

**ExpressCluster<sup>®</sup> X SingleServerSafe 3.1**  
**for Windows**

Configuration Guide

12/10/2012  
4th Edition



## Revision History

Edition	Revised Date	Description
First	10/11/2011	New manual
2nd	3/31/2012	Corresponds to the internal version 11.13.
3rd	9/30/2012	Corresponds to the internal version 11.15.
4th	12/10/2012	Corresponds to the internal version 11.17.

© Copyright NEC Corporation 2011. All rights reserved.

## **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® X is a registered trademark of NEC Corporation.

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.

Oracle, Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

WebOTX is a registered trademark of NEC Corporation.

SVF is a registered trademark of WingArc Technologies, Inc.

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

<b>Preface</b>	<b>xi</b>
Who Should Use This Guide	xi
How This Guide Is Organized	xi
Terms Used in This Guide	xii
ExpressCluster X SingleServerSafe Documentation Set	xiii
Conventions	xiv
Contacting NEC	xv
<b>Section I</b>	<b>Overview of ExpressCluster X SingleServerSafe</b>
<b>Chapter 1</b>	<b>ExpressCluster X SingleServerSafe</b>
ExpressCluster X SingleServerSafe	20
How an error is detected in ExpressCluster X SingleServerSafe	21
<b>Section II</b>	<b>Configuration of ExpressCluster X SingleServerSafe</b>
<b>Chapter 2</b>	<b>Creating configuration data</b>
Checking the values to be specified	26
Sample environment	26
Starting up the WebManager	28
What is the WebManager?	28
Setting up JAVA runtime environment to a management PC	29
Starting up the WebManager	29
Creating the configuration data	30
1. Setting up the server	31
1-1 Setting up the server	31
2. Setting up groups	32
2-1 Adding a group	32
2-2 Adding a group resource (application resource)	36
3. Setting up monitor resources	40
3-1 Adding a monitor resource (IP monitor resource)	40
3-2 Adding a monitor resource (application monitor resource)	45
Saving configuration data	49
Applying configuration data	51
Differences regarding the use of the offline version of the Builder	53
1. Setting up the server	53
1-1 Setting up a server	53
2. Saving configuration data	55
3. Applying configuration data	56
<b>Chapter 3</b>	<b>LAN board redundancy function</b>
Understanding LAN board redundancy	58
Setting up LAN board redundancy	59
<b>Section III</b>	<b>Resource details</b>
<b>Chapter 4</b>	<b>Group resource details</b>
Group resources	66
System requirements for VM resource	66
Setting up application resources	67
Displaying and changing the application resource details	67
Setting up script resources	72
Tips for creating scripts	77

Displaying and changing the script resource details .....	77
Using the simple selection function of a script template .....	81
Using the simple selection function of a script template .....	81
Setting up service resources .....	83
Notes on service resources .....	83
Displaying and changing the service resource details .....	83
Setting up VM resources .....	86
Displaying and changing the VM resource details .....	86
<b>Chapter 5</b> <b>Monitor resource details.....</b>	<b>89</b>
Monitor resources .....	90
Monitor resources that require a license .....	93
Applications supported by monitoring options .....	94
Common settings for monitor resources .....	100
Displaying and changing parameters of a monitor resource .....	107
Setting up application monitor resources.....	108
Monitoring by application monitor resources .....	108
Note on application monitor resources .....	108
Setting up service monitor resources .....	109
Monitoring by service monitor resources.....	109
Note on service monitor resources .....	109
Setting up disk RW monitor resources .....	110
Monitoring by disk RW monitor resources .....	110
Displaying and changing disk RW monitor resource details .....	110
Setting up IP monitor resources .....	113
Monitoring by IP monitor resources.....	113
Displaying and changing IP monitor resource details .....	114
Setting up NIC link up/down monitor resources .....	116
Note on NIC link up/down monitor resources .....	116
Configuration and range of NIC link up/down monitoring.....	116
Displaying and changing the NIC link up/down monitor resource details .....	116
Setting up custom monitor resources .....	118
Monitoring by custom monitor resources .....	118
Note on custom monitor resources .....	118
Displaying and changing the details of the custom monitoring resources .....	118
Setting up multi target monitor resources .....	121
Note on the multi target monitor resource.....	121
Status of the multi target monitor resource .....	121
Displaying and changing the details of the multi target monitor resource .....	122
Setting up message receive monitor resources .....	125
Monitoring by message receive monitor resource .....	125
Notes on message receive monitor resources .....	125
Displaying and changing the details of the Message receive monitor resources.....	125
Setting up VM monitor resources .....	127
Notes on VM monitor resources .....	127
Monitoring by VM monitor resources .....	127
Setting up process name monitor resources .....	128
Notes on process name monitor resources .....	128
Monitoring by process name monitor resources .....	129
Displaying and changing the process name monitor resource details .....	129
Setting up DB2 monitor resources .....	131
Notes on DB2 monitor resource .....	131
Monitoring by DB2 monitor resources .....	132
Displaying and changing the disk DB2 monitor resource details .....	133
Setting up FTP monitor resources .....	135
Notes on FTP monitor resources.....	135
Monitoring by FTP monitor resources.....	135
Displaying and changing the FTP monitor resource details.....	136
Setting up HTTP monitor resources.....	138
Notes on HTTP monitor resources .....	138
Monitoring by HTTP monitor resources .....	138
Displaying and changing the HTTP monitor resource details .....	139

Setting up IMAP4 monitor resources .....	141
Notes on IMAP4 monitor resources .....	141
Monitoring by IMAP4 monitor resources .....	141
Displaying and changing the IMAP4 monitor resource details .....	142
Setting up ODBC monitor resources .....	144
Notes on ODBC monitor resources .....	144
Monitoring by ODBC monitor resources .....	145
Displaying and changing the ODBC monitor resource details .....	146
Setting up Oracle monitor resources .....	148
Notes on Oracle monitor resources .....	148
Monitoring by Oracle monitor resources.....	149
Displaying and changing the Oracle monitor resource details .....	150
Setting up OracleAS monitor resources .....	154
Notes on OracleAS monitor resources .....	154
Monitoring by OracleAS monitor resources.....	154
Displaying and changing the OracleAS monitor resource details .....	155
Setting up OfficeScan CL monitor resources.....	157
Notes on OfficeScan CL monitor resources .....	157
Monitoring by OfficeScan CL monitor resources.....	157
Displaying and changing OfficeScan CL monitor resource details.....	157
Setting up OfficeScan SV monitor resources.....	158
Notes on OfficeScan SV monitor resources .....	158
Monitoring by OfficeScan SV monitor resources.....	158
Displaying and changing OfficeScan SV monitor resource details.....	158
Setting up POP3 monitor resources .....	159
Notes on POP3 monitor resources.....	159
Monitoring by POP3 monitor resources.....	159
Displaying and changing the POP3 monitor resource details.....	160
Setting up PostgreSQL monitor resources .....	162
Notes on PostgreSQL monitor resources.....	162
Monitoring by PostgreSQL monitor resources.....	164
Displaying and changing the PostgreSQL monitor resource details.....	165
Setting up SMTP monitor resources .....	167
Notes on SMTP monitor resources.....	167
Monitoring by SMTP monitor resources.....	167
Displaying and changing the SMTP monitor resource details.....	168
Setting up SQL Server monitor resources .....	170
Notes on SQL Server monitor resources .....	170
Monitoring by SQL Server monitor resources .....	171
Displaying and changing the SQL Server monitor resource details .....	172
Setting up Tuxedo monitor resources .....	174
Notes on Tuxedo monitor resources .....	174
Monitoring by Tuxedo monitor resources .....	174
Displaying and changing the Tuxedo monitor resource details .....	175
Setting up Weblogic monitor resources .....	176
Notes on Weblogic monitor resources .....	176
Monitoring by Weblogic monitor resources .....	176
Displaying and changing the Weblogic monitor resource details .....	177
Setting up WebOTX monitor resources .....	179
Notes on WebOTX monitor resources .....	179
Monitoring by WebOTX monitor resources .....	179
Displaying and changing the WebOTX monitor resource details Websphere .....	180
Setting up Websphere monitor resources .....	181
Notes on Websphere monitor resources .....	181
Monitoring by Websphere monitor resources .....	181
Displaying and changing the Websphere monitor resource details .....	182
Setting up JVM monitor resources .....	184
Note on JVM monitor resources .....	184
Monitoring by JVM monitor resources.....	184
Linking with the load balancer (JVM monitor health check function) .....	188
Linking with the load balancer (target Java VM load calculation function).....	190
Linking with the BIG-IP Local Traffic Manager.....	194
Monitoring WebLogic Server.....	199

Monitoring WebOTX.....	201
Monitoring a Java process of the WebOTX domain agent .....	201
Monitoring a Java process of a WebOTX process group .....	202
Receiving WebOTX notifications .....	203
Monitoring Tomcat .....	204
Monitoring SVF .....	205
Displaying and changing the JVM monitor resource details.....	206
Memory tab .....	210
Thread tab.....	212
GC tab.....	213
WebLogic tab.....	214
Load Balancer Linkage tab .....	216
Load Balancer Linkage tab .....	217
Setting up system monitor resources.....	219
Notes on system monitor resource .....	219
Monitoring by system monitor resources .....	220
Displaying and changing the system monitor resource details .....	224
<b>Chapter 6</b>	<b>Other setting details..... 231</b>
Cluster properties .....	232
Info tab.....	232
Port No. tab.....	233
Monitor tab .....	235
Recovery tab.....	237
Alert Service tab.....	242
WebManager tab .....	250
Alert Log tab.....	256
Delay Warning tab.....	257
Power Saving tab.....	258
JVM monitor tab .....	260
Server properties .....	268
Info tab.....	268
Warning Light tab.....	270
BMC tab.....	270
HBA tab .....	270
<b>Section IV</b>	<b>How monitoring works ..... 271</b>
<b>Chapter 7</b>	<b>Monitoring details..... 273</b>
Always monitor and Monitors while activated.....	274
Enabling and disabling Dummy failure of monitor resources .....	275
Monitor resource monitor interval .....	276
Action when an error is detected by a monitor resource.....	281
Recovering from a monitor error (normal) .....	282
Activation or deactivation error for the recovery target during recovery .....	282
Recovery/pre-recovery action script .....	283
Delay warning of a monitor resource .....	286
Waiting for a monitor resource to start monitoring.....	288
Limiting the reboot count for error detection by a monitor resource .....	291
<b>Section V</b>	<b>Release Notes ..... 293</b>
<b>Chapter 8</b>	<b>Notes and Restrictions ..... 295</b>
Designing a system configuration.....	296
NIC link up/down monitor resource.....	296
ExpressCluster X Alert Service .....	296
Notes on LAN board redundancy .....	296
JVM monitor resources .....	296
Mail reporting .....	297
Creating configuration data .....	298
Final action for a group resource deactivation error .....	298



Delay warning rate .....	298
WebManager reload interval .....	298
Notes on the Builder.....	298
Double-byte character set that can be used in script comments.....	299
JVM monitor resource settings .....	300
System monitor resource settings.....	300
Upper limits of registration.....	301
<b>Appendix .....</b>	<b>303</b>
<b>Appendix A                      Index .....</b>	<b>305</b>



# 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      “LAN board redundancy function” : Describes the LAN board redundancy function.

### **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      “Other setting details”: Provides details on the other settings for ExpressCluster X SingleServerSafe.

### **Section IV      How monitoring works**

Chapter 7      “Monitoring details”: Provides details on how several types of errors are detected.

### **Section V      Release Notes**

Chapter 8      “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 manuals consist 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
<b>Bold</b>	Indicates graphical objects, such as fields, list boxes, menu selections, buttons, labels, icons, etc.	In <b>User Name</b> , type your name. On the <b>File</b> menu, click <b>Open Database</b> .
Angled bracket within the command line	Indicates that the value specified inside of the angled bracket can be omitted.	<code>clpstat -s [-h <i>host_name</i>]</code>
Monospace (courier)	Indicates path names, commands, system output (message, prompt, etc), directory, file names, functions and parameters.	<code>c:¥Program files¥EXPRESSCLUSTER</code>
<b>Monospace bold (courier)</b>	Indicates the value that a user actually enters from a command line.	Enter the following: <code>clpcl -s -a</code>
<i>Monospace italic (courier)</i>	Indicates that users should replace italicized part with values that they are actually working with.	<code>clpstat -s [-h <i>host_name</i>]</code>

## **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.....	20
How an error is detected in ExpressCluster X SingleServerSafe .....	21

## 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.

In addition, ExpressCluster X SingleServerSafe allows you to have a redundant LAN board configuration. You can have two LAN boards and use one of them for communication. If ExpressCluster X SingleServerSafe detects an error in the active LAN board, it switches to the other LAN board to continue communication.

---

**Note:**

As indicated above, in many cases, a physical hardware failure cannot be recovered from just by rebooting the server. While you can set up redundant LAN boards, you should also consider taking measures to protect against other physical hardware failures, such as making hardware redundant and using 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:**

- 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.
  - 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.



# **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. Setting up a redundant LAN board configuration is also discussed.

Chapter 2	Creating configuration data
Chapter 3	LAN board redundancy function





## 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.....	26
Starting up the WebManager.....	28
Creating the configuration data .....	30
1. Setting up the server.....	31
2. Setting up groups .....	32
3. Setting up monitor resources .....	40
Saving configuration data.....	49
Applying configuration data.....	51
Differences regarding the use of the offline version of the Builder.....	53
1. Setting up the server.....	53
2. Saving configuration data.....	55
3. Applying configuration data.....	56

## 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
	System drive	C:
group	Type	Failover
	Group name	failover1
	Startup server	server1
First group resources	Type	Application resources
	Group resource name	appli1
	Resident Type	Resident
	Start Path	Path of execution file
First monitor resource	Type	Disk RW monitor resources
	Monitor resource name	diskwlocal
	File Name	C:¥diskwlocal.dat
	I/O size	2000000
	Action when stalling is detected	Generating of intentional Stop Error
	Recovery Target	server1
	Final Action	Generating of intentional Stop Error
Second monitor resources	Type	IP monitor resources
	Monitor resource name	ipw1
	Monitor IP address	192.168.0.254 (gateway)
	Recovery Target	server1(server name)
	Reactivation threshold	-
	Final Action	Stop service and reboot OS
Third monitor resources	Type	Application monitor
	Monitor resource name	appliw1
	Target Resource	appli1
	Recovery Target:	failover1

Target	Parameter	Value
	Reactivation threshold	3
	Final Action:	Stop service and reboot OS

**Note:**

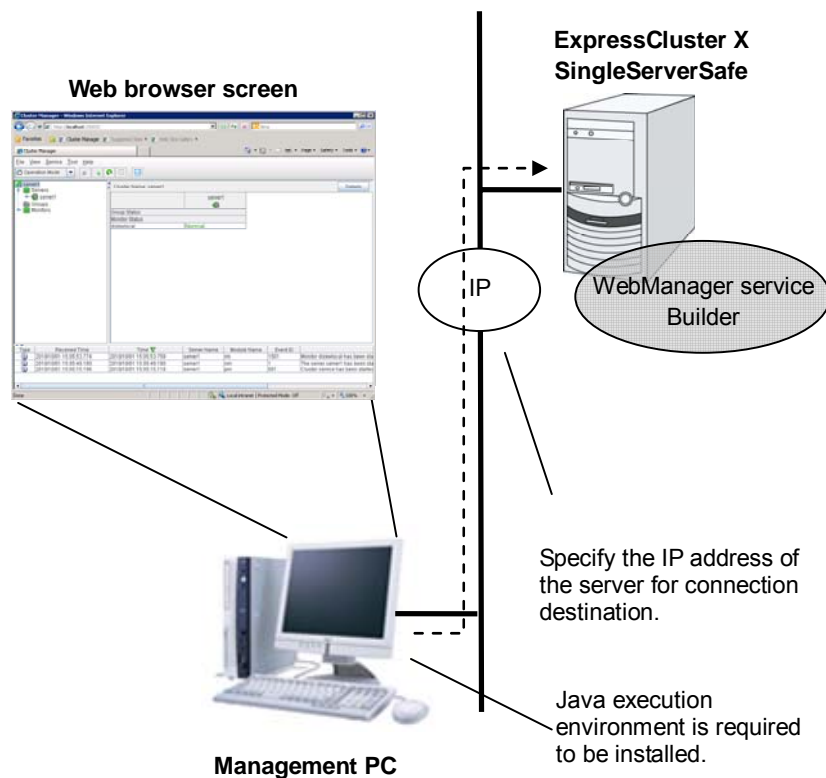
"Disk RW monitor" is automatically specified for the first monitor resource. The system drive information specified during the server setup process is applied.

## 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)) 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.

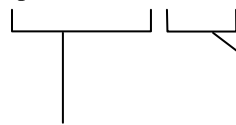
## Starting up the WebManager

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.

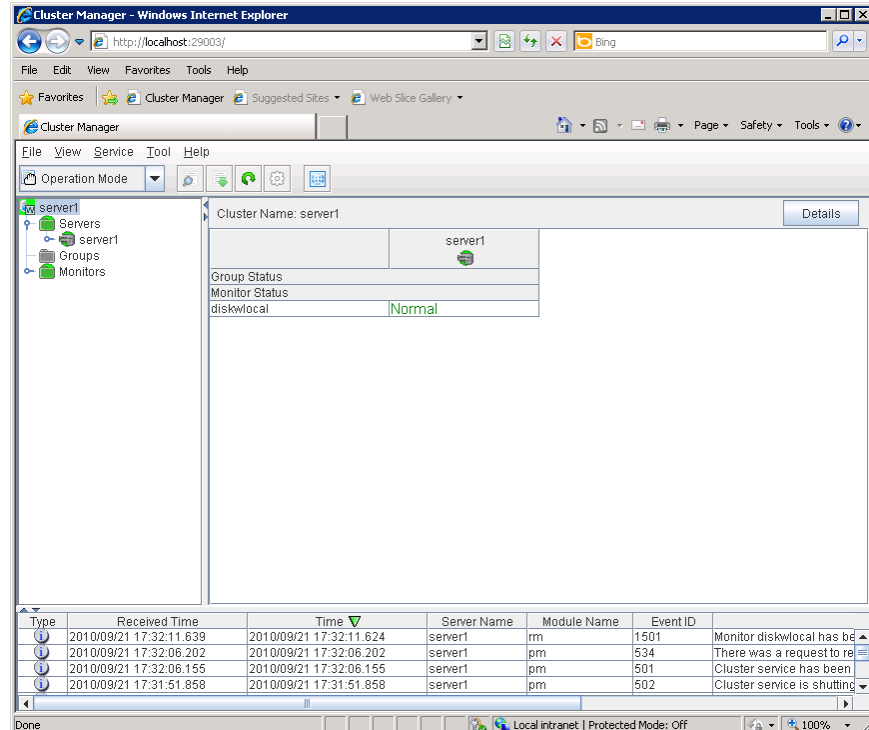
`http://192.168.0.1:29003/`



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 or select [Config Mode] on the dropdown menu of the toolbar 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 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 as many resources as the number of targets you want to monitor.

#### **3-1 Adding a monitor resource**

Add a monitor resource that performs monitoring.

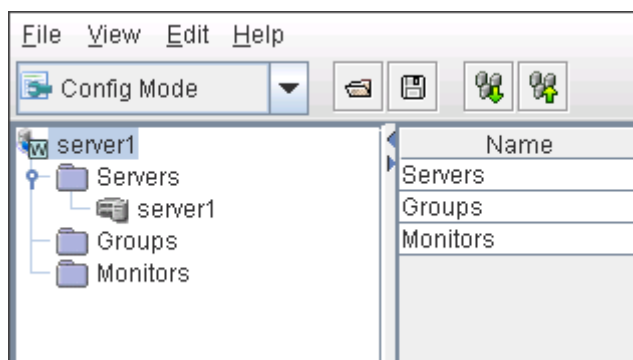
# 1. Setting up the server

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

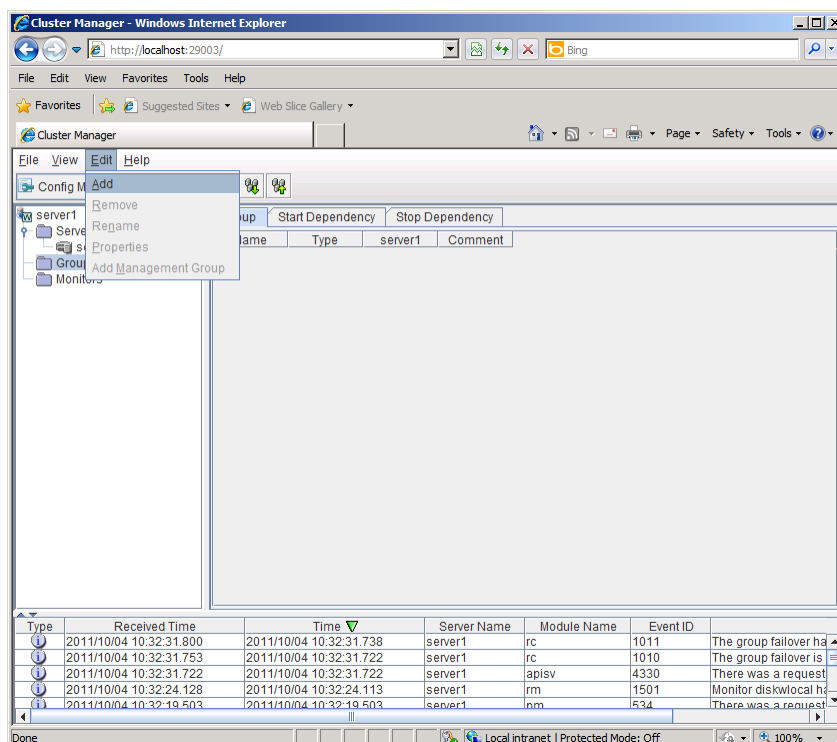
A group is a set of services and processes necessary to perform an independent operation in the system.

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.

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

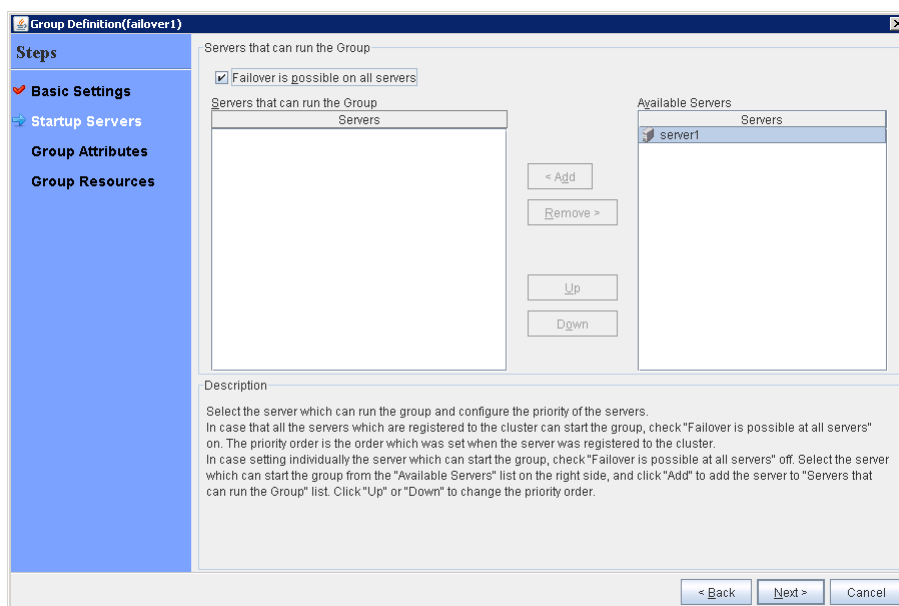
The screenshot shows the 'Group Definition' dialog box. On the left, a 'Steps' pane lists 'Basic Settings', 'Startup Servers', 'Group Attributes', and 'Group Resources'. The 'Basic Settings' section is active. In the 'Group Definition' area, the 'Type' dropdown is set to 'failover'. Below it is an unchecked checkbox labeled 'Use Server Group Settings'. The 'Name' text box contains 'failover1', and the 'Comment' text box is empty. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A 'Description' section at the bottom of the main area contains the following text: 'Select group type. If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover". If using server group, check the "Use Server Group".'

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

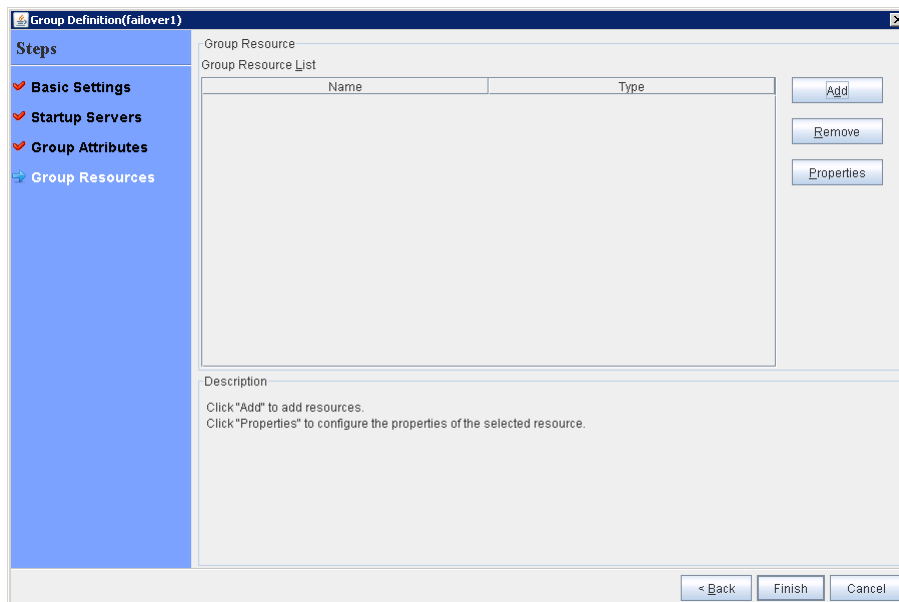
This screenshot shows the same 'Group Definition' dialog box at a lower resolution. The 'Description' field is now a tooltip, indicated by a green question mark icon and the label 'Description'. The tooltip text is: 'Select group type. If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover". If using server group, check the "Use Server Group".'

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

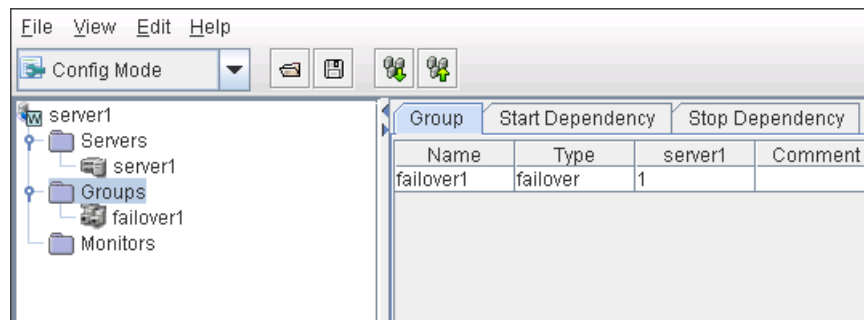
3. Make sure that the **Failover is possible on all servers** check box is selected, and then click **Next**.



4. This dialog box is used to specify the values of the failover group attributes. Click **Next** without specifying anything. The **Group Resource List** is displayed.



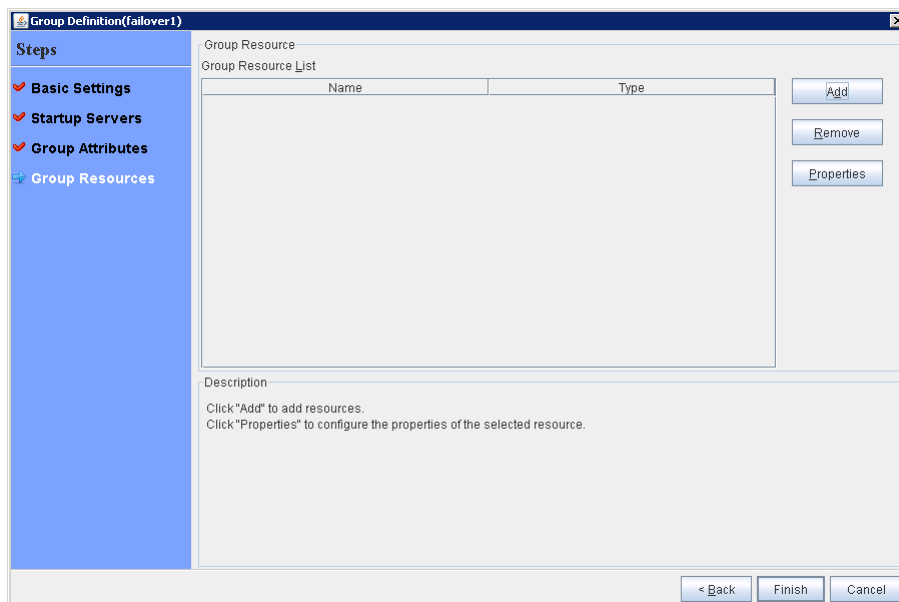
The table view is as follows.



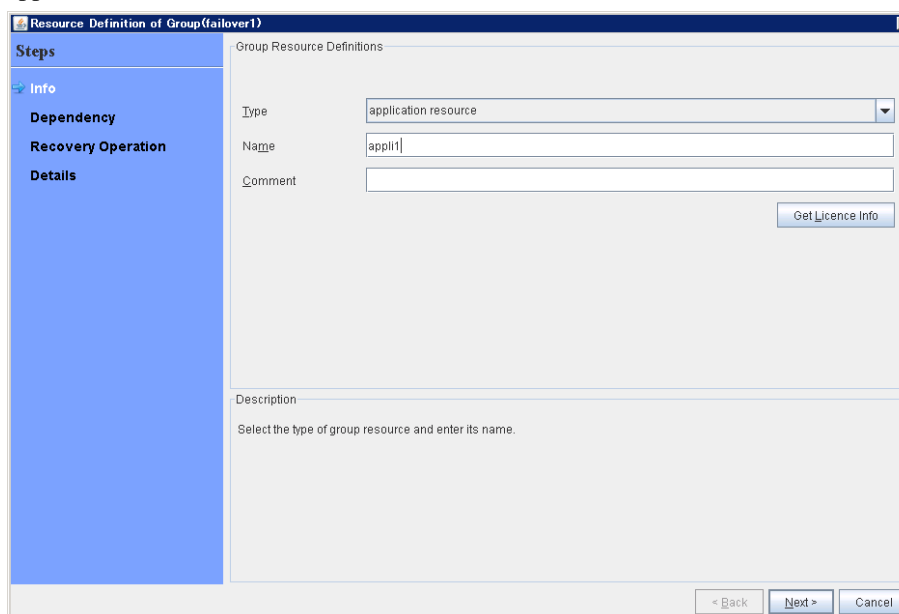
## 2-2 Adding a group resource (application resource)

Add an application resource that can start and stop the application.

1. Click **Add** in **Group Resource List**.



2. The **Resource Definition of Group(failover1)** dialog box is displayed. Select the group resource type (application resource) in the **Type** box, and enter the group resource name appli1 in the **Name** box. Click **Next**.



### Note:

The available types are **Application resource**, **Script resource**, and **Service resource**. When selecting **Virtual machine** for the type of the group in "2-1 Adding a group", **Virtual machine resource** is selectable.

3. A page for setting up a dependency is displayed. Click **Next**.

Resource Definition of Group(failover1)

Steps

- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency**
- Recovery Operation
- Details

☐ Follow the default dependency

Dependent Resources

Name	Resource type
------	---------------

< Add

Remove >

Available Resources

Name
------

< Back   Next >   Cancel

4. **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** are displayed. Click **Next**.

Resource Definition of Group(failover1)

Steps

- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency
- Recovery Operation**
- Details

Recovery Operation at Activity Failure Detection

Retry Count: 0 time

Failover Target Server

☐ Stable Server   ☒ Maximum Priority Server

Failover Threshold

☐ Set as much as the number of the servers   ☒ Set Number

Final Action: Stop the cluster service and reboot OS

☐ Execute Script before Final Action   Settings

Recovery Operation at Deactivation Failure Detection

Retry Count at Deactivation Failure: 0 time

Final Action: Stop the cluster service and shutdown OS

☐ Execute Script before Final Action   Settings

< Back   Next >   Cancel

5. Select **Resident** in the **Resident Type**. And specify the path of the execution file for the **Start Path**.

Resource Definition of Group(failover1)

Steps

- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency
- Recovery Operation
- Details

Resident Type

☒ Resident ☐ Non-Resident

Start Path

Stop Path

Tuning

< Back Finish Cancel

**Note:**

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

6. Click **Finish**.  
An application resource is added to the **Group Resource List**.

Group Definition(failover1)

Steps

- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources

Group Resource

Group Resource List

Name	Type
appl1	application resource

Add

Remove

Properties

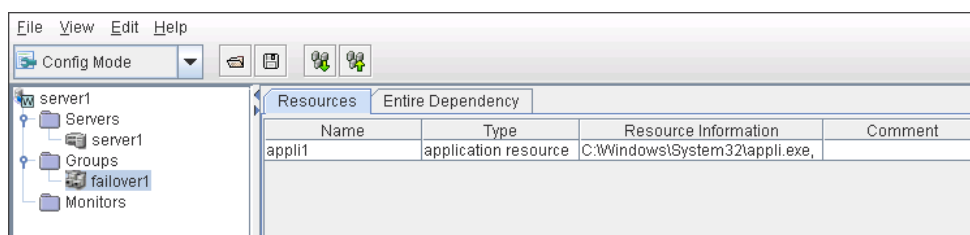
Description

Click "Add" to add resources.  
Click "Properties" to configure the properties of the selected resource.

< Back Finish Cancel

**7. Click Finish.**

The table view is as follows.

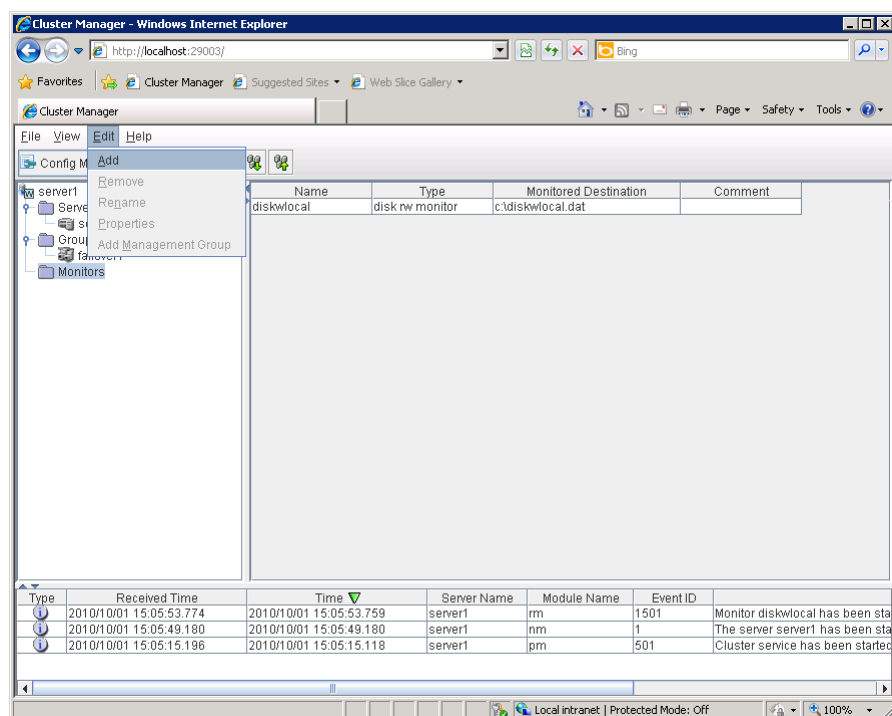


### 3. Setting up monitor resources

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** 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**.

The screenshot shows the 'Monitor Resource Definition' dialog box. On the left, the 'Steps' pane is active, showing 'Info', 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The main area is titled 'Monitor Resource Definition'. It contains a 'Type' dropdown menu with 'ip monitor' selected, a 'Name' text box with 'ipw1' entered, and an empty 'Comment' text box. A 'Get License Info' button is located to the right of the 'Comment' box. Below these fields is a 'Description' section with the text: 'Select the type of monitor resource and enter its name.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Note:**

Monitor resources are displayed in **Type**. Select the resource you want to monitor.

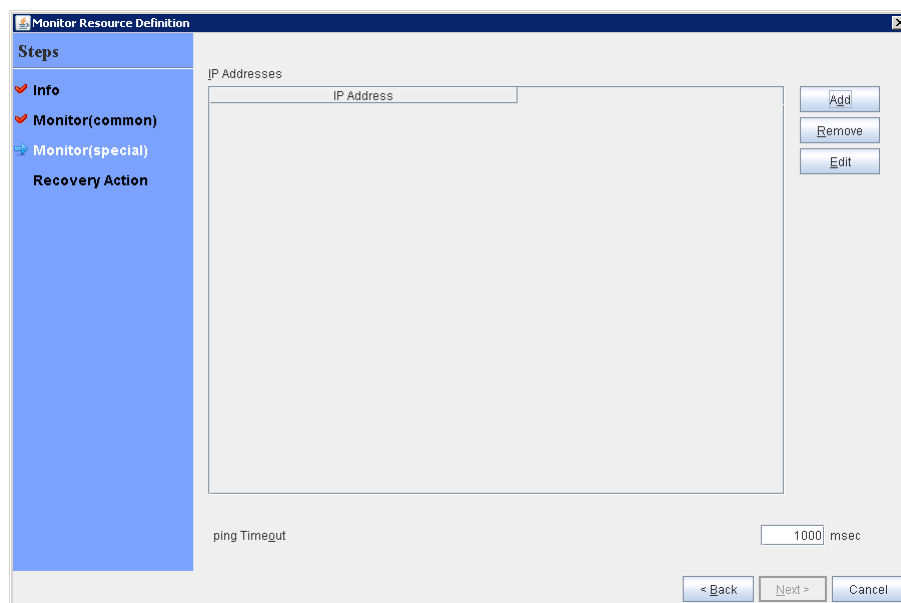
If the licenses for optional products have not been installed, the resources and monitor resources corresponding to those licenses are not shown in the list on the Builder (online version).

If any monitor resources are not displayed in the list box of [Type] even though the licenses are registered, please click [Get License Info] button.

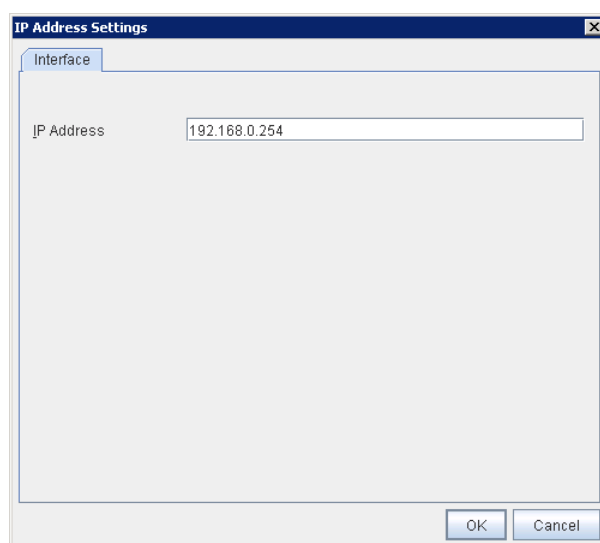
3. Enter the monitor settings. Change nothing from the default values. Click **Next**.

The screenshot shows the 'Monitor Resource Definition' dialog box at Step 3. The left pane shows 'Info', 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The main area contains several settings: 'Interval' (60 sec), 'Timeout' (60 sec), 'Retry Count' (1 time), and 'Wait Time to Start Monitoring' (0 sec). Below these is the 'Monitor Timing' section with two radio buttons: 'Always' (selected) and 'Active'. Under 'Monitor Timing' is a 'Target Resource' text box with a 'Browse' button to its right. At the bottom is a section titled 'Choose servers that execute monitoring' with a 'Server' button. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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**.



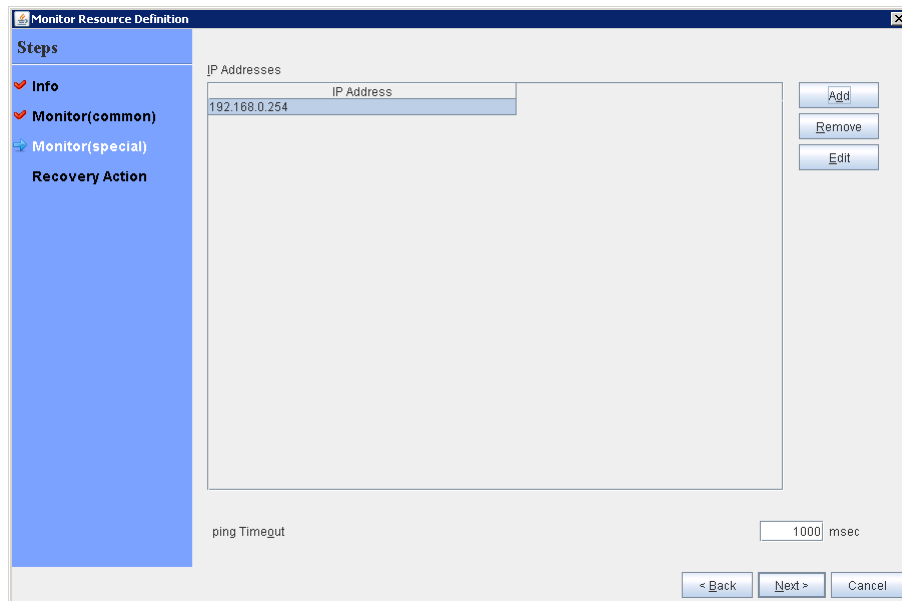
---

**Note:**

For monitoring target of the IP monitor resource, specify an IP address of the device (i.e., gateway) that is assumed to be always active on public LAN

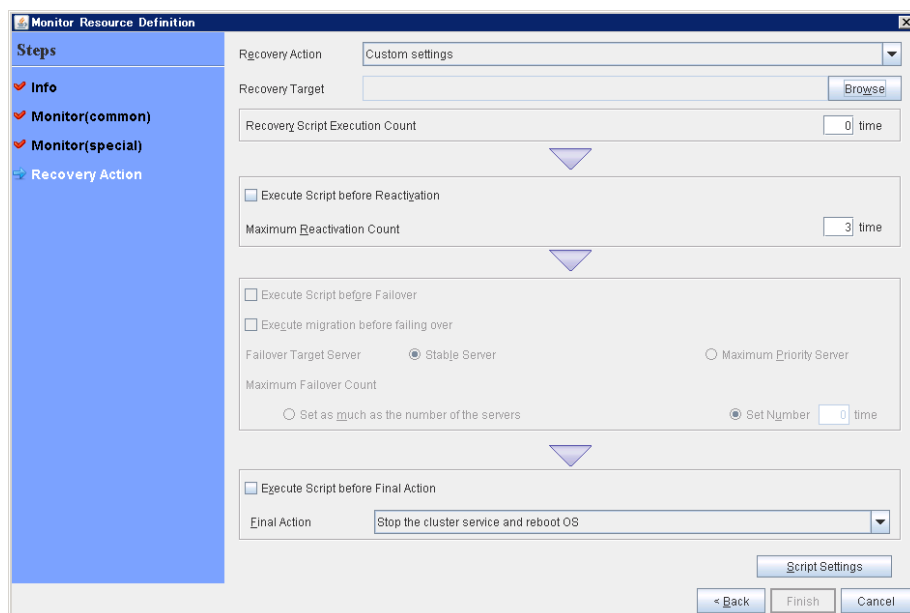
---

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



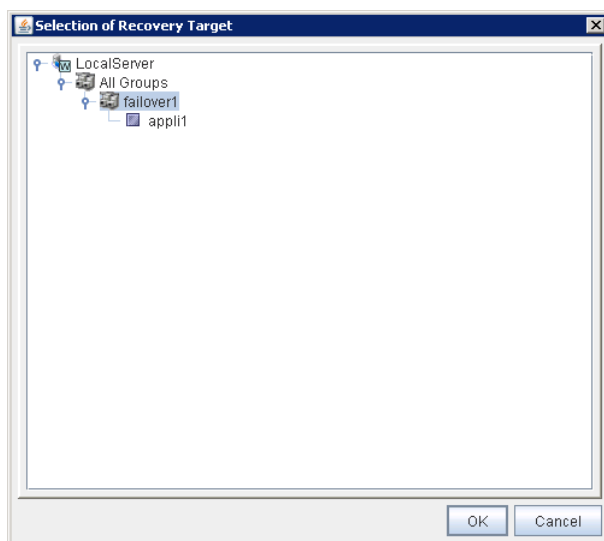
The screenshot shows the 'Monitor Resource Definition' dialog box with the 'IP Addresses' step selected in the left sidebar. The main area contains a table with one row: '192.168.0.254'. To the right of the table are buttons for 'Add', 'Remove', and 'Edit'. Below the table is a 'ping Timeout' field set to '1000' msec. At the bottom are 'Back', 'Next >', and 'Cancel' buttons.

7. Specify the recovery target. Click **Browse**.

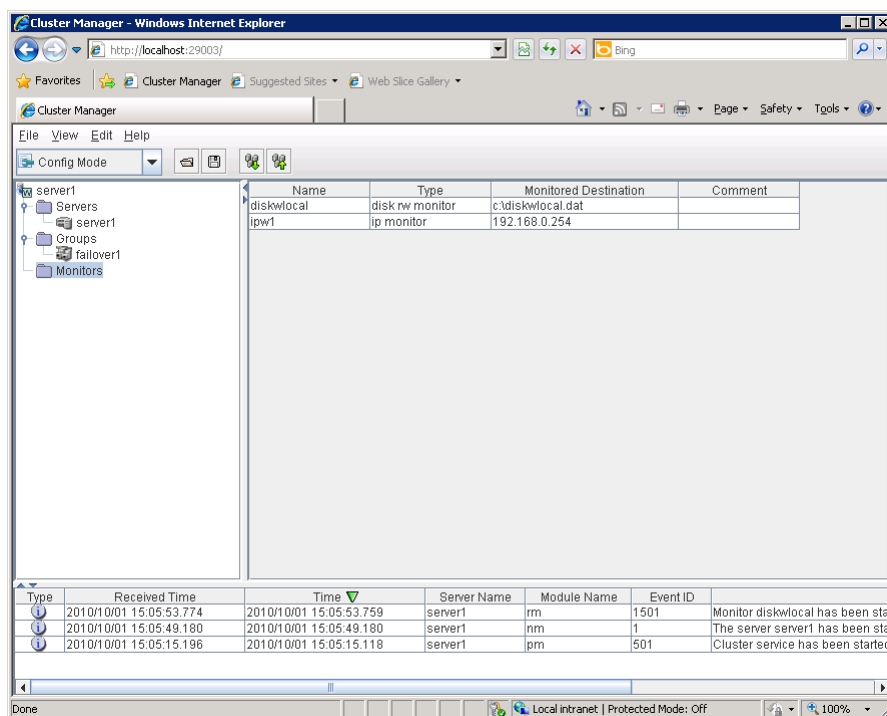


The screenshot shows the 'Monitor Resource Definition' dialog box with the 'Recovery Action' step selected in the left sidebar. The main area contains several configuration options: 'Recovery Action' is set to 'Custom settings'; 'Recovery Target' has a 'Browse' button; 'Recovery Script Execution Count' is set to '0' time; 'Execute Script before Reactivation' is unchecked; 'Maximum Reactivation Count' is set to '3' time; 'Execute Script before Failover' is unchecked; 'Execute migration before failing over' is unchecked; 'Failover Target Server' has 'Stable Server' selected; 'Maximum Failover Count' has 'Set Number' selected and set to '0' time; 'Execute Script before Final Action' is unchecked; and 'Final Action' is set to 'Stop the cluster service and reboot OS'. At the bottom are 'Script Settings', 'Back', 'Finish', and 'Cancel' buttons.

8. Click failover1 in the displayed tree view. Click **OK**. “failover1” is set in the **Recovery Target**.



9. Click **OK**.  
After the settings are specified, the window appears as follows.



## 3-2 Adding a monitor resource (application monitor resource)

1. Click the Monitors object in the tree view, and then click **Add** in the **Edit** menu. The **Monitor Resource Definition** is displayed.
2. Select the monitor resource type (application monitor) in the **Type** box, and enter the monitor resource name appliw1 in the **Name** box. Click **Next**.

**Monitor Resource Definition**

**Steps**

- Info
- Monitor(common)**
- Monitor(special)
- Recovery Action

Monitor Resource Definition

Type: application monitor

Name: appliw1

Comment:

Get Licence Info

Description

Select the type of monitor resource and enter its name.

< Back Next > Cancel

3. Enter the monitoring settings. Click **Browse**.

**Monitor Resource Definition**

**Steps**

- Info
- Monitor(common)
- Monitor(special)
- Recovery Action**

Interval: 60 sec

Timeout: 60 sec

Retry Count: 1 time

Wait Time to Start Monitoring: 0 sec

Monitor Timing

☐ Always

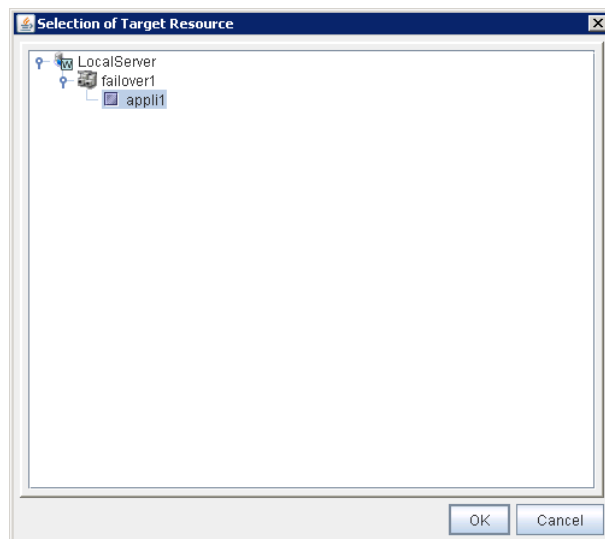
☒ Active

Target Resource: Browse

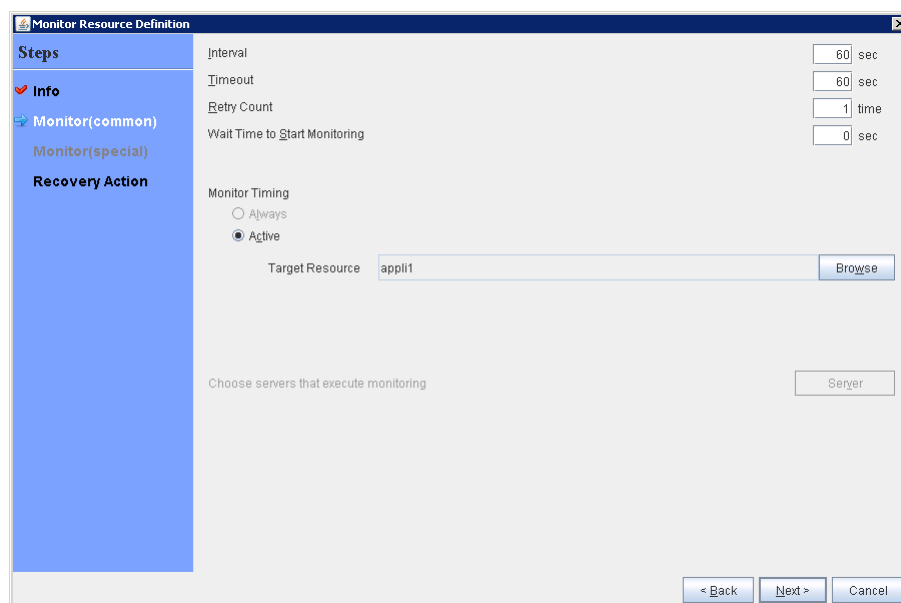
Choose servers that execute monitoring: Server

< Back Next > Cancel

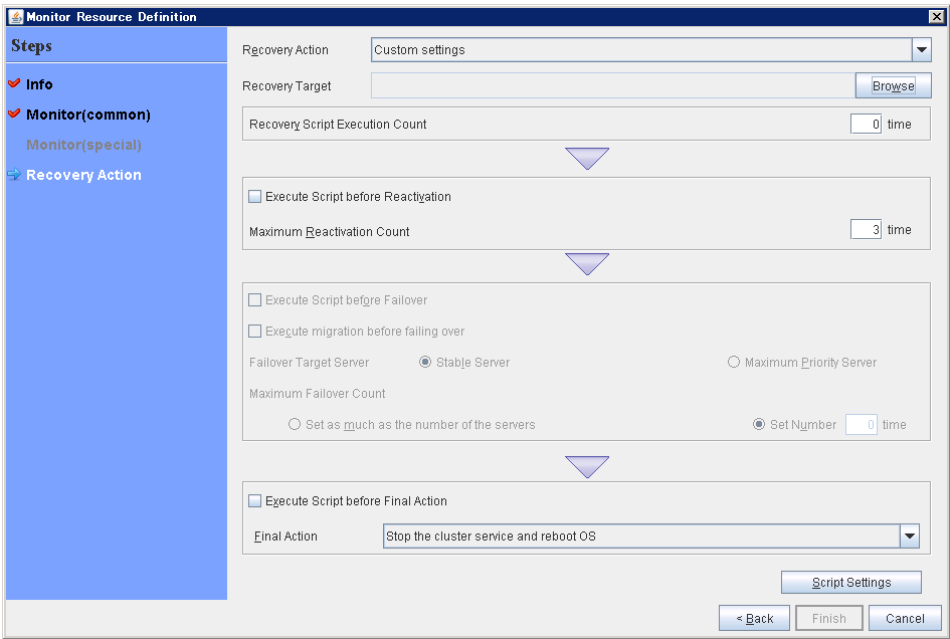
4. Click **appli1** in the displayed tree view, and then click **OK**.



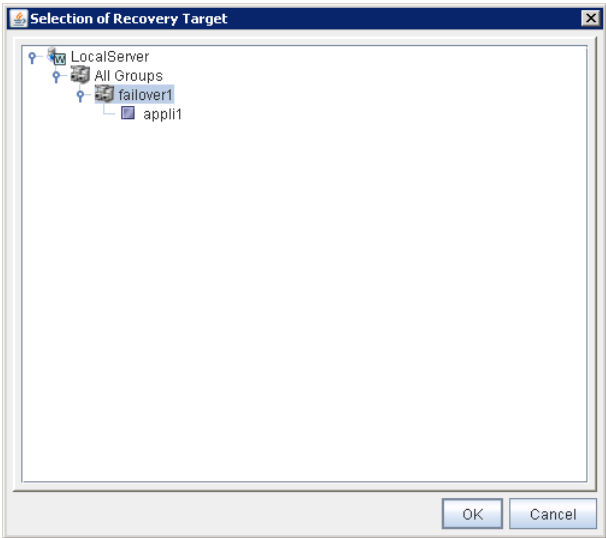
5. **appli1** is specified for **Target Resource**. Click **Next**.

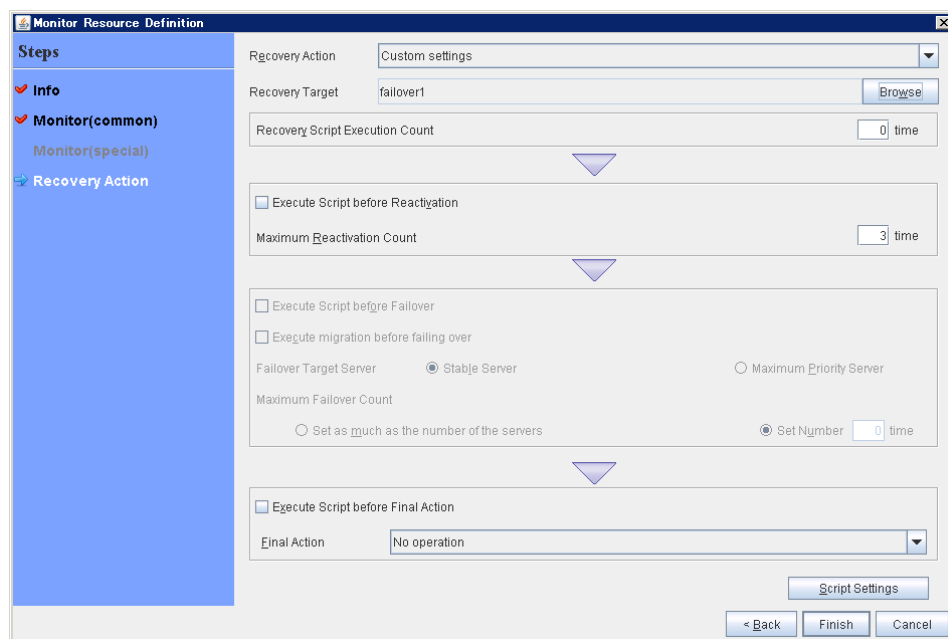


6. Set the recovery target. Click **Browse**.



7. Click **failover1** in the displayed tree view. Click **OK**.



**8. failover1 is set in the Recovery Target.**

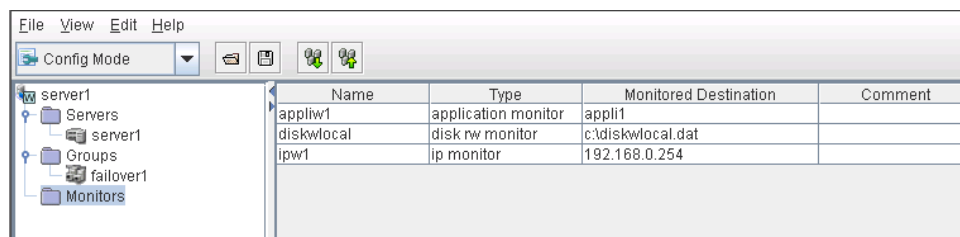
The **Monitor Resource Definition** dialog box is shown. The **Steps** pane on the left has **Recovery Action** selected. The main area contains the following settings:

- Recovery Action:** Custom settings
- Recovery Target:** failover1 (with a **Browse** button)
- Recovery Script Execution Count:** 0 time
- ☐ **Execute Script before Reactivation**
- Maximum Reactivation Count:** 3 time
- ☐ **Execute Script before Failover**
- ☐ **Execute migration before failing over**
- Failover Target Server:** ☒ Stable Server ☐ Maximum Priority Server
- Maximum Failover Count:** ☐ Set as much as the number of the servers ☒ Set Number 0 time
- ☐ **Execute Script before Final Action**
- Final Action:** No operation

Buttons at the bottom: **Script Settings**, **< Back**, **Finish**, and **Cancel**.

**9. Click Finish.**

The table view will look similar to the following.



The screenshot shows a configuration tool window with a tree view on the left and a table on the right. The tree view shows a hierarchy: **server1** > **Servers** > **server1** > **Groups** > **failover1** > **Monitors**. The table on the right displays the following data:

Name	Type	Monitored Destination	Comment
appli1	application monitor	appli1	
diskwlocal	disk rw monitor	c:\diskwlocal.dat	
ipw1	ip monitor	192.168.0.254	

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

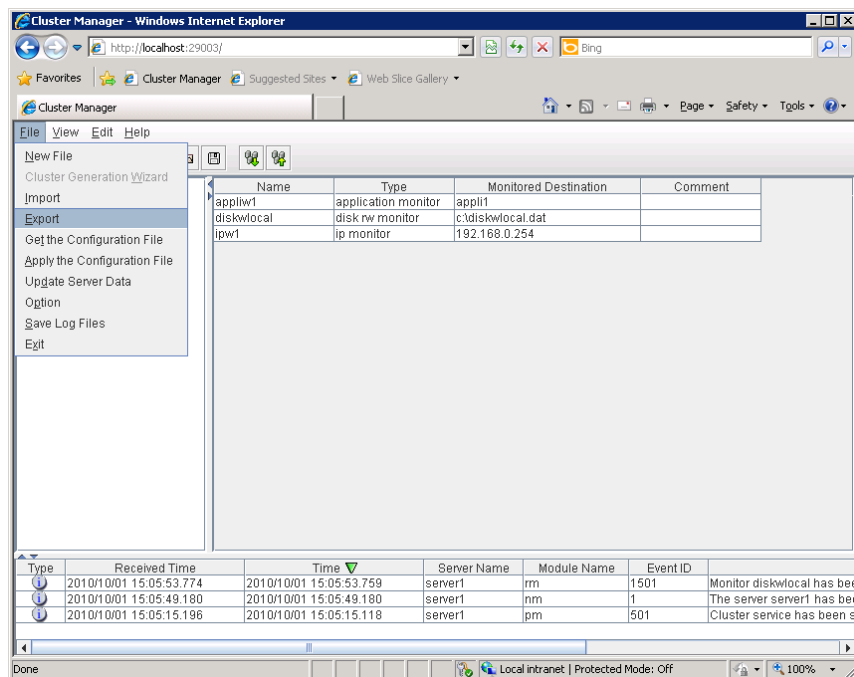


## Saving configuration data

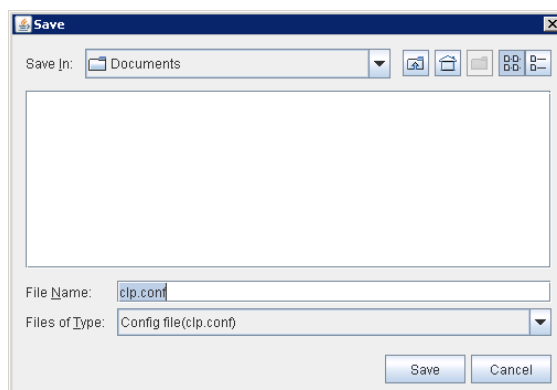
The created configuration data can be saved in a folder on your PC or in external media.

To save the configuration data, follow the procedure below.

1. Select **Export** on the **File** menu or on the toolbar in the Builder (WebManager Config Mode) window.



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



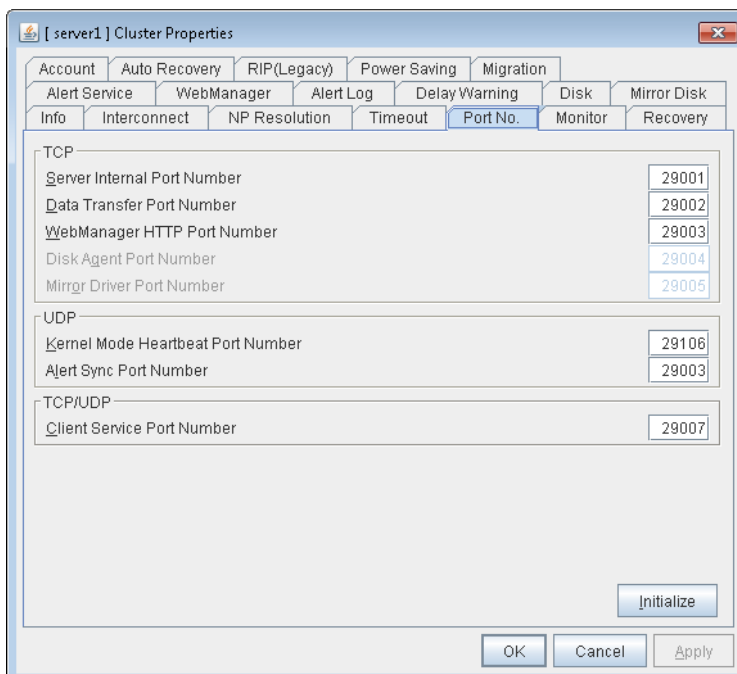
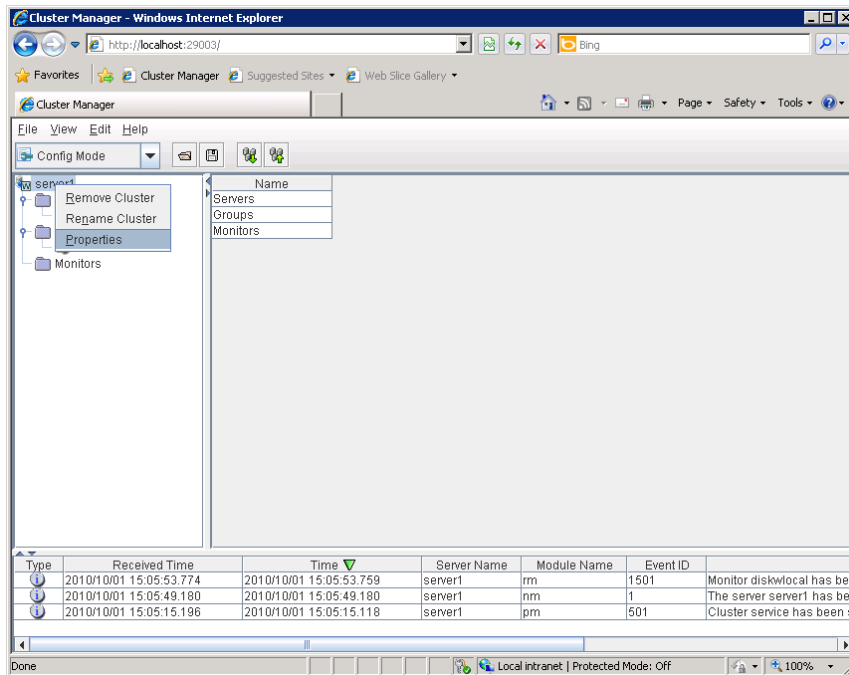
### Note:

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.

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

**Note:**

If you specified a port number for **Port Number** that differed from the default value when installing ExpressCluster X SingleServerSafe, click **Cluster Properties** and then the **Port No.** tab and change the value of **WebManager HTTP Port Number** to the same value as that specified at the time of installation, before saving the configuration data.

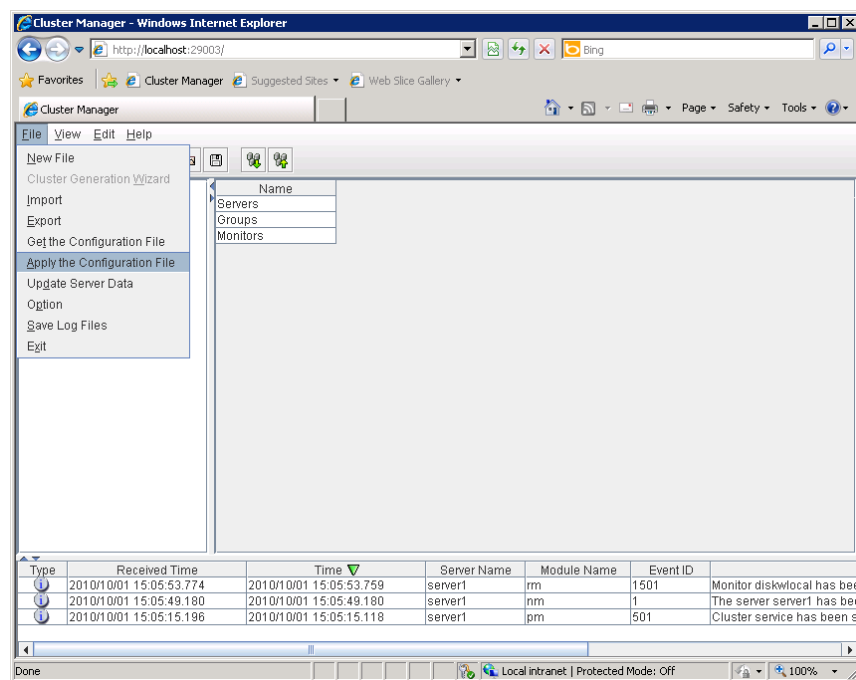


## Applying configuration data

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

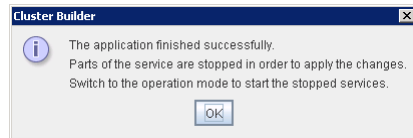
To apply the configuration data, follow the procedure below.

1. Click **Apply the Configuration File** on the **File** menu or toolbar on WebManager Config Mode window.



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

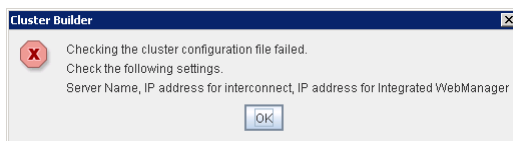
3. If the upload succeeds, the following dialog box is displayed (the messages on the following dialog box will be different depends on cluster configuration).



---

**Note:**

If the upload fails, perform the operations by following the displayed message.



# Differences regarding the use of the offline version of the Builder

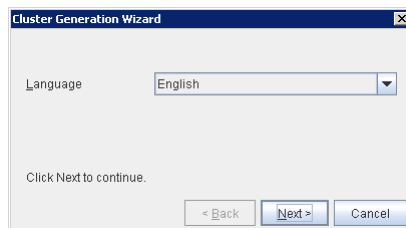
When using the offline version of the Builder, you need to use different procedures for creating configuration data initially and having the data applied.

## 1. Setting up the server

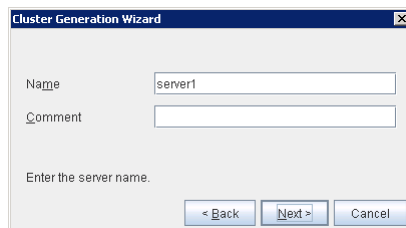
Because the offline version of the Builder cannot automatically acquire information about the server to be set up, you need to manually specify configuration data.

### 1-1 Setting up a server

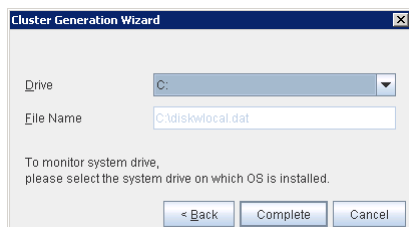
1. On the **File** menu, click **Cluster Generation Wizard**.
2. The **Cluster Generation Wizard** window is displayed. In the **Language** field, select the language used on the machine where the WebManager runs. Click **Next**.



3. Enter the server name **server1** in the **Name** box. Click **Next**.



4. A dialog box is displayed for entering information about the disk RW monitor resource. Select the drive letter **C:** as the drive in which the OS is installed. Click **Complete**.



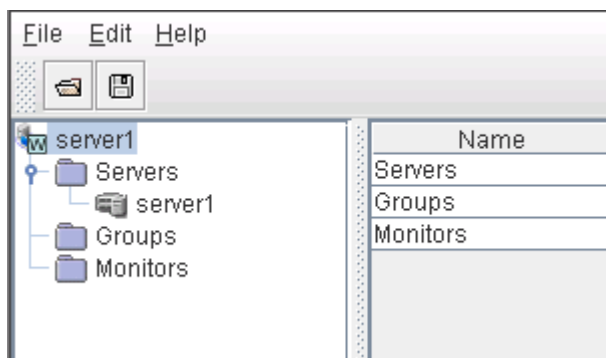
---

**Note:**

For details about the disk RW monitor resource, see Chapter 5 , "Monitor resource details."

---

The table view is as follows:

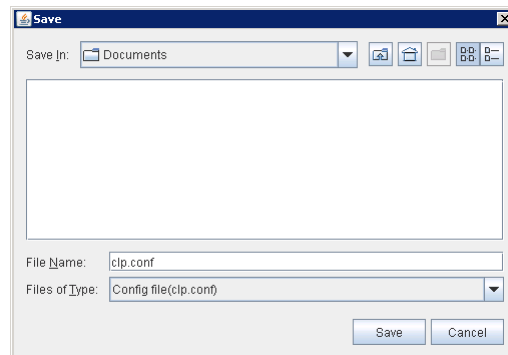


## 2. Saving configuration data

To apply configuration data to the server you will set up, save the data to external media. As external media, you can specify a file sharing server on the network, a floppy disk, a USB memory device, or other media.

To save the configuration data, follow the procedure below.

1. Select **Export** on the **File** menu or toolbar of the Builder.
2. In the following dialog box, select the external media to which to save the data, and then click **Save**.



### 3. Applying configuration data

To allow the server you will set up to access configuration data, reference the shared folder or take another appropriate step, such as inserting a floppy disk or USB memory device into the server.

On the server you will set up, run the command to apply the configuration data. For details about the command, see "Applying configuration data" in Chapter 2, "ExpressCluster X SingleServerSafe command reference" in the *Operation Guide*.



# Chapter 3      LAN board redundancy function

This chapter describes the LAN board redundancy function.

This chapter covers:

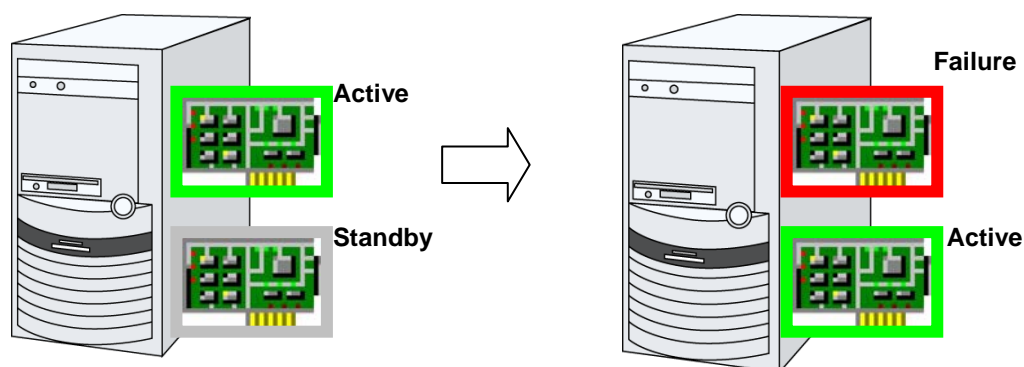
Understanding LAN board redundancy .....	58
Setting up LAN board redundancy .....	59

## Understanding LAN board redundancy

LAN board redundancy prevents the server from stopping its operation in the event of a LAN board failure.

Mount two LAN boards on the server, and set them up in the same way. Run the server using only one of the LAN boards. If the active LAN board fails, the other LAN board is automatically switched to.

This prevents the server from stopping its operation in the event of a LAN board failure.



---

**Note:**

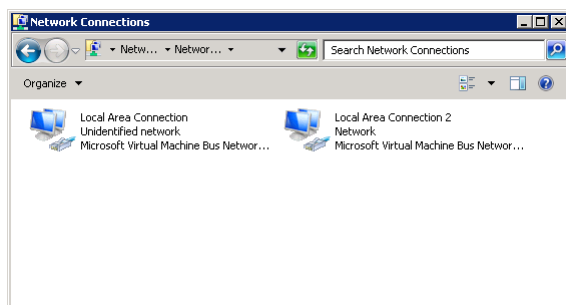
If using an FT server, use the FT server redundancy function instead of the LAN board redundancy function of ExpressCluster X SingleServerSafe. If you use the redundancy function of ExpressCluster X SingleServerSafe, the redundancy function might malfunction.

---

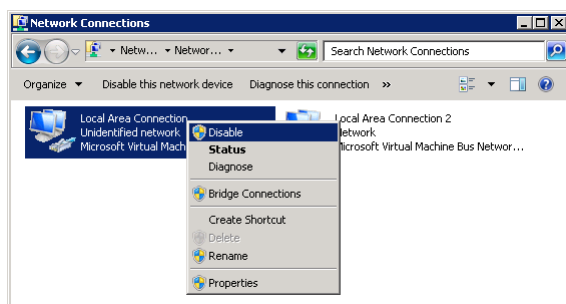
## Setting up LAN board redundancy

To set up LAN board redundancy, follow the procedure below.

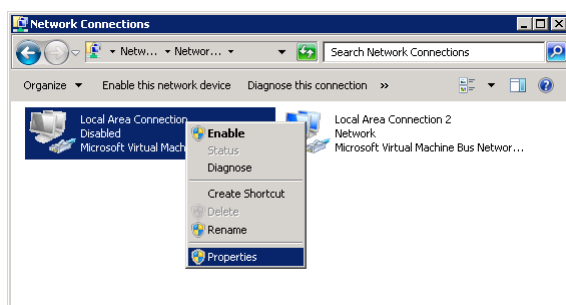
1. Open the **Network Connections** window.  
Under **LAN or High-Speed Internet**, network connection icons are displayed that correspond to the two LAN boards.



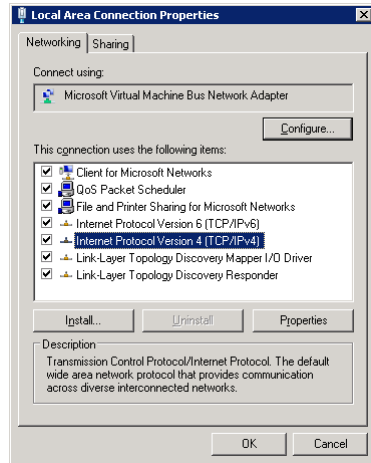
2. Right-click one of the icons, and then select **Disable** in the displayed menu.



3. Right-click the icon again, and then select **Properties** in the displayed menu.

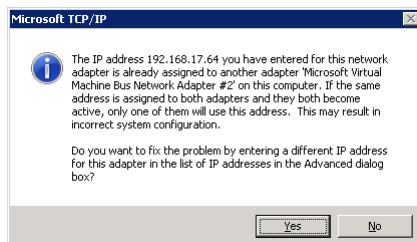


4. When the **Properties** dialog box is displayed, select **Internet Protocol (TCP/IP)**, and then click the **Properties** button. Set the IP address and all other data to the same values as those of the other LAN board.

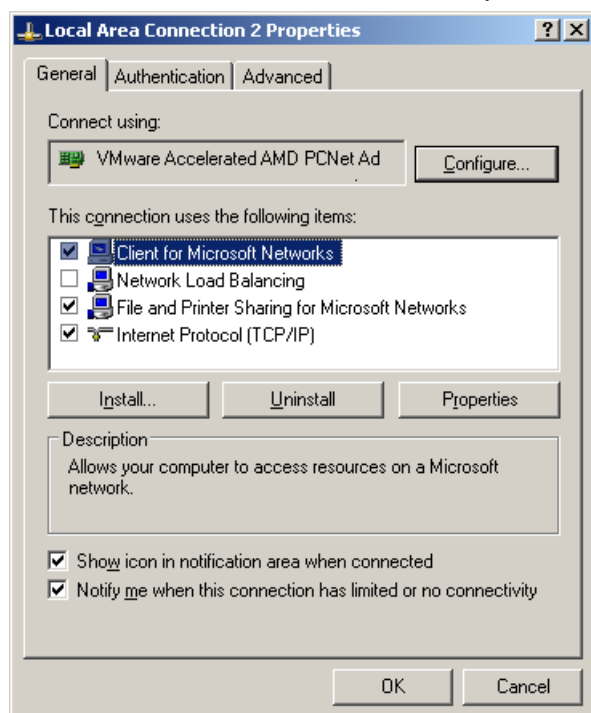


This completes the setup. After the server is rebooted, redundancy control begins for the LAN boards when the ExpressCluster SingleServerSafe service starts.

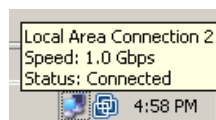
Because the LAN boards use the same IP address, the message below might be displayed. In this case, click **No**.



In Windows Server 2003 environment, if you select **Show icon in notification area when connected** in the **Properties** dialog box, the task tray will display an icon or balloon message to indicate the LAN board status (error/recovery).



The task tray will display following icon:





## 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
Chapter 5	Monitor resource details
Chapter 6	Other setting details





# Chapter 4      Group resource details

This chapter provides details about group resources.  
This chapter covers:

Group resources .....	66
Setting up application resources .....	67
Setting up script resources.....	72
Setting up service resources .....	83
Setting up VM resources .....	86

## Group resources

The following resources can be defined as group resources.

Group resource name	Function	Abbreviation
Application resource	Provides a mechanism for starting and stopping an application (including a user-created application).	appli
Script resource	Provides a mechanism for starting and stopping a script (BAT) such as a user-created script.	script
Service resource	Provides a mechanism for starting and stopping a service such as a database or Web service.	service
VM resource	Starts and stops a virtual machine.	vm

## System requirements for VM resource

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

Virtualization platform	Version	Remarks
Hyper-V	Hyper-V 1.0	
	Hyper-V 2.0	
	Windows Server 2012 Hyper-V	

## Setting up application resources

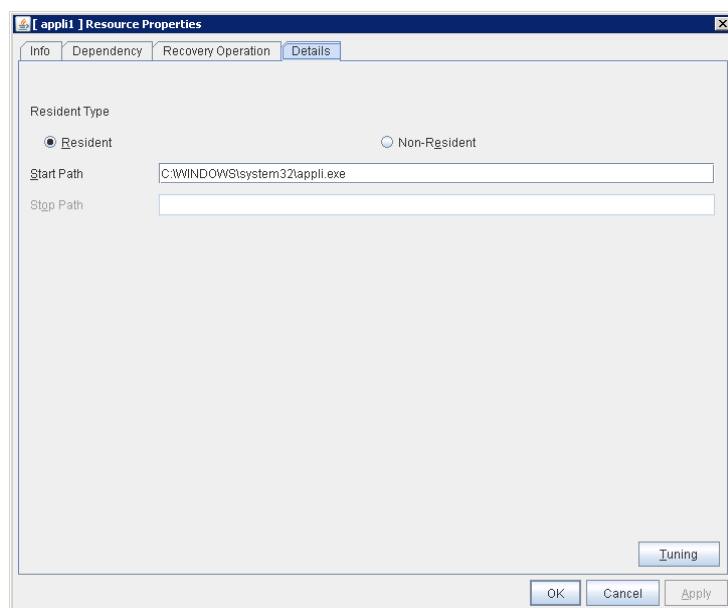
You can register applications that are to be managed by ExpressCluster X SingleServerSafe and executed when a group starts or stops. It is also possible to register your own applications in application resources.

Applications are programs that are executable from the command line and have an extension such as exe, cmd, or bat.

## Displaying and changing the application resource details

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

### Resource Properties: Details tab



#### Resident Type (default: **Resident**)

Specify the type of the application. Choose one of the types below.

##### ◆ Resident

Select this when the application resides in ExpressCluster.

##### ◆ Non-resident

Select this when the application does not reside in ExpressCluster (and control returns to the system immediately after the application is executed).

#### Start Path (within 1,023 bytes)

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

**Stop Path** (within 1,023 bytes)

Specify the name of the file that can be run when the application resource is stopped. This cannot be set when the resident type is Resident.

---

**Note:**

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

---

**Tuning**

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

**Application Resource Tuning Properties****Parameter tab**

Detailed parameter settings are displayed on this tab.

The screenshot shows the 'Application Resource Tuning Properties' dialog box with the 'Parameter' tab selected. The dialog is divided into 'Start' and 'Stop' sections. In the 'Start' section, 'Synchronous' is selected with a radio button, and the 'Timeout' is set to 1800 seconds. There is a text field for 'Normal Return Value'. The 'Stop' section also has 'Synchronous' selected with a radio button and a 'Timeout' of 1800 seconds, with a corresponding 'Normal Return Value' text field. Below these sections is a 'Target YCOM Resource Name' dropdown menu and a checkbox for 'Allow to Interact with Desktop'. At the bottom right is an 'Initialize' button, and at the bottom center are 'OK', 'Cancel', and 'Apply' buttons.

**Synchronous (Start)**

This setting is not available for a resident application.

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

**Asynchronous (Start)**

This setting is not available for a resident application.

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

**Normal Return Value (Start)**

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

Specify what error code returned from the executable file set by **Start Path** is normal when

**Resident Type is Non-resident.**

## ◆ When there is no value

The return value is ignored. This is the same operation as the X2.1 and earlier.

## ◆ When there is a value

Observe the following input rules.

- Values can be separated by commas (for example, 0, 2, 3).
- Values can be specified using a hyphen (for example, 0-3).

---

**Note:**

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

---

**Synchronous (Stop)**

If the application is resident, select this to wait for the currently running application to stop.

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

**Asynchronous (Stop)**

If the application is resident, select this so as not to wait for the currently running application to stop.

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

**Normal Return Value (Stop)**

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

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

## ◆ When there is no value

The return value is ignored. This is the same operation as the X2.1 and earlier.

## ◆ When there is a value

Observe the following input rules.

- Values can be separated by commas (for example, 0, 2, 3).
- Values can be specified using a hyphen (for example, 0-3).

---

**Note:**

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

---

**Timeout (Start) (1 to 9999)**

This setting is not available for a resident application.

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

**Timeout (Stop) (1 to 9999)**

Configure the timeout value to wait (synchronous) for currently running resident application(s) to stop or for a non-resident application to stop when the application is run.

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

**Target VCOM Resource Name**

Not used.

**Allow to Interact with the Desktop**

Specify whether to allow the application to be run to interact with desktop. If this is selected, the application screen is displayed on the desktop when the application starts running. This setting is not available when an **Exec User** is specified on the **Start** and **Stop** tabs.

**Initialize**

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

**Start and Stop tabs**

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

The screenshot shows the 'Application Resource Tuning Properties' dialog box with the 'Start' tab selected. The 'Parameter' tab is also visible. The 'Stop' tab is disabled. The 'Current Directory' field is empty. The 'Option Parameter' field is empty. The 'Window Size' dropdown is set to 'Hide'. The 'Exec User' section is expanded, showing 'Domain', 'Account', and 'Password' fields, all of which are empty. A 'Change' button is next to the 'Password' field. There is a checkbox for 'Execute from the Command Prompt' which is unchecked. An 'Initialize' button is at the bottom right. At the very bottom are 'OK', 'Cancel', and 'Apply' buttons.

**Current Directory** Within 1023 bytes

Specify a directory for running the application.

**Option Parameter** Within 1023 bytes

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

Example: "param" 1 param2

**Window Size**

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

- **Hide**

The application is not displayed.

- **Normal**

The application is displayed in a regular window size.

- **Maximize**

The application is displayed in a maximum window size.

- **Minimize**

The application is displayed in a minimum window size.

**Exec User Domain**

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

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

**Exec User Account**

Specify the user account that runs the application.

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

**Exec User Password**

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

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

**Execute from the Command Prompt**

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

**Initialize**

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

## Setting up script resources

You can register scripts that are to be managed by ExpressCluster X SingleServerSafe and executed when a group starts or stops. It is also possible to register your own scripts for script resources.

Start and stop scripts are provided for script resources. These are executed when starting and stopping a group, respectively. Their file names are fixed.

start.bat	Start script
stop.bat	Stop script



**Group A start script: a sample of stop.bat**

```
rem *****
rem *          START.BAT          *
rem *****
```

```
IF "%CLP_EVENT%" = "START" GOTO NORMAL
IF "%CLP_EVENT%" = "FAILOVER" GOTO FAILOVER
IF "%CLP_EVENT%" = "RECOVER" GOTO RECOVER
```

Refer to the environment variable of the script starting factor to determine the process to be executed.

```
GOTO no_arm
```

ExpressCluster is not active.

```
:NORMAL
IF "%CLP_DISK%" = "FAILURE" GOTO ERROR_DISK
```

**Process overview:**

Application's normal startup process

*When to start this process:*

Normal startup

```
IF "%CLP_SERVER%" = "OTHER" GOTO ON_OTHER1
```

Refer to the environment variable of the executing server to determine the process to be executed.

**Process overview:**

A process to be executed only when the application is normally started on the primary server

*When to start this process:*

Normal startup

```
GOTO EXIT
```

```
:ON_OTHER1
```

**Process overview:**

A process to be executed only when the application is normally started on a server other than the primary server

*When to start this process:*

**Not used for SingleServerSafe.**

```
GOTO EXIT
```

```
:FAILOVER
```

Refer to the DISK connection information environment variable to handle the error.

```
IF "%CLP_DISK%" = "FAILURE" GOTO ERROR_DISK
```

**Process overview:**

Application's normal startup process

*When to start this process:*

**Not used for SingleServerSafe.**

IF "%CLP\_SERVER%" = "OTHER" GOTO ON\_OTHR2

Refer to the environment variable of the executing server to determine the process to be executed.

*Process overview:*

A process to be executed only when the application is started on the primary server after failover

*When to start this process::*

**Not used for SingleServerSafe.**

GOTO EXIT

:ON\_OTHER2

*Process overview:*

A process to be executed only when the application is started on a non-primary server after failover

*When to start this process::*

**Not used for SingleServerSafe.**

GOTO EXIT

:RECOVER

*Process overview:*

Recovery processing after cluster recovery

*When to start this process:*

Cluster recovery

GOTO EXIT

:ERROR\_DISK

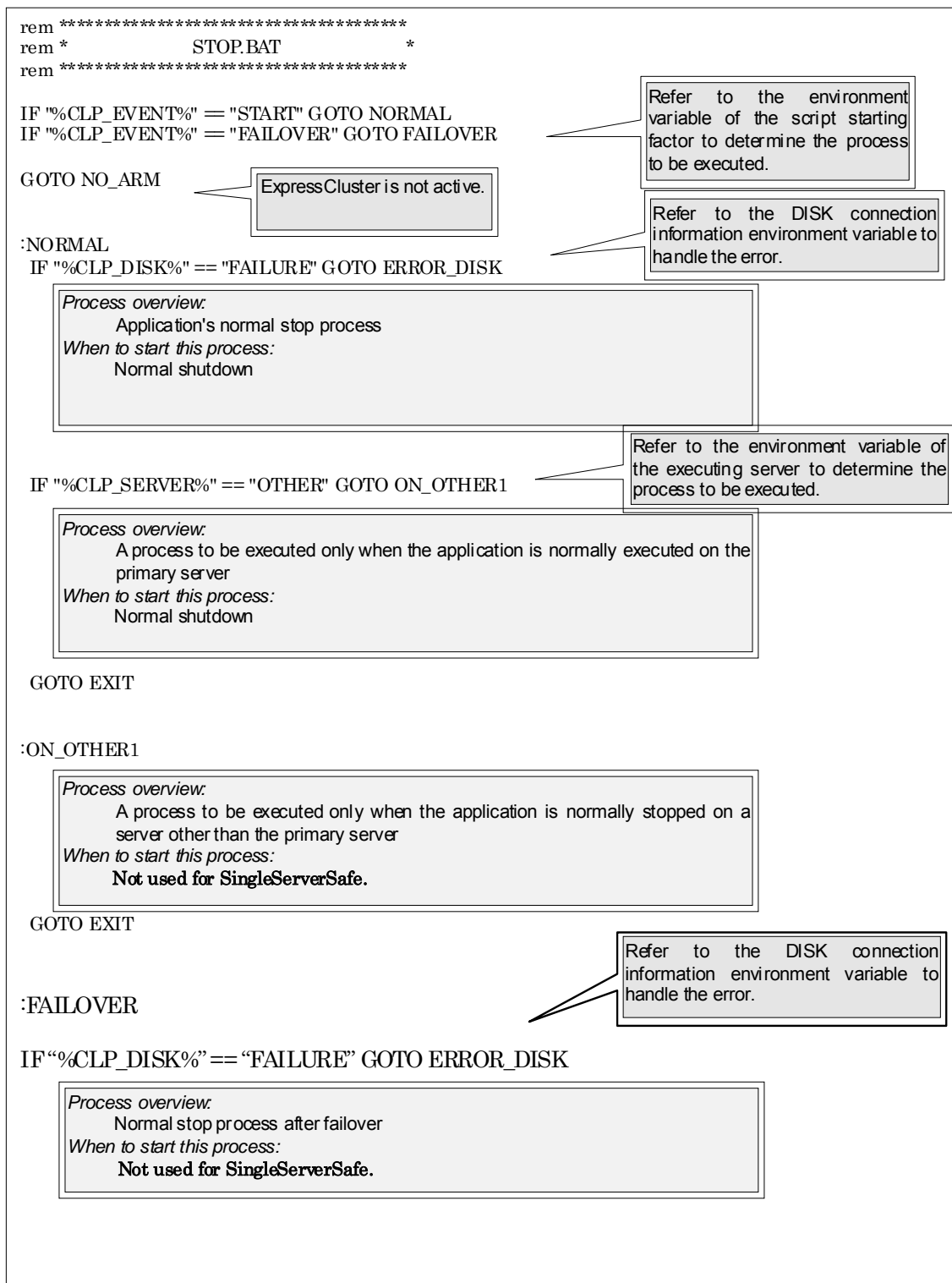
Disk-related error handling

:no\_arm

:EXIT

exit

## Group A stop script: a sample of stop.sh



IF "%CLP\_SERVER%" = "OTHER" GOTO ON\_OTHR2

Refer to the environment variable of the executing server to determine the process to be executed.

*Process overview:*

A process to be executed only when the application is stopped on the primary server after failover

*When to start this process::*

**Not used for SingleServerSafe.**

GOTO EXIT

:ON\_OTHER2

*Process overview:*

A process to be executed only when the application is stopped on a non-primary server after failover

*When to start this process::*

**Not used for SingleServerSafe.**

GOTO EXIT

:ERROR\_DISK

Disk-related error  
handling

:NO\_ARM

:EXIT

exit

## Tips for creating scripts

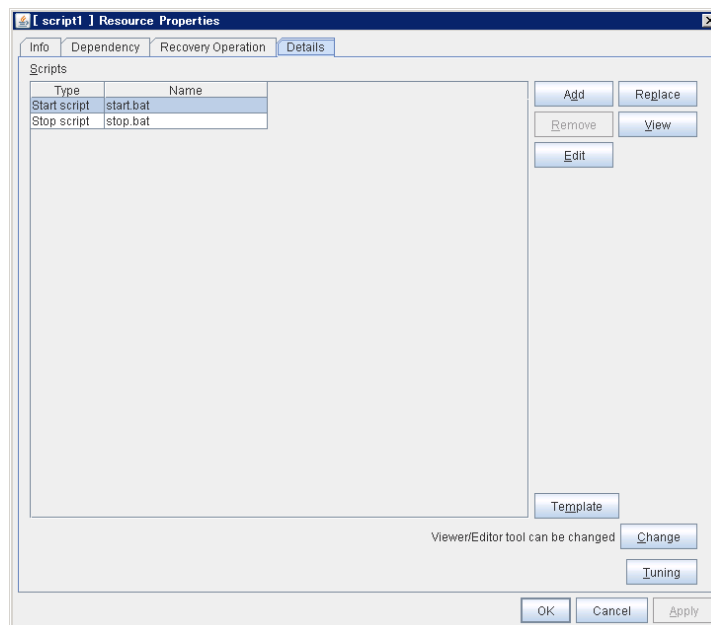
- ◆ The clplogcmd command, though which message output on the WebManager alert view is possible, is available.

## Displaying and changing the script resource details

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

### Resource Properties: Details tab

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



#### Add

Use this button to add a script other than **start.bat** script and **stop.bat** script.

#### Remove

Use this button to delete a script. The **start.bat** script and **stop.bat** script cannot be deleted.

#### View

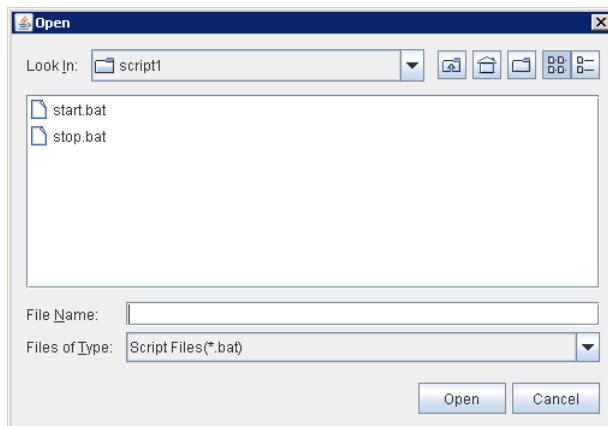
Use this button to display the selected script file on the script editor. The information edited and stored with the editor is not applied. You cannot display the script file if it is currently displayed or edited.

### 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.



---

### Note:

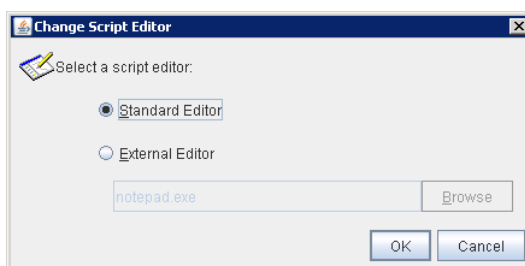
The file will not be deleted even if you delete a script file from the Builder. If the cluster configuration data is reloaded by restarting the Builder after deleting the script file, the deleted script file will be displayed in the **Scripts**.

---

The content of the script file selected in the **Resource 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.

### Change

Click here to display the **Change Script Editor** dialog. 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.

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

### Tuning

Open the **Script Resource Tuning Properties** dialog box. You can make advanced settings for the script resource.

## Script Resource Tuning Properties

### Parameter tab

Detailed parameter settings are displayed on this tab.

### Common to all start scripts and stop scripts

#### Synchronous

Select this button to wait for a script to end when it is run.

#### Asynchronous

This cannot be selected.

#### Normal Return Value

Configure what error code from the script is normal.

##### ◆ When there is no value

The return value is ignored. This is the same operation as the X2.1 and earlier.

##### ◆ When there is a value

Observe the following input rules.

- Values can be separated by commas (for example, 0, 2, 3).
- Values can be specified using a hyphen (for example, 0-3).

---

#### Note:

When specifying a value to **Normal Return Value**, set the same value to start script and stop script.

An error cannot be detected when 1 is specified as **Normal Return Value** because 1 is returned when an error occurs with cmd.exe which executes the script.

---

#### Timeout 1 to 9999

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

**Target VCOM Resource Name**

Not used.

**Allow to Interact with Desktop**

Specify whether to allow the script to be run to communicate with desktop. If this is selected, progress status of the script can be checked on the screen. It is effective if used when debugging the script.

---

**Note:**

For Windows Server 2008 or later, command prompt window that execute start.bat or stop.bat can not be displayed even if **Allow to Interact with Desktop** is enabled.

---

**Initialize**

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



## Using the simple selection function of a script template

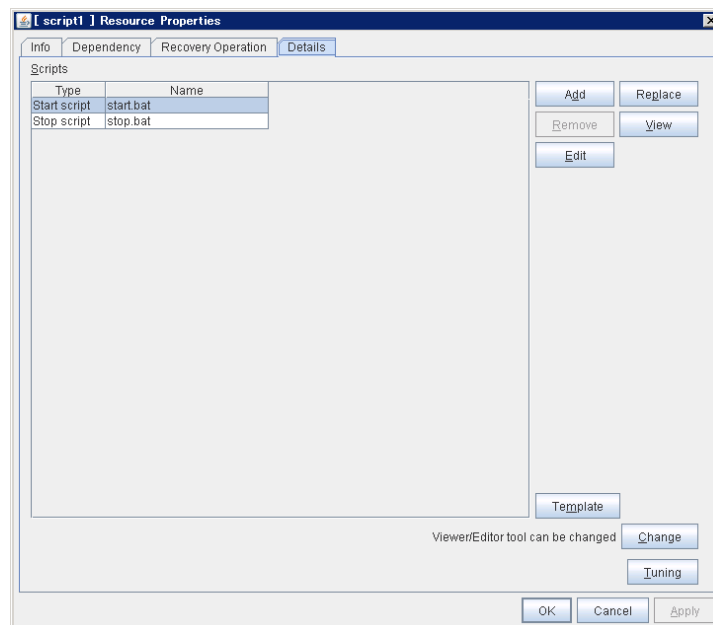
Selecting an application from the script resource enables you to automatically replace the necessary script template. You can simply create a script by editing the template script.

**Note:**

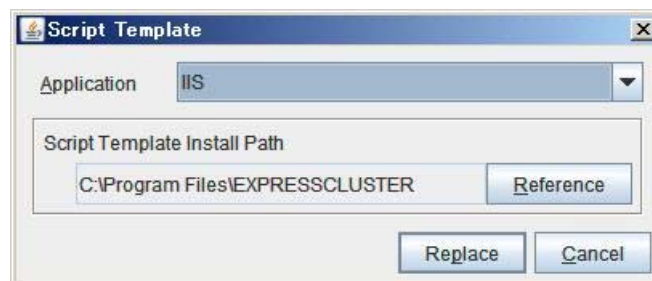
To use this function, you must install the script template in advance.

## Using the simple selection function of a script template

1. From the tree view displayed in the left pane of the Builder, click the icon of the group to which the script resource whose script template to be replaced belongs.
2. A group resource list is displayed in the table view to the right of the window. Right-click the target script resource name and then click the **Details** tab of **Properties**.



3. Click **Template**.
4. 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.

### Reference

Clicking **Reference** displays 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 the script resource details".

---

## Setting up service resources

You can register services that are to be managed by ExpressCluster X SingleServerSafe and executed when a group starts or stops. It is also possible to register your own services to service resources.

A service resource refers to a service managed by the OS service control manager.

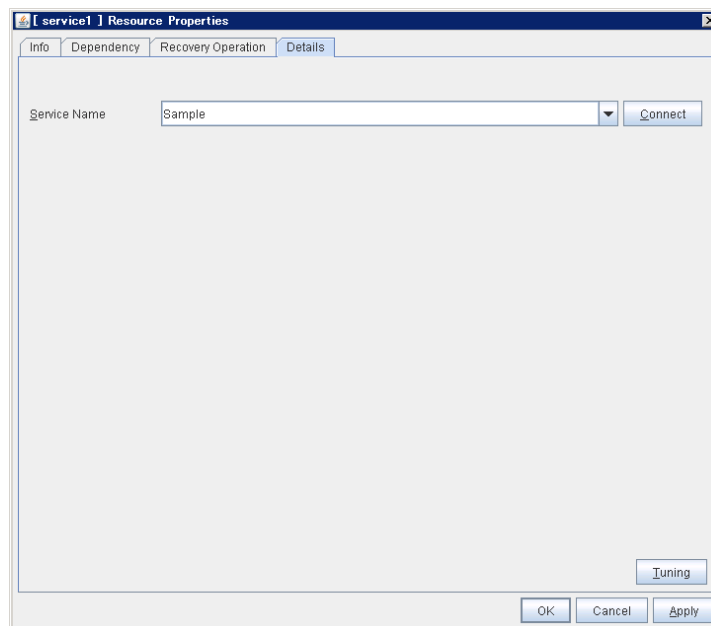
### Notes on service resources

- Generally, the service executed by the service resource is set to manual start. In case of the service which is executed by automatic start or the service which may be executed by other than the service resource, it is necessary to check on **Do not assume it as an error when the service is already started** which is described below in **Service** tab of **Service resource tuning properties**. If this check box is off, activation fails when executing service start processing by the service resource to the service which has already been executed.

### Displaying and changing the service resource details

- In the tree view shown on the left pane of the Builder, click the icon of the group to which the service resource whose detailed information you want to display or change belongs.
- The list of group resources is displayed in the table view on the right pane of the screen. Right-click the name of the service resource that you want to display or change. Click **Properties**, and then click **Details** tab.
- Display and/or change the settings by following the description below.

#### Resource Properties: Details tab



**Service Name** (within 1023 bytes)

Specify the service name or service display name used in the service resource.

Combo box options display the list of the service display names of the services collected from the server.

**Connect**

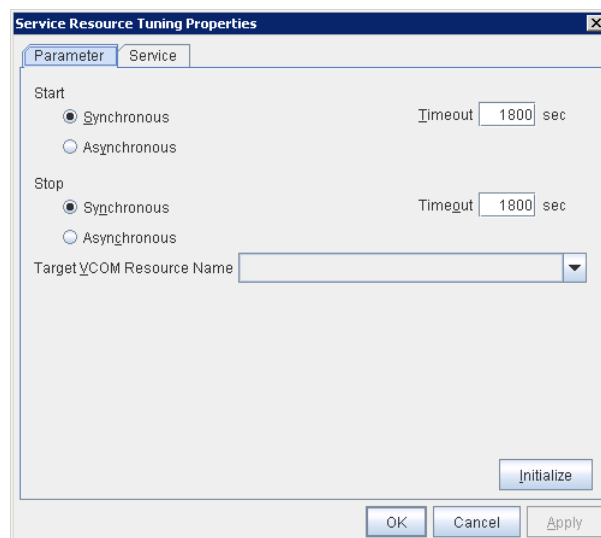
Collects the service list from the server and updates the service display name list to be displayed in the **Service Name** combo box.

**Tuning**

Open the **Service Resource Tuning Properties** dialog box. You can make advanced settings for the service resource.

**Service Resource Tuning Properties****Parameter tab**

Detailed parameter settings are displayed on this tab.

**Synchronous**

When the service is started up, it waits for “Started.” Typically, the status changes from “Stopping” to “Started” when the service is started.

When stopping the service, it waits for that the status of service becomes “Stopped.” Typically, the status changes from “Stopping” to “Stopped” when the service is stopped.

**Asynchronous**

No synchronization is performed.

**Timeout** (1 to 9999)

Specify the timeout for the status of the service to become “Started” at the time starting the service. The timeout can be specified only when **Synchronous** is selected. If the status of the service does not change to “Started” within the timeout, it is determined as an error.

Specify the timeout for the stats of the service to become “Stopped” at the time stopping the service. The timeout can be specified only when **Synchronous** is selected. If the status of the service does not change to “Stopped” within the timeout, it is determined as an error.

**Target VCOM Resource Name**

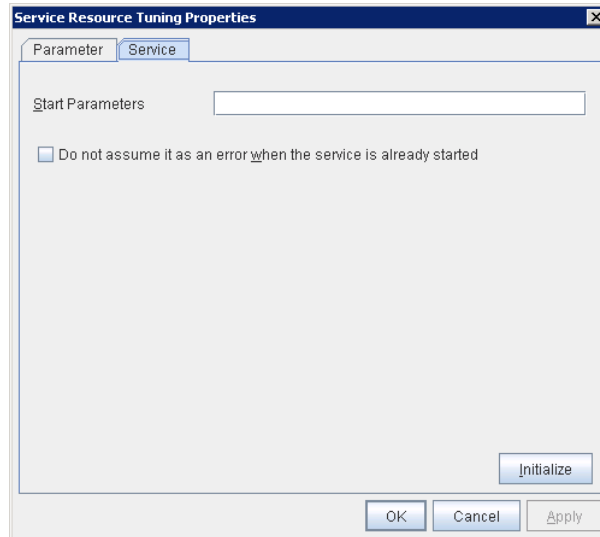
Not used.

### Initialize

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

### Service tab

The settings for the service are displayed.



**Start Parameters** Within 1023 bytes

Specify a parameter for the service. When there are multiple parameters, leave a space between parameters. For a parameter that includes a space, enclose the parameter by double quotation marks. Note that backslash \ cannot be used.

Example: "param 1" param2

### Do not assume it as an error when the service is already started

- When selected

When the service is started, if the service is already started up, activation status is kept.

- When cleared

When the service is started, if the service is already started up, it is considered as activation error.

### Initialize

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

## Setting up VM resources

VM resources control virtual machines set up on the following virtualization platform:

Hyper-V

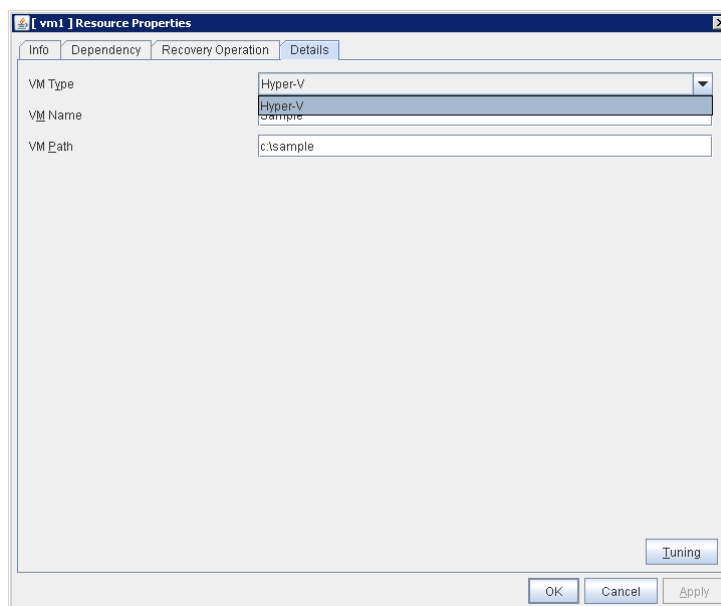
VM monitor resources control virtual machines by using a WMI interface.

VM resources start or stop virtual machines.

## Displaying and changing the VM resource details

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

### Resource Properties: Details tab



### VM Type

Specify the virtualization platform on which the virtual machine is set up. Currently, only Hyper-V is supported.

### VM Name

Enter the virtual machine name displayed in the Hyper-V Manager.

### VM Path

Enter the path of the virtual machine configuration file.

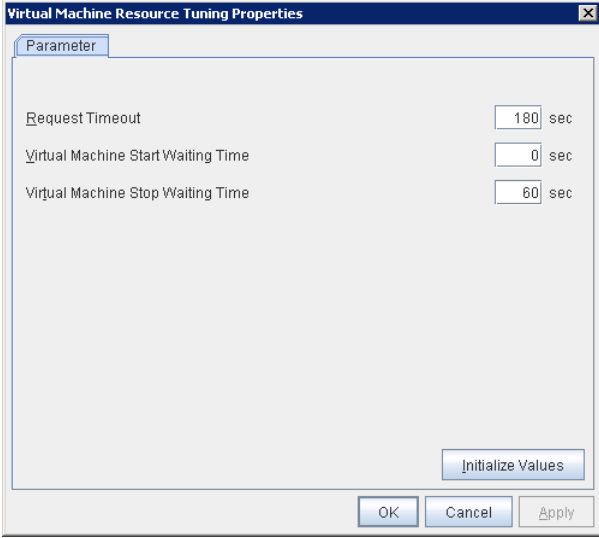
## Tuning

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

### Virtual Machine Resource Tuning Properties

#### Parameter tab

Detailed settings for the parameters are displayed.



The screenshot shows the 'Virtual Machine Resource Tuning Properties' dialog box with the 'Parameter' tab selected. It contains three parameters with input fields and units:

Parameter	Value	Unit
Request Timeout	180	sec
Virtual Machine Start Waiting Time	0	sec
Virtual Machine Stop Waiting Time	60	sec

At the bottom right of the parameter list is an 'Initialize Values' button. At the bottom of the dialog box are 'OK', 'Cancel', and 'Apply' buttons.

#### 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

Specify the wait time to wait for the startup completion of the guest OS on the virtual machine and the application after the request to the virtual machine to start up completes and the status of the virtual machine becomes running at the resource activation.

#### Virtual Machine Stop Waiting Time

Specify the wait time for the shutdown of the guest OS on the virtual machine at the resource deactivation.

#### Initialize Values

Clicking **Initialize Values** sets the values of all the items to the defaults.





# 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 .....	90
Common settings for monitor resources .....	100
Setting up application monitor resources .....	108
Setting up service monitor resources .....	109
Setting up disk RW monitor resources .....	110
Setting up IP monitor resources .....	113
Setting up NIC link up/down monitor resources .....	116
Setting up custom monitor resources .....	118
Setting up multi target monitor resources .....	121
Setting up message receive monitor resources .....	125
Setting up VM monitor resources .....	127
Setting up process name monitor resources .....	128
Setting up DB2 monitor resources .....	131
Setting up FTP monitor resources .....	135
Setting up HTTP monitor resources .....	138
Setting up IMAP4 monitor resources .....	141
Setting up ODBC monitor resources .....	144
Setting up Oracle monitor resources .....	148
Setting up OracleAS monitor resources .....	154
Setting up POP3 monitor resources .....	159
Setting up PostgreSQL monitor resources .....	162
Setting up SMTP monitor resources .....	167
Setting up SQL Server monitor resources .....	170
Setting up Tuxedo monitor resources .....	174
Setting up Weblogic monitor resources .....	176
Setting up WebOTX monitor resources .....	179
Setting up Websphere monitor resources .....	181
Setting up JVM monitor resources .....	184
Setting up system monitor resources .....	219

## 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:
Application monitor resource	Monitors application resources.	When activated (Fixed)	appli
Service monitor resource	Monitors service resources.	When activated (Fixed)	service
Disk RW monitor resource	Monitors disk devices by writing dummy data to the file system.	Always or <b>when activated</b>	All resources
IP monitor resource	Monitors IP addresses and communication paths by using the ping command and checking whether there is a response .	<b>Always</b> or when activated	All resources
NIC Link Up/Down monitor resource	Acquires the NIC link status to monitor whether the link is up or down.	<b>Always</b> or when activated	All resources
Custom monitor resource	Performs monitoring by executing any script.	<b>Always</b> or when activated	All resources
Multi target monitor resource	Performs monitoring by using multiple monitor resources in combination.	When activated (Fixed)	All resources
Message receive monitor resource	Specifies the action to take when an error message is received and how the message is displayed on the WebManager.	Always (Fixed)	None
VM monitor resource	Provides a mechanism for monitoring a virtual machine started by a VM resource.	When activated (Fixed)	vm
Process Name monitor resource	Monitors monitor the process of specified processes.	<b>Always</b> or 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	When activated	All

	mechanism for monitoring an HTTP server.	(Fixed)	resources
IMAP4 monitor resource	Provides a mechanism for monitoring an IMAP server.	When activated (Fixed)	All resources
ODBC monitor resource	Provides a mechanism for monitoring an ODBC accessible database.	When activated (Fixed)	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
SMTP monitor resource	Provides a mechanism for monitoring an SMTP server.	When activated (Fixed)	All resources
SQL Server monitor resource	Provides a mechanism for monitoring an SQL server database.	When activated (Fixed)	All resources
Tuxedo monitor resource	Provides a mechanism for monitoring a Tuxedo application server.	When activated (Fixed)	All resources
OfficeScan CL monitor resource	Provides a mechanism for monitoring an OfficeScan client.	Always (Fixed)	None
OfficeScan SV monitor resource	Provides a mechanism for monitoring an OfficeScan server.	When activated (Fixed)	All resources
Weblogic monitor resource	Provides a mechanism for monitoring a WebLogic application server.	When activated (Fixed)	All resources
WebOTX monitor resource	Provides a mechanism for monitoring a WebOTX application server.	When activated (Fixed)	All resources
Websphere monitor resource	Provides a mechanism for monitoring a WebSphere application server.	When activated (Fixed)	All resources
JVM monitor resources	Provides a	<b>Always</b> or	All

	mechanism for monitoring a Java VM.	when activated	resources
System monitor resources	Provides a mechanism for monitoring a System Resource.	Always (Fixed)	All resources

## Monitor resources that require a license

Monitor resources listed below require a license since they are optional products.

To use these monitor resources, obtain and register a product license.

Optional product name	Monitor resource name
ExpressCluster X Database Agent 3.1 for Windows	DB2 monitor resources
	ODBC monitor resources
	Oracle monitor resources
	PostgreSQL monitor resources
	SQL Server monitor resources
ExpressCluster X Internet Server Agent 3.1 for Windows	FTP monitor resources
	HTTP monitor resources
	IMAP4 monitor resources
	POP3 monitor resources
	SMTP monitor resources
ExpressCluster X Application Server Agent 3.1 for Windows	OracleAS monitor resources
	Tuxedo monitor resources
	Websphere monitor resources
	Weblogic monitor resources
	WebOTX monitor resources
ExpressCluster X Anti-Virus Agent 3.1 for Windows	OfficeScan CL monitor resource
	OfficeScan SV monitor resource
ExpressCluster X Java Resource Agent 3.1 for Windows	JVM monitor resources
ExpressCluster X System Resource Agent 3.1 for Windows	System monitor resources

For the procedure for registering a license, see the *Installation Guide*.

## Applications supported by monitoring options

The following applications are the target monitoring options that are supported.

IA32 version

Monitor resource	Application to be monitored	ExpressCluster Version	Remarks
Oracle monitor	Oracle 10g Release 2 (10.2)	11.00 or later	
	Oracle 11g Release 1 (11.1)	11.00 or later	
	Oracle 11g Release 2 (11.2)	11.00 or later	
DB2 monitor	DB2 V9.5	11.00 or later	
	DB2 V9.7	11.00 or later	
	DB2 V10.1	11.13 or later	
PostgreSQL monitor	PostgreSQL 8.1	11.00 or later	
	PostgreSQL 8.2	11.00 or later	
	PostgreSQL 8.3	11.00 or later	
	PostgreSQL 8.4	11.00 or later	
	PostgreSQL 9.0	11.03 or later	
	PostgreSQL 9.1	11.03 or later	
	PostgreSQL 9.2	11.17 or later	
	PowerGres on Windows V6.0	11.00 or later	
	PowerGres on Windows V6.1	11.00 or later	
	PowerGres on Windows V6.2	11.00 or later	
	PowerGres on Windows V6.3	11.00 or later	

	PowerGres on Windows V7.0	11.00 or later	
	PowerGres on Windows V7.1	11.00 or later	
	PowerGres on Windows V9.0	11.03 or later	
SQL Server monitor	SQL Server 2005	11.00 or later	
	SQL Server 2008	11.00 or later	
	SQL Server 2008 R2	11.00 or later	
	SQL Server 2012	11.13 or later	
Tuxedo monitor	Tuxedo 10g R3	11.00 or later	
	Tuxedo 11g R1	11.10 or later	
OracleAS monitor	Oracle Application Server 10g Release 3 (10.1.3)	11.00 or later	
	Oracle Application Server 10g Release 3 (10.1.4)	11.00 or later	
Weblogic monitor	WebLogic Server 10g R3	11.00 or later	
	WebLogic Server 11g R1	11.00 or later	
	WebLogic Server 11g R2	11.00 or later	
	WebLogic Server 12c	11.13 or later	
Websphere monitor	WebSphere 6.1	11.00 or later	
	WebSphere 7.0	11.00 or later	
	WebSphere 8.0	11.15 or later	
WebOTX monitor	WebOTX V8.0	11.00 or later	
	WebOTX V8.1	11.00 or later	
	WebOTX V8.2	11.00 or later	

	WebOTX V8.3	11.03	
	WebOTX V8.4	11.10	
OfficeScan CL monitor	OfficeScan Corporate Edition 10.5	11.00 to 11.04	
OfficeScan SV monitor			
JVM monitor	WebLogic Server 11g R1	11.10 or later	
	WebLogic Server 12c	11.13 or later	
	WebOTX V8.2	11.10 or later	
	WebOTX V8.3	11.10 or later	
	WebOTX V8.4	11.10 or later	
	WebOTX Enterprise Service Bus V8.4	11.13 or later	
	WebOTX Enterprise Service Bus V8.5	11.15 or later	
	Apache Tomcat 6.0	11.13 or later	
	Apache Tomcat 7.0	11.13 or later	
	WebSAM SVF for PDF 9.0	11.13 or later	
	WebSAM SVF for PDF 9.1	11.14 or later	
	WebSAM Report Director Enterprise 9.0	11.13 or later	
	WebSAM Report Director Enterprise 9.1	11.15 or later	
	WebSAM Universal Connect/X 9.0	11.13 or later	
	WebSAM Universal Connect/X 9.1	11.15 or later	
System monitor	N/A	11.10 or later	



x86\_64 version

Monitor resource	Application to be monitored	ExpressCluster Version	Remarks
Oracle monitor	Oracle 10g Release 2 (10.2)	11.00 or later	
	Oracle 11g Release 1 (11.1)	11.00 or later	
	Oracle 11g Release 2 (11.2)	11.00 or later	
DB2 monitor	DB2 V9.5	11.00 or later	
	DB2 V9.7	11.00 or later	
	DB2 V10.1	11.13 or later	
PostgreSQL monitor	PostgreSQL 9.0	11.03 or later	
	PostgreSQL 9.1	11.13 or later	
	PostgreSQL 9.2	11.17 or later	
	PowerGres on Windows V9.0	11.03 or later	
SQL Server monitor	SQL Server 2005	11.00 or later	
	SQL Server 2008	11.00 or later	
	SQL Server 2008 R2	11.00 or later	
	SQL Server 2012	11.13 or later	
Tuxedo monitor	Tuxedo 11g R1	11.10 or later	
Weblogic monitor	WebLogic Server 10g R3	11.00 or later	
	WebLogic Server 11g R1	11.00 or later	
	WebLogic Server 11g R2	11.00 or later	
	WebLogic Server 12c	11.13 or later	

Websphere monitor	WebSphere 6.1	11.00 or later	
	WebSphere 7.0	11.00 or later	
	WebSphere 8.0	11.15 or later	
WebOTX monitor	WebOTX V8.0	11.00 or later	
	WebOTX V8.1	11.00 or later	
	WebOTX V8.2	11.00 or later	
	WebOTX V8.3	11.03 or later	
	WebOTX V8.4	11.10 or later	
OfficeScan CL monitor	OfficeScan Corporate Edition 10.5	11.00 to 11.04	
OfficeScan SV monitor			
JVM monitor	WebLogic Server 11g R1	11.10 or later	
	WebLogic Server 12c	11.13 or later	
	WebOTX V8.2	11.10 or later	
	WebOTX V8.3	11.10 or later	
	WebOTX V8.4	11.10 or later	
	WebOTX Enterprise Service Bus V8.4	11.13 or later	
	WebOTX Enterprise Service Bus V8.5	11.15 or later	
	Apache Tomcat 6.0	11.13 or later	
	Apache Tomcat 7.0	11.13 or later	
	WebSAM SVF for PDF 9.0	11.13 or later	
	WebSAM SVF for PDF 9.1	11.14 or later	

	WebSAM Report Director Enterprise 9.0	11.13 or later	
	WebSAM Report Director Enterprise 9.1	11.15 or later	
	WebSAM Universal Connect/X 9.0	11.13 or later	
	WebSAM Universal Connect/X 9.1	11.15 or later	
System monitor	N/A	11.10 or later	

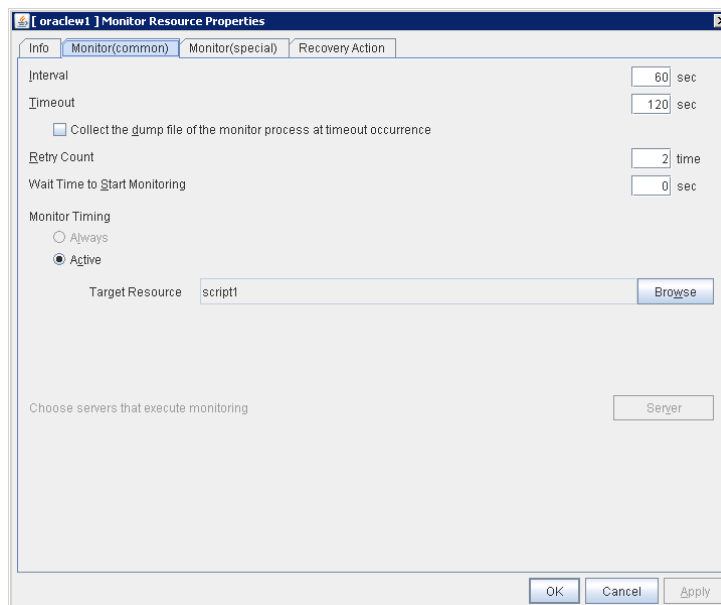
## Common settings for monitor resources

The configuration window for each group resource has the **Tuning** button. The items that are specified using this button are common.

This section describes common parameters of monitor resource in Monitor(common) tab.

### 1. Setting up the monitor processing

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 name of the monitor resource whose settings you want to change. Click **Properties**, and then click the **Monitor(common)** tab.
3. On the **Monitor(common)** 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)

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 (for Oracle monitor resource only)**

Specify whether collecting the dump file of the ExpressCluster monitoring process when time out occurs. This item is not displayed with the monitor resource which has no dump collecting function.

The collected dump file is saved in work\rm\resource name\errinfo.cur folder under

ExpressCluster install folder. When collection is executed more than once, the folder names of the past collection information are renamed as errinfo.1, errinfo.2. And the folders are saved by 5 generations from the latest information.

**Retry Count (0 to 999)**

Specify how many times an error should be detected in a row after the first one is detected before the status is determined as error.

If you set this to zero (0), the status is determined as error at the first detection of an error.

**Wait Time to Start Monitoring (0 to 9999)**

Set the wait time to start monitoring.

**Monitor Timing:**

Set the monitoring timing.

- **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 while activated is shown.

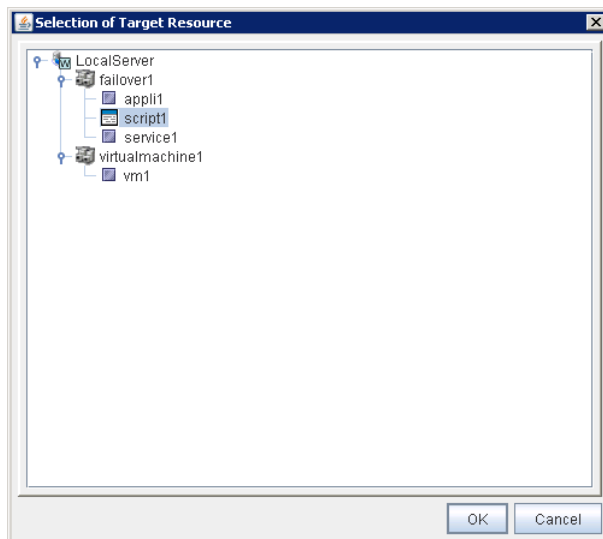
**Browse**

Click this button to open the dialog box to select the target resource. Server names and resource names are displayed in a tree. Select the target resource, and then click **OK**.

**Choose servers that execute monitoring**

Not used.

Clicking **Browse** for **Monitor Timing** displays a window for selecting the monitor target.

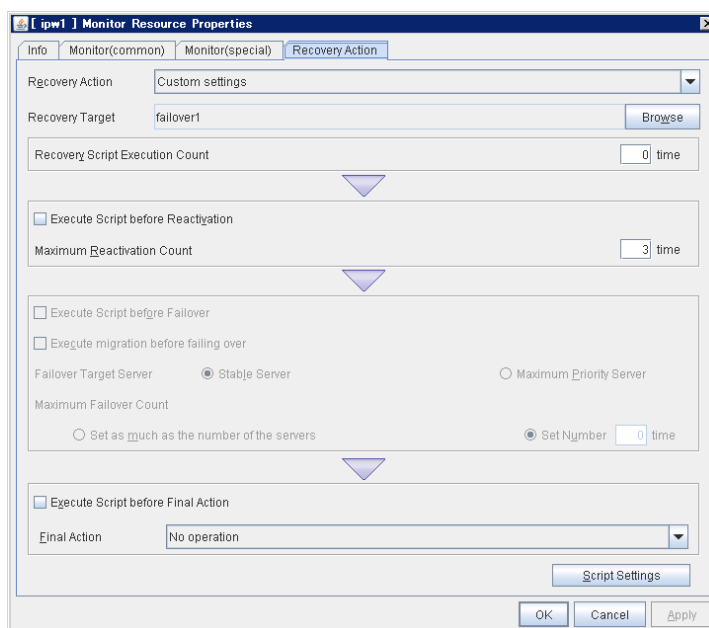


Select the resource to be monitored, and then click **OK**.

## 2. Setting up the recovery processing

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 name of the monitor resource whose settings you want to change. Click **Properties**, and then click the **Recovery Action** tab.
3. On the **Recovery Action** tab, you can see and/or change the settings of monitor resource by following the description below.

### Ordinary monitor resource (except Message Receive Monitor resource)



## Message Receive Monitor

The screenshot shows the 'mrw1 | Monitor Resource Properties' dialog box with the 'Recovery Action' tab selected. The 'Recovery Action' dropdown is set to 'Execute the final action'. The 'Recovery Target' text box contains 'failover1' and has a 'Browse' button to its right. Below these are three checkboxes: 'Execute migration before failing over' (unchecked), 'Execute Failover to outside the Server Group' (unchecked), and 'Execute Script before Recovery Action' (unchecked). There are two radio buttons: 'Stable Server' (selected) and 'Maximum Priority Server' (unselected). Below the radio buttons is a 'Final Action' dropdown set to 'No operation'. At the bottom right is a 'Script Settings' button. The bottom of the dialog has 'OK', 'Cancel', and 'Apply' buttons.

In this dialog box, you can configure the recovery target and an action to be taken at the time when an error is detected. By setting this, it allows failover of the group, restart of the resource or the group 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.

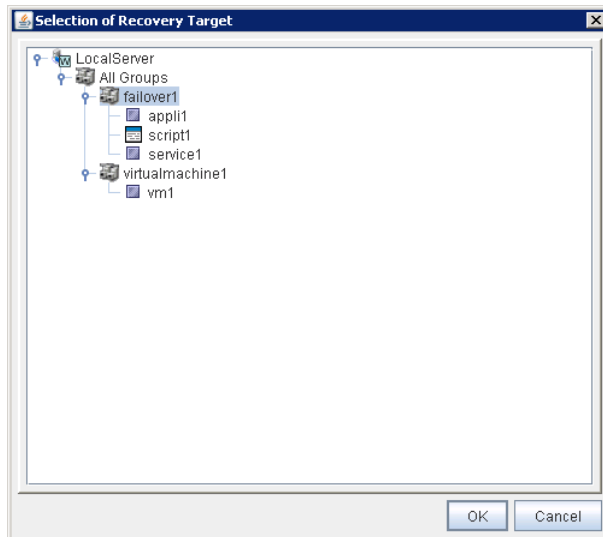
- **Restart the recovery target**  
The group or group resource selected as the recovery target is reactivated. If reactivation fails, or if the same error is detected after reactivation, the action selected for **Final Action** is performed.
- **Execute Only Final Action**  
The action selected for **Final Action** is performed.
- **Custom**  
The group or group resource selected as the recovery target is reactivated repeatedly until the maximum reactivation count is reached. If the maximum reactivation count is reached while reactivation continues to fail or the same error continues to be detected after reactivation, the action selected for **Final Action** is performed.

### Recovery Target

This field displays the object of the target to be recovered upon detection of an error.

**Browse**

Click this button to open the dialog box in which you can select the target resource. LocalServer, All Groups, and the group names and resource names that are registered in the cluster are shown in a tree view. Select the target resource and click **OK**.

**Recovery Script Execution Count (0 to 99)**

Specify the number of times to allow execution of the script configured by **Script Settings** when an error is detected. If this is set to zero (0), the script does not run.

**Execute Script before Reactivation**

Specify whether to run the script before reactivation.

**Maximum Reactivation Count (0 to 99)**

When **Custom** is selected for **Recovery Action**, specify the maximum number of times the recovery target is to be reactivated. If this is set to zero (0), no reactivation is executed. For Message Receive Monitor resource, this parameter can not be set.

**Execute Script before Failover**

Not used.

**Execute migration before failing over**

Not used.

**Failover Target Server:**

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 **Settings**.
- When cleared  
Any script/command is not run.



### Execute Script before Recovery Action

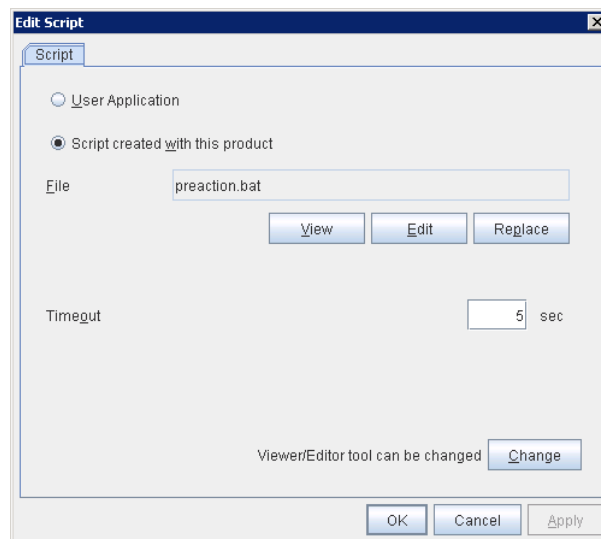
Select whether script is run or not before executing recovery action.

This can be set only for a message receive monitor resource.

- When selected  
A script/command is run before executing recovery action. To configure the script/command setting, click **Script Settings**.
- When cleared  
Any script/command is not run.

### Script Settings

Click here to display the **Edit Script** dialog box. Set the recovery script/command.



### User Application

Use an executable file (executable batch file or execution file) on the server as a script. For the file name, specify an absolute path or name of the executable file of the local disk on the server. If you specify only the name of the executable file, you must configure the path with environment variable in advance. If there is any blank in the absolute path or the file name, put them in double quotation marks (“”) as follows.

Example:

“C:\Program Files\script.bat”

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

Example:

cscript script.vbs

Each executable file is not included in the cluster configuration information of the Builder. They must be prepared on each server since 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 cluster configuration information.

**File** (Within 1023 bytes)

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

**View**

Click here to display the script file 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**

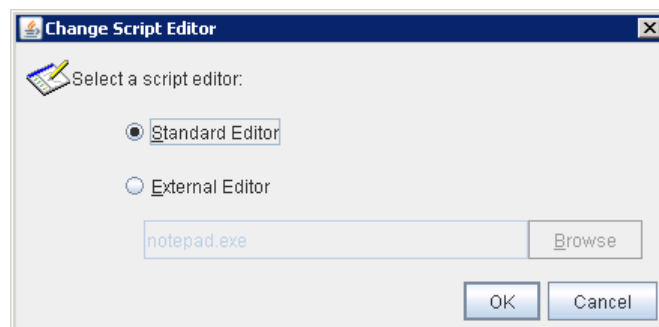
Click here to replace the contents of a script file with the contents of the script file which you selected in the file selection dialog box when you select **Script created with this product**. You cannot replace the script file if it is currently displayed or edited. Select a script file only. Do not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

**Timeout** (1 to 9999)

Specify the maximum time to wait for completion of script to be executed. The default value is set as 5.

**Change**

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

**Standard Editor**

Select here to use a standard editor (Notepad (notepad.exe)) as a script editor.

**External Editor**

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

**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:**

Use **No Operation** to:

- Suppress the final action temporarily
  - Show only alerts on detection of an error
  - Take the final action practically with multi-target monitor resources
-

- ◆ **Stop Group**

When a group or group resource is selected as a monitor target, this option stops the group or the group that the group resource belongs. When **All Groups** is selected, all the groups running on the server of which a monitor resource has detected an error are stopped. This is disabled when a LocalServer is selected as a monitor target.

- ◆ **Stop cluster service**

ExpressCluster X SingleServerSafe is stopped.

- ◆ **Stop cluster service and shutdown 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.

- ◆ **Generating of intentional Stop Error**

A stop error is intentionally generated for the server.

## Displaying and changing parameters of a monitor resource

Some monitor resources require parameter setting for monitoring. For displaying and changing parameters, please refer to explanations of each monitor resource that described on following pages.

## Setting up application monitor resources

Application monitor resources monitor application resources. Monitoring starts when the application resource is activated. The application resource can be monitored if it is specified as a Resident type resource.

### Monitoring by application monitor resources

They regularly monitor whether applications are active or not. When they detect that applications do not exist, it is determined to be an error.

### Note on application monitor resources

An application monitor resource monitors a successfully activated application resource. The application resource can be monitored if it is specified as a resident type resource.

Application monitor resources are automatically registered when the resident type is set to **Resident** on addition of an application resource. Application monitor resources corresponding to an application resource are automatically registered.

Application monitor resources are initially defaulted, so configure appropriate resource settings as needed.

On addition of an application resource whose resident type is **Non-Resident**, application monitor resources cannot be added to it.

## Setting up service monitor resources

Service monitor resources monitor service resources. Monitoring starts when the service resource is activated.

### Monitoring by service monitor resources

They regularly check the service status with the service control manager and if the status of the service resource becomes Stopped, it is considered as an error.

### Note on service monitor resources

This monitor resource is automatically registered when a service resource is added. A service monitor resource corresponding to a service resource is automatically registered. Service monitor resources are initially defaulted, so configure appropriate resource settings as needed.

## Setting up disk RW monitor resources

Disk RW monitor resources monitor disk devices by writing dummy data to the file system.

Disk RW monitor resources are registered by default.

### Monitoring by disk RW monitor resources

Disk RW monitor resources write data to the specified file system (basic volume or dynamic volume) with the specified I/O size and evaluate the result.

They solely evaluate whether data was written with the specified I/O size but do not evaluate validity of data. (Created file is deleted after writing)

OS and disk get highly loaded if the size of I/O is large.

Depending on the shared disk and interfaces in your environment, various caches for reading may be implemented. Because of this, if the size of I/O is small, a cache hit may occur and an error in writing may not get detected.

Intentionally generate a disk error to confirm that the size of I/O is sufficient to detect an error.

---

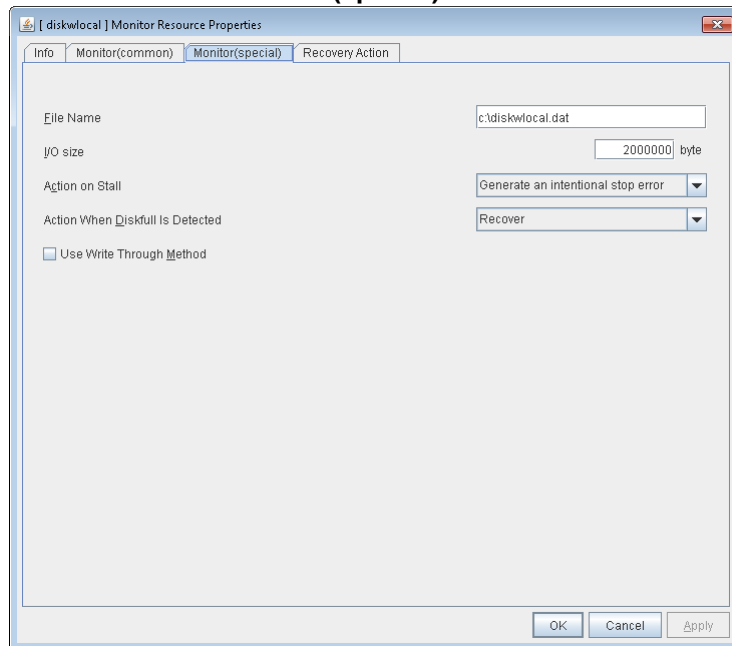
**Note:**

If you want multipath software to initiate a path failover when a disk path is not connected, specify a longer monitoring timeout time (for which the default value is 300 seconds) for the disk RW monitor resource than the path failover time.

---

### Displaying and changing disk RW monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target disk RW monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

**Monitor resource Monitor(special) tab****File Name** (within 1023 bytes)

Enter the file name to access. This file is created upon monitoring and deleted after I/O completes.

**Note:**

Specify an absolute path for the file name. If a relative path is specified for the file name, the disk RW monitor resource may monitor the unexpected place.

**Important:**

Do not specify any existing file for the file name. If an existing file is specified for the file name, the data of the file is lost.

**I/O size** (1 to 9999999; default: 2000000)

Specify the I/O size for the disk to monitor.

### Action on Stall

Specify the action to take when stalling is detected.

- ◆ **No Operation**

No action is taken.

- ◆ **HW Reset**

Reset the hardware.

- ◆ **Generate an intentional stop error** (default)

Intentionally cause a stop error.

### Action When Diskfull Is Detected

Select the action when diskfull (state in which the disk being monitored has no free space) is detected

- Recover  
The disk monitor resource recognizes an error upon the detection of disk full.
- Do not recover  
The disk monitor resource recognizes a caution upon the detection of disk full.

### Use Write Through Method

Applies the Write Through method to the monitor I/O method.

- If the Write Through method is enabled, the error detection precision of the disk RW monitor will improve. However, the I/O load on the system may increase.



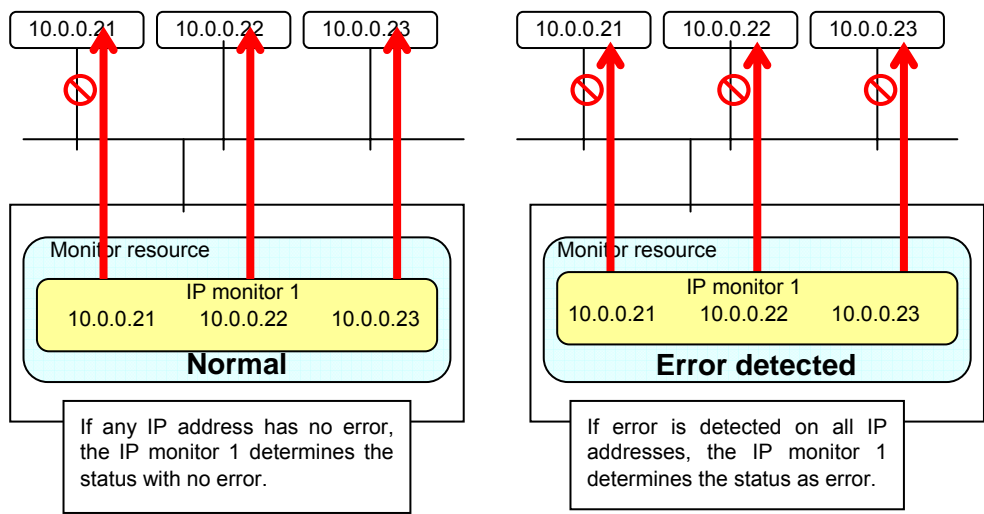
# Setting up IP monitor resources

IP monitor resource is a monitor resource which monitors IP addresses by using the ping command depending on whether there is a response or not.

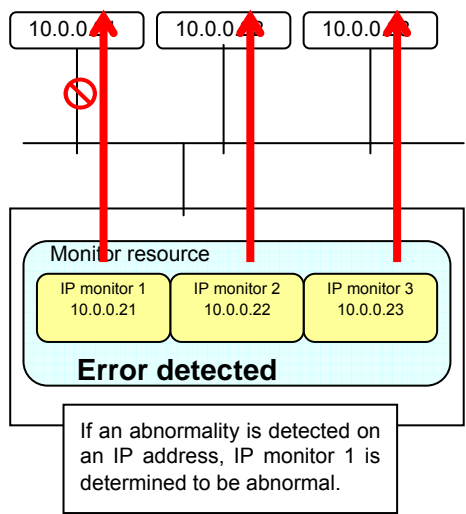
## Monitoring by IP monitor resources

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.

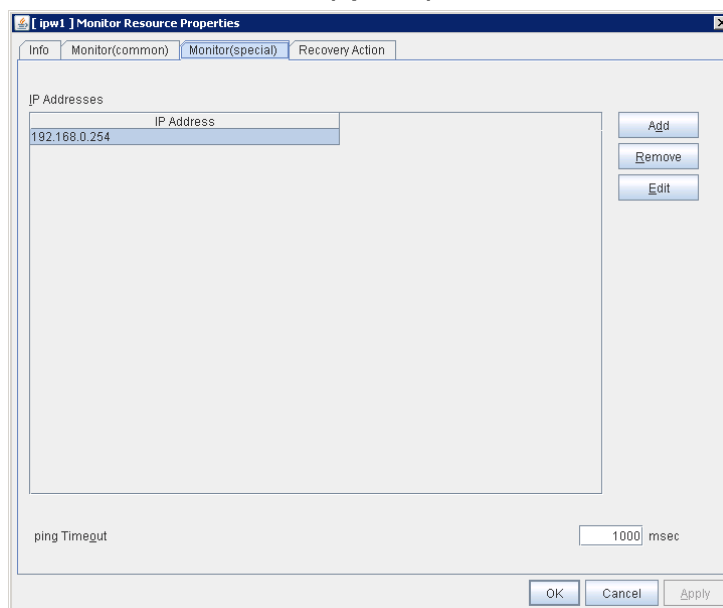


## Displaying and changing IP monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target IP monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

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

### Monitor resource Monitor(special) tab



#### Add

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

#### 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 then click **OK**.

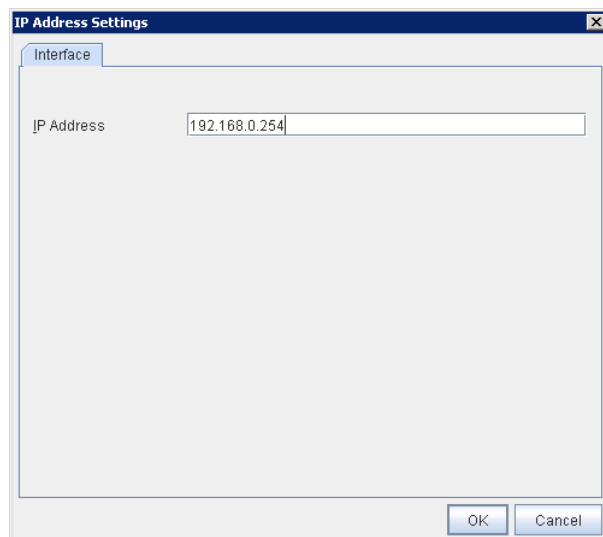
#### Ping Timeout (1 to 999,999; default: 1,000)

Specify the timeout of the ping to be sent to monitor the IP address in milliseconds.

## IP Address Settings

### Interface tab

The detailed setting for interface is displayed.



### IP Address (within 255 bytes)

Enter an IP address to be monitored in this field, and then click **OK**. Enter an IP address that is always available for communication.

## Setting up NIC link up/down monitor resources

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

### Note on NIC link up/down monitor resources

- ◆ In some NIC drivers, required DeviceIoControl function may not be supported. You cannot use this monitor resource in such a case.

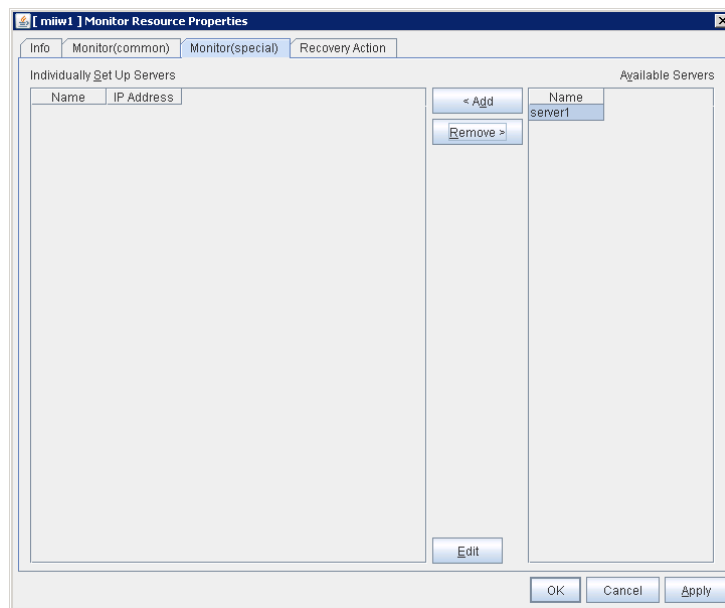
### Configuration and range of NIC link up/down monitoring

- ◆ The DeviceIoControl function 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.)
- ◆ When you are monitoring any NIC directly connected to another server by using a cross cable, an error is detected if the other server goes down (because a link cannot be established).  
The recovery action to be taken at detection of error should be configured with the appropriate value.  
For example, if you select **Stop cluster service and reboot OS**, the OS will be restarted an endless number of times.

### Displaying and changing the NIC link up/down monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target NIC Link Up/Down monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

NIC Link UP/Down monitor resource acquires the status of the specified NIC Link and monitors the status of being up and down of the Link.

**Monitor resource Monitor(special) tab****Add**

Add the server to be monitored to the list of monitoring servers. Click **Edit** to display the **IP Address Settings** dialog box.

**Remove**

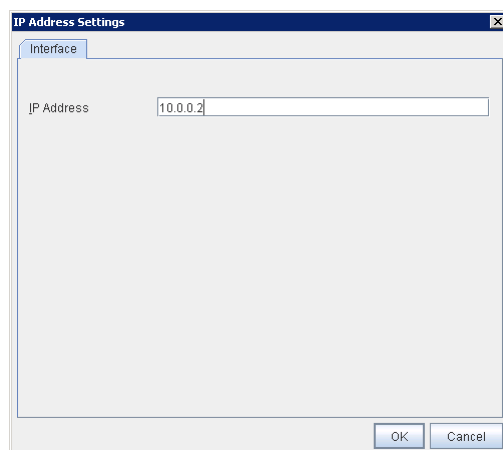
Delete the server to be monitored from the list of monitoring servers.

**Edit**

Edit the IP address of the NIC of the server to be monitored.

**IP Address Settings****Interface tab**

The detailed setting for interface is displayed.

**IP Address (within 47 bytes)**

Specify the IP address of the NIC to be monitored.

## Setting up custom monitor resources

Custom monitor resources monitor system by executing an arbitrary script.

### 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.

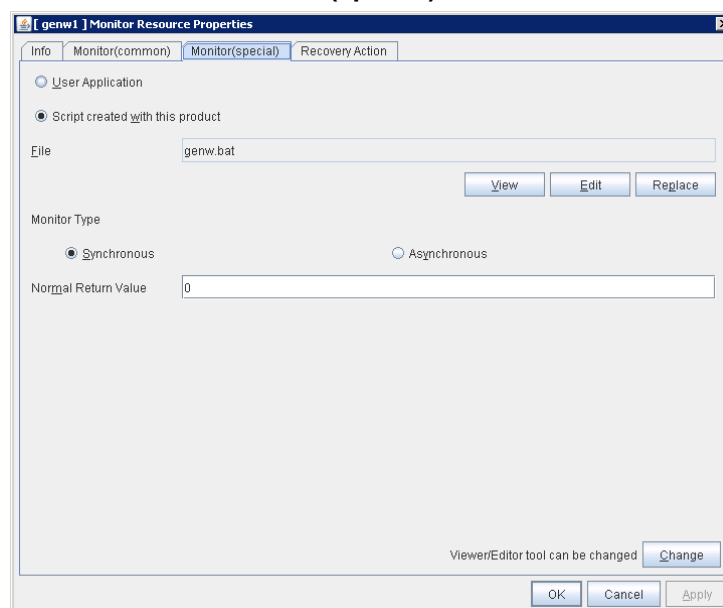
### Note on custom monitor resources

When **Asynchronous** is selected as the monitor type and a monitor error occurs due to the disappearance of the process to be monitored, the script is not re-executed while monitoring continues.

## Displaying and changing the details of the custom monitoring resources

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

### Monitor resource Monitor(special) tab



### User Application

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

These executable files are not included in the configuration data of the Builder. They must be prepared on the server since 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 1023 bytes)

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

#### View

Click here to display the script file 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

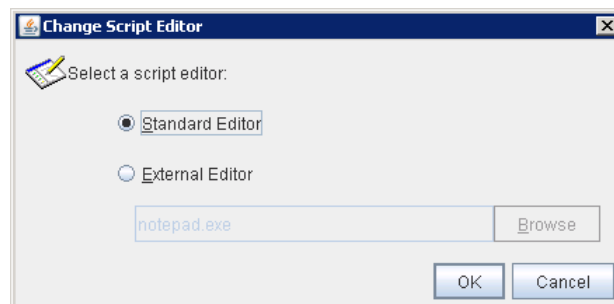
Click here to edit the script file with the editor when you select **Script created with this product**. Overwrite the script file to apply the change. If the selected script file is being viewed or edited, you cannot edit it. You cannot modify the name of the script file.

#### 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. You can change editor for displaying or editing a script to an arbitrary editor.



#### Standard Editor

Select here to use a standard editor (Notepad in Windows) as a script editor.

#### External Editor

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

#### Monitor Type

Select a monitor type.

##### ◆ Synchronous (default)

Custom monitor resources regularly run a script and detect errors from its error code.

##### ◆ Asynchronous

Custom monitor resources run a script upon start monitoring and detect errors if the script process disappears.

**Normal Return Value** (within 1023 bytes)

When **Asynchronous** is selected for **Monitor Type**, set the values of script error code to be determined as normal. If you want to set two or more values here, separate them by commas like 0,2,3 or connect them with a hyphen to specify the range like 0-3.

Default value: 0



## Setting up multi target monitor resources

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

### Note on the multi target monitor resource

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

### Status of the multi target monitor resource

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)	Offline (offline)
Monitor resource2 status:	Normal (normal)	Normal (normal)	Caution (caution)	Caution (caution)
	Error (error)	Caution (caution)	Error (error)	Error (error)
	Offline (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.

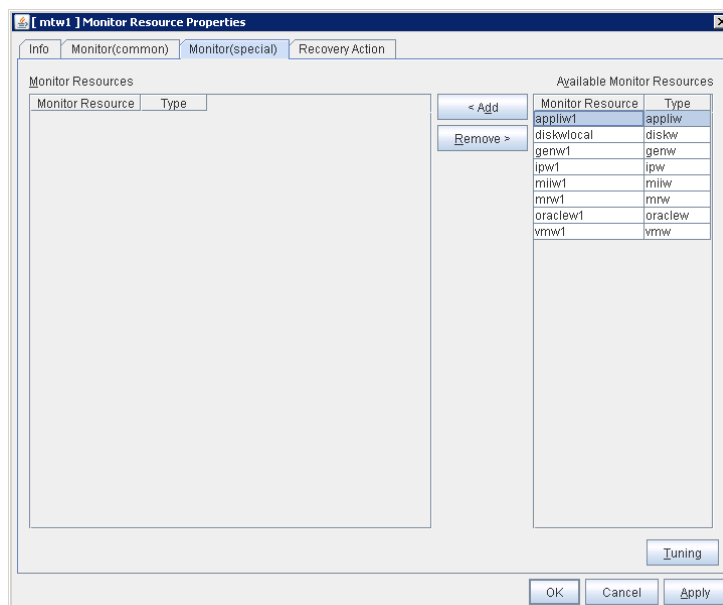
## Displaying and changing the details of the multi target monitor resource

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target multi target monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

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.

### Monitor resource Monitor(special) tab



#### Add

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

#### Remove

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

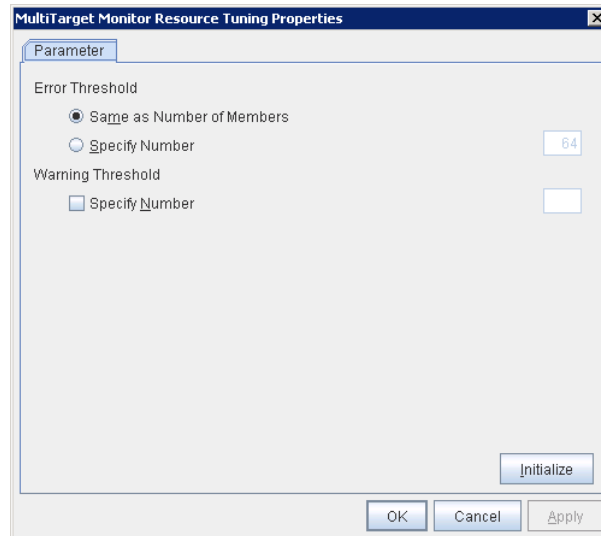
#### Tuning

Use this button to display the **MultiTarget Monitor Resource Tuning Properties** dialog box. You can make advanced settings for the multi target monitor resource.

## MultiTarget Monitor Resource Tuning Properties

### Parameter tab

The detailed setting for parameters is displayed.



### 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.

## Setting up message receive monitor resources

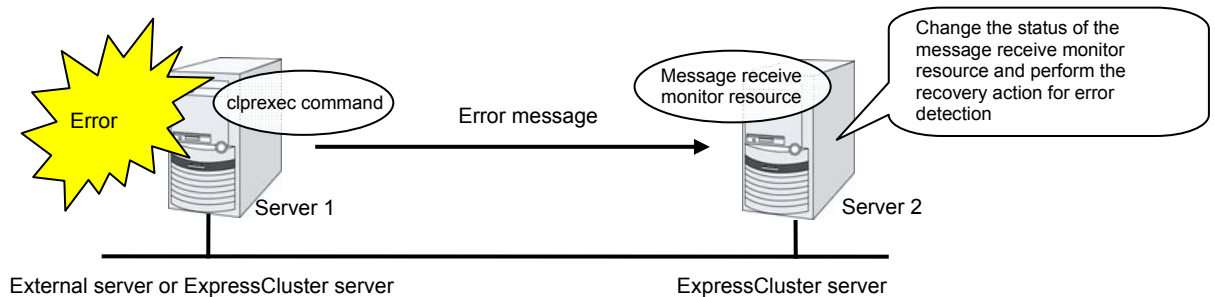
Message receive monitor resources are passive monitors. They do not perform monitoring by themselves.

When an error message issued using the `clprexec` command is received from an outside source, the message receive monitor resources change their status and perform recovery from the error.

### Monitoring by message receive monitor resources

When an error message is received from an outside source, the resource recovers the message receive monitor resource whose monitor type and monitor target have been reported. (The monitor target 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.

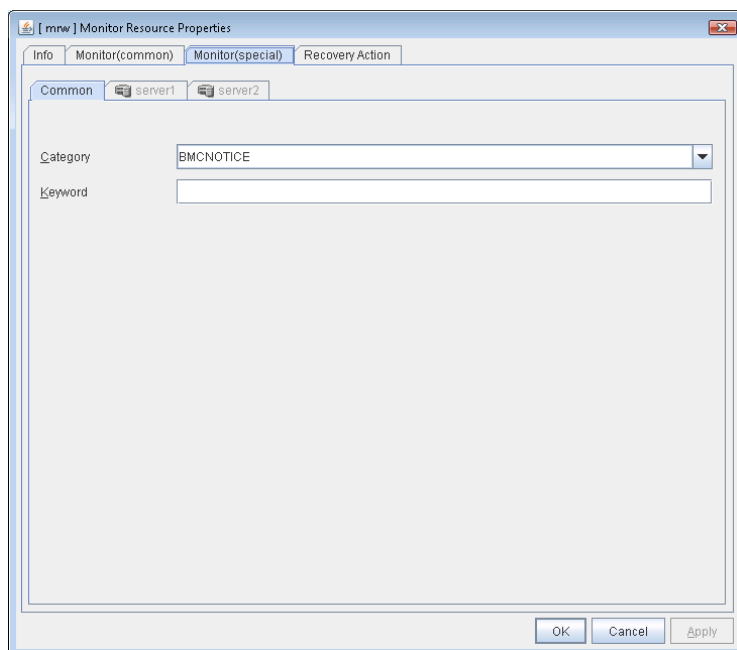


### Notes on message receive monitor resources

- ◆ If a message receive monitor resource is paused when an error message is received from outside, error correction is not performed.
- ◆ If an error message is received from outside, the status of the message receive monitor resource becomes "error". The error status of the message receive monitor resource is not automatically restored to "normal". To restore the status to normal, use the `clprexec` command. For details about 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.

### Displaying and changing the details of the Message receive monitor resources

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target Message receive monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

**Monitor resource Monitor(special) tab**

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

**Category** (within 32 bytes)

Specify the category specified with -k argument of clprexec command. You can specify any character string.

**Keyword** (within 1,023 bytes)

Specify the keyword specified with -k argument of clprexec command.

## Setting up VM monitor resources

A VM monitor resource monitors the startup status of a virtual machine managed by a VM resource.

No setting needs to be specified specifically for VM monitor resources.

### Notes on VM monitor resources

- ◆ For the version of the supported virtualization platform, see "System requirements for VM resource" in Chapter 4 , "Group resource details".

### Monitoring by VM monitor resources

A VM monitor resource performs monitoring in the manner below, according to the virtualization platform.

Hyper-V

VM monitor resources monitor the startup status of a virtual machine by using a WMI interface.

An error is detected if the virtual machine is stopped or otherwise affected by any resource other than a VM resource.

## Setting up process name monitor resources

Process name monitor resources monitor the process of arbitrary process name.

### Notes on process name monitor resources

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

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

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

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

If the name of the target process is 1024 bytes or longer, only the first 1023 bytes will be recognized as the process name. When specifying a process name by using a wild card (such as \*), specify a character string that appears in the first 1023 bytes of the process name.

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

Use the following command to check the name of a process that is actually running and specify the name for the monitor target process name.

ExpressCluster installation path\bin\GetProcess.vbs

When the above command is executed, GetProcess\_Result.txt is output to the folder in which the command is executed. Open GetProcess\_Result.txt and specify the CommandLine section of the process being displayed. If the output information includes double quotations (""), specify the section including the double quotations.

Example of output file

```
2012/07/26 12:03:13
Caption  CommandLine
services.exe      C:¥WINDOWS¥system32¥services.exe
svchost.exe       C:¥WINDOWS¥system32¥svchost -k rpcss
explorer.exe      C:¥WINDOWS¥Explorer.EXE
```

To monitor svchost.exe shown in the above command output information, specify C:\WINDOWS\system32\svchost -k rpcss as the monitor target process name.



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

## Monitoring by process name monitor resources

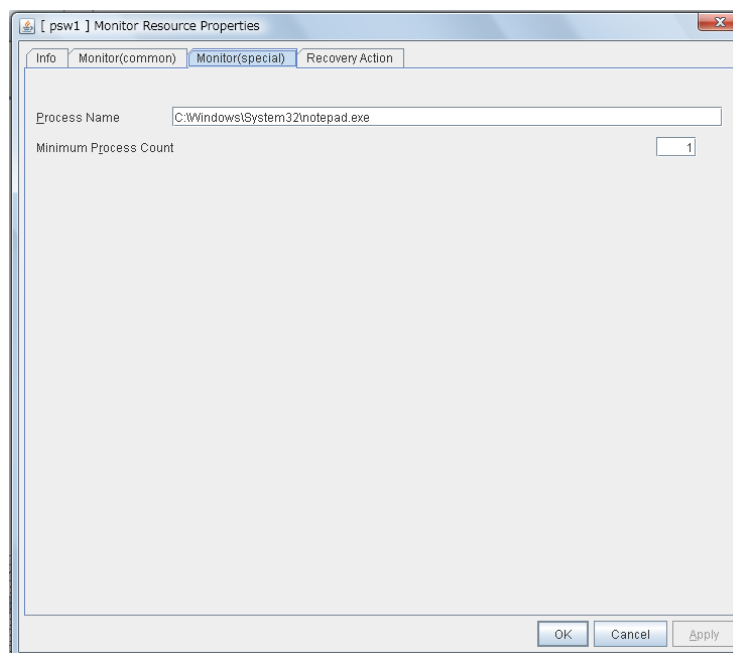
Those processes having the specified process name are monitored. If Minimum Process Count is set to 1, the process ID is determined by the process name, and the error state is determined if the process ID vanishes. Process stalls cannot be detected.

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

## Displaying and changing the process name monitor resource details

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 detailed settings by following the description below.

### Monitor resource Monitor(special) tab



### Process Name

Specify the name of the process to be monitored. You must specify the process name.

Default value: None

Wild cards can be used to specify process names in the three patterns described below. Patterns other than these cannot be used.

prefix search : <character string included in process name>\*

suffix search : \*<character string included in process name>

partial search : \*<character string included in process name>\*

### **Minimum Process Count (1 to 999)**

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

## Setting up DB2 monitor resources

DB2 monitor resources monitor DB2 database that runs on the server.

### Notes on DB2 monitor resources

For the supported version of DB2, see "Applications supported by monitoring options" in Chapter 5, "Monitor resource details."

DLL interface (DB2CLI.DLL/DB2CLI64.DLL) needs to be installed on servers where monitoring is performed because DB2 CLI is used for monitoring.

For target monitoring resources, specify a service resource or a script resource that starts DB2. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

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.

A monitor table is created when monitoring starts. When monitoring is stopped due to the group stopping, the monitor table is deleted. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. Note that, if the server is shut down due to a system failure or other cause before the group is stopped, the monitor table is not deleted. In this case, an alert message saying that "a monitor table exists" might be displayed next time monitoring is started. This is not an error.

DB2 may output operation logs for each monitoring. Configure DB2 settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection "Monitoring by DB2 monitor resources", when "Level 1" is selected, ExpressCluster does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

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

Create a monitor table using either of the following methods:

**(In the following example, the monitor table is named DB2WATCH)**

```
sql> create table DB2WATCH (num int not null primary key);
sql> insert into DB2WATCH values(0);
sql> commit;
```

## Monitoring by DB2 monitor resources

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

- ◆ Level 1 (monitoring by select)

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

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement

- ◆ Level 2 (monitoring by update/select)

Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement
- (3) The written data is not the same as the read data

## Displaying and changing the disk DB2 monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target DB2 monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### Monitor Level

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

- ◆ Level 1 (monitoring by select)  
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
- ◆ Level 2 (monitoring by update/select)  
Monitoring with reference to and update of the monitoring table. SQL statements issued to the monitor table are of (create / update / select / drop) type.

Default value: Level 2 (monitoring by update/select)

#### Database Name (within 255 bytes)

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

Default value: None

**Instance Name** (within 255bytes)

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

Default value: DB2

**User Name** (within 255 bytes)

Specify the user name to log on to the database.

Default value: db2admin

**Password** (within 255 bytes)

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

Default value: None

**Monitor Table Name** (within 255 bytes)

Specify the name of a monitor table created on the database. 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.

Default value: DB2WATCH

## Setting up FTP monitor resources

FTP monitor resources monitor FTP services that run on the server. FTP monitor resources monitor FTP protocol and they are not intended for monitoring specific applications. FTP monitor resources monitor various applications that use FTP protocol.

### Notes on FTP monitor resources

For monitoring target resources, specify service resources or script resources that start FTP monitor resources. Monitoring starts after target resource is activated. However, if FTP monitor resources cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

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

FTP service may output 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.

## Displaying and changing the FTP monitor resource details

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

### Monitor resource Monitor(special) tab

#### IP Address (within 255 bytes)

Specify the IP address of the FTP server to be monitored. Specifying this item cannot be omitted. Usually, specify the loopback address (127.0.0.1) to connect to the FTP server that runs on the local server. If the addresses for which connection is possible are limited by FTP server settings, specify an address for which connection is possible. 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 65535)

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. Click **Change** and enter the password in the dialog box.

Default value: None

## Setting up HTTP monitor resources

HTTP monitor resources monitor HTTP services that run on the server. HTTP monitor resources monitor HTTP protocol but they are not intended for monitoring specific applications. HTTP monitor resources monitor various applications that implement HTTP protocol.

### Notes on HTTP monitor resources

For monitoring target resources, specify service resources or script resources that start HTTP services. Monitoring starts after a target resource is activated. However, if HTTP service cannot be started immediately after the target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

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 service may output operation logs for each monitoring operation. Configure HTTP settings if this needs to be adjusted.

HTTP monitor resources does not support the client authentication.

### Monitoring by HTTP monitor resources

HTTP monitor resources monitor the following:

HTTP monitor resources connect to the HTTP server and execute the command for acquiring HTTP header.

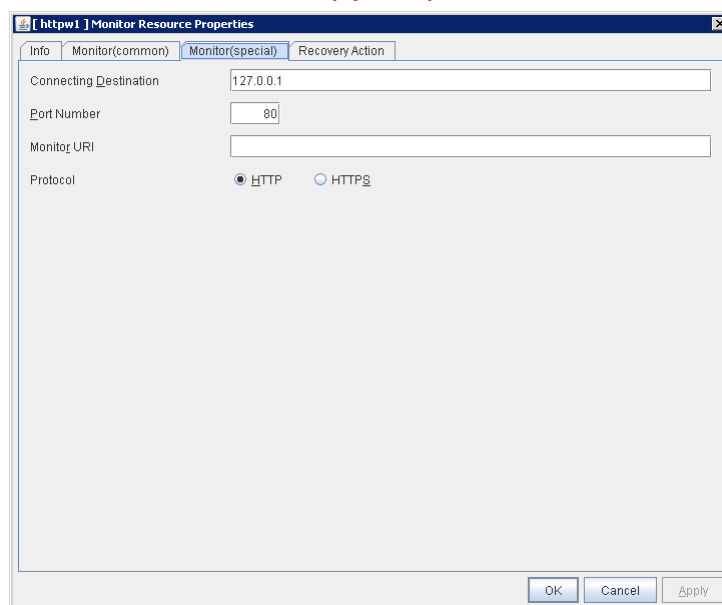
As a result of monitoring, the following is considered as an error:

- (1) When connection to the HTTP service fails.
- (2) When an error is notified as a response to the command.

## Displaying and changing the HTTP monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen.  
Right click the target HTTP monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab



#### Connecting Destination (within 255 bytes)

Specify the IP address of the HTTP server to be monitored. Be sure to specify the name. Usually, specify the loopback address (127.0.0.1) to connect to the HTTP server that runs on the local server. If the addresses for which connection is possible are limited by HTTP server settings, specify an address for which connection is possible. 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: 127.0.0.1

#### Port Number (1 to 65535)

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

Default value: 80 (HTTP)  
443 (HTTPS)

**Monitor URI** (within 255 bytes)

Specify the URI of the HTTP to be monitored.

If URI is not specified, the document root is monitored. It is not necessary to create a monitoring page.

If a URI is specified, that URI is monitored. The specified URI needs to allow anonymous access.

Write the following in URI form from the DocumentRoot.

(Example) When the URI of the web page to be monitored is as follows:

`http://WebServer:80/watch/sample.htm`

`/watch/sample.htm`

Default value: None

**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.

## 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.

### Notes on IMAP4 monitor resources

As the monitoring target resource, specify a service resource or script 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.

## Displaying and changing the IMAP4 monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target IMAP4 monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### IP Address (within 255 bytes)

Specify the IP address of the IMAP4 server to be monitored. Specifying this item cannot be omitted.

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

**Authentication Method**

Select the authentication method to log on to IMAP4. It must follow the settings of IMAP4 being used:

◆ **AUTHENTICATE LOGIN** (default value)

The encryption authentication method that uses the AUTHENTICATE LOGIN command.

◆ **LOGIN**

The plaintext method that uses the LOGIN command.

## Setting up ODBC monitor resources

ODBC monitor resources monitor ODBC database that runs on the server.

### Notes on ODBC monitor resources

Because the ODBC driver is used for monitoring, set up the data source in advance by using the ODBC data source administrator of Windows. Add the data source to the system data source.

For monitoring target resources, specify service resources or script resources that start the database. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

To monitor a 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 database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**.

A monitor table is created when monitoring starts. When monitoring is stopped due to the group stopping, the monitor table is deleted. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. Note that, if the server is shut down due to a system failure or other cause before the group is stopped, the monitor table will not be deleted. In this case, an alert message saying that "a monitor table exists" might be displayed next time monitoring is started. This is not an error.

ODBC database may output operation logs for each monitoring. Configure the database settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection "Monitoring by ODBC monitor resources", when "Level 1" is selected, ExpressCluster does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

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

Create a monitor table using either of the following methods:

**(In the following example, the monitor table is named ODBCWATCH)**

```
sql> create table ODBCWATCH (num int not null primary key);
sql> insert into ODBCWATCH values(0);
sql> commit;
```



## Monitoring by ODBC monitor resources

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

- ◆ Level 1 (monitoring by select)

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

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement

- ◆ Level 2 (monitoring by update/select)

Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.

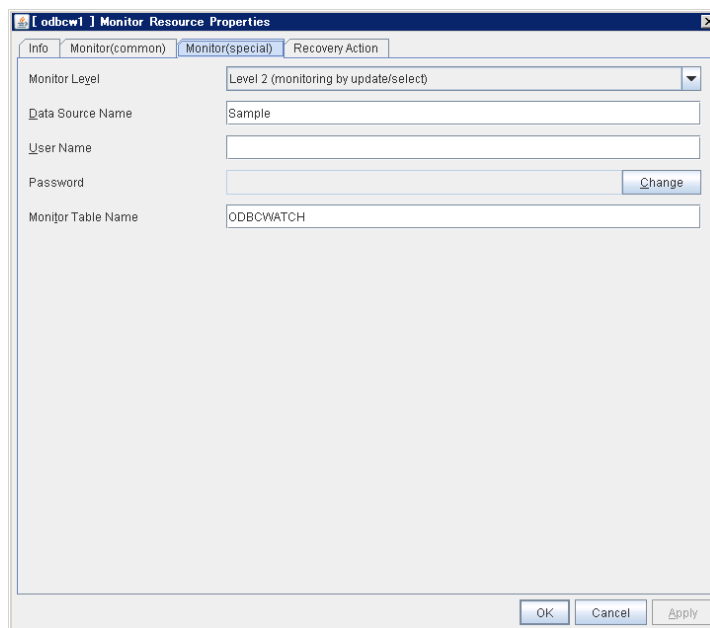
An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement
- (3) The written data is not the same as the read data

## Displaying and changing the ODBC monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target ODBC monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab



#### Monitor Level

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

- ◆ Level 1 (monitoring by select)  
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
- ◆ Level 2 (monitoring by update/select)  
Monitoring with reference to and update of the monitoring table. SQL statements issued to the monitor table are of (create / update / select / drop) type.

Default value: Level 2 (monitoring by update/select)

#### Data Source Name (within 255 bytes)

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

Default value: None

#### User Name (within 255 bytes)

Specify the user name to log on to the database. You do not have to specify if the user name is specified in the data source settings.

Default value: None

**Password** (within 255 bytes)

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

Default value: None

**Monitor Table Name** (within 255 bytes)

Specify the name of a monitor table created on the database. 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.

Default value: ODBCWATCH

## Setting up Oracle monitor resources

Oracle monitor resources monitor Oracle database that runs on the server.

### Notes on Oracle monitor resources

For the supported Oracle version, see "Applications supported by monitoring options" in Chapter 5, "Monitor resource details."

Interface DLL (OCI.DLL) needs to be installed on the server where monitoring is performed because Oracle OCI is used for monitoring.

For a target monitoring resource, specify a service resource or a script resource that can start Oracle. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

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 monitor table is created when monitoring starts. When monitoring is stopped due to the group stopping, the monitor table is deleted. When monitoring is temporarily stopped or when server fails before the group stops due to system error, the monitor table will not be deleted. Note that, if the server is shut down due to a system failure or other cause before the group is stopped, the monitor table will not be deleted. In this case, an alert message saying that "a monitor table exists" might be displayed next time monitoring is started. This is not an error.

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

- CREATE TABLE
- DROP ANY TABLE
- SELECT
- INSERT
- UPDATE
- SELECT permission to V\$PROCESS

Oracle database may output operation logs for each monitoring. Configure the Oracle settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection "Monitoring by Oracle monitor resources", when "Level 1" is selected, ExpressCluster does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

Selectable monitor level	Prior creation of a monitor table
Level 0 (database status)	Optional
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional

Create a monitor table using either of the following methods:

**(In the following example, the monitor table is named ORAWATCH)**

```
sql> create table ORAWATCH (num int primary key);
sql> insert into ORAWATCH values(0);
sql> commit;
```

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

## Monitoring by Oracle monitor resources

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

### ◆ Level 0 (database status)

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

An error is recognized if:

- (1) The DB (instance) status is in the inactive state (MOUNTED, STARTED)

### ◆ Level 1 (monitoring by select)

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

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement

### ◆ Level 2 (monitoring by update/select)

Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement
- (3) The written data is not the same as the read data

## Displaying and changing the Oracle monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target Oracle monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

The screenshot shows the 'Monitor Resource Properties' dialog box with the 'Monitor(special)' tab selected. The dialog contains the following fields and options:

- Monitor Type:** Listener and Instance Monitor (dropdown)
- Monitor Level:** Level 2 (monitoring by update/select) (dropdown)
- Connect String:** oraclew (text field)
- User Name:** sys (text field)
- Password:** (text field) with a 'Change' button
- Authentication:**
  - ☐ OS Authentication
  - ☒ SYSDBA
  - ☐ DEFAULT
- Monitor Table Name:** ORAWATCH (text field)
- ORACLE\_HOME:** (text field)
- Character Set:** (Following the setting of the application) (dropdown)
- ☐ Collect detailed application information at failure occurrence
- Collection Timeout:** 600 sec (text field)
- ☐ Set error during Oracle initialization or shutdown
- Buttons:** OK, Cancel, Apply

### Monitor Type

Select the Oracle features to be monitored.

#### ◆ Monitor Listener and Instance

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 direct (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 by the connect string is established, and any error in the connection operation is ignored. This is used to set the recovery action for a non-connection error together with an Oracle monitor resource for which **Monitor Listener only** is specified.

Default value: Monitor Listener and Instance

### Monitor Level

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

#### ◆ Level 0 (database status)

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

#### ◆ Level 1 (monitoring by select)

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

#### ◆ Level 2 (monitoring by update/select)

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

Default value: Level 2 (monitoring by update/select)

### Connect String (within 255 bytes)

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

When **Monitor Type** is set to **Monitor Instance only**, set ORACLE\_SID.

Monitor Type	ORACLE_HOME	Connect Command	Monitor Level
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. Be sure to specify this when a method other than **Monitor Listener only** is selected for **Monitor Method** or when OS authentication is used.

Default value: sys

**Password** (within 255 bytes)

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

Default value: None

**OS Authentication**

Specify the authentication method to log on to the Oracle monitor. It must follow the Oracle monitor settings.

- ◆ When selected:  
Use OS authentication.
- ◆ When cleared (default value):  
Use database authentication.

**Authority Method**

Select the user authority to log on to the Oracle monitor. This must be set according to the authority of the specified user name.

- ◆ SYSDBA (default value)  
Connect with SYSDBA authority.
- ◆ DEFAULT  
Connect with general user authority.

**Monitor Table Name** (within 255 bytes)

Specify the name of a monitor table created on the database. 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.

Default value: ORAWATCH

**ORACLE\_HOME** (within 255 bytes)

Specify the path name configured in ORACLE\_HOME. Begin with [/]. This is used when **Monitor Type** is set to **Monitor Listener only** or **Monitor Instance only**.

Default value: None



**Character Set**

Select the character set for Oracle. When the language for Oracle is not Japanese or English, select AMERICAN\_AMERICA.US7ASCII.

- ◆ (Following the setting of the application) (default)  
The Oracle character set installed in the server is used.
- ◆ AMERICAN\_AMERICA.US7ASCII  
Connect with general user authority.

**Collect detailed application information at failure occurrence**

Specify whether to collect detailed Oracle information if an Oracle database error is detected.

- ◆ When selected:  
Detailed Oracle information is collected.
- ◆ When cleared (default value):  
Detailed Oracle information is not collected.

To use this function, because the database processing for collecting information is performed using a local system account, the local system account requires DBA privileges. When using this function, the local system account needs DBA authorization because the database processing for information collection is executed by the local system account. The collected information is saved in work\rm\resource name\errinfo.cur folder under ExpressCluster install folder. When collection is executed more than once, the folder names of the past collection information are renamed as errinfo.1, errinfo.2. And the folders are saved by 5 generations from the latest information.

---

**Note:**

When the oracle service is stopped due to cluster stop or other reasons while collecting, the correct information may not be collected.

---

**Collection Timeout (1 to 9,999)**

Specify the timeout time for collecting detailed information in seconds.

Default value: 120

**Set error during Oracle initialization or shutdown**

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

Disable this function when Oracle automatically restarts in cooperation with Oracle Clusterware or the like during operation. Monitoring becomes normal even during Oracle initialization or shutdown.

However, a monitor error occurs if Oracle initialization or shutdown continues for one hour or more.

Default value: Disabled

## Setting up OracleAS monitor resources

OracleAS monitor resource monitors Oracle application server that operates on servers.

### Notes on OracleAS monitor resources

For the supported Oracle AS version, see "Applications supported by monitoring options" in Chapter 5 , "Monitor resource details."

For monitor target resources, specify service resources or script resources etc. that starts up OracleAS. After the target resource is activated, monitoring is started. When OracleAS cannot start running immediately after the target resource is activated, adjust the time in **Wait Time** to start monitoring.

If there is any component which does not start in OracleAS instance when monitor target resources are activated, edit opmn.xml file to change the status of the component to "disabled". For details on opmn.xml file, refer to OracleAS manual.

OracleAS may report operation log etc. for every monitoring operation, which should be controlled by the OracleAS settings.

### Monitoring by OracleAS monitor resources

OracleAS monitor resource monitors the following:

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

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.

## Displaying and changing the OracleAS monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target OracleAS monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### Instance Name (within 255bytes)

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

Default value: None

#### Installation Path (within 1,023 bytes)

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

Default value: *C:\product\10.1.3.2\companionCDHome\_1*

### Monitor Method

Select the OracleAS features to be monitored.

- ◆ opmn process and component monitor  
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 component specified in **Component List**.

### Component List (within 1,023 byte)

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**.

## Setting up OfficeScan CL monitor resources

OfficeScan CL monitor resource is a monitor resource that monitors OfficeScan Client operating on servers.

### Notes on OfficeScan CL monitor resources

For the supported virus buster versions, see "Applications supported by monitoring options" in Chapter 5 , "Monitor resource details".

If OfficeScan CL monitor detects issues, this monitor restarts OfficeScan NT Listener service as described below. Then, OfficeScan CL monitor may detect timeout error if it takes long time to restart the service. Please set sufficient timeout (default: 120 sec) for this monitor resource.

### Monitoring by OfficeScan CL monitor resources

OfficeScan CL monitor resource monitors the following issues.

- Monitors whether or not OfficeScan NT Listener service is active.
- Monitors the connection status between OfficeScan Client and Server.

If OfficeScan CL monitor detects errors about above issues, this monitor restarts OfficeScan NT Listener service to solve them. If it failed to solve errors, error message will be appeared on WebManager.

### Displaying and changing OfficeScan CL monitor resource details

There is no detail configuration in OfficeScan CL monitor resource.

## Setting up OfficeScan SV monitor resources

OfficeScan SV monitor resource is a monitor resource that monitors OfficeScan Server operating on servers.

### Notes on OfficeScan SV monitor resources

For the supported virus buster versions, see "Applications supported by monitoring options" in Chapter 5 , "Monitor resource details".

### Monitoring by OfficeScan SV monitor resources

OfficeScan SV monitor resource monitors following issues.

- Stall monitoring of virus checking pattern distribution function.

### Displaying and changing OfficeScan SV monitor resource details

There is no detail configuration in OfficeScan SV monitor resource.

## Setting up POP3 monitor resources

POP3 monitor resources monitor POP3 services that run on the server. POP3 monitor resources monitor POP3 protocol but they are not intended for monitoring specific applications. POP3 monitor resources monitor various applications that use POP3 protocol.

### Notes on POP3 monitor resources

For monitoring target resources, specify service resources or script resources that start POP3 services. Monitoring starts after target resource is activated. However, if POP3 services cannot be started immediately after target resource is activated, adjust the time using **Wait Time to Start Monitoring**.

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

### Monitoring by POP3 monitor resources

POP3 monitor resources monitor the following:

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.

## Displaying and changing the POP3 monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target POP3 monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### IP Address (within 255 bytes)

Specify the IP address of the POP3 server to be monitored. Specifying this item cannot be omitted.

Usually, specify the loopback address (127.0.0.1) to connect to the POP3 server that runs on the local server. If the addresses for which connection is possible are limited by POP3 server settings, specify an address for which connection is possible. 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 65535)

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

**Authentication Method**

Select the authentication method to log on to POP3. It must follow the settings of POP3 being used:

◆ APOP (default value)

The encryption authentication method that uses the APOP command.

◆ USER/PASS

The plaintext method that uses the USER/PASS command.

## Setting up PostgreSQL monitor resources

PostgreSQL monitor resources monitor PostgreSQL database that runs on the server.

### Notes on PostgreSQL monitor resources

For the supported PostgreSQL/PowerGres version, see "Applications supported by monitoring options" in Chapter 5, "Monitor resource details"

Interface DLL (LIBPQ.DLL) needs to be installed on the server where monitoring is performed because PostgreSQL/PowerGres library is used for monitoring. Specify the path of this DLL to the environmental variable when monitoring PostgreSQL.

For a target monitoring resource, specify a service resource or a script resource that can start PostgreSQL/PowerGres. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

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**.

A monitor table is created when monitoring starts. When monitoring is stopped due to the group stopping, the monitor table is deleted. When monitoring is temporarily stopped or when the server fails before the failover group stops due to system error, the monitor table is not deleted. Note that, if the server is shut down due to a system failure or other cause before the group is stopped, the monitor table will not be deleted. In this case, an alert message saying that "a monitor table exists" might be displayed next time monitoring is started. This is not an error.

PostgreSQL/PowerGres may output operation logs for each monitoring. Configure the PostgreSQL/PowerGres settings if this needs to be adjusted.

Because PostgreSQL is open-source software (OSS), its operation is checked but not guaranteed. Make sure to use PostgreSQL after evaluating it by yourself.

If PostgreSQL monitoring is performed, an error indicating that no library can be found may be output depending on the OS and PostgreSQL versions. In this case, add PostgreSQL bin to the PATH of the system environment variable. After that, restart the cluster.

**When adding PATH to the environment variable (The following is an example of PATH of PostgreSQL9.1 bin.)**

C:\Program Files\PostgreSQL\9.1\bin

When this monitor resource is used, messages like those shown below are output to a log on the PostgreSQL side. These messages are output by the monitor processing and do not indicate any problems.

```
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle ERROR: table "psqlwatch" does not exist
YYYY-MM-DD hh:mm:ss JST moodle moodle STATEMENT: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: CREATE TABLE psqlwatch
(num INTEGER NOT NULL PRIMARY KEY)
YYYY-MM-DD hh:mm:ss JST moodle moodle NOTICE: CREATE TABLE / PRIMARY
KEY will create implicit index "psqlwatch_pkey" for table "psql watch"
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
```

Regarding the monitor levels described in the next subsection "Monitoring by PostgreSQL monitor resources", when "Level 1" is selected, ExpressCluster does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

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

Create a monitor table using either of the following methods:

**(In the following example, the monitor table is named PSQLWATCH)**

```
sql> create table PSQLWATCH (num int not null primary key);  
sql> insert into PSQLWATCH values(0);  
sql> commit;
```

## Monitoring by PostgreSQL monitor resources

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

- ◆ Level 1 (monitoring by select)

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

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement

- ◆ Level 2 (monitoring by update/select)

Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of ( create / update / select / reindex / drop / vacuum ) type.

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement
- (3) The written data is not the same as the read data

## Displaying and changing the PostgreSQL monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target PostgreSQL monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### Monitor Level

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

- ◆ Level 1 (monitoring by select)  
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
- ◆ Level 2 (monitoring by update/select)  
Monitoring with reference to and update of the monitoring table. SQL statements issued to the monitor table are of (create / update / select / reindex / drop / vacuum ) type.

Default value: Level 2 (monitoring by update/select)

#### Database Name (within 255 bytes)

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

Default value: None

**IP Address:**

Specify the IP address of the database server to be monitored. 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 Number**

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

Default value: 5432

**User Name** (within 255 bytes)

Specify the user name to log on to the database.

Default value: postgres

**Password** (within 255 bytes)

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

Default value: None

**Monitor Table Name** (within 255 bytes)

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.

Default value: PSQLWATCH

## Setting up SMTP monitor resources

SMTP monitor resources monitor SMTP services that run on the server. SMTP monitor resources monitor SMTP protocol but they are not intended for monitoring specific applications. SMTP monitor resources monitor various applications that use SMTP protocol.

### Notes on SMTP monitor resources

For monitoring target resources, specify service resources or script resources that start SMTP. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

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**.

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

### Monitoring by SMTP monitor resources

SMTP monitor resources monitor the following:

POP3 monitor resources connect to the POP3 server and execute the command to verify the operation.

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

- (1) When connection to the SMTP server fails.
- (2) When an error is notified as a response to the command.

## Displaying and changing the SMTP monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target SMTP monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### IP Address

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

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

Default value: 25

#### User Name (within 255 bytes)

Specify the user name to log on to SMTP. If no user name is specified, SMTP authentication is not performed.

Default value: None



**Password** (within 255 bytes)

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

Default value: None

**Authentication Method**

Select the authentication method to log on to the SMTP. It must follow the settings of SMTP being used:

◆ **CRAM-MD5** (default value)

The encryption authentication method that uses the CRAM-MD5 command.

◆ **LOGIN**

The plaintext method that uses the LOGIN command.

**E-mail Address** (within 255 bytes)

Specify the email address used for monitoring. If nothing is specified, monitoring is performed using the command to verify the operation. The command that uses a dummy e-mail address is executed internally. If an email address is specified, monitoring is performed by running SMTP command to the specified e-mail address and verifying the result of it. It is recommended to have an e-mail address dedicated to monitoring.

Default value: None

## Setting up SQL Server monitor resources

SQL Server monitor resources monitor SQL Server database that runs on the server.

### Notes on SQL Server monitor resources

For the supported SQL Server version, see "Applications supported by monitoring options" in Chapter 5, "Monitor resource details"

For target monitoring resource, specify a service resource that can start SQL Server. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

To monitor an SQL Server 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 SQL Server database to become accessible after the VM resource is activated for **Wait Time to Start Monitoring**. Also, set up the SQL Server client on the host OS side, where monitor resources run, and specify the name of the virtual machine server as the instance name of the monitor target.

A monitor table is created when monitoring starts. When monitoring is stopped due to the group stopping, the monitor table is deleted. When monitoring is temporarily stopped or when server fails before the failover group stops due to system error, the monitor table will not be deleted. Note that, if the server is shut down due to a system failure or other cause before the group is stopped, the monitor table will not be deleted. In this case, an alert message saying that "a monitor table exists" might be displayed next time monitoring is started. This is not an error.

SQL Server may output operation logs for each monitoring. Configure the SQL Server settings if this needs to be adjusted.

Regarding the monitor levels described in the next subsection "Monitoring by SQL Server monitor resources", when "Level 1" is selected, ExpressCluster does not create monitor tables during monitoring. Instead, monitor tables must be created manually beforehand.

Selectable monitor level	Prior creation of a monitor table
Level 0 (database status)	Optional
Level 1 (monitoring by select)	Required
Level 2 (monitoring by update/select)	Optional

Create a monitor table using either of the following methods:

**(In the following example, the monitor table is named SQLWATCH)**

```
sql> create table SQLWATCH (num int not null primary key)
sql> go
sql> insert into SQLWATCH values(0)
sql> go
sql> commit
sql> go
```

## Monitoring by SQL Server monitor resources

SQL Server monitor resources perform monitoring according to the specified monitor level.

- ◆ Level 0 (database status)

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

An error is recognized if:

- (1) The database status is not online

- ◆ Level 1 (monitoring by select)

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

An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement

- ◆ Level 2 (monitoring by update/select)

Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.

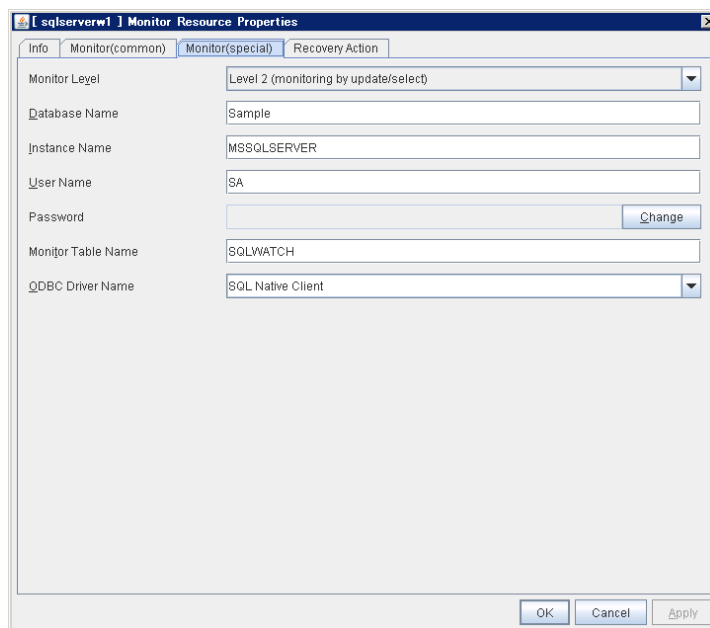
An error is recognized if:

- (1) A database connection could not be established
- (2) An error message is sent in response to an SQL statement
- (3) The written data is not the same as the read data

## Displaying and changing the SQL Server monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target SQL Server monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab



#### Monitor Level

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

- ◆ Level 0 (database status)  
The SQL Server management table (sys.databases) is referenced to check the DB status.
- ◆ Level 1 (monitoring by select)  
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
- ◆ Level 2 (monitoring by update/select)  
Monitoring with reference to and update of the monitoring table. SQL statements issued to the monitor table are of (create / update / select / drop) type.

Default value: Level 2 (monitoring by update/select)

#### Database Name (within 255 bytes)

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

Default value: None

**Instance Name** (within 255bytes)

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

Also, when monitoring an SQL Server database running on a guest OS of a virtual machine controlled by a VM resource, it is necessary to specify the server name of the virtual machine in the format of "*server-name\instance-name*."

Default value: MSSQLSERVER

**User Name** (within 255 bytes)

Specify the user name to log on to the database. If the user name is not specified, Windows authentication is used.

Default value: SA

**Password** (within 255 bytes)

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

Default value: None

**Monitor Table Name** (within 255 bytes)

Specify the name of a monitor table created on the database. 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.

Default value: SQLWATCH

**ODBC Driver Name** (within 255 bytes)

Select the driver name of the target database shown in the **ODBC** tab when you click **Start -> Administrative Tools -> Data Sources (ODBC)**.

Select **SQL Native Client** in SQL Server 2005.

Select **SQL Server Native Client 10.0** in SQL Server 2008.

Select **SQL Server Native Client 11.0** in SQL Server 2012.

Default value: SQL Native Client

## Setting up Tuxedo monitor resources

Tuxedo monitor resources monitor Tuxedo that runs on the server.

### Notes on Tuxedo monitor resources

For the supported Tuxedo version, see "Applications supported by monitoring options" in Chapter 5, "Monitor resource details"

For target monitoring resource, specify a script resource that can start Tuxedo. Monitoring starts after the target resource is activated; however, if Tuxedo cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

Tuxedo may output operation logs for each monitoring. Configure the Tuxedo settings if this needs to be adjusted.

### Monitoring by Tuxedo monitor resources

Tuxedo monitor resources monitor the following:

Tuxedo monitor resources connect to the Tuxedo and execute API to verify the operation.

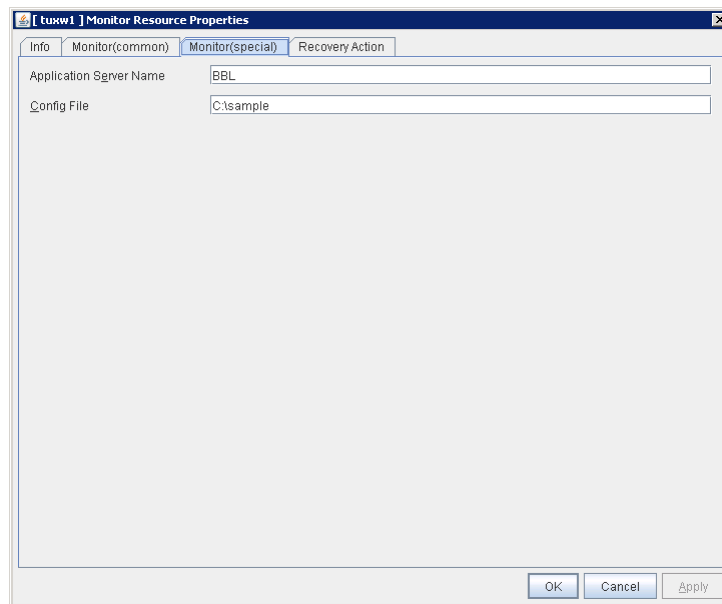
As a result of monitoring, the following is considered as an error:

(1) When an error is reported during the connection to the application server and/or the acquisition of the status.

## Displaying and changing the Tuxedo monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target Tuxedo monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab



#### **Application Server Name** (within 255 bytes)

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

Default value: BBL

#### **Config File** (within 1,023 bytes)

Specify the placement file name of Tuxedo. Specifying this item cannot be omitted.

Default value: None

## Setting up Weblogic monitor resources

Weblogic monitor resources monitor WebLogic that runs on the server.

### Notes on Weblogic monitor resources

For the supported WebLogic version, see "Applications supported by monitoring options" in Chapter 5 , "Monitor resource details."

For target monitoring resource, specify a script resource that can start Weblogic. Monitoring starts after the target resource is activated; however, if WebLogic cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

A Java environment is required to start monitoring with this command. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

WebLogic may output operation logs for each monitoring. Configure the WebLogic settings if this needs to be adjusted.

### Monitoring by Weblogic monitor resources

Weblogic monitor resources monitor the following:

Weblogic monitor resources use the webLogic. Admin (Ping) command to verify the operation.

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

- (1) When an error is reported as the response to the Ping.



## Displaying and changing the Weblogic monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target Weblogic monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### IP Address (within 80 bytes)

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

Default value: 127.0.0.1

#### Port (1024 to 65535)

Specify the port number used to connect to the server. Specifying this item cannot be omitted.

Default value: 7002

#### 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 1023 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 1023 bytes)

Specify the file in which the password required to access to a config file path is saved. Specify the full path of the file. 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 1023 bytes)

Specify the authentication file when authenticating SSL. You must specify this when the authentication method is **CustomTrust**.

Default value: None

**Installation Path** (within 1023 bytes)

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

Default value: C:\bea\weblogic92

## Setting up WebOTX monitor resources

WebOTX monitor resources monitor WebOTX that runs on the server.

### Notes on WebOTX monitor resources

For the supported WebOTX version, see "Applications supported by monitoring options" in Chapter 5 , "Monitor resource details."

For target monitoring resource, specify a script resource that can start WebOTX. Monitoring starts after the target resource is activated; however, if WebOTX cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

A Java environment is required to start monitoring with this command. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

WebOTX may output operation logs for each monitoring. Configure the WebOTX settings if this needs to be adjusted.

### Monitoring by WebOTX monitor resources

WebOTX monitor resources monitor the following.

WebOTX monitor resources use the serverStatus.bat command to verify the operation.

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

- (1) When an error is reported with the state of the acquired application server.

## Displaying and changing the WebOTX monitor resource details Websphere

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target WebOTX monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab

#### **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** (1024 to 65535)

Specify the port number used to connect to the server. Specifying this item cannot be omitted.

Default value: 6212

#### **User Name** (within 255 bytes)

Specify the user name of WebOTX. Specifying this item cannot be omitted.

Default value:None

#### **Password** (within 255 bytes)

Specify the password of WebOTX.

Default value: None

## Setting up Websphere monitor resources

Websphere monitor resources monitor WebSphere that runs on the server.

### Notes on Websphere monitor resources

For the supported WebSphere version, see "Applications supported by monitoring options" in Chapter 5, "Monitor resource details."

For target monitoring resource, specify a service resource that can start WebSphere. Monitoring starts after the target resource is activated; however, if the database cannot be started right after the target resource is activated, adjust the time by using **Wait Time to Start Monitoring**.

A Java environment is required to start monitoring with this command. The application server system uses Java functions. Therefore if Java stalls, it may be recognized as an error.

WebSphere may output operation logs for each monitoring. Configure the Websphere settings if this needs to be adjusted.

### Monitoring by Websphere monitor resources

Websphere monitor resources monitor the following:

Websphere monitor resources use the serverStatus.bat command to verify the operation.

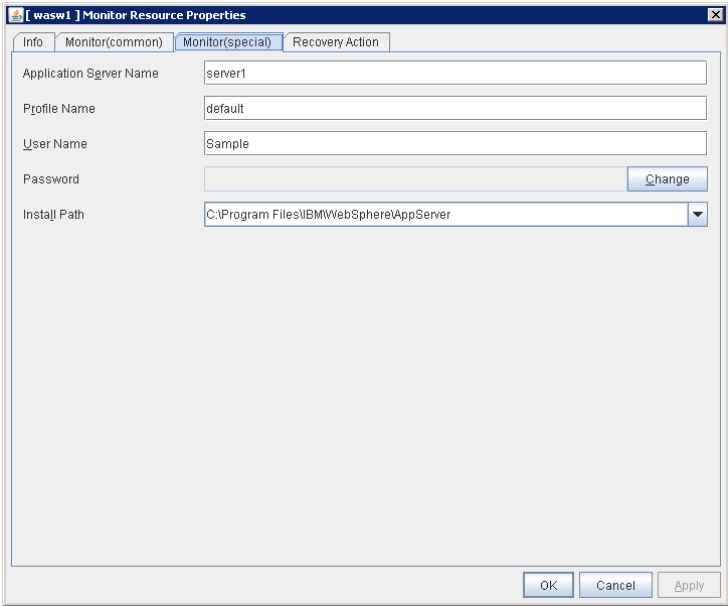
As a result of monitoring, the following is considered as an error:

- (1) When an error is reported with the state of the acquired application server.

## Displaying and changing the Websphere monitor resource details

1. Click **Monitors** on the tree view displayed on the left side of the Builder window.
2. List of the monitor resources is displayed in the table view on the right side of the screen. Right click the target Websphere monitor resource, and click the **Monitor(special)** tab in the **Monitor Resource Properties** window.
3. On the **Monitor(special)** tab, you can see and/or change the settings of monitor resource by following the description below.

### Monitor resource Monitor(special) tab



#### **Application Server Name** (within 255 bytes)

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

Default value: server1

#### **Profile Name** (within 1023 bytes)

Specify the profile name of WebSphere. Specifying this item cannot be omitted.

Default value: default

#### **User Name** (within 255 bytes)

Specify the user name of WebSphere. Specifying this item cannot be omitted.

Default value:None

#### **Password** (within 255 bytes)

Specify the password of WebSphere.

Default value: None

**Installation Path** (within 1023 bytes)

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

Default value: *C:\Program Files\IBM\WebSphere\AppServer*

## 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.

### Note on JVM monitor resources

The **Java installation path** on the **JVM monitor** tab of **Cluster Properties** must be set. before adding JVM monitor resource.

For a target resource, specify an application server running on Java VM such as WebLogic Server or WebOTX. As soon as the JVM monitor resource has been activated, the Java Resource Agent starts monitoring, but if the target (WebLogic Server or WebOTX) cannot start running immediately after the activation of the JVM monitor resource, use **Wait Time to Start Monitoring** to compensate.

### Monitoring by JVM monitor resources

JVM monitor resource monitors the following:

Monitors application server by using JMX (Java Management Extensions).

The monitor resource determines the following results as errors:

- Target Java VM or application server cannot be connected
- The value of the used amount of resources obtained for the Java VM or application server exceeds the user-specified threshold a specified number of times (error decision threshold) consecutively

As a result of monitoring, an error is regarded as having been solved if:

- The 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.

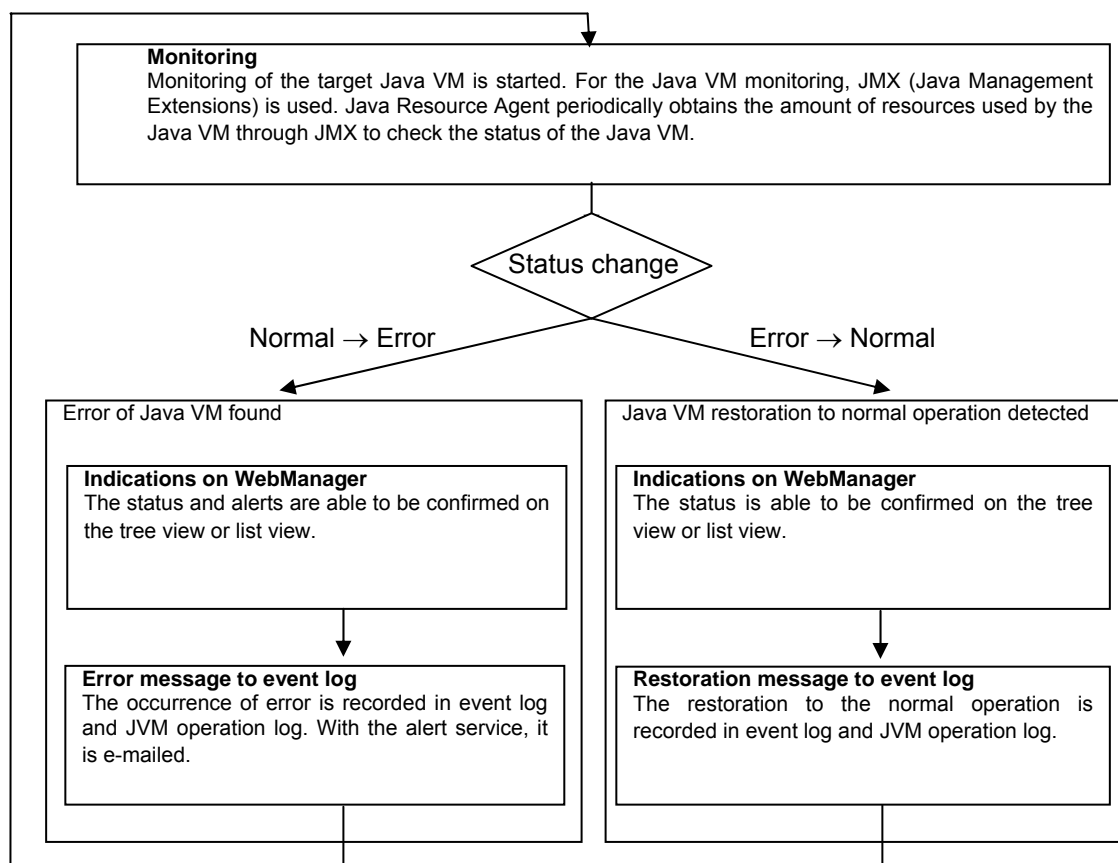
---

**Note:**

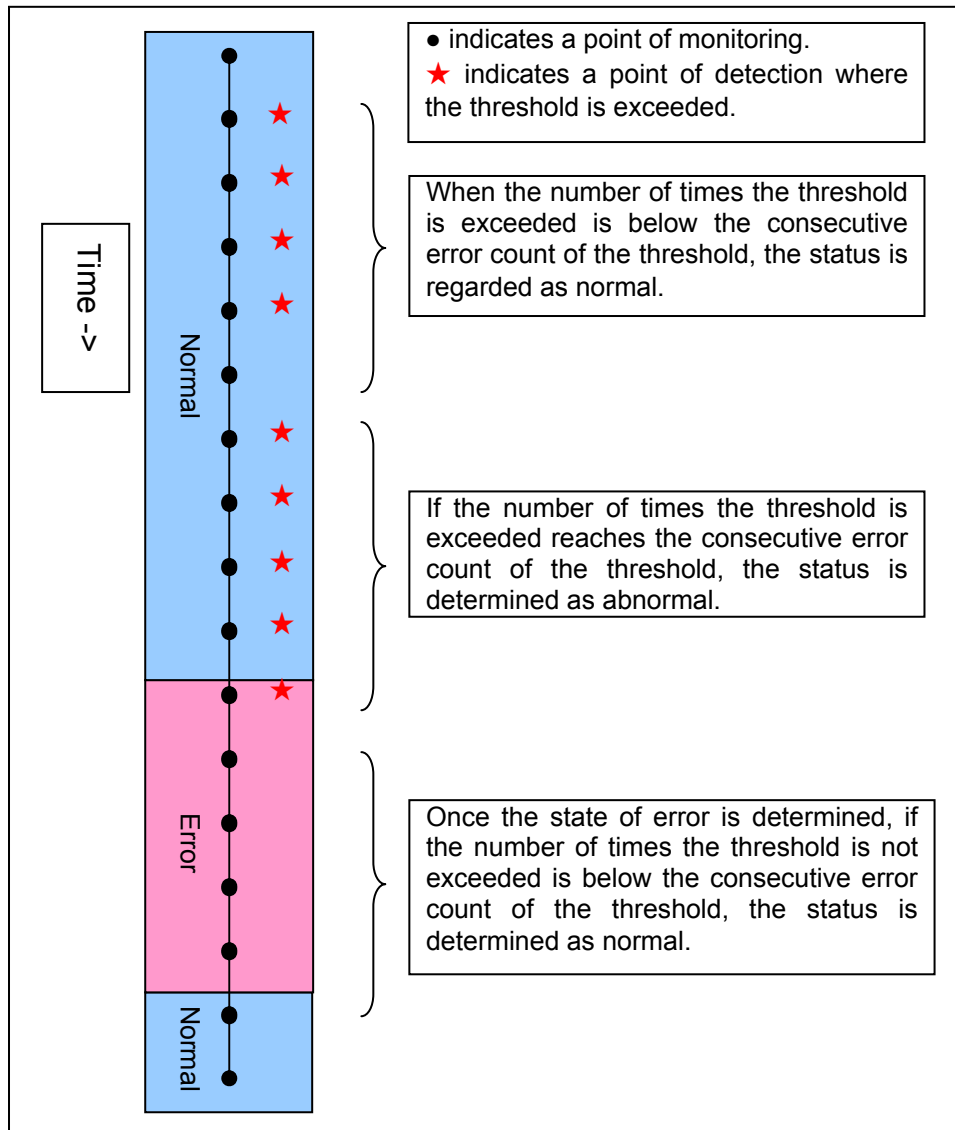
**Collect Cluster Logs** in the WebManager **Tools** menu does not handle the configuration file and log files of the target (WebLogic or WebOTX).

---

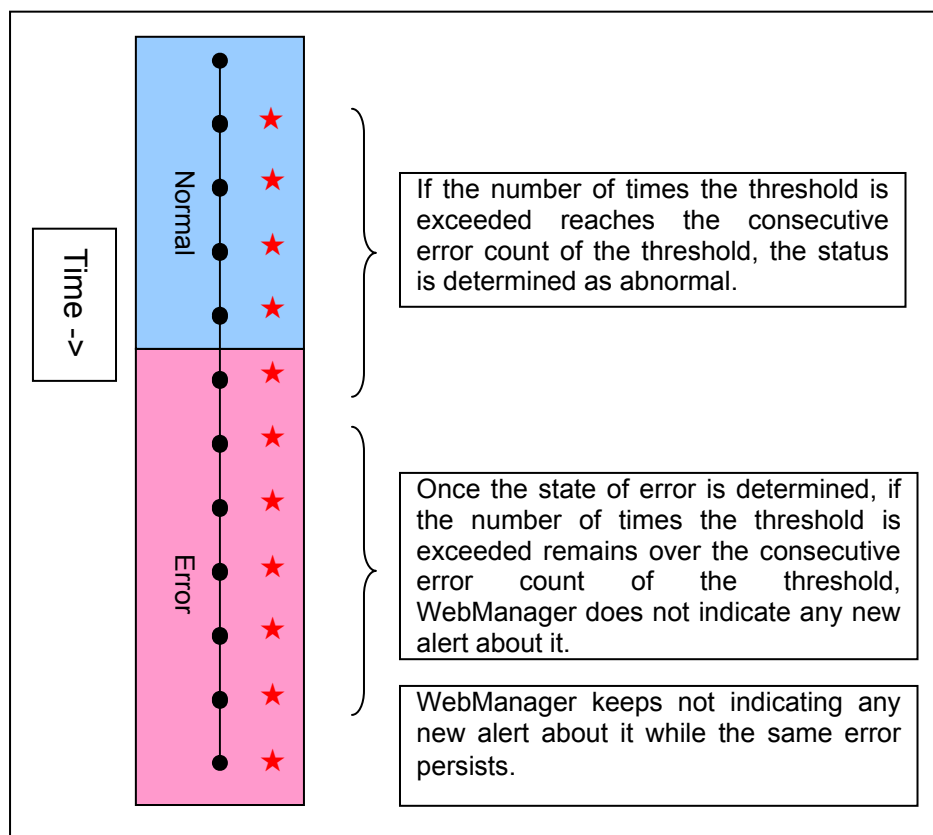




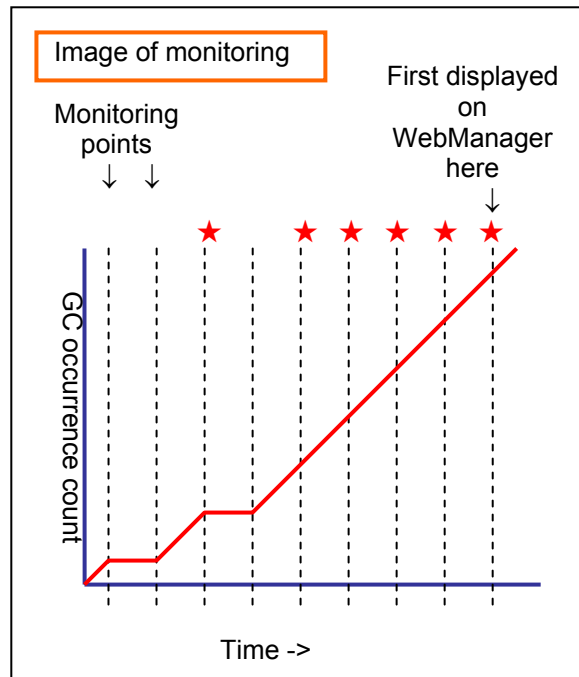
The standard operations when the threshold is exceeded are as described below.



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 during JVM monitoring 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 (JVM monitor 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 JVM monitor 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.

When a load balancing system is configured with the load balancer on the server, the JVM monitoring 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).

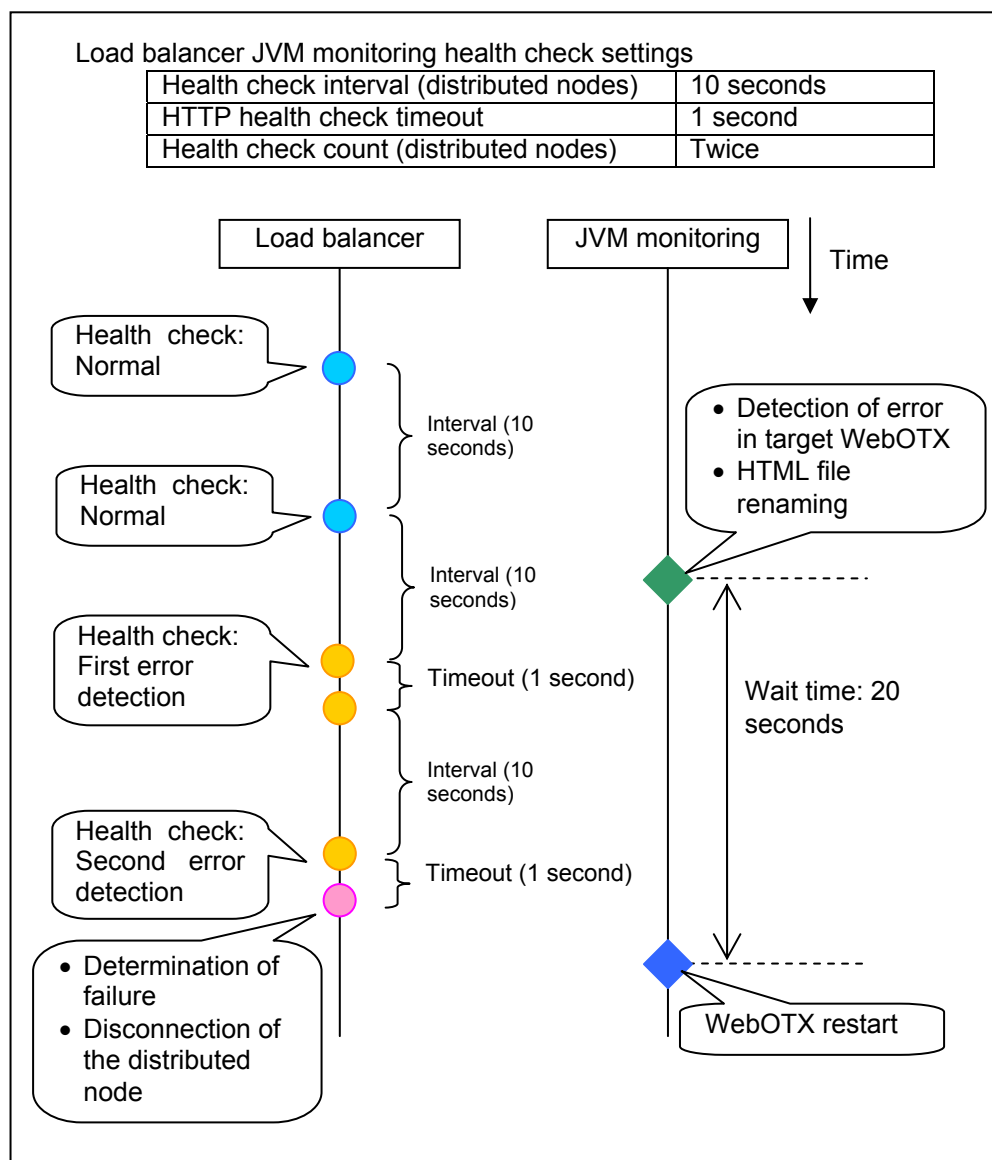
The JVM monitoring halts for the wait time, or 20 seconds, after renaming the HTML file. The wait time is intended to prevent WebOTX from being restarted before the load balancer finishes disconnecting the distributed node.

Once the JVM monitoring 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 -> **adBalancer** -> **stem 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  $\geq$  (health check (distributed node) interval + HTTP health check timeout) x health check (distributed node) count



Settings must also be specified on the load balancer side.

For Express5800/LB400\*, specify load dispersion environment settings by using the Management Console of the load balancer. For setting details, refer to the *Express5800/LB400\* User's Guide (Software)*.

For a load balancer other than Express5800/LB400\*, refer to the relevant manual.

## 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. The load balancer linkage provides a JVM monitor 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 the function, configure the settings through the **Monitor(Special)** tab. The CPU load-dependent weighting function of the load balancer is linked.

- **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.

### Note:

Execute the command from an account having the Administrator privilege.

By using a registry editor, Please set the following registry key value Execute

IA32 version

Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\NEC\IPLB4\Parameter\JVMSaver...	Description	Value	Default
Enabled	Enables or disables the function.	0 or 1 0: Disable 1: Enable	0
JVMSaverCheckInterval	Specify the execution interval for the target Java VM load calculation command, in seconds.	1 to 2147483646	120 (seconds)
ActionTimeout	Specify the timeout for the target Java VM load calculation command, in seconds.	1 to 2147483646	1800 (seconds)
CommandPath	Specify the path for the target Java VM	Please specify	none

ExpressCluster X SingleServerSafe 3.1 for Windows Configuration Guide

	load calculation command.	below. For Windows Server 2003, Windows Server 2008 ("" please enclose):  "<ExpressCluster install path> %ha%jra%bin%clpjra _lbadmin.bat" weight	
--	---------------------------	---	--

x86\_64 version

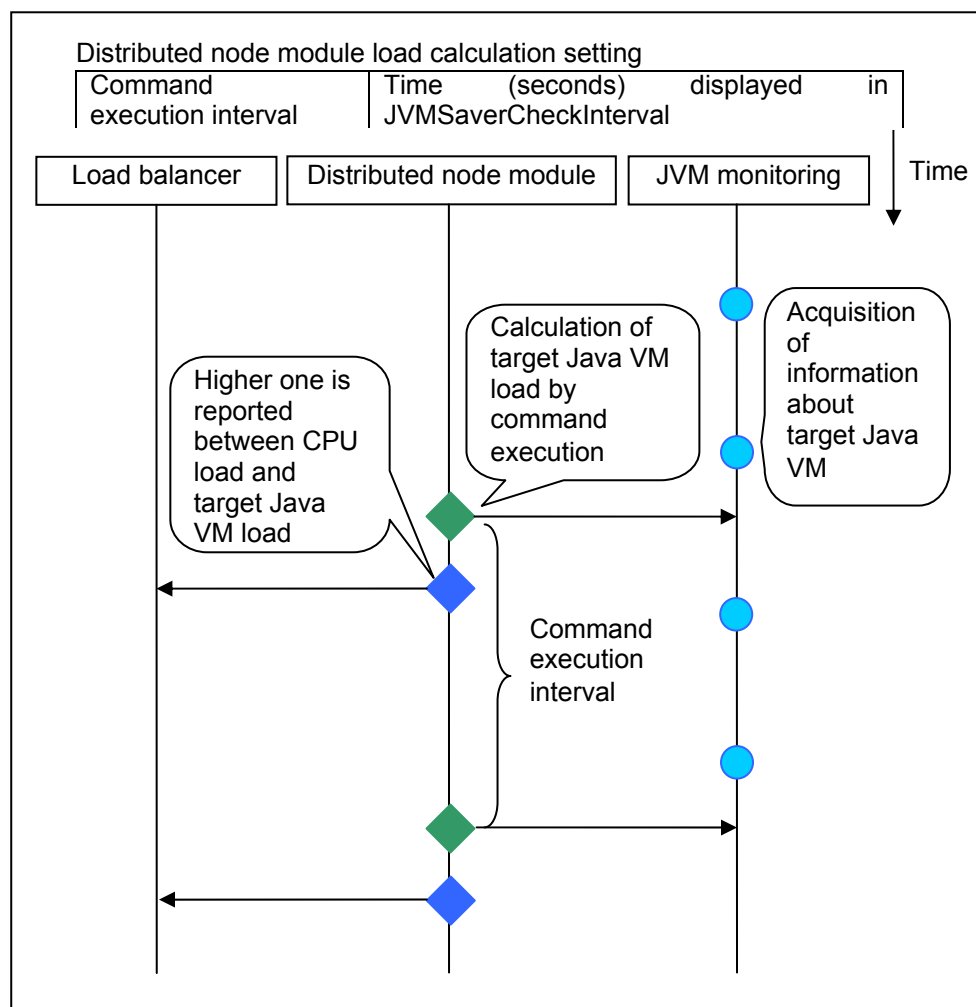
Registry key: HKEY_LOCAL_MACHINE\Software\Wow6432Node\NEC\IPLB4\Parameter\JVMSaver...	Description	Value	Default
Enabled	Enables or disables the function.	0 or 1 0: Disable 1: Enable	0
JVMSaverCheckInterval	Specify the execution interval for the target Java VM load calculation command, in seconds.	1 to 2147483646	120 (seconds)
ActionTimeout	Specify the timeout for the target Java VM load calculation command, in seconds.	1 to 2147483646	1800 (seconds)
CommandPath	Specify the path for the target Java VM load calculation command.	Please specify below. For Windows Server 2003, Windows Server 2008 ("" please enclose):  "<ExpressCluster install path> %ha%jra%bin%clpjra _lbadmin.bat" weight  For Windows Server 2008 R2: <ExpressCluster install path> %ha%jra%bin%clpjra _lbadmin.bat weight	none

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. The threshold 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)

For the distributed node module installed on a server on which JVM monitoring 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.



Settings must also be specified on the load balancer side.

In the case of Express5800/LB400\*, specify load dispersion environment settings by using the Management Console of the load balancer. For setting details, refer to the *Express5800/LB400\* User's Guide (Software)*.

For load balancers other than Express5800/LB400\*, refer to the relevant manual.

The dispersed node module must be restarted in order to apply the JVM monitor settings. The module must also be restarted when changing the setting of the load calculation function of the Java VM to be monitored from enabled to disabled and vice versa.



If you are using Windows, restart the iplb4 service by clicking **Start -> Control Panel -> Management Tools -> Services**.

## 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]

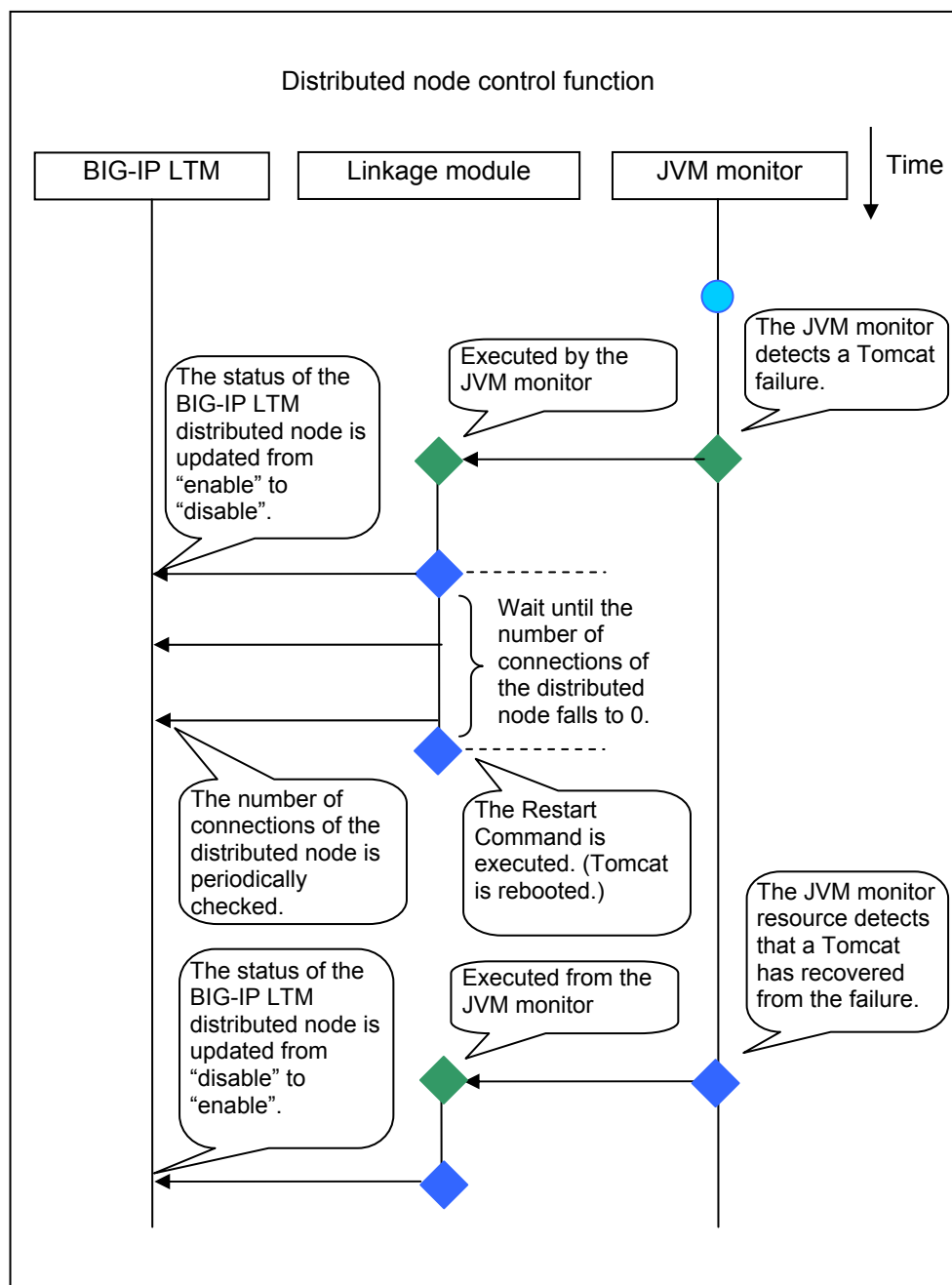
If the relevant server configures the BIG-IP LTM load distribution system, when the JVM monitor detects a Tomcat failure (for example: the amount of collection information exceeds the specified threshold), iControl is used to update the BIG-IP LTM distributed node status from “enable” to “disable”.

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.

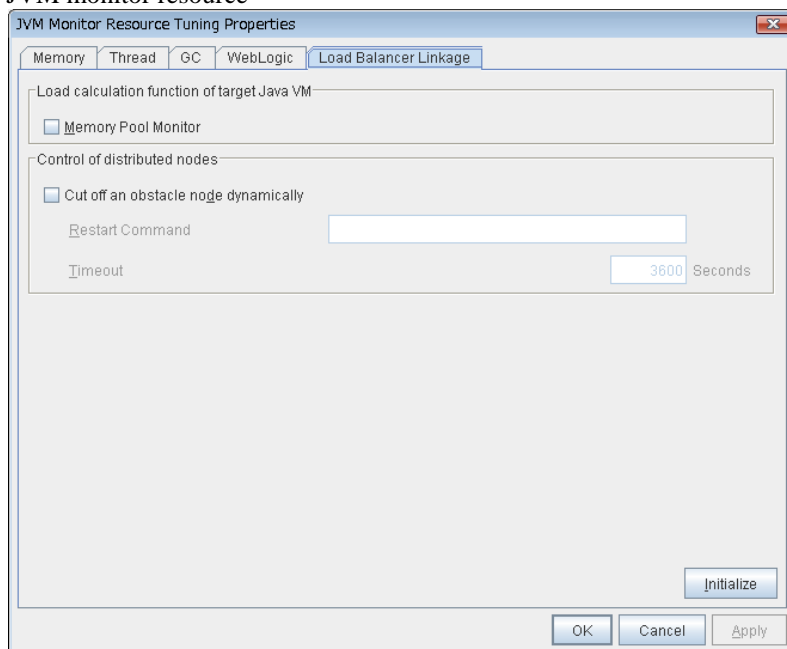
Obtain the Java VM load from the following expression. The threshold is the value obtained by multiplying the entire amount of the Java heap area by the use ratio set with **Monitor(special)** tab - **Tuning** property - **Memory** tab - **Monitor Heap Memory Rate** - **Total Usage**.

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.

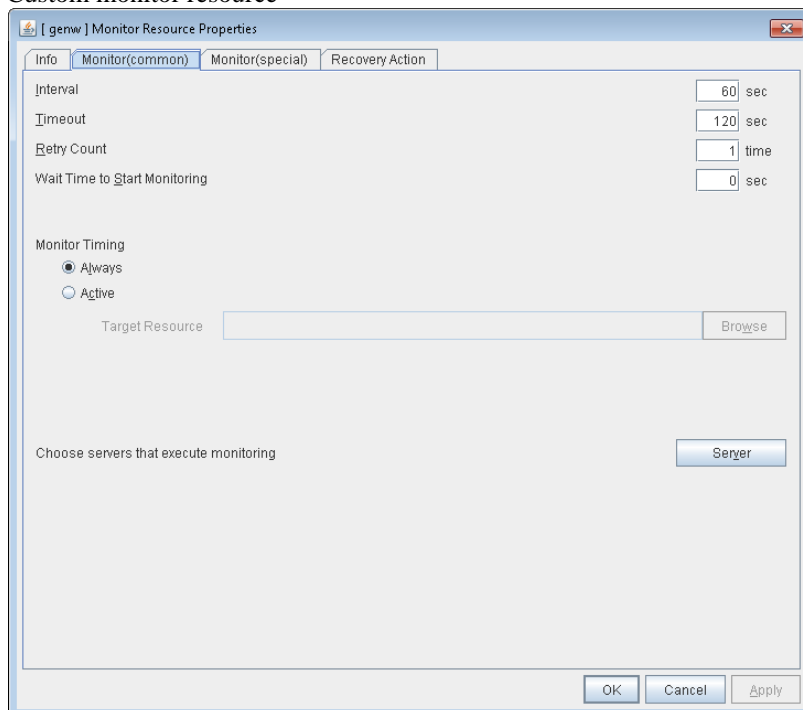
Set the following ExpressCluster settings with the Builder.

- JVM monitor resource

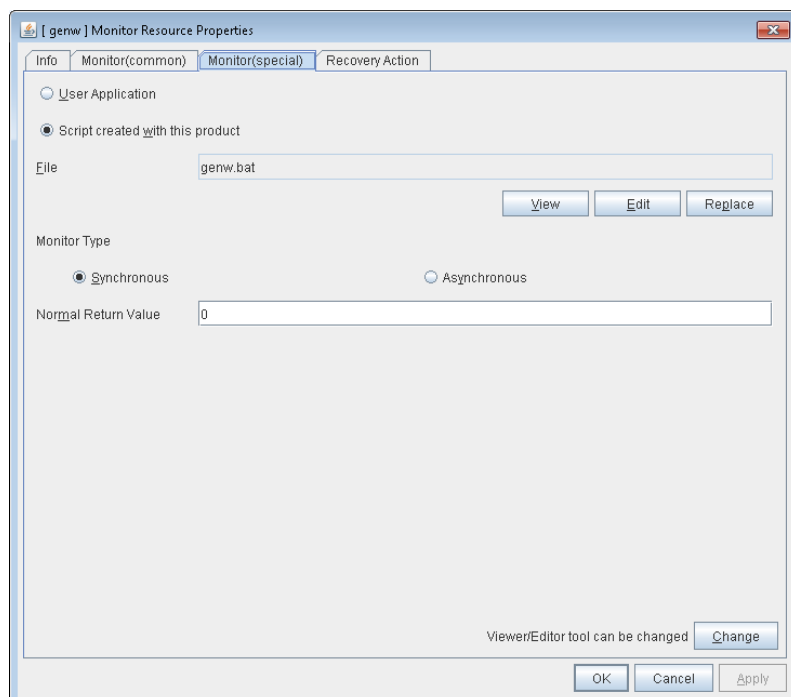


**Properties - Monitor(special) tab -> Tuning property - Load Balancer Linkage tab**  
Select the **Memory Pool Monitor** check box.

- Custom monitor resource



**Properties - Monitor(common) tab**  
Select the **Monitor Timing - Always** radio button.



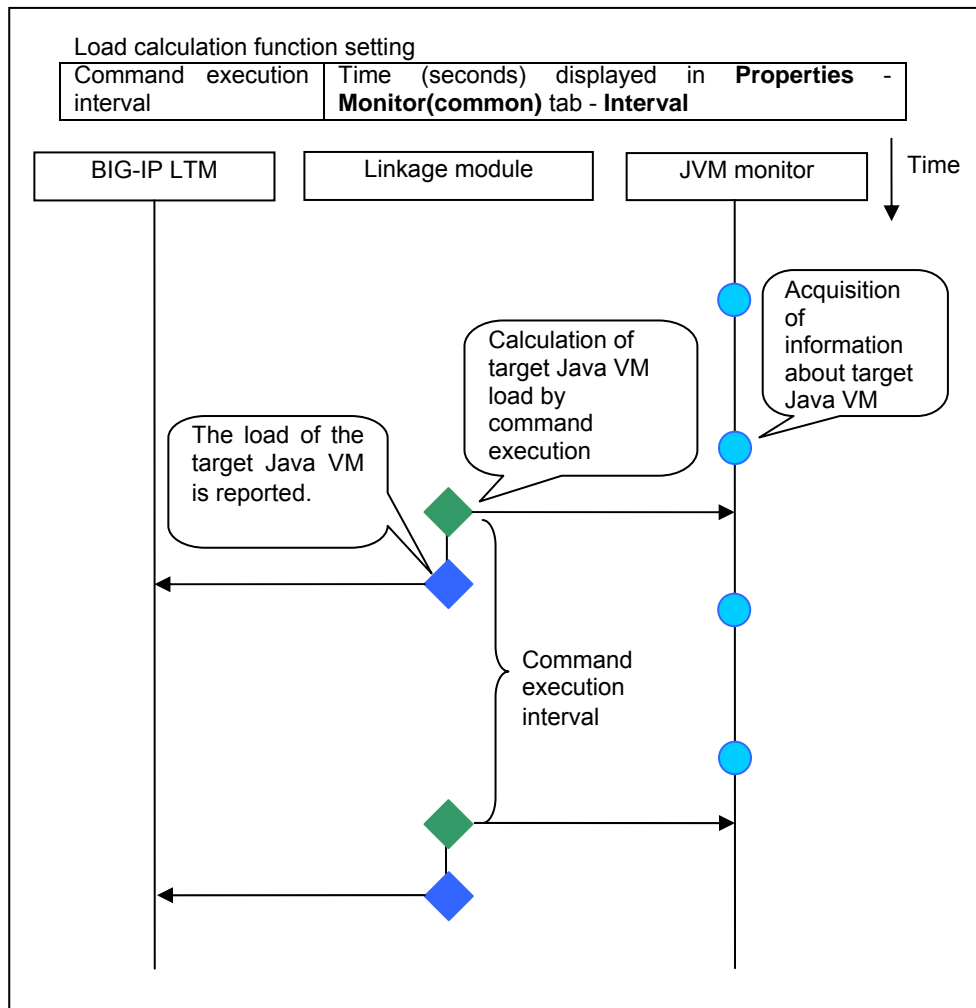
#### Properties - Monitor(special) tab

Select **Script created by this product(W)**. Select **File - Edit** and then add the following boldfaced section.

```
rem *****
rem *                genw.bat                *
rem *****
echo START
"<Installation      Path      of      ExpressCluster
>\ha\jra\bin\clpjra_bigip.exe" weight
echo EXIT
```

Select the **Monitor Type - Synchronous** radio button.

In the BIG-IP LTM setting, specify **Ratio(node)** in **LocalTraffic - Pools:PoolList - Relevant pool - Members - LoadBalancing - Load Balancing Method** of BIG-IP Configuration Utility



## 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.
3. Regarding the target server, select **Configuration-General**, and then check the port number through which a management connection is established with **Listen Port**.
4. Stop WebLogic Server. For how to stop WebLogic Server, refer to “Starting and stopping WebLogic Server” in the WebLogic Server manual.
5. Open the WebLogic Server startup script.
6. Write the following instructions in the script.

➤ When the target is the WebLogic Server managing server:

```
✓ set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
```

\*Write each line of coding on one line.

---

### Note:

For **n**, specify the number of the port used for monitoring. The specified port number **must be different from that of the listen port for the target Java VM**. If there are other target WebLogic Server entities on the same machine, specify a port number different from those for the listening port and application ports of the other entities.

---

➤ When the target is a WebLogic Server managed server:

```
✓ if "%SERVER_NAME%" == "SERVER_NAME"(
  set JAVA_OPTIONS=%JAVA_OPTIONS%
  -Dcom.sun.management.jmxremote.port=n
  -Dcom.sun.management.jmxremote.ssl=false
  -Dcom.sun.management.jmxremote.authenticate=false
)
```

\*Write all the if statement lines (lines 2 to 5) on one line.

---

### Note:

For **SERVER\_NAME**, specify the name of the target server confirmed by **Select Target Server**. If more than one server is targeted, change the server name on the settings (line 1 to 6) for each server.

---

**Note:**

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%**

**-Dweblogic.Name=%SERVER\_NAME%**

**-Djava.security.policy=%WL\_HOME%\server\lib\weblogic.policy %JAVA\_OPTIONS**

**% %PROXY\_SETTINGS% %SERVER\_CLASS%**

*\*Write the above coding on one line.*

---

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. Start WLST (wlst.cmd) of the target WebLogic Server.  
To do this, select **Start** menu-**Oracle WebLogic-WebLogic Server** <version number>-**Tools-WebLogic Scripting Tool**.
10. On the prompt window displayed, execute the following commands. Replace the **USERNAME**, **PASSWORD**, **SERVER\_ADDRESS**, **SERVER\_PORT**, and **DOMAIN\_NAME** with those for the domain environment.  

```
>connect('USERNAME','PASSWORD','t3://SERVER_ADDRESS:SERVER_PORT')
>edit()
>startEdit()
>cd('JMX/DOMAIN_NAME')
>set('PlatformMBeanServerUsed','true')
>activate()
>exit()
```
11. 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 the console” in the *WebOTX Operation (Web Administration Console)*.

The settings differ depending on whether a Java process of the JMX agent running on WebOTX or the Java process of a process group is to be monitored. Configure the settings according to the target of monitoring.

### 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 console.
2. In the tree view, select **<domain\_name>-TP System-Application Group-<application\_group\_name>-Process Group-<process\_group\_name>**.
3. For the **Other Arguments** attributes on the **JVM Options** tab on the right, specify the following Java options on one line. For *n*, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with 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~~
4. Then, click **Update**. After the configuration is completed, restart the process group.

These settings can be made by using **Java System Properties**, accessible from the **Java System Properties** tab of the WebOTX administration console. When making these settings by using the console, do not designate “-D” and set the strings prior to “=” in “name” and set the strings subsequent to “=” in “value”.

---

### Note:

If restart upon a process failure is configured as a function of the WebOTX process group, and when the process group is restarted as the recovery processing by ExpressCluster, the WebOTX process group may fail to function correctly. For this reason, when monitoring the WebOTX process group, make the following settings for the JVM monitor resource by using the 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 event log.

**%1\$s:Notification received. %2\$s.**

**%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 Tomcat

This section describes how to configure a target Tomcat to be monitored by the JVM monitor resource.

1. Stop Tomcat, and then open **Start** → (*Tomcat\_Program\_folder*) → **Configure Tomcat**.
2. In the Java Options of Java of the open window, specify the following settings 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
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** → **Monitor(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 file.

Monitor target	File to be edited
Report Director EnterpriseServer	<SVF installation path> ¥launcher¥ReportDirectorEnterpriseServer.run
Report Director SvF Server	<SVF installation path> ¥launcher¥ReportDirectorSvFServer.run
Report Director Spool Balancer	<SVF installation path> ¥launcher¥ReportDirectorSpoolBalancer.run
Tomcat	The window indicated by carrying out the following <SVF installation path> ¥apache-tomcat¥bin¥tomcat5w.exe //ES//SVFWebService

2. The following contents are inserted in the part where Arguments is designated just after the setting point of "-Xms". For *n*, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the 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**

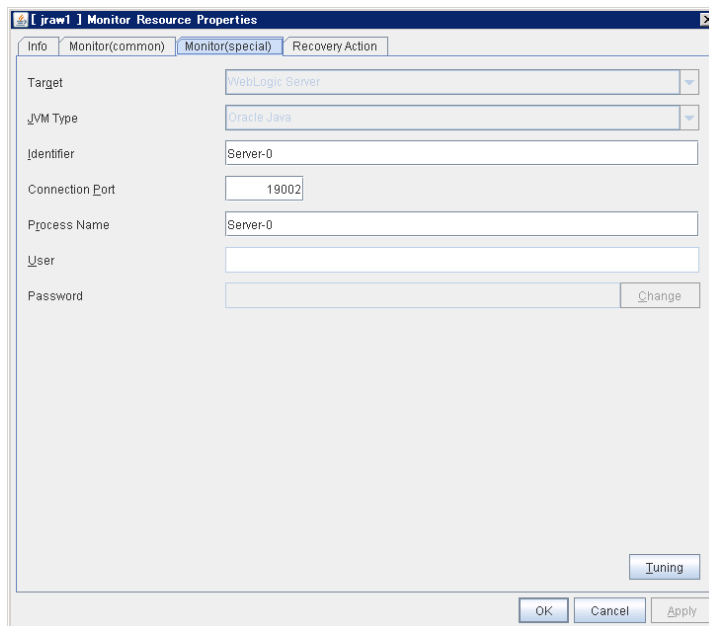
**-Dcom.sun.management.jmxremote.authenticate=false**

3. 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** → **Monitor (special)** tab → **Process Name**), specify the following.

Monitor target	Identifier, Process Name
Report Director EnterpriseServer	RDEServer
Report Director SvF Server	RDSvFServer
Report Director Spool Balancer	ReportDirectorSpoolBalancer
Tomcat	Tomcat

## Displaying and changing the JVM monitor resource details

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 **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.



### Target

Select the target to be monitored from the list. When monitoring WebSAM SVF for PDF, WebSAM Report Director Enterprise, or WebSAM Universal Connect/X, select **WebSAM SVF**. When monitoring a Java application that you created, select **Java Application**.

Default: None

### JVM Type

Select the Java VM on which the target application to be monitored is running.

Default: None

**Identifier** (within 255 bytes)

Specify a name to uniquely identify the target Java VM. You must specify the identifier.

- ◆ When the target is **WebLogic Server**  
Set this according to “Monitoring WebLogic Server”, item 2.
- ◆ When the target is **WebOTX Process Group**  
Specify the name of the process group.
- ◆ When the target is **WebOTX Domain Agent**  
Specify the name of the domain.
- ◆ When the target is **WebOTX ESB**  
Same as for **WebOTX Process Group**.
- ◆ When the target is **Tomcat**  
Specify this according to “Monitoring Tomcat”.
- ◆ When the target is **WebSAM SVF**  
Specify this according to “Monitoring SVF”.
- ◆ When the target is **Java applications**  
Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

**Connection Port** (1024 to 65535)

Specify the number of the port to be used for connection with 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**  
Specify the connection port number according to “Monitoring WebLogic Server”, item 6.
- ◆ When the target is **WebOTX Process Group**  
Specify this according to “Monitoring a Java process of a WebOTX process group”.
- ◆ When the target is **WebOTX Domain Agent**  
Specify “domain.admin.port” of  
“(WebOTX\_installation\_path)\%<domain\_name>.properties”.
- ◆ When the target is **WebOTX ESB**  
Same as for **WebOTX Process Group**.
- ◆ When the target is **Tomcat**  
Specify as described in “Monitoring Tomcat”.
- ◆ When the target is **WebSAM SVF**  
Specify this according to “Monitoring SVF”.
- ◆ When the target is **Java applications**  
Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

**Process Name** (within 255 bytes)

Specify a process name to uniquely identify the target Java VM process.

- ◆ When the target is **WebLogic Server**  
Specify a string to uniquely identify the target Java VM process.

- ◆ 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 **WebOTX ESB**  
Same as for **WebOTX Process Group**.
- ◆ When the target is **Tomcat**  
Specify this according to "Monitoring Tomcat".
- ◆ When the target is **WebSAM SVF**  
Specify this according to "Monitoring SVF".
- ◆ When the target is **Java applications**  
Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

**User** (within 255 bytes)

Specify the name of the administrator who will be making a connection with the target Java VM. When **WebOTX Domain Agent** is selected as the target, specify the "domain.admin.user" value of "(WebOTX\_installation\_path)\<domain\_name>.properties".

Default: None



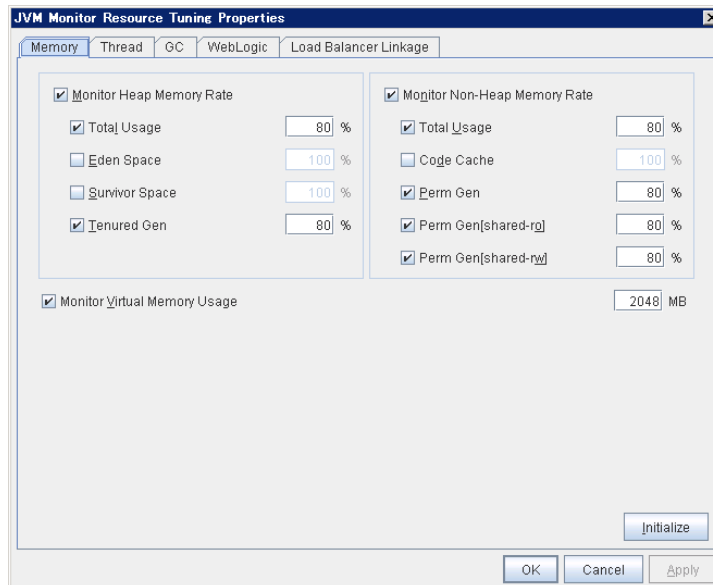
**Password** (within 255 bytes)

Specify the password for the administrator who will be making a connection with the target Java VM. When **WebOTX Domain Agent** is selected as the target, specify the “domain.admin.passwd” value of “(WebOTX\_installation\_path)\<domain\_name>.properties”. Click **Change** and enter the password in the dialog box. The letters of the password are not displayed.

Default: None

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



### Monitor Heap Memory Rate

Enables the monitoring of the usage rates of the Java heap areas used by the target Java VM.

- ◆ When selected:  
Monitoring enabled
- ◆ When cleared (default):  
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.

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.

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.

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:  
Monitoring enabled
- ◆ When cleared (default):  
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)**

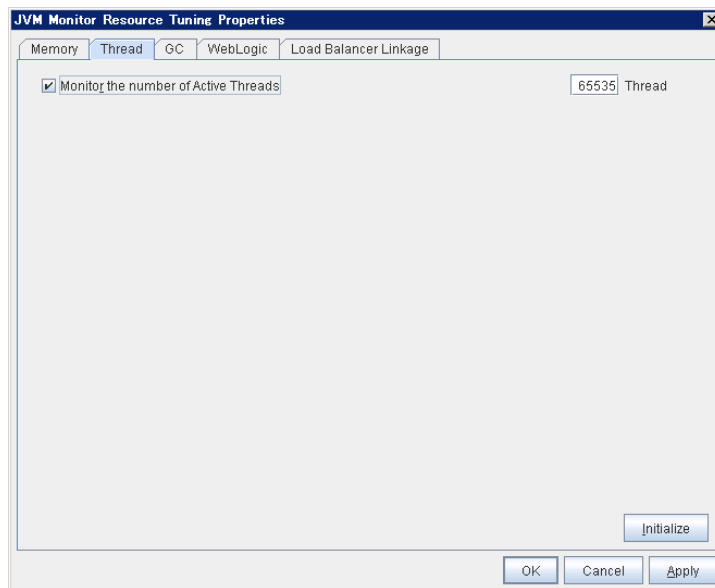
Specify the threshold for the usage of the virtual memory used by the target Java VM. When the target Java VM consists of 64-bit processes, uncheck this check box.

Default: 2048[MB]

**Initialize**

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

## Thread tab



### Monitor the number of Active Threads (1 to 65535)

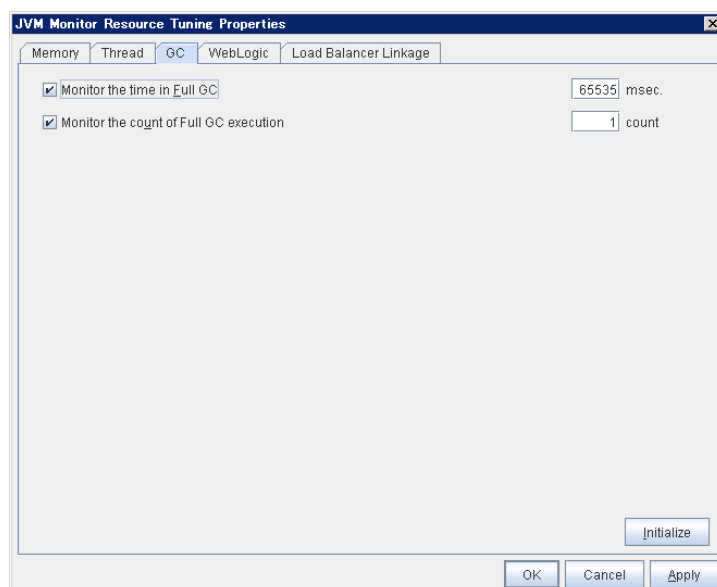
Specify the upper limit threshold for the number of threads running on the monitor target Java VM.

Default: 65535 [threads]

### 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)

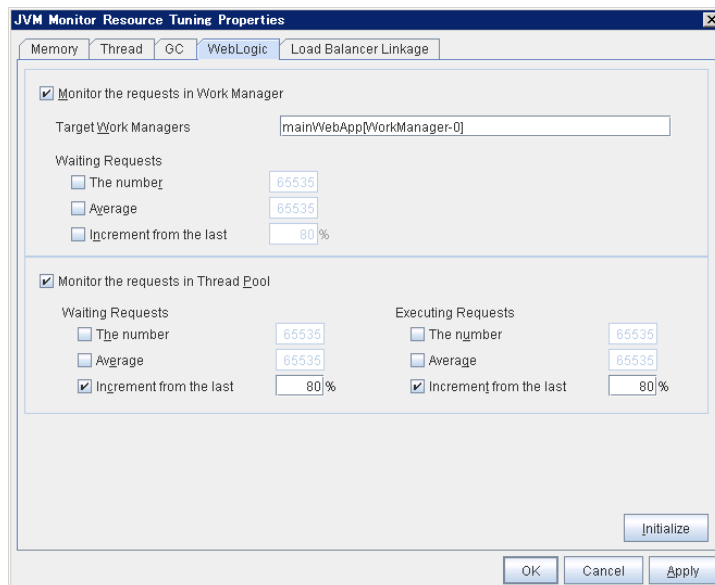
Specify the threshold for the number of times Full GC occurs since previous measurement on the target Java VM.

Default: 1 (time)

### Initialize

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

## WebLogic tab



### 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**

Enables the monitoring of the number of wait requests (number of HTTP requests queued in the WebLogic Server) and the number of executing requests (number of HTTP requests queued in the WebLogic Server) in the target WebLogic Server thread pool.

- ◆ When selected:  
Monitoring enabled
- ◆ When cleared (default):  
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)

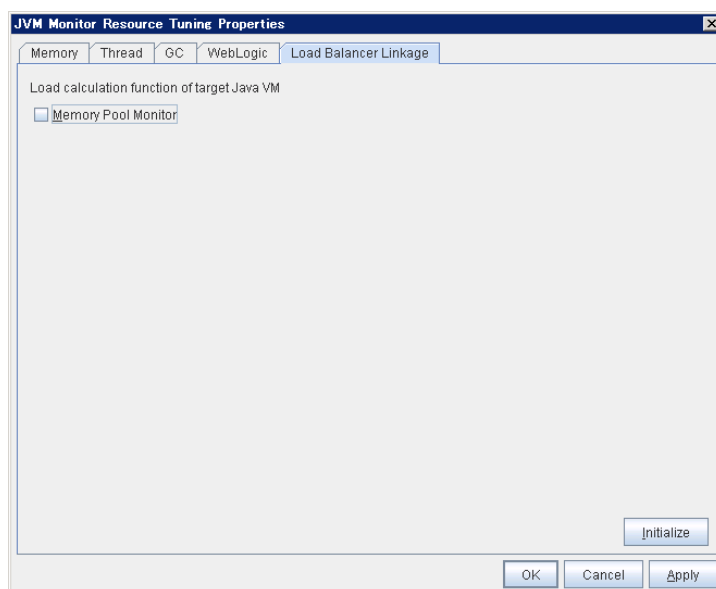
Specify the threshold for the increment of the number of requests executed per unit of time since the previous measurement.

Default: 80[%]

**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.

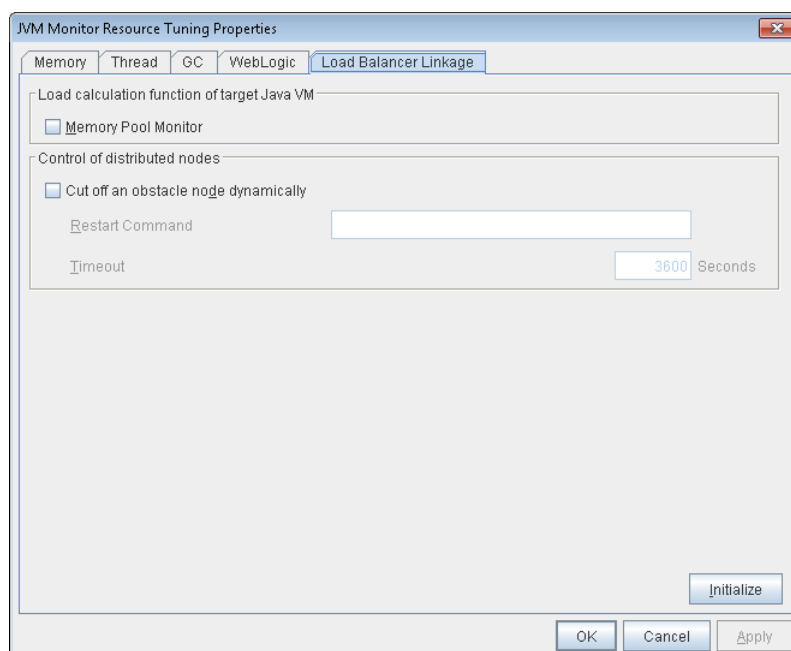
- ◆ When selected:  
Monitoring enabled
- ◆ When cleared (default):  
Monitoring disabled

### Initialize

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



## Load Balancer Linkage tab



This screen appears when **BIG-IP LTM** is selected as the load balancer type.

### Memory Pool Monitor

Enables the monitoring of the memory pool when notifying the load balancer of dynamic load information.

- When 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 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 rebooted when resident monitoring is performed and a monitor target failure is detected. For a restart command, specify the common value for every 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.

## Setting up system monitor resources

System monitor resources monitor the resources used by processes. The resources periodically collect statistical information about resources used by processes and analyze the information according to given knowledge data. System monitor resources serve to detect the exhaustion of resources early according to the results of analysis.

### Notes on system monitor resource

System Resource Agent may output operation logging for each monitoring operation. Configure System Resource Agent according to the desired logging output settings.

For the recovery target, specify the resource to which fail-over is performed upon the detection of an error in resource monitoring by System Resource Agent.

The use of the default System Resource Agent settings is recommended.

Errors in resource monitoring may be undetectable when:

A system resource value repeatedly exceeds and then falls below a threshold.

In a case like where the system is high loaded, it may take a long time to collect statistical information and the interval of statistical information collection may be unapplied.

When a service of System Resource Agent stops, a pop-up dialog box may show a message telling that the stop sequence did not end within the specified duration of time. Click the **OK** button to the message to close the dialog box, and then wait until the service gets to the “stopped” status.

If date or time of OS has been changed during System Resource Agent's operation, resource monitoring may operate wrongly as follows since the timing of analyze which is normally done at 10 minute intervals may be changed at first time after changing date or time. In such case, suspend and resume cluster.

- Error is not detected after passing specified duration to detect error.
- Error is detected before passing specified duration to detect error.

Once the cluster has been suspended and resumed, the collection of information is started from that point of time.

The amount of process resources 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 smaller value than the actual disk size when specifying the disk size for free space monitoring of disk resources. If a larger value specified, a lack-of-free-space error will be detected.

If the monitored disk is exchanged, the following information analyzed up to then will be cleared if it differs from the information in the previous disk:

- Total disk capacity
- File system

When monitoring disk resources, only hard disks can be monitored.

Up to 26 disk units can be simultaneously monitored by the disk resource monitoring function.

If **system monitor** is not displayed in the **Type** column on the monitor resource definition screen, select **Get License Info** and then acquire the license information.

## Monitoring by system monitor resources

System monitor resources monitor the following:

Periodically collect the amounts of process resources, system resources and disk resources used and then analyze the amounts.

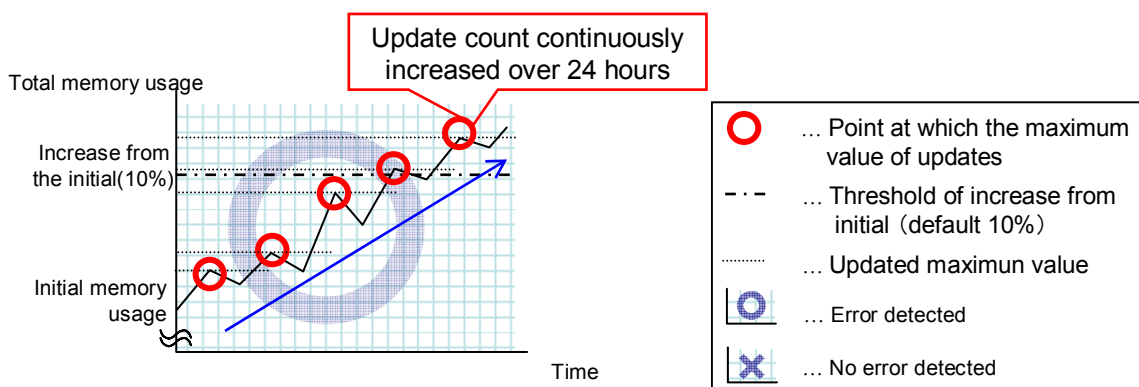
An error is recognized if the amount of a resource used exceeds a pre-set threshold.

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, or number of threads) operated by using the default values, a resource error is reported after 24 hours.

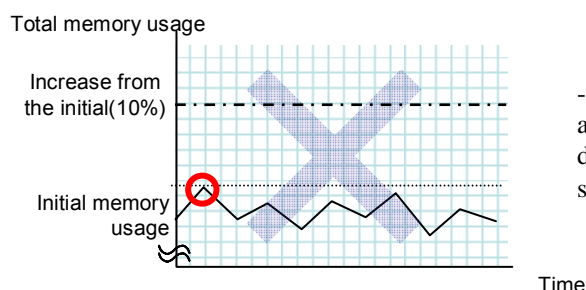
The following chart describes how process resource monitoring detects memory usage errors.

- ◆ In the following example, as time progresses, memory usage increases and decreases, the maximum value is updated more times than specified, and increases by more than 10% from its initial value.



-> Memory leak will be detected as memory usage continuously increased over 24hours (by default), and it increased more than 10% from its initial value.

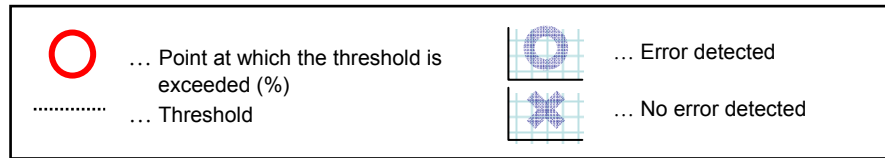
- ◆ In the following example, memory usage increases and decreases, but remains within a set range.



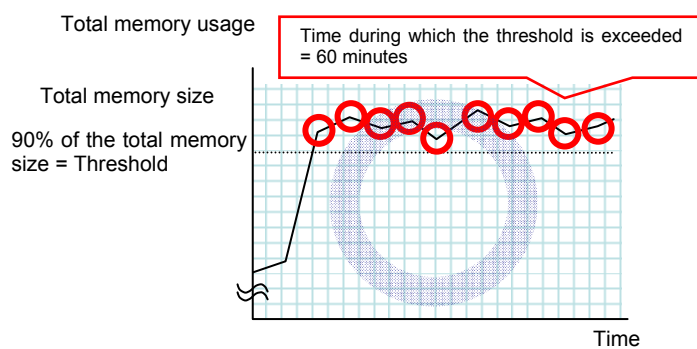
-> Memory leak will not be detected as memory usage repeat increasing and decreasing within certain range (below specific value).

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.

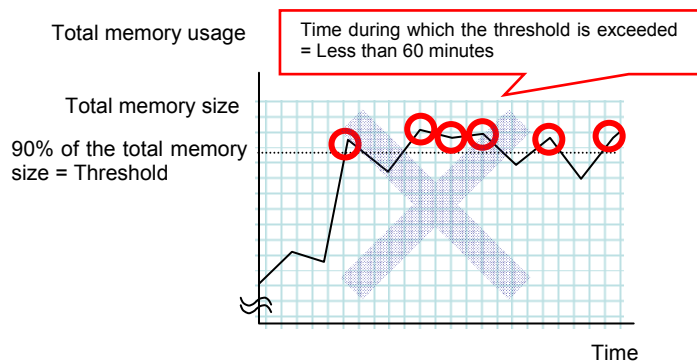


- ◆ The total memory usage remains at the total memory usage threshold or higher as time passes, for at least a certain duration of time.



→ 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.



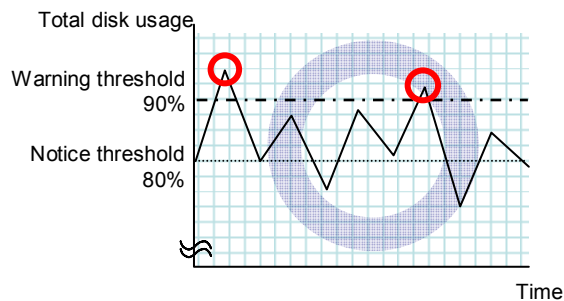
→ The total memory usage is temporarily at the total memory usage threshold (90%) or higher, but goes below the threshold before it remains at the threshold or higher continuously for the monitoring duration time (60 minutes); no total memory usage error is detected.

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.

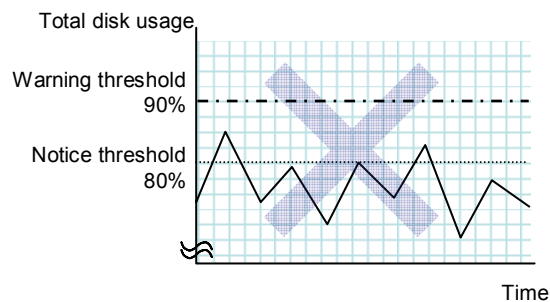
**Monitoring disk usage by warning level**

- ◆ In the following example, disk usage exceeds the threshold which is specified as the warning level upper limit.



-> Disk usage error will be detected as disk usage exceeds the threshold which is configured as warning level upper limit.

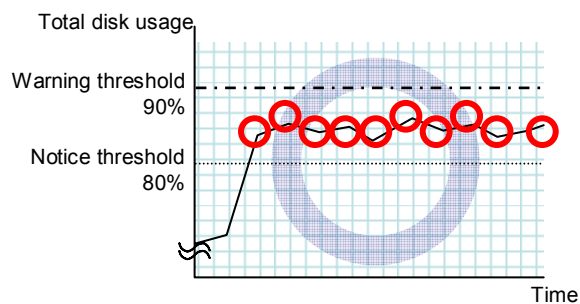
- ◆ In the following example, disk usage increases and decreases within certain range, and does not exceed the threshold which is specified as the warning level upper limit.



-> Disk usage error will not be detected as disk usage repeats increasing and decreasing within certain range (below warning level upper limit).

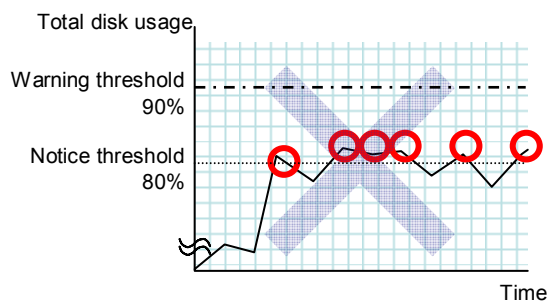
**Monitoring disk usage by notice level**

- ◆ In the following example, disk usage continuously exceeds the threshold specified as the notification level upper limit, and the duration exceeds the set length.



-> Disk usage error will be detected as disk usage continuously exceeds notice level upper limit.

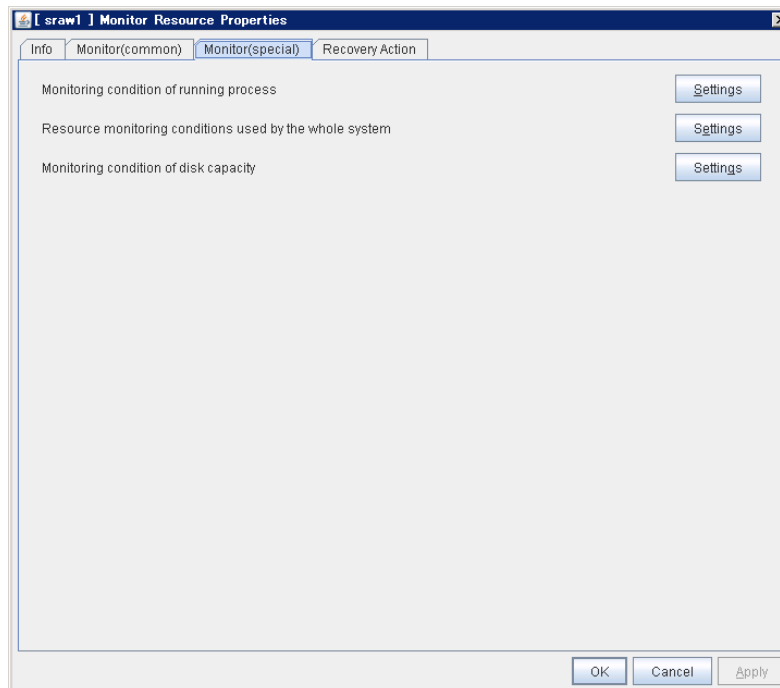
- ◆ In the following example, disk usage increases and decreases within a certain range, and does not exceed the threshold specified as the notification level upper limit.



-> Disk usage error will not be detected as disk usage repeat increasing and decreasing around notice level upper limit.

## Displaying and changing the system monitor resource details

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; the following pop-up dialog box appears. Configure detailed settings for the monitoring of error detection according to the following descriptions.

Click the **Settings** button for **Process detail settings**; the process settings dialog box appears.

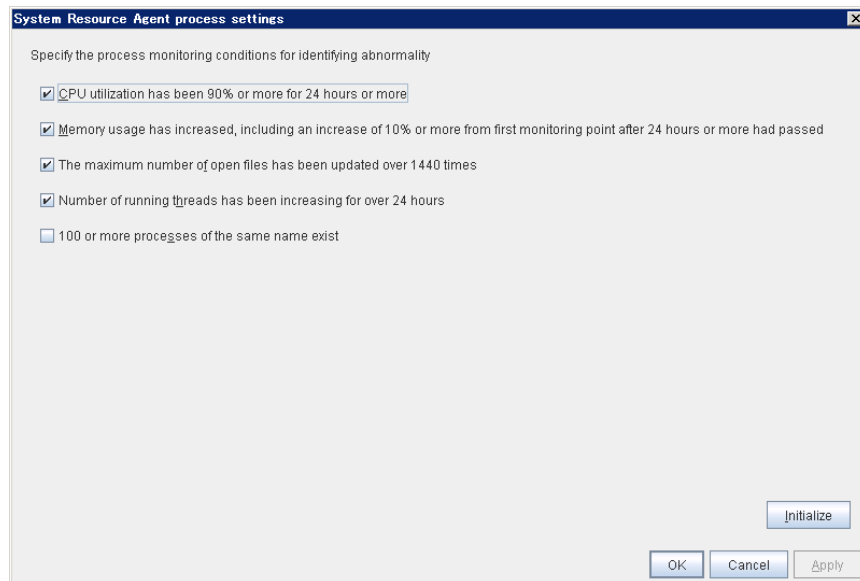
Click the **Settings** button for **Resource monitoring conditions used by the whole system**; the system settings dialog box appears.

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 1440 times**

Enables the monitoring of processes for which the maximum number of open files has been exceeded over 1440 times.

- ◆ When selected:  
Monitoring is enabled for processes for which the maximum number of open files has been exceeded over 1440 times.
- ◆ When cleared:  
Monitoring is disabled for processes for which the maximum number of open files has been exceeded over 1440 times.

**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.

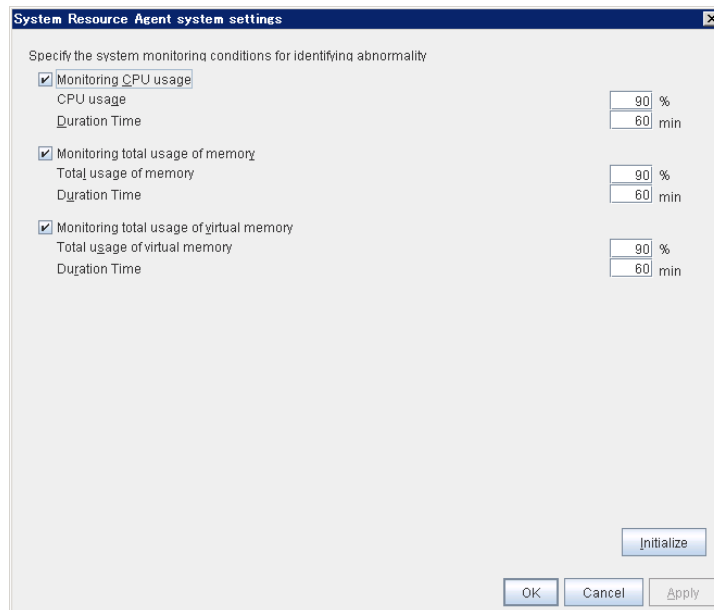
- ◆ When selected:  
Monitoring is enabled for processes for which the number of running threads has been increasing for over 24 hours.
- ◆ When cleared:  
Monitoring is disabled for processes for which the number of running threads has been increasing for over 24 hours.

**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 (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)**

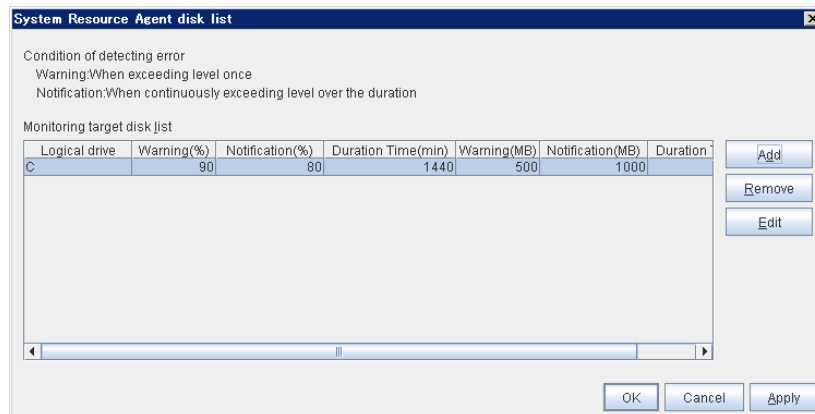
Specify the threshold for the detection of a virtual memory usage error.

### **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.

## System Resource Agent disk list



### Add

Click this to add disks to be monitored. The **Input of watch condition** dialog box appears.

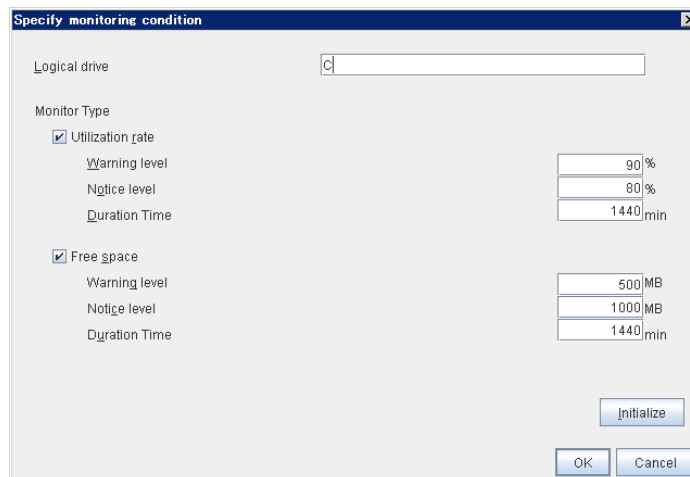
Configure the detailed monitoring conditions for error determination, according to the descriptions given in the **Input of watch condition** dialog box.

### 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**.



### Logical drive

Set the logical drive to be monitored.

### Utilization 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.

# Chapter 6      Other setting details

This chapter provides details about the other items to be specified for ExpressCluster X SingleServerSafe.

This chapter covers:

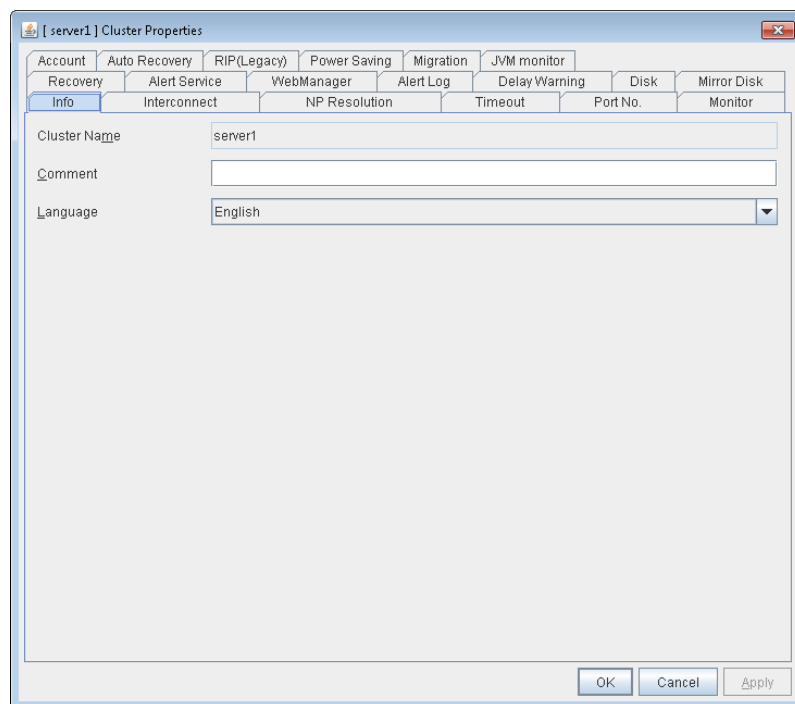
Cluster properties .....	232
Server properties .....	268

## 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.



#### Cluster 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



## Port No. tab

Specify TCP port numbers and UDP port numbers.

### TCP

No TCP port numbers can be overlapped.

- **Server Internal Port Number** (1 to 65,535 <sup>1</sup>)  
This port number is used for internal communication.
- **Data Transfer Port Number** (1 to 65,535 <sup>1</sup>)  
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 <sup>1</sup>)  
This port number is used for a browser to communicate with the ExpressCluster Server.
- **Disk Agent Port Number** (1 to 65,535 <sup>1</sup>)  
Not used.
- **Mirror Driver Port Number** (1 to 65,535 <sup>1</sup>)  
Not used.

### UDP

No UDP port numbers can be overlapped.

- **Kernel Mode Heartbeat Port Number** (1 to 65,535 <sup>1</sup>)  
This port number is used for the kernel mode heartbeat.
- **Alert Sync Port Number** (1 to 65,535 <sup>1</sup>)  
This port number is used to synchronize alert messages.

<sup>1</sup> It is strongly recommended not to use well-known ports, especially reserved ports from 1 to 1,023.  
Section III Resource details

### **TCP/UDP**

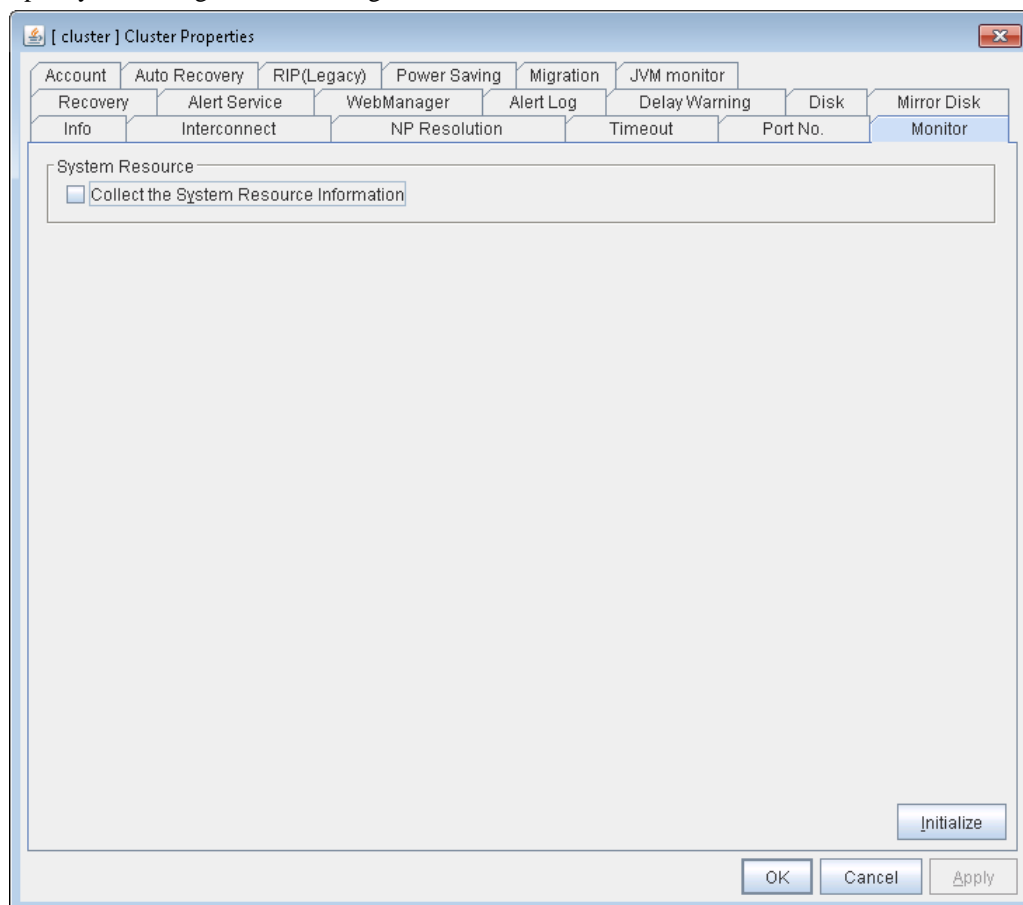
- **Client Service Port Number** (1 to 65,535 <sup>1</sup>)  
This port number is used for the client service.

### **Initialize**

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

## Monitor tab

Specify the settings for monitoring.



### System Resource

Select whether to collect system resource information.

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

- When the check box is selected

System resource information related to the CPU, memory, processes, and others is collected regularly while the cluster is running.

The collected system resource information is collected when the `clplogcc` command or WebManager collects logs.

Specify type 1 to collect the log by the `clplogcc` command; specify Pattern 1 to collect the log by the WebManager. For details on log collection, see “Collecting logs (`clplogcc` command)” in Chapter 2, “ExpressCluster X SingleServerSafe command reference” and “Collecting logs by using the WebManager” in Chapter 1, “Functions of the WebManager” in the *ExpressCluster X SingleServerSafe Operation Guide*.

A disk area of 450 MB or more is required to store the resource information, depending on the system operating conditions such as the number of processes that are running.

- When the check box is not selected  
No system resource information is collected.

## Recovery tab

Specify the settings for recovery.

### Reboot Limitation

You can specify the **Reboot OS** or **Shut down OS** as the final action at abnormality detection for group resources and monitor resources. If either of them is selected, reboot may be repeated infinitely. By setting the reboot limit, you can prevent repeated reboots.

#### ◆ Max Reboot Count (0 to 99)

Specify how many times the operating system can reboot. The number specified here is separately counted for group resource and monitor resource.

#### ◆ Max Reboot Count Reset Time (0 to 999)

When the max reboot count is specified, if the operation keeps running normally for the time specified here, the reboot count is reset. The time specified here is separately counted for group resource and monitor resource.

#### Note:

If **Max Reboot Count** is set to 1 or greater, set **Max Reboot Count Reset Time** also to 1 or greater. If the time to reset the maximum reboot count is set to zero (0), the number of reboot will be unavailable, thus, shutdown/reboot are executed every time at failure detection regardless of the maximum reboot count.

### 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.

**Action When the Cluster Service Process Is Abnormal**

Specify an action at process abnormality of the cluster service.

- ◆ Shut down the OS  
Shut down the OS.
- ◆ Generate an intentional stop error  
Generate a stop error (Panic) intentionally and restart the server.
- ◆ Reset the hardware  
Restart the server by HW reset.

**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.
  - 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 resource, JVM monitor resource, and system resource information collection function.

---

**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 triggered by monitor resource error is not performed. Even if this function is enabled, recovery from a group resource activation failure will still be performed.

---

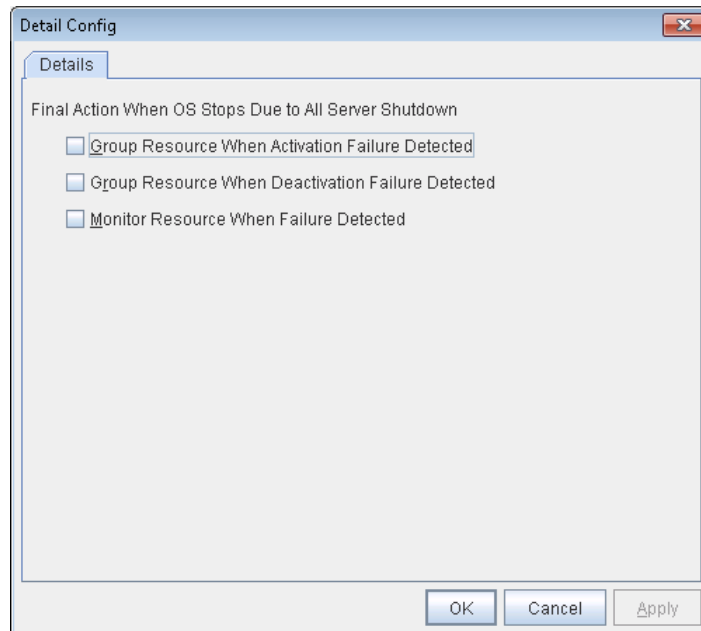
---

This function is not enabled by the stall detection function of the disk RW 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 if all other servers are stopped.

#### Group Resource When Deactivation Failure Detected

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

#### Monitor Resource When Failure Detected

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

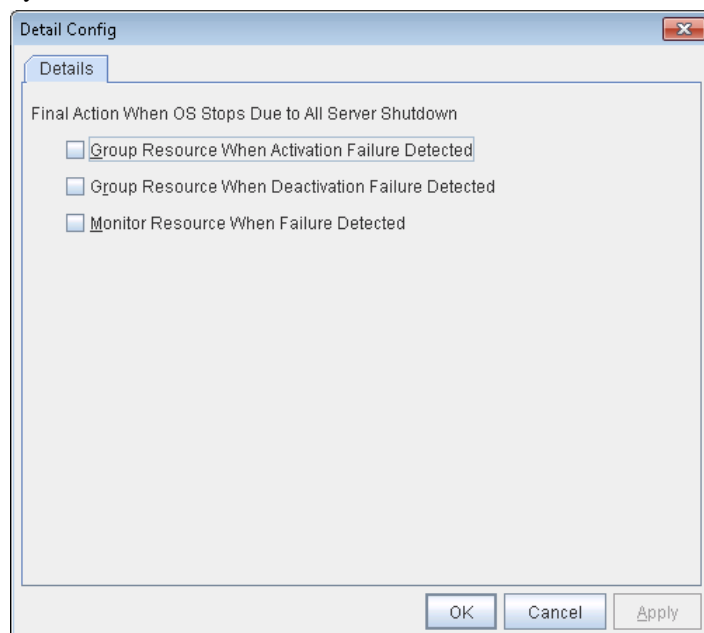
---

#### Note:

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

### Disable the Final Action when OS Stops Due to Failure Detection

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



#### Group Resource When Activation Failure Detected

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

#### Group Resource When Deactivation Failure Detected

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

#### Monitor Resource When Failure Detected

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



**Note:**

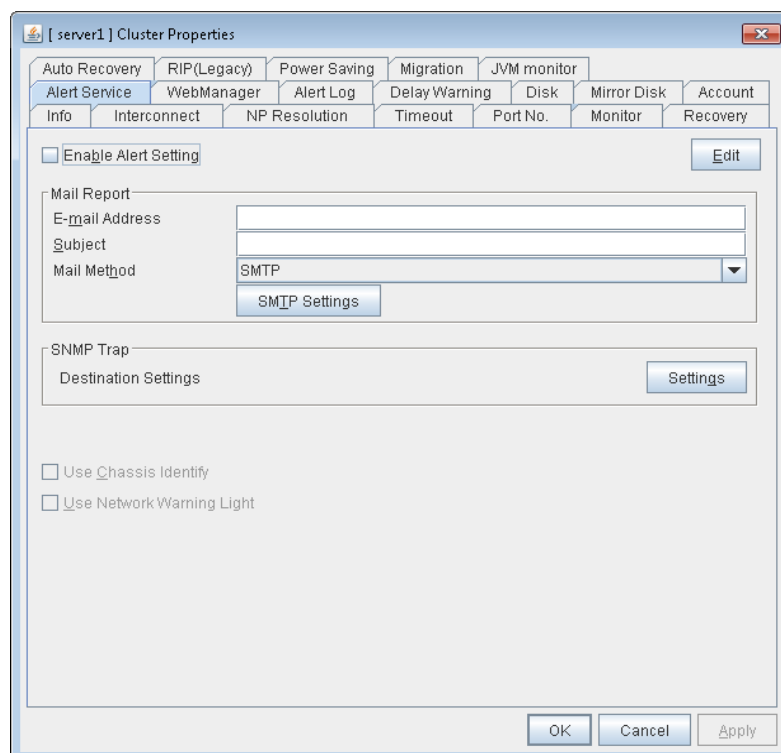
- If errors were detected on multiple servers almost at the same time, and the final action was taken for those servers, the final action which accompanies the OS stop may be taken for all the servers even if the final action caused by an error detection in a monitor resource is set to be suppressed.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

## Alert Service tab

Specify the alert service, chassis identify, and network warning light.

### Note:

To use the mail alert function, obtain ExpressCluster X Alert Service 3.1 for Windows, and register the 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 default settings of the destination address, see "Messages reported by event log and alert" in Chapter 5, "Error 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. In this version, SMTP is the only option in this.

- ◆ SMTP  
Sends the alert by directly communicating with the SMTP server.

### Destination Settings

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

### Use Chassis Identify

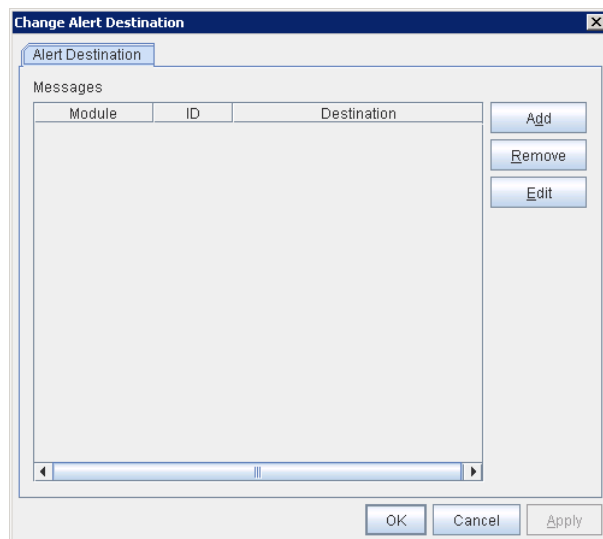
Not used.

### Use Network Warning Light

Not used.

### Change Alert Destination

Select **Edit** to display the dialog box where you can change alert destination.



**Add**

Add the alert ID of the destination which you want to customize. Click **Add** to open the dialog box for entering the message.

Enter the message

Message

Category: Process

Module Type: apisv

Event ID:

Destination

Send	Destination
<input type="checkbox"/>	WebManager.AlertLog
<input type="checkbox"/>	Alert Extension
<input type="checkbox"/>	Mail Report
<input type="checkbox"/>	SNMP Trap
<input type="checkbox"/>	EventLog(DisableOnly)

Command:

Add Remove Edit

OK Cancel

**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 message ID of the module type for which you want to change the destination. For the message ID, see "Messages reported by event log and alert" in Chapter 7, "Error messages" in the *Operation Guide*.

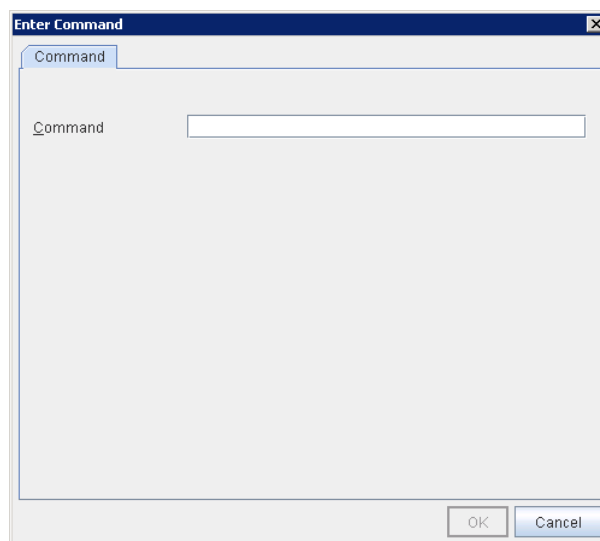
### Destination

Select a message destination from the following options.

- **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.
- **EventLog (DisableOnly)**  
Disables the settings for the OS to report logs to the event log. You cannot configure the settings to report messages that are not reported to event logs.)
- **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.



### Command (within 511 bytes)

Enter any command you want to use.

- **Keyword**  
If you specify %%MSG%%, the message of the target event ID is inserted.  
You cannot specify multiple %%MSG%% for one command.  
Configure the command within 511 bytes including the description of %%MSG%%.  
The string %%MSG%% may include a space. If you specify it as an argument for a command, add backslashes (\) and double quotation marks ("), as in \%%MSG%%".

**Remove**

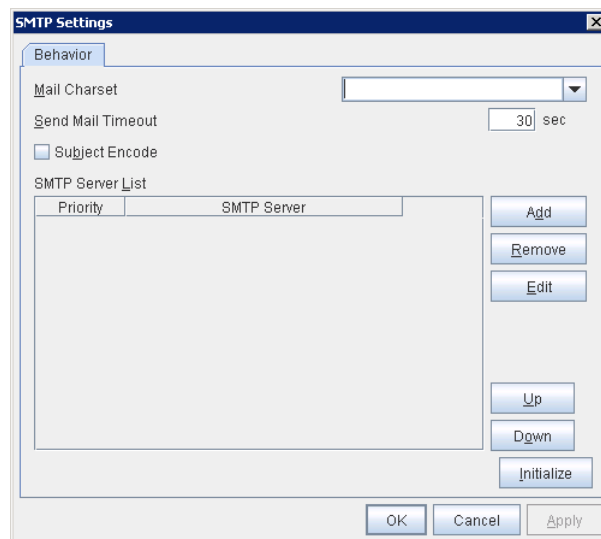
Click this to remove a command of the alert extension function. Select the command, and then, click **Remove**.

**Edit**

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

**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**

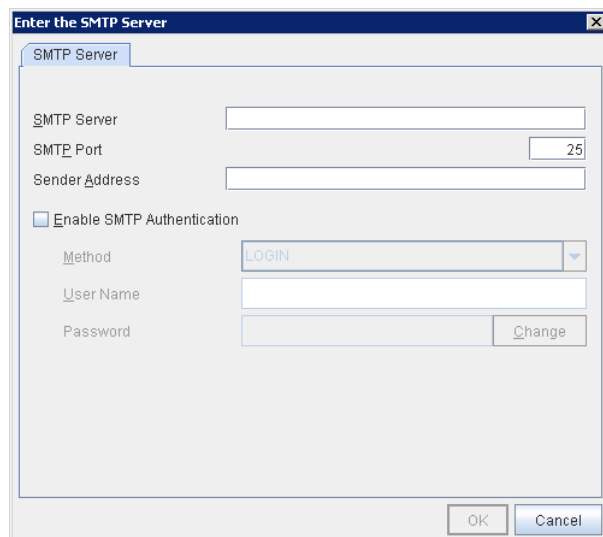
Configure whether or not to encode the subject of e-mails.

**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.



**SMTP Server** (within 255 bytes)

Configure the IP address 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.

**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.

### Remove

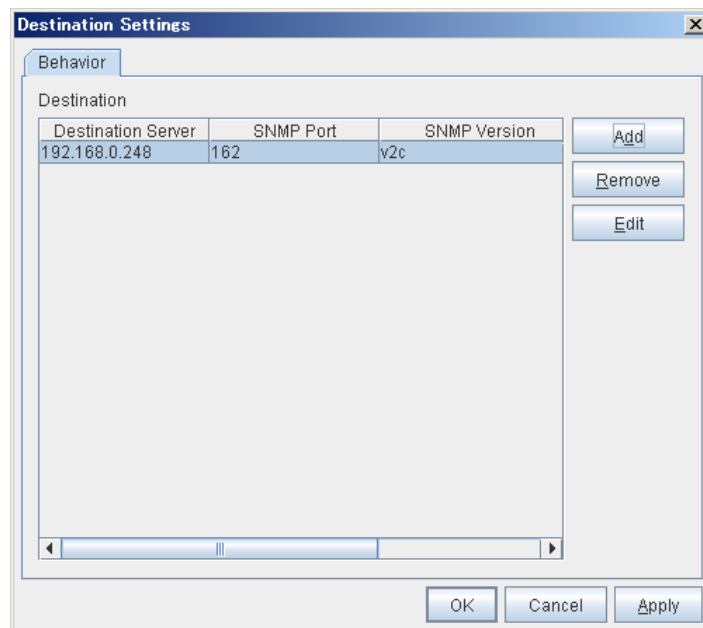
Select this to remove the SMTP server.

### Edit

Use this button to modify the settings of SMTP server.

### SNMP Settings

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



### Destination

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

### Add

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

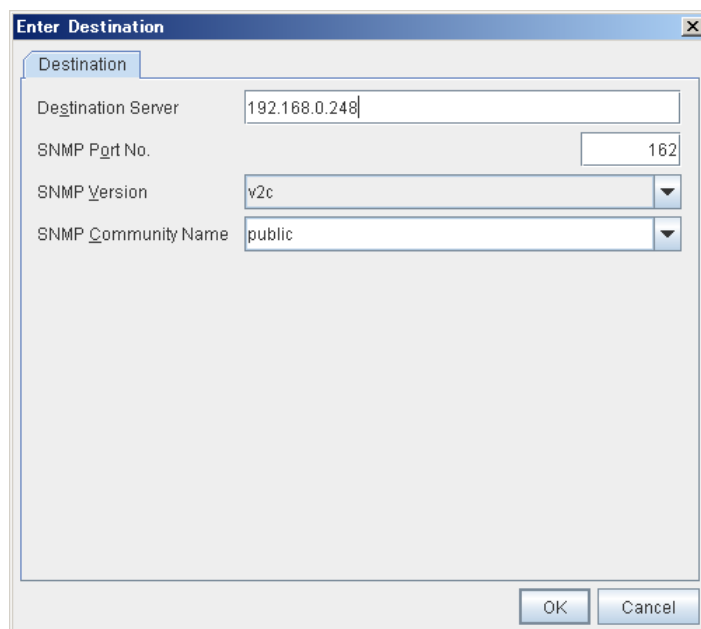
### Remove

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



**Edit**

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

A screenshot of a Windows-style dialog box titled "Enter Destination". It has a tab labeled "Destination". Inside the dialog, there are four fields: "Destination Server" with the text "192.168.0.248", "SNMP Port No." with the value "162", "SNMP Version" with a dropdown menu showing "v2c", and "SNMP Community Name" with a dropdown menu showing "public". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Destination	
Destination Server	192.168.0.248
SNMP Port No.	162
SNMP Version	v2c
SNMP Community Name	public

**Destination Server (up to 255 bytes)**

Configure the name of the SNMP trap transmission destination server.

**SNMP Port No. (1-65535)**

Configure the port number of the SNMP trap transmission destination.

**SNMP Version**

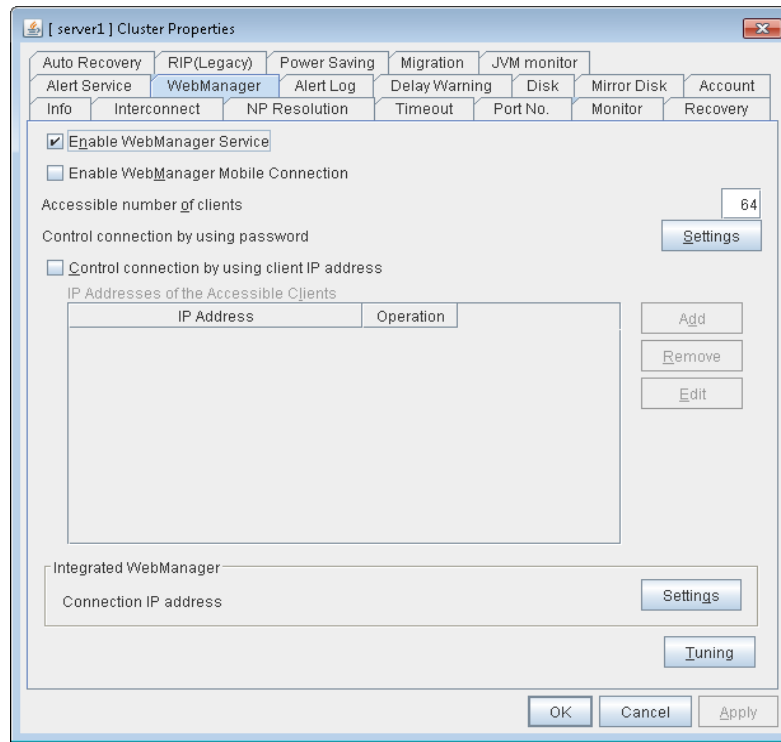
Configure the SNMP version of the SNMP trap transmission destination.

**SNMP Community Name (up to 255 bytes)**

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

## WebManager tab

Specify 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

Enables the mobile WebManager.

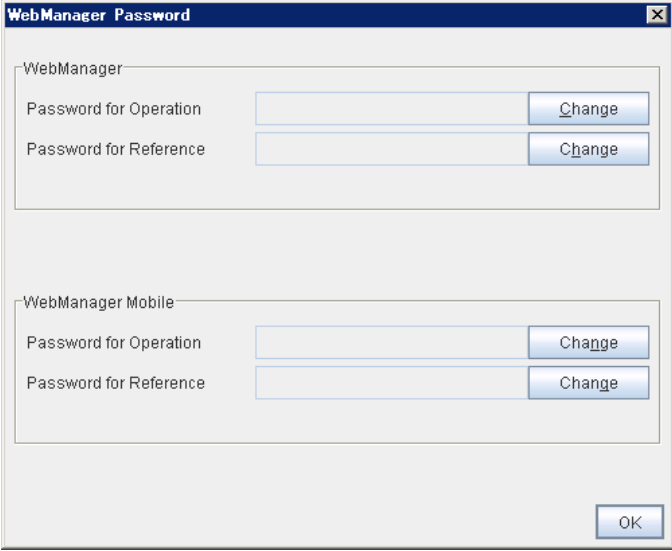
- ◆ When selected:  
The WebManager Mobile is enabled.
- ◆ When cleared:  
The WebManager Mobile is disabled.

### 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.



The **WebManager Password** dialog box contains two sections: **WebManager** and **WebManager Mobile**. Each section has two text input fields: **Password for Operation** and **Password for Reference**. To the right of each field is a **Change** button. At the bottom right of the dialog is an **OK** button.

### WebManager

#### ◆ Password for Operation

Set a password to connect to the WebManager in the 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.

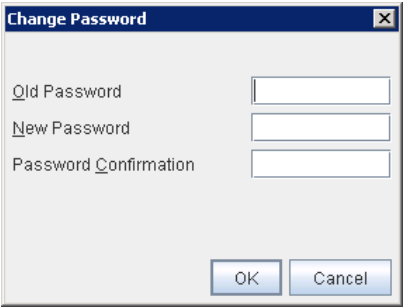
### WebManager Mobile

#### ◆ Password for Operation

Set a password that must be entered to enable connection to the WebManager Mobile in the operation 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 Mobile in the reference mode.  
Click **Change** to display the **Change Password** dialog box.



The **Change Password** dialog box contains three text input fields: **Old Password**, **New Password**, and **Password Confirmation**. At the bottom are **OK** and **Cancel** buttons.

- **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**.

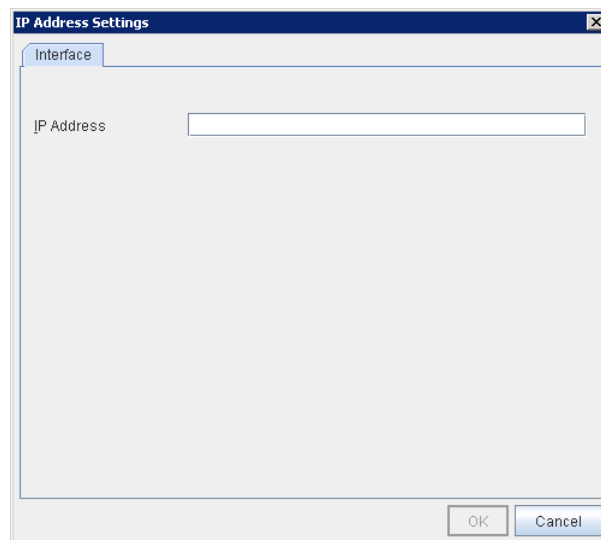
#### Control connection by using client IP address

If selected, accesses are controlled by client IP addresses.

- ◆ When selected:  
**Add**, **Remove** and **Edit** buttons are enabled.
- ◆ When cleared:  
**Add**, **Remove** and **Edit** buttons 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.

### Operation

Specify the operation rights for IP addresses that are registered in **IP Addresses of the Accessible Clients**.

◆ When selected:

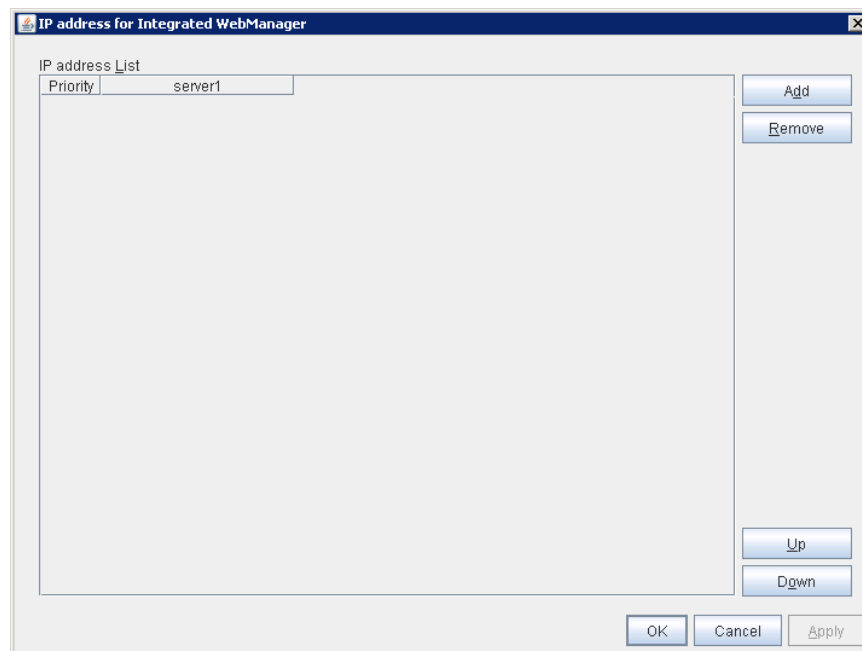
A client can operate ExpressCluster X SingleServerSafe and display its status.

◆ 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 server and select or enter IP address for the IP address of server.

◆ **Remove**

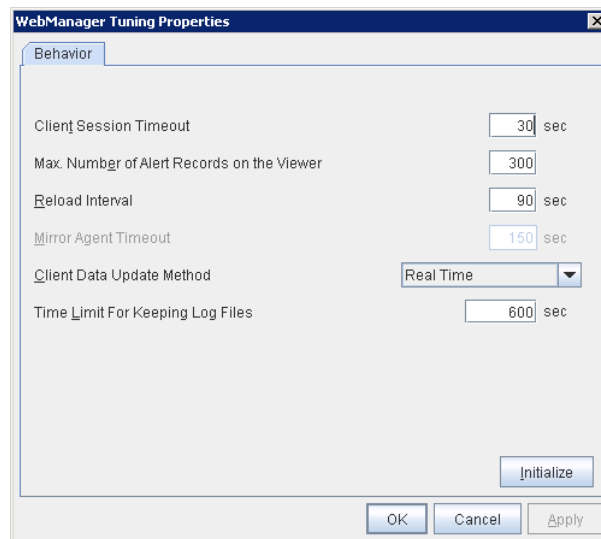
Remove the communication path. Select the communication path to be removed and click **Remove**, then the selected path is removed.

◆ **Up, Down**

When configuring more than one IP addresses for the Integrated WebManager, the communication path with smaller number of **Priority** column is used preferentially for the control communication. 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 the Viewer** (1 to 999)

Specify the maximum number of alert viewer records to display on the Alert Viewer of the WebManager.

- ◆ **Reload Interval** (0 to 999)

At this time interval, the WebManager screen is refreshed.

- ◆ **Mirror Agent Timeout** (1 to 999)

Not used.

- ◆ **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)

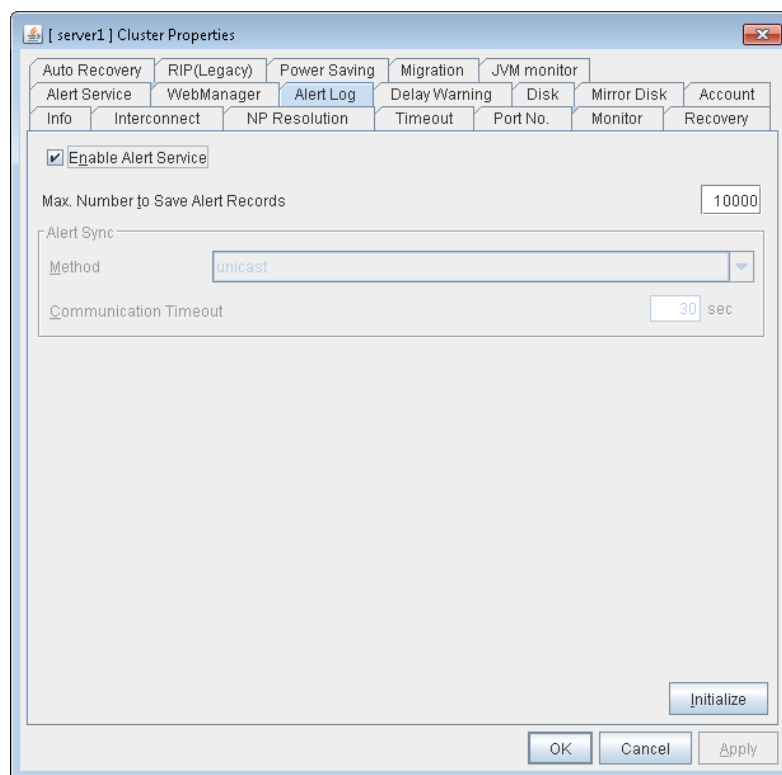
Time limit determines when the log collection information temporarily saved on the server will be deleted. When the time specified here has elapsed, the log collection information will be deleted unless you save the file when the dialog box asking you if you save the log collection information is displayed.

- ◆ **Initialize**

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

## Alert Log tab

Specify the settings for the alert log.



### Enable Alert Service

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

- ◆ When selected:  
ExpressCluster Web Alert service is enabled.
- ◆ When cleared:  
ExpressCluster Web Alert service is disabled.

### Max. Number to Save Alert Records (1 to 99,999)

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

### Alert Sync: Method

Not used.

### Alert Sync: Communication Timeout (1 to 300)

Not used.

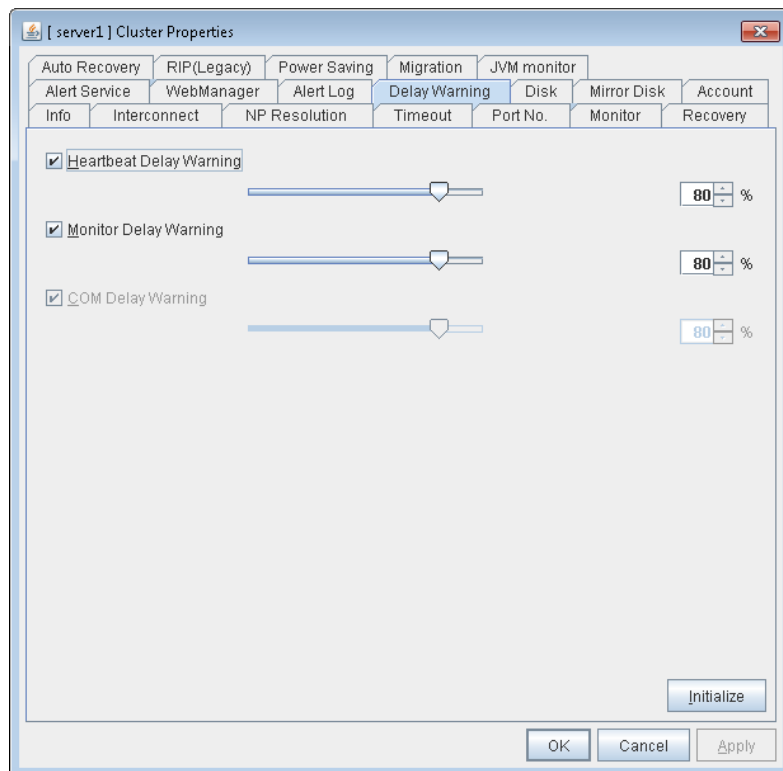
### Initialize

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



## Delay Warning tab

Specify the settings for **Delay Warning** on this tab. For details about **Delay Warning**, see “Monitoring details” in “Chapter 7”.



### Heartbeat Delay Warning (1 to 99)

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.

### Monitor Delay Warning (1 to 99)

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.

### COM Delay Warning (1 to 99)

Not used.

### Initialize

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

### Note:

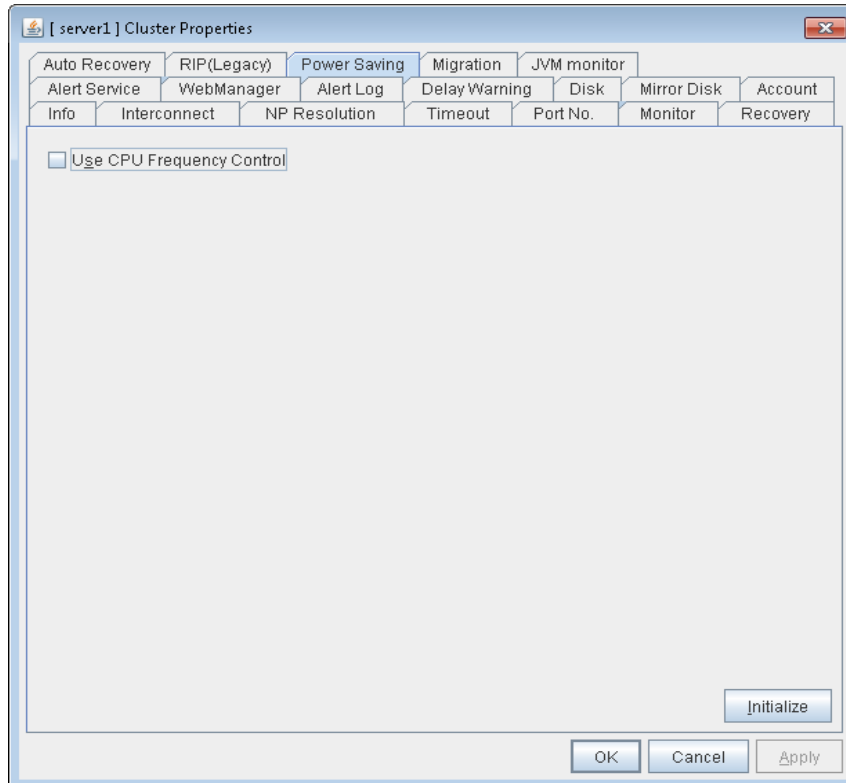
If you specify 0% for the delay warning, an alert log is shown in every heartbeat interval and monitor interval.

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.

## Power Saving tab

Specify 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. If you uncheck the checkbox, CPU frequency control is disabled.

### Initialize

This operation is used to return the value to the default value.

---

### Related Information:

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

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 using the command or the WebManager are discarded after stop/start or suspend/resume and that the CPU frequency is controlled by ExpressCluster X SingleServerSafe.

---

---

### Note:

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

---

**Note:**

If you disable CPU frequency control function with CPU frequency changed, the CPU frequency does not return to the state before changing. In this case, return the CPU frequency to the defined value by the following way.

Windows Server 2003:

Execute the following command at a command prompt.

```
# powercfg /X "always on" /processor-throttle-ac none
```

The character string to be specified with /X option is the name selected in the current setting of [Power Options] -> [Power Schemes] in [Control Panel].

Windows Server 2008:

Select [Balanced] in [Power Options] -> [Select a power plan] in [Control Panel].

---

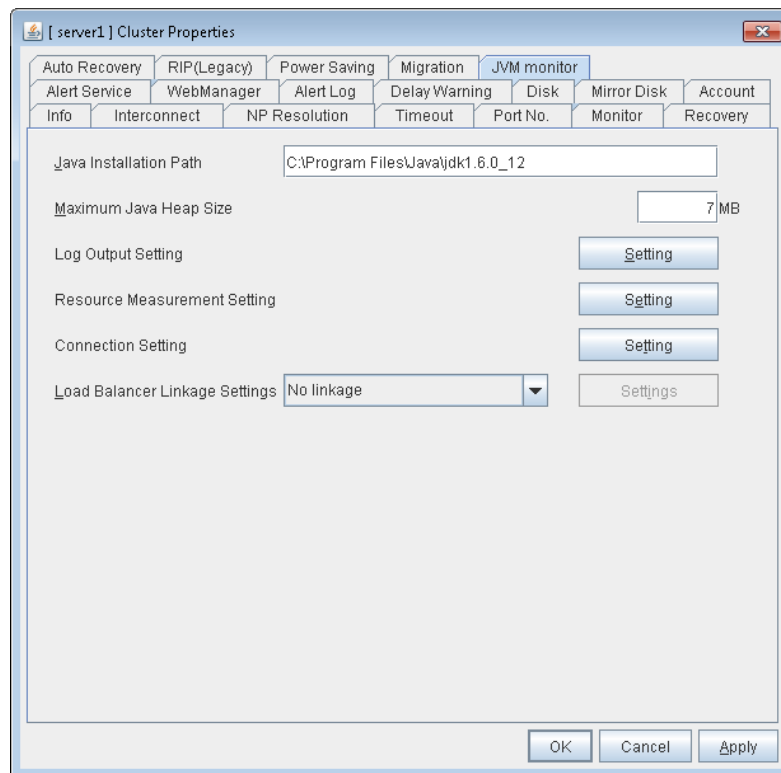
## JVM monitor tab

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. Specification example: C:\Program Files\Java\jre6

### 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 the Oracle Java, specify a value equal to or larger than 7.

### Log Output Setting

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

### Resource measurement Setting

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

### Connection Setting

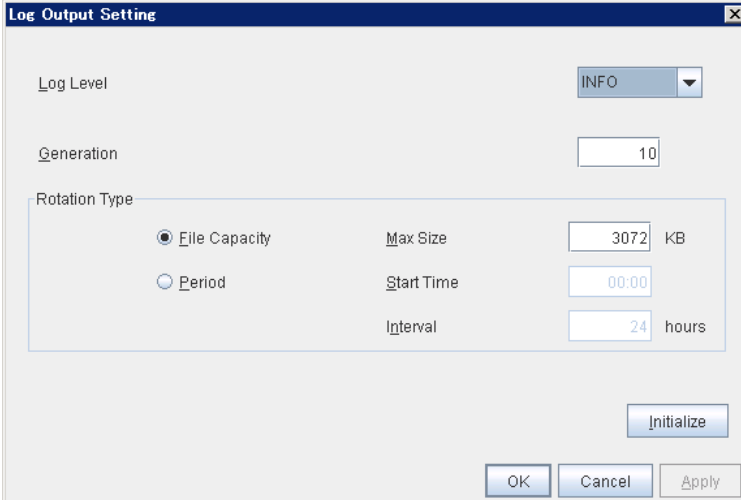
Click the **Setting** button to open the **Connection Setting** dialog box.

**Load Balancer Linkage Settings**

Click the **Setting** button to open the **Load Balancer Linkage Settings** dialog box.

### Log Output Setting

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

The image shows a Windows-style dialog box titled "Log Output Setting". It contains several configuration fields: "Log Level" is a dropdown menu currently set to "INFO"; "Generation" is a text input field containing the number "10"; "Rotation Type" is a section with two radio buttons, "File Capacity" (which is selected) and "Period"; under "File Capacity", there is a "Max Size" field set to "3072 KB"; under "Period", there is a "Start Time" field set to "00:00" and an "Interval" field set to "24 hours". At the bottom right of the dialog is an "Initialize" button. At the very bottom are three buttons: "OK", "Cancel", and "Apply".

#### Log Level

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

#### Generation (2 to 100)

Set the number of generations to be retained for the log output by the JVM monitor.

#### Rotation Type

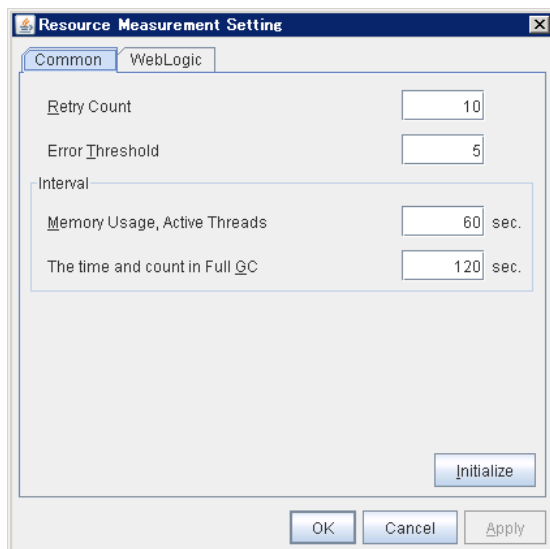
Select a rotation type for the log output by the JVM monitor. If you select **File Capacity** as the rotation type, set the maximum size (200 to 2097151), in kilobytes, for each log file such as the JVM operation log. If you select **Period** as the rotation type, set the log rotation start time in “hh:mm”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

#### Initialize

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

### Resource Measurement Setting [Common]

Clicking **Setting** displays the **Resource Measurement Setting** dialog box. For details on the scheme for error judgment by the JVM monitor, see Chapter 5 , “Monitor resource details”.



#### Retry Count (1 to 1440)

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

#### Error Threshold (1 to 10)

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

#### Memory Usage, Active Threads (15 to 600)

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

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

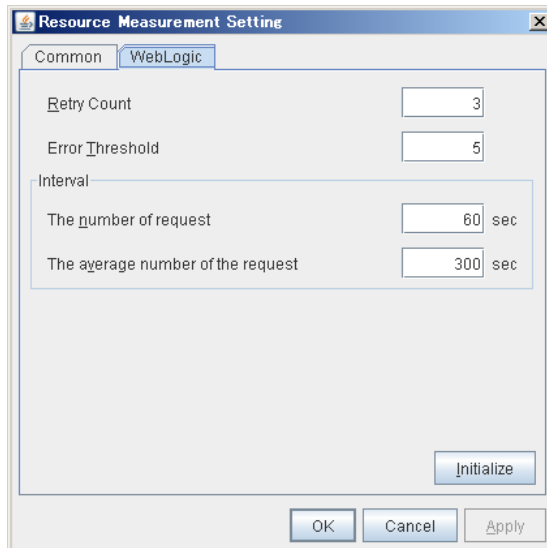
Set the interval at which the JVM monitor measures the time and count in Full GC execution.

#### Initialize

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

**Resource Measurement Setting [WebLogic]**

Clicking **Setting** displays the **Resource Measurement Setting** 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 performed when the usage of the Java VM or the application server resources collected by the JVM monitor via resource measurement continuously exceed the customer-defined threshold.

**The number of request (15 to 600)**

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

**The average number of the request (15 to 600)**

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

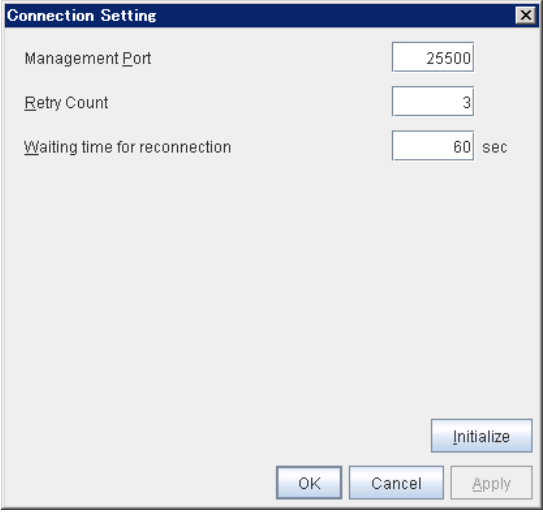
**Initialize**

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



### Connection Setting

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



The **Connection Setting** dialog box contains the following fields and buttons:

- Management Port:** A text box with the value 25500.
- Retry Count:** A text box with the value 3.
- Waiting time for reconnection:** A text box with the value 60, followed by the unit "sec".
- Buttons:** "Initialize", "OK", "Cancel", and "Apply" are located at the bottom right.

#### 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 42424 to 61000.

#### Retry Count for (1 to 5)

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

#### Waiting time for reconnection (15 to 60)

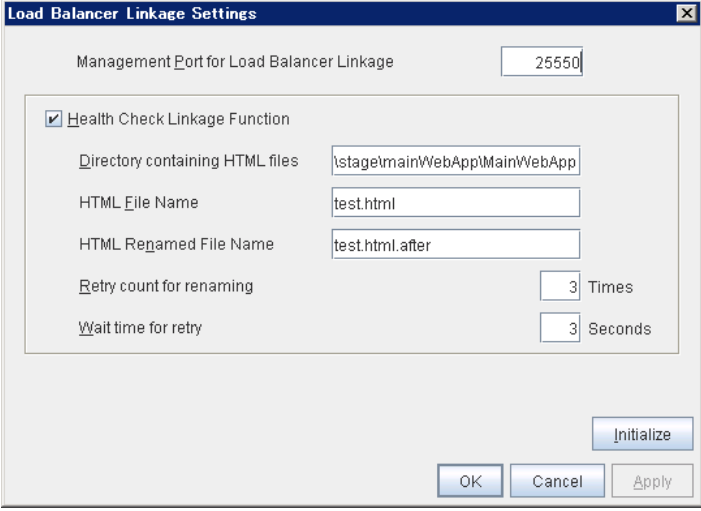
Set the interval at which the JVM monitor retries connection if it fails in Java VM connection.

#### Initialize

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

### Load Balancer Linkage Settings

Clicking **Setting** displays the **Load Balancer Linkage Settings** dialog box.



The **Load Balancer Linkage Settings** dialog box contains the following fields and buttons:

- Management Port for Load Balancer Linkage:** A text box with the value 25550.
- Health Check Linkage Function:** A checked checkbox.
- Directory containing HTML files:** A text box with the value `\stage\mainWebApp\MainWebApp`.
- HTML File Name:** A text box with the value `test.html`.
- HTML Renamed File Name:** A text box with the value `test.html.after`.
- Retry count for renaming:** A text box with the value 3, followed by the unit "Times".
- Wait time for retry:** A text box with the value 3, followed by the unit "Seconds".
- Buttons:** "Initialize", "OK", "Cancel", and "Apply" are located at the bottom right.

**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.

**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 255 bytes)

Set the directory in which the HTML file used by the load balancer health check function is stored.

**HTML File Name**(up to 255 bytes)

Set the HTML file name used by the load balancer health check function.

**HTML Renamed File Name**(up to 255 bytes)

Set the HTML renamed file name used by the load balancer health check function.

**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 retry interval 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.

Load Balancer Linkage Settings

Management Port for Load Balancer Linkage: 25550

mgmt IP address:

User Name: admin

Password: [Change]

Communications Port: 443

List of IP address of distributed nodes

Server Name	IP address

[Add] [Remove]

[Initialize]

[OK] [Cancel] [Apply]

**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.

**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.

**Communications Port**(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 computer name. For the IP address, specify the value set to **Members** in **LocalTraffic - 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 add, remove, and edit interfaces, such as IP addresses and devices, that are used by the server. From the aspect of network environment, IP addresses have the following restrictions:

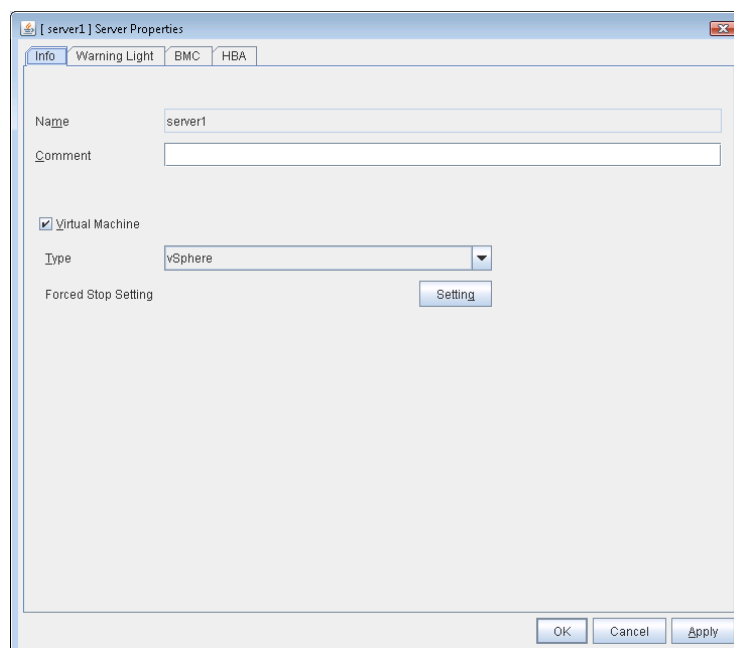
- One server cannot have two or more IP addresses that belong to the same network address. Likewise, containment is not allowed as follows.

IP address: 10.1.1.10, Subnet mask: 255.255.0.0

IP address: 10.1.2.10, Subnet mask: 255.255.255.0

## 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, 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.

## **HBA tab**

Not used.

# Section IV    How monitoring works

This section provides details about how monitoring with ExpressCluster X SingleServerSafe works

Chapter 7        Monitoring details





# Chapter 7      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:

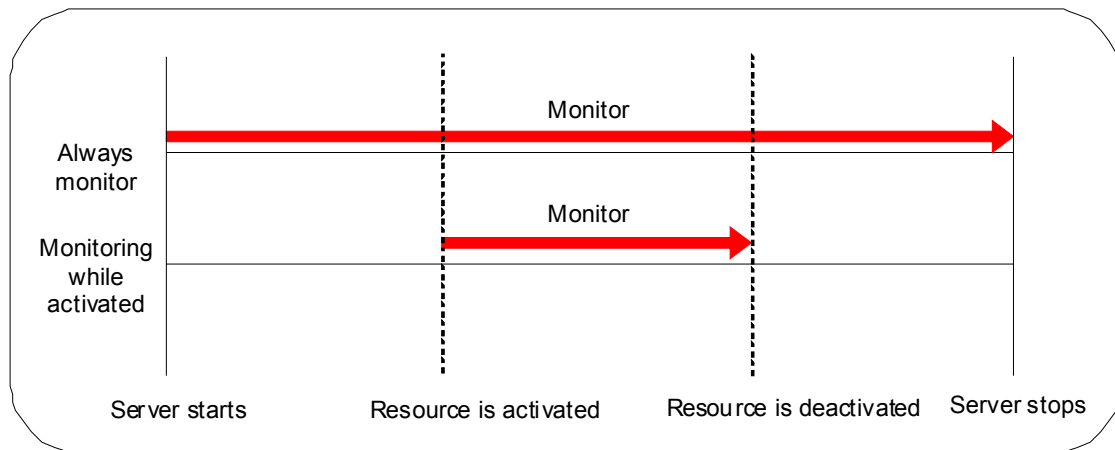
Always monitor and Monitors while activated .....	274
Enabling and disabling Dummy failure of monitor resources .....	275
Monitor resource monitor interval.....	276
Action when an error is detected by a monitor resource .....	281
Recovering from a monitor error (normal) .....	282
Activation or deactivation error for the recovery target during recovery.....	282
Recovery/pre-recovery action script.....	283
Delay warning of a monitor resource .....	286
Waiting for a monitor resource to start monitoring.....	288
Limiting the reboot count for error detection by a monitor resource .....	291

## 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 resource is activated (until that resource is deactivated (stopped)).

Some monitor resources have a fixed monitor timing, while others allow you to choose between two monitor timing options.



## 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, refer to 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 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 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

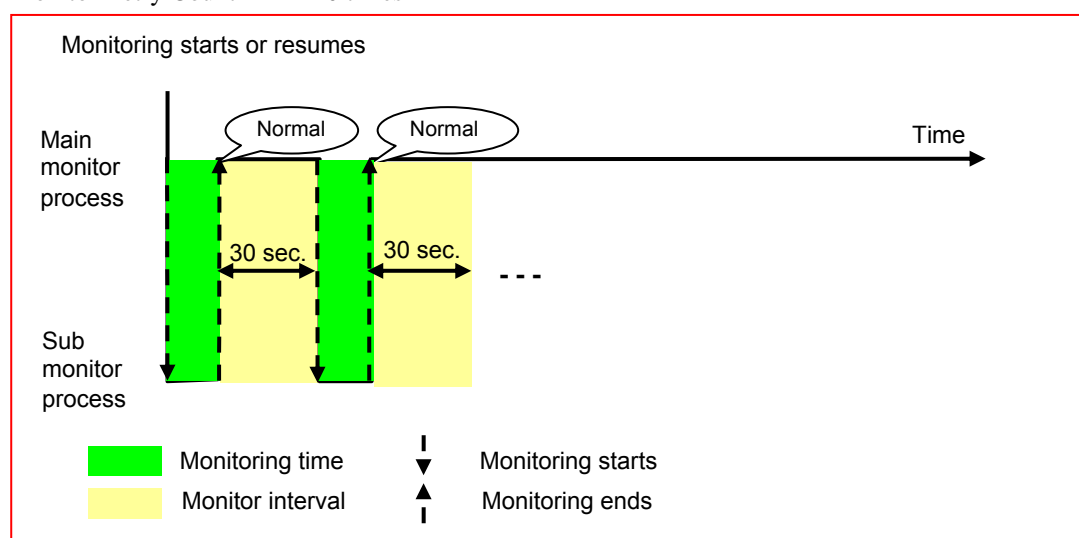
Examples of behavior when the following values are set.

<Monitor>

Monitor Interval 30 sec

Monitor Timeout 60 sec

Monitor Retry Count 0 times



**When an error is detected (without monitor retry setting)**

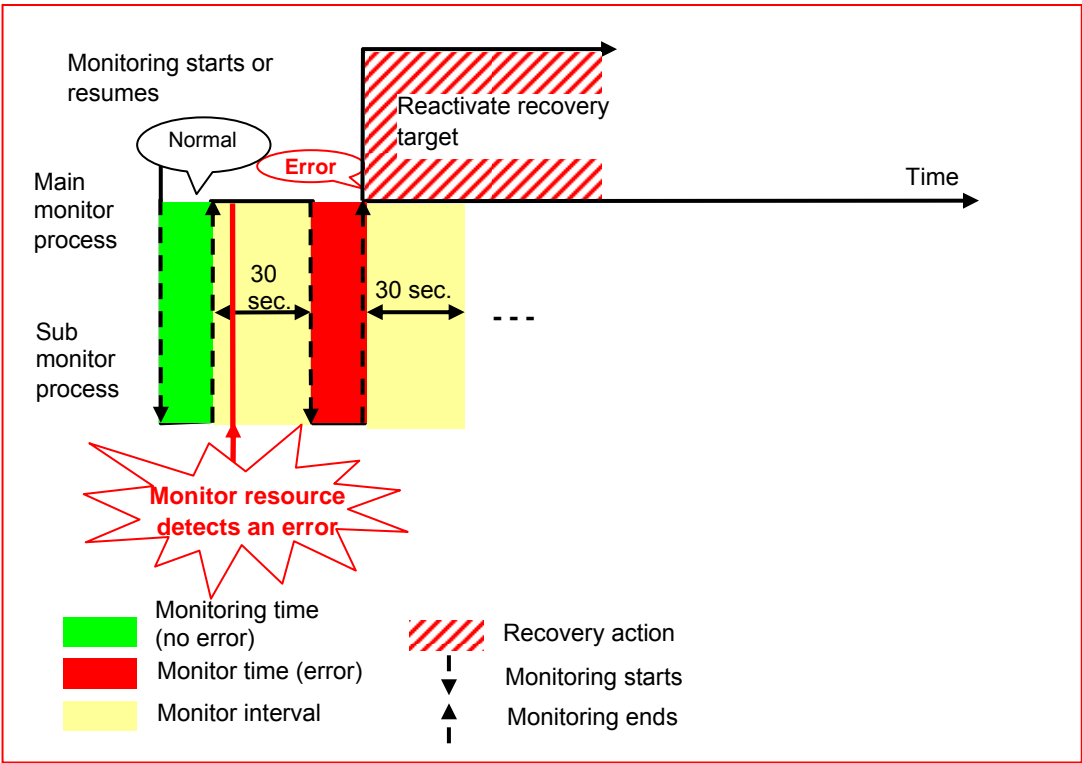
Examples of behavior when the following values are set.

<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	0 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)**

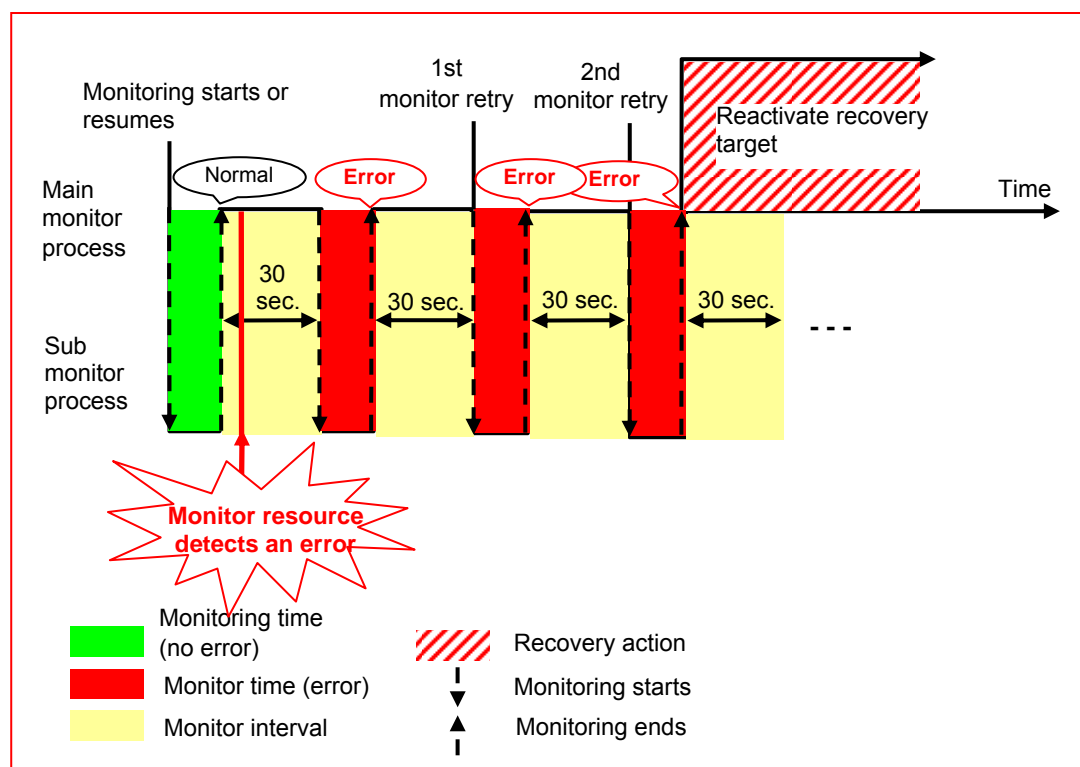
Examples of behavior when the following values are set.

## &lt;Monitor&gt;

Monitor Interval	30 sec
Monitor Timeout	60 sec
Monitor Retry Count	2 times

## &lt;Error Detection&gt;

Recovery Action	Restart the recovery target
Recovery Target	Group
Recovery Script Execution Count	0 time
Reactivation Threshold	0 time
Final Action	No Operation



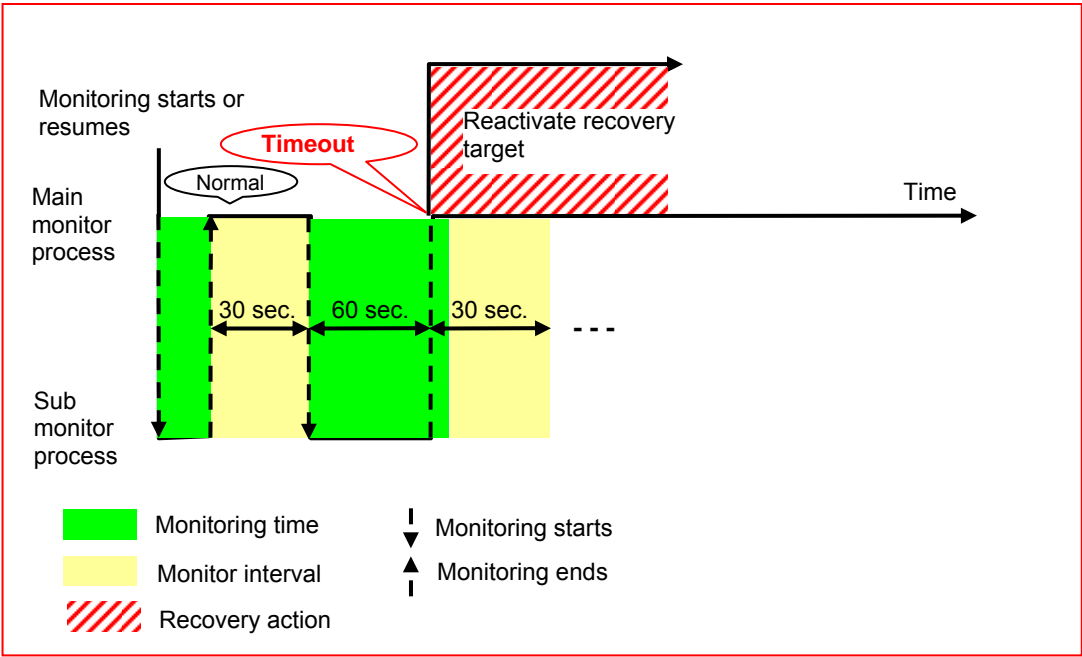
After an error occurs, it is detected next time monitoring is performed, and then, if recovery cannot be achieved before the monitor retry count is reached, the recovery target is reactivated.

**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            0 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 times

<Error Detection>

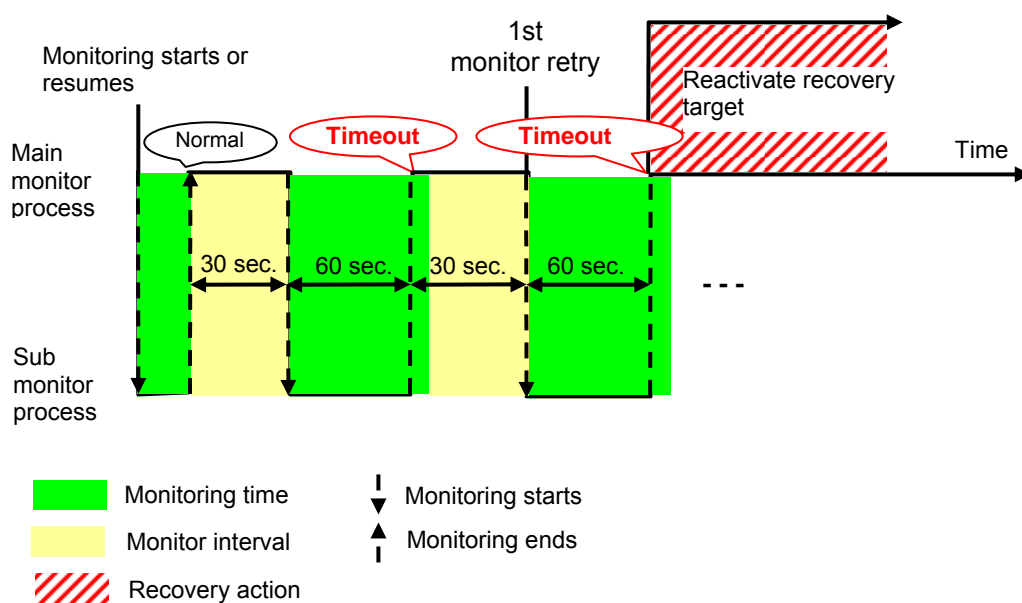
Recovery Action Restart the recovery target

Recovery Target Group

Recovery Script Execution Count 0 time

Reactivation Threshold 0 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 the recovery script: this takes place when an error is detected in a monitor target.
- ◆ Reactivation of the recovery target: this takes place if the recovery script is executed up to the recovery script execution count. When the execution of a pre-reactivation script is specified, reactivation starts after that script has been executed.
- ◆ 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 <sup>2</sup>	Final Action <sup>3</sup>
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 -> last operation), if a group resource (an application resource, service resource, or other resource) is specified as a recovery target and when a monitor resource detects an error.

- ◆ Stopping/suspending the cluster
- ◆ Starting/stopping/moving 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.

<sup>2</sup> Effective only when the value for the reactivation threshold is set to 1 (one) or greater.

<sup>3</sup> Effective only when an option other than No Operation is selected.

## **Recovering from a monitor error (normal)**

When the recovery of a monitor resource is detected during a recovery action or after all recovery actions are completed following the detection of a monitor error, the counter for the reactivation threshold maintained by that monitor resource is 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.

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 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_ACTION ...Recovery action type	RECOVERY	Execution as a recovery script.
	RESTART	Execution before reactivation.
	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.
CLP_FAILOVERCOUNT ...Failover count	Failover count	Not used.

### Writing recovery/pre-recovery action scripts

This section explains the environment variables mentioned above, using a practical scripting example.

#### Example of a recovery/pre-recovery action script

```
rem *****
rem *           preaction.bat           *
rem *****

echo START

IF "%CLP_ACTION%" == "" GOTO NO_CLP

IF "%CLP_ACTION%" == "RECOVERY" GOTO RECOVERY
IF "%CLP_ACTION%" == "RESTART" GOTO RESTART
IF "%CLP_ACTION%" == "FINALACTION" GOTO FINALACTION
GOTO NO_CLP
```

```
:RECOVERY
echo RECOVERY COUNT : %CLP_RECOVERYCOUNT%
```

*Processing type:*  
Recovery  
*Execution timing of the processing:*  
Recovery action: Recovery script

```
GOTO EXIT
```

```
:RESTART
echo RESTART COUNT : %CLP_RESTARTCOUNT%
```

*Processing type:*  
Pre-reactivation processing  
*Execution timing of the processing:*  
Recovery action: Reactivation

```
GOTO EXIT
```

```
:FINALACTION
echo FINAL ACTION
```

*Processing type:*  
Recovery  
*Execution timing of the processing:*  
Recovery action: Final action

```
GOTO EXIT
```

```
:NO_CLP
```

```
:EXIT
echo EXIT
```

#### Tips for recovery/pre-recovery action script coding

Pay careful attention to the following points when coding the script.

- ◆ When the script contains a command that requires a long time to run, log the end of execution of that command. The logged information can be used to identify the nature of the error if a problem occurs. `clplogcmd` is used to log the information.

**Note on the recovery/pre-recovery action script**

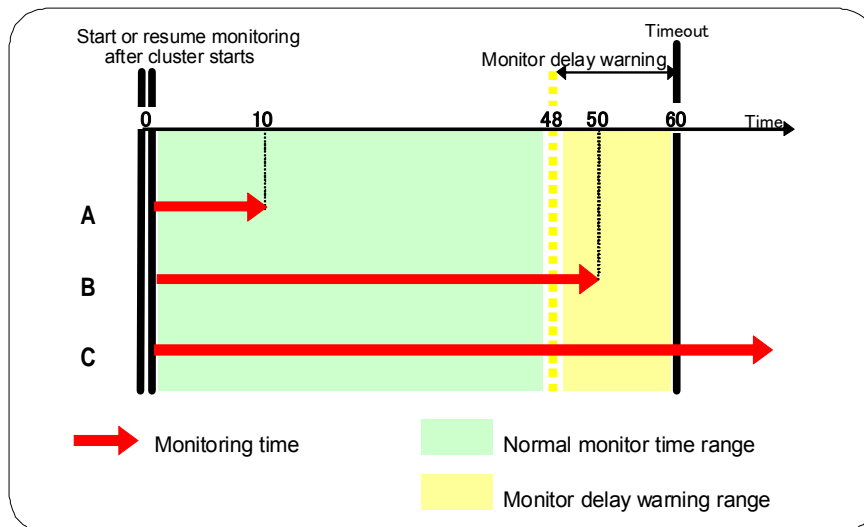
- ◆ None.

## 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 time for monitor processing is 10 seconds. The monitor resource is in normal status. In this case, no alert is used.
- B.** The time for monitor processing is 50 seconds and the delay of monitoring is detected during this time. The monitor resource is in the normal status. In this case, an alert is used because the delay warning rate has exceeded 80%.
- C.** The time for monitor processing has exceeded 60 seconds of the monitoring timeout and the delay of monitoring is detected. The monitor resource has a problem. In this case, no alert is used.

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.

---

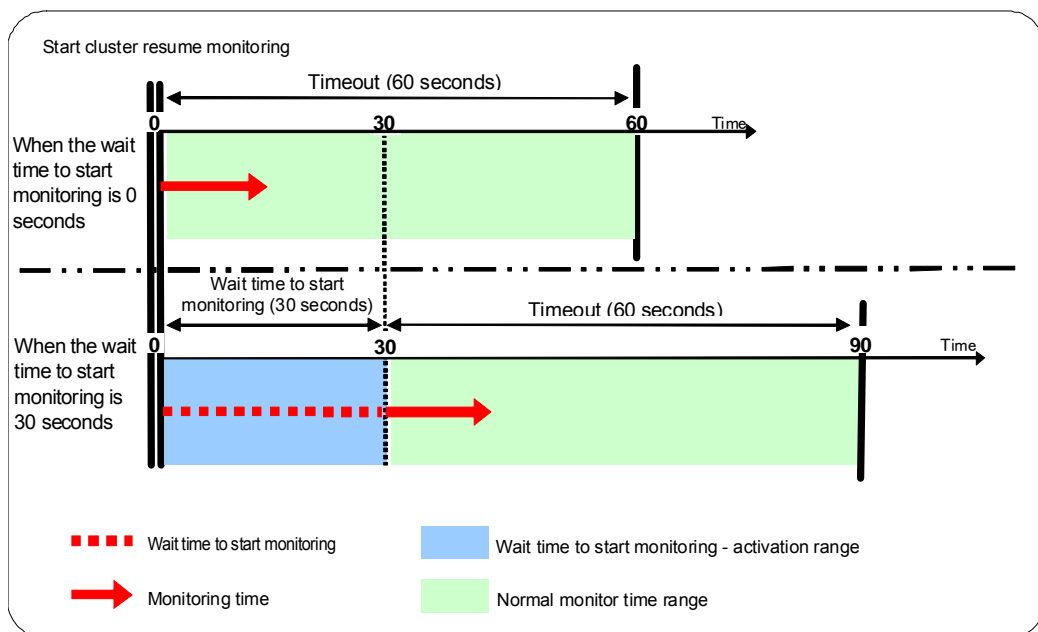
## Waiting for a monitor resource to start monitoring

“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 the application resource monitored by application monitor resource, and when they cannot be recovered by reactivation.

For example, when the monitor wait time is set to 0 (zero), recovery may be endlessly repeated. See the example below:



**Configuration of application monitor resource**

&lt;Monitor&gt;

Interval 5 sec

Timeout 60 sec

Retry Count 0 times

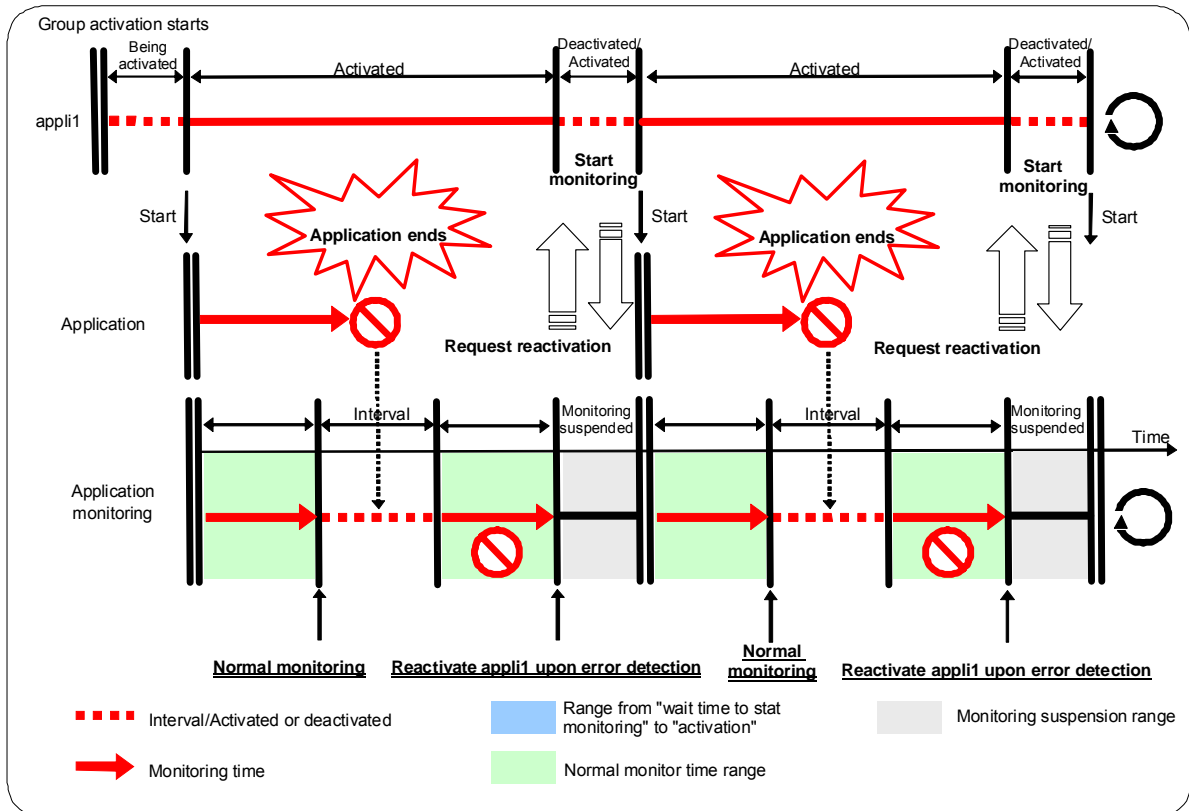
Wait Time to Start Monitoring 0 sec (default)

&lt;Error Detection&gt;

Recovery Action Restart the following target

Recovery Target appli1

Final Action Stop Group



The reason why recovery action is endlessly repeated is because the initial monitor resource polling has terminated successfully. The current count of recoveries the monitor resource has executed is reset when the status of the monitor resource becomes normal (finds no error in the monitor target). Because of this, the current count is always reset to 0 and reactivation for recovery is endlessly repeated.

You can prevent this problem by setting the wait time to start monitoring.

By default, 60 seconds is set as the wait time from the application startup to the end.

**Configuration of application monitor resource**

&lt;Monitor&gt;

Interval 5 sec

Timeout 60 sec

Retry Count 0 times

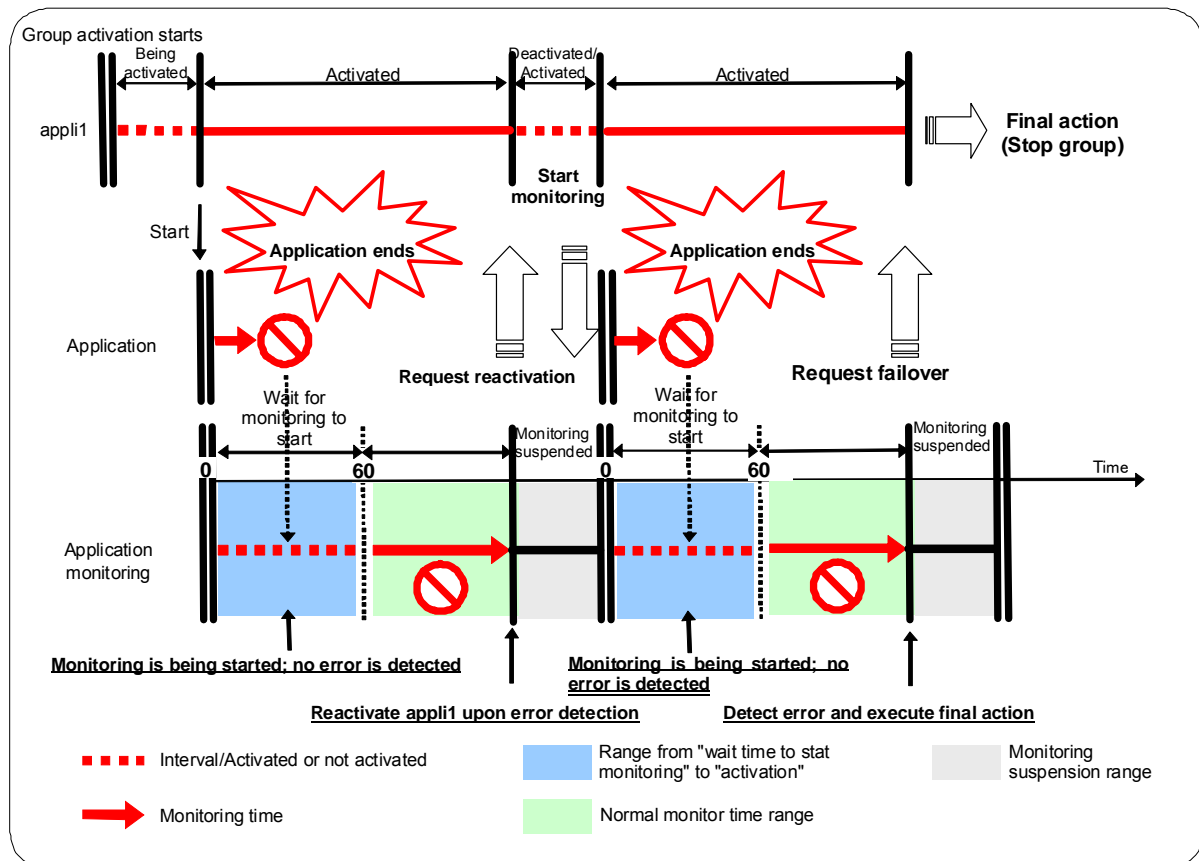
Wait Time to Start Monitoring: 60 sec

&lt;Error Detection&gt;

Recovery Action Restart the following target

Recovery Target appl1

Final Action Stop Group



## Limiting the reboot count for error detection by a monitor resource

When **Stop cluster service and shutdown OS** or **Stop cluster service and reboot OS** is selected as a final action to be taken when an error is detected by the monitor resource, the number of shutdowns or reboots can be limited.

Run the `clpregctrl` command to reset the reboot count. For details about the `clpregctrl` command, see Chapter 2, "ExpressCluster X SingleServerSafe command reference" in the *ExpressCluster X SingleServerSafe for Windows Operation Guide*.

---

**Note:**

The number of reboots resulting from the final action due to group activation or deactivation errors and that resulting from the final action due to monitor resource errors 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.

---



# 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 8          Notes and Restrictions



# Chapter 8      Notes and Restrictions

This chapter provides information on known problems and how to troubleshoot the problems.

This chapter covers:

Designing a system configuration.....	296
Creating configuration data .....	298
Upper limits of registration.....	301

## Designing a system configuration

This section describes the items to note when selecting hardware and designing a system configuration.

### NIC link up/down monitor resource

Some NIC boards and drivers do not support required DeviceIoControl function. This monitor resource cannot be used in such a case. To use this monitor resource, use the trial license and check the operation in advance.

### ExpressCluster X Alert Service

The license for the ExpressCluster X Alert Service allows you to use the mail report function, but not the warning light function.

### Notes on LAN board redundancy

Because a pair of LAN boards is used as a single LAN board, you cannot use the two LAN boards at the same time. To connect to multiple networks, you need three or more LAN boards. When you have four or more LAN boards, you can set up two or more redundant pairs of LAN boards. Note that these redundant LAN board pairs are fixed and cannot be changed dynamically.

When the server is running, there is no need to know which of the two LAN boards is in use. One of them is automatically put into the active state, while the other is put into the standby state.

If errors persist in both of the LAN boards, they are repeatedly switched between. Therefore, set up ExpressCluster X SingleServerSafe to perform IP address monitoring, and make sure that the active IP address is always specified and monitored on the network associated with the IP address specified for the redundant LAN boards. If both LAN boards fail simultaneously, the IP address monitoring process detects an error, causing the server to be rebooted. Rebooting the server might not achieve error recovery but helps you recognize the error.

- ◆ If a LAN board fails while data is sent or received, the data transmission or receive ends abnormally even though the other LAN board is switched to. In this case, send or receive the data again.
- ◆ If you manually disable both LAN boards in a redundant configuration at the same time, redundancy control is not exerted. Make sure that one of them is enabled.
- ◆ Some applications that have a LAN board monitoring function (such as Intel® Proset II) might regard the switch to the other LAN board as an error. Before putting the redundant configuration into actual use, check the operation.
- ◆ Do not manually enable both LAN boards in a redundant configuration at the same time. If you enable both LAN boards, the one that was enabled last does not work properly. Therefore, if you enable both LAN boards and then disable the one that was enabled first, a network failure occurs, potentially shutting down the ExpressCluster X SingleServerSafe service. This might also cause other applications to malfunction. If you enable the two LAN boards at the same time, disable both LAN boards, and then enable one of them.

### 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 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.
- ◆ If you want to take advantage of the target Java VM load calculation function of coordination load balancer is recommended for use in SingleServerSafe.

## Mail reporting

The mail reporting function is not supported by STARTTLS and SSL.

## Creating configuration data

This section describes the items to note before designing and creating configuration data based on the system configuration.

### Final action for 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 specify **No Operation** in the actual production environment.

### 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 specified as the delay monitoring rate  
The delay warning will not be issued.

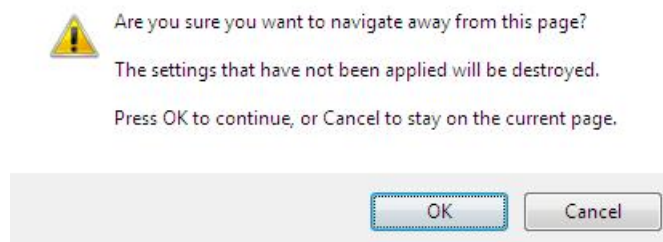
Be sure not to set a low value, such as 0%, except for a test operation.

### WebManager reload interval

- ◆ Do not set the “Reload Interval” on the WebManager tab or less than 30 seconds. If you set it for less than 30 seconds, it may affect the performance of ExpressCluster X SingleServerSafe.

### Notes on the Builder

- ◆ The configuration data of the following products is not compatible.
  - A Builder other than that for ExpressCluster X SingleServerSafe 3.1for Windows
  - The Builder of ExpressCluster for Linux
  - The Builder of ExpressCluster for Windows Value Edition
- ◆ Closing the Web browser (by clicking **Exit** from the menu), the dialog box to confirm to save is displayed.

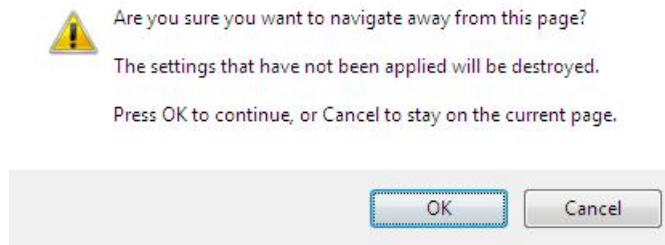


When you continue to edit, click the **Cancel** button.

**Note:**

This dialog box is not displayed if JavaScript is disabled.

- ◆ Reloading the Web browser (by selecting Refresh from the menu or tool bar), the dialog box to confirm to save is displayed.



When you continue to edit, click the **Cancel** button.

**Note:**

This dialog box is not displayed if JavaScript is disabled.

- ◆ If you change the screen resolution while the Builder is running, the Java VM stack trace (example: NullPointerException) may be logged on the Java console. The Builder can keep running.
- ◆ If you press Esc while a pull-down menu of your browser is displayed, the Java VM stack trace (example: NullPointerException) may be logged on the Java console. The Builder can keep running.
- ◆ In some cases, you cannot use the keyboard because the keyboard focus of the Builder becomes disabled (the focus changes to the Web browser). Click the Builder window and get the focus back to the Builder.
- ◆ When you are using the multi-display function, do not run the Builder on the secondary display. Otherwise, it may not work properly. For example, the screen is not displayed. Use the Builder on the primary display.
- ◆ If you specify a number smaller than the current one for **Max. Number to Save Alert Records** on the **Alert Log** tab (see “**Alert Log** tab” on page 161), all alert logs are deleted. Take into account the available disk space, and specify the number before you start the operation.
- ◆ In the environment where both Microsoft Windows Vista and Internet Explorer 7 are used, disable **Protected Mode** on the security setting of Internet Explorer 7.
- ◆ The JIS 2004-unique characters supported by Microsoft Windows Vista are not supported. Thus, you cannot enter or view the characters added by JIS 2004.
- ◆ When going through the reverse proxy server, the Builder will not operate properly.

## Double-byte character set that can be used in script comments

Scripts edited in Windows environment are dealt as Shift-JIS code, and scripts edited in Linux environment are dealt as EUC code. In case that other character codes are used, character corruption may occur depending on environment.

## JVM monitor resource settings

- ◆ When the monitoring target is WebLogic, 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**
- ◆ To use the Java Resource Agent, install the Java runtime environment (JRE) described in "Setting up JAVA runtime environment to a management PC" in Chapter 2, "Creating configuration data" or a Java development kit (JDK). You can use either the same JRE or JDK as that used by the monitoring target (WebLogic Server or WebOTX) or a different one. If both JRE and JDK are installed on a server, you can use either one.

## System monitor resource settings

- ◆ Pattern of detection by resource monitoring

The System Resource Agent performs detection by using thresholds and monitoring duration time as parameters.

The System Resource Agent collects the data (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).

## Upper limits of registration

	Builder version	You can register up to
Cluster	3.0.0-1 or later	1
Server	3.0.0-1 or later	32
Server Group	3.0.0-1 or later	9
Group	Earlier than 3.1.0-1	64
	3.1.0-1 or later	128
Group resource (Per one group)	Earlier than 3.1.0-1	256
	3.1.0-1 or later	512
Monitor resource	3.0.0-1 or later	384
Heartbeat resource	3.0.0-1 or later	16
Network Partition Resolution Resource	3.0.0-1 or later	64
Mirror disk resources and hybrid disk resources (Per cluster) in total	3.0.0-1 or later	8
Mirror Disk Connect	3.0.0-1 or later	16



# Appendix

- Index





# Appendix A Index

## A

Action when an error is detected by a monitor resource, 281  
Activation or deactivation error for the recovery target, 282  
Adding a monitor resource, 40  
Alert Log tab, 256  
Alert Service tab, 242  
Always monitor and Monitors while activated, 274  
Applications supported, 94  
Applying configuration data, 51

## B

BMC tab, 270

## C

Checking the values to be specified, 26  
Common settings for monitor resource, 100  
Configuration and range of NIC link up/down monitoring, 116  
Considerations for service resources, 83  
CPU usage, 227  
Creating the configuration data, 30

## D

Delay warning of a monitor resource, 286  
Delay warning rate, 298  
Delay Warning tab, 257  
Differences regarding the use of the offline version of the Builder, 53  
Displaying and changing disk RW monitor resource details, 110  
Displaying and changing IP monitor resource details, 114  
Displaying and changing parameters of a monitor resource, 107  
Displaying and changing the application resource details, 67  
Displaying and changing the details of the custom monitoring resources, 118  
Displaying and changing the details of the Message receive monitor resources, 125  
Displaying and changing the details of the multi target monitor resource, 122  
Displaying and changing the disk DB2 monitor resource details, 133  
Displaying and changing the FTP monitor resource details, 136  
Displaying and changing the HTTP monitor resource details, 139  
Displaying and changing the IMAP4 monitor resource details, 142

displaying and changing the JVM monitor resource details, 206  
Displaying and changing the NIC link up/down monitor resource details, 116  
Displaying and changing the ODBC monitor resource details, 146  
Displaying and changing the Oracle monitor resource details, 150  
Displaying and changing the OracleAS monitor resource details, 155  
Displaying and changing the POP3 monitor resource details, 160  
Displaying and changing the PostgreSQL monitor resource details, 165  
Displaying and changing the process name monitor resource details, 129  
Displaying and changing the script resource details, 77  
Displaying and changing the service resource details, 83  
Displaying and changing the SMTP monitor resource details, 168  
Displaying and changing the SQL Server monitor resource details, 172  
Displaying and changing the system monitor resource details, 224  
Displaying and changing the Tuxedo monitor resource details, 175  
Displaying and changing the VM resource details, 86  
Displaying and changing the Weblogic monitor resource details, 177  
Displaying and changing the WebOTX monitor resource details, 180  
Displaying and changing the Websphere monitor resource details, 182  
Double-byte character set, 299  
Duration Time, 227

## E

Enabling and disabling Dummy failure of monitor resources, 275  
environment variables, 283  
ExpressCluster X Alert Service, 296  
ExpressCluster X SingleServerSafe, 20

## F

Final action, 298

## G

GC tab, 213  
Group resource, xi, 26, 63, 65, 127, 298  
Group resources, 66

## H

HBA tab, 270  
How an error is detected, 19, 21

## I

Info tab, 232, 268  
IP Address Settings, 115, 117

## J

JVM monitor resource, 300  
JVM monitor resources, 184  
JVM monitor tab, 260

## L

LAN board redundancy function, 57  
Limiting the reboot count, 291  
Linking with the BIG-IP Local Traffic Manager, 194  
linking with the load balancer, 188, 190  
Load Balancer Linkage tab, 216, 217

## M

Mail reporting, 297  
Memory tab, 210  
Monitor resource, xi, 21, 26, 54, 63, 89, 131, 148, 154, 157, 158, 162, 170, 174, 176, 179, 181, 263, 264  
Monitor resource monitor interval, 276  
Monitor resources, 90  
Monitor tab, 235  
Monitoring by application monitor resources, 108  
Monitoring by custom monitor resources, 118  
Monitoring by DB2 monitor resources, 132  
Monitoring by disk RW monitor resources, 110  
Monitoring by FTP monitor resources, 135  
Monitoring by HTTP monitor resources, 138  
Monitoring by IMAP4 monitor resources, 141  
Monitoring by IP monitor resources, 113  
Monitoring by JVM monitor resources, 184  
Monitoring by message receive monitor resources, 125  
Monitoring by ODBC monitor resources, 145  
Monitoring by Oracle monitor resources, 149  
Monitoring by OracleAS monitor resources, 154  
Monitoring by POP3 monitor resources, 159  
Monitoring by PostgreSQL monitor resources, 164  
Monitoring by service monitor resources, 109  
Monitoring by SMTP monitor resources, 167  
Monitoring by SQL Server monitor resources, 171  
Monitoring by system monitor resources, 220  
Monitoring by Tuxedo monitor resources, 174  
Monitoring by VM monitor resources, 127  
Monitoring by Weblogic monitor resources, 176  
Monitoring by WebOTX monitor resources, 179  
Monitoring by Websphere monitor resources, 181

Monitoring SVF, 205  
Monitoring Tomcat, 204  
Monitoring WebLogic Server, 199  
Monitoring WebOTX, 201  
MultiTarget Monitor Resource Tuning Properties, 123

## N

NIC link up/down monitor resource, 296  
Note on application monitor resources, 108  
Note on custom monitor resources, 118  
Note on JVM monitor resources, 184  
Note on NIC link up/down monitor resources, 116  
Note on service monitor resources, 109  
Note on the multi target monitor resource, 121  
Notes on DB2 monitor resources, 131  
Notes on FTP monitor resources, 135  
Notes on HTTP monitor resource, 138  
Notes on IMAP4 monitor resources, 141  
Notes on LAN board redundancy, 296  
Notes on message receive monitor resources, 125  
Notes on ODBC monitor resources, 144  
Notes on Oracle monitor resources, 148  
Notes on OracleAS monitor resources, 154  
Notes on POP3 monitor resources, 159  
Notes on PostgreSQL monitor resources, 162  
Notes on process name monitor resources, 128  
Notes on SMTP monitor resources, 167  
Notes on SQL Server monitor resources, 170  
Notes on system monitor resources, 219  
Notes on the Builder, 298  
Notes on Tuxedo monitor resources, 174  
Notes on VM monitor resources, 127  
Notes on Weblogic monitor resources, 176  
Notes on WebOTX monitor resources, 179  
Notes on Websphere monitor resources, 181

## P

Port No. tab, 233  
Power Saving tab, 258  
Process name monitor resources, 128

## R

Recovering from a monitor error (normal), 282  
Recovery tab, 237  
Recovery/pre-recovery action script, 283  
Reload interval, 298

## S

Sample environment, 26  
Saving configuration data, 49, 55  
Service Resource Tuning Properties, 84  
Setting LAN board redundancy, 59  
Setting up application monitor resources, 108  
Setting up application resources, 67  
Setting up custom monitor resources, 118  
Setting up DB2 monitor resources, 131

---

Setting up disk RW monitor resources, 110  
Setting up FTP monitor resources, 135  
Setting up HTTP monitor resources, 138  
Setting up IMAP4 monitor resources, 141  
Setting up IP monitor resources, 113  
Setting up JAVA runtime environment, 29  
Setting up message receive monitor resources, 125  
Setting up multi target monitor resources, 121  
Setting up NIC link up/down monitor resources, 116  
Setting up ODBC monitor resources, 144  
Setting up Oracle monitor resources, 148  
Setting up OracleAS monitor resources, 154  
Setting up POP3 monitor resources, 159  
Setting up PostgreSQL monitor resources, 162  
Setting up script resources, 72  
Setting up service monitor resources, 109  
Setting up service resources, 83  
Setting up SMTP monitor resources, 167  
Setting up SQL Server monitor resources, 170  
Setting up Tuxedo monitor resources, 174  
Setting up VM monitor resources, 127  
Setting up VM resources, 86  
Setting up Weblogic monitor resources, 176  
Setting up WebOTX monitor resources, 179  
Setting up Websphere monitor resources, 181  
Starting up the WebManager, 28, 29  
Status of the multi target monitor resource, 121  
System monitor resources, 219

System requirements for VM resource, 66

## T

Thread tab, 212  
Tips for creating scripts, 77  
Tips for recovery/pre-recovery action script coding, 284

## U

Understanding LAN board redundancy, 58  
Upper limits, 295, 301  
Using the simple selection function of a script template, 81

## V

Virtual Machine Resource Tuning Properties, 87

## W

Waiting for a monitor resource to start monitoring, 288  
Warning Light tab, 270  
WebLogic tab, 214  
WebManager, 28  
WebManager tab, 250  
Writing recovery/pre-recovery action scripts, 284