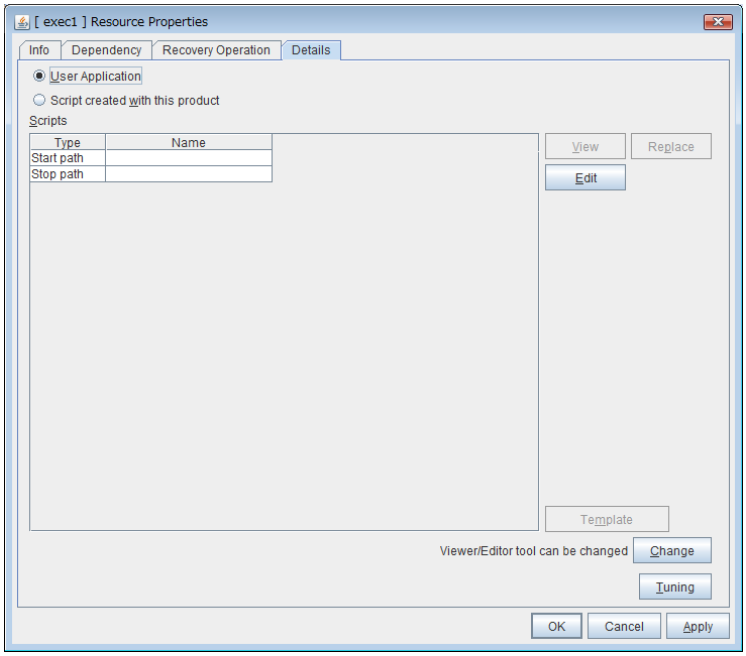
Displaying and changing EXEC resource scripts using a user-created application

1. From the tree view displayed on the left pane of the Builder, click the icon of the group to which the EXEC resource whose detail information you want to display and change belongs.
2. The list of group resources is displayed on the table view in the right pane of the screen. Right-click the EXEC resource name. Then click **Properties** and select the **Details** tab.
3. Click **User Application** on the **Details** tab.
4. The settings of multi target monitor resource can be displayed and changed by following the description below.

   Select any file as the EXEC resource executable file. Specified executable file names are listed on **Scripts**.

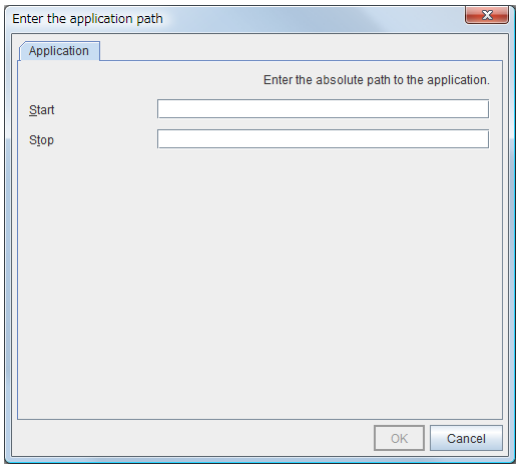
   Executable files mean executable shell scripts and binary files.

   The standard script editor specified for the Linux Builder is vi. To close the view/edit window, use the q command of vi.



Edit

Specify an EXEC resource executable file name. The **Enter the application path** dialog box is displayed.



Start (within 1,023 bytes)

Enter an executable file name to be run when the EXEC resource starts. This must start with "/." Arguments can be specified.

Stop (within 1,023 bytes)

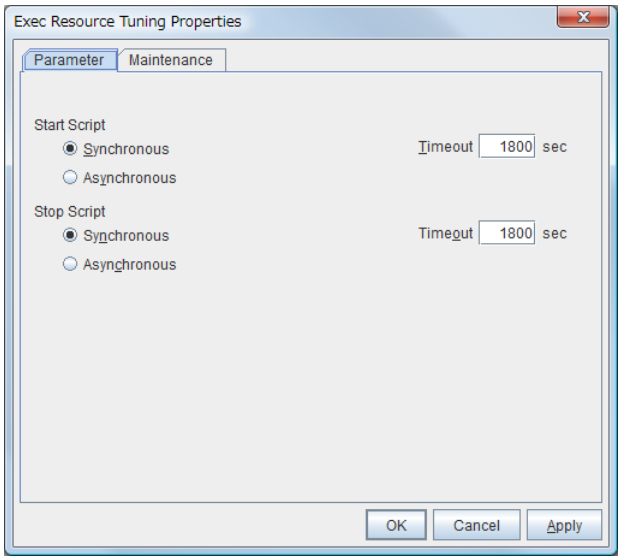
Enter an executable file name to be run when the EXEC resource exits. This must start with "/." The stop script is optional.

For the executable file name, specify the full path of the file on the server, starting with "/". Arguments can be specified.

Tuning an EXEC resource

1. From the tree view displayed on the left pane of the Builder, click the icon of the group to which the EXEC resource whose detail information you want to display and change belongs.
2. The list of group resources is displayed on the table view in the right pane of the screen. Right-click the EXEC resource name. Then click **Properties** and select the **Details** tab.
3. In the **Details** tab, click **Tuning**. The **Exec Resource Tuning Properties** dialog box is displayed.
4. The settings of multi target monitor resource can be displayed and changed by following the description below.

Parameter tab



Common to all start scripts and stop scripts

Synchronous

Select this button to wait for a script to end when it is run. Select this option for executable files that are not resident (the process is returned immediately after the script completion).

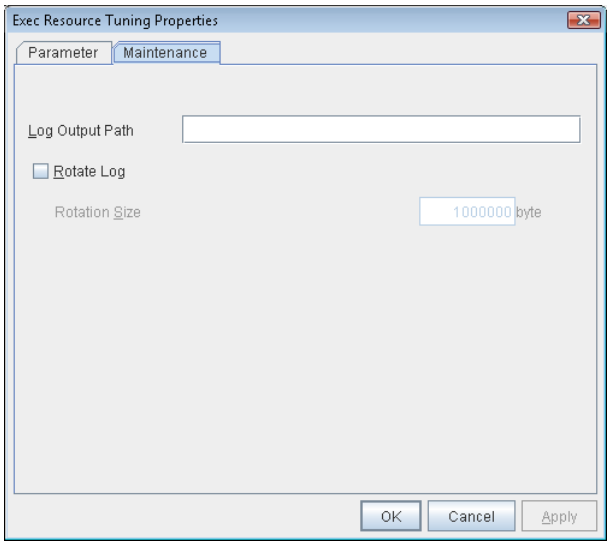
Asynchronous

Does not wait for the script to end when it is run. Select this for resident executable files.
The script can be monitored by PID monitor resource if **Asynchronous** is selected.

Timeout (1 to 9,999)

When you want to wait for a script to end (when selecting **Synchronous**), specify how many seconds you want to wait before a timeout. The timeout can be specified only when **Synchronous** is selected. If the script does not complete within the specified time, it is determined as an error.

Maintenance tab



Log Output Path (within 1,023 bytes)

Specify the redirect destination path of standard output and standard error output for EXEC resource scripts and executable files. If this box is left blank, messages are directed to /dev/null. The name should begin with "/."

If the **Rotate Log** check box is off, note the amount of available disk space in the file system because no limit is imposed on message output.

If the i686 version is used, the files must be periodically removed because EXEC resource activation and deactivation is disabled when the file size exceeds 2GB.

If the **Rotate Log** check box is on, the log file to be output is rotated. Note the following items.

You must specify a log output path within 1009 bytes. If you specify a path of 1010 bytes or more, the log is not output.

You must specify a log file name within 31 bytes. If you specify a log file name of 32 bytes or more, the log is not output.

When using multiple custom monitor resources, the rotation size may not be normally recognized if you specify resources with the same file name, even if the paths differ. (ex. /home/foo01/log/genw.log, /home/foo02/log/genw.log)

Rotate Log

Clicking **Rotate Log** when the **Rotate Log** check box is not checked outputs the execution logs of the EXEC resource script and the executable file without imposing any limit on the file size. Clicking **Rotate Log** when the **Rotate Log** check box is selected rotates and outputs messages.

Rotation Size 1 to 999999999

If the **Rotate Log** check box is selected, specify a rotation size.

The structures of the log files to be rotated and output are as follows:

File name	Description
file_name for the **Log Output Path** specification	Newest log
file_name.pre for the **Log Output Path** specification	Previously rotated log

Setting up VM resources

Dependencies of VM resources

By default, hybrid disk resources do not depend on any group resource type.

What is the VM resource?

A VM resource is used to control virtual machines (guest OSs) from the host OS on the virtual platform.

Starts and stops a virtual machine.

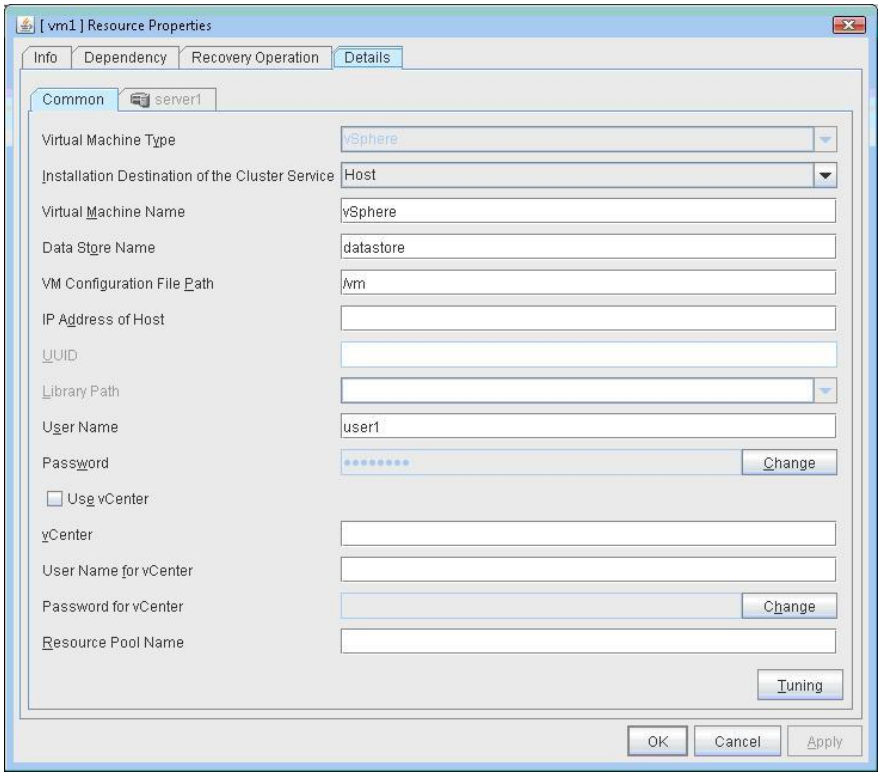
Notes on VM resources

- VM resources are enabled only when EXPRESSCLUSTER is installed in the host OS in the virtualization platform (vSphere, XenServer, KVM).
- A VM resource can be registered with a group for which the group type is virtual machine.
- Only one VM resource can be registered per group.

Displaying and changing details of a VM resource

1. In the tree view displayed in the left pane of the Builder, click the icon of the group to which the VM resource whose details you want to display, specify, or change belong.
2. The list of group resources is displayed on the table view in the right pane of the screen. Right-click the target VM resource name, and then click the **Details** tab in **Property**.
3. In the **Details** tab, display or change the details settings according to the following description.

Resource details tab (vSphere)



Virtual Machine Type

Specify the type of the virtual platform.

Installation Destination of the Cluster Service

Specify the type of OS under which EXPRESSCLUSTER is installed. Selecting the guest OS automatically selects the **Use vCenter** check box.

Virtual Machine Name (within 255 bytes)

Enter the name of the virtual machine. This is omissible when the VM Configuration File Path is input. If the virtual machine name may be changed on the virtual platform side, set the VM Configuration File Path.

Data Store Name (up to 255 bytes)

specify the name of data store containing the virtual machine configuration information.

VM Configuration File Path (within 1,023 bytes)

Specify the path storing information about the virtual machine configuration.

IP Address of Host

Specify the management IP address of the host. You must specify the IP address of host for each server, using individual server settings.

User Name (within 255 bytes)

Specify the user name used to activate the virtual machine.

Password (within 255 bytes)

Specify the password used to activate the virtual machine.

Use vCenter

Specify whether to use vCenter.

vCenter (within 1,023 bytes)

Specify the vCeneter host name.

User Name for vCenter (within 255 bytes)

Specify the user name to connect with vCenter.

Password for vCenter (within 255 bytes)

Specify the password to connect with vCenter.

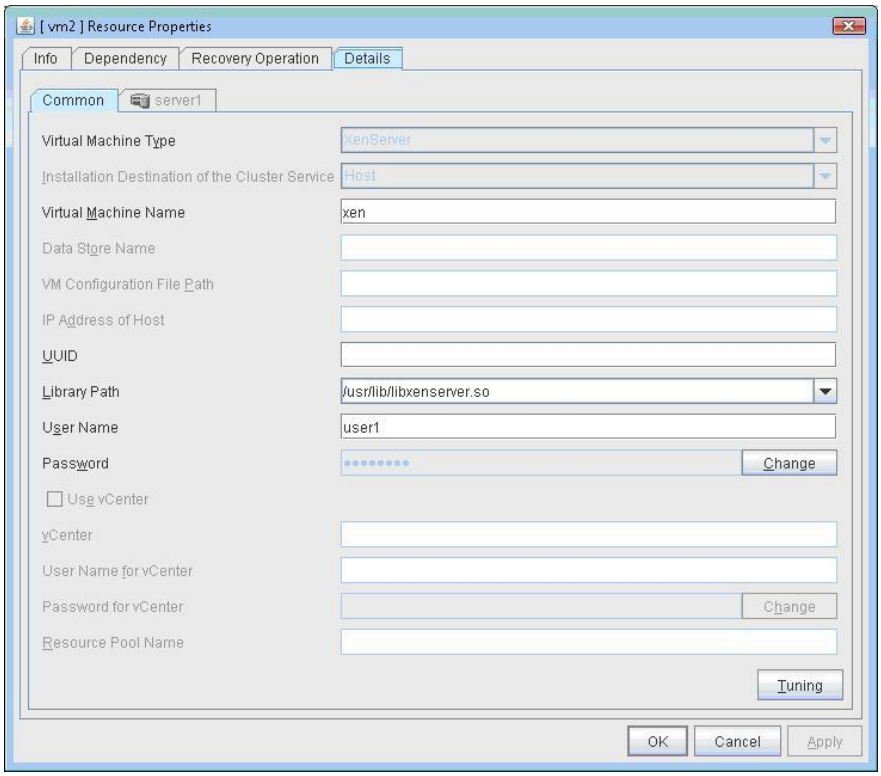
Resource Pool Name (within 80 bytes)

Specify the name of the resource pool to activate the virtual machine.

Tuning

This displays the **VM Resource Tuning Properties** dialog box. Specify detailed settings for the VM resource.

Resource details tab (XenServer)



Virtual Machine Type

Specify the type of the virtual platform.

Virtual Machine Name (within 255 bytes)

Enter the name of the virtual machine. This is omissible when the UUID is set. If the virtual machine name may be changed on the virtual platform side, set the UUID.

UUID

Specify the UUID (Universally Unique Identifier) to identify the virtual machine.

Library Path (within 1,023 bytes)

Specify the library path to be used for control of XenServer.

User Name (within 255 bytes)

Specify the user name used to activate the virtual machine.

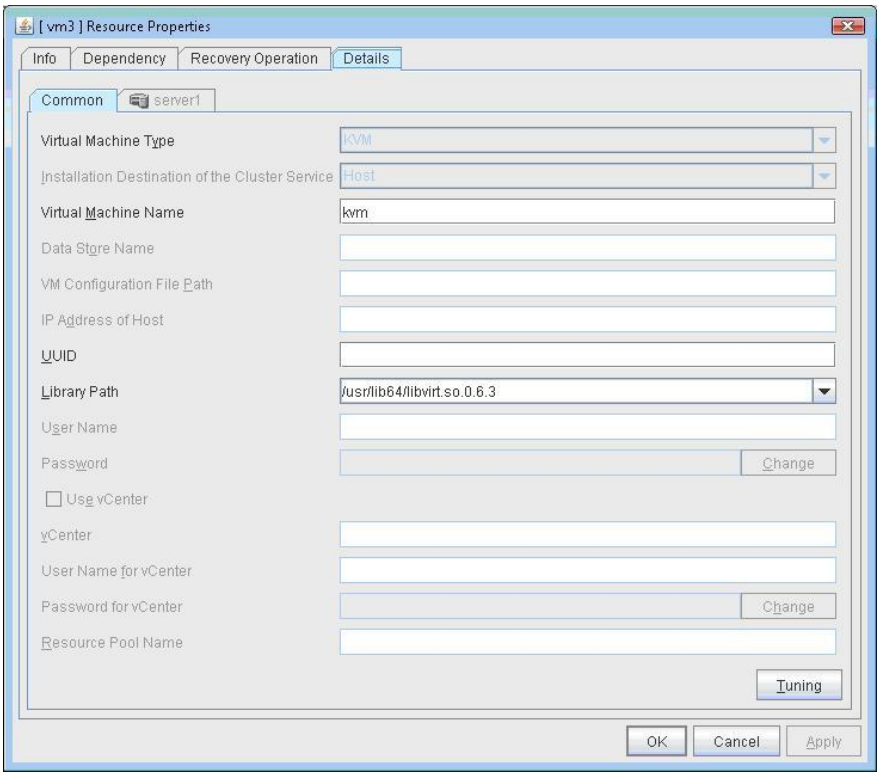
Password (within 255 bytes)

Specify the password used to activate the virtual machine.

Tuning

This displays the **VM Resource Tuning Properties** dialog box. Specify detailed settings for the VM resource.

Resource details tab (KVM)



Virtual Machine Type

Specify the type of the virtual platform.

Virtual Machine Name (within 255 bytes)

Enter the name of the virtual machine. This is omissible when the UUID is set.

UUID

Specify the UUID (Universally Unique Identifier) to identify the virtual machine.

Library Path (within 1,023 bytes)

Specify the library path to be used for control of KVM.

Tuning

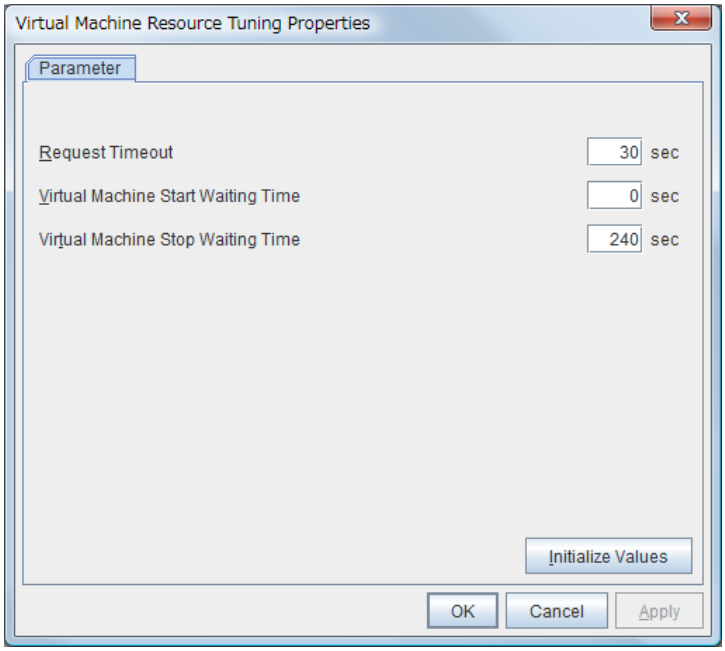
This displays the **VM Resource Tuning Properties** dialog box. Specify detailed settings for the VM resource.

Tuning the VM resource

1. Click **Tuning** on the **VM Resource** tab.

2. The VM resource tuning properties screen is displayed. The settings of VM resource can be displayed and changed by following the description below.

VM resource tuning properties



Request Timeout

Specify how long the system waits for completion of a request such as to start or stop a virtual machine.

If the request is not completed within this time, a timeout occurs and resource activation or deactivation fails.

Virtual Machine Start Waiting Time

The system definitely waits this time after requesting the virtual machine to startup.

Virtual Machine Stop Waiting Time

The maximum time to wait for the stop of the virtual machine. Deactivation completes at the timing the stop of the virtual machine.

Chapter 5 Monitor resource details

This chapter provides details about monitor resources. A monitor resource is the unit used when EXPRESSCLUSTER X SingleServerSafe performs monitoring.

This chapter covers:

Monitor Resources

The following resources can be defined as monitor resources:

Monitor resource name	Function	Monitor Timing: (Default values are shown in bold.)	Target Resource
Disk monitor resource	Monitors disk devices.	**Always**/When activated	All resources
IP monitor resource	Monitors IP addresses and communication paths by using the ping command and checking whether there is a response.	**Always**/When activated	All resources
NIC Link Up/Down monitor resource	Acquires the NIC link status to monitor whether the link is up or down.	**Always**/When activated	All resources
PID monitor resource	PID monitor resource monitors a successfully activated EXEC resource.	**Always**/When activated	All resources
User mode monitor resource	Determines a user space stall to be an error.	Always (Fixed)	-
Multi target monitor resource	Performs monitoring by using multiple monitor resources in combination.	When activated (Fixed)	All resources
Software RAID monitor resource	Monitors software RAID devices.	Always (Fixed)	None
Custom monitor resource	Performs monitoring by executing any script.	**Always**/When activated	All resources
Volume manager monitor resource	Provides a monitoring mechanism for multiple storage devices and disks.	Always/**When activated**	All
VM monitor resource	Provides a mechanism for monitoring a virtual machine started by a VM resource.	Always (Fixed)	vm
Message receive monitor resource	Sets up error-handling actions executed on reception of an error message and displays error message in the WebManager.	Always (Fixed)	None

Process Name monitor resource	Monitors monitor the process of specified processes.	**Always**/When activated	All resources
DB2 monitor resource	Provides a mechanism for monitoring an IBM DB2 database.	When activated (Fixed)	All resources
FTP monitor resource	Provides a mechanism for monitoring an FTP server.	When activated (Fixed)	All resources
HTTP monitor resource	Provides a mechanism for monitoring an HTTP server.	When activated (Fixed)	All resources
IMAP4 monitor resource	Provides a mechanism for monitoring an IMAP server.	When activated (Fixed)	All resources
MySQL monitor resource	Provides a mechanism for monitoring a MySQL database.	When activated (Fixed)	All resources
NFS monitor resource	Provides a mechanism for monitoring an NFS file server.	**Always**/When activated	All resources
Oracle monitor resource	Provides a mechanism for monitoring an Oracle database.	When activated (Fixed)	All resources
OracleAS monitor resource	Provides a mechanism for monitoring an Oracle application server.	When activated (Fixed)	All resources
POP3 monitor resource	Provides a mechanism for monitoring a POP server.	When activated (Fixed)	All resources
PostgreSQL monitor resource	Provides a mechanism for monitoring a PostgreSQL database.	When activated (Fixed)	All resources
Samba monitor resource	Provides a mechanism for monitoring a samba file server.	**Always**/When activated	All resources
SMTP monitor resource	Provides a mechanism for monitoring an SMTP server.	When activated (Fixed)	All resources
Sybase monitor resource	Provides a mechanism for monitoring a Sybase database.	When activated (Fixed)	All resources

Tuxedo monitor resources	Provides a mechanism for monitoring a Tuxedo application server.	When activated (Fixed)	All resources
Weblogic monitor resources	Provides a mechanism for monitoring a WebLogic application server.	When activated (Fixed)	All resources
Websphere monitor resources	Provides a mechanism for monitoring a WebSphere application server.	When activated (Fixed)	All resources
WebOTX monitor resources	Provides a mechanism for monitoring a WebOTX application server.	When activated (Fixed)	All resources
JVM monitor resources	Provides a mechanism for monitoring a Java VM.	**Always**/When activated	exec resource
System monitor resources	Provides a mechanism for monitoring a System Resource.	Always (Fixed)	All resources

Status of monitor resources after monitoring starts

The status of some monitor resources might be “Caution” if there is a period of time following the start of monitoring in which monitoring of that resource is not yet ready.

Caution status is possible for the following monitor resources.

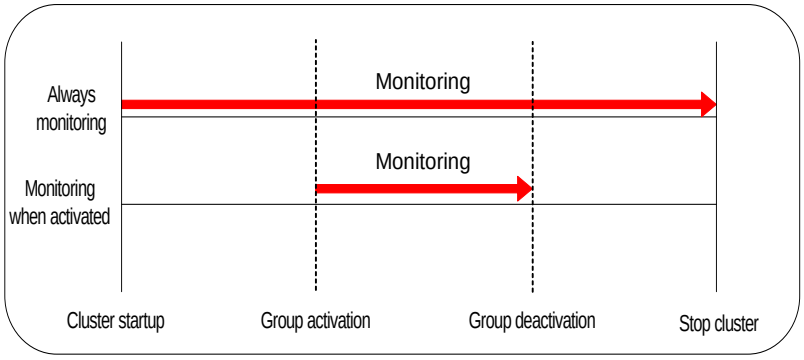
- Message Receive Monitor Resource
- Custom Monitor Resource (whose monitor type is **Asynchronous**)
- DB2 Monitor Resource
- System Monitor Resource
- JVM Monitor Resource
- MySQL Monitor Resource
- Oracle Monitor Resource
- PostgresSQL Monitor Resource
- Process Name Monitor Resource
- Sybase Monitor Resource

Monitor timing of monitor resource

There are two types of monitoring by monitor resources; **Always** and **Active**.

The monitoring timing differs depending on monitor resources:

- Always:
  Monitoring is performed by monitor resource all the time.
- Active:
  Monitoring is performed by monitor recourse while specified group resource is active.
  Monitor resource does not monitor while group resource is not activated.



Suspending and resuming monitoring on monitor resources

Monitor resource can temporarily suspend monitoring and resume it.
Monitoring can be suspended and resumed by the following two methods:

- Operation on the WebManager
- Operation by the clpmonctrl command
  The clpmonctrl command can control only monitor resources on the server where this command is run.

Some monitor resources can suspend and resume monitoring and others cannot. For details, see the list below.

Monitor Resource	Control
Disk Monitor Resource	Possible
IP Monitor Resource	Possible
User-mode Monitor Resource	Possible
NIC Link Up/Down Monitor Resource	Possible
PID Monitor Resource	Possible
Multi Target Monitor Resource	Possible
Custom Monitor Resource	Possible
DB2 Monitor Resource	Possible
Software RAID Monitor Resource	Possible
Process Name Monitor Resource	Possible
DB2 Monitor resource	Possible
FTP Monitor Resource	Possible

HTTP Monitor Resource	Possible
IMAP4 Monitor Resource	Possible
MySQL Monitor Resource	Possible
NFS Monitor Resource	Possible
Oracle Monitor Resource	Possible
OracleAS Monitor Resource	Possible
POP3 Monitor Resource	Possible
PostgreSQL Monitor Resource	Possible
Samba Monitor Resource	Possible
SMTP Monitor Resource	Possible
Sybase Monitor Resource	Possible
Tuxedo Monitor Resource	Possible
Weblogic Monitor Resource	Possible
Websphere Monitor Resource	Possible
WebOTX Monitor Resource	Possible
VM Monitor Resource	Possible
Message Receive Monitor Resource	Possible
JVM Monitor Resource	Possible
System Monitor Resource	Possible

On the WebManager, right-click menus of the monitor resources which cannot control monitoring are disabled. The clpmonctrl command only controls the resources which can control monitoring. For monitor resources which cannot control monitoring, a warning message is displayed and controls are not performed.

Suspending monitoring on a monitor resource is disabled if one of the following operations is performed.

- Resume operation on WebManager
- Resume operation by using the clpmonctrl command
- Stop the cluster
- Suspend the cluster

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 WebManager (verification mode)
  On the WebManager(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 only monitor resources on the server where this command is run. 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 Chapter 2, "EXPRESSCLUSTER X SingleServerSafe command reference, Controlling monitor resources (clpmonctrl command)" in the *Operation Guide*.

Dummy failure of a monitor resource is disabled if the following operations are performed.

- Dummy failure was disabled on WebManager (verification mode)
- "Yes" was selected from the dialog box displayed when the WebManager 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

Monitor priority of the monitor resources

To assign a higher priority for monitor resources to monitor when the operating system is heavily loaded, the nice value can be set to all monitor resources except the user space monitor resource.

- The nice value can be specified through minus 19 (low priority) to plus 20 (high priority). Detection of the monitor timeout can be controlled by setting a higher priority to the nice value.

Changing the name of a monitor resource

1. In the tree view shown on the left pane of the Builder, click the **Monitors** icon. In the table view shown on the right side of the screen, right-click the icon of the monitor resource whose name you want to change, and click **Rename Monitor Resource**.
2. Enter a new name in the **Change Monitor Resource Name** dialog box.

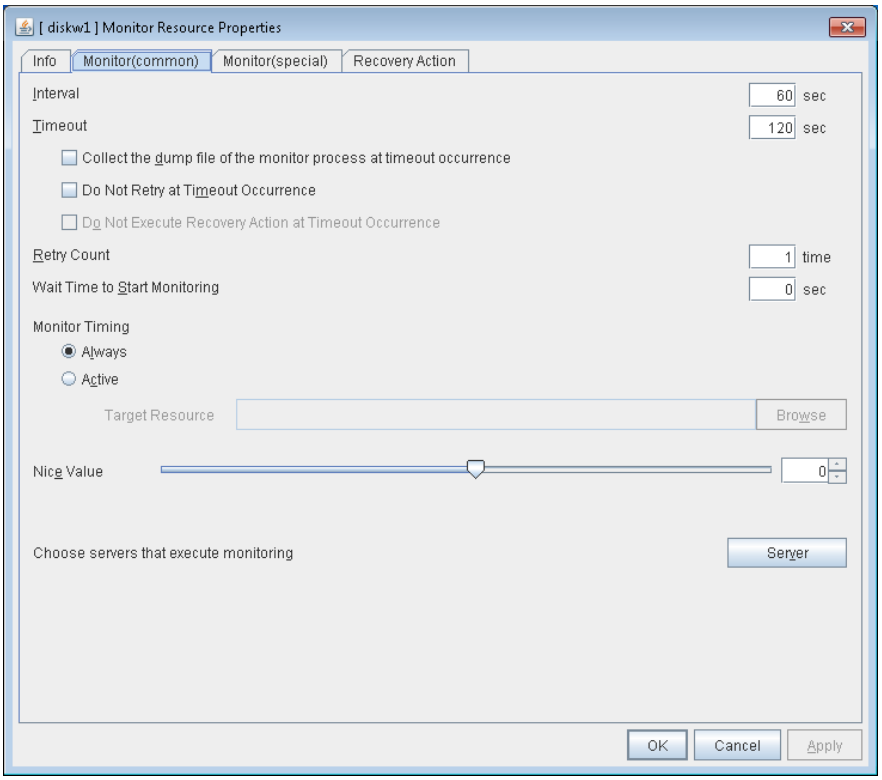
Displaying and changing the comment of a monitor resource (Monitor resource properties)

1. In the tree view shown on the left pane of the Builder, right-click the **Monitors** icon. In the table view shown on the right side of the screen, right-click the icon of the monitor resource whose comment you want to change, and then click **Properties**. **Monitor Resource Properties** dialog box is displayed.
2. On the **Info** tab, the monitor resources name and comment are shown. Enter a new comment (within 127 bytes).

Note:
You cannot change the monitor resource name on the **Info** tab. To change the name, right-click the **Monitors** icon as described in the step 1 above. Click **Rename Monitor Resource** and enter a new name.

Displaying and changing the settings of a monitor resource (Common to monitor resources)

1. In the tree view shown on the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is shown in the table view on the right side of the screen. Right-click the name of the monitor resource whose settings you want to change. Click **Properties**, and then click the **Monitor** tab.
3. On the **Monitor** tab, you can see and/or change the settings of monitor resource by following the description below.



Interval 1 to 999

Specify the interval to check the status of monitor target.

Timeout 5 to 999[1]

When the normal status cannot be detected within the time specified here, the status is determined to be error.

Collect the dump file of the monitor process at timeout occurrence

In case that this function is enabled, the dump information of the timed out monitor resource is collected when the monitor resource times out. Dump information is collected up to 5 times.

[1] When ipmi is set as a monitoring method for the user-mode monitor resource, 255 or less should be specified.

Do Not Retry at Timeout Occurrence

When this function is enabled, recovery action is executed immediately if a monitor resource timeout occurs.

Do not Execute Recovery Action at Timeout Occurrence

When this function is enabled, recovery action is not executed if a monitor resource timeout occurs.

This can be set only when the **Do Not Retry at Timeout Occurrence** function is enabled.

Note:

For the following monitor resources, the **Do Not Retry at Timeout Occurrence** and **Do Not Execute Recovery Action at Timeout Occurrence** functions cannot be set.

- user-mode monitor resources
- custom monitor resources (whose monitor type is **Asynchronous**)
- multi target monitor resources
- VM monitor resources
- message receive monitor resources
- JVM monitor resources
- system monitor resources

Retry Count 0 to 999

Specify how many times an error should be detected in a row after the first one is detected before the status is determined as error. If this is set to zero (0), the status is determined as error at the first detection of an error.

Wait Time to Start Monitoring 0 to 9999
Set the wait time to start monitoring.

Notes:

If timeout of monitor resource is longer than “Wait Time to start Monitoring”, the value of the timeout will be used for “Wait Time to Start Monitoring” for following monitor resources.

- Message receive monitor resource
- Custom monitor resource (whose monitor type is **Asynchronous**)
- DB2 Monitor Resource
- System Monitor Resource
- JVM Monitor Resource
- MySQL Monitor Resource
- Oracle Monitor Resource
- PostgresSQL Monitor Resource
- Process Name Monitor Resource
- Sybase Monitor Resource

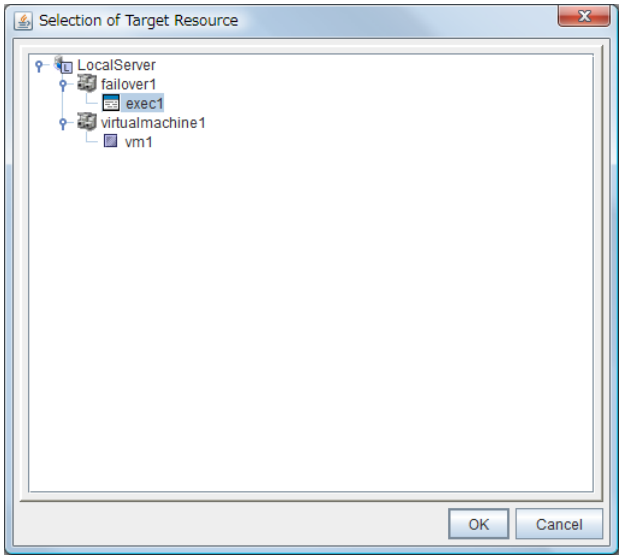
Monitor Timing
Set the monitoring timing. Select the timing from:

◆ 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 the LocalServer and cluster are shown in a tree view. Select the target resource and click **OK**.



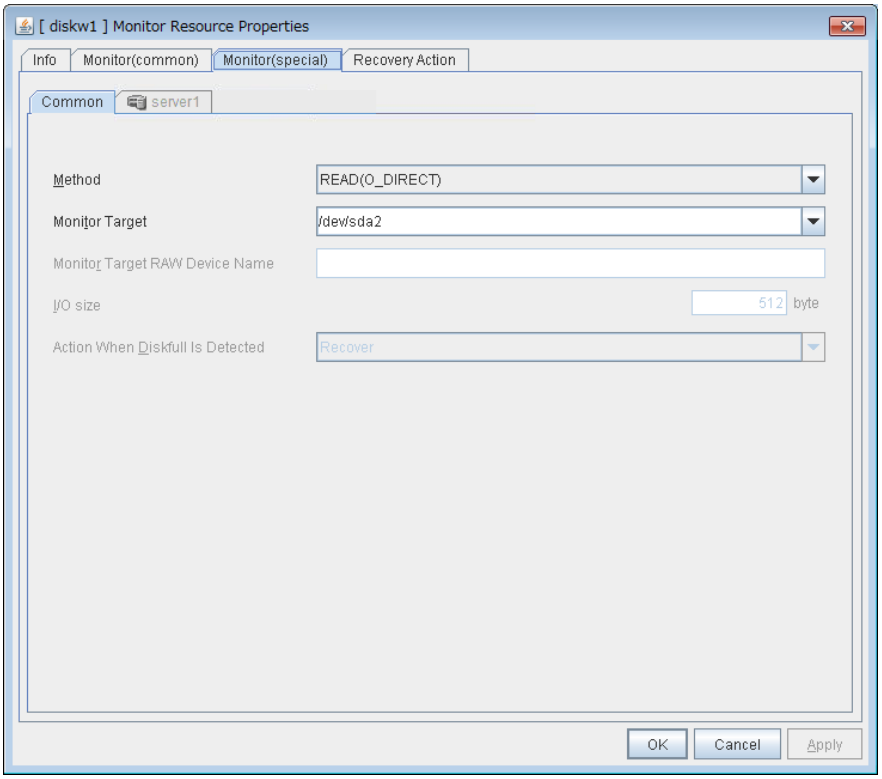
Nice Value
Set the nice value of a process.

Setting up disk monitor resources

Disk monitor resources monitor disk devices.

It is recommended to READ (O_DIRECT) for monitoring the disk that the disk monitor resource (TUR) cannot be used.

1. Click the **Monitors** icon on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the disk monitor resource whose settings you want to change.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Monitor method

Specify how you want to monitor a disk device from one of the following options.

- TUR
- TUR(generic)
- TUR(legacy)
- READ
- READ (O_DIRECT)
- WRITE (FILE)
- READ (RAW)
- READ (VXVM)

Monitoring target (within 1,023 bytes)

- When the monitoring method is WRITE (FILE):

  Specify the path name of the file to be monitored. This must start with "/."

  Specify the file name with the absolute path. If you specify the file name of an existing file, it is overwritten and the data in the file is lost.

- When the monitoring method is READ (O_DIRECT)

  Specify the path name of the file to be monitored. This must start with "/."

  Specify the file name with the absolute path. If you specify the file name of an existing file, it is overwritten and the data in the file is lost.

- When the monitoring method is READ (RAW)

  The monitor target may be omitted. However, the monitor target raw device name must be specified. Specify this mode only when binding and monitoring the device. It is not possible to specify the device name for a partition device that has been mounted or will possible be mounted for monitoring.
  In addition, a whole device (whole disk) of a partition device that has been mounted or will possibly be mounted cannot be specified for monitoring. Allocate a partition dedicated to monitoring. (Allocate 10 MB or more to the monitoring partition). The partition must start with "/".

- When the monitoring method is READ (VXVM)

  The fields are dim and not selectable.

- When the monitoring method is other than the above

  When the monitoring method is other than the above: This must start with "/."

Monitor target raw device name (within 1,023 bytes)

This is specifiable only when the monitoring method is READ (RAW) or READ (VXVM).

- When the monitoring method is READ (RAW)

  Enter a device name for raw accessing. Any raw device already registered with the **Disk I/F List** of the server properties is unregisterable. For a raw device of a VxVM volume, select READ (VXVM) for the monitoring method.

- When the monitoring method is READ (VXVM)

  Set the VxVM volume raw device name. If the volume raw device file system is not vxfs, it cannot be monitored. This must start with "/."

I/O size (1 to 99,999,999)

Specify the size of I/O for reading or reading/writing when READ or WRITE (FILE) is selected as a monitoring method.

* When READ (RAW) , READ(O_DIRECT) or READ (VXVM) is specified, the **I/O size** text box is dim. A single sector is read from the target device.
* If TUR, TUR (generic), or TUR (legacy) is specified, this setting is ignored.

Action when diskfull is detected

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.

* If READ, READ (RAW), READ (VXVM), READ (O_DIRECT), TUR, TUR (generic), or TUR (legacy) is specified, the **Action when diskfull is detected** option is grayed out.

When a local disk is specified in **Target Device Name**, a local disk on the server can be monitored.

◆ Example of settings to monitor the local disk /dev/sdb by using the READ method, and to reboot the OS when an error is detected:

Setting item	Value	Remarks
Target Device Name:	/dev/sdb	SCSI disk in the second machine.
Monitor Method:	READ	READ method.
Recovery Target:	server	-
Final Action:	The service will be stopped and the OS will be restarted	Reboot the OS.

◆ Example of settings to monitor the local disk /dev/sdb by using the **TUR(generic) method** and select **No Operation** (merely show an alert on the WebManager) when an error is detected:

Setting item	Value	Remarks
Target Device Name:	/dev/sdb	SCSI disk in the second machine.
Monitor Method:	TUR(generic)	SG_IO method
Final Action:	No Operation	

Monitoring by disk monitor resources

Two ways of monitoring are employed by the disk monitor resource: READ and TUR.

- Notes on TUR:
  - You cannot run the Test Unit Ready or SG_IO command of SCSI on a disk or disk interface (HBA) that does not support it.
    Even if your hardware supports this command, consult the driver specifications because the driver may not support it.
  - ioctl may be incorrectly executed for an LVM logical volume (LV) device. Use READ for LV monitoring.
  - A TUR method cannot be used for the IDE interface disk.
  - In the case of the disk of S-ATA interface, it may be recognized as the IDE interface disk (hd) or as the SCSI interface disk (sd) depending on the type of a disk controller and the distribution to be used. When the disk is recognized as the IDE interface, no TUR methods can be used. If the disk is recognized as the SCSI interface, TUR (genetic) cannot be used but TUR (legacy) can be used.
  - Test Unit Ready, compared to Read, burdens OS and disks less.
  - In some cases, Test Unit Ready may not be able to detect actual errors in I/O to media.
  - In an environment in which the OS kernel is updated (kernel-2.6.18-274.18.1.el5 or later, kernel-2.6.32-220.2.1.el6 or later), you cannot use a partition on the disk by setting it as the target to be monitored.
  - Some disk devices may temporarily return Unit Attention at TUR issue, depending on the device status.
    The temporary return of Unit Attention does not signify a problem. If the TUR retry count is set to 0, however, the above return is determined to be an error and the disk monitor resource becomes abnormal.
    To avoid this meaningless error detection, set the retry count to one or more.

TUR monitoring provides the following three choices.

- TUR
  - ioctl is used by the following steps and the status of the device is determined by the result of the command:
    Run the ioctl (SG_GET_VERSION_NUM) command. The status is determined by the return value of ioctl and the version of SG driver.
    If the ioctl command runs successfully and the version of SG driver is 3.0 or later, execute ioctl TUR (SG_IO) using the SG driver.
    If the ioctl command fails or the version of SG driver is earlier than 3.0, execute ioctl TUR which is defined as a SCSI command.
- TUR(legacy)
  - Monitoring is performed by using ioctrl (Test Unit Ready). Test Unit Ready (TUR) which is defined as a SCSI command is used against the specified device, and the status of the device is determined by the result of the command.
- TUR(generic)
  - Monitoring is executed by using ioctl TUR (SG_IO). ioctl TUR (SG_IO) which is defined as a SCSI command is used against the specified device, and the status of the device is determined by the result of the command. Even with a SCSI disk, SG_IO may not work successfully depending o the OS or distribution.

READ monitoring is performed as described below.

- The specified size of the specified device (disk device or partition device) or file is read. Judgement is performed by the size that could be read.

- Dummy Read reads the specified size data on the specified device (disk device or partition device). Based on the result (the size of data actually read), the status is judged.
- Dummy Read is for determining if the specified size of data can be read. Validity of the data read is not judged.
- Burden of the load experienced by the OS and disk is proportional to the size of the data on the specified disk to be read.
- See "I/O size when READ is selected for disk monitor resources" on page 101 to configure the read size.

READ (O_DIRECT) monitoring is performed as described below.

- A single sector on the specified device (disk device or partition device) or the file are read without using the cache (O_DIRECT mode), and the result (the size of the data successfully read) is used to make a judgment.
- Judgment is based on whether or not reading has been performed successfully. Validity of the read data is not judged.

READ (RAW) monitoring is performed as described below.

- Reading is monitored for the specified device without using the OS cache, in the same way as READ (O_DIRECT).
- Judgment is based on whether or not reading has been performed successfully. Validity of the read data is not judged.
- When the READ (raw) monitoring method is specified, partitions that have been or will possibly be mounted cannot be monitored. In addition, a whole device (whole disk) that includes partitions that have been or will possibly be mounted cannot be monitored. Allocate a partition dedicated to monitoring and specify it as the disk monitor resource. (Allocate 10 MB or more to the monitoring partition).

READ (VXVM) monitoring is performed as described below.

- Like the READ (O_DIRECT) monitoring method, the process to read the specified device is monitored without using the OS cache.
- Judgment is based on whether or not reading has been performed successfully. Validity of the read data is not judged.
- The READ (VXVM) monitoring method can be used only when the file system of the volume raw device is vxfs.

WRITE (FILE) monitoring is performed as described below.

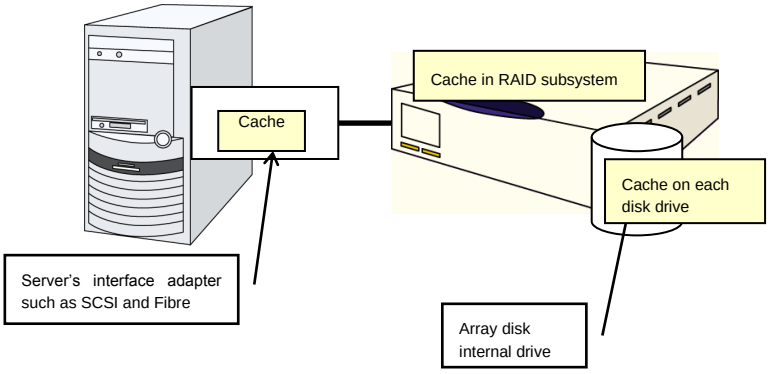
- The file of the specified path is created, written, and deleted to be judged.
- Validity of the written data is not judged.

I/O size when READ is selected for disk monitor resources

Enter the size of data when READ is selected as a method of monitoring.

Depending on the shared disk and interfaces in your environment, various caches for reading may be implemented. Because of this, when the specified read size is too small, READ may hit in cache, and may not be able to detect read errors.

When you specify a READ I/O size, verify that READ can detect I/O errors on the disk with that size by intentionally creating I/O errors.

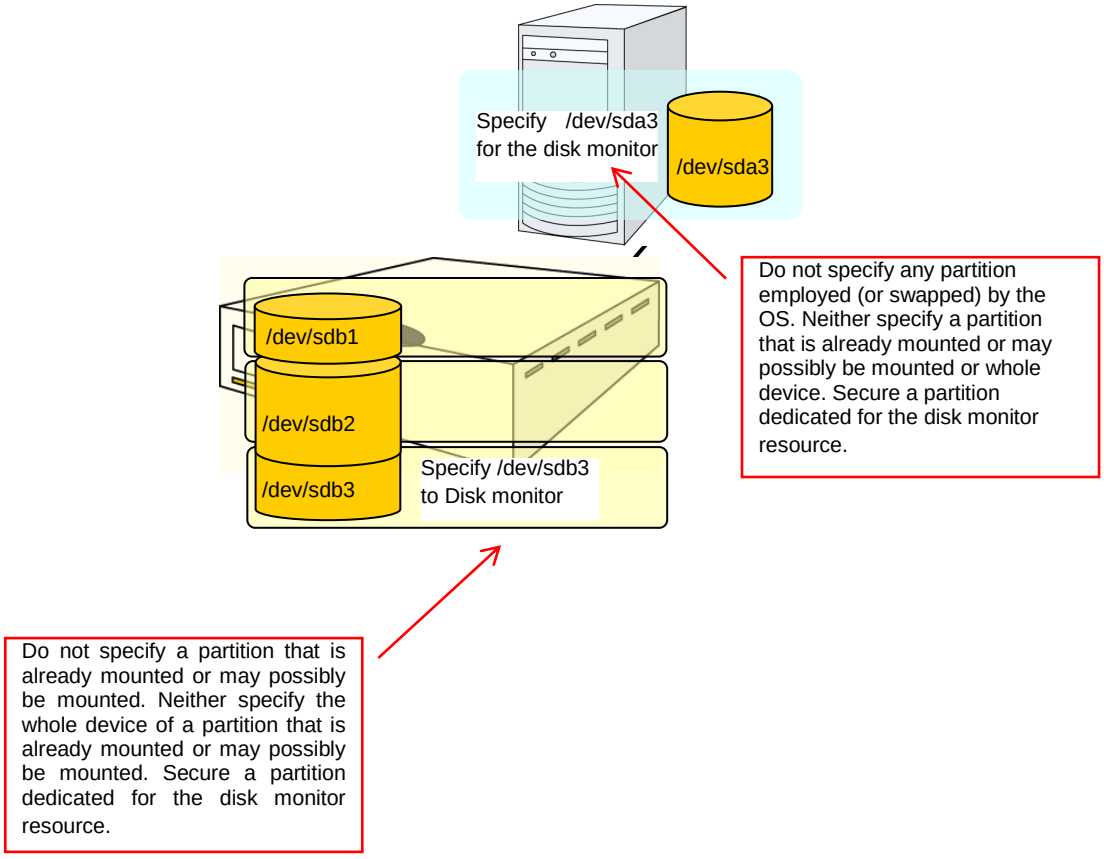


Note:
This figure illustrates a typical example of shared disks. This is not applicable to all array units.

Setup example when READ (raw) is selected for the disk monitor resource

Example of disk monitor settings

- Disk monitor resource (internal HDD monitoring by READ (RAW))
- Disk monitor resource (shared disk monitoring by READ (RAW))

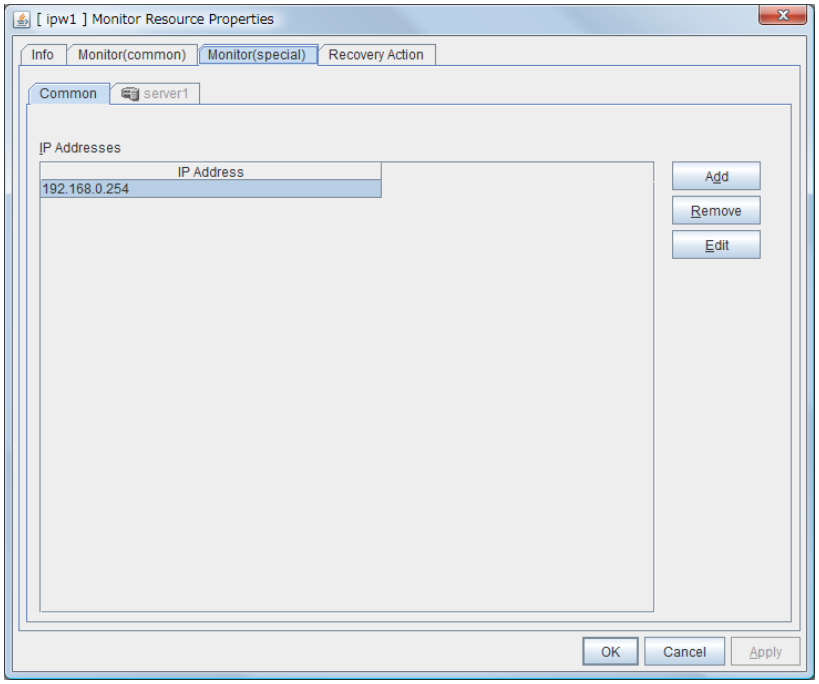


Setting up IP monitor resources

IP monitor resource monitors IP addresses using the ping command.

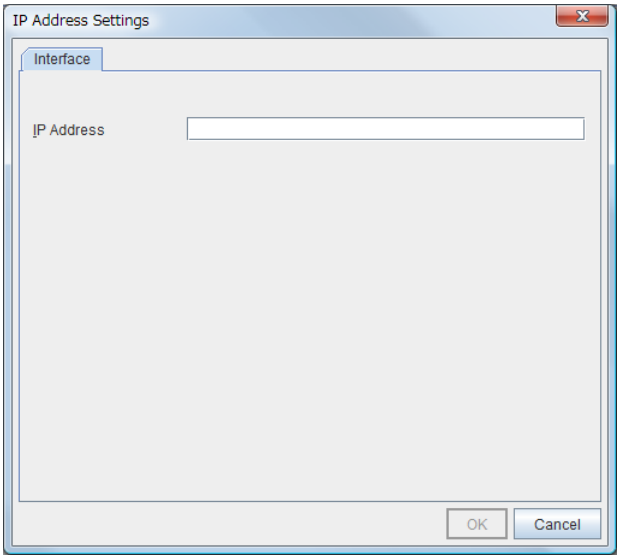
1. Click the **Monitors** icon on the tree view displayed on the left side of the **Builder** window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target IP monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.

IP addresses to be monitored are listed in **IP Addresses**.



Add

Click **Add** to add an IP address to be monitored. Click **Edit** to display the **IP Address Settings** dialog box.



IP Address (within 255 bytes)

Enter an IP address or a host name to be monitored in this field and click **OK**. The IP address or host name you enter here should be the one that exists on the public LAN. If you set the host name, set the name resolution to OS. (ex. By adding entry to /etc/hosts)

Remove

Click **Remove** to remove an IP address selected in **IP Addresses** from the list so that it will no longer be monitored.

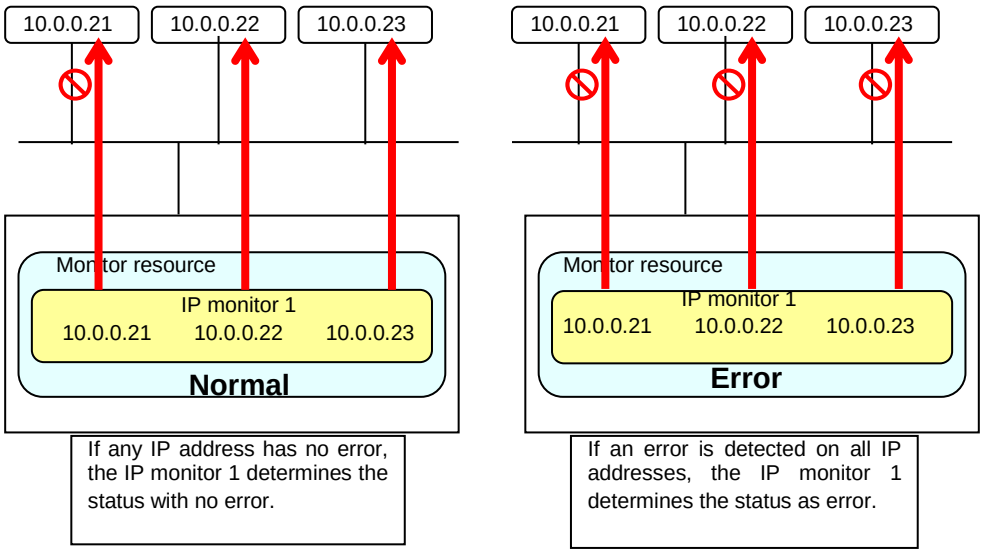
Edit

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**.

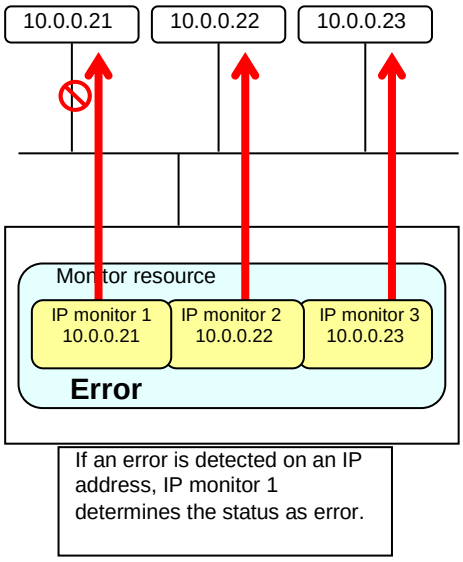
Monitoring by IP monitor resources

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.

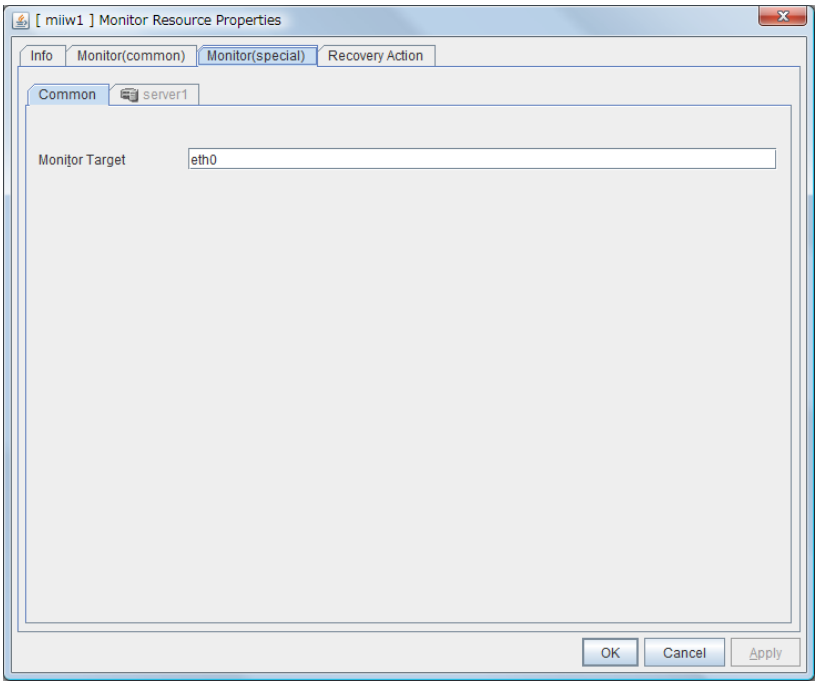


◆ If you want to establish error when any one of IP addresses has an error, create one IP monitor resource for each IP address.



Setting up NIC Link Up/Down monitor resources

NIC Link Up/Down monitor resource obtains the information on how the specified NIC is linked monitors the linkage is up or down.



Monitor Target (within 15 bytes)

Enter the name of the NIC interface you want to monitor. You can monitor Bond devices (e.g. bond.600) and team devices (e.g. team0). You can also monitor VLAN and tagVLAN (setting example: eth0.8).

System requirements for NIC Link Up/Down monitor resources

Network interfaces supporting NIC Link UP/Down monitor resource

NIC Link UP/Down monitor resource has been tested to work in the following network interfaces.

Ethernet Controller(Chip)	Bus	Driver version
Intel 82557/8/9	PCI	3.5.10-k2-NAPI
Intel 82546EB	PCI	7.2.9
Intel 82546GB	PCI	7.3.20-k2-NAPI 7.2.9
Intel 82573L	PCI	7.3.20-k2-NAPI
Intel 80003ES2LAN	PCI	7.3.20-k2-NAPI
Broadcom BCM5721	PCI	7.3.20-k2-NAPI

Notes on NIC Link Up/Down monitor resources

Some NIC boards and drivers do not support required ioctl( ).
The propriety of a NIC Link Up/Down monitor resource of operation can be checked by the ethtool command which each distributor offers.

```
ethtool eth0
Settings for eth0:
       Supported ports: [ TP ]
       Supported link modes:   10baseT/Half 10baseT/Full
                               100baseT/Half 100baseT/Full
                               1000baseT/Full
       Supports auto-negotiation: Yes
       Advertised link modes:  10baseT/Half 10baseT/Full
                               100baseT/Half 100baseT/Full
                               1000baseT/Full
       Advertised auto-negotiation: Yes
       Speed: 1000Mb/s
       Duplex: Full
       Port: Twisted Pair
       PHYAD: 0
       Transceiver: internal
       Auto-negotiation: on
       Supports Wake-on: umbg
       Wake-on: g
       Current message level: 0x00000007 (7)
       Link detected: yes
```

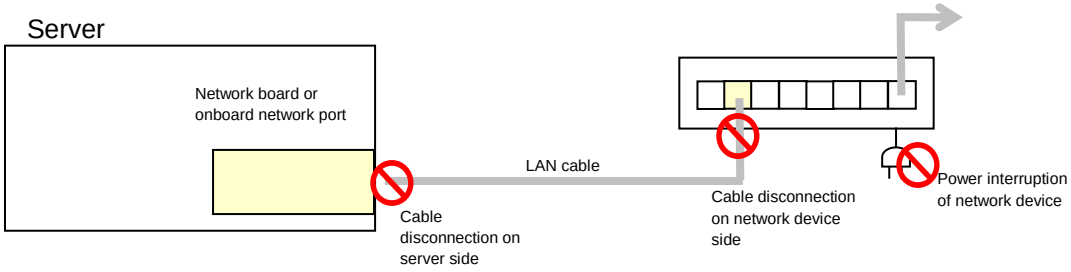
- When the LAN cable link status ("Link detected: yes") is not displayed as the result of the `ethtool` command:
  - It is highly likely that NIC Link Up/Down monitor resource of EXPRESSCLUSTER is not operable. Use IP monitor resource instead.

- When the LAN cable link status ("Link detected: yes") is displayed as the result of the `ethtool` command:
  - In most cases NIC Link Up/Down monitor resource of EXPRESSCLUSTER can be operated, but sometimes it cannot be operated.
  - Particularly in the following hardware, NIC Link Up/Down monitor resource of EXPRESSCLUSTER may not be operated. Use IP monitor resource instead.
  - When hardware is installed between the actual LAN connector and NIC chip such as a blade server

When you check if NIC Link Up/Down monitor resource can be used with the use of EXPRESSCLUSTER on a machine for production environment, follow the steps below.

1. Register NIC Link Up/Down monitor resource with the configuration data.
   Select **No Operation** for the configuration of recovery operation of NIC Link Up/Down monitor resource upon error detection.
2. Start the server.
3. Check the status of NIC Link Up/Down monitor resource.
   If the status of NIC Link Up/Down monitor resource is abnormal while LAN cable link status is normal, NIC Link Up/Down monitor resource cannot be used.
4. If NIC Link Up/Down monitor resource status becomes abnormal when LAN cable link status is made abnormal status (link down status), NIC Link Up/Down monitor resource can be used.
   If the status remains to be normal, NIC Link Up/Down monitor resource cannot be used.

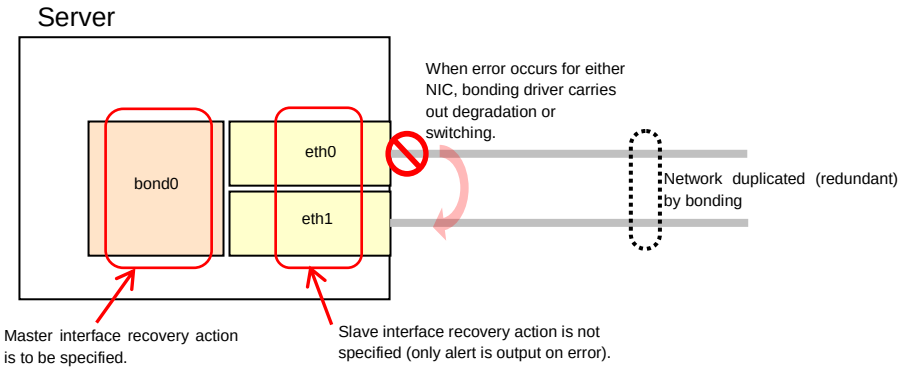
Configuration and range of NIC link up/down monitoring



- The `ioctl`( ) to the NIC driver is used to find how the server is linked to the network. (For the IP monitoring, the status is judged by the ping response from the specified IP address.)
- NICs dedicated to interconnects (mirror connects) can be specified. However, if two nodes are connected by cross cables and one server goes down, an error is also detected for the other server (because the link is not established).
  The recovery action to be taken at detection of error should be configured with the appropriate value.
  For example, if **Stop cluster daemon and reboot OS** is selected, other servers will continue to restart the OS endlessly.

When the network is employing bonding, both the slave interface (eth0, eth1...) and master interface (bond0...) may also be subject to monitoring, making the availability of bonding valid. In that case, the following settings are recommended.

- Slave interface
  - Recovery on error detection: Nothing
    If only one cable (eth0) fails, EXPRESSCLUSTER does not perform a recovery action and just outputs an alert.
    Network recovery is handled by bonding.
- Master interface
  - Recovery on error detection: Shutdown or another setting
    If all slave interfaces fail (the master interface goes down), EXPRESSCLUSTER performs a recovery action.



Setting up PID monitor resources

PID monitor resource monitors a successfully activated EXEC resource. By monitoring the presence of process ID, an error is established when the process ID disappears.

The EXEC resource to be monitored is set according to the steps described in "Target Resource" of "Common settings for monitor resources" on page 259. The EXEC resource can be monitored if its settings for activation are configured to **Asynchronous**. You cannot detect stalled status of the process.

Note:
To monitor for the stalling of components such as databases, samba, apache, sendmail, purchase EXPRESSCLUSTER monitoring options.

Notes on PID monitor resources

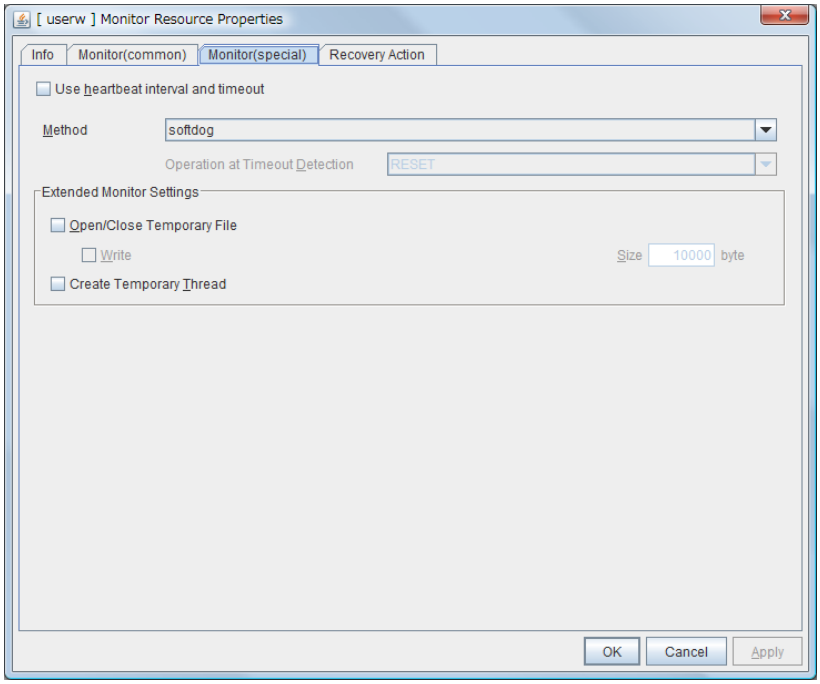
PID monitor resource monitors a successfully activated EXEC resource. The EXEC resource can be monitored if its settings for activation are configured to **Asynchronous**.

Setting up user-mode monitor resources

User-mode monitor resource considers stalling in user space as an error.

The resource is automatically registered. For the monitoring method, the user-mode monitor resource for softdog is automatically registered.

1. Click the **Monitors** icon on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the target user-mode monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Use heartbeat interval and timeout

Select this check box if you use heartbeat's interval and timeout for monitor's interval and timeout.

- When selected:

  Heartbeat interval and timeout are used.

- When cleared:

  Interval and timeout specified on the **Monitor** tab are used. You need to set a larger value for timeout than interval. When ipmi is specified as the monitoring method, the timeout time must be 255 or less.

Monitor method

Choose how you want to monitor the user-mode monitor resource from the following. You can not select a method which has already been used for other user-mode monitor resource.

- softdog
  The softdog driver is used.
- ipmi
  The ipmiutil is used.
- keepalive
  The clpkhb and clpka drivers are used.
- none
  Uses nothing.

Operation at timeout detection

Select the final action. This can be set only when the monitoring method is keepalive.

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

Open/Close dummy file

Select this check box if you want to open/close a dummy file at every interval when you execute monitoring.

- When selected:
  A dummy file will be opened/closed.
- When cleared:
  A dummy file will not be opened/closed.

With Writing:

Select this check box if you have chosen to open/close a dummy file and want to write in dummy data.

- When selected:
  Dummy data is written into a dummy file.
- When cleared:
  Dummy data is not written into a dummy file.

Size (1 to 9,999,999)

If you have chosen to write dummy data into a dummy file, specify the size to write in.

Create dummy thread

Select this check box if you want to create a dummy thread when monitoring is performed.

- When selected:
  Dummy thread will be created.
- When cleared:
  Dummy thread will not be created.

Drivers user-mode monitor resources depend on

Monitor by: softdog

softdog

- This driver is necessary when softdog is used for monitoring.
- Configure a loadable module. Static driver cannot be used.
- Monitoring can not be started if the softdog driver is unable to use.

Monitor by: keepalive

clpka

clpkhb

- When keepalive is the monitoring method, the clpkhb and clpka drivers of EXPRESSCLUSTER are required.
- The clpka and clpkhb drivers are provided by EXPRESSCLUSTER. For the supported range, refer to “Supported distributions and kernels” in the Installation Guide.
- If the clpkhb and clpka drivers cannot be used, monitoring cannot be started.

rpm the user-mode monitor resources depend on

Monitor method ipmi

ipmiutil

- When the monitoring method is ipmi, the rpm must be installed.
- If the rpm is not installed, monitoring cannot be started.

How user-mode monitor resources perform monitoring

You can select how a user-mode monitor resource monitors its target from the following:

Monitor by: softdog

When the monitoring method of the user-mode monitor resource is softdog, the OS softdog driver is used.

Monitor by: ipmi

When the monitoring method is ipmi, ipmiutil is used.

If ipmiutil is not installed, ipmiutil must be installed.

Monitor by: keepalive

When the monitoring method is keepalive, clpkhb and clpka drivers are used.

Note:
For the distributions and versions of the kernels valid for the clpkhb and clpka drivers, refer to "Supported distributions and kernels" in the *Installation Guide*.
Also check this information before applying a security patch released by the distributor to a server already in operation (kernel upgrade).

Monitor by: none

"none" is a monitoring method is used for evaluation. This only executes operations of the advanced settings of the user-mode monitor resource. Do not use this in a production environment.

Advanced settings for user-mode monitor resources

Opening/closing of a dummy file, writing to a dummy file and creating a dummy thread are the configurations that allow advance user-mode monitor resource. If any of these configurations fail, the timer will not be updated. If a configuration continues to fail for the time period set for the timeout or heartbeat timeout, the OS is reset.

Open/Close dummy file

A dummy file is created, opened, closed and then deleted at every monitoring interval repeatedly.

- When this advanced function is set and there is no free disk space, opening the dummy file fails and the OS is reset.

Write data into a dummy file

A specified size of data is written into a dummy file at every monitoring interval.

- This advanced function is not available unless opening/closing a dummy file is set.

Create dummy thread

A dummy thread is created at every monitoring interval.

User-mode monitor resource logic

The following sections describe how processes and features differ by ways of monitoring. For the shutdown monitoring, only Step 1 in each process overview is performed.

Monitor by: ipmi

- Process overview

  Following steps below from 2 to 7 are repeated.

  1. Set the IPMI timer
  2. `Open()` a dummy file
  3. Execute `write()` to the dummy file
  4. Execute `fdatasync()` to the dummy file
  5. `Close()` the dummy file
  6. Create a dummy thread
  7. Refresh the IPMI timer

     - Steps 2 to 6 of the process overview are for advanced settings. To execute these steps, you need to configure each setting.

- When a timeout does not occur (steps 2 to 7 above are performed without any problem):
  No recovery action, including a reset, is performed.
- When a timeout occurs (when any of steps 2 to 7 above is stopped or delayed):
  A reset is performed by using BMC (the server's internal management function).
- Advantages

  - BMC (the server's internal management function) is used, so the kernel space is unlikely to fail and the possibility of a successful reset is high.

- Disadvantages

  - Due to the dependency on the hardware, this method is unusable on a server that does not support IPMI or is unable to run ipmiutil.
  - This method cannot be used on a server on which ESMPRO/ServerAgent is used.
  - It might not be possible to use this method together with server monitoring software provided by another server vendor.
  - ipmiutil is not provided for some architectures.

Monitor by: softdog

◆ Process overview

Following steps below from 2 to 7 are repeated.

1. Set up softdog
2. `Open()` a dummy file
3. Execute `write()` to the dummy file
4. Execute `fdatasync()` to the dummy file
5. `Close()` the dummy file
6. Create a dummy thread
7. Refresh the softdog timer

- Steps 2 to 6 of the process overview are for advanced settings. To execute these steps, you need to configure each setting.

◆ When a timeout does not occur (steps 2 to 7 above are performed without any problem):
No recovery action, including a reset, is performed.

◆ When a timeout occurs (when any of steps 2 to 7 above is stopped or delayed):
A reset is performed by softdog.ko.

◆ Advantages

- Because it does not depend on the hardware, this method can be used if the softdog kernel module is available.
(Some distributions do not include softdog by default, so check whether softdog exists before setting it up.)

◆ Disadvantages

- Because softdog depends on the timer logic of the kernel space, a reset might not be performed if an error occurs in the kernel space.

Monitoring by: keepalive

- Process overview

  Following steps below from 2 to 7 are repeated.

  1. Set the keepalive timer
  2. `Open()` a dummy file
  3. Execute `write()` to the dummy file
  4. Execute `fdatasync()` to the dummy file
  5. `Close()` the dummy file
  6. Create a dummy thread
  7. Update the keepalive timer

  - Steps 2 to 6 of the process overview are for advanced settings. To execute these steps, you need to configure each setting.

- When a timeout does not occur (steps 2 to 7 above are performed without any problem):
  No recovery action, including a reset, is performed.
- When a timeout occurs (i.e. any of Steps 2 to 7 is stopped or delayed):
  - A reset or panic is generated by clpka.ko according to the action setting.
- Advantages
  - A panic can be specified as the action.
- Disadvantages
  - The distributions, architectures, and kernel versions (provided drivers) for which keepalive can operate are restricted.
  - Because clpka is dependent on the timer logic of the kernel space, reset may not be performed if an error occurs in the kernel space.

Checking whether ipmi can operate

To simply check for whether the server supports ipmiutil, perform the following procedure.

1. Install the downloaded ipmiutil rpm package.[2]
2. Run `/usr/sbin/wdt` or `/usr/sbin/iwdt`.
3. Check the execution result.

When the result is displayed as shown below (the result of running /usr/sbin/wdt)

(The following shows an example. The values may be different depending on the hardware.)

```
wdt ver 1.8
-- BMC version 0.8, IPMI version 1.5
wdt data: 01 01 01 00 31 17 31 17
Watchdog timer is stopped for use with BIOS FRB2. Logging
            pretimeout is 1 seconds, pre-action is None
            timeout is 593 seconds, counter is 593 seconds
            action is Hard Reset
```

ipmiutil is usable. ipmi is selectable for the monitoring method.

When the result is displayed as shown below (the result of running /usr/sbin/wdt)

```
wdt version 1.8
ipmignu_cmd timeout, after session activated
```

ipmiutil is unusable. Do not select ipmi for the monitoring method.

Used ipmi commands

For user-mode monitor resource/shutdown monitoring, the following ipmiutil command and options are used.

command	Option	When to use	
		User-mode stall monitoring	Shutdown monitoring
wdt iwdt	-e (start timer)	Upon starting	Upon starting monitoring
	-d (stop timer)	Upon stopping	Upon stopping (SIGTERM enabled)
	-r (refresh timer)	At the start/monitoring interval	Upon starting monitoring
	-t (set timeout value)	Upon changing the start/monitoring interval	Upon starting monitoring

[2] For some distributions, this is installed with the distribution. If so, the ipmi-util rpm package does not have to be installed.

Notes on user-mode monitor resources

Common notes on all the monitoring methods:

- When configuration information is created using the Builder, a user-mode monitor resource is automatically created using the softdog monitoring method.
- User-mode monitor resources with different monitoring methods can be added. A user-mode monitor resource that was automatically created using the softdog monitoring method can be deleted.
- When a user-mode monitor resource fails to activate because, for example, the softdog driver of the OS does not exist, the clpkhb or clpka driver of EXPRESSCLUSTER does not exist, or the ipmiutil rpm file has not been installed, the message "Monitor userw failed." is displayed in the alert view of the WebManager. In the tree view of the WebManager or information displayed by the clpstat command, **Normal** is displayed as the resource status and **Offline** is displayed as the server status.

Notes on monitoring by ipmi

- For notes on ipmi, see "ipmi command used" in "Displaying and changing the settings when an error is detected by a monitor resource (Common to monitor resources)".

The operation has been checked with the following combinations.

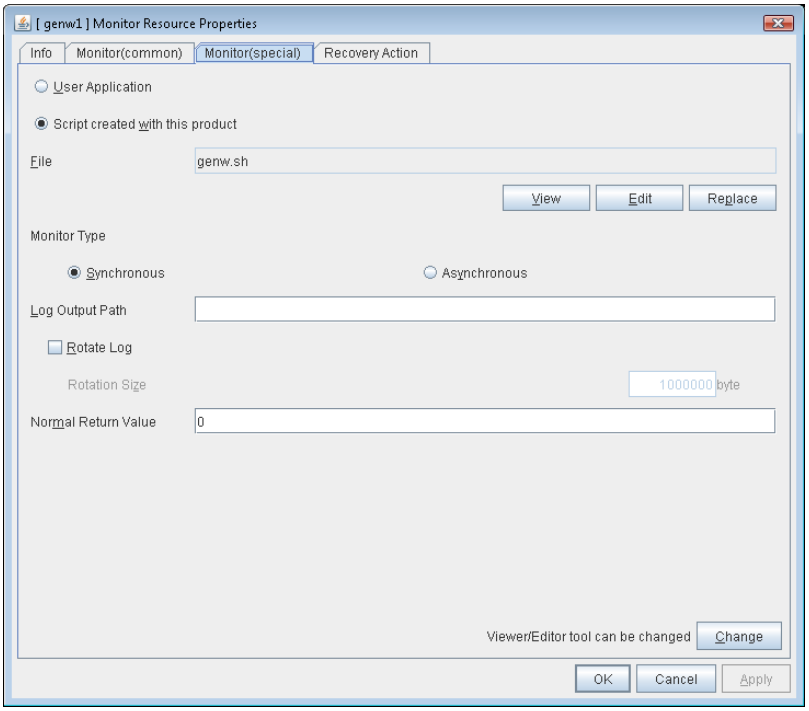
Distribution	kernel version	Version of ipmiutil	Server
Red Hat Enterprise Linux AS 5 (update1)	2.6.18-53.el5	ipmiutil-1.7.9-1.x86_64.rpm	Express5800/120Rg-1
Red Hat Enterprise Linux AS 4 (update6)	2.6.9-67.EL smp	ipmiutil-2.0.8-1.x86_64.rpm	Express5800/120Rg-1
Asianux Server 3	2.6.18-8.10AXxen	ipmiutil-1.7.9-1.x86_64.rpm	Express5800/120Rg-2
Red Hat Enterprise Linux AS 5 (update4)	2.6.18-164.el5	Ipmiutil-2.6.1-1.x86_64.rpm	Express5800/120Rf-1

Note:
When server monitoring software provided by another server vendor such as ESMPRO/ServerAgent is used, do not select IPMI as the monitoring method.
Such server monitoring software and ipmiutil both use BMC (Baseboard Management Controller) on the server, which causes a conflict and makes monitoring impossible.

Setting up custom monitor resources

Custom monitor resources monitor system by executing an arbitrary script.

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right click the target custom monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display or change the detailed settings by following the description below.



User Application

Use an executable file (executable shell script file or execution file) on the server as a script. For the file name, specify an absolute path or name of the executable file of the local disk on the server.

These executable files are not included in the configuration data of the Builder. They must be prepared on the server because they cannot be edited or uploaded by the Builder.

Script created with this product

Use a script file which is prepared by the Builder as a script. You can edit the script file with the Builder if you need. The script file is included in the configuration data.

File (within 1,023 bytes)

Specify the script to be executed (executable shell script file or execution file) when you select **User Application** with its absolute path on the local disk of the server.

View

Click here to display the script file with the editor when you select **Script created with this product**. The information edited and stored with the editor is not applied. You cannot display the script file if it is currently displayed or edited.

Edit

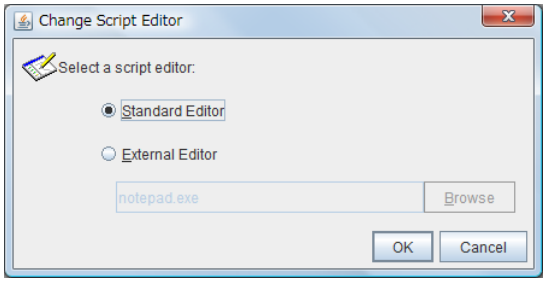
Click here to edit the script file with the editor when you select **Script created with this product**. Overwrite the script file to apply the change. If the selected script file is being viewed or edited, you cannot edit it. You cannot modify the name of the script file.

Replace

Click here to replace the content of the script file with that of the script file you selected in the file selection dialog box, when **Script created with this product** is selected. 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.

Change

Click here to display the **Change Script Editor** dialog box. You can change editor for displaying or editing a script to an arbitrary editor.



Standard Editor

Select this option to use the standard editor for editing scripts.

- Linux: vi (vi which is detected by the user's search path)
- Windows: Notepad (notepad.exe which is detected by the user's search path)

External Editor

Select here to specify an arbitrary script editor. Click Browse to specify the editor to be used.

To specify a CUI-based external editor on Linux, create a shell script.

The following is a sample shell script to run vi:

xterm -name clpedit -title "Cluster Builder" -n "Cluster Builder" -e vi "$1"

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.

Log Output Path (within 1,023 bytes)

Specify log output path for the script of custom monitor resource.

Pay careful attention to the free space in the file system because the log is output without any limitations when the file name is specified and the Rotate Log check box is unchecked.

When the **Rotate Log** check box is checked, output log files are rotated.

Rotate Log

Turn this off to output execution logs of scripts and executable files with no limit on the file size. Turn it on to rotate and output the logs. In addition, note the following.

Enter the log path in 1009 bytes or less in Log Output Path. If the path exceeds 1009 bytes, the logs are not output.

The log file name must be 31 bytes or less. If the name exceeded 32 bytes, the logs are not output.

If some custom monitor resouces are configured to rotate logs, and the log file names are the same but the log paths are different, the Log Rotate Size may be incorrect.
(ex. /home/foo01/log/genw.log, /home/foo02/log/genw.log)

Rotation Size (1 to 9999999)

Specify a file size for rotating files when the Rotate Log check box is checked.

The log files that are rotated and output are configured as described below.

File name	Description
Log Output Path specified_file_name	Latest log file.
Log Output Path specified_file_name.pre	Former log file that has been rotated.

Normal Return Value (within 1,023 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

Notes on custom monitor resources

When the monitor type is **Asynchronous**, and the monitoring retry count is set to 1 or more, monitoring cannot be performed correctly. When you set the monitor type to **Asynchronous**, also specify 0 as the monitoring retry count.

EXPRESSCLUSTER X 3.0.4-1 and earlier versions allowed the monitor resource monitoring setting **Collect the dump file of the monitor process at timeout occurrence** to be configured, but this function did not provide sufficient useful information for custom monitor resources. Therefore, this function has been dropped from EXPRESSCLUSTER X 3.1 and later versions from those configurable for custom monitor resources.
To use an alternative logging function, specify **Log Output Path** for custom monitor resources to output logs.

When Script Log Rotate is enabled, the logs are written to the specified file after the script finishes.
If the monitor type is set to **Asynchronous**, the script does not finish and the logs are not written. Therefore, it is recommended that you disable Script Log Rotate. If the monitor type is set to **Synchronous**, redirect the standard output of the resident process started in the start script to /dev/null.

Monitoring by custom monitor resources

Custom monitor resources monitor system by an arbitrary script.

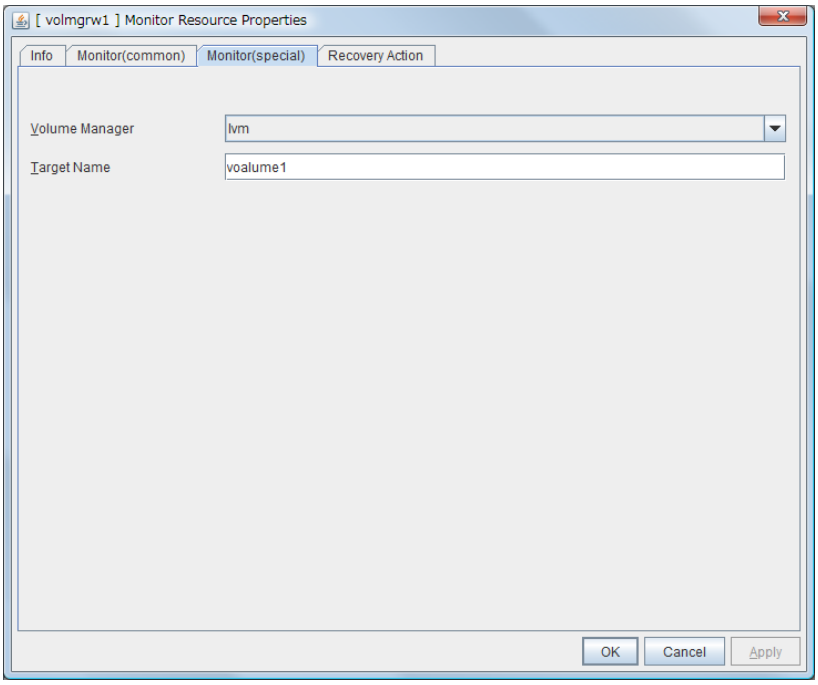
When **Monitor Type** is **Synchronous**, custom monitor resources regularly run a script and detect errors from its error code.

When **Monitor Type** is **Asynchronous**, custom monitor resources run a script upon start monitoring and detect errors if the script process disappears.

Setting up volume manager monitor resources

Volume manager monitor resources monitor logical disks managed by the volume manager.

1. Click the **Monitors** icon in the tree view on the left side of the Builder window.
2. The list of monitor resources is shown in the table view on the right side of the screen. Right-click the target volume manager monitor resource name, and then click the **Monitor(special)** tab in **Property**.
3. On the **Monitor(special)** tab, you can display or change detailed settings by following the description below.



Volume Manager

Specify the type of volume manager that manages the monitor target logical disks. The following volume managers are supported:

- lvm (LVM volume group)
- vxvm (VxVM daemon)

Target Name(within 1023 bytes)

Specify the name of the monitor target in the <VG name> format (only the target name is used).

When the volume manager is lvm, it's possible to control multiple volumes together.

More than one volume is delimited with an one-byte space.

When the volume manager is vxvm, this setting need not be entered.

Notes on volume manager monitor resources

When the volume manager is VxVM, volmgrw uses the daemon monitoring method. Therefore, registering multiple items in a single cluster is meaningless.

When specifying VxVM as the volume manager, do not specify the recovery target.

Volume manager monitor resources are configured with their default settings; change the settings as needed.

Monitoring by volume manager monitor resources

The monitoring method used by volume manager monitor resources depends on the type of volume manager that manages the target logical disks.

The following volume managers are supported:

- lvm (LVM volume group)
- vxvm (VxVM daemon)

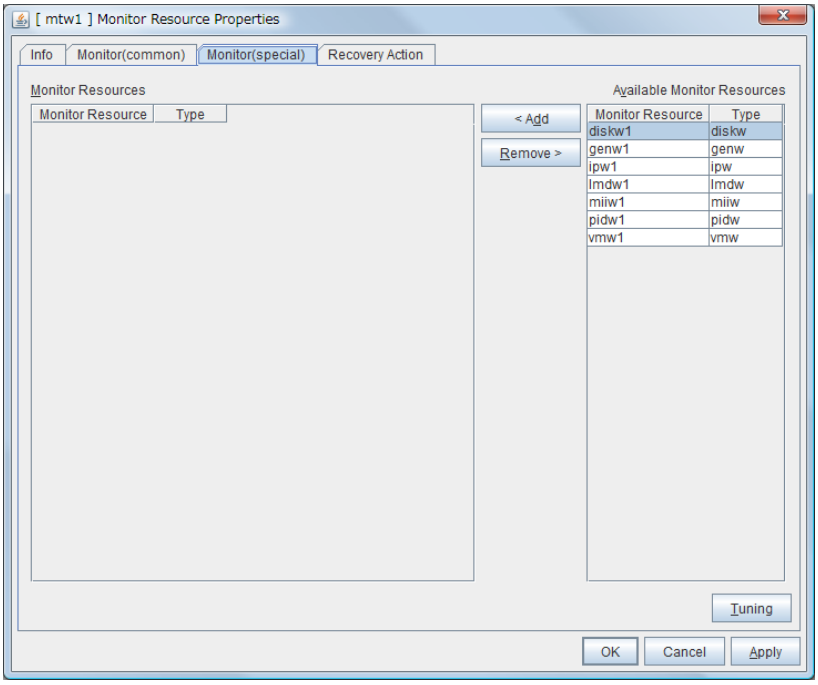
Setting up multi target monitor resources

The multi target monitor resource monitors more than one monitor resources.

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.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right click the target multi target monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Add

Click **Add** to add a selected monitor resource to **Monitor Resources**.

Remove

Click **Remove** to delete a selected monitor resource from **Monitor Resources**.

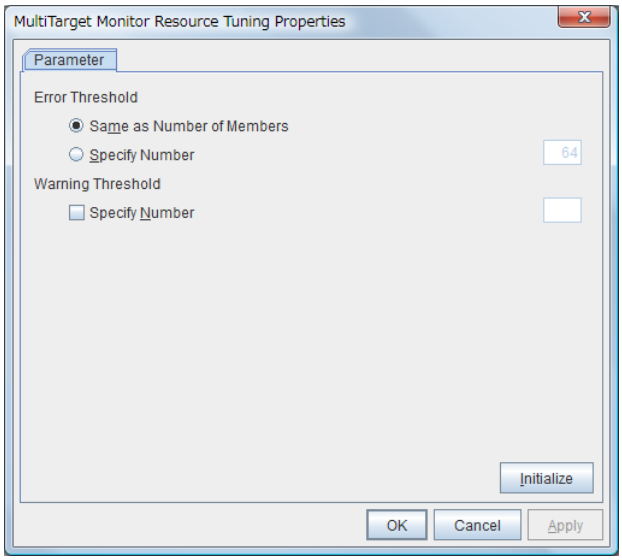
Notes on multi target monitor resources

The multi target monitor resources regard the offline status of registered monitor resources as being an error. For this reason, for a monitor resource that performs monitoring when the target is active is registered, the multi target monitor resource might detect an error even when an error is not detected by the monitor resource. Do not, therefore, register monitor resources that perform monitoring when the target is active.

Tuning a multi target monitor resource

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the target multi target monitor resource name.
3. Click **Properties**, and then click **Parameters**. Click **Tuning** on the **Monitor(special)** tab. The **MultiTarget Monitor Resource Tuning Properties** dialog box is displayed.
4. The settings of multi target monitor resource can be displayed and changed by following the description below.

Parameter tab



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.”

Specify how many of the monitor resources specified under the multi target monitor resource need to have the "Error" or "Offline" status before the status of the multi target monitor resource is judged to be "Error."

This can be set when **Specify Number** is selected for **Error Threshold**.

Warning Threshold

- When 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 cleared:

Multi target monitor resources do not display an alert.

Initialize

This operation is used to return the value to the default value. By selecting **Initialize**, initial values are configured for all items.

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

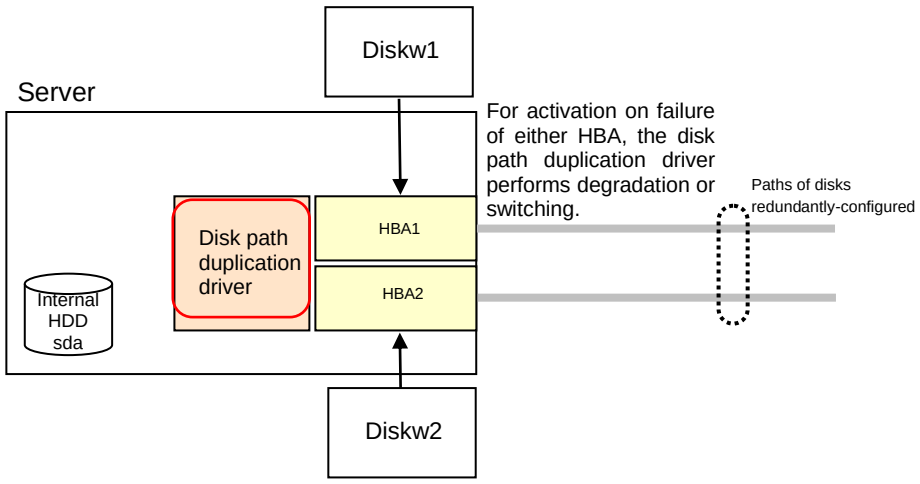
The table below describes status of a multi target monitor resource:

Multi target monitor resource status		**Monitor resource1 status**		
		normal (normal)	error (error)	Already stopped (offline)
Monitor resource2 Status:	normal (normal)	normal (normal)	caution (caution)	caution (caution)
	error (error)	caution (caution)	error (error)	error (error)
	Already stopped (offline)	caution (caution)	error (error)	normal (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.

Example multi target monitor resource configuration

◆ Example of the disk path duplication driver usage
The status can be an error only if disk devices (such as /dev/sdb and /dev/sdc) fail at the same time.



- Monitor **resources** to be registered with the multi target monitor resources (mtw1):
  - diskw1
  - diskw2
- Error Threshold and **Warning** Threshold of multi target monitor resource (mtw1)
  - Error threshold 2
  - Warning threshold 0
- Detailed settings of the monitor resource to be registered with the multi target monitor resource (mtw1)
  - Disk monitor resource (diskw1)

Monitored device name	/dev/sdb
Reactivation threshold	0
Failover threshold	0
Final action	No Operation

  - Disk monitor resource (diskw2)

Monitored device name	/dev/sdc
Reactivation threshold	0
Failover threshold	0
Final action	No Operation

◆ With the settings above, even if either of diskw1 and diskw2, which are registered as monitor resources of the multi target monitor resource detects an error, no actions for the monitor resource having the error are taken.

◆ Actions for an error set to the multi target monitor resource are executed when the status of both diskw1 and diskw2 become error, or when the status of two monitor resources become error and offline.

Setting up software RAID monitor resources

The software RAID monitor resource is to monitor software RAID devices.

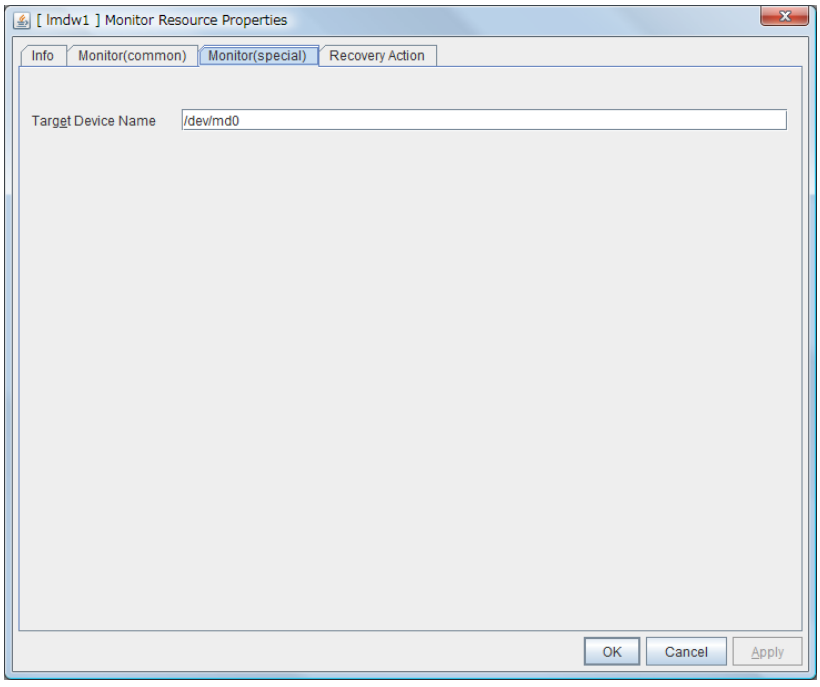
Monitoring by software RAID monitor resources

The software RAID monitor resource is used to monitor software RAID devices by using the md driver. If either disk is faulty and software RAID is degraded, WARNING is issued.

Note) If both disks are faulty, any error cannot be detected; restore the disks when a notification about degradation is posted.

Displaying and changing details of a software RAID monitor resource

1. Click the **Monitors** icon on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target software RAID monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



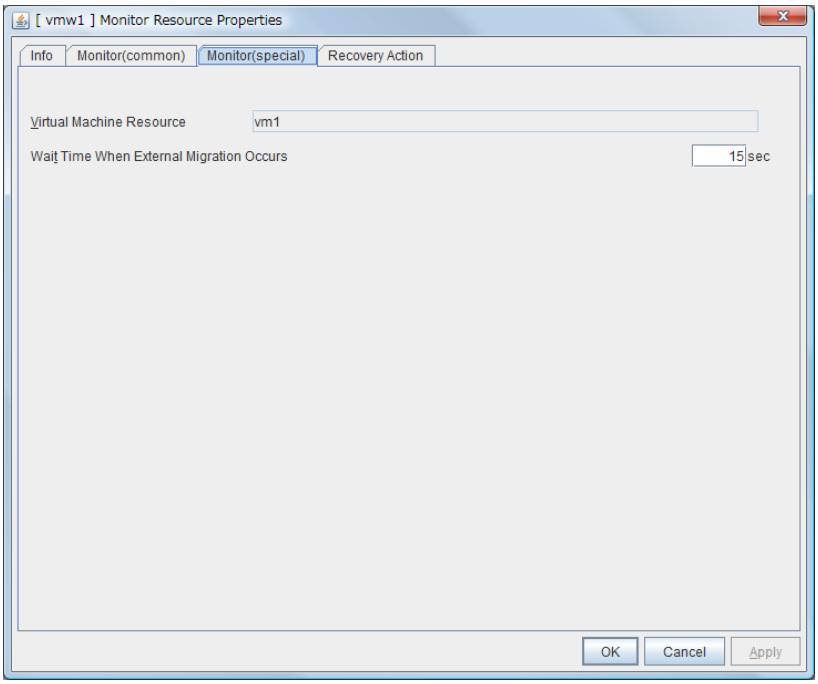
Target Device Name (within 1,023 bytes)

Specify the name of the md device to be monitored.

Setting up VM monitor resources

The VM monitor resource is used to check whether the virtual machine is alive.

1. Click the **Monitor Resource** icon in the tree view on the left side of the Builder window.
2. The list of monitor resources is shown in the table view on the right side of the screen. Right-click the target VM monitor resource name, and then click the **Monitor(special)** tab in **Property**.
3. On the **Monitor(special)** tab, you can display or change detailed settings by following the description below.



Wait Time for External Migration

Specify the time to wait for the completion of the migration.

Notes on VM monitor resources

- This resource is automatically registered when a virtual machine resource is added.
- Concerning the VM versions checked for the operation, refer to "Application supported by the monitoring options" in the Installation Guide.
- The times counter of the recovery action kept by the monitor resource is not reset even though the virtual machine monitor resource recovery is detected while recovery action is in transit, or after all the recovery action have completed. Execute either one of the following procedures when you want to reset the times counter of the recovery action.
  - Reset the times counter of the recovery action by the clpmonctrl command.
  - Execute cluster stop/start by clpcl command or WebManager.

Monitoring by VM monitor resources

The VM monitor resource performs monitoring as described below.

When the virtual machine is vSphere

VMware vSphere API is used to monitor the virtual machine.

As a result of monitoring, the following is considered as an error:

(1) The VM status is POWEROFF/SHUTDOWN/SUSPENDED

(2) The VM status could not be obtained

When the virtual machine is Xenserver

A general virtualization library is used to monitor the virtual machine.

As a result of monitoring, the following is considered as an error:

(1) The VM status is HALTED/PAUSED/SUSPENDED

(2) The VM status could not be obtained

When the virtual machine is Kvm

A general virtualization library is used to monitor the virtual machine.

As a result of monitoring, the following is considered as an error:

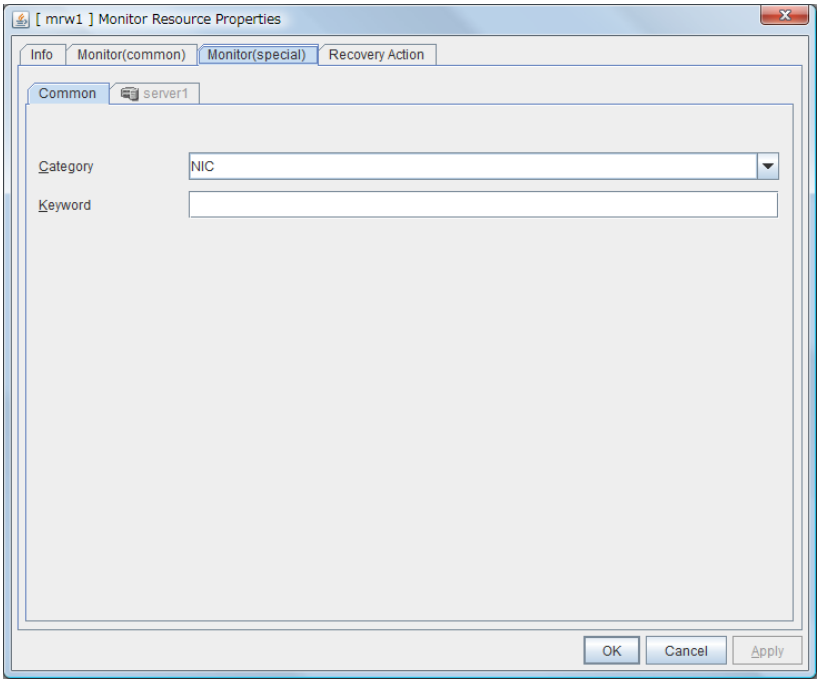
(1) The VM status is BLOCKED/SHUTDOWN/PAUSED/SHUTOFF/CRASHED/NOSTATE

(2) The VM status could not be obtained

Setting up message receive monitor resources

Message receive monitor resources are passive monitors. They do not perform monitoring by themselves.
When an error message is received from an outside of EXPRESSCLUSTER, the message receive monitor resources change their status and perform recovery from the error.

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the target message receive monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



For **Category** and **Keyword**, specify a keyword passed using the -k parameter of the clprexec command. The keyword can be omitted.

Category (within 32 bytes)

Specify a monitor type.
You can select the default character string from the list box or specify any character string.

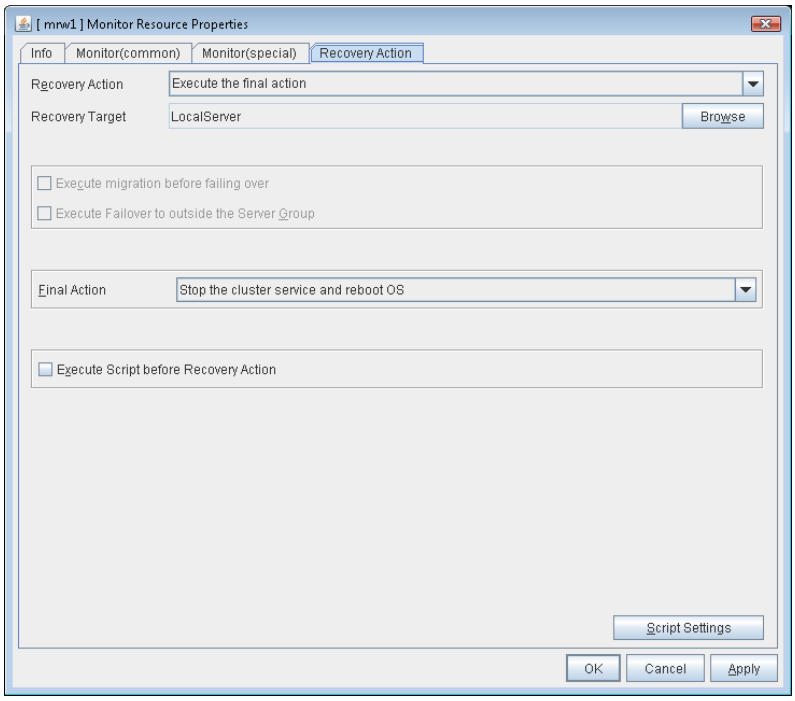
Keyword (within 1,023 bytes)

Specify a keyword passed using the -k parameter of the clprexec command.

Setting up how the message receive monitor resource is to act upon error detection

Specify the recovery target and the action upon detecting an error. For message receive monitor resources, select **Reactivate Recovery Target** or **Final Action** as the action to take when an error is detected. However, recovery will not occur if the recovery target is not activated.

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is shown in the table view on the right side of the screen. Right-click the target monitor resource name, and then click the Recovery Action tab in Property.
3. On the Recovery Action tab, you can display or change the monitoring settings by following the description below.



Recovery Action

Select the action to take when a monitor error is detected.

- **Executing the recovery script**
  Execute the recovery script when a monitor error is detected.
- **Restart the recovery target**
  Restart the group or group resource selected as the recovery target when a monitor error is detected.
- **Execute the final action**
  Execute the selected final action when a monitor error is detected.

Execute Script before Recovery Action

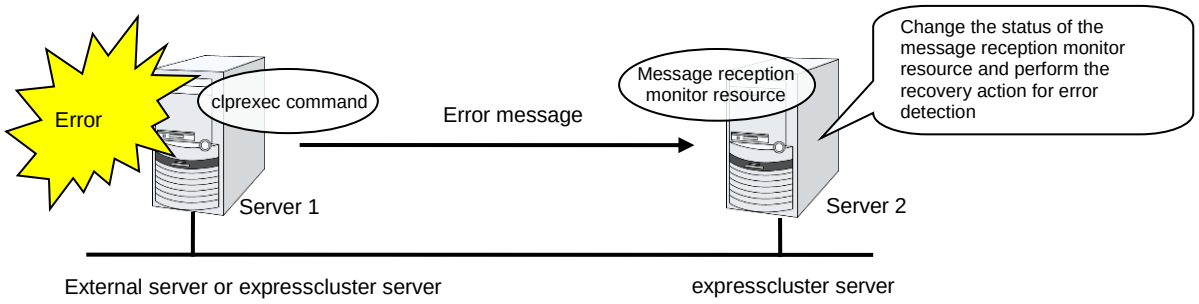
Executes the script before the operation performed upon error detection selected as the recovery action.

- When selected
  A script/command is executed before reactivation. To configure the script/command setting, click Settings.
- When cleared
  Any script/command is not executed.

* For the settings of the items other than those mentioned above, see “2. Setting up the recovery processing” in “Common settings for monitor resources” in "Chapter 5 Monitor resource details”.

Monitoring by message reception 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.



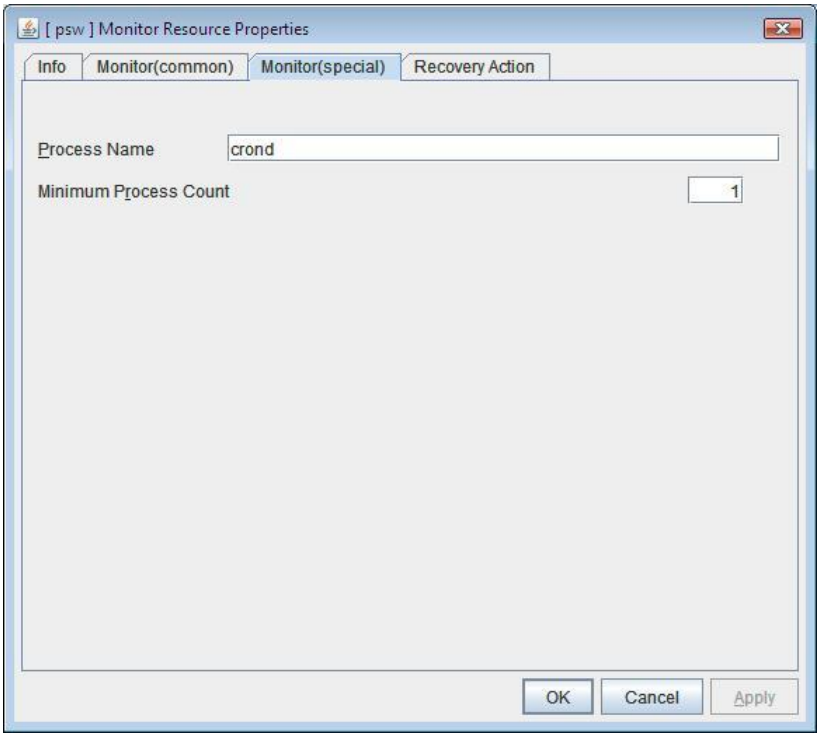
Notes on message reception monitor resources

- If a message receive monitor resource is paused when an error message is received from outside, error correction is not performed.
- If an error message is received from outside, the status of the message receive monitor resource becomes "error". The error status of the message receive monitor resource is not automatically restored to "normal". To restore the status to normal, use the clprexec command. For details about the clprexec command, see Chapter 2, "EXPRESSCLUSTER X SingleServerSafe command reference" in the *Operation 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.

Setting up Process Name monitor resources

Process name monitor resources monitor the process of specified processes. Process stalls cannot be detected.

1. Click the **Monitors** icon on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is shown in the table view on the right side of the screen. Right-click the target monitor resource name, and then click the **Monitor(special)** tab in **Properties**.
3. On the **Monitor(special)** tab, display or change the advanced settings by following the instructions below.



Process name (within 1,023 bytes)

Set the name of the target process. The process name can be obtained by using the ps(1) command.

Wild cards can be used to specify a process name by using one of the following three patterns. No other wild card pattern is permitted.

[prefix search] <string included in the process name>*

[suffix search] *<string included in the process name>

[partial search] *<string included in the process name>*

Minimum Process Count (1 to 999)

Set the process count to be monitored for the monitor target process. If the number of processes having the specified monitor target process name falls short of the set value, an error is recognized.

Notes on process name monitor resources

If you set 1 for **Minimum Process Count**, and if there are two or more processes having the process name specified for the monitor target, only one process is selected under the following conditions and is subject to monitoring.

1. When the processes are in a parent-child relationship, the parent process is monitored.
2. When the processes are not in a parent-child relationship, the process having the earliest activation time is monitored.
3. When the processes are not in a parent-child relationship and their activation times are the same, the process having the lowest process ID is monitored.

If monitoring of the number of started processes is performed when there are multiple processes with the same name, specify the process count to be monitored for **Minimum Process Count**. If the number of processes with the same name falls short of the specified minimum count, an error is recognized. You can set 1 to 999 for **Minimum Process Count**. If you set 1, only one process is selected for monitoring.

Up to 1023 bytes can be specified for the monitor target process name. To specify a monitor target process with a name that exceeds 1023 bytes, use a wildcard (*).

If the name of the target process is 1024 bytes or longer, only the first 1023 bytes can be recognized as the process name. If you use a wild card (such as *) to specify a process name, specify a string containing the first 1023 or fewer bytes.

If the name of the target process is long, the latter part of the process name is omitted and output to the log.

If the name of the target process includes double quotations(“”) or a comma (,), the process name might not be correctly output to an alert message.

Check the monitor target process name which is actually running by ps(1) command, etc, and specify the monitor target process name.

execution result

```
# ps -eaf
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 Sep12 ?        00:00:00 init [5]
  :
root        5314       1  0 Sep12 ?        00:00:00 /usr/sbin/acpid
root        5325       1  0 Sep12 ?        00:00:00 /usr/sbin/sshd
htt         5481       1  0 Sep12 ?        00:00:00 /usr/sbin/htt -retryonerror 0
  :
```

From the above command result,"/usr/sbin/htt –retryonerror 0" is specified as monitor target process name in the case of monitoring "/usr/sbin/htt".

The process name specified for the name of the target process specifies the target process, using the process arguments as part of the process name. To specify the name of the target process, specify the process name containing the arguments. To monitor only the process name with the arguments excluded, specify it with the wildcard (*) using right truncation or partial match excluding the arguments.

How process name monitor resources perform monitoring

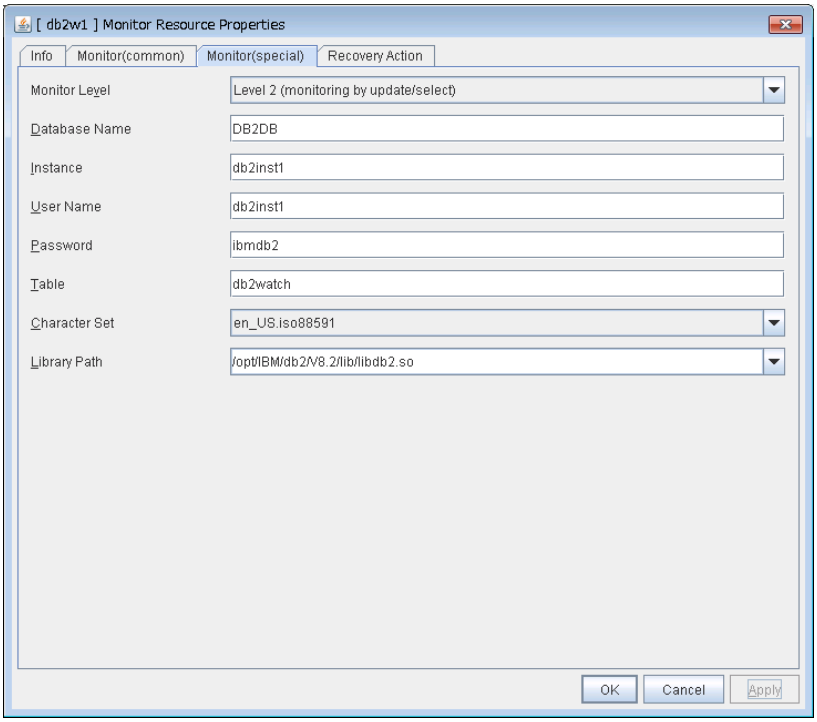
The process name monitor resource monitors a process having the specified process name. If **Minimum Process Count** is set to 1, the process ID is identified from the process name and the deletion of the process ID is treated as an error. Process stalls cannot be detected.

If **Minimum Process Count** is set to a value greater than 1, the number of processes that have the specified process name are monitored. The number of processes to be monitored is calculated using the process name, and if the number falls below the minimum count, an error is recognized. Process stalls cannot be detected.

Setting up DB2 monitor resources

The DB2 monitor resource is used to monitor a DB2 database operating on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target DB2 monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (within 255 bytes)

Specify the database name to be monitored. Specifying this item cannot be omitted.

Default value: None

Instance (within 255bytes)

Specify the database instance name. Specifying this item cannot be omitted.

Default value: db2inst1

User Name (within 255 bytes)

Specify the user name to log on to the database. Specifying this item cannot be omitted.

Specify a DB2 user accessible to the specified database.

Default value: db2inst1

Password (within 255 bytes)

Specify the password to log on to the database. Specifying this item cannot be omitted.

Default value: ibmdb2

Table (within 255 bytes)

Specify the name of a monitor table created on the database. Specifying this item cannot be omitted. Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Be sure to set the name different from the reserved word in SQL statements. Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database specifications.

Default value: db2watch

Character Set

Specify the character set of DB2. Specifying this item cannot be omitted.

Default value: None

Library Path (within 1,023 bytes)

Specify the home path to DB2. Specifying this item cannot be omitted.

Default value: /opt/IBM/db2/V8.2/lib/libdb2.so

Note on DB2 monitor resources

For the supported versions of DB2, see ”Software Applications supported by monitoring options” of “Software” in Chapter 3, “Installation requirements for EXPRESSCLUSTER” in the Getting Started Guide.

This monitoring resource monitors DB2, using the CLI library of DB2. For this reason, it is required to execute “source instance user home/sqllib/db2profile” as root user. Write this in a start script.

To monitor a DB2 database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the DB2 database to become accessible after the VM resource is activated for Wait Time to Start Monitoring. Also, set up the DB2 client on the host OS side, where monitor resources run, and register the database on the virtual machine to the database node directory.

If the code page of the database and the one of this monitor resource differ, this monitor resource cannot access to the DB2 database. Set an appropriate character code as necessary.

To check the code page of database, execute “db2 get db cfg for Database_name.” For details, see DB2 manual.

If values of database name, instance name, user name and password specified by a parameter differ from the DB2 environment for monitoring, DB2 cannot be monitored. Error message is displayed. Check the environment.

If “Level 1” or “Level 2” is selected as a monitor level described in the next subsection “How DB2 monitor resources perform monitoring”, monitor tables must be created manually beforehand.
A monitor error occurs if there is no monitor table at the start of monitoring in “Level 1”.
If there is no monitor table at the start of monitoring in “Level 2”, EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the WebManager alert view does not have the monitor table is displayed.
The load on the monitor at “Level 3” is higher than that at “Level 1” and “Level 2” because the monitor in “Level 3” creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Required
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named db2watch)
sql> create table <user_name>.db2watch (num int not null primary key)
sql> insert into db2watch values(0)
sql> commit

Use EXPRESSCLUSTER command
clp_db2w --createtable -n <DB2_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_db2w --deletetable -n <DB2_monitor_resource_name>

How DB2 monitor resources perform monitoring

DB2 monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

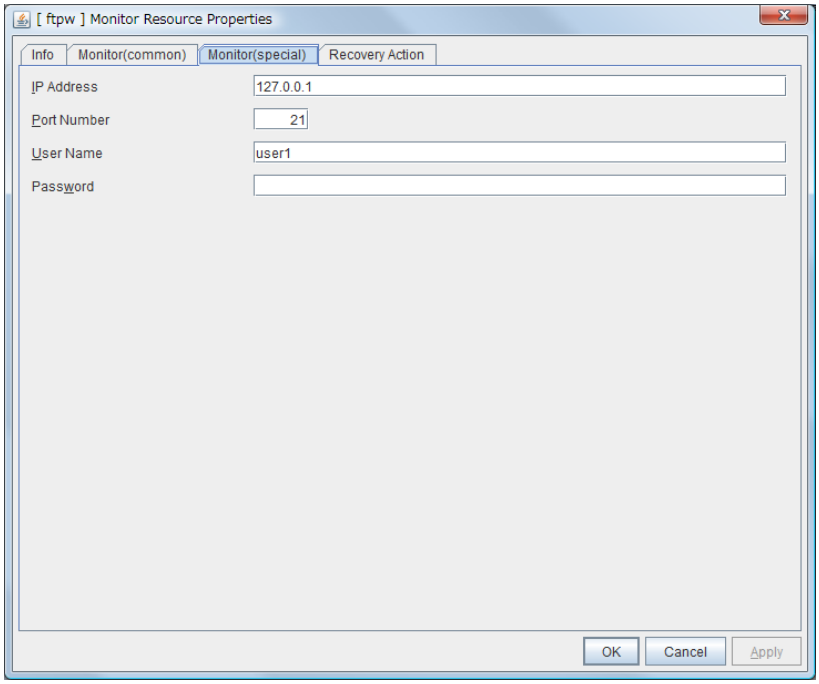
  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

Setting up FTP monitor resources

The FTP monitor resource is to monitor the FTP service running on a 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.

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right click the target FTP monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



IP Address (within 79 bytes)

Specify the IP address of the FTP server to be monitored. Specifying this item cannot be omitted. If it is multi-directional standby server, specify FIP.

Usually, the FTP server running on the local server is connected, thus the loopback address (127.0.0.1) is to be configured. If accessible addresses are limited by the FTP server settings, specify an accessible address (e.g., floating IP address). To monitor an FTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1 to 65,535)

Specify the FTP port number to be monitored. Specifying this item cannot be omitted.

Default value: 21

User Name (within 255 bytes)

Specify the user name to log on to FTP.

Default value: None

Password (Within 255 bytes)

Specify the password to log on to FTP.

Default value: None

Notes on FTP monitor resources

Specify the EXEC resource that activates FTP for the target. 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.**

To monitor an FTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the FTP server to become accessible after the VM resource is activated for **Wait Time to Start Monitorin**g.

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.

Monitoring by FTP monitor resources

FTP monitor resources monitor the following:

FTP monitor resources connect to the FTP server and execute the command for acquiring the file list.

As a result of monitoring, the following is considered as an error:

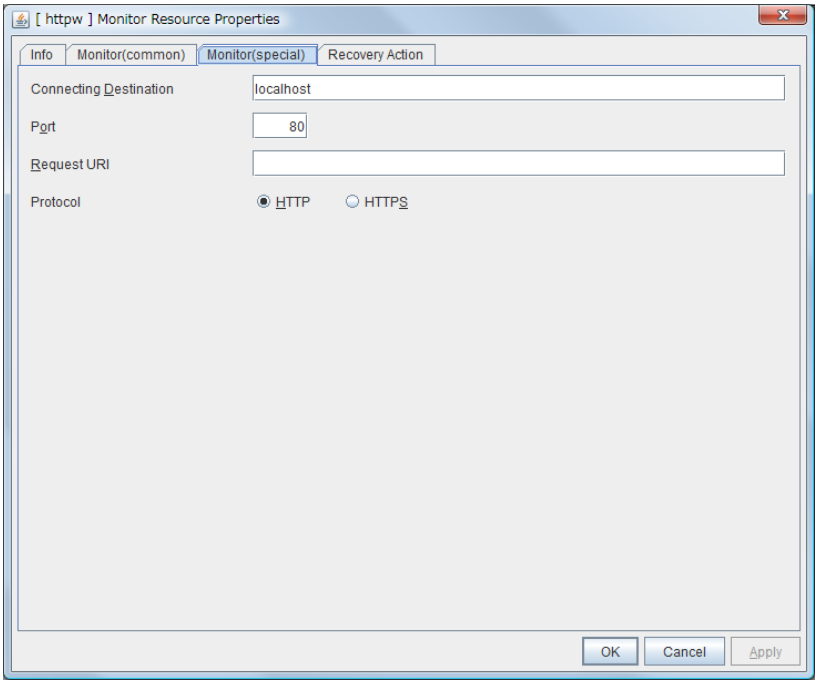
(1) When connection to the FTP service fails.

(2) When an error is notified as a response to the FTP command.

Setting up HTTP monitor resources

The HTTP monitor resource is to monitor the HTTP daemon running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target HTTP monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Connecting Destination (within 255 bytes)

Specify the name of the HTTP server to be monitored. Specifying this item cannot be omitted.
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. To monitor an HTTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: localhost

Port Number (1 to 65,535)

You must specify the port number of the HTTP to be monitored. Specifying this item cannot be omitted.

Default value: 80 (HTTP)
443 (HTTPS)

Request URI (within 255 bytes)

Configure the Request URI (e.g, "/index.html").

Default value: None

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.

Default value: HTTP

Notes on HTTP monitor resources

Concerning the HTTP versions checked for the operation, refer to "Application supported by the monitoring options" in the *Installation Guide*.

To monitor an HTTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the HTTP server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

HTTP monitor resource does not support the client authentication.

Monitoring by HTTP monitor resources

HTTP monitor resources monitor the following:

A connection is made with the HTTP daemon on the server and the HEAD request is issued to monitor the HTTP daemon.

As a result of monitoring, the following is considered as an error:

(1) An error is posted for the connection with the HTTP daemon

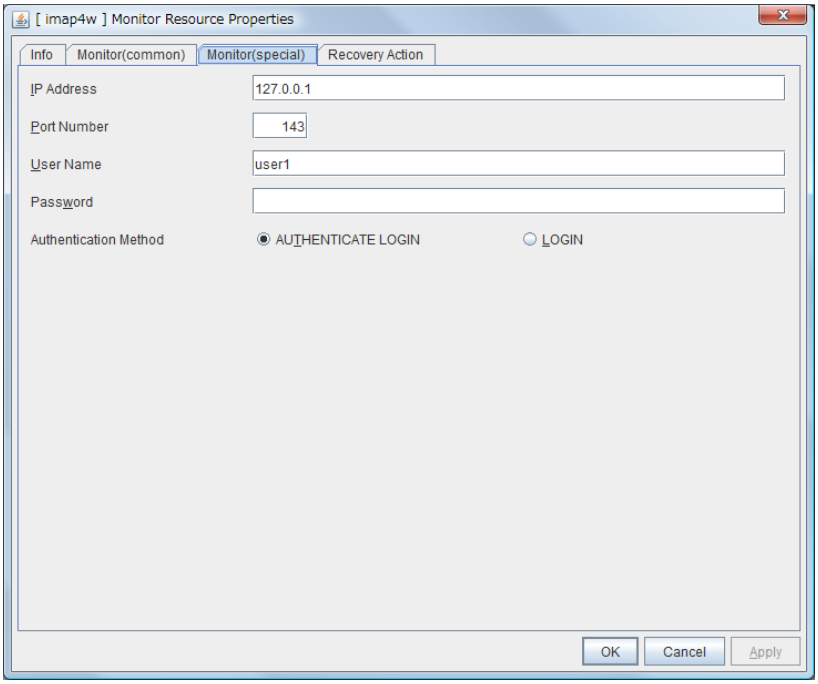
(2) The response message to the HEAD request issued does not begin with "HTTP/"

(3) The status code of the response to the HEAD request issued is 400 to 499 or 500 to 599 (when a non-predefined URI is specified for the Request URI)

Setting up 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.

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target IMAP4 monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



IP Address (within 79 bytes)

Specify the IP address of the IMAP4 server to be monitored. Specifying this item cannot be omitted. If it is multi-directional standby server, specify FIP.

Usually, specify the loopback address (127.0.0.1) to connect to the IMAP4 server that runs on the local server. If the addresses for which connection is possible are limited by IMAP4 server settings, specify an address for which connection is possible. To monitor an IMAP4 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1 to 65,535)

Specify the port number of the IMAP4 to be monitored. Specifying this item cannot be omitted.

Default value: 143

User Name (within 255 bytes)

Specify the user name to log on to IMAP4.

Default value: None

Password (within 255 bytes)

Specify the password to log on to IMAP4. Click **Change** and enter the password in the dialog box.

Default value: None

Authority 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.

Notes on IMAP4 monitor resources

For the target to be monitored, specify the EXEC resource that starts the IMAP4 server. Monitoring starts after the target resource is activated. However, if the IMAP4 server cannot be started immediately after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

To monitor an IMAP4 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the IMAP4 server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

The IMAP4 server might output an operation log or other data for each monitoring operation. If this needs to be adjusted, specify the IMAP4 server settings as appropriate.

Monitoring by IMAP4 monitor resources

IMAP4 monitor resources monitor the following:

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:

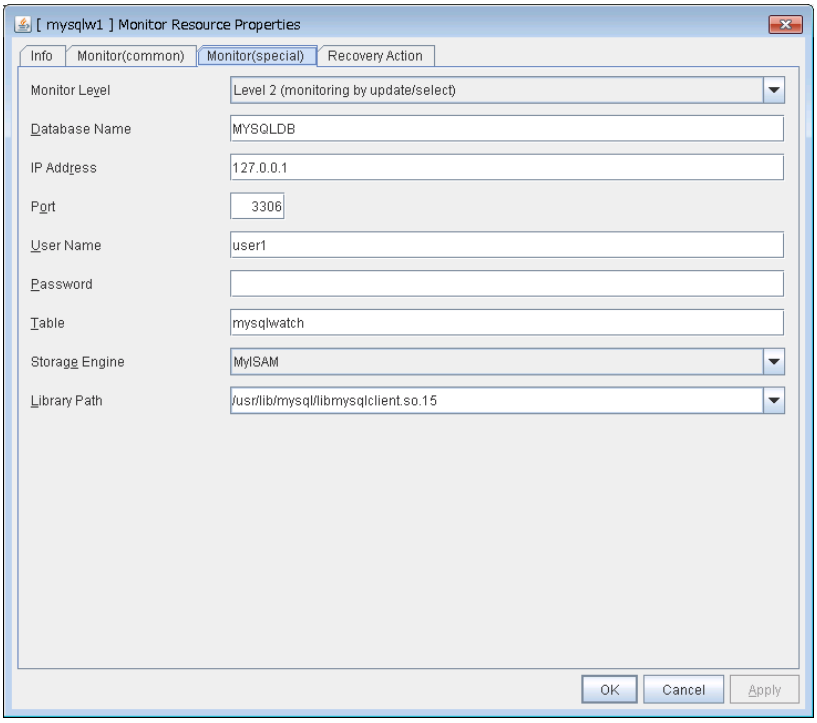
(1) When connection to the IMAP4 server fails.

(2) When an error is notified as a response to the command.

Setting up MySQL monitor resources

MySQL monitor resource monitors MySQL database that operates on servers.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the target MySQL monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (within 255 bytes)

Specify the database name to be monitored. Specifying this item cannot be omitted.

Default value: None

IP Address (within 79 bytes)

Specify the IP address of the database server to be monitored. Specifying this item cannot be omitted.

Usually, a connection is made with the MySQL server running on the local server, thus the loopback address (127.0.0.1) is to be configured. If a MySQL database running on a guest OS of a virtual machine controlled by a VM resource is monitored, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port (1 to 65,535)

Specify the port number for connection. Specifying this item cannot be omitted.

Default value: 3,306

User Name (within 255 bytes)

Specify the user name to log on to the database. Specifying this item cannot be omitted.

Specify the MySQL user who can access the specified database.

Default value: None

Password (within 255 bytes)

Specify the password to log on to the database.

Default value: None

Table (within 255 bytes)

Specify the name of a monitor table created on the database. Specifying this item cannot be omitted. 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: mysqlwatch

Storage Engine

Specify the storage engine to create monitoring tables. Specifying this item cannot be omitted.

Default value: MyISAM

Library Path (within 1,023 bytes)

Specify the library path to MySQL. Specifying this item cannot be omitted.

Default value: /usr/lib/mysql/libmysqlclient.so.15

Note on MySQL monitor resources

For the supported versions of MySQL, see ”Software Applications supported by monitoring options” in Chapter 3, “Installation requirements for EXPRESSCLUSTER” in the Getting Started Guide.

This monitor resource monitors MySQL using the libmysqlclient library of MySQL.

If this monitor resource fails, check that “libmysqlclient.so.xx” exists in the installation directory of the MySQL library.

To monitor a MySQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the MySQL database to become accessible after the VM resource is activated for Wait Time to Start Monitoring.

If a value specified by a parameter differs from the MySQL environment for monitoring, an error message is displayed on the WebManager alert view. Check the environment.

If “Level 1” or “Level 2” is selected as a monitor level described in the next subsection “How MySQL monitor resources perform monitoring”, monitor tables must be created manually beforehand.
A monitor error occurs if there is no monitor table at the start of monitoring in “Level 1”.
If there is no monitor table at the start of monitoring in “Level 2”, EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the WebManager alert view does not have the monitor table is displayed.
The load on the monitor at “Level 3” is higher than that at “Level 1” and “Level 2” because the monitor in “Level 3” creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Required
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named mysqlwatch)
sql> create table mysqlwatch (num int not null primary key) ENGINE=<engine>;
sql> insert into mysqlwatch values(0);
sql> commit;

Use EXPRESSCLUSTER commands
clp_mysqlw --createtable -n <MySQL_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_mysqlw --deletetable -n <MySQL_monitor_resource_name>

How MySQL monitor resources perform monitoring

MySQL monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

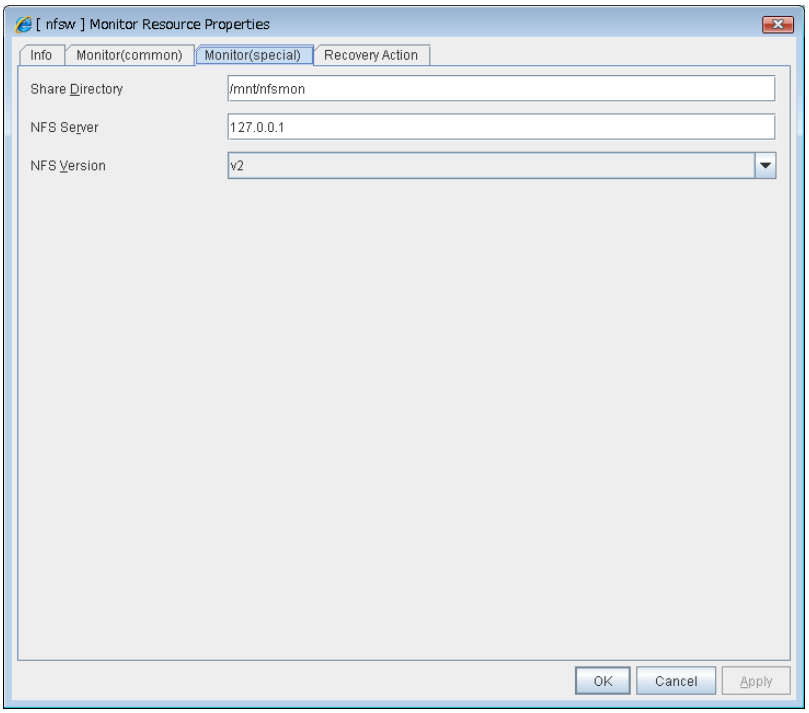
  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

Setting up NFS monitor resources

NFS monitor resource monitors NFS file server that operates on servers.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the target NFS monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Share Directory (within 1,023 bytes)

Specify a directory for sharing files. Specifying this item cannot be omitted.

Default value: None

NFS Server (within 79 bytes)

Specify an IP address of the server that monitors NFS. Specifying this item cannot be omitted.

Usually, a connection is made with the NFS file server running on the local server, thus the loopback address (127.0.0.1) is to be configured. If an NFS file server running on a guest OS of a virtual machine controlled by a VM resource is monitored, specify the IP address of the virtual machine.

Default value: 127.0.0.1

NFS Version

Select one NFS version for NFS monitoring, from the following choices. Be careful to set this NFS version. In RHEL 7, the NFS version v2 is not supported.

- v2

  Monitors NFS version v2.

- v3

  Monitors NFS version v3.

- v4

  Monitors NFS version v4.

Default value: v2

System requirements for NFS monitor resource

The use of NFS monitor resources requires that the following already be started:

<For Red Hat Enterprise Linux 5 >

- nfs
- portmap
- nfslock (unnecessary for NFS v4)

< For Red Hat Enterprise Linux 6,7 >

- nfs
- rpcbind
- nfslock (unnecessary for NFS v4)

Notes on NFS monitor resources

Concerning the NFS versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

Specify the exports file for the shared directory to be monitored to enable the connection from a local server.

To monitor an NFS file server running on a guest OS of a virtual machine controlled by a VM resource, specify the VM resource for the target of monitoring and set **Wait Time to Start Monitoring** with sufficient time to wait the NFS file server to be connectable after VM resource activation.

It is handled as an error that the deletion of nfsd with the version specified for **NFS version** of the **Monitor(special)** tab and `mountd` corresponding the nfsd is detected. The correspondence between nfsd vesions and `mountd` versions is as follows.

nfsd version	mountd version
v2 (udp)	v1 (tcp) or v2 (tcp)
v3 (udp)	v3 (tcp)
v4 (tcp)	-

Monitoring by NFS monitor resources

NFS monitor resource monitors the following:

Connect to the NFS server and run NFS test command.

As a result of monitoring, the following is considered as an error:

<For Red Hat Enterprise Linux 5 >

(1) Response to the NFS service request is invalid

(2) mountd is deleted (excluding NFS v4)

(3) nfsd is deleted

(4) The portmap service is stopped

(5) The export area is deleted (excluding NFS v4)

<For Red Hat Enterprise Linux 6,7>

(1) Response to the NFS service request is invalid

(2) mountd is deleted (excluding NFS v4)

(3) nfsd is deleted

(4) The rpcbind service is stopped

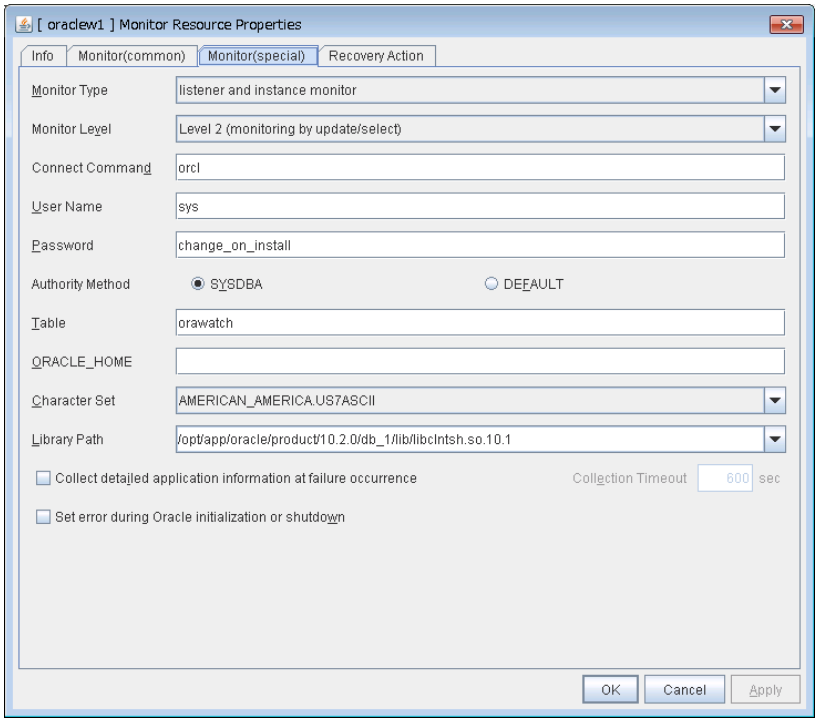
(5) The export area is deleted (excluding NFS v4)

When an error is repeated the number of times set to retry count, it is considered as NFS error.

Setting up Oracle monitor resources

Oracle monitor resource monitors Oracle database that operates on servers.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target Oracle monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Monitor Type

Select the Oracle features to be monitored.

- Monitor Listener and Instance (default)

  According to the specified monitor level, database connection, reference, and update operations are monitored.

- Monitor Listener only

  To check for the listener operation, use the tnsping Oracle command. For a monitor resource 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.

- Monitor Instance only

  A direction (BEQ) connection to the database is established, bypassing the listener and, according to the specified monitor level, database connection, reference, and update operations are monitored. For a monitor resource property, ORACLE_HOME must be set. This is used for direct instance monitoring and recovery action setting without routing through the listener.

  If ORACLE_HOME is not set, only the connection specified with the connect string is established, and any error in the connection operation is ignored. This is used to set the recovery action for a non-connection error together with an Oracle monitor resource for which **Monitor Listener only** is specified.

Monitor Level

Select one of the following levels. When the monitor type is set to Monitor Listener only, the monitor level setting is ignored.

- Level 0 (database status)

  The Oracle management table (V$INSTANCE table) is referenced to check the DB status (instance status). This level corresponds to simplified monitoring without SQL statements being executed for the monitor table.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Connect Command (Within 255 bytes)

Specify the connect string for the database to be monitored. You must specify the connect string.

When **Monitor Type** is set to **Monitor Instance only**, set ORACLE_SID.

Monitor Type	ORACLE_HOME	Connect Command	Monitor Level
Monitor Listener and Instance	Need not be specified	Specify the connect string	As specified
Monitor Listener only	Monitoring dependent on Oracle command if specified	Specify the connect string	Ignored
	Check for connection to the instance through the listener if not specified	Specify the connect string	Ignored
Monitor Instance only	Check for the instance by BEQ connection if specified	Specify ORACLE_SID	As specified
	Check for the instance through the listener if not specified	Specify the connect string	As specified

Default value: None for the connect string

User Name (within 255 bytes)

Specify the user name to log on to the database. You must specify the name.

Specify the Oracle user who can access the specified database.
Default value: sys

Password (within 255 bytes)

Specify the password to log on to the database.
Default value: change_on_install

Authority Method

Specify the database user authentication.
Default value: SYSDBA

Table (within 255 bytes)

Specify the name of a monitor table created on the database. You must specify the name.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Be sure to set the name different from the reserved word in SQL statements.
Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database 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: None

Character Set

Specify the character set of Oracle. Specifying this item cannot be omitted.
Default value: JAPANESE_JAPAN.JA16EUC

Library Path (within 1,023 bytes)

Specify the library path of Oracle Call Interface (OCI). Specifying this item cannot be omitted.
Default value: /opt/app/oracle/product/10.2.0/db_1/lib/libclntsh.so.10.1

Collect detailed application information at failure occurrence

In case that this function is enabled, when Oracle monitor resource detects errors, the detailed Oracle information is collected. The detailed Oracle information is collected up to 5 times.

Note: In case of stopping the oracle service while collecting the information due to the cluster stop, correct information may not be collected.

Default value: Disabled

Collection Timeout

Specify the timeout value for collecting detailed information.
Default value: 600

Set error during Oracle initialization or shutdown

If this function is enabled, a monitor error occurs immediately when Oracle start or shutdown in progress is detected.
Disable this function when Oracle is automatically restarted during operation in cooperation with Oracle Clusterware or the like. Monitoring becomes normal even during Oracle start or shutdown. However, a monitor error occurs if Oracle start or shutdown continues for one hour or more.
Default value: Disabled

Notes on Oracle monitor resources

For the supported versions of Oracle, see “Software Applications supported by monitoring options” in Chapter 3, “Installation requirements for EXPRESSCLUSTER” in the Getting Started Guide.

This monitor resource monitors Oracle with the Oracle interface (Oracle Call Interface). For this reason, the library for interface (libclntsh.so) needs to be installed on the server for monitoring.

To monitor an Oracle database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the Oracle database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**. Also, set up the Oracle client on the host OS side, where monitor resources run, and specify the connection string for connecting to the Oracle database on the virtual machine.

A connection timeout is detected if 90% of the value set for timeout has passed and the Oracle monitor resource has not been able to connect to Oracle.

If values of a connection string, user name and password specified by a parameter are different from the Oracle environment for monitoring, Oracle monitoring cannot be done. Error message is displayed. Check the environment.

For the user specified with the user name parameter, the default is sys, but when a monitoring-dedicated user has been configured, for each monitor level the following access permissions must be provided for that user (if the sysdba permission is not provided):

Monitor level	Necessary permissions
Level 0 (database status)	SELECT permission for V$INSTANCE
Level 1 (monitoring by select)	SELECT permission for a monitor table
Level 2 (monitoring by update/select)	CREATE TABLE / DROP ANY TABLE / INSERT permission for a monitor table / UPDATE permission for a monitor table /SELECT permission for a monitor table
Level 3 (create/drop table each time)	CREATE TABLE / DROP ANY TABLE / INSERT permission for a monitor table / UPDATE permission for a monitor table /SELECT permission for a monitor table

If the administrator user authentication method is only the OS authentication by setting “NONE” to “REMOTE_LOGIN_PASSWORDFILE” in the initialization parameter file, specify a database user without SYSDBA authority for the user name of the parameter.

When specifying a database user with SYSDBA authority, an error occurs when this monitor resource starts, causing the monitoring process not to be executed.

If sys is specified for the user name, an Oracle audit log may be output. If you do not want to output large audit logs, specify a user name other than sys.

Use the character set supported by OS when creating a database.

If Japanese is set to NLS_LANGUAGE in the Oracle initialization parameter file, specify English by NLS_LANG (environment variable of Oracle.) Specify the character set corresponds to the database.

Select the language displayed in the EXPRESSCLUSTER Web Manager alert viewer and OS messages (syslog) for the character code of the monitor resource if an error message is generated from Oracle.

However, as for an error of when connecting to the database such as incorrect user name and alert message may not be displayed correctly.

For the NLS parameter and NLS_LANG settings, see the *Globalization Support Guide* by Oracle Corporation.

The character code settings have no effect on the operation of Oracle.

If "Level 1" or "Level 2" is selected as a monitor level described in the next subsection "How Oracle monitor resources perform monitoring", monitor tables must be created manually beforehand.
A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1".
If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the WebManager alert view 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)	Required
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

When creating by SQL statements (in the following example, the monitor table is named orawatch)
sql> create table orawatch (num number(11,0) primary key);
sql> insert into orawatch values(0);
sql> commit;

*Create this in a schema for the user specified with the user name parameter.

When using EXPRESSCLUSTER commands
clp_oraclew --createtable -n <Oracle monitor resource name>
*When the user other than sys is specified for the user name parameter and the sysdba permission is not provided for that user, CREATE TABLE permission is required for that user.
When deleting the created monitor table manually, run the following command:
clp_oraclew --deletetable -n <Oracle monitor resource name>

The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

In addition, the Oracle resource usage continues to increase. Therefore, it is not recommended to perform monitoring at "Level 3" during usual operations, except for an operation in which an Oracle instance is periodically restarted.

How Oracle monitor resources perform monitoring

Oracle monitor resources perform monitoring according to the specified monitor level.

- Level 0 (database status)

  The Oracle management table (V$INSTANCE table) is referenced to check the DB status (instance status). This level corresponds to simplified monitoring without SQL statements being executed for the monitor table.

  An error is recognized if:

(1) The Oracle management table (V$INSTANCE table) status is in the inactive state (MOUNTED,STARTED)

(2) The Oracle management table (V$INSTANCE table) database_status is in the inactive state (SUSPENDED,INSTANCE RECOVERY)

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

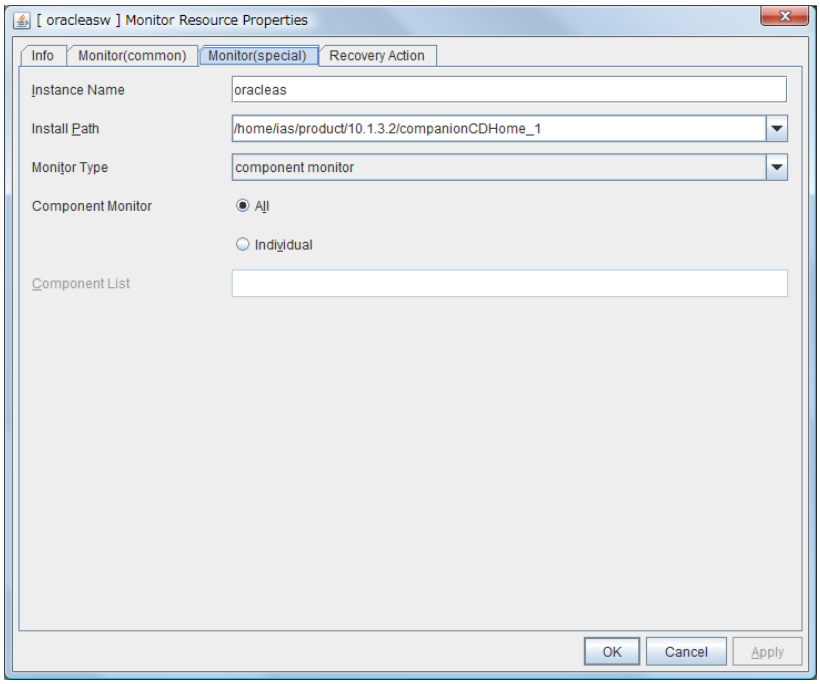
  (2) The written data is not the same as the read data

  For all monitor levels 0 to 3, a specific error (ORA-1033 Oracle Initialization or shutdown) is regarded as being the normal state.

Setting up OracleAS monitor resources

The OracleAS monitor resource is to monitor the Oracle application server running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target OracleAS monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Instance Name (within 255 bytes)

Specify the instance to be monitored. Specifying this item cannot be omitted.

Default value: None

Install Path (within 1,023 bytes)

Specify the installation path of Oracle application. Specifying this item cannot be omitted.

Default value: `/home/ias/product/10.1.3.2/companionCDHome_1`

Monitor Method

Select the Oracle application server function(s) to be monitored.

- opmn process and component concurrent monitoring

  Both opmn process activation/deactivation monitoring and component status monitoring are performed.

- opmn process monitor

  Only opmn process activation/deactivation monitoring is performed.

- Component monitor (default)

  Only component status monitoring is performed.

Component Monitor

Select whether you specify monitor target component individually when **opmn process and component monitor** or **component monitor** is selected as **Monitor Type**.

- All (default)

  All components are monitored.

- Individual

  Only the components specified in **Component List** are monitored.

Component List (within 1,023 bytes)

Enter a target component name of **component monitor**. If you want to specify two or more components, separate them by comma ",". Make sure to set this when **Individual** is selected in **Component Monitor**.

Notes on OracleAS monitor resources

Concerning the Oracle application server versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

For the target to be monitored, specify the EXEC resource that starts the Oracle application server. Monitoring starts after the target resource is activated; however, if the Oracle application server cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

Concerning activation of the target resource, if there is a component that is not activated by any instance of the Oracle application server, edit the opmn.xml file so that the status of the component is "disabled". For details about the opmn.xml file, refer to the Oracle application server manuals.

The Oracle application server may make an output to the operation log every monitoring action; appropriately configure the logging control on the Oracle application server side.

Monitoring by OracleAS monitor resources

The OracleAS monitor resource performs monitoring as described below.

It uses the OracleAS opmnctl command to monitor the application server.

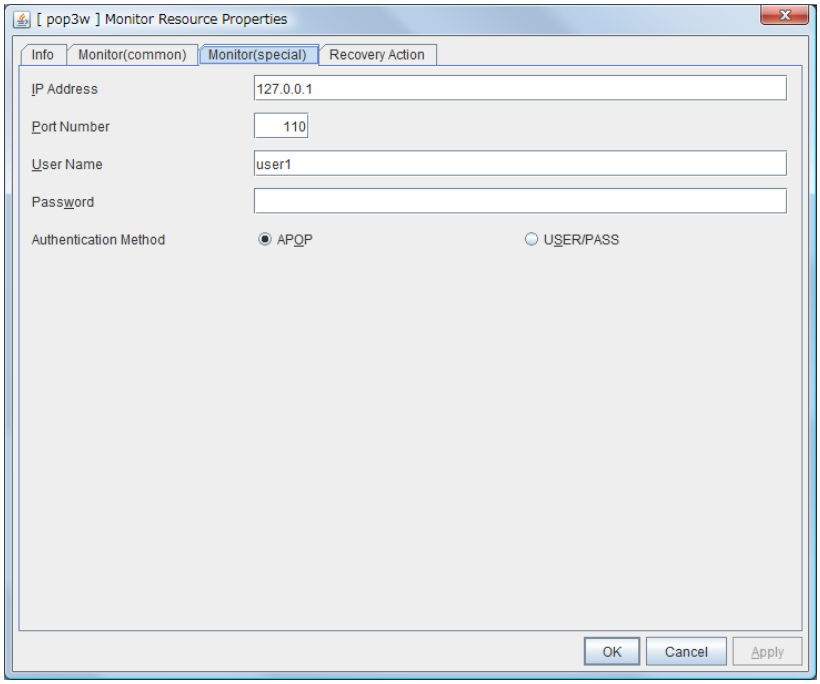
As a result of monitoring, the following is considered as an error:

When an error is reported with the state of the acquired application server.

Setting up POP3 monitor resources

The POP3 monitor resource is to monitor the POP3 service running on a 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.

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target POP3 monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



IP Address (within 79 bytes)

Specify the IP address of the POP3 server to be monitored. Specifying this item cannot be omitted. If it is multi-directional standby server, specify FIP.

Usually, the POP3 server running on the local server is connected, thus the loopback address (127.0.0.1) is to be configured. If accessible addresses are limited by the POP3 server settings, specify an accessible address (e.g., floating IP address). To monitor a POP3 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1 to 65,535)

Specify the POP3 port number to be monitored. Specifying this item cannot be omitted.

Default value: 110

User Name (within 255 bytes)

Specify the user name to log on to POP3.

Default value: None

Password (within 255 bytes)

Specify the password to log on to POP3. Click **Change** and enter the password in the dialog box.

Default value: None

Authority 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.

Notes on POP3 monitor resources

For the target to be monitored, specify the EXEC resource that starts the POP3 server. Monitoring starts after target resource is activated. However, if POP3 services cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

To monitor a POP3 server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the POP3 server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

POP3 services may produce operation logs for each monitoring. Configure the POP3 settings if this needs to be adjusted.

Monitoring by POP3 monitor resources

The POP3 monitor resource performs monitoring as described below.

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:

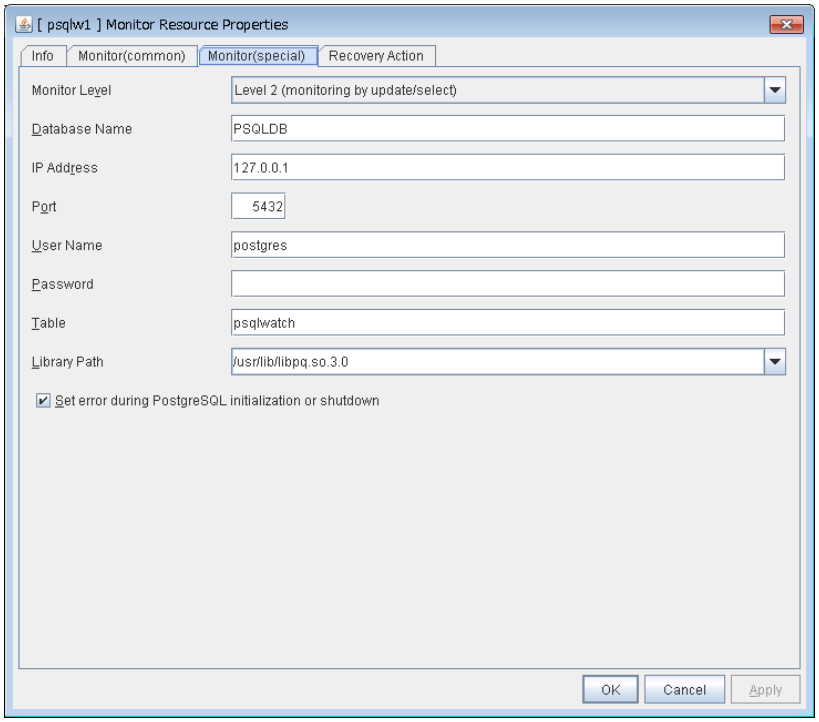
(1) When connection to the POP3 server fails.

(2) When an error is notified as a response to the command.

Setting up PostgreSQL monitor resources

PostgreSQL monitor resource monitors PostgreSQL database that operates on servers.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target PostgreSQL monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update / select / reindex / vacuum) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / reindex / drop / vacuum) type.

Default: Level 2 (monitoring by update/select)

Database Name (within 255 bytes)

Specify the database name to be monitored. Specifying this item cannot be omitted.

Default value: None

IP Address (within 79 bytes)

Specify the IP address of the server to connect. Specifying this item cannot be omitted.

Usually, specify the loopback address (127.0.0.1) to connect to the PostgreSQL server that runs on the local server. To monitor a PostgreSQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port (1 to 65,535)

Specify the port number for connection. Specifying this item cannot be omitted.

Default value: 5,432

User Name (within 255 bytes)

Specify the user name to log on to the database. Specifying this item cannot be omitted.

Specify the PostgreSQL user who can access the specified database.

Default value: postgres

Password (within 255 bytes)

Specify the password to log on to the database.

Default value: None

Table (within 255 bytes)

Specify the name of a monitor table created on the database. Specifying this item cannot be omitted.

Make sure not to specify the same name as the table used for operation because a monitor table will be created and deleted. Be sure to set the name different from the reserved word in SQL statements.

Some characters cannot be used to specify a monitor table name according to the database specifications. For details, refer to the database specifications.

Default value: psqlwatch

Library Path (within 1,023 bytes)

Specify the home path to PostgreSQL. Specifying this item cannot be omitted.

Default value: `/usr/lib/libpq.so.3.0`

Set error during PostgreSQL initialization or shutdown

When this function is enabled, a monitor error occurs immediately upon the detection of PostgreSQL start or shutdown in progress.

When this function is disabled, monitoring becomes normal even during PostgreSQL start or shutdown.

However, a monitor error occurs if PostgreSQL start or shutdown continues for one hour or more.

Default value: Enabled

Notes on PostgreSQL monitor resources

Concerning the PostgreSQL versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

This monitor resource uses the libpq library of PostgreSQL to monitor PostgreSQL.

If this monitor resource fails, set the application library path to the path where the libpq library of PostgreSQL exists.

To monitor a PostgreSQL database that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the PostgreSQL database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

If a value specified by a parameter differs from the PostgreSQL environment for monitoring, a message indicating an error is displayed on the alert view of the WebManager. Check the environment.

For client authentication, on this monitor resource, the following authentication methods that can be set to the “pg_hba.conf” file has been checked its operation.
trust, md5, password

When this monitor resource is used, messages like those shown below are output to a log on the PostgreSQL side. These messages are output by the monitor processing and do not indicate any problems.
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle ERROR: table "psqlwatch" does not exist
YYYY-MM-DD hh:mm:ss JST moodle moodle STATEMENT: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: CREATE TABLE psqlwatch (num INTEGER NOT NULL PRIMARY KEY)
YYYY-MM-DD hh:mm:ss JST moodle moodle NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "psqlwatch_pkey" for table "psql watch"
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch

If “Level 1” or “Level 2” is selected as a monitor level described in the next subsection “How PostgreSQL monitor resources perform monitoring”, monitor tables must be created manually beforehand.
A monitor error occurs if there is no monitor table at the start of monitoring in “Level 1”.
If there is no monitor table at the start of monitoring in “Level 2”, EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the WebManager alert view does not have the monitor table is displayed.
The load on the monitor at “Level 3” is higher than that at “Level 1” and “Level 2” because the monitor in “Level 3” creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Required
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named psqlwatch)
sql> CREATE TABLE psqlwatch (num INTEGER NOT NULL PRIMARY KEY);
sql> INSERT INTO psqlwatch VALUES(0) ;
sql> COMMIT;

Use EXPRESSCLUSTER commands
clp_psqlw --createtable -n <PostgreSQL_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_psqlw --deletetable -n <PostgreSQL_monitor_resource_name>

How PostgreSQL monitor resources perform monitoring

PostgreSQL monitor resources perform monitoring according to the specified monitor level.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (update / select / reindex / vacuum) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (create / insert / select / reindex / drop / vacuum) type.

  An error is recognized if:

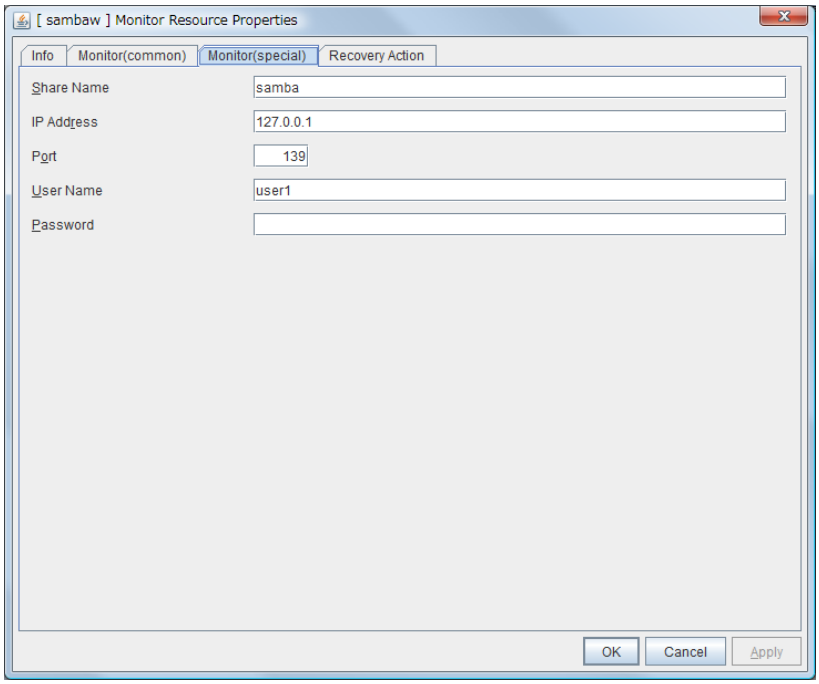
  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

Setting up Samba monitor resources

Samba monitor resource monitors samba file server that operates on servers.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target samba monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Shared Name (within 255 bytes)

Specify the shared name of samba server to be monitored. Specifying this item cannot be omitted.

Default value: None

IP Address (within 79 bytes)

Specify the IP address of samba server. Specifying this item cannot be omitted.

Usually, a connection is made with the samba file server running on the local server, thus the loopback address (127.0.0.1) is to be configured. If a samba file server running on a guest OS of a virtual machine controlled by a VM resource is monitored, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1 to 65,535)

Specify the port number to be used by samba daemon. Specifying this item cannot be omitted.

Default value: 139

User Name (within 255 bytes)

Specify the user name to log on to the samba service. Specifying this item cannot be omitted.

Default value: None

Password (within 255 bytes)

Specify the password to log on to the samba service.

Default value: None

Notes on Samba monitor resources

Concerning the samba versions checked for the operation, refer to "Application supported by the monitoring options" in the *Installation Guide*.

If this monitor resource fails, the parameter value and samba environment may not match. Check the samba environment.

Specify the smb.conf file for the shared name to be monitored to enable a connection from a local server. Allow guest connection when the security parameter of the smb.conf file is "share."

Samba functions except file sharing and print sharing are not monitored.

To monitor a samba file server running on a guest OS of a virtual machine controlled by a VM resource, specify the VM resource for the target of monitoring and set **Wait Time to Start Monitoring** with sufficient time to wait the samba file server to be connectable after VM resource activation.

If the smbmount command is run on the monitoring server when the samba authentication mode is "Domain" or "Server," it may be mounted as a user name specified by the parameter of this monitor resource.

Monitoring by Samba monitor resources

Samba monitor resource monitors the following:

By connecting to samba server and verify establishment of tree connection to resources of the samba server.

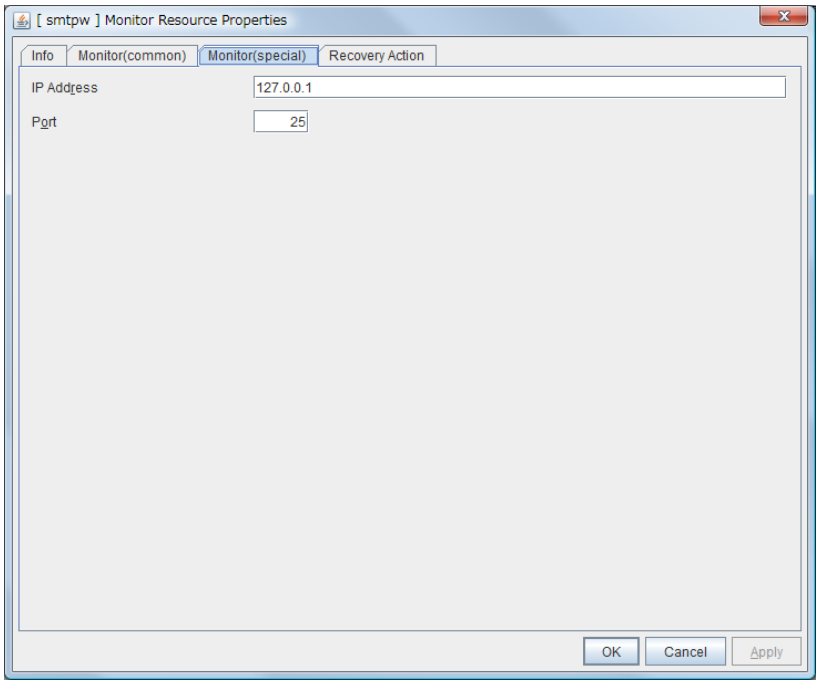
As a result of monitoring, the following is considered as an error:

(1) A response to samba service request is invalid.

Setting up SMTP monitor resources

The SMTP monitor resource is to monitor the SMTP daemon running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target SMTP monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



IP Address (within 79 bytes)

Specify the IP address of the SMTP server to be monitored. Specifying this item cannot be omitted.

Usually, specify the loopback address (127.0.0.1) to connect to the SMTP server that runs on the local server. To monitor an SMTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the IP address of the virtual machine.

Default value: 127.0.0.1

Port Number (1 to 65,535)

Specify the port number of the SMTP to be monitored. Specifying this item cannot be omitted.

Default value: 25

Notes on SMTP monitor resources

Concerning the SMTP versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

If the load average remains exceeding the value of RefuseLA configured in the sendmail.def file for a specified duration of time, the monitor resource may regard the phenomenon as an error.

To monitor an SMTP server that runs in the guest OS on a virtual machine controlled by a VM resource, specify the VM resource as the monitor target and specify enough wait time for the SMTP server to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

Monitoring by SMTP monitor resources

SMTP monitor resources monitor the following:

A connection is made with the SMTP daemon on the server and the NOOP command is executed to monitor the SMTP daemon.

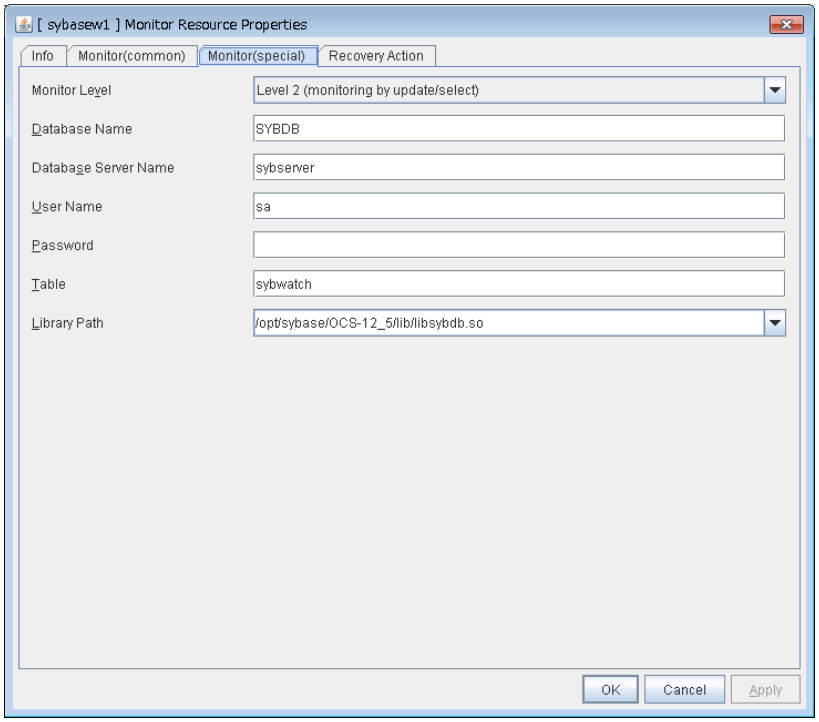
As a result of monitoring, the following is considered as an error:

(1) An error is posted about the response to the connection with the SMTP daemon or NOOP command execution.

Setting up Sybase monitor resources

The Sybase monitor resource is to monitor the Sybase database running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target Sybase monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Monitor Level

Select one of the following levels. You cannot omit this level setting.

- Level 0 (database status)

  The Sybase management table (sys.sysdatabases) is referenced to check the DB status. This level corresponds to simplified monitoring without SQL statements being issued for the monitor table.

- Level 1 (monitoring by select)

  Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. SQL statements executed for the monitor table are of (update/select) type.
  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

- Level 3 (create/drop table each time)

Creation/deletion of the monitor table by statement as well as update. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

Default: Level 2 (monitoring by update/select)

Database Name (within 255 bytes)

Specify the database name to be monitored. Specifying this item cannot be omitted.

Default value: None

Database server name (within 255 bytes)

Specify the name of the database server to be monitored. Specifying this item cannot be omitted.

Default value: None

User Name (within 255 bytes)

Specify the user name to log on to the database. Specifying this item cannot be omitted.

Specify a Sybase user accessible to the specified database.

Default value: sa

Password (within 255 bytes)

Specify the password to log on to the database.

Default value: None

Table (within 255 bytes)

Specify the name of a monitor table created on the database. Specifying this item cannot be omitted.

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: sybwatch

Library Path (within 1,023 bytes)

Specify the library path of Sybase. Specifying this item cannot be omitted.

Default value: `/opt/sybase/OCS-12_5/lib/libsybdb.so`

Notes on Sybase monitor resources

For the supported versions of Sybase, see "Software Applications supported by monitoring options" in Chapter 3, "Installation requirements for EXPRESSCLUSTER" in the *Getting Started Guide*.

This monitor resource monitors ASE using Open Client DB-Library/C of ASE.

If a value specified by a parameter differs from the ASE environment for monitoring, an error message is displayed on the WebManager alert view. Check the environment.

If "Level 1" or "Level 2" is selected as a monitor level described in the next subsection "How Sybase monitor resources perform monitoring", monitor tables must be created manually beforehand.
A monitor error occurs if there is no monitor table at the start of monitoring in "Level 1".
If there is no monitor table at the start of monitoring in "Level 2", EXPRESSCLUSTER automatically creates the monitor table. In this case, a message indicating that the WebManager alert view does not have the monitor table is displayed.
The load on the monitor at "Level 3" is higher than that at "Level 1" and "Level 2" because the monitor in "Level 3" creates or deletes monitor tables for each monitoring.

Selectable monitor level	Prior creation of a monitor table
Level 0 (database status)	Optional
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Required
Level 3 (create/drop table each time)	Optional

Create a monitor table using either of the following methods:

Use SQL statements (in the following example, the monitor table is named sybwatch)
sql> CREATE TABLE sybwatch (num INT NOT NULL PRIMARY KEY)
sql> GO
sql> INSERT INTO sybwatch VALUES(0)
sql> GO
sql> COMMIT
sql> GO

Use EXPRESSCLUSTER commands
clp_sybasew --createtable -n <Sybase_monitor_resource_name>
To manually delete a monitor table, execute the following command:
clp_sybasew --deletetable -n <Sybase_monitor_resource_name>

Monitoring by Sybase monitor resources

Sybase monitor resources perform monitoring according to the specified monitor level.

- Level 0 (database status)

  The Sybase management table (sys.sysdatabases) is referenced to check the DB status. This level corresponds to simplified monitoring without SQL statements being issued for the monitor table.

  An error is recognized if:

  (1) The database status is in an unusable state, e.g., offline.

- Level 1 (monitoring by select)

Monitoring with only reference to the monitor table. SQL statements executed for the monitor table are of (select) type.

An error is recognized if:

(1) An error message is sent in response to a database connection or SQL statement message

- Level 2 (monitoring by update/select)

  Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (update/select) type.

  If a monitor table is automatically created at the start of monitoring, the SQL statement (create/insert) is executed for the monitor table.

  An error is recognized if:

  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

- Level 3 (create/drop table each time)

  Creation/deletion of the monitor table by statement as well as update. One SQL statement can read/write numerical data of up to 11 digits. SQL statements executed for the monitor table are of (create / insert / select / drop) type.

  An error is recognized if:

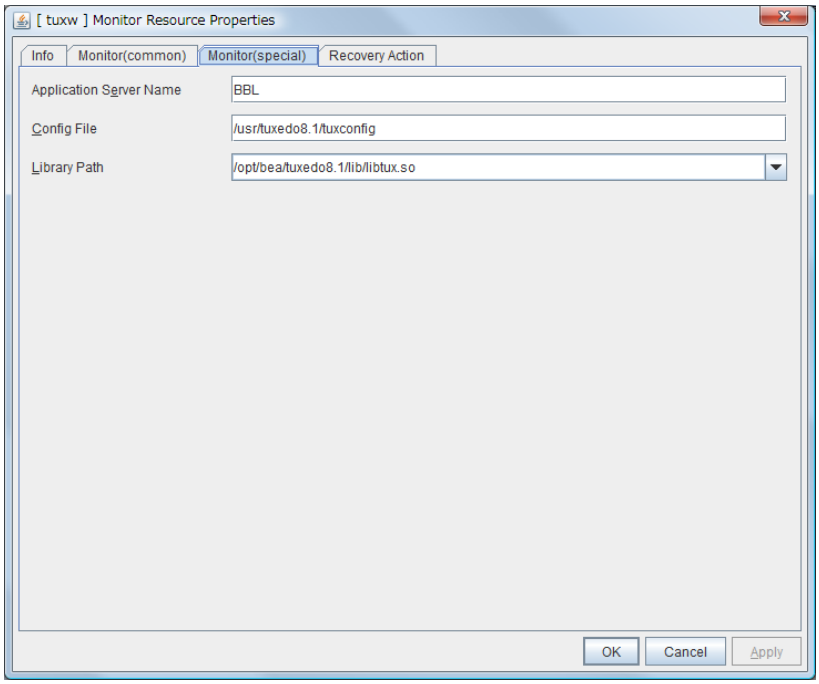
  (1) An error message is sent in response to a database connection or SQL statement message

  (2) The written data is not the same as the read data

Setting up Tuxedo monitor resources

The Tuxedo monitor resource is to monitor Tuxedo running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target Tuxedo monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Application Server Name (within 255 bytes)

Specify the application server name to be monitored. Specifying this item cannot be omitted.

Default value: BBL

TUXCONFIG File Name (within 1,023 bytes)

Specify the placement file name of Tuxedo. Specifying this item cannot be omitted.

Default value: None

Library Path (within 1,023 bytes)

Specify the library path of Tuxedo. Specifying this item cannot be omitted.

Default value: /opt/bea/tuxedo8.1/lib/libtux.so

Notes on Tuxedo monitor resources

Concerning the Tuxedo versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

If a Tuxedo library (such as libtux.so) does not exist, the monitor resource cannot perform monitoring.

Monitoring by Tuxedo monitor resources

The Tuxedo monitor resource performs monitoring as described below.

Tuxedo monitor resources connect to the Tuxedo and execute API to verify the operation.

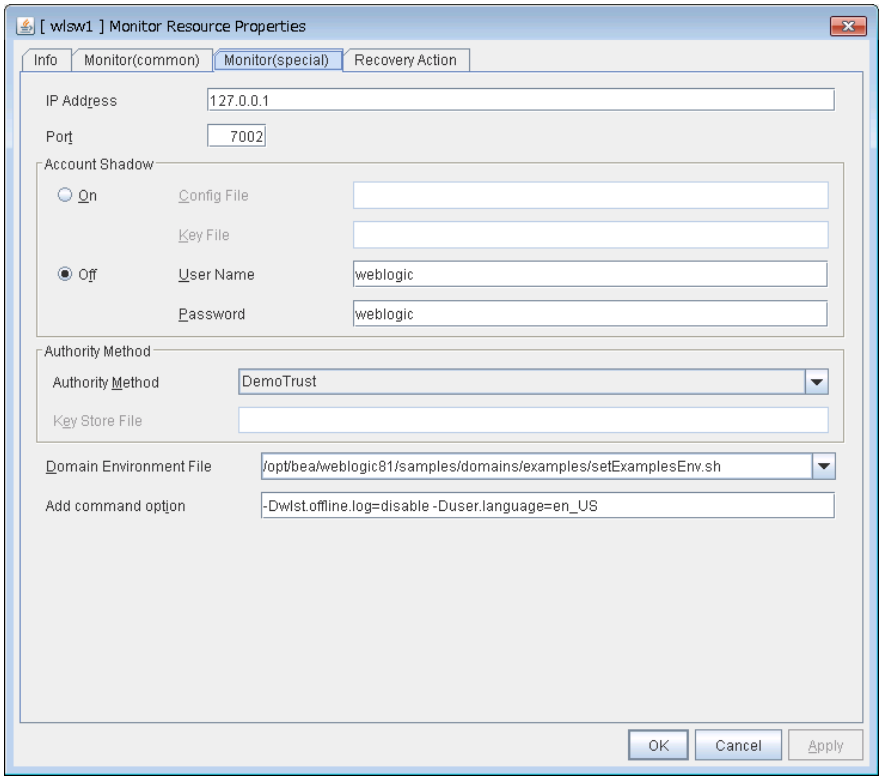
As a result of monitoring, the following is considered as an error:

(1) When an error is reported during the connection to the application server and/or the acquisition of the status.

Setting up Weblogic monitor resources

The Weblogic monitor resource is to monitor Weblogic running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target Weblogic monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



IP Address (within 79 bytes)

Specify the IP address of the server to be monitored. Specifying this item cannot be omitted.
Default value: 127.0.0.1

Port Number (1 to 65,535)

Specify the port number used to connect to the server. Specifying this item cannot be omitted.
Default value: 7,002

Account Shadow

When you specify a user name and a password directly, select **Off**. If not, select **On**. Specifying this item cannot be omitted.
Default value: Off

Config File (within 1,023 bytes)

Specify the file in which the user information is saved. Specifying this item cannot be omitted if **Account Shadow** is **On**.
Default value: None

Key File (within 1,023 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. Specifying this item cannot be omitted if **Account Shadow** is **On**.

Default value: None

User Name (within 255 bytes)

Specify the user name of WebLogic. Specifying this item cannot be omitted if **Account Shadow** is **Off**.

Default value: weblogic

Password (within 255 bytes)

Specify the password of WebLogic.

Default value: weblogic

Authority Method

Specify the authentication method when connecting to an application server. Specifying this item cannot be omitted.

Default value: DemoTrust

Key Store File (within 1,023 bytes)

Specify the authentication file when authenticating SSL. You must specify this when the authentication method is **CustomTrust**.

Default value: None

Domain Environment File (within 1,023 bytes)

Specify the name of the Weblogic domain environment file. Specifying this item cannot be omitted.

Default value: /opt/bea/weblogic81/samples/domains/examples/setExamplesEnv.sh

Additional command option (within 1,023 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

Notes on Weblogic monitor resources

Concerning the Weblogic versions checked for the operation, refer to "Application supported by the monitoring options" in the *Installation Guide*.

To perform monitoring by using the monitor resource, the JAVA environment is required. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

If Weblogic monitor resources are not available at the startup of WebLogic, they will be judged as being abnormal. Adjust [Wait Time to Start Monitoring], or start WebLogic before the startup of the Weblogic monitor resources (for example, specify the script resource for starting Weblogic as a monitor target resource).

Monitoring by Weblogic monitor resources

Weblogic monitor resources monitor the following:

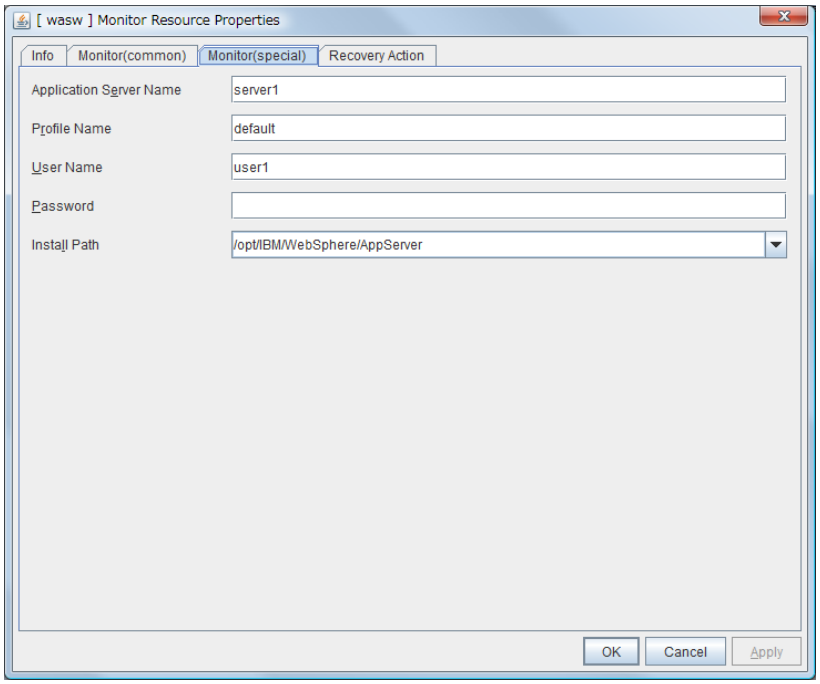
Monitors the application server by performing connect with the “webLogic.WLST” command.

This monitor resource determines the following results as an error:
(1) An error reporting as the response to the `connect`.

Setting up Websphere monitor resources

The Websphere monitor resource is to monitor Websphere running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target Websphere monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Application Server (within 255 bytes)

Specify the application server name to be monitored. Specifying this item cannot be omitted.

Default value: server1

Profile Name (within 1,023 bytes)

Specify the name of the profile of the application server to be monitored. Specifying this item cannot be omitted.

Default value: default

User Name (within 255 bytes)

Specify the Websphere user name. Specifying this item cannot be omitted.

Default value:None

Password (within 255 bytes)

Specify the Websphere password.

Default value: None

Install Path (within 1,023 bytes)

Specify the Websphere installation path. Specifying this item cannot be omitted.

Default value: /opt/IBM/WebSphere/AppServer

Notes on Websphere monitor resources

Concerning the Websphere versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

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.

Monitoring by Websphere monitor resource

The Websphere monitor resource performs monitoring as described below.

Websphere's serverStatus.sh command is employed for application server monitoring.

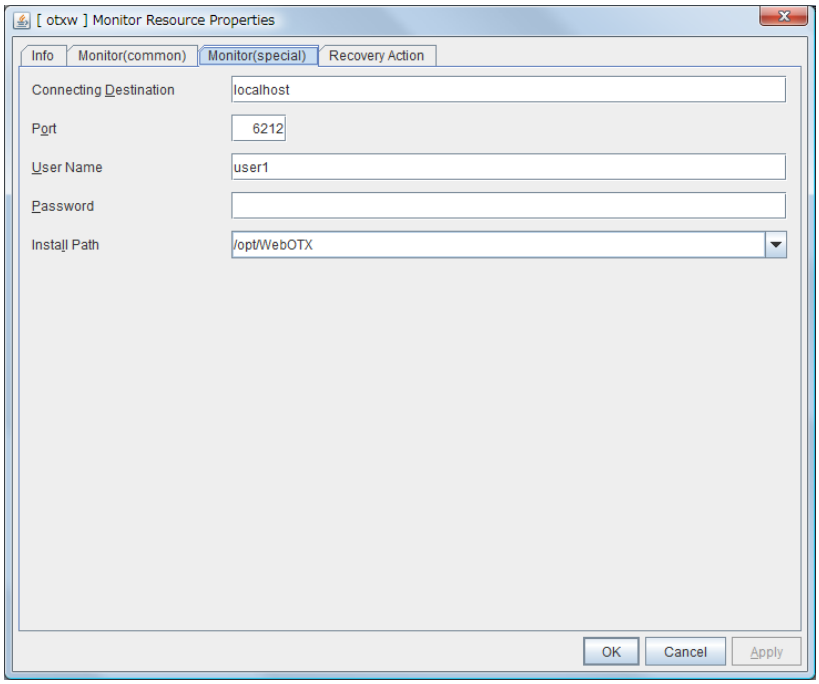
As a result of monitoring, the following is considered as an error:

(1) When an error is reported with the state of the acquired application server.

Setting up WebOTX monitor resources

The WebOTX monitor resource is to monitor WebOTX running on a server.

1. From the tree view displayed in the left pane of the Builder, click the **Monitors** icon.
2. The list of monitor resources is displayed on the table view in the right pane of the window. Right-click the name of the target WebOTX monitor resource, and then click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can display and/or change the detailed settings by following the description below.



Connecting Destination (within 255 bytes)

Specify the server name of the server to be monitored. Specifying this item cannot be omitted.

Default value: localhost

Port Number (1 to 65,535)

Specify the port number used to connect to the server. Specifying this item cannot be omitted.

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: 6,212

User Name (within 255 bytes)

Specify the user name of WebOTX. Specifying this item cannot be omitted.

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 1,023 bytes)

Specify the WebOTX installation path. Specifying this item cannot be omitted.

Default value: /opt/WebOTX

Notes on WebOTX monitor resources

Concerning the WebOTX versions checked for the operation, refer to “Application supported by the monitoring options” in the *Installation Guide*.

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.

Monitoring by WebOTX monitor resources

The WebOTX monitor resource performs monitoring as described below.

WebOTX's otxadmin.sh command is employed for application server monitoring.

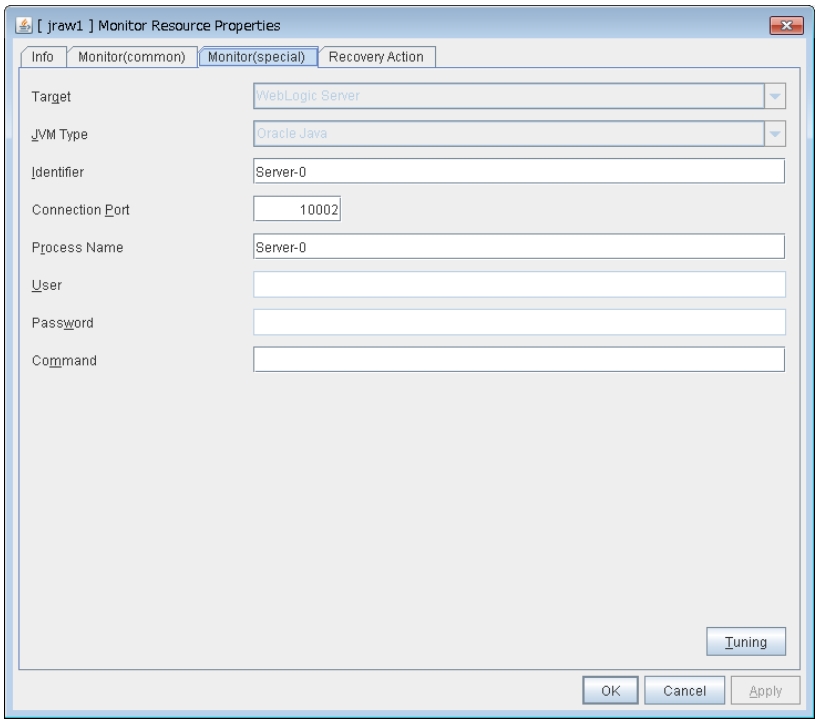
As a result of monitoring, the following is considered as an error:

(1) When an error is reported with the state of the acquired application server.

Setting up 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.

1. Click the **Monitors** icon on the tree view displayed on the left side of the Builder window.
2. A list of the monitor resources is displayed in the table view on the right side of the screen. Right-click the target JVM monitor resource, and click the **Parameter** tab in the **Monitor Resource Property** window.
3. On the **Parameter** tab, you can see and/or change the detailed settings as described below.



Target

Select the target to be monitored from the list. When monitoring WebSAM SVF for PDF, WebSAM Report Director Enterprise, or WevSAM Universal Connect/X, select **WebSAM SVF**. When monitoring a Java application that you created, select **Java Application**.

Select **JBoss** when monitoring the standalone mode of JBoss Enterprise Application Platform 5 or earlier or when monitoring the standalone mode of JBoss Enterprise Application Platform 6 or later. Select **JBoss Domain Mode** when monitoring the domain mode of JBoss Enterprise Application Platform 6 or later.

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.

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** 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.

For each monitor target, the following are selectable.

- When the target is **WebLogic Server**
  Oracle Java, **Oracle Java(usage monitoring)**, and **Oracle JRockit** are selectable.
- When the target is **Tomcat**
  Oracle Java, Oracle Java(usage monitoring), and **OpenJDK** are selectable.
- When the target is other than **WebLogic Server** and **Tomcat**
  Oracle Java and **Oracle Java(usage monitoring)** are selectable.

Default: None

Identifier (within 255 bytes)

The identifier is set to differentiate the relevant JVM monitor resource from another JVM monitor resource when the information on the application to be monitored is output to the JVM operation log of the relevant JVM monitor resource. For this purpose, set a unique character string between JVM monitor resources. You must specify the identifier.

- When the target is **WebLogic Server**
  Set the name of the server instance to be monitored, according to "Monitoring WebLogic Server", item 2.
- When the target is **WebOTX Process Group**
  Specify the name of the process group.
- When the target is **WebOTX Domain Agent**
  Specify the name of the domain.
- When the target is **JBoss** or **JBoss Domain Mode**
  Specify this according to "Monitoring JBoss".
- When the target is **Tomcat**
  Specify this according to "Monitoring Tomcat".
- When the target is **WebOTX ESB**
  Same as for **WebOTX Process Group**.

- When the target is **WebSAM SVF**
  Specify this according to “Monitoring SVF”.
- When the target is **iPlanet Web Server**
  Specify this according to “Monitoring iPlanet Web Server”.
- When the target is **Java Application**
  Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

Connection Port (1024 to 65535)

Set the port number used by the JVM monitor resource when it establishes a JMX connection to the target Java VM. The JVM monitor resource obtains information by establishing a JMX connection to the target Java VM. Therefore, to register the JVM monitor resource, it is necessary to specify the setting by which the JMX connection port is opened for the target Java VM. You must specify the connection port. This is common to all the servers in the cluster. A value between 42424 and 61000 is not recommended.

- When the target is **WebLogic Server**
  Set the connection port number according to “Monitoring WebLogic Server”, item 6.
- When the target is **WebOTX Process Group**
  Specify this according to “Monitoring a Java process of a WebOTX process group”.
- When the target is **WebOTX Domain Agent**
  Specify “domain.admin.port” of
  “(WebOTX_installation_path)/<*domain_name*>.properties”.
- When the target is **JBoss**
  Specify as described in “Monitoring JBoss”.
- When the taret is **JBoss Domain Mode**
  It is unnecessary to set the port number.
- When the target is **Tomcat**
  Specify as described in “Monitoring Tomcat”.
- When the target is **WebOTX ESB**
  Same as for **WebOTX Process Group**.
- When the target is **WebSAM SVF**
  Specify this according to “Monitoring SVF”.
- When the target is **iPlanet Web Server**
  Specify this according to “Monitoring iPlanet Web Server”.
- When the target is **Java Application**
  Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

Process Name (within **1024** bytes)

Set a **Process Name** to identify the target JVM monitor resource when outputting information of the monitor target to the JVM operation log of the JVM monitor resource. Therefore, be sure to specify a character string that is unique among JVM monitor resources.

- When the target is **WebLogic Server**
  Specify a unique server instance name for a process name to identify the target Java VM process. If the process name consisting of only a server instance name is not unique, specify a process name by combining a server instance name and **Connection Port** number.
  Example: When the server instance name is ServerA and the **Connection Port** number is 7001, the **Process Name** is ServerA7001.

- When the target is other than **WebOTX Process Group**
  Specify the name of the process group. If you are specifying multiple settings, specify a string that can be uniquely identified across the group process so that no name is specified more than the same process group.
- When the target is **WebOTX Domain Agent**
  Specify "-Dwebotx.funcid=agent -Ddomain.name=<*domain_name*>".
- When the target is **JBoss**
  Specify this according to “Monitoring JBoss”.
- When the target is **Tomcat**
  Specify this according to “Monitoring Tomcat”.
  - When the target is **WebOTX ESB**
    Same as for **WebOTX Process Group**.
  - When the target is **WebSAM SVF**
    Specify the port number according to “Monitoring SVF”.
  - When the target is **iPlanet Web Server**
    Specify the port number according to “Monitoring iPlanet Web Server”.
  - When the target is **Java Application**
    Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

User (within 255 bytes)

Specify the name of the administrator who will be making a connection with the target Java VM.

- When **WebOTX Domain Agent** is selected as the target
  Specify the “domain.admin.user” value of “/opt/WebOTX/<*domain_name*>.properties”.
- When the target is other than **WebOTX Domain Agent**
  This cannot be specified.

Default: None

Password (within 255 bytes)

Specify the password for the administrator who will be making a connection with the target Java VM.

- When **WebOTX Domain Agent** is selected as the target
  Specify the “domain.admin.passwd” value of “/opt/WebOTX/<*domain_name*>.properties”.
- When the target is other than **WebOTX Domain Agent**
  This cannot be specified.

Default: None

Command (within 255 bytes)

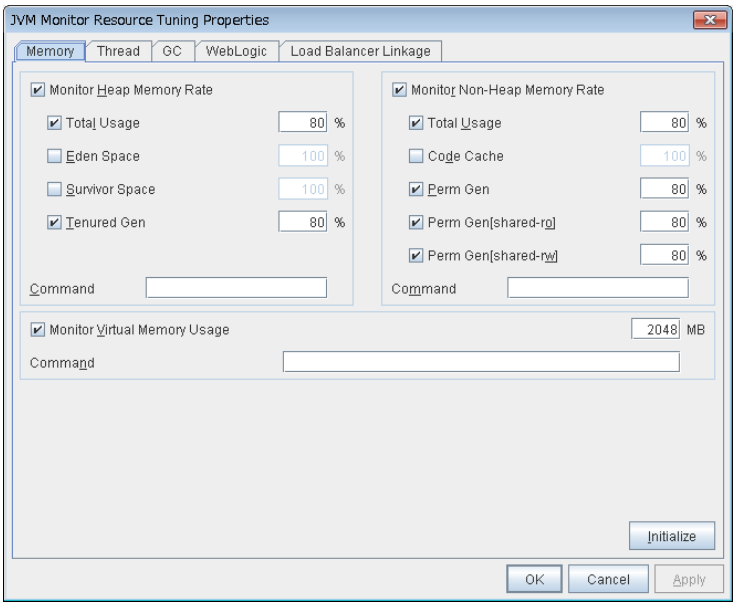
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes (“”) to specify it.

Example: “/usr/local/bin/command” arg1 arg2
Specify the commands that will be executed if connection to the monitor target Java VM cannot be established or if an error is detected in the process for acquiring the amount of resource usage on the Java VM.
See “Executing a command corresponding to cause of each detected error.”

Default: None

When you click Tuning, the following information is displayed in the pop-up dialog box. Make detailed settings according to the descriptions below.

Memory tab (when Oracle Java or OpenJDK is selected for JVM Type)



Monitor Heap Memory Rate

Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- When selected (default):
  Monitoring enabled
- When cleared:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java heap areas used by the target Java VM.

Default: 80[%]

Eden Space (1 to 100)

Specify the threshold for the usage rate of the Java Eden Space used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Eden Space.

Default: 100[%]

Survivor Space (1 to 100)

Specify the threshold for the usage rate of the Java Survivor Space used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Survivor Space.

Default: 100[%]

Tenured Gen (1 to 100)

Specify the threshold for the usage rate of the Java Tenured(Old) Gen area used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Survivor Space.

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 selected (default):
  Monitoring enabled
- When cleared:
  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.

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.

Default: 80[%]

Monitor Virtual Memory Usage (1 to 3072)

Specify the threshold for the usage of the virtual memory used by the target Java VM. JVM monitor resources do not support the monitoring of virtual memory usage when target Java VM consists of 64-bit processes. Therefore, when the target Java VM consists of 64-bit processes, uncheck this check box.

Default: 2048[MB]

Command (within 255 bytes)

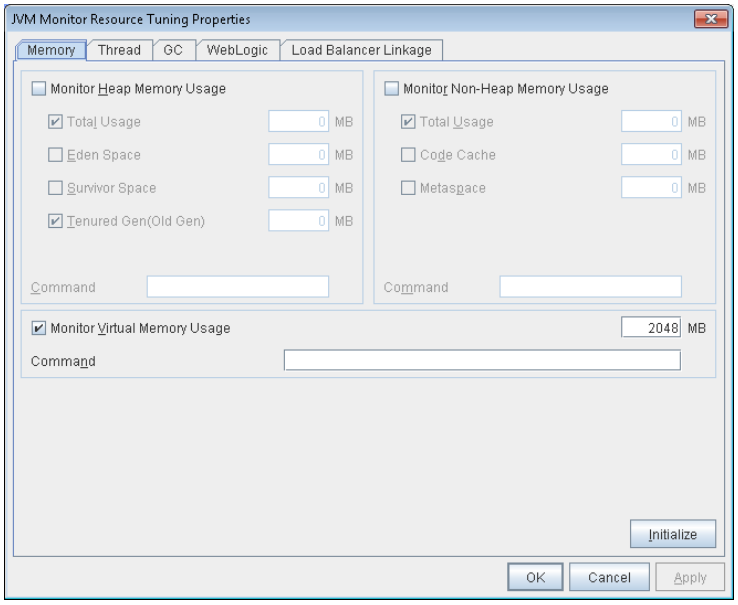
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes (“”) to specify it. Example) “/usr/local/bin/command” arg1 arg2
Specify the commands that will be executed if errors are detected in the process for checking the amount of the usage of the Java heap area, Java non-heap area, and virtual memory in the monitor target Java VM.
See “Executing a command corresponding to cause of each detected error”.

Default: None

Initialize

Click Initialize to set all the items to their default values.

Memory tab (when Oracle Java(usage monitoring) is selected for JVM Type)



Monitor Heap Memory Usage

Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- When the check box is selected:
  Monitoring enabled
- When the check box is not selected (default):
  Monitoring disabled

Total Usage (1 to 102400)

Specify the threshold for the usage rate of the Java heap areas used by the target Java VM.

Default: 0[MB]

Eden Space (1 to 102400)

Specify the threshold for the usage rate of the Java Eden Space used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Eden Space.

Default: 0[MB]

Survivor Space (1 to 102400)

Specify the threshold for the usage rate of the Java Survivor Space used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Survivor Space.

Default: 0[MB]

Tenured Gen (1 to 102400)

Specify the threshold for the usage rate of the Java Tenured(Old) Gen area used by the target Java VM. If G1 GC is specified as the GC method, read it as G1 Old Gen.

Default: 0[MB]

Monitor Non-Heap Memory Usage

Enables the monitoring of the usage rates of the Java non-heap areas used by the target Java VM.

- When the check box is selected:
  Monitoring enabled
- When the check box is not selected (default):
  Monitoring disabled

Total Usage (1 to 102400)

Specify the threshold for the usage rateof the Java non-heap areas used by the target Java VM.
Default: 0[MB]

Code Cache (1 to 102400)

Specify the threshold for the usage rateof the Java Code Cache area used by the target Java VM.
Default: 0[MB]

Metaspace (1 to 102400)

Specify the threshold for the usage rateof the Metaspace area used by the target Java VM.
Default: 0[MB]

Monitor Virtual Memory Usage (1 to 3072)

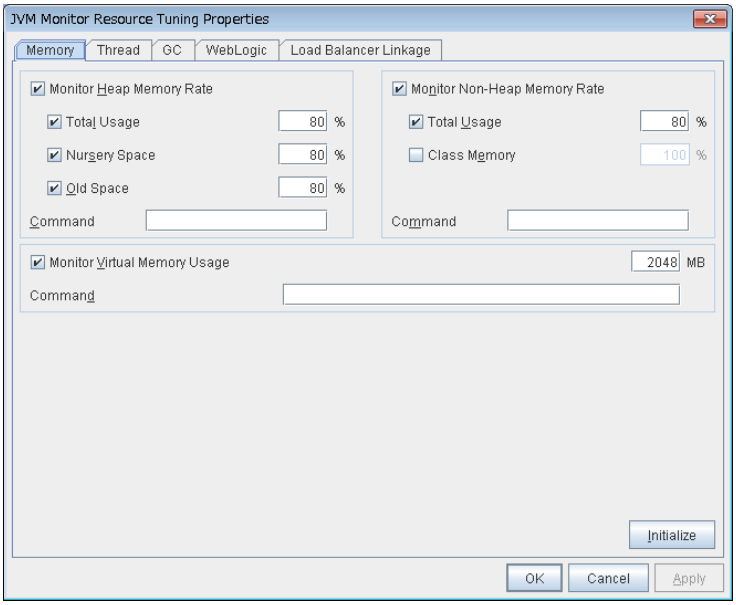
Specify the threshold for the usage of the virtual memory used by the target Java VM. JVM monitor resources do not support the monitoring of virtual memory usage when target Java VM consists of 64-bit processes. Therefore, when the target Java VM consists of 64-bit processes, uncheck this check box.
Default: 2048[MB]

Command (within 255 bytes)

Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes (“”) to specify it. Example) "/usr/local/bin/command" arg1 arg2
Specify the commands that will be executed if errors are detected in the Java heap area, Java non-heap area, and virtual memory usage amount 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.

Memory tab (when Oracle JRockit is selected)



Displayed only when **JRockit** is selected for **JVM Type**.

Monitor Heap Memory Rate

Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- When selected (default):
  Monitoring enabled
- When cleared:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java heap areas used by the target Java VM.

Default: 80[%]

Nursery Space (1 to 100)

Specify the threshold for the usage rate of the Java Nursery Space used by the target JRockit JVM.

Default: 80[%]

Old Space (1 to 100)

Specify the threshold for the usage rate of the Java Old Space used by the target JRockit JVM.

Default: 80[%]

Monitor Non-Heap Memory Rate

Enables the monitoring of the usage rates of the Java non-heap areas used by the target Java VM.

- When selected (default):
  Monitoring enabled
- When cleared:
  Monitoring disabled

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java non-heap areas used by the target Java VM.

Default: 80[%]

Class Memory (1 to 100)

Specify the threshold for the usage rate of the Java Class Memory used by the target JRockit JVM.

Default: 100[%]

Monitor Virtual Memory Usage (1 to 3072)

Specify the threshold for the usage of the virtual memory used by the target Java VM. JVM monitor resources do not support the monitoring of virtual memory usage when target Java VM consists of 64-bit processes. Therefore, when the target Java VM consists of 64-bit processes, uncheck this check box.

Default: 2048[MB]

Command (within 255 bytes)

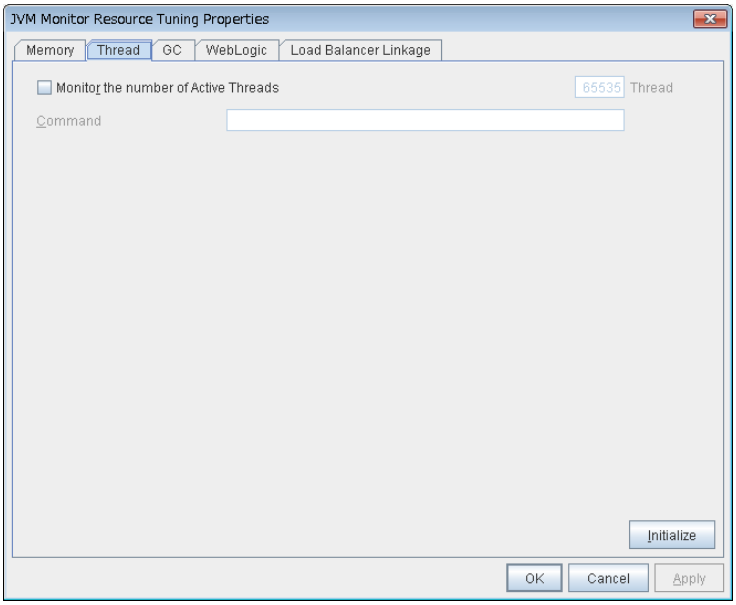
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes ("") to specify it. Example) "/usr/local/bin/command" arg1 arg2
Specify the commands that will be executed if errors are detected in the process for checking the amount of the usage of the Java heap area, Java non-heap area, and virtual memory in the monitor target Java VM.
See "Executing a command corresponding to cause of each detected error".

Default: None

Initialize

Click Initialize to set all the items to their default values.

Thread tab



Monitor the number of Active Threads (1 to 65535)

Specify the upper limit threshold for the number of threads running on the monitor target Java VM.

Default: 65535 [threads]

Command (within 255 bytes)

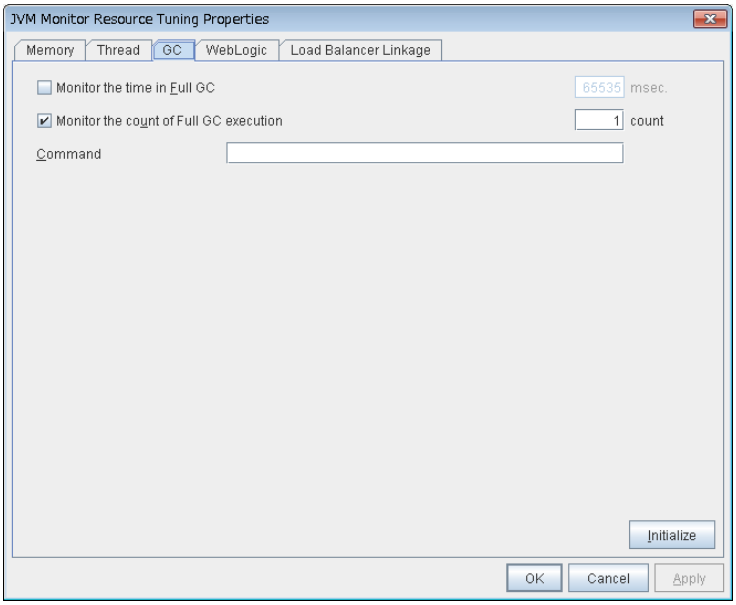
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes (“”) to specify it. Example) “/usr/local/bin/command” arg1 arg2
Specify the commands that will be executed if errors are detected in the process for checking the number of active threads in the monitor target Java VM.
See “Executing a command corresponding to cause of each detected error”.

Default: None

Initialize

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

GC tab



Monitor the time in Full GC (1 to 65535)

Specify the threshold for the Full GC execution time since previous measurement on the target Java VM. The threshold for the Full GC execution time is the average obtained by dividing the Full GC execution time by the number of times Full GC occurs since the previous measurement.

To determine the case in which the Full GC execution time since the previous measurement is 3000 milliseconds and Full GC occurs three times as an error, specify 1000 milliseconds or less.

Default: 65535 [milliseconds]

Monitor the count of Full GC execution (1 to 65535)

Specify the threshold for the number of times Full GC occurs since previous measurement on the target Java VM.

Default: 1 (time)

Command (within 255 bytes)

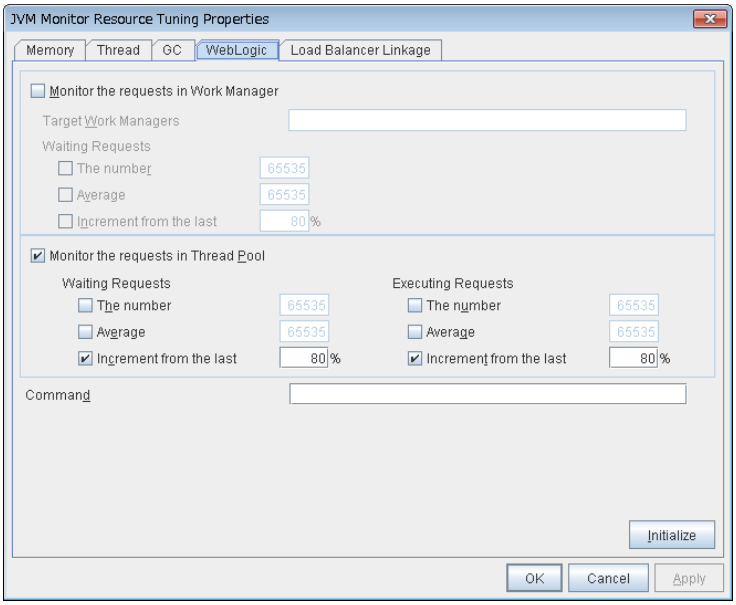
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes (“”) to specify it. Example) “/usr/local/bin/command” arg1 arg2
Specify the commands that will be executed if errors are detected in the process for measuring time in Full GC and the count of Full GC execution in the monitor target Java VM.
See “Executing a command corresponding to cause of each detected error”.

Default: None

Initialize

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

WebLogic tab



Displayed only when **WebLogic Server** is selected for **Target**.

Monitor the requests in Work Manager

Enables the monitoring of the wait requests by Work Managers on the WebLogic Server.

- When selected:
  Monitoring enabled
- When cleared (default):
  Monitoring disabled

Target Work Managers

Specify the names of the Work Managers for the applications to be monitored on the target WebLogic Server. To monitor Work Managers, you must specify this setting.

App1[*WM1*,*WM2*,…];*App2*[*WM1*,*WM2*,…];…

For *App* and *WM*, only ASCII characters are valid (except Shift_JIS codes 0x005C and 0x00A1 to 0x00DF).

To specify an application that has an application archive version, specify “application_name#version” in *App*.

When the name of the application contains "[" and/or "]", prefix it with ¥¥.

(Ex.) When the application name is app[2], enter app¥¥[2¥¥].

Default: None

The number (1 to 65535)

Specify the threshold for the wait request count for the target WebLogic Server Work Manager(s).

Default: 65535

Average (1 to 65535)

Specify the threshold for the wait request count average for the target WebLogic Server Work Manager(s).

Default: 65535

Increment from the last (1 to 1024)

Specify the threshold for the wait request count increment since the previous measurement for the target WebLogic Server Work Manager(s).

Default: 80[%]

Monitor the requests in Thread Pool

In WebLogic Server thread pool to be monitored, the number of wait requests, and the monitoring settings of the number of executing request. The number of requests, HTTP requests and the number that was waiting to be processed and run inside WebLogic Server, and includes the number of requests of the processing performed by the internal EJB call and WebLogic Server. However, it can not judge an abnormal state to be increased. Please specify if you want to the collection of JVM statistics log.

- When selected (default):
  Monitoring enabled
- When cleared:
  Monitoring disabled

Wait Requests The number (1 to 65535)

Specify the threshold for the wait request count.

Default: 65535

Wait Request Average (1 to 65535)

Specify the threshold for the wait request count average.

Default: 65535

Wait Request Increment from the last (1 to 1024)

Specify the threshold for the wait request count increment since the previous measurement.

Default: 80[%]

Executing Requests The number (1 to 65535)

Specify the threshold for the number of requests executed per unit of time.

Default: 65535

Executing Requests Average (1 to 65535)

Specify the threshold for the average count of requests executed per unit of time.

Default: 65535

Executing Requests Increment from the last (1 to 1024)

Specify the threshold for the increment of the number of requests executed per unit of time since the previous measurement.

Default: 80[%]

Command (within 255 bytes)

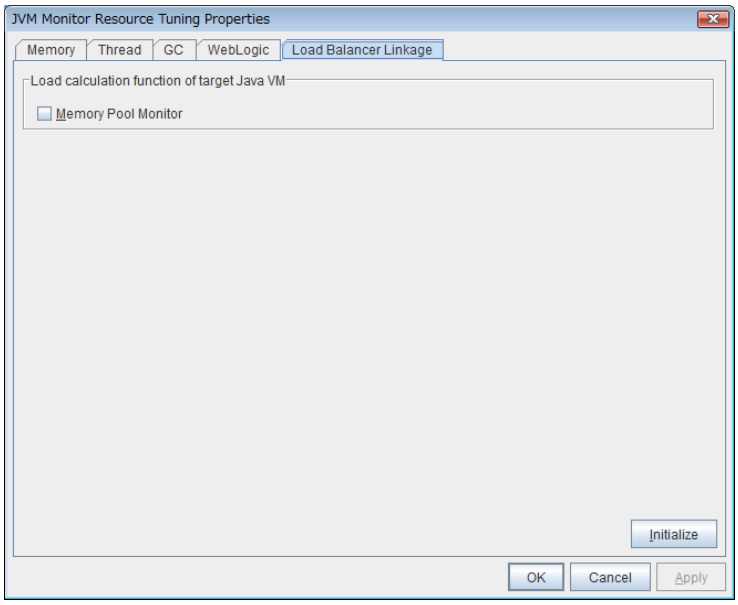
Specify the commands that will be executed if errors in the monitor target Java VM are detected. A specific command and argument(s) can be specified for each error cause. Use an absolute path to specify each command. Place the executable file name in double quotes (“”) to specify it. Example) “/usr/local/bin/command” arg1 arg2
Specify the commands that will be executed if errors are detected in the process for executing requests in the Work Manager and Thread Pool of WebLogic Server.
See “Executing a command corresponding to cause of each detected error”.

Default: None

Initialize

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

Load Balancer Linkage tab



This screen appears when an item other than **BIG-IP LTM** is selected as the load balancer type.

Memory Pool Monitor

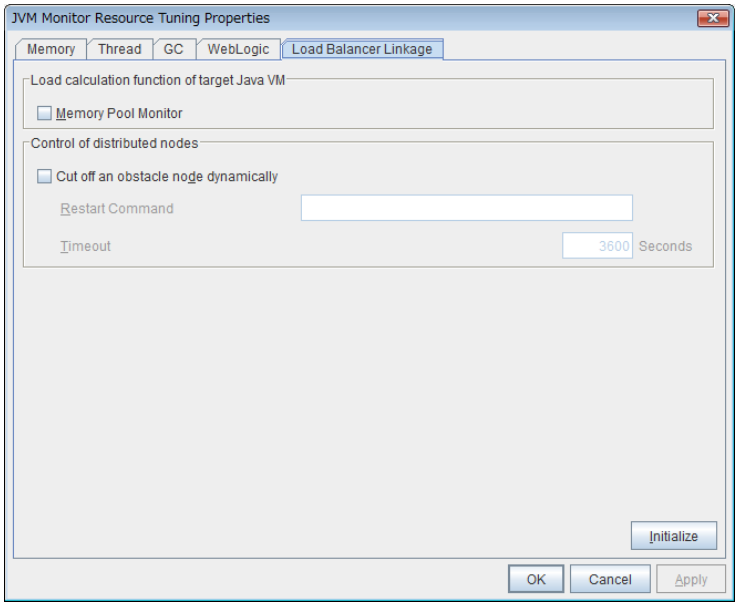
Enables the monitoring of the memory pool when notifying the load balancer of dynamic load information.

- When selected:
  Monitoring enabled
- When cleared (default):
  Monitoring disabled

Initialize

Click the **Initialize** button to set all the items to their default values.

Load Balancer Linkage tab (BIG-IP LTM)



This screen appears when **BIG-IP LTM** is selected as the load balancer type.

Memory Pool Monitor

Enables the monitoring of the memory pool when notifying the load balancer of dynamic load information.

- When selected:
  Monitoring enabled
- When cleared (default):
  Monitoring disabled

Cut off an obstacle node dynamically

When the JVM monitor detects a monitor target failure (example: the collection information exceeds the configured threshold), it sets whether to update the status of the BIG-IP LTM distributed node from “enable” to “disable.”

- When selected:
  Update the status from enable to disable.
- When cleared (default):
  Do not update.

Restart Command

Specify the absolute path of the command to be executed after waiting until the number of connections of the distributed node becomes 0. This function is effective when the monitor target is restarted when resident monitoring is performed and a monitor target failure is detected. Specify the same value between JVM monitor resources.

Timeout (0 to 2592000)

After updating the distributed node status from “enable” to “disable,” the JVM monitor sets the timeout used when waiting until the number of connections of the distributed node falls to 0. If the timeout elapses, [**Restart Command**] is not executed.

Default: 3600 [sec]

Initialize

Click the **Initialize** button to set **Memory Pool Monitor**, **Cut off an obstacle node dynamically**, and **Timeout** to their default values.

Note on JVM monitor resources

Java install path on the JVM 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.

How JVM monitor resources perform monitoring

JVM monitor resource monitors the following:

Monitors application server by using JMX (Java Management Extensions).

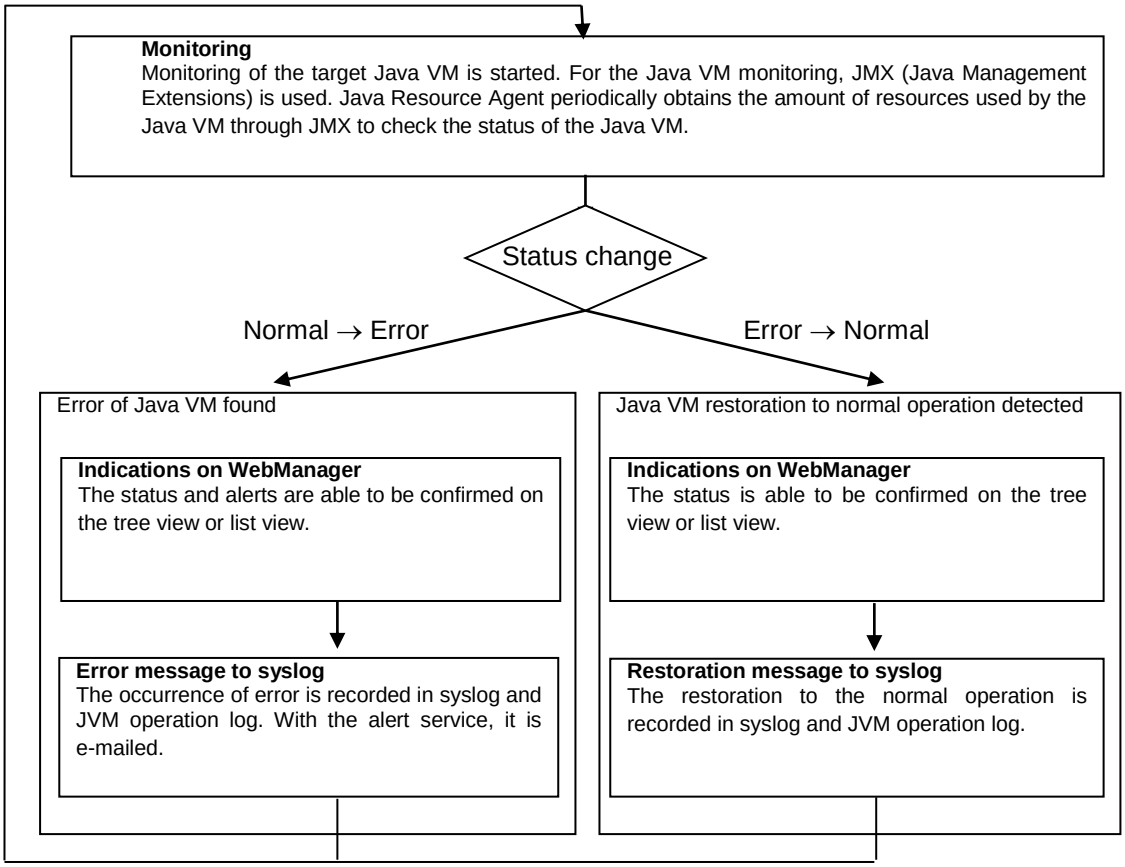
The monitor resource determines the following results as errors:

- Target Java VM or application server cannot be connected
- The value of the used amount of resources obtained for the Java VM or application server exceeds the user-specified threshold a specified number of times (error decision threshold) consecutively

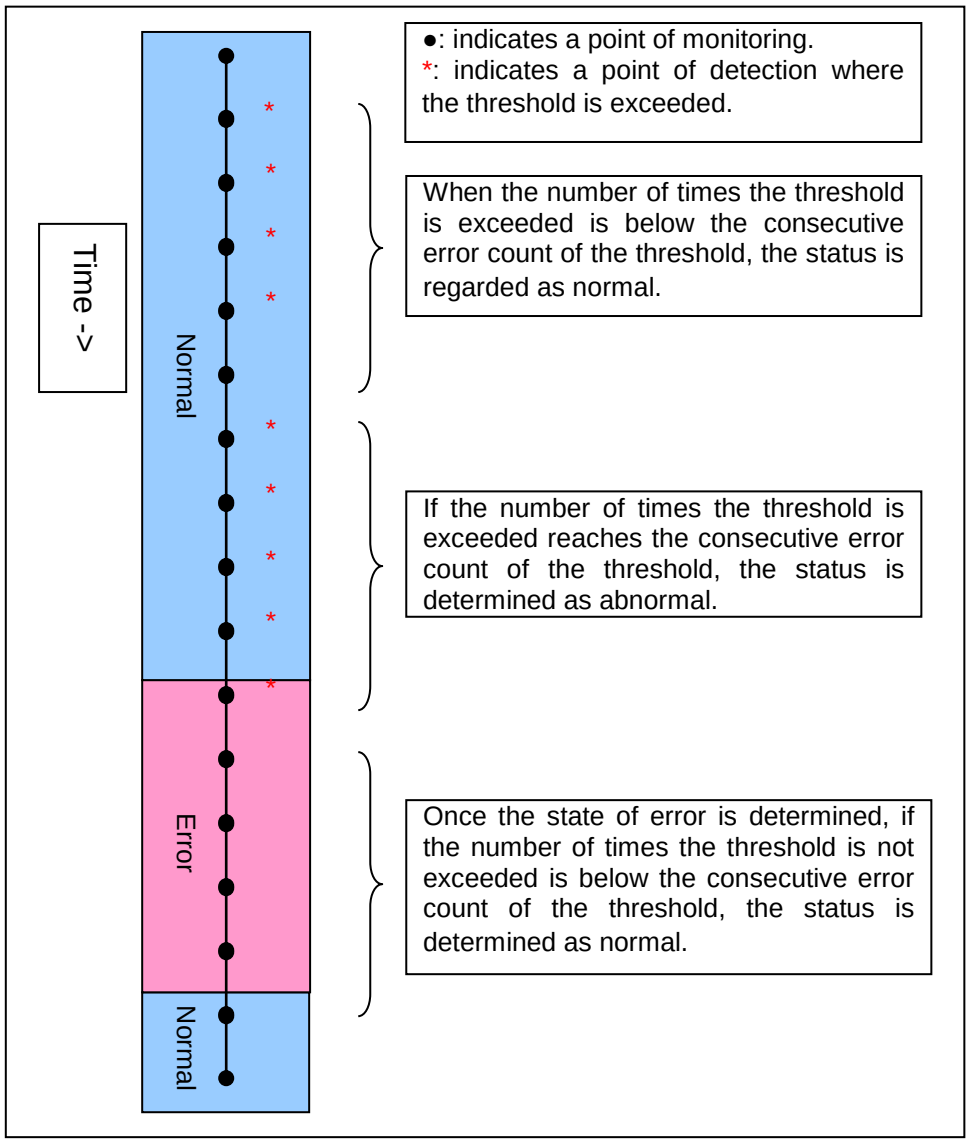
As a result of monitoring, an error is regarded as having been solved if:

- The used amount of resources obtained for the Java VM or application server remains below the user-specified threshold the number of times specified by the error decision threshold.

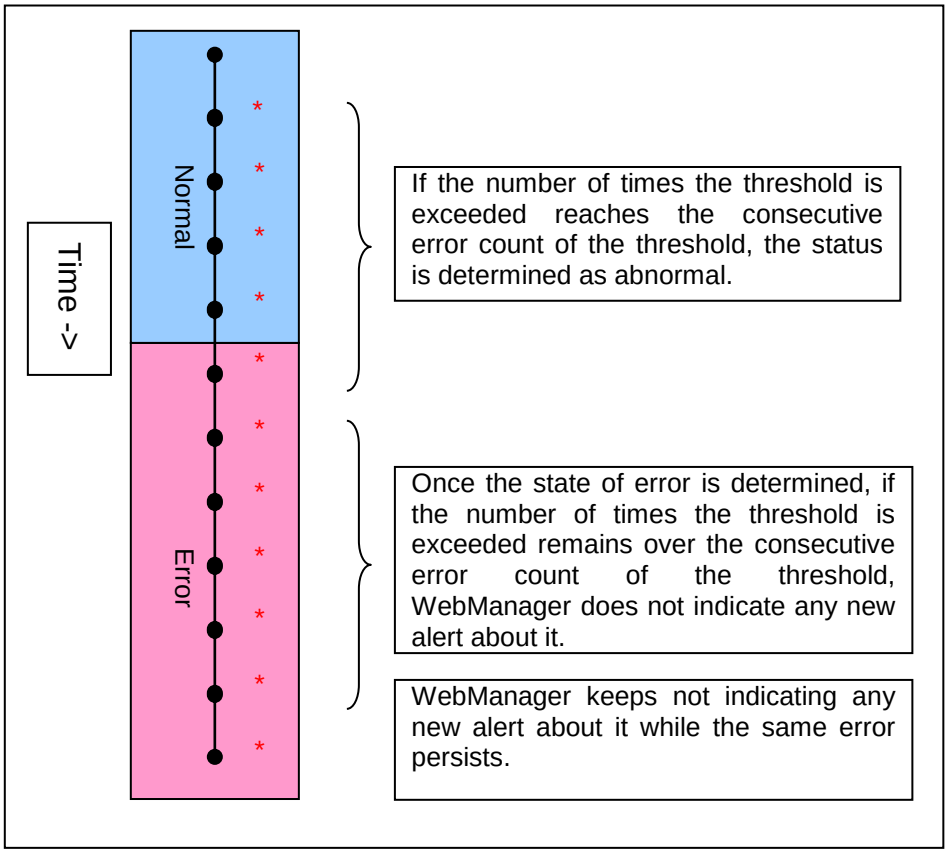
Note:
Collect Cluster Logs in the WebManager **Tools** menu does not handle the configuration file and log files of the target (WebLogic Server or WebOTX).



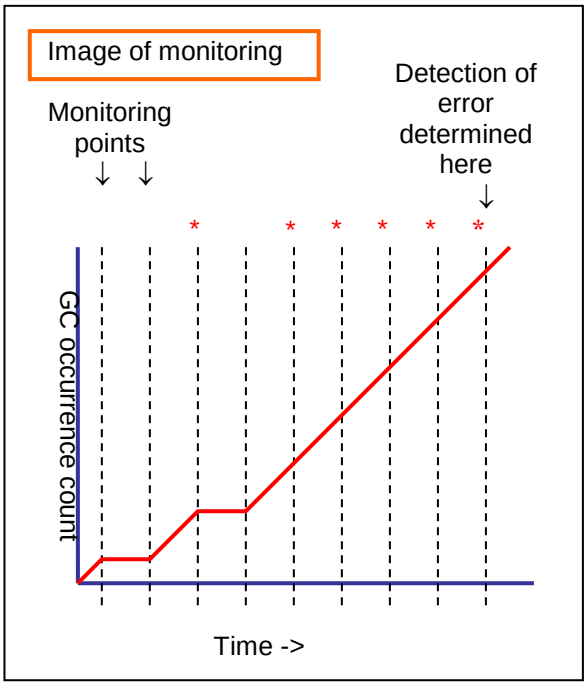
The standard operations when the threshold is exceeded are as described below.



The operations performed if an error persists are as described below.



The following example describes the case of monitoring Full GC (Garbage Collection).
The JVM monitor resource recognizes a monitor error if Full GC is detected consecutively the number of times specified by the error threshold. In the following chart, * indicates that Full GC is detected by the JVM monitor resource when the error threshold is set to 5 (times).
Full GC has a significant influence on the system, thus the recommended error threshold is 1 time.



Linking with the load balancer (health check function)

Target load balancer: Load balancer with health check function for HTML files

JVM monitor resources can link with the load balancer. This section describes an example of linking when WebOTX is used as the application to be monitored. The load balancer linkage provides a health check function and target Java VM load calculation function. To link with the BIG-IP Local Traffic Manager, see "Linking with the BIG-IP Local Traffic Manager".

Distributed nodes are servers that are subject to load balancing, while the distributed node module is installed in the distributed nodes. The distributed node module is included in Express5800/LB400*, MIRACLE LoadBalancer. For Express5800/LB400*, refer to the *Express5800/LB400* User's Guide (Software)*. For load balancers other than Express5800/LB400*, refer to the relevant manual.

To use the function, configure the settings through the Builder cluster property→**JVM Monitor** tab→**Load Balancer Linkage Settings** dialog box; the health check function of the load balancer is linked.

When a load balancing system is configured with the load balancer on the server, the JVM monitor resource renames the HTML file specified by **HTML File Name** to the name specified by **HTML Renamed File Name** upon the detection of a WebOTX error (for example, exceeding the threshold for collected information).

The JVM monitor resource halts for the wait time, or 20 seconds, after renaming the HTML file. The wait time is intended to prevent WebOTX from being restarted before the load balancer finishes disconnecting the distributed node.

Once the JVM monitor resource detects the normality of WebOTX (e.g., the threshold specified for the collected information is not exceeded after reconnection) after WebOTX rebooting, the HTML file name set with **HTML Renamed File Name** is restored to that specified by **HTML File Name**.

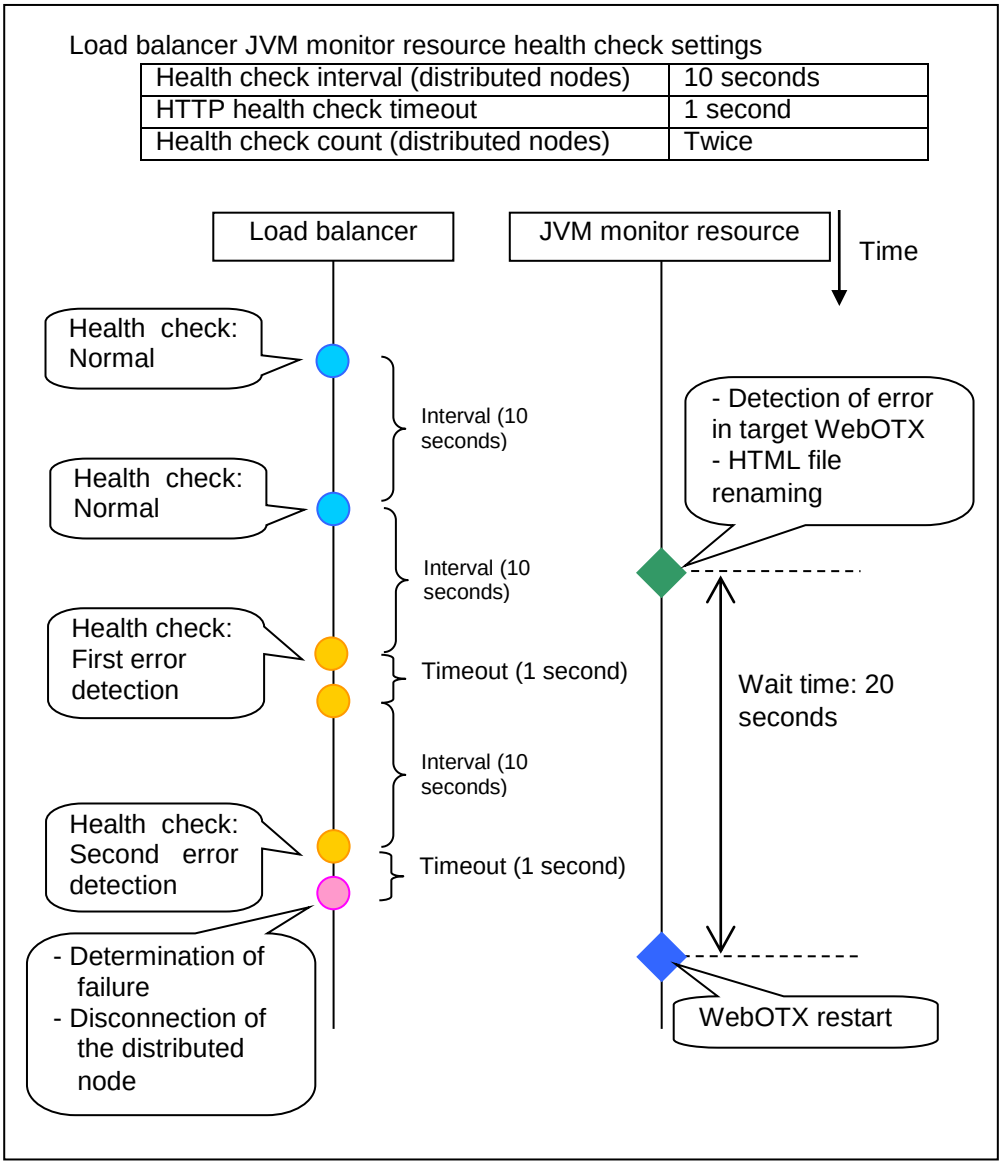
The load balancer periodically health-checks the HTML file, and if a health check fails, the distributed node is determined to be not alive, so that the load balancer disconnects that distributed node. In the case of Express5800/LB400*, configure the health check interval, health check timeout, and retry count to determine the node down state by the health check with the health check (distributed node) interval parameter, HTTP health check timeout parameter, and health check (distributed node) count parameter, that are accessible from **ManagementConsole** for the load balancer→**LoadBalancer→System Information**. For how to configure load balancers other than Express5800/LB400*, refer to the relevant manual.

Configure the parameters using the following as a reference.

20-second wait time >= (health check (distributed node) interval + HTTP health check timeout) x health check (distributed node) count

Load balancer JVM monitor resource health check settings

Health check interval (distributed nodes)	10 seconds
HTTP health check timeout	1 second
Health check count (distributed nodes)	Twice



Linking with the load balancer (target Java VM load calculation function)

Target load balancer: Express5800/LB400*, MIRACLE LoadBalancer

JVM monitor resources can link with the load balancer. This section describes an example of linking when WebOTX is used as the application to be monitored. The load balancer linkage provides a health check function and target Java VM load calculation function. To link with the BIG-IP Local Traffic Manager, see "Linking with the BIG-IP Local Traffic Manager".

Distributed nodes are servers that are subject to load balancing, while the distributed node module is installed in the distributed node. The distributed node module is included in Express5800/LB400*, MIRACLE LoadBalancer. For Express5800/LB400*, refer to the *Express5800/LB400* User's Guide (Software)*. For load balancers other than Express5800/LB400*, refer to the relevant manual.

To use this function, the following settings are required. This function works together with the CPU load-dependent weighting function of the load balancer.

- Properties - Monitor(special) tab → Tuning property - Memory dialog box - Monitor Heap Memory Rate - Total Usage
- **Properties** - **Monitor(special)** tab→ **Tuning** property - **Load Balancer Linkage** dialog box - **Memory Pool Monitor**

According to the following steps, first install the distributed node module on each server, and then execute the load balancer linkage setup command clpjra_lbsetup.sh to configure the distributed node modules.

Note:
Execute the command from an account having the root privilege.

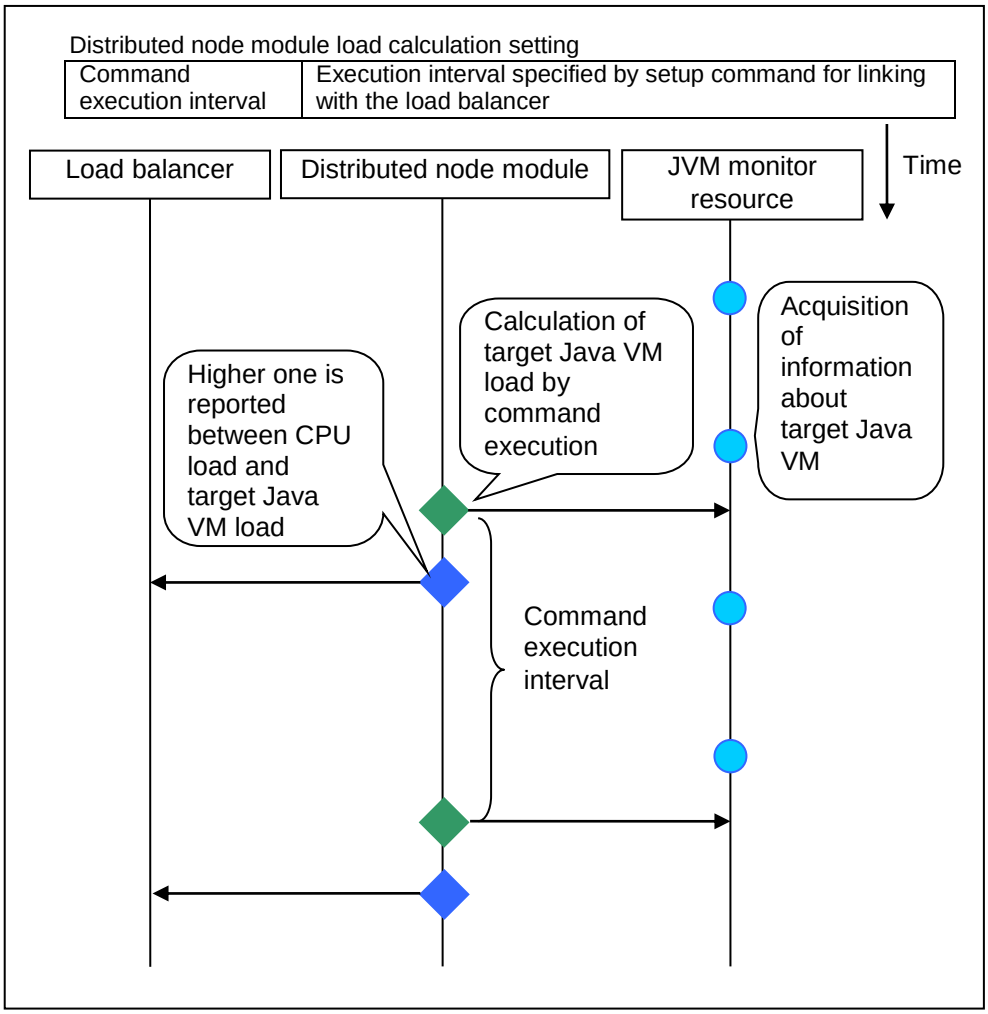
1. Execute [EXPRESSCLUSTER_installation_folder]/ha/jra/bin/clpjra_lbsetup.sh. The functions of the arguments are as described below.
(Example) `clpjra_lbsetup.sh -e 1 -i 120 -t 180`

Argument	Description	Value
-e	Enables or disables the function.	0 or 1 0: Disable 1: Enable
-i	Specify the execution interval for the target Java VM load calculation command, in seconds.	1 to 2147483646
-t	Specify the timeout for the target Java VM load calculation command, in seconds.	1 to 2147483646

The JVM monitor resource calculates the load on the target Java VM according to the information obtained about the Java memory. Obtain the Java VM load from the following expression. The threshold is the value obtained by multiplying the entire amount of the Java heap area by the use ratio set with the **Monitor(special)** tab - **Tuning** property - **Memory** tab - **Monitor Heap Memory Rate** - **Total Usage**.

Java VM load (%) = current memory usage (MB) x 100/threshold (MB)

For the distributed node module installed on a server on which JVM monitor resource is running, commands are periodically executed to compare the obtained target Java VM load with the CPU load obtained separately, and to notify the load balancer of the higher load value as a CPU load. The load balancer distributes the traffic (requests) to the appropriate servers according to the CPU load of the distributed node.



Linking with the BIG-IP Local Traffic Manager

Target load balancer: BIG-IP Local Traffic Manager

The JVM monitor resource can link with BIG-IP LTM. Hereafter, the explanation assumes the use of Tomcat as the application server to be monitored. Linkage with BIG-IP LTM offers the distributed node control function and the target Java VM load calculation function.

The linkage between BIG-IP LTM and the JVM monitor resource is realized with the BIG-IP series API (iControl).

The distributed node is the load distribution server, and the linkage module is that which is installed in each distributed node. The linkage module is contained in Java Resource Agent.

To use the distributed node control function, specify the setting with Builder Cluster Properties -> JVM monitor tab -> Load Balancer Linkage Settings dialog box, JVM monitor resource Properties - Monitor(special) tab - Tuning property - Load Balancer Linkage tab.

To use the target Java VM load calculation function, specify the setting with Builder Cluster Properties -> JVM monitor tab -> Load Balancer Linkage Settings dialog box.

The following BIG-IP LTM linkage error message is output to the JVM operation log. For details, see "JVM monitor resource log output messages."

Error: Failed to operate clpjra_bigip.[error code]

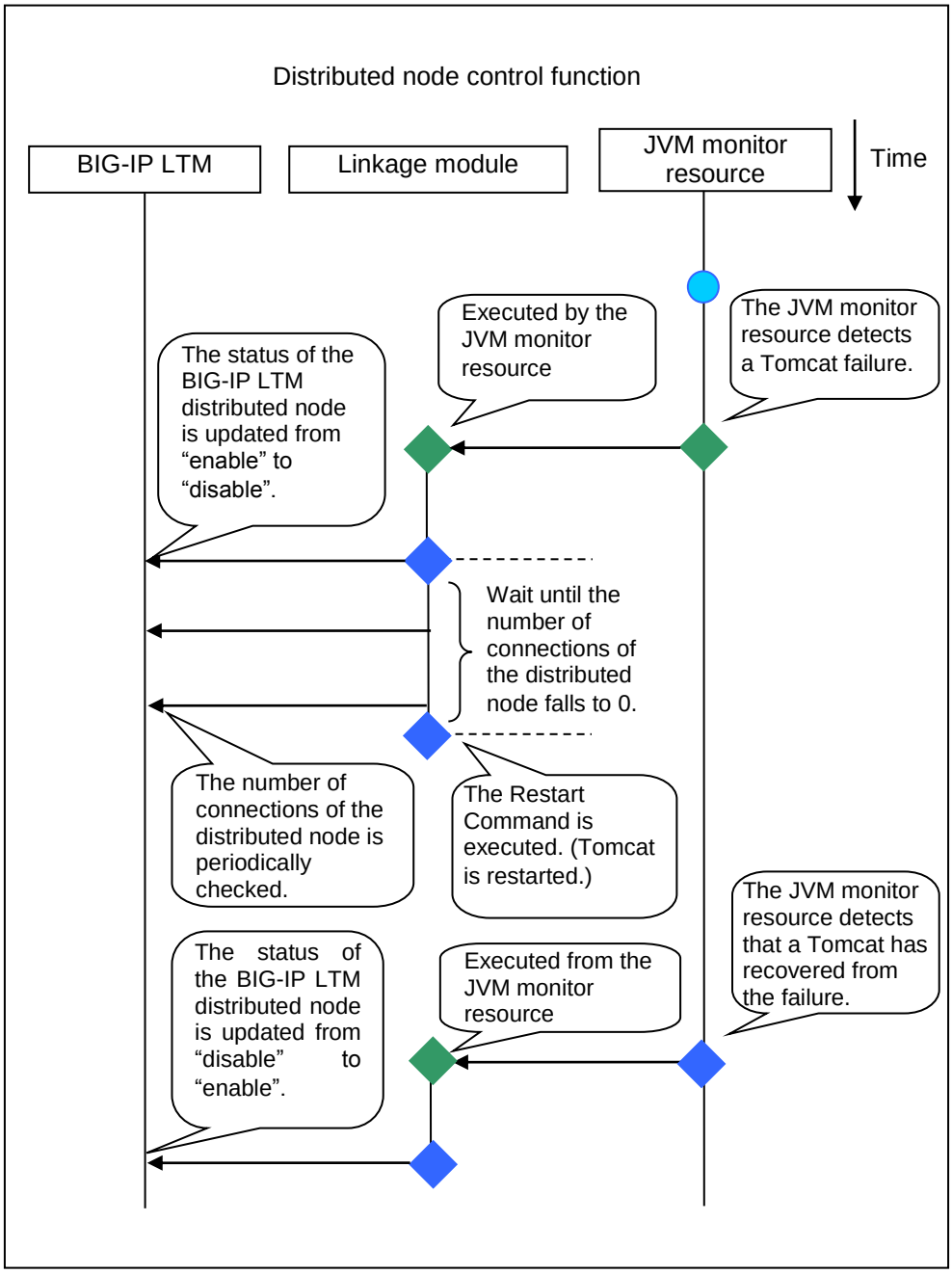
If the relevant server configures the BIG-IP LTM load distribution system, when the JVM monitor detects a Tomcat failure (for example: the amount of collection information exceeds the specified threshold), iControl is used to update the BIG-IP LTM distributed node status from "enable" to "disable."

After updating the status of the distributed node of BIG-IP LTM, the JVM monitor waits until the number of connections of the distributed node falls to 0. After waiting, it executes Restart Command specified on the JVM monitor resource Properties - Monitor(special) tab -> Tuning property - Load Balancer Linkage tab. It does not execute the action specified by Restart Command if the number of connections of the distributed node does not fall to 0, even if Timeout elapses, as specified on the JVM monitor resource Properties - Monitor(special) tab -> Tuning property - Load Balancer Linkage tab.

When the JVM monitor detects a Tomcat failure recovery, it uses iControl to update the status of the BIG-IP LTM distributed node from "disable" to "enable." In this case, it does not execute the action specified by Restart Command specified on the JVM monitor resource Properties - Monitor(special) tab -> Tuning property - Load Balancer Linkage tab.

If the distributed node status is "disable", BIG-IP LTM determines the distributed node to be down and therefore disconnects it. Use of the distributed node control function requires no related setting for BIG-IP LTM.

The distributed node status is updated by BIG-IP LTM when the JVM monitor detects a failure or failure recovery. Therefore, after the failover generated by an operation other than JVM monitoring, the distributed node status of BIG-IP LTM may be "enable".



The JVM monitoring calculates the load on the target Java VM according to the information obtained about the Java memory.

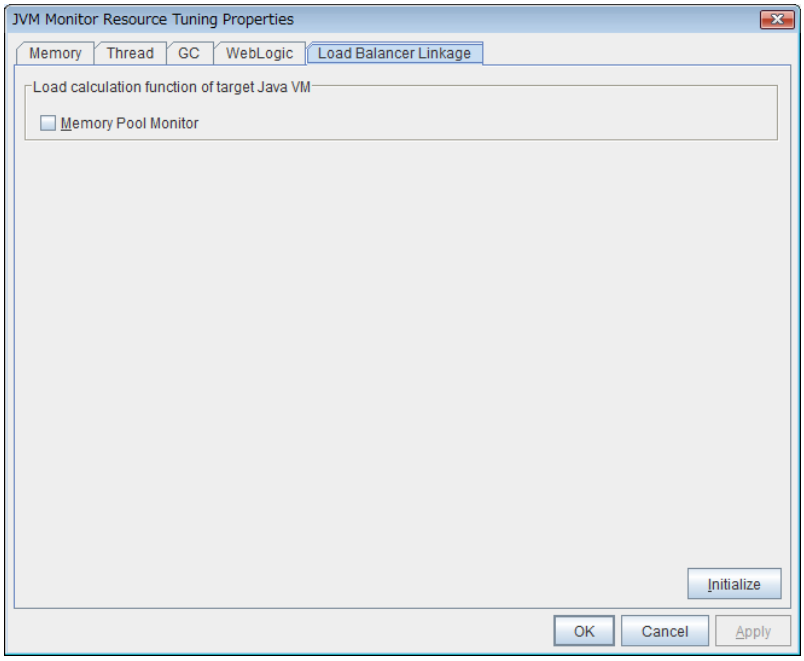
Obtain the Java VM load from the following expression. Java VM load(%) is the value obtained by multiplying the entire amount of the Java heap area by the use ratio set with **Monitor(special)** tab - **Tuning** property - **Memory** tab - **Monitor Heap Memory Rate** - **Total Usage**.

Java VM load (%) = current memory usage (MB) x 100/threshold (MB)

The linkage module installed on the server on which the JVM monitor runs executes a command at regular intervals, and reports the load collected on the target Java VM to BIG-IP LTM. BIG-IP LTM distributes the traffic (request) to the optimal server according to the load status of Java VM of the distributed node.

Set the following EXPRESSCLUSTER settings with the Builder.

- JVM monitor resource



Properties - Monitor(special) tab -> Tuning property - Load Balancer Linkage tab
Select the Memory Pool Monitor] check box.

- Custom monitor resource
  Properties - Monitor(common) tab
  Select the **Monitor Timing - Always** radio button.

  Properties - Monitor(special) tab
  Select **Script created with this product.**
  Select File - Edit and then add the following boldfaced section.

#! /bin/sh

#**

#* genw.sh *

#**

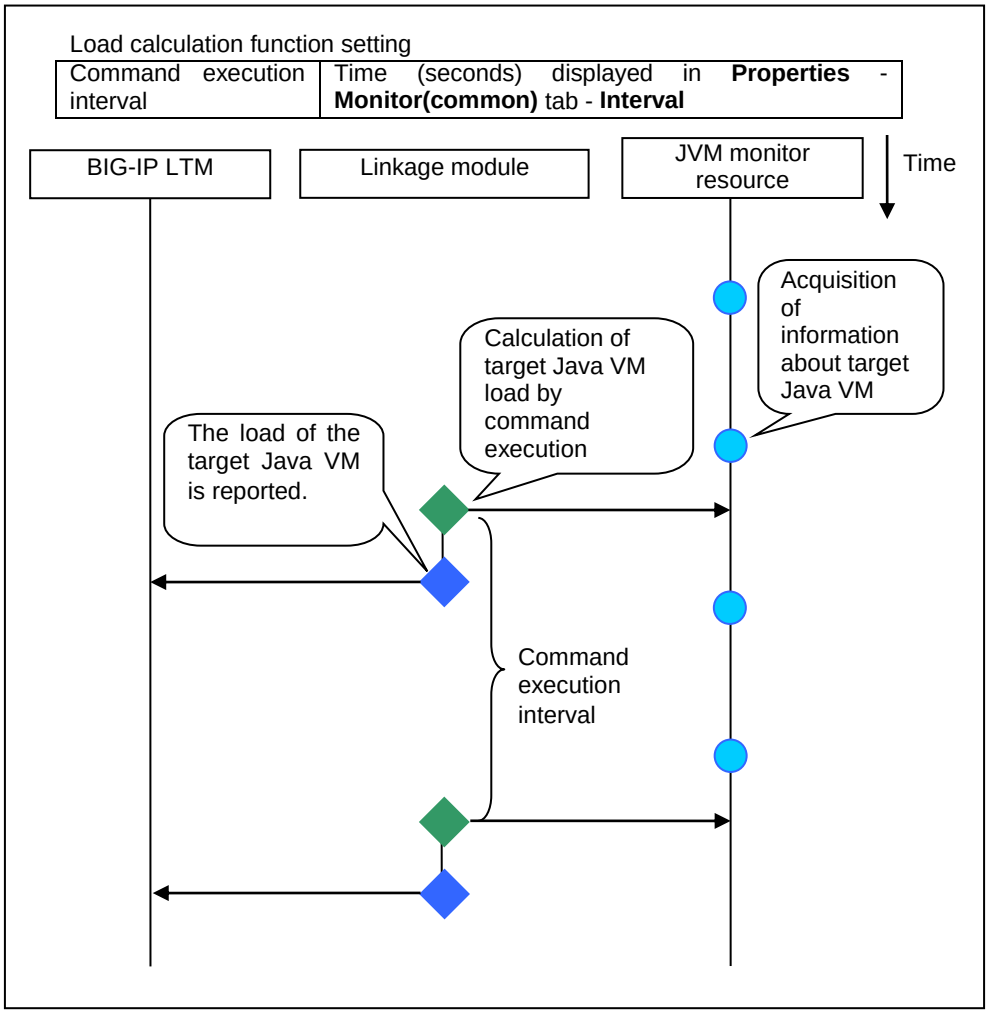
ulimit -s unlimited

${CLP_PATH}/ha/jra/bin/clpjra_bigip weight

exit 0

  Select the **Monitor Type - Synchronous** radio button.

In the BIG-IP LTM setting, specify **Ratio(node)** in **LocalTrafic - Pools:PoolList - Relevant pool - Members - LoadBalancing - Load Balancing Method** of BIG-IP Configuration Utility.


Load calculation function setting
Command execution interval
Time (seconds) displayed in Properties - Monitor(common) tab - Interval
BIG-IP LTM
Linkage module
JVM monitor resource
Time
Acquisition of information about target Java VM
Calculation of target Java VM load by command execution
The load of the target Java VM is reported.
Command execution interval

JVM statistics log

JVM monitor resources collect statistics information on the monitor target Java VM. The information is stored in CSV-format files, as JVM statistics logs.

The following "monitor items" see the parameters on the [Monitor(special)] tab of [Properties] of the JVM monitor resources.
Statistical information is collected and output to its corresponding JVM statistical log when an item is selected and the threshold value is set for the item. If a monitor item is not selected, statistical information on the item will be neither collected nor output to its corresponding JVM statistical log.
The following table lists the monitor items and the corresponding JVM statistics logs.

Monitor items	Corresponding JVM statistics log
[Memory] tab - [Monitor Heap Memory Rate] [Memory] tab - [Monitor Non-Heap Memory Rate]	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
[Memory] tab - [Monitor Virtual Memory Usage]	jraruntime.stat
[WebLogic] tab - [Monitor the requests in Work Manager]	wlworkmanager.stat
[WebLogic] tab - [Monitor the requests in Thread Pool]	wlthreadpool.stat

Java memory area usage check on monitor target Java VM (jramemory.stat)

The jramemory.stat log file records the size of the Java memory area used by the monitor target Java VM. Its file name will be either of the following, depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: jramemory<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jramemory<*YYYYMMDDhhmm*>.stat

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording.
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Name of the Java memory pool; for details, refer to "Java memory pool name".
4	Half-size alphanumeric characters and symbols	Type of Java memory pool. Heap, Non-Heap
5	Half-size numeric characters	Memory size that the Java VM requests from the OS at startup; this is expressed in bytes. (init) At the startup of the monitor target Java VM, the size can be specified using the following Java VM startup options. • HEAP:-Xms • NON_HEAP permanent area (Perm Gen): -XX:PermSize • NON_HEAP code cache area (Code Cache): -XX:InitialCodeCacheSize
6	Half-size numeric characters	Memory size currently used by the Java VM; this is expressed in bytes. (used)

7	Half-size numeric characters	Memory size guaranteed for use by the operation of the Java VM; this is expressed in bytes. (committed) This size varies depending on the memory use; it is always equal to the value of "used" or larger but equal to or smaller than the value of "max".
8	Half-size numeric characters	Maximum memory size that the Java VM can use; this is expressed in bytes. (max) The size can be specified using the following Java VM startup options. • HEAP:-Xmx • NON_HEAP permanent area (Perm Gen): -XX:MaxPermSize • NON_HEAP code cache area (Code Cache): -XX:ReservedCodeCacheSize Example) java -XX:MaxPermSize=128m -XX:ReservedCodeCacheSize=128m javaAP In this example, max of NON_HEAP becomes 128 m + 128 m = 256 m. (Note) When the same value is specified for -Xms and -Xmx, "init" may become larger than "max". This is because "max" of HEAP is determined by subtracting half the size of the Survivor Space from the area size determined by the specification of -Xmx.
9	Half-size numeric characters	Peak size of the memory used after startup of the measurement target Java VM; when the name of the Java memory pool is HEAP or NON_HEAP, this size becomes equal to that of the memory currently used by the Java VM (used). This is expressed in bytes.
10	Half-size numeric characters	Memory size equal to "max" (No. 8 field) × the threshold (%) when the Java memory pool type (No. 4 field) is HEAP; it is expressed in bytes. When the Java memory pool type is other than HEAP, it is 0.

Thread operation status check on monitor target Java VM (jrathread.stat)

The jrathread.stat log file records the thread operation status of the monitor target Java VM. Its file name will be either of the following depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: jrathread<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jrathread<*YYYYMMDDhhmm*>.stat

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording.
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric	Number of active threads in the monitor target Java

	characters and symbols	VM.
4	[Half-size numeric characters: half-size numeric characters:...]	Deadlocked thread ID in the monitor target Java VM; this contains the IDs of all the deadlocked threads, in order.
5	Half-size alphanumeric characters and symbols	Detailed information on deadlocked threads in the monitor target Java VM; it contains information on all the deadlocked threads, in order, in the following format. ThreadName, ThreadID, ThreadStatus, UserTime, CpuTime, WaitedCount, WaitedTime, isInNative, isSuspended <line feed> stacktrace<line feed> : stacktrace<line feed> stacktrace=ClassName, FileName, LineNumber, MethodName, isNativeMethod

GC operation status check on monitor target Java VM (jragc.stat)

The jragc.stat log file records the GC operation status of the monitor target Java VM. Its file name will be either of the following, depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type]-[File Capacity] is selected: jragc<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jragc<*YYYYMMDDhhmm*>.stat

JVM monitor resources output two types of GC information: Copy GC and Full GC.
With Oracle Java, JVM monitor resources count the increment in the count of execution of the following GC as Full GC.

- MarksweepCompact
- MarkSweepCompact
- PS Marksweep
- ConcurrentMarkSweep

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording.
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	GC name of 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

		When the monitor target Java VM is Oracle JRockit The GC name to be indicated is one of the following. Garbage collection optimized for throughput Old Collector Garbage collection optimized for short pausetimes Old Collector Garbage collection optimized for deterministic pausetimes Old Collector Static Collector Static Old Collector Garbage collection optimized for throughput Young Collector
4	Half-size numeric characters	Count of GC execution during the period from startup of the monitor target Java VM to measurement; the count includes the GC executed before the JVM monitor resource starts monitoring.
5	Half-size numeric characters	Total time in GC execution during the period from startup of the monitor target Java VM to measurement; this is expressed in milliseconds. This includes the time taken for the GC executed before the JVM monitor resource starts monitoring.

Virtual memory usage check on monitor target Java VM (jraruntime.stat)

The jraruntime.stat log file records the size of the virtual memory used by the monitor target Java VM. Its file name will be either of the following depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: jraruntime<*integer_starting_with_0*>.stat

  When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: jraruntime<*YYYYMMDDhhmm*>.stat

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording.
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size numeric characters	Start time of the monitor target Java VM, expressed in milliseconds.
4	Half-size numeric characters	Operating time of the monitor target Java VM, expressed in milliseconds.
5	Half-size alphanumeric characters and symbols	Size of the virtual memory used by the monitor target Java VM; this also includes the amount of memory used in the heap area, non-heap area, and stack area. [process_name:PID,size_of_memory_used:] This is expressed in bytes.

Operation status check on Work Manager of WebLogic Server (wlworkmanager.stat)

The wlworkmanager.stat log file records the operation status of the Work Manager of the WebLogic Server. Its file name will be either of the following depending on the Rotation Type

selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: wlworkmanager<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: wlworkmanager<*YYYYMMDDhhmm*>.stat

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording.
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Application name.
4	Half-size alphanumeric characters and symbols	Work Manager name.
5	Half-size numeric characters	Request execution count.
6	Half-size numeric characters	Number of wait requests.

Operation status check on Thread Pool of WebLogic Server (wlthreadpool.stat)

The wlthreadpool.stat log file records the operation status of the thread pool of the WebLogic Server. Its file name will be either of the following depending on the Rotation Type selected in the Log Output Setting dialog box.

- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is selected: wlthreadpool<*integer_starting_with_0*>.stat
- When Cluster Properties - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is selected: wlthreadpool<*YYYYMMDDhhmm*>.stat

The data format is as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording.
2	Half-size alphanumeric characters and symbols	Name of monitor target Java VM; this is specified in [Properties] - [Monitor(special)] tab - [Identifier] in JVM monitor resources.
3	Half-size numeric characters	Total request execution count.
4	Half-size numeric characters	Number of requests queued in the WebLogic Server.
5	Half-size numeric characters	Request execution per unit time count (seconds).
6	Half-size numeric characters	Number of threads for executing the application.
7	Half-size numeric characters	Number of threads in idle state.
8	Half-size numeric characters	Number of executing threads.
9	Half-size numeric characters	The number of threads in stand-by state.

Java memory pool name

This section describes the Java memory pool name output as memory_name in messages to the JVM operation log file. It also describes the Java memory pool name output to the JVM statistics log file, jramemory.stat log file.

The character strings of the Java memory pool names are not determined by the JVM monitor resources. Character strings received from the monitor target Java VM are output as Java

memory pool names.
Their specifications are not open for Java VM, and accordingly, are subject to change without notice with any version upgrade of Java VM.
Therefore, we do not recommend monitoring Java memory pool names contained in messages.

The following monitor items see the parameters on the [Memory] tab of the [Monitor(special)] tab in [Properties] of the JVM monitor resources.
The following Java memory pool names have been confirmed on actual machines running Oracle Java and JRockit.

When "-XX:+UseSerialGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When "-XX:+UseParallelGC" and "-XX:+UseParallelOldGC" are specified as the startup options for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	PS Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	PS Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	PS Old Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	PS Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When "-XX:+UseConcMarkSweepGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jrammemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	Par Eden Space
[Monitor Heap Memory Rate] - [Survivor	Par Survivor Space

Space]	
[Monitor Heap Memory Rate] - [Tenured Gen]	CMS Old Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	CMS Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[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, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseParallelGC" and "-XX:+UseParallelOldGC" are specified as startup options for the monitor target Java VM, the No. 3 Java memory pool name in the 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, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseConcMarkSweepGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the 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]	Par Eden Space

[Monitor Heap Memory Usage]-[Survivor Space]	Par Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	CMS Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseParNewGC" is added as a startup option of the target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows. For Java 9, if -XX:+UseParNewGC is specified, the monitor target Java VM does not start.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Par Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Par Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and “-XX::+UseG1GC” is specified as a startup option for the monitor target Java VM the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	G1 Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	G1 Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen(Old Gen)]	G1 Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace

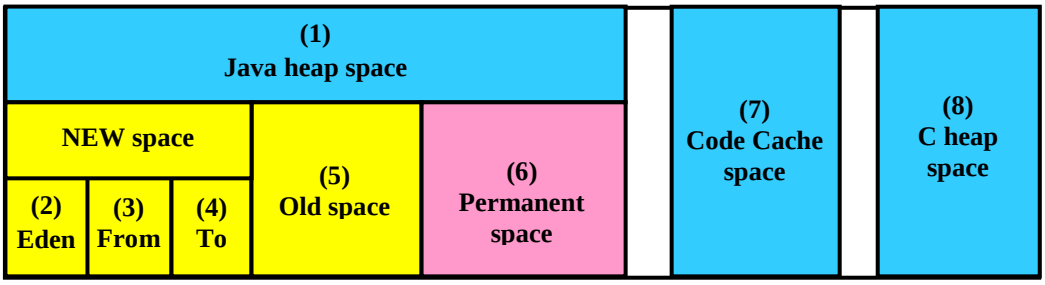
When the monitor target Java VM is Oracle JRockit (when [JRockit] is selected for [JVM Type]), the No. 3 Java memory pool name in the jramemory.stat log file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP memory
[Monitor Heap Memory Rate] - [Nursery Space]	Nursery
[Monitor Heap Memory Rate] - [Old Space]	Old Space
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP

[Monitor Non-Heap Memory Rate] - [Class Memory]	Class Memory

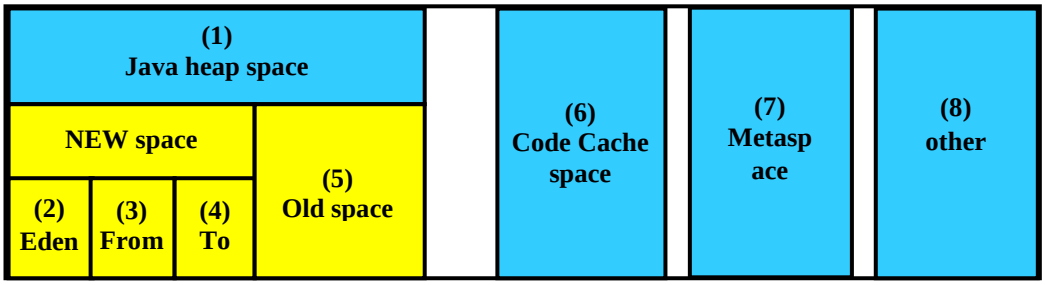
Java memory pool names appearing in the jrammemory.stat log file, a JVM statistics log file, correspond to the Java VM memory space as follows.

◆ For Oracle Java 6/Oracle Java 7



No. in diagram	Monitor item	Java memory pool name in jrammemory.stat log file
(1)	[Monitor Heap Memory Rate] - [Total Usage]	HEAP
(2)	[Monitor Heap Memory Rate] - [Eden Space]	EdenSpace PS Eden Space Par Eden Space
(3)+(4)	[Monitor Heap Memory Rate] - [Survivor Space]	Survivor Space PS Survivor Space Par Survivor Space
(5)	[Monitor Heap Memory Rate] - [Tenured Gen]	Tenured Gen PS Old Gen CMS Old Gen
(6)	[Monitor Non-Heap Memory Rate] - [Perm Gen] [Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]] [Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen Perm Gen [shared-ro] Perm Gen [shared-rw] PS Perm Gen CMS Perm Gen
(7)	[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
(8)	-	-
(6)+(7)	[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP * No stack trace is included.

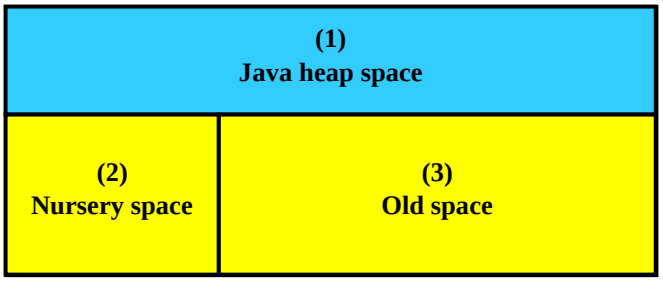
◆ For Oracle Java 8/Oracle Java 9



Number in diagram	Monitor item	Java memory pool name in jrammemory.stat log file
(1)	[Monitor Heap Memory Usage] -	HEAP

	[Total Usage]	
(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 CMS Old Gen G1 Old Gen
(6)	[Monitor Non-Heap Memory Usage] - [Code Cache]	Code Cache
(7)	[Monitor Non-Heap Memory Usage] - [Metaspace]	Metaspace
(8)	-	Compressed Class Space, etc.
(6)+(7)+(8)	[Monitor Non-Heap Memory Usage] - [Total Usage]	NON_HEAP

◆ For Oracle JRockit



No. in diagram	Monitor item	Java memory pool name in jrammemory.stat log file
(1)	[Monitor Heap Memory Rate] - [Total Usage]	HEAP memory
(2)	[Monitor Heap Memory Rate]-[Nursery Space]	Nursery
(3) (Note)	[Monitor Heap Memory Rage]-[Old Space]	Old Space
-	[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
-	[Monitor Non-Heap Memory Rate] - [Class Memory]	Class Memory

(Note)
"Old Space", a Java memory pool name in the jrammemory.stat log file, does not indicate the value corresponding to the old space of the Heap but rather the value corresponding to the entire "Heap memory". Independent measurement of only (3) is not possible.

Executing a command corresponding to cause of each detected error

EXPRESSCLUSTER does not provide a means for executing specific commands based on the causes of detected monitor resource errors.
JVM monitor resources can execute specific commands according to error causes. If an error is detected, JVM monitor resources will execute an appropriate command.

The following setting items specify the commands that will be executed according to the error cause.

Error cause	Setting item
• Failure in connection to the monitor target Java VM • Failure in resource measurement	[Monitor(special)] tab - [Command]
• Heap memory rate • Non-heap memory rate • Virtual memory usage • Heap memory usage • Non-heap memory usage	[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]
• Number of active threads	[Monitor(special)] tab - [Tuning] properties - [Thread] tab - [Command]
• Time in Full GC • Count of Full GC execution	[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]
• Requests in Work Manager of WebLogic • Requests in Thread Pool of WebLogic	[Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Command]

[Command] passes the details of an error cause as the arguments of a command with the arguments attached to the end of [Command]. A Command that is specialized for dealing with specific error causes can be defined by designing and specifying a script etc. for [Command]. The following character strings are passed as the arguments.
When multiple character strings are stated as possible arguments, one will be passed according to the GC type of the monitor target Java VM. For details about their differences, see "Java memory pool name".
The statements "(For Oracle Java)" and "(For Oracle JRockit)" suggest that different character strings are used according to the JVM type. When there is no such statement, the same character strings are used equally for all JVM types.

Details of error causes	Character string passed as argument
• Failure in connection to the monitor target Java VM • Failure in resource measurement	No character string defined
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Monitor Memory Heap Rate] - [Total Usage] (For Oracle Java)	HEAP
[Memory] tab - [Monitor Memory Heap Rate] - [Eden Space] (For Oracle Java)	EdenSpace PSEdenSpace ParEdenSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Survivor Space] (For Oracle Java)	SurvivorSpace PSSurvivorSpace ParSurvivorSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Tenured Gen] (For Oracle Java)	TenuredGen PSOldGen CMSOldGen
[Memory] tab - [Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP

(For Oracle Java)	
[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 Virtual Memory Usage] - (For Oracle Java)	Vmsize
[Memory] tab - [Monitor Heap Memory Usage]-[Total Usage] (for Oracle Java(usage monitoring))	HEAP
[Memory] tab - [Monitor Heap Memory Usage]-[Eden Space] (for Oracle Java(usage monitoring))	EdenSpace PSEdenSpace ParEdenSpace G1EdenSpace
[Memory] tab - [Monitor Heap Memory Usage]-[Survivor Space] (for Oracle Java(usage monitoring))	SurvivorSpace PSSurvivorSpace ParSurvivorSpace G1SurvivorSpace
[Memory] tab - [Monitor Heap Memory Usage]-[Tenured Gen] (for Oracle Java(usage monitoring))	TenuredGen PSOldGen CMSOldGen G1OldGen
[Memory] tab - [Non-Heap 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 Memory Heap Rate] - [Total Usage] (For Oracle JRockit)	HEAP Heap
[Memory] tab - [Monitor Memory Heap Rate] - [Nursery Space] (For Oracle JRockit)	Nursery
[Memory] tab - [Monitor Memory Heap Rate] - [Old Space] (For Oracle JRockit)	OldSpace
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Total Usage] (For Oracle JRockit)	NON_HEAP
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Class Memory] (For Oracle JRockit)	ClassMemory
[Memory] tab - [Monitor Virtual Memory Usage] - (For Oracle JRockit)	Vmsize
[Thread] tab - [Monitor the number of Active Threads]	Count

[GC] tab - [Monitor the time in Full GC]	Time
[GC] tab - [Monitor the count of Full GC execution]	Count
[WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, The number]	WorkManager_PendingRequests
[WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, The number]	ThreadPool_PendingUserRequestCount
[WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, The number]	ThreadPool_Throughput

The following are examples of execution.
Example 1)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	/usr/local/bin/downcmd
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the count of Full GC execution]	1
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If Full GC is executed as many times, in succession, as specified by the Error Threshold (three times), the JVM monitor resources will detect a monitor error and execute a command corresponding to "/usr/local/bin/downcmd Cont".

Example 2)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	"/usr/local/bin/downcmd" GC
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the time in Full GC]	65536
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the time in Full GC exceeds 65535 milliseconds as many times, in succession, as specified by the Error Threshold (three times), the JVM monitor resources will detect a monitor error and execute a command corresponding to "/usr/local/bin/downcmd GC Time".

Example 3)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]	"/usr/local/bin/downcmd" memory
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Monitor Heap Memory Rate]	On
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Eden Space]	80
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Survivor Space]	80
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the usage rate of the Java Eden Space and that of the Java Survivor Space exceed 80% as many times, in succession, as specified by the Error Threshold (three times), the JVM monitor resources will detect a monitor error and execute a command corresponding to "/usr/local/bin/downcmd memory EdenSpace SurvivorSpace".

Timeout (seconds) for waiting for the completion of execution of the command specified by [Command] is set by specifying [Command Timeout] in the [JVM monitor] tab of the Cluster Properties window. The same value is applied to the timeout of [Command] of each of the above-mentioned tabs; the timeout cannot be specified for each [Command] separately.
If a timeout occurs, the system will not perform processing for forced termination of the

[Command] process; the operator must perform post-processing (e.g. forced termination) of the [Command] process. When a timeout occurs, the following message is output to the JVM operation log:

action thread execution did not finish. action is alive = <*command*>.

Note the following.

- No [Command] is executed when restoration of the Java VM to normal operation (error -> normal operation) is detected.
- [Command] is executed upon the detection of an error in the Java VM (when threshold exceeding occurs as many times, in succession, as specified by the error threshold). It is not executed at each threshold exceeding.
- Note that specifying [Command] on multiple tabs allows multiple commands to be executed if multiple errors occur simultaneously, causing a large system load.
- [Command] may be executed twice simultaneously when the following two items are monitored: [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, The Number]; [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, Average].

  This is because errors may be detected simultaneously for the following two items: [Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [WebLogic] tab - [Interval, The number of request]; [Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [WebLogic] tab - [Interval, The average number of the request]. To prevent this from occurring, specify only one of the two items as a monitor target. This applies to the following combinations of monitor items.

  - [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, The Number] and [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, Average]
  - [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, The Number] and [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, Average]

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 Builder tree view. See "Understanding JVM monitor resources".

3. Regarding the target server, select **Configuration-General**, and then check the port number though which a management connection is established with **Listen Port**.

4. Stop WebLogic Server. For how to stop WebLogic Server, refer to "Starting and stopping WebLogic Server" in the WebLogic Server manual.

5. Start the management server start script of WebLogic Server (startWebLogic.sh).

6. Write the following instructions in the script.

   - When the target is the WebLogic Server managing server:
     - ✓
     ```
     JAVA_OPTIONS="${JAVA_OPTIONS}
     -Dcom.sun.management.jmxremote.port=n
     -Dcom.sun.management.jmxremote.ssl=false
     -Dcom.sun.management.jmxremote.authenticate=false"
     ```
     *Write each line of coding on one line.

   - When the target is a WebLogic Server managed server:
     - ✓
     ```
     if [ "${SERVER_NAME}" = "SERVER_NAME" ]; then
      JAVA_OPTIONS="${JAVA_OPTIONS}
     -Dcom.sun.management.jmxremote.port=n
     -Dcom.sun.management.jmxremote.ssl=false
     -Dcom.sun.management.jmxremote.authenticate=false"
     fi
     ```
     *Write all the if statement lines (lines 2 to 5) on one line.

Note:
For ***n***, specify the number of the port used for monitoring. The specified port number **must be different from that of the listen port for the target Java VM.** If there are other target WebLogic Server entities on the same machine, specify a port number different from those for the listening port and application ports of the other entities.

Note:
For ***SERVER_NAME***, specify the name of the target server confirmed by **Select Target Server**. If more than one server is targeted, change the server name on the settings (line 1 to 6) for each server.

Note:
When the target is WebLogic Server 11gR1(10.3.3) or later, add the following options:

-Djavax.management.builder.initial=weblogic.management.jmx.

mbeanserver.WLSMBeanServerBuilder

Note:
Place the above addition prior to the following coding:

${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
-Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy ${PROXY_SETTINGS}
${SERVER_CLASS}

*Write the above coding on one line.

* The above java arguments differ depending on the WebLogic version. There is no problem by specifying JAVA_OPTIONS before using java.

Note:
For monitoring **Perm Gen[shared-ro]** or **Perm Gen[shared-rw]** on the **Memory** tab, add the following line:

-client –Xshare:on –XX:+UseSerialGC

7. Redirect the standard output and standard error output of the target WebLogic Server to a file. For how to configure these settings, refer to the WebLogic Server manual. Configure the settings if you want to include the standard output and standard error output in information to be collected. When configuring the settings, be careful to secure sufficient hard disk space.
8. Configure the settings so as to output the GC log to the target WebLogic Server. For how to configure these settings, refer to the WebLogic Server manual. Configure the settings if you want to include the GC log in information to be collected. When configuring the settings, be careful to secure sufficient hard disk space.
9. Make the following settings.

   Start WLST (wlst.sh) of the target WebLogic Server. On the console window displayed, execute the following commands:

   ```
   >connect('USERNAME','PASSWORD','t3://SERVER_ADDRESS:SERVER_PORT')
   > edit()
   > startEdit()
   > cd('JMX/DOMAIN_NAME')
   > set('PlatformMBeanServerUsed','true')
   > activate()
   > exit()
   ```

   Replace the **USERNAME**, **PASSWORD**, **SERVER_ADDRESS**, **SERVER_PORT**, and **DOMAIN_NAME** above with those for the domain environment.

10. Restart the target WebLogic Server.

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 and stopping administration tool" in the *WebOTX Operation (Web Administration Tool)*.

The settings differ depending on whether a Java process of the JMX agent running on WebOTX or the Java process of a process group is to be monitored. Configure the settings according to the target of monitoring.

Monitoring a Java process of the WebOTX domain agent

There is no need to specify any settings. If you are using V8.30, please upgrade to V8.31 or later.

Monitoring a Java process of a WebOTX process group

1. Connect to the domain by using the administration tool.
2. In the tree view, select **<domain_name>-TP System-Application Group-<application_group_name>-Process Group-<process_group_name>**.
3. For the **Other Arguments** attributes on the **JVM Options** tab on the right, specify the following Java options on one line. For ***n***, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monitor (special)** tab → **Connection Port**).

   ```
   -Dcom.sun.management.jmxremote.port=n
   -Dcom.sun.management.jmxremote.ssl=false
   -Dcom.sun.management.jmxremote.authenticate=false
   -Djavax.management.builder.initial=com.nec.webotx.jmx.mbeanserver.JmxMBeanServerBuilder
   ```

   * In the case of WebOTX V9.2 or later, it is unnecessary to specify -Djavax.management.builder.initial.

4. Then, click **Update**. After the configuration is completed, restart the process group.

   These settings can be made by using **Java System Properties,** accessible from the **Java System Properties** tab of the WebOTX administration tool. When making these settings by using the tool, do not designate -D and set the strings prior to = in name and set the strings subsequent to = in value.

Note:
If restart upon a process failure is configured as a function of the WebOTX process group, and when the process group is restarted as the recovery processing by EXPRESSCLUSTER, the WebOTX process group may fail to function correctly. For this reason, when monitoring the WebOTX process group, make the following settings for the JVM monitor resource by using the Builder.

Tab name for setting	Item name	Setting value
Monitor(common)	Monitor Timing	Always
Recovery Action	Recovery Action	Execute only the final action
Recovery Action	Final Action	No operation

Linking with the load balancer is not supported for WebOTX process group monitoring.

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

Monitoring JBoss

JBoss Enterprise Application Platform 6 and later versions support two management modes, namely, standalone mode and domain mode. When monitoring JBoss with the JVM monitor resources, the following three cases must be handled separately and in different ways.

- JBoss Enterprise Application Platform 5 or earlier
- Standalone mode of JBoss Enterprise Application Platform 6
- Domain mode of JBoss Enterprise Application Platform 6

This section describes how to configure a target JBoss to be monitored by the JVM monitor resource.

JBoss Enterprise Application Platform 5 or earlier

1. Stop JBoss, and then open (*JBoss_installation_path*)/bin/run.conf by using editor software.
2. In the configuration file, specify the following settings on one line. For ***n***, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monitor (special)** tab → **Connection Port**).

   ```
   JAVA_OPTS="${JAVA_OPTS}
   - Dcom.sun.management.jmxremote.port=n
   - Dcom.sun.management.jmxremote.ssl=false
   - Dcom.sun.management.jmxremote.authenticate=false"
   ```

3. Save the settings, and then start JBoss.
4. With Builder (table view → **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., JBoss). With Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monitor (Special)** tab → **Process Name**), set [com.sun.management.jmxremote.port=*n*] (*n* is the port number specified in 2).

Standalone mode of JBoss Enterprise Application Platform 6

1. Stop JBoss, and then open (*JBoss_installation_path*)/bin/standalone.conf by using editor software.
2. In the configuration file, specify the following settings. For ***n***, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Builder (table view - JVM Monitor Resource Name - Property - Monitor(special) tab - Connection Port).

   Add the following before "if ["x$JBOSS_MODULES_SYSTEM_PKGS" = "x"]; then".
   ```
   JBOSS_MODULES_SYSTEM_PKGS="org.jboss.logmanager"
   ```

   Add the following after "if ["x$JAVA_OPTS" = "x"]; then … fi:".
   ```
   JAVA_OPTS="$JAVA_OPTS
   -Xbootclasspath/p:$JBOSS_HOME/modules/org/jboss/logmanager/main/jbos
   s-logmanager-1.3.2.Final-redhat-1.jar"
   JAVA_OPTS="$JAVA_OPTS
   -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
   JAVA_OPTS="$JAVA_OPTS           -Dcom.sun.management.jmxremote.port=n
   -Dcom.sun.management.jmxremote.ssl=false
   -Dcom.sun.management.jmxremote.authenticate=false"
   ```

   * The storage directory and file name of jboss-logmanager-*.jar differ depending on the JBoss version. Therefore, specify the path accoding to the installation environment.

3. Save the settings, and then start JBoss.
4. With Builder (table view - 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. JBoss). With Builder (table view - JVM Monitor Resource Name - [Property] - [Monitor(special)] tab - Process Name), set "com.sun.management.jmxremote.port=*n*" (*n* is the port number specified in 2).

Domain mode of JBoss Enterprise Application Platform 6

1. With Builder (table view - 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. JBoss). With Builder (table view - JVM Monitor Resource Name - [Property] - [Monitor(special)] tab - Process Name), specify all the Java VM startup options so that JBoss can be uniquely identified.

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 (*Tomcat_installation_path*)/bin/catalina.sh by using editor software. If Tomcat is installed from rpm package, open /etc/sysconfig/tomcat6 or /etc/sysconfig/tomcat.
2. In the configuration file, for the Java options, specify the following settings on one line. For ***n***, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Builder (table view - **JVM Monitor Resource Name** - **Property** - **Monitor (special)** tab - **Connection Port**).

```
CATALINA_OPTS="${CATALINA_OPTS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false"
```

Note:
If edit file is catalina.sh, write the above addition prior to the following coding.

```
if [ "$1" = "debug" ] ; then
    if $os400; then
        echo "Debug command not available on OS400"
        exit 1
    else
```

3. Save the settings, and then start Tomcat.
4. With Builder (table view - **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). With Builder (table view - **JVM Monitor Resource Name** - **Property** - **Monito (special)** tab - **Process Name**), set "com.sun.management.jmxremote.port=*n*" (*n* is the port number specified in 2).

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 corresponding script.

Monitor target	Script to be edited
Simple Httpd Service (for 8.x)	<SVF installation path>/bin/SimpleHttpd
Simple Httpd Service (for 9.x)	<SVF installation path>/bin/UCXServer
RDE Service	<SVF installation path>/rdjava/rdserver/rd_server_startup.sh
	<SVF installation path>/rdjava/rdserver/svf_server_startup.sh
RD Spool Balancer	<SVF installation path>/rdjava/rdbalancer/rd_balancer_startup.sh
Tomcat (for 8.x)	<SVF installation path>/rdjava/apache-tomcat-5.5.25/bin/catalina.sh
Tomcat (for 9.x)	<SVF installation path>/apache-tomcat/bin/catalina.sh
SVF Print Spooler Service	<SVF installation path>/bin/spooler

2. In the configuration file, for the Java options, specify the following settings on one line. For ***n***, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monitor (special)** tab → **Connection Port**).

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false"
```

3. If the monitor target is RDE Service, add ${JAVA_OPTIONS} into the following startup path and rd_balancer_startup.sh.

```
java -Xmx256m -Xms256m -Djava.awt.headless=true ${JAVA_OPTIONS}
-classpath $CLASSPATH jp.co.fit.vfreport.RdSpoolPlayerServer &
```

4. With the Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monitor (special)** tab → **Identifier**), and with the Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monito (special)** tab → **Process Name**), specify the following.

Monitor target	Identifier, Process Name
Simple Httpd Service	SimpleHttpd
RDE Service	ReportDirectorServer
	RdSpoolPlayerServer
RD Spool Balancer	ReportDirectorSpoolBalancer
Tomcat (for 8.x)	Bootstrap
Tomcat (for 9.x)	-Dcom.sun.management.jmxremote.port=*n*
SVF Print Spooler Service	spooler.Daemon

Monitoring iPlanet Web Server

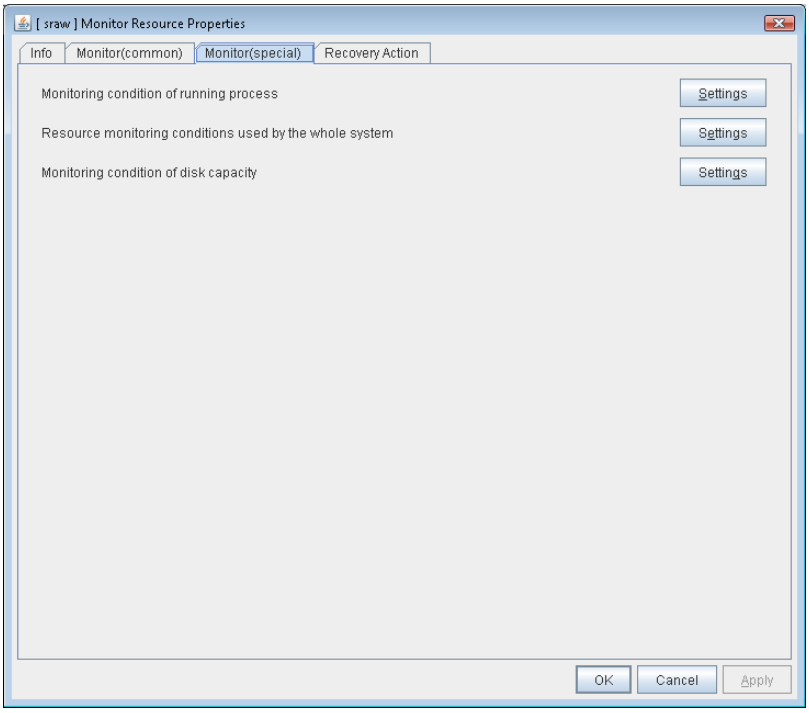
This section describes how to configure a target iPlanet Web Server to be monitored by the JVM monitor resource.

1. Stop the iPlanet Web Server, and then, using an editor, open (iPlanet Web Server installation path)/(monitored server name)/config/server.xml.
2. In /server/jvm/jvm-options, specify the following settings on one line. For ***n***, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Builder (table view → **JVM Monitor Resource Name** → **Property** → **Monitor (special)** tab → **Connection Port**).
```
<java-options>                    -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 the iPlanet Web Server.

Setting up system monitor resources

System monitor resources periodically collect statistical information about resources used by processes 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.

1. Click the **Monitors** icon on the tree view displayed on the left side of the Builder window.
2. A list of the monitor resources is displayed in the table view on the right side of the screen. Right-click the target system monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Property** window.
3. On the **Monitor(special)** tab, you can see and/or change the detailed settings as described below.



Settings

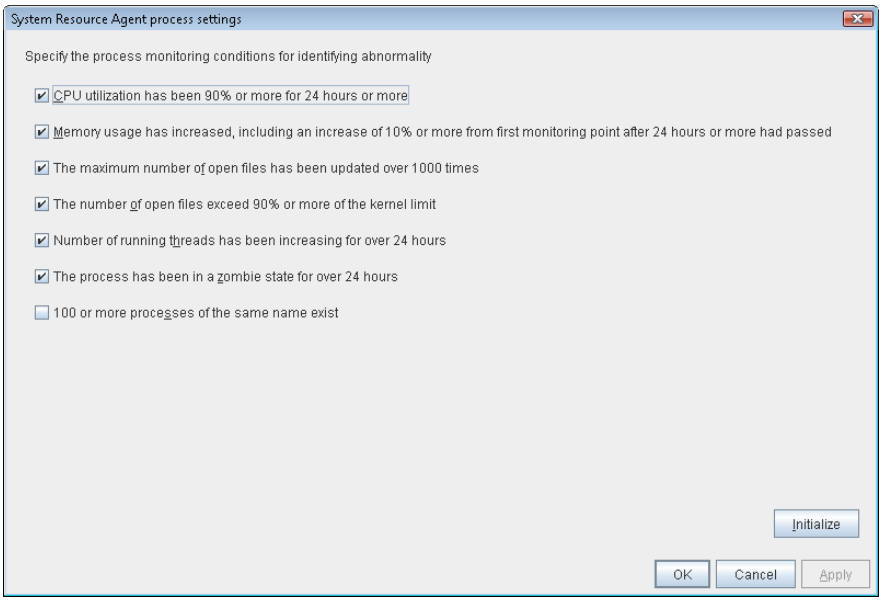
Click the **Settings** button for **Process detail settings**; the process settings dialog box appears.

Click the **Settings** button for **Resource monitoring conditions used by the whole system**; the system settings dialog box appears.

Click the **Settings** button for **Monitoring disk space**; the disk list dialog box appears.

Configure detailed settings for the monitoring of error detection according to the descriptions of the dialog boxes.

System Resource Agent process settings



CPU utilization has been 90% or more for 24 hours or more

Enables the monitoring of processes for which CPU utilization has been continuously 90% or more for 24 hours or more.

- When selected:
  Monitoring is enabled for processes for which CPU utilization has been continuously 90% or more for 24 hours or more.
- When cleared:
  Monitoring is disabled for processes for which CPU utilization has been continuously 90% or more for 24 hours or more.

Memory usage has increased, including an increase of 10% or more from first monitoring point after 24 hours or more had passed

Enables the monitoring of processes for which the memory usage has increased, including an increase of 10% or more from the first the monitoring point after 24 hours or more had passed.

- When selected:
  Monitoring is enabled for processes for which the memory usage has increased, including an increase of 10% or more from the first monitoring point after 24 hours or more has passed.
- When cleared:
  Monitoring is disabled for processes for which the memory usage has increased, including an increase of 10% or more from the first monitoring point after 24 hours or more has passed.

The maximum number of open files has been updated over 1000 times

Enables the monitoring of processes for which the maximum number of open files has been exceeded over 1000 times.

- When selected:
  Monitoring is enabled for processes for which the maximum number of open files has been exceeded over 1000 times.
- When cleared:
  Monitoring is disabled for processes for which the maximum number of open files has been exceeded over 1000 times.

The number of open files exceed 90% or more of the kernel limit

Enables the monitoring of processes for which the number of open files exceeds 90% or more of the kernel limit.

- When selected:
  Monitoring is enabled for processes for which the number of open files exceeds 90% or more of the kernel limit.
- When cleared:
  Monitoring is disabled for processes for which the number of open files exceeds 90% or more of the kernel limit.

Number of running threads has been increasing for over 24 hours

Enables the monitoring of processes for which the number of running threads has been increasing for over 24 hours.

- When selected:
  Monitoring is enabled for processes for which the number of running threads has been increasing for over 24 hours.
- When cleared:
  Monitoring is disabled for processes for which the number of running threads has been increasing for over 24 hours.

The process has been in a zombie state for over 24 hours

Enables the monitoring of processes that have been in a zombie state for over 24 hours.

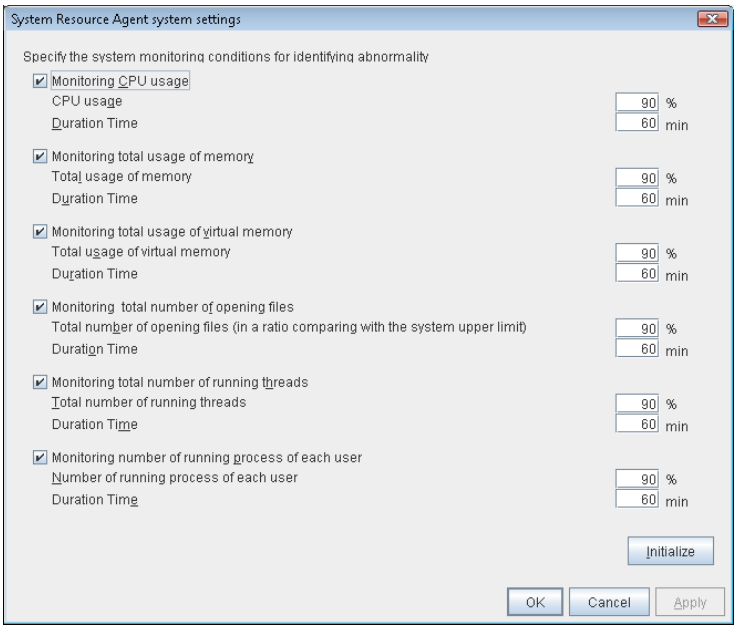
- When selected:
  Monitoring is enabled for processes that have been in a zombie state for over 24 hours.
- When cleared:
  Monitoring is disabled for processes that have been in a zombie state for over 24 hours.

100 or more processes of the same name exist

Enables the monitoring of processes for which there are 100 or more processes having the same name.

- When selected:
  Monitoring is enabled for processes for which there are 100 or more processes having the same name.
- When cleared:
  Monitoring is disabled for processes for which there are 100 or more processes having the same name.

System Resource Agent system settings



Monitoring CPU usage

Enables CPU usage monitoring.

- When selected:
  Monitoring is enabled for the CPU usage.
- When cleared:
  Monitoring is disabled for the CPU usage.

CPU usage (0 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 selected:
  Monitoring is enabled for the total usage of memory.
- When cleared:
  Monitoring is disabled for the total usage of memory.

Total usage of memory e (0 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 selected:
  Monitoring is enabled for the total **usage of virtual memory**.
- When cleared:
  Monitoring is disabled for the total **usage of virtual memory**.

Total usage of virtual memory (0 to 100)

Specify the threshold for the detection of a virtual memory usage error.

Duration Time (1 to 1440)

Specify the duration for detecting a total virtual memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total number of opening files

Enables the monitoring of the total number of open**ing** files.

- When selected:
  Monitoring is enabled for the total number of open**ing** files.
- When cleared:
  Monitoring is disabled for the total number of open**ing** files.

Total number of opening files (in a ratio comparing with the system upper limit) (0 to 100)

Specify the threshold for the detection of an error related to the total number of opening files (percentage of the system upper limit).

Duration Time (1 to 1440)

Specify the duration for detecting an error with the total number of opening files.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total number of running threads

Enables the monitoring of the total number of running threads.

- When selected:
  Monitoring is enabled for the total number of running threads.
- When cleared:
  Monitoring is disabled for the total number of running threads.

Total number of running **threads** (0 to 100)

Specify the threshold for the detection of an error related to the total number of running threads (percentage of the system upper limit).

Duration Time (1 to 1440)

Specify the duration for detecting an error with the total number of running threads.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring number of running processes of each user

Enables the monitoring of the number of processes being run **of each user**.

- When selected:
  Monitoring is enabled for the number of processes being run **of each user**.
- When cleared:
  Monitoring is disabled for the number of processes being run **of each user**.

Number of running processes of each user (0 to 100)

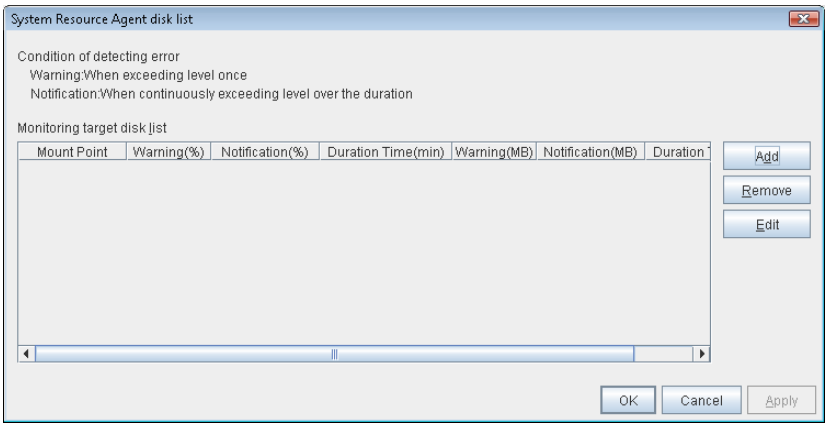
Specify the threshold for the detection of an error related to the number of processes being run **of each user** (percentage of the system upper limit).

Duration Time (1 to 1440)

Specify the duration for detecting an error with the number of processes being run **of each user**.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

System Resource Agent disk list



Add

Click this to add disks to be monitored. The **Input of watch condition** dialog box appears.

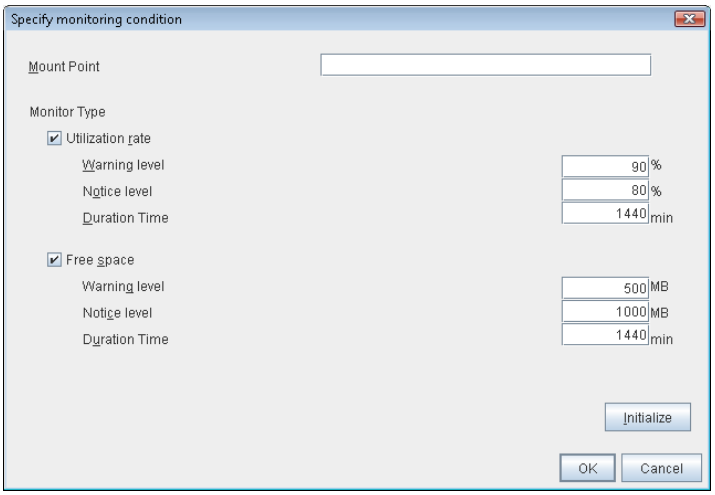
Configure the detailed monitoring conditions for error determination, according to the descriptions given in the **Input of watch condition** dialog box.

Remove

Click this to remove a disk selected in **Disk List** so that it will no longer be monitored.

Edit

Click this to display the **Input of watch condition** dialog box. The dialog box shows the monitoring conditions for the disk selected in **Disk List**. Edit the conditions and click **OK**.



Mount point (within 1,024 bytes)

Set the mount to be monitored. The name must begin with a forward slash (/).

Utillization rate

Enables the monitoring of the disk usage.

- When selected:
  Monitoring is enabled for the disk usage.
- When cleared:
  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 selected:
  Monitoring is enabled for the free disk space.
- When cleared:
  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.

Notes on system monitor resource

To use a system monitor resource, zip and unzip packages must have been installed on the servers.

System Resource Agent may output operation logging for each monitoring operation.

For the recovery target, specify the resource to which fail-over is performed upon the detection of an error in resource monitoring by System Resource Agent.

The use of the default System Resource Agent settings is recommended.

Errors in resource monitoring may be undetectable when:

- A value repeatedly exceeds and then falls below a threshold during whole system resource monitoring.

Swapped out processes are not subject to the detection of resource errors.

If the date or time of the OS has been changed while System Resource Agent is running, resource monitoring may operate incorrectly as described below since the timing of analysis which is normally done at 10 minute intervals may differ the first time after the date or time is changed.

If either of the following occur, suspend and resume cluster.

- No error is detected even after the specified duration for detecting errors has passed.
- An error is detected before the specified duration for detecting errors has elapsed.

Once the cluster has been suspended and resumed, the collection of information is started from that point of time.

For the SELinux setting, set permissive or disabled.

The enforcing setting may disable the communication needed by EXPRESSCLUSTER.

The amount of process resources and system resources used is analyzed at 10-minute intervals. Thus, an error may be detected up to 10 minutes after the monitoring session.

The amount of disk resources used is analyzed at 60-minute intervals. Thus, an error may be detected up to 60 minutes after the monitoring session.

Specify a value smaller than the actual disk size when specifying the disk size for free space monitoring of a disk resource. If a value is specified that is larger than the actual disk size, an error will be detected due to insufficient free space.

If the monitored disk has been replaced, analyzed information up until the time of the disk replacement will be cleared if one of the following items of information differs between the previous and current disks.

- Total disk capacity
- File system

Disk resource monitoring can only monitor disk devices.

For server for which no swap was allocated, uncheck the monitoring of total virtual memory usage.

Disk usage information collected by System Resource Agent is calculated by using the total disk space and free disk space. This value may slightly differ from the disk usage which df(1) command shows because it uses a different calculation method.

Up to 64 disk units can be simultaneously monitored by the disk resource monitoring function.

How system monitor resources perform monitoring

System monitor resources monitor the following:

Periodically collect the amounts of process resources, system resources and disk resources used and then analyze the amounts.

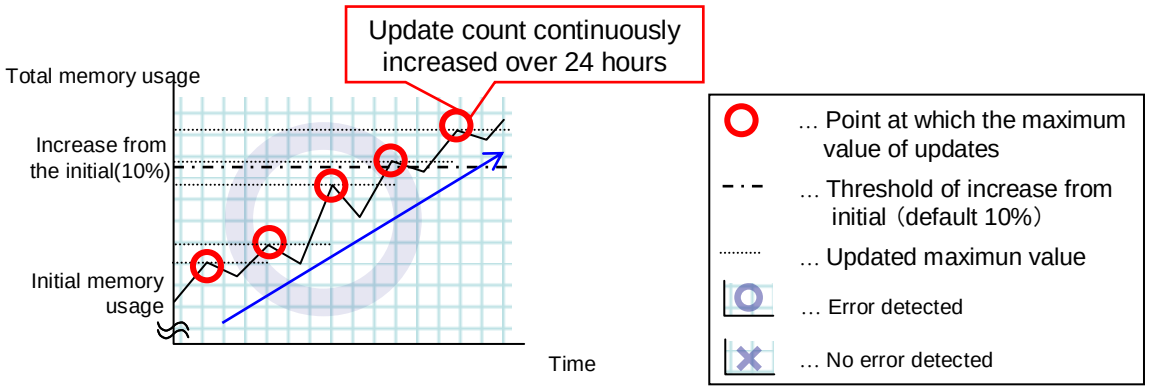
An error is recognized if the amount of a resource used exceeds a pre-set threshold.

When an error detected state persists for the monitoring duration, it is posted as an error detected during resource monitoring.

If process resource monitoring (of the CPU, memory, number of threads, or number of zombie processes) operated by using the default values, a resource error is reported after 24 hours.

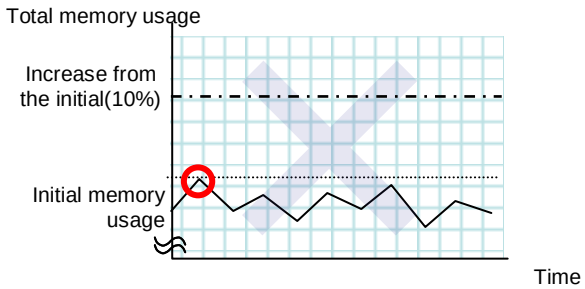
The following chart describes how process resource monitoring detects memory usage errors.

- In the following example, as time progresses, memory usage increases and decreases, the maximum value is updated more times than specified, and increases by more than 10% from its initial value.



→ Memory leak will be detected as memory usage continuously increased over 24hours (by default), and it increased more than 10% from its initial value.

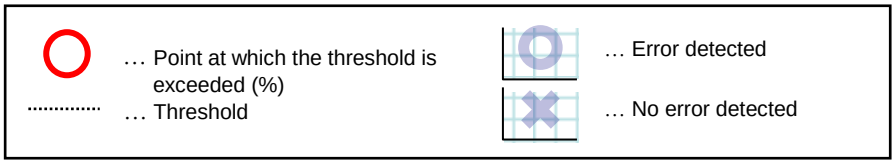
- In the following example, memory usage increases and decreases, but remains within a set range.



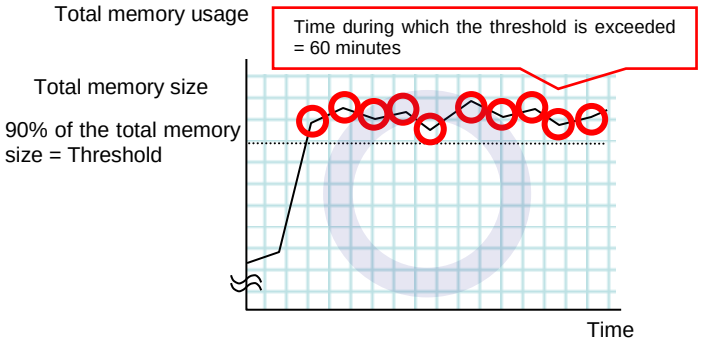
→ Memory leak will not be detected as memory usage repeat increasing and decreasing within certain range (below specific value).

System resource monitoring with the default values reports an error found in resource monitoring 60 minutes later if the resource usage does not fall below 90%.

The following shows an example of error detection for the total memory usage in system resource monitoring with the default values.

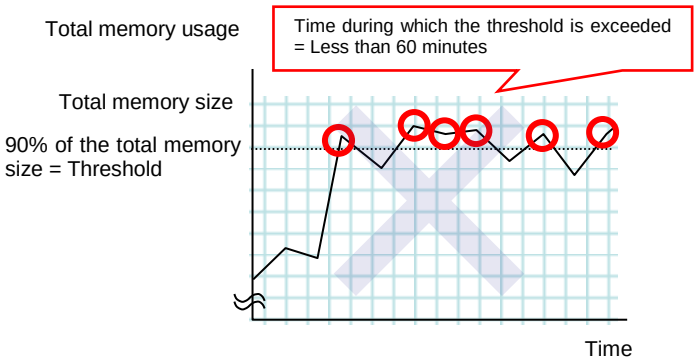


- The total memory usage remains at the total memory usage threshold or higher as time passes, for at least a certain duration of time.



→ The total memory usage remains at the threshold (90%) or higher continuously for the monitoring duration time (60 minutes) or longer; detection of a total memory usage error is recognized.

- The total memory usage rises and falls in the vicinity of the total memory usage threshold as time passes, but always remains under that threshold.



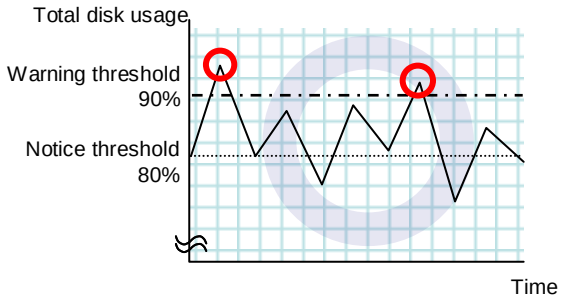
→ The total memory usage is temporarily at the total memory usage threshold (90%) or higher, but goes below the threshold before it remains at the threshold or higher continuously for the monitoring duration time (60 minutes); no total memory usage error is detected.

If disk resource monitoring operated under the default settings, it will report a notice level error after 24 hours.

The following chart describes how disk resource monitoring detects disk usage errors when operating under the default settings.

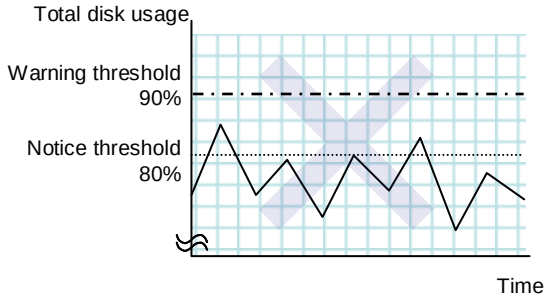
Monitoring disk usage by warning level

- In the faollowing example, disk usage exceeds the threshold which is specified as the warning level upper limit.



→ Disk usage error will be detected as disk usage exceed the threshold which configured as warning level upper limit.

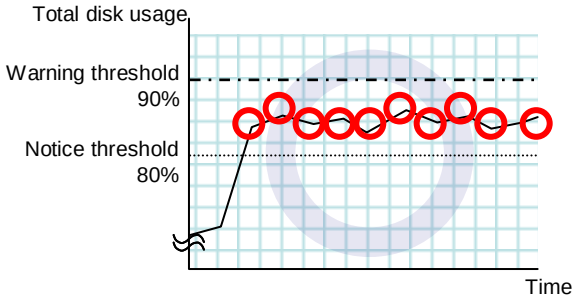
- In the faollowing example, disk usage increases and decreases within certain range, and does not exceed the threshold which is specified as the warning level upper limit.



→ Disk usage error will not be detected as disk usage repeat increasing and decreasing within certain range(below warning level upper limit).

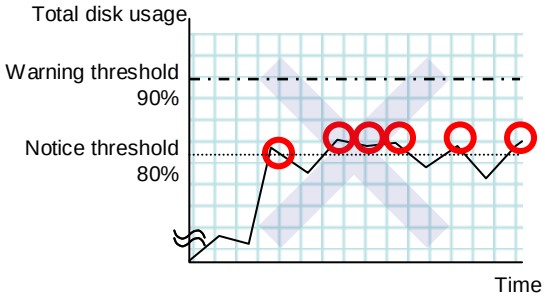
Monitoring disk usage by notice level

- In the faollowing example, disk usage continuously exceeds the threshold specified as the notification level upper limit, and the duration exceeds the set length.



→ Disk usage error will be detected as disk usage continuously exceed notice level upper limit.

- In the faollowing example, disk usage increases and decreases within a certain range, and does not exceed the threshold specified as the notification level upper limit.

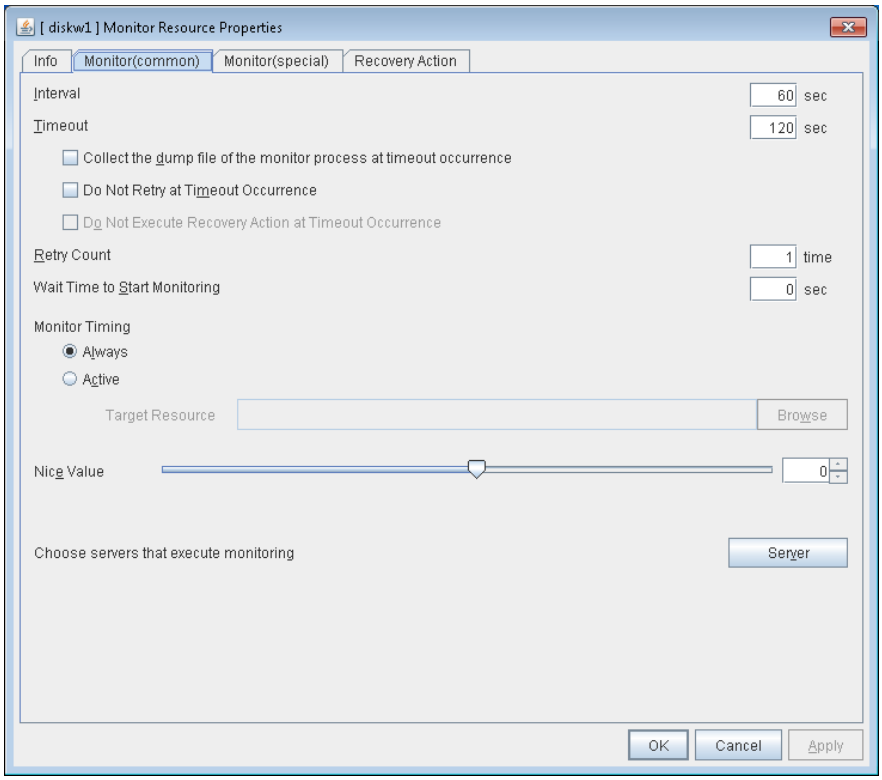


→ Disk usage error will not be detected as disk usage repeat increasing and decreasing around notice level upper limit.

Common settings for monitor resources

These settings are common to the monitor resources.

1. Setting up monitor processing



Interval (1 to 999)

Specify the interval to check the status of monitor target.

Timeout (5 to 999 [3])

When the normal status cannot be detected within the time specified here, the status is determined to be error.

Collect the dump file of the monitor process at timeout occurrence

In case that this function is enabled, the dump information of the timed out monitor resource is collected when the monitor resource times out. The collected dump information is written to the /opt/nec/clusterpro/work/rm/"monitor_resource_name"/errinfo.cur folder. When dump is performed more than once, the existing folders are renamed errinfo.1, errinfo.2, and so on. Dump information is collected up to 5 times.

Do Not Retry at Timeout Occurrence

When this function is enabled, recovery action is executed immediately if a monitor resource timeout occurs.

[3] The value of 255 or less is required to be set when configuring ipmi for monitoring method on User-Mode Monitor Resource.

Do not Execute Recovery Action at Timeout Occurrence

When this function is enabled, recovery action is not executed if a monitor resource timeout occurs.

This can be set only when the **Do Not Retry at Timeout Occurrence** function is enabled.

Note:

For the following monitor resources, the **Do Not Retry at Timeout Occurrence** and **Do Not Execute Recovery Action at Timeout Occurrence** functions cannot be set.

- user-mode monitor resources
- custom monitor resources (whose monitor type is **Asynchronous**)
- multi target monitor resources
- VM monitor resources
- message receive monitor resources
- JVM monitor resources
- system monitor resources

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 9,999)

Set the wait time to start monitoring.

Notes:

If timeout of monitor resource is longer than “Wait Time to start Monitoring”, the value of the timeout will be used for “Wait Time to Start Monitoring” for following monitor resources.

- Message receive monitor resource
- Custom monitor resource (whose monitor type is **Asynchronous**)
- DB2 Monitor Resource
- System Monitor Resource
- JVM Monitor Resource
- MySQL Monitor Resource
- Oracle Monitor Resource
- PostgresSQL Monitor Resource
- Process Name Monitor Resource
- Sybase Monitor Resource

Monitor Timing:

Set the monitoring timing.

[Always]
Monitoring is always performed.

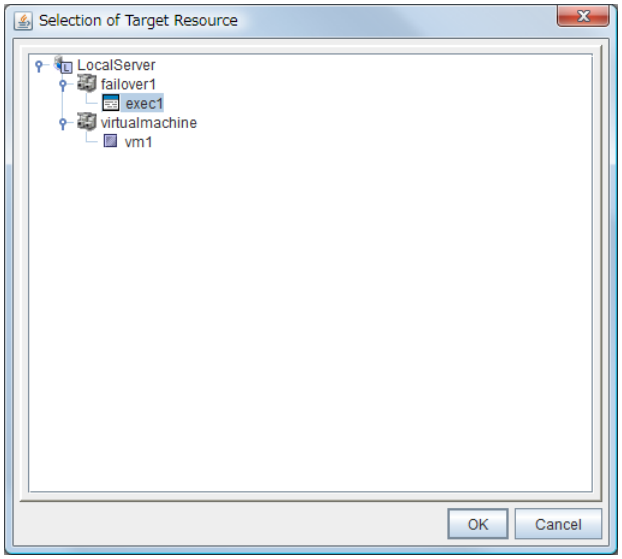
[While Activated]
Monitoring is not started until the specified resource is activated.

Target Resource:

The resource which will be monitored when activated is shown.

Browse

Click this button to open the dialog box to select the target resource. The group names and resource names that are registered in the LocalServer and cluster are shown in a tree view. Select the target resource and click **OK**.

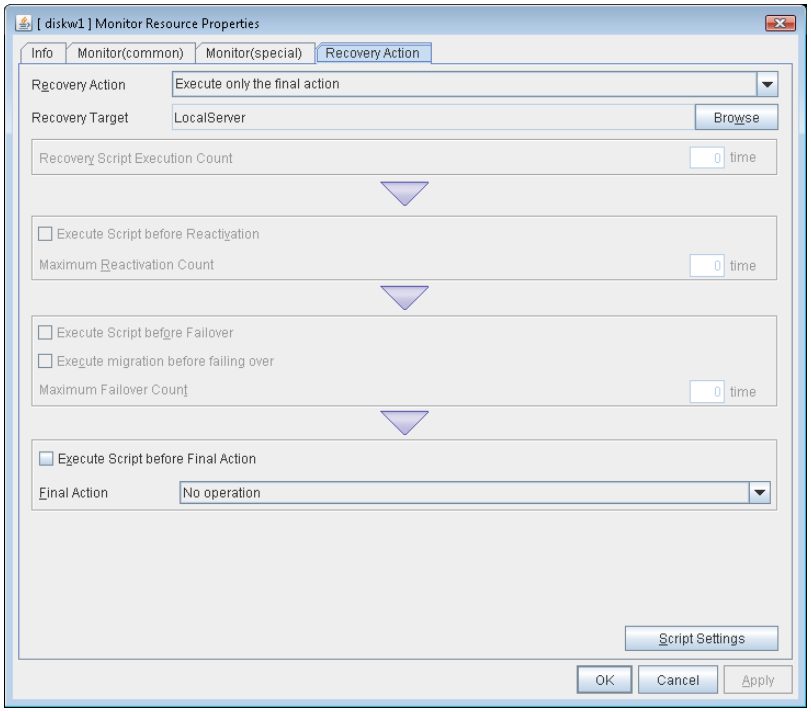


nice value

Set the nice value of a process.

2. Setting up the recovery processing

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 restart of the group, restart of the resource, and restart of the server when an error is detected. However, recovery will not occur if the recovery target is not activated.



Recovery Action

Specify the operation to perform when an error is detected.

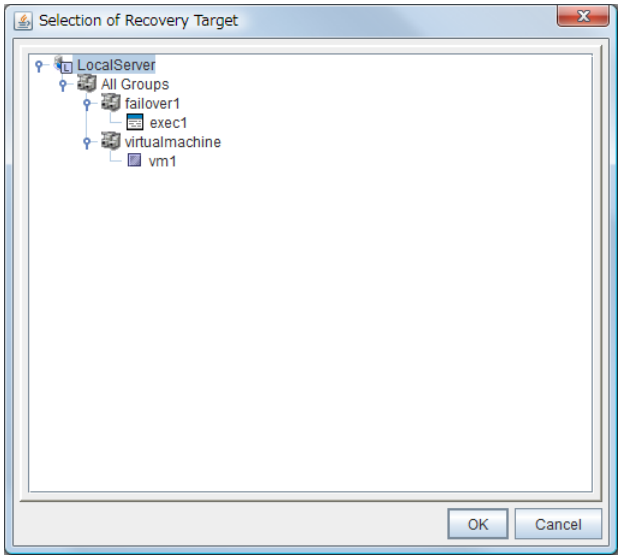
- **Restart the recovery target**
  Reactivate the selected group or group resource as the recovery target. When reactivation fails or the same error is detected after reactivation, execute the selected action as the final action.
- **Execute only the final action**
  Execute the selected action as the final action.
- **Custom setting**
  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 the selected action as the final action.

Recovery Target:

A target is shown, which is to be recovered when it is determined as a resource error.

Browse

Click this button to open the dialog box in which the target resource can be selected. The LocalServer, All Groups and group names and resource names that are registered in the cluster are shown in a tree view. Select the target resource and click **OK**.



Recovery Script Execution Count (0 to 99)

Specify the number of times to allow execution of the script configured by **Script Settings** when an error is detected. If this is set to zero (0), the script does not run.

Execute Script before Reactivation

- When selected:
  A script/command is executed before reactivation. To configure the script/command setting, click **Script Settings**.
- When cleared:
  Any script/command is not executed.

Max 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.

Execute Script before Failover

Not used.

Execute Migration before Failover

Not used.

Maximum Failover Count

Not used.

Execute Script before Final Action

Select whether script is run or not before executing final action.

- When selected:

  A script/command is run before executing final action. To configure the script/command setting, click **Script Settings**.

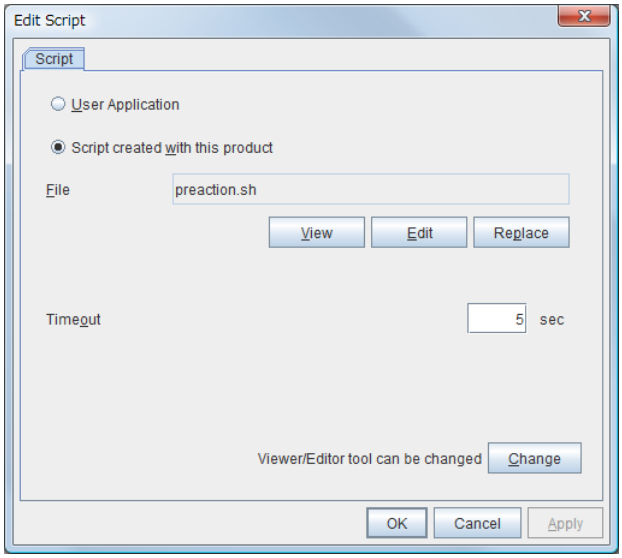
- When cleared:

  Any script/command is not run.

When clicking **Script Settings** of **Execute Script before Final Action, Edit Script** dialog box is displayed. Set script or script file, and click **OK**.

Script Settings

Click here to display the **Edit Script** dialog box. Configure the recovery or pre-recovery action script or commands.



User Application

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

Example:

```
“/tmp/user application/script.sh”
```

These executable files are not included in the configuration data of the Builder. As the files cannot be edited or uploaded, they are necessary to be prepared on the server.

Script created with this product

Use a script file which is prepared by the Builder as a script. You can edit the script file with the Builder if you need. The script file is included in the configuration data.

File (within 1,023 bytes)

Specify the script to be executed (executable shell script file or execution file) when selecting **User Application**.

View

Click here to display the script file with the editor when you select **Script created with this product**. The information edited and stored with the editor is not applied. You cannot display the script file if it is currently displayed or edited.

Edit

Click here to edit the script file with the editor when you select **Script created with this product**. Overwrite the script file to apply the change. You cannot edit the script file if it is currently displayed or edited. You cannot modify the name of the script file.

Replace

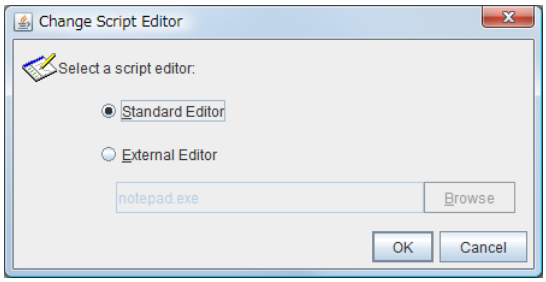
Click here to replace the content of the script file with that of the script file you selected in the file selection dialog box, when **Script created with this product** is selected. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not select binary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

Timeout (1 to 99)

Specify the maximum time to wait for completion of script to be executed. The default value is set as 5.

Change

Click here to display the **Change Script Editor** dialog box. You can change editor for displaying or editing a script to an arbitrary editor.



Standard Editor

Select this option to use the standard editor for editing scripts.

- Linux: vi (vi which is detected by the user's search path)
- Windows: Notepad (notepad.exe which is detected by the user's search path)

External Editor

Select here to specify an arbitrary script editor. Click Browse to specify the editor to be used.

To specify a CUI-based external editor on Linux, create a shell script.

The following is a sample shell script to run vi:

```
xterm -name clpedit -title "Cluster Builder" -n "Cluster Builder" -e
vi "$1"
```

Final Action:

Select the recovery action to perform after a recovery attempt through reactivation fails.

Select the final action from the following:

- **No Operation**
  No action is taken.

  Note:

  Select **No Operation** only when temporarily canceling the final action,displaying only an alert when an error is detected, and executing the final action by multi target monitor resource.

- **Stop Resource**

  When a group resource is selected as a recovery target, the selected group resource and group resources that depend on the selected group resource are stopped.
  This option is disabled when “LocalServer”, “All Groups”, or a group is selected.

- **Stop Group**

  When a group is selected as a recovery target, that group is stopped. When a group resource is selected as a recovery target, the group that the group resource belongs is stopped. When "All Groups" is selected, stop all the groups running on the server of which the monitor resource has detected errors. This option is disabled when a cluster is selected as a recovery target.

- **Stop cluster service**

  EXPRESSCLUSTER X SingleServerSafe is stopped.

- **Stop cluster service and shut down OS**

  EXPRESSCLUSTER X SingleServerSafe is stopped, and the OS is shut down.

- **Stop cluster service and reboot OS**

  EXPRESSCLUSTER X SingleServerSafe is stopped, and the OS is rebooted.

- **sysrq Panic**

  Performs the sysrq panic.

  Note:

  If performing the sysrq panic fails, the OS is shut down.

- **Keepalive Reset**

  Resets the OS using the clpkhb or clpka driver.

  Note:

  If resetting keepalive fails, the OS is shut down.
  Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported.

- **Keepalive Panic**

  Performs the OS panic using the clpkhb or clpka driver.

  Note:

  If performing the keepalive panic fails, the OS is shut down.
  Do not select this action on the OS and kernel where the clpkhb and clpka drivers are not supported.

- **BMC reset**

  Perform hardware reset on the server by using the ipmi command.

  Note:

  If resetting BMC fails, the OS is shut down.
  Do not select this action on the server where the ipmitool or ipmiutil is not installed, or the ipmitool command, the hwreset command or the ireset command does not run.

- **BMC power off**

  Powers off the OS by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

  Note:

  If powering off BMC fails, the OS is shut down.
  Do not select this action on the server where the ipmitool or ipmiutil is not installed, or the ipmitool command, the hwreset command or the ireset command does not run.

- **BMC power cycle**

  Performs the power cycle (powering on/off) of the server by using the ipmi command. OS shutdown may be performed due to the ACPI settings of the OS.

  Note:
  If performing the power cycle of BMC fails, the OS is shut down.
  Do not select this action on the server where the ipmitool or ipmiutil is not installed, or the ipmitool command, the hwreset command or the ireset command does not run.

- **BMC NMI**

  Uses the ipmi command to cause NMI occur on the server. The behavior after NMI is generated depends on the OS settings.

  Note:
  If BMC NMI fails, the OS shutdown is shut down.
  Do not select this action on the server where the ipmitool or ipmiutil is not installed, or the ipmitool command, the hwreset command or the ireset command does not run.

Chapter 6 Heartbeat resources

This chapter provides detailed information on heartbeat resources.

This chapter covers:

Heartbeat resources list

The heartbeat resource is used to monitor whether servers are activated. Heartbeat device types are:

Heartbeat Resource Name	Abbreviation	Functional Overview
LAN heart beat resource	lanhb	Uses a LAN to monitor if servers are activated.

- You need to set one LAN heartbeat resource.

Setting up LAN heartbeat resources

Notes on LAN heartbeat resources

- You need to set one LAN heartbeat resource.

Chapter 7 Details of other settings

This chapter provides details about the other items to be specified for EXPRESSCLUSTER X SingleServerSafe.

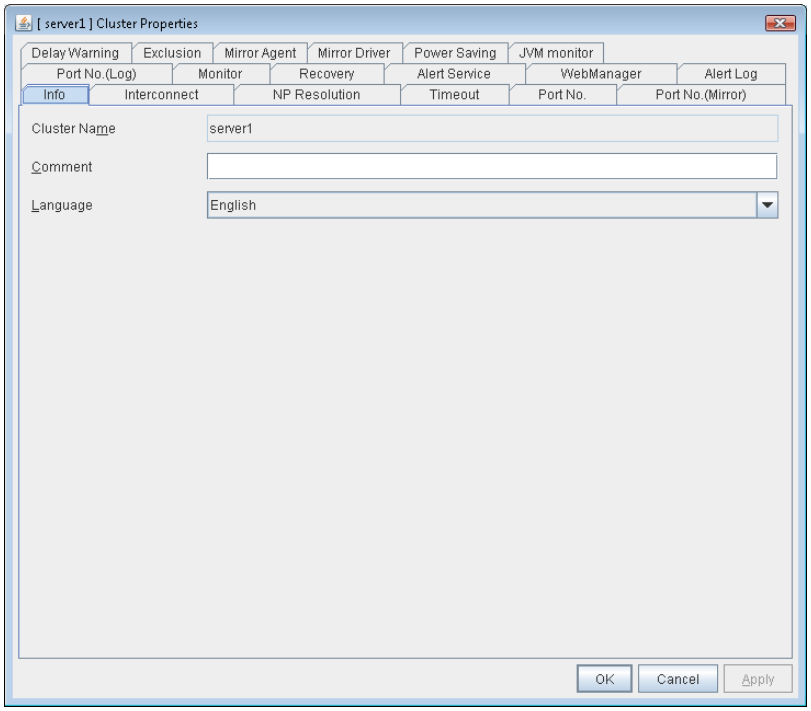
This chapter covers:

Cluster properties

In the **Cluster Properties** window, you can view and change the detailed data of EXPRESSCLUSTER X SingleServerSafe.

Info tab

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



Name:

Displays the server name. You cannot change the name here.

Comment (within 127 bytes)

Enter a new comment. You can only enter one byte English characters.

Language

Choose one of the display languages below. Specify the language (locale) of OS on which the WebManager runs.

- English
- Japanese
- Chinese

Interconnect tab

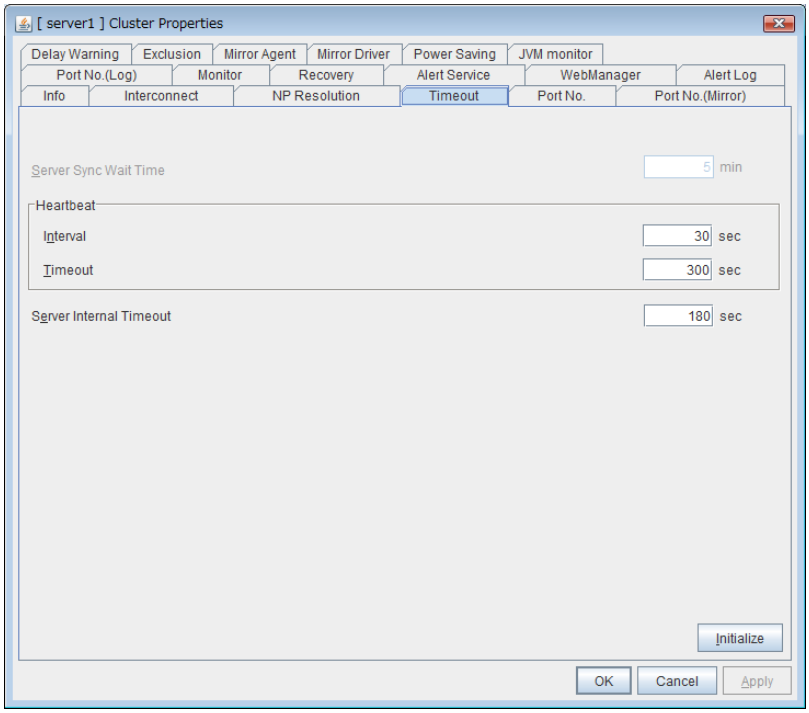
Not used.

NP Resolution tab

Not used.

Timeout tab

Specify values such as time-out on this tab.



Server Sync Wait Time (0 to 99)

Not used.

Heartbeat

Heartbeat interval and heartbeat time-out.

- **Interval** (1 to 99)

  Interval of heartbeats.

- **Timeout** (2 to 9999)

  A failed server is determined if there is no response for the time specified here.

- This time-out should be longer than the interval.
- To perform the shutdown monitoring (see on page 279), this time-out should be longer than the time it takes to shut down applications and the operating system.

Server Internal Timeout (1 to 9999)

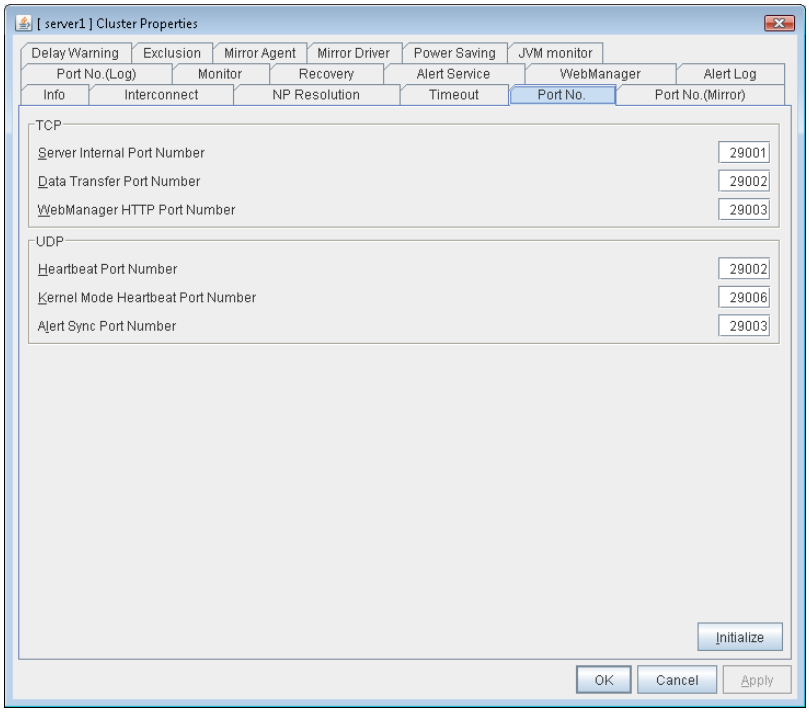
The time-out to be used in the EXPRESSCLUSTER Server internal communications.

Initialize

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

Port No. tab

Specify TCP port numbers and UDP port numbers.



TCP

No TCP port numbers can be overlapped.

- Internal communication port number (1 to 65,535 [4])
  This port number is used for internal communication.
- Data transfer port number (1 to 65,535 [4])
  This port number is used for transactions such as applying and backing up the configuration data, sending and receiving the license data, and running commands.
- WebManager HTTP Port Number (1 to 65,535 [4])
  This port number is used for a browser to communicate with the EXPRESSCLUSTER Server.

UDP

No UDP port numbers can be overlapped.

- Kernel mode heartbeat port number (1 to 65,535 [4])
  This port number is used for the kernel mode heartbeat.
  Not used.
- Alert synchronous port number (1 to 65,535 [4])
  This port number is used to synchronize alert messages between servers.

Initialize

This operation is used to return the value to the default value. Clicking the **Initialize** button resets the values of all items to the default values.

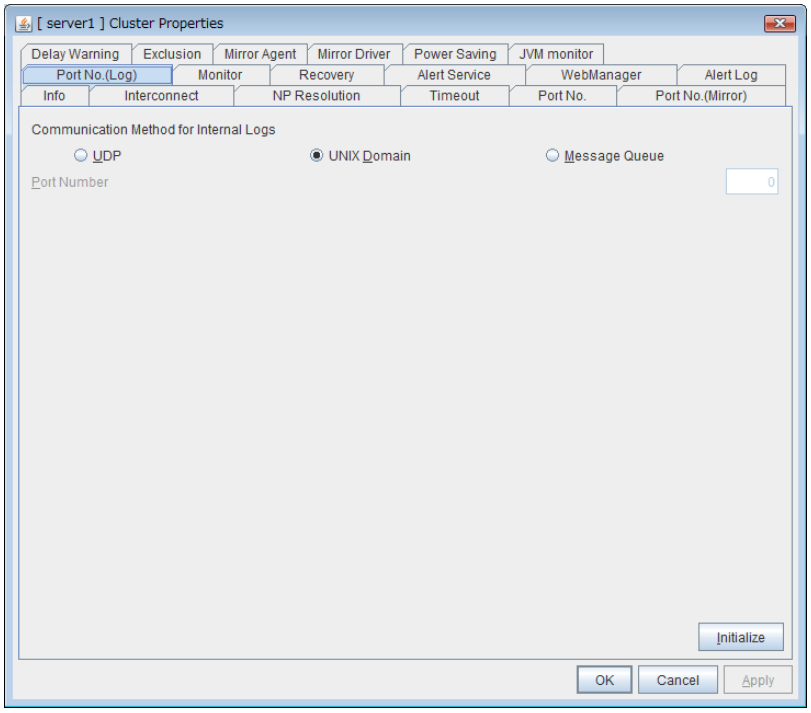
[4] It is strongly recommended not to use well-known ports, especially reserved ports from 1 to 1,023.

Port No. (Mirror) tab

Not used.

Port No. (Log) tab

Specify the communication method for internal logs.



Communication Method for Internal Logs

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

Note:

UDP cannot be used with SuSE Linux Enterprise Server 11.

Port No.(1 to 65535)

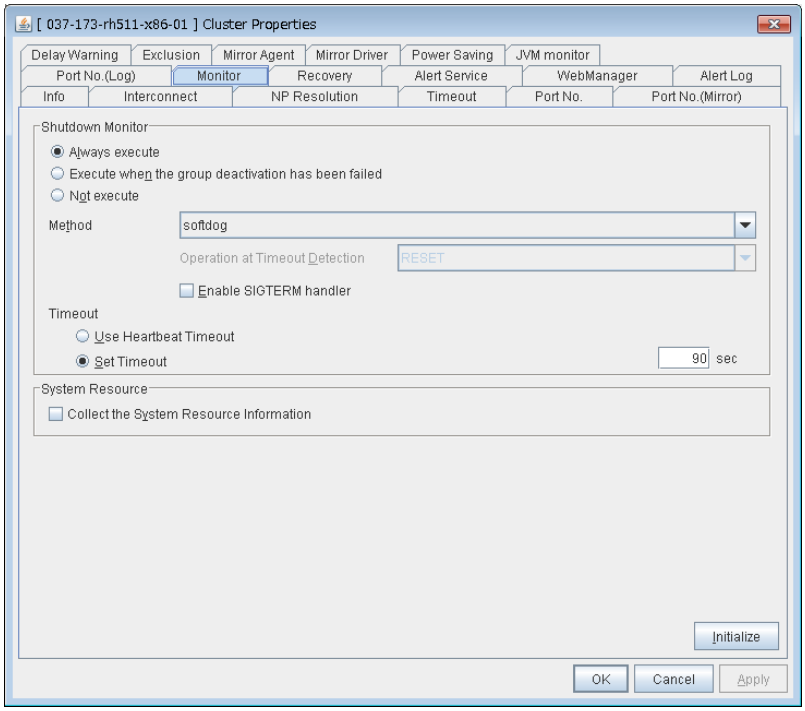
This is the port number used when UDP is selected for the communication method for internal logs.

Initialize

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

Monitor tab

Configure the settings for monitoring.



Shutdown Monitor

Monitors whether or not the operating system is stalling when an EXPRESSCLUSTER command to shut down the server is run. The cluster service forcibly resets the operating system or performs a panic of the operating system if it determines the OS stall. Server panic can be set when the monitoring method is keepalive.

- **Always execute:**

  If selected, the shutdown monitor is performed. For the heartbeat time-out, specify a longer time than the time required to shut down every application and the operating system (see “Timeout tab” on page 275).

- **Execute when the group deactivation has been failed:**

  The shutdown monitor is applied only when a group cannot be deactivated. For the heartbeat time-out, specify a longer time than the time required to shut down every application and the operating system (see “Timeout tab” on page 275).

- **Not execute:**

  If selected, the shutdown monitor is not performed.

- **Method**

  Select the shutdown monitor method from:

  - softdog
  - ipmi
  - keepalive

- **Operation at Timeout Detection**

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

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

- **Enable SIGTERM handler**

  Select this to enable SIGTERM handler when performing the shutdown monitor.

  Note:

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

- **Use Heartbeat Timeout**

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

- **Timeout (2 to 9999)**

  Specify a time-out when the heartbeat time-out value is not used as shutdown monitoring time-out.

System Resource

Select whether to collect system resource information.

System resource information is collected regularly so as to improve system operability.

- When the check box is selected

  System resource information related to the CPU, memory, processes, and others is collected regularly while the server is running.

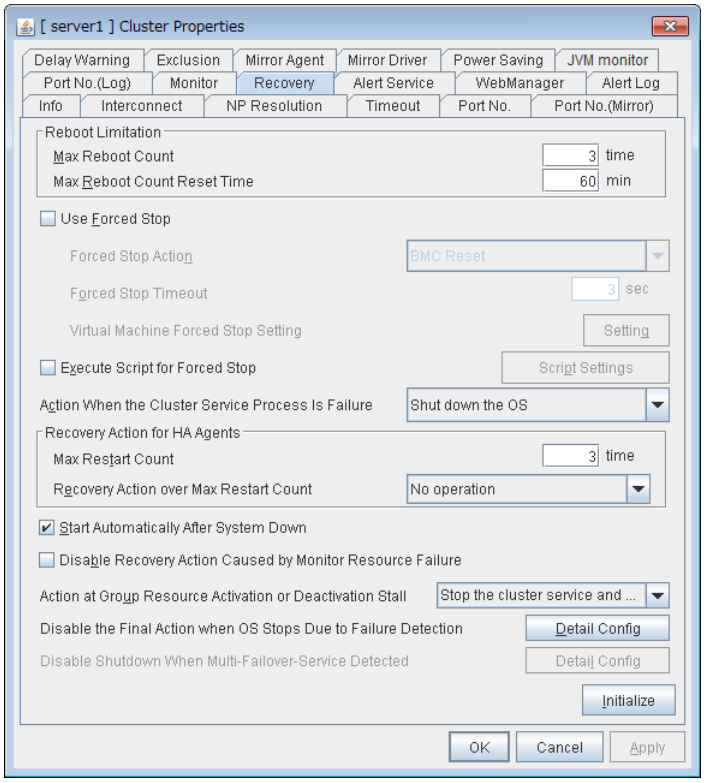
  The collected system resource information is collected when the `clplogcc` command or WebManager collects logs. When collecting logs, specify Pattern 1 or type1. A disk area of 450 MB or more is required to store the resource information, depending on the system operating conditions such as the number of processes that are running.

- When the check box is cleared

  No system resource information is collected.

Recovery tab

Specify the settings for recovery.



Reboot Limitation

In case that the final action of the group resource and the monitor resource when an error is detected is configured so that the OS reboot accompanies, reboot may be repeated infinitely. By setting the reboot limit, you can prevent repeated reboots.

- **Max Reboot Count** (0 to 99)

  Specify how many times the operating system can reboot. The number specified here is separately counted for group resource and monitor resource.

- **Max Reboot Count Reset Time** (0 to 999)

  When the max reboot count is specified, if the operation from the cluster startup keeps running normally for the time specified here, the reboot count is reset. The time specified here is separately counted for group resource and monitor resource.

Note:

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

Use Forced Stop

Not used.

Forced stop action

Not used.

Forced Stop Timeout (0 to 99)

Not used.

Virtual Machine Forced Stop Setting

Not used.

Execute Script for Forced Stop

Not used.

Script Setting

Not used.

Action When the Cluster Service Process Is Abnormal

Specify the action against process error in daemon.

- Shut down OS

  Shuts down the OS.

- Reboot OS

  Reboots the OS.

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 cluster service
    Stops the cluster service of the server that detected an error.
  - Stop cluster service and shutdown OS
    Stops the cluster service of the server that detected an error, and then shuts down the OS.
  - Stop cluster service and reboot OS
    Stops the cluster service of the server that detected an error, and then reboots the OS.

Note:

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

Start Automatically After System Down

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

Disable Recovery Action Caused by Monitor Resource Error

- When the checkbox is selected

  The recovery action is disabled when the monitor resource is error.

- When the checkbox is cleared

  The recovery action is enabled when the monitor resource is error.

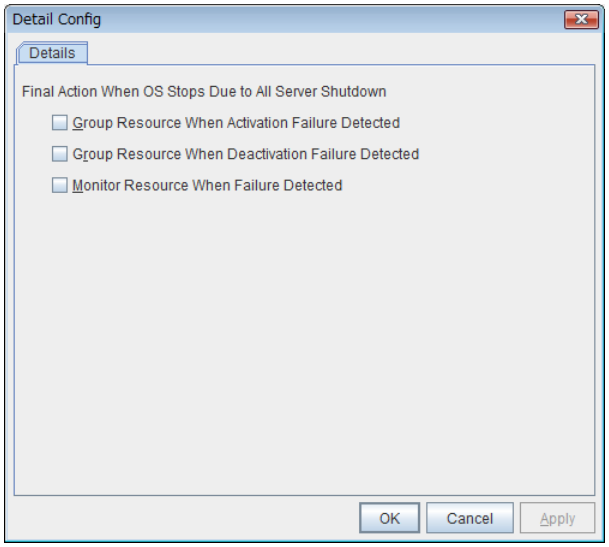
Note:
When recovery action was disabled, recovery action caused by monitor resource error is not performed. Even if this function is enabled, recovery from a group resource activation failure will still be performed.

This function is not available on the monitor in user mode.

This option is not available for the message receive monitor resource.

Disable the Final Action when OS Stops Due to Failure Detection

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



- **Group Resource When Activation Failure Detected**

  If the final action caused by an activation error detection in a group resource accompanies the OS stop, the final action is suppressed.

- **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.

- **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.

Note:

- The message receive monitor resource does not become the target for which the final action caused by error detection is suppressed.

- The following situations lead to an OS stop during the final action when an activation/deactivation error is detected in a group resource and during the final action when a monitor resource error is detected.
  - Cluster service stop and OS shutdown
  - Cluster service stop and OS restart
  - sysrq panic
  - keepalive reset
  - keepalive panic
  - BMC reset
  - BMC power off
  - BMC power cycle
  - BMC NMI

Disable Shutdown When Multi-Failover Detected

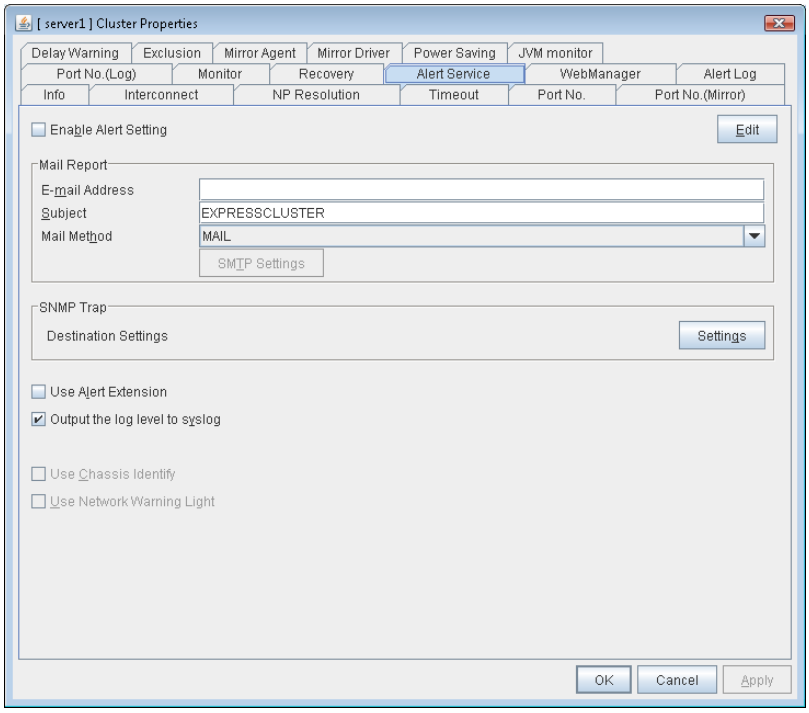
Not used.

Alert Service tab

Configure alert notification settings.

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

Note:
To use the mail report function, purchase EXPRESSCLUSTER X Alert Service 3.3 for Linux and register your license.



Enable Alert Setting

Configures whether or not to modify the default value of the alert settings. To modify the settings, click **Edit** to configure the destination address.

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

For the predefined alert destinations, refer to the "syslog and alert mail report messages" in the *Operation Guide*.

E-mail Address (within 255 bytes)

Enter the mail address of alert destination. To specify multiple mail addresses, separate each of them by semi-colon ";".

Subject (within 127 bytes)

Enter the mail subject.

Mail Method

Configure the mail method.

- MAIL
  This method uses the mail command. Check that a mail is sent to the mail address by using the mail command in advance.
- SMTP
  This method allows mailing through direct communication with the SMTP server.

Use Alert Extension

Configure whether or not to execute an optional command when EXPRESSCLUSTER sends an alert. For using Alert Extension function, select **Enable Alert Setting**, and click **Edit** to configure the command.

By canceling **Enable Alert Setting**, the configured command is temporarily disabled.

Output logging levels in syslog

Output syslog messages produced by EXPRESSCLUSTER X SingleServerSafe during operation with their levels.

Use Chassis Identify

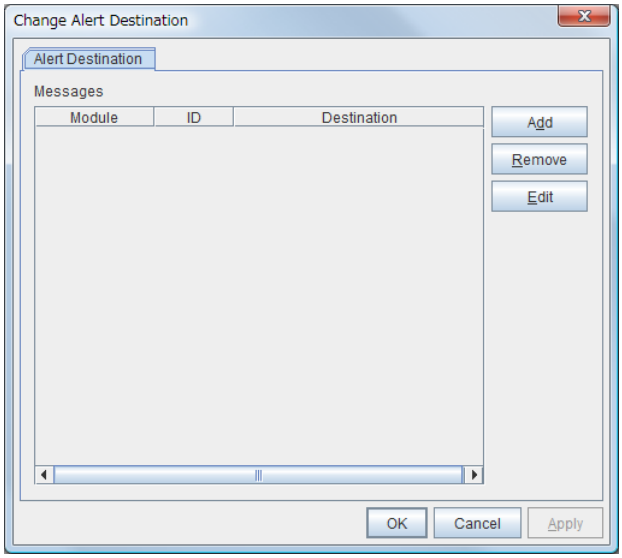
Not used.

Use Network Warning Light

Not used.

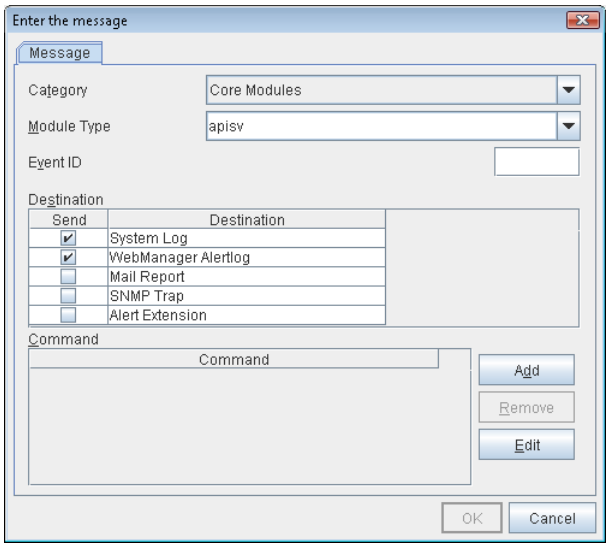
Change Alert Destination

Select **Edit** to display the dialog box where you can change alert destination.



Add

Add module types or event IDs for which the destinations are to be customized. Click **Add** to open the dialog box for entering the message.



Category

Select a main category of module types.

Module Type (within 31 bytes)

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

Event ID

Enter the event type of the module type for which you want to change the destination address. For the event ID, refer to "syslog and alert mail report messages" in the *Operation Guide*.

Destination

Select a message destination from the following options.

- System Log
  This sends message to syslog of the OS.
- WebManager Alertlog
  This sends messages to the alert view of the WebManager.
- Alert Extension
  This executes the specified function by using the alert extension function. Modify the extension settings by using the **Add** button and/or the **Edit** button. (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.

Add

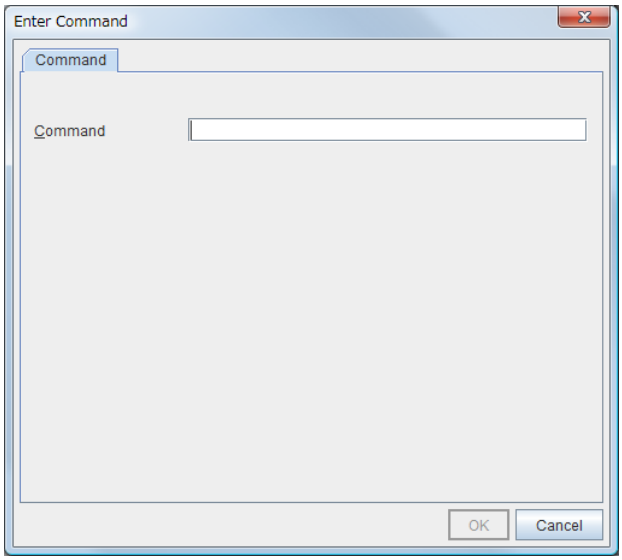
Add a command of the alert extension function. Click **Add** button to display the dialog box for entering a command. Up to 4 commands can be registered with one event ID.

Remove

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

Edit

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



Command (within 511 bytes)

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

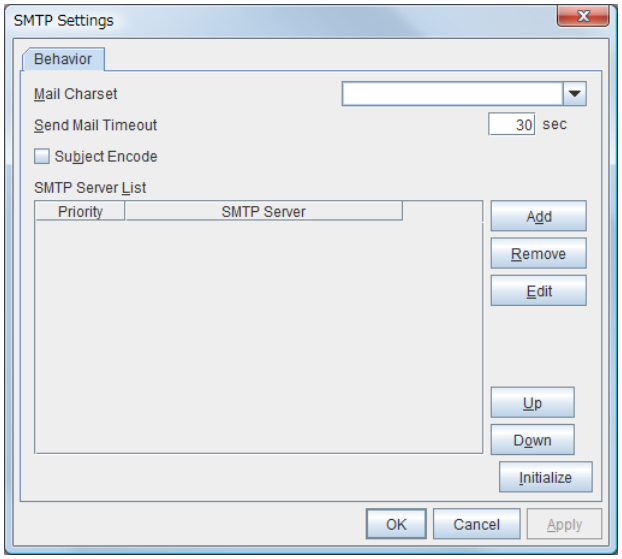
- Keyword
  If you specify **%%MSG%%**, the body message of the target event ID is inserted.
  You cannot specify multiple %%MSG%% for one command.
  Configure the command within 511 bytes including the description of %%MSG%%. As blank characters can be included in %%MSG%%, specify as ”%%MSG%%” when specifying it for a command argument.

Setting example

```
/usr/local/bin/snmptrap -v1 -c HOME 10.0.0.2 0 10.0.0.1 1 0 ‘’
1 s “%%MSG%%”
```

SMTP Settings

Click this to display the **SMTP Settings** dialog box which is 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 the communication with SMTP server.

Subject Encode

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

SMTP Server List

Use this button to display a SMTP server that has been configured. Only one SMTP server can be configured in this version.

Add

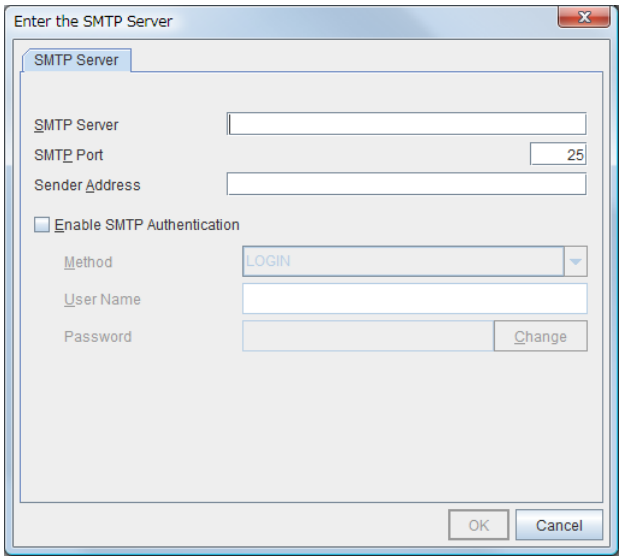
Use this button to add a SMTP server. Click **Add** to open the **Enter the SMTP Server** dialog box.

Remove

Select this to remove the SMTP server.

Edit

Use this button to modify the settings of SMTP server.



SMTP Server (within 255 bytes)

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

SMTP Port (1 to 65,535)

Configure the port number of the SMTP server.

Sender Address (within 255 bytes)

Configure the address from which mail report is sent.

Enable SMTP Authentication

Configure whether or not to enable SMTP authentication.

Authority Method

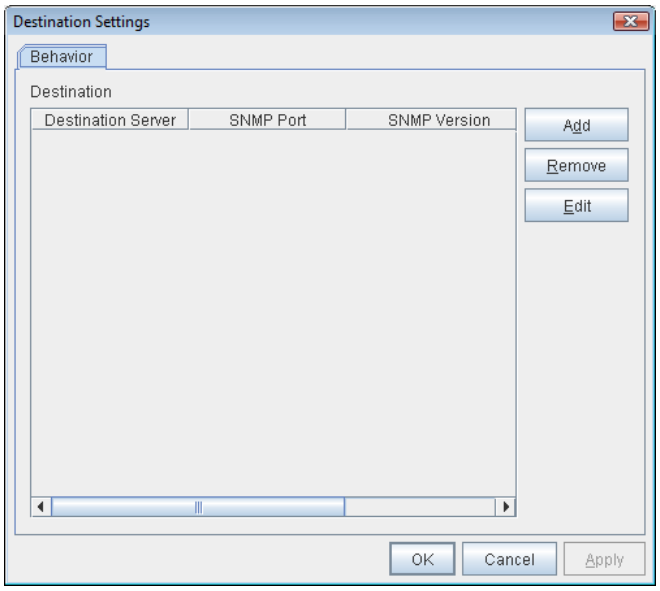
Select a method of SMTP authentication.

User Name (within 255 bytes)

Configure the user name used for SMTP authentication.

Password (within 255 bytes)

Configure the password used for SMTP authentication.



Destination

Displays the set SNMP trap transmission destinations. With this version, up to 255 SNMP trap transmission destinations can be set.

Add

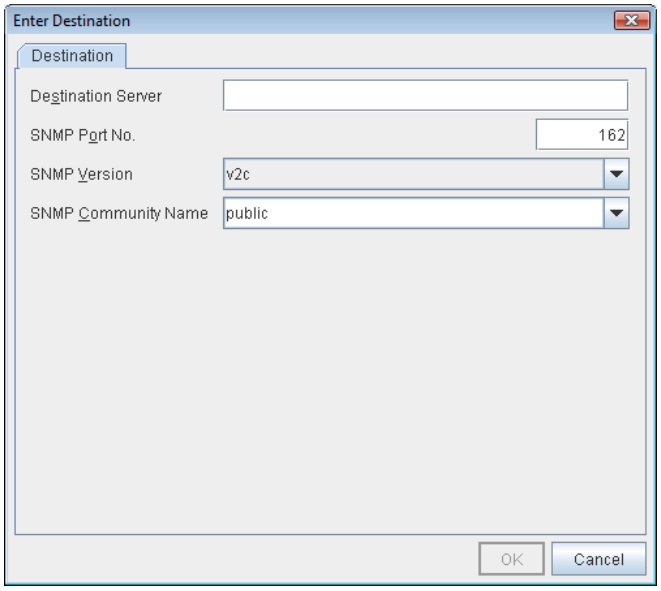
Adds an SNMP trap transmission destination. Click **Add** to display the Change SNMP Destination dialog box.

Remove

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

Edit

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



Destination Server (up to 255 bytes)

Configure the name of the SNMP trap transmission destination server.

SNMP Port (1-65535)

Configure the port number of the SNMP trap transmission destination.

SNMP Version

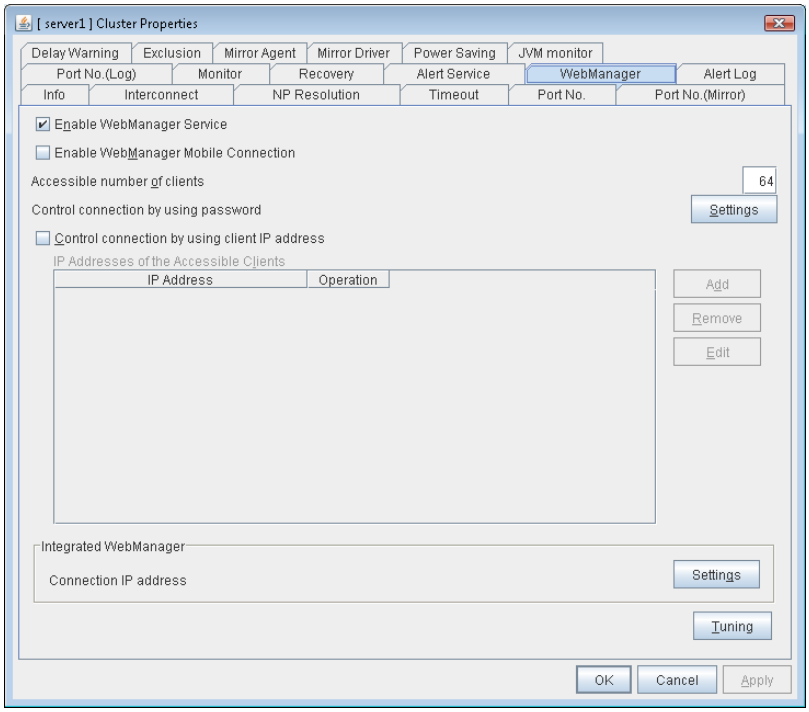
Configure the SNMP version of the SNMP trap transmission destination.

SNMP Community Name (up to 255 bytes)

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

WebManager tab

Use this tab to configure the settings for the WebManager.



Enable WebManager Service

The WebManager service is enabled.

- When selected:

  The WebManager service is enabled.

- When cleared:

  The WebManager service is disabled.

Enable WebManager Mobile Connection.

- When selected:

  The WebManager Mobile is enabled.

- When cleared:

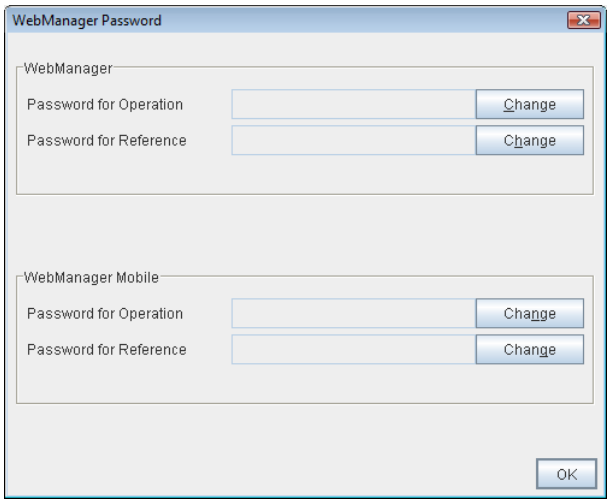
  The WebManager Mobile is disabled.

Accessible number of clients (1 to 999)

Specify the number of client machines that can be connected.

Control connection by using password

Click the **Settings** button to open the **WebManager Password** dialog box.



WebManager

- **Password for Operation**

Set a password that must be entered to enable connection to the WebManager in operation mode, config mode, or simulate mode.
Click **Change** to display the **Change Password** dialog box.

- **Password for Reference**

Set a password that must be entered to enable connection to the WebManager in reference mode. Click **Change** to display the **Change Password** dialog box.

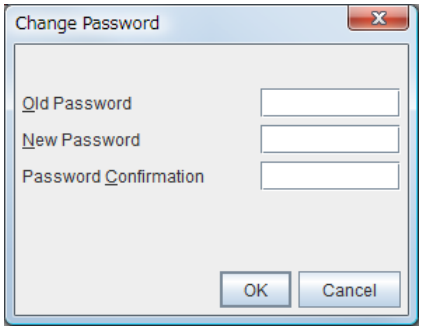
WebManager Mobile

- **Password for Operation**

Set a password that must be entered to enable connection to the WebManager in operation mode.
Click **Change** to display the **Change Password** dialog box.

- **Password for Reference**

Set a password to connect to the WebManager in the reference mode.
Click **Change** to display the **Change 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**.

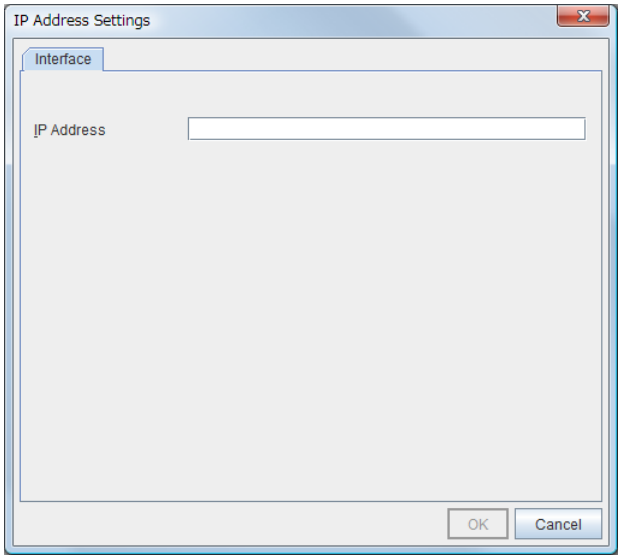
Control connection by using client IP address

If selected, accesses are controlled by client IP addresses.

- When selected:
  Add, **Remove** and **Edit** are enabled.
- When cleared:
  Add, **Remove** and **Edit** are disabled.

Add

Use **Add** to add an IP address in **IP Addresses of the Accessible Clients**. By clicking **Add**, the **IP Address Settings** dialog box is displayed to enter an IP address. 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 **IP Addresses of the Accessible Clients**. Select an IP address you want to remove in **IP Addresses of the Accessible Clients** and click **Remove**.

Edit

Use **Edit** to change an IP address. Select an IP address you want to edit in **IP Addresses of the Accessible Clients** and click **Edit**. A dialog box where the specified IP address is preset is displayed. The rights for operating the edited IP addresses remain the same.

Note:
The client IP address used to allow this connection is also used to restrict connections for external operations using clprexec.

Control connection by using client IP address

Sets the operation rights for IP addresses that are registered in **IP Addresses of the Accessible Clients**.

◆ When selected:

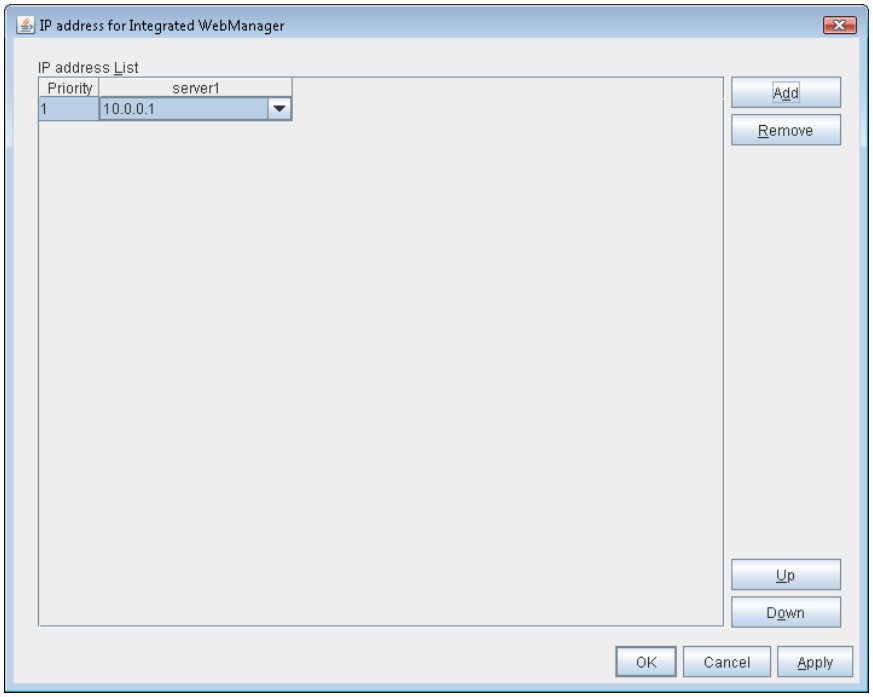
A client can operate EXPRESSCLUSTER X SingleServerSafe and display its status.

◆ When cleared:

The client can only display the status of EXPRESSCLUSTER X SingleServerSafe.

IP address for Integrated WebManager

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



- Add

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

- Remove

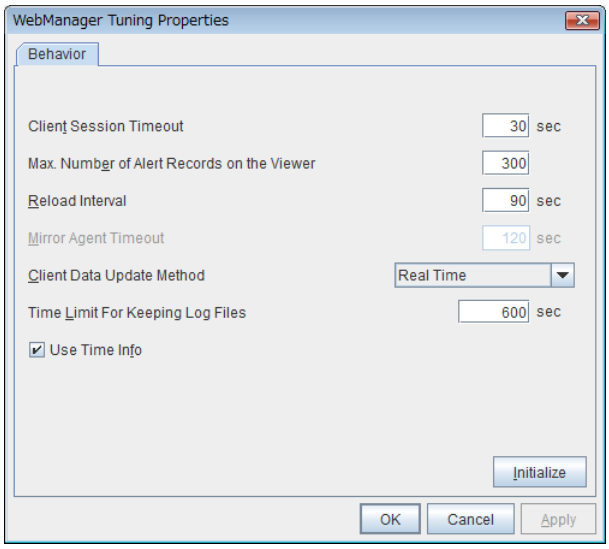
Remove the communication path. Select the communication path to be removed and click **Remove**, then the selected path is removed.

- Up, Down

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 **Up** and **Down** to change the order of the selected row.

Tuning

Use **Tuning** to tune the WebManager. Click **Tuning** to open the **WebManager Tuning Properties** dialog box.



- Client Session Timeout (1 to 999)

A timeout is determined if the time specified here elapses after the last communication between the WebManager server and the WebManager.

- Max. Number of Alert Records on Viewer (1 to 999)

Specify the maximum number of alert viewer records to display on the **Alert Viewer** of the WebManager.

- Screen data update interval (0 to 999)

At this time interval, the WebManager screen is refreshed.

- Mirror agent timeout (1 to 999)

A timeout is determined if the time specified here elapses till the mirror disk information is acquired.

◆ Client Data Update Method

You can select the method to update the screen data of the WebManager from the following.

- Polling
  The screen data is updated regularly.
- Real Time
  The screen data is updated on the real time.

◆ Time Limit For Keeping Log Files (60 to 43,200)

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 Display Function**
  Specify whether the time information display function is enabled or disabled.

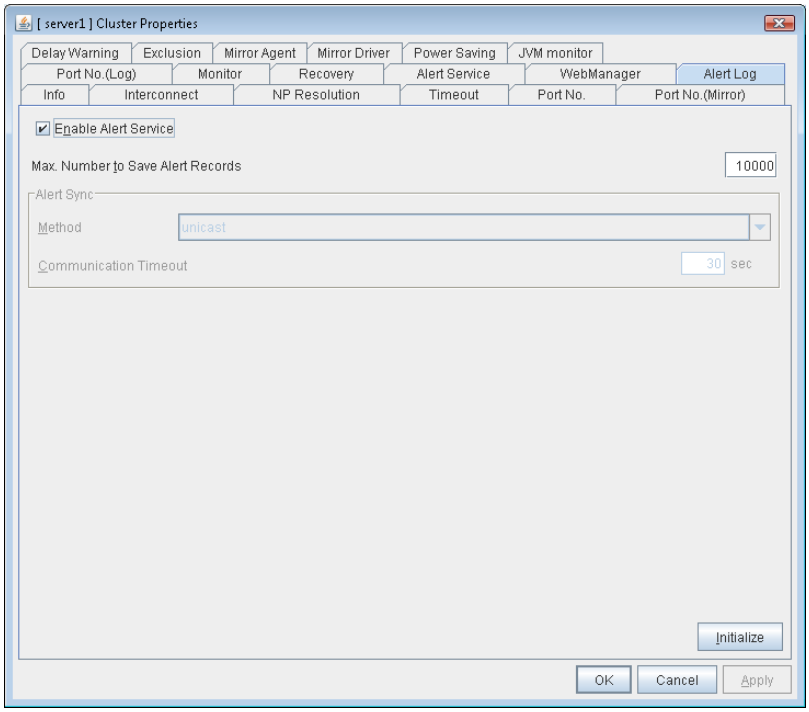
- When selected:
  The time information display function is enabled.
- When cleared:
  The time information display function is disabled.

◆ Initialize

This operation is used to return the value to the default value. Clicking the **Initialize** button resets the values of all items to the default values.

Alert Log tab

Configure the settings for the alert log.



Enable Alert Service

Select this to start alert service for the server.

- When selected:

Alert service is enabled.

- When cleared:

Alert service is disabled.

Max. Number to Save Alert Records (1 to 99,999)

Alert service for server can retain alert messages up to this number.

Alert Sync: Method

Not used.

Alert Sync: Communication Timeout (1 to 300)

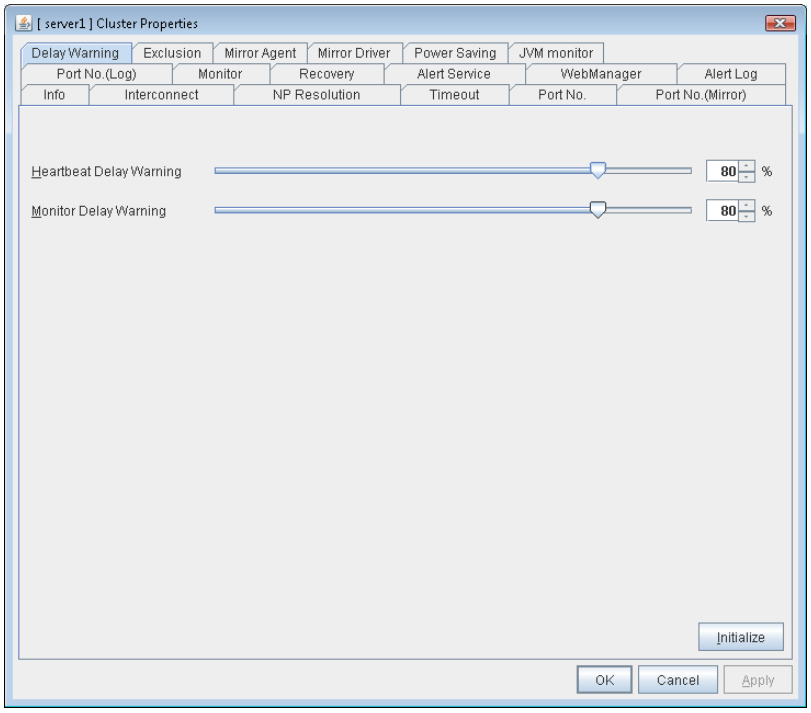
Not used.

Initialize

This operation is used to return the value to the default value. Clicking the **Initialize** button resets the values of all items to the default values.

Delay Warning tab

Specify the settings for **Delay Warning** on this tab. For details about **Delay Warning**, see "Delay warning of a monitor resource" in "Chapter 8 Monitoring details".



Heartbeat Delay Warning (0 to 100)

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

Monitor Delay Warning (0 to 100)

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

Note:

If you specify 0% for the delay warning, an alert log is shown in every heartbeat interval and monitor interval.

Setting 0% allows you to see the time spent for monitoring. This will be helpful particularly in a test operation.

Make sure not to set low values such as 0% in the production environment.

Exclusion tab

Not used.

Mirror Agent tab ~ For the Replicator/Replicator DR~

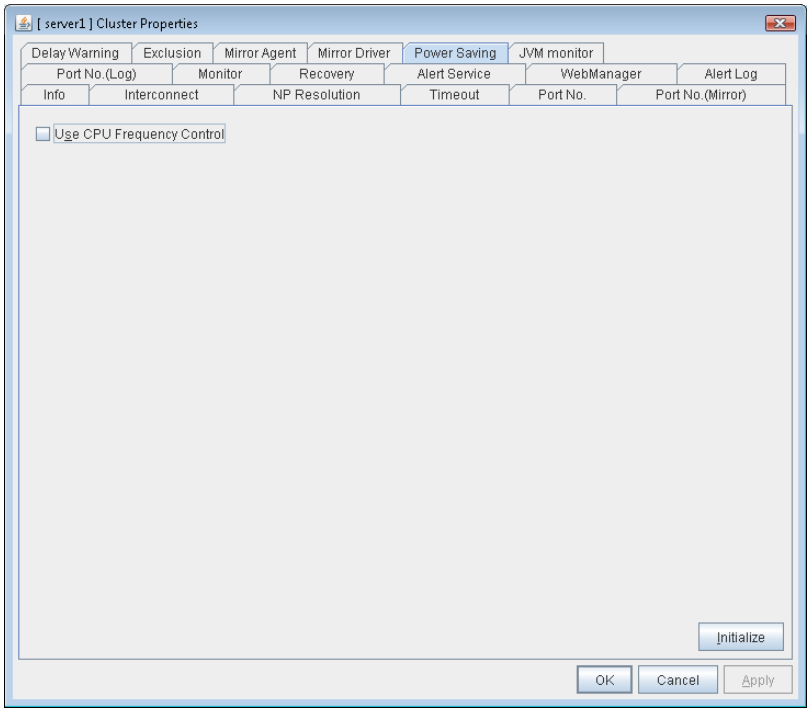
Not used.

Mirror driver tab ~ For Replicator/Replicator DR ~

Not used.

Power saving tab

Configure whether or not to use the function to turn it to power-saving mode by controlling the CPU frequency of the standby server.



Use CPU Frequency Control

Select the checkbox when you use CPU frequency control.

Select the checkbox to set the CPU frequency to high at group activation and set the CPU frequency of the server to low after group deactivation.

Clear the checkbox to disable the CPU frequency control.

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

- When selected:

CPU frequency control is performed.

- When cleared:

CPU frequency control is not performed.

Initialize

This operation is used to return the value to the default value. Clicking the **Initialize** button resets the values of all items to the default values.

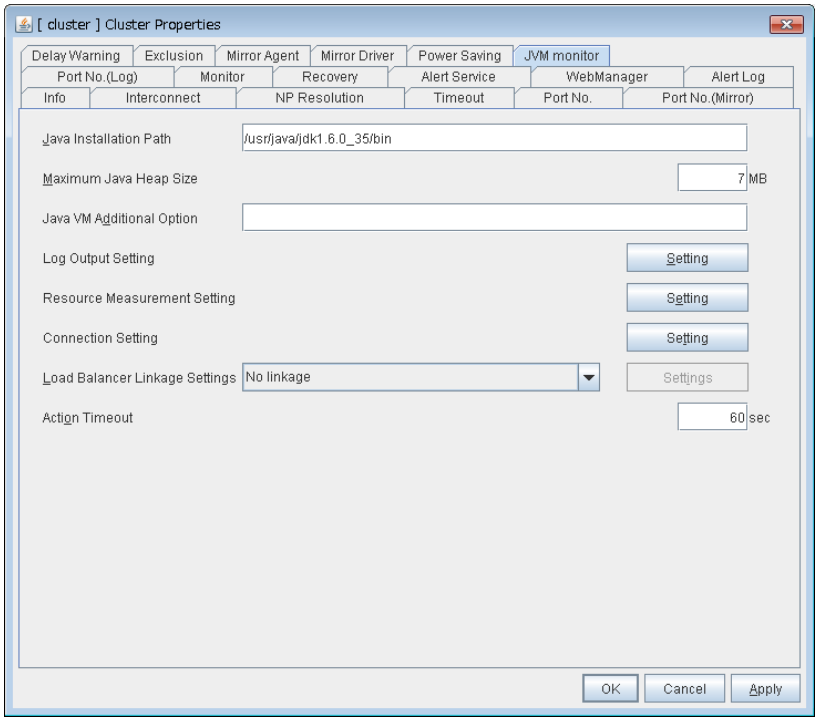
Note:
To perform CPU frequency control, the frequency must be changeable with a BIOS setting, the CPU must support frequency control by the OS power management function, and the kernel must support such control.

JVM monitor tab

Configure detailed parameters for the JVM monitor.

NOTE:

To display the **JVM monitor** tab on the online version Builder, you need to execute **Update Server Info** from the **File** menu after the license for Java Resource Agent is registered.



Java Installation Path (up to 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.

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. If using Oracle's Java, specify more than 7. Specify if the JRockit is more than 16.

Java VM Additional Option (up to 1024 bytes)

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

Log Output Setting

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

Resource Measurement Setting

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

Connection Setting

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

Load Balancer Linkage Setting

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

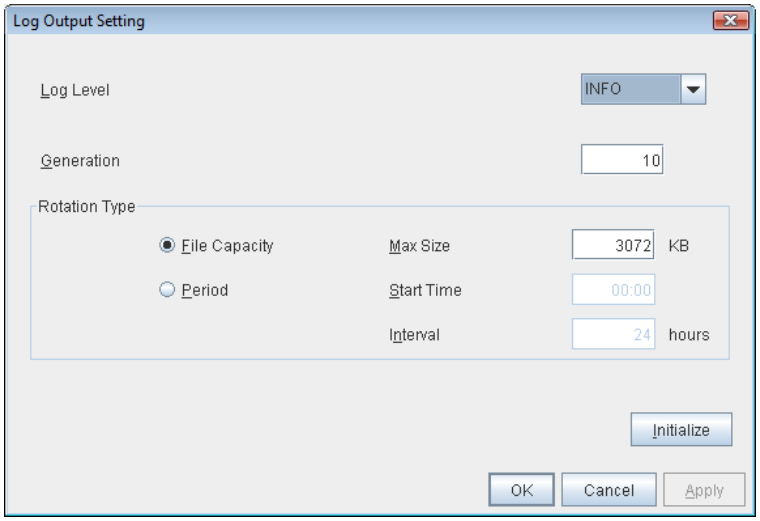
Select the load balancer type from the list. To perform load balancer linkage, select the load balancer you are using. To cancel the load balancer linkage, select **No linkage**.

Action Timeout (30 to 300)

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

Log Output Setting

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



Log Level

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

Generation (2 to 100)

Set the number of generations to be retained for log output by the JVM monitor.

Rotation Type

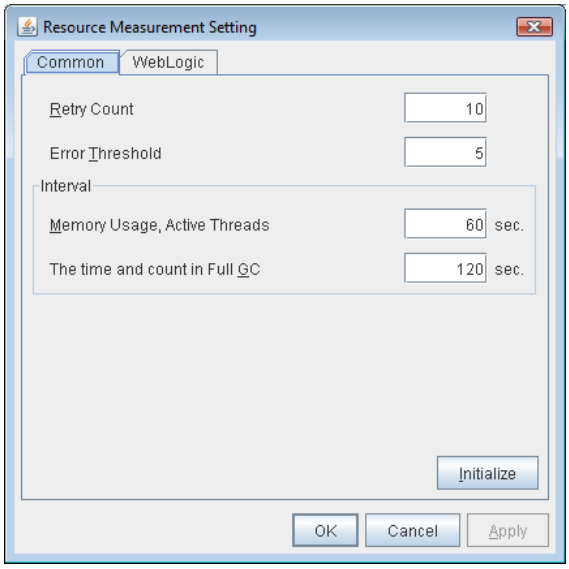
Select a rotation type for the log output by the JVM monitor. If you select **File Capacity** as the rotation type, set the maximum size (200 to 2097151), in kilobytes, for each log file such as the JVM operation log. If you select **Period** as the rotation type, set the log rotation start time in "hh:mm" 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 Settings [Common]

Clicking **Setting** displays the **Resource Measurement Settings** dialog box. For details on the scheme for error judgment by the JVM monitor, see Chapter 5, "Monitor resource details".



Retry Count (1 to 1440)

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

Error Threshold (1 to 10)

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

Memory Usage, Active Threads (15 to 600)

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

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

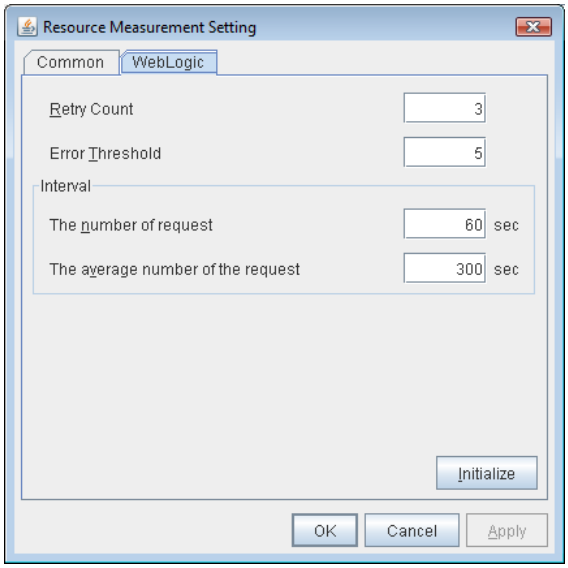
Set the **interval** at which the JVM monitor measures the time and count in Full GC execution.

Initialize

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

Resource Measurement Settings [WebLogic]

Clicking **Setting** displays the **Resource Measurement Settings** dialog box. For details on the scheme for error judgment by the JVM monitor, see Chapter 5, “Monitor resource details”.



Retry Count (1 to 5)

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

Error Threshold (1 to 10)

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

The number of request (15 to 600)

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

The average number of the request (15 to 600)

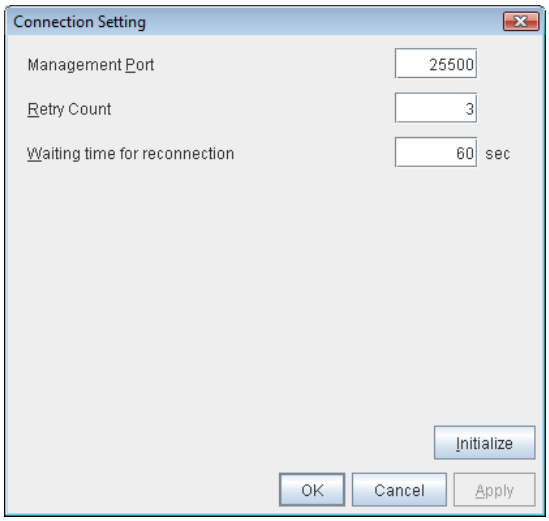
Set the interval at which the JVM monitor measures the average number of work manager or thread pool requests during WebLogic monitor. Set a value that is an integer multiple of the value set in **The number of request**.

Initialize

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

Connection Setting

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



Management Port (10000 to 65535)

Set the number of the port connected to the monitor target Java VM. This setting becomes common for all the servers in the cluster. Do not set 32768 to 61000.

Retry Count (1 to 5)

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

Waiting time for reconnection (15 to 60)

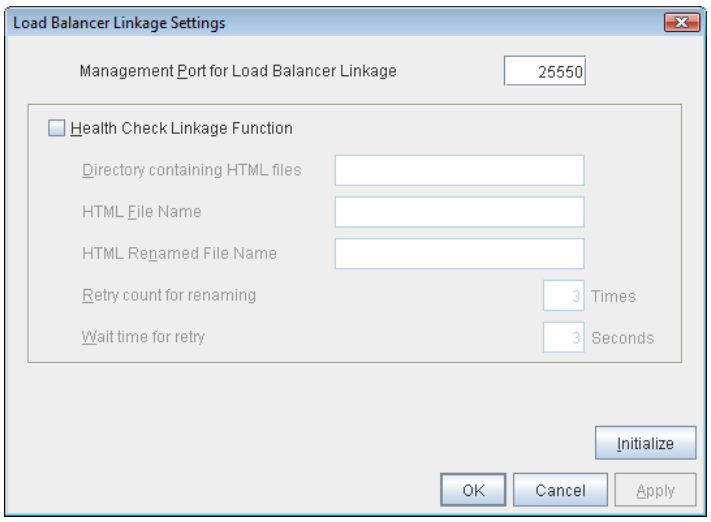
Set the interval at which the JVM monitor retries connection if it fails in Java VM connection.

Initialize

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

Load Balancer Linkage Settings

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



Management Port for Load Balancer Linkage (10000 to 65535)

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

Health Check Linkage Function

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

Directory containing HTML files (up to 1023 bytes)

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

HTML File Name (up to 255 bytes)

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

HTML Renamed File Name (up to 255 bytes)

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

Retry count for renaming (0 to 5)

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

Wait time for retry (1 to 60)

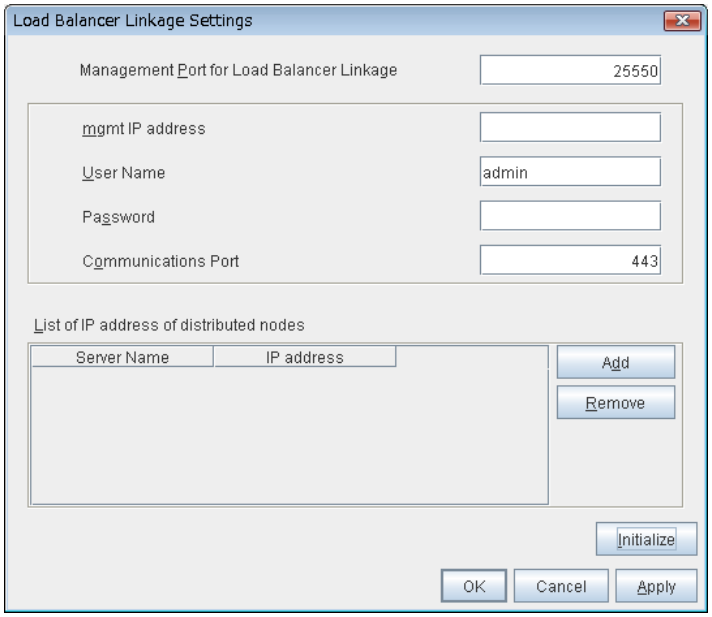
Set the interval at which HTML file renaming is retried if it fails.

Initialize

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

Load Balancer Linkage Settings

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



Management Port for Load Balancer Linkage (10000 to 65535)

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

mgmt IP address

Set the BIG-IP LTM IP address.

Management User Name (up to 255 bytes)

Set the BIG-IP LTM management user name.

Password (up to 255 bytes)

Set the BIG-IP LTM management user password.

Communication Port Number (10000 to 65535)

Set the communication port number for BIG-IP LTM.

Add

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

Remove

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

Initialize

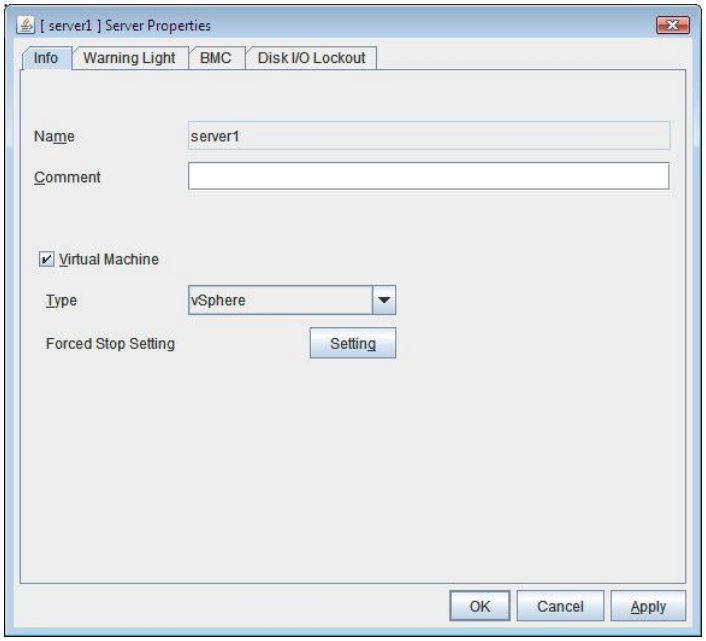
Clicking **Initialize** returns the management port for load balancer linkage, management user name, and communication port number to the default settings.

Server properties

In the **Server Properties** window, you can edit the special settings of the server.

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.

Comment (within 127 bytes)

You can specify a comment for the server. You can only enter one byte English characters.

Virtual Machine

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

- On

If selected, the server is a virtual machine (guest OS). You can configure this virtual machine.

- Off

If selected, the server is a physical machine. You cannot configure a virtual machine.

Type

Specify the type of virtual infrastructure.

- vSphere

  Virtual infrastructure provided by VMware, Inc.
- KVM

  Linux kernel virtual infrastructure.
- XenServer

  Virtual infrastructure provided by Citrix Systems, Inc.
- Container

  Virtual infrastructure provided by Oracle Systems, Inc.
- Hyper-V

  Virtual infrastructure provided by Microsoft Corporation.
- other

  Specify this option to use any other virtual infrastructure.

Forced Stop Setting

Not used.

Warning Light tab

Not used.

BMC tab

Not used.

Disk I/O Lockout tab

Not used.

Section IV How monitoring works

This section provides details about how monitoring with EXPRESSCLUSTER X SingleServerSafe works.

Chapter 8 Monitoring details

Chapter 8 Monitoring details

This chapter provides details about how several different types of errors are detected, in order to help you find out how to best set up the monitor interval, monitor timeout, and monitor retry count.

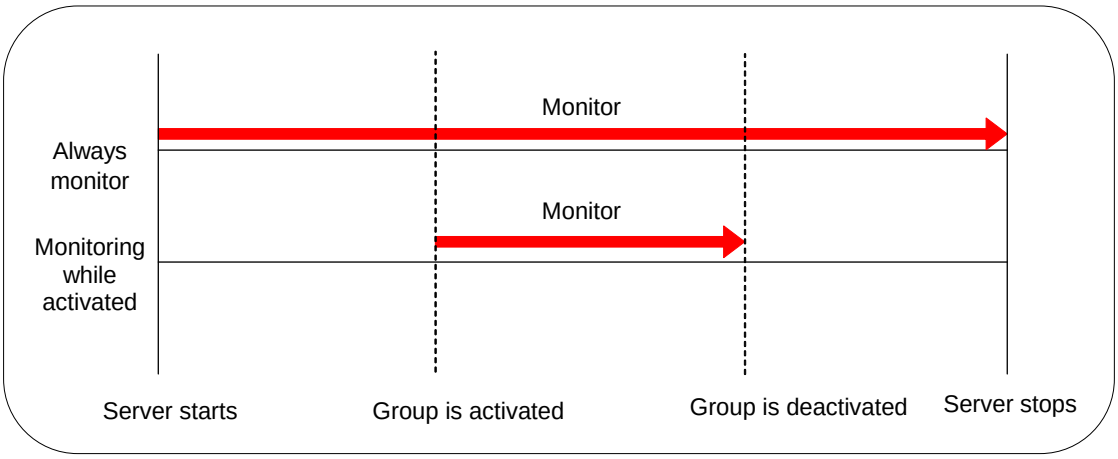
This chapter covers:

Always monitor and Monitors while activated

When **Always monitor** is selected, monitoring begins when the server is up and running and EXPRESSCLUSTER X SingleServerSafe is ready to run.

When **Monitors while activated** is selected, monitoring is performed from when a specified group is activated (until that group is deactivated (stopped)).

Some monitor resources have a fixed monitor timing, while others allow you to choose between two monitor timing options.



Monitor resource monitor interval

All monitor resources monitor their targets at every monitoring interval.

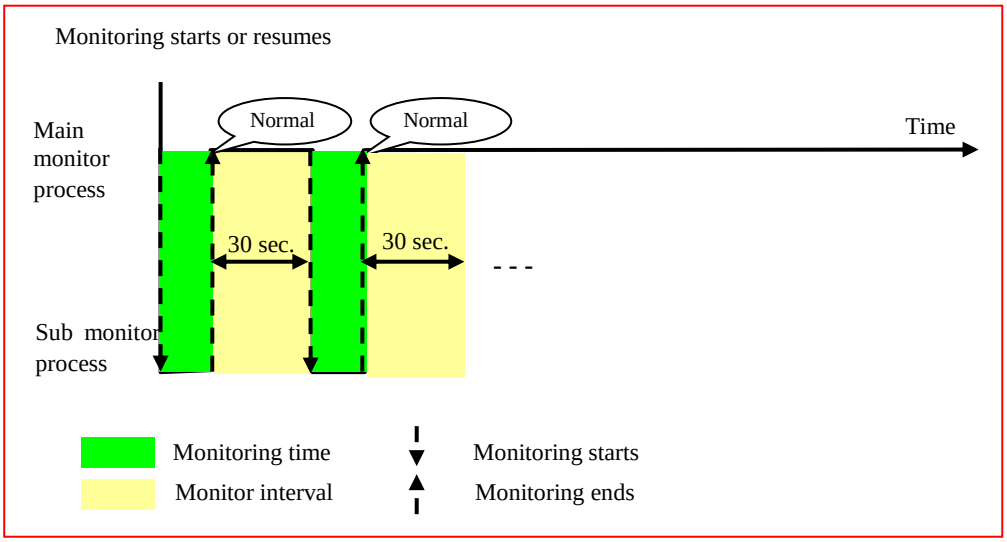
Following are different timelines illustrating how a monitor resource performs monitoring with or without an error based on the specified monitor interval.

When no error is detected

Examples of behavior when the following values are set.

<Monitor>

Monitor Interval	30 sec
Monitor Timeout	60 sec
Monitor Retry Count	0 times



When an error is detected (without monitor retry setting)

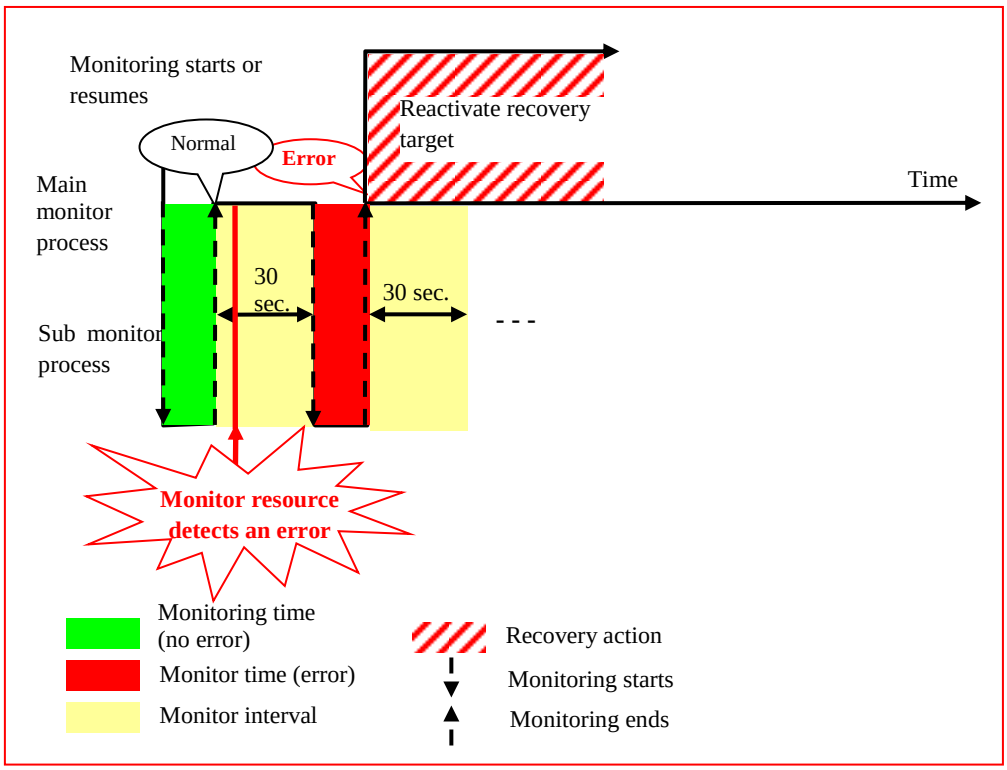
Examples of behavior when the following values are set.

<Monitor>

Monitor Interval	30 sec
Monitor Timeout	60 sec
Monitor Retry Count	0 times

<Error Detection>

Recovery Action	Restart the recovery target
Recovery Target	Group
Recovery Script Execution Count	0 time
Reactivation Threshold:	One time
Final Action	No Operation



After an error occurs, it is detected next time monitoring is performed, and then the recovery target is reactivated.

When an error is detected (with monitor retry settings)

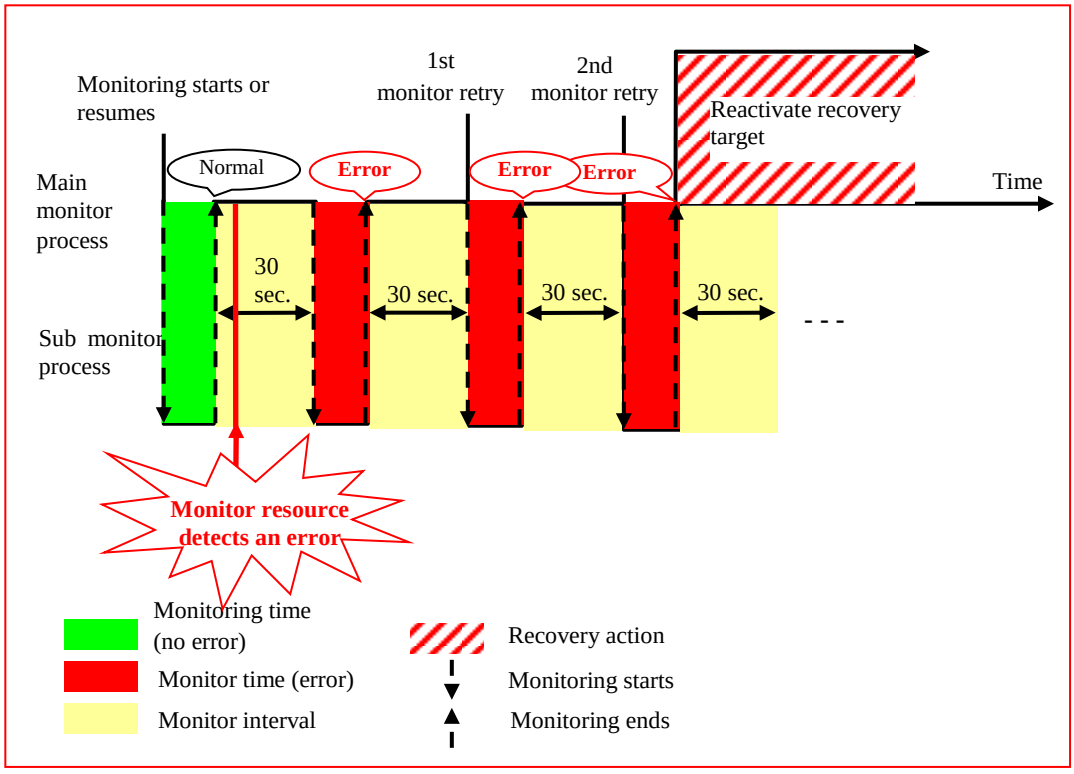
Examples of behavior when the following values are set.

<Monitor>

Monitor Interval	30 sec
Monitor Timeout	60 sec
Monitor Retry Count	2 times

<Error Detection>

Recovery Action	Restart the recovery target
Recovery Target	Group
Recovery Script Execution Count	0 time
Reactivation Threshold:	One time
Final Action	No Operation



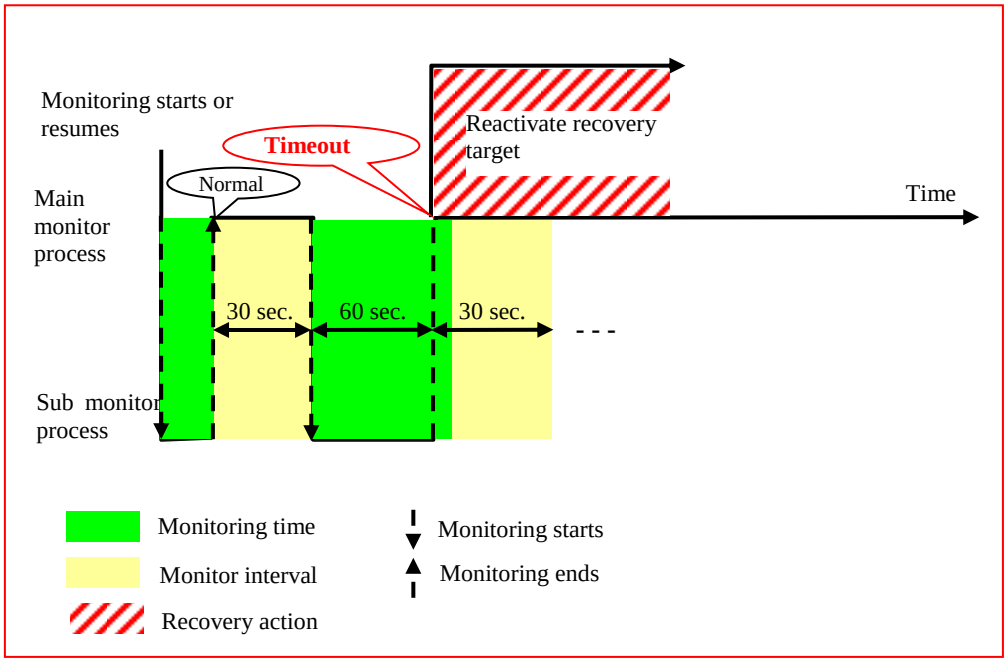
After an error occurs, it is detected next time monitoring is performed, and then, if recovery cannot be achieved before the monitor retry count is reached, the recovery target is reactivated.

When an error is detected (without monitor retry settings)

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 0 times

<Error Detection>
Recovery Action Restart the recovery target
Recovery Target Group
Recovery Script Execution Count 0 time
Reactivation Threshold: One time
Final Action No Operation



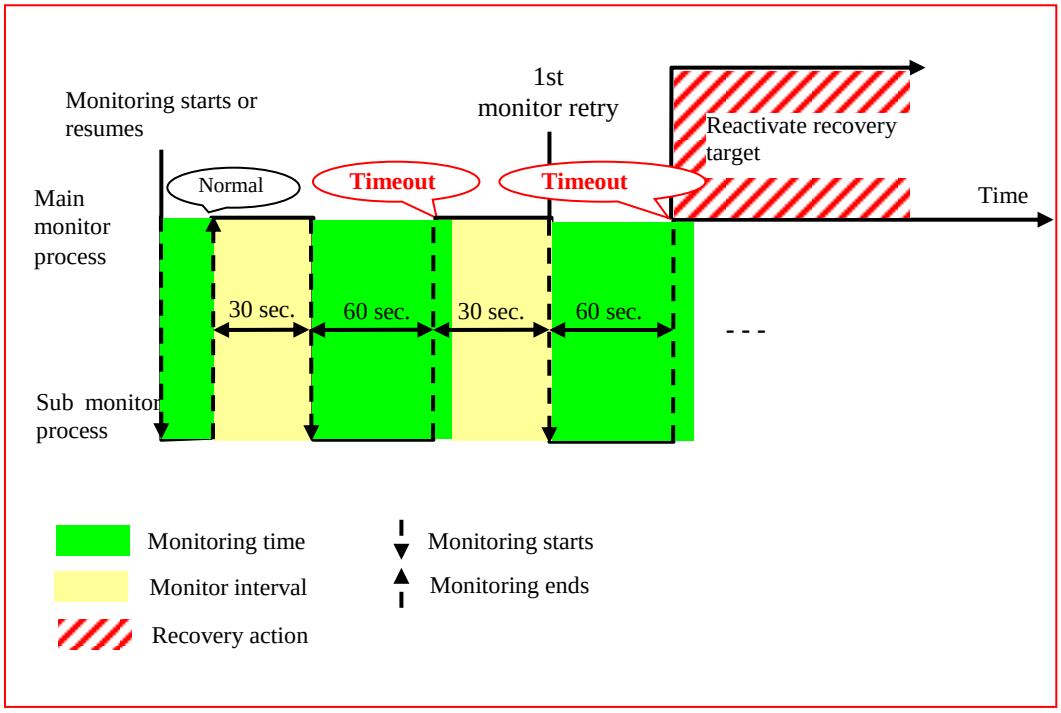
After a monitor timeout occurs, the recovery target is immediately reactivated for the recovery action.

When a monitoring timeout is detected (with monitor retry setting)

Examples of behavior when the following values are set.

<Monitor>
Monitor Interval 30 sec
Monitor Timeout 60 sec
Monitor Retry Count 1 time

<Error Detection>
Recovery Action Restart the recovery target
Recovery Target Group
Recovery Script Execution Count 0 time
Reactivation Threshold: One time
Final Action No Operation



After a monitor timeout occurs, another monitor attempt is made and, if it fails, the recovery target is reactivated.

Action 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 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.
- When an error is detected in the monitor target, the recovery target is reactivated. (This is not the case if **Execute Only Final Action** is selected for **Recovery Action** or if **Maximum Reactivation Count** is set to 0 in **Custom**).
- If reactivation fails or the error is detected again after reactivation, the final action is performed. (If **Maximum Reactivation Count** is set to 2 or greater in **Custom**, reactivation is retried the specified number of times.).

No recovery action is taken if the status of the recovery target is:

Recovery Target	Status	Reactivation[5]	Final Action[6]
Group/ Group Resource	Already stopped	No	No
	Being activated/stopped	No	No
	Already activated	Yes	Yes
	Error	Yes	Yes
Local Server	-	-	Yes

Note:
Do not perform the following operations by using the WebManager or command line while recovery processing is changing (reactivation -> final action), if a group resource (such as an EXEC resource or VM resource) is specified as a recovery target and when a monitor resource detects an error.

- Stopping/suspending the server
- Starting/stopping 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 the status of the monitor resource recovers from the error (becomes normal), the settings for the reactivation count and whether to execute the final action are reset. Note that, when a group or group resource is specified as the recovery target, these counters are reset only when the status of all the monitor resources for which the same recovery target is specified become normal.

An unsuccessful recovery action is also counted as part of the reactivation count.

[5] Effective only when the value for the reactivation threshold is set to 1 (one) or greater.
[6] Effective only when an option other than **No Operation** is selected.

Recovering from a monitor error (normal)

When return of the monitor resource is detected during or after recovery actions following the detection of a monitoring error, counts for the thresholds shown below are reset:

- Recovery Script Execution Count
- Reactivation Count

Whether or not to execute the final action is reset (execution required).

Activation or deactivation error for the recovery target during recovery

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.

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 X SingleServerSafe full version number)	EXPRESSCLUSTER X SingleServerSafe full version number	EXPRESSCLUSTER X SingleServerSafe full version number. (Example) 3.3.0-1
CLP_VERSION_MAJOR (EXPRESSCLUSTER X SingleServerSafe major version)	EXPRESSCLUSTER X SingleServerSafe major version	EXPRESSCLUSTER X SingleServerSafe major version. (Example) 3
CLP_PATH (EXPRESSCLUSTER X SingleServerSafe installation path)	EXPRESSCLUSTER X SingleServerSafe installation path	Path of EXPRESSCLUSTER X SingleServerSafe installation. (Example) /opt/nec/clusterpro
CLP_OSNAME (Server OS name)	Server OS name	Name of the server OS on which the script is executed. (Example) (1) When the OS name could be acquired: Red Hat Enterprise Linux Server release 6.0 (Santiago) (2) When the OS name could not be acquired: Linux
CLP_OSVER (Server OS version)	Server OS version	Version of the server OS on which the script is executed. (Example) (1) When the OS version could be acquired:6.0 (2) When the OS version could not be acquired: *None
CLP_ACTION	RECOVERY	Execution as a recovery script.

(Recovery action type)	RESTART	Execution before reactivation.
	FAILOVER	Execution before failover. Not used.
	FINALACTION	Execution before final action.
CLP_RECOVERYCOUNT (Recovery script execution count)	Recovery Script Execution Count	Count for recovery script execution.
CLP_RESTARTCOUNT (Reactivation count)	Reactivation count	Count for reactivation.

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

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

if [ "$CLP_ACTION" = "RECOVERY" ]
then
    Processing type:
        Recovery
    Execution timing for the processing:
        Recovery action: Recovery script

elif [ "$CLP_ACTION" = "RESTART" ]
then
    Processing type:
        Pre-reactivation processing
    Execution timing for the processing:
        Recovery action: Reactivation

elif [ "$CLP_ACTION" = "FAILOVER" ]
then
    Processing type:
        Recovery
    Execution timing for the processing:
        Recovery action: Failover

elif [ "$CLP_ACTION" = "FINALACTION" ]
then
    Processing type:
        Recovery
    Execution timing for the processing:
        Recovery action: Final action

fi
exit 0
```

Branched according to the environment variables for the cause of execution of the script.

Tips for recovery/pre-recovery action script coding

Pay careful attention to the following points when coding the script.

- When the script contains a command that requires a long time to run, log the end of execution of that command. The logged information can be used to identify the nature of the error if a problem occurs. clplogcmd is used to log the information.
- How to use clplogcmd in the script
  With clplogcmd, messages can be output to WebManager alert view or OS syslog. For clplogcmd, see "Outputting messages (clplogcmd command)" in Chapter 2, "EXPRESSCLUSTER X SingleServerSafe command reference" in Operation guide.

  (Ex. : Scripting image)
  ```
  clplogcmd -m "recoverystart.."
  recoverystart
  clplogcmd -m "OK"
  ```

Note on the recovery/pre-recovery action script

- Stack size for commands and applications activated from the script

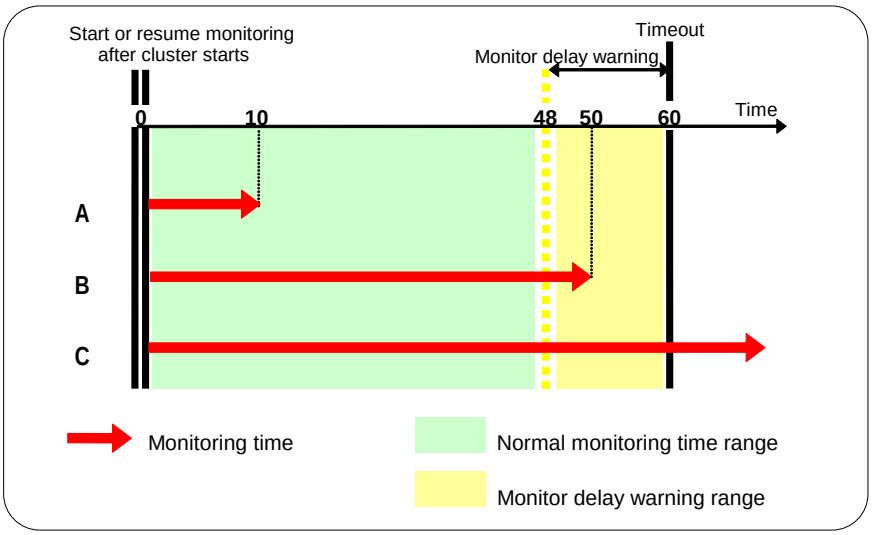
  The recovery/pre-recovery action script runs with the stack size configured to 2 MB. If the script has a command or application that requires a stack size of 2 MB or more to run, a stack overflow occurs.
  If a stack overflow error occurs, adjust the stack size before the command or application is activated.

Delay warning of a monitor resource

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.



A. The polling time of monitoring is 10 seconds. The target of the monitor resource is in normal status. In this case, no alert is used.

B. The polling time of monitoring is 50 seconds and the delay of monitoring is detected during this time. The target of the monitor resource is in the normal status. In this case, an alert is used because the delay warning rate has exceeded 80%.

C. The polling time of monitoring has exceeded 60 seconds of the monitoring timeout and the delay of monitoring is detected. The target of the monitor resource has a problem. In this case, no alert is used.

If the delay warning rate is set to 0 or 100:

- When 0 is set to the delay monitoring rate

  An alert for the delay warning is used at every monitoring.
  By using this feature, the time for monitor processing for the monitor resource can be calculated at the time the server is heavily loaded, which will allow you to determine the time for monitoring timeout of a monitor resource.

- When 100 is set to the delay monitoring rate

  The delay warning will not be is used.

Note:
Be sure not to set a low value, such as 0%, except for a test operation.

Related Information:
To configure the delay warning of monitor resources, click **Cluster Properties** and select **Monitor Delay Warning** in the **Delay Warning** tab.

Waiting for a monitor resource to start monitoring

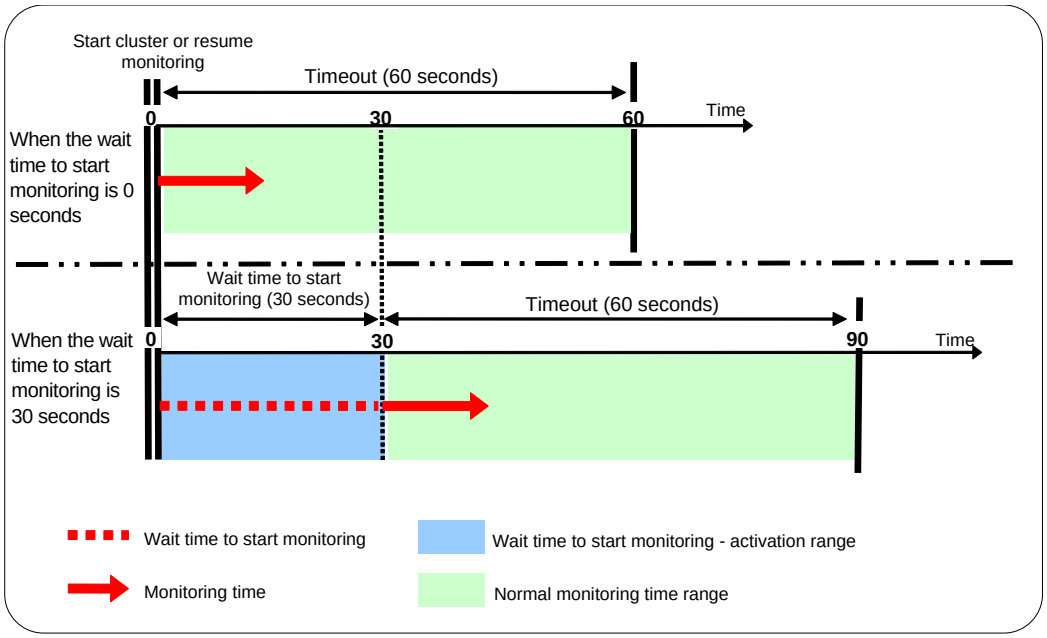
"Wait Time to Start Monitoring" refers to start monitoring after the time period specified as the waiting time elapses.

The following describes how monitoring differs when the wait time to start monitoring is set to 0 second and 30 seconds.

Configuration of monitor resource

<Monitor>

Interval	30 sec
Timeout	60 sec
Retry Count	0 times
Wait Time to Start Monitoring	0 sec / 30 sec



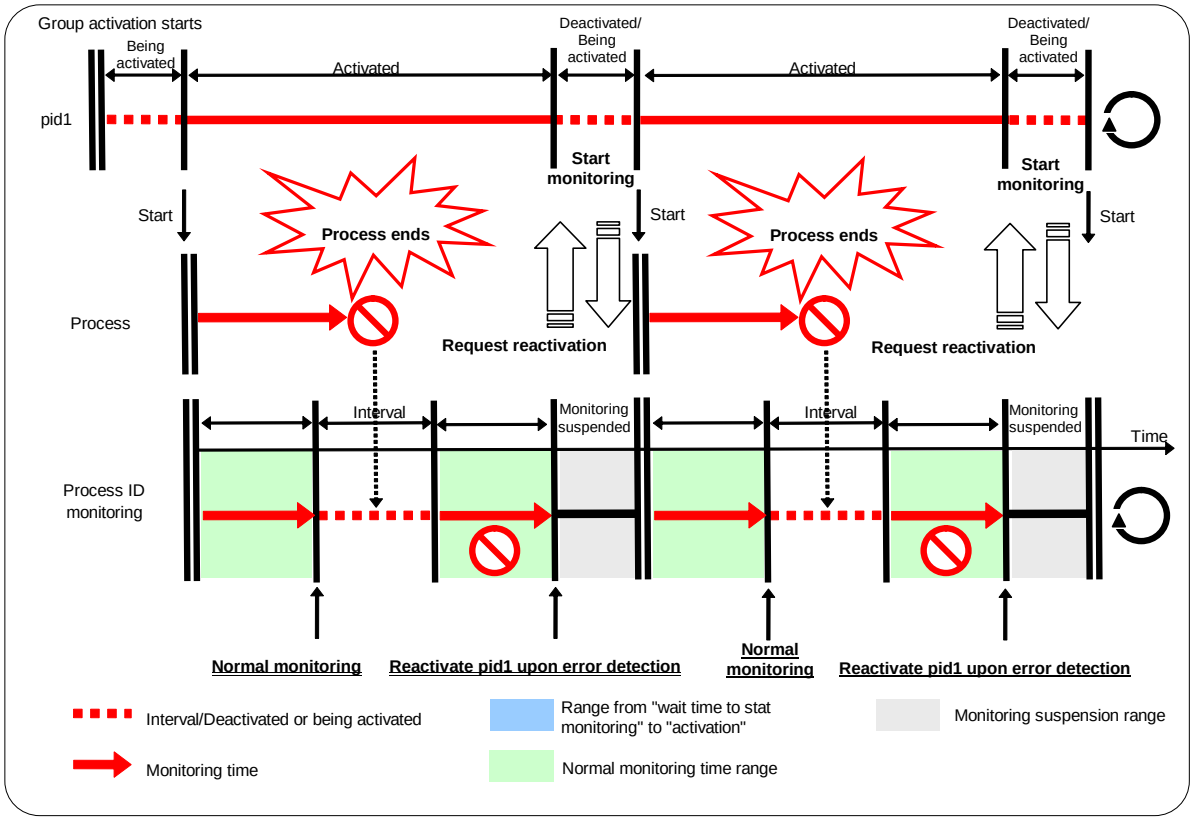
Note:
Monitoring will restart after the time specified to wait for start monitoring has elapsed even when the monitor resource is suspended and/or resumed by using the monitoring control commands.

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 an EXEC resource monitored by the PID monitor resource, and when they cannot be recovered by reactivation.

For example, when the monitor wait time is set to 0 (zero), recovery may be endlessly repeated. See the example below:

Configuration of PID monitor resource

<Monitor>	
Interval	5 sec
Timeout	60 sec
Retry Count	0 times
Wait Time to Start Monitoring	0 sec (default)
<Error Detection>	
Recovery Action	Restart the recovery target
Recovery Target	exec
Reactivation Threshold:	One time
Final Action	Stop Group



The reason why recovery action is endlessly repeated is because the initial monitor resource processing has terminated successfully. The current count of recoveries the monitor resource has executed is reset when the status of the monitor resource becomes normal (finds no error in the monitor target). Because of this, the current count is always reset to 0 and reactivation for recovery is endlessly repeated.

You can prevent this problem by setting the wait time to start monitoring.

By default, 60 seconds is set as the wait time from the application startup to the end.

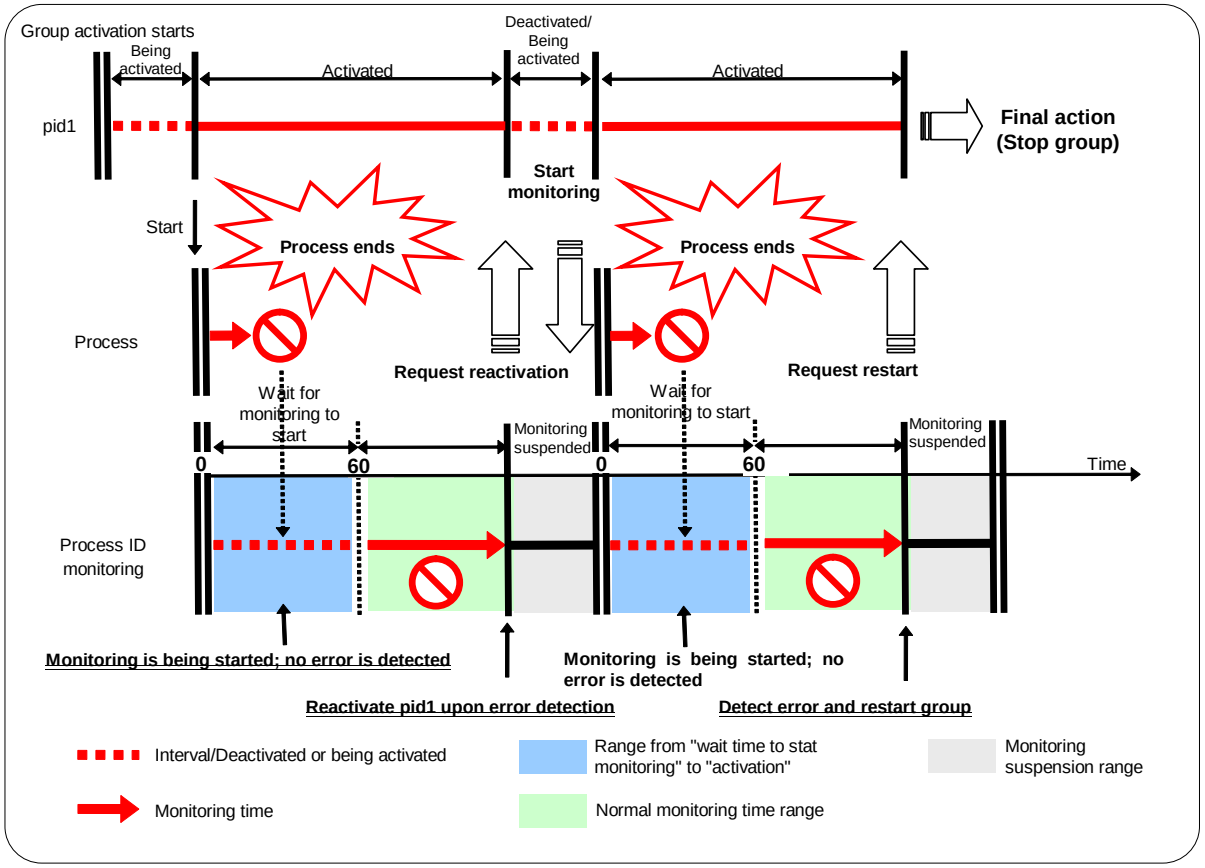
Configuration of PID monitor resource

<Monitor>

Interval	5 sec
Timeout	60 sec
Retry Count	0 times
Wait Time to Start Monitoring:	60 sec

<Error Detection>

Recovery Action	Restart the recovery target
Recovery Target	exec
Reactivation Threshold:	One time
Final Action	Stop Group



Limiting the reboot count for error detection

In case that the final action when an error is detected at activation or deactivation, or the final action of the monitor resource when an error is detected is configured so that the OS reboot accompanies, 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. When you reset the reboot count, use the clpregctrl command.

Section V Release notes

This section describes the restrictions on EXPRESSCLUSTER X SingleServerSafe, as well as the known problems and how to prevent them.

Chapter 9 Notes and restrictions

Chapter 9 Notes and restrictions

This chapter provides information on known problems and how to troubleshoot the problems.

This chapter covers:

Designing a system configuration

This section describes the matters to be careful of in configuring the system.

Supported operating systems for the Builder and WebManager

- Use a Web browser and Java Runtime supporting 32-bit machine to run the Builder and WebManager on an x86_64 machine.

JVM monitor resources

- Up to 25 Java VMs can be monitored concurrently. The Java VMs that can be monitored concurrently are those which are uniquely identified by the Builder (with **Identifier** in the **Monitor (special)** tab).
- Connections between Java VMs and Java Resource Agent do not support SSL.
- If, during the monitoring of Java VM, there is another process with the same name as the monitoring target, C heap monitoring may be performed for a different monitoring target.
- It may not be possible to detect thread deadlocks. This is a known problem in Java VM. For details, refer to "Bug ID: 6380127" in the Oracle Bug Database.
- Monitoring of the WebOTX process group is disabled when the process multiplicity is two or more. WebOTX V8.4 and later can be monitored.
- The Java Resource Agent can monitor only the Java VMs on the server on which the JVM monitor resources are running.
- The Java Resource Agent can monitor only one JBoss server instance per server.
- The Java installation path setting made by the Builder (with **Java Installation Path** in the **JVM monitor** tab in **Cluster Property**) is shared by the servers in the cluster. The version and update of Java VM used for JVM monitoring must be the same on every server in the cluster.
- The management port number setting made by the Builder (with **Management Port** in the **Connection Setting** dialog box opened from the **JVM monitor** tab in **Cluster Property**) is shared by all the servers in the cluster.
- Application monitoring is disabled when an application to be monitored on the IA32 version is running on an x86_64 version OS or when an application to be monitored on an x86_64 version is running on an IA32 version OS.
- If a large value such as 3,000 or more is specified as the maximum Java heap size by the Builder (by using Maximum Java Heap Size on the **JVM monitor** tab in **Cluster Property**), The Java Resource Agent will fail to start up. The maximum heap size differs depending on the environment, so be sure to specify a value based on the capacity of the mounted system memory.
- Using SingleServerSafe is recommended if you want to use the target Java VM load calculation function of the coordination load balancer. It's supported only by Red Hat Enterprise Linux.
- If "-XX:+UseG1GC" is added as a startup option of the target Java VM, the settings on the Memory tab on the Monitor(special) tab in Property of JVM monitor resources cannot be monitored before Java 7.
  It's possible to watch by choosing [Oracle Java (usage monitoring)] in [JVM Type] on the Monitor(special) tab after Java 8.

Mail reporting

The mail reporting function is not supported by STARTTLS and SSL.

Items to check when creating configuration data

This section describes the items to note before designing and creating configuration data based on the system configuration.

Environment variable

The following scripts cannot be executed under the environment where more than 255 environmental variables are set. When using the following function of resource, set the number of environmental variables less than 256.

- Start/Stop script executed by EXEC resource when activating/deactivating
- Script executed by Custom monitor Resource when monitoring
- Script before final action after the group resource or the monitor resource error is detected.

Server reset, server panic, and power off

When EXPRESSCLUSTER performs "Server reset," "Server panic," or "Server power off," the servers are not shut down normally. Therefore, the following may occur.

- Damage to a mounted file system
- Loss of unsaved data

“Server reset” or “Server panic” occurs under the following settings:

- Action upon an error when activating or deactivating a group resource
  -sysrq Panic
  -keepalive Reset
  -keepalive Panic
  -BMC Reset
  -BMC Power Off
  -BMC Cycle
  -BMC NMI
- Final action when a monitor resource detects an error
  -sysrq Panic
  -keepalive Reset
  -keepalive Panic
  -BMC Reset
  -BMC Power Off
  -BMC Cycle
  -BMC NMI
- Action when a user space monitoring timeout is detected
  - softdog monitoring method
  - ipmi monitoring method
  - keepalive monitoring method

Note:
A server panic can be specified when the monitoring method is keepalive.

- Shutdown monitoring
  - softdog monitoring method
  - ipmi monitoring method
  - keepalive monitoring method

Note:
Server panic can be set when the monitoring method is keepalive.

Final action upon a group resource deactivation error

If select **No Operation** as the final action when a deactivation error is detected, the group does not stop but remains in the deactivation error status.
Make sure not to set **No Operation** in the production environment.

Verifying raw device for VxVM

Check the raw device of the volume raw device in advance:

Import all disk groups which can be activated on one server and activate all volumes before installing EXPRESSCLUSTER.

Run the command below:

```
# raw -qa
/dev/raw/raw2:  bound to major 199, minor 2
/dev/raw/raw3:  bound to major 199, minor 3
```

(A) (B)

Example: Assuming the disk group name and volume name are:

- Disk group name: dg1
- Volume name under dg1: vol1, vol2

1. Run the command below:

```
# ls -l /dev/vx/dsk/dg1/
brw-------   1 root     root     199,   2 May 15 22:13 vol1
brw-------   1 root     root     199,   3 May 15 22:13 vol2
```

(C)

2. Confirm that major and minor numbers are identical between (B) and (C).

Never use these raw devices (A) as an EXPRESSCLUSTER disk monitor resource for which the monitor method is not READ(VxVM).

Delay warning rate

If the delay warning rate is set to 0 or 100, the following can be achieved:

- When 0 is set to the delay monitoring rate

  An alert for the delay warning is issued at every monitoring.
  By using this feature, you can calculate the polling time for the monitor resource at the time the server is heavily loaded, which will allow you to determine the time for monitoring timeout of a monitor resource.

- When 100 is set to the delay monitoring rate
  The delay warning will not be issued.

Be sure not to set a low value, such as 0%, except for a test operation.

TUR monitoring method for disk monitor resources

- This method cannot be used for a disk or disk interface (HBA) that does not support the SCSI Test Unit Ready command or SG_IO command.
  Even if your hardware supports these commands, consult the driver specifications because the driver may not support them.
- For an S-ATA interface disk, the OS identifies the device as an IDE interface disk (hd) or SCSI interface disk (sd) depending on the disk controller type or distribution.
  When the device is identified as using the IDE interface, TUR cannot be used.
  When the device is identified as using the SCSI interface, TUR (legacy) can be used. TUR (generic) cannot be used.
- TUR methods burdens OS and disk load less compared to Read methods.
- In some cases, Test Unit Ready may not be able to detect actual errors in I/O to media.

WebManager reload interval

- Do not set the **Reload Interval** on the WebManager tab or less than 30 seconds.

Double-byte character set that can be used in script comments

- Scripts edited in Linux environment are dealt as EUC code, and scripts edited in Windows environment are dealt as Shift-JIS code. In case that other character codes are used, character corruption may occur depending on environment.

IP address for Integrated WebManager settings

- **Public LAN IP address** setting, EXPRESSCLUSTER X2.1 or before, is available in the Builder at **IP address for Integrated WebManger** which is on the **WebManager** tab of **Cluster Properties**.

System monitor resource settings

- Pattern of detection by resource monitoring
  The System Resource Agent detects by using thresholds and monitoring duration time as parameters.
  The System Resource Agent collects the data (number of opened files, number of user processes, number of threads, used size of memory, CPU usage rate, and used size of virtual memory) on individual system resources continuously, and detects errors when data keeps exceeding a threshold for a certain time (specified as the duration time).

Message receive monitor resource settings

- Error notification to message receive monitor resources can be done in following way:
  - using the `clprexec` command.
- To use the `clprexec` command, use the relevant file stored on the EXPRESSCLUSTER CD. Use this method according to the OS and architecture of the notification-source server. The notification-source server must be able to communicate with the notification-destination server.

JVM monitor resource settings

- When the monitoring target is the WebLogic Server, the maximum values of the following JVM monitor resource settings may be limited due to the system environment (including the amount of installed memory):
  - **The number** under **Monitor the requests in Work Manager**
  - **Average** under **Monitor the requests in Work Manager**
  - **The number** of **Waiting Requests** under **Monitor the requests in Thread Pool**
  - **Average** of **Waiting Requests** under **Monitor the requests in Thread Pool**
  - **The number** of **Executing Requests** under **Monitor the requests in Thread Pool**
  - **Average** of **Executing Requests** under **Monitor the requests in Thread Pool**
- When the monitoring-target is a 64-bit JRockit JVM, the following parameters cannot be monitored because the maximum amount of memory acquired from the JRockit JVM is a negative value that disables the calculation of the memory usage rate:
  - **Total Usage** under **Monitor Heap Memory Rate**
  - **Nursery Space** under **Monitor Heap Memory Rate**
  - **Old Space** under **Monitor Heap Memory Rate**
  - **Total Usage** under **Monitor Non-Heap Memory Rate**
  - **ClassMemory** under **Monitor Non-Heap Memory Rate**
- To use the Java Resource Agent, install the Java runtime environment (JRE) described in "Operation environment for JVM Monitor" in Chapter 1, "*Installation Guide*" You can use either the same JRE as that used by the monitoring target (WebLogic Server or WebOTX) or a different JRE.
- The monitor resource name must not include a blank.
- **Command**, which is intended to execute a command for a specific failure cause upon error detection, cannot be used together with the load balancer linkage function.

Notes when changing the EXPRESSCLUSTER configuration

The section describes what happens when the configuration is changed after starting to use EXPRESSCLUSTER in the cluster configuration.

Dependency between resource properties

When the dependency between resources has been changed, the change is applied by suspending and resuming the cluster.

If a change in the dependency between resources that requires the resources to be stopped during application is made, the startup status of the resources after the resume may not reflect the changed dependency.

Dependency control will be performed at the next group startup.

Adding and deleting group resources

When you move a group resource to another group, follow the procedure shown below.

If this procedure is not followed, the cluter may not work normally.

Example) Moving exec1 (exec resource) from failover1 group to failover2 group

1. Delete exec1 from failover1.
2. Reflect the setting to the system.
3. Add exec1 to failover2.
4. Reflect the setting to the system.

Number of components of each type that can be registered

	Builder version	You can register up to
Server	3.0.0-1 or later	1
group	3.0.0-1 or under	64
	3.1.0-1 later	128
Group resource (Per group)	3.0.0-1 or under	128
	3.1.0-1 later	512
Monitor resource	3.0.0-1 or later	512
System monitor resource	3.1.0-1 or later	1

Appendix A Index

J

L

M

N

O

P

R

S

T

U

V

W