



**EXPRESSCLUSTER X SingleServerSafe 4.3 for Windows
Configuration Guide**

Release 1

NEC Corporation

Apr 09, 2021

TABLE OF CONTENTS:

1	Preface	1
1.1	Who Should Use This Guide	1
1.2	How This Guide Is Organized	2
1.3	Terms Used in This Guide	3
1.4	EXPRESSCLUSTER X SingleServerSafe Documentation Set	4
1.5	Conventions	5
1.6	Contacting NEC	6
2	EXPRESSCLUSTER X SingleServerSafe	7
2.1	EXPRESSCLUSTER X SingleServerSafe	8
2.2	How an error is detected in EXPRESSCLUSTER X SingleServerSafe	9
3	Creating configuration data	11
3.1	Checking the values to be specified	12
3.2	Starting up the Cluster WebUI	13
3.3	Creating the configuration data	15
3.4	Saving configuration data	20
3.5	Applying configuration data	21
4	Group resource details	23
4.1	Group resources	24
4.2	Setting up application resources	25
4.3	Setting up script resources	31
4.4	Setting up service resources	39
4.5	Setting up VM resources	42
5	Monitor resource details	45
5.1	Monitor resources	47
5.2	Monitor resource properties	52
5.3	Setting up application monitor resources	61
5.4	Setting up service monitor resources	62
5.5	Setting up disk RW monitor resources	63
5.6	Setting up IP monitor resources	65
5.7	Setting up NIC link up/down monitor resources	68
5.8	Setting up custom monitor resources	70
5.9	Setting up multi target monitor resources	72
5.10	Setting up message receive monitor resources	75
5.11	Setting up VM monitor resources	77
5.12	Setting up process name monitor resources	78
5.13	Setting up DB2 monitor resources	80

5.14	Setting up FTP monitor resources	83
5.15	Setting up HTTP monitor resources	85
5.16	Setting up IMAP4 monitor resources	88
5.17	Setting up ODBC monitor resources	90
5.18	Setting up Oracle monitor resources	93
5.19	Setting up POP3 monitor resources	99
5.20	Setting up PostgreSQL monitor resources	101
5.21	Setting up SMTP monitor resources	105
5.22	Setting up SQL Server monitor resources	107
5.23	Setting up Tuxedo monitor resources	111
5.24	Setting up Weblogic monitor resources	112
5.25	Setting up WebOTX monitor resources	116
5.26	Setting up Websphere monitor resources	118
5.27	Setting up JVM monitor resources	120
5.28	Setting up System monitor resources	167
5.29	Setting up Process resource monitor resources	177
5.30	Setting up user mode monitor resources	182
6	Other setting details	185
6.1	Cluster properties	186
6.2	Server properties	227
6.3	Upper limits of registration	229
7	Monitoring details	231
7.1	Always monitor and Monitors while activated	232
7.2	Enabling and disabling Dummy failure of monitor resources	233
7.3	Monitor resource monitor interval	234
7.4	Action when an error is detected by a monitor resource	239
7.5	Recovering from a monitor error (normal)	240
7.6	Activation or deactivation error for the recovery target during recovery	241
7.7	Recovery/pre-recovery action script	242
7.8	Delay warning of a monitor resource	245
7.9	Waiting for a monitor resource to start monitoring	246
7.10	Limiting the reboot count for error detection by a monitor resource	250
8	Notes and Restrictions	251
8.1	Designing a system configuration	252
8.2	Notes when creating the cluster configuration data	253
8.3	Notes when changing the EXPRESSCLUSTER configuration	255
9	Legal Notice	257
9.1	Disclaimer	257
9.2	Trademark Information	258
10	Revision History	259

PREFACE

1.1 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 SingleServer-Safe.

1.2 How This Guide Is Organized

- *2. EXPRESSCLUSTER X SingleServerSafe*: Provides a product overview of EXPRESSCLUSTER X SingleServerSafe.
- *3. Creating configuration data*: Describes how to start the Cluster WebUI / WebManager and the procedures to create the configuration data by using a sample configuration.
- *4. Group resource details*: Provides details on group resources, which are used as a unit for controlling an application by using EXPRESSCLUSTER X SingleServerSafe.
- *5. Monitor resource details*: Provides details on monitor resources, which are used as a unit when EXPRESSCLUSTER X SingleServerSafe executes monitoring.
- *6. Other setting details*: Provides details on the other settings for EXPRESSCLUSTER X SingleServerSafe.
- *7. Monitoring details*: Provides details on how several types of errors are detected.
- *8. Notes and Restrictions*: Describes known problems and how to prevent them.

1.3 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.

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

1.4 EXPRESSCLUSTER X SingleServerSafe Documentation Set

The EXPRESSCLUSTER X SingleServerSafe manuals consist of the four 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 SingleServerSafe Legacy Feature Guide

This guide is intended for system engineers who want to introduce systems using EXPRESSCLUSTER X SingleServerSafe and describes EXPRESSCLUSTER X SingleServerSafe 4.3 WebManager and Builder.

1.5 Conventions

In this guide, **Note**, **Important**, **See also** are used as follows:

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

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

See also:

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

The following conventions are used in this guide.

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

1.6 Contacting NEC

For the latest product information, visit our website below:

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

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:

- *2.1. EXPRESSCLUSTER X SingleServerSafe*
- *2.2. How an error is detected in EXPRESSCLUSTER X SingleServerSafe*

2.1 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.

2.2 How an error is detected in EXPRESSCLUSTER X SingleServer-Safe

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 "[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.

CREATING CONFIGURATION DATA

In EXPRESSCLUSTER X SingleServerSafe, data describing how a system is set up is called configuration data. Configuration data is created using Cluster WebUI. This chapter describes how to start the Cluster WebUI and the procedure for creating configuration data by using a sample cluster configuration.

This chapter covers:

- 3.1. *Checking the values to be specified*
- 3.2. *Starting up the Cluster WebUI*
- 3.3. *Creating the configuration data*
- 3.4. *Saving configuration data*
- 3.5. *Applying configuration data*

3.1 Checking the values to be specified

Before creating configuration data by using the Cluster WebUI, check the values you are going to specify as the configuration data. Write down the values to make sure there is no missing information.

3.1.1 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 "[4. Group resource details](#)" and "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	User mode monitor resources
	Monitor resource name	userw
	User Heartbeat Interval/Timeout	On
	Monitoring Method	keepalive
	Action When Timeout Occurs	Generating of intentional Stop Error
	Create a Dummy Thread	On
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
	Reactivation threshold	3
	Final Action:	Stop service and reboot OS

Note: The values of "User mode monitor resources" for the first monitor resources are automatically specified.

3.2 Starting up the Cluster WebUI

The configuration data can be created by accessing the Cluster WebUI. This section describes the overview of the Cluster WebUI and how to create the configuration data.

3.2.1 What is Cluster WebUI?

The Cluster WebUI is a function for monitoring the server status, starting and stopping servers and groups, and collecting operation logs through a web browser.

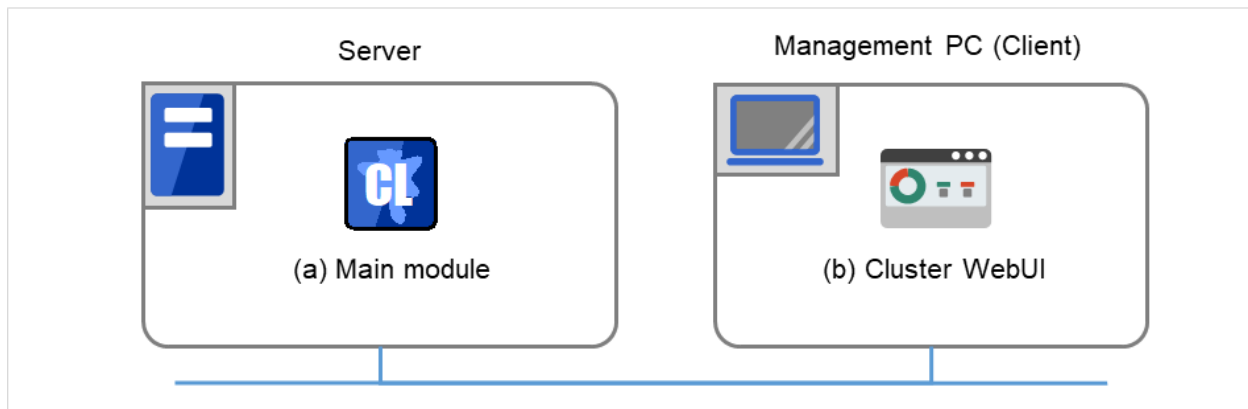


Fig. 3.1: Cluster WebUI

3.2.2 Starting the Cluster WebUI

The following describes how to start the Cluster WebUI.

1. Start your Web browser.

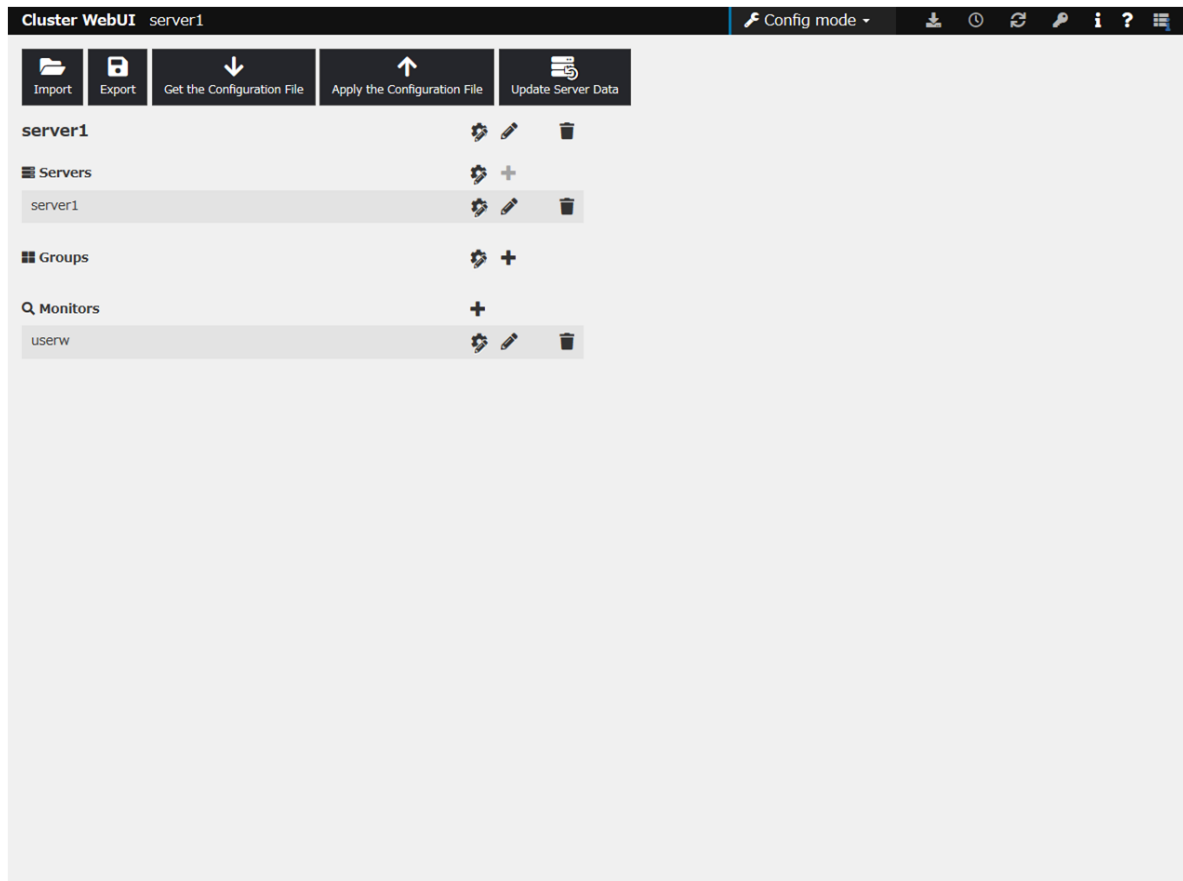
Enter the IP address and port number of the server where EXPRESSCLUSTER X SingleServerSafe is installed in the browser address bar.

`http://ip-address:port/`

ip-address Specify the IP address of a server where EXPRESSCLUSTER X SingleServerSafe is installed. In the case of a local server, a local host can be specified.

port Specify the same port number as that specified for WebManager at installation (default: 29003).

2. The Cluster WebUI starts.



3. From the drop-down menu of the toolbar, select **Config Mode** to switch to the config mode.

See also:

To enable encrypted communication with EXPRESSCLUSTER Server, see "6.1.9. *WebManager tab*" in "6. *Other setting details*". Enter the following to perform encrypted communication.

`https://192.168.0.1:29003/`

3.3 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.

- *3.3.1. Setting up the server*

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

- *3.3.1. Setting up the server*

Specify the server name to be configured.

- *3.3.2. 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.

- *3.3.2. Adding a group*

Add a group.

- *3.3.2. Adding a group resource (application resource)*

Add a resource that can start and stop an application.

- *3.3.3. 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.

- *3.3.3. Adding a monitor resource (IP monitor resource)*

Add a monitor resource that performs monitoring.

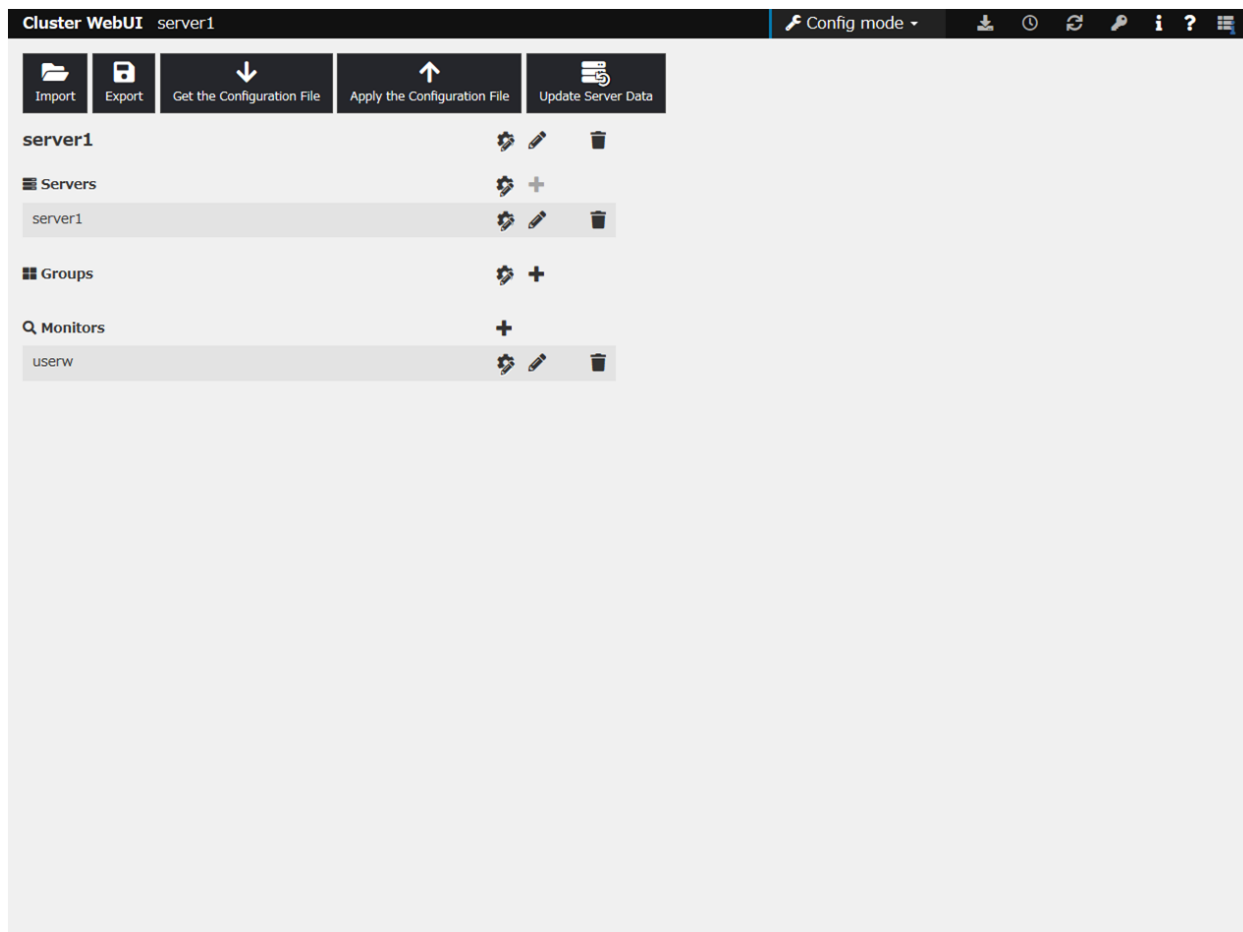
3.3.1 Setting up the server

Set up the server.

Setting up the server

The server settings are automatically created when you reboot the OS after installing EXPRESSCLUSTER X Single-ServerSafe. When you switch from the Cluster WebUI's operation mode window to the Config Mode window, you will see the created data.

The window is as follows:



3.3.2 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.

Adding a group

Set up a group.

1. Click **Add group** in **Groups**.
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**.

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

Group Definition failover X

Basic Settings ✓ → **Startup Servers** → Group Attributes → Group Resource

Failover is possible at all servers ☒

Server

server1

i Select the server which can run the group and configure the priority of the servers.

In case that all the servers which are registered to the cluster can start the group, check "Failover is possible at all servers" on. The priority order is the order which was set when the server was registered to the cluster.

In case setting individually the server which can start the group, check "Failover is possible at all servers" off. Select the server which can start the group from the "Available Servers" list on the right side, and click "Add" to add the server to "Servers that can run the Group" list. Click "↑" or "↓" to change the priority order.

◀ Back Next ▶ Cancel

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.

Adding a group resource (application resource)

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

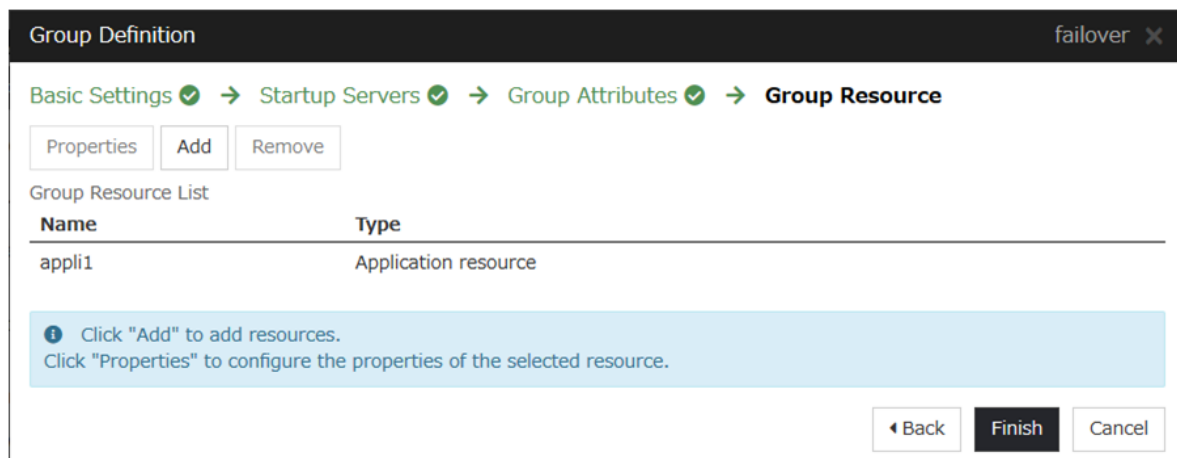
1. Click **Add** in **Group Resource List**.
2. The **Resource Definition of Group(failover1)** dialog box is displayed. Select the group resource type (**application resource**) in the **Type** box, and enter the group resource name appli1 in the **Name** box. Click **Next**.

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**.
4. **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** are displayed. Click **Next**.
5. Select **Resident** in the **Resident Type**. And specify the path of the execution file for the **Start Path**.

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**.



7. Click **Finish**.

3.3.3 Setting up monitor resources

Add a monitor resource that monitors the specified target.

Adding a monitor resource (IP monitor resource)

1. Click **Add monitor resource** in **Monitors**. 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**.

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 Cluster WebUI.

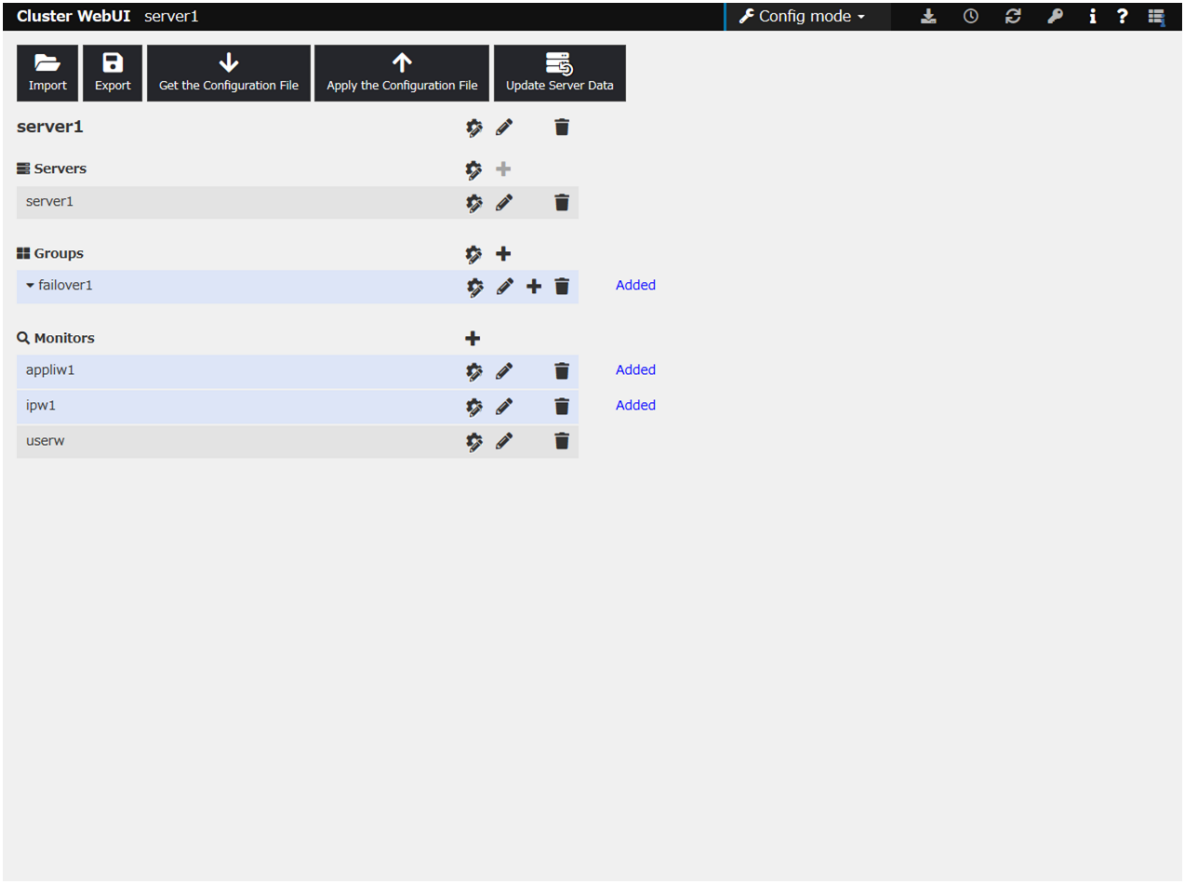
If any monitor resources are not displayed in the list box of **Type** even though the licenses are registered, please click **Get License Info** button.

3. Enter the monitor settings. Change nothing from the default values. Click **Next**.
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**.
7. Specify the recovery target. Click **Browse**.
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.



This concludes creating the configuration data. Proceed to the next section "3.4. Saving configuration data".

3.4 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. Click **Export** in the config mode of Cluster WebUI.
2. Select a location to save the data and save it.

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.

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.

3.5 Applying configuration data

After creating configuration data by using the config mode of Cluster WebUI, apply the configuration data to the server.

To apply the configuration data, follow the procedure below.

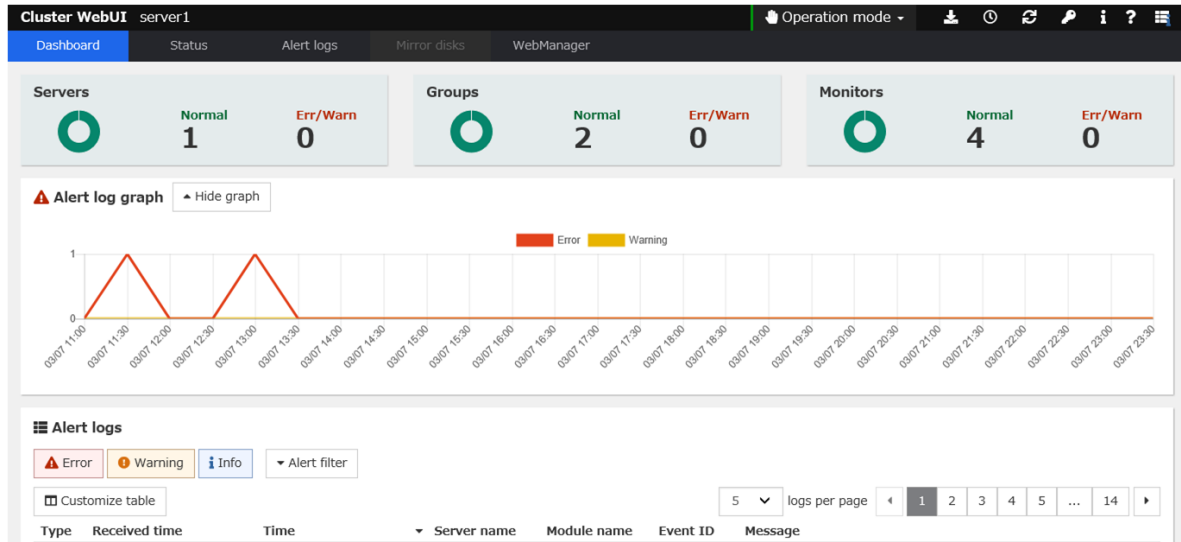
1. Click **Apply the Configuration File** in the config mode of Cluster WebUI.
2. Depending on the difference between the existing configuration data and the configuration data you are uploading, a pop-up window might be displayed to prompt you to check the operation necessary to upload the data.


If there is no problem with the operation, click **OK**.

When the upload ends successfully, a popup message saying "The application finished successfully." is displayed. Click OK.

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

3. The status will be displayed on the Cluster WebUI.



For how to operate and check the Cluster WebUI, see the online manual from the  button on the upper right of the screen.

GROUP RESOURCE DETAILS

This chapter provides details about group 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.

This chapter covers:

- 4.1. *Group resources*
- 4.2. *Setting up application resources*
- 4.3. *Setting up script resources*
- 4.4. *Setting up service resources*
- 4.5. *Setting up VM resources*

4.1 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

4.1.1 System requirements for VM resource

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

Virtualization platform	Version	Remarks
Hyper-V	Windows Server 2012 Hyper-V Windows Server 2012 R2 Hyper-V	

Note: VM resources do not work on Windows Server 2016.

4.2 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.

4.2.1 Details tab

The screenshot shows a window titled 'Resource Properties | appli1'. It has four tabs: 'Info', 'Dependency', 'Recovery Operation', and 'Details' (which is selected). Under 'Resident Type', there are two radio buttons: 'Resident' (selected) and 'Non-Resident'. Below this, 'Start Path*' has a text box containing 'C:\Windows\System32\app'. 'Stop Path' has an empty text box. A 'Tuning' button is on the left. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

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 1023 bytes)

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

Stop Path (within 1023 bytes)

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

The operation is as described below if the resident type is Resident.

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

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

Tuning

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

Application Resource Tuning Properties

Parameter tab

Detailed parameter settings are displayed on this tab.

The screenshot shows the 'Application Resource Tuning Properties' dialog box with the 'Parameter' tab selected. The dialog has a title bar and three tabs: 'Parameter', 'Start', and 'Stop'. The 'Parameter' tab is active, showing various settings for application resources. The 'Start' section has two radio buttons: 'Synchronous' (selected) and 'Asynchronous'. To the right of the 'Synchronous' radio button is a 'Timeout*' field with a value of '1800' and a unit of 'sec'. Below this is a 'Normal Return Value' text box. The 'Stop' section also has two radio buttons: 'Synchronous' (selected) and 'Asynchronous'. To the right of the 'Synchronous' radio button is a 'Timeout*' field with a value of '1800' and a unit of 'sec'. Below this is another 'Normal Return Value' text box. There is a 'Target VCOM' dropdown menu with a downward arrow. Below that is a 'Resource Name' text box. There are two checkboxes: 'Allow to Interact with Desktop' and 'Kill the application when exit', both of which are currently unchecked. Below these is an 'Exec User' dropdown menu with the text 'Set Up Individually' and a downward arrow. At the bottom left is an 'Initialize' button. At the bottom right are three buttons: 'OK', 'Cancel', and 'Apply'.

Synchronous (Start)

This setting is not available for a resident application.

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

Asynchronous (Start)

This setting is not available for a resident application.

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

Normal Return Value (Start) (Within 1023 bytes)

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

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

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

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

Synchronous (Stop)

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

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

Asynchronous (Stop)

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

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

Normal Return Value (Stop) (Within 1023 bytes)

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

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

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

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

Timeout (Start) (1 to 9999)

This setting is not available for a resident application.

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

Timeout (Stop) (1 to 9999)

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

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.

Kill the application when exit

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

Exec User

Specify a user who executes the application. The user can be selected from the users registered in the **Account** tab of **Cluster Properties**.

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

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

Initialize

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

Start and Stop tabs

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

Current Directory (Within 1023 bytes)

Specify a directory for running the application.

Option Parameter (Within 1023 bytes)

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

Example: "param 1" param2

Window Size

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

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

Exec User Domain

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.

4.3 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 *****

rem Allot a process by referencing environment variables for script starting_
↪ factors.
IF "%CLP_EVENT%"=="START" GOTO NORMAL
IF "%CLP_EVENT%"=="FAILOVER" GOTO FAILOVER
IF "%CLP_EVENT%"=="RECOVER" GOTO RECOVER

rem EXPRESSCLUSTER is not running.
GOTO no_arm

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

    rem Write the normal startup process of an operation here.
    rem This process is executed at the following timing:
    rem
    rem Normal startup
    rem

rem Allot a process by referencing environmental variables for a server_
↪ where the script is run.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER1

    rem Write a process to be executed only if an operation is normally_
    ↪ started on the primary server.
    rem
    rem This process is executed at the following timing:
    rem
    rem Normal startup
    rem

GOTO EXIT

:ON_OTHER1

rem Write a process to be executed only if an operation is normally started_
↪ on other than the primary server.
rem
rem
rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
rem

GOTO EXIT

:FAILOVER

rem Handle an error by referencing environmental variables for DISK_
↪ connection data.
```

(continues on next page)

(continued from previous page)

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

    rem Write the startup process of an operation.
    rem
    rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
    rem

rem Allot a process by referencing environmental variables for a server_
↪where the script is run.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER2

    rem Write a process to be executed only if an operation is started on_
↪the primary server.
    rem
    rem
    rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
    rem

GOTO EXIT

:ON_OTHER2

rem Write process to be executed only if an operation is started on other_
↪than the primary server.
rem
rem
rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
rem

GOTO EXIT

:RECOVER

rem Write the recovery process after the resumption of a cluster.
rem This process is executed at the following timing:
rem
rem Resumption of the cluster
rem

GOTO EXIT

:ERROR_DISK

rem Write disk-related error handling processes.

:no_arm

:EXIT
exit
```

Group A stop script: a sample of stop.sh

```
rem *****
rem *                               STOP.BAT                               *
rem *****

rem Allot a process by referencing environment variables for script starting_
↪factors.
IF "%CLP_EVENT%"=="START" GOTO NORMAL
IF "%CLP_EVENT%"=="FAILOVER" GOTO FAILOVER

rem EXPRESSCLUSTER is not running.
GOTO NO_ARM

:NORMAL
rem Handle an error by referencing environmental variables for DISK_
↪connection data.
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem Write the normal shutdown process of an operation here.
    rem This process is executed at the following timing:
    rem
    rem Normal shutdown
    rem

rem Allot a process by referencing environmental variables for a server_
↪where the script is run.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER1

    rem Write a process to be executed only if an operation is processed on_
↪the primary server.
    rem
    rem This process is executed at the following timing:
    rem
    rem Normal shutdown
    rem

GOTO EXIT

:ON_OTHER1

rem Write a process to be executed only if an operation is normally shut_
↪down on other than the primary server.
rem
rem
rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
rem

GOTO EXIT

:FAILOVER

rem Handle an error by referencing environmental variables for DISK_
↪connection data.
```

(continues on next page)

(continued from previous page)

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

    rem Describe the normal shutdown process after the failover.
    rem
    rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
    rem

rem Allot a process by referencing environmental variables for a server_
↪where the script is run.
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER2

    rem Write a process to be executed only if an operation is terminated on_
↪the primary server.
    rem
    rem
    rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
    rem

GOTO EXIT

:ON_OTHER2

rem Write a process to be executed only if an operation is terminated on_
↪other than the primary server after the failover.
rem
rem
rem This process is not executed by EXPRESSCLUSTER X SingleServerSafe.
rem

GOTO EXIT

:ERROR_DISK

rem Write disk-related error handling processes.

:NO_ARM

:EXIT
exit
```

4.3.1 Tips for creating scripts

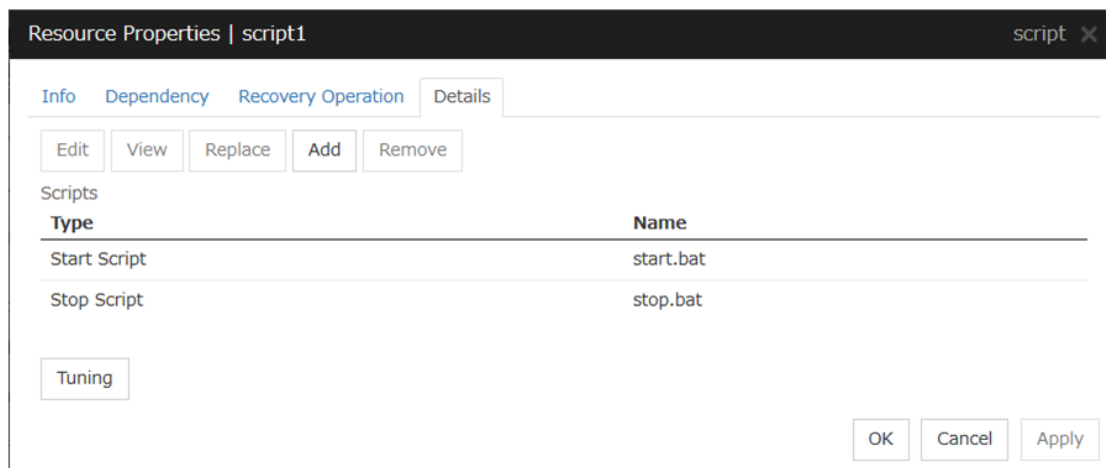
- The clplogcmd command, though which message output on the alert log is possible, is available.

4.3.2 Notes on script resources

Stop the processing by using the exit command in the script activated through the start command, when the start command is used in the start/stop script.

4.3.3 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.

Note:

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

Do not use "& (ampersand)" nor "=" (equal mark)" for the name of a script to be added.

Remove

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

View

Use this button to display the selected script file. You cannot display the script file if it is currently displayed or edited.

Edit

Use this button to edit the selected script file. Click **Save** to apply the change. 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 Cluster WebUI. If the cluster configuration data is reloaded by restarting the Cluster WebUI after deleting the script file, the deleted script file will be displayed in the **Scripts**.

The content of the script file selected in the **Resource Properties** is replaced with the one selected in the **Open** dialog box. 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.

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.

Script Resource Tuning Properties

Start

☒ Synchronous **Timeout*** 1800 sec

☐ Asynchronous

Normal Return Value

Perform recovery processing ☐

Stop

☒ Synchronous **Timeout*** 1800 sec

☐ Asynchronous

Normal Return Value

Target VCOM Resource Name ▼

Allow to Interact with Desktop ☐

Exec User ▼

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.

- 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.

Perform recovery processing

Specify whether to run a start script or not in any of the following timings:

- When the server is recovered
- When a monitor resource/ARMLOAD command error is detected
- When the group resource activation terminates due to an error

When executed as the recovery operation, RECOVER is set for CLP_EVENT, the environment variable.

Timeout (1 to 9999)

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

Target VCOM Resource Name

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.

Exec User

Specify a user who executes the script. The user can be selected from the users registered in the **Account** tab of **Cluster Properties**.

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

Initialize

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

4.4 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.

4.4.1 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.
- The service executed by the service resource is not controlled by applications other than EXPRESSCLUSTER. Therefore, it is recommended to set the recovery operation not to be performed by the service control manager. If a service is set to restart upon the recovery operation by the service control manager, an unexpected action might be performed due to duplication with the recovery operation by EXPRESSCLUSTER.

4.4.2 Details tab

The screenshot shows a dialog box titled 'Resource Properties | service1'. It has four tabs: 'Info', 'Dependency', 'Recovery Operation', and 'Details'. The 'Details' tab is selected. Inside the dialog, there is a 'Service Name*' label followed by a text box containing 'myservice' and a dropdown arrow. To the right of the text box is a 'Connect' button. Below the text box is a 'Tuning' button. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

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.

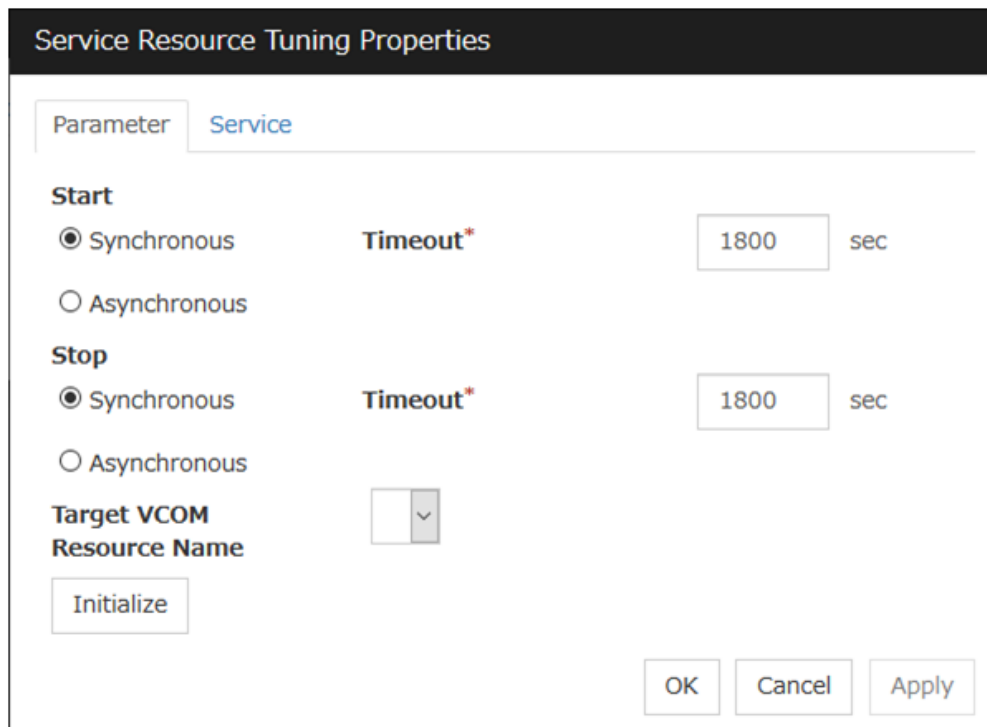
Tuning

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.



The image shows a dialog box titled "Service Resource Tuning Properties". It has two tabs: "Parameter" and "Service", with "Service" currently selected. The dialog is divided into sections for "Start" and "Stop" operations. Each section has two radio buttons: "Synchronous" (selected) and "Asynchronous". To the right of these is a "Timeout*" label followed by a text input field containing "1800" and the unit "sec". Below these sections is a "Target VCOM Resource Name" label and a dropdown menu showing a downward arrow. At the bottom left is an "Initialize" button, and at the bottom right are "OK", "Cancel", and "Apply" buttons.

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

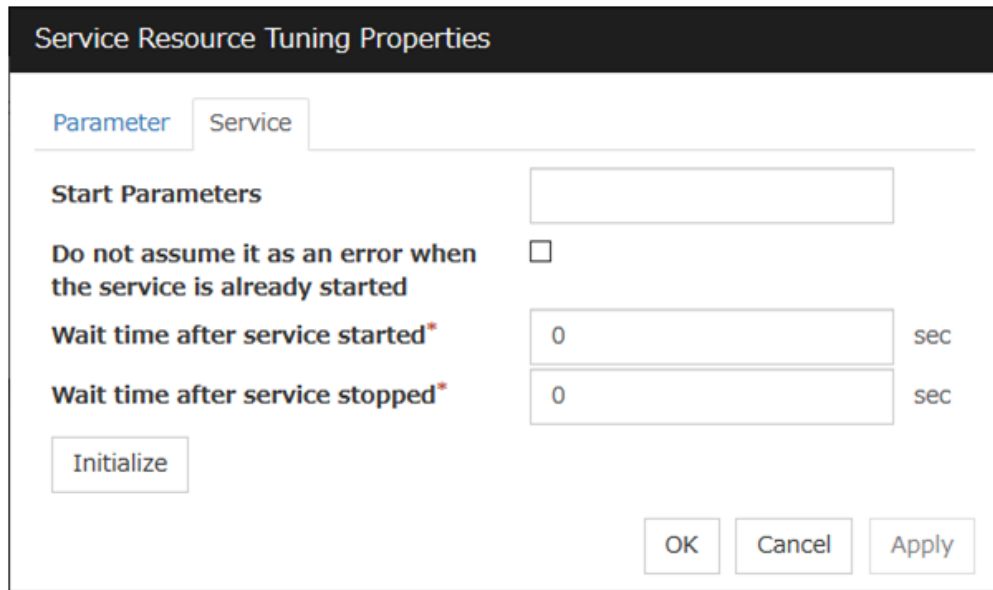
Not used.

Initialize

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

Service tab

The settings for the service are displayed.



The image shows a dialog box titled "Service Resource Tuning Properties". It has two tabs: "Parameter" and "Service". The "Service" tab is selected. Inside the dialog, there are four main sections: "Start Parameters" with a text input field; "Do not assume it as an error when the service is already started" with an unchecked checkbox; "Wait time after service started*" with a numeric input field set to "0" and a "sec" label; and "Wait time after service stopped*" with a numeric input field set to "0" and a "sec" label. At the bottom left is an "Initialize" button, and at the bottom right are "OK", "Cancel", and "Apply" buttons.

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.

Wait after the service is started (0 to 9999)

Specify the time to wait after the service is started.
The service resource activation will be completed after waiting for the specified time.

Wait after the service is stopped (0 to 9999)

Specify the time to wait after the service is stopped.
The service resource deactivation will be completed after waiting for the specified time.

Initialize

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

4.5 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.

4.5.1 Notes on VM resources

- A VM resource can be registered with a group for which the group type is virtual machine.
- Only one VM resource can be registered per group.
- VM resources are effective when EXPRESSCLUSTER is installed on host OS of virtual infrastructure (Hyper-V).
- If VM resources are stopped, the VM is deleted from Hyper-V manager.

4.5.2 Details tab

The screenshot shows a dialog box titled 'Resource Properties | vm1' with a close button (X) in the top right corner. The 'Details' tab is selected, showing the following fields:

- VM Type:** A dropdown menu with 'Hyper-V' selected.
- VM Name*:** A text input field containing 'vm1'.
- VM Path*:** A text input field containing 'X:\vm0'.
- Tuning:** A button located below the VM Path field.

At the bottom right of the dialog box are three buttons: 'OK', 'Cancel', and 'Apply'.

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.

Virtual Machine Resource Tuning Properties

Parameter

Request Timeout*	180	sec
Virtual Machine Start Waiting Time*	0	sec
Virtual Machine Stop Waiting Time*	600	sec

Initialize

OK Cancel Apply

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.

MONITOR RESOURCE DETAILS

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

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.

This chapter covers:

- *5.1. Monitor resources*
- *5.2. Monitor resource properties*
- *5.3. Setting up application monitor resources*
- *5.4. Setting up service monitor resources*
- *5.5. Setting up disk RW monitor resources*
- *5.6. Setting up IP monitor resources*
- *5.7. Setting up NIC link up/down monitor resources*
- *5.8. Setting up custom monitor resources*
- *5.9. Setting up multi target monitor resources*
- *5.10. Setting up message receive monitor resources*
- *5.11. Setting up VM monitor resources*
- *5.12. Setting up process name monitor resources*
- *5.13. Setting up DB2 monitor resources*
- *5.14. Setting up FTP monitor resources*
- *5.15. Setting up HTTP monitor resources*
- *5.16. Setting up IMAP4 monitor resources*
- *5.17. Setting up ODBC monitor resources*
- *5.18. Setting up Oracle monitor resources*
- *5.19. Setting up POP3 monitor resources*
- *5.20. Setting up PostgreSQL monitor resources*
- *5.21. Setting up SMTP monitor resources*
- *5.22. Setting up SQL Server monitor resources*
- *5.23. Setting up Tuxedo monitor resources*

- 5.24. *Setting up Weblogic monitor resources*
- 5.25. *Setting up WebOTX monitor resources*
- 5.26. *Setting up Websphere monitor resources*
- 5.27. *Setting up JVM monitor resources*
- 5.28. *Setting up System monitor resources*
- 5.29. *Setting up Process resource monitor resources*
- 5.30. *Setting up user mode monitor resources*

5.1 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 when activated	All resources
IP monitor resource	Monitors IP addresses and communication paths by using the ping command and checking whether there is a response .	Always 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.	Always or when activated	All resources
Custom monitor resource	Performs monitoring by executing any script.	Always 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 Cluster WebUI.	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.	Always 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 mechanism for monitoring an HTTP server.	When activated (Fixed)	All resources

Continued on next page

Table 5.1 – continued from previous page

Monitor resource name	Function	Monitor Timing: (Default values are shown in bold.)	Target Resource:
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
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
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 mechanism for monitoring a Java VM.	Always or when activated	All resources
System monitor resources	Provides a mechanism for monitoring a System Resource.	Always (Fixed)	All resources
Process resource monitor resources	Provides a mechanism for monitoring process resources.	Always (Fixed)	All resources
User mode monitor resource	Provides a mechanism for monitoring any user space stalls.	Always (Fixed)	None

5.1.1 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 4.3 for Windows	DB2 monitor resources
	ODBC monitor resources
	Oracle monitor resources
	PostgreSQL monitor resources
	SQL Server monitor resources
EXPRESSCLUSTER X Internet Server Agent 4.3 for Windows	FTP monitor resources
	HTTP monitor resources
	IMAP4 monitor resources
	POP3 monitor resources
	SMTP monitor resources
EXPRESSCLUSTER X Application Server Agent 4.3 for Windows	Tuxedo monitor resources
	Websphere monitor resources
	Weblogic monitor resources
	WebOTX monitor resources
EXPRESSCLUSTER X Java Resource Agent 4.3 for Windows	JVM monitor resources
EXPRESSCLUSTER X System Resource Agent 4.3 for Windows	System monitor resources
	Process resource monitor resources

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

5.1.2 Applications supported by monitoring options

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

x86_64 version

Monitor resource	Application to be monitored	EXPRESSCLUSTER Version	Remarks
Oracle monitor	Oracle Database 12c Release 1 (12.1)	12.00 or later	
	Oracle Database 12c Release 2 (12.2)	12.00 or later	
	Oracle Database 18c (18.3)	12.10 or later	
	Oracle Database 19c (19.3)	12.10 or later	
DB2 monitor	DB2 V10.5	12.00 or later	
	DB2 V11.1	12.00 or later	
	DB2 V11.5	12.20 or later	
PostgreSQL monitor	PostgreSQL 9.3	12.00 or later	
	PostgreSQL 9.4	12.00 or later	

Continued on next page

Table 5.3 – continued from previous page

Monitor resource	Application to be monitored	EXPRESSCLUSTER Version	Remarks
	PostgreSQL 9.5	12.00 or later	
	PostgreSQL 9.6	12.00 or later	
	PostgreSQL 10	12.00 or later	
	PostgreSQL 11	12.10 or later	
	PostgreSQL 12	12.22 or later	
	PowerGres on Windows V9.1	12.00 or later	
	PowerGres on Windows V9.4	12.00 or later	
	PowerGres on Windows V9.6	12.00 or later	
	PowerGres on Windows V11	12.10 or later	
SQL Server monitor	SQL Server 2014	12.00 or later	
	SQL Server 2016	12.00 or later	
	SQL Server 2017	12.00 or later	
	SQL Server 2019	12.20 or later	
Tuxedo monitor	Tuxedo 12c Release 2 (12.1.3)	12.00 or later	
Weblogic monitor	WebLogic Server 11g R1	12.00 or later	
	WebLogic Server 11g R2	12.00 or later	
	WebLogic Server 12c R2 (12.2.1)	12.00 or later	
	WebLogic Server 14c (14.1.1)	12.20 or later	
Websphere monitor	WebSphere Application Server 8.5	12.00 or later	
	WebSphere Application Server 8.5.5	12.00 or later	
	WebSphere Application Server 9.0	12.00 or later	
WebOTX monitor	WebOTX Application Server V9.1	12.00 or later	
	WebOTX Application Server V9.2	12.00 or later	
	WebOTX Application Server V9.3	12.00 or later	
	WebOTX Application Server V9.4	12.00 or later	
	WebOTX Application Server V9.5	12.00 or later	
	WebOTX Application Server V10.1	12.00 or later	
	WebOTX Application Server V10.3	12.30 or later	
JVM monitor	WebLogic Server 11g R1	12.00 or later	

Continued on next page

Table 5.3 – continued from previous page

Monitor resource	Application to be monitored	EXPRESSCLUSTER Version	Remarks
	WebLogic Server 12c R2 (12.2.1)	12.00 or later	
	WebLogic Server 14c (14.1.1)	12.20 or later	
	WebOTX Application Server V9.1	12.00 or later	
	WebOTX Application Server V9.2	12.00 or later	
	WebOTX Application Server V9.3	12.00 or later	
	WebOTX Application Server V9.4	12.00 or later	
	WebOTX Application Server V9.5	12.00 or later	
	WebOTX Application Server V10.1	12.00 or later	
	WebOTX Application Server V10.3	12.30 or later	
	WebOTX Enterprise Service Bus V8.4	12.00 or later	
	WebOTX Enterprise Service Bus V8.5	12.00 or later	
	WebOTX Enterprise Service Bus V10.3	12.30 or later	
	Apache Tomcat 8.5	12.00 or later	
	Apache Tomcat 9.0	12.00 or later	
	WebSAM SVF for PDF 9.1	12.00 or later	
	WebSAM SVF for PDF 9.2	12.00 or later	
	WebSAM Report Director Enterprise 9.1	12.00 or later	
	WebSAM Report Director Enterprise 9.2	12.00 or later	
	WebSAM Universal Connect/X 9.1	12.00 or later	
	WebSAM Universal Connect/X 9.2	12.00 or later	
System monitor	N/A	12.00 or later	
Process resource monitor	N/A	12.10 or later	

5.2 Monitor resource properties

5.2.1 Info tab

The screenshot shows the 'Monitor Resource Properties' dialog box for resource 'ipw1'. The 'Info' tab is selected. It contains fields for 'Name' (ipw1) and 'Comment'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Name

The monitor resource name is displayed.

Comment (Within 127 bytes)

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

5.2.2 Monitor (common) tab

The screenshot shows the 'Monitor Resource Properties' dialog box for resource 'oraclew'. The 'Monitor(common)' tab is selected. It contains various configuration options: 'Interval*' (60 sec), 'Timeout*' (120 sec), 'Collect the dump file of the monitor process at timeout occurrence' (checkbox), 'Do Not Retry at Timeout Occurrence' (checkbox), 'Action at Timeout Occurrence' (Recover), 'Retry Count*' (2 time), 'Wait Time to Start Monitoring*' (0 sec), 'Monitor Timing' (Always/Active radio buttons), 'Target Resource*' (appli), 'Choose servers that execute monitoring' (Server), and 'Send polling time metrics' (checkbox). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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.

Do Not Retry at Timeout Occurrence

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

Do not Execute Recovery Action at Timeout Occurrence

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

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

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

- Custom monitor resource (only when Monitor Type is **Asynchronous**)
 - multi target monitor resource
 - message receive monitor resource
 - VM monitor resource
 - JVM monitor resource
 - System monitor resource
 - Process resource monitor resource
 - User mode monitor resource
-

Retry Count (0 to 999)

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

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

Wait Time to Start Monitoring (0 to 9999)

Set the wait time to start monitoring.

Monitor Timing:

Set the monitoring timing.

- **Always**
Monitoring is always performed.
- **While Activated**
Monitoring is not started until the specified resource is activated.

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



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

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.

Send polling time metrics

Enable or disable sending metrics: data on the monitoring process time taken by the monitor resource.

- If the check box is checked:
The metrics are sent.
- If the check box is not checked:
The metrics are not sent.

Note:

For using the Amazon CloudWatch linkage function, enabling this option allows you to send data on the monitoring process time taken by any monitor resource.

Send polling time metrics cannot be set for the following monitor resources:

- Message receive monitor resource
-

5.2.3 Monitor (special) tab

Some monitor resources require the parameters at the monitoring operation to be configured. The parameters are described in the explanation part about each resource.

5.2.4 Recovery Action tab

Ordinary monitor resource (except Message Receive Monitor resource)

Monitor Resource Properties | ipw1 ipw X

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

Recovery Action Execute only the final action ▼

Recovery Target * LocalServer Browse

Recovery Script Execution Count 0 time

Execute Script before Reactivation ☐

Maximum Reactivation Count 0 time

Execute Script before Failover ☐

Execute migration before Failover ☐

Failover Target Server ☒ Stable server ☐ Maximum priority server

Maximum Failover Count 0 time

Execute Script before Final Action ☐

Final Action No operation ▼

Script Settings

OK Cancel Apply

Message Receive Monitor

The screenshot shows the 'Monitor Resource Properties' dialog box for resource 'mrw1'. The 'Recovery Action' tab is selected. The 'Recovery Action' dropdown is set to 'Execute the final action'. The 'Recovery Target' is '[All Groups]' with a 'Browse' button next to it. Below this, there are three options: 'Execute migration before Failover' (unchecked), 'Failover Target Server' (radio buttons for 'Stable server' and 'Maximum priority server', with 'Stable server' selected), and 'Execute Failover to outside the Server Group' (unchecked). The 'Final Action' dropdown is set to 'Stop the cluster service and reboot OS'. At the bottom, 'Execute Script before Recovery Action' is unchecked, and there is a 'Script Settings' button. At the very bottom are '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**

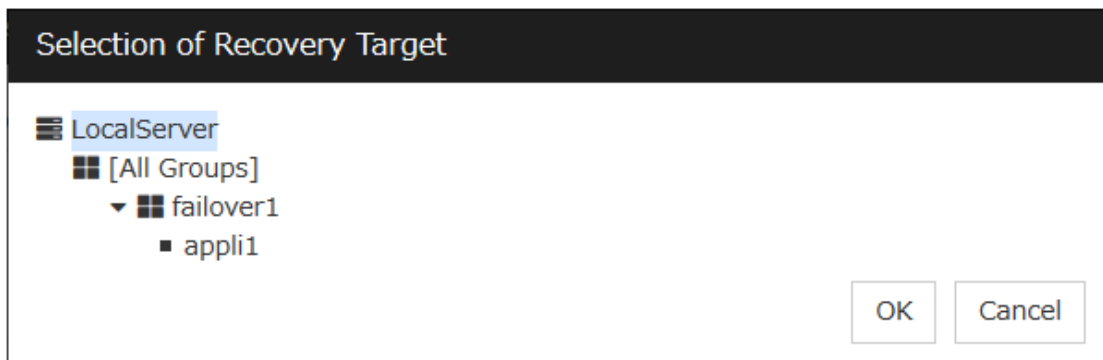
The group or group resource selected as the recovery target is reactivated repeatedly until the maximum reactivation count is reached. If the maximum reactivation count is reached while reactivation continues to fail or the same error continues to be detected after reactivation, the action selected for **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.

Edit Script

☐ User Application
☒ Script created with this product

File preaction.bat Edit View Replace

Timeout* 5 sec

Exec User ▼

OK Cancel Apply

User Application

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

Example:

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

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

Example:

```
cscript script.vbs
```

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

Script created with this product

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

File (Within 1023 bytes)

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

View

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

Edit

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

Replace

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

Timeout (1 to 9999)

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

Exec User

Specify a user who executes the script. The user can be selected from the users registered in the **Account** tab of **Cluster Properties**.

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

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 Resource

When a group resource is selected as a recovery target, the selected group resource and group resources that depend on the selected group resource are stopped.

This option is disabled when "LocalServer", "All Groups", or a group is selected.

- Stop Group

When a group or group resource is selected as a 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 recovery 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.

5.3 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.

5.3.1 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.

5.3.2 Note on application monitor resources

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

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

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

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

5.4 Setting up service monitor resources

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

5.4.1 Monitoring by service monitor resources

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

5.4.2 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.

5.5 Setting up disk RW monitor resources

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

5.5.1 Monitoring by disk RW monitor resources

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

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

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

Depending on 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.

5.5.2 Monitor (special) tab

Monitor Resource Properties | diskw1

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

File Name* C:\Check.txt

I/O size* 2000000 byte

Action on Stall* Generate an intentional stop error

Action When Diskfull Is Detected* Recover

Use Write Through Method ☐

OK Cancel Apply

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.

Stalling is detected if I/O control is not returned from the OS within the time specified in **Timeout** of the **Monitor (common)** tab.

- **No Operation**
No action is taken.
- **HW Reset**
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.

5.6 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.

5.6.1 Monitoring by IP monitor resources

IP monitor resource monitors specified IP addresses by using the ping command. If all IP addresses do not respond, the status is determined to be error.

- If you want to establish error when all of the multiple IP addresses have error, register all those IP addresses with one IP monitor resource.

The following figure is an example where all the IP addresses are registered with one IP monitor resource. If any one of the specified IP addresses is normal, IP monitor 1 is determined to be normal.

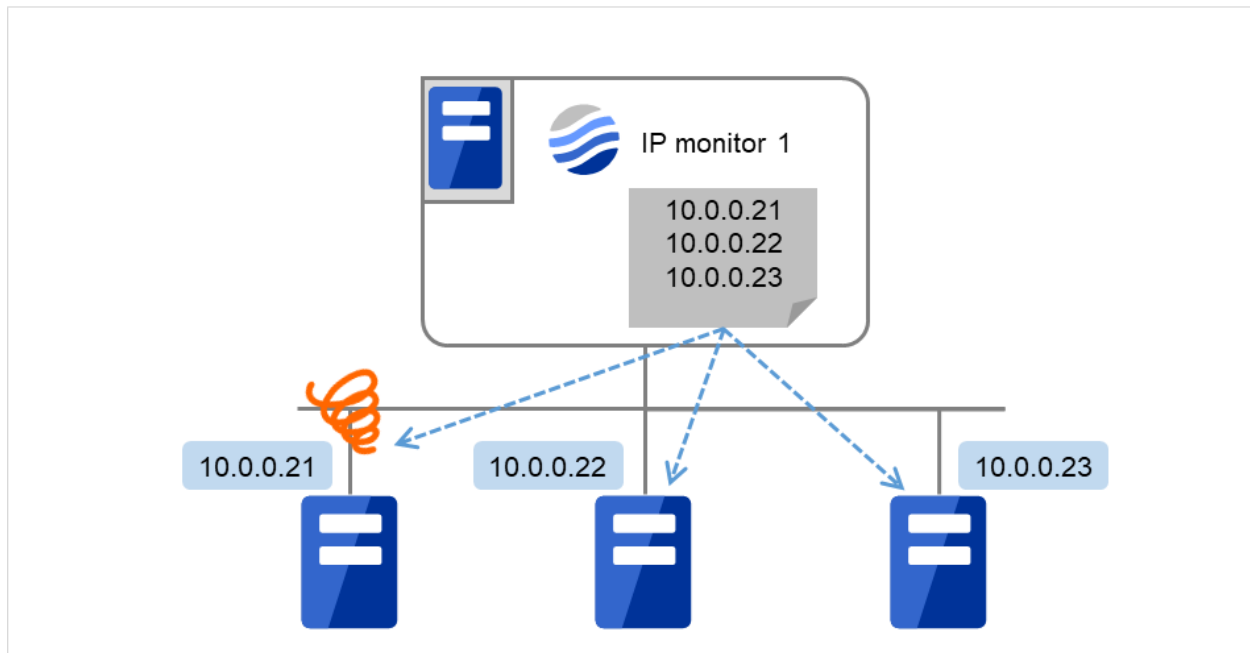


Fig. 5.1: Registering all the IP addresses with one IP monitor resource (in a normal case)

The following figure is an example where all the IP addresses are registered with one IP monitor resource. If all of the specified IP addresses have an error, IP monitor 1 is determined to have an error.

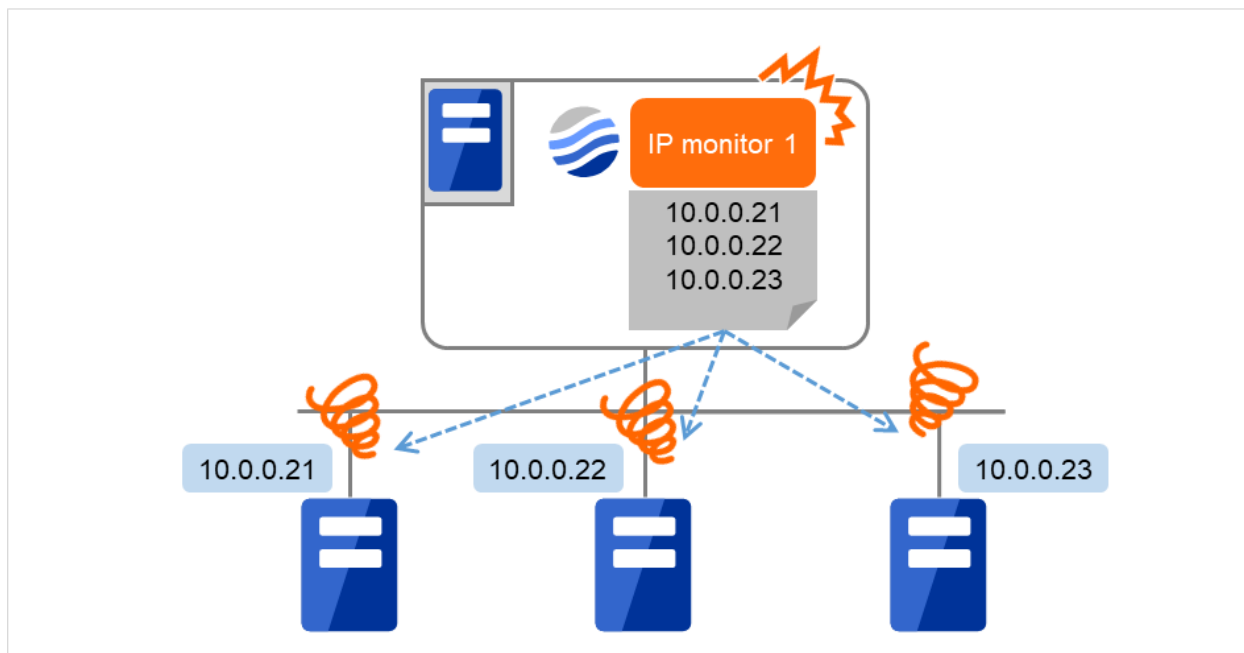


Fig. 5.2: Registering all the IP addresses with one IP monitor resource (when an error is detected)

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

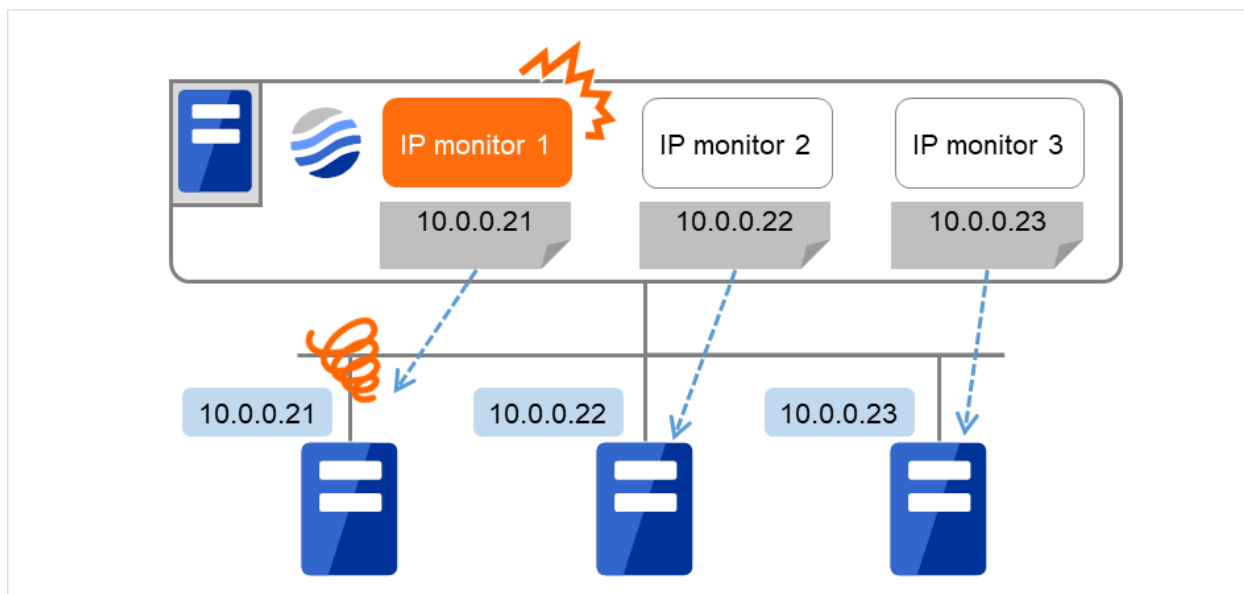


Fig. 5.3: Registering a different IP address with each of the IP monitor resources (when an error is detected)

5.6.2 Monitor (special) tab

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

Monitor Resource Properties | ipw1

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

Edit Add Remove

IP Address List

IP Address
192.168.0.1

ping Timeout* msec

OK Cancel Apply

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

The detailed setting for interface is displayed.

IP Address Settings

IP Address*

OK Cancel

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.

5.7 Setting up NIC link up/down monitor resources

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

5.7.1 Configuration and range of NIC link up/down monitoring

- When you are monitoring any NIC directly connected to another server by using a LAN 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.

5.7.2 Monitor (special) tab

Monitor Resource Properties | miiw1

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

Individually Set Up Servers

Name	IP Address
server1	192.168.0.1

Edit

Available Servers

Name

No Available Servers

Add

Remove

OK Cancel Apply

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

IP Address Settings

IP Address* 192.168.0.1

OK Cancel

IP Address (within 47 bytes)

Specify the IP address of the NIC to be monitored.

5.8 Setting up custom monitor resources

Custom monitor resources monitor system by executing an arbitrary script.

5.8.1 Monitoring by custom monitor resources

Custom monitor resources monitor system by an arbitrary script.

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

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

5.8.2 Note on custom monitor resources

- When a command for outputting a message (standard output, error output) in response to the prompt is executed as part of a batch file, the batch file may stop during execution of the command. Therefore, specify (perform redirection to) a file or nul as the message output destination.
- When the monitor type is set to **Asynchronous**, configure for the timeout a larger value than the waiting time for the monitor start.

5.8.3 Monitor (special) tab

Monitor Resource Properties | genw1 genw X

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

☐ User Application
☒ Script created with this product

File genw.bat Edit View Replace

Monitor Type ☒ Synchronous ☐ Asynchronous

Normal Return Value* 0

Kill the application when exit ☐

Wait for activation monitoring to stop before stopping the cluster ☐

Exec User ▼

OK Cancel Apply

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 Cluster WebUI. They must be prepared on the server since they cannot be edited or uploaded by the Cluster WebUI.

Script created with this product

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

File (within 1023 bytes)

Specify the script to be executed (executable shell script file or execution file) when you select User Application with its absolute path on the local disk of the server. However, no argument can be specified after the script.

View

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

Edit

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

Replace

Click here to replace the 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.

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

Forcibly Terminate Application When Stopping

Specify whether or not to forcibly terminate the application as termination of monitoring stop. If this is selected, the application is forcibly terminated instead of normal termination. This is effective only when **Monitor Type** is set to **Asynchronous**.

Exec User

Specify a user who executes the script. The user can be selected from the users registered in the **Account** tab of **Cluster Properties**.

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

Wait for activation monitoring to stop before stopping the cluster

The cluster stop waits until the custom monitor resource is stopped. This is effective only when the monitoring timing is set to **Active**.

5.9 Setting up multi target monitor resources

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

5.9.1 Note on the multi target monitor resource

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

5.9.2 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:

	Monitor resource1 status (Normal (normal))	Monitor resource1 status (Error (error))	Monitor resource1 status (Offline (offline))
Monitor resource2 status (Normal (normal))	Normal (normal)	Caution (caution)	Caution (caution)
Monitor resource2 status (Error (error))	Caution (caution)	Error (error)	Error (error)
Monitor resource2 status (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.

5.9.3 Monitor (special) tab

Monitor resources are grouped and the status of the group is monitored. You can register up to 64 monitor resources in the **Monitor Resources**.

When the only one monitor resource set in the **Monitor Resources** is deleted, the multi target monitor resource is deleted automatically.

Monitor Resource Properties | mtw1

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

Monitor Resources

Monitor Resource	Type
appliw1	appliw
genw1	genw

Available Monitor Resources

Monitor Resource	Type
ipw1	ipw
miiw1	miiw
servicew1	servicew

Add Remove

Tuning

OK Cancel Apply

Add

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

Remove

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

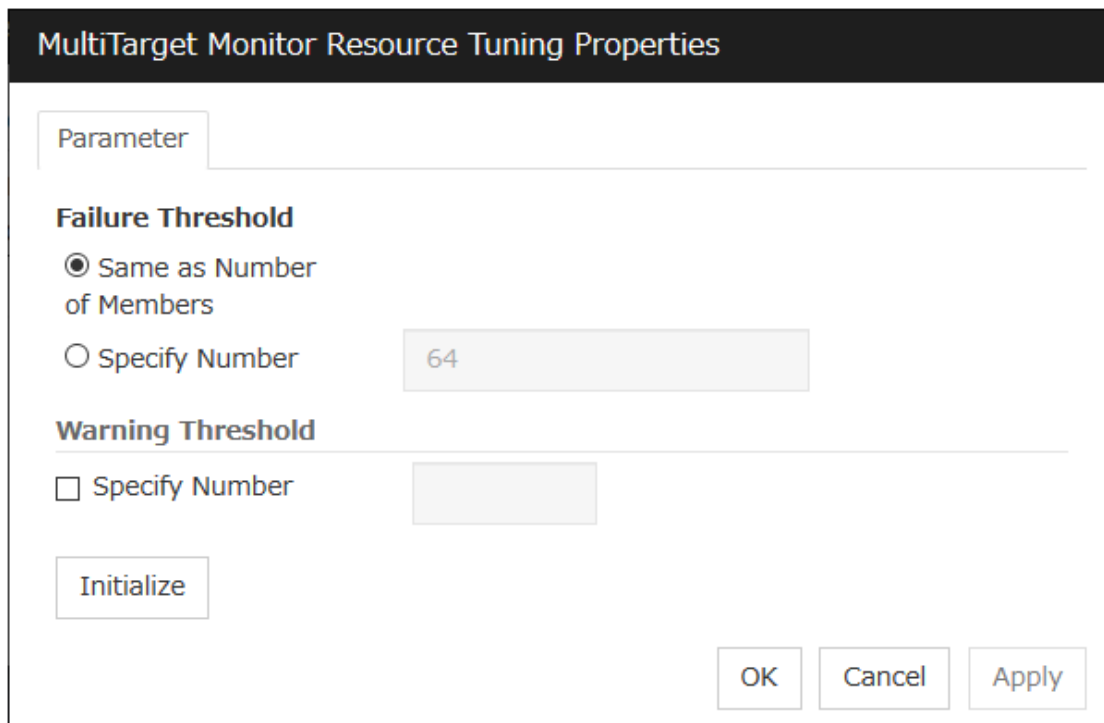
Tuning

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.



The image shows a dialog box titled "MultiTarget Monitor Resource Tuning Properties". It has a tab labeled "Parameter". Under the "Failure Threshold" section, there are two radio buttons: "Same as Number of Members" (which is selected) and "Specify Number" (with a text box containing "64"). Under the "Warning Threshold" section, there is a checkbox labeled "Specify Number" which is currently unchecked, followed by an empty text box. At the bottom left is an "Initialize" button, and at the bottom right are "OK", "Cancel", and "Apply" buttons.

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

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

5.10 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.

5.10.1 Monitoring by message receive monitor resources

When an error message is received from an outside source, the resource recovers the message receive monitor resource whose 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.

The following figure is an example of the configuration where a message receive monitor resource is used. The message receive monitor resource, when notified of the occurrence of an error, changes its status and executes the recovery action in response to error detection.

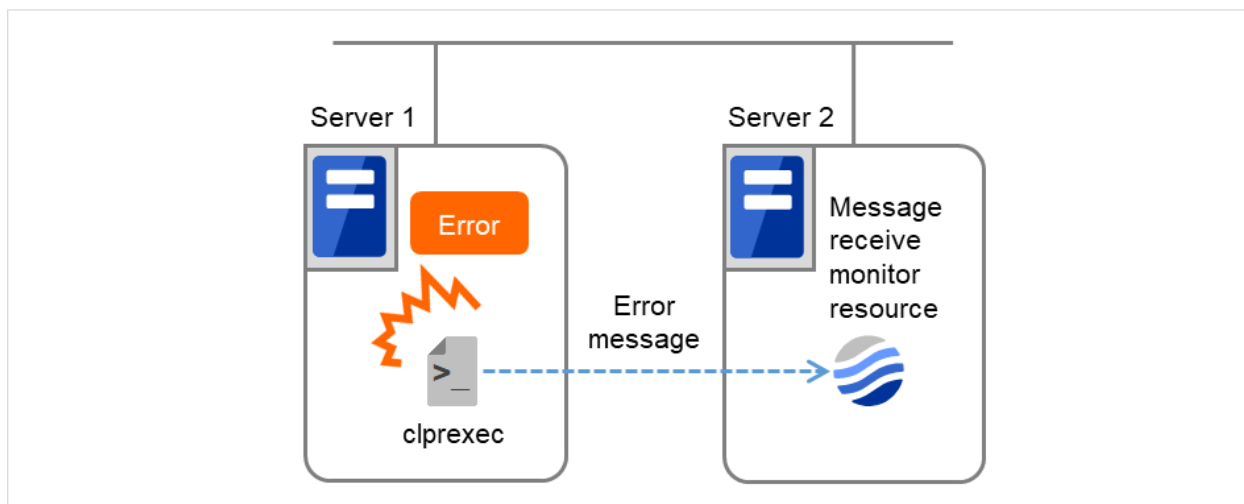


Fig. 5.4: A configuration where a message receive monitor resource is used

5.10.2 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 "EXPRESSCLUSTER X SingleServerSafe command reference" in the "EXPRESSCLUSTER X SingleServerSafe 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.

5.10.3 Monitor (special) tab

The screenshot shows a window titled "Monitor Resource Properties | mrw1" with a close button "mrw X". Inside the window, there are four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is currently selected. Below the tabs, there is a section labeled "Common" with the text "server1". Underneath, there are two fields: "Category*" with a dropdown menu showing "BMCNOTICE" and a downward arrow, and "Keyword" with a text box containing "192.168.0.1:162". At the bottom right of the dialog, there are three buttons: "OK", "Cancel", and "Apply".

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.

5.11 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.

5.11.1 Notes on VM monitor resources

- For the version of the supported virtualization platform, see "System requirements for VM resource" in "[4. Group resource details](#)".

5.11.2 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.

5.12 Setting up process name monitor resources

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

5.12.1 Notes on process name monitor resources

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

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

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

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

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

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

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

```
EXPRESSCLUSTER installation path\bin\GetProcess.vbs
```

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

Example of output file

```
20XX/07/26 12:03:13
Caption      CommandLine
services.exe C:\WINDOWS\system32\services.exe
svchost.exe  C:\WINDOWS\system32\svchost -k rpcss
explorer.exe C:\WINDOWS\Explorer.EXE
```

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

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

5.12.2 Monitoring by process name monitor resources

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

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

5.12.3 Monitor (special) tab

The screenshot shows a dialog box titled "Monitor Resource Properties | psw1". It has four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is selected. Inside this tab, there are two input fields: "Process Name*" with the value "C:¥Windows¥System32¥app" and "Minimum Process Count*" with the value "1". At the bottom right, there are three buttons: "OK", "Cancel", and "Apply".

Process Name (within 1023 bytes)

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

Default value: None

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

- prefix search : <character string included in process name>*
- suffix search : *<character string included in process name>
- partial search : *<character string included in process name>*

Minimum Process Count (1 to 999)

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

5.13 Setting up DB2 monitor resources

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

5.13.1 Notes on DB2 monitor resources

For the supported version of DB2, see "5.1.2. *Applications supported by monitoring options*" in "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 section "5.13.2. *Monitoring by DB2 monitor resources*", note the following:

At "Level 1", a monitor error occurs if there is no monitor table at the start of monitoring. Create a monitor table as shown below.

At "Level 2", if there is no monitor table at the start of monitoring, EXPRESSCLUSTER automatically creates a monitor table. At the same time, a message notifying that there is no monitor table is displayed in the Cluster WebUI alert log.

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
```

5.13.2 Monitoring by DB2 monitor resources

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

- **Level 1 (monitoring by select)**
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
An error is recognized if:
 - (1) A database connection could not be established
 - (2) An error message is sent in response to an SQL statement
- **Level 2 (monitoring by update/select)**
Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.
An error is recognized if:
 - (1) A database connection could not be established
 - (2) An error message is sent in response to an SQL statement
 - (3) The written data is not the same as the read data

5.13.3 Monitor (special) tab

Monitor Resource Properties | db2w1

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

Monitor Level* Level 2 (monitoring by update/select) ▾

Database Name* DB2DB

Instance Name* DB2

User Name db2admin

Password [masked] Change

Monitor Table Name* DB2WATCH

OK Cancel Apply

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.

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

Default value: DB2WATCH

5.14 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.

5.14.1 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.

5.14.2 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.

5.14.3 Monitor (special) tab

The screenshot shows a window titled "Monitor Resource Properties | ftpw1" with a close button (X) in the top right corner. The window has four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is currently selected. Inside this tab, there are four input fields: "IP Address*" with the value "127.0.0.1", "Port Number*" with the value "21", "User Name" (empty), and "Password" (empty). To the right of the "Password" field is a "Change" button. At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Apply".

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

5.15 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.

5.15.1 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 do not support client authentication or digest authentication.

5.15.2 Monitoring by HTTP monitor resources

HTTP monitor resources monitor the following:

Monitors the HTTP daemon by connecting to the HTTP daemon on the server and issuing a HTTP request.

This monitor resource determines the following results as an error:

- (1) an error is notified during the connection to the HTTP daemon.
- (2) the response message to the HTTP request is not started with "/HTTP"
- (3) the status code for the response to the HTTP request is in 400s and 500s (when URI other than the default is specified to the request URI)

5.15.3 Monitor (special) tab

Monitor Resource Properties | httpw1

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

Connecting Destination* 127.0.0.1

Port Number* 80

Monitor URI

Protocol ☒ HTTP ☐ HTTPS

Request Type ☒ HEAD ☐ GET

User Name

Password Change

OK Cancel Apply

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.

Note: If you select HTTPS, GET requests are issued regardless of which request type you choose.

Request Type

Specify a type of HTTP request for accessing the HTTP server. Setting this parameter is mandatory.

Default value: HEAD

User Name(within 255 bytes)

Specify a user name for logging in to the HTTP server.

This specification is necessary only for basic authentication.

Default value: None

Password(within 255 bytes)

Specify a password for logging in to the HTTP server.

This specification is necessary only for basic authentication.

Default value: None

5.16 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.

5.16.1 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.

5.16.2 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.

5.16.3 Monitor (special) tab

Monitor Resource Properties | imap4w1 imap4w X

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

IP Address* 127.0.0.1

Port Number* 143

User Name

Password Change

Authentication Method ☒ AUTHENTICATE LOGIN ☐ LOGIN

OK Cancel Apply

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 189 bytes)

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

Default value: None

Authentication Method

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

- **AUTHENTICATE LOGIN** (default value)

The encryption authentication method that uses the AUTHENTICATE LOGIN command.

- **LOGIN**

The plaintext method that uses the LOGIN command.

5.17 Setting up ODBC monitor resources

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

5.17.1 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 section "[5.17.2. Monitoring by ODBC monitor resources](#)", note the following:

At "Level 1", a monitor error occurs if there is no monitor table at the start of monitoring. Create a monitor table as shown below.

At "Level 2", if there is no monitor table at the start of monitoring, EXPRESSCLUSTER automatically creates a monitor table. At the same time, a message notifying that there is no monitor table is displayed in the Cluster WebUI alert log.

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;
```

5.17.2 Monitoring by ODBC monitor resources

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

- Level 1 (monitoring by select)
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.
An error is recognized if:
 - (1) A database connection could not be established
 - (2) An error message is sent in response to an SQL statement
- Level 2 (monitoring by update/select)
Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / drop) type.
An error is recognized if:
 - (1) A database connection could not be established
 - (2) An error message is sent in response to an SQL statement
 - (3) The written data is not the same as the read data

5.17.3 Monitor (special) tab

The screenshot shows the 'Monitor Resource Properties' dialog box for resource 'odbcw1'. The 'Monitor(special)' tab is selected. The 'Monitor Level' is set to 'Level 2 (monitoring by update/select)'. The 'Data Source Name' is 'ODBC1'. The 'User Name' field is empty. The 'Password' field is masked with a grey box, and there is a 'Change' button next to it. The 'Monitor Table Name' is 'ODBCWATCH'. At the bottom right, there are 'OK', 'Cancel', and 'Apply' buttons.

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.

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

Default value: ODBCWATCH

5.18 Setting up Oracle monitor resources

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

5.18.1 Notes on Oracle monitor resources

For the supported Oracle version, see "5.1.2. *Applications supported by monitoring options*" in "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, for each monitor level the following access permissions must be provided for that user (if the sysdba permission is not provided):

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

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

Regarding the monitor levels described in the next section "5.18.2. *Monitoring by Oracle monitor resources*", note the following:

At "Level 1", a monitor error occurs if there is no monitor table at the start of monitoring. Create a monitor table as shown below.

At "Level 2", if there is no monitor table at the start of monitoring, EXPRESSCLUSTER automatically creates a monitor table. At the same time, a message notifying that there is no monitor table is displayed in the Cluster WebUI alert log.

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.

5.18.2 Monitoring by Oracle monitor resources

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

- Level 0 (database status)
The Oracle management table (V\$INSTANCE table) is referenced to check the DB status (instance status). This level corresponds to simplified monitoring without SQL statements being executed for the monitor table. An error is recognized if:
 - (1) The 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

5.18.3 Monitor (special) tab

Monitor Resource Properties | oraclew1 oraclew X

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

Monitor Type* Listener and Instance Monitor ▼

Monitor Level* Level 2 (monitoring by update/select) ▼

Connect Command* orcl

User Name sys

Password Change

OS Authentication ☐

Authority Method ☒ SYSDBA ☐ DEFAULT

Monitor Table Name* ORAWATCH

ORACLE_HOME

Character Set* (Following the setting of the application) ▼

Collect detailed application information at failure occurrence ☐

Collection Timeout 600 秒

Set error during Oracle initialization or shutdown ☐

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 properties, `ORACLE_HOME` must be set.

If `ORACLE_HOME` is not set, only connection operations for the items specified in the connect string are monitored. Use this to attempt recovery by restarting the Listener service upon a connection error.

Selecting this setting causes the monitor level setting to be ignored.

- **Monitor Instance only**

A 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 properties, `ORACLE_HOME` must be set. This is used for direct instance monitoring and recovery action setting without routing through the listener.

A multi-tenant Oracle12c database cannot be monitored using a BEQ connection.

If `ORACLE_HOME` is not set, only the connection specified by the connect string is established,

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

Default value: 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.

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

Default value: ORAWATCH

ORACLE_HOME (within 255 bytes)

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

Default value: None

Character Set

Select the character set for Oracle. 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.

Do not perform the manual operation such as Group stop or Group move while collecting information. Monitoring process may not work normally depending on the timing of the manual operation.

Collection Timeout (1 to 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

5.19 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.

5.19.1 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.

5.19.2 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.

5.19.3 Monitor (special) tab

The screenshot shows a dialog box titled "Monitor Resource Properties | pop3w1" with a close button (X) in the top right corner. The dialog has four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is currently selected. It contains the following fields and controls:

- IP Address***: A text box containing "127.0.0.1".
- Port Number***: A text box containing "110".
- User Name**: An empty text box.
- Password**: A password field (masked) with a "Change" button to its right.
- Authentication Method**: Two radio buttons:
• ☒ APOP
• ☐ USER/PASS

At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Apply".

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.

5.20 Setting up PostgreSQL monitor resources

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

5.20.1 Notes on PostgreSQL monitor resources

For the supported PostgreSQL/PowerGres version, see " 5.1.2. *Applications supported by monitoring options* " in "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 PostgreSQL9.6 bin.)

```
C:\Program Files\PostgreSQL\9.6\bin
```

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

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

Regarding the monitor levels described in the next section "Monitoring by PostgreSQL monitor resources", note the following:

At "Level 1", a monitor error occurs if there is no monitor table at the start of monitoring. Create a monitor table as shown below.

At "Level 2", if there is no monitor table at the start of monitoring, EXPRESSCLUSTER automatically creates a monitor table. At the same time, a message notifying that there is no monitor table is displayed in the Cluster WebUI alert log.

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;
```

5.20.2 Monitoring by PostgreSQL monitor resources

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

- Level 1 (monitoring by select)
Monitoring with only reference to the monitor table. SQL statements issued to the monitor table are of (select) type.

An error is recognized if:

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

- Level 2 (monitoring by update/select)
Monitoring with reference to and update of the monitoring table. One SQL statement can read/write numerical data of up to 10 digits. At monitoring start/end, the monitor table is created/deleted. SQL statements issued to the monitor table are of (create / update / select / reindex / drop / vacuum) type.

An error is recognized if:

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

5.20.3 Monitor (special) tab

Monitor Level

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

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

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

Database Name (within 255 bytes)

Specify the database name to be monitored. 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.

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

Default value: PSQLWATCH

Set error during PostgreSQL initialization or shutdown

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

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

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

Default value: Enabled

5.21 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.

5.21.1 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.

5.21.2 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.

5.21.3 Monitor (special) tab

The screenshot shows the 'Monitor Resource Properties' dialog box for a resource named 'smtpw1'. The 'Monitor(special)' tab is selected, displaying fields for configuring SMTP monitoring. The fields include 'IP Address*' (127.0.0.1), 'Port Number*' (25), 'User Name' (empty), 'Password' (masked with a grey box and a 'Change' button), 'Authentication Method' (radio buttons for 'CRAM-MD5' and 'LOGIN', with 'CRAM-MD5' selected), and 'E-mail Address' (empty). At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Field	Value
IP Address*	127.0.0.1
Port Number*	25
User Name	
Password	[Masked]
Authentication Method	CRAM-MD5 (selected)
E-mail Address	

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

5.22 Setting up SQL Server monitor resources

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

5.22.1 Notes on SQL Server monitor resources

For the supported SQL Server version, see "5.1.2. *Applications supported by monitoring options*" in "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 section "5.22.2. *Monitoring by SQL Server monitor resources*", note the following:

At "Level 1", a monitor error occurs if there is no monitor table at the start of monitoring. Create a monitor table as shown below.

At "Level 2", if there is no monitor table at the start of monitoring, EXPRESSCLUSTER automatically creates a monitor table. At the same time, a message notifying that there is no monitor table is displayed in the Cluster WebUI alert log.

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

Create a monitor table using either of the following methods:

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

- When SET IMPLICIT_TRANSACTIONS is OFF:

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

- When SET IMPLICIT_TRANSACTIONS is ON:

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

5.22.2 Monitoring by SQL Server monitor resources

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

- Level 0 (database status)

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

An error is recognized if:

- (1) The database status is not online

- Level 1 (monitoring by select)

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

An error is recognized if:

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

- Level 2 (monitoring by update/select)

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

An error is recognized if:

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

5.22.3 Monitor (special) tab

Monitor Level

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

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

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

Database Name (within 255 bytes)

Specify the database name to be monitored. 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.

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

Default value: SQLWATCH

ODBC Driver Name (within 255 bytes)

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

Select **SQL Server Native Client 11.0** in SQL Server 2014.

Select ODBC Driver 13 for SQL Server in SQL Server 2016, SQL Server 2017.

Select ODBC Driver 17 for SQL Server in SQL Server 2019.

Default value: ODBC Driver 13 for SQL Server

5.23 Setting up Tuxedo monitor resources

Tuxedo monitor resources monitor Tuxedo that runs on the server.

5.23.1 Notes on Tuxedo monitor resources

For the supported Tuxedo version, see "5.1.2. Applications supported by monitoring options" in "5. Monitor resource details".

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

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

5.23.2 Monitoring by Tuxedo monitor resources

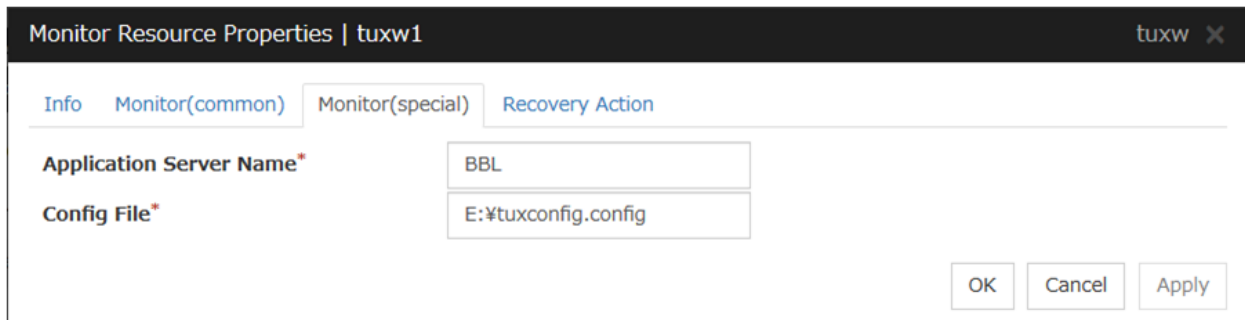
Tuxedo monitor resources monitor the following:

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.

5.23.3 Monitor (special) tab



The screenshot shows a dialog box titled "Monitor Resource Properties | tuxw1". It has four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is selected. Inside this tab, there are two labeled text input fields: "Application Server Name*" with the value "BBL" and "Config File*" with the value "E:\tuxconfig.config". At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Apply".

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

5.24 Setting up Weblogic monitor resources

Weblogic monitor resources monitor WebLogic that runs on the server.

5.24.1 Notes on Weblogic monitor resources

For the supported WebLogic version, see "5.1.2. Applications supported by monitoring options" in "5. Monitor resource details".

If WebLogic cannot run immediately after startup, it is recognized as an error. To prevent this, adjust **Wait Time to Start Monitoring**. Or, make sure that WebLogic starts first (for example, by specifying the script resource and application resource that starts WebLogic as the monitor target resource).

If the selected monitoring method is WLST for this monitor resource, the monitoring requires a JAVA environment. Since the JAVA functions are used by the application server system, a stall of JAVA (if any) may be recognized as an error.

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

5.24.2 Monitoring by Weblogic monitor resources

Weblogic monitor resource monitors the following:

- Monitoring method: if REST API is selected

WebLogic offers REST APIs called WebLogic RESTful management services.

The REST APIs allow you to monitor the application server.

As a result, an error is considered to be found if:

1. There is an error message in response to the REST API.

Note: Compared with the WLST monitoring method, REST API can reduce the CPU load of the application server under the monitoring.

- Monitoring method: if WLST is selected

Monitors the application server by performing connect with the "weblogic.WLST" command.

This monitor resource determines the following results as an error:

1. An error reporting as the response to the connect.

The operations are as follows, based on **Authentication Method**.

- DemoTrust: SSL authentication method using authentication files for demonstration of WebLogic
- CustomTrust: SSL authentication method using user-created authentication files
- Not Use SSL: SSL authentication method is not used.

5.24.3 Monitor (special) tab

Monitor Resource Properties | wls1 wls1 X

[Info](#)
[Monitor\(common\)](#)
[Monitor\(special\)](#)
[Recovery Action](#)

IP Address*

Port Number*

Monitor Type

☒ REST API
 ☐ WLST

Protocol

☒ HTTP
 ☐ HTTPS

User Name*

Password

Account Shadow

☐ On

Config File
 Key File

☒ Off

User Name
 Password

Authority Method

Authority Method

Key Store File

Install Path

Add command option

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 (1 to 65535)

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

Default value: 7002

Monitor Method

Specify the method of monitoring the server. Setting this parameter is mandatory.

Default value: REST API

Protocol

Specify the protocol of the server to be monitored. Setting this parameter is mandatory if REST API is selected in **Monitor Method**.

Default value: HTTP

User Name (Within 255 bytes)

Specify the name of the WebLogic user. Setting this parameter is mandatory if REST API is selected in **Monitor Method**.

Default value: weblogic

Password (Within 255 bytes)

Specify the password for WebLogic, if necessary, with REST API selected in **Monitor Method**.

Default value: None

Account Shadow

When you specify a user name and a password directly, select **Off**. If not, select **On**. 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: None

Authority Method

Specify the authentication method when connecting to an application server. Specifying this item cannot be omitted.

Specify DemoTrust or Custom Trust for **Authority Method**, in order to execute monitoring by using the SSL communication.

It is determined whether to use DemoTrust or CustomTrust, according to the setting of Weblogic Administration Console.

When Keystores of Weblogic Administration Console is set to Demo Identity and Demo Trust, specify Demo Trust. In this case, you do not need to make settings for Key Store File.

When Keystores of Weblogic Administration Console is set to Custom Identity and Custom Trust, specify Custom Trust. In this case, you need to make settings for Key Store File.

Default value: DemoTrust

Key Store File (within 1023 bytes)

Specify the authentication file when authenticating SSL. You must specify this when the **Authority Method** is **CustomTrust**. Set the file specified in Custom Identity Key Store File on Weblogic Administration Console.

Default value: None

Installation Path (within 255 bytes)

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

Default value: C:\Oracle\Middleware\Oracle_Home\wlserver

Additional command option (within 1023 bytes)

Set this value when changing the option to be passed to the webLogic.WLST command.

Default value: -Dwlst.offline.log=disable -Duser.language=en_US

5.25 Setting up WebOTX monitor resources

WebOTX monitor resources monitor WebOTX that runs on the server.

5.25.1 Notes on WebOTX monitor resources

For the supported WebOTX version, see "5.1.2. Applications supported by monitoring options" in "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.

WebOTX monitor resource monitors application servers by using the otxadmin.bat command which Web OTX offers. \${AS_INSTALL}\bin where the otxadmin.bat command is arranged is not included in environment variable PATH any more in WebOTX V10.1 or later. When monitoring WebOTX V10.1 or later, configure either of the following settings.

- Add the path where **otxadmin.bat** command is located to the system environment variable, PATH.
- Set the install path of WebOTX Application Server to **Install Path**. (e.g. C : \WebOTX)

5.25.2 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.

5.25.3 Monitor (special) tab

Monitor Resource Properties | obxw1

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

Connecting Destination* localhost

Port Number* 6212

User Name* user1

Password Change

Install Path C:\WebOTX

OK Cancel Apply

Connecting Destination (Within 255 bytes)

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

Default value: localhost

Port Number (1 to 65535)

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

When monitoring a WebOTX user domain, specify the management port number for the WebOTX domain. The management port number is the number which was set for "domain.admin.port" of <domain_name>.properties when the domain was created. Refer to the WebOTX documents for details of <domain_name>.properties

Default value: 6212

User Name (Within 255 bytes)

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

When monitoring a WebOTX user domain, specify the login user name for the WebOTX domain.

Default value:None

Password (Within 255 bytes)

Specify the password of WebOTX.

Default value: None

Install Path (Within 255 bytes)

Specify the install path of WebOTX Application Server. You must configure this setting when monitoring WebOTX Application Server V10.1 or later.

Default value: None

5.26 Setting up Websphere monitor resources

Websphere monitor resources monitor WebSphere that runs on the server.

5.26.1 Notes on Websphere monitor resources

For the supported WebSphere version, see "5.1.2. Applications supported by monitoring options" in "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.

5.26.2 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.

5.26.3 Monitor (special) tab

The screenshot shows a window titled "Monitor Resource Properties | wasw1" with a close button "wasw X". It has four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is active. It contains the following fields and controls:

- Application Server Name***: Text box containing "server1".
- Profile Name***: Text box containing "default".
- User Name***: Text box containing "user1".
- Password**: Masked text box (gray) with a "Change" button to its right.
- Install Path***: Text box containing "C:\Program Files\IBM\We..." with a dropdown arrow.

At the bottom right are three buttons: "OK", "Cancel", and "Apply".

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

5.27 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.

5.27.1 Note on JVM monitor resources

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

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

The setting of **Monitor(common)** tab-**Retry Count** is invalid. When you'd like to delay error detection, please change the setting of **Cluster Properties-JVM monitor** tab-**Resource Measurement Settings [Common]-Retry Count**.

The status of the JVM monitor resource is "Warning" from when monitoring is started to when the monitoring processing is actually performed. In this status, the following message is output to the alert log. Ignore this message because it only indicates just that monitoring is in preparation.

Monitor jaw is in the warning status. (100 : not ready for monitoring.)

5.27.2 Monitoring by JVM monitor resources

JVM monitor resource monitors the following:

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

The monitor resource determines the following results as errors:

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

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

- The value falls below the threshold when restarting the monitoring after the recovery action.

Note: Collect Cluster Logs in the Cluster WebUI does not handle the configuration file and log files of the target (WebLogic or WebOTX).

The following figure shows the monitoring operation by the JVM monitor resource.

Monitoring of the target Java VM is started. ... a)

JMX (Java Management Extensions) is used for monitoring Java VM.

Java Resource Agent periodically obtains the amount of used resources through JMX to check the status of Java VM.

When the status changes from Normal to Error, an error in Java VM is indicated in Cluster WebUI, where its status and alert can be checked. ... b)

An error is notified to the event log and JVM operation log. ... c)

If an alert service is used, a notification via an e-mail is available.

After a), if the status is changed from Error to Normal, Cluster WebUI indicates Java VM has been restored. ... d)

The restoration of Java VM is notified to the event log and JVM operation log. ... e)

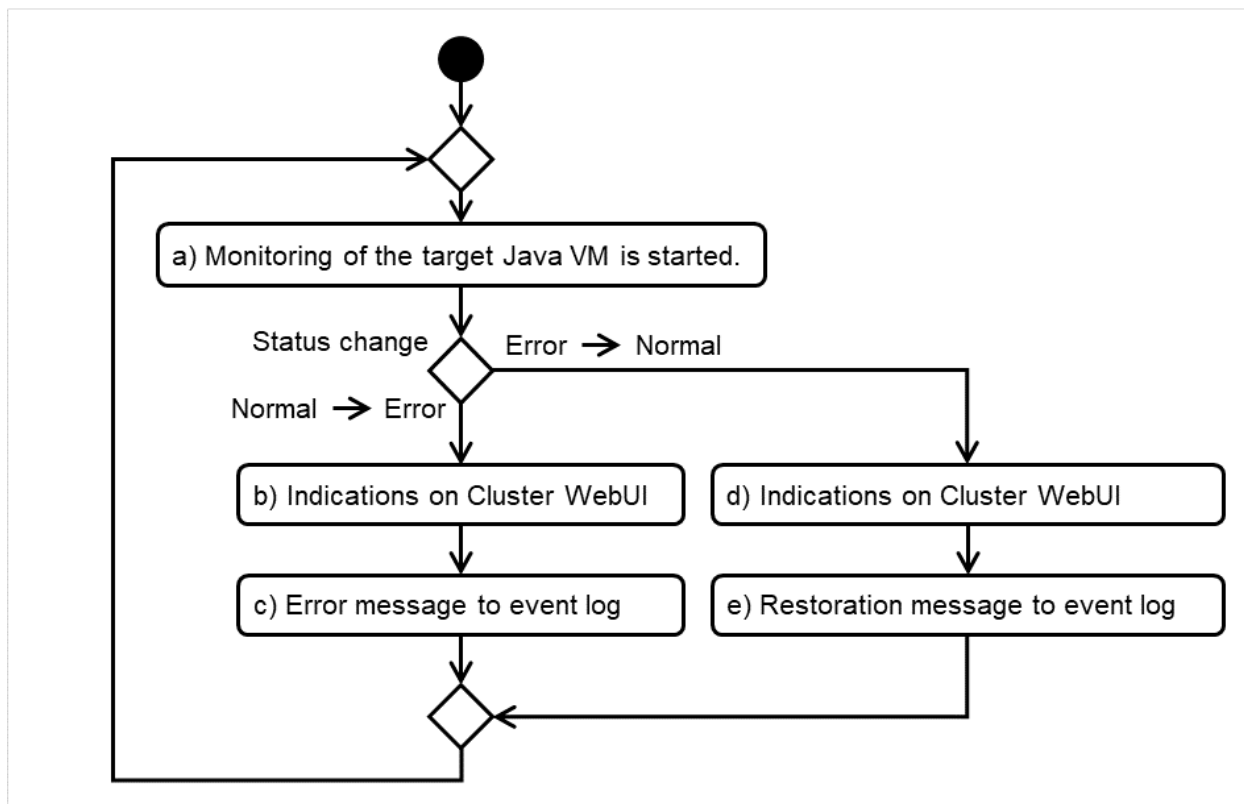


Fig. 5.5: Monitoring flow by the JVM monitor resource

The operations performed if an error persists are as described below.

If the value consecutively exceeds the threshold the number of the error decision threshold, it is determined as an error.

After determining as an error, even if the value consecutively exceeds the number of times of the error decision threshold again, Cluster WebUI does not display an alert again.

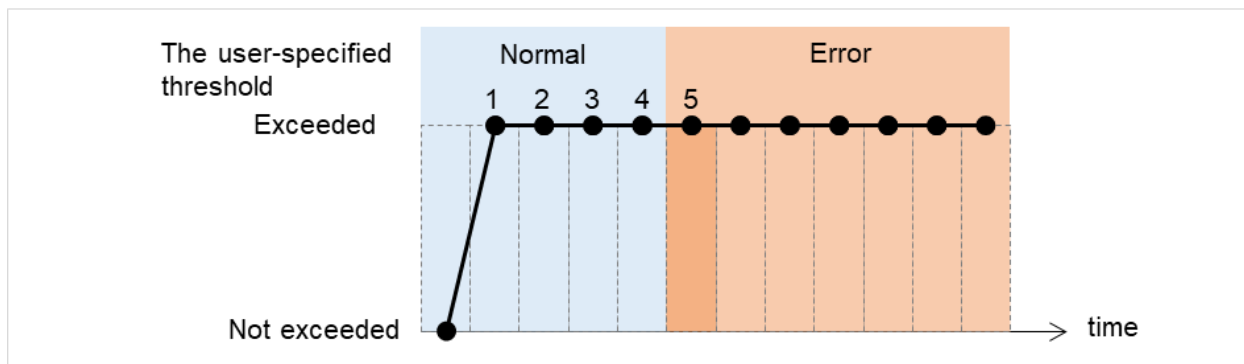


Fig. 5.7: Behavior with an error persistent

The following example describes the case of monitoring Full GC (Garbage Collection).

In this example, the horizontal axis shows the lapse of time.

The upper part of the figure shows whether Full GC occurred or not, while the lower part shows how many times Full GC occurred consecutively.

The JVM resource detects an error when Full GC consecutively occurs the number of times of the error judgment threshold.

With the error decision threshold set at five times, the JVM resource detects an error when the Full GC has been detected five times.

Full GC has a significant influence on the system, thus the recommended error threshold is 1 time.

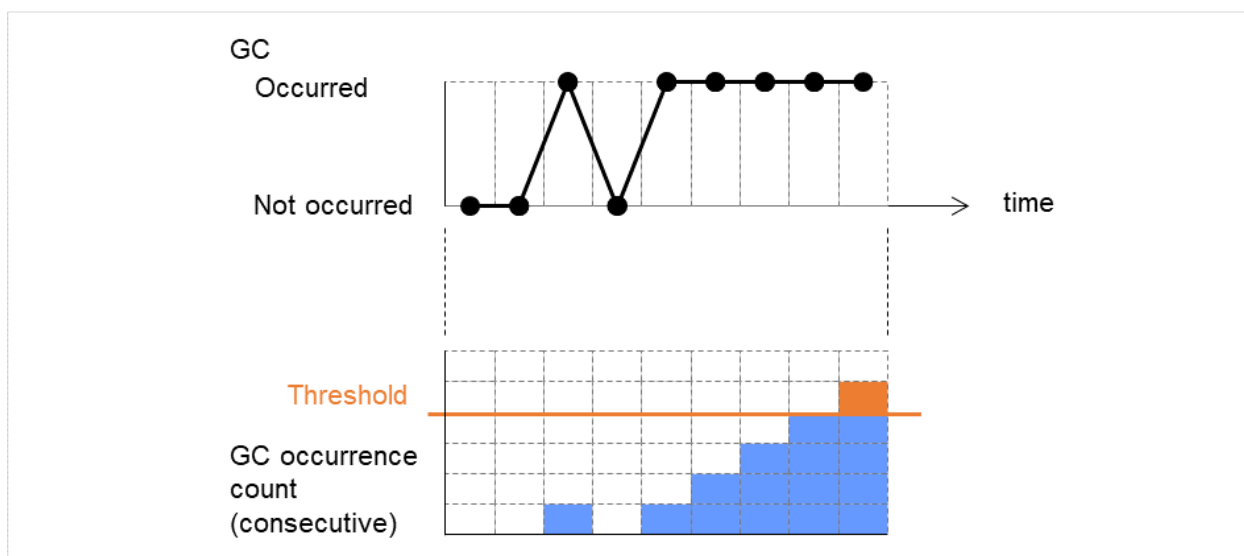


Fig. 5.8: Monitoring image (with the error decision threshold set at five times)

5.27.3 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 "5.27.5. *Linking with the BIG-IP Local Traffic Manager*".

Distributed nodes are servers that are subject to load balancing, while the distributed node module is installed in the distributed nodes. The distributed node module is included in InterSec/LB400*.

To use the function, configure the settings through the Cluster WebUI **Cluster Properties** -> **JVM Monitor** tab -> **Load Balancer Linkage Settings** dialog box.

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 InterSec/LB400*, configure the health check interval, health check timeout, and retry count to determine the node down state by the health check with the health check (distributed node) interval parameter, HTTP health check timeout parameter, and health check (distributed node) count parameter, that are accessible from **ManagementConsole** for the load balancer -> **LoadBalancer** -> **System Information**.

Configure the parameters using the following as a reference.

20-second wait time \geq (health check (distributed node) interval + HTTP health check timeout) x health check (distributed node) count

- Settings of the JVM monitor resource health check function for the load balancer:
 - Health check (distributed node) interval: 10 seconds
 - HTTP health check timeout: 1 second
 - Health check (distributed node) count: 2 times

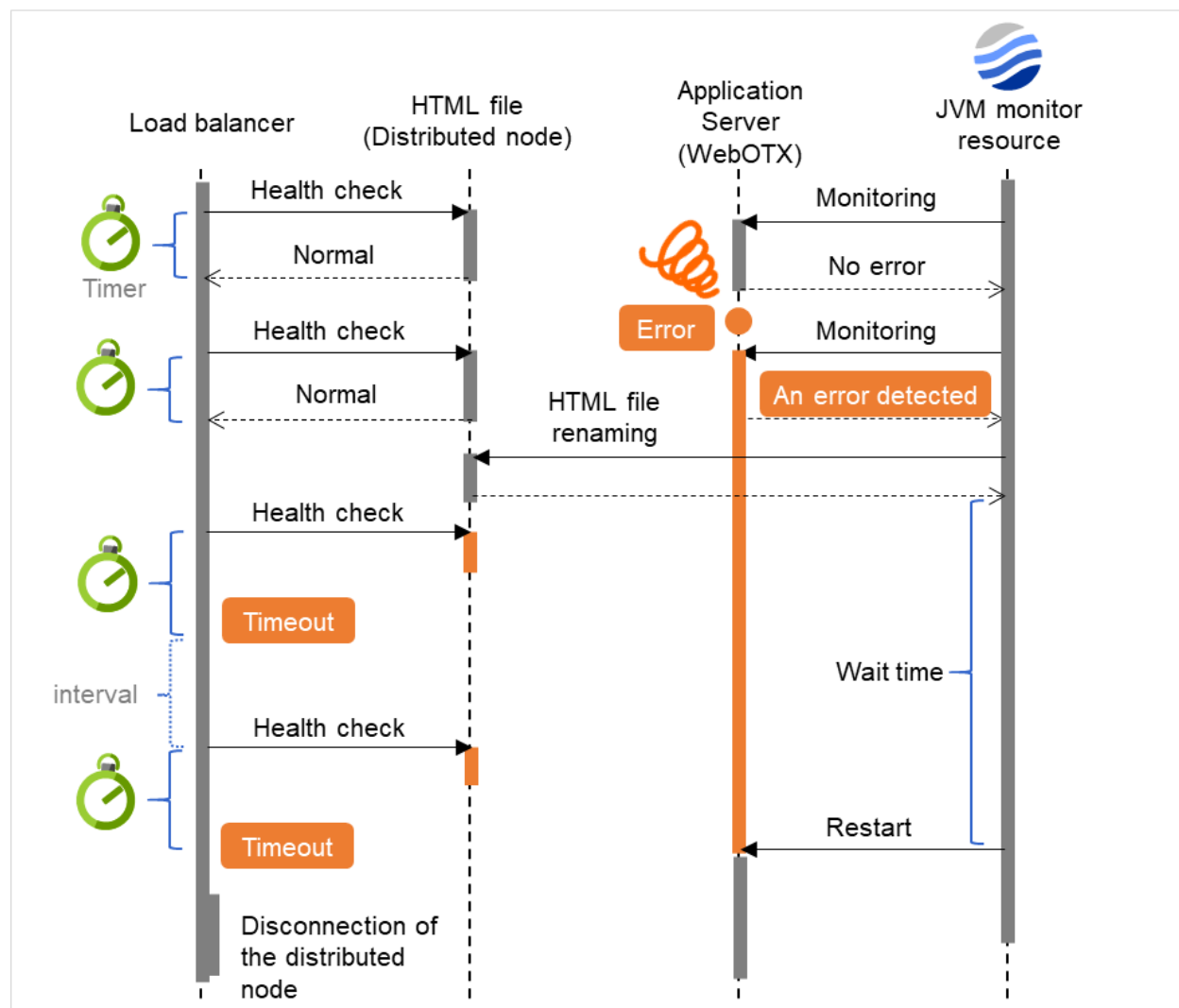


Fig. 5.9: JVM monitor resource health check function for the load balancer

Settings must also be specified on the load balancer side.

For InterSec/LB400*, specify load dispersion environment settings by using the Management Console of the load balancer.

5.27.4 Linking with the load balancer (target Java VM load calculation function)

Target load balancer: InterSec/LB400*

JVM monitor resources can link with the load balancer. 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 " *5.27.5. Linking with the BIG-IP Local Traffic Manager*".

Distributed nodes are servers that are subject to load balancing, while the distributed node module is installed in the distributed node. The distributed node module is included in InterSec/LB400*.

To use 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 Properties - Memory** dialog box - **Monitor Heap Memory Rate - Total Usage**
- **Properties - Monitor(special)** tab -> **Tuning Properties - Load Balancer Linkage** dialog box - **Memory Pool Monitor**

According to the following steps, first install the distributed node module on each server.

Note: Execute the command from an account having the Administrator privilege.

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

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. <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 Properties - Memory** tab -

Monitor Heap Memory Rate - Total Usage.

Java VM load (%) = current memory usage (MB) x 100/threshold (MB)

For the distributed node module installed on a server on which JVM 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 of the load calculation function for the distributed node module:
 - Command execution interval: JVMsaverCheckInterval (in seconds)

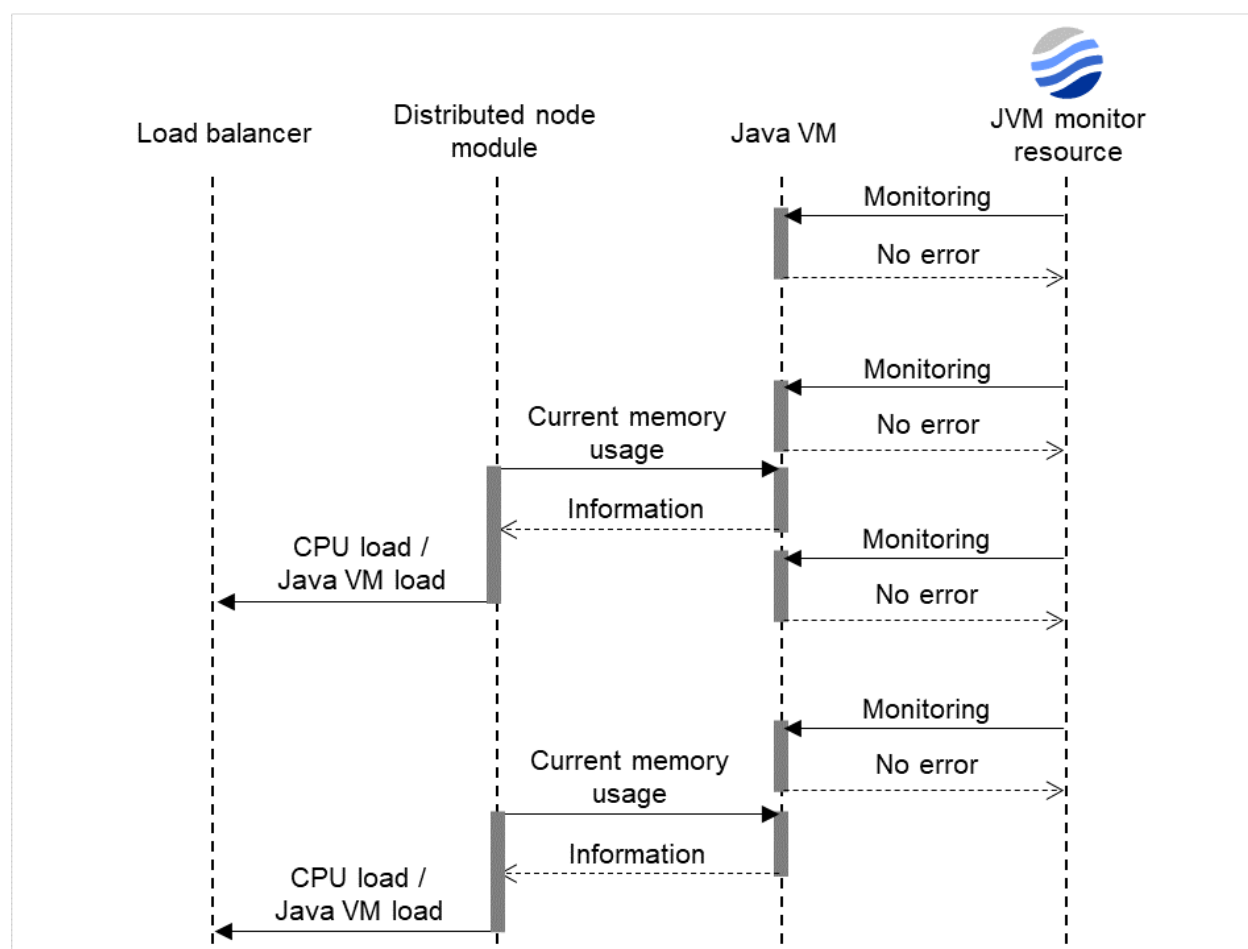


Fig. 5.10: Load calculation function for the distributed node module

Settings must also be specified on the load balancer side.

In the case of InterSec/LB400*, specify load dispersion environment settings by using the Management Console of the load balancer.

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 -> Administrative Tools -> Services**.

5.27.5 Linking with the BIG-IP Local Traffic Manager

Target load balancer: BIG-IP Local Traffic Manager

The JVM monitor resource can link with BIG-IP LTM. Hereafter, the explanation assumes the use of Tomcat as the application server to be monitored. Linkage with BIG-IP LTM offers the distributed node control function and the target Java VM load calculation function.

The linkage between BIG-IP LTM and the JVM monitor resource is realized with the BIG-IP series API (iControl).

The distributed node is the load distribution server, and the linkage module is that which is installed in each distributed node. The linkage module is contained in Java Resource Agent.

To use the distributed node control function, specify the setting with Cluster WebUI **Cluster Properties -> JVM monitor** tab -> **Load Balancer Linkage Settings** dialog box, **JVM monitor resource Properties - Monitor(special)** tab - **Tuning Properties - Load Balancer Linkage** tab.

To use the target Java VM load calculation function, specify the setting with Cluster WebUI **cluster properties -> JVM monitor** tab -> **Load Balancer Linkage Settings** dialog box.

The following BIG-IP LTM linkage error message is output to the JVM operation log. For details, see "JVM monitor resource log output messages" in "Error messages" in the "Reference Guide" for EXPRESSCLUSER.

```
Error: Failed to operate clpjra_bigip.[error code]
```

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

After updating the status of the distributed node of BIG-IP LTM, the JVM monitor waits until the number of connections of the distributed node falls to 0. After waiting, it executes **Restart Command** specified on the **JVM monitor resource Properties - Monitor(special)** tab -> **Tuning Properties - Load Balancer Linkage** tab. It does not execute the action specified by **Restart Command** if the number of connections of the distributed node does not fall to 0, even if **Timeout** elapses, as specified on the **JVM monitor resource Properties - Monitor(special)** tab -> **Tuning Properties - Load Balancer Linkage** tab.

When the JVM monitor detects a Tomcat failure recovery, it uses iControl to update the status of the BIG-IP LTM distributed node from "disable" to "enable." In this case, it does not execute the action specified by **Restart Command** specified on the JVM monitor resource **Properties - Monitor(special)** tab -> **Tuning Properties - Load Balancer Linkage** tab.

If the distributed node status is "disable", BIG-IP LTM determines the distributed node to be down and therefore disconnects it. Use of the distributed node control function requires no related setting for BIG-IP LTM.

The distributed node status is updated by BIG-IP LTM when the JVM monitor detects a failure or failure recovery. Therefore, after the failover generated by an operation other than JVM monitoring, the distributed node status of BIG-IP LTM may be "enable".

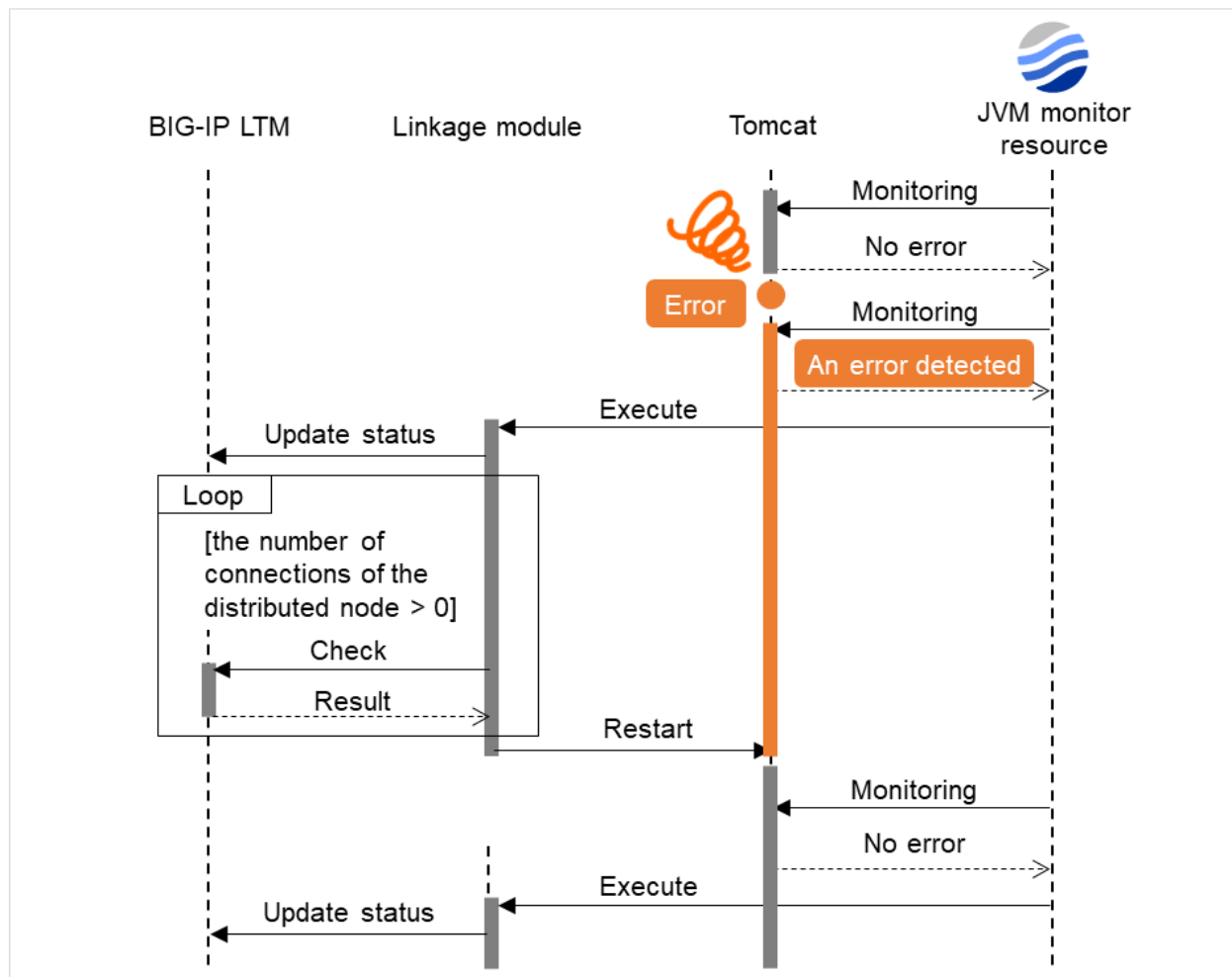


Fig. 5.11: Distributed node control function

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 Properties** - **Memory** tab - **Monitor Heap Memory Rate** - **Total Usage**.

$$\text{Java VM load (\%)} = \text{current memory usage (MB)} \times 100 / \text{threshold (MB)}$$

The linkage module installed on the server on which the JVM monitor runs executes a command at regular intervals, and reports the load collected on the target Java VM to BIG-IP LTM. BIG-IP LTM distributes the traffic (request) to the optimal server according to the load status of Java VM of the distributed node.

Set the following EXPRESSCLUSTER settings with the Cluster WebUI.

- JVM monitor resource

JVM Monitor Resource Tuning Properties

Memory Thread GC WebLogic **Load Balancer Linkage**

Load calculation function of target Java VM

Memory Pool Monitor ☒

Control of distributed nodes

Cut off an obstacle node dynamically ☐

Restart Command

Timeout 3600 sec

Initialize

OK Cancel Apply

Properties - Monitor(special) tab -> Tuning Properties- Load Balancer Linkage tab

Select the **Memory Pool Monitor** check box.

- Custom monitor resource

Properties - Monitor(common) tab

Select the **Monitor Timing - Always** radio button.

Properties - Monitor(special) tab

Select **Script created with this product**. Select **File - Edit** to add the emphasized part as described below:

```
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

- Settings of the load calculation function:
 - Command execution interval: **Properties - Monitor(common) tab - Interval** (in seconds)

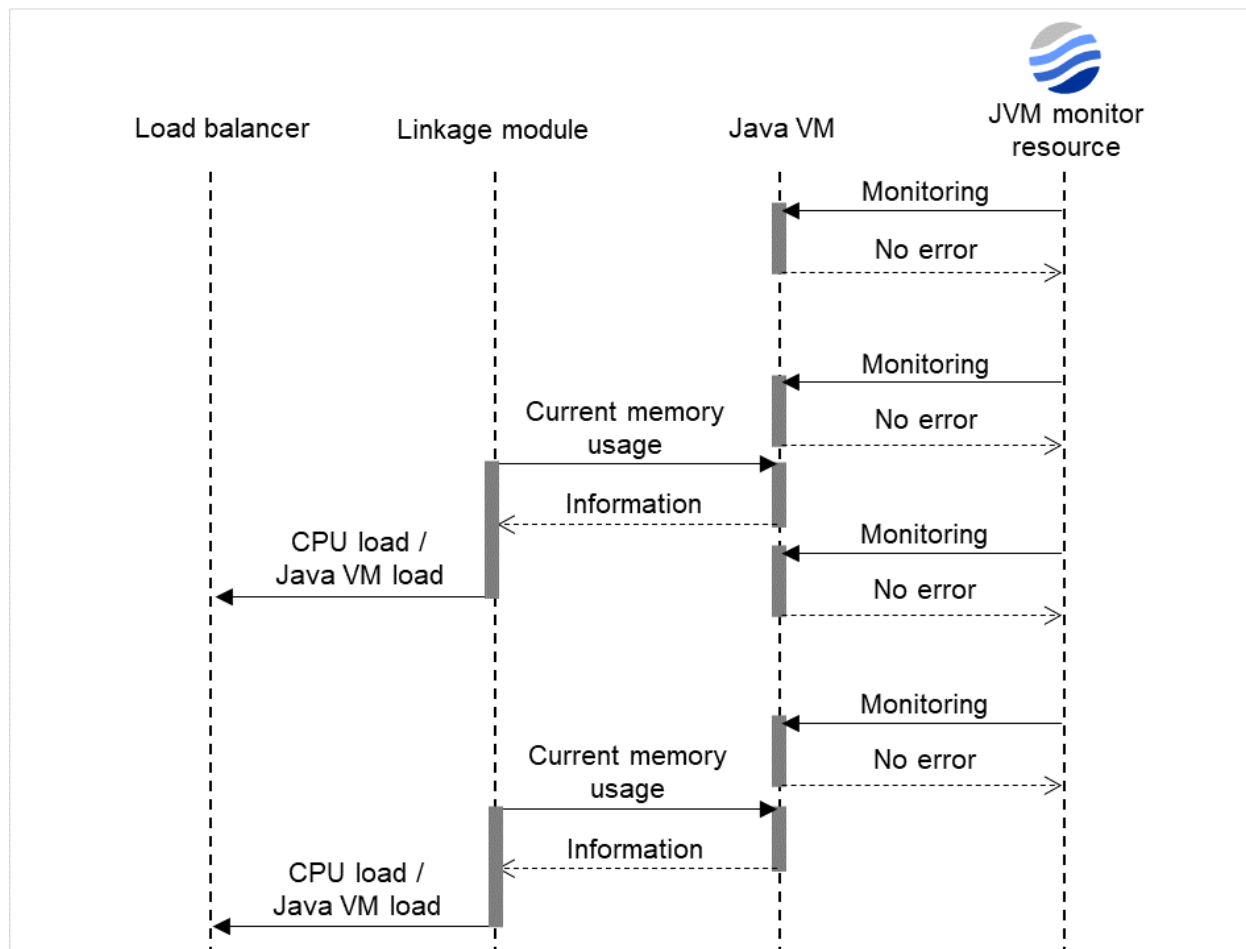


Fig. 5.12: Load calculation function

5.27.6 JVM statistical log

JVM monitor resources collect statistical information on the monitor target Java VM. The information is stored on CSV-format files, JVM statistical logs. The file is created in the following location:

```
<EXPRESSCLUSTER install path>\log\ha\jra\*.stat
```

The following "monitor items" refer to parameters in the [Monitor(special)] tab in the [Properties] of the JVM monitor resources.

Statistical information is collected and output to its corresponding JVM statistical log when an item is selected and the threshold value is set for the item. If a monitor item is not selected, statistical information on the item will be neither collected nor output to its corresponding JVM statistical log.

The following table lists monitor items and their corresponding JVM statistical logs.

Monitor items	Corresponding JVM statistical log
[Memory] tab - [Monitor Heap Memory Rate] [Memory] tab - [Monitor Non-Heap Memory Rate] [Memory] tab-[Monitor Heap Memory Usage] [Memory] tab -[Monitor Non-Heap Memory Usage]	jramemory.stat
[Thread] tab - [Monitor the number of Active Threads]	jrathread.stat
[GC] tab - [Monitor the time in Full GC] [GC] tab - [Monitor the count of Full GC execution]	jragc.stat
[WebLogic] tab - [Monitor the requests in Work Manager] [WebLogic] tab - [Monitor the requests in Thread Pool] When either of the above monitor items is checked, both of the logs, such as wlworkmanager.stat and wlthreadpool.stat, are output. No functions to output only one of the two logs are provided.	wlworkmanager.stat wlthreadpool.stat

5.27.7 Java memory area usage check on monitor target Java VM (jramemory.stat)

The jramemory.stat log file records the size of the Java memory area used by the monitor target Java VM. Its file name becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: `jramemory<integer starting with 0>.stat`
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: `jramemory<YYYYMMDDhhmm>.stat`

Its data formats are as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Name of the Java memory pool; for details, refer to "5.27.12. Java memory pool name".
4	Half-size alphanumeric characters and symbols	Type of the Java memory pool Heap, Non-Heap

Continued on next page

Table 5.14 – continued from previous page

No	Format	Description
5	Half-size numeric characters	<p>Memory size that the Java VM requests from the OS at startup; it is expressed in bytes. (init)</p> <p>At the startup of the monitor target Java VM, the size can be specified by the following Java VM startup options.</p> <ul style="list-style-type: none"> - HEAP:-Xms - NON_HEAP permanent area (Perm Gen): -XX:PermSize - NON_HEAP code cache area (Code Cache): -XX:InitialCodeCacheSize
6	Half-size numeric characters	Memory size currently used by the Java VM; it is expressed in bytes. (used)
7	Half-size numeric characters	<p>Memory size guaranteed for current use in operation of the Java VM; it is expressed in bytes. (committed)</p> <p>This size varies depending on memory use; it is always equal to the value of "used" or larger but equal to the value of "max" or smaller.</p>
8	Half-size numeric characters	<p>Maximum memory size that the Java VM can use; it is expressed in bytes. (max)</p> <p>The size can be specified by the following Java VM startup options.</p> <ul style="list-style-type: none"> - HEAP:-Xmx - NON_HEAP permanent area (Perm Gen): -XX:MaxPermSize - NON_HEAP code cache area (Code Cache): -XX:ReservedCodeCacheSize <p>Example)</p> <pre>java -XX:MaxPermSize=128m -XX:ReservedCodeCacheSize=128m javaAP</pre> <p>In this example, max of NON_HEAP becomes 128 m + 128 m = 256 m.</p> <p>(Note)</p> <p>When the same value is specified for -Xms and -Xmx, "ini" may become larger than "max". This is because "max" of HEAP is determined by subtracting half the size of Survivor Space from the area size ensured by specification of -Xmx.</p>

Continued on next page

Table 5.14 – continued from previous page

No	Format	Description
9	Half-size numeric characters	Peak size of the memory used after startup of the measurement target Java VM; when the name of the Java memory pool is HEAP or NON_HEAP, this size becomes equal to that of the memory currently used by the Java VM (used). It is expressed in bytes.
10	Half-size numeric characters	<p>Ignore this value when Oracle Java(usage monitoring) is selected for JVM Type.</p> <p>When the item other than Oracle Java(usage monitoring) for JVM Type, memory size equal to "max" (No. 8 field) * the threshold (%) when the Java memory pool type (No. 4 field) is HEAP; it is expressed in bytes.</p> <p>When the Java memory pool type is not HEAP, it is 0.</p>

5.27.8 Thread operation status check on monitor target Java VM (jrathread.stat)

The jrathread.stat log file records the thread operation status of the monitor target Java VM. Its file name becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: jrathread<integer starting with 0>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: jrathread<YYYYMMDDhhmm>.stat

Its data formats are as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	The number of active threads in the monitor target Java VM
4	[Half-size numeric characters: half-size numeric characters:...]	Deadlocked thread ID in the monitor target Java VM; it contains the IDs of all deadlocked threads successively.

Continued on next page

Table 5.15 – continued from previous page

No	Format	Description
5	Half-size alphanumeric characters and symbols	<p>Detailed information on deadlocked threads in the monitor target Java VM; it contains information on all deadlocked threads successively in the following format.</p> <p>ThreadName, ThreadID, ThreadStatus, UserTime, CpuTime, WaitedCount, WaitedTime, isInNative, isSuspended <line feed> stacktrace<line feed> : stacktrace<line feed> stacktrace=ClassName, FileName, LineNumber, MethodName, isNativeMethod</p>

5.27.9 GC operation status check on monitor target Java VM (jragc.stat)

The jragc.stat log file records the GC operation status of the monitor target Java VM. Its file name becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type]-[File Capacity] is checked: jragc<integer starting with 0>.stat
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: jragc<YYYYMMDDhhmm>.stat

JVM monitor resources output two types of GC information: Copy GC and Full GC.

On Oracle Java, JVM monitor resources count the increment in the count of execution of the following GC as Full GC.

- MarkSweepCompact
- MarkSweepCompact
- PS MarkSweep
- ConcurrentMarkSweep

Its data formats are as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.

Continued on next page

Table 5.16 – continued from previous page

No	Format	Description
3	Half-size alphanumeric characters and symbols	GC name of the monitor target Java VM When the monitor target Java VM is Oracle Java The GC name to be indicated is one of the following. Copy MarksweepCompact MarkSweepCompact PS Scavenge PS Marksweep ParNew ConcurrentMarkSweep
4	Half-size numeric characters	Count of GC execution during the period from startup of the monitor target Java VM to measurement; the count includes GC executed before the JVM monitor resources starts monitoring.
5	Half-size numeric characters	Total time in GC during the period from startup of the monitor target Java VM to measurement; it is expressed in milliseconds. It includes time taken for GC executed before the JVM monitor resources starts monitoring.

5.27.10 Operation status check on Work Manager of WebLogic Server (wlworkmanager.stat)

The wlworkmanager.stat log file records the operation status of the Work Manager of the WebLogic Server. Its file name becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: `wlworkmanager<integer starting with 0>.stat`
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: `wlworkmanager<YYYYMMDDhhmm>.stat`

Its data formats are as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size alphanumeric characters and symbols	Application name
4	Half-size alphanumeric characters and symbols	Work Manager name
5	Half-size numeric characters	Count of request execution
6	Half-size numeric characters	The number of wait requests

5.27.11 Operation status check on Thread Pool of WebLogic Server (wlthreadpool.stat)

The wlthreadpool.stat log file records the operation status of the thread pool of the WebLogic Server. Its file name becomes either of the following two depending on the Rotation Type selected on the Log Output Setting dialog box.

- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [File Capacity] is checked: `wlthreadpool<integer starting with 0>.stat`
- When [Cluster Properties] - [JVM monitor] tab - [Log Output Setting] - [Rotation Type] - [Period] is checked: `wlthreadpool<YYYYMMDDhhmm>.stat`

Its data formats are as follows.

No	Format	Description
1	yyyy/mm/dd hh:mm:ss.SSS	Date and time of log recording
2	Half-size alphanumeric characters and symbols	Name of the monitor target Java VM; it has been specified in [Properties] - [Monitor(special)] tab - [Identification name] in JVM monitor resources.
3	Half-size numeric characters	Total count of request execution
4	Half-size numeric characters	The number of requests queued in the WebLogic Server
5	Half-size numeric characters	Count of request execution per unit time (second)
6	Half-size numeric characters	The total number of threads for executing the application
7	Half-size numeric characters	The number of threads in an idle state
8	Half-size numeric characters	The number of executing threads
9	Half-size numeric characters	The number of threads in a stand-by state

5.27.12 Java memory pool name

This section describes the Java memory pool name outputted as `memory_name` in messages to the JVM operation log file. It also describes the Java memory pool name outputted to a JVM statistical log file, `jramemory.stat` log file.

The character strings of Java memory pool names are not determined by JVM monitor resources. Character strings received from the monitor target Java VM are output as Java memory pool names.

Their specifications are not open for Java VM, and accordingly, are subject to change without notice in a version upgrade of Java VM.

Therefore, we do not recommend monitoring Java memory pool names contained in messages.

The following monitor items refer to parameters in the [Memory] tab of the [Monitor(special)] tab in the [Properties] of the JVM monitor resources.

The following memory pool names have been confirmed on actual machines operating on Oracle Java.

When **Oracle Java** is selected for **JVM Type** and "-XX:+UseSerialGC" is specified as a startup option of the monitor target Java VM, the No. 3 Java memory pool name in the `jramemory.stat` log file appears as follows.

Monitor item	Character string outputted as <code>memory_name</code>
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP

Continued on next page

Table 5.19 – continued from previous page

Monitor item	Character string outputted as memory_name
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When **Oracle Java** is selected for **JVM Type** and "-XX:+UseParallelGC" and "-XX:+UseParallelOldGC" are specified as startup options of the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat log file appears as follows.

Monitor item	Character string outputted as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	PS Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	PS Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	PS Old Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	PS Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When **Oracle Java** is selected for **JVM Type** and "-XX:+UseConcMarkSweepGC" is specified as a startup option of the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat log file appears as follows.

Monitor item	Character string outputted as memory_name
[Monitor Heap Memory Rate] - [Total Usage]	HEAP
[Monitor Heap Memory Rate] - [Eden Space]	Par Eden Space
[Monitor Heap Memory Rate] - [Survivor Space]	Par Survivor Space
[Monitor Heap Memory Rate] - [Tenured Gen]	CMS Old Gen
[Monitor Non-Heap Memory Rate] - [Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Rate] - [Code Cache]	Code Cache
[Monitor Non-Heap Memory Rate] - [Perm Gen]	CMS Perm Gen
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[Monitor Non-Heap Memory Rate] - [Perm Gen[shared-rw]]	Perm Gen [shared-rw]

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseSerialGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	Tenured Gen

Continued on next page

Table 5.22 – continued from previous page

Monitor item	Character string output as memory_name
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9 or later, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap pro-filed]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseParallelGC" and "-XX:+UseParallelOldGC" are specified as startup options for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	PS Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	PS Survivor Space
[Monitor Heap Memory Usage]- [Tenured Gen]	PS Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9 or later, no output)
[Monitor Non-Heap Memory Usage]- [Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap pro-filed]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseConcMarkSweepGC" is specified as a startup option for the monitor target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Par Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Par Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	CMS Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9 or later, no output)
[Monitor Non-Heap Memory Usage]- [Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap pro-filed]	CodeHeap profiled nmethods

Continued on next page

Table 5.24 – continued from previous page

Monitor item	Character string output as memory_name
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseParNewGC" is added as a startup option of the target Java VM, the No. 3 Java memory pool name in the jramemory.stat file will be as follows. For Java 9 or later, if -XX:+UseParNewGC is specified, the monitor target Java VM does not start.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	Par Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	Par Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen]	Tenured Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

When [Oracle Java(usage monitoring)] is selected for [JVM Type] and "-XX:+UseG1GC" is specified as a startup option for the monitor target Java VM the No. 3 Java memory pool name in the jramemory.stat file will be as follows.

Monitor item	Character string output as memory_name
[Monitor Heap Memory Usage]-[Total Usage]	HEAP
[Monitor Heap Memory Usage]-[Eden Space]	G1 Eden Space
[Monitor Heap Memory Usage]-[Survivor Space]	G1 Survivor Space
[Monitor Heap Memory Usage]-[Tenured Gen(Old Gen)]	G1 Old Gen
[Monitor Non-Heap Memory Usage]-[Total Usage]	NON_HEAP
[Monitor Non-Heap Memory Usage]-[Code Cache]	Code Cache (For Java 9 or later, no output)
[Monitor Non-Heap Memory Usage]-[Metaspace]	Metaspace
[Monitor Non-Heap Memory Usage]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap profiled]	CodeHeap profiled nmethods
[Monitor Non-Heap Memory Usage]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[Monitor Non-Heap Memory Usage]-[Compressed Class Space]	Compressed Class Space

Java memory pool names appearing in the jramemory.stat log file, a JVM statistical log file, correspond to the Java VM memory space as follows.

- For Oracle Java 7

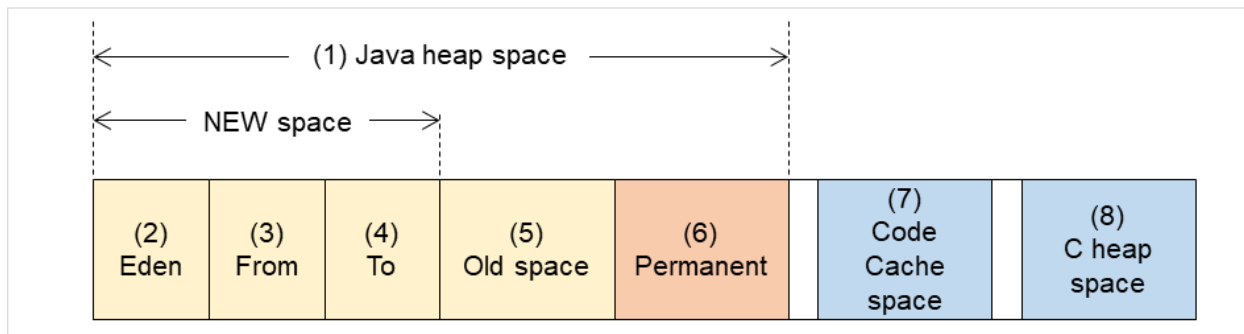


Fig. 5.13: Java VM memory space (Oracle Java 7)

Number in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(1)	[Monitor Heap Memory Rate] - [Total Usage]	HEAP
(2)	[Monitor Heap Memory Rate] - [Eden Space]	EdenSpace PS Eden Space Par Eden Space
(3)+(4)	[Monitor Heap Memory Rate] - [Survivor Space]	Survivor Space PS Survivor Space Par Survivor Space
(5)	[Monitor Heap Memory Rate]-[Tenured Gen]	Tenured Gen PS Old Gen CMS Old Gen
(6)	[Monitor Non-Heap Memory Rate]-[Perm Gen] [Monitor Non-Heap Memory Rate]-[Perm Gen[shared-ro]] [Monitor Non-Heap Memory Rate]-[Perm Gen[shared-rw]]	Perm Gen Perm Gen [shared-ro] Perm Gen [shared-rw] PS Perm Gen CMS Perm Gen
(7)	[Monitor Non-Heap Memory Rate]-[Code Cache]	Code Cache
(8)	-	-

Continued on next page

Table 5.27 – continued from previous page

Number in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(6)+(7)	[Monitor Non-Heap Memory Rate]- [Total Usage]	NON_HEAP * No stack trace is included.

- For Oracle Java 8/Oracle Java 9/Oracle Java 11

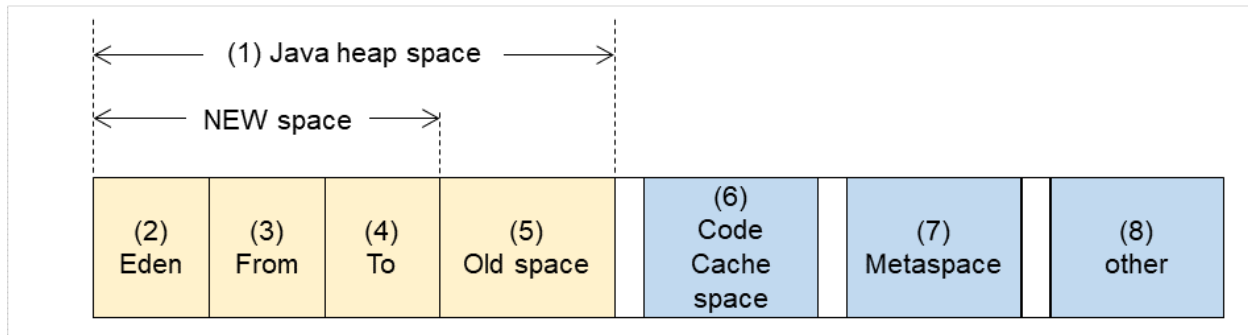


Fig. 5.14: Java VM memory space (Oracle Java 8/Oracle Java 9/Oracle Java 11)

Number in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(1)	[Monitor Heap Memory Usage] - [Total Usage]	HEAP
(2)	[Monitor Heap Memory Usage] - [Eden Space]	EdenSpace PS Eden Space Par Eden Space G1 Eden Space
(3)+(4)	[Monitor Heap Memory Usage] - [Survivor Space]	Survivor Space PS Survivor Space Par Survivor Space G1 Survivor Space
(5)	[Monitor Heap Memory Usage] - [Tenured Gen]	Tenured Gen PS Old Gen CMS Old Gen G1 Old Gen
(6)	[Monitor Non-Heap Memory Usage] - [Code Cache]	Code Cache (For Java 9 or later, no output)

Continued on next page

Table 5.28 – continued from previous page

Number in diagram	Monitor item	Java memory pool name in jramemory.stat log file
(6)	[Monitor Non-Heap Memory Usage]- [CodeHeap non-nmethods]	CodeHeap non-nmethods (Only for Java 9 or later, it is output.)
(6)	[Monitor Non-Heap Memory Usage]- [CodeHeap profiled]	CodeHeap profiled nmethods (Only for Java 9 or later, it is output.)
(6)	[Monitor Non-Heap Memory Usage]- [CodeHeap non-profiled]	CodeHeap non-profiled nmethods (Only for Java 9 or later, it is output.)
(7)	[Monitor Non-Heap Memory Usage] - [Metaspace]	Metaspace
(8)	[Monitor Non-Heap Memory Usage]- [Compressed Class Space]	Compressed Class Space.
(6)+(7)+(8)	[Monitor Non-Heap Memory Usage] - [Total Usage]	NON_HEAP

5.27.13 Executing command corresponding to cause of each detected error

EXPRESSCLUSTER does not provide means for executing specific commands according to the causes of detected monitor resource errors.

JVM monitor resources can execute specific commands according to error causes. If an error is detected, JVM monitor resources will execute an appropriate command.

The following setting items specify commands that will be executed according to error causes.

Error cause	Setting item
- Failure in connection to the monitor target Java VM - Failure in resource measurement	[Monitor(special)] tab - [Command]
- Heap memory rate - Non-heap memory rate - Heap memory usage - Non-heap memory usage	[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]
• The number of active threads	[Monitor(special)] tab - [Tuning] properties - [Thread] tab - [Command]
- Time in Full GC - Count of Full GC execution	[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]
- Requests in Work Manager of WebLogic - Requests in Thread Pool of WebLogic	[Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Command]

A [Command] passes the detail of an error cause as the arguments of a command with the arguments attached to the end of the [Command]. A Command further specialized for dealing with specific error causes can be defined by designing and specifying a script etc. for a [Command]. The following character strings are passed as the arguments. When multiple character strings are stated as possible arguments, one of them will be passed according to the CG type of the monitor target Java VM. For the details of their differences, refer to "5.27.12. *Java memory pool name*". Statements "(For Oracle Java)", "(For Oracle Java(usage monitoring))" suggest that different character strings are used according to the JVM type. When no such statement is contained, the same character strings will be equally used for all JVM types.

Details of error causes	Character string for argument
- Failure in connection to the monitor target Java VM - Failure in resource measurement	No character string defined
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Monitor Memory Heap Rate] - [Total Usage] (For Oracle Java)	HEAP
[Memory] tab - [Monitor Memory Heap Rate] - [Eden Space] (For Oracle Java)	EdenSpace PSEdenSpace ParEdenSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Survivor Space] (For Oracle Java)	SurvivorSpace PSSurvivorSpace ParSurvivorSpace
[Memory] tab - [Monitor Memory Heap Rate] - [Tenured Gen] (For Oracle Java)	TenuredGen PSOldGen CMSOldGen
[Memory] tab - [Monitor Non-Heap Memory Rate] - [Total Usage] (For Oracle Java)	NON_HEAP
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Code Cache] (For Oracle Java)	CodeCache

Continued on next page

Table 5.30 – continued from previous page

Details of error causes	Character string for argument
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Perm Gen] (For Oracle Java)	PermGen PSPermGen CMSPermGen
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Perm Gen[shared-ro]] (For Oracle Java)	PermGen[shared-ro]
[Memory] tab - [Monitor Memory Non-Heap Rate] - [Perm Gen[shared-rw]] (For Oracle Java)	PermGen[shared-rw]
[Memory] tab - [Monitor Heap Memory Usage]-[Total Usage] (Oracle Java(usage monitoring))	HEAP
[Memory] tab - [Monitor Heap Memory Usage]-[Eden Space] (Oracle Java(usage monitoring))	EdenSpace PSEdenSpace ParEdenSpace G1EdenSpace
[Memory] tab - [Monitor Heap Memory Usage]-[Survivor Space] (Oracle Java(usage monitoring))	SurvivorSpace PSSurvivorSpace ParSurvivorSpace G1SurvivorSpace
[Memory] tab - [Monitor Heap Memory Usage]-[Tenured Gen] (Oracle Java(usage monitoring))	TenuredGen PSOldGen CMSOldGen G1OldGen
[Memory] tab - [Monitor Non-Heap Memory Usage]-[Total Usage] (Oracle Java(usage monitoring))	NON_HEAP
[Memory] tab - [Monitor Non-Heap Memory Usage]-[Code Cache] (Oracle Java(usage monitoring))	CodeCache

Continued on next page

Table 5.30 – continued from previous page

Details of error causes	Character string for argument
[Memory] tab - [Monitor Non-Heap Memory Usage]-[Metaspace] (Oracle Java(usage monitoring))	Metaspace
[Thread] tab - [Monitor the number of Active Threads]	Count
[GC] tab - [Monitor the time in Full GC]	Time
[GC] tab - [Monitor the count of Full GC execution]	Count
[WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, The number]	WorkManager_PendingRequests
[WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, The number]	ThreadPool_PendingUserRequestCount
[WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, The number]	ThreadPool_Throughput

The following are examples of execution.

Example 1)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	\Program Files\bin\command.bat
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the count of Full GC execution]	1
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If Full GC is executed successively as many times as specified by the Error Threshold (three times), JVM monitor resources will detect a monitor error and execute a command corresponding to \Program Files\bin\command.bat Count.

Example 2)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Command]	\Program Files\bin\command.bat GC
[Monitor(special)] tab - [Tuning] properties - [GC] tab - [Monitor the time in Full GC]	65536
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the time in Full GC exceeds 65535 milliseconds successively as many times as specified by the Error Threshold (three times), JVM monitor resources will detect a monitor error and execute a command corresponding to "\Program Files\bin\command.bat GC Time".

Example 3)

Setting item	Setting information
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Command]	\Program Files\bin\command.bat memory
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Monitor Heap Memory Rate]	On
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Eden Space]	80
[Monitor(special)] tab - [Tuning] properties - [Memory] tab - [Survivor Space]	80
[Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [Common] tab - [Error Threshold]	3

If the usage rate of the Java Eden Space and that of the Java Survivor Space exceed 80% successively as many times as specified by the Error Threshold (three times), JVM monitor resources will detect a monitor error and execute a command corresponding to "`\Program Files\bin\command.bat memory EdenSpace SurvivorSpace`".

Timeout (second) for waiting for the completion of execution of the command specified by the [Command] is set by specifying the [Command Timeout] in the [JVM monitor] of the Cluster Properties window. The same value is applied to the timeout of the [Command] of each of the above-mentioned tabs; the timeout cannot be specified for each [Command] separately.

If a timeout occurs, the system will not perform processing for forced termination of the [Command] process; the operator needs to perform post-processing (e.g. forced termination) of the [Command] process. When a timeout occurs, the following message is output to the JVM operation log:

```
action thread execution did not finish. action is alive = <command>
```

Note the following cautions.

- No [Command] is executed when restoration of the Java VM to normal operation (error -> normal operation) is detected.
- A [Command] is executed upon detection of an error of the Java VM (when threshold crossing occurs successively as many times as specified by the error threshold). It is not executed at each threshold crossing.
- Note that specifying a [Command] on multiple tabs allows multiple commands to be executed if multiple errors occur simultaneously, causing a large system load.
- A [Command] may be executed twice simultaneously when the following two items are monitored: [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, The Number]; [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Work Manager] - [Waiting Requests, Average].

This is because errors may be detected simultaneously on the following two items: [Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [WebLogic] tab - [Interval, The number of request]; [Cluster] properties - [JVM monitor] tab - [Resource Measurement Setting] - [WebLogic] tab - [Interval, The average number of the request]. To avoid this phenomenon, specify only one of the two items as a monitor target. This applies to the following combinations of monitor items.

- [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, The Number] and [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Waiting Requests, Average]
- [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, The Number] and [Monitor(special)] tab - [Tuning] properties - [WebLogic] tab - [Monitor the requests in Thread Pool] - [Executing Requests, Average]

5.27.14 Monitoring WebLogic Server

For how to start the operation of the configured target WebLogic Server as an application server, see the manual for WebLogic Server.

This section describes only the settings required for monitoring by the JVM monitor resource.

1. Start WebLogic Server Administration Console.

For how to start WebLogic Server Administration Console, refer to "Overview of Administration Console" in the WebLogic Server manual.

Select **Domain Configuration-Domain-Configuration-General**. Make sure that **Enable Management Port** is **unchecked**.

2. Select **Domain Configuration-Server**, and then select the name of the server to be monitored. Set the selected server name as the identifier on the **Monitor(Special)** tab from **Properties** that can be selected in the config mode of Cluster WebUI.
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
-Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.
↪WLSMBeanServerBuilder
```

*Write each line of coding on one line.

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

- When the target is a WebLogic Server managed server:

```
if "%SERVER_NAME%" == "SERVER_NAME" (
    set JAVA_OPTIONS=%JAVA_OPTIONS%
    -Dcom.sun.management.jmxremote.port=n
    -Dcom.sun.management.jmxremote.ssl=false
    -Dcom.sun.management.jmxremote.authenticate=false
    -Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.
    ↪WLSMBeanServerBuilder
)
```

*Write all the if statement lines on one line.

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

Note: Place the above addition prior to the following coding:

```
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS%  
-Dweblogic.Name=%SERVER_NAME%  
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy %JAVA_OPTIONS  
% %PROXY_SETTINGS% %SERVER_CLASS%
```

*Write the above coding on one line.

7. If monitoring a request of work manager and thread pool, configure the following settings:

Start WLST (wlst.cmd) of the target WebLogic Server.

To do this, select Start menu-Oracle WebLogic-WebLogic Server <version number>-Tools-WebLogic Scripting Tool.

On the prompt window displayed, execute the following commands.

```
> connect ('USERNAME', 'PASSWORD', 't3://SERVER_ADDRESS:SERVER_PORT')  
> edit()  
> startEdit()  
> cd ('JMX/DOMAIN_NAME')  
> set ('PlatformMBeanServerUsed', 'true')  
> activate()  
> exit()
```

Replace the **USERNAME**, **PASSWORD**, **SERVER_ADDRESS**, **SERVER_PORT**, and **DOMAIN_NAME** with those for the domain environment.

8. Restart the target WebLogic Server.

5.27.15 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.

5.27.16 Monitoring a Java process of the WebOTX domain agent

There is no need to specify any settings.

5.27.17 Monitoring a Java process of a WebOTX process group

1. Connect to the domain by using the administration console.
2. In the tree view, select <domain_name>-TP System-Application Group-<application_group_name>-Process Group-<process_group_name>.
3. For the **Other Arguments** attributes on the **JVM Options** tab on the right, specify the following Java options on one line. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified for the settings is specified with Cluster WebUI (Monitor Resource Properties - Monitor(special) tab - Connection Port).

```
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djavax.management.builder.initial=com.nec.webotx.jmx.mbeanserver.
↪ JmxMBeanServerBuilder
```

* In the case of WebOTX V9.2 or later, it is unnecessary to specify -Djavax.management.builder.initial.

4. Then, click **Update**. After the configuration is completed, restart the process group.

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

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

Tab name for setting	Item name	Setting value
Monitor(common)	Monitor Timing	Always
Recovery Action	Recovery Action	Execute only the final action
Recovery Action	Final Action	No operation

Linking with the load balancer is not supported for WebOTX process group monitoring.

5.27.18 Receiving WebOTX notifications

By registering a specific listener class, notification is issued when WebOTX detects a failure. The JVM monitor resource receives the notification and outputs the following message to the JVM operation log.

```
%1$s:Notification received. %2$s.
```

%1\$s and %2\$s each indicates the following:

```
%1$s: Monitored Java VM
%2$s: Message in the notification (ObjectName=,type=,message=)
```

At present, the following is the detailed information on MBean on the monitorable resource.

ObjectName	[domainname]:j2eeType=J2EEDomain,name=[domainname],category=runtime
notification type	nec.webotx.monitor.alivecheck.not-alive
Message	failed

5.27.19 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 Cluster WebUI (**Monitor Resource Properties -> Monitor(special) tab -> Connection Port**).

```
-Dcom.sun.management.jmxremote.port=n  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.authenticate=false
```

3. Save the settings, and then start Tomcat.
4. With Cluster WebUI (**JVM Monitor Resource Name -> Properties -> Monitor(special) tab -> Identifier**), specify a unique string that is different from those for the other monitor targets (e.g., tomcat).

5.27.20 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	%FIT_PRODUCTS_BASE%\SetupUtils\setup_tomcat.bat

2. (When the monitor target is Tomcat:)
Insert the additional description to --JvmOption of :install within setup_tomcat.bat in the following way. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Cluster WebUI (**Monitor Resource Properties - Monitor(special) tab - Connection Port**).

Before the change:

```
--JvmOptions=...
```

After the change:

```
--JvmOptions=...;-Dcom.sun.management.jmxremote.port=n;-Dcom.sun.management.  
->jmxremote.ssl=false;-Dcom.sun.management.jmxremote.authenticate=false
```

3. (When the monitor target is other than Tomcat:)

The following contents are inserted in the part where Arguments is designated just after the setting point of "-Xms". For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Cluster WebUI (**Monitor Resource Properties -> Monitor (special) tab -> Connection Port**).

```
-Dcom.sun.management.jmxremote.port=n -Dcom.sun.management.jmxremote.ssl=false -  
↪Dcom.sun.management.jmxremote.authenticate=false
```

5.27.21 Monitoring a Java application that you created

This section describes the procedure to configure Java application which is monitored by JVM monitor resource. Specify the following Java option in one row to the option for Java application startup while Java application (the monitor target) is stopped. For **n**, specify the port number. If there is more than one Java VM to be monitored on the same machine, specify a unique port number. The port number specified here is also specified with the Cluster WebUI (**Monitor Resource Properties - Monitor(special) tab - Connection Port**).

```
-Dcom.sun.management.jmxremote.port=n -Dcom.sun.management.jmxremote.ssl=false -Dcom.  
↪sun.management.jmxremote.authenticate=false
```

Some Java applications require the following to be additionally specified.

```
-Djavax.management.builder.initial=<Class name of MBeanServerBuilder>
```

5.27.22 Monitor (special) tab

Monitor Resource Properties | jraw1

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

Target: WebLogic Server

JVM Type: Oracle Java

Identifier*: Server-0

Connection Port*: 19002

Process Name:

User:

Password: Change

Command:

Tuning

OK Cancel Apply

Target

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

Default: None

JVM Type

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

For Java 8 or later, select **Oracle Java(usage monitoring)**. For Java 8, the following specification changes have been made.

- It has become impossible to acquire the maximum value of each memory in a non-heap area.
- Perm Gen has been changed to Metaspace.
- Compressed Class Space was added.

For Java 8, therefore, the monitor items on the **Memory** tab have been changed as below.

- Monitoring for the use rate has been changed to monitoring for the amount used.
- **Perm Gen**, **Perm Gen[shared-ro]**, and **Perm Gen[shared-rw]** cannot be monitored. Clear the check box.
- **Metaspace** and **Compressed Class Space** can be monitored.

For Java 9, the following specification changes have been made.

- **Code Cache** has been divided.

For Java9, therefore, the monitor items on the **Memory** tab have been changed as below.

- **Code Cache** cannot be monitored. Clear the check box.
- **CodeHeap non-nmethods**, **CodeHeap profiled** and **CodeHeap non-profiled** can be monitored.

Default: None

Identifier (within 255 bytes)

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 " 5.27.14. *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 " 5.27.19. *Monitoring Tomcat* ".
- When the target is **WebSAM SVF**
Specify this according to " 5.27.20. *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. A value between 42424 and 61000 is not recommended.

- When the target is **WebLogic Server**
Specify the connection port number according to " 5.27.14. *Monitoring WebLogic Server*", item 6.
- When the target is **WebOTX Process Group**
Specify this according to " 5.27.17. *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 " 5.27.19. *Monitoring Tomcat* ".
- When the target is **WebSAM SVF**
Specify this according to " 5.27.20. *Monitoring SVF* ".
- When the target is **Java applications**
Specify a uniquely identifiable string for the monitored Java VM process.

Default: None

Process Name (within 255 bytes)

This does not need to be configured because the monitor target Java VM can be identified by **Connction Port**. The internal version 11.35 or earlier required the process name to be specified since this parameter was used for the identification when the data of virtual memory usage amount was obtained or when the data of the monitor target was output to the JVM operation log. However, in and after the internal version 12.00, **Monitor Virtual Memory Usage** was deleted. Therefore, it cannot be specified.

Default: None

User (within 255 bytes)

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

Default: None

Password (within 255 bytes)

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

Default: None

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").

Example) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the commands to execute if it is impossible to connect to the target Java VM and if an error is detected in acquiring the resource amount used.

See also " 5.27.13. *Executing command corresponding to cause of each detected error* ".

Default: None

When you click **Tuning**, the following information is displayed in the pop-up dialog box. Make detailed settings according to the descriptions below.

5.27.23 Memory tab (when Oracle Java is selected for JVM Type)

The screenshot shows the 'JVM Monitor Resource Tuning Properties' dialog box with the 'Memory' tab selected. The dialog has five tabs: Memory, Thread, GC, WebLogic, and Load Balancer Linkage. The 'Memory' tab contains two main sections: 'Monitor Heap Memory Rate' and 'Monitor Non-Heap Memory Rate'. Each section has a list of memory areas with checkboxes and input fields for usage percentages. The 'Monitor Heap Memory Rate' section includes 'Total Usage' (checked, 80%), 'Eden Space' (unchecked, 100%), 'Survivor Space' (unchecked, 100%), and 'Tenured Gen' (checked, 80%). The 'Monitor Non-Heap Memory Rate' section includes 'Total Usage' (checked, 80%), 'Code Cache' (unchecked, 100%), 'Perm Gen' (checked, 80%), 'Perm Gen[shared-ro]' (checked, 80%), and 'Perm Gen[shared-rw]' (checked, 80%). Each section also has a 'Command' input field. At the bottom left is an 'Initialize' button, and at the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Section	Item	Checked	Value	Unit
Monitor Heap Memory Rate	Total Usage	✓	80	%
	Eden Space	✗	100	%
	Survivor Space	✗	100	%
	Tenured Gen	✓	80	%
Monitor Non-Heap Memory Rate	Total Usage	✓	80	%
	Code Cache	✗	100	%
	Perm Gen	✓	80	%
	Perm Gen[shared-ro]	✓	80	%
	Perm Gen[shared-rw]	✓	80	%

Monitor Heap Memory Rate

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

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

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java heap areas used by the target Java VM.

Default: 80[%]

Eden Space (1 to 100)

Specify the threshold for the usage rate of the Java Eden Space used by the target Java VM.If G1 GC is specified as the GC method of the target Java VM, read it as G1 Eden Space.

Default: 100[%]

Survivor Space (1 to 100)

Specify the threshold for the usage rate of the Java Survivor Space used by the target Java VM.If G1 GC is specified as the GC method of the target Java VM, read it as G1 Survivor

Default: 100[%]

Tenured Gen (1 to 100)

Specify the threshold for the usage rate of the Java Tenured(Old) Gen area used by the target Java VM. If G1 GC is specified as the GC method of the target Java VM, read it as G1 Old Gen.

Default: 80[%]

Monitor Non-Heap Memory Rate

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

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

Total Usage (1 to 100)

Specify the threshold for the usage rate of the Java non-heap areas used by the target Java VM.

Default: 80[%]

Code Cache (1 to 100)

Specify the threshold for the usage rate of the Java Code Cache area used by the target Java VM.

Default: 100[%]

Perm Gen (1 to 100)

Specify the threshold for the usage rate of the Java Perm Gen area used by the target Java VM.

Default: 80[%]

Perm Gen[shared-ro] (1 to 100)

Specify the threshold for the usage rate of the Java Perm Gen [shared-ro] area used by the target Java VM.

Default: 80[%]

Perm Gen[shared-rw] (1 to 100)

Specify the threshold for the usage rate of the Java Perm Gen [shared-rw] area used by the target Java VM.

Default: 80[%]

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").

Example) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the commands to execute if an error is detected in the Java heap area and Java non-heap area of the target Java VM.

See also " [5.27.13. Executing command corresponding to cause of each detected error](#) ".

Default: None

Initialize

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

5.27.24 Memory tab (when Oracle Java(usage monitoring) is selected for JVM Type)

JVM Monitor Resource Tuning Properties

Memory Thread GC WebLogic Load Balancer Linkage

☐ **Monitor Heap Memory Usage**

☒ Total Usage 0 MB

☐ Eden Space 0 MB

☐ Survivor Space 0 MB

☒ Tenured Gen(Old Gen) 0 MB

Command

☐ **Monitor Non-Heap Memory Usage**

☒ Total Usage 0 MB

☐ Code Cache 0 MB

☐ CodeHeap non-nmethods 0 MB

☐ CodeHeap profiled 0 MB

☐ CodeHeap non-profiled 0 MB

☐ Compressed Class Space 0 MB

☐ Metaspace 0 MB

Command

Initialize

OK Cancel Apply

Monitor Heap Memory Usage

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

- When the check box is selected:
Monitoring is enabled.
- When the check box is not selected (default):
Monitoring is disabled.

Total Usage (0 to 102400)

Specify the threshold for the amount of the Java heap areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Eden Space (0 to 102400)

Specify the threshold for the amount of the Java Eden Space used by the target Java VM. If zero is specified, this item is not monitored. If G1 GC is specified as the GC method of the target Java VM, read it as G1 Eden Space.

Default: 0[MB]

Survivor Space (0 to 102400)

Specify the threshold for the amount of the Java Survivor Space used by the target Java VM. If zero is specified, this item is not monitored. If G1 GC is specified as the GC method of the target Java VM, read it as G1 Survivor Space.

Default: 0[MB]

Tenured Gen (0 to 102400)

Specify the threshold for the amount of the Java Tenured(Old) Gen area used by the target Java VM. If zero is specified, this item is not monitored. If G1 GC is specified as the GC method of the target Java VM, read it as G1 Old Gen.

Default: 0[MB]

Monitor Non-Heap Memory Usage

Enables the monitoring of the amounts of the Java non-heap areas used by the target Java VM.

- When the check box is selected:
Monitoring is enabled.
- When the check box is not selected (default):
Monitoring is disabled.

Total Usage (0 to 102400)

Specify the threshold for the usage amount of the Java non-heap areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Code Cache (0 to 102400)

Specify the threshold for the usage amount of the Java Code Cache area used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

CodeHeap non-nmethods (0 to 102400)

Specify the threshold for the usage rate of the Java CodeHeap non-nmethods areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

CodeHeap profiled (0 to 102400)

Specify the threshold for the usage rate of the Java CodeHeap profiled nmethods areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

CodeHeap non-profiled (0 to 102400)

Specify the threshold for the usage rate of the Java CodeHeap non-profiled nmethods areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Compressed Class Space (0 to 102400)

Specify the threshold for the usage rate of the Compressed Class Space areas used by the target Java VM. If zero is specified, this item is not monitored.

Default: 0[MB]

Metaspace (0 to 102400)

Specify the threshold for the usage rate of the Metaspace area used by the target Java VM

Default: 0[MB]

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").

Example) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the commands to execute if an error is detected in the Java heap area and Java non-heap area of the target Java VM.

See also " 5.27.13. *Executing command corresponding to cause of each detected error* ".

Default: None

Initialize

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

5.27.25 Thread tab

The screenshot shows the 'JVM Monitor Resource Tuning Properties' dialog box with the 'Thread' tab selected. The 'Memory' tab is also visible. The 'Thread' tab contains a checkbox labeled 'Monitor the number of Active Threads' which is checked. To the right of this checkbox is a text input field containing the value '65535'. Below the checkbox is a label 'Command' followed by a text input field. At the bottom left of the dialog is an 'Initialize' button. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Monitor the number of Active Threads (1 to 65535)

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

Default: 65535 [threads]

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").

Example) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the command to execute if an error is detected in the number of threads currently running in the target Java VM.

See also " 5.27.13. *Executing command corresponding to cause of each detected error* ".

Default: None

Initialize

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

5.27.26 GC tab

The screenshot shows the 'JVM Monitor Resource Tuning Properties' dialog box with the 'GC' tab selected. The dialog has five tabs: Memory, Thread, GC, WebLogic, and Load Balancer Linkage. The 'GC' tab contains the following controls:

- A checkbox labeled 'Monitor the time in Full GC' is unchecked. To its right is a text input field containing '65535' and a unit dropdown menu set to 'msec'.
- A checkbox labeled 'Monitor the count of Full GC execution' is checked. To its right is a text input field containing '1' and a unit dropdown menu set to 'count'.
- A text input field labeled 'Command' is empty.
- An 'Initialize' button is located below the 'Command' field.
- 'OK', 'Cancel', and 'Apply' buttons are located at the bottom right of the dialog.

Monitor the time in Full GC (1 to 65535)

Specify the threshold for the Full GC execution time since previous measurement on the target Java VM. The threshold for the Full GC execution time is the average obtained by dividing the Full GC execution time by the number of times Full GC occurs since the previous measurement.

To determine the case in which the Full GC execution time since the previous measurement is 3000 milliseconds and Full GC occurs three times as an error, specify 1000 milliseconds or less.

Default: 65535 [milliseconds]

Monitor the count of Full GC execution (1 to 65535)

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

Default: 1 (time)

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").

Example) "`Program Files\bin\command.bat`" arg1 arg2

Here, specify the commands to execute if an error is detected in the Full GC execution time and Full GC execution count of the target Java VM.

See also " [5.27.13. Executing command corresponding to cause of each detected error](#) ".

Default: None

Initialize

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

5.27.27 WebLogic tab

JVM Monitor Resource Tuning Properties

Memory

Thread

GC

WebLogic

Load Balancer Linkage

Monitor the requests in Work Manager

☐

Target Work Managers

Waiting Requests

☐

The number

65535

☐

Average

65535

☒

Increment from the last

80

%

Monitor the requests in Thread Pool

☒

Waiting Requests

☐

The number

65535

☐

Average

65535

☒

Increment from the last

80

%

Executing Requests

☐

The number

65535

☐

Average

65535

☒

Increment from the last

80

%

Command

Initialize

OK

Cancel

Apply

Monitor the requests in Work Manager

Enables the monitoring of the wait requests by Work Managers on the WebLogic Server.

- When selected(default):
Monitoring enabled
- When cleared:
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[%]

Command (within 255 bytes)

Specify the command to execute if an error is detected in the target Java VM. It is possible to specify the command to execute for each error cause, as well as arguments. Specify a full path. Enclose an executable file name with double quotes ("").

Example) "\Program Files\bin\command.bat" arg1 arg2

Here, specify the commands to execute if an error is detected in the requests in the thread pool or in the work manager of the WebLogic Server.

See also " 5.27.13. *Executing command corresponding to cause of each detected error* ".

Default: None

Initialize

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

5.27.28 Load Balancer Linkage tab

The screenshot shows a dialog box titled "JVM Monitor Resource Tuning Properties". It has five tabs: "Memory", "Thread", "GC", "WebLogic", and "Load Balancer Linkage". The "Load Balancer Linkage" tab is selected. Below the tabs, there is a section titled "Load calculation function of target Java VM". Inside this section, there is a checkbox labeled "Memory Pool Monitor" which is currently unchecked. Below the checkbox is an "Initialize" button. At the bottom right of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

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 initialize all the items to their default values.

5.27.29 Load Balancer Linkage tab(BIG-IP LTM)

The screenshot shows a dialog box titled "JVM Monitor Resource Tuning Properties". It has five tabs: "Memory", "Thread", "GC", "WebLogic", and "Load Balancer Linkage". The "Load Balancer Linkage" tab is selected. Below the tabs, there are three sections: "Load calculation function of target Java VM" with a checkbox for "Memory Pool Monitor"; "Control of distributed nodes" with a checkbox for "Cut off an obstacle node dynamically"; and "Restart Command" with a text input field and a "Timeout" field set to "3600" with a "sec" label. There is an "Initialize" button on the left and "OK", "Cancel", and "Apply" buttons on the right.

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.

Note: Linking with the BIG-IP Local Traffic Manager requires an OpenSSL library. However, OpenSSL 1.1.0 or later is not supported.

5.28 Setting up System monitor resources

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

5.28.1 Notes on system monitor resource

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

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

Errors in resource monitoring may be undetectable when:

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

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

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

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

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

The amount of system resources used is analyzed at 10-minute intervals. Thus, an error may be detected up to 10 minutes after the monitoring session.

The amount of disk resources used is analyzed at 60-minute intervals. Thus, an error may be detected up to 60 minutes after the monitoring session.

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

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

- Total disk capacity
- File system

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

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

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

The status of the system monitor resource is Warning from when start of monitoring is enabled to when the monitoring processing is actually performed. In this status, the following message is output to the alert log.

```
Monitor sraw is in the warning status. (191 : Command succeeded.)
```

5.28.2 Monitoring by System monitor resources

System monitor resources monitor the following:

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

An error is recognized if the amount of a resource used exceeds a pre-set threshold. When an error detected state persists for the monitoring duration, it is posted as an error detected during resource monitoring.

System resource monitoring with the default values reports an error found in resource monitoring 60 minutes later if the resource usage does not fall below 90%.

The following shows an example of error detection for the total memory usage in system resource monitoring with the default values.

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

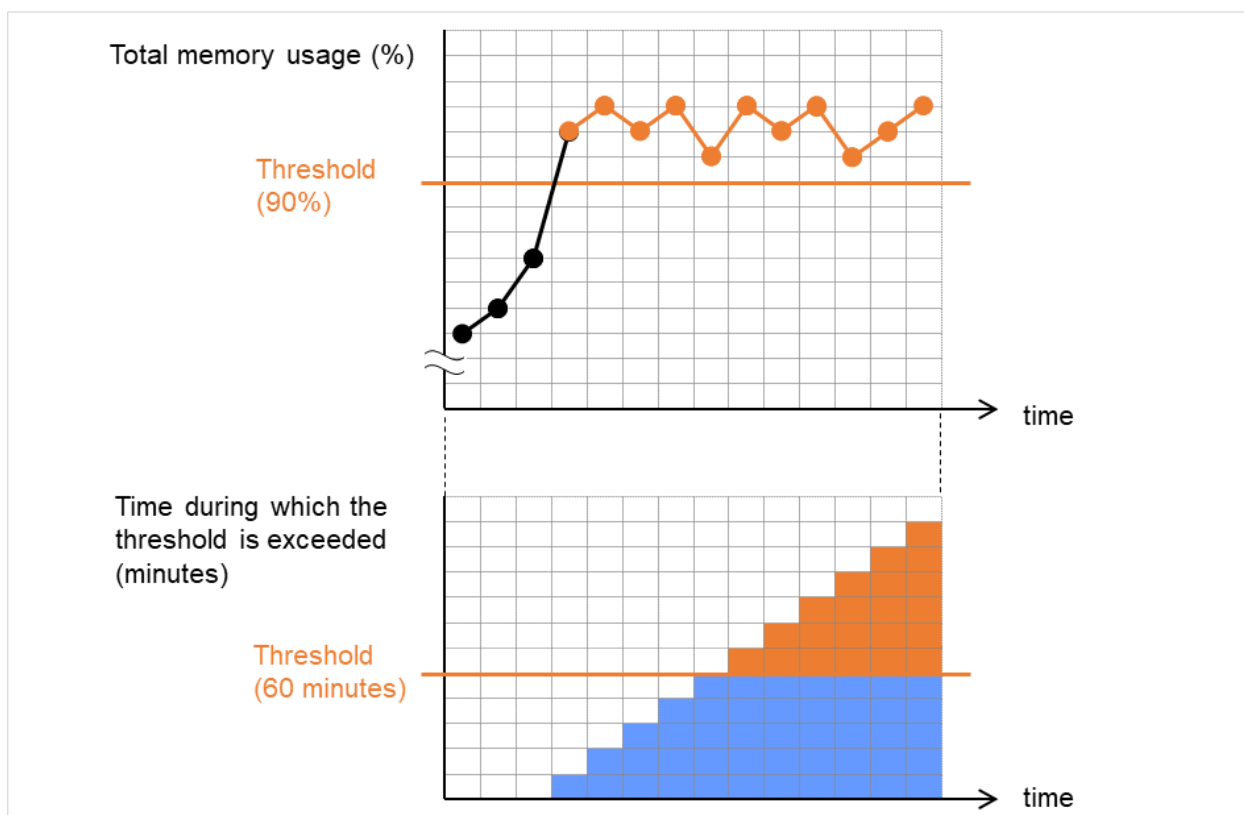


Fig. 5.15: The total memory usage remains at the total memory usage threshold or higher for a certain duration of time (an error detected)

- 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 following figure shows the total memory usage temporarily exceeding the total memory usage threshold (90%). This state of exceeding the threshold, however, does not persist for the monitoring duration (60 minutes) and thus an error in the total memory usage is not detected.

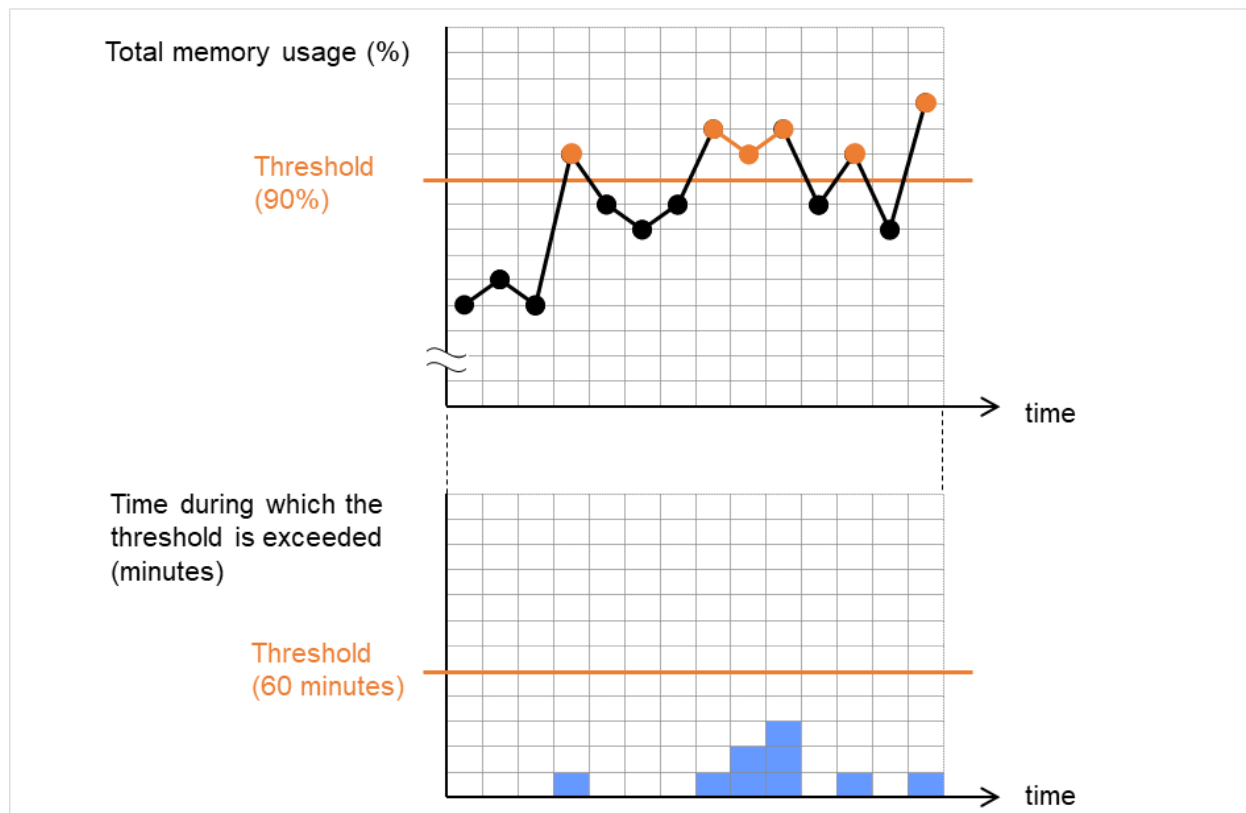


Fig. 5.16: The state of exceeding the total memory usage threshold does not persist for a certain duration of time (no error detected)

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.

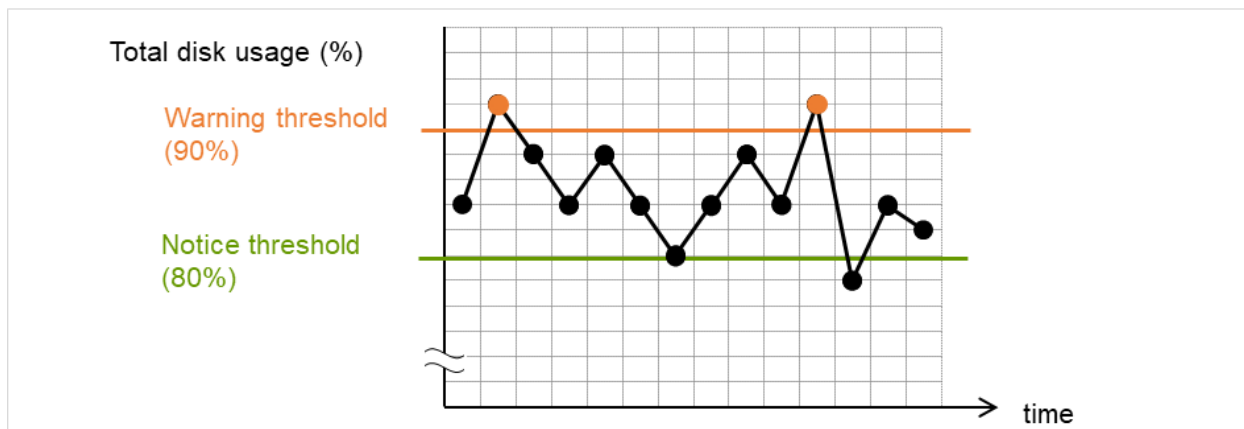


Fig. 5.17: Disk usage exceeds the warning level upper limit (an error detected)

- 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 increases and decreases in a range where it does not exceed the warning level upper limit, which is not determined as an error in monitoring the usage.

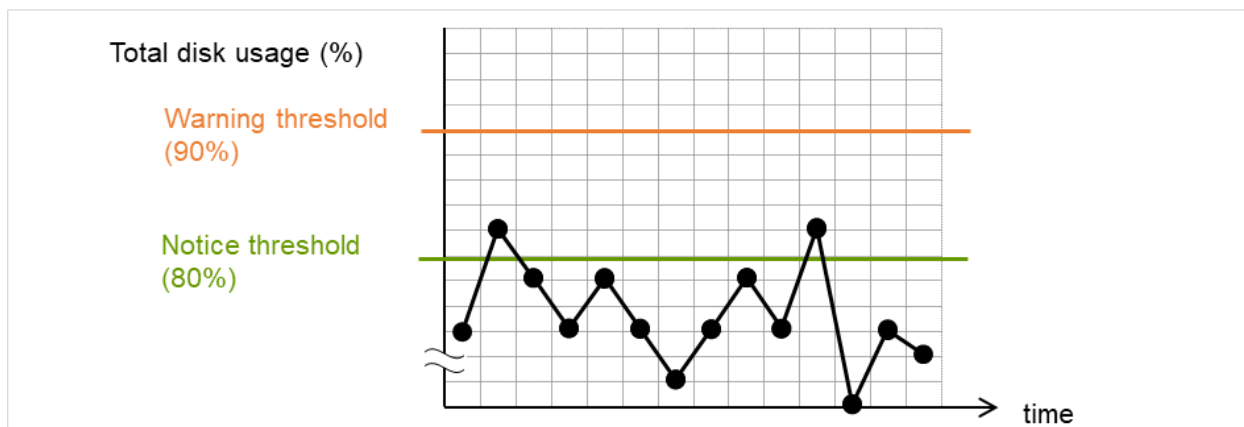


Fig. 5.18: Disk usage does not exceed the warning level upper limit (no error detected)

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 continuously exceeds the notification level upper limit, which is determined as an error in monitoring the disk usage.

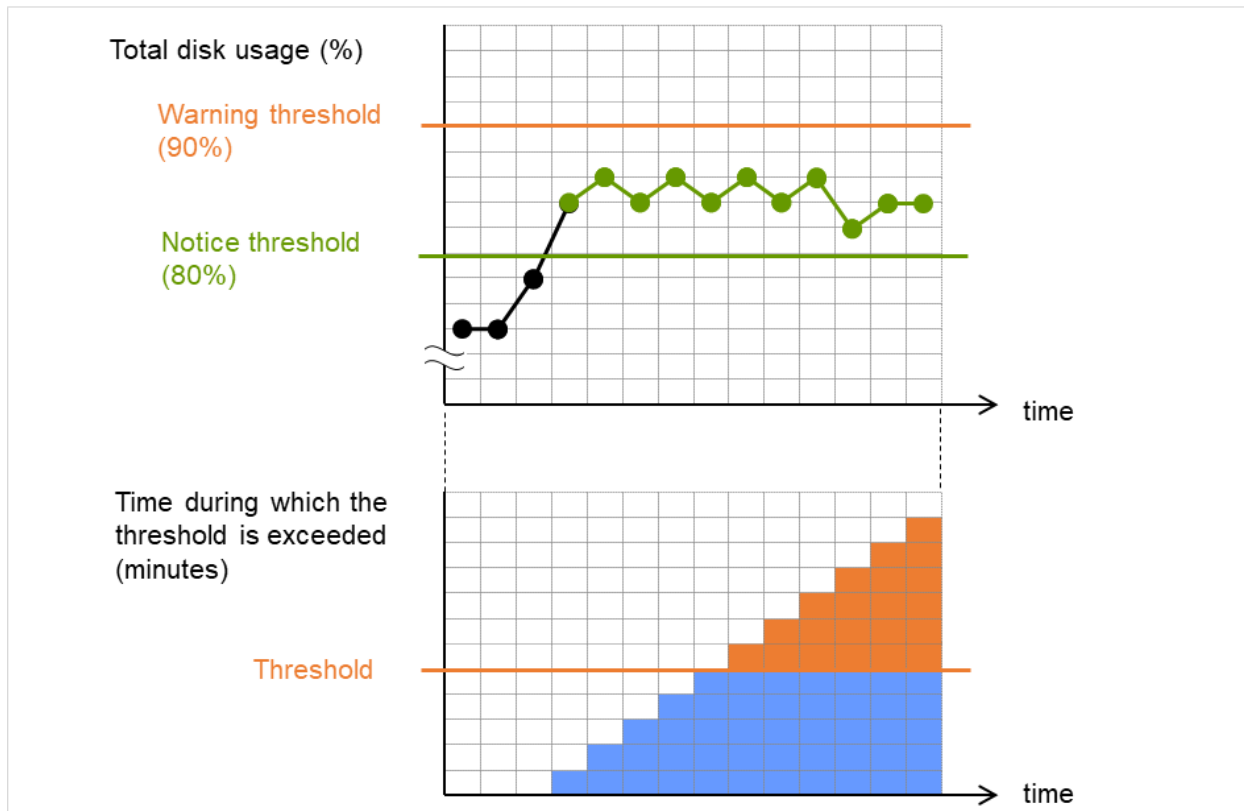


Fig. 5.19: Disk usage exceeds the notification level upper limit for a certain duration of time (an error detected)

- 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 rises and falls in the vicinity of the notification level upper limit, which is not determined as an error in monitoring the disk usage.

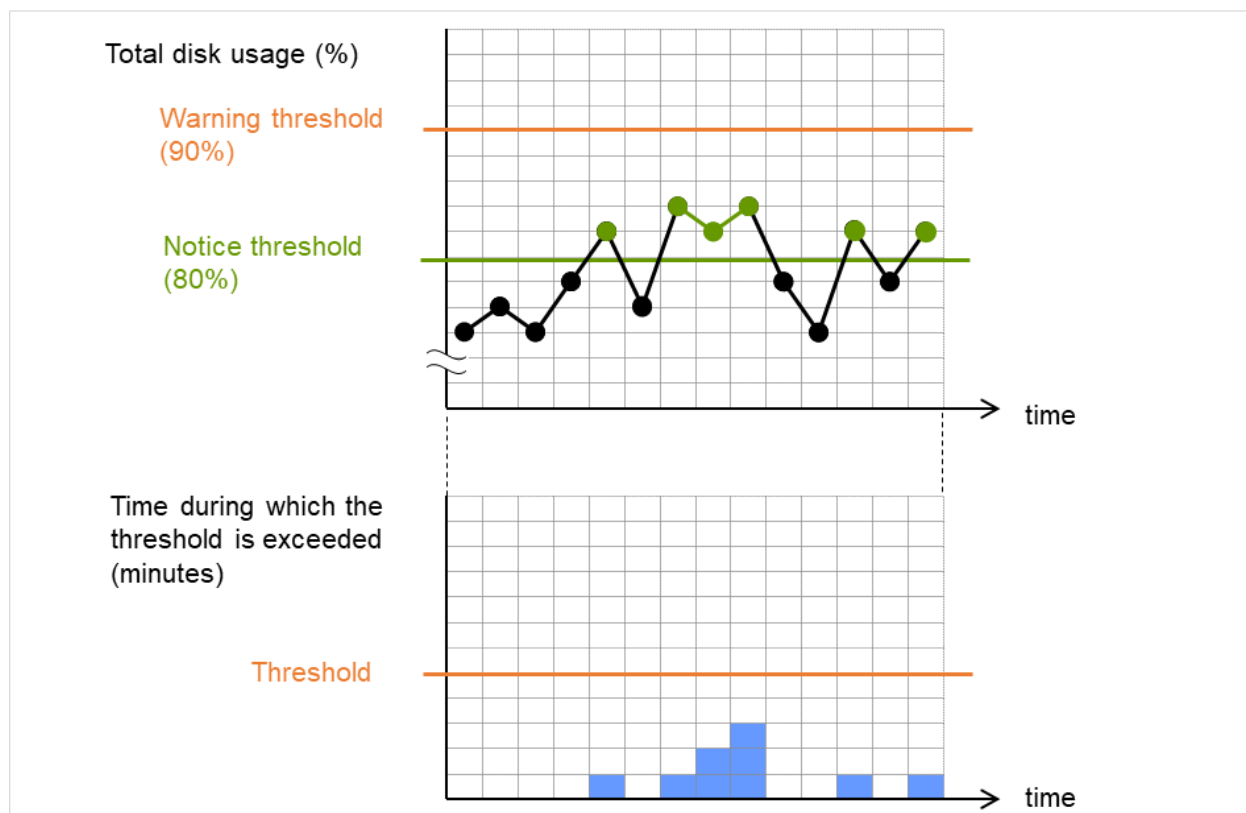


Fig. 5.20: The state of exceeding the notification level threshold in disk usage does not persist for a certain duration of time (no error detected)

5.28.3 Monitor (special) tab

Monitor Resource Properties | saw1 sraw X

[Info](#)
[Monitor\(common\)](#)
[Monitor\(special\)](#)
[Recovery Action](#)

Specify the system monitoring conditions for identifying abnormality

Monitoring CPU usage ☒

CPU usage* %

Duration Time* min

Monitoring total usage of memory ☒

Total usage of memory* %

Duration Time* min

Monitoring total usage of virtual memory ☒

Total usage of virtual memory* %

Duration Time* min

Condition of detecting failure
Warning:When exceeding level once
Notification:When continuously exceeding level over the duration

Monitoring target disk list

Logical drive	Warning(%)	Notification(%)	Duration Time(min)	Warning(MB)	Notification(MB)	Duration Time(min)
No monitoring target disks						

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 (1 to 100)

Specify the threshold for the detection of the CPU usage.

Duration Time (1 to 1440)

Specify the duration for detecting the CPU usage.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total usage of memory

Enables the monitoring of the total usage of memory.

- When 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 (1 to 100)

Specify the threshold for the detection of a memory use amount error (percentage of the memory size implemented on the system).

Duration Time (1 to 1440)

Specify the duration for detecting a total memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring total usage of virtual memory

Enables the monitoring of the total usage of virtual memory.

- When 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 (1 to 100)

Specify the threshold for the detection of a virtual memory usage error.

Duration Time (1 to 1440)

Specify the duration for detecting a total virtual memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Add

Click this to add disks to be monitored. The **Input of watch condition** dialog box appears.

Configure the detailed monitoring conditions for error determination, according to the descriptions given in the **Input of watch condition** dialog box.

Remove

Click this to remove a disk selected in **Disk List** so that it will no longer be monitored.

Edit

Click this to display the **Input of watch condition** dialog box. The dialog box shows the monitoring conditions for the disk selected in **Disk List**. Edit the conditions and click **OK**.

Specify monitoring condition

Logical drive*

Monitor Type

Utilization rate
☒

Warning level*
%

Notice level*
%

Duration Time*
min

Free space
☒

Warning level*
MB

Notice level*
MB

Duration Time*
min

Initialize

OK
Cancel

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.

5.29 Setting up Process resource monitor resources

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

5.29.1 Notes on Process resource monitor resource

The use of the default process resource monitor resources settings is recommended.

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

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

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

Once the cluster has been suspended and resumed, the collection of information is started from that point of time. The amount of process resources used is analyzed at 10-minute intervals. Thus, an error may be detected up to 10 minutes after the monitoring session.

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

The status of the process resource monitor resource is Warning from when start of monitoring is enabled to when the monitoring processing is actually performed. In this status, the following message is output to the alert log.

```
Monitor psrw is in the warning status. (191 : normal.)
```

To return the status of the process resource monitor resource from error to normal, perform either of the following:

- Suspending and resuming the cluster
- Stopping and starting the cluster

5.29.2 Monitoring by Process resource monitor resources

Process resource monitor resources monitor the following:

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

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

When an error detected state persists for the monitoring duration, it is posted as an error detected during resource monitoring.

If process resource monitoring (of the CPU, memory, or number of threads) operated by using the default values, a resource error is reported after 24 hours.

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

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

The maximum value is kept updated for more than 24 hours (default) and the memory usage increases by more than 10% from its initial value, which is determined as a memory leak.

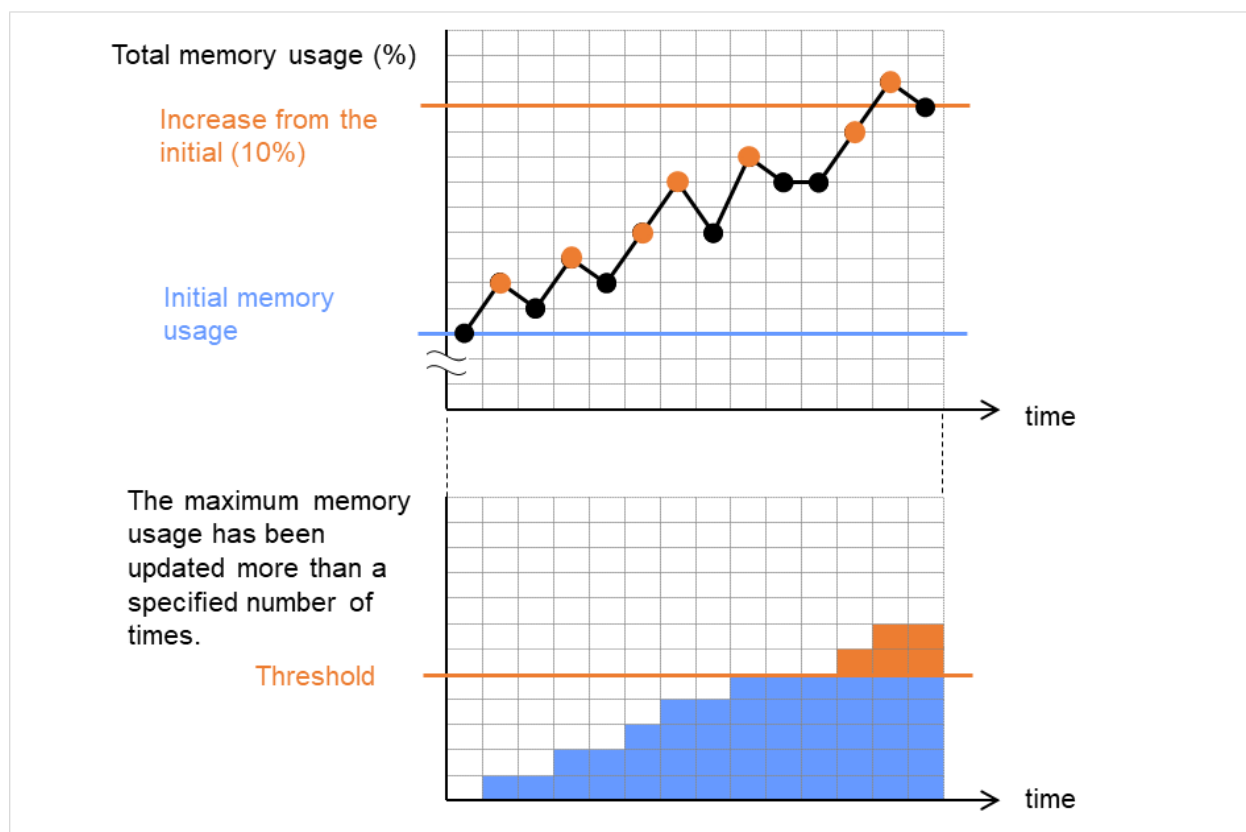


Fig. 5.21: The maximum value of the memory usage is updated more than the specified number of times, and the memory usage increases by more than 10% from its initial value (an error detected)

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

The memory usage increases and decreases within a set range, which is not determined as a memory leak.

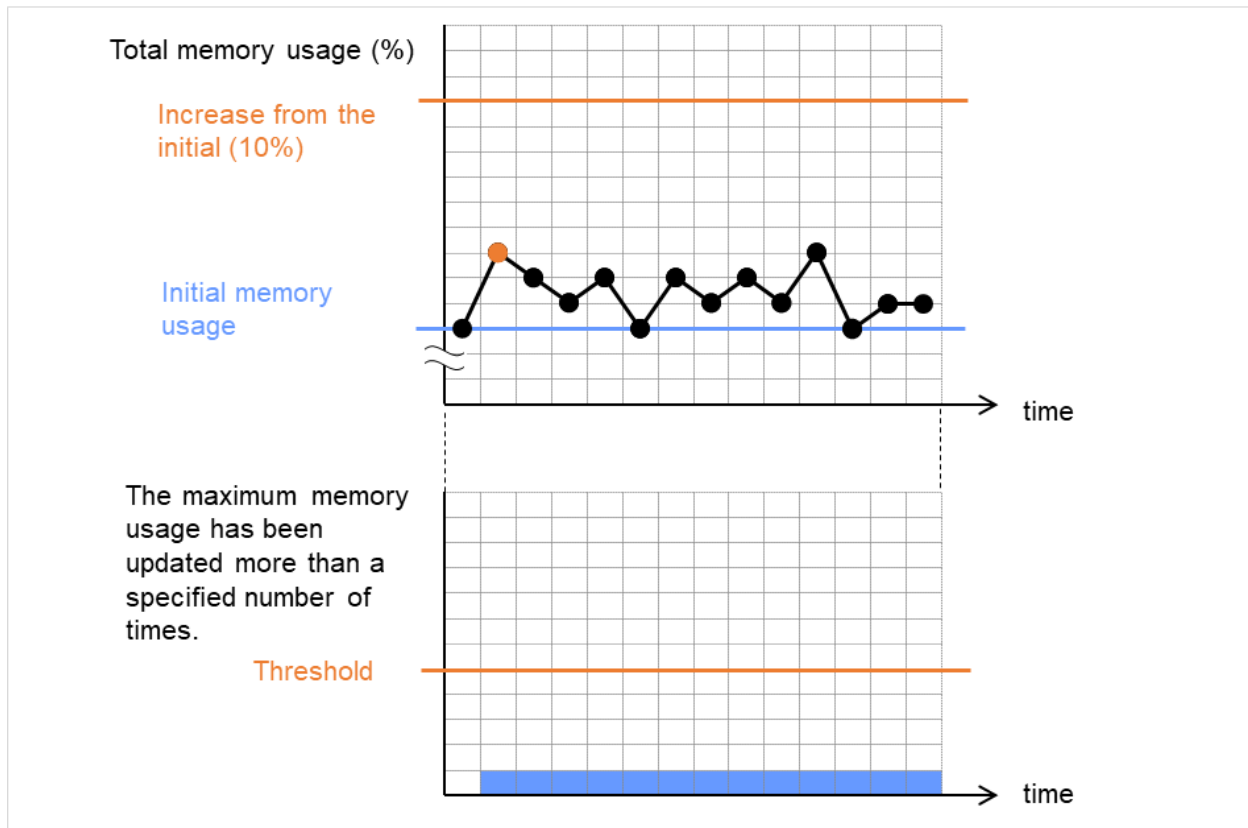


Fig. 5.22: The memory usage increases and decreases within a set range (no error detected)

5.29.3 Monitor (special) tab

Monitor Resource Properties | psrw1

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

Specify the process monitoring conditions for identifying failure

Monitoring CPU usage ☒

CPU usage* 90 %

Duration Time* 1440 min

Monitoring usage of memory ☒

Rate of Increase from the First Monitoring Point* 10 %

Duration Time* 1440 min

Monitoring number of opening files(maximum number) ☐

Refresh Count 1440 time

Monitoring number of running threads ☒

Duration Time* 1440 min

Monitoring Processes of the Same Name ☐

Count 100

Initialize

OK Cancel Apply

Monitoring CPU usage

Enables CPU usage monitoring.

- When the check box is selected:
Monitoring is enabled for the CPU usage.
- When the checkbox is not selected:
Monitoring is disabled for the CPU usage.

CPU usage (1 to 100)

Specify the threshold for the detection of the CPU usage.

Duration Time (1 to 4320)

Specify the duration for detecting the CPU usage.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring usage of memory

Enables the monitoring of the usage of memory.

- When the check box is selected:
Monitoring is enabled for the usage of memory.

- When the checkbox is not selected:
Monitoring is disabled for the usage of memory.

Rate of Increase from the First Monitoring Point (1 to 1000)

Specify the threshold for the detection of a memory use amount error.

Duration Time (1 to 4320)

Specify the duration for detecting a memory usage error.

If the threshold is continuously exceeded over the specified duration, the detection of an error is recognized.

Monitoring number of opening files (maximum number)

Enables the monitoring of the number of opening files (maximum number).

- When the check box is selected:
Monitoring is enabled for the number of opening files.
- When the checkbox is not selected:
Monitoring is disabled for the number of opening files.

Refresh Count (1 to 4320)

Specify the refresh count for the detection of the number of opening files error.

If the number of opening files maximum value is updated more count than specified, the detection of an error is recognized.

Monitoring number of running threads

Enables the monitoring of the number of running threads.

- When the check box is selected:
Monitoring is enabled for the number of running threads.
- When the checkbox is not selected:
Monitoring is disabled for the number of running threads.

Duration Time (1 to 4320)

Specify the duration for detecting an error with the number of running threads.

If the processes for which the number of running threads is passed more than specified times, the detection of an error is recognized.

Monitoring Processes of the Same Name

Enables the monitoring of the processes of the same name

- When the check box is selected:
Monitoring is enabled for the processes of the same name.
- When the checkbox is not selected:
Monitoring is disabled for the processes of the same name.

Count (1 to 10000)

Specify the count for detecting an error with the processes of the same name.

If the processes of the same name has been exists more than specified numbers, the detection of an error is recognized.

5.30 Setting up user mode monitor resources

The user mode monitor resources monitor any user space stalls.

The user mode monitor resources are registered by default.

5.30.1 Monitoring by user mode monitor resources

The user mode monitor resources monitor the following:

After the start of monitoring, a user mode monitor resource starts the keepalive timer and then updates the keepalive timer at monitoring intervals. It detects an error if the timer is not updated during a set duration as a result of a user space stall.

A user mode monitor resource has a setting for extending the monitoring by creating a dummy thread. If this setting is enabled, it creates a dummy thread at monitoring intervals. If it fails to create a dummy thread, it does not update the keepalive timer.

The processing logic of the user mode monitor resources is as follows:

- Overview of processing

The following steps 2 and 3 are repeated.

1. Set the keepalive timer
2. Create a dummy thread
3. Update the keepalive timer

Step 2 is a process for advanced monitor setting. If this is not set, the process is not started.

- Behavior when a timeout does not occur (steps 2 and 3, above, are processed properly)
Recovery processing such as reset is not executed.
- Behavior when a timeout occurs (Either of steps 2 or 3, above, is stopped or delayed)
According to the action settings, a reset or panic is generated by the clphb driver.

5.30.2 Monitor (special) tab

The screenshot shows a dialog box titled "Monitor Resource Properties | userw1" with a close button (X) in the top right corner. The dialog has four tabs: "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor(special)" tab is currently selected. Inside this tab, there are two dropdown menus: "Method*" with "keepalive" selected, and "Operation at Timeout Detection*" with "Stop Error" selected. Below these is a section titled "Extended Monitor Settings" which contains a checkbox labeled "Create Temporary Thread" that is checked. At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Apply".

Monitor Method

Specify how the user space is monitored.

- keepalive
The clphb driver is used.

Action When Timeout Occurs

Specify the action to take when a timeout occurs.

- No Operation
No action is taken.
- HW Reset
Reset the hardware.
- Generate an intentional stop error
Intentionally cause a stop error.

Note: A dummy failure cannot be triggered by an action when a timeout occurs.

Create a Dummy Thread

Specify whether or not to create a dummy thread when monitoring.

- When the checkbox is selected (default value)
Create a dummy thread.
- When the checkbox is not selected
Do not create a dummy thread.

OTHER SETTING DETAILS

This chapter provides details about the other items to be specified for EXPRESSCLUSTER X SingleServerSafe. 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.

This chapter covers:

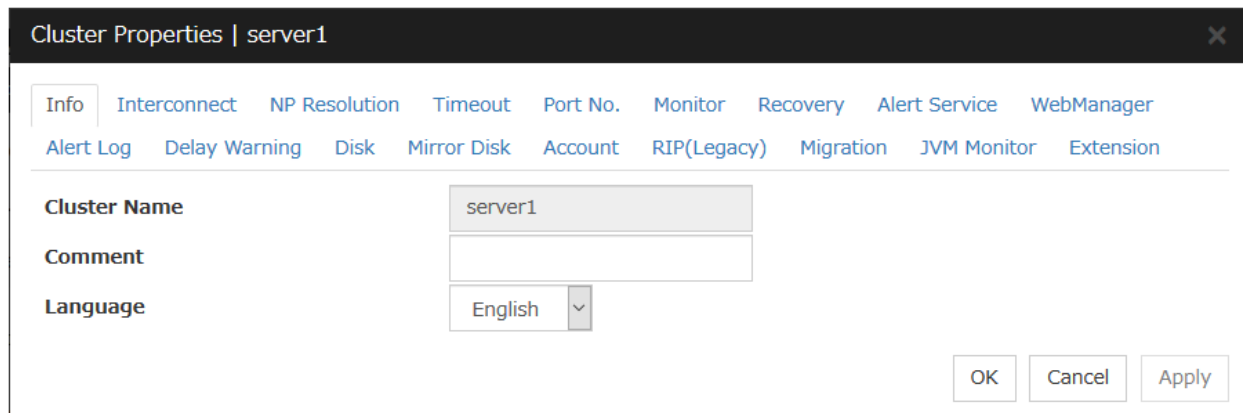
- 6.1. *Cluster properties*
- 6.2. *Server properties*
- 6.3. *Upper limits of registration*

6.1 Cluster properties

In the **Cluster Properties** window, you can view and change the detailed data of EXPRESSCLUSTER X Single-ServerSafe.

6.1.1 Info tab

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



The screenshot shows the 'Cluster Properties' window for 'server1'. The 'Info' tab is selected. The window has a dark title bar and a light gray background. The 'Info' tab is highlighted in blue. Below the tabs, there are three input fields: 'Cluster Name' with the value 'server1', 'Comment' which is empty, and 'Language' with a dropdown menu showing 'English'. At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Apply'.

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 Cluster WebUI runs.

- English
- Japanese
- Chinese

6.1.2 Interconnect tab

Not used.

6.1.3 NP Resolution tab

Not used.

6.1.4 Timeout tab

Specify values such as time-out on this tab.

Cluster Properties | server1

Info Interconnect NP Resolution **Timeout** Port No. Monitor Recovery Alert Service WebManager
Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration JVM Monitor Extension

Network initialization complete wait time* 3 min

Server Sync Wait Time 5 min

Heartbeat

Interval* 30 sec

Timeout* 300 sec

Server Internal Timeout* 180 sec

Initialize

OK Cancel Apply

Network initialization complete wait time (0 to 99)

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

Server Sync Wait Time (0 to 99)

Not used.

Heartbeat

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

Server Internal Timeout (1 to 9999)

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

Initialize

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

6.1.5 Port No. tab

Specify TCP port numbers and UDP port numbers.

Cluster Properties | server1

InfoInterconnectNP ResolutionTimeoutPort No.MonitorRecoveryAlert ServiceWebManagerAlert LogDelay WarningDiskMirror DiskAccountRIP(Legacy)MigrationJVM MonitorExtension

TCP

Server Internal Port Number*

29001

Data Transfer Port Number*

29002

WebManager HTTP Port Number*

29003

Disk Agent Port Number

29004

Mirror Driver Port Number

29005

UDP

Kernel Mode Heartbeat Port Number*

29106

Alert Sync Port Number*

29003

TCP/UDP

Client Service Port Number*

29007

Initialize

OKCancelApply

TCP

No TCP port numbers can be overlapped.

- **Server Internal Port Number** (1 to 65,535¹)
This port number is used for internal communication.
- **Information Base Port Number** (1 to 65,535¹)
This port number is used for cluster information management.
- **Data Transfer Port Number** (1 to 65,535¹)
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 65,535¹)
This port number is used for a browser to communicate with the EXPRESSCLUSTER Server.
- **API HTTP Port Number** (1 to 65,535¹)
This port number is used for a RESTful API client to communicate with the EXPRESSCLUSTER server.
- **API Internal Communication Port Number** (1 to 65,535¹)
This port number is used for RESTful-API internal communication.

¹ It is strongly recommended not to use well-known ports, especially reserved ports from 1 to 1,023.

- **Disk Agent Port Number** (1 to 65,535¹)
Not used.
- **Mirror Driver Port Number** (1 to 65,535¹)
Not used.

UDP

No UDP port numbers can be overlapped.

- **Kernel Mode Heartbeat Port Number** (1 to 65,535¹)
This port number is used for the kernel mode heartbeat.
- **Alert Sync Port Number** (1 to 65,535¹)
This port number is used to synchronize alert messages.

TCP/UDP

- **Client Service Port Number** (1 to 65,535¹)
This port number is used for the client service.

Initialize

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

6.1.6 Monitor tab

Specify the settings for monitoring.

Cluster Properties | server1

Info Interconnect NP Resolution Timeout Port No. **Monitor** Recovery Alert Service WebManager
Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration JVM Monitor Extension

System Resource

Collect the System Resource Information ☐

Initialize

OK Cancel Apply

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 Cluster WebUI collects logs.

Specify type 1 to collect the log by the clplogcc command; specify Pattern 1 to collect the log by the Cluster WebUI. For details on log collection, see "Collecting logs (clplogcc command)" in "EXPRESSCLUSTER X SingleServerSafe command reference" in the "EXPRESSCLUSTER X SingleServerSafe Operation Guide", or the online manual.

A disk area of 450 MB or more is required to store the resource information, depending on the system operating conditions such as the number of processes that are running.

- When the check box is not selected:
No system resource information is collected.

6.1.7 Recovery tab

Specify the settings for recovery.

The screenshot shows the 'Cluster Properties' dialog box for 'server1', with the 'Recovery' tab selected. The dialog has a dark title bar and a light gray background. At the top, there is a horizontal menu with tabs: Info, Interconnect, NP Resolution, Timeout, Port No., Monitor, Recovery (selected), Alert Service, WebManager, API, Encryption, Alert Log, Delay Warning, Disk, Mirror Disk, Account, RIP(Legacy), Migration, JVM Monitor, Cloud, and Extension. Below the tabs, the 'Recovery' section contains several settings:

- Action When the Cluster Service Process Is Failure***: A dropdown menu set to 'Emergency shutdown'.
- Recovery Action for HA Agents**: A section with two settings:
 - Max Restart Count***: A text input field containing '3' and a unit dropdown set to 'time'.
 - Recovery Action over Max Restart Count***: A dropdown menu set to 'No operation'.
- Action at Group Resource Activation or Deactivation Stall***: A dropdown menu set to 'Emergency shutdown'.
- Disable the Final Action when OS Stops Due to Failure Detection**: A button labeled 'Detailed Settings'.
- Disable Shutdown When Multi-Failover-Service Detected**: A button labeled 'Detailed Settings'.
- Initialize**: A button at the bottom left.

At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Action When the Cluster Service Process Is Failure

Specify an action at process abnormality of the cluster service.

- Emergency shutdown
Shutdown the server.
- 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.
 - No operation
 - Stop the cluster service
Stops the cluster service of the server that detected an error.
 - Stop the cluster service and shutdown OS
Stops the cluster service of the server that detected an error, and then shuts down the OS.
 - Stop the cluster service and reboot OS
Stops the cluster service of the server that detected an error, and then reboots the OS.

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

Action at Group Resource Activation or Deactivation Stall

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

- Emergency shutdown
Shutdown the server on which a stall occurred.
- Intentionally causing a stop error
Intentionally cause a stop error (Panic) on the server on which a stall occurred.
- Nothing (handle a stall as an activation/deactivation failure)
Use this to perform recovery upon the detection of an activation/deactivation failure of a group resource.

Note: If a stall occurs with "Nothing (handle a stall as an activation/deactivation failure)" specified, the effect on the group resources is undefined, so we do not recommend changing the setting to "Nothing (handle a stall as an activation/deactivation failure)". If you do specify "Nothing (handle a stall as an activation/deactivation failure)", set the recovery operation upon the detection of an activation/deactivation failure of a group resource as described below.

- Activation/deactivation retry threshold: 0 (times)
- Failover threshold: 0 (times)
- Final action: Intentionally causing a stop error

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

Disable the Final Action when OS Stops Due to Failure Detection

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

Detailed Settings

Final Action When OS Stops Due to All Server Shutdown

Group Resource When Activation Failure Detected ☐

Group Resource When Deactivation Failure Detected ☐

Monitor Resource When Failure Detected ☐

- **Group Resource When Activation Failure Detected**

If the final action caused by an activation error detection in a group resource accompanies the OS stop, the final action is suppressed.

- **Group Resource When Deactivation Failure Detected**

If the final action caused by a deactivation error detection in a group resource accompanies the OS stop, the final action is suppressed.

- **Monitor Resource When Failure Detected**

If the final action caused by an error detection in a monitor resource accompanies the OS stop, the final action is suppressed.

Note:

- The message receive monitor resource does not become the target for which the final action caused by error detection is suppressed.
- The following situations lead to an OS stop during the final action when an activation/deactivation error is detected in a group resource and during the final action when a monitor resource error is detected.
 - Cluster service stop and OS shutdown
 - Cluster service stop and OS restart
 - Generation of an intentional stop error

Disable Shutdown When Multi-Failover-Service Detected

Not used.

6.1.8 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 4.3 for Windows, and register the license.

Cluster Properties | server1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery **Alert Service** WebManager
API Encryption Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration
JVM Monitor Cloud Extension

Enable Alert Setting ☐ [Edit](#)

Mail Report

E-mail Address

Subject

Mail Method

SNMP Trap

Destination Settings

Use Chassis Identify ☐

☒ Execute Repeatedly Interval sec

☐ Do not Execute Repeatedly

Use Network Warning Light ☐

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 "Error messages" in the "EXPRESSCLUSTER X SingleServerSafe 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 **Settings** to configure the SNMP trap transmission destination.

Use Chassis Identify

Not used.

Execute Repeatedly

Not used.

Do not Execute Repeatedly

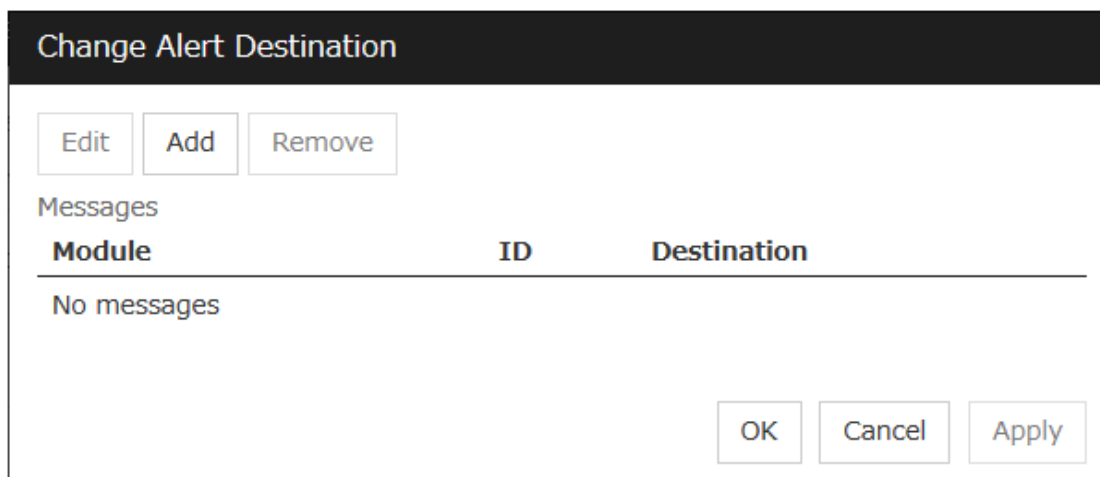
Not used.

Use Network Warning Light

Not used.

Change Alert Destination

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



The dialog box titled "Change Alert Destination" has a dark header bar. Below the header, there are three buttons: "Edit", "Add", and "Remove". Underneath these buttons is a section labeled "Messages". Inside this section is a table with three columns: "Module", "ID", and "Destination". The table is currently empty, with the text "No messages" displayed below the column headers. At the bottom right of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

Module	ID	Destination
No messages		

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

Category

Process

Module Type*

apisv

Event ID*

1

Destination

☐ Alert Logs

☐ Alert Extension

☐ Mail Report

☐ SNMP Trap

☐ Message Topic

☐ Event Log(DisableOnly)

Command

EditAddRemove

No commands

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 "Error messages" in the "EXPRESSCLUSTER X SingleServerSafe Operation Guide".

Destination

Select a message destination from the following options.

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

- **Mail Report**
Uses the mail report function.
- **SNMP Trap**
Uses the SNMP trap transmission function to send messages.
- **Message Topic**
This sends message to Amazon SNS.
- **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.)

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

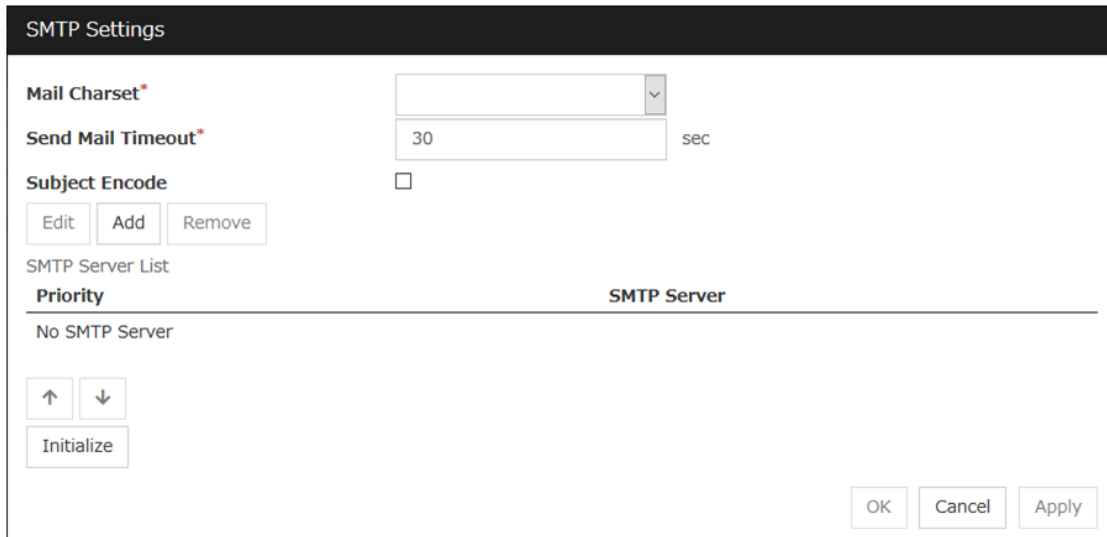
Click this to remove a command of the alert extension function. Select the command, and then, click **Remove**.

Edit

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

SMTP Settings

Click **SMTP Settings** to display the **SMTP Settings** dialog box used for the mail alert.

The image shows a 'SMTP Settings' dialog box. It has a dark title bar. Inside, there are several sections. The first section is 'Mail Charset*' with a dropdown menu. The second is 'Send Mail Timeout*' with a text box containing '30' and a 'sec' label. The third is 'Subject Encode' with a checkbox. Below these are three buttons: 'Edit', 'Add', and 'Remove'. The next section is 'SMTP Server List' which contains a table with two columns: 'Priority' and 'SMTP Server'. The table is currently empty, showing 'No SMTP Server'. Below the table are two arrow buttons (up and down) and an 'Initialize' button. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Priority	SMTP Server
No SMTP Server	

Mail Charset (within 127 bytes)

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

Send Mail Timeout (1 to 999)

Configure the timeout value for the communication with SMTP server.

Subject Encode

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

SMTP Server List

Use this button to display a SMTP server that has been configured. Only one SMTP server can be configured in this version.

Add

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

Remove

Select this to remove the SMTP server.

Edit

Use this button to modify the settings of SMTP server.

Enter the SMTP Server

SMTP Server*

SMTP Port*

Sender Address

Enable SMTP Authentication ☐

Authentication Method

User Name

Password

SMTP Server (within 255 bytes)

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

SMTP Port (1 to 65,535)

Configure the port number of the SMTP server.

Sender Address (within 255 bytes)

Configure the address from which mail report is sent.

Enable SMTP Authentication

Configure whether or not to enable SMTP authentication.

Method

Select a method of SMTP authentication.

User Name (within 255 bytes)

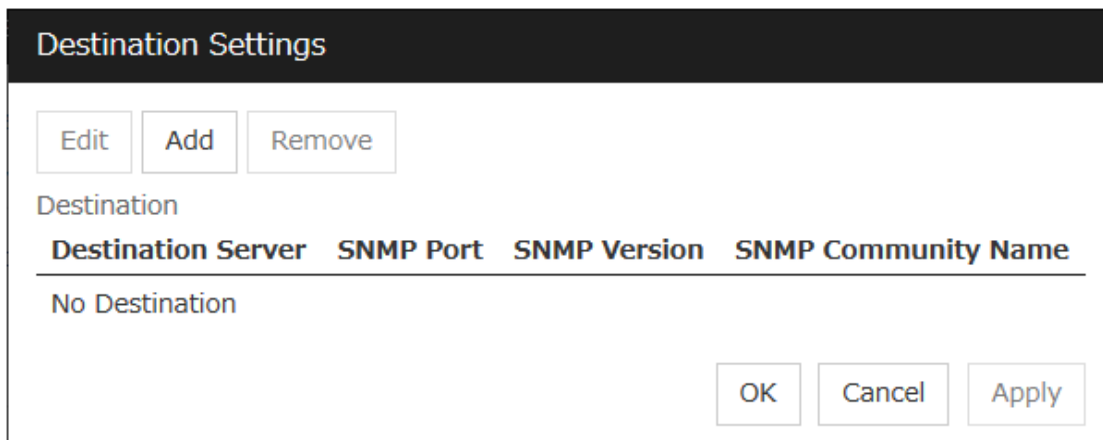
Configure the user name used for SMTP authentication.

Password (within 255 bytes)

Configure the password used for SMTP authentication.

SNMP Settings

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



The **Destination Settings** dialog box features a dark header bar with the title. Below the header, there are three buttons: **Edit**, **Add**, and **Remove**. A section titled **Destination** contains a table with the following headers: **Destination Server**, **SNMP Port**, **SNMP Version**, and **SNMP Community Name**. The table currently shows a single entry: **No Destination**. At the bottom right of the dialog are three buttons: **OK**, **Cancel**, and **Apply**.

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.



The **Enter Destination** dialog box has a dark header bar with the title. It contains four labeled input fields: **Destination Server*** (text box), **SNMP Port*** (text box with value 162), **SNMP Version** (dropdown menu with value v2c), and **SNMP Community Name*** (text box with value public). At the bottom right are **OK** and **Cancel** buttons.

Destination Server (within 255 bytes)

Configure the name of the SNMP trap transmission destination server.

SNMP Port No. (1 to 65535)

Configure the port number of the SNMP trap transmission destination.

SNMP Version

Configure the SNMP version of the SNMP trap transmission destination.

SNMP Community Name (within 255 bytes)

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

6.1.9 WebManager tab

Specify the settings for the WebManager Server.

Cluster Properties | server1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service **WebManager**

API Encryption Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration

JVM Monitor Cloud Extension

Enable WebManager Service ☒

Communication Method

☒ HTTP

☐ HTTPS

Accessible number of clients*

Control connection by using password

Control connection by using client IP address ☐

Cluster WebUI Operation Log

Output Cluster WebUI Operation Log ☐

Log output path

File Size MB

Integrated WebManager

Connection IP address

! If OS Authentication Method is configured, it is recommended to configure HTTPS for Communication Method.

Enable WebManager Service

The WebManager service is enabled.

- When selected:
The WebManager service is enabled.
- When cleared:
The WebManager service is disabled.

Communication Method

- HTTP

No encryption is used for communicating with a client.

- HTTPS

Encryption is used for communicating with a client.

Accessible number of clients (1 to 999)

Specify the number of client machines that can be connected.

Control connection by using password

Click the **Settings** button to open the **Password** dialog box.

Password Settings

☒ Cluster Password Method

Password for Operation

Change

Password for Reference

Change

☐ OS Authentication Method

Add

Remove

Edit

Authorized Group List

Group	Operation
No authorized groups	

Login Session Lifetime Period

min

Automatic Logout Time Period

min

Lockout Threshold

time

Lockout Time

min

Initialize

ⓘ If OS Authentication Method is configured, it is recommended to configure HTTPS for Communication Method.

OK

Cancel

Apply

Cluster Password Method / OS Authentication Method

Choose a login method for Cluster WebUI from below.


- Cluster Password Method

Performs authentication with an operation/reference password you set.

- OS Authentication Method
Performs authentication with user and password of OS.

Cluster Password Method

- Password for Operation
Set a password to connect to the Cluster WebUI in the operation mode.
Click **Change** to display the **Enter Password** dialog box.
- Password for Reference
Set a password to connect to the Cluster WebUI in the reference mode.
Click **Change** to display the **Enter Password** dialog box.

A dialog box titled "Enter password" with a dark header. It contains three input fields: "Old Password", "Password", and "Password Confirmation". The "Old Password" field is the top one, followed by "Password", and then "Password Confirmation". At the bottom right, there are two buttons: "OK" and "Cancel".

Enter password	
Old Password	<input type="text"/>
Password	<input type="text"/>
Password Confirmation	<input type="text"/>
<div>OK Cancel</div>	

- **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**.

OS Authentication Method

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

- If the server belongs to a work group:
Register users and a group to the server.
- If the server belongs to a domain:
Register users and a group to a domain.

Add

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



The dialog box has a title bar labeled "Group Name". Inside, there is a label "Group Name*" followed by a text input field. At the bottom right, there are two buttons: "OK" and "Cancel".

- **Group Name** (Within 255 bytes)
Enter the name of the group to be authorized. Users belonging to the specified group are authorized. Groups must be registered to the server in advance.

Remove

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

Edit

Used to edit a group. From **Authorized Group List**, select a group to be edited. Then click **Edit**. The **Group Name** dialog box appears with the selected group entered. The control permission does not change in this procedure.

Operation

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

- If the check box is checked:
Users belong to the group can operate the cluster and view the status.
- If the check box is not checked:
Users belongs to the group can only view the status.

Login Session Lifetime Period (0 to 52560)

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

Automatic Logout Time Period (0 to 99999)

Sets the logout time for the automatic logout when there is no communication between Cluster WebUI and WebManager server. If this is set to zero (0), no automatic logout occurs.

Lockout Threshold (0 to 999)

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

Lockout Time (1 to 99999)

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

Initialize

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

Control connection by using client IP address

If selected, accesses are controlled by client IP addresses.

- When selected:

Add, **Remove** and **Edit** buttons are displayed.

- When cleared:
Add, **Remove** and **Edit** buttons are not displayed.

Add

Use **Add** to add an IP address in **Connection Permit Client IP Address List**. 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.

The image shows a dialog box titled "IP Address" with a dark header bar. Below the header, the text "IP Address*" is displayed next to a text input field. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

- **IP Address** (within 80 bytes)
Specify a client IP address that can be connected.
 - IP address: 10.0.0.21
 - Network address: 10.0.1.0/24

Remove

Use **Remove** to remove an IP address from **Connection Permit Client IP Address List**. Select an IP address you want to remove in **Connection Permit Client IP Address List** and click **Remove**.

Edit

Use **Edit** to change an IP address. Select an IP address you want to edit in **Connection Permit Client IP Address List** 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 **Connection Permit Client IP Address List**.

- 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.

Output Cluster WebUI Operation Log

Allows you to output the operation log of Cluster WebUI.

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

Log output path (Within 255 bytes)

Specify the output destination directory of the Cluster WebUI operation log with an absolute path consisting of ASCII characters.

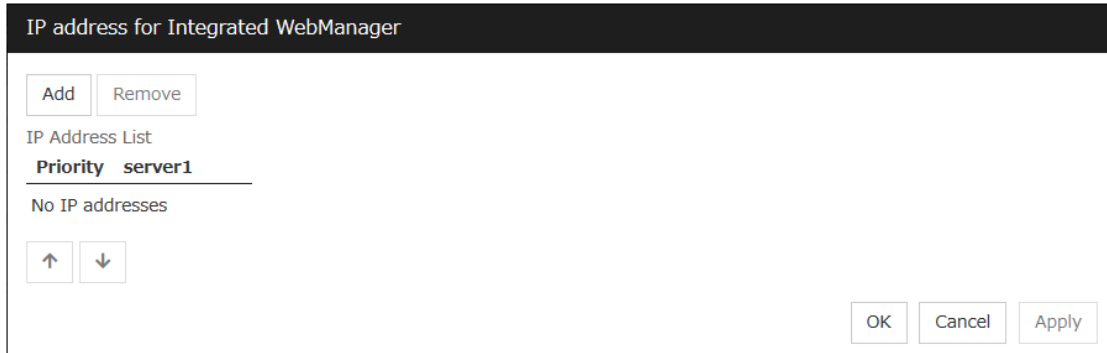
File Size (1 to 10)

Specify the size of Cluster WebUI operation log.

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

IP address for Integrated WebManager

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



The dialog box titled "IP address for Integrated WebManager" contains the following elements:

- Buttons: "Add" and "Remove" at the top left.
- Section: "IP Address List" with a sub-header "Priority server1".
- Table: A table with one row containing the text "No IP addresses".
- Buttons: Up and down arrows below the table.
- Buttons: "OK", "Cancel", and "Apply" at the bottom right.

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

Tuning

Use **Tuning** to tune the WebManager Server. Click **Tuning** to open the **WebManager Tuning Properties** dialog box.

WebManager Tuning Properties

Behavior

Client Session Timeout*	30	sec
Screen Data Refresh Interval*	90	sec
Mirror Agent Timeout	150	sec
Time Limit For Keeping Log Files*	600	sec
Use Time Information Display Function	<input checked="" type="checkbox"/>	

Initialize

OK Cancel Apply

- **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 Cluster WebUI.
- **Reload Interval** (0 to 999)
At this time interval, the Cluster WebUI screen is refreshed.
- **Mirror Agent Timeout** (1 to 999)
Not used.
- **Time Limit For Keeping Log Files** (60 to 43,200)
Time limit determines when the log collection information temporarily saved on the server will be deleted. When the time specified here has elapsed, the log collection information will be deleted unless you save the file when the dialog box asking you if you save the log collection information is displayed.
- **Use Time Info**
Specify whether the time information display function is enabled or disabled.
 - **When the check box is selected**
The time information display function is enabled.
 - **When the check box is not selected**
The time information display function is disabled.
- **Initialize**
Used for initializing the value to the default value. Click Initialize to initialize all the items to their default values.

6.1.10 API Tab

Specify the settings for the API service.

Cluster Properties | cluster

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager **API** Encryption Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration Cloud Extension

Enable API Service ☐

Communication Method

☐ HTTP

☒ HTTPS

Set a privilege per group ☐

Control connection by using client IP address ☐

Tuning

! If enable API service, it is recommended to configure HTTPS for Communication Method.

OK Cancel Apply

Enable API Service

API services are enabled.

- If the check box is checked:
API services are enabled.
- If the check box is not checked:
API services are disabled.

Communication Method

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

Control a privilege of operating clusters per group

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

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

Login users must be registered beforehand in the server which issues the request. More specifically, a group must be registered to the server and the users must belong to it as the control permission of a cluster is assigned per group.

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

- If the server belongs to a domain:
Register users and groups in the domain.

Add

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

The image shows a dialog box titled "Group Name" with a dark header bar. Below the header, there is a text input field with the placeholder text "Group Name*" in red. To the right of the input field are two buttons: "OK" and "Cancel".

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

Remove

Use this option to delete a group from **Authorized Group List**.

From **Authorized Group List**, select a group to be deleted. Then, click **Remove**.

Edit

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

Operation

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

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

Control connection by using client IP address

The connection is controlled by the client IP address.

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

Add

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

A dialog box titled "IP Address" with a dark header. Below the header, the text "IP Address*" is followed by a text input field. At the bottom right, there are two buttons: "OK" and "Cancel".

IP Address

IP Address*

OK Cancel

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

Specify a client IP address allowed for the connection.

- Example for IP address: 10.0.0.21
- Example for network address: 10.0.1.0/24

Remove

Used to remove an IP address from **Connection Permit Client IP Address List**. From **Connection Permit Client IP Address List**, select the IP address to be removed, and click **Remove**.

Edit

Used to edit an IP address. From **Connection Permit Client IP Address List**, select the IP address you want to edit, and click **Edit**. Then the **IP address** dialog box where the specified IP address is preset is displayed.

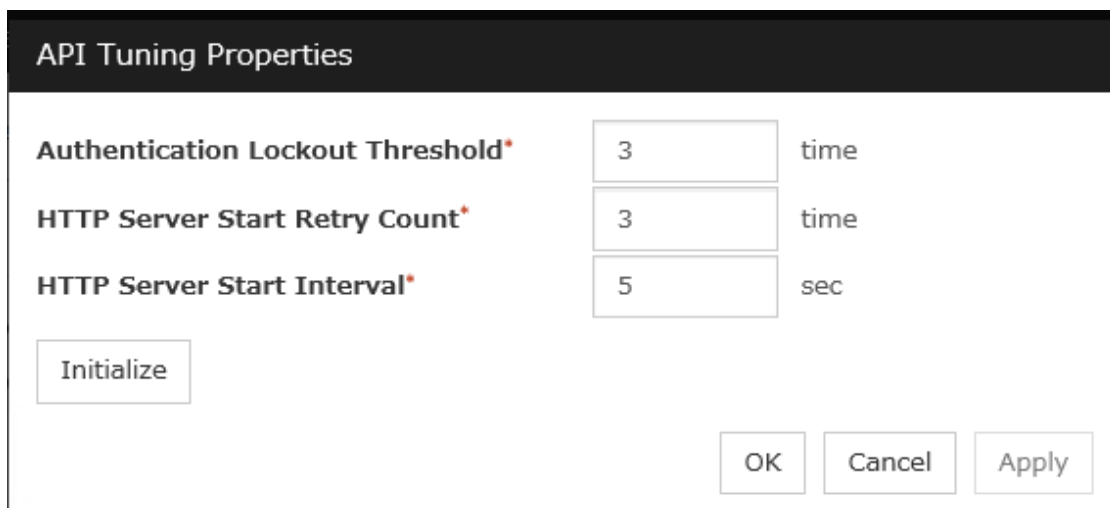
Operation

Set operation rights for any of the IP addresses registered in **Connection Permit Client IP Address List**.

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

Tuning

Used to adjust the API service. Click **Tuning** to display the **API Tuning Properties** dialog box.

A dialog box titled "API Tuning Properties" with a dark header. Below the header, there are three rows of settings. Each row has a label, a text input field, and a unit. The first row is "Authentication Lockout Threshold*" with a value of "3" and unit "time". The second row is "HTTP Server Start Retry Count*" with a value of "3" and unit "time". The third row is "HTTP Server Start Interval*" with a value of "5" and unit "sec". At the bottom left, there is an "Initialize" button. At the bottom right, there are three buttons: "OK", "Cancel", and "Apply".

API Tuning Properties

Authentication Lockout Threshold* 3 time

HTTP Server Start Retry Count* 3 time

HTTP Server Start Interval* 5 sec

Initialize

OK Cancel Apply

- **Authentication Lockout Threshold**

Specify the number of times of repeated authentication failures to log in to HTTP server that sets the lockout.

- **HTTP Server Start Retry Count**

Specify the maximum number of HTTP server startup retry when API service fails to start it up.

- **HTTP Server Start Interval**

Specify the interval between when API service fails to start up HTTP server and when it retries the startup next time.

- **Initialize**

Used to restore the default value. All the items restore the default values when **Initialize** is clicked.

6.1.11 Encryption tab

Specify the settings for a file and a library to be used for the encryption of cluster related services.

Cluster Properties | cluster

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager
API Encryption Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration Extension

Certificate File

Private Key File

SSL Library

Crypto Library

i The name and path of the OpenSSL library may be different.
Please confirm before setting.

OK Cancel Apply

Certificate File

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

Private Key File

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

SSL Library

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

Crypto Library

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

6.1.12 Alert Log tab

Specify the settings for the alert log.

Cluster Properties | server1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager

Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration JVM Monitor Extension

Enable Alert Service ☒

Max. Number to Save Alert Records* 10000

Alert Sync

Method unicast

Communication Timeout 30 sec

Initialize

OK Cancel Apply

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

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

6.1.13 Delay Warning tab

Specify the settings for **Delay Warning** on this tab. For details about **Delay Warning**, see "*Delay warning of a monitor resource*" in "*7. Monitoring details*".

The screenshot shows the 'Cluster Properties | server1' dialog box with the 'Delay Warning' tab selected. The tab contains three sections: 'Heartbeat Delay Warning', 'Monitor Delay Warning', and 'COM Delay Warning'. Each section has a checked checkbox, a horizontal slider set to 80%, and a text box displaying '80 %'. Below these sections is an 'Initialize' button. At the bottom right of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

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

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

6.1.14 Disk tab

Not used.

6.1.15 Mirror Disk tab

Not used.

6.1.16 Account tab

The **Account** tab is used to register and/or delete the user account that is used in the /U option of the **ARMLOAD** command (compatible command) or the script executed by the cluster system. You can set up to 16 (sixteen) user accounts.

The screenshot shows the 'Cluster Properties | server1' dialog box. The 'Account' tab is selected. At the top, there are buttons for 'Edit', 'Add', and 'Remove'. Below these is the 'Account List' section, which contains a table with the header 'User Name' and one row with the text 'No accounts'. At the bottom right of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Add

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

The 'Enter account' dialog box has a dark header. It contains two input fields: 'User Name*' and 'Password'. To the right of the 'Password' field is a 'Change' button. At the bottom right are 'OK' and 'Cancel' buttons.

- **User Name**
Enter a user account name to be registered. When specifying an account of a domain, enter, for example, "*Domain Name\Account Name*".
- **Password**
Enter a password of the user account to be registered.

Remove

Use **Remove** to remove a user account from the Account List. Select the user account you want to remove from **Account** and then click **Remove**.

Edit

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

6.1.17 RIP (Legacy) tab

Not used.

6.1.18 Migration tab

Not used.

6.1.19 JVM monitor tab

Configure detailed parameters for the JVM monitor.

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

Cluster Properties | server1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager

API Encryption Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration

JVM Monitor Cloud Extension

Java Installation Path

Maximum Java Heap Size*

16

MB

Java VM Additional Option

Log Output Setting

Settings

Resource Measurement Setting

Settings

Connection Setting

Settings

Load Balancer Linkage Settings*

No linkage

Settings

Action Timeout*

60

sec

OK

Cancel

Apply

Java Installation Path (Within 255 bytes)

Set the Java VM install path used by the JVM monitor. Specify an absolute path using ASCII characters. Do not add "\" to the end of the path. Specification example: C:\Program Files\Java\jdk1.8.0_102

Maximum Java Heap Size (7 to 4096)

Set, in megabytes, the maximum Java VM heap size used by the JVM monitor (equivalent to -Xmx of the Java VM startup option).

Java VM Additional Option (Within 1024 bytes)

Set the Java VM startup option used by the JVM monitor. However, specify -Xmx for **Maximum Java Heap Size**. Specification example: -XX:+UseSerialGC

Log Output Setting

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

Resource measurement Setting

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

Connection Setting

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

Load Balancer Linkage Settings

Click the **Settings** button to open the **Load Balancer Linkage Settings** dialog box.

Action Timeout (30 to 300)

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

Log Output Setting

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

The screenshot shows the 'Log Output Setting' dialog box. It has a title bar 'Log Output Setting'. Inside, there are several settings: 'Log Level*' is set to 'INFO' via a dropdown; 'Generation*' is set to '10' in a text box; 'Rotation Type' has two options, 'File size' (selected with a radio button) and 'Time'; 'Max Size*' is set to '3072' in a text box, with a unit 'KB' to its right; 'Start Time' is set to '00:00' in a text box; and 'Interval' is set to '24' in a text box, with a unit 'hours' to its right. At the bottom left is an 'Initialize' button. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Log Level

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

Generation (2 to 100)

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

Rotation Type

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

Initialize

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

Resource Measurement Setting [Common]

Clicking **Settings** displays the **Resource Measurement Setting** dialog box. For details on the scheme for error judgment by the JVM monitor, see "[5. Monitor resource details](#)".

Resource Measurement Setting

Common WebLogic

Retry Count* 10 time

Failure Threshold* 5 time

Interval

Memory Usage,Active Threads* 60 sec

The time and count in Full GC* 120 sec

Initialize

OK Cancel Apply

Retry Count (1 to 1440)

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

Error Threshold (1 to 10)

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

Memory Usage, Active Threads (15 to 600)

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

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

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

Initialize

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

Resource Measurement Setting [WebLogic]

Clicking **Settings** displays the **Resource Measurement Setting** dialog box. For details on the scheme for error judgment by the JVM monitor, see "[5. Monitor resource details](#)".

Resource Measurement Setting

Common

WebLogic

Retry Count*

3

time

Failure Threshold*

5

time

Interval

The number of request*

60

sec

The average number of the request*

300

sec

Initialize

OK

Cancel

Apply

Retry Count (1 to 5)

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

Error Threshold (1 to 10)

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

The number of request (15 to 600)

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

The average number of the request (15 to 600)

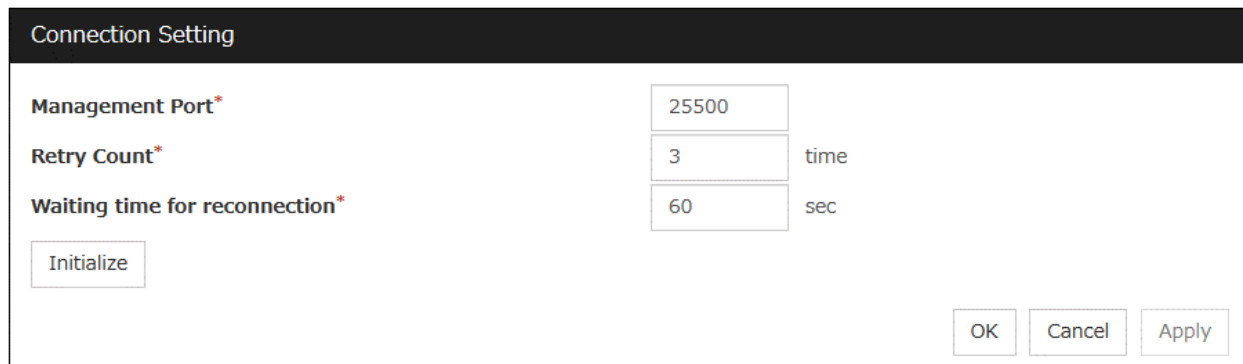
Set the interval at which the JVM monitor measures the average number of work manager or thread pool requests during WebLogic monitor. Set a value that is an integer multiple of the value set in **Interval: The number of request**.

Initialize

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

Connection Setting

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



The **Connection Setting** dialog box contains three input fields: **Management Port*** with the value 25500, **Retry Count*** with the value 3 and a unit of 'time', and **Waiting time for reconnection*** with the value 60 and a unit of 'sec'. There is an **Initialize** button on the left and **OK**, **Cancel**, and **Apply** buttons on the right.

Management Port (1 to 65535)

Sets the port number internally used by the JVM monitor resource. Make sure not to set the port number that has been used by other functions or programs. Set the number of the port connected to the monitor target Java VM. 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)

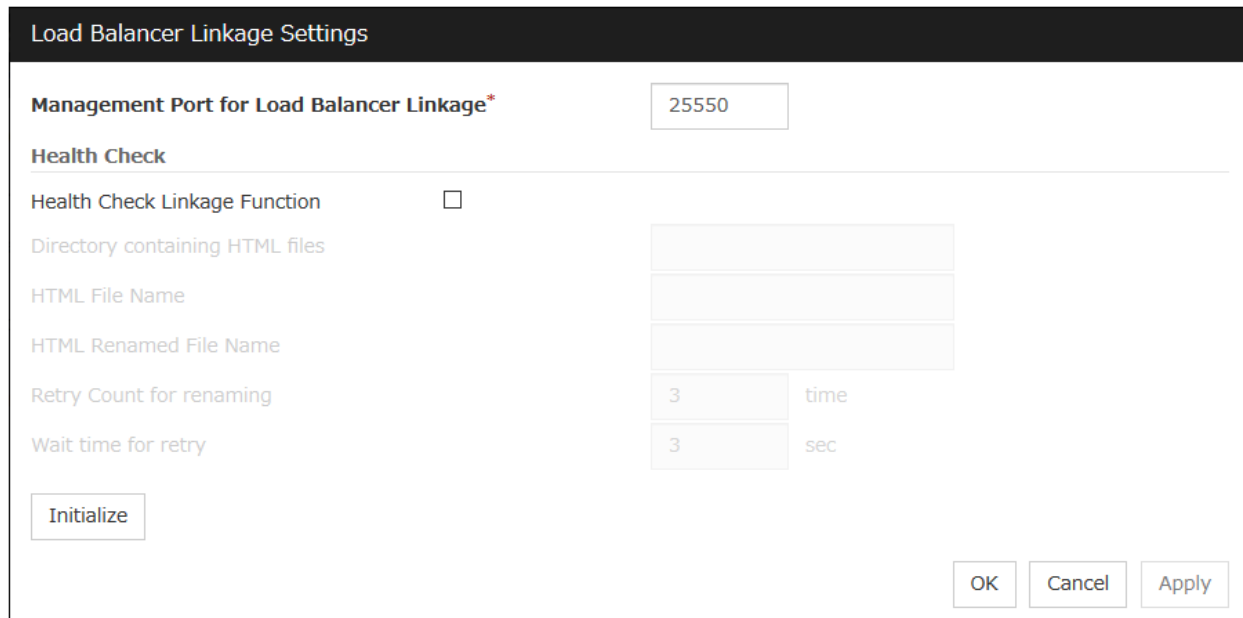
Set the interval at which the JVM monitor retries connection if it fails in Java VM connection.

Initialize

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

Load Balancer Linkage Settings

Clicking **Settings** displays the **Load Balancer Linkage Settings** dialog box.



The **Load Balancer Linkage Settings** dialog box features a **Management Port for Load Balancer Linkage*** field set to 25550. Below this is a **Health Check** section with a **Health Check Linkage Function** checkbox (unchecked). Further down are three disabled text input fields: **Directory containing HTML files**, **HTML File Name**, and **HTML Renamed File Name**. At the bottom of this section are two disabled input fields: **Retry Count for renaming** (value 3, unit 'time') and **Wait time for retry** (value 3, unit 'sec'). An **Initialize** button is on the left, and **OK**, **Cancel**, and **Apply** buttons are on the right.

Management Port for Load Balancer Linkage (1 to 65535)

Set the port number used by the load balancer linkage function. 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 (Within 255 bytes)

Set the HTML file name used by the load balancer health check function.

HTML Renamed File Name (Within 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 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

Connect Info

mgmt IP address*

User Name*

admin

Password*

●●●●●●●●

Change

Communications Port*

443

List of address of distributed nodes

Add

Remove

Server	IP Address

Initialize

OK

Cancel

Apply

Management Port for Load Balancer Linkage (1 to 65535)

Set the port number used by the load balancer linkage function. Do not set 42424 to 61000.

mgmt IP address

Set the BIG-IP LTM IP address.

User Name (Within 255 bytes)

Set the BIG-IP LTM management user name.

Password (Within 255 bytes)

Set the BIG-IP LTM management user password.

Communications Port (1 to 65535)

Set the communication port number for BIG-IP LTM.

Add

Add the server name and IP address for the distributed node. For the server name, specify the 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.

6.1.20 Cloud tab

Configure functions for cloud environments.

Enable Amazon SNS linkage function

Enable or disable the Amazon SNS linkage function.

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

TopicArn

Set TopicArn for the Amazon SNS linkage function.

Enable Amazon CloudWatch linkage function

Enable or disable the Amazon CloudWatch linkage function.

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

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

Namespace

Set Namespace for the Amazon CloudWatch linkage function.

Interval for Sending Metrics

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

6.1.21 Extension tab

Configure other cluster settings.

Cluster Properties | server1

[Info](#)
[Interconnect](#)
[NP Resolution](#)
[Timeout](#)
[Port No.](#)
[Monitor](#)
[Recovery](#)
[Alert Service](#)
[WebManager](#)
[API](#)
[Encryption](#)
[Alert Log](#)
[Delay Warning](#)
[Disk](#)
[Mirror Disk](#)
[Account](#)
[RIP\(Legacy\)](#)
[Migration](#)
[Extension](#)

Reboot Limitation

Max Reboot Count*

3

time

Max Reboot Count Reset Time*

60

min

Use Forced Stop

☐

Forced Stop Action

BMC Power Off

Forced Stop Timeout

3

sec

Virtual Machine Forced Stop Setting

Settings

Execute Script for Forced Stop

☐

Script Settings

Use CPU Frequency Control

☐

Auto Return

☒ On
☐ Off

Failover Count Method

☒ Server
☐ Cluster

Grace period of server group failover policy

0

sec

Disable Cluster Operation (Recommended for maintenance purposes)

Group Automatic Startup

☐

Recovery Operation when Group Resource Activation Failure Detected

☐

Recovery Operation when Group Resource Deactivation Failure Detected

☐

Recovery Action when Monitor Resource Failure Detected

☐

Cluster Statistics

Group	<input checked="" type="checkbox"/>	File Size	1	MB
Group Resource	<input checked="" type="checkbox"/>	File Size	1	MB
Monitor Resource	<input checked="" type="checkbox"/>	File Size	10	MB

Initialize

OK

Cancel

Apply

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 from the cluster startup keeps running normally for the time specified here, the reboot count is reset. The time specified here is separately counted for group resource and monitor resource.

Note: If **Max Reboot Count** is set to 1 or greater, 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.

Execute Script for Forced Stop

Not used.

Script Settings

Not used.

Use CPU Frequency Control

Select the checkbox when you use CPU frequency control. If you uncheck the checkbox, CPU frequency control is disabled.

See also:

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, the settings changed by the command are given higher priority regardless of whether the group is started or stopped. Note that the settings changed by using the command 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 2012:

Select [Balanced] in [Power Options] -> [Select a power plan] in [Control Panel].

Windows Server 2016:

Select [Balanced] in [Power Options] -> [Choose or customize a power plan] in [Control Panel].

Auto Return

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

Failover Count Method

Not used.

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

Not used.

Disable cluster operation

- Group Automatic Startup
 - If the check box is checked:
The group automatic startup is disabled.
 - If the check box is not checked:
The group automatic startup is not disabled.
- Recovery operation when a group resource activation error is detected
 - If the check box is checked:
This disables the recovery operation when group resource activation failure detected.
 - If the check box is not checked:
This does not disable the recovery operation when group resource activation failure detected.
- Recovery operation when a group resource deactivation error is detected
 - If the check box is checked:
This disables the recovery operation when group resource deactivation failure detected.
 - If the check box is not checked:
This does not disable the recovery operation when group resource deactivation failure detected.
- Recovery action when a monitor resource error is detected
 - If the check box is checked:
This disables the recovery action when monitor resource failure detected.
 - If the check box is not checked:

This does not disable the recovery action when monitor resource failure detected.

Note:

Disabling the recovery action when monitor resource failure detected does not affect the following actions.

- Action when the stall failure of disk RW monitor resources is detected
 - Action when the user mode monitor resources timeout occurs
 - Recovery action of the message receive monitor resource
-

Cluster Statistics

You can collect and see data on the cluster operation such as the required time of a group failover and that of resource activation.

For more information, see "Cluster statistics information collection function" in "The system maintenance information" in the "EXPRESSCLUSTER X Maintenance Guide".

- When selected:
The cluster statistical information is collected.
 - **File Size** (1 to 99)
Specify the size of the cluster statistical information file.
When the collected information reaches the specified size, rotation occurs to save up to two generations of the data.
- When cleared:
The cluster statistical information is not collected.

Initialize

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

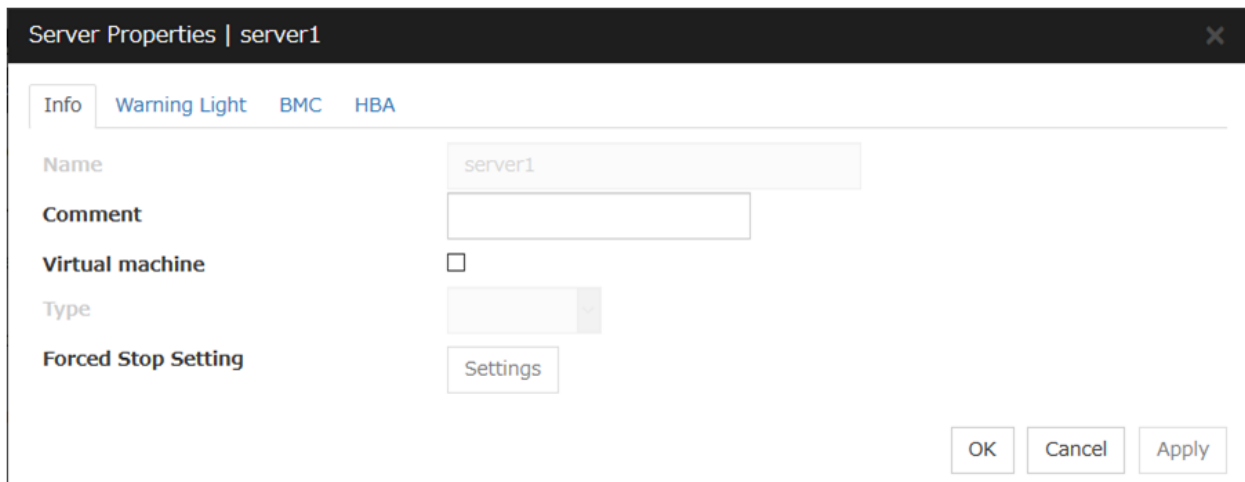
6.2 Server properties

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

6.2.1 Info tab

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



The screenshot shows the 'Server Properties' window for 'server1'. The 'Info' tab is selected, showing fields for Name (server1), Comment (empty), Virtual machine (unchecked), Type (dropdown), and Forced Stop Setting (Settings button). The window has OK, Cancel, and Apply buttons at the bottom right.

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.

6.2.2 Warning Light tab

Not used.

6.2.3 BMC tab

Not used.

6.2.4 HBA tab

Not used.

6.3 Upper limits of registration

	Version	You can register up to
Server	4.0.0-1 or later	1
Group	4.0.0-1 or later	128
Group resource (Per one group)	4.0.0-1 or later	512
Monitor resource	4.0.0-1 or later	384
System monitor resource	4.0.0-1 or later	1
Process resource monitor resource	4.0.0-1 or later	1

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:

- *7.1. Always monitor and Monitors while activated*
- *7.2. Enabling and disabling Dummy failure of monitor resources*
- *7.3. Monitor resource monitor interval*
- *7.4. Action when an error is detected by a monitor resource*
- *7.5. Recovering from a monitor error (normal)*
- *7.6. Activation or deactivation error for the recovery target during recovery*
- *7.7. Recovery/pre-recovery action script*
- *7.8. Delay warning of a monitor resource*
- *7.9. Waiting for a monitor resource to start monitoring*
- *7.10. Limiting the reboot count for error detection by a monitor resource*

7.1 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.

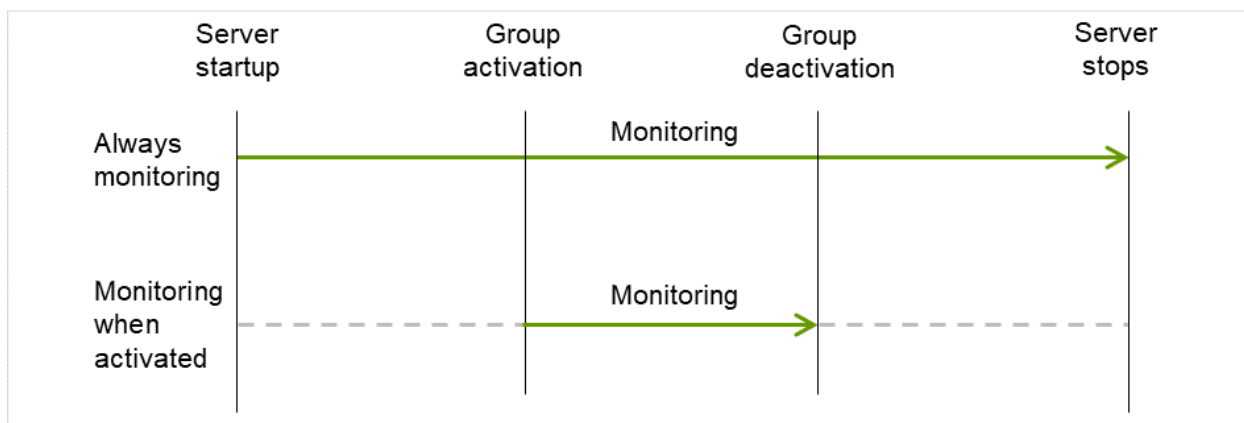


Fig. 7.1: Always monitor and Monitors while activated for a monitor resource

7.2 Enabling and disabling Dummy failure of monitor resources

You can enable and disable dummy failure of monitor resources.

Use one of the following methods to enable or disable dummy failure.

- Operation on Cluster WebUI (verification mode)
On the Cluster WebUI(Verification mode), shortcut menus of the monitor resources which cannot control monitoring are disabled.
- Operation by using the clpmonctrl command
The clpmonctrl command can control 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 "Controlling monitor resources (clpmonctrl command)" in "EXPRESSCLUSTER X SingleServerSafe command reference" in the "EXPRESSCLUSTER X SingleServerSafe Operation Guide".

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

- Dummy failure was disabled on Cluster WebUI (verification mode)
- "Yes" was selected from the dialog displayed when the Cluster WebUI mode changes from verification mode to a different mode.
- -n was specified to enable dummy failure by using the clpmonctrl command
- Stop the cluster
- Suspend the cluster

7.3 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

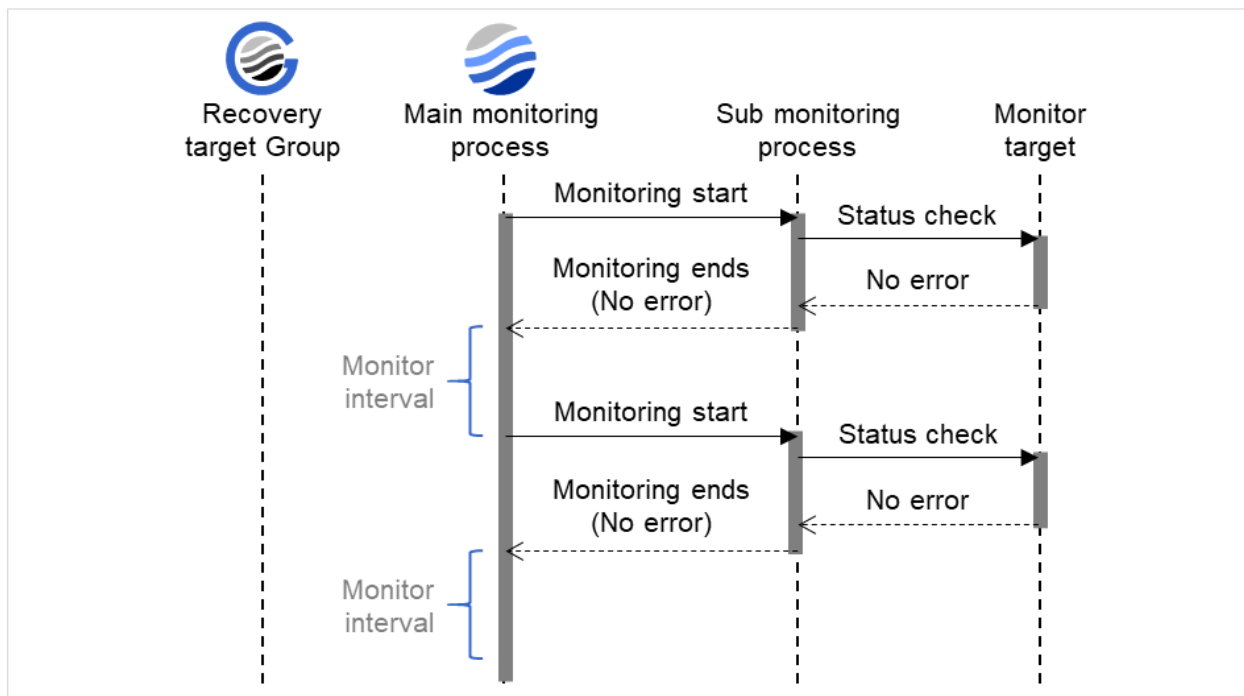


Fig. 7.2: Monitoring interval (no error detected)

When an error is detected (without monitor retry settings)

After an error occurs, it is detected next time monitoring is performed, and then the recovery target is reactivated.

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

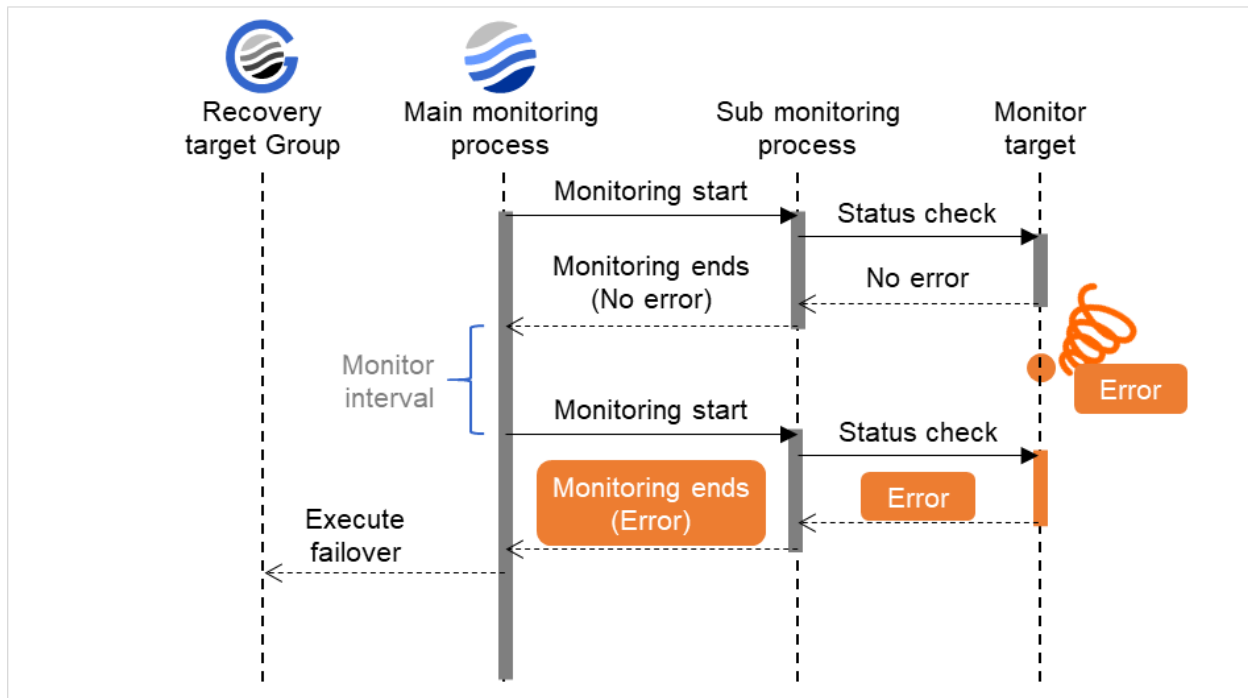


Fig. 7.3: Monitoring interval (an error detected, without monitor retry settings)

When an error is detected (with monitor retry settings)

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.

Examples of behavior when the following values are set.

<Monitor>

Monitor Interval 30 sec

Monitor Timeout 60 sec

Monitor Retry Count 2 times

<Error Detection>

Recovery Action Restart the recovery target

Recovery Target Group
 Recovery Script Execution Count 0 time
 Reactivation Threshold 0 time
 Final Action No Operation

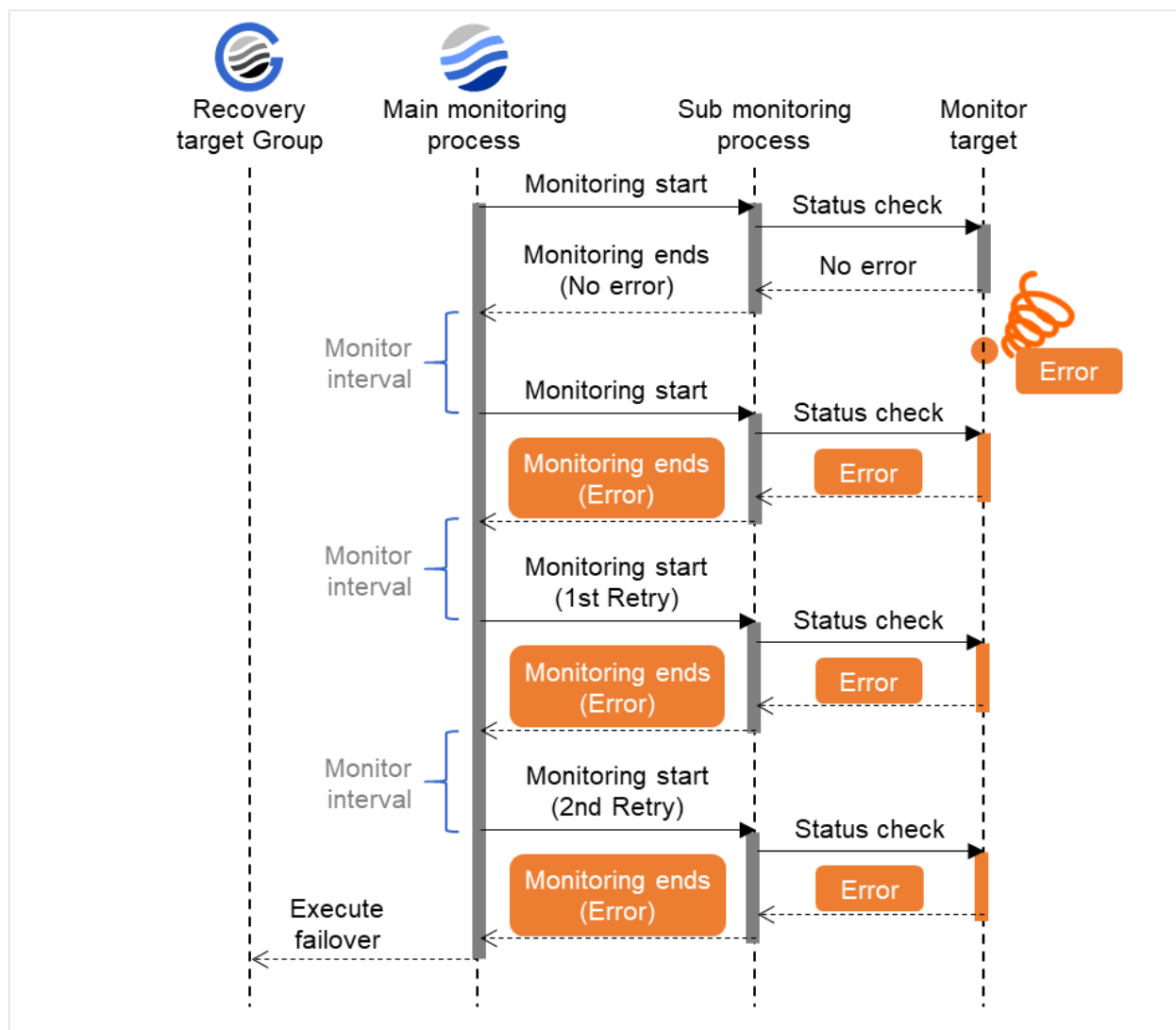


Fig. 7.4: Monitoring interval (an error detected, with monitor retry settings)

When an error is detected (without monitor retry settings)

After a monitor timeout occurs, the recovery target is immediately reactivated for the recovery action.
 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

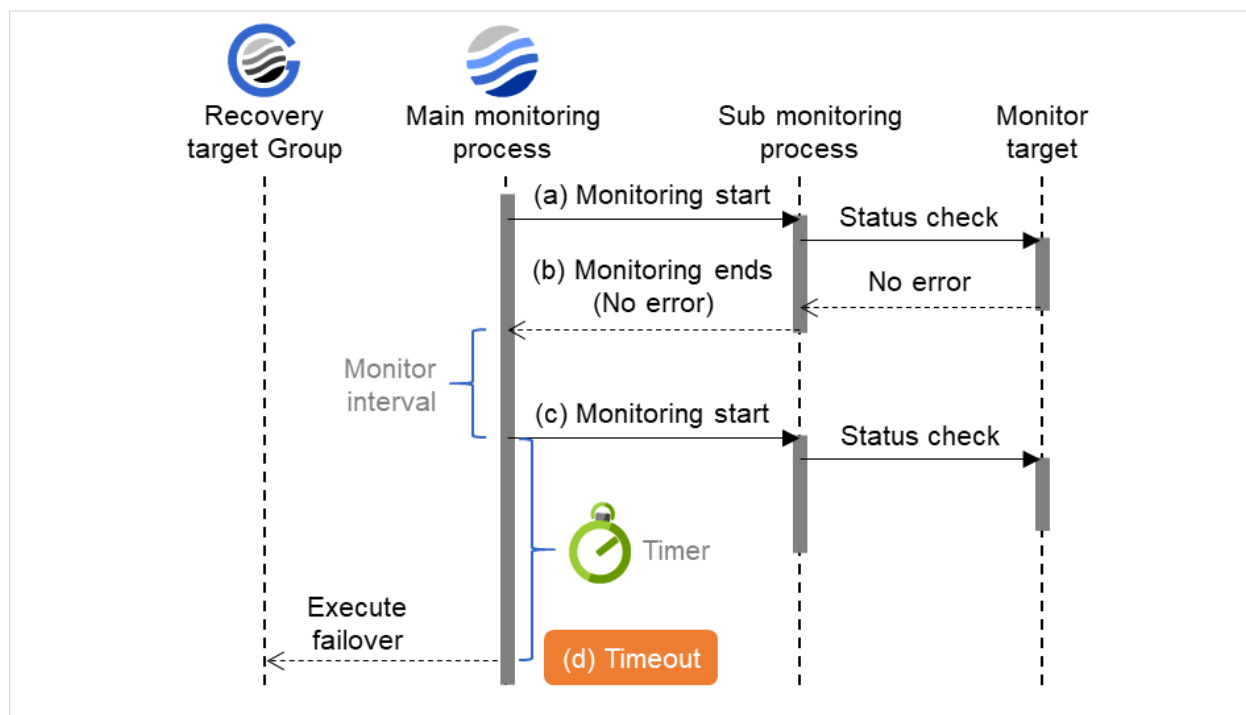


Fig. 7.5: Monitoring interval (a monitoring timeout detected, without monitor retry settings)

When a monitoring timeout is detected (with monitor retry setting)

After a monitor timeout occurs, another monitor attempt is made and, if it fails, the recovery target is reactivated.

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

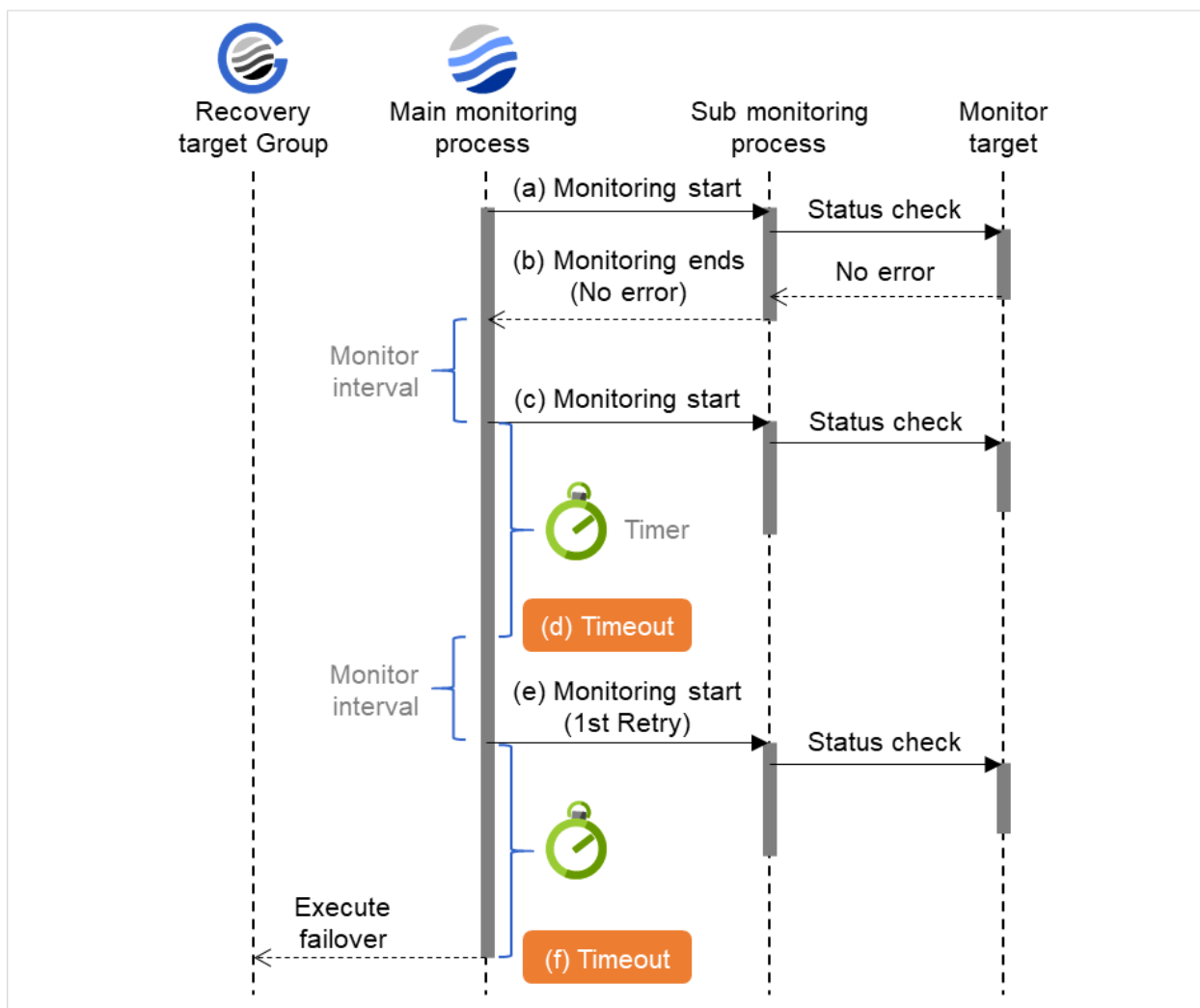


Fig. 7.6: Monitoring interval (a monitoring timeout detected, with monitor retry settings)

7.4 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 ²	Final Action ³
Group/Group Resource	Already stopped	No	No
	Being activated/stopped	No	No
	Already activated	Yes	Yes
	Error	Yes	Yes
Local Server	-	-	Yes

Yes: Recovery action is taken No: Recovery action is not taken

Note: Do not perform the following operations by using the Cluster WebUI 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.

² Effective only when the value for the reactivation threshold is set to 1 (one) or greater.

³ Effective only when an option other than No Operation is selected.

7.5 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).

7.6 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.

7.7 Recovery/pre-recovery action script

Upon the detection of a monitor resource error, a recovery script can be configured to run. Alternatively, before the reactivation or final action of a recovery target, a pre-recovery action script can be configured to run.

The script is a common file.

Environment variables used in the recovery/pre-recovery action script

EXPRESSCLUSTER sets status information (the recovery action type) in the environment variables upon the execution of the script.

The script allows you to specify the following environment variables as branch conditions according to the operation of the system.

Environment variable	Value of the environment variable	Description
CLP_MONITORNAME ...Monitor resource name	Monitor resource name	Name of the monitor resource in which an error that causes the recovery/pre-recovery action script to run is detected.
CLP_VERSION_FULL ...EXPRESSCLUSTER full version	EXPRESSCLUSTER full version	Represents the EXPRESSCLUSTER full version. Example: 12.30
CLP_VERSION_MAJOR ...EXPRESSCLUSTER major version	EXPRESSCLUSTER major version	Represents the EXPRESSCLUSTER major version. Example: 12
CLP_PATH ...EXPRESSCLUSTER installation path	EXPRESSCLUSTER installation path	Represents the path where EXPRESSCLUSTER is installed. Example: C:\Program Files\EXPRESSCLUSTER SSS
CLP_OSNAME ...Server OS name	Server OS name	Represents the OS name of the server where the script was executed. Example: Windows Server 2012 Standard

Continued on next page

Table 7.2 – continued from previous page

Environment variable	Value of the environment variable	Description
CLP_OSVER ...Server OS version	Server OS version	Represents the OS version of the server where the script was executed. Example: 6.2.0.0.274.3
CLP_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.

Note: On Windows Server 2016 or later, CLP_OSVER is set the same information as on Windows Server 2012 R2.

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%
```

(continues on next page)

(continued from previous page)

```
rem Write the recovery process here.
rem This process is executed at the following timing:
rem
rem Recovery action: Recovery script

GOTO EXIT

:RESTART
echo RESTART COUNT: %CLP_RESTARTCOUNT%

rem Write the pre-reactivation process here.
rem This process is executed at the following timing:
rem
rem Recovery action: Reactivation

GOTO EXIT

:FINALACTION
echo FINALACTION

rem Write the recovery process here.
rem This process is executed at the following timing:
rem
rem Recovery action: Final action

GOTO EXIT

:NO_CLP

:EXIT
echo EXIT
exit
```

Tips for recovery/pre-recovery action script coding

Pay careful attention to the following points when coding the script.

- When the script contains a command that requires a long time to run, log the end of execution of that command. The logged information can be used to identify the nature of the error if a problem occurs. clplogcmd is used to log the information.

Note on the recovery/pre-recovery action script

- None.

7.8 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.

In this example, the monitoring timeout is set to 60 seconds, the delay warning rate is set to the default value, 80% (48 seconds), and the arrows show the polling time for the monitoring.

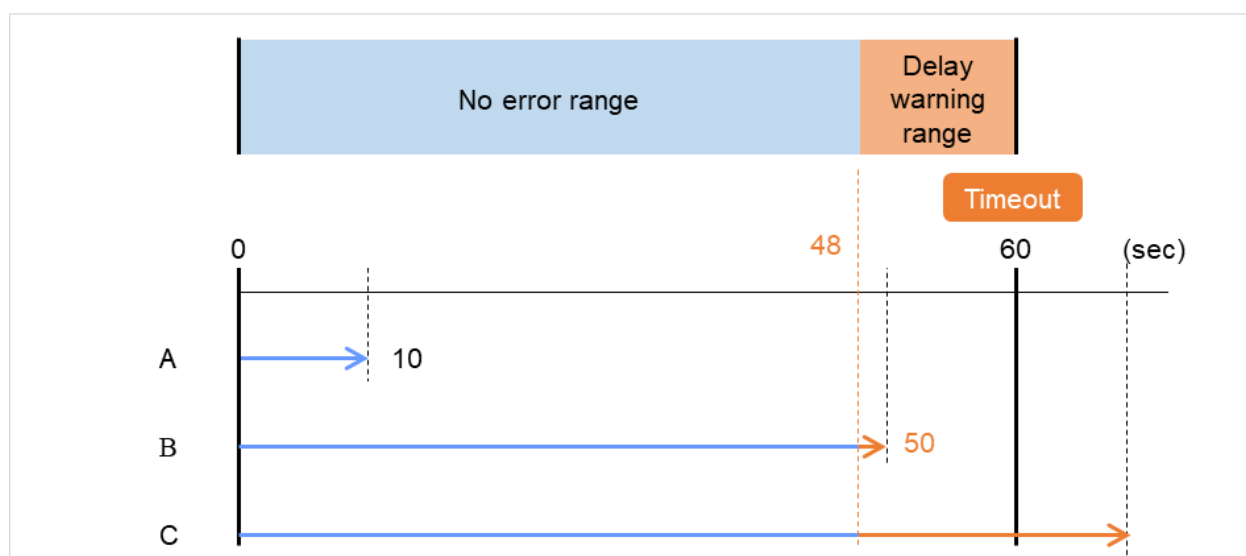


Fig. 7.7: Monitoring polling time and delay warning

- A. The time for monitor processing is 10 seconds. The monitor resource is in normal status.
In this case, no alert is used.
- B. The time for monitor processing is 50 seconds and the delay of monitoring is detected during this time. The monitor resource is in the normal status.
In this case, an alert is used because the delay warning rate has exceeded 80%.
- C. The time for monitor processing has exceeded 60 seconds of the monitoring timeout and the delay of monitoring is detected. The monitor resource has a problem.
In this case, no alert is used.

See also:

To configure the delay warning of monitor resources, click **Cluster Properties** and select **Monitor Delay Warning** in the **Delay Warning** tab.

7.9 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

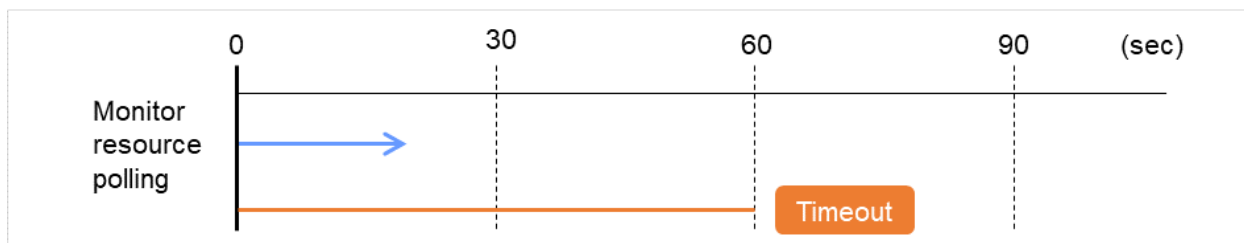


Fig. 7.8: Waiting for a monitor resource to start monitoring (the wait time to start monitoring set to 0 second)

Configuration of monitor resource

<Monitor>
Interval 30 sec
Timeout 60 sec
Retry Count 0 times
Wait Time to Start Monitoring 30 sec

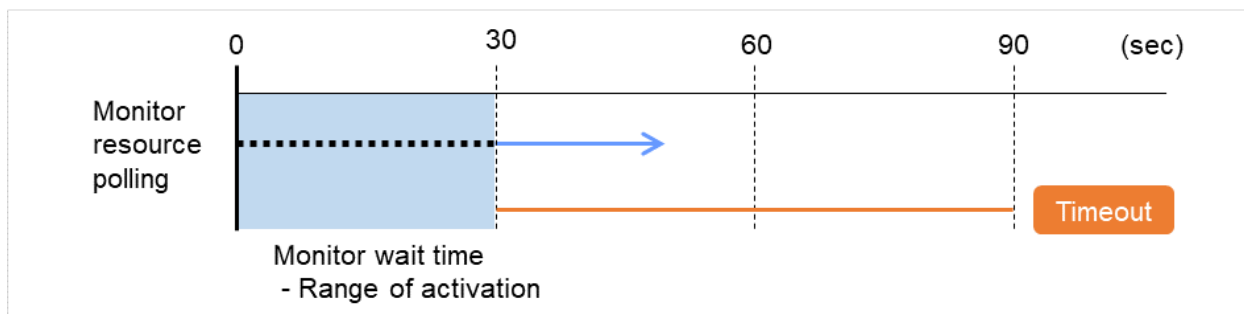


Fig. 7.9: Waiting for a monitor resource to start monitoring (the wait time to start monitoring set to 30 second)

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

<Monitor>

Interval 5 sec

Timeout 60 sec

Retry Count 0 times

Wait Time to Start Monitoring 0 sec (default)

<Error Detection>

Recovery Action Restart the following target

Recovery Target appli1

Final Action Stop Group

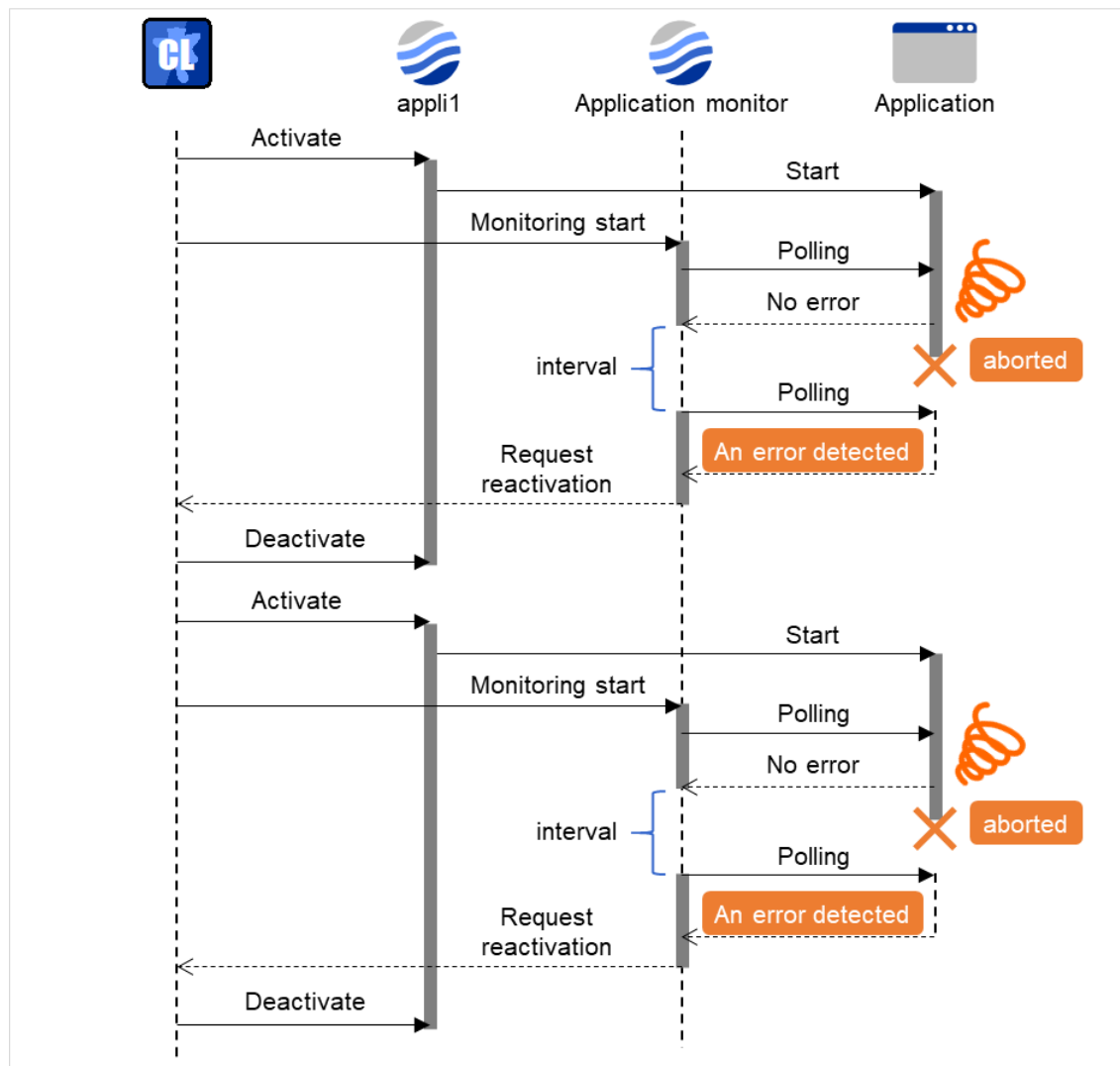


Fig. 7.10: Waiting for a monitor resource to start monitoring (the wait time to start monitoring set to 0 second)

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

```

<Monitor>
Interval 5 sec
Timeout 60 sec
Retry Count 0 times
    
```

Wait Time to Start Monitoring: 60 sec

<Error Detection>

Recovery Action Restart the following target

Recovery Target appli1

Final Action Stop Group

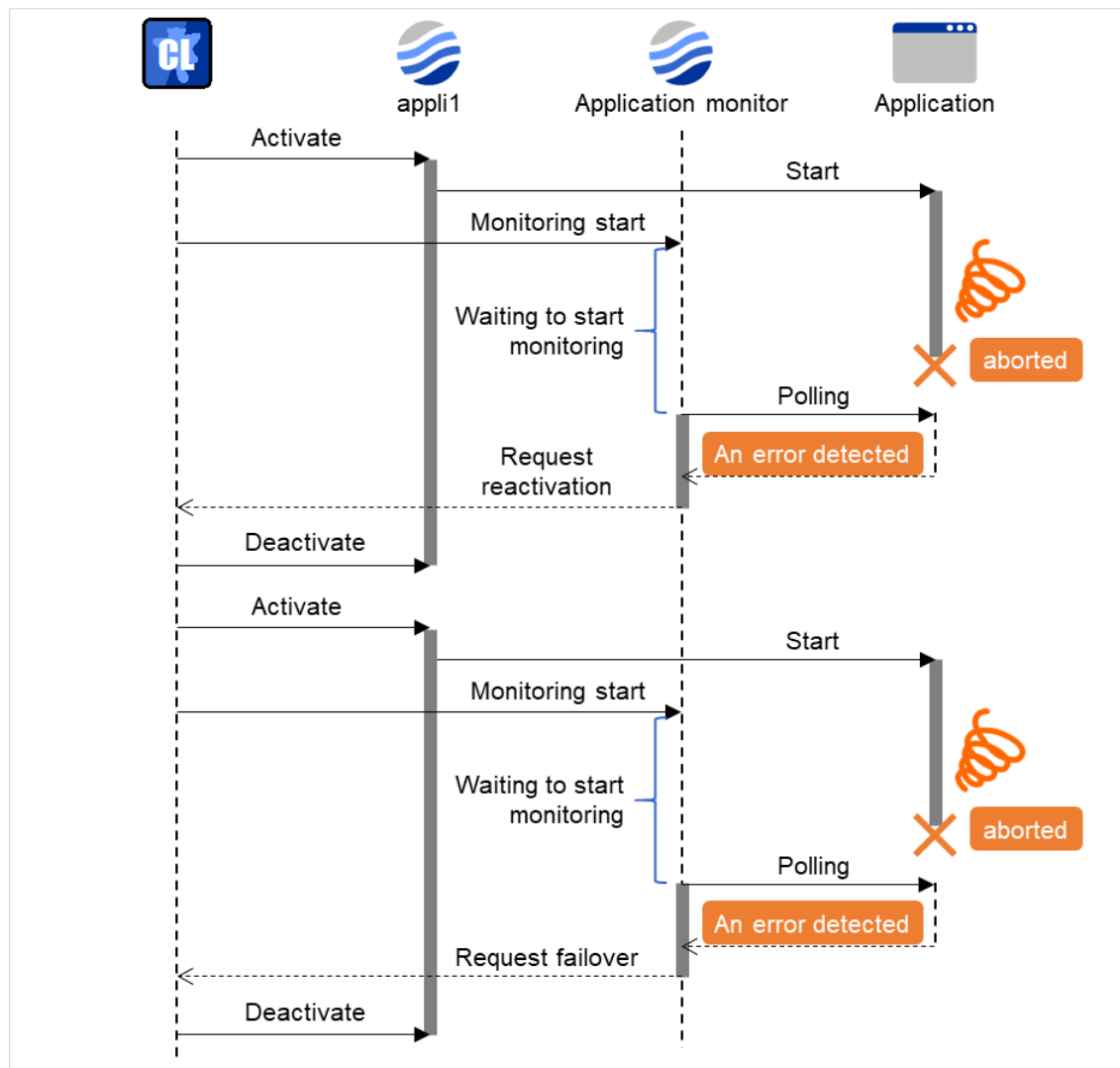


Fig. 7.11: Waiting for a monitor resource to start monitoring (the wait time to start monitoring set to 60 second)

7.10 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 "EXPRESS-CLUSTER X SingleServerSafe command reference" in the "EXPRESSCLUSTER X SingleServerSafe 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.

NOTES AND RESTRICTIONS

This chapter provides information on known problems and how to troubleshoot the problems.

This chapter covers:

- 8.1. *Designing a system configuration*
- 8.2. *Notes when creating the cluster configuration data*
- 8.3. *Notes when changing the EXPRESSCLUSTER configuration*

8.1 Designing a system configuration

This section describes the items to note when selecting hardware and designing a system configuration.

8.1.1 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.

8.1.2 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 Cluster WebUI (with **Identifier** in the **Monitor (special)** tab)
- Connections between Java VMs and JVM monitor resources 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
- The JVM monitor resources can monitor only the Java VMs on the server on which the JVM monitor resources are running.
- Application monitoring is disabled when an application to be monitored on the IA32 version is running on an x86_64 version OS.
- If a large value such as 3,000 or more is specified as the maximum Java heap size by the Cluster WebUI (by using **Maximum Java Heap Size** on the **JVM monitor** tab in **Cluster Property**), The JVM monitor resources 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.
- If "-XX:+UseG1GC" is added as a startup option of the target Java VM, the settings on the **Memory** tab on the **Monitor(special)** tab in **Property** of JVM monitor resources cannot be monitored before Java 7.
It's possible to monitor by choosing **Oracle Java (usage monitoring)** in **JVM Type** on the **Monitor(special)** tab after Java 8.

8.2 Notes when creating the cluster configuration data

This section describes the items to note before designing and creating configuration data based on the system configuration.

8.2.1 Folders and files in the location pointed to by the EXPRESSCLUSTER X SingleServerSafe installation path

The folders and files in the location pointed to by the EXPRESSCLUSTER X SingleServerSafe installation path must not be handled (edited, created, added, or deleted) by using any application or tool other than EXPRESSCLUSTER X SingleServerSafe.

Any effect on the operation of a folder or file caused by using an application or tool other than EXPRESSCLUSTER X SingleServerSafe will be outside the scope of NEC technical support.

8.2.2 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.

8.2.3 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.

8.2.4 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.

8.2.5 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 " Operation environment for JVM monitor" in " Checking system requirements for EXPRESSCLUSTER X SingleServerSafe" in " About EXPRESSCLUSTER X SingleServerSafe" in the " Installation Guide", 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.
 - To monitor resource name must not include a blank.
 - **Command** that is used to run a command according to a failure cause when a failure is detected and the load balancer function cannot be used together.

8.2.6 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).

8.2.7 Recovery operation when a service fails in a Windows Server 2012-based system

In a Windows Server 2012-based system, the operation actually performed when a service fails if **Restart Computer** is set as the recovery operation to perform when a service fails (terminates abnormally) has been changed from the conventional one, OS restart (Windows Server 2008 or earlier), to OS restart with a STOP error.

For details of this change, refer to the following information:

Reference: <http://support.microsoft.com/kb/2848819>

The EXPRESSCLUSTER services for which **Restart Computer** is set as the recovery operation by default are the following:

- EXPRESSCLUSTER Disk Agent service
- EXPRESSCLUSTER Server service
- EXPRESSCLUSTER Transaction service

8.3 Notes when changing the EXPRESSCLUSTER configuration

The section describes what happens when the configuration is changed after starting to use EXPRESSCLUSTER in the cluster configuration.

8.3.1 Dependency between resource properties

When the dependency between resources has been changed, the change is applied by suspending and resuming the cluster.

If a change in the dependency between resources that requires the resources to be stopped during application is made, the startup status of the resources after the resume may not reflect the changed dependency.

Dependency control will be performed at the next group startup.

8.3.2 Adding and deleting group resources

When you move a group resource to another group, follow the procedure shown below.

If this procedure is not followed, the cluster may not work normally.

Example) Moving script1 (floating ip resource) from failover1 group to failover2 group

1. Delete script1 from failover1.
2. Reflect the setting to the system.
3. Add script1 to failover2.
4. Reflect the setting to the system.

8.3.3 Setting cluster statistics information of message receive monitor resources

Once the settings of cluster statistics information of monitor resource has been changed, the settings of cluster statistics information are not applied to message receive monitor resources even if you execute the suspend and resume. Reboot the OS to apply the settings to the message receive monitor resources.

LEGAL NOTICE

9.1 Disclaimer

- Information in this document is subject to change without notice.
- NEC Corporation is not liable for technical or editorial errors or omissions in the information in this document. You are completely liable for all risks associated with installing or using the product as described in this manual to obtain expected results and the effects of such usage.
- The information in this document is copyrighted by NEC Corporation. No part of this document may be reproduced or transmitted in any form by any means, electronic or mechanical, for any purpose, without the express written permission of NEC Corporation.

9.2 Trademark Information

- EXPRESSCLUSTER® is a registered trademark of NEC Corporation.
- Microsoft, Windows, Windows Server, Internet Explorer, Azure, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- Apache Tomcat, Tomcat, and Apache are registered trademarks or trademarks of Apache Software Foundation.
- Citrix, Citrix XenServer, and Citrix Essentials are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other countries.
- SVF is a registered trademark of WingArc Technologies, Inc.
- Oracle, Oracle Database, Solaris, MySQL, Tuxedo, WebLogic Server, Container, Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates.
- IBM, DB2, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.
- PostgreSQL is a registered trademark of the PostgreSQL Global Development Group.
- VMware, vCenter Server, and vSphere is registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- PowerGres is a registered trademark of SRA OSS, Inc.
- F5, F5 Networks, BIG-IP, and iControl are trademarks or registered trademarks of F5 Networks, Inc. in the United States and other countries.
- WebOTX is a registered trademark of NEC Corporation.
- WebSAM is a registered trademark of NEC Corporation.
- Other product names and slogans written in this manual are trademarks or registered trademarks of their respective companies.

REVISION HISTORY

Edition	Revised Date	Description
1st	Apr 09, 2021	New manual

© Copyright NEC Corporation 2021. All rights reserved.