Hinemos ver4.1

User's Manual, Edition 1.0

Copyright (c) 2013 NTT DATA CORPORATION

Contents

Copyright (c) 2013 NTT DATA CORPORATION

Copyright (c) 2013 NTT DATA CORPORATION

Copyright (c) 2013 NTT DATA CORPORATION

This software was developed in response to the delegation of the second half open-source-software activity infrastructure improvement enterprise in fiscal year 2004 by the INFORMATION-TECHNOLOGY PROMOTION AGENCY (IPA), an independent administrative agency.

- The theme name is "Development of an Integrated Manager for Distributed Facilities."
- http://www.ipa.go.jp/about/jigyoseika/04fy-pro/open.html

For the latest information about Hinemos, please visit the Hinemos web portal (http://www.hinemos.info).

Copyright (c) 2013 NTT DATA CORPORATION

1 Hinemos Overview

1.1 System Overview

Hinemos is an operations management tool intended to operate multiple computers with the image of a single computer. It provides users with a feature to register computers in groups depending on the operation purposes, and an environment that is easy to monitor or operate with a GUI corresponding to the operation purpose.

Use of Hinemos enables groups of business systems comprising multiple computers with differing purposes to achieve efficient operation in fewer steps.

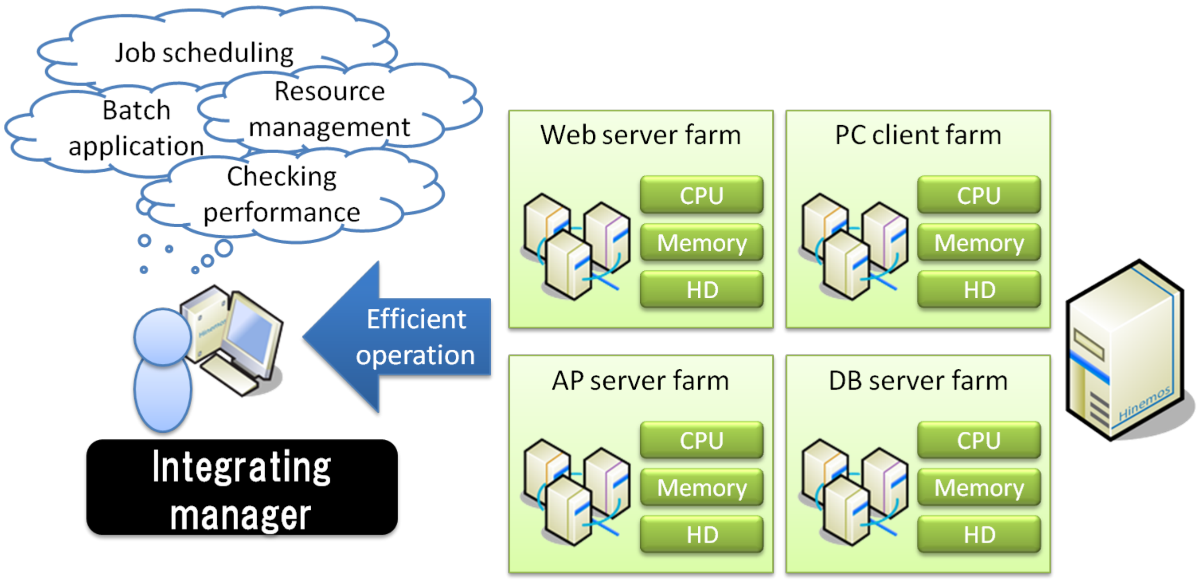


Figure 1-1 An Example of Hinemos Usage

1.2 Feature Overview

The features that comprise Hinemos are shown in Table 1-1.

Table 1-1 Available Features (by platform)

Feature		Linux	Windows	NW equipment
Integration Interaface		◎	◎	◎
Repository		◎	◎	◎
Calendar		◎	◎	◎
Monitor	Scope Monitor	◎	◎	◎
	Status Monitor	◎	◎	◎
	Event Monitor	◎	◎	◎
Monitor Setting	Notification	◎	◎	◎
	Mail Template	◎	◎	◎

Monitor Setting (particular)	Hinemos Agent Monitor	○	○	–
	HTTP Monitor (number/character string)	◎ *7	◎ *7	–
	Resource Monitor (SNMP)	◎ *2	◎ *2*4	◎ *6
	Resource Monitor (WBEM)	◎ *3	–	◎ *6
	PING monitor	◎	◎	◎
	Service Port Monitor	◎ *7	◎ *7	◎ *7
	Process Monitor (SNMP)	◎ *2	◎ *2	–
	Process Monitor (WBEM)	◎ *3	–	–
	SNMP Monitor (number/character string)	◎ *2	◎ *2	◎
	SQL Monitor (number/character string)	◎ *7	◎ *7	◎
	System Log Monitor	◎ *1	○	◎
	Logfile Monitor	○	○	–
	Custom Monitor	○	○	○ *8
	SNMPTRAP Monitor	◎	◎	◎
	Windows Service Monitor	–	◎	–
	Windows Event Monitor	–	○	–
Characteristics	Download	◎	◎	◎
	Graph Search	◎	◎	◎
Job	Run Command	○	○ *9	–
	File Transfer	○	–	–
Collective Run		◎ *5	–	–
Maintenance	History Delete	◎	◎	◎
Account		◎	◎	◎

◎ Can be used agent-lessly

○ Hinemos Agent installation is required

- No feature

*1 Monitoring is enabled by configuring the monitoring rsyslog/syslogd even if not installing the Hinemos Agent.

*2 Monitoring is enabled by configuring the OS standard SNMP agent even if not installing the Hinemos Agent.

*3 The following items need to be implemented.

- WBEM switching settings

  Refer to section 7.8.2 "Method for switching SNMP and WBEM" in the the Administrator's Guide.
- Sets the WinRM user name, User password, Port number, Protocol, Version, Time out and Retry count in the Repository registration information.

  Refer to Creating/Changing/Deleting a Node.

*4 The monitor network I/O can be enabled even if not installing the Windows Agent.

*5 Additional setup is required after installation. Please refer to the Administrator's Guide, Section 6 - "Collective Run".

*6 HinemosUtility is required. (Some may be supported by the general features.)

*7 Platform independent.

*8 A network device may be enabled by running a command to monitor the network device indirectly from a server capable of running the command.

*9 Jobs can be run with the same user permission as Hinemos Agent.

1.2.1 Integration Interface

This feature integrates the operation interfaces used by the operator. Integration of the GUI supports various operation management tasks on screen. Operability can be improved by configuring the various management operation interfaces for each business system or user, and by configuring and saving the interface layout (perspective).

In addition, concurrent access by multiple operators is supported. In the job management feature, Edit Mode is used to ensure mutual exclusion while multiple operators are working at the same time.

1.2.2 Repository

This feature integrates the information required for managing the overall system. Node structure information and asset management information can be registered in the repository. Furthermore, that information can be freely grouped in a hierarchy perspective for management. In Hinemos, this group is referred to as a "Scope".

The operator can arrange scope nodes depending on the administrative purposes or stratify scopes in hierarchies for organization. The repository information configured here can be used from other features.

Example) For hierarchical scopes, multiple scopes can be registered in the hierarchy: ["Nippon building"⊃"4th floor"⊃"west floor"] for location, ["headquarter"⊃"sales"] for organization.

1.2.3 Calendar

This feature is used to set up the working/non-working periods and determine whether or not to run. It can be used from various features.

With this feature, the working days and holidays can be set in the calendar feature, and that setting information can be used from both the Monitor Setting and Job feature.

1.2.4 Notification

This feature notifies the monitoring results and the job execution results for each monitoring feature. Various methods of notification are available, including Status Notification or Event Notification displayed on the Monitor Settings Perspective interface and Mail Notification sent by e-mail.

With this feature, an e-mail is sent when an incident occurs, enabling a job to be run that will restart the related product.

1.2.5 Monitor & Performance

This feature enables failure detection and acquisition of performance information by scope. This enables the user to operate nodes through the GUI of the managed system according to the "Scope". Therefore, it is easy to check the operating status and setup.

More than 10 types of monitoring are available, such as resource usage status and service operation status.

1.2.6 Job

This feature automates regular operations and automates routine tasks and other operations when an incident occurs.

With this feature, personnel costs distributed across routine operations can be reduced.

1.2.7 Collective Run

Collective Run is a batch processing feature that allows multiple nodes to operate at once. Group units for batch processing are managed by the "Scope" classification, so the operation will not become complicated even if the number of nodes increases, preventing an increase in work due to system expansion.

When a massive number of identical tasks must be performed for multiple nodes, such as applying a security patch, this feature can be used to perform batch operations in "Scope" units, to simplify and speed up operations.

1.2.8 Maintenance

This feature is used in the administration of Hinemos itself, and is necessary for the operation of Hinemos. Deletion of history information, which will gradually accumulate in the internal database, can be performed.

1.2.9 Account

The user management feature provides a management interface for user and role definition, as well as access permission configuration.

This feature is used to organize operation permission by role. This enables you to perform operations with high-level security.

Copyright (c) 2013 NTT DATA CORPORATION

2 Integrated Interface Feature

2.1 Overview

The integrated interface feature provides the following functions.

- Displays an integration of various operation management interface
- Operation of each feature via an integrated interface
- Customize the interface layout (perspective)
- Save/restore a customized interface layout (perspective)

2.2 Starting the Hinemos Manager

Start up the Hinemos Manager according to the Installation Manual.

2.3 Starting the Hinemos Client

Start up the Hinemos Client according to the Installation Manual.

2.4 Logging In

Login to Hinemos using the specified user information described below.

1. Select "Connection" - "Login" from the menu bar. The Connection[Login] dialog will appear.
2. Enter user ID and password, then click the "Login" button.

Default password

Immediately after the installation, only the user account below will exist.

User: hinemos
Password: hinemos

2.5 Logout

Logout with the procedure below.

1. Select "Connection" - "Logout" from the menu bar.

Upon logout, the interface layout (Perspective) will be initialized.

2.6 Select the Interface Layout (Perspective)

The following 9 initial interface layouts will be available.

- Account
- Calendar
- Job
- Maintenance
- Repository
- Collective Run

Copyright (c) 2013 NTT DATA CORPORATION

- Performance
- Monitor
- Monitor Setting

Please follow the procedures below to select a interface layout.

1. **Select "Perspective" - "Open Perspective" from the menu bar.**
   The Perspective selection dialog will appear. In this software, perspective refers to a specific interface configuration.

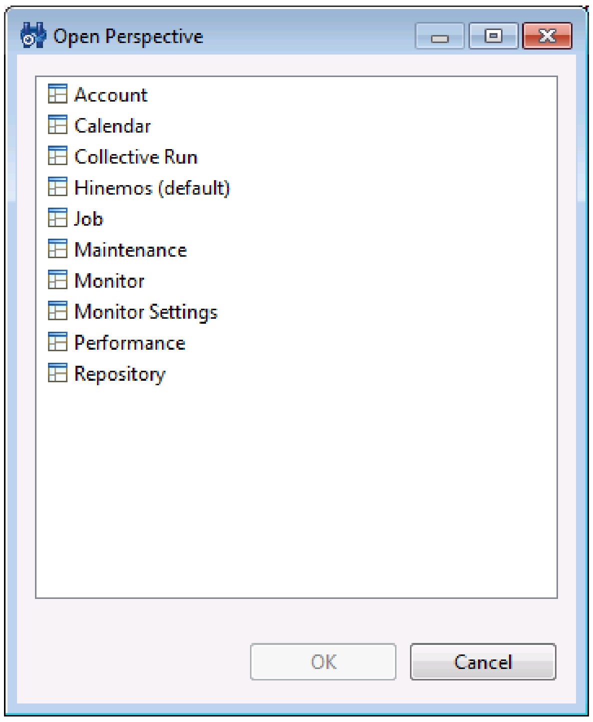


Figure 2-1 Perspective Selection Dialog

2. Select the interface layout (Perspective) to display.
3. Click the "OK" button.

Opening the view of a feature without opening its interface layout (Perspective)

For example, the node management feature view of the repository (Repository[Node] view) can be opened while the interface layout for the Job is open. Select the features or view to open in the "View" menu from the menu bar. Then open the view for the selected feature.

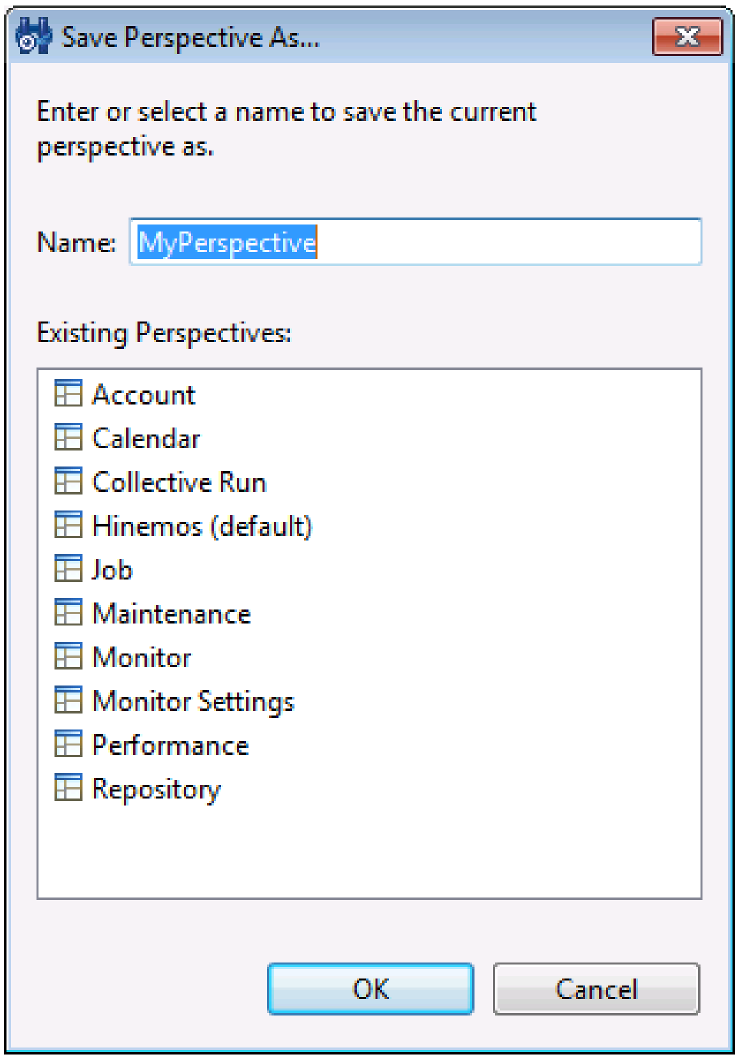
2.7 Saving the Interface Layout (Perspective)

Customized interface layouts can be saved with a different name. A interface layout saved with a different name is added as one of the choices in the Perspective selection dialog box.

To save a customized interface layout with a different name, follow the procedure below.

1. Right click on a perspective tab and then click "Save As..." from the list shown. The "Save Perspective As..." dialog will appear.
2. Input a name in the "Name" input box.
3. Click the "OK" button.

Copyright (c) 2013 NTT DATA CORPORATION



Enter or select a name to save the current perspective as.

Name: MyPerspective

Figure 2-2 Save Perspective As... Dialog

Restoring an interface layout (Perspective) to default

Right-click on a perspective tab, then click "Reset" in the displayed menu to the restore the default interface layout.

Deleting a saved perspective

In Hinemos4.1, individual delete of a saved perspective is not available. You can manually remove the following file to restore the whole perspective list to default. Note that you have to stop Hinemos Client at first. In addition, just in case you might want it back again, it is always better to keep a backup before deleting the file.

> **Location:** C:\Users\<USER>\AppData\Roaming\hinemos\Client4.1\workspace\.metadata\.plugins\org.eclipse.e4.workbench **File name:** workbench.xmi

Copyright (c) 2013 NTT DATA CORPORATION

3 Repository Feature

3.1 Overview

The repository feature provides features for registering, modifying, and deleting information managed by Hinemos.

3.1.1 Repository

The Repository is a database that accumulates information on management objects that are managed with Hinemos, in a format that enables management by Scope. Information registered in the repository is used for other features.

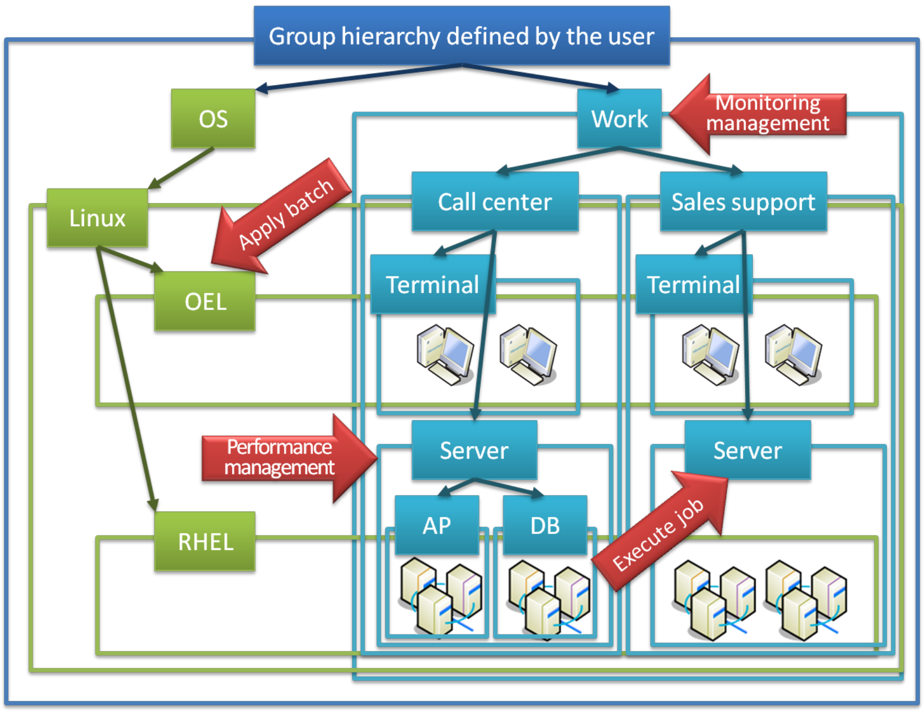


Figure 3-1 Repository Image

3.1.2 Scope and Node

In Hinemos, management objects are handled through the two units, "Scope" and "Node".

- Node

  Virtualization of actual machine for management. The following information can be registered as node informa tion.

  - Hardware, Network, OS information
  - Service (SNMP, WBEM, IPMI, WinRM)
  - Device information (CPU, Memory, NIC, Disk, File system, General Device)
  - Server Virtualization, Network Virtualization, Cloud Management
  - Other Features

- Scope

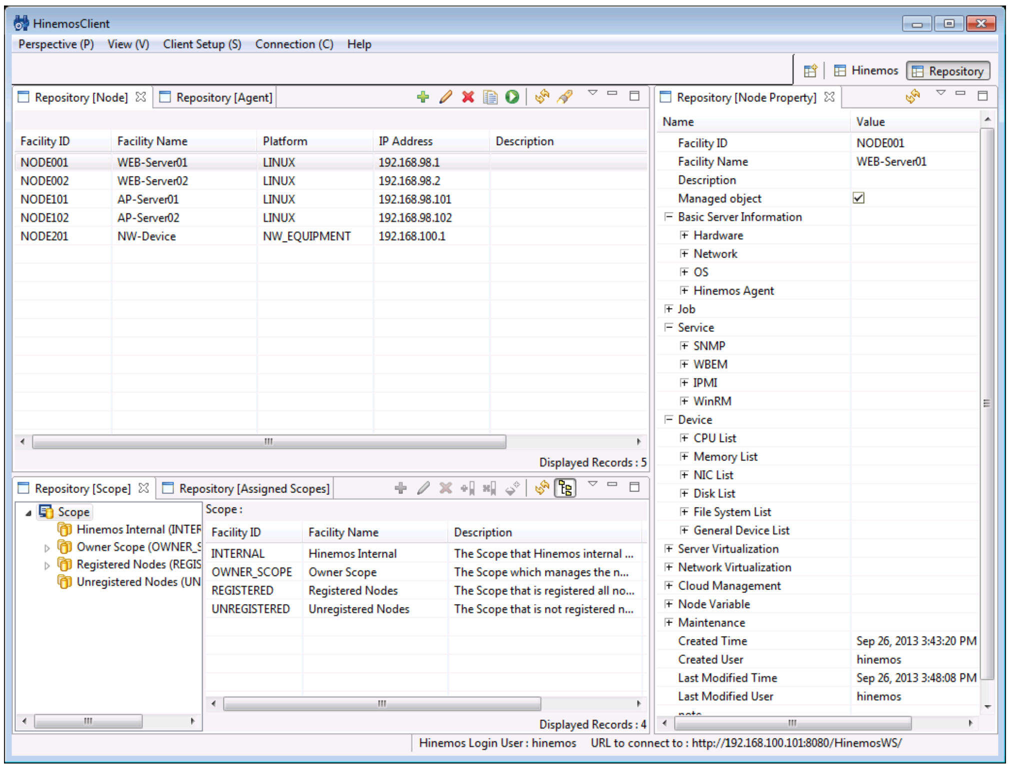
  Grouping of multiple nodes. Many processing units provided by the Hinemos feature are in the scope unit. Proce ss applied to the scope is reflected to each node that is registered.

  Multiple sub-scopes can be registered in a scope. In this case, the scope is in a hierarchical structure, and form s a tree.

Copyright (c) 2013 NTT DATA CORPORATION

3.2 Interface Composition

3.2.1 Default Interface



Facility ID	Facility Name	Platform	IP Address	Description
NODE001	WEB-Server01	LINUX	192.168.98.1	
NODE002	WEB-Server02	LINUX	192.168.98.2	
NODE101	AP-Server01	LINUX	192.168.98.101	
NODE102	AP-Server02	LINUX	192.168.98.102	
NODE201	NW-Device	NW_EQUIPMENT	192.168.100.1	

Displayed Records : 5

Scope :

Facility ID	Facility Name	Description
INTERNAL	Hinemos Internal	The Scope that Hinemos internal ...
OWNER_SCOPE	Owner Scope	The Scope which manages the n...
REGISTERED	Registered Nodes	The Scope that is registered all no...
UNREGISTERED	Unregistered Nodes	The Scope that is not registered n...

Displayed Records : 4

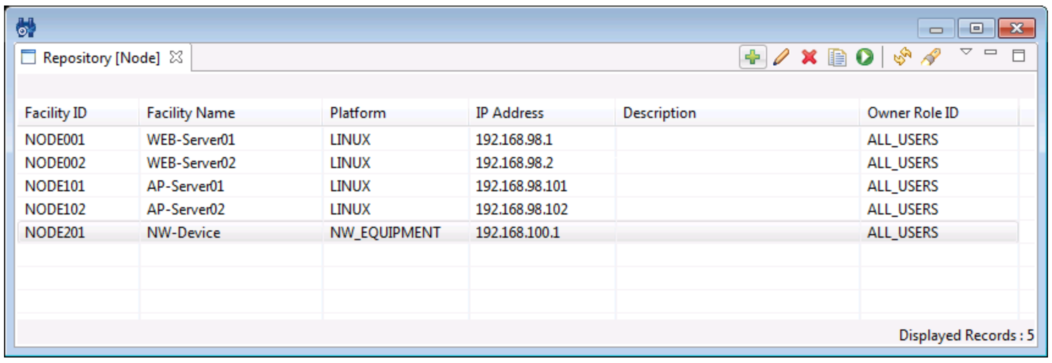
Name	Value
Facility ID	NODE001
Facility Name	WEB-Server01
Description	
Managed object	☑
Basic Server Information	
Hardware	
Network	
OS	
Hinemos Agent	
Job	
Service	
SNMP	
WBEM	
IPMI	
WinRM	
Device	
CPU List	
Memory List	
NIC List	
Disk List	
File System List	
General Device List	
Server Virtualization	
Network Virtualization	
Cloud Management	
Node Variable	
Maintenance	
Created Time	Sep 26, 2013 3:43:20 PM
Created User	hinemos
Last Modified Time	Sep 26, 2013 3:48:08 PM
Last Modified User	hinemos

Hinemos Login User : hinemos URL to connect to : http://192.168.100.101:8080/HinemosWS/

Figure 3-2 Default Interface of Repository Feature

3.2.2 Repository[Node] View

The Repository[Node] view displays a list of registered nodes. Operations related to node information, such as regis tration or deleting of a node, can be performed in this view.



Facility ID	Facility Name	Platform	IP Address	Description	Owner Role ID
NODE001	WEB-Server01	LINUX	192.168.98.1		ALL_USERS
NODE002	WEB-Server02	LINUX	192.168.98.2		ALL_USERS
NODE101	AP-Server01	LINUX	192.168.98.101		ALL_USERS
NODE102	AP-Server02	LINUX	192.168.98.102		ALL_USERS
NODE201	NW-Device	NW_EQUIPMENT	192.168.100.1		ALL_USERS

Displayed Records : 5

Figure 3-3 Repository[Node] View

Table 3-1 Toolbar

Icon	Button name	Description
✚	Create	Create node information.
✎	Modify	Modify node information.
✖	Delete	Delete node information.
📄	Copy	Copy node information.
🖌	Filter	Configure filter of node information list.
▶	Run	Run a program on client.

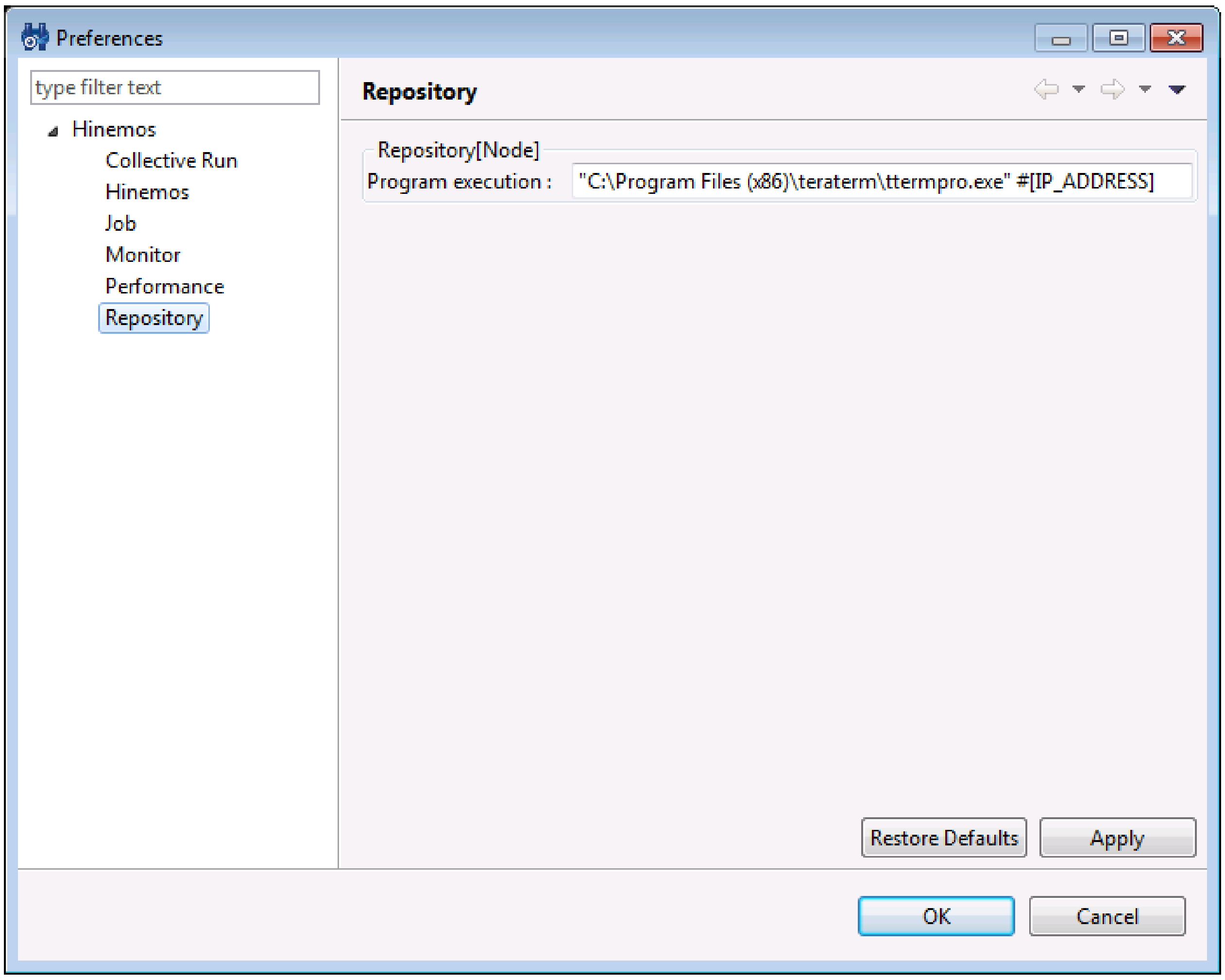
Copyright (c) 2013 NTT DATA CORPORATION

↻	Update	Update contents of Repository[Node] view.

Specifying a program for the "Program Execution" button

Follow the following steps to specify a program.

1. Click "Client Setup" on the menu bar and then select "Select". A setting dialog will show up.
2. Expand "Hinemos" and select "Repository" from the tree pane positioned on the left hand side.



Program execution : "C:\Program Files (x86)\teraterm\ttermpro.exe" #[IP_ADDRESS]

Figure 3-4 Client Setup dialog

3. The following setting can be configured for Repository[Node] view.

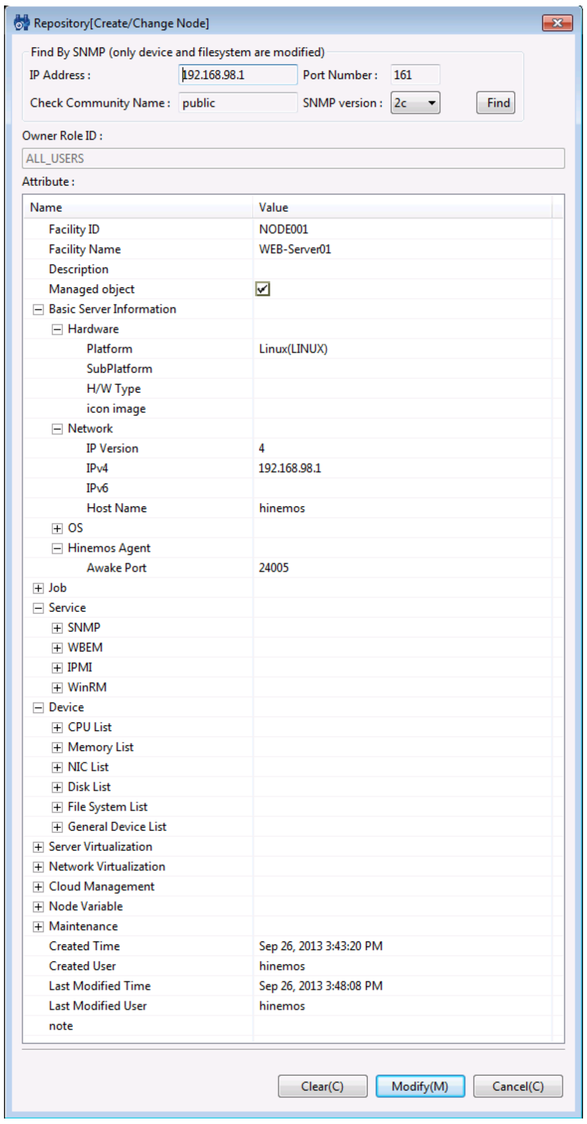
- Program execution:

  Specify path to the program to execute. Node variables can be used in the path string. Node variables will be automatically replaced to the information of Repository[Node] view when the "Program Execution" button is clicked. (Refer to Table 7-24, Node Variable List, regarding node variables)

  e.g. "C:\Program Files (x86)\teraterm\ttermpro.exe" #[IP_ADDRESS]

3.2.3 Repository[Node Property] View

Repository[Node Property] view is the view that displays the registered content of nodes. It displays the node information selected in Repository[Node] view.



Repository[Create/Change Node]

Find By SNMP (only device and filesystem are modified)

IP Address : 192.168.98.1 Port Number : 161

Check Community Name : public SNMP version : 2c Find

Owner Role ID :

ALL_USERS

Attribute :

Name	Value
Facility ID	NODE001
Facility Name	WEB-Server01
Description	
Managed object	☑
⊟ Basic Server Information	
⊟ Hardware	
Platform	Linux(LINUX)
SubPlatform	
H/W Type	
icon image	
⊟ Network	
IP Version	4
IPv4	192.168.98.1
IPv6	
Host Name	hinemos
⊞ OS	
⊟ Hinemos Agent	
Awake Port	24005
⊞ Job	
⊟ Service	
⊞ SNMP	
⊞ WBEM	
⊞ IPMI	
⊞ WinRM	
⊟ Device	
⊞ CPU List	
⊞ Memory List	
⊞ NIC List	
⊞ Disk List	
⊞ File System List	
⊞ General Device List	
⊞ Server Virtualization	
⊞ Network Virtualization	
⊞ Cloud Management	
⊞ Node Variable	
⊞ Maintenance	
Created Time	Sep 26, 2013 3:43:20 PM
Created User	hinemos
Last Modified Time	Sep 26, 2013 3:48:08 PM
Last Modified User	hinemos
note	

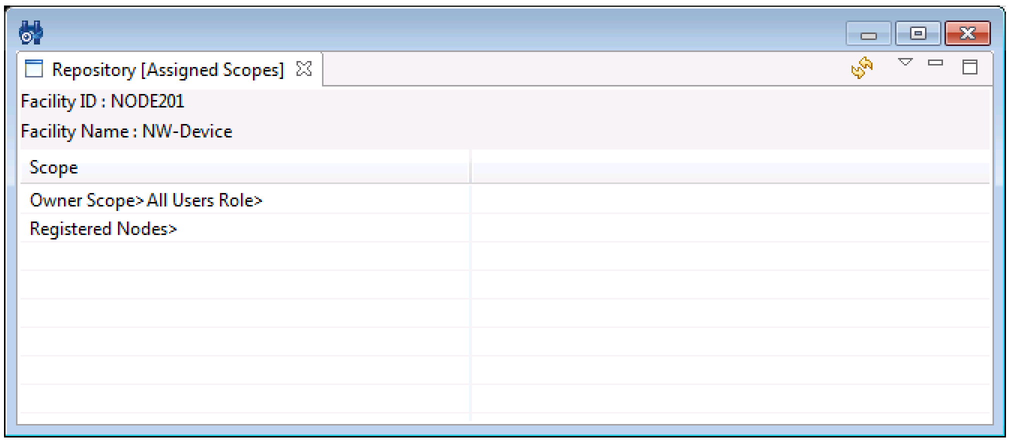
Figure 3-5 Repository[Node Property] View

Table 3-2 Toolbar

Icon	Button name	Description
⟳	Update	Update contents of Repository[Node Property] view

3.2.4 Repository[Assigned Scopes] View

Repository[Assigned Scopes] view displays the list of node assignments to scopes. It displays the assigned status of nodes selected in Repository[Node] view.



Facility ID : NODE201

Facility Name : NW-Device

Scope
Owner Scope>All Users Role>
Registered Nodes>

Figure 3-6 Repository[Assigned Scopes] View

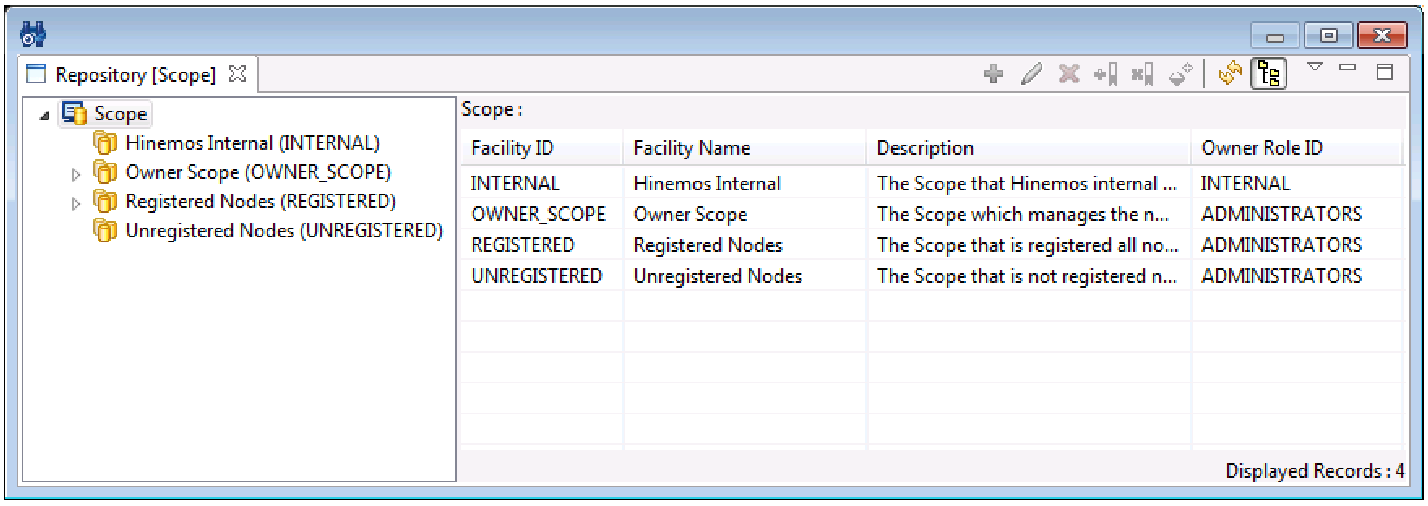
Copyright (c) 2013 NTT DATA CORPORATION

Table 3-3 Toolbar

Icon	Button name	Description
⟳	Update	Update contents of Repository[Assigned Scopes].

3.2.5 Repository[Scope] View

Repository[Scope] view displays information of registered nodes. In this view, operations such as registering or deleting of scopes, and node assignment to scopes, can be performed.



Repository [Scope]

- Scope
  - Hinemos Internal (INTERNAL)
  - Owner Scope (OWNER_SCOPE)
  - Registered Nodes (REGISTERED)
  - Unregistered Nodes (UNREGISTERED)

Scope :

Facility ID	Facility Name	Description	Owner Role ID
INTERNAL	Hinemos Internal	The Scope that Hinemos internal ...	INTERNAL
OWNER_SCOPE	Owner Scope	The Scope which manages the n...	ADMINISTRATORS
REGISTERED	Registered Nodes	The Scope that is registered all no...	ADMINISTRATORS
UNREGISTERED	Unregistered Nodes	The Scope that is not registered n...	ADMINISTRATORS

Displayed Records : 4

Figure 3-7 Repository[Scope] View

Table 3-4 Toolbar

Icon	Button name	Description
✚	Create	Create scope.
✎	Modify	Modify attribution information of scope.
✖	Delete	Delete scope.
✚▮	Assign	Assign node to scope.
✖▮	Release	Release node assignment assigned to scope.
◆	Object Privilege Settings	Assign object privilege to scope.
⟳	Update	Update contents of Repository[Scope] view.
⊞	Show Scope Tree Pane	Toggle the display of the scope tree.

In addition, four scopes, Owner Scope (OWNER_SCOPE), Hinemos Internal (INTERNAL), Registered Nodes (REGISTERED) and Unregistered Nodes (UNREGISTERED), are built into Hinemos; delete/modify/assign cannot be performed. The features for each scope are as follows.

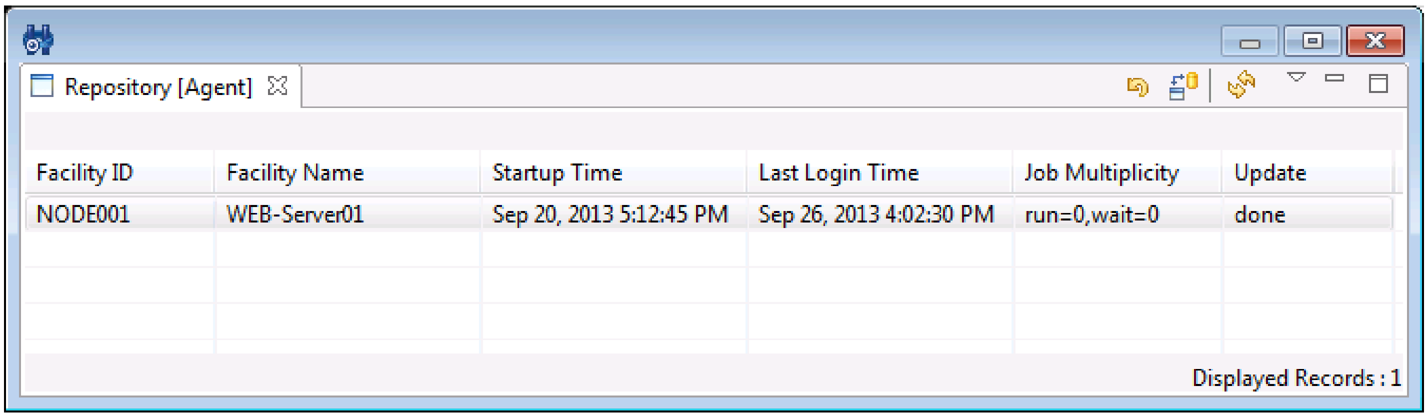
Table 3-5 List of Built-in Scope

Scope	Description
Owner Scope (OWNER_SCOPE)	Scope for confirming information between nodes and their owner role .
Hinemos Internal (INTERNAL)	Scope for storing events occurring in internal Hinemos (internal error and others).
Registered Nodes (REGISTERED)	Scope for confirming information of all registered nodes.
Unregistered Node (UNREGISTERED)	Scope used when receiving system logs and SNMPTRAP from a node not registered in Hinemos.

Copyright (c) 2013 NTT DATA CORPORATION

3.2.6 Repository[Agent] View

This view displays the information on the Hinemos Agent connected to the Hinemos Manager. In this view, you can confirm the agent list, restart the agent, or update the agent.



Facility ID	Facility Name	Startup Time	Last Login Time	Job Multiplicity	Update
NODE001	WEB-Server01	Sep 20, 2013 5:12:45 PM	Sep 26, 2013 4:02:30 PM	run=0,wait=0	done

Displayed Records : 1

Figure 3-8 Repository[Agent] View

Table 3-6 Toolbar

Icon	Button name	Description
↺	Agent restart	Restarts the Hinemos Agent.
⇅	Module update	Updates the Hinemos modules
⟳	Update	Update contents of the Repository[Agent] view.

3.3 Procedure to Create a Scope Tree

Scope tree is created by the following procedures.

1. Register node information
2. Create scope (scope tree)
3. Assign node to scope

Scope can have multiple sub-scopes, and form trees with a hierarchy structure.

Through registration of multiple nodes in scope, nodes can group and operate together. In addition, a single node can be assigned to multiple scopes.

3.4 Creating/Changing/Deleting a Node

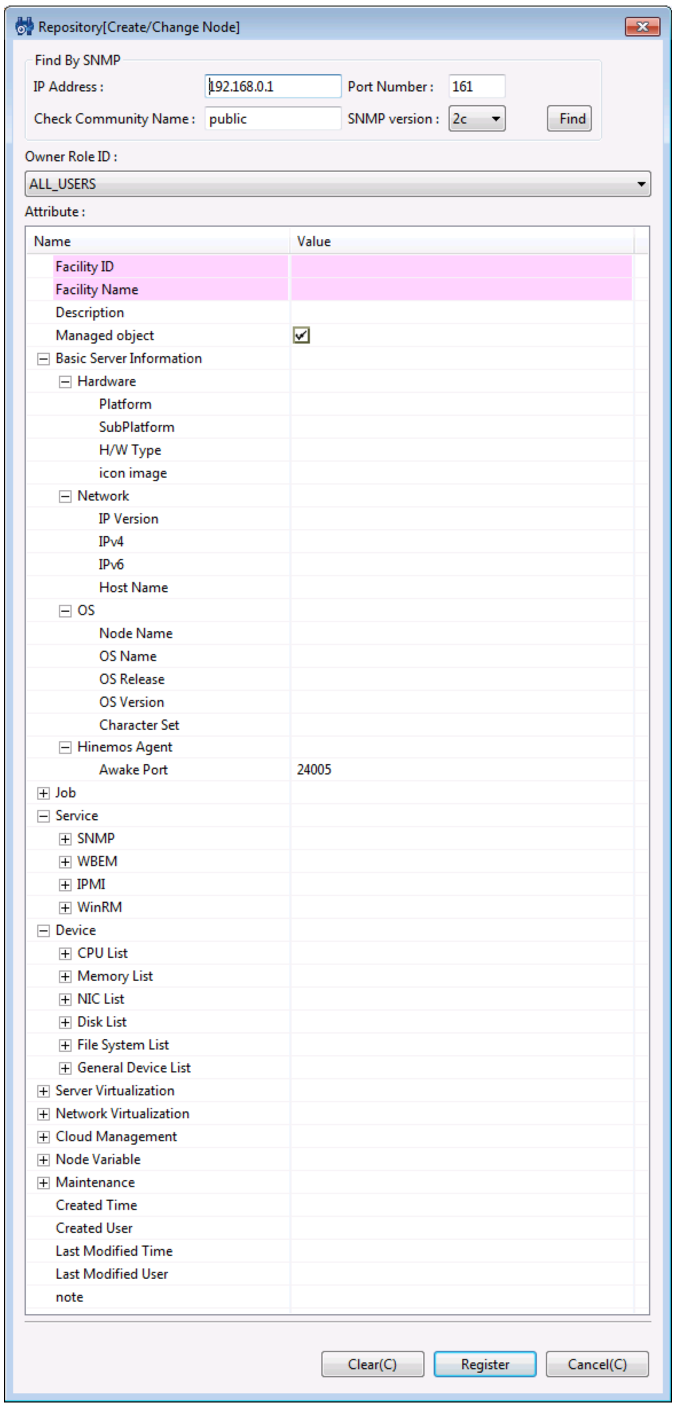
3.4.1 Creating Node Information

Node information is referenced by all features. Since incorrect data can trigger operation errors, use care in setting.

Node information can be registered in the repository by following the procedure below.

1. Click the "Create" button in Repository[Node] view. The Repository[Create/Change Node] dialog box will open.

Copyright (c) 2013 NTT DATA CORPORATION



IP Address : 192.168.0.1 Port Number : 161

Check Community Name : public SNMP version : 2c

Owner Role ID : ALL_USERS

Name	Value
Facility ID	
Facility Name	
Description	
Managed object	☑
⊟ Basic Server Information	
⊟ Hardware	
Platform	
SubPlatform	
H/W Type	
icon image	
⊟ Network	
IP Version	
IPv4	
IPv6	
Host Name	
⊟ OS	
Node Name	
OS Name	
OS Release	
OS Version	
Character Set	
⊟ Hinemos Agent	
Awake Port	24005
⊞ Job	
⊟ Service	
⊞ SNMP	
⊞ WBEM	
⊞ IPMI	
⊞ WinRM	
⊟ Device	
⊞ CPU List	
⊞ Memory List	
⊞ NIC List	
⊞ Disk List	
⊞ File System List	
⊞ General Device List	
⊞ Server Virtualization	
⊞ Network Virtualization	
⊞ Cloud Management	
⊞ Node Variable	
⊞ Maintenance	
Created Time	
Created User	
Last Modified Time	
Last Modified User	
note	

Figure 3-9 Repository[Create/Change Node] Dialog

2. Enter the attribute information. In the properties table where the list of attributes are displayed, click the record for entry, and enter the attribute value. For items that can be registered and their contents, please refer to Table 3-7 Contents of node information.

   Also, you can acquire part of the information for the target node by clicking Find after entering the IP address, Port number, Community Name, and version of "Find By SNMP". The device registered by Find obtains only data that has been input/output more than once since the OS reboot. When repository.find.by.snmp.verbose=true is added to hinemos.properties, the device that did not have data I/O is also added. Further, when acquiring information on the object node using "Find By SNMP", be careful of the following points:

- The Platform column will be "Other" when acquiring network device information.
- For Windows Server where the SNMP expansion agent is not installed, registration of node information will fail when acquiring information using SNMP version 1. Please use version 2c to acquire the information. Further, the node information can be registered for Windows servers with the SNMP expansion agent installed, regardless of which version.

3. Click the "Register" button. The currently entered node information will be registered.

   When a node is created it is automatically assigned to the "Registered Nodes (REGISTERED)" Scope.

Copyright (c) 2013 NTT DATA CORPORATION

Table 3-7 Details of node information

Name	Value	Note
Facility ID	Text	No duplicate, non-multibyte characters
Facility Name	Text	
Description	Text	
Management object	Checkbox	Switches whether or not to run Monitor or Job
Server Basic Information		
Hardware		
Platform	List	Select from "Linux", "Windows", "Network Equipment", "Other"
Sub-Platform	List	
H/W Type	Text	
icon image	Text	
Network		
IP Version	List	Enter version (4 or 6) for the address that is used (4:IPv4, 6:IPv6)
IPv4 address	Text	If "4" is entered in the IP Version, refer to the value here for the IP address of the node used for other features
IPv6 address	Text	If "6" is entered in the IP Version, refer to the value here for the IP address of the node used for other features
Host Name	Text	Multiple can be registered
OS		
Node Name	Text	Enter the host name of the target machine. Used in the system log monitoring feature
OS Name	Text	
OS Release	Text	
OS Version	Text	
Character Set	Text	
Hinemos Agent		
Awake Port	Numeric	Destination port of awake packet
Job		
Job Priority	Text	Job Priority (if blank, 16)
Job Multiplicity	Text	Maximum number of concurrent jobs (if blank, 0)
Service		
SNMP		Monitoring using SNMP (SNMP Monitor, Process Monitor, Resource Monitor) uses this value
Port Number	Numeric	Refer to the value here for the port number of SNMP (if blank, 161)
Community Name	Text	Refer to the value here for the community name of SNMP (if blank, public)
Version	List	Select either "1" or "2c". Refer to the value here for the version of SNMP (if blank, 2c)
Timeout	Numeric	Refer to the value here for the timeout of SNMP (ms) (if blank, 5000 ms)
Retry Count	Numeric	Refer to the value here for the SNMP retry count (if blank, 3)
WBEM		Monitoring using WBEM (Process Monitor, Resource Monitor) uses this value
User Name	Text	Refer to the value here for the OS user name connecting to the CIM server (if blank, root)

Copyright (c) 2013 NTT DATA CORPORATION

User password	Text	Refer to the value here for the password of OS user connecting to the CIM server (if blank, password)
Port Number	Numeric	Refer to the value here for the port number connecting to the CIM server (if blank, 5988)
Protocol	List	Refer to the value here for the protocol connecting to the CIM server (if blank, http)
Timeout	Numeric	Refer to the value here for the port time out (ms) connecting to the CIM server (if blank, 5000 ms)
Retry Count	Numeric	Refer to the value here for the retry count when connecting to the CIM server (if blank, 3 times)
IPMI		
Address	Text	Refer to the value here for the IPMI address
Port Number	Numeric	Refer to the value here for the IPMI port number
User	Text	Refer to the value here for the user name connecting to the IPMI
User password	Text	Refer to the value here for the password of OS user connecting to the IPMI
Timeout	Numeric	Refer to the value here for the timeout for connecting to the IPMI
Retry Count	Numeric	Refer to the value here for the retry count for connecting to the IPMI (if blank, 3 times)
Protocol	Text	Refer to the value here for the protocol connecting to the IPMI
IPMI Level	Text	Refer to the value here for the IPMI Level connecting to the IPMI
WinRM		Monitoring using (Windows Service Monitor) uses this value
User Name	Text	Refer to the value here for the user name connecting to the WinRM
User password	Text	Refer to the value here for the password of OS user connecting to the WinRM
Version	Text	Refer to the value here for the WinRM connection version (enter 1.1 or 2.0)
Port Number	Numeric	Refer to the value here for the port number connecting to the WinRM (Default 80 port for http WinRM1.1 (Default 443 port for https WinRM1.1 (Default 5985 port for http WinRM2.0 (Default 5986 port for https WinRM2.0
Protocol	List	Refer to the value here for the protocol connecting to the WinRM (enter http or https)
Timeout	Numeric	Refer to the value here for the timeout for connecting to the WinRM
Retry Count	Numeric	Refer to the value here for the retry count for connecting to the WinRM (if blank, 3 times)
Device		
CPU Information		
CPU		Multiple can be registered. Used by the Resource Monitor
Display Name	Text	
Device Name	Text	
Device INDEX	Numeric	
Device Type	Text	cpu (Fixed Value)
Device Size	Numeric	
Device Size Unit		
Description	Text	
Memory Information		

Copyright (c) 2013 NTT DATA CORPORATION

Memory		
Display Name	Text	
Device Name	Text	
Device INDEX	Numeric	
Device Type		mem (Fixed Value)
Device Size	Numeric	
Device Size Unit		
Description	Text	
NIC information		
NIC		Multiple can be registered. Used by the Resource Monitor
Display Name	Text	
Device Name	Text	
Device INDEX	Numeric	
Device Type		nic (Fixed Value)
Device Size	Numeric	
Device Size Unit		
Description	Text	
NIC IP Address	Text	
NIC MAC Address	Text	
Disk Information		
Disk		Multiple can be registered. Used by the Resource Monitor
Display Name	Text	
Device Name	Text	
Device INDEX	Numeric	
Device Type		disk (Fixed Value)
Device Size	Numeric	
Device Size Unit		
Description	Text	
Disk Rpm		
File System Information		
File System		
Display Name	Text	
Device Name	Text	
Device INDEX	Numeric	
Device Type		filesystem (Fixed Value)
Device Size	Numeric	
Device Size Unit		
Description	Text	
File System Type		
General Device List		
General Device		
Display Name	Text	
Device Name	Text	

Device INDEX	Numeric	
Device Type		
Device Size	Numeric	
Device Size Unit		
Description	Text	
Server Virtualization		
Node Type	List	Utilized when using VM Management Option
Management Node	List	Utilized when using VM Management Option
Virtual Machine Index	Numeric	Utilized when using VM Management Option
Virtual Machine Name	Text	Utilized when using VM Management Option
Virtualization Solution	Text	Utilized when using VM Management Option
Virtual Machine ID	Text	Utilized when using VM Management Option
Virtual Machine User	Text	Utilized when using VM Management Option
Virtual Machine Connection User Password	Text	Utilized when using VM Management Option
Virtual Machine Connection Protocol	List	Utilized when using VM Management Option
Network Virtualization		
Virtual Switch Type	List	
Virtual Switch Host Node	List	
OpenFlow		
Datapath ID	Text	When the OpenFlow support switch is registered as a node and the host equipped with the OpenFlow virtual switch is set as a node, enter the data path ID assigned to the switch as base 16 (e.g., 0000001458F4584B).
Controller IP address	Text	Enter the IP address (e.g., 192.168.1.101) for the OpenFlow controller connected to the switch/virtual switch supporting OpenFlow.
Cloud Management		
Node type	Text	Used by Cloud Management Option
Cloud Service	Text	Used by Cloud Management Option
Cloud	Text	Used by Cloud Management Option
Account Resource	Text	Used by Cloud Management Option
Cloud Resource Type	Text	Used by Cloud Management Option
Cloud Resource ID	Text	Used by Cloud Management Option
Cloud Region	Text	Used by Cloud Management Option
Cloud Zone	Text	Used by Cloud Management Option
Node Variable		
Node Variable		
Node Connection Name	Text	
Node Connection Value	Text	
Maintenance		
Administrator	Text	
Contact	Text	
Created Time	Text	
Created User	Text	

Last Change Time	Text	
User Last Changed	Text	
Note	Text	

Behavior if management object is unchecked

If "management object" is not checked, monitoring, job, and batch control processes will not run. As a result, even if notifications are configured in monitoring features, there will be no notifications. Also, history of the corresponding nodes will not be created for the job and batch control features. Depending on whether "management object" is checked or unchecked, the node icon that appears in the scope tree etc. will change as shown in Table 3-8.

Table 3-8 Node Display Icon

Icon	Description
▮	Appears when "management object"is checked.
⬚	Appears when "management object"is unchecked.

Method of adding/deleting items where multiple registrations are possible

- Method of adding items
  1. Select the "Name" column where multiple registrations are possible ("Network - Host Name", "Device", "File System", "note"), then right-click.
  2. A menu showing options to Copy or Delete will be displayed.
  3. Choose Copy.
- Method of deleting items
  1. Select the items where multiple registrations are possible ("Server Basic Information - Network - Host Name", "Device" and "Note") and right click.
  2. A menu showing options to Copy or Delete will be displayed.
  3. Select Delete.

Method of confirming commands of SNMP and WBEM

The following items are explained in advance as commands necessary for operating SNMP/WBEM polling on the monitored server by CLI (Command Line Interface). This command is not required for the operating environments of the Hinemos Manager and the Hinemos Agent, but since it is useful for confirming operations, its installation is recommended.

- For SNMP, use the snmpwalk command. To use this command, please install the net-snmp-utils package in a Red Hat Enterprise Linux environment which is used for operation.
- For WBEM, use the wbemcli command. To use this command, please install the sblim-wbemcli package in a Red Hat Enterprise Linux environment which is used for operation. (Installation of the top-pegasus package is also required for installation of the sblim-wbemcli package)

Entering device information

To collect the performance values of each device in the resource monitor, device information of the nodes must be registered in the registry information.

Method of registering disk information

- If using SNMP for monitoring

1. Run the following command to find disc information.

```
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.4.1.2021.13.15.1.1.2
```

2. Input the numbers following "UCD-DISKIO-MIB::diskIODevice." in the left column of the output results in " Device - Disk Information - Disk - Device Index".
3. Input the value (output to the right of STRING:) of "UCD-DISKIO-MIB::diskIODevice.xx" in "Device - Disk Information - Disk - Device Name".
4. Enter any name for the Display Name (if registered name is long, it may not display on the screen.)

Example) If the output is as follows, the registered contents of the device will be as shown in Table 3-9.

```
UCD-DISKIO-MIB::diskIODevice.1 = STRING: hda
UCD-DISKIO-MIB::diskIODevice.2 = STRING: hda1
UCD-DISKIO-MIB::diskIODevice.3 = STRING: hda2
UCD-DISKIO-MIB::diskIODevice.4 = STRING: hdb
UCD-DISKIO-MIB::diskIODevice.5 = STRING: hdb1
```

Table 3-9 Configuring Device Items

Device	Item	Configured value
First device	Display Name	(any string)
	Device Name	hda
	Device Index	1
Second Device	Device Name	(any string)
	Device Name	hda1
	Device Index	2
Third Device	Device Name	(any string)
	Device Name	hda2
	Device Index	3
Fourth Device	Device Name	(any string)
	Device Name	hdb
	Device Index	4
Fifth Device	Device Name	(any string)
	Device Name	hdb1
	Device Index	5

Copyright (c) 2013 NTT DATA CORPORATION

- If using WBEM for monitoring (only compatible with Linux)

  1. Run the following command to find disc information.

     ```
     $ wbemcli ei \
       'http://(user name of target machine):(user's password of target machine)@(IP address of target machine):5988/root/cimv2:Linux_BlockStorageStatisticalData'
     ```

  2. Enter the characters following the output results for "ElementName" in "Device - Disk Information - Disk - Device Index".
  3. Enter any name for the Display Name (if registered name is long, it may not display on the screen.)

Example) If the output is as follows, the registered contents of the device will be as shown in Table 3-10.

```
localhost:5988/root/cimv2:Linux_BlockStorageStatisticalData.InstanceID="Linux:eins.cc.osdc.co.jp_sda" ・・・ partially omitted ・・・
ElementName="sda",StartStatisticTime ・・・ following abbreviated ・・・
localhost:5988/root/cimv2:Linux_BlockStorageStatisticalData.InstanceID="Linux:eins.cc.osdc.co.jp_hda"  ・・・ partially omitted ・・・
ElementName="hda",StartStatisticTime ・・・ following abbreviated ・・・
```

(User name of target machine: root, IP address of the target machine: localhost)

Table 3-10 Configuring Device Items

Device	Item	Configured value
First device	Display Name	(any string)
	Device Name	sda
	Device Index	0
Second Device	Device Name	(any string)
	Device Name	hda
	Device Index	0

NIC information registration method

- If using SNMP for monitoring

  1. To find NIC information, run the following command.

     ```
     $ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.2.2.1.2
     ```

  2. Enter the number following "IF-MIB::ifDescr." in "Device Index".
  3. Enter the value for the output results of "IF-MIB::ifDescr" (output on the right of STRING:) in "Device - NIC Information - NIC - Device name". (This device name can be changed to any name. if the registered name is long, it may not display on the screen.)

- If using WBEM for monitoring

  NIC information cannot be monitored in WBEM.

Entering file system information

To collect the file system usage per mount point in the performance management feature, the node file system information must be registered in Repository information.

Method of registering mount point information

- If using SNMP for monitoring

1. To find mount point information, run the following command.

```
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.25.2.3.1.3
```

2. From output value (STRING: output on the right) of "HOST-RESOURCES-MIB::hrStorageDescr.xx", Select the mount point to monitor and enter the "Device - File System Information - File System - Device Name". This is not required when the OS of target node is Windows.
3. From the numbers following "HOST-RESOURCES-MIB::hrStorageDescr." on the left side of the output results, enter the numeric value corresponding to the mount point entered in 2 in the "Device - File System Information - File System – File system INDEX".
4. Enter any name for the Display Name (if registered name is long, it may not display on the screen).

Example) If the output is as follows, the registered contents of the file system will be as shown in Table 3-11.

```
HOST-RESOURCES-MIB::hrStorageDescr.1 = STRING: Memory Buffers
HOST-RESOURCES-MIB::hrStorageDescr.2 = STRING: Real Memory
HOST-RESOURCES-MIB::hrStorageDescr.3 = STRING: Swap Space
HOST-RESOURCES-MIB::hrStorageDescr.4 = STRING: /
HOST-RESOURCES-MIB::hrStorageDescr.5 = STRING: /sys
HOST-RESOURCES-MIB::hrStorageDescr.6 = STRING: /boot
HOST-RESOURCES-MIB::hrStorageDescr.7 = STRING: /proc/sys/fs/binfmt_misc
HOST-RESOURCES-MIB::hrStorageDescr.8 = STRING: /var/lib/nfs/rpc_pipefs
```

Table 3-11 Configuring File System Items

File system	Item	Configured value
First file system	Display Name	(any string)
	File System Index	4
	Mount Point	/
Second file system	Display Name	(any string)
	File System Index	6
	Mount Point	/boot

- If using WBEM for monitoring (only compatible with Linux)

1. To find mount point information, run the following command.

```
$ wbemcli ei 'http://(user name of target machine):(user's password of target machine)@(IP address of target machine):5988/root/cimv2: Linux_Ext3FileSystem'
```

2. Enter string following the output "Root=" in "Mount Point".
3. Enter any name for the Display Name (if registered name is long, it may not display on the screen).

   Example) If the output is as follows, the registered contents of the file system will be as shown in Table 3-12.

```
localhost:5988/root/cimv2:Linux_Ext3FileSystem.CreationClassName="Linux_Ext3FileSystem" ・・・ partially omitted ・・・
Root="/",BlockSize=4096 ・・・ following abbreviated ・・・
localhost:5988/root/cimv2:Linux_Ext3FileSystem.CreationClassName="Linux_Ext3FileSystem" ・・・ partially omitted ・・・
Root="/boot",BlockSize=1024 ・・・ following abbreviated ・・・
```

Table 3-12 Configuring File System Items

File system	Item	Configured value
First file system	Display Name	(any string)
	File System Index	0
	Mount Point	/

Copyright (c) 2013 NTT DATA CORPORATION

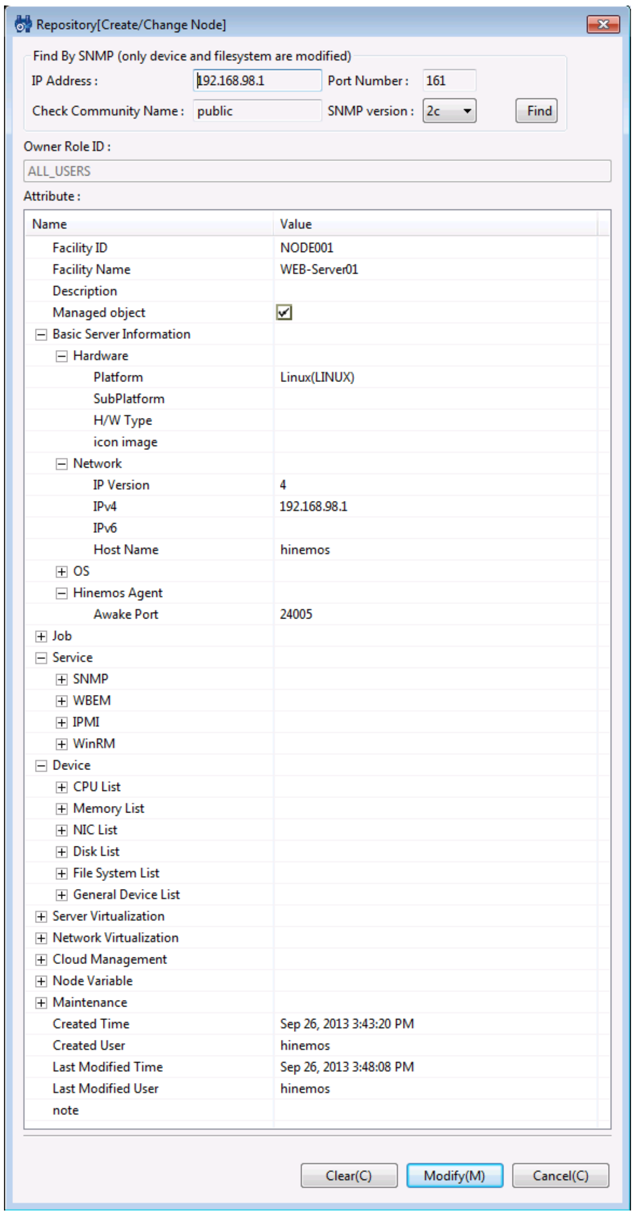
Second file system	Display Name	(any string)
	File System Index	0
	Mount Point	/boot

3.4.2 Changing node information

The node information registered in the Repository can be changed. There are two methods of changing node information.

- Changing node base

1. Select the node to change from the node list table in Repository[Node] view, and then click the "Modify" button. With selected node information entered, The Repository[Create/Change Node] dialog box will open.
2. Select "Node base (Only one node)" from the Registration Method radio button.
3. Edit attribute information. Click the record to change in the properties table where the list of attributes are displayed, then enter the attribute value. By clicking on the Find, just the device and file system information of targeted node information can be obtained by using SNMP. Find registers only the devices (disk, nic) with data that have had more than one IN/OUT since the OS reboot, and does not obtain devices that have not had a single data flow since the OS reboot.
4. Click the "Modify" button. The currently entered node information will be registered.



Repository[Create/Change Node]

Find By SNMP (only device and filesystem are modified)

IP Address : 192.168.98.1 Port Number : 161

Check Community Name : public SNMP version : 2c

Owner Role ID : ALL_USERS

Attribute :

Name	Value
Facility ID	NODE001
Facility Name	WEB-Server01
Description	
Managed object	☑
⊟ Basic Server Information	
⊟ Hardware	
Platform	Linux(LINUX)
SubPlatform	
H/W Type	
icon image	
⊟ Network	
IP Version	4
IPv4	192.168.98.1
IPv6	
Host Name	hinemos
⊞ OS	
⊟ Hinemos Agent	
Awake Port	24005
⊞ Job	
⊟ Service	
⊞ SNMP	
⊞ WBEM	
⊞ IPMI	
⊞ WinRM	
⊟ Device	
⊞ CPU List	
⊞ Memory List	
⊞ NIC List	
⊞ Disk List	
⊞ File System List	
⊞ General Device List	
⊞ Server Virtualization	
⊞ Network Virtualization	
⊞ Cloud Management	
⊞ Node Variable	
⊞ Maintenance	
Created Time	Sep 26, 2013 3:43:20 PM
Created User	hinemos
Last Modified Time	Sep 26, 2013 3:48:08 PM
Last Modified User	hinemos
note	

Figure 3-10 Repository[Create/Change Node] Dialog

Copyright (c) 2013 NTT DATA CORPORATION

3.4.3 Deleting Node Information

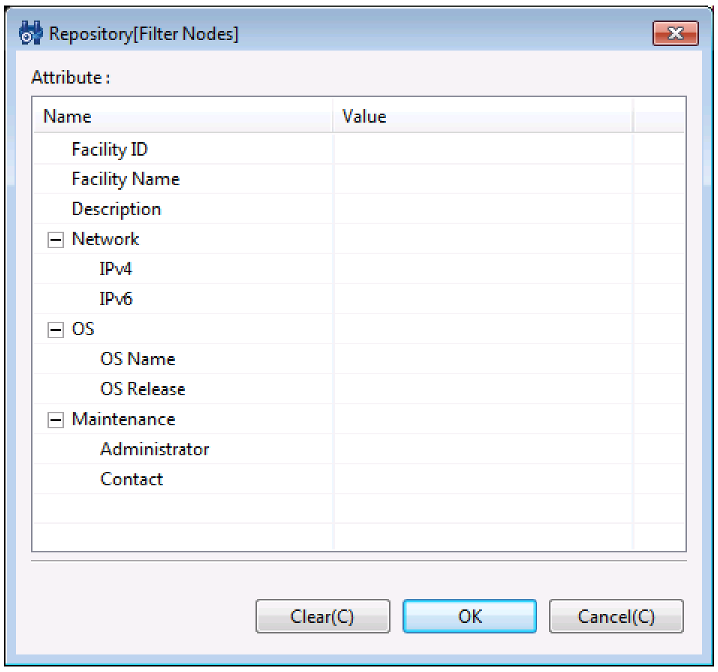
Select the node to change from the node list table in the Repository[Node] view, then click the "Delete" button.

3.4.4 Filtering the Node Information List

The filter can narrow down and display only the node information that matches a specified attribute.

1. Click the "Filter" button in the Repository[Node] view. The Repository[Filter Nodes] dialog will open.
2. Enter the refining conditions for filtering. In the properties table where the list of attributes are displayed, click on the records for refinement, and enter the attribute value. Please leave blank the attribute values that do not apply to the refining.
3. Click the "OK" button in the Repository[Filter Nodes] dialog box, then close the dialog.

   To cancel a filter setting, click the "Cancel" button.



Repository[Filter Nodes]

Attribute :

Name	Value
Facility ID	
Facility Name	
Description	
⊟ Network	
IPv4	
IPv6	
⊟ OS	
OS Name	
OS Release	
⊟ Maintenance	
Administrator	
Contact	

Figure 3-11 Repository[Filter Nodes] Dialog

3.5 Confirming property information

Confirm the property information of a node by selecting the node from the list table in Repository[Node] view. The selected node property information and node assignment status are displayed in Repository[Node Property] and Repository[Assigned Scopes] view. Click the "Update" button in each view if the node information settings are changed but not applied.

3.6 Creating/Changing/Deleting Scopes

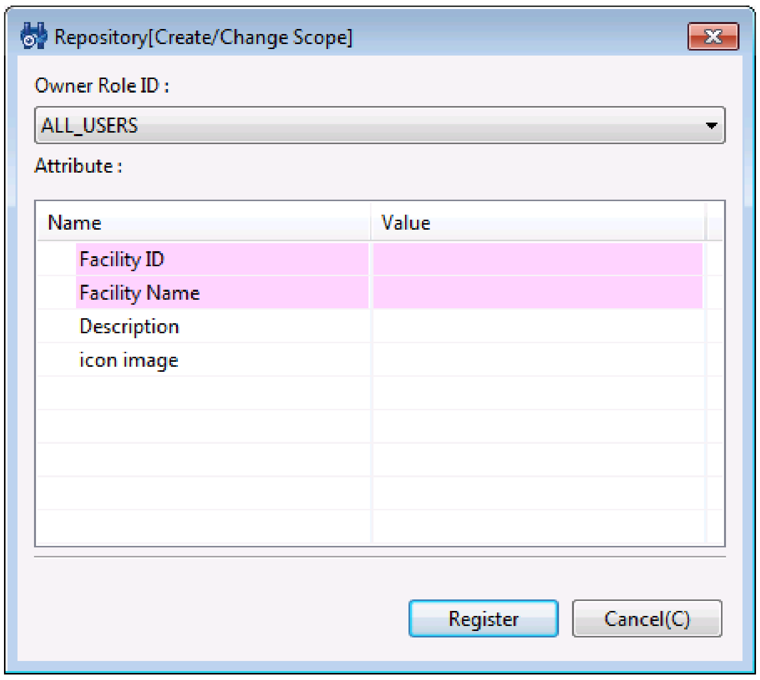
3.6.1 Creating a Scope

A Scope can be created in the repository using the following procedure.

1. From the scope tree in the Repository[Scope] view, choose a scope to be the parent scope. A new scope is created under the selected scope, thus creating a hierarchy structure.
2. Click the "Create" button in the Repository[Scope] view. The Repository[Create/Change Scope] dialog will open.

Copyright (c) 2013 NTT DATA CORPORATION

3. Enter the attribute information. In the properties table where the list of attributes are displayed, click on the record for entry, and enter the attribute value. The Facility ID and Facility Name are mandatory items (may not be omitted). In addition, the Facility ID must be unique on the system. Duplicate Facility IDs cannot be registered (not case sensitive).
4. Click the "Register" button. The entered scope will be registered.



Repository[Create/Change Scope]

Owner Role ID : ALL_USERS

Attribute :

Name	Value
Facility ID	
Facility Name	
Description	
icon image	

Figure 3-12 Repository[Create/Change Scope] Dialog

3.6.2 Changing the Scope Information

The scope information registered in the repository can be changed.

1. Select the scope to change from the scope tree in Repository[Scope] view.
2. Click the "Modify" button in the Repository[Scope] view. With the attribute information of the scope entered, the Repository[Create/Change Scope] dialog will open.
3. Modify the attribute information. In the properties table where the list of attributes are displayed, click the record for entry, and modify the attribute value.
4. Click the "Register" button. The entered scope will be registered.

3.6.3 Deleting a Scope

1. Select the scope to delete from the scope tree in Repository[Scope] view.
2. Click the "Delete" button in the Repository[Scope] view.

3.7 Node Assignment

3.7.1 Node Assignment

Assignment of a node to a scope. It is possible to assign a single node to multiple scopes.

1. From the scope tree in the Repository[Scope] view, select the scope subject to node assignment. The node will be placed under the scope selected, thus creating a hierarchy structure.
2. Click the "Assign" button in the Repository[Scope] view. The Repository[Select Nodes] dialog will open.

Copyright (c) 2013 NTT DATA CORPORATION

3. Select the node to add to scope from the list of nodes displayed. It is possible to select multiple nodes at once. (Use the Ctrl key.)
4. Click the "Assign" button. The selected node is assigned to the scope.

To refine nodes that appear in the list by specifying conditions

The nodes appearing in the list can be refined by using the filter feature.

1. Click the "Filter" button in the Repository[Select Nodes] dialog. The Repository[Filter Nodes] dialog will open.
2. Enter the refining conditions for filtering. In the properties table where the list of attributes are displayed, click on the records for refinement, and enter the attribute value. Please leave blank the attribute values that do not apply to the refining.
3. Click the "OK" button in the Repository[Filter Nodes] dialog box, then close the dialog. To cancel a filter setting, click the "Cancel" button.

3.7.2 Releasing a Node Assignment

Please follow the procedure below to release an assigned node from a scope.

1. From the scope tree in Repository[Scope] view, select the scope. The node assignment included in the selected scope can be released.
2. Click the "Release" button in the Repository[Scope] view. The Repository[Select Nodes] dialog will open.
3. The selected scope will display a list of nodes that are currently assigned to it. Select the node to release the assignment. It is possible to select multiple nodes at once. (Use the Ctrl key.)
4. Click the "OK" button. The selected node assignment will be released.

To cancel the node assignment release, click the "Cancel" button.

3.8 Restart and Update the Agent

3.8.1 AGENT Restart

Agent restart is a feature for restarting the selected Hinemos Agent from the Hinemos Manager.

1. From the Repository[Agent] view, select the agent. (Multiple agents can be selected at the same time.) (Use the Ctrl key.)
2. Click the "Restart" button.

The selected agent will restart.

3.8.2 Agent Update

Agent Update is a feature for remote update of the library file of the selected Hinemos Agent from the Hinemos Manager.

When you run Agent Update, the Hinemos Manager uses the library file (/opt/hinemos/lib/agent/) it holds to update the following library file for the selected Hinemos Agent, and then restarts the Hinemos Agent.

- (For a Linux Agent) /opt/hinemos_agent/lib/
- (For a Windows Agent) [Hinemos Agent install directory]\lib\

1. From the Repository[Agent] view, select the agent. (Multiple agents can be selected at the same time.) (Use the Ctrl key.)
2. Click the "Module Update" button.

The module is updated for the selected agent, and restarted.

The image that is generally used is as follows.

1. The new library is placed in the Hinemos Manager's agent library location (/opt/hinemos/lib/agent/).
2. Confirm that the update row in the Repository[Agent] view has become "not.yet".
3. Select the agent to update from the Repository[Agent] view . (Multiple selections are possible.)
4. Click the "Update" button.
5. Confirm that the update row in the Repository[Agent] view has become "done".

Copyright (c) 2013 NTT DATA CORPORATION

4 Calendar Feature

4.1 Overview

You can configure the operating/non-operating periods for the monitoring and job management features, and then save it for reference as a calendar.

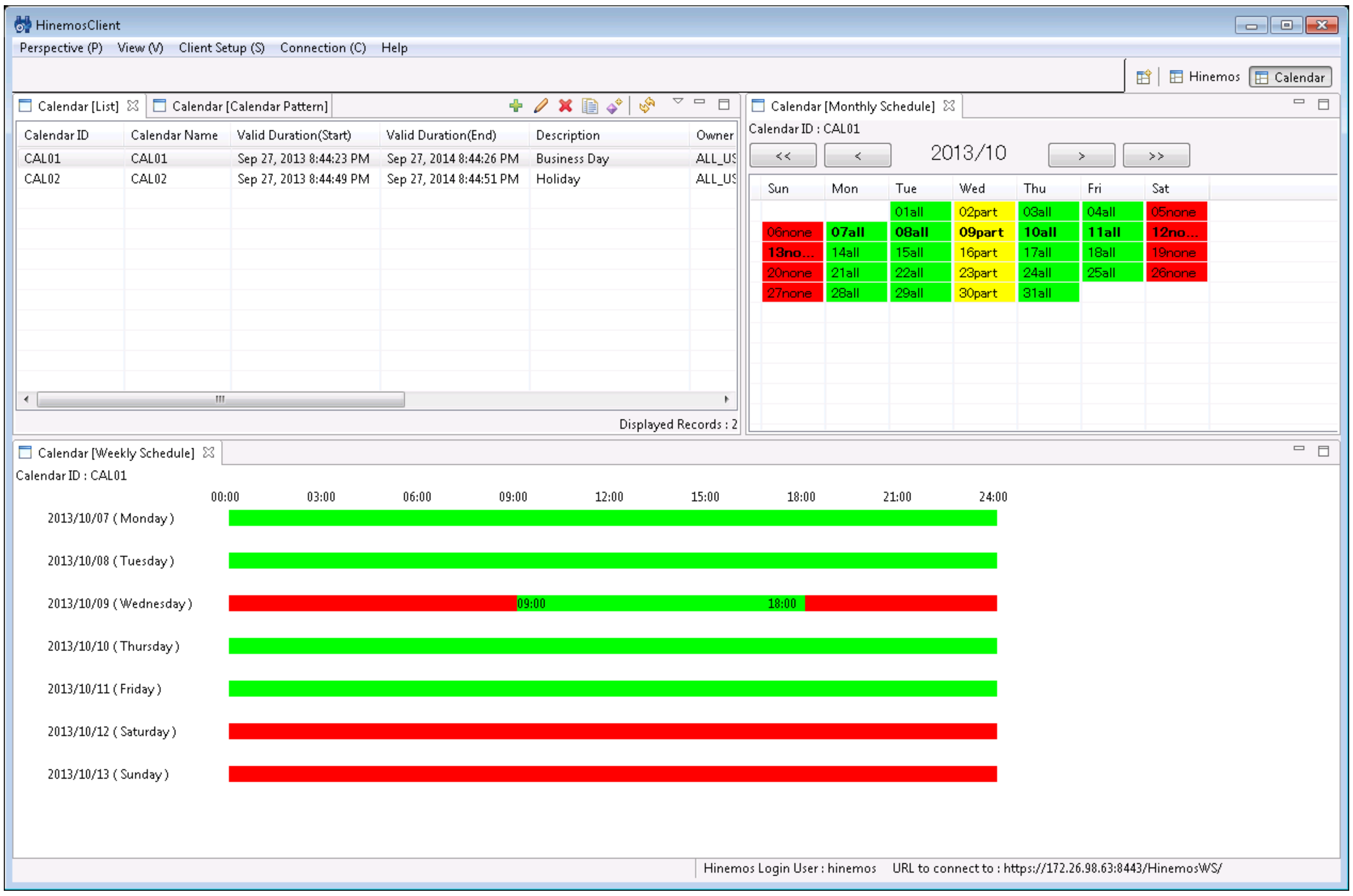
The operating period can be configured by the two following methods.

1. You can set the operating times and non-operating times for the calendar in units of years, months, days, or weekdays.
2. You can collectively specify irregular schedules such as national holidays and business days, etc.

You can set only specific days as operating days or non-operating days.

4.2 Interface Composition

4.2.1 Default Interface



Calendar ID	Calendar Name	Valid Duration(Start)	Valid Duration(End)	Description	Owner
CAL01	CAL01	Sep 27, 2013 8:44:23 PM	Sep 27, 2014 8:44:26 PM	Business Day	ALL_US
CAL02	CAL02	Sep 27, 2013 8:44:49 PM	Sep 27, 2014 8:44:51 PM	Holiday	ALL_US

Displayed Records : 2

Calendar ID : CAL01

2013/10

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		01all	02part	03all	04all	05none
06none	07all	08all	09part	10all	11all	12no...
13no...	14all	15all	16part	17all	18all	19none
20none	21all	22all	23part	24all	25all	26none
27none	28all	29all	30part	31all		

Calendar ID : CAL01

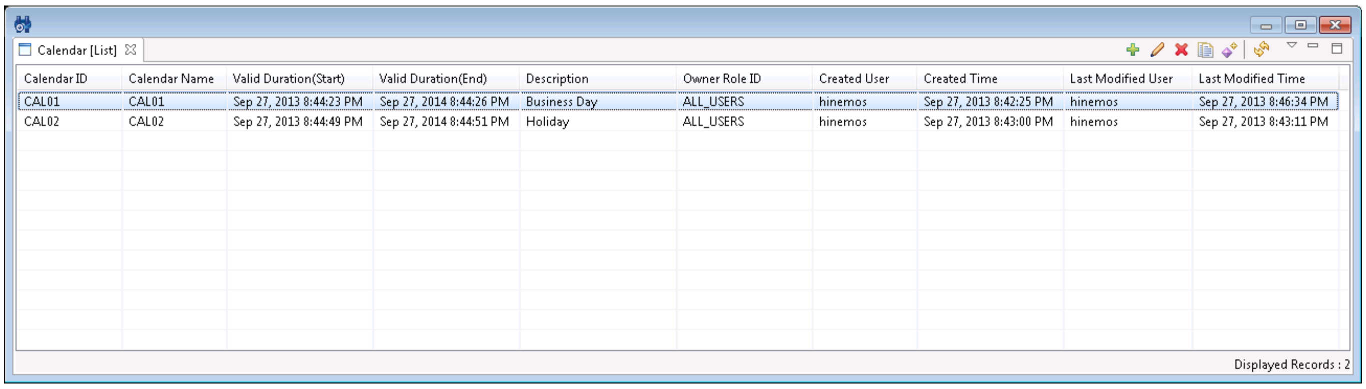
2013/10/07 (Monday)
2013/10/08 (Tuesday)
2013/10/09 (Wednesday)
2013/10/10 (Thursday)
2013/10/11 (Friday)
2013/10/12 (Saturday)
2013/10/13 (Sunday)

Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 4-1 Default Interface of Calendar Feature

4.2.2 Calendar[List] view

Copyright (c) 2013 NTT DATA CORPORATION



Calendar ID	Calendar Name	Valid Duration(Start)	Valid Duration(End)	Description	Owner Role ID	Created User	Created Time	Last Modified User	Last Modified Time
CAL01	CAL01	Sep 27, 2013 8:44:23 PM	Sep 27, 2014 8:44:26 PM	Business Day	ALL_USERS	hinemos	Sep 27, 2013 8:42:25 PM	hinemos	Sep 27, 2013 8:46:34 PM
CAL02	CAL02	Sep 27, 2013 8:44:49 PM	Sep 27, 2014 8:44:51 PM	Holiday	ALL_USERS	hinemos	Sep 27, 2013 8:43:00 PM	hinemos	Sep 27, 2013 8:43:11 PM

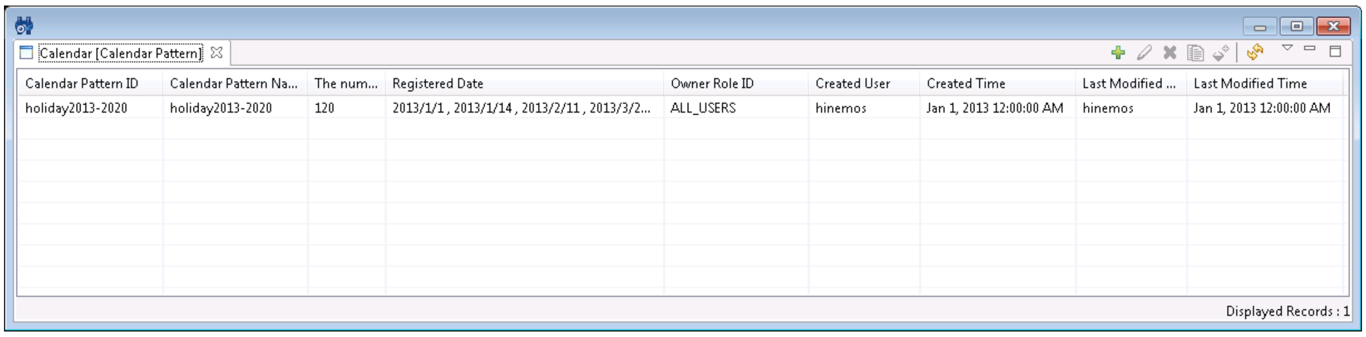
Displayed Records : 2

Figure 4-2 Calendar[List] View

Table 4-1 Toolbar

Icon	Button name	Description
✚	Create	Create calendar information.
✎	Change	Change calendar information.
✖	Delete	Delete calendar information.
📄	Copy	Copy calendar information.
◆	Object Privilege Settings	Assign object privilege to calendar.
⟳	Update	Update the contents of the Calendar[List] view.

4.2.3 Calendar[Calendar Pattern] view



Calendar Pattern ID	Calendar Pattern Na...	The num...	Registered Date	Owner Role ID	Created User	Created Time	Last Modified ...	Last Modified Time
holiday2013-2020	holiday2013-2020	120	2013/1/1 , 2013/1/14 , 2013/2/11 , 2013/3/2...	ALL_USERS	hinemos	Jan 1, 2013 12:00:00 AM	hinemos	Jan 1, 2013 12:00:00 AM

Displayed Records : 1

Figure 4-3 Calendar[Calendar Pattern] View

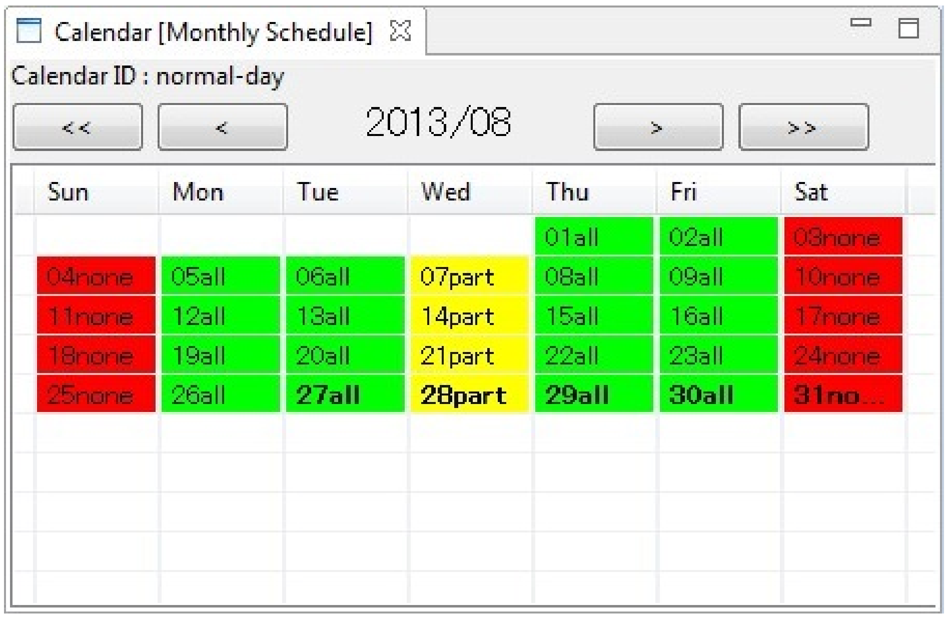
Table 4-2 Toolbar

Icon	Button name	Description
✚	Create	Create calendar pattern information.
✎	Modify	Change calendar pattern information.
✖	Delete	Delete calendar pattern information.
📄	Copy	Copy calendar pattern information
◆	Object Privilege Settings	Assign object privilege to calendar pattern.
⟳	Update	Update contents of the Calendar[Pattern] view.

4.2.4 Calendar[Month Plan] View

Displays the details of the calendar settings that were selected in the Calendar[List] view. You can use the buttons to switch between year and month.

Copyright (c) 2013 NTT DATA CORPORATION



Calendar [Monthly Schedule]

Calendar ID : normal-day

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				01all	02all	03none
04none	05all	06all	07part	08all	09all	10none
11none	12all	13all	14part	15all	16all	17none
18none	19all	20all	21part	22all	23all	24none
25none	26all	**27all**	**28part**	**29all**	**30all**	**31no...**

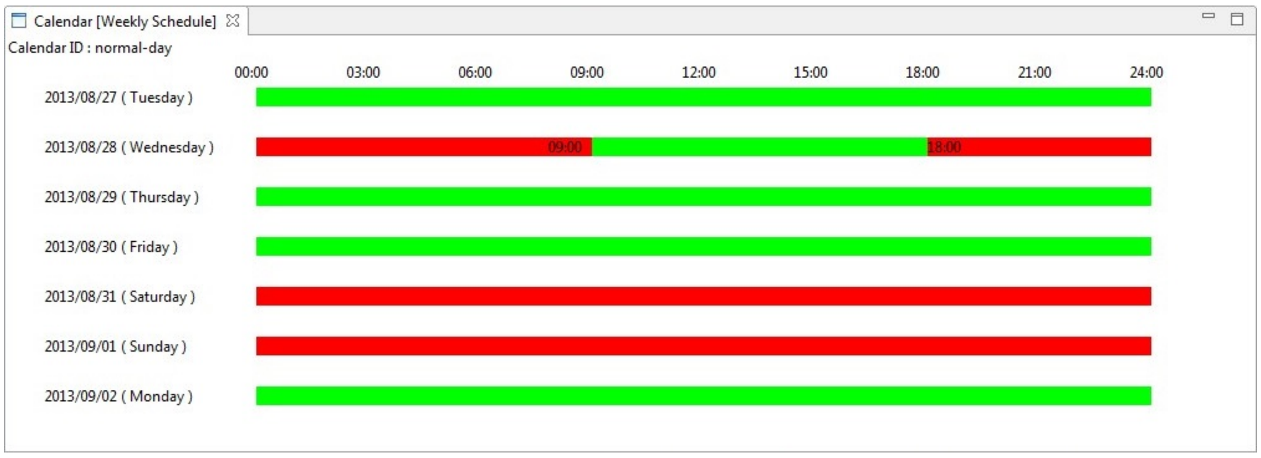
Figure 4-4 Calendar[Month Plan] View

Table 4-3 Toolbar

Button	Button name	Description
<	Previous month	Moves the month display to the previous month.
>	Next month	Advances the month display by one month.
<<	Previous year	Moves the year display to the previous year.
>>	Next year	Advances the year display by one year.

4.2.5 Calendar[Week Plan] View

Displays the detailed plan for one week from the date selected in the Calendar[Week Plan] view.



Calendar [Weekly Schedule]

Calendar ID : normal-day

Figure 4-5 Calendar[Week Plan] View

4.2.6 Calendar[Week Plan] view

The Calendar[Month Plan] view displays the details of the calendar settings selected in the Calendar[List] view. Displays the all-day operating days, all-day non-operating days and part operating days (part non-operating day s) using colors and symbols.

Table 4-4 Description of the Calendar[Week Plan] View Display

Display	Name	Description

ddall	All-day operating day	Operating 00:00:00 - 24:00:00
ddnone	Non-operating day	Not Operating 00:00:00 - 24:00:00
ddpart	Part operating Part non-operating	Only operating for some hours in a day i.e.) Operating 06:00:00 - 15:00:00

4.2.7 Calendar[Week Plan] View Confirmation

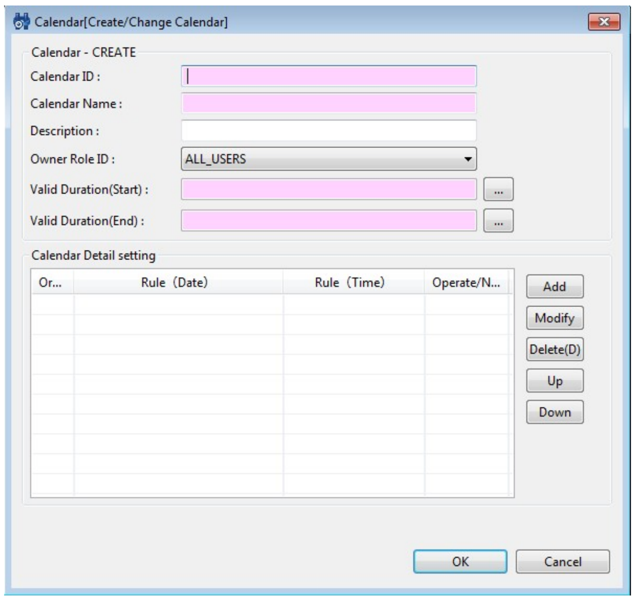
Displays the detailed plan for one week from the date selected in the Calendar[Week Plan] view. The operating times and non-operating times in a day are distinguished as follows.

- Operating time ······· Displayed in green
- Non-operating time ······· Displayed in red

4.3 Creating a Calendar

4.3.1 Registering a Calendar

1. Click the "Create" button on the Calendar[List] view. The Calendar[Create/Change Calendar] dialog will be displayed.
2. Specify the Calendar ID, Calendar Name and Description. Always be sure to enter the "Calendar ID" and "Calendar Name", since both are mandatory fields. The "Calendar ID" must be unique on the system.



Calendar[Create/Change Calendar]

Calendar - CREATE

Calendar ID :

Calendar Name :

Description :

Owner Role ID : ALL_USERS

Valid Duration(Start) :

Valid Duration(End) :

Calendar Detail setting

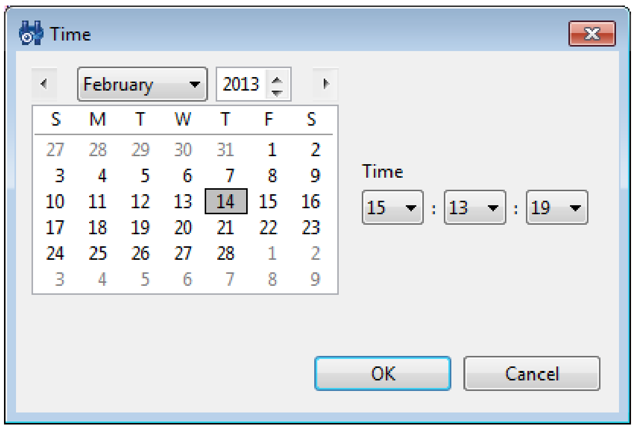
Or...	Rule（Date）	Rule（Time）	Operate/N...

Figure 4-6 Calendar[Create/Change Calendar] Dialog

3. Enter a Valid Duration (Start) and Valid Duration (End) in the Time dialog. The dialog can be opened by clicking the button next to the input field. Please select the date in the dialog. Select a time with the combo box. Calendar creation is valid only during the period (from the time specified for the start to just before the time specified as the end) specified here. Important points about the Valid Duration: **The time specified as Valid Duration (start) becomes valid and calendars can be created. However, The time specified as Valid Duration (end) becomes invalid and calendars can't be created.**

   For example) if the Valid Duration is set as "10/1 00:00:00" ~ "11/1 00:00:00",

   ⇒ "10/1 00:00:00" will be operating and "11/1 00:00:00" will be non-operating.



S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

Time 15 : 13 : 19

Figure 4-7 Time Dialog

4. Configure the calendar details. The detailed schedule is entered using the Calendar Detail dialog to enter the detailed schedule. Refer to 'Calendar Detail Setting'_ regarding setting the calendar details.
5. Click the "OK" button. The Calendar[Create/Change Calendar] dialog closes and the calendar added in the Calendar[List] view is added.

4.3.2 Changing the calendar Registration

1. Select the calendar to be changed in the Calendar[List] view, then click the "Modify" button. The Calendar[Create/Change Calendar] dialog is displayed.
2. Change the content and click the "OK" button.

4.3.3 Deleting a Calendar

1. Select the calendar to be deleted in the Calendar[List] view, then click the "Delete" button. In this case, the calendar can't be deleted if the calendar is being referenced by another function.

4.3.4 Copy a Calendar

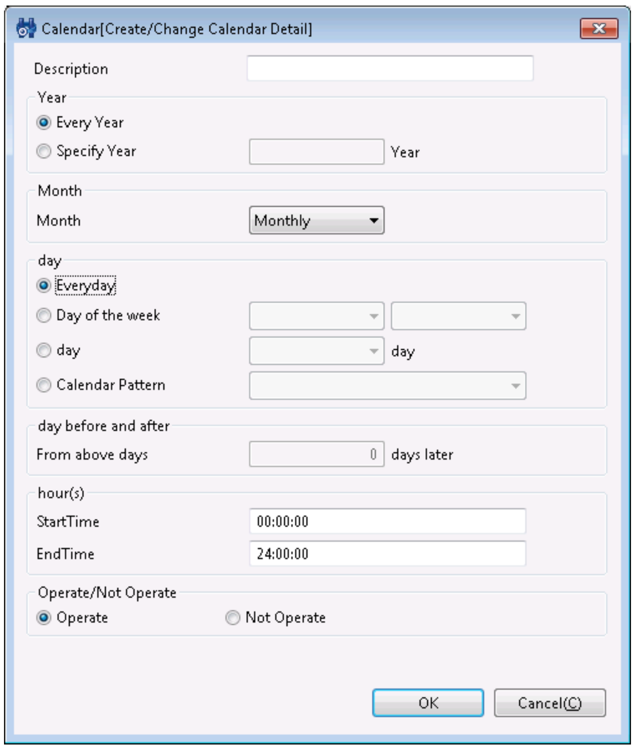
1. Select the calendar to be copied in the Calendar[List] view, then click the "Copy" button. The Calendar[Create/Change Calendar] dialog is displayed.
2. Change the Calendar ID and click the "OK" button.

4.4 Calendar Detail setting

4.4.1 Registering Calendar Details

Copyright (c) 2013 NTT DATA CORPORATION

1. Click the "Add" button in the Calendar Detail setting in the Calendar[Create/Change Calendar] dialog. The Calendar[Create/Change Calendar Detail] dialog is displayed.



Calendar[Create/Change Calendar Detail]

Description

Year
● Every Year
○ Specify Year Year

Month
Month: Monthly

day
● Everyday
○ Day of the week
○ day day
○ Calendar Pattern

day before and after
From above days 0 days later

hour(s)
StartTime 00:00:00
EndTime 24:00:00

Operate/Not Operate
● Operate ○ Not Operate

Figure 4-8 Calendar[Create/Change Calendar Detail] Dialog

2. Enter the detail settings. Refer to Table 4-4 Calendar Detail Settings for details on items that can be set.
3. Click the "OK" button. The entered details are displayed in the Calendar Detail Setting list in the Calendar[Create/Change Calendar] dialog.

Table 4-5 Calendar Detail Setting Details

Configuration items		Input type	Description
Description		Text	Enter a description of the detail setting.
Year	Every year	Radio button	"Every year" is selected as the default value.
	Specify	Radio button Text	Select "Specify" Enter the using Western calendar years.
Month	Month	Combo box	Select "Monthly" or from "January" ~ "December".
Day	Everyday	Radio button	"Everyday" is selected as the default value.
	Weekday	Radio button Combo box	Select "Weekday" Select "Weekly" or from "1st" ~ "5th". Select from "Sunday" ~ "Saturday".
	Day	Radio button Combo box	Select "Day" Select from "1" ~ "5".
	Calendar Pattern (*1)	Radio button Combo box	Select "Calendar Pattern". Select the Calendar Pattern definition with the combo box.
Days before and after		Text	"0" is entered as the default value. Enter a negative ("-") value to specify days previous.

Copyright (c) 2013 NTT DATA CORPORATION

Hours (*2)	Start time End time	Text	Enter the hours, minutes and seconds in "hh:mm:ss" format. The range of time that can be specified is "00:00:00" ~ "48:00:00" Also, enter the time so that the Start time < End time. The time specified here (from the time specified as the Start time, to the time just before the specified End time) is the only time valid for detail settings.
Operating/Non-operating		Radio button	Select "Operating" or Not Operating" using the radio buttons.

*1: Refer to 'Calendar Pattern Settings' regarding the Calendar Patterns.
*2: The time specified as the Start time is valid for operating. However, the time specified as the End time is invalid so that jobs will not be executed at the End time.

For example) if the Start time and End time are set as "10/1 9:00:00 AM" and "10/2 9:00:00 AM", "10/1 9:00:00 AM" will be valid and "10/2 9:00:00 AM" will be invalid.

4.4.2 Changing Calendar Details

1. Select the Calendar Detail setting to be changed in the Calendar[Create/Change Calendar] dialog, then click the "Modify" button. The Calendar[Create/Change Calendar Detail] dialog box is displayed.
2. Change the content and click the "Modify" button.

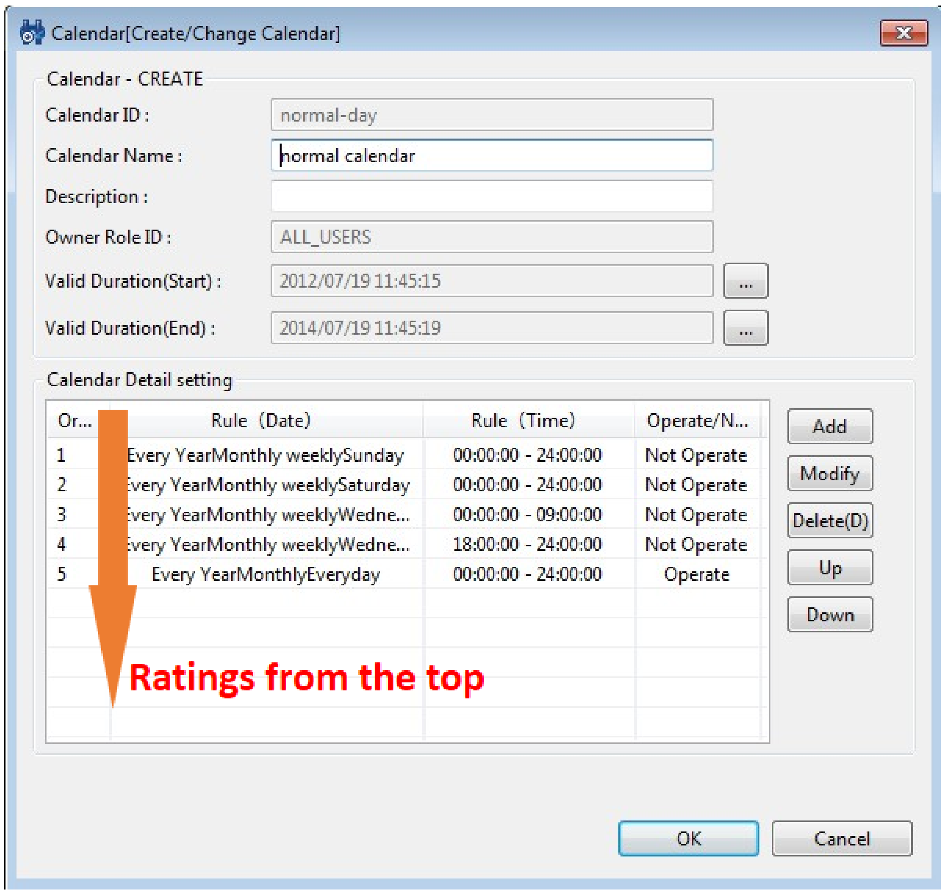
4.4.3 Deleting Calendar Details

1. Select the setting to be deleted in the Calendar[Create/Change Calendar] view, then click the "Delete" button.

4.4.4 Priority of Calendar Details

You can set the priority in the Calendar Detail Definitions. The definitions are evaluated in order from the top (in order from the lowest number). If it conforms to the definitions, subsequent Calendar Detail Definitions won't be evaluated. New definitions will be set as the lowest priority order. To change the priority order, select the definition to be changed from the Calendar Detail setting list, and click the "Up" button or the "Down" button. An example of the evaluation according to the priority order is as follows.

Copyright (c) 2013 NTT DATA CORPORATION



Calendar[Create/Change Calendar]

Calendar - CREATE

Calendar ID :	normal-day
Calendar Name :	normal calendar
Description :	
Owner Role ID :	ALL_USERS
Valid Duration(Start) :	2012/07/19 11:45:15
Valid Duration(End) :	2014/07/19 11:45:19

Calendar Detail setting

Or...	Rule (Date)	Rule (Time)	Operate/N...
1	Every YearMonthly weeklySunday	00:00:00 - 24:00:00	Not Operate
2	Every YearMonthly weeklySaturday	00:00:00 - 24:00:00	Not Operate
3	Every YearMonthly weeklyWedne...	00:00:00 - 09:00:00	Not Operate
4	Every YearMonthly weeklyWedne...	18:00:00 - 24:00:00	Not Operate
5	Every YearMonthlyEveryday	00:00:00 - 24:00:00	Operate

Ratings from the top

Figure 4-9 Calendar Priority Order

Definition example) Refer to Figure 4-9 Calendar Priority Order.

- Valid Duration: 2013/3/1 00:00:00 ~ 2014/3/1 00:00:00
- **Calendar Detail Definition:**

  1. Every Year Monthly 15th 00:00:00 - 30:00:00 Non-operating
  2. Every Year Monthly holiday2013-2020 (*1) 00:00:00 - 30:00:00 Non-operating
  3. Every Year Monthly Monday 00:00:00 - 30:00:00 Operating

  *1: "holiday2013-2020" is a holiday pattern inserted by default during installation

Process example)

- If the current date and time is "2013/03/25 (Monday) 08:00 ⇒ Calendar Detail Definition 3) is satisfied, and therefore Operating
- If the current date and time is "2013/03/26 (Tuesday) 04:00 ⇒ 06:00 - 30:00 in Calendar Detail Definition 3) is satisfied, and therefore Operating
- If the current date and time is "2013/03/26 (Tuesday) 08:00 ⇒ None of the above Calendar Detail Definition is satisfied, and therefore Non-operating
- If the current date and time is "2013/04/15 (Monday) 08:00 ⇒ Calendar Detail Definition 1) is satisfied, and therefore Non-operating
- If the current date and time is "2013/04/29 (Holiday, Monday) 08:00 ⇒ Calendar Detail Definition 2) is satisfied, and therefore Non-operating
- If the current date and time is "2014/03/03 (Monday) 08:00 ⇒ Exceeded the Valid Duration, and therefore Non-operating

Copyright (c) 2013 NTT DATA CORPORATION

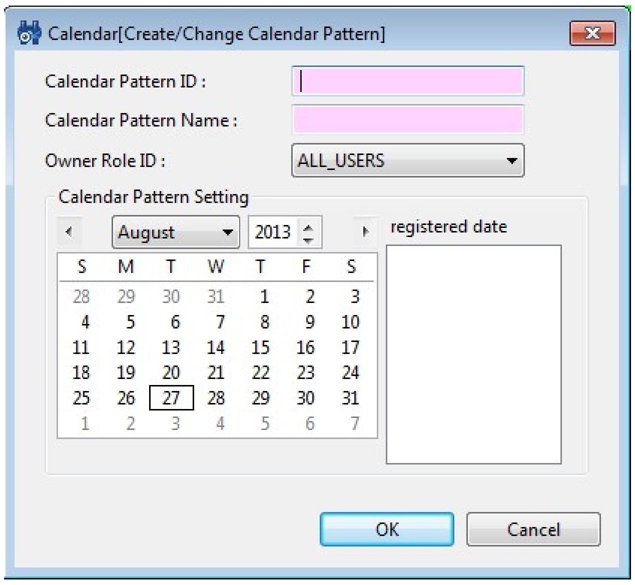
4.5 Calendar Pattern Setting

You can set an irregular schedule (business days and holidays) that is difficult to achieve with just year, month, day and day of the week. You can set a specific schedule as Operating and Not Operating by setting a Calendar Pattern.

* The actual holiday might be changed according to law, so please confirm the setting of default calendar pattern before using.

4.5.1 Calendar Pattern Registration

1. Click the "Create" button in the Calendar[Calendar Pattern] view. The Calendar[Create/Change Calendar Pattern] dialog is displayed.
2. Specify the Calendar Pattern ID, Calendar Pattern Name and Description. Always be sure to enter the Calendar Pattern ID and Calendar Pattern Name, since both are mandatory fields. The Calendar Pattern ID must be unique on the system.



Calendar[Create/Change Calendar Pattern]

Calendar Pattern ID :

Calendar Pattern Name :

Owner Role ID : ALL_USERS

Calendar Pattern Setting

August 2013

S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

registered date

Figure 4-10 Calendar[Create/Change Calendar Pattern] Dialog

3. Set the schedule by clicking on a date in the calendar in the dialog.
4. The set schedule can be released by clicking again.
5. Click the "OK" button. The Calendar[Create/Change Calendar Pattern] dialog closes. The created Calendar Pattern is added to the Calendar[Calendar Pattern] view.

4.5.2 Modifying a Calendar Pattern

1. Select the setting to be changed in the Calendar[Calendar Pattern] view, then click the "Modify" button. The Calendar[Calendar Pattern] dialog is displayed.
2. Change the content and click the "Modify" button.

4.5.3 Delete a Calendar Pattern

1. Select the setting to be deleted in the Calendar[Calendar Pattern] view, then click the "Delete" button. In this case, a Calendar Pattern can't be deleted if the Calendar Pattern is being referenced by another calendar setting.

4.5.4 Copy a Calendar Pattern

1. Select the calendar to be copied in the Calendar[Calendar Pattern] view, then click the "Copy" button. The Calendar[Calendar Pattern] dialog is displayed.
2. Change the Calendar Pattern ID and click the "OK" button.

Copyright (c) 2013 NTT DATA CORPORATION

5 Monitor Feature

5.1 Overview

This feature monitors the system and application logs, and the status of the managed nodes.

Specific log information can be specified for the monitoring log, and the information of the monitoring log displayed by scope in a list. In addition, the status can be displayed in a "Status" list.

The following are provided as the main features.

- Display list of log and status information

  You can display a list of log and status information by scope. The highest level of priority in the monitoring log information of a scope will be displayed as the priority of the scope itself. Also the total number for each priority is collected and displayed. You can filter and display the monitoring log information according to the attribute item condition. A monitoring log flag shows whether the operator has confirmed the log or not. The "Confirm" operation can be used to hide the confirmed monitoring log information from the list.

- Drill down display

  You can "drill down" to reference a lower hierarchy of the log information to match the scope hierarchy structure. Scopes are displayed in a hierarchal list on the screen. By selecting a scope in the tree you can "drill down" to display detailed information of the scope hierarchy structure. The whole scope can be confirmed first, followed by the detailed status.

- Notification feature

  You can send e-mail or execute jobs according to the priority of the monitor log information.

- Calendar feature

  You can register and refer to the calendar where the working time and the nonworking time are configured, and specify the periods when monitoring is enabled or disabled.

- Job execution triggered by notification

  You can execute jobs triggered by notifications in conjunction with the Job Management feature.

Copyright (c) 2013 NTT DATA CORPORATION

5.2 Screen Structure

5.2.1 Initial Screen Structure

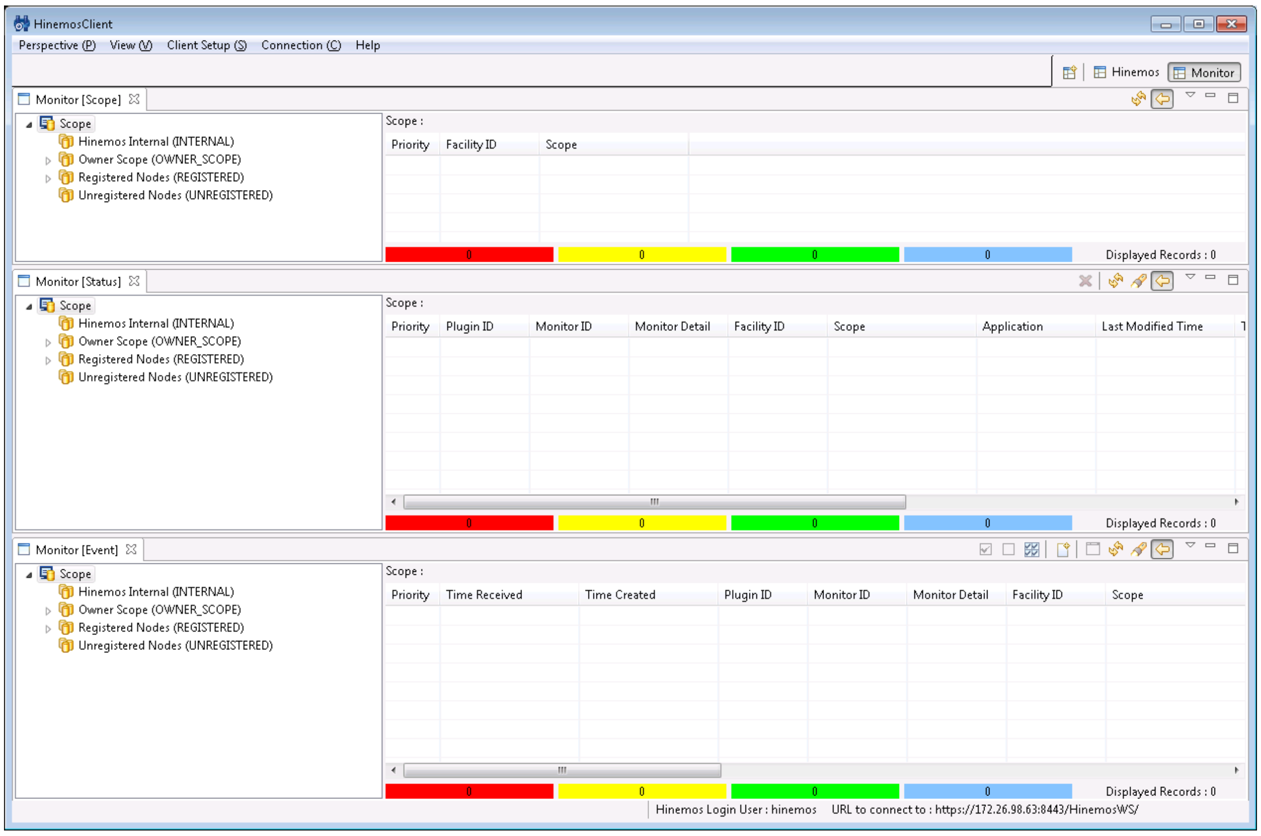


Figure 5-1 Initial Screen Structure

5.2.2 Monitor[Scope] View

The Monitor[Scope]view displays the scope status. The log and status information for each log are displayed in this view.

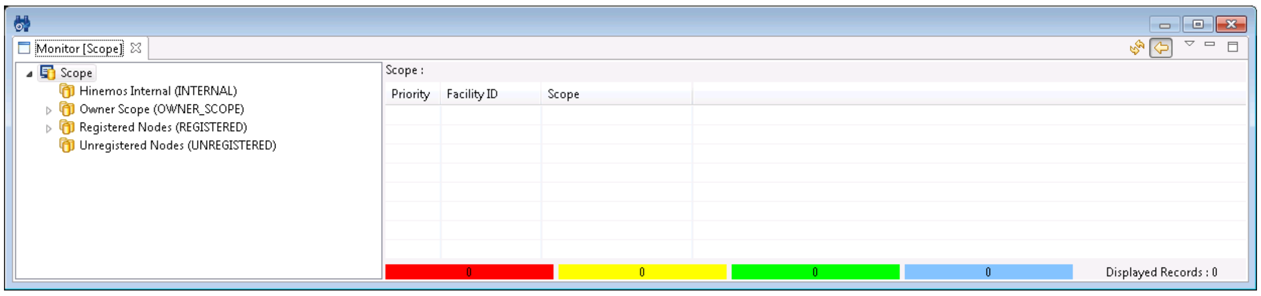

Monitor [Scope]
Scope
Hinemos Internal (INTERNAL)
Owner Scope (OWNER_SCOPE)
Registered Nodes (REGISTERED)
Unregistered Nodes (UNREGISTERED)
Scope :
Priority
Facility ID
Scope
0
0
0
0
Displayed Records : 0

Figure 5-2 Monitor[Scope] View

Table 5-1 Toolbar

Icon	Button name	Description
🔄	Update	Update the contents of the view with new information.
⇦	Show Scope Tree Pane	Select display/nondisplay of the scope tree.

At the bottom of the view, the total number of logs is displayed in different colors and counted by priority. Also, the total number of logs shown is displayed in "Displayed Records".

5.2.3 Monitor[Status] View

The Monitor[Status] view displays the scope status.

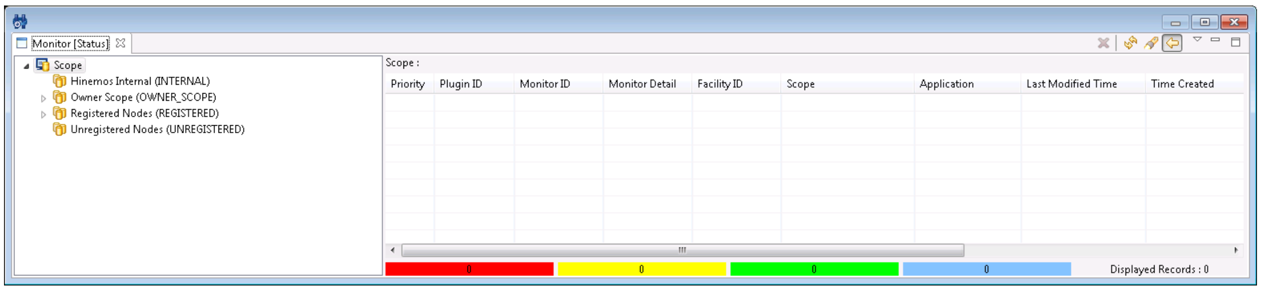


Figure 5-3 Monitor[Status] View

Table 5-2 Toolbar

Icon	Button name	Description
✖	Delete	Delete the status.
⟳	Update	Update the contents of the view with new information.
🖉	Filter	Perform filter monitoring for the status list.
⇦	Show Scope Tree Pane	Select display/nondisplay of the scope tree.

At the bottom of the view, the total number of logs is displayed in different colors and counted by priority. Also, the total number of logs shown is displayed in "Displayed Records".

5.2.4 Monitor[Event] View

The Monitor[Event] view displays the log information being collected.

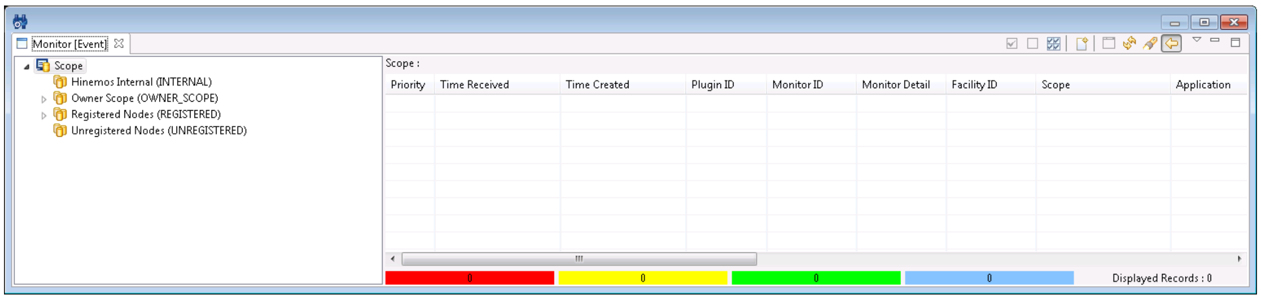


Figure 5-4 Monitor[Event] View

Table 5-3 Toolbar

Icon	Button name	Description
☑	Confirmed	Confirms the process of an event. The user running this process is saved as the confirmation user
□	Change to Unconfirmed	Change the "Confirmed" event to "Unconfirmed". The user running this process is saved as the confirmation user
☑☑	Confirm All	Confirm all events to which the condition applies.
🗋	Download	Output a list of events to a file.
▤	Detail	Display detailed contents of an event.
⟳	Update	Update the contents of the view with new information.
🖉	Filter	Performs a filter of the event list.
⇦	Show Scope Tree Pane	Select display/nondisplay of the scope tree.

At the bottom of the view, the total number of logs is displayed in different colors and counted by priority. Also, the total number of logs shown is displayed in "Displayed Records".

Copyright (c) 2013 NTT DATA CORPORATION

* The total number of event information displayed in the Monitor[Event] view is not the total number of event information stored in the Hinemos database.

* You can configure the maximum number of events to display in the Monitor[Event] view. Refer to Changing the Display Limits for Monitoring Screen Update Interval and History for each type of setting dialog condition.

5.3 Prerequisites for Usage

When performing settings in the monitor feature, the following setting must be performed beforehand.

- A monitoring target must be registered as a node and assigned to one of the scopes in the repository.
- The notification method must be configured and registered in the notification feature for monitor settings
- An calendar must be registered at first, in order to be referred to as the valid monitoring period of a monitor setting.
- A job must be registered beforehand in order to be used as job execution that triggered by notification.

5.4 Confirm the Monitor results in the Monitor[Scope] view

The aggregate status and event for each scope is displayed in the Monitor[Scope] view. When a scope is selected from the tree pane on the left side, the status of the selected scope is displayed. The scope with the highest priority from the selected scope is displayed on the right side (including the scope itself).

The displayed status and event information are:

- Status/event with the highest priority
- The last status/event output (if there are multiple status/event output with the same priority)

There are four levels of priority used in Hinemos.

- Critical … Displayed in red
- Warning … Displayed in yellow
- Info … Displayed in green
- Unknown … Displayed in light blue

Priority levels are:

Critical > Unknown > Warning > Info

5.5 Confirm the Monitor Results in the Monitor[Status] View

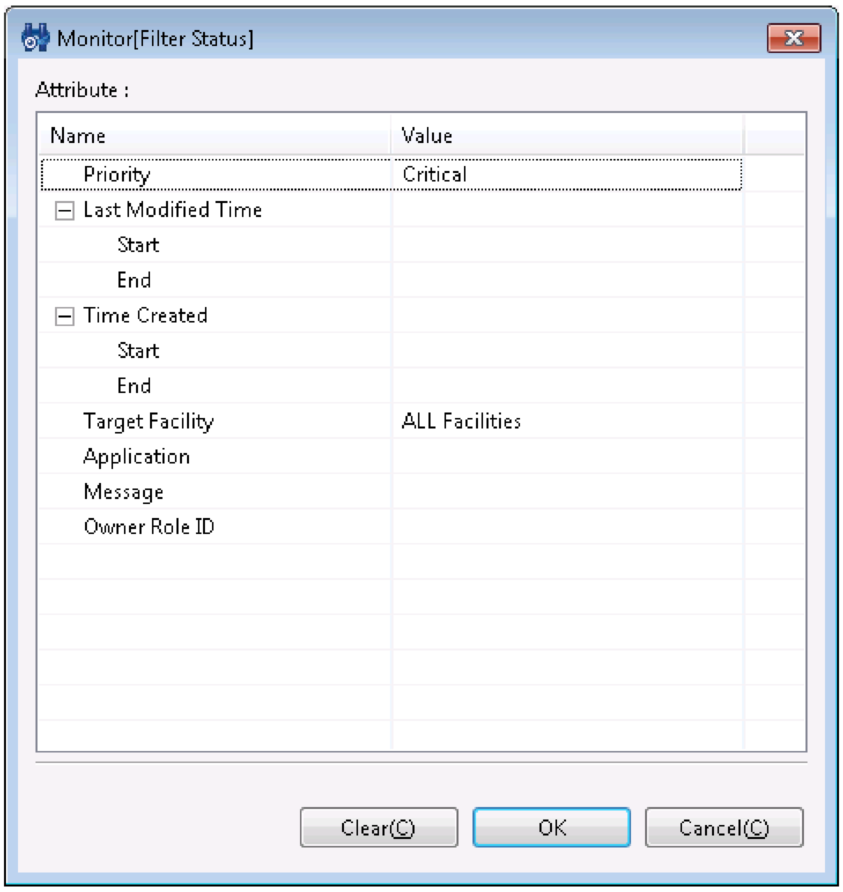
In the status monitoring feature, a list of notification information from the monitoring feature will be displayed as the status information for each scope. The information shown here is different than the information shown in the Monitor[Event] view. It always shows only the newest status. The status notification is identified by the "Plugin ID" and the "Monitor ID". When both "Plugin ID" and "Monitor ID" receive matching notification, the status will be updated.

5.5.1 Delete the Status Notification Results

In the Monitor[Status] view select the notification to delete, and then click on the "Delete" button.

5.5.2 Filtering of Status Notification Results

1. Click the "Filter" button in the Monitor[Status] view. The Monitor[Filter Status] dialog is displayed.



Attribute :

Name	Value
Priority	Critical
⊟ Last Modified Time	
Start	
End	
⊟ Time Created	
Start	
End	
Target Facility	ALL Facilities
Application	
Message	
Owner Role ID	

Figure 5-5 Monitor[Filter Status] Dialog

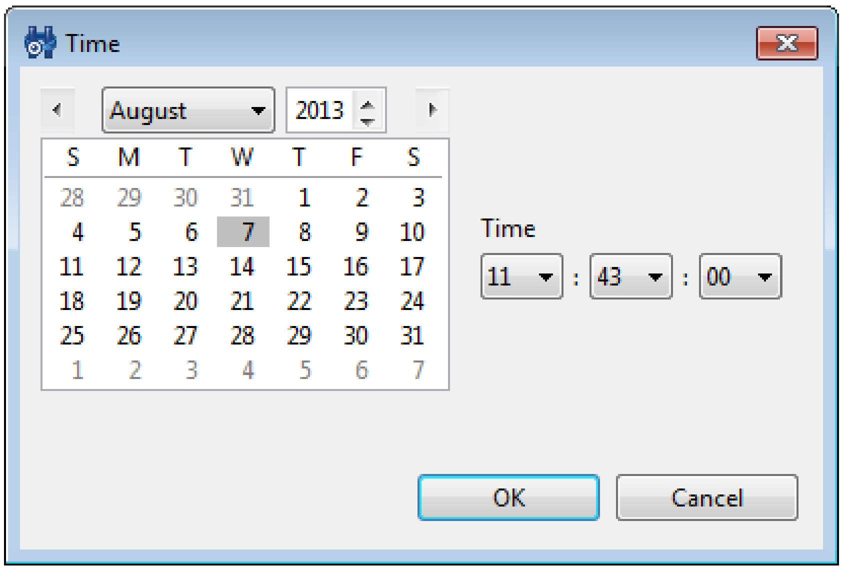
2. Configure the filter condition. When an item is not included in the condition, please leave the field blank. (Please click on the "Clear" button to change the filter conditions back to the default conditions).

- Priority:

  Make "Priority" a filter condition. Select the priority level from the combo box.

- Last Change Time:

  Make "Last Change Time" a filter condition. Clicking the button on the right side of the input field opens the time dialog. Please select a date. Select a time from the combo box.



August 2013

S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Time

11 : 43 : 00

Figure 5-6 Time Dialog

- Time Created:

  Make "Time Created" a filter condition. Clicking the button on the right side of the input field opens the time dialog. Please select a date. Select a time from the combo box.

- Target Facility:

  You can select the facility (scopes and nodes) to display.

  - ALL Facilities ... Display the selected scope and all nodes included in the selected scope
  - Sub-scope Facilities Only ... Display the selected scope and only the scope and the node included in the selected scope

- Application:

  Make "Application" a filter condition. Please enter alphanumeric text in the input field. The string entered here will be filtered.

- Message:

  Make" Message" a filter condition. Please enter alphanumeric text in the input field. The string entered here will be filtered.

- Owner Role ID :

  Specify an Owner Role ID as a filter condition. Please enter alphanumeric text in the input field. The results fully-matched with the input text will be shown.

3. Click the "OK" button. The Monitor[Filter Status] dialog closes, and only the notifications that met the configured conditions are displayed in the Monitor[Status] view.

The field displaying the scope will be renamed as the "Filtered List" and the icon will change to the "Filter" button pressed.

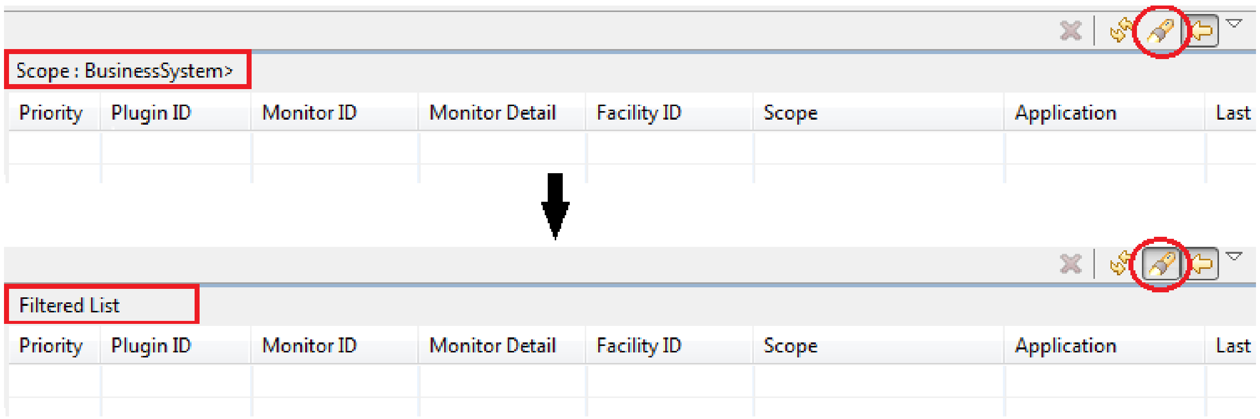


Figure 5-7 Filtered List

5.5.3 Delete Filtering of Status Notification Results

Click the (pressed) "Filter" button in the Monitor[Status] view.

5.5.4 Date Item Displayed in the Monitor[Status] View

The table below describes the Date item displayed in the Monitor[Status] view.

Table 5-4 Date Item in the Monitor[Status] View

Item	Target OS time	Description
Last Change Time	Hinemos Manager server	Display the time when the last monitoring was executed.
Time Created	Hinemos Manager server	Display the time when the first monitoring was executed. If the status information was once deleted, display the time when the first monitoring was executed after it was deleted. If the priority was changed and notified, display the time when the changed monitoring was executed.

5.6 Confirm the Monitor Results in the Monitor[Event] View

5.6.1 Confirmation of the Event Notification Results

Select the notification to be confirmed in the list of events in the Monitor[Event] view, and then click the "Confirmed" button. The confirmation flag of the specified notification is "Confirmed", and the user that executed the confirmation process is saved as the "Confirmation User".

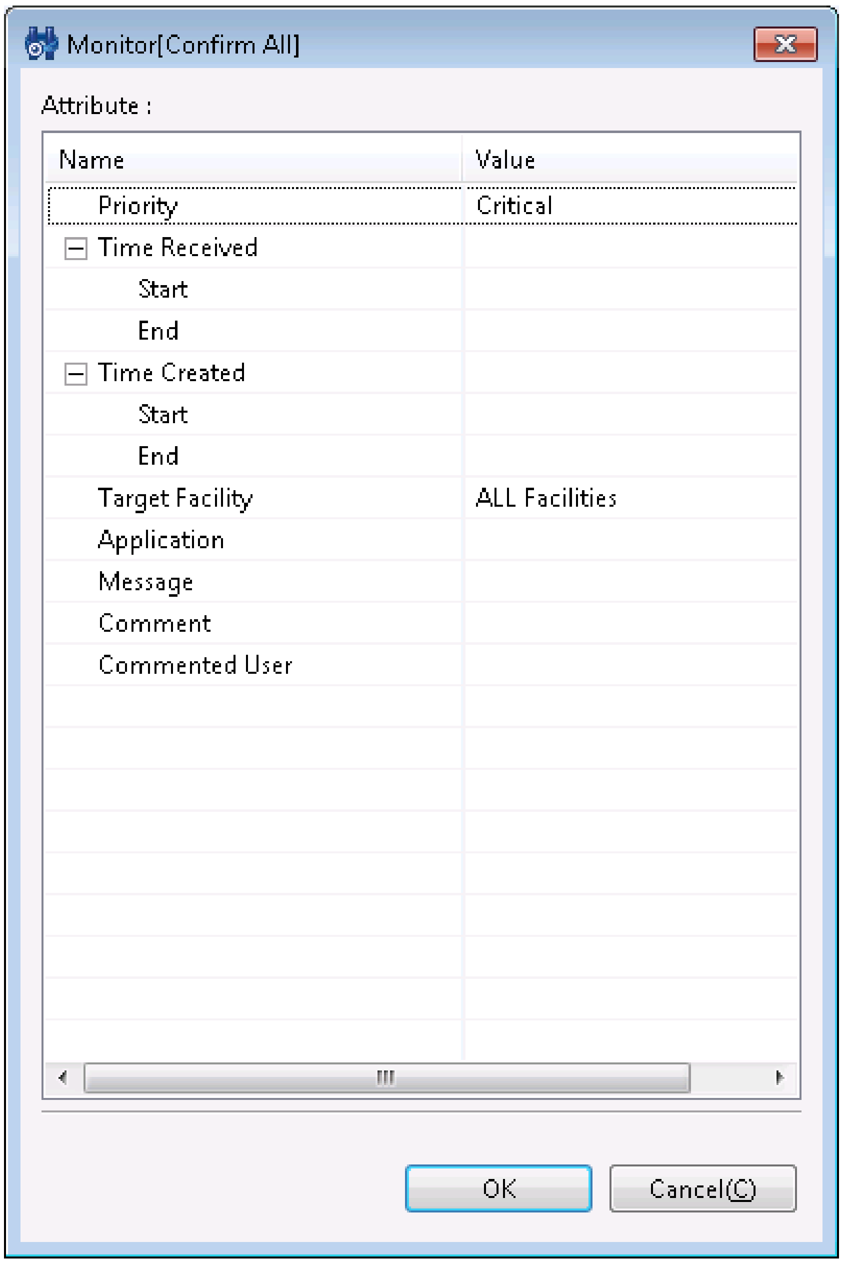
To change confirmed notification to unconfirmed

1. Configure the filtering in the Monitor[Event] view so that the unconfirmed notification is displayed in the list of events (Please refer to the section Filtering of Event Notification Results for the setting process).
2. Select the notification to change, and then click on the "Change Unconfirmed" button. The confirmation flag of the selected notification is "Unconfirmed", and the user that carries out this process is saved as the "Confirmation User".

Collectively confirm notifications that match the conditions

The Monitor[Confirm All] dialog is displayed when the "Confirm All" button in the Monitor[Event] view is clicked. Next, add refiners to filter specific content. The setting is same as the procedure for filtering (for details, please refer to Filtering of Status Notification Results).

The confirmation flag of the specified notifications is "Confirmed", and the user that carried out the confirmation process is saved as the "Confirmation User".



Monitor[Confirm All]

Attribute :

Name	Value
Priority	Critical
⊟ Time Received	
Start	
End	
⊟ Time Created	
Start	
End	
Target Facility	ALL Facilities
Application	
Message	
Comment	
Commented User	

Figure 5-8 Monitor[Confirm All] Dialog

Copyright (c) 2013 NTT DATA CORPORATION

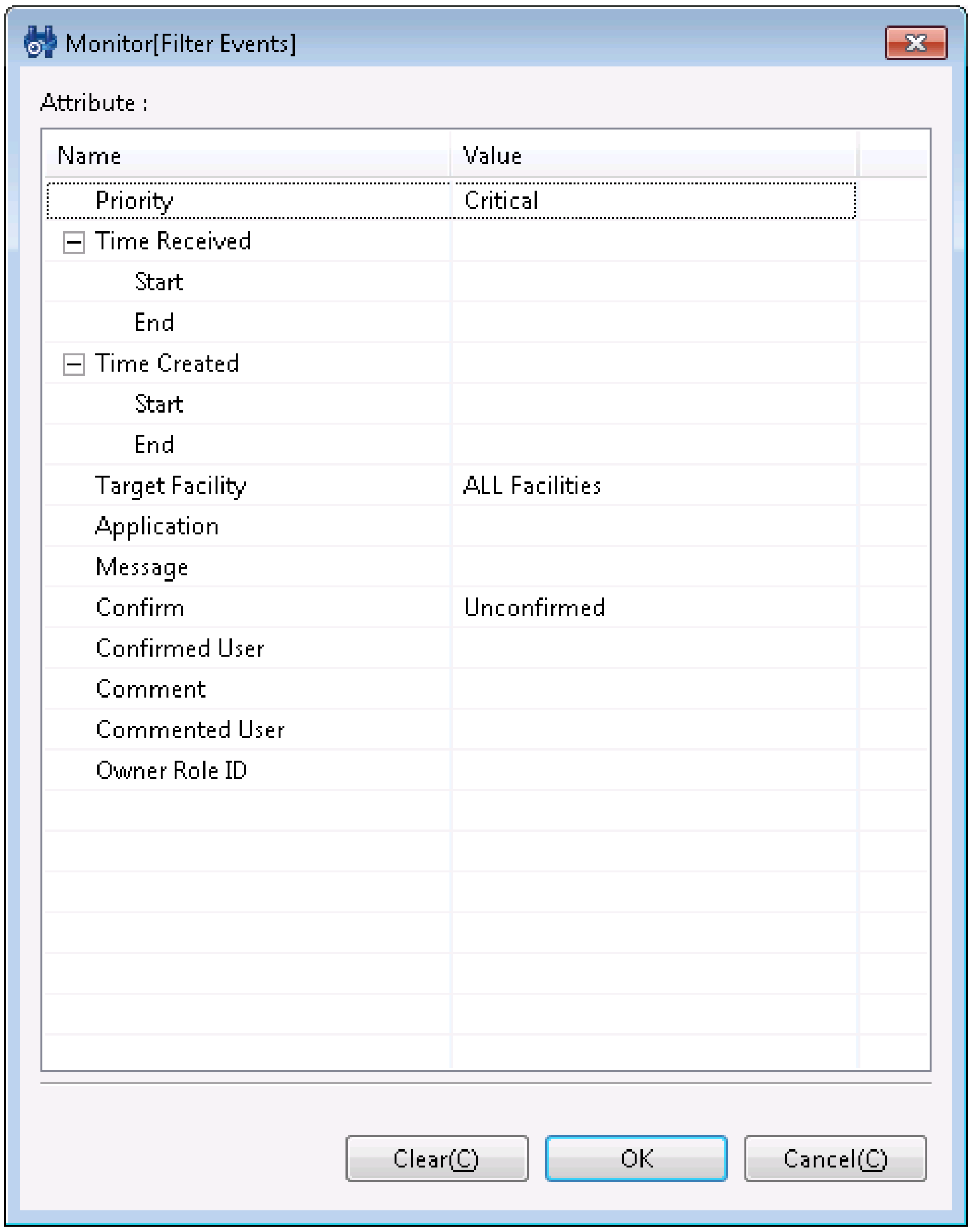
5.6.2 Filtering of Event Notification Results

The Monitor[Filter Events] dialog is displayed when the "Filter" button in the Monitor[Event] view is clicked. Next, s pecify the refiner. The setting method is similar to status filtering, but the following items can be specified as wel l. (Refer to the section Filtering of Status Notification Results for details)

- Confirmed:

  Specify the status of the confirmation flag. Specify "Unconfirmed" or "Confirmed" from the combo box.
- Confirmation User:

  Specify the user that carried out the confirmation process. Please enter alphanumeric text in the input field.



Monitor[Filter Events]

Attribute :

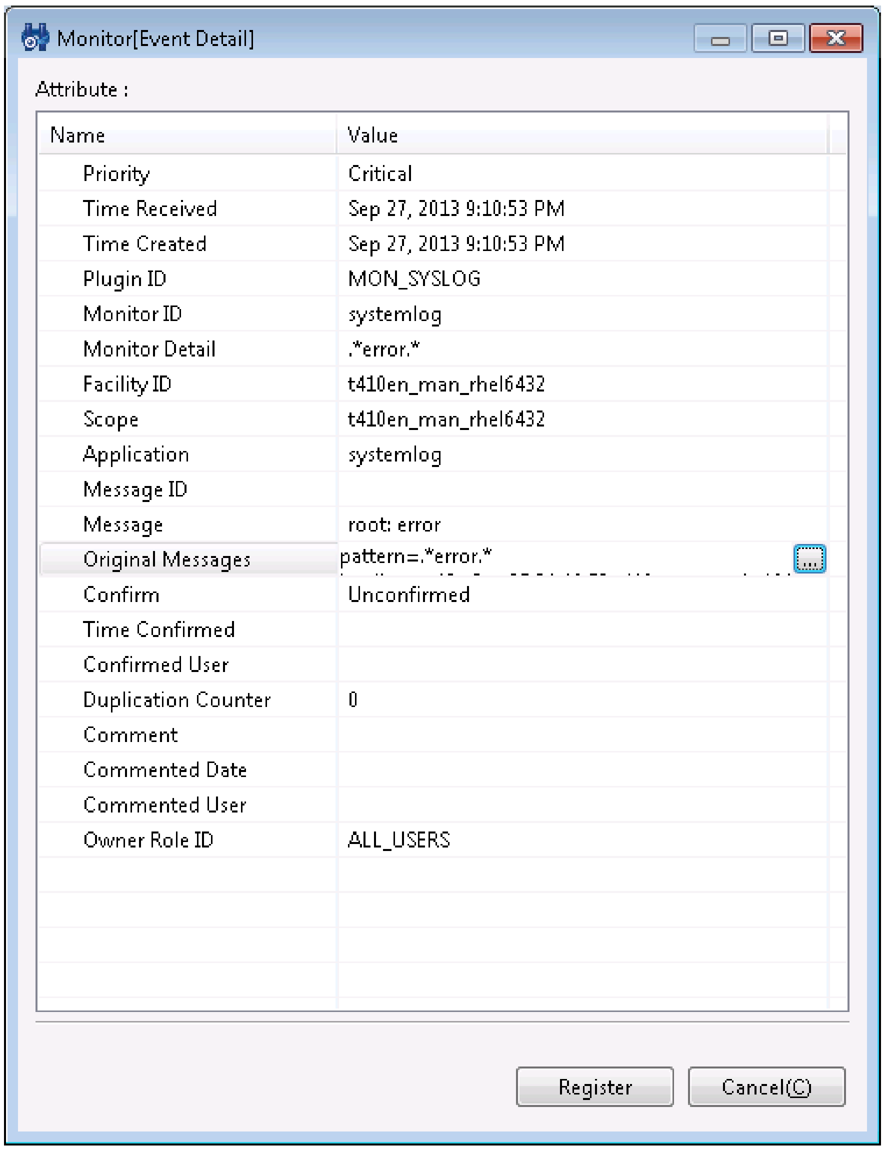
Name	Value
Priority	Critical
⊟ Time Received	
Start	
End	
⊟ Time Created	
Start	
End	
Target Facility	ALL Facilities
Application	
Message	
Confirm	Unconfirmed
Confirmed User	
Comment	
Commented User	
Owner Role ID	

Figure 5-9 Monitor[Filter Events] Dialog

5.6.3 Confirming Detailed Contents of Event Notification Results

Select an event from the list of events in the Monitor[Event] view, and then double-click on it or click the "Detail" button. The Monitor[Detail] dialog is displayed.

Copyright (c) 2013 NTT DATA CORPORATION



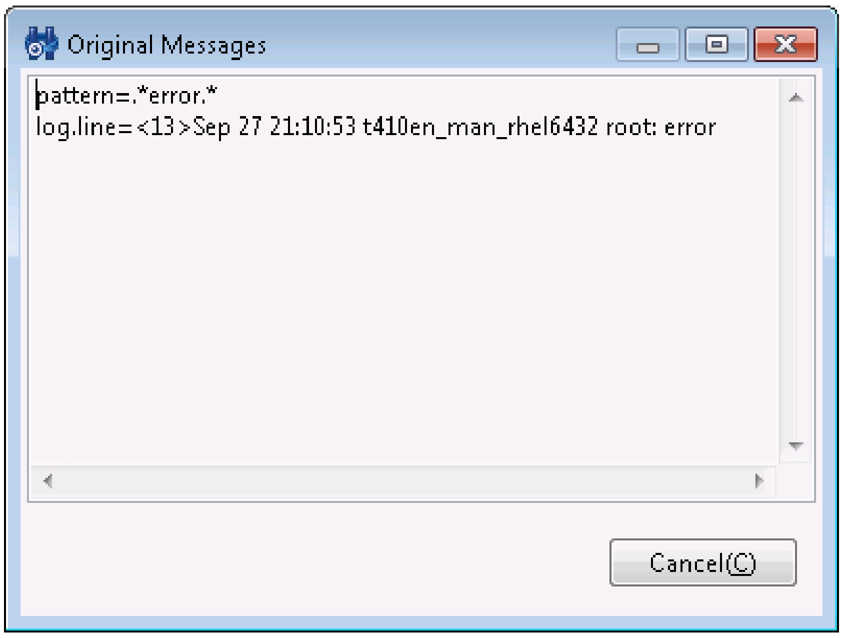
Attribute :

Name	Value
Priority	Critical
Time Received	Sep 27, 2013 9:10:53 PM
Time Created	Sep 27, 2013 9:10:53 PM
Plugin ID	MON_SYSLOG
Monitor ID	systemlog
Monitor Detail	.*error.*
Facility ID	t410en_man_rhel6432
Scope	t410en_man_rhel6432
Application	systemlog
Message ID	
Message	root: error
Original Messages	pattern=.*error.*
Confirm	Unconfirmed
Time Confirmed	
Confirmed User	
Duplication Counter	0
Comment	
Commented Date	
Commented User	
Owner Role ID	ALL_USERS

Figure 5-10 Monitor[Event Detail] Dialog

Confirming the original message

The "..." button is displayed on the far right when the "Original Messages" field in the Monitor[Detail] dialog is selected. The original Messages dialog is displayed when this button is clicked, and the original message is confirmed.



```
pattern=.*error.*
log.line=<13>Sep 27 21:10:53 t410en_man_rhel6432 root: error
```

Figure 5-11 Original Messages Dialog

If strings starting with the following URL schemes are included in the original messages, the browser is launched when the string is clicked, and then the relevant page (file) is displayed.

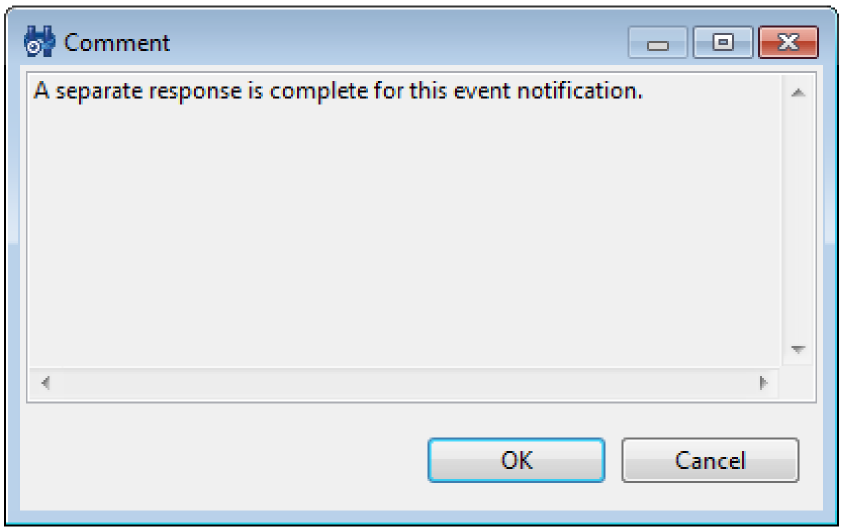
Copyright (c) 2013 NTT DATA CORPORATION

- **http://**
- **https://**
- **ftp://**
- **file://**

Adding comments to the Event Notification Results

You can add a comment for each event notification result.

1. A "..." button is displayed on the far right when the "Comment" field in the Monitor[Event Detail] dialog is sele cted. A comment input dialog is displayed when you click this button to add or edit comments.
2. Click the "OK" button in the comment dialog, then close the comment dialog.
3. When you click the "Register" button in the Monitor[Event Detail] dialog, the comment is registered.



A separate response is complete for this event notification.

Figure 5-12 Comment Input Dialog

5.6.4 Report Output of the Event Notification Results

The event notification results can be output to a file. The event information is output in CSV format.

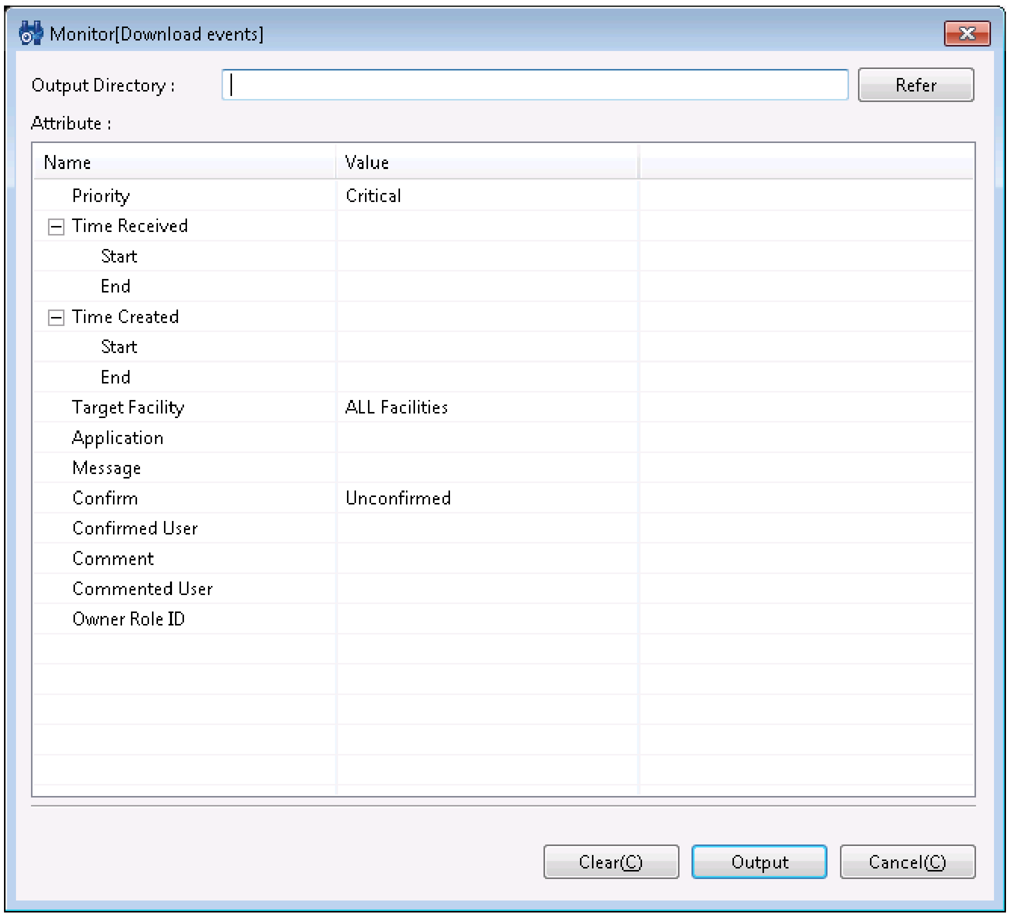
Note) The maximum number of event information downloads is limited. (Refer to section 5.1.1 "Setting the Maximum Download Conditions" in the Administrator's Guide for details.)

You can output a report using the following procedures.

1. Click the "download" button in the Monitor[Event] view. The monitor[Download events] dialog will be displayed.
2. Enter the destination file.
3. Specify the refiner for the output event. The setting method is similar to the procedure for filtering events (For details, please refer to the section Filtering of Event Notification Results)
4. Click on the "Output" button.

Configured refiner can be cleared by clicking on the "Clear" button.

Copyright (c) 2013 NTT DATA CORPORATION



Output Directory :

Attribute :

Name	Value
Priority	Critical
Time Received	
Start	
End	
Time Created	
Start	
End	
Target Facility	ALL Facilities
Application	
Message	
Confirm	Unconfirmed
Confirmed User	
Comment	
Commented User	
Owner Role ID	

Figure 5-13 Monitor[Download events] Dialog

5.6.5 Date Item for the Event Monitor

The table below describes the date items displayed in the Monitor[Event] view.

Table 5-5 Data Items in the Monitor[Event] View

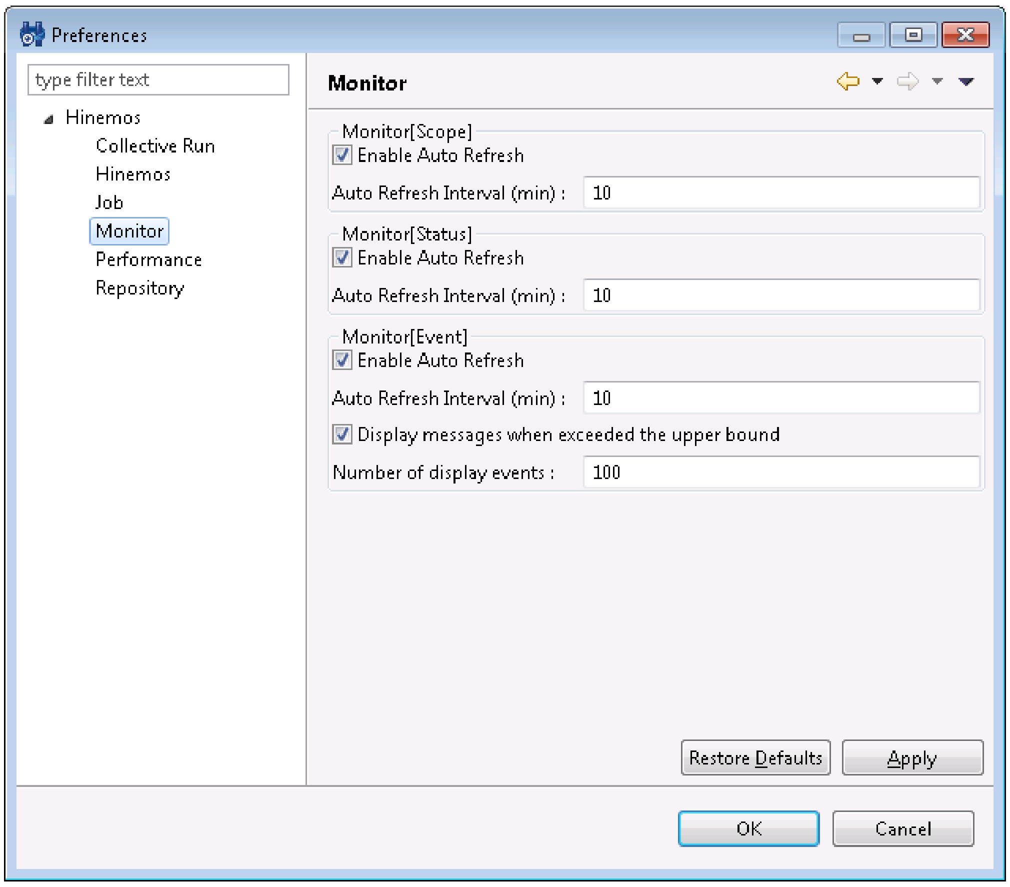
Time	Target OS time	Description
Time Received	Hinemos Manager server	Display the time when an event was stored in the managed DB (PostgreSQL) from the Hinemos Manager side.
Time Created	Hinemos Manager server (Other than System Log Monitor and Logfile Monitor), Target server (For System Log Monitor and Logfile Monitor)	Display the time when monitored. In general, this time is the time of the Hinemos Manager server because it is monitored by the Hinemos Manager. For the System Log Monitor, the log output time in the system log packet will be used. For the Logfile Monitor, the time of sending log, which is detected by Hinemos Agent and sent to Hinemos Manager, will be used. Similarly SNMPTRAP Monitor is a method for monitoring the receive type, but with SNMPTrap, the Hinemos Manager server receive time is used.

5.7 Changing the Display Limits for Monitoring Screen Update Interval and History

The screen information is updated regularly by obtaining manager information from the client at regular intervals. Update interval can be changed by the following procedures.

1. Select "Client Setup" - "Setup" from the menu bar. The preferences dialog is displayed.

Copyright (c) 2013 NTT DATA CORPORATION



Monitor

Monitor[Scope]

☑ Enable Auto Refresh

Auto Refresh Interval (min) : 10

Monitor[Status]

☑ Enable Auto Refresh

Auto Refresh Interval (min) : 10

Monitor[Event]

☑ Enable Auto Refresh

Auto Refresh Interval (min) : 10

☑ Display messages when exceeded the upper bound

Number of display events : 100

Figure 5-14 Preferences Dialog

2. Select Hinemos - Monitor in the tree pane on the left side.
3. The following setting can be made for each Monitor[Scope] view. You can perform the following various settings.

- Enable Auto Refresh:

  The contents of the view will be updated at the specified auto refresh interval when this check box is checked. If unchecked, the contents will not be updated unless the "Update" button is clicked.

- Auto Refresh Interval (min):

  If Auto Refresh is enabled, specify the refresh interval in minutes.

In addition, it is possible to set the limit for items to display related to the Monitor[Event] view.

- Display messages when the upper bound is exceeded:

  Output message if this check box is checked and if accumulated number of events exceeds the specified number of display events. If unchecked, a message will not be output even if the number of events exceeds the number of display events.

- Number of display events:

  Specify the number of histories displayed at once.

Copyright (c) 2013 NTT DATA CORPORATION

6 Monitor Settings Feature

6.1 Overview

This is a feature for centralized management of the monitor settings. You can confirm the various monitor settings that are set in a list, and add, change or delete the monitor settings. Also, with this feature you can add, change or delete the notification settings that define the notification method for monitor results. The main features that can be set for the Monitor Settings Perspective are as follows.

- Monitor Settings Feature

  This is a feature to set up the Monitor. Monitoring of log information and status information for monitored nodes in each Scope prepared in advance can be set up in the Hinemos Repository Management feature. You can perform notification and confirmation of the monitor results in various locations, based on the setting and with the notification method designated in the notification feature. Also, the monitor results can be accumulated by performance value through numeric monitoring (Refer to Numeric Monitoring for details) and the result can be displayed as a graph in the Performance Management feature or downloaded in CSV format.

- Notification Feature

  This is a feature to set up the notification method for the monitor results. The method and details of notification and the notification destination can be specified for each level of monitor results priority, based on the monitor settings.

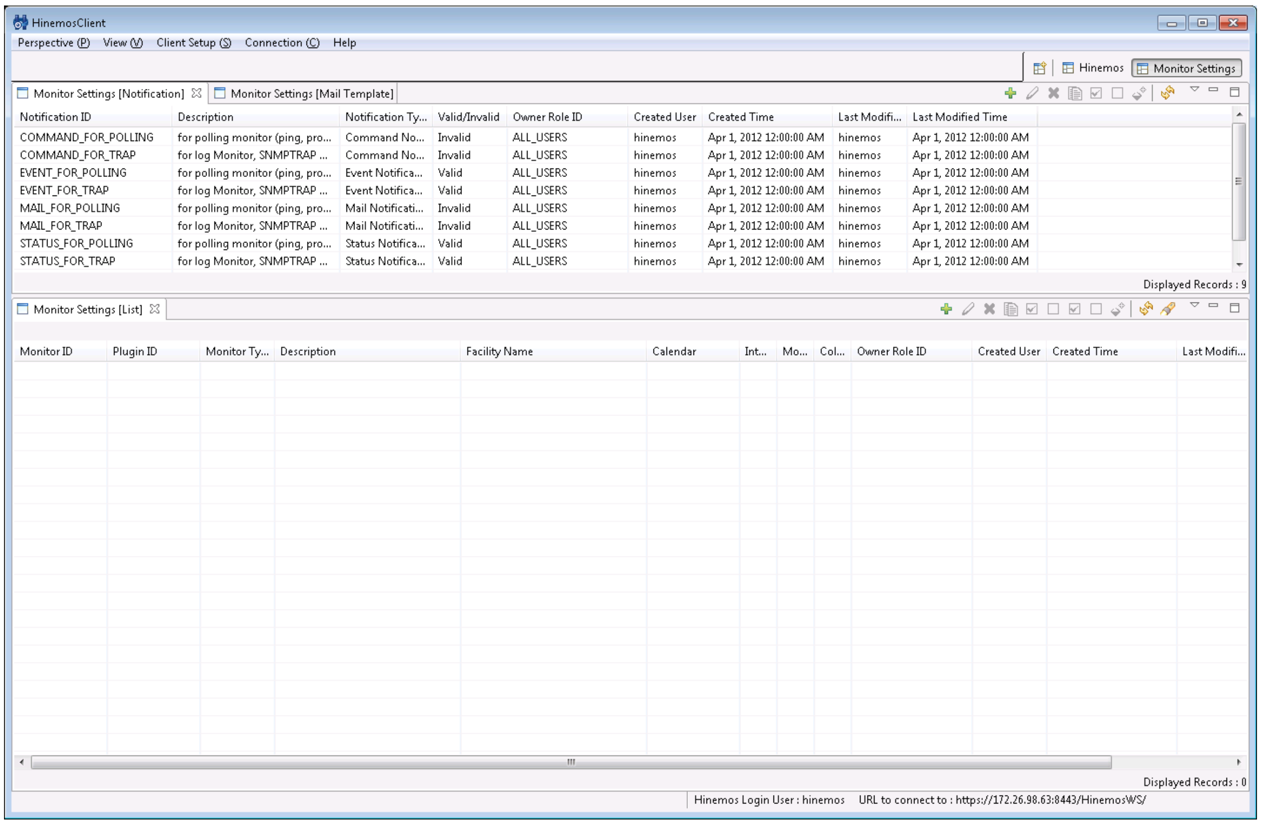
- Mail Template Feature

  This feature specifies the e-mail style when the monitor results are notified by e-mail based on the monitor results. Specific monitor result details can be included with the use of fixed variables in the e-mail content.

Refer to the next section for details on each of the monitor settings.

6.2 Interface Composition

6.2.1 Default Interface



Notification ID	Description	Notification Ty...	Valid/Invalid	Owner Role ID	Created User	Created Time	Last Modifi...	Last Modified Time
COMMAND_FOR_POLLING	for polling monitor (ping, pro...	Command No...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
COMMAND_FOR_TRAP	for log Monitor, SNMPTRAP ...	Command No...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
EVENT_FOR_POLLING	for polling monitor (ping, pro...	Event Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
EVENT_FOR_TRAP	for log Monitor, SNMPTRAP ...	Event Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
MAIL_FOR_POLLING	for polling monitor (ping, pro...	Mail Notificati...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
MAIL_FOR_TRAP	for log Monitor, SNMPTRAP ...	Mail Notificati...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
STATUS_FOR_POLLING	for polling monitor (ping, pro...	Status Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
STATUS_FOR_TRAP	for log Monitor, SNMPTRAP ...	Status Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM

Displayed Records : 9

Monitor ID	Plugin ID	Monitor Ty...	Description	Facility Name	Calendar	Int...	Mo...	Col...	Owner Role ID	Created User	Created Time	Last Modifi...

Displayed Records : 0

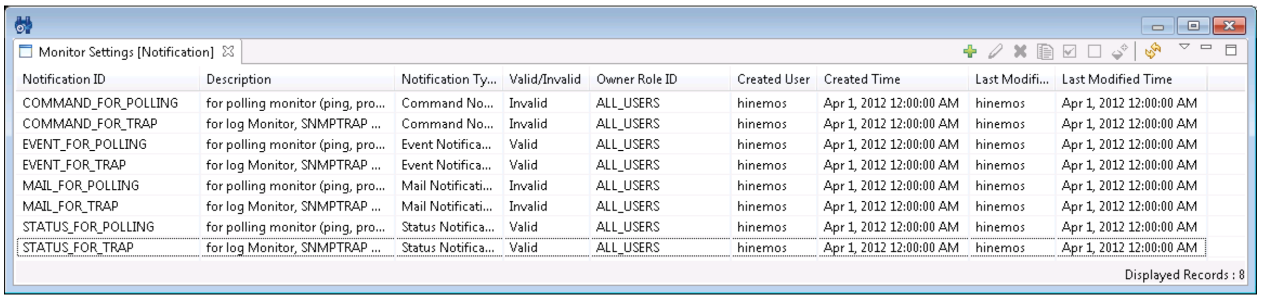
Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 6-1 Default Interface of Monitor Settings Feature

Copyright (c) 2013 NTT DATA CORPORATION

6.2.2 Monitor Settings[Notification] View

The registered notification settings can be viewed as a list. In this view, you can create, change or delete notification information, enable settings, disable settings and perform operations related to notification setting information.



Monitor Settings [Notification]

Notification ID	Description	Notification Ty...	Valid/Invalid	Owner Role ID	Created User	Created Time	Last Modifi...	Last Modified Time
COMMAND_FOR_POLLING	for polling monitor (ping, pro...	Command No...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
COMMAND_FOR_TRAP	for log Monitor, SNMPTRAP ...	Command No...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
EVENT_FOR_POLLING	for polling monitor (ping, pro...	Event Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
EVENT_FOR_TRAP	for log Monitor, SNMPTRAP ...	Event Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
MAIL_FOR_POLLING	for polling monitor (ping, pro...	Mail Notificati...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
MAIL_FOR_TRAP	for log Monitor, SNMPTRAP ...	Mail Notificati...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
STATUS_FOR_POLLING	for polling monitor (ping, pro...	Status Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
STATUS_FOR_TRAP	for log Monitor, SNMPTRAP ...	Status Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM

Displayed Records : 8

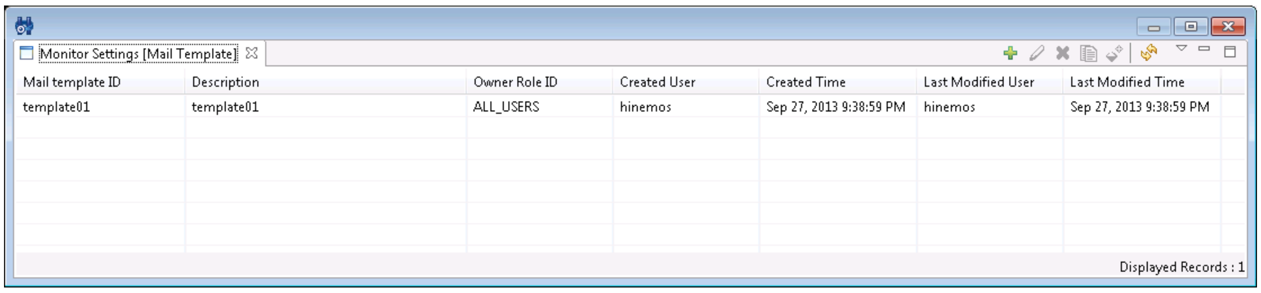
Figure 6-2 Monitor[Notification] View

Table 6-1 Toolbar

Icon	Button name	Description
✚	Create	Create a new notification setting.
✎	Change	Change the selected notification setting.
✖	Delete	Delete the selected notification setting.
📄	Copy	Copy the selected notification setting.
☑	Valid	Enable the selected notification setting.
□	Invalid	Disable the selected notification setting.
◆	Object Privilege Settings	Configure object privilege for the selected notification setting.
⟳	Update	Update the table contents with the latest information.

6.2.3 Monitor Settings[Mail template] View

The registered mail templates can be viewed as a list. In this view, you can perform operations related to the mail template setting operation, such as registering, changing or deleting, etc., the mail templates.



Monitor Settings [Mail Template]

Mail template ID	Description	Owner Role ID	Created User	Created Time	Last Modified User	Last Modified Time
template01	template01	ALL_USERS	hinemos	Sep 27, 2013 9:38:59 PM	hinemos	Sep 27, 2013 9:38:59 PM

Displayed Records : 1

Figure 6-3 Monitor Settings[Mail template] View

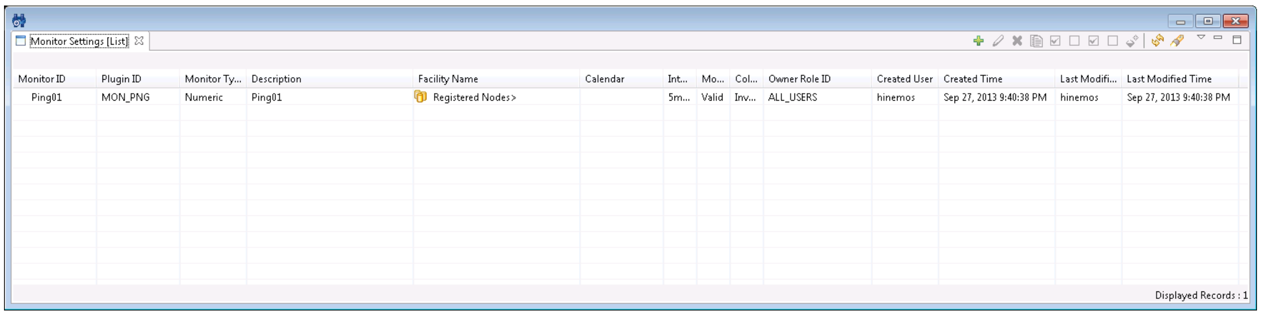
Table 6-2 Toolbar

Icon	Button name	Description
✚	Create	Create a new mail template.
✎	Change	Change the selected mail template.
✖	Delete	Delete the selected mail template.
📄	Copy	Copy the selected mail template.
◆	Object Privilege Settings	Configure object privilege for the selected mail template.
⟳	Update	Update the table contents with the latest information.

Copyright (c) 2013 NTT DATA CORPORATION

6.2.4 Monitor Settings[List] View

The registered Monitor Settings can be viewed as a list. In this view, you can create, change or delete monitor information, enable settings, disable settings and perform operations related to monitor setting information.



Monitor ID	Plugin ID	Monitor Ty...	Description	Facility Name	Calendar	Int...	Mo...	Col...	Owner Role ID	Created User	Created Time	Last Modifi...	Last Modified Time
Ping01	MON_PNG	Numeric	Ping01	Registered Nodes>		5m...	Valid	Inv...	ALL_USERS	hinemos	Sep 27, 2013 9:40:38 PM	hinemos	Sep 27, 2013 9:40:38 PM

Displayed Records : 1

Figure 6-4 Monitor Settings[List] View

Table 6-3 Toolbar

Icon	Button name	Description
✚	Create	Create a new monitor setting.
✎	Change	Change the selected monitor setting.
✖	Delete	Delete the selected monitor setting.
📄	Copy	Copy the selected monitor setting.
☑	Valid	Enable the selected monitor setting.
□	Invalid	Disable the selected monitor setting.
☑	Collection Settings	Enable the selected collection strings.
□	Collection Settings	Disable the selected collection strings.
◆	Object Privilege Settings	Configure object privilege for the selected monitor setting.
⟳	Update	Update the table contents with the latest information.
✎	Filter	Filter the displayed monitor Settings list.

6.3 Notification Feature

6.3.1 Overview

In the notification feature, there is a feature to set the notification method for the monitor results of each monitor feature and for the job execution results. This feature enables display of the monitoring results for each monitor feature and information for the job execution results on the Monitor Settings Perspective, and e-mail notification. Also, you can register a job or run commands according to the monitoring results and job execution results.

With the notification feature, you can specify and save various notification methods. The saved notification information can be referenced and used as a "Template" when notification is performed in the various Hinemos features. When the notification settings designated in the notification feature are specified in the monitor setting or the job setting side, use the "Notification ID" for the notification setting registered in the notification feature.

The following six notification methods can be set in the notification feature.

- Status Notification
- Event Notification
- Mail Notification
- Job Notification
- Log Escalation Notification
- Command Notification

Copyright (c) 2013 NTT DATA CORPORATION

6.3.2 Status Notification

Status notification is a notification feature you can use when you want to confirm the monitor results for each monitor feature and the latest status of the job execution results from the Hinemos Client. Normally, you would use this when you want to confirm the monitor results for each monitor feature and the latest status of the job execution results in real time.

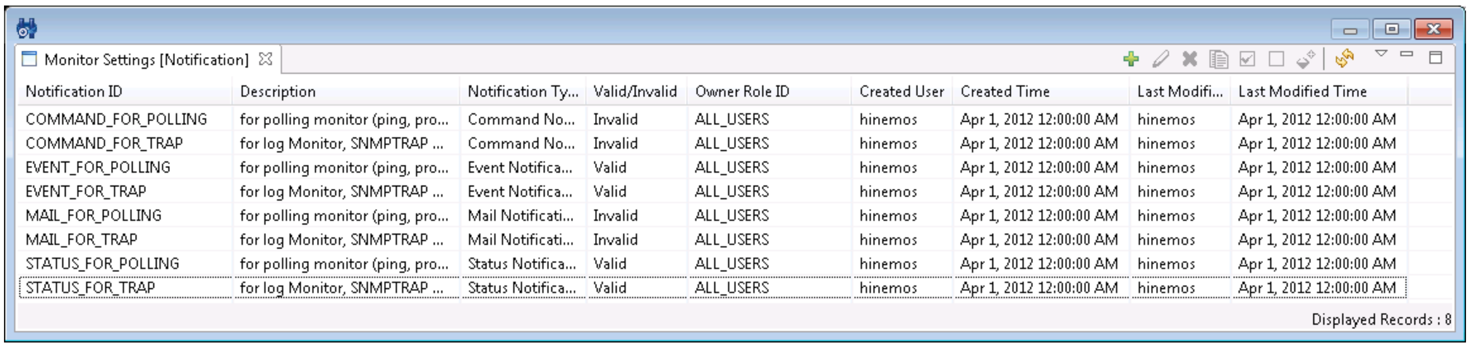
The status notification results are displayed in the Monitor[Status] view. In the notification information displayed in the Monitor[Status] view, the notification information is always overwritten with the latest monitor results and job execution results, etc.

The method for creating new status notification settings is as follows:

1. Open Monitor Settings Perspective.
2. Click the "Create" button in the upper right part of the Monitor Settings[Notification] view; the "Notification Type dialog opens.
3. Select Status Notification, then click the "next" button.
4. Make an entry in the Notification (Status) [Create - Change] dialog and click the "OK button.

Also, The method for changing/deleting an existing status notification settings is as follows:

1. Open Monitor Settings Perspective.
2. Select the existing setting from the Monitor Settings [Notification] view and click the "Modify" / "Delete" button in the upper right part.
3. To make a change, change the input value in the Notification (Status) [Create - Change] dialog and click the " OK button.



Monitor Settings [Notification]

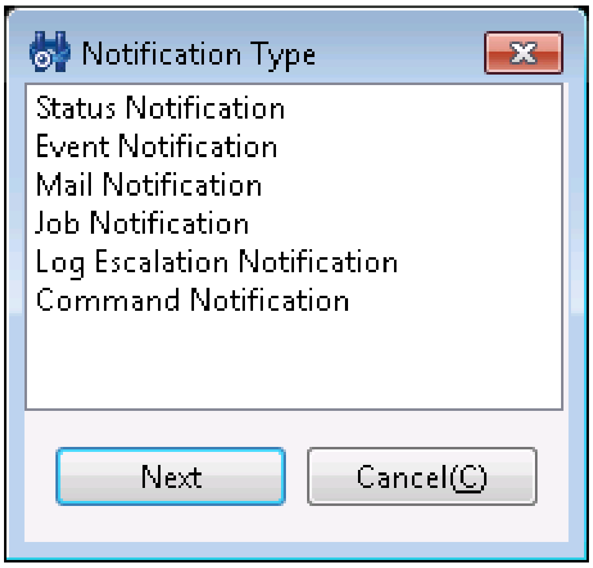
Notification ID	Description	Notification Ty...	Valid/Invalid	Owner Role ID	Created User	Created Time	Last Modifi...	Last Modified Time
COMMAND_FOR_POLLING	for polling monitor (ping, pro...	Command No...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
COMMAND_FOR_TRAP	for log Monitor, SNMPTRAP ...	Command No...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
EVENT_FOR_POLLING	for polling monitor (ping, pro...	Event Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
EVENT_FOR_TRAP	for log Monitor, SNMPTRAP ...	Event Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
MAIL_FOR_POLLING	for polling monitor (ping, pro...	Mail Notificati...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
MAIL_FOR_TRAP	for log Monitor, SNMPTRAP ...	Mail Notificati...	Invalid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
STATUS_FOR_POLLING	for polling monitor (ping, pro...	Status Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
STATUS_FOR_TRAP	for log Monitor, SNMPTRAP ...	Status Notifica...	Valid	ALL_USERS	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM

Displayed Records : 8

Figure 6-5 Monitor Settings [Notification] View

Registering Notification Settings

1. Click the "Add" button from the Monitor Settings [Notification] view. The Notification Type dialog box will open.



Notification Type

Status Notification
Event Notification
Mail Notification
Job Notification
Log Escalation Notification
Command Notification

Figure 6-6 Notification Type Dialog

2. Select Status Notification, then click the "next" button. The Notification(Status)[Create/Change] dialog opens.

3. Configure the following items.

- Notification ID:

  Enter the notification ID as text. This will be used as an ID to identify which notification feature to use for the monitor and job settings.

- Description:

  Enter a description of the notification setting as text.

- Owner Role ID:

  Select an Owner Role ID for the notification setting. Refer to Account Feature section for more details about Owner Role.

- Initial notification after priority changes:

  - Notify for the first time if the monitoring results are consecutively set at the same priority for more than 0 times

    You can specify the timing of the initial notification. After the priority of monitor results for the monitored node changes, notification first occurs when the same priority continues for the specified number of times (if 1 is specified, notification occurs immediately when a priority changes). However, there will be no notification when the priority of the previous notification and the priority of the monitor results after the current change are the same.

- Second and later notifications after the priority change:

  You can specify a suppression method when the priority results are the same as the monitor results. Select from the following three suppression methods.

  - Always notify

    Notification is not suppressed even if the notification results are the same priority.

  - Do not notify for 0 minute(s) when notification priority is same as previous.

    Notification will not be made for the specified period if notice is given once, followed by monitor results with the same priority. Please enter the suppression time period in minutes in the text box.

  - Do not notify

    Notification will not be made as long as the priority does not change, if notice is given once, followed by monitor results with the same priority.

  In addition, use the following keys to determine the notification suppression.

  - Monitor Type
  - Monitor ID
  - Monitor Detail (The value saved differs for each monitor feature. Refer to the values in Table 6-4 Monitor Detail for details.)
  - Notification ID
  - Facility ID
  - Priority

Table 6-4 Monitor Detail Values

Monitor Function	Monitor Detail
Hinemos Agent Monitor	(blank)
Ping Monitor	(blank)
HTTP Monitor (Numeric)	(blank)
HTTP Monitor (String)	Pattern Matching Expression
SQL Monitor (Numeric)	(blank)
SQL Monitor (String)	Pattern Matching Expression
Process Monitor	(blank)

Windows Service Monitor	(blank)
Service Port Monitor	(blank)
Resource Monitor	Device Name
SNMP Monitor (Numeric)	(blank)
SNMP Monitor (String)	Pattern Matching Expression
Custom Monitor	Device Name
System Log Monitor	Pattern Matching Expression
Logfile Monitor	Pattern Matching Expression
SNMPTRAP Monitor	"OID"_"Generic ID"_"Specific ID"
Windows Event Monitor	Pattern Matching Expression

- Status Notification:

  Please check the priority check boxes for the status notification.

- Duration of Status Information:

  Please select the duration period for status information.

- Process after duration:

  Status information that has passed the duration period can be processed by the following two methods.

  - Delete the record

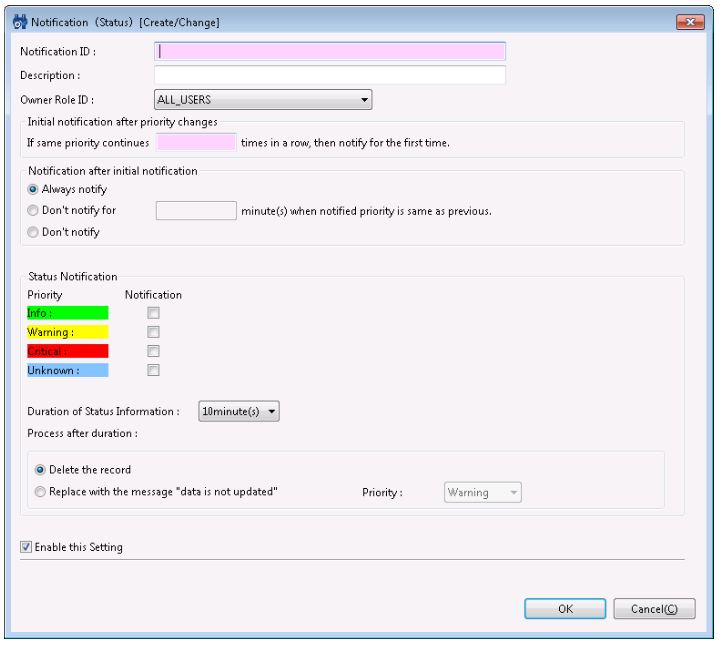
    After the duration period has passed, the status information is deleted from the Monitor[Status] view.

  - Replace with the message "data is not updated"

    When the duration period has passed, the display contents of the status information is replaced with the message "data is not updated". At that time, the priority can be changed. Please select the priority to change.

- Enabling this Setting:

  When checked, the notification setting selected in each monitoring feature and the Job Management feature is valid. If unchecked, the setting is disabled, and although the setting is saved, the notification process will not be executed.



Notification (Status) [Create/Change]

Notification ID :

Description :

Owner Role ID : ALL_USERS

Initial notification after priority changes

If same priority continues times in a row, then notify for the first time.

Notification after initial notification

● Always notify

○ Don't notify for minute(s) when notified priority is same as previous.

○ Don't notify

Status Notification

Priority	Notification
Info :	□
Warning :	□
Critical :	□
Unknown :	□

Duration of Status Information : 10minute(s)

Process after duration :

● Delete the record

○ Replace with the message "data is not updated" Priority : Warning

☑ Enable this Setting

Figure 6-7 Notification (Status) [Create/Change] Dialog

4. Click the "OK" button. The newly created setting will be added to the notification list.

Changing Notification Settings

1. Select the field to change in Monitor Settings [Notification], then click the "Modify" button. The Notification(Status)[Create/Change] dialog opens.
2. Edit the setting details, and then click the "OK" button. (refer to "Registering Notification Settings" for the procedures for entering settings)

Deleting Notification Settings

1. Select the field to delete in Monitor Settings [Notification], then click the "Delete" button.

Changing the Valid/Invalid Setting in the Notification Settings

1. The valid/invalid settings can be collectively changed in the notification settings. Select the setting to change from the settings list (can select multiple), then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

Table 6-5 Configuration Items of Notification(Status)

Configuration item			Input type	Description
Notification ID			Text	Enter an ID to identify the notification setting.
Description			Text	Enter a description of the notification setting.
Owner Role ID			Select from list	Select an Owner Role ID for the notification setting.
Initial notification after priority changes			Numeric	Enter the suppression setting for when the same notification information continues to occur.
Second or later notification after the priority change			Select with the radio button (part text)	Enter the notification method for the second or later time when the same notification information continues to occur. · Always notify Select when not suppressing the second or later notification. · Do not notify for the same priority for 0 minutes after the previous notification Select when suppressing by time the second or later notification. · Do not notify Select when not performing a second or later notification.
Status Notification	Notification (Information / Warning / Critical / Unknown)		Checkbox	Select the priority for notification.
	Duration of Status Information		Select from list	Select duration period of the status information.
	Handling after duration has passed	Delete the information/ Replace with message that is not updated	Select with the radio button	Select the process method for status information that has exceeded the duration period. · Delete the information Delete from Monitor[Status] view when the duration period has passed · Replace with the message "Not updated" When the duration period has passed, replace the display contents of status information with the message "Not updated",
		Priority	Select from list	If selecting "Replace with the message data is not updated" , replace the message with the priority here.
Enable this setting			Checkbox	Check to enable notification settings. It will return to the same setting if not checked and notification will not be performed.

Notification example

The following shows an example of notification settings and whether there is notification or not.

Table 6-6 Example 1 of Notification Settings and Whether There Is Notification or Not

	Initial notification	Continued from the first time		Continued from the second time	
	Second or later notification	Always notify	Do not notify	Do not notify	Do not notify
	Notification priority	All	All	All	Warning, Critical, Unknown
Time (Minutes)	Priority	-	-	-	-
0	Information	o	o	-	-
5	Information	o	-	o	-
10	Information	o	-	-	-
15	Warning	o	o(*1)	-*2	-
20	Information	o	o	-	-
25	Information	o	-	-	-
30	Information	o	-	-	-
35	Critical	o	o	-	-
40	Critical	o	-	o	o
45	Critical	o	-	-	-
50	Information	o	o	-	-
55	Information	o	-	o	-
Note		Not recommended because it increases the load on Hinemos	Notification only when changed However, cases such as *1 with a momentary resource surplus will also be detected.	Polling group monitor is recommended (*3)	Polling group monitor is recommended (*3)

o : Notification will be sent; - : Notification will not be sent

*2: There is no notification because the warning did not continue two or more times.

*3: Polling group monitoring is Hinemos Agent Monitor, HTTP Monitor, Ping Monitor, SNMP Monitor, SQL Monitor, Windows Service Monitor, Custom Monitor, Service Port Monitor, Process Monitor and Resource Monitor.

Table 6-7 Example 2 of Notification Settings and Whether There Is Notification or Not

	Initial Notification	Continues one or more times	
	Second or later notification	Always notify	Do not notify for 3 minutes
	Notification Priority	All	All
Time	Priority	-	-
0:00:01	Warning	o	o
0:00:05	Warning	o	-
0:00:09	Warning	o	-
0:00:13	Warning	o	-
0:00:17	Warning	o	-
0:03:30	Warning	o	o
0:15:30	Warning	o	o
0:15:41	Warning	o	-
Note			Trap group monitoring recommended (*1)

o : Notification will be sent; - : Notification will not be sent

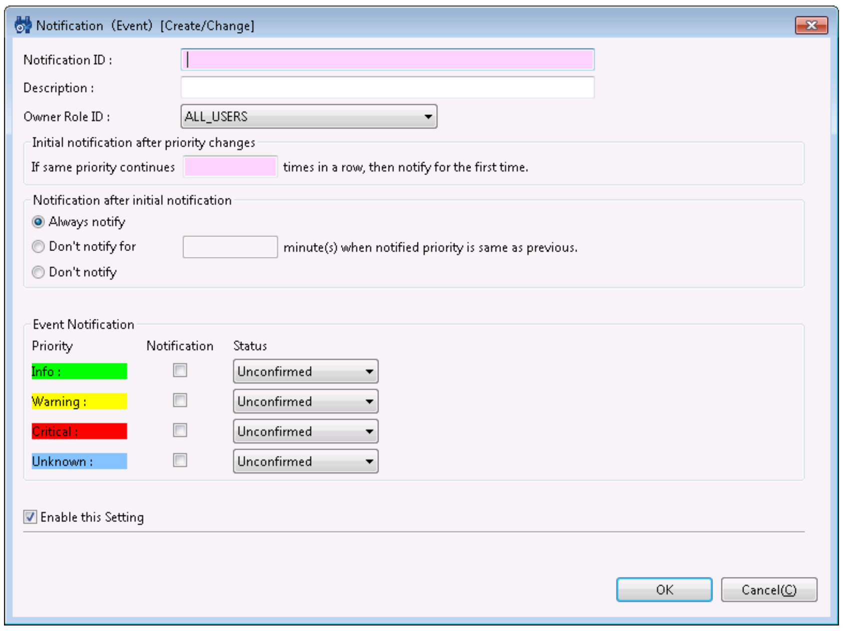
*1: Trap group monitoring includes SNMPTRAP Monitor, System Log Monitor, Logfile Monitor and Windows Event Monitor.

6.3.3 Event Notification

Event notification is used when you want to confirm the monitor results for each monitor feature and save the job execution results as history from the Hinemos Client. Normally, not just the current status, but information including the previous status is saved as the execution results for the monitor results and jobs for each monitor feature, and this can be used to confirm the history.

The event notification results are displayed in the Monitor[Event] view. In the notification information displayed in the Monitor[Event] view, the notification information is not overwritten with the latest monitor results and job execution results, etc.

Refer to the setting procedure in Status Notification for the process for setting the event notifications.



Notification (Event) [Create/Change]

Notification ID :

Description :

Owner Role ID : ALL_USERS

Initial notification after priority changes

If same priority continues times in a row, then notify for the first time.

Notification after initial notification

● Always notify

○ Don't notify for minute(s) when notified priority is same as previous.

○ Don't notify

Event Notification

Priority	Notification	Status
Info :	□	Unconfirmed
Warning :	□	Unconfirmed
Critical :	□	Unconfirmed
Unknown :	□	Unconfirmed

☑ Enable this Setting

Figure 6-8 Notification(Event)[Create/Change] Dialog

Table 6-8 Notification (Event) [Create/Change]

Configuration item	Input type	Description
Notification ID	Text	Enter an ID to identify the notification setting.
Description	Text	Enter a description of the notification setting.
Owner Role ID	Select from list	Select an Owner Role ID for the notification setting.
Initial notification after priority changes	Numeric	Enter the suppression setting for when the same notification information continues to occur.
Second or later notification after the priority change	Select with the radio button (part text)	Enter the notification method for the second or later time when the same notification information continues to occur. · Always notify Select when not suppressing the second or later notification. · Do not notify for the same priority for 0 minutes after the previous notification Select when suppressing by time the second or later notification. · Do not notify Select when not performing a second or later notification.

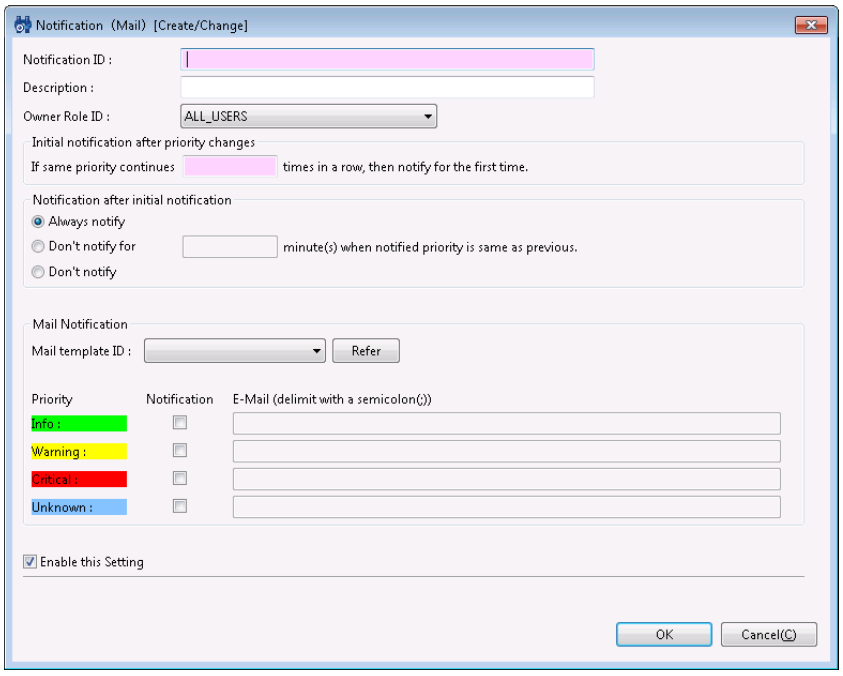
Copyright (c) 2013 NTT DATA CORPORATION

Event Notification	Notification (Information / Warning / Critical / Unknown)	Check box	Select the priority for an event notification.
	Status (Information / Warning / Critical / Unknown)	Select from list	You can select from notification of "Unconfirmed" or "Confirmed" for notification of an event. The confirmed notification event will not appear in Monitor[Event] view even if notified (but it can be displayed if you set "Confirmed" events to display in "Filtering" in the Monitor [Event] view.
Enable this setting		Checkbox	Check to enable notification settings. It will return to the same setting if not checked and notification will not be performed.

6.3.4 Mail Notification

Mail Notification is a feature for notification by external e-mail of the monitoring results and the job execution results for each monitoring feature. (When performing mail notification, special settings for the Hinemos Manager environment settings are necessary, in addition to the settings from the Hinemos Client. (Refer to 5.2.1 "Enable Mail Notification" in the Administrator's Guide for details.

Refer to the setting procedures in Status Notification for the process thereafter.



Notification (Mail) [Create/Change]

Notification ID :

Description :

Owner Role ID : ALL_USERS

Initial notification after priority changes

If same priority continues times in a row, then notify for the first time.

Notification after initial notification

● Always notify

○ Don't notify for minute(s) when notified priority is same as previous.

○ Don't notify

Mail Notification

Mail template ID : Refer

Priority	Notification	E-Mail (delimit with a semicolon(;))
Info :	□	
Warning :	□	
Critical :	□	
Unknown :	□	

☑ Enable this Setting

Figure 6-9 Notification (Mail) [Create/Change] Dialog

Table 6-9 Configuration Items of Notification (Mail)

Configuration item	Input type	Description
Notification ID	Text	Enter an ID to identify the notification setting.
Description	Text	Enter a description of the notification setting.
Owner Role ID	Select from list	Select an Owner Role ID for the notification setting.
Initial notification after priority changes	Numeric	Enter the suppression setting for when the same notification information continues to occur.

Copyright (c) 2013 NTT DATA CORPORATION

Second or later notification after the priority change		Select with the radio button (part text)	Enter the notification method for the second or later time when the same notification information continues to occur. · Always notify Select when not suppressing the second or later notification. · Do not notify for the same priority for 0 minutes after the previous notification Select when suppressing by time the second or later notification. · Do not notify Select when not performing a second or later notification.
Mail Notification	Mail template ID Select from list	Specify mail template ID used to	send mail (refer to Mail Template Feature).
	Notification (Information / Warning / Critical / Unknown)	Checkbox	Select the priority to send mail
	E-Mail address (Information / Warning / Critical / Unknown)	Text	Enter the e-mail address (*1). Separate Multiple e-mail addresses by semicolon. (Note: even if same e-mail addresses are repeated multiple times, the notification e-mail to the same address will be sent only once.) Further, 1024 bytes of e-mail addresses can be registered. (including spaces and semicolons)
Enable this setting		Checkbox	Check to enable notification settings. It will return to the same setting if not checked and notification will not be performed.

*1: The domain part of an email address will be validated according to RFC 822 and RFC 1034. Common examples not based on RFC 822 and RFC 1034 are shown as follows.

- Characters other than alphanumeric characters, "-" (hyphen) and "." (period) are used in the domain part.
- Continuous "." (period) are used in the domain part.
- A "-" (hyphen) or "." (period) are used at the end of the domain part.

When a Mail Template is Not Specified

If a mail template is not specified, the following content is sent.

Table 6-10 Sent Contents When a Mail Template is Not Specified

Type	Content
Subject	Hinemos Notification(#[PRIORITY])
Body	Date and Time Created: #[GENERATION_DATE] Application: #[APPLICATION] Priority: #[PRIORITY] Message: #[MESSAGE] Scope: #[SCOPE]

When sending an e-mail, each monitoring result is replaced with its corresponding content as follows.

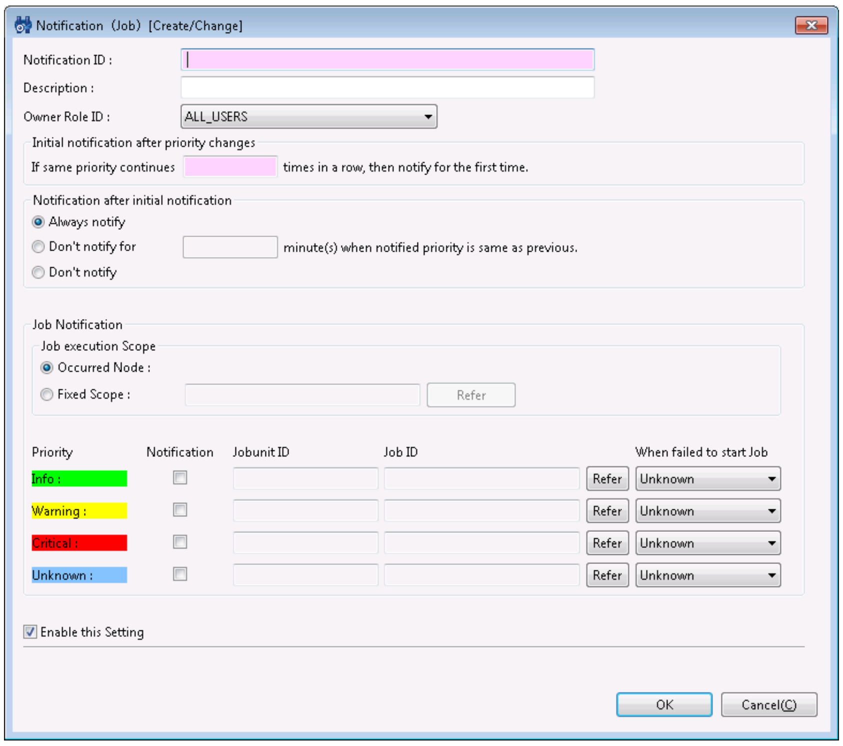
- #[PRIORITY] ... Replaced by the Priority according to the locale of Hinemos Manager
- #[GENERATION_DATE] ... Replaced by the Date and Time Created
- #[SCOPE] ... Replaced by the Facility Name
- #[APPLICATION] ... Replaced by the Application
- #[MESSAGE] ... Replaced by the Message

6.3.5 Job Notification

The job notification feature provides notification of the monitor results for each monitor feature and the job execution results based on job execution.

Refer to Job Management Feature for settings for the job to be executed.

Refer to the setting procedures in Status Notification for the process thereafter.



Notification (Job) [Create/Change]

Notification ID :

Description :

Owner Role ID : ALL_USERS

Initial notification after priority changes

If same priority continues times in a row, then notify for the first time.

Notification after initial notification

● Always notify

○ Don't notify for minute(s) when notified priority is same as previous.

○ Don't notify

Job Notification

Job execution Scope

● Occurred Node :

○ Fixed Scope : Refer

Priority	Notification	Jobunit ID	Job ID		When failed to start Job
Info :	□			Refer	Unknown
Warning :	□			Refer	Unknown
Critical :	□			Refer	Unknown
Unknown :	□			Refer	Unknown

☑ Enable this Setting

OK Cancel(C)

Figure 6-10 Notification(Job)[Create/Change] Dialog

Table 6-11 Configuration Items of Notification (Job)

Configuration item	Input type	Description
Notification ID	Text	Enter an ID to identify the notification setting.
Description	Text	Enter a description of the notification setting.
Owner Role ID	Select from list	Select an Owner Role ID for the notification setting.
Initial notification after priority changes	Numeric	Enter the suppression setting for when the same notification information continues to occur.
Second or later notification after the priority change	Select with the radio button (part text)	Enter the notification method for the second or later time when the same notification information continues to occur. · Always notify Select when not suppressing the second or later notification. · Do not notify for the same priority for 0 minutes after the previous notification Select when suppressing by time the second or later notification. · Do not notify Select when not performing a second or later notification.

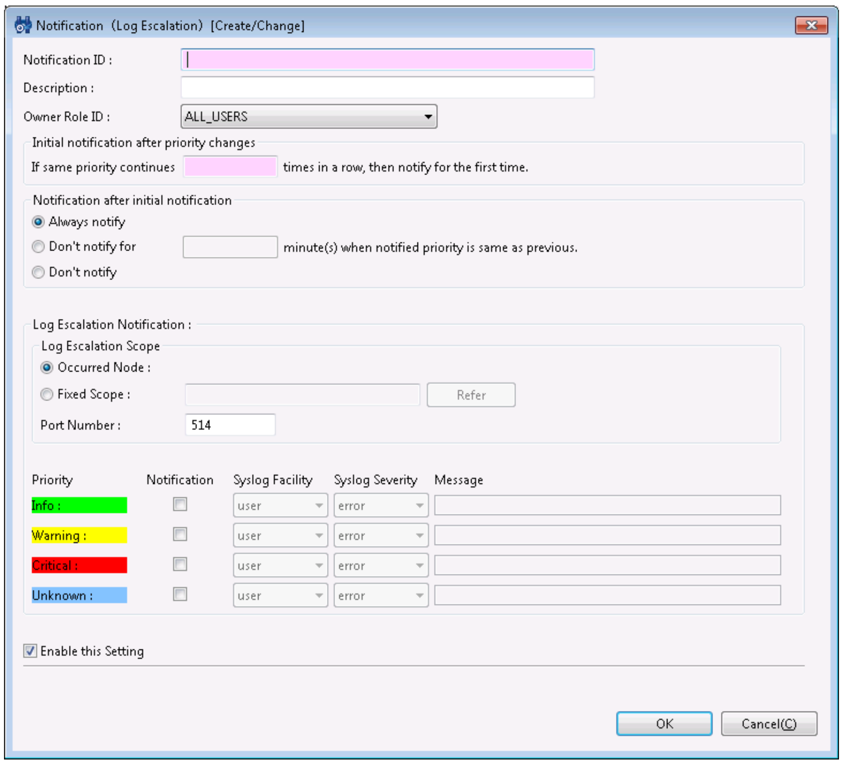
Copyright (c) 2013 NTT DATA CORPORATION

Job Notification Job execution Scope	Scope where the event occurred Fixed Scope	Select with the radio button	Specify scope (or node) for job execution. · Scope where the event occurred Scope (or node) where the notification information occurred will be the job execution target. · Fixed Scope Select the scope (or node) for job execution from the scope tree. To make the scope (or node) specified here the object of job execution, the Job Parameter (#[FACILITY_ID]) must be enabled for the job execution scope specified below.
Job Notification	Notification (Information / Warning / Critical / Unknown)	Checkbox	Select the priority for job execution.
	Job unit ID, Job ID (Information / Warning / Critical / Unknown)	Select from the job tree	Select the job to execute.
	When failed to start Job (Information / Warning / Critical / Unknown)	Select from the list	Set the priority for calling the job when the job call failed.
Enable this setting		Checkbox	Check to enable notification settings. It will return to the same setting if not checked and notification will not be performed.

6.3.6 Log Escalation Notification

Log escalation notification is a feature to send an external notification by log (syslog format) of the monitoring results for each monitoring feature and the job execution results.

Refer to the setting procedure in Status Notification for the process for setting the log escalation notifications.



Notification (Log Escalation) [Create/Change]

Notification ID :

Description :

Owner Role ID : ALL_USERS

Initial notification after priority changes

If same priority continues times in a row, then notify for the first time.

Notification after initial notification

● Always notify

○ Don't notify for minute(s) when notified priority is same as previous.

○ Don't notify

Log Escalation Notification :

Log Escalation Scope

● Occurred Node :

○ Fixed Scope :

Port Number : 514

Priority	Notification	Syslog Facility	Syslog Severity	Message
Info :	□	user	error	
Warning :	□	user	error	
Critical :	□	user	error	
Unknown :	□	user	error	

☑ Enable this Setting

Figure 6-11 Notification(Log Escalation)[Create/Change] Dialog

Table 6-12 Configuration Items of Notification(Log Escalation)

Configuration item	Input type	Description
Notification ID	Text	Enter an ID to identify the notification setting.

Copyright (c) 2013 NTT DATA CORPORATION

Description		Text	Enter a description of the notification setting.
Owner Role ID		Select from list	Select an Owner Role ID for the notification setting.
Initial notification after priority changes		Numeric	Enter the suppression setting for when the same notification information continues to occur.
Second or later notification after the priority change		Select with the radio button (part text)	Enter the notification method for the second or later time when the same notification information continues to occur. · Always notify Select when not suppressing the second or later notification. · Do not notify for the same priority for 0 minutes after the previous notification Select when suppressing by time the second or later notification. · Do not notify Select when not performing a second or later notification.
Log Escalation Notification Log Escalation Scope	Scope where the event occurred Fixed Scope	Specify the scope (or node) which sent the log.	· Scope where the event occurred The scope (or node) with notification information is the send target for the log. · Fixed Scope From the scope tree, select the scope (or node) for the log.
	Port Number	Text	Specify the port number (UDP) for sending the log (default is syslog 514).
Log Escalation Notification	Notification (Information / Warning / Critical / Unknown)	Checkbox	Select the priority to send the log.
	Syslog Facility (Information / Warning / Critical / Unknown)	Select from list	Select Facility when sending the log.
	Syslog Severity (Information / Warning / Critical / Unknown)	Select from the list	Select Severity when sending the log.
	Message (Information / Warning / Critical / Unknown)	Text	Enter message to send.
Enable this setting		Checkbox	Check to enable notification settings. It will return to the same setting if not checked and notification will not be performed.

Syslog message in the Log Escalation Notification

Send log in syslog format (RFC 3164).

Syslog messages are composed of a PRI part, a HEADER part, and a MSG part (maximum size of syslog messages is 1024bytes).

```
<PRI> HEADER MSG
```

PRI part:

The value calculated from Severity and Facility in the Log Escalation Notification is configured.
Since syslog is standard, refer to RFC 3164 for the detailed calculation method.

HEADER part:

Creation time of the syslog message and the node name (default) of the Hinemos Manager is configured.
* In addition to the node name of the Hinemos Manager, a specified string or facility ID of the facility can be set where the event occurred. Refer to 5.3 "Log Escalation Notification" in the Administrator's Guide for the setting method.

MSG part:

Content specified in "Message" is configured.
The MSG part is composited of TAG field and CONTENT field. The character set used in these two fields should be explicitly configured as specified in RFC 3164. The length of character set used in TAG field is 32 or less and a non-alphanumeric character such as ":" (colon) is used to separate them.

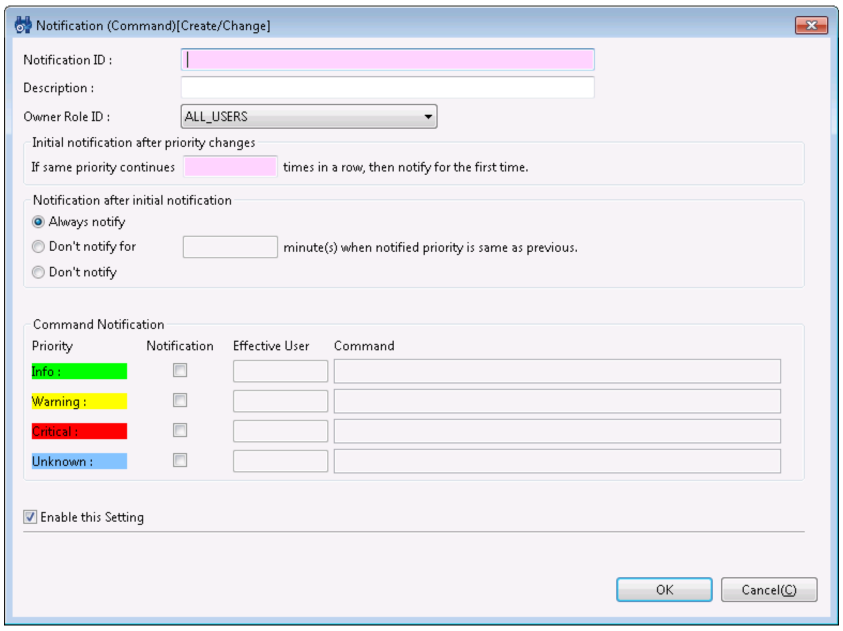
To display monitoring result in the message

Entering the designated replacement strings in messages sent by the log escalation notification enables insertion of details corresponding to the monitoring results. For the designated strings, refer to Table 6-16 List of strings supporting replacement (Mail Template Feature).

6.3.7 Command Notification

The command notification feature provides notification of the monitor results for each monitor feature and the command execution results based on job execution.

Refer to the setting procedure in Status Notification for the process for setting the command notifications.



Notification (Command)[Create/Change]

Notification ID :

Description :

Owner Role ID : ALL_USERS

Initial notification after priority changes

If same priority continues times in a row, then notify for the first time.

Notification after initial notification

● Always notify

○ Don't notify for minute(s) when notified priority is same as previous.

○ Don't notify

Command Notification

Priority	Notification	Effective User	Command
Info :	□		
Warning :	□		
Critical :	□		
Unknown :	□		

☑ Enable this Setting

Figure 6-12 Notification (Command)[Create/Change] Dialog

Table 6-13 Configuration Items of Notification (Command)

Configuration item	Input type	Description
Notification ID	Text	Enter an ID to identify the notification setting.
Description	Text	Enter a description of the notification setting.
Owner Role ID	Select from list	Select an Owner Role ID for the notification setting.
Initial notification after priority changes	Numeric	Enter the suppression setting for when the same notification information continues to occur.
Second or later notification after the priority change	Select with the radio button (part text)	Enter the notification method for the second or later time when the same notification information continues to occur. · Always notify Select when not suppressing the second or later notification. · Do not notify for the same priority for 0 minutes after the previous notification Select when suppressing by time the second or later notification. · Do not notify Select when not performing a second or later notification.

Copyright (c) 2013 NTT DATA CORPORATION

Command Notification	Notification (Information / Warning / Critical / Unknown)	Checkbox	Select the priority for command execution.
	Effective User (Information / Warning / Critical / Unknown)	Text	Specify the effective user.
	Command (Information / Warning / Critical / Unknown)	Text	Specify the effective command. If the designated strings are entered, the string will be replaced with detail corresponding to each monitoring result.*
Enable this setting		Checkbox	Check to enable notification settings. It will return to the same setting if not checked and notification will not be performed.

* Refer to Table 6-16 List of strings supporting replacement (Mail Template Feature) for the designated strings.

Command Notification Timeout

The default timeout for command notification is 15 seconds.

6.3.8 Notification Message

When notifying results from the Monitor Settings feature and the Job Management feature, the job result is notified as a message or an original message. Display the list of message and original messages formats by distinguish functions.

Table 6-14 Notification Content of Message ·#[MESSAGE] Strings

Feature		Status		Message/#[MESSAGE] strings
Monitor Settings feature	Hinemos Agent	Successful value acquisition	Format	Hinemos Agent is available
			Example	Hinemos Agent is available
		Failed value acquisition	Format	Hinemos Agent is not available
			Example	Hinemos Agent is not available
Monitor Settings feature	PING	Successful value acquisition	Format	Packets: Sent = [number of ping execution], Received = [number of responses received], Lost =[number of lost response] ([response rate]% loss)
			Example	Packets: Sent = 1, Received = 1, Lost = 0 (0% loss)
Monitor Settings feature	HTTP(Numeric)	Successful value acquisition	Format	Response Time(msec) : [Response Time]
			Example	Response Time(msec) : 25
		Failed value acquisition	Format	Could not get value
			Example	Could not get value

Copyright (c) 2013 NTT DATA CORPORATION

Monitor Settings feature	HTTP(String)	Successful value acquisition	Format	User defined (strings configured in the "Message" column of the Monitor Setting)
			Example	JBossFilterMessage
		Failed value acquisition	Format	Could not get value
			Example	Could not get value
Monitor Settings feature	SQL (Numeric)	Successful value acquisition	Format	Acquired value : [Acquired value]
			Example	Acquired value : 1.0
		Failed value acquisition	Format	Failed to execute SQL statement
			Example	Failed to execute SQL statement
Monitor Settings feature	SQL(String)	Successful value acquisition	Format	User defined (strings configured in the "Message" column of the Monitor Settings
			Example	HinemosFilter
		Failed value acquisition	Format	Failed to execute SQL statement
			Example	Failed to execute SQL statement
Monitor Settings feature	Process	Successful value acquisition	Format	Number of process : [number of process]
			Example	Number of process : 1
		Failed value acquisition	Format	Timed out
			Example	Timed out
Monitor Settings feature	Windows service	Successful value acquisition	Format	[Service name] Service is Running
			Example	SNMP Service is Running
		Failed value acquisition	Format	[Service name] Service is not Running
			Example	SNMP Service is not Running
Monitor Settings feature	Service Port	Successful value acquisition	Format	Response Time = [Response Time] ms ([Service port - Service Protocol] / [Port Number])
			Example	Response Time = 1ms(DNS/53)
		Failed value acquisition	Format	[Detailed information] ([Service port - Service Protocol] /[Port Number])
			Example	Connection refused[SocketException](DNS/53)

Monitor Settings feature	Resource	Successful value acquisition	Format	[Monitor Item] : [Collection value]
			Example	File System Utilization[/] : 13.651
		Failed value acquisition	Format	[Monitor Item] : Could not get value
			Example	File system usage [/] : Could not get value
Monitor Settings feature	SNMP(Numeric)	Successful value acquisition	Format	Acquired value : [Acquired value]
			Example	Acquired value : 0.0
		Failed value acquisition	Format	Could not get value [Detailed information]
			Example	Could not get value snmpTimeoutError./192.168.0.1 .1.3.6.1.4.1.2021.11.53.0
Monitor Settings feature	SNMP(String)	Successful value acquisition	Format	User defined (strings configured in the "Message" column of the Monitor Settings
			Example	HOSTNAME
		Failed value acquisition	Format	Could not get value [Detailed information]
			Example	Could not get value snmpTimeoutError./192.168.0.1 .1.3.6.1.2.1.1.5.0
Monitor Settings feature	Custom	Failed value acquisition	Format	VALUE : [Item name] = [Value]
			Example	VALUE : FOO = 123.0
		Failed value acquisition	Format	[Detailed information]
			Example	FAILURE : command execution failed (timeout or no stdout)...
Monitor Settings feature	System log	Successful value acquisition	Format	User defined (strings configured in the "Message" column of the Monitor Settings (If the replacement string #[LOG_LINE] in the "Message" column is specified, it will be replaced in the log details of the system log)
			Example	SYSLOG01_MSG
Monitor Settings feature	Log file	Successful value acquisition	Format	[log content of Log file]
			Example	Apr 16 16:36:57 common_db root: syslog-test-info
Monitor Settings feature	SNMPTRAP	Successful value acquisition	Format	["Message" defined by Trap Definition]
			Example	Agent Interface Up (linkUp Trap)interface Network01
Monitor Settings feature	Windows Event	Successful value acquisition	Format	<[Event Log];[Event Source];[Initial of Event Level] [Event ID];>[Message] (If the replacement string #[LOG_LINE] in the "Message" column is specified, it will be replaced in the log details of the system log.)
			Example	<Application;EventCreate;I1000;>log-test-info

Copyright (c) 2013 NTT DATA CORPORATION

Job Management feature	Execute command	Starting Start Command	Format	Job[[Job Name]([Job ID])]started successfully (Session ID: [Job Session ID])
		Ending Start Command	Format	Job[[Job Name]([Job ID])] stopped (End Status: Normal)(Session ID:[Job Session ID]) Job[[Job Name]([Job ID])] stopped (End Status: Warning) (Session ID:[Job Session ID]) Job[[Job Name]([Job ID])] stopped (End Status: Error) (Session ID:[Job Session ID])
		Delay of start	Format	Job[[Job Name]([Job ID])] Delay of start occurred (Session ID:[Job Session ID])
		Delay of end	Format	Job[[Job Name]([Job ID])] Delay of end occurred (Session ID:[Job Session ID])
Job Management feature	File Transfer	Starting File Transfer	Format	File Job[[Job Name]([Job ID])]started successfully (Session ID:[Job Session ID])
		Ending File Transfer	Format	File Transfer Job[[Job Name]([Job ID])] stopped (End Status: Normal)(Session ID:[Job Session ID]) File Transfer Job[[Job Name]([Job ID])] stopped (End Status: Warning)(Session ID:[Job Session ID]) File Transfer Job[[Job Name]([Job ID])] stopped (End Status: Error)(Session ID:[Job Session ID])
Common feature	Maintenance	Success	Format	Maintenance ID[[Maintenance ID]] stopped (End Status: Success)
			Example	Maintenance ID[MT_PRF-DEFAULT] stopped (End Status: Success)

Table 6-15 Notification content of Original Message ·#[ORIGINAL_MSG] strings

Feature		Status		Original Message#[ORIGINAL_MSG] strings
Monitor Settings feature	Hinemos Agent	Successful value acquisition	Format	-(*2)
			Example	-
		Failed value acquisition	Format	-(*2)
			Example	-
Monitor Settings feature	PING	Successful value acquisition	Format	Pinging [target IP address] (target IP address) . [Detailed information]
			Example	Pinging 192.168.0.1 (192.168.0.1) . Ping statistics for 192.168.0.1: Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),Approximate round trip times in milli-seconds: Minimum = 0.64ms, Maximum = 0.64ms, Average = 0.64ms

Copyright (c) 2013 NTT DATA CORPORATION

Monitor Settings feature	HTTP (Numeric)	Successful value acquisition	Format	URL : [Monitored URL] Status code : [Status code of HTTP](0 if cannot acquire) Header : [HTTP Header section] Body : [HTTP Body section]
			Example	URL : http://192.168.0.1/index.html Status code : 200 Header : Date: Mon, 16 Apr 2012 05:18:57 GMT Server: Apache/2.2.3 (Red Hat) Last-Modified: Fri, 23 Mar 2012 02:25:10 GMT Content-Type: text/html; charset=UTF-8 Body : <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml
		Failed value acquisition	Format	Error Message URL : [Monitored URL] Status code : [Status code of HTTP](0 if cannot acquire) Header : [HTTP Header section] Body : [HTTP Body section]
			Example	http requesting failure. (I/O error : unreachable or timeout) URL : http://192.168.0.1/index.html Status code : 0
Monitor Settings feature	HTTP(String)	Successful value acquisition	Format	Refer to HTTP(Numeric)
			Example	Refer to HTTP(Numeric)
		Failed value acquisition	Format	Refer to HTTP(Numeric)
			Example	Refer to HTTP(Numeric)
Monitor Settings feature	SQL(Numeric)	Successful value acquisition	Format	Value of Record : [Value of Record], Number of Records : [Number of Records] Connection URL : [Connection URL]
			Example	Value of Record : hinemos, Number of Records : 1 Connection URL : jdbc:postgresql://192.168.0.1/postgres
		Failed value acquisition	Format	SQL Statement : [Issued SQL Statement](Error message) Connection URL : [Connection URL]
			Example	SQL Statement : SELECT 1 (FATAL: no pg_hba.conf entry for host "192.168.0.1", user "hinemos", database "hinemos1") Connection URL : jdbc:postgresql://192.168.0.1/postgres
Monitor Settings feature	SQL(String)	Successful value acquisition	Format	Refer to SQL(Numeric)
			Example	Refer to SQL(Numeric)
		Failed value acquisition	Format	Refer to SQL(Numeric)
			Example	Refer to SQL(Numeric)

Copyright (c) 2013 NTT DATA CORPORATION

Monitor Settings feature	Process	Successful value acquisition	Format	Command : [Matching strings specified for the "Command" column in the settings], Command Line Arguments : [Matching strings specified for the "Command Line Arguments" column in the settings]
			Example	Command : .*snmp.*, Argument : .*
		Failed value acquisition	Format	Command : [Matching strings specified for the "Command" column in the settings], Command Line Arguments : [Matching strings specified for the "Command Line Arguments" column in the settings]
			Example	Command : .*snmp.*, Argument : .*
Monitor Settings feature	Windows service	Successful value acquisition	Format	[Service name] Service is Running
			Example	SNMP Service is Running
		Failed value acquisition	Format	[Service name] Service is another state : Stopped
			Example	SNMP Service is another state : Stopped
Monitor Settings feature	Service - Port	Successful value acquisition	Format	Monitoring the [Service Port name or "port"] of [Host name][[IP Address]]:[Port Number]. [Detailed information]
			Example	Monitoring the port of common_port[192.168.0.1]:143. Mon Apr 16 19:06:18 JST 2012 Tried to Connect: Response Time = 1ms
		Failed value acquisition	Format	Monitoring the port of [Host name][[IP Address]]:[Port Number]. [Detailed information]
			Example	Monitoring the port of common_port[192.168.0.1]:143. Mon Apr 16 14:55:18 JST 2012 Tried to Connect: Connection refused[SocketException]
Monitor Settings feature	Resource	Successful value acquisition	Format	[Monitor Item] : [Collection value] [Detailed information](Only for device-specific information)
			Example	File System Utilization[/] : 13.651 Device Name : / Device Index : 4
		Failed value acquisition	Format	[Monitor Item] : NaN
			Example	File System Utilization[/] : NaN
Monitor Settings feature	SNMP(Numeric)	Successful value acquisition	Format	OID : [OID]
			Example	OID : .1.3.6.1.4.1.2021.11.53.0
		Failed value acquisition	Format	OID : [OID]
			Example	OID : .1.3.6.1.4.1.2021.11.53.0

Copyright (c) 2013 NTT DATA CORPORATION

Monitor Settings feature	SNMP(String)	Successful value acquisition	Format	OID : [OID], Value : [Value]
			Example	OID : .1.3.6.1.2.1.1.5.0, Value : st17-01
		Failed value acquisition	Format	OID : [OID]
			Example	OID : .1.3.6.1.2.1.1.5.0
Monitor Settings feature	Custom	Failed value acquisition	Format	VALUE : [Output results] = [Value] COMMAND : [Run Command] [Detailed information]
			Example	VALUE : FOO = 123.0 COMMAND : sh -c echo "FOO,123" COLLECTION DATE : 2012-04-16 19:52:00 executed at 2012-04-16 19:52:50 exited (or timeout) at 2012-04-16 19:52:50 EXIT CODE : 0 [STDOUT] FOO,123 [STDERR]
		Failed value acquisition	Format	[Detailed information] COMMAND :[Run Command] [Detailed information]
			Example	FAILURE : command execution failed (timeout or no stdout)... COMMAND : sh -c dir "FOO,123" COLLECTION DATE : 2012-04-16 20:03:00 executed at 2012-04-16 20:03:42 exited (or timeout) at 2012-04-16 20:03:42 EXIT CODE : 2 [STDOUT] [STDERR]
Monitor Settings feature	System log	Successful value acquisition	Format	pattern=[Pattern string]log.line[Content of Log file]
			Example	pattern=.*Warn.* log.line=<13>Jul 17 15:52:42 test_rhel6432 root: Warn
Monitor Settings feature	Log file	Successful value acquisition	Format	log.file=[Filename]pattern=[Pattern string] log.line=[Content of Log file]
			Example	log.file=/tmp/test.log pattern=.*Warn.* log.line=Test Warn
Monitor Settings feature	SNMPTRAP	Successful value acquisition	Format	OID=[OID] TrapName=[Trap Name defined by Trap Definition] CommunityName=[Community Name defined by Trap Definition] VarBind=[VarBind list defined by Trap Definition] Message=[Detailed message defined by Trap Definition] (*1)
			Example	OID=1.3.6.1.4.1.1991 TrapName=vendor/foundry/traps/snTrapL4LinkDown CommunityName=public VarBind=BBBB,CCCC Message=The SNMP trap that is geterated when ISP link goes down snL4TrapLinkName BBBB; snL4LinkVirtualInterface CCCCC;
Monitor Settings feature	Windows Event	Successful value acquisition	Format	pattern=[Pattern string]xAlog.line= <[Event Log];[Event Source];[Initial of Event Level] [Event ID];>[Message]
			Example	pattern=.*log-test-info.*xAlog.line= <Application;EventCreate;I1000;>log-test-info

Copyright (c) 2013 NTT DATA CORPORATION

Job Management feature	Execute Command	Starting Start Command	Format	-(*2)
		Ending Start Command	Format	-(*2)
		Delay of start	Format	-(*2)
		Delay of end	Format	-(*2)
	File Transfer	Starting File Transfer	Format	-(*2)
		Ending File Transfer	Format	-(*2)
Common feature	Maintenance	Success	Format	[Maintenance Type]: [Deleted number] records
			Example	DELETE_RERF_DATA : 0 records

* The CommunityName and Varbind in the original message can be hidden by changing the following parameters in hinemos.properties.

```
monitor.snmptrap.org.message.community=false
monitor.snmptrap.org.message.varbind=false
```

*2 "-" means that nothing was displayed in the original message. Also, it does not mean that "#[ORG_MESSAGE]" was substituted for "-" .

6.4 Mail Template Feature

6.4.1 Overview

The mail template feature sets and saves a sample of the mail subject and body that will be sent to the notification destination in a template format. Mail templates created with this feature are designated as mail notification setting units when used by the notification feature with job management and the monitor feature. Mail templates created using this feature use the "Mail template ID" when specified by the mail notification feature.

6.4.2 Mail Template Registration

The mail template can be registered by the following the procedures.

1. Click the "Create" button in the Monitor Setting[Mail Template] view.

2. The Mail template[Create/Modify] dialog opens.

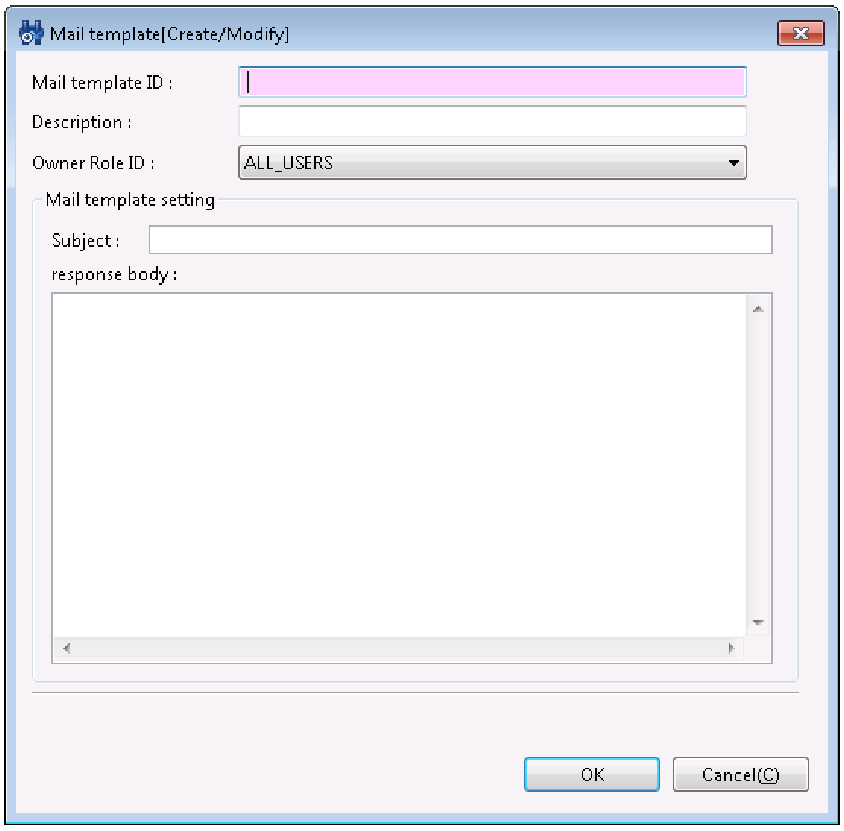


Figure 6-13 Mail template ID[Create/Modify] Dialog

3. Set up the mail template ID. Features that use mail templates can select a mail template by specifying this ID.
4. Enter the Description field in alphanumeric text.
5. Select an Owner Role ID from the drop-down list.
6. Enter the Subject in alphanumeric text.
7. Enter the response body in alphanumeric text.

- To display the monitoring result in the Subject or the response body

  If the following designated strings are entered, when sending the e-mail, the string will be replaced with corre sponding content to each monitoring result.

Table 6-16 List of Strings Supporting Replacement

Strings	Contents for replacement
#[PRIORITY]	Priority according to the locale of the Hinemos Manager.
#[PRIORITY_NUM]	Convert to Priority (numeric) (Critical:0 Unknown:1 Warning:2 Info:3).
#[PRIORITY_JP]	Convert to Priority (Japanese).
#[PRIORITY_EN]	Convert to Priority (English).
#[PLUGIN_ID]	Replace by Plugin ID (For details, refer to Table 6-15 List of Plugin ID).
#[MONITOR_ID]	Replace by Monitor ID.
#[MONITOR_DESCRIPTION]	Replace by description of a specific monitor.
#[MONITOR_OWNER_ROLE_ID]	Replace by Owner Role ID of a specific monitor.
#[CALENDAR_ID]	Replace by Calendar ID.
#[FACILITY_ID]	Replace by Facility ID.
#[FACILITY_NAME]	Replace by Facility Name.
#[SCOPE]	Replace by Scope Name.

Copyright (c) 2013 NTT DATA CORPORATION

#[NODE_NAME]	Replace by Node Name (If monitoring result is scope, will not be replaced).
#[IP_ADDRESS]	Replace by IP Address (If monitoring result is per scope, will not be replaced).
#[IP_ADDRESS_V4]	Replace by IPv4 Address (If monitoring result is per scope, will not be replaced).
#[IP_ADDRESS_V6]	Replace by IPv6 Address (If monitoring result is per scope, will not be replaced).
#[GENERATION_DATE]	Replace by Time Created.
#[APPLICATION]	Replace by Application.
#[MESSAGE_ID]	Replace by Message ID.
#[MESSAGE]	Replace by Message.
#[ORG_MESSAGE]	Replace by Original Messages.
#[NOTIFY_ID]	Replace by Notification ID.
#[NOTIFY_DESCRIPTION]	Replace by description of a specific notification.

When replacing the character string for #[MESSAGE], #[ORG_MESSAGE], if the replacement string includes a backslash (\) or control code, etc., the same string can be replaced according to the list in Table 6-17 #[MESSAGE], #[ORG_MESSAGE].

Table 6-17 #[MESSAGE], #[ORG_MESSAGE] Replacement Support List

Characters	Contents for replacement
Backslash (\)	\\ (The representation is double byte, but it is actually replaced by two half width backslashes.)
Quote (')	\'
Double quote (")	\"
Back quote (`)	\`
Control code	from 0x00 - 0x20, 0x7F (Example: Line feed LF -> 0x0A)

This is noted as ":original" but you can disable the replacement handling noted in Table 6-17 in #[MESSAGE], #[ORG_MESSAGE]. (Example : #[MESSAGE:original])

If notified from each function, the corresponding Plugin ID (#[PLUGIN_ID]) for replacement is as follows.

Table 6-18 List of Plugin IDs

Hinemos functions	Replacement strings of Plugin ID
Monitor Settings	MON
Hinemos Agent Monitor	MON_AGT
HTTP Monitor	MON_HTP
Ping Monitor	MON_PNG
SNMP Monitor	MON_SNMP
SNMPTRAP Monitor	MON_SNMP_TRP
SQL Monitor	MON_SQL
Windows Service Monitor	MON_WINSERVICE
Windows Event Monitor	MON_WINEVENT
Custom Monitor	MON_CUSTOM
Service Port Monitor	MON_PRT
System Log Monitor	MON_SYSLOG
Process Monitor	MON_PRC
Resource Monitor	MON_PRF
Logfile Monitor	MON_LOGFILE

Job Management	JOB
Self Check	SYS_SFC
Maintenance	MAINTENANCE

Note) The name of the Plugin ID cannot be changed.

[Example of creating a Mail Template]

```
[==========Subject starts here========]
Hinemos event [#[FACILITY_ID]]
[===========Subject ends here=========]
[==========response body starts here========]
The following events occurred.

Node : #[FACILITY_ID]
Priority : #[PRIORITY]
Time Created : #[GENERATION_DATE]
Message :
#[APPLICATION] [#[GENERATION_DATE]] #[ORG_MESSAGE]

Above.
[===========response body ends here=========]
```

6.4.3 Changing the Mail Template

1. Select the subject to change in the Monitor Settings [Mail template[List]] dialog, then click the "Modify" button. The Mail template[Create/Modify] dialog opens.
2. Edit the contents of the configuration, then click the "OK" button (refer to the Mail Template Registration section for the setting procedures).

6.4.4 Deleting the Mail Template

Select the subject to delete in the Monitor Settings [Mail template[List]] dialog, then click the "Delete" button.

6.5 Monitor Settings Feature (Create - Change - Delete - Setting Enable - Disable)

6.5.1 Overview

The monitor settings feature performs operations related to the monitor settings such as to create, change, delete, enable or disable monitor settings. Perform operations related to monitor settings in the Monitor Setting[List] view.

6.5.2 Create Monitor Settings

Creating various new monitor settings is performed in the setting dialog for each monitor feature. The setting dialog can be opened with the following operations.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select the monitor feature you want to use from the Monitor Type dialog and click the "Next" button

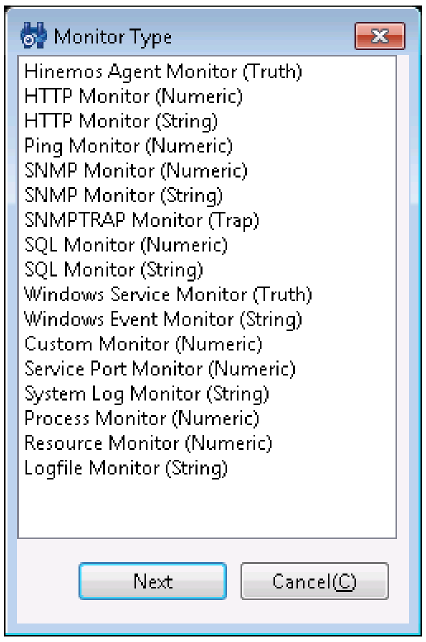


Figure 6-14 Monitor Type Dialog

3. A dialog for setting the various monitor settings opens.

Refer to the next section for each of the monitor setting methods.

6.5.3 Changing Monitor Settings

Changing the settings for existing monitor settings is performed in the setting dialog for each monitor feature. The setting dialog can be opened with the following operations.

1. Select the monitor setting which you would like to change from the Monitor Setting[List] view.
2. Click the "Modify" button in the Monitor Setting[List] view.
3. A dialog for setting the various monitor settings opens.
4. After changing the settings, you can save the setting changes by clicking the "OK" button at the bottom of the settings dialog.

Refer to the next section for each of the monitor setting methods.

6.5.4 Deleting Monitor Setting

Delete existing monitor settings from the Monitor Setting[List] view. Delete existing monitor settings with the following operation.

1. Select the monitor setting which you would like to delete from the Monitor Setting[List] view.
2. Click the "Delete" button from the Monitor Setting[List] view.
3. After confirming the deletion details displayed in the confirmation dialog, and if there are no problems, then click the "OK" button.

Further, if you delete the settings ("Collect" is valid in the monitor settings) for a monitor result that has accumulated "Numeric Monitoring", by default the collection values that had been collected to that point by that monitor setting will be deleted when the monitor setting is deleted.

This setting can be changed. Refer to 7.9 "Numeric Value Monitoring Collection Value Setting" in the Administrator's Guide for details.

6.5.5 Monitor Enable for the Monitor Setting

With Hinemos, the various monitor settings can be saved as Valid or Invalid. Also, the saved monitor settings can be enabled or disabled at any time by user operation.

Copyright (c) 2013 NTT DATA CORPORATION

The operation to enable existing monitor settings is:

- Check the "Monitor" checkbox in the setting dialog for the various monitor settings.
- Use the "Monitor Valid" button in the Monitor Setting[List] view.

This operation can be performed with either of the above methods.

Refer to the following chapter for the setting method when enabling an existing monitor setting with the "Monitor" checkbox in the various monitor setting dialogs.

When enabling existing monitor settings, perform the following operation with the "Monitor Valid" button in the Monitor Setting[List] view.

1. Select the monitor setting that you would like to enable from the Monitor Setting[List] view. In this case, the operation to enable the monitor can be performed collectively by selecting multiple monitor settings.
2. Click the "Monitor Valid" button in the Monitor Setting[List] view.
3. After confirming the enable details displayed in the confirmation dialog, and if there are no problems, then click the "OK" button.

6.5.6 Monitor Disable for the Monitor Setting

The operation to disable existing monitor settings is:

- Remove the check from the "Monitor" checkbox in the setting dialog for the various monitor settings.
- Use the "Monitor Invalid" button in the Monitor Setting[List] view.

This operation can be performed with either of the above methods.

Refer to the following chapter for the setting method when disabling an existing monitor setting with the "Monitor" checkbox in the various monitor setting dialogs.

When disabling existing monitor settings, perform the following operation with the "Monitor Invalid" button in the Monitor Setting[List] view.

1. Select the monitor setting that you would like to disable from the Monitor Setting[List] view. In this case, the operation to disable the monitor can be performed collectively by selecting multiple monitor settings.
2. Click the "Monitor Invalid" button in the Monitor Setting[List] view.
3. After confirming the disable details displayed in the confirmation dialog, and if there are no problems, then click the "OK" button.

6.5.7 Collection Enable for the Monitor Setting

With Hinemos, when performing numeric value monitoring (refer to Numeric Monitoring for details) in the various monitor settings, the monitor results can be collected and saved for each monitor setting unit. Also, the saved monitor setting collector settings can be enabled or disabled at any time by user operation.

The operation to enable existing monitor settings collector settings is:

- Check the "Collector" checkbox in the setting dialog for the various monitor settings.
- Use the "Collector Valid" button in the Monitor Setting[List] view.

This operation can be performed with either of the above methods.

Refer to the following chapter for the setting method when disabling an existing monitor setting collector setting with the "Collector" checkbox in the various monitor setting dialogs.

When enabling existing monitor setting collector settings, perform the following operation with the "Collector Valid" button in the Monitor Setting[List] view.

1. Select the collector setting that you would like to enable from the Monitor Setting[List] view. In this case, the operation to enable the collector can be performed collectively by selecting multiple monitor settings.
2. Click the "Collector Valid" button in the Monitor Setting[List] view.

Copyright (c) 2013 NTT DATA CORPORATION

3. After confirming the enable details displayed in the confirmation dialog, and if there are no problems, then click the "OK" button.

6.5.8 Collection Disable for the Monitor Setting

The operation to disable existing monitor settings collector settings is:

- Remove the check from the "Collector" checkbox in the setting dialog for the various monitor settings.
- Use the "Collector Invalid" button in the Monitor Setting[List] view.

This operation can be performed with either of the above methods.

Refer to the following chapter for the setting method when disabling an existing monitor setting with the "Collector" checkbox in the various monitor setting dialogs.

When disabling existing monitor setting collector settings, perform the following operation with the "Collector Invalid" button in the Monitor Setting[List] view.

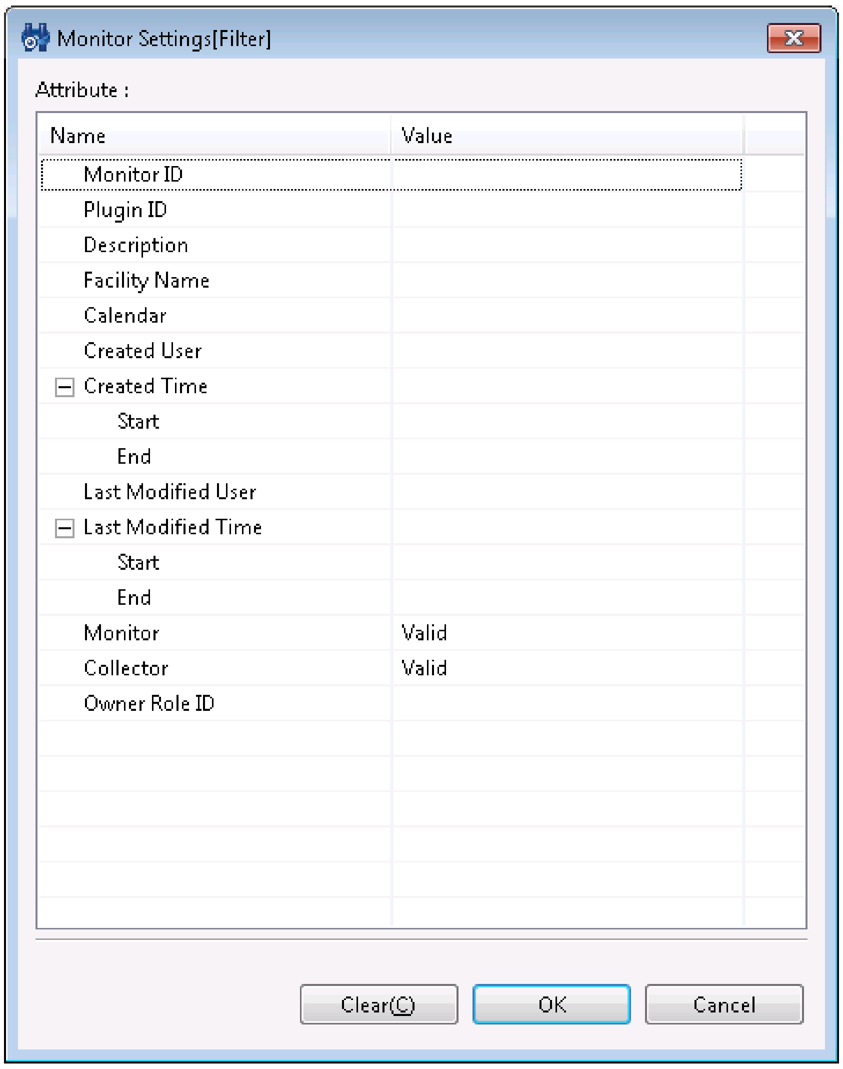
1. Select the collector setting that you would like to disable from the Monitor Setting[List] view. In this case, the operation to disable the collector can be performed collectively by selecting multiple monitor settings.
2. Click the "Collector Invalid" button in the Monitor Setting[List] view.
3. After confirming the disable details displayed in the confirmation dialog, and if there are no problems, then click the "OK" button.

6.5.9 Filtering Monitor Settings

By using the "Filter" button, you can display only those monitor settings out of the existing monitor settings that meet the filter conditions in the Monitor Settings[Filter] dialog.

1. Click the "Filter" button in the Monitor Setting[List] view. The Monitor Setting[List] dialog is displayed.

Copyright (c) 2013 NTT DATA CORPORATION



Monitor Settings[Filter]

Attribute :

Name	Value
Monitor ID	
Plugin ID	
Description	
Facility Name	
Calendar	
Created User	
⊟ Created Time	
Start	
End	
Last Modified User	
⊟ Last Modified Time	
Start	
End	
Monitor	Valid
Collector	Valid
Owner Role ID	

Figure 6-15 Monitor Setting[Filter] Dialog

2. Configure the filter condition. When an item is not included in the condition, please leave the field blank. (Please click on the "Clear" button to change the filter conditions back to the default conditions).

- Monitor ID

Make "Monitor ID" a filter condition.

- Plugin ID

Make the Plugin ID of the monitor setting a filter condition.

- Description

Make the "Description" text of the monitor setting a filter condition.

- Facility Name

Make the monitored facility name of the monitor setting a filter condition.

- Calendar

Make the calendar ID for the calendar specified in the monitor setting a filter condition.

- Created User

Make the new created user in the monitor setting a filter condition.

- Created Time

Make the created time for the monitor setting a filter condition. Clicking the button on the right side of the input field opens the time dialog. Please select a date and time. Select the date and time from the combo box.

- User Last Changed

Copyright (c) 2013 NTT DATA CORPORATION

Make the User Last Changed in the monitor setting a filter condition.

- Last Change Time

Make the Last Change Time in the monitor setting a filter condition. Clicking the button on the right side of th e input field opens the time dialog. Please select a date and time. Select the date and time from the combo box.

- Monitor

Make the "Valid", "Invalid" status in the monitor setting a filter condition.

- Collector

Make the "Valid", "Invalid" status for the collector in the monitor setting a filter condition.

-Owner Role ID

Specify an Owner Role ID of Monitor Settings as a filter condition.

7 Monitor Settings Feature (Monitor Type)

7.1 Monitor Type

There are four types of categories of monitor settings that can be created from the Monitor Settings[List].

- Numeric monitoring
- Character string monitoring
- Truth monitoring
- Trap monitoring

Following is an explanation of the characteristics of each of those features.

7.1.1 Numeric Monitoring

- Monitor Target

  With numeric monitoring, numeric values are the target of monitoring. A threshold value determination is performed for the target numeric values, the priority, Normal, Warning or Critical is judged and notification is sent. If the monitoring target numeric values cannot be obtained, the priority is "Unknown".

  i.e.) HTTP Monitor (Numeric) default setting

  - Monitor target: Response Time
  - Threshold value setting:

    Normal: (lower limit) more than 0 msec, (upper limit) up to 1000 msec

    Warning: (lower limit) more than 1000 msec, (upper limit) up to 3000 msec

    Critical: Other than normal or critical

    Unknown: Timeout occurs
  - Timeout: 5000 msec

  The monitoring target numeric values differ depending on each of the features. Refer to the section for the object feature for more information.

- Monitoring Operation

  When judgement of the priority of the monitor results for the numeric values acquired from the monitor target is performed, the priority is judged (decided) according to the following procedure.

  1. If acquisition of the numeric value for the monitor target failed (including when acquisition was attempted and timeouts) -> the priority is judged to be "Unknown"
  2. If the priority of the numeric value for the monitor target is included in the threshold value for "Normal" -> the priority is judged to be "Normal"
  3. If the priority of the numeric value for the monitor target is included in the threshold value for "Warning" -> the priority is judged to be "Warning"
  4. If the priority of the numeric value for the monitor target is not included in the threshold values for "Normal" or "Warning" -> the priority is judged to be "Critical"

- Collection value accumulation

  The monitoring target numeric value can be accumulated as the collection values only for numeric monitoring. The accumulated collection values can be displayed as a graph or downloaded in CSV format with the Performance Management feature.

  Accumulation of collection values is started by enabling the "Collector" check on the [Create - Change] dialog for monitor.

Copyright (c) 2013 NTT DATA CORPORATION

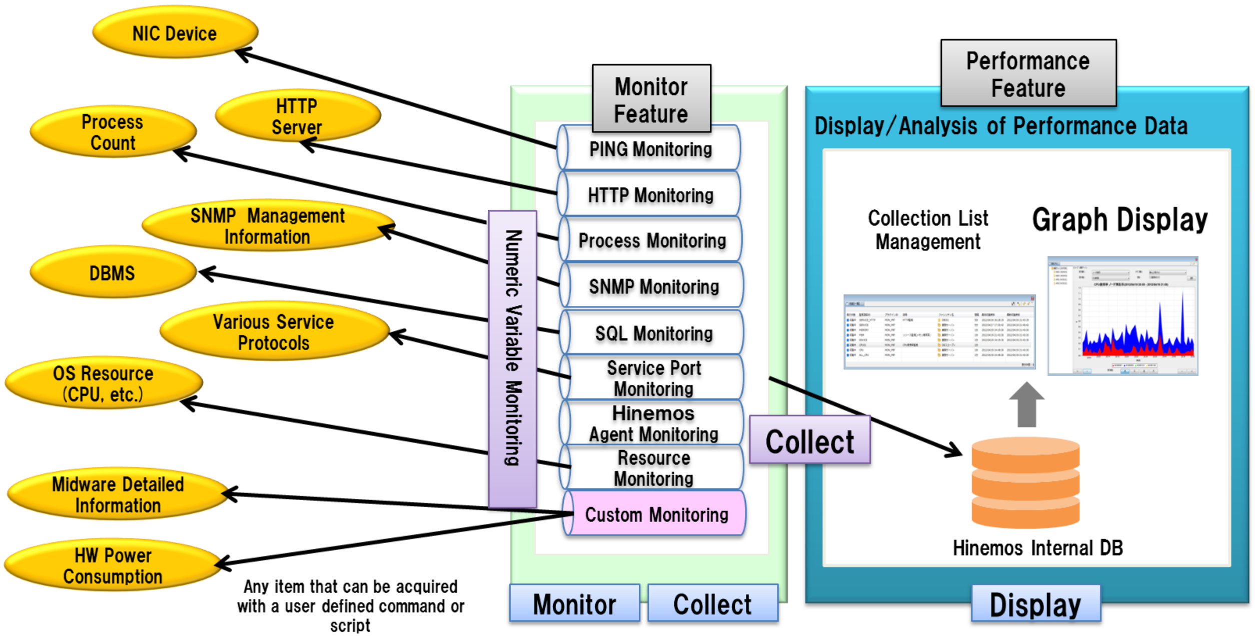


Figure 7-1 Accumulation of Numerical Monitoring and Graph Display

The numeric values handled by the Hinemos Performance Management feature become the values handled by numeric monitoring. Except for Resource Monitor, the display name for the collection value (Collected Item Name) and units (Collected Item Units) can be changed in the client setting screen.

The list of numeric values handled by numeric monitoring other than the Resource Monitor is shown in the table belo w.

Table 7-1 List of Numeric Values Handled by Numeric Monitoring Other Than Resource Monitor

Monitor Type	Collected Item Name	Collected Item Units
HTTP Monitor (Numeric value)	Response Time	msec
PING Monitor (Numeric value)	Response Time	msec
SNMP Monitor (Numeric value)	Value *1	(Blank character string)*1
SQL Monitor (Numeric value)	Value *1	(Blank character string)*1
Custom Monitor (Numeric value)	(Blank character string)*1	(Blank character string)*1
Service Port Monitor (Numeric value)	Response Time	msec
Process Monitor (Numeric value)	Number of Processes	Units

*1 The display name and units are not set up for the general monitor features.

The collection value that can be acquired with the Resource Monitor depends on the platform of the node property. You can select from Linux, Windows, Network Equipment and Other by default for the platform, but there are no co llection values that can be acquired if it is Other.

Also, SNMP (default) and WBEM are the protocols used to acquire the collection values. When these protocols differ, the collection values they can acquire also differ. Refer to 7.8 "Polling Protocol Settings" in the Administrator's G uide for the method for changing the protocol.

You can acquire detailed collection data for each device with the Resource Monitor. The device types cpu, mem, disk, nic and filesystem correspond to the specified collection value items. These collection values for each device can o nly be acquired where the repository CPU information, memory information, NIC information, disk information and fi le system information are for registered nodes. If a scope or node is specified as the monitor target, refer to the s ection on the Resource Monitor for details on the collection values for each device that can be acquired.

The numeric values handled by the Resource Monitor are shown in the table below.

Table 7-2 List of Values Collected by the Resource Monitor

Category	Collected Item Name	Collected Units	Device Type	SNMP			WBEM
				Linux	Windows	Network Equipment	Linux
CPU Related	CPU Usage	%	-	◎	o	-	◎
	CPU Usage (User)	%	-	◎	o	-	◎
	CPU Usage (System)	%	-	◎	o	-	◎
	CPU Usage (Nice Process)	%	-	◎	o	-	-
	CPU Usage (I/O Wait)	%	-	◎	o	-	◎
	CPU Usage by Core	%	cpu	◎	◎	-	-
	Interrupt Rate	count/s	-	◎	o	-	-
	Context Switches	count/s	-	◎	o	-	-
	1 Minute Load Averages	units/s	-	◎	-	-	-
	5 Minute Load Averages	units/s	-	◎	-	-	-
	15 Minute Load Averages	units/s	-	◎	-	-	-
	CPU Usage (using by VM Management Option) CPU Usage (using by VM Management Option)	Mhz	-	-	-	-	-
	CPU Deficiency (using by VM Management Option)	msec	-	-	-	-	-
Disk Related	Disk I/O Count for Each Device	count/s	disk	◎	o	-	◎
	Disk I/O Count For Each Device (Read)	count/s	disk	◎	o	-	◎
	Disk I/O Count For Each Device (Write)	count/s	disk	◎	o	-	◎
	Disk I/O Bytes For Each Device	byte/s	disk	◎	o	-	◎
	Disk I/O Bytes For Each Device (Read)	byte/s	disk	◎	o	-	◎
	Disk I/O Bytes For Each Device (Write)	byte/s	disk	◎	o	-	◎
File System Related	File System Usage	%	filesystem	◎	◎	-	-
	File System Usage (ext3)	%	filesystem	-	-	-	◎
	File System Usage (ext4)	%	filesystem	-	-	-	◎
	Mass Storage File System Usage	%	filesystem	◎*2	-	-	-

Copyright (c) 2013 NTT DATA CORPORATION

Memory Related	Memory Usage	%	-	◎	o	-	◎
	Memory Usage (Swap)	%	-	◎	o	-	◎
	Memory Usage (Physical)	%	-	◎	o	-	◎
	Swap Space Memory Usage	%	-	◎	o	-	◎
	Memory Usage in Physical Memory	%	-	◎	o	-	◎
	Physical Memory Usage (User)	%	-	◎	o	-	-
	Physical Memory Usage (Buffer)	%	-	◎	o	-	-
	Physical Memory Usage (Cached)	%	-	◎	o	-	-
	Swap I/O	kB/s	-	◎	o	-	◎
	Swap I/O (In)	kB/s	-	◎	o	-	-
	Swap I/O (Out)	kB/s	-	◎	o	-	-
	Memory Amount Used (using by VM Management Option)	MB	-	-	-	-	-
	Swap Block Count	blocks/s	-	◎	-	-	-
	Swap Block Count (In)	blocks/s	-	◎	-	-	-
	Swap Block Count (Out)	blocks/s	-	◎	-	-	-
	Swap Amount Used (using by VM Management Option)	MB	-	-	-	-	-
Network Related	Packet Count	count/s	-	◎	◎*1	◎	-
	Packet Count (received)	count/s	-	◎	◎*1	◎	-
	Packet Count (sent)	count/s	-	◎	◎*1	◎	-
	Packets For Each Device	count/s	nic	◎	◎*1	◎	-
	Packets For Each Device (received)	count/s	nic	◎	◎*1	◎	-
	Packets For Each Device (sent)	count/s	nic	◎	◎*1	◎	-
	Error Packet Count	count/s	-	◎	◎*1	◎	-
	Error Packet Count (received)	count/s	-	◎	◎*1	◎	-
	Error Packet Count (sent)	count/s	-	◎	◎*1	◎	-
	Error Packets For Each Device	count/s	nic	◎	◎*1	◎	-
	Error Packets For Each Device (received)	count/s	nic	◎	◎*1	◎	-
	Error Packets For Each Device (sent)	count/s	nic	◎	◎*1	◎	-
	Network Amount used	byte/s	-	◎	◎*1	◎	-
	Network Amount used (received)	byte/s	-	◎	◎*1	◎	-
	Network Amount used (sent)	byte/s	-	◎	◎*1	◎	-
	Network Amount Used For Each Device	byte/s	nic	◎	◎*1	◎	-
	Network Amount Used For Each Device (received)	byte/s	nic	◎	◎*1	◎	-
	Network Amount Used For Each Device (sent)	byte/s	nic	◎	◎*1	◎	-

◎ Can be used agent-lessly

o Hinemos Agent installation is required

*1 Even if you do not use the SNMP extension agent included with the Hinemos Agent, you can do the same monitoring by specifying the SNMP agent that came with OS.

*2 See Section 7.10.1, "Settings for mass storage filesystem monitoring", in the Administrator's Guide for details about Mass Storage File System Usage.

The related collection values for some of the items with Resource Monitor can be collected in a batch as specification items. The various collection values of the detail items and the specification items included in the collection values are as follows:

Copyright (c) 2013 NTT DATA CORPORATION

Table 7-3 List of Collection Values of the Specification Items and the Specification Items Included in the Collection Values

Category	Collection values of the specification items	Detail item
CPU Related	CPU Usage	CPU Usage (user)
		CPU Usage (System)
		CPU Usage (Nice Process)
		CPU Usage (IO Wait)
Disk Related	Disk IO Count For Each Device	Disk IO Count For Each Device (Read)
		Disk IO Count For Each Device (Write)
	Disk IO Amount For Each Device	Disk IO Amount For Each Device (Read)
		Disk IO Amount For Each Device (Write)
Memory Related	Memory Usage	Memory Usage (Swap)
		Memory Usage (Physical)
	Memory Usage in Physical Memory	Memory Usage in Physical Memory (user)
		Memory Usage in Physical Memory (buffer)
		Memory Usage in Physical Memory (cache)
	Swap I/O	Swap I/O (In)
		Swap I/O (Out)
	Swap Block Count	Swap Block Count (In)
		Swap I/O (Out)
Network Related	Packet Count	Packet Count (received)
		Packet Count (sent)
	Packet Count for Each Device	Packet Count for Each Device (received)
		Packet Count for Each Device (sent)
	Error Packet Count	Error Packet Count (received)
		Error Packet Count (sent)
	Error Packet Count for Each Device	Error Packet Count for Each Device (received)
		Error Packet Count for Each Device (received)
	Network Information Amount	Network Information Amount (received)
		Network Information Amount (sent)
	Network Information Amount for Each Device	Network Information Amount for Each Device (received)
		Network Information Amount for Each Device (sent)

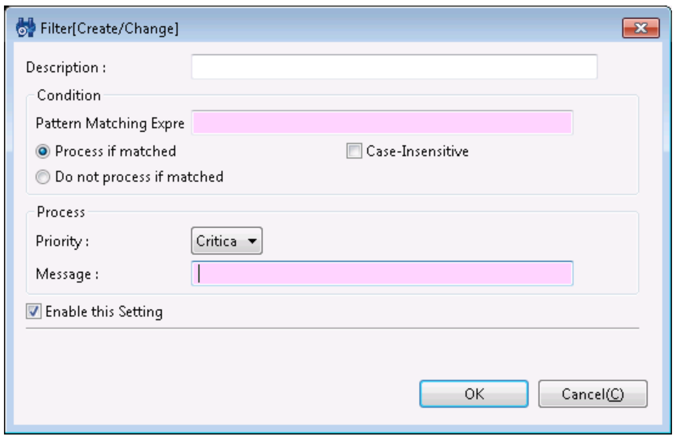
7.1.2 Character String Monitoring

- Monitor Target

Character string values are the target of character string monitoring. Filtering is performed on the filter list with pattern matching expression specified for the character strings sent or acquired from the monitoring target, and notification is performed according to the settings specified in the conforming filter conditions.

Items that can be specified as filter conditions:

- Pattern matching strings (regular expression)
- Distinguish /Do not distinguish between upper and lower case
- Process/Do not process if the condition is matched
- Priority
- Message (using the notification feature)



Filter[Create/Change]

Description :

Condition

Pattern Matching Expre

● Process if matched □ Case-Insensitive

○ Do not process if matched

Process

Priority : Critica

Message :

☑ Enable this Setting

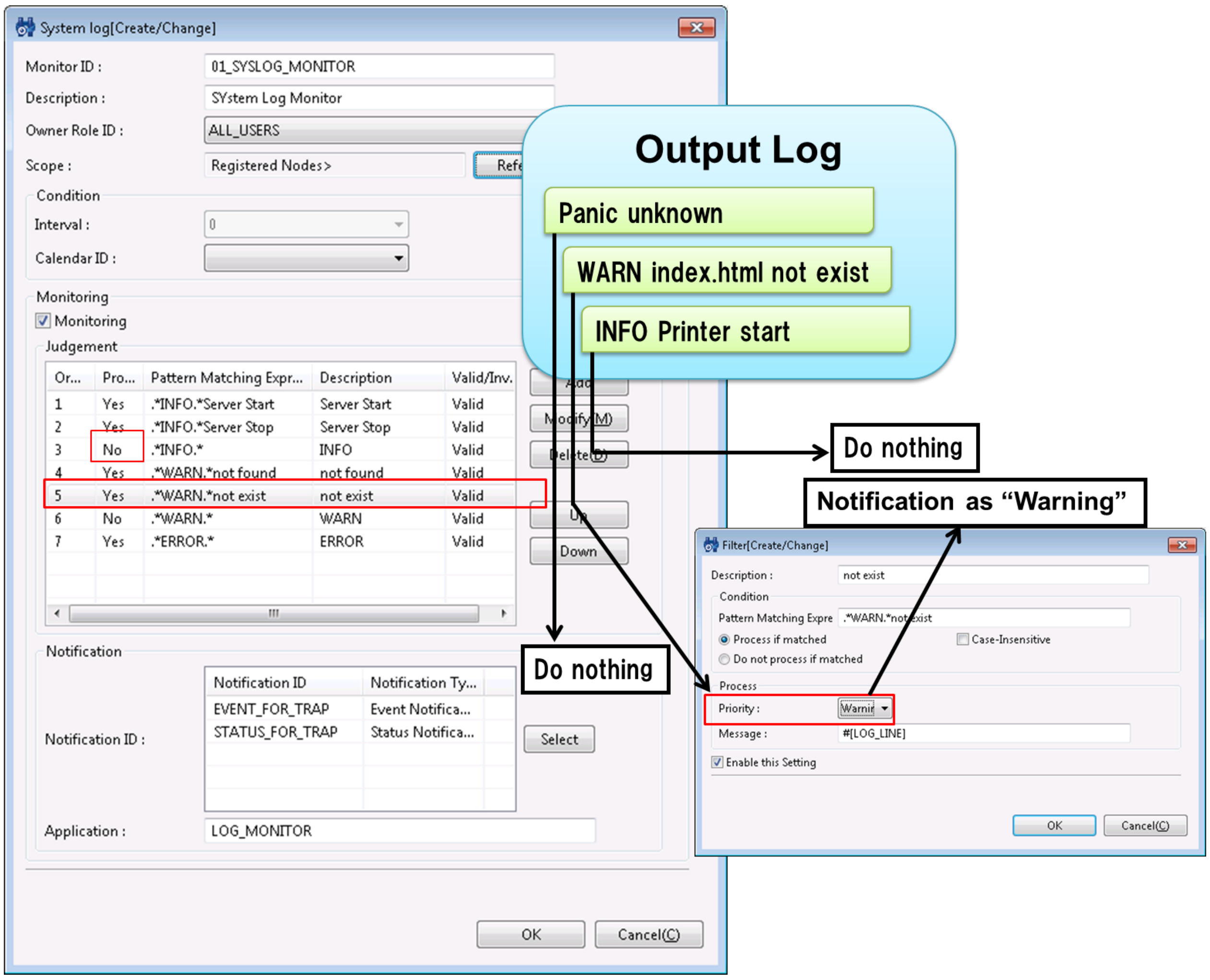
Figure 7-2 Filter [Create/Change] Dialog

Table 7-4 Configuration Items on Filter [Create/Change] Dialog

Configuration item		Input type	Description
Description		Text	Enter a description of the pattern matching setting.
Condition	Pattern Matching Expression	Text	Specify a string for the pattern matching condition in regular expression.
	Process if matched No/Yes	Radio Button	· Process if matched If the specified pattern matching expression matches, follow the setting defined by the process and it is a notification target. · Do not process if matched If the specified pattern matching expression matches, processing will not continue and it will not be a notification target.
	Case-insensitive	Checkbox	Check to perform string matching without distinguishing between upper and lower case characters.
Processing	Priority	Select from list	Select the notification priority.
	Message	Text	Enter a message in alphanumeric text. *The replacement string #[LOG_LINE] can be specified for System Log Monitor, Logfile Monitor and Windows Event Monitor. #[LOG_LINE] can replace the details of detected logs.
Enable this Setting		Checkbox	Pattern matching condition is enabled when checked. If not checked, the pattern matching setting cannot be used for string matching.

- Monitoring Operation

An order is defined for each filter condition in the filter list where the pattern matching strings are defined. Filtering is performed in order from the newest. If there are multiple filter conditions that match, the processing defined by the first matching filter is performed. No processing is performed if there are no matching filter conditions.



System log[Create/Change]

Monitor ID : 01_SYSLOG_MONITOR

Description : SYstem Log Monitor

Owner Role ID : ALL_USERS

Scope : Registered Nodes>

Condition

Interval : 0

Calendar ID :

Monitoring

☑ Monitoring

Judgement

Or...	Pro...	Pattern Matching Expr...	Description	Valid/Inv.
1	Yes	.*INFO.*Server Start	Server Start	Valid
2	Yes	.*INFO.*Server Stop	Server Stop	Valid
3	No	.*INFO.*	INFO	Valid
4	Yes	.*WARN.*not found	not found	Valid
5	Yes	.*WARN.*not exist	not exist	Valid
6	No	.*WARN.*	WARN	Valid
7	Yes	.*ERROR.*	ERROR	Valid

Notification

Notification ID :

Notification ID	Notification Ty...
EVENT_FOR_TRAP	Event Notifica...
STATUS_FOR_TRAP	Status Notifica...

Application : LOG_MONITOR

Filter[Create/Change]

Description : not exist

Condition

Pattern Matching Expre .*WARN.*not exist

● Process if matched

○ Do not process if matched

□ Case-Insensitive

Process

Priority : Warnir

Message : #[LOG_LINE]

☑ Enable this Setting

Figure 7-3 String Filtering

7.1.3 Truth Monitoring

- Monitor Target

  Truth monitoring judges whether the status of the monitoring target is "OK" or "NG" (no good) and monitors the judged result. A priority of Normal, Warning, Critical or Unknown is set for each "OK" and "NG". If acquisition of information for the status of the object being monitored fails, and the monitoring judgement cannot be performed, the priority of the judgement results is Unknown.

7.1.4 TRAP Monitoring

- Monitor Target

  This category only applies to SNMPTRAP Monitoring. Which OID for the MIB is monitored is set in the monitoring target. A priority of Normal, Warning, Critical or Unknown can be set for each of these OIDs. If there is an OID that matches the SNMPTRAP that was sent, notification is sent with the defined priority.

7.2 Monitor Classification

Hinemos has various monitoring features to enable support for varied applications and objectives. An explanation of the details of each feature is given in the following chapter, but the application and objectives of each monitoring feature is classified and a summary explanation is given here. (*)

- General IP network device Alive/Status Monitoring

PING Monitor	Monitors the Alive status by judging whether or not there is a PING response from the monitoring target.
SNMPTRAP Monitor	Acquires the status of the target device by receiving the SNMPTRAP from the target device.

- Product and Process Alive/Status Monitoring

Hinemos Agent Monitor	Monitors the Alive status of the Hinemos Agent.
HTTP Monitor	Monitors the status from the HTTP response details, existence of a response and the response time for the Web server.
SQL Monitor	Monitors the status from the SQL response details, existence of a response and the response time for the DB server.
Process Monitor	Monitors the status from the number of processes that are running.
Windows Service Monitor	Monitors the Windows service status.
Service Port Monitor	Monitors the status from existence of a response and the response time for a specific service port.
SNMPTRAP Monitor	Monitors the status by the SNMPTRAP generated by processes such as middleware.

- Resource status monitoring for the various devices

Resource Monitor	Acquires resource information for the monitoring target and monitors that status.

- Log message monitoring

System Log Monitor	Monitors the messages output by the system logs of the various OSs.
Logfile Monitor	Monitors the messages output by a particular log file.
Windwos Event Monitor	Monitors the messages output by the Windows Event Log.

- General / Extensible monitor feature

SNMP Monitor	Monitors details of the response from the general protocol SNMP.
Custom Monitor	Monitors the execution results of a user defined command or script.

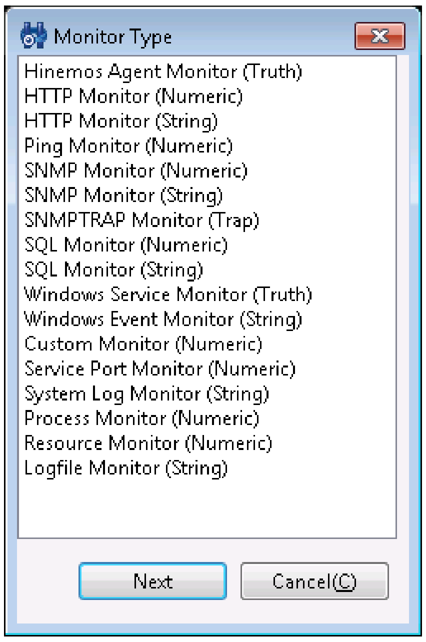
(*) There may be some redundancy depending on usage because they can be used for a variety of applications.

7.3 Hinemos Agent Monitor

The Hinemos Agent monitor feature monitors the Hinemos Agent status and provides notification. The Hinemos Agent monitor feature belongs to the truth monitoring category.

The Hinemos Agent monitor is set up from the Hinemos Agent[Create/Change] dialog. The Hinemos Agent[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Settings[List] view.
2. Select Hinemos Agent Monitor (Truth) from the Monitor Type dialog, and click the "Next" button.



Monitor Type

Hinemos Agent Monitor (Truth)
HTTP Monitor (Numeric)
HTTP Monitor (String)
Ping Monitor (Numeric)
SNMP Monitor (Numeric)
SNMP Monitor (String)
SNMPTRAP Monitor (Trap)
SQL Monitor (Numeric)
SQL Monitor (String)
Windows Service Monitor (Truth)
Windows Event Monitor (String)
Custom Monitor (Numeric)
Service Port Monitor (Numeric)
System Log Monitor (String)
Process Monitor (Numeric)
Resource Monitor (Numeric)
Logfile Monitor (String)

Figure 7-4 Monitor Type Dialog

3. The Hinemos Agent[Create/Change] dialog opens.

Registering Monitoring Setting

1. The Hinemos Agent[Create/Change] dialog opens.
2. Set up the following items.

- Monitor ID:

  Enter the Monitor ID as text. The Monitor ID is used as an ID to identify which monitoring configuration generated the notification.

- Description:

  Enter a description of the monitoring setting as text.

- Owner Role ID:

  Select an Owner Role ID for the monitoring setting. Refer to Account Feature section for more details about Owner Role.

- Scope:

  Enter the target scope. Click the "Refer" button on the right to display the Select Scope dialog. Select the target scope from the scope tree in the dialog.

3. Set up the monitoring conditions. Enter the following items.

- Interval:

  Check the connection to the Hinemos Agent at the interval specified here.

- Calendar ID:

  Select the calendar ID for the calendar you want to set up. Monitoring is enabled only during the period configured as working hours in the calendar (Refer to the section, Calendar Feature for more details on the calendar). If Calendar ID is not selected, the monitoring is enabled all day.

4. Specify whether to enable this setting. Set it with the checkbox below.

   When checked, the setting is enabled. If unchecked and it is specified as disabled, the setting is saved, but the monitoring process will not be executed.

5. Define the priority for each monitor result. Enter the following items.

- OK:

  If the connection status with the Hinemos Agent is checked and communication is possible, notification is made with the priority set here.

- NG:

  If the connection status with the Hinemos Agent is checked and communication is not possible, notification is made with the priority set here.

6. Configure the notification details. Enter the following items.

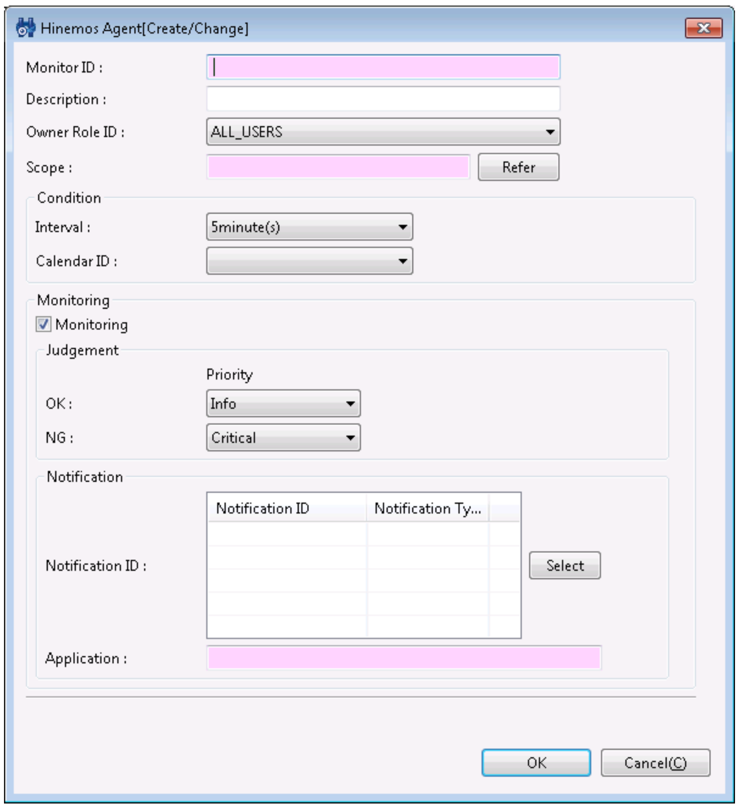
- Notification ID:

  Select from the list the Notification ID that is the notification method used in the notification setting. (Refer to the section Notification Feature regarding notification settings) When you click the "Select" button on the right, the Notification[List] dialog is displayed. Select the notification method.

- Application:

  Enter an application name in alphanumeric text. This is displayed as the notification information.

7. Click the "OK" button. The newly created setting is added to the setting list.


Hinemos Agent[Create/Change]

Owner Role ID : ALL_USERS

Interval : 5minute(s)

☑ Monitoring

OK : Info

NG : Critical

Figure 7-5 Hinemos Agent[Create/Change] Dialog

Changing the Monitor Settings

1. Select the object to change from the monitor setting list displayed in the Monitor Settings[List] dialog, then click the "Modify" button. The Hinemos Agent[Create/Change] dialog opens.
2. Edit the setting details, and then click the "OK" button. (Refer to "Registering Monitor Setting" for the procedures for entering settings)

Deleting Monitor Setting

Select the object to delete from the monitor setting list displayed in the Monitor Settings[List] dialog, then click the "Delete" button.

Changing the Valid/Invalid Setting in the Monitor Setting

You can collectively change the valid/invalid settings in the monitor setting. Select the settings to change from the monitor setting list displayed in the Monitor Settings[List] dialog (multiple can be selected). Then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

Table 7-5 Configuration Items of Hinemos Agent Monitor

Configuration item	Input type	Description

Monitor ID			Text	Enter an ID to identify which notification setting caused the notification.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar
Monitor	Monitor		Checkbox	When checked, the monitoring setting is enabled. If unchecked, the setting is disabled. The setting will be saved, but the monitoring process will not be executed.
	OK/NG	Priority	Select from list	If the monitor result is judged to be OK/NG, the priority for notification of the monitor results is specified.
Notification	Notification ID		Select from list	Select a notification ID to be used as a notification method.
	Application		Text	Enter an application name to be displayed as the notification information.

7.4 HTTP Monitor

The HTTP Monitor feature monitors the WEB server status using the HTTP(HTTPS) protocol and provides notification of those results. The HTTP Monitor feature belongs in the category of numeric monitoring or string monitoring.

The following two types of monitoring methods are provided.

- Threshold monitoring of the response time of the HTTP request
- String matching on the page obtained by the HTTP request

Further, perform the setup for HTTPS described in 7.3 "HTTP Monitor" in the Administrator's Guide when monitoring the WEB server status using the HTTPS protocol.

HTTP Monitor is setup in the HTTP[Create/Change] dialog. The HTTP[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Settings[List] view.
2. The HTTP[Create/Change] dialog opens.

   - To perform threshold monitoring of the response time of the HTTP request, select HTTP Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
   - To perform string matching on the page obtained by the HTTP request, select HTTP Monitor (String) from the Monitor Type dialog and click the "Next" button.

3. The HTTP[Create/Change] dialog opens.

Registering Monitoring Setting

To register threshold monitoring of the response time of the HTTP request

1. Click the "Create" button in the upper right part of the Monitor Settings[List] view to display the "Monitor Type" dialog.
2. Select HTTP Monitor (Numeric) and click the "Next" button to display the HTTP[Create/Change] dialog.
3. Enter the following items for the monitor target.

- Monitor ID:

  Enter the Monitor ID as text. The Message ID is used as an ID to identify the monitor setting that output the message information.

- Description:

  Enter a description for the monitoring setting as text.

- Owner Role ID:

  Select an Owner Role ID for the monitoring setting. Refer to Account Feature section for more details about Owner Role.

- Scope:

  Click the "Refer" button shown on the right to display the Select Scope dialog. Select the scope or node that is monitor target from the scope tree in the displayed dialog. If you selected a scope, all of the nodes assigned under it are monitor targets.

4. Enter the following items for the monitor setting operation.

- Interval:

  This is the interval for monitor setting operation. An HTTP request is generated and the Web server status is confirmed at this interval.

- Calendar ID:

  The Calendar ID registered to the calendar feature is assigned and the interval for monitor setting operation can be specified. The monitor setting will only operate at the interval specified as the operating times in the calendar. (Refer to the section, Calendar Feature for more details on the calendar)

  The monitor settings will always operate if a Calendar ID is not selected.

- Check Settings:
- URL

  Enter the URL that is the object of the HTTP request as text.

  The URL can be set up to a maximum of 2083 characters. A node variable can also be included in the URL string. (Refer to Table 7-24, Node Variable List, regarding node variables)

  Example: http://#[IP_ADDRESS]/index.html

- Time out (msec)

  Enter the time-out value for the HTTP request. When there is a timeout because the Web server response was late, it is notified with the priority "Unknown".

5. Enter the following items for the value of the threshold value judgement for the monitor target.

- Monitor:

  Checked when judging the threshold value against the response time for the HTTP request.

- Response Time (msec):

  Enter the threshold value for the response time of the HTTP request.

  If within the range of "Information", it is notified as "Information" priority.

  If it is outside the range of "Information" and is in the range of "Warning", it is notified as "Warning" priority.

  If it is not in the range of "Information" or "Warning", it is notified as "Critical" priority.

- Notification ID:

  Click the "Select" button shown on the right to display the Notification[List] dialog.

  Select the Notification ID assigned to the monitor target from the Notification ID list registered in the notification feature shown in the dialog. (Refer to Notification Feature regarding the notification setup)

- Application:

  Enter the string to be displayed as the application name for the notification feature as text.

6. Enter the following items for the value of the collection for the monitor target.

- Collector:

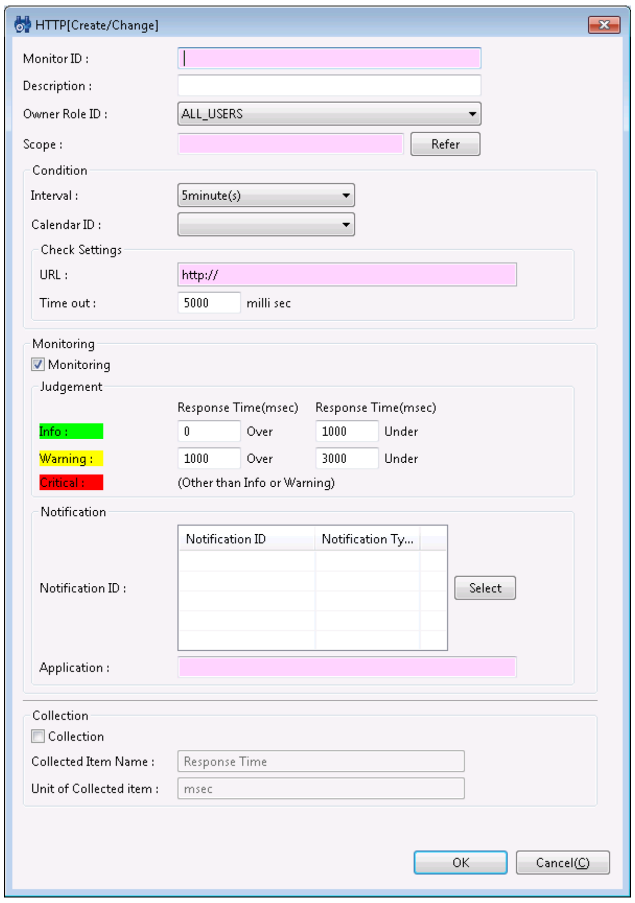
  Checked when collecting and accumulating the response time for the HTTP request. This is connected to the Performance Management feature and the accumulated response time can be displayed as a graph.

- Collected Item Name:

  Enter the display name for the collected value. This display name is used by the Performance Management feature's graph, etc.

- Collection units:

  Enter the units for the collected value. These units are used by the Performance Management feature's graph, etc.


HTTP[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

URL : http://

Time out : 5000 milli sec

Monitoring

☑ Monitoring

Judgement

	Response Time(msec)		Response Time(msec)	
Info :	0	Over	1000	Under
Warning :	1000	Over	3000	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Collection

☐ Collection

Collected Item Name : Response Time

Unit of Collected item : msec

Figure 7-6 HTTP[Create/Change] Dialog (Numeric)

7. Edit the necessary items, then click the "OK" button

To register the character matching monitor setting for the data acquired with the HTTP request

1. Click the "Create" button in the upper right part of the Monitor Settings[List] view to display the "Monitor Type" dialog.
2. Select HTTP Monitor (String) and click the "Next" button to display the HTTP[Create/Change] dialog.
3. Enter the following items for the monitor target.

- Monitor ID:

  Enter the Monitor ID as text. The Message ID is used as an ID to identify the monitor setting that output the message information.

- Description:

  Enter a description for the monitoring setting as text.

- Owner Role ID:

  Select an Owner Role ID for the monitoring setting. Refer to Account Feature section for more details about Owner Role.

- Scope:

  Click the "Refer" button shown on the right to display the Select Scope dialog. Select the scope or node that is monitor target from the scope tree in the displayed dialog. If you selected a scope, all of the nodes assigned under it are monitor targets.

Copyright (c) 2013 NTT DATA CORPORATION

4. Enter the following items for the monitor setting operation.

- Interval:

  This is the interval for monitor setting operation. An HTTP request is generated and the Web server status is confirmed at this interval.

- Calendar ID:

  The Calendar ID registered to the calendar feature is assigned and the interval for monitor setting operation can be specified. The monitor setting will only operate at the interval specified as the operating times in the calendar. (Refer to the section, Calendar Feature for more details on the calendar)

  The monitor settings will always operate if a Calendar ID is not selected.

- Check Settings:

  - URL

    Enter the URL that is the object of the HTTP request as text. The URL can be set up to a maximum of 2083 characters. A node variable can also be included in the URL string. (Refer to Table 7-24, Node Variable List, regarding node variables)

    Example: http://#[IP_ADDRESS]/index.html

  - Time out (msec)

    Enter the time-out value for the HTTP request. When there is a timeout because the Web server response was late, it is notified with the priority "Unknown".

5. Enter the following items related to string matching for the monitor target.

- Monitor:

  For the data (string) obtained by HTTP request, this is checked when performing monitoring by string matching.

Copyright (c) 2013 NTT DATA CORPORATION

- Judge:

  You can add, change and delete pattern matching conditions for string matching.

  - Adding a pattern matching condition:

    Click the "Add" button, and the Filter[Create/Change] dialog is displayed.

    Edit the necessary items below, then click the "OK" button

    - Description:

      Enter a description related to the pattern matching condition as text.

    - Condition:

      - Pattern Matching Expression:

        Enter the expression to be used in string matching. (Refer to http://docs.oracle.com/javase/jp/6/api/java/util/regex/Pattern.html regarding expressions)

      - Do not classify Large/Small Characters

        Check this to do string matching without distinguishing between upper and lower case characters.

      - Process if matched:

        If a string exists in the string acquired by the HTTP request that matches the pattern matching expression, follow the settings defined in process.

      - Do not process if matched

        If a string exists in the string acquired by the HTTP request that matches the pattern matching expression, there is no further matching process.

    - Processing:

      If "Process if matched" is selected, enter the following items.

      - Priority:

        Select the priority for notification.

      - Message:

        Enter a message assigned to the notification information.

    - Enabling this Setting:

      Check this to enable the pattern matching condition.

  - Changing the Pattern Matching condition:

    From the list of pattern matching conditions displayed in Judge, select the object to change, and then click the "Modify" button. Edit the entry items in the Filter[Create/Change] dialog and click the "OK" button. (Refer to Adding Pattern Matching Conditions for the setting details for each entry item)

  - Deleting a Pattern Matching Condition:

    From the list of pattern matching conditions displayed in Judge, select the object to delete, and then click the "Delete" button.

  - Changing Precedence of Pattern Matching Conditions:

    The Matching process is processed in Order from pattern matching condition with the smallest "Order" number.

    If a matching pattern matching condition is found, the process defined in that file's settings is followed, and further pattern matching conditions will not be evaluated. To change the precedence of the pattern matching conditions, select the subject to change from the list of pattern matching conditions, and click the "Up" button or the "Down" button.

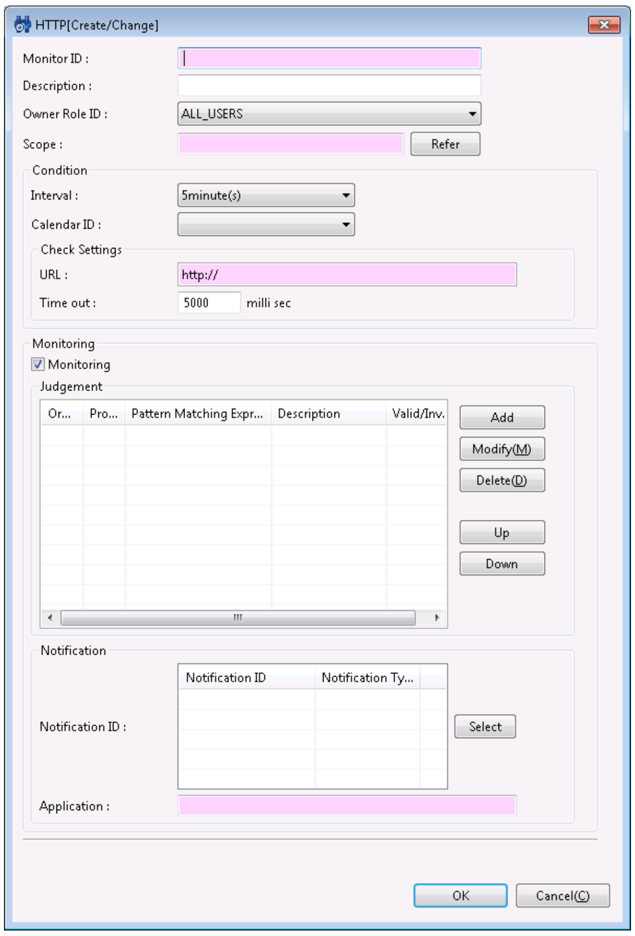
- Notification ID:

  Click the "Select" button shown on the right to display the Notification[List] dialog.

  Select the Notification ID assigned to the monitor target from the Notification ID list registered in the notification feature shown in the dialog. (Refer to Notification Feature regarding the notification setup)

- Application:

  Enter the string to be displayed as the application name for the notification feature as text.


HTTP[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

URL : http://

Time out : 5000 milli sec

Monitoring

☑ Monitoring

Judgement

Or...	Pro...	Pattern Matching Expr...	Description	Valid/Inv.

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Figure 7-7 HTTP[Create/Change] Dialog (string)

6. Edit the necessary items, then click the "OK" button

Changing the Monitor Setting

1. Select the field to change in Monitor Setting[List], then click the "Modify" button.
2. Edit the entry items in the displayed HTTP[Create/Change] dialog and click the "OK" button.

Deleting Monitor Setting

1. Select the field to delete in Monitor Setting[List], then click the "Delete" button.

Changing the Valid/Invalid Setting in the Monitor Setting

You can collectively change the valid/invalid settings in the monitor settings. Select the settings to change from the monitor setting list displayed in the Monitor Settings[List] dialog (multiple can be selected). Then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

Changing the Valid/Invalid Setting in the Collection Settings

You can collectively change the valid/invalid settings in the collection settings. Select the settings to change from the monitor setting list displayed in the Monitor Settings[List] dialog (multiple can be selected). Then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

Table 7-6 Configuration Items of HTTP Monitor (Numeric)

Configuration item	Input type	Description

Copyright (c) 2013 NTT DATA CORPORATION

Monitor ID			Text	Enter an ID to identify the monitor setting which output the notification information.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope or node as object for monitoring.
Condition	Interval		Select from list	Select the monitoring interval.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If selected, the monitor setting will operate in the time zone specified in the calendar operation time.
	Check Set up	URL	Text	Enter the URL that is the object of the HTTP request. (a node variable can be included)
		Time out(sec)	Text(numeric)	Enter the time for the HTTP request time out.
Monitor	Monitor		Checkbox	Check to perform monitoring by threshold value judgement.
	Judge	Lower Threshold	Text (numeric)	Enter the lower limit for the threshold value judgement. (To judge "More than" the lower limit)
		Upper Threshold	Text (numeric)	Specify the upper limit value for the threshold value judgement. (To judge "Less than" the upper limit)
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

Copyright (c) 2013 NTT DATA CORPORATION

Table 7-7 Configuration Items of HTTP Monitor (String)

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify the monitor setting which output the notification information.
Description			Text	Enter a description of the monitoring setting.
Scope			Select from the scope tree	Select a scope or node as object for monitoring.
Condition	Interval		Select from list	Select the monitoring interval.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If selected, the monitor setting will operate in the time zone specified in the calendar operation time.
	Check Set up	URL	Text	Enter the URL that is the object of the HTTP request. (a node variable can be included)
		Time out(sec)	Text(numeric)	Enter the time for the HTTP request time out.
Monitor	Monitor		Checkbox	Check to perform monitoring by string matching.
	Judge	Order	Change the order with the "Up" button or the "Down button	String matching is checked in order from the one with the smallest order number.
		Edit	Edit string matching with the "Add" button, the "Modify" button, or the "Delete" button	Edit the pattern matching expression to be used for string matching.
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.

Table 7-8 Detailed Conditions of the HTTP Monitor

Item	Condition
Character code for matching the string monitoring	Auto-detect HTTP response
HTTP Monitor Condition	HTTP Response ·Status code=200 ·Content-type is text Note 1) It is not possible to monitor the redirecting URL Note 2) It is not possible to monitor the string of the redirecting URL when the Web browser function transitions from a URL to a different URL Note 3) String matching is not possible if "text" is not included in "Content-type" (in this case, "Failed to check because Content-Type was not "TEXT"" is displayed) Note 4) String matching is not possible if the PDF file, the DOC file, the image file and others are directly specified as the URL (in this case, "Failed to check because Content-Type was not "TEXT"" is displayed)
Monitoring the BASIC authentication page	Monitoring is not possible with the HTTP Monitor feature
Response time of the HTTP Monitor	The period starting from the time when HTTP request is sent until the response data is received

Original message	Status code/header body **Example)** Status code: Status code=200 Header: Date, Server, Last-Modified, ... Body: <html>~</html>
Pattern matching target range	**Body:** <html>~</html>

Copyright (c) 2013 NTT DATA CORPORATION

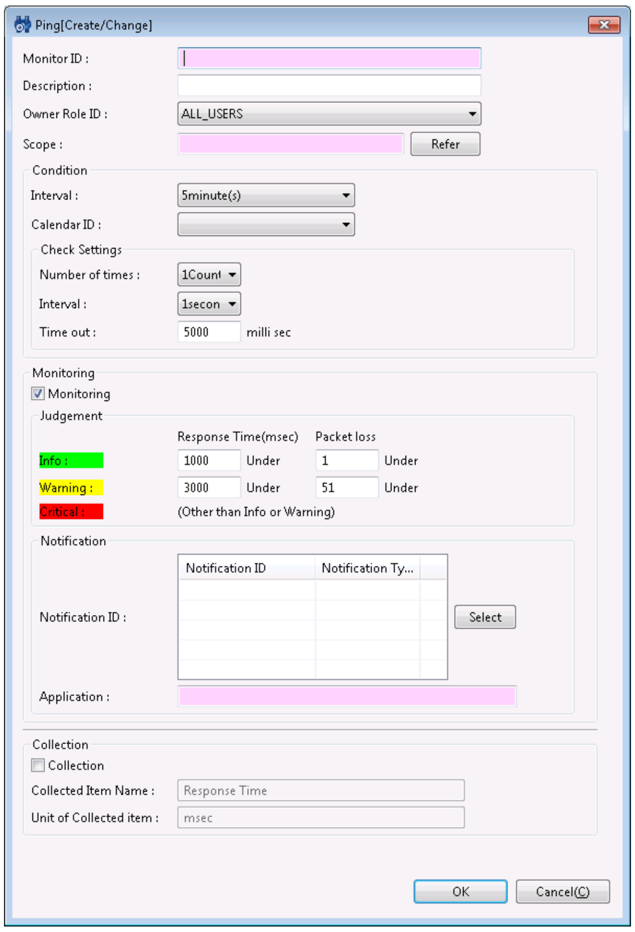
7.5 Ping Monitor

The Ping Monitor feature monitors and gives notification of the Alive status of the monitor target node by transmission and reception of a PING from the Hinemos Manager. The Ping monitor feature belongs to the truth monitoring category.

Ping Monitor is setup in the Ping[Create/Change] dialog. The Ping[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Ping Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
3. The Hinemos Agent[Create/Change] dialog opens.

Refer to the set up process in HTTP Monitor (Numeric) in HTTP Monitor for the configuration procedure from here.



Ping[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

Number of times : 1Count

Interval : 1secon

Time out : 5000 milli sec

Monitoring

☑ Monitoring

Judgement

	Response Time(msec)		Packet loss	
Info :	1000	Under	1	Under
Warning :	3000	Under	51	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Collection

□ Collection

Collected Item Name : Response Time

Unit of Collected item : msec

Figure 7-8 Ping[Create/Change] Dialog

Copyright (c) 2013 NTT DATA CORPORATION

Table 7-9 Configuration Items of Ping Monitor

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify which notification setting generated the notification.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar
	Check Settings	Number of times	Select from list	Specify the number of ping executions when checked once.
		Interval	Select from list	Specify the interval for ping executions when checked once.
		Time out(msec)	Text (numeric)	Specify the ping time-out.
Monitor	Monitor		Checkbox	Check to perform monitoring by threshold value judgement.
	Judge **Information /** Warning	Greater than or equal to Response Time (msec)	Text (numeric)	Enter the lower limit for the response time. (To judge "More than" the lower limit)
		Less than Response Time (msec)	Text (numeric)	Specify the upper limit for the response time. (To judge "Less than" the upper limit)
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

The priority for Ping Monitor is judged by the average response time for the number of times the Ping was successful.

Note) Regarding the protocol for the ping Monitor,

the default ping protocol used in Hinemos is ICMP. ICMP is a protocol generally used by ping. If a router or FW is located on the managed node, configure them so that ICMP passes through the router and FW.

Also, it is possible to change the configuration file, and then use TCP echo (TCP 7).

Copyright (c) 2013 NTT DATA CORPORATION

7.6 SNMP Monitor

The SNMP Monitor feature performs monitoring of the values acquired by SNMP polling. The SNMP Monitor feature belongs in the category of numeric monitoring or string monitoring. If a value obtained by SNMP is a numerical value, you can evaluate threshold of the numerical value. If the value obtained by SNMP is a string, you can monitor with regular expression pattern matching.

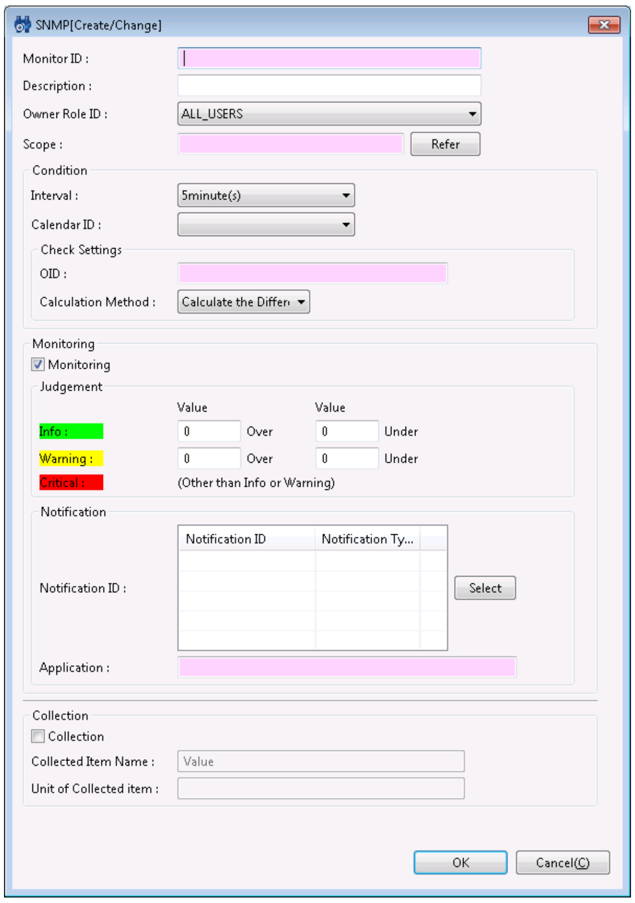
SNMP Monitor is set up in the SNMP[Create/Change] dialog. The SNMP[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. The SNMP[Create/Change] dialog will open.

- To perform threshold monitoring of the numeric value acquired by SNMP, select SNMP Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
- To perform string matching on the string acquired by SNMP, select SNMP Monitor (String) from the Monitor Type dialog and click the "Next" button.

3. The SNMP[Create/Change] dialog opens.

Refer to the setting process in HTTP Monitor (Numeric) or HTTP Monitor (String) in HTTP Monitor for the setting process from here.


SNMP[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope : Refer

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

OID :

Calculation Method : Calculate the Differ

Monitoring

☑ Monitoring

Judgement

	Value		Value	
Info :	0	Over	0	Under
Warning :	0	Over	0	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Select

Application :

Collection

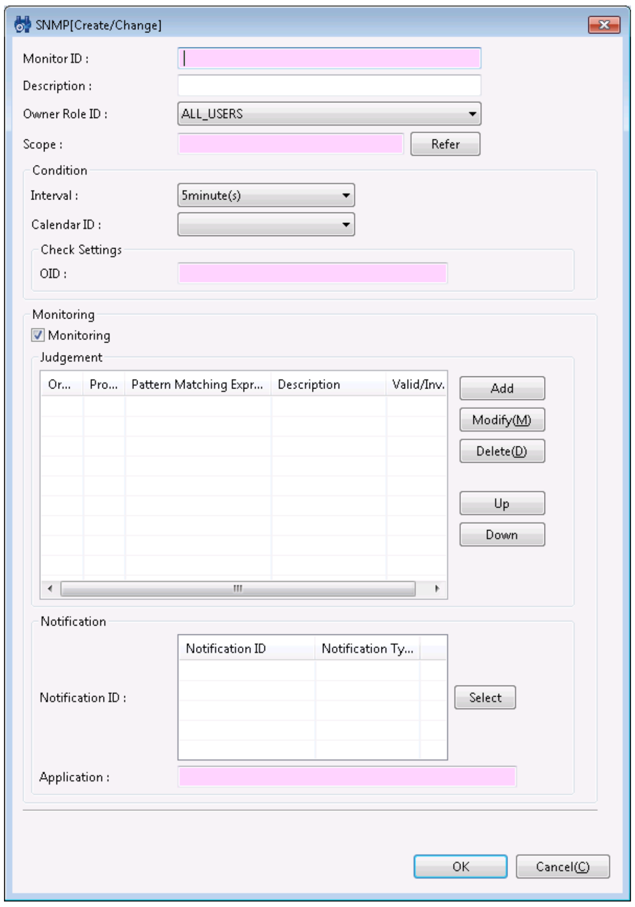
☐ Collection

Collected Item Name : Value

Unit of Collected item :

OK Cancel(C)

Figure 7-9 SNMP [Create/Change] Dialog (Numeric)



SNMP[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope : Refer

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

OID :

Monitoring

☑ Monitoring

Judgement

Or...	Pro...	Pattern Matching Expr...	Description	Valid/Inv.

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Figure 7-10 SNMP[Create/Change] Dialog (string)

Table 7-10 Configuration Items of SNMP Monitor (Numeric)

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify which notification setting generated the notification.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar
	Check Setting	OID	Text	Specify the OID for SNMP polling. (The MIB symbol name cannot be specified.)
		Calculation Method	Select from list	Specify the calculation method. ・**Do Nothing** Judge the threshold value for the acquired value as is. ・**Calculate the Difference** Judge the threshold value from the difference of the acquired value and the previously acquired value.

Copyright (c) 2013 NTT DATA CORPORATION

Monitor	Monitor		Checkbox	Check to perform monitoring by threshold value judgement.
	Judge **Information /** Warning	Greater than or equal to Acquired value	Text (numeric)	Enter the lower limit for the acquired value. (To judge "More than" the lower limit)
		Less than Acquired value	Text (numeric)	Specify the upper limit value for the acquired value. (To judge " Less than" the upper limit)
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

The following types can be monitored by the SNMP Monitor (numeric).

- Integer32
- Counter32
- Counter64
- Gauge32
- OCTET STRING (only if the obtained value can be converted into an actual value)

Table 7-11 Configuration Items of SNMP Monitor (String)

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify which notification setting generated the notification.
Description			Text	Enter a description of the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar
	Check Setting	OID	Text	Specify the OID for SNMP polling. (The MIB symbol name cannot be specified.)

Copyright (c) 2013 NTT DATA CORPORATION

Monitor	Monitor		Checkbox	Check to perform monitoring by string matching.
	Judge	Order	Change the order with the "Up" button or the "Down button	String matching is checked in order from the one with the smallest order number.
		Edit	Edit string matching with the "Add" button, the "Modify" button, or the "Delete" button	Edit the pattern matching expression to be used for string matching.
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.

Only strings comprised of ASCII can be monitored by SNMP Monitor(string).

You cannot monitor strings with multi byte characters. If multi byte characters are included in the subject string, the feature will not work effectively even if the filtered string contains only ASCII.

7.7 SNMPTRAP Monitor

SNMPTRAP Monitor allows receiving and notification of SNMPTRAPs with Hinemos Manager. The SNMPTRAP Monitor feature belongs to the Trap monitoring category.

Note) Currently, Hinemos supports SNMP protocol versions 1 and 2c for the SNMPTRAP monitoring feature usage.

The SNMP Monitor is set up in the SNMPTRAP[Create/Change] dialog. The SNMPTRAP[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select SNMP Monitor (Trap) from the Monitor Type dialog and click the "Next" button.
3. The SNMPTRAP[Create/Change] dialog opens.

Registering Settings

1. The SNMPTRAP[Create/Change] dialog opens.
2. Set up the following items.

- Monitor ID:

  Enter the Monitor ID as text. The Monitor ID is used as an ID to identify which monitoring configuration generated the notification.

- Description:

  Enter a description of the monitoring setting as text.

- Owner Role ID:

  Select an Owner Role ID for the monitoring setting. Refer to Account Feature section for more details about Owner Role.

- Scope:

  Enter the target scope. When the "Select" button on the right is clicked on, the select Scope dialog opens. Select the target scope from the scope tree in the dialog.

  "Unregistered node (UNREGISTERED)" scope can be selected in SNMPTRAP Monitor. If "Unregistered node (UNREGISTERED)" is selected here, it is processed according to the trap condition of the nodes other than nodes registered in the repository.

- Calendar ID:

  Select the calendar ID for the calendar you want to set up. Monitoring is enabled only during the period configured as working hours in the calendar (Refer to the section, Calendar Feature for more details on the calendar). If Calendar ID is not selected, the monitoring is enabled all day.

3. Set up the Community

   - Do not check community name:

     If "Don't check community name" is selected, SNMPTRAP is received for all community names, regardless of the community name.

   - Community Name

     To receive only specific community names, select "Community Name" and specify the community name.

4. Specify the Encoding Character Code

   - No Encoding Character Code:

     If "No Encoding Character Code" is selected, multi byte encoding character code will not be used in SNMPTRAP. Multi byte characters other than UTF-8 are corrupted.

   - Character Code of SNMPTRAP

     If SNMPTRAP includes multi byte characters other than UTF-8, select "Character Code of SNMPTRAP" and specify the multi byte character code included in SNMPTRAP. There are two character codes that can be entered here as the character code are EUC-JP and MS932.

5. Select the receiving trap from those below, and then click the radio button.

   - Monitor specific OID
   - Monitor all OID registered in the master DB
   - Monitor OID not registered in the master DB

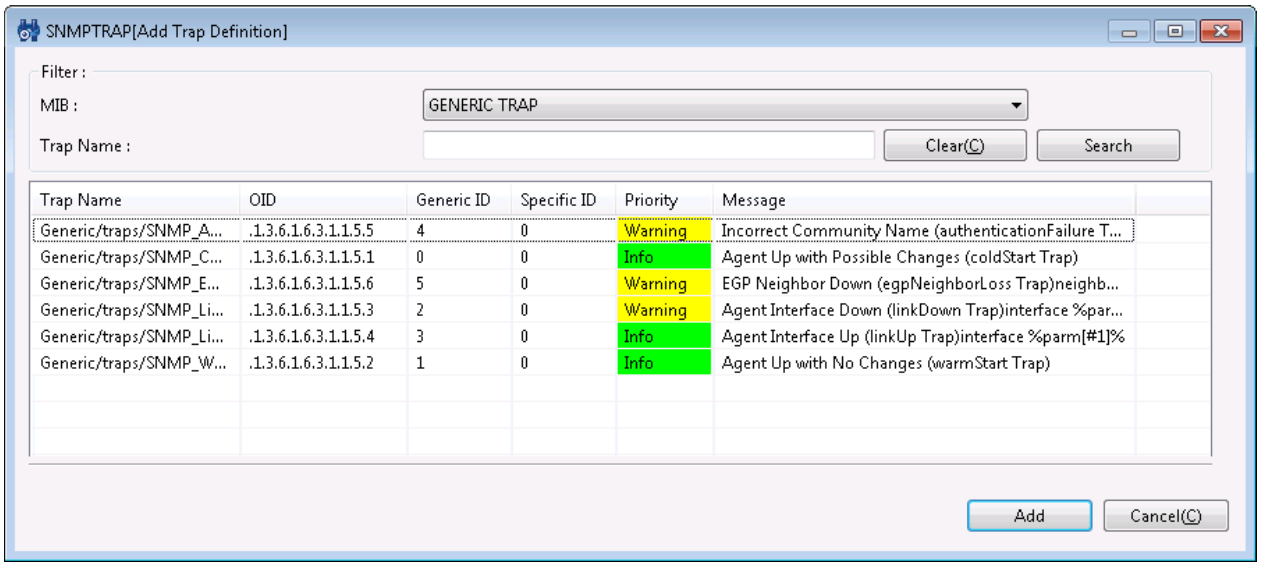
   When monitoring the specified OID, perform step 6.

6. You can add, change, and delete trap definitions using the following procedures.

   Adding Trap Definitions

   Click on the "Add" button. The SNMPTRAP[Add Trap Definition] dialog is displayed.

Copyright (c) 2013 NTT DATA CORPORATION



SNMPTRAP[Add Trap Definition]

Filter :

MIB : GENERIC TRAP

Trap Name :

Trap Name	OID	Generic ID	Specific ID	Priority	Message
Generic/traps/SNMP_A...	.1.3.6.1.6.3.1.1.5.5	4	0	Warning	Incorrect Community Name (authenticationFailure T...
Generic/traps/SNMP_C...	.1.3.6.1.6.3.1.1.5.1	0	0	Info	Agent Up with Possible Changes (coldStart Trap)
Generic/traps/SNMP_E...	.1.3.6.1.6.3.1.1.5.6	5	0	Warning	EGP Neighbor Down (egpNeighborLoss Trap)neighb...
Generic/traps/SNMP_Li...	.1.3.6.1.6.3.1.1.5.3	2	0	Warning	Agent Interface Down (linkDown Trap)interface %par...
Generic/traps/SNMP_Li...	.1.3.6.1.6.3.1.1.5.4	3	0	Info	Agent Interface Up (linkUp Trap)interface %parm[#1]%
Generic/traps/SNMP_W...	.1.3.6.1.6.3.1.1.5.2	1	0	Info	Agent Up with No Changes (warmStart Trap)

Figure 7-11 SNMPTRAP[Add Trap Definition] Dialog

From the information of trap definitions registered in the DB by the filtering, refine and display a list of traps. Filtering is performed with the following two items.

- MIB:

  Select the object MIB from the combo box list.

- Trap Name:

  Enter the matching condition for the trap name in regular expression.

Select the trap to be added (can select multiple) from the displayed refined list, and then click the "Add" button. The SNMPTRAP[Add Trap Definition] dialog closes. The trap is added in the trap list for the SNMPTRAP[Create/Change] dialog.

Changing Trap Definitions

Select the subject to be changed from the trap list (can select multiple), and then click the "Modify" button. The SNMPTRAP[Change Trap Definition] dialog opens. Edit, and then click the "OK" button.

If multiple are selected to change, The SNMPTRAP[Change Trap Definition] dialog for the next trap opens. You can make consecutive changes for multiple trap definitions. Click the "Cancel" button to end the modification of the TRAP definitions.

You can edit the following four items.

- Valid/Invalid:

  Specify whether or not to have notification when the subject trap is received.

- Priority

  Specify the priority to notify when the subject trap is received.

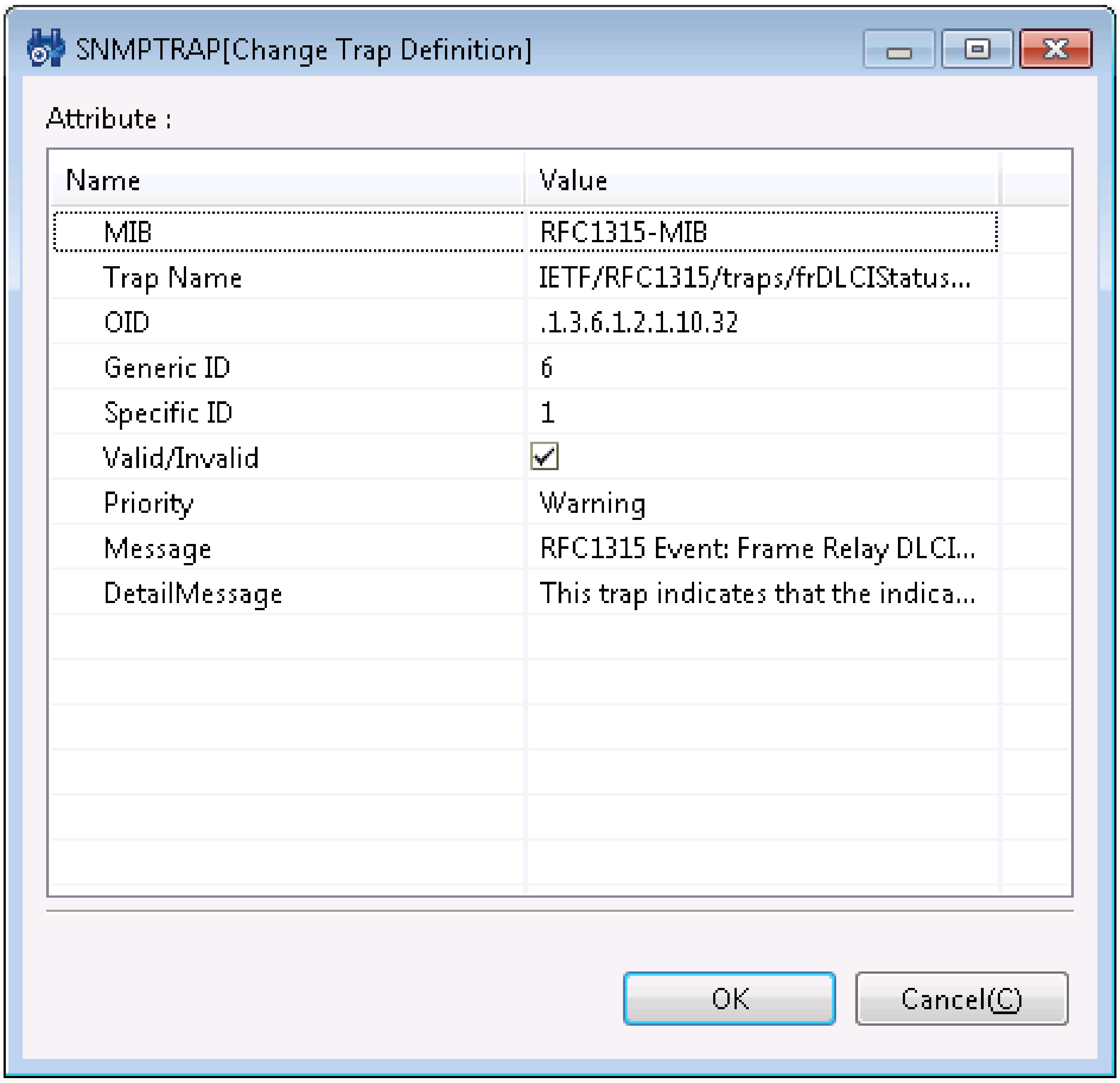
- Message

  Specify a message to notify when the subject trap is received.

- Detail Message

  Specify an original message to notify when the subject trap is received.

  In describing "%parm[#n]%", notify by replacing the n-th variable that is bound to the received trap.



Attribute :

Name	Value
MIB	RFC1315-MIB
Trap Name	IETF/RFC1315/traps/frDLCIStatus...
OID	.1.3.6.1.2.1.10.32
Generic ID	6
Specific ID	1
Valid/Invalid	☑
Priority	Warning
Message	RFC1315 Event: Frame Relay DLCI...
DetailMessage	This trap indicates that the indica...

Figure 7-12 SNMPTRAP[Change Trap Definition] Dialog

Deleting Trap Definitions

Select the subject to change from the trap list (can select multiple), then click the "Delete" button.

6. Enter the notification setting.

- Notification ID:

  Select from the list the Notification ID that is the notification method used in the notification setting. (Refer to the section Notification Feature regarding notification settings) When you click the "Select" button on the right, the Notification[List] dialog is displayed. Select the notification method.

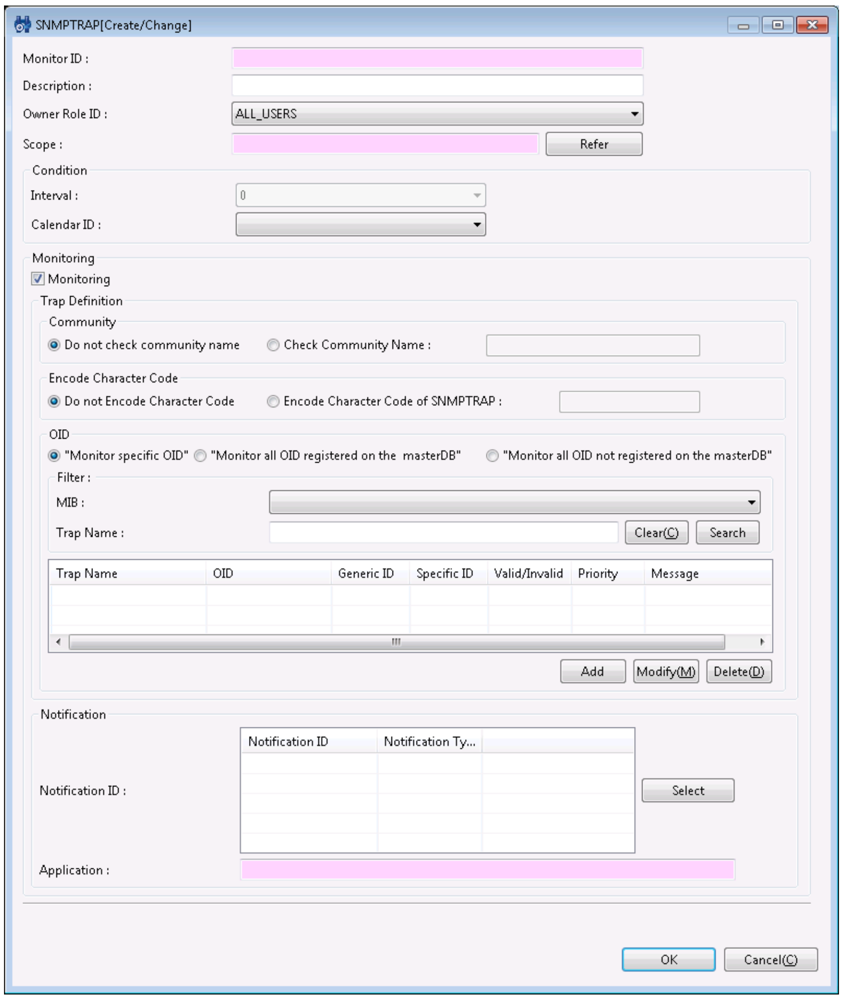
- Application:

  Enter an application name in alphanumeric text. This is displayed as the notification information.

7. Specify whether to enable this setting. Set it with the checkbox below.

- Enabling this Setting:

  When checked, the setting is enabled. If unchecked, the setting is disabled, and although the setting is saved, the monitoring process will not be executed.



Owner Role ID : ALL_USERS

Interval : 0

☑ Monitoring

● Do not check community name ○ Check Community Name :

● Do not Encode Character Code ○ Encode Character Code of SNMPTRAP :

● "Monitor specific OID" ○ "Monitor all OID registered on the masterDB" ○ "Monitor all OID not registered on the masterDB"

Figure 7-13 SNMPTRAP[Create/Change] Dialog

8. Click the "OK" button. The newly created setting is added to the setting list.

Changing the Setting

1. Select the subject to be changed from the setting list, and then click the "Modify" button. The SNMPTRAP[Create/Change] dialog will open.

2. Edit the setting details, and then click the "OK" button. (Refer to "Adding Settings" for the procedures for entering settings).

Deleting Monitor Settings

Select the object to delete from the setting list, and then click the "Delete" button.

Changing the Valid/Invalid Setting in the Monitor Settings

You can collectively change the valid/invalid settings in the monitor settings. Select the setting to change from the setting list (can select multiple). Then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

7.8 SQL Monitor

The SQL Monitor feature runs the SQL statement via the JDBC Driver for the DB server (RDBMS) and monitors the results. The SQL Monitor feature belongs in the category of numeric monitoring or string monitoring.

The following two types of monitoring methods are provided.

- Threshold monitoring for the numeric value returned as the SQL execution result
- Pattern matching for the string returned as the SQL execution result

The SQL Monitor is set up in the SQL[Create/Change] dialog. The SQL[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.

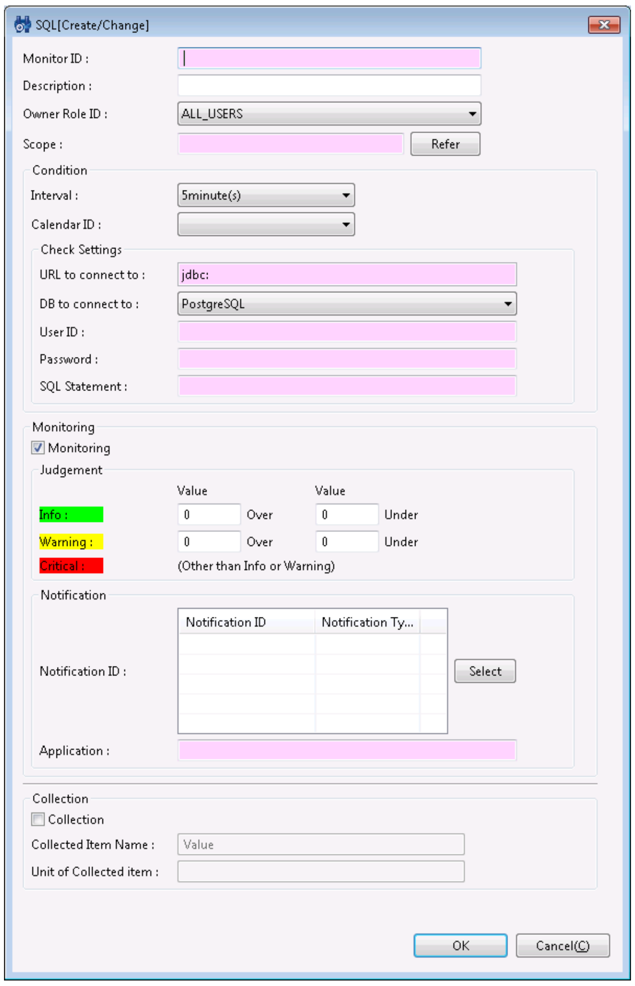
2. The SQL[Create/Change] dialog opens.

(1) To perform threshold monitoring for the numeric value returned as the SQL execution result, select SQL Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.

(2) To perform pattern matching for the string returned as the SQL execution result, select SQL Monitor (String) from the Monitor Type dialog and click the "Next" button.

3. The SQL [Create/Change] dialog opens.

Refer to the setting method in HTTP Monitor (Numeric) or HTTP Monitor (String) in HTTP Monitor for the noted process from here.


SQL[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

URL to connect to : jdbc:

DB to connect to : PostgreSQL

User ID :

Password :

SQL Statement :

Monitoring

☑ Monitoring

Judgement

	Value		Value	
Info :	0	Over	0	Under
Warning :	0	Over	0	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

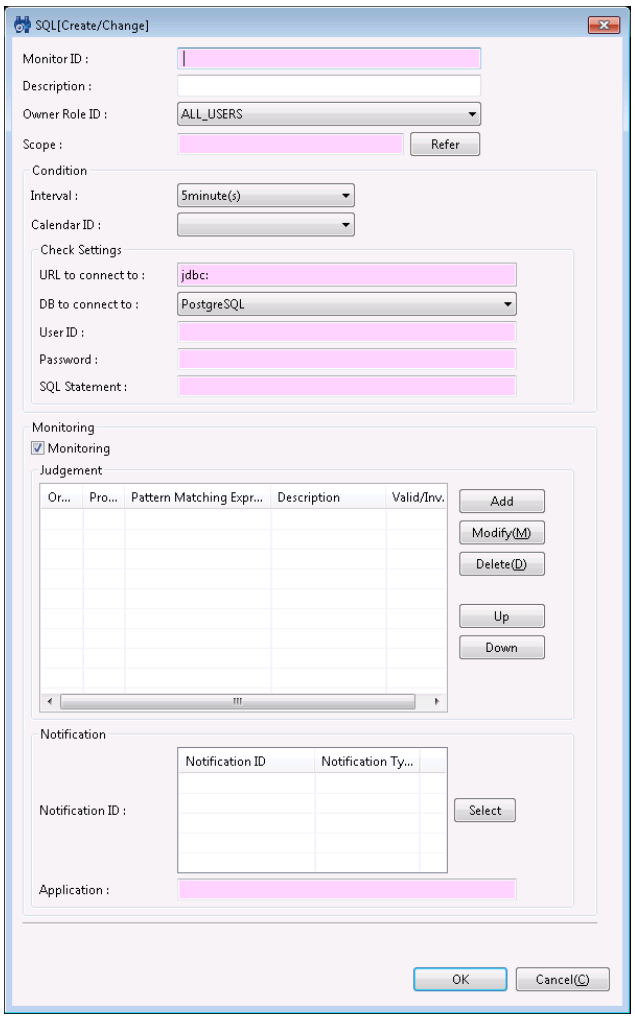
Collection

□ Collection

Collected Item Name : Value

Unit of Collected item :

Figure 7-14 SQL [Create/Change] Dialog (Numeric)



Owner Role ID : ALL_USERS

Interval : 5minute(s)

URL to connect to : jdbc:

DB to connect to : PostgreSQL

☑ Monitoring

Figure 7-15 SQL [Create/Change] Dialog (string)

Table 7-12 Configuration Items of SQL Monitor (Numeric)

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify the monitor setting which output the no tification information.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope or node as object for monitoring.
Cond ition	Interval		Select from list	Select the monitoring interval.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If s elected, the monitor setting will operate in the time zone speci fied in the calendar operation time.
	Check Set up	Connection URL	Text	Enter the URL for the RDBMS that the JDBC Driver connects to. (a node variable can be included) **Example)** jdbc:postgresql://192.168.0.1:5432/database
		Connection DB	Select from list	Select the destination RDBMS.
		User ID	Text	Input a user ID when connecting to RDBMS.
		Password	Text	Input a password when connecting to RDBMS.
		SQL State ment	Text	Specify the SQL segment (SQL segment that returns a numeric value) to run during monitoring. **Example)** select count(*) from table;

Monitor	Monitor		Checkbox	Check to perform monitoring by threshold value judgement.
	Judge	Lower Threshold	Text (numeric)	Enter the lower limit for the threshold value judgement. (To judge "More than" the lower limit)
		Upper Threshold	Text (numeric)	Specify the upper limit value for the threshold value judgement. (To judge "Less than" the upper limit)
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

Table 7-13 Configuration Items of SQL Monitor (String)

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify the monitor setting which output the notification information.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope or node as object for monitoring.
Condition	Interval		Select from list	Select the monitoring interval.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If selected, the monitor setting will operate in the time zone specified in the calendar operation time.
	Check Set up	Connection URL	Text	Enter the URL for the RDBMS that the JDBC Driver connects to. (a node variable can be included) **Example)** jdbc:postgresql://192.168.0.1:5432/database
		Connection DB	Select from list	Select the destination RDBMS.
		User ID	Text	Input a user ID when connecting to RDBMS.
		Password	Text	Input a password when connecting to RDBMS.
		SQL Statement	Text	Specify the SQL segment (SQL segment that returns a numeric value) to run during monitoring. Example) select count(*) from table;
Monitor	Monitor		Checkbox	Check to perform monitoring by string matching.
	Judge	Order	Change the order with the "Up" button or the "Down button	String matching is checked in order from the one with the smallest order number.
		Edit	Edit string matching with the "Add" button, the "Modify" button, or the "Delete" button	Edit the pattern matching expression to be used for string matching.
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.

Table 7-14 Tested RDBMS

RDBMS	JDBC Driver version
PostgreSQL 9.1.9	9.1-903 JDBC 4

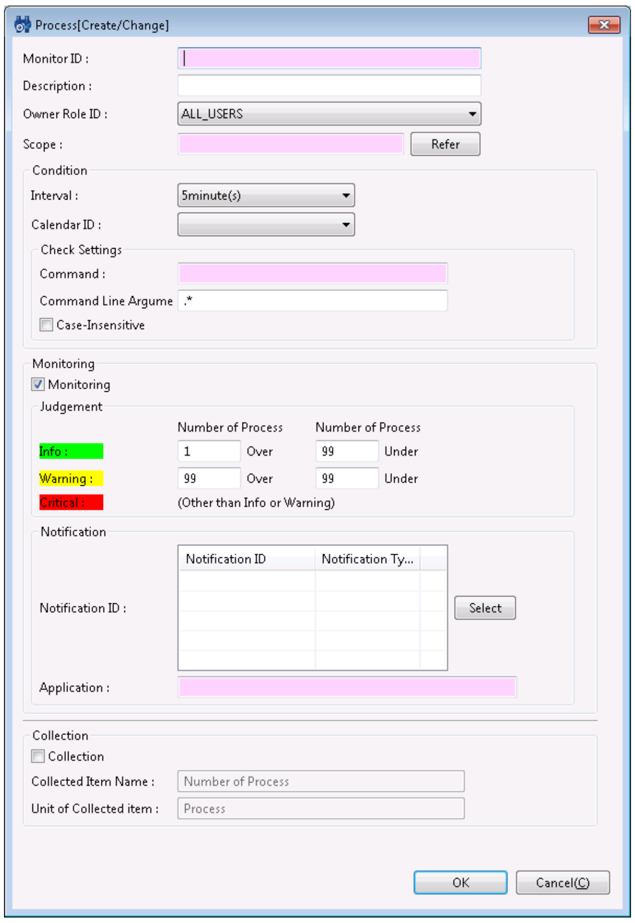
7.9 Process Monitor

The process monitor feature monitors the number of processes that are operating on the managed node with SNMP polling or WBEM polling (Linux only). The Process monitor feature belongs to the Numeric monitoring category.

The Process Monitor is set up in the Process[Create/Change] dialog. The Process[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Process Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
3. The Process [Create/Change] dialog will open.

Refer to the setting method noted in HTTP Monitor (Numeric) or HTTP Monitor (String) in HTTP Monitor for the process from here.



Process[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

Command :

Command Line Argume .*

☐ Case-Insensitive

Monitoring

☑ Monitoring

Judgement

	Number of Process		Number of Process	
Info :	1	Over	99	Under
Warning :	99	Over	99	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Collection

☐ Collection

Collected Item Name : Number of Process

Unit of Collected item : Process

Figure 7-16 Process[Create/Change] Dialog

The SNMP configuration must be registered in the repository of the managed node if changing the port number, the community name, and the SNMP version during the SNMP polling (refer to Creating/Changing/Deleting a Node for details).

If changing the connection user, the port number, the time-out, the retry count, etc. during the WBEM polling of each WBEM node, the WBEM configuration must be registered in the registered information repository of the managed node (refer to Creating/Changing/Deleting a Node for details).

Table 7-15 Configuration Items of Process Monitor

Configuration item	Input type	Description
Monitor ID	Text	Enter an ID to identify which notification setting generated the notification.

Copyright (c) 2013 NTT DATA CORPORATION

Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar
	Check Settings	Command	Text	Specify the command name of the process. It is possible to enter regular expression.
		Command Line Arguments	Text	Specify an argument of the process. Enter a regular expression. * If specifying any argument, it is necessary to enter ". *" (single-byte characters).
		Case-insensitive	Checkbox	Check this to do string matching case-insensitively.
Monitor	Monitor		Checkbox	Check to perform monitoring by threshold value judgement.
	Judge **Information /** Warning	Greater than or equal to Number of Processes	Text (numeric)	Enter the lower limit for the number of processes. (To judge "More than" the lower limit)
		Less than Number of Processes	Text (numeric)	Specify the upper limit value for the number of processes. (To judge "Less than" the upper limit)
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

Method to obtain process information

- If using SNMP

  "Command" and "Command Line Arguments" matching is performed on the results obtained for the OID below.

Table 7-16 OID for SNMP Polling to Obtain Process Information

1.3.6.1.2.1.25.4.2.1.2	(HOST-RESOURCES-MIB::hrSWRunName)
1.3.6.1.2.1.25.4.2.1.4	(HOST-RESOURCES-MIB::hrSWRunPath)
1.3.6.1.2.1.25.4.2.1.5	(HOST-RESOURCES-MIB::hrSWRunParameters)

- If using WBEM (only compatible with Linux)

  "Command" and "Command Line Arguments" matching is performed on the results obtained for the class below.

```
Linux_UnixProcess
```

Pattern matching in case of the Linux Agent

- If using SNMP

Specify "Command"

Specify "Command" from the polling execution result for 1.3.6.1.2.1.25.4.2.1.4(HOST-RESOURCES-MIB::hrSWRunPath).

- Confirmation command:

```
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.25.4.2.1.4
```

- Execution result:

```
HOST-RESOURCES-MIB::hrSWRunPath.[PID] = STRING: "[command path name]"
```

The [command path name] output here has matching by regular expression executed with the specified [Command] field.
Example)
HOST-RESOURCES-MIB::hrSWRunPath.21000 = STRING: "/usr/sbin/snmpd"

Specify "Command Line Arguments"

Specify the "Command Line Arguments" from the polling execution result for 1.3.6.1.2.1.25.4.2.1.(-RESOURCES-MIB::hrSWRunParameters).

- Confirmation command:

```
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.25.4.2.1.5
```

- Execution result:

```
HOST-RESOURCES-MIB::hrSWRunParameters.[PID] = STRING: "[startup parameter]"
```

The [startup parameter] output here has matching by regular expression executed with the specified [Command Line Arguments] field.
Example)
HOST-RESOURCES-MIB::hrSWRunParameters.21000 = STRING: "-Lsd -Lf /dev/null -p /var/run/snmpd.pid -a"

- Set up example

  If monitoring the number of above processes, configure the following.

- Command : /usr/sbin/snmpd
- Command Line Arguments : -Lsd -Lf /dev/null -p /var/run/snmpd.pid -a

Copyright (c) 2013 NTT DATA CORPORATION

- If using WBEM

  Specify "Command" and "Command Line Arguments"

  From the polling result against Linux_UnixProcess, specify the "Command" and the "Command Line Arguments" from the "Parameters" property.

  - Confirmation command:

    ```
    $ wbemcli ei 'http://(user name of target machine):(user's password of target machine)@(IP address of target machine):5988/root/cimv2:Linux_UnixProcess'
    ```

  - Execution result:

    ```
    (IP address of target machine):5988/(user name of the target machine)/cimv2:Linux_UnixProcess.CreationClassName="Linux_UnixProcess" ...partially omitted...
    Parameters="[command path name],"[argument 1]","[argument 2]" ...omitted hereafter...
    ```

  The [command path name] and the [argument] output here have the matching process by regular expression executed with the specified "Command" field and "Command Line Arguments" field.

  Example)

  (IP address of target machine):5988/root/cimv2:Linux_UnixProcess.CreationClassName="Linux_UnixProcess" ...partially omitted... Parameters="syslog-ng","-f","/etc/syslog-ng/syslog-ng.conf",ProcessNiceValue=0 ...omitted hereafter...

  - Example setting

    If monitoring the number of above processes, configure the following.

    - Command : syslog-ng
    - Command Line Arguments : -f /etc/syslog-ng/syslog-ng.conf

Pattern matching in the case of a Windows Agent

Specify "Command"

Specify "Command" from the polling result for 1.3.6.1.2.1.25.4.2.1.2(HOST-RESOURCES-MIB:: hrSWRunName) and 1.3.6.1.2.1.25.4.2.1.4(HOST-RESOURCES-MIB::hrSWRunPath).

Copyright (c) 2013 NTT DATA CORPORATION

- Confirmation command:

```
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.25.4.2.1.2
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.25.4.2.1.4
```

- Execution result:

```
HOST-RESOURCES-MIB::hrSWRunName.[PID] = STRING: "[command name]"
HOST-RESOURCES-MIB::hrSWRunPath.[PID] = STRING: "[command path name]"
```

The combined "Command name" and "Command path name" output here has matching by regular expression executed with the specified [Command] field.

Example)

HOST-RESOURCES-MIB::hrSWRunName.1372 = STRING: "snmp.exe"
HOST-RESOURCES-MIB::hrSWRunPath.1372 = STRING: "C:\WINDOWS\System32\"

In this case, the matching target is "C:\WINDOWS\System32\snmp.exe".

Specify "Command Line Arguments"

Specify the "Command Line Arguments" from the polling execution result for 1.3.6.1.2.1.25.4.2.1.(-RESOURCES-MIB::hrSWRunParameters).

- Confirmation command:

```
$ snmpwalk -c public -v 2c (IP address of target machine)  1.3.6.1.2.1.25.4.2.1.5
```

- Execution result:

```
HOST-RESOURCES-MIB::hrSWRunParameters.[PID] = STRING: "[startup parameter]"
```

The [startup parameter] output here has matching by regular expression executed with the specified [Command Line Arguments] field.

Example)

HOST-RESOURCES-MIB::hrSWRunParameters. 1372 = ""
Since the matching argument is identified blank, the "Command Line Arguments" field is configured blank.

7.10 Windows Service Monitor

The Windows Service Monitor feature monitors whether or not the specified Windows service has a status of "Started" on the management object Windows Server. The Windows Service Monitor feature belongs to the truth monitoring category.

Windows Remote Management (hereafter WinRM) must be set up on the management object Windows Server. Refer to 7.6, "Windows Service Monitor" in the Administrator's Guide regarding the method for setting up WinRM on the management object Windows Server. To connect to WinRM for the management object, the WinRM user name, password, port number, protocol, time out and retry count must be set in the Repository registration information. Refer to Creating/Changing/Deleting a Node for details.

The Windows Service Monitor is set up in the Windows Service Monitor[Create/Change] dialog. The Windows Service Monitor[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Windows Service Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
3. The Hinemos Agent[Create/Change] dialog opens.

Refer to the Hinemos Agent Monitor feature for the setting method.

Table 7-17 Configuration Items of Windows Service Monitor

Configuration item	Input type	Description

Monitor ID			Text	Enter an ID to identify which notification setting caused the notification.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar
	Check Set up	Windows Service Name	Text	Specify the Windows Service Name for the monitor target. Specified Windows Service Name This is an example of the "Service name" of the service dialog displayed in "Control Panel" - "Administrative Tools" - "Services". The service name is judged to completely agree.
Monitor	Monitor		Checkbox	When checked, the monitoring setting is enabled. If unchecked, the setting is disabled. The setting will be saved, but the monitoring process will not be executed.
	OK/NG	Priority	Select from list	If the monitor result is judged to be OK/NG, the priority for notification of the monitor results is specified.
Notification	Notification ID		Select from list	Select a notification ID to be used as a notification method.
	Application		Text	Enter an application name to be displayed as the notification information.

- Method to obtain Windows Service Information

  Windows Service Monitor uses WinRM and acquires the Windows Service Information shown in Table 7-18.

Table 7-18 Windows Service Information

Class name	Property	Description
Win32 Service	Name	Windows Service Name
Win32 Service	State	Status (Running or not)

- Windows Service Information Object

  Run the wsman command and you can confirm the information for the object of the Windows Service Monitor. (If the WinRM protocol is set up in HTTP)

  * Install the wsmancli package in the Red Hat Enterprise Linux environment to perform the operation to use this command.

  - Command for monitor (Acquire the Windows service list):

```
(root) # wsman -u [user name] -p [password] -y basic -h [IP Address] -P 5985 -d 6 \
enumerate http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_
```

  - Command for monitor (Set up the Windows service name):

```
(root) # wsman -u [user name] -p [password] -y basic -h [IP Address] -P 5985 -d 6 \
get http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Service?Name=[service name]
```

The Name property is compared to string specified in the "Windows Service Name" field and the target service is set up. Also, depending on whether the State property is "Running" or not, the status of the target service will be judged (OK/NG).

7.11 Windows Event Monitor

The Windows Event Monitor feature monitors the Windows Event Logs on monitoring targets and sends notification based on the specified conditions. The Windows Service Monitor feature belongs to the String monitoring category.

- Environmental requirements for using Windows Event Log

Table 7-19 Environmental requirements for using Windows Event Log

OS	.NET Framework	Windows PowerShell	Cmdlet
Windows Server 2003	3.5 or later	2.0	Get-EventLog
Windows Server 2003 R2			
Windows Server 2008		2.0, 3.0	Get-EventLog, Get-WinEvent
Windows Server 2008 R2			
Windows Server 2012		3.0	Get-EventLog, Get-WinEvent

In addition, Windows PowerShell Script Execution Policy need to be set as "Unrestricted" or "RemoteSigned". Use Set-ExecutionPolicy cmdlet to change the user preference for the Windows PowerShell execution policy as follows.

```
> Set-ExecutionPolicy Unrestricted
```

  - Get-EventLog : http://technet.microsoft.com/en-us/library/hh849834.aspx
  - Get-WinEvent : http://technet.microsoft.com/en-us/library/hh849682.aspx

- Acquisition of Windows Event Log

  Windows Event Monitor acquires Windows Event Log by the following commands.

  - Get-WinEvent cmdlet (Windows PowerShell)
  - Get-EventLog cmdlet (Windows PowerShell)
  - wevtutil.exe command

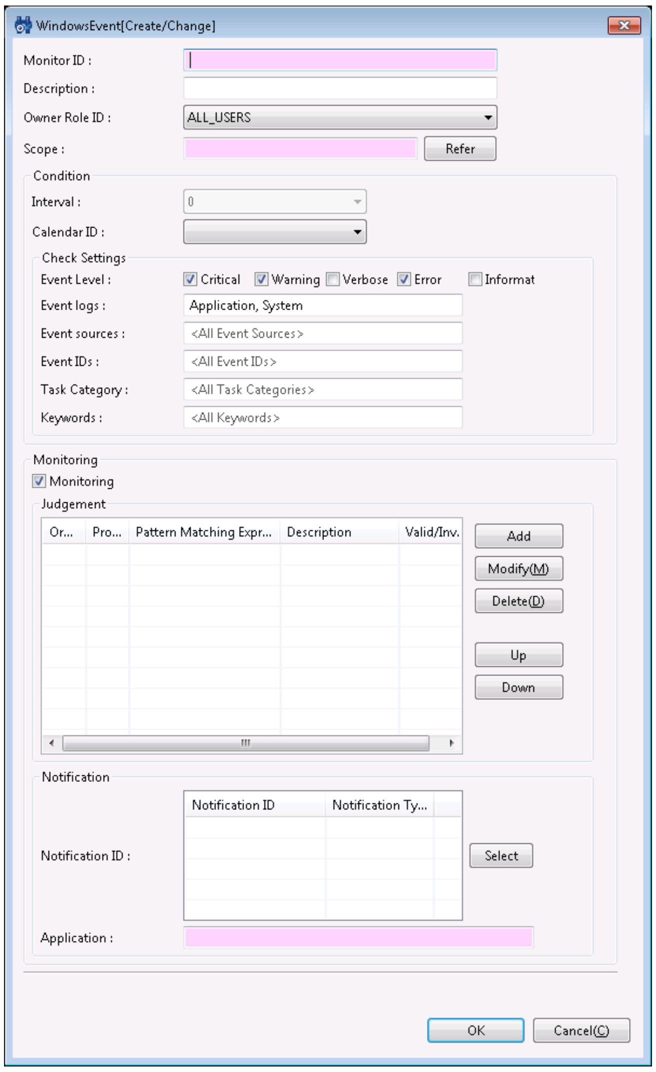
Refer to Chapter 14, Hinemos Agent Configuration List, of the Administrator's Guide for more details.

Windows Event Monitor is set up in the Windows Event[Create/Change] dialog. Follow the following steps to open the Windows Event[Create/Change] dialog.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Windows Event Monitor (String) from the Monitor Type dialog, and click the "Next" button.
3. The Windows Event[Create/Change] dialog shows up.

After these steps, follow the configuration instruction in HTTP Monitor section to proceed.

Copyright (c) 2013 NTT DATA CORPORATION



WindowsEvent[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 0

Calendar ID :

Check Settings

Event Level : ☑ Critical ☑ Warning □ Verbose ☑ Error □ Informat

Event logs : Application, System

Event sources : <All Event Sources>

Event IDs : <All Event IDs>

Task Category : <All Task Categories>

Keywords : <All Keywords>

Monitoring

☑ Monitoring

Judgement

Or...	Pro...	Pattern Matching Expr...	Description	Valid/Inv.

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Figure 7-17 Windows Event[Create/Change] Dialog

Table 7-20 Configuration Items of Windows Event Monitor

Configuration item	Input type	Description
Monitor ID	Text	Enter an ID to identify which notification setting caused the notification.
Description	Text	Enter a description of the monitoring setting.
Owner Role ID	Select from list	Select an Owner Role ID for the monitoring setting.
Scope	Select from the scope tree	Select a scope subject for monitoring.

Copyright (c) 2013 NTT DATA CORPORATION

Condition	Interval		Select from list	This monitoring is performed during log acquisition so the monitor interval cannot be selected.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If selected, the monitor setting will operate in the time zone specified in the calendar operation time.
	Check Set up	Event Level (*1)	Checkbox	Select the Event Level to monitor. (Severe/Warning/Detail/Error/Information)
		Event Log	Text (Comma delimited)	Enter the event log name of the monitoring target.
		Event Source	Text (Comma delimited)	Enter the event source name of the monitoring target.
		Event ID	Text (Numeric/Comma delimited)	Enter the event ID of the monitoring target.
		Task Category (*2)	Text (Numeric/Comma delimited)	Enter the task category of the monitoring target.
		Keyword (*3)	Text (String or Numeric/ Comma delimited)	Enter the keyword of the monitoring target.
Monitor	Monitor		Checkbox	Check to perform monitoring by string matching.
	Judge	Order	Change the order with the "Up" button or the "Down button"	String matching is checked in ascending order of order numbers.
		Edit	Edit string matching with the "Add" button, the "Modify" or the " Delete" button	Edit the pattern matching expression to be used for string matching.
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application Application	Text Text	Enter an application name that is assigned as the notification information.

***1 The "Audit Success" and "Audit Failure" of Windows Server 2003 is treated as "Information" level.**

In order to monitor "Audit Success" or "Audit Failure" on Windows Server 2003, you have to select "Information" as event level and enter "Audit Success" or "Audit Failure" as keyword.

***2 If you intend to specify a task category, you have to specify a numeric value for the category of monitoring target.**

To confirm whether a value for task category is appropriate, see "Configuration check for Windows Event Monitor" described below. However, this setting is not available on Windows Server 2003.

***3 If you intend to specify a keyword, you have to enter a specific string or number for the keyword of monitoring target.**

The specific string for the keyword is shown as Table 7-21. Besides the string, the corresponding numeric values is also available to use. To confirm whether a value for keyword is appropriate, see "Configuration check for Windows Event Monitor" described below. However, this setting is not available on Windows Server 2003.

Table 7-21 Specific Keywords of Windows Event Monitor

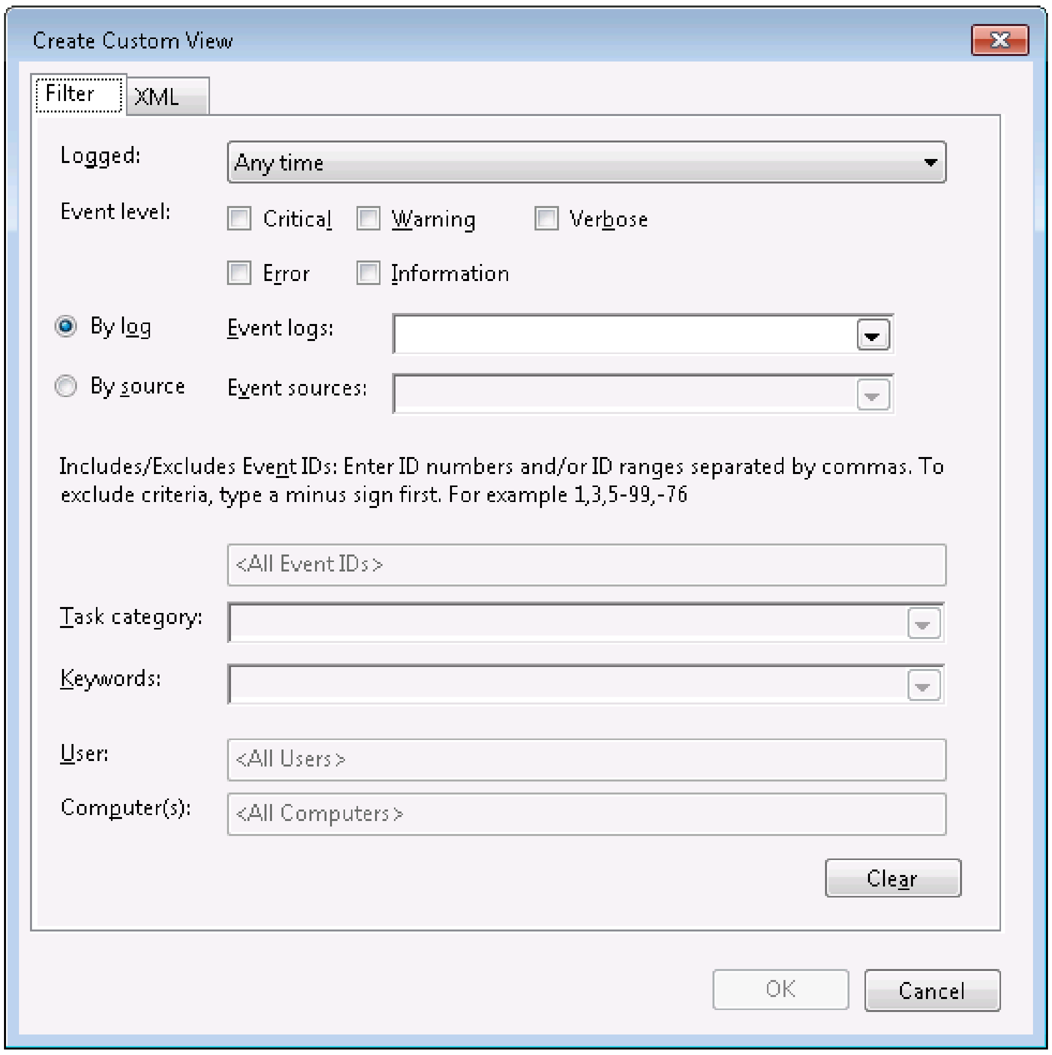
Item	Keyword (String)	Keyword (Numeric)
Audit Failure	Audit Failure FailureAudit	4503599627370496
Audit Success	Audit Success SuccessAudit	9007199254740992
Classic	Classic	36028797018963968
Correlation Hint	Correlation Hint	18014398509481984

Response Time	Response Time	281474976710656
SQM	SQM	2251799813685248
WDI Context	WDI Context	562949953421312
WDI Diagnosis	WDI Diag	1125899906842624

- Configuration check for Windows Event Monitor

  The setting values used for Windows Event Monitor are corresponding to those of Windows Event Viewer.

  A Custom View is used to display the events monitored by Windows Event Monitor. To create a Custom View, open Event Viewer and then select "Create Custom View". Fill the settings on "Filter" tab. After that, you can click on "XML" tab and all the settings entered on "Filter" tab will be shown as XML query.



Create Custom View

Filter | XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs:

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

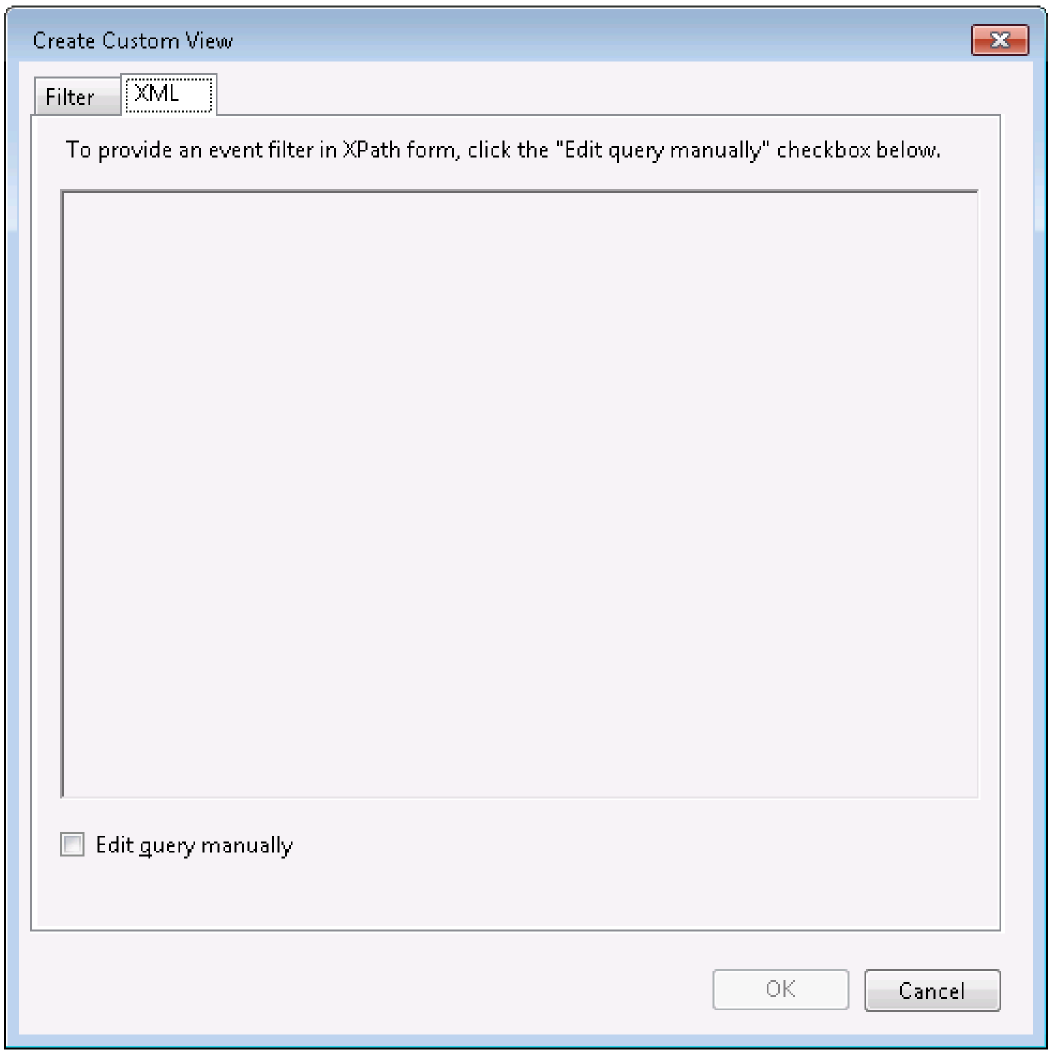
Keywords:

User: <All Users>

Computer(s): <All Computers>

Figure 7-18 Filter Tab of Event Viewer

Copyright (c) 2013 NTT DATA CORPORATION



To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

□ Edit query manually

Figure 7-19 XML Tab of Event Viewer

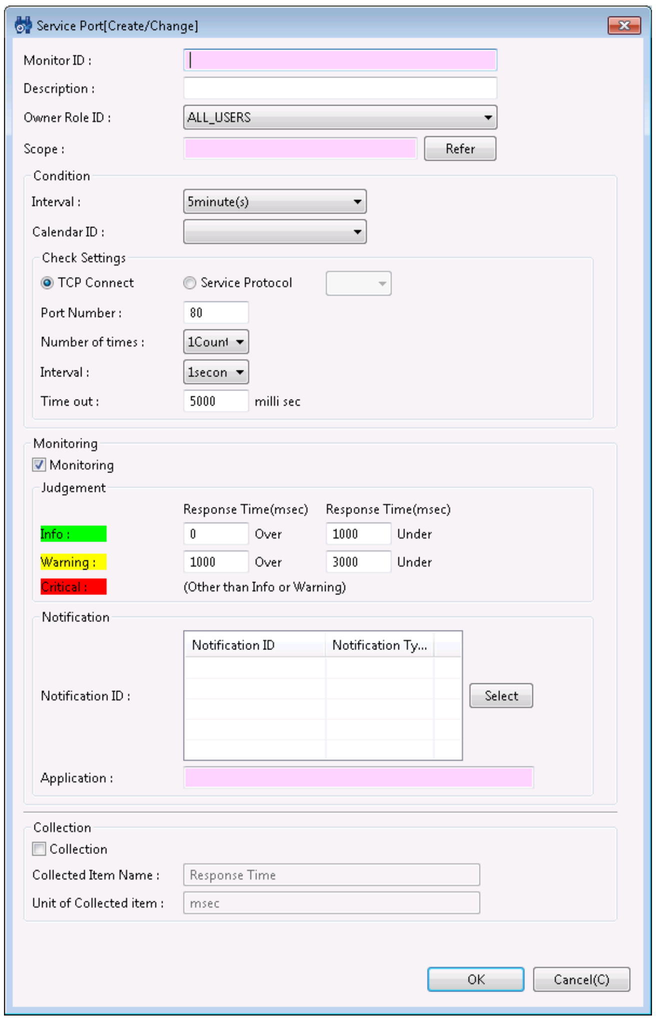
7.12 Service Port Monitor

The Service Port Monitor feature establishes a connection to the monitored node's port and monitors if the service is operating correctly on the monitored node. The Service Port Monitor feature belongs to the truth monitoring category.

The Service Port Monitor is set up from the Service Port[Create/Change] dialog. The Service Port[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Service Port Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
3. The Service Port[Create/Change] dialog opens.

Refer to the set up process in HTTP Monitor (Numeric) in HTTP Monitor for the configuration procedure from here.



Service Port[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

● TCP Connect ○ Service Protocol

Port Number : 80

Number of times : 1Count

Interval : 1secon

Time out : 5000 milli sec

Monitoring

☑ Monitoring

Judgement

	Response Time(msec)		Response Time(msec)	
Info :	0	Over	1000	Under
Warning :	1000	Over	3000	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Collection

□ Collection

Collected Item Name : Response Time

Unit of Collected item : msec

Figure 7-20 Service Port[Create/Change] Dialog

Table 7-22 Configuration Items of Service Port Monitor

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify which notification setting generated by which monitor setting.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope subject for monitoring.
Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring will be enabled only during the time when configured as working hours on the calendar.
	Check setting	TCP Connect /Service Protocol		Select the protocol to monitor. (TCP/FTP/SMTP(S)/POP3(S)/IMAP(S)/NTP/DNS)
		Port Number	Text (Numeric)	Specify the port number to monitor.
		Number of time	Select from list	Specify the number of attempts to establish the connection when checked once.
		Interval	Select from list	Specify the interval between each attempt to establish the connection when checked once.
		Time out(msec)	Text (numeric)	Specify the time-out for the connection establishment.
Monitor	Monitor		Checkbox	When checked, monitoring is enabled. If unchecked and specified disable, the configuration is saved, but the monitoring process will not be executed.
	Judge Information/Warning	Minimum of Response time (msec)	Text (numeric)	**Specify the minimum threshold of the response time.** (To judge "More than" the lower limit)
		Maximum of Response time (msec)	Text (numeric)	**Specify the maximum threshold of the response time.** (To judge "Less than" the upper limit)
	Notification	Notification ID	Select from list	Select from the list the Notification ID that is the notification method used in the notification setting.
		Application	Text	Enter an application name to be displayed as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

In Service Port Monitor, judgement of importance level will change according to the selected monitoring protocol of check setting.

- If "TCP Connect" is selected, the importance level is judged by the time used for establishing a connection.
- If "Service Protocol" is selected, the importance level is judged by the response time of each service protocol.

7.13 Custom Monitor

The Custom Monitor feature regularly runs a command specified by a user and monitors the result. The Custom monitor feature belongs to the Numeric monitoring category.

Copyright (c) 2013 NTT DATA CORPORATION

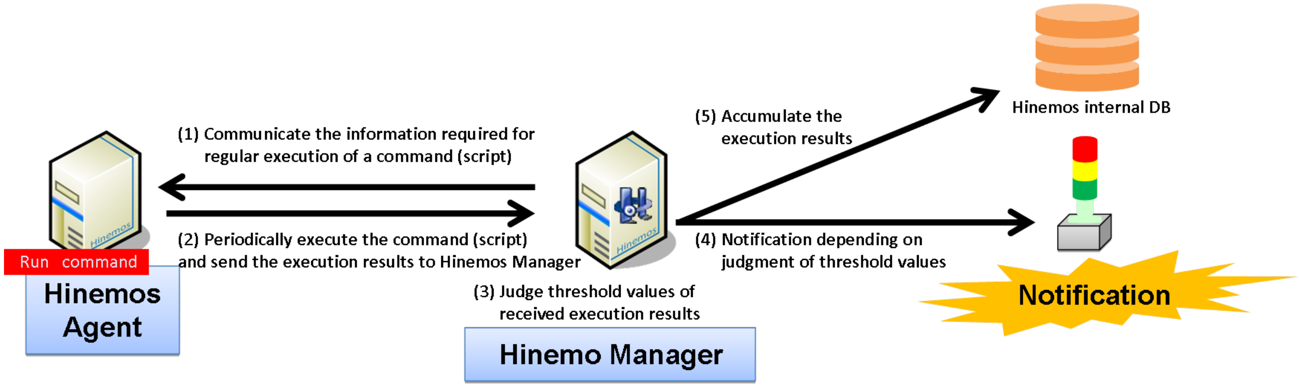

(1) Communicate the information required for regular execution of a command (script)
(2) Periodically execute the command (script) and send the execution results to Hinemos Manager
(3) Judge threshold values of received execution results
(4) Notification depending on judgment of threshold values
(5) Accumulate the execution results
Run command
Hinemos Agent
Hinemo Manager
Hinemos internal DB
Notification

Figure 7-21 Custom Monitor Overview

Further, when using Custom Monitor, the Hinemos Agent must be operating on the target node.

The following type of monitoring method is provided.

- Threshold monitoring of the numeric value output as the standard output by the command

An operation outline of the Custom Monitor feature is shown below.

1. Custom Monitor is set up from the Hinemos Client.
2. The set information is sent from the Hinemos Manager to the Hinemos Agent.
3. The Hinemos Agent runs the specified command for each monitor interval.
4. The Hinemos Agent classifies the command's execution results (standard output) Key, Value and sends the pair (Key, Value) to the Hinemos Manager.
5. The Hinemos Manager performs threshold judgement on the VALUE of the sent pair (Key, Value).

The standard output from the command that is the execution target must be in the following format.

```
KEY_1,VALUE_1
KEY_2,VALUE_2
KEY_3,VALUE_3
...
```

The KEY must be a string that cannot include half width commas (,) and line returns (MS932 for Windows agent and UTF-8 for other agents). The VALUE must be a 64-bit single-precision floating-point value (4.9e-324~1.7976931348623157e+308). Threshold value judgement is performed on the monitor target with that pair (KEY, VALUE) and notification is made of the monitor details of the notification information with the embedded format of the key.

Also, since multiple pairs can be included in the standard output of the command, output each pair as 1 line. (The code for a new line is CRLF for the Windows agent and LF for other agents)

Further, if the command execution time goes long and there is a timeout, and the pair is confirmed to not meet the above format, it will be judged that the value that is the monitor target could not be determined, and notified with priority "Unknown".

Custom Monitor is set up in the Custom Monitor [Create/Change] dialog. The Custom[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Custom Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
3. The Custom Monitor [Create/Change] dialog opens.

Registering Monitoring Setting

1. The Custom Monitor [Create/Change] dialog opens.
2. Set up the following items.

- Monitor ID:

  Enter the Monitor ID as text. The Monitor ID is used as an ID to identify which monitoring configuration generated the notification.

Copyright (c) 2013 NTT DATA CORPORATION

- Description:

  Enter a description of the monitoring setting as text.

- Owner Role ID:

  Select an Owner Role ID for the monitoring setting. Refer to Account Feature section for more details about Owner Role.

- Scope:

  Enter the target scope. Click the "Refer" button on the right to display the Select Scope dialog. Select the target scope from the scope tree in the dialog.

3. Set up the monitoring conditions. Enter the following items.

- Interval:

  Check the connection to the Hinemos Agent at the interval specified here.

- Calendar ID:

  Select the calendar ID for the calendar you want to set up. Monitoring is enabled only during the period configured as working hours in the calendar (Refer to the section, Calendar Feature for more details on the calendar). If Calendar ID is not selected, the monitoring is enabled all day.

- Check Settings:

  - Execute command(s) on selected node.

    Specify the execution unit for the command. If you want to execute a command from a single Hinemos Agent and acquire the target scope information, specify it here. (Refer to Figure 7-22, "Command Execution Units" for details.)

  - Effective User:

    Specify the user to execute the command.

    - Agent startup user:

      User who started the Hinemos Agent, which is set as the destination of a job execution, becomes an Effective User.

    - Specify a user:

      You can also specify a user manually.

  - Command:

    Specify the command to execute.

  - Timeout:

    Specify the interval until timeout after command execution.

Copyright (c) 2013 NTT DATA CORPORATION

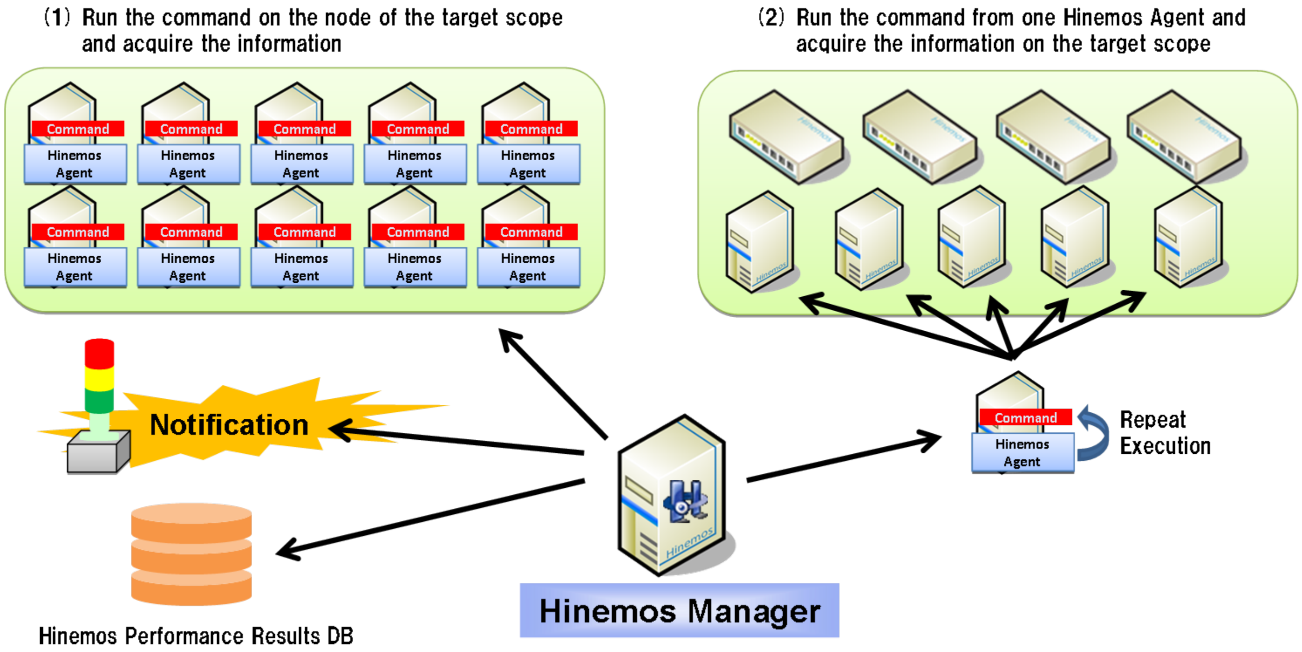

(1) Run the command on the node of the target scope and acquire the information
(2) Run the command from one Hinemos Agent and acquire the information on the target scope
Command
Hinemos Agent
Notification
Repeat Execution
Hinemos Performance Results DB
Hinemos Manager

Figure 7-22 Command Execution Units

4. Define the priority for each monitor result. Enter the following items.

- Monitor:

  Check this to perform threshold value judgement on the numeric value output as standard output by the comm and.

- Value:

  Enter the threshold value for the numeric value output as standard output by the command.

  If within the range of "Information", it is notified as "Information" priority.

  If it is outside the range of "Information" and is in the range of "Warning", it is notified as "Warning" priority.

  If it is not in the range of "Information" or "Warning", it is notified as "Critical" priority.

5. Configure the notification details. Enter the following items.

- Notification ID:

  Select from the list the Notification ID that is the notification method used in the notification setting. (Refer to the section Notification Feature regarding notification settings) When you click the "Select" button on the right, the Notification[List] dialog is displayed. Select the notification method.

- Application:

  Enter an application name in alphanumeric text. This is displayed as the notification information.

6. Enter the following items for the value of the collection for the monitor target.

- Collector:

  Check this to collect and accumulate the numeric value output as standard output by the command. This is con nected to the Performance Management feature and the accumulated response time can be displayed as a grap h.

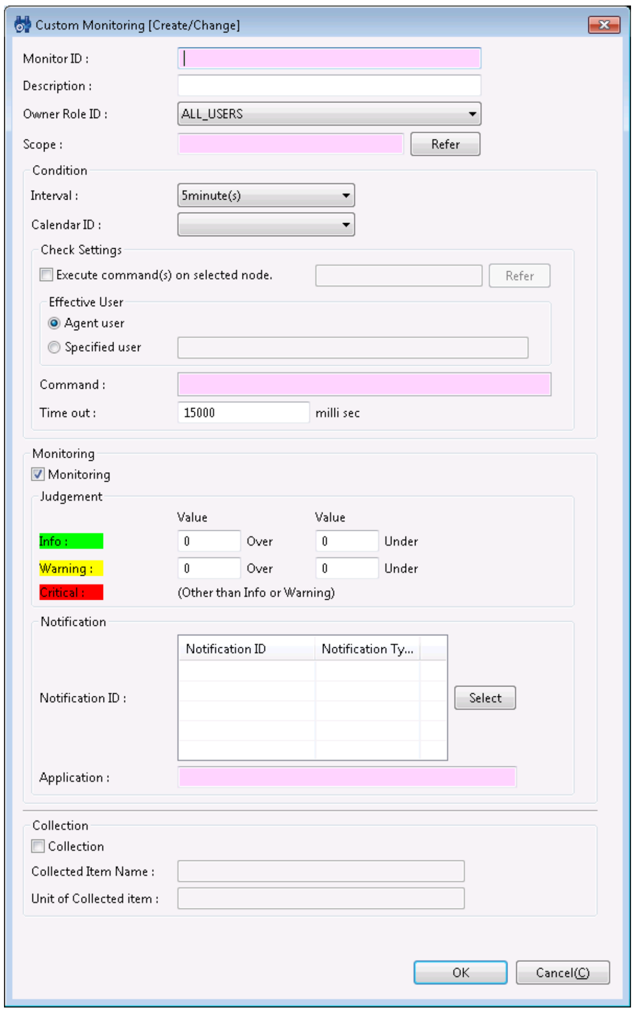
- Collected Item Name:

  Enter the display name for the collected value. This display name is used by the Performance Management feat ure's graph, etc.

- Collection units:

  Enter the units for the collected value. These units are used by the Performance Management feature's graph, etc.

Copyright (c) 2013 NTT DATA CORPORATION



Custom Monitoring [Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 5minute(s)

Calendar ID :

Check Settings

□ Execute command(s) on selected node.

Effective User

● Agent user

○ Specified user

Command :

Time out : 15000 milli sec

Monitoring

☑ Monitoring

Judgement

	Value		Value	
Info :	0	Over	0	Under
Warning :	0	Over	0	Under
Critical :	(Other than Info or Warning)			

Notification

Notification ID :

Notification ID	Notification Ty...

Application :

Collection

□ Collection

Collected Item Name :

Unit of Collected item :

Figure 7-23 Custom Monitoring [Create/Change] Dialog

Changing the Monitor Setting

1. Select the object to change from the monitor setting list displayed in the Monitor Settings[List] dialog, then click the "Modify" button. The Custom Monitoring [Create/Change] dialog opens.

2. Edit the setting details, and then click the "OK" button. (Refer to "Registering Monitor Settings" in the previous chapter for the procedures for entering settings).

Deleting Monitor Settings

Select the object to delete from the monitor setting list displayed in the Monitor Settings[List] dialog, then click the "Delete" button.

Changing the Valid/Invalid Setting in the Monitor Settings

You can collectively change the valid/invalid settings in the monitor settings. Select the settings to change from the monitor setting list displayed in the Monitor Settings[List] dialog (multiple can be selected). Then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

Table 7-23 Configuration Items of Custom Monitor

Configuration item	Input type	Description
Monitor ID	Text	Enter an ID to identify which notification setting generated the notification.
Description	Text	Enter a description of the monitoring setting.
Owner Role ID	Select from list	Select an Owner Role ID for the monitoring setting.
Scope	Select from the scope tree	Select a scope subject for monitoring.

Copyright (c) 2013 NTT DATA CORPORATION

Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring is enabled only during the period configured as working hours in the calendar.
	Check Settings	Run the commands together on the specified node	Checkbox	Check to run the command on one Hinemos Agent.
			Select from the scope tree	Select the node with the Hinemos Agent installed. The command will be repeatedly executed for the number of nodes included in the target scope on that node. (When combined with the command with the node variable embedded, the node information such as IP address can be specified in the command's argument, and can be used for monitoring with devices where the Hinemos Agent cannot be installed.)
		Execution user	Text	Enter the user name who will execute the command. (With the Windows agent, you cannot specify other that the Hinemos Agent's startup user)
		Command	Text	Specify the command to execute. (The node variable can be embedded)
		Timeout	Text (Numeric)	Enter the maximum execution interval for the command. The command will pause if it continues to run past this time.
Monitor	Monitor		Checkbox	Check to perform monitoring by threshold value judgement.
	Judge **Information /** Warning	Greater than or equal to Acquired value	Text (numeric)	Enter the lower limit for the acquired value. (To judge " More than" the lower limit)
		Less than Acquired value	Text (numeric)	Specify the upper limit value for the acquired value. (To judge "Less than" the upper limit)
	Notification	Notification ID	Select from list	Select from the list the Notification ID that is the notification method used in the notification setting.
		Application	Text	Enter an application name to be displayed as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name that is the description for the collected value.
	Collected value units		Text	Enter the units for the collected value.

Table 7-24 Node Variables

String	Content to replace
#[FACILITY_ID]	Facility ID for each node included in the target scope
#[FACILITY_NAME]	Facility Name for each node included in the target scope
#[IP_ADDRESS_VERSION]	IP Address Version for each node included in the target scope
#[IP_ADDRESS]	IP Address (IPv4 or IPv6 according to the IP address version) for each node included in the target scope
#[IP_ADDRESS_V4]	IPv4 Address Version for each node included in the target scope
#[IP_ADDRESS_V6]	IPv6 Address Version for each node included in the target scope
#[NODE_NAME]	Node Name for each node included in the target scope
#[OS_NAME]	OS Name for each node included in the target scope
#[OS_RELEASE]	OS Release for each node included in the target scope
#[OS_VERSION]	OS Version for each node included in the target scope

#[CHARSET]	Character Set for each node included in the target scope
#[SNMP_PORT]	SNMP Port Number for each node included in the target scope
#[SNMP_COMMUNITY]	SNMP Community Name for each node included in the target scope
#[SNMP_VERSION]	SNMP Version for each node included in the target scope
#[SNMP_TIMEOUT]	SNMP Timeout for each node included in the target scope
#[SNMP_TRIES]	SNMP retry count for each node included in the target scope
#[WBEM_PORT]	WBEM Port Number for each node included in the target scope
#[WBEM_PROTOCOL]	WBEM protocol for each node included in the target scope
#[WBEM_TIMEOUT]	WBEM Timeout for each node included in the target scope
#[WBEM_TRIES]	WBEM retry count for each node included in the target scope
#[WBEM_PASSWORD]	WBEM password for each node included in the target scope
#[IPMI_IP_ADDRESS]	IPMI IP Address for each node included in the target scope
#[IPMI_PORT]	IPMI Port Number for each node included in the target scope
#[IPMI_TIMEOUT]	IPMI Timeout for each node included in the target scope
#[IPMI_TRIES]	IPMI retry count for each node included in the target scope
#[IPMI_PROTOCOL]	IPMI protocol for each node included in the target scope
#[IPMI_LEVEL]	IPMI level for each node included in the target scope
#[IPMI_USER]	IPMI user for each node included in the target scope
#[IPMI_PASSWORD]	IPMI user password for each node included in the target scope
#[WINRM_USER]	WinRM user for each node included in the target scope
#[WINRM_PASSWORD]	WinRM user password for each node included in the target scope
#[WINRM_VERSION]	WinRM Version for each node included in the target scope
#[WINRM_PORT]	WinRM Port Number for each node included in the target scope
#[WINRM_PROTOCOL]	WinRM protocol for each node included in the target scope
#[WINRM_TIMEOUT]	WinRM Timeout for each node included in the target scope
#[WINRM_TRIES]	WinRM retry count for each node included in the target scope
#[VM_NODE_TYPE]	Server virtualization node type for each node included in the target scope
#[VM_NAME]	Server virtualization virtual machine name for each node included in the target scope
#[VM_ID]	Server virtualization virtual machine ID for each node included in the target scope
#[VM_USER]	Server virtualization virtual machine user for each node included in the target scope
#[VM_PASSWORD]	Server virtualization virtual machine password for each node included in the target scope
#[VM_PROTOCOL]	Server virtualization virtual machine protocol for each node included in the target scope
#[VSWITCH_TYPE]	Network virtualization virtual switch type for each node included in the target scope
#[OF_DATAPATHID]	Network virtualization OpenFlow Datapath ID for each node included in the target scope
#[OF_CTRL_IP_ADDRESS]	Network virtualization OpenFlow Controller Address for each node included in the target scope
#[<NODE VARIABLES>]	Node Variable (the node variable name is specified in the <NODE_VARIABLES>) for each node included in the target scope

7.14 System Log Monitor

The System Log Monitor feature performs filtering of the monitored node's system log and notifies when the output log matches the specified matching condition. The System Log Monitor feature belongs to the String monitoring category.

Matching Process

In System Log Monitor, you can monitor logs in syslog format (RFC 3164) (total length of the packet must be less than 1024byte).

syslog message is composed of PRI section, HEADER section, and MSG section.

```
<PRI> HEADER MSG
```

Example)

```
<13>Mar 12 16:38:58 host01 root: error
```

PRI section:

The value calculated from the "Severity" and "Facility" is set up in PRI section.
Since syslog is standard, refer to RFC 3164 for the detailed calculation method.

HEADER section:

HEADER section is composed of "TIMESTAMP" and "HOSTNAME".
"TIMESTAMP" is configured in the "mm dd hh:mm:ss" format.
Configure the host name or the IP address for "HOSTNAME".

MSG section:

The section after the HEADER is the MSG section..
Typically, the MSG section begins with the additional information related to the process that generated the message, followed by the message itself.

The syslog source node is identified using the HOSTNAME section in the HEADER section. For example, if the HEADER section in the syslog message is "Feb 25 14:09:07 webserver", "webserver" is the HOSTNAME section. When a syslog message is sent from an external server, Hinemos scans the HOSTNAME part of the syslog message and the node properties "Node Name", "IP address" (IPv4 address or IPv6 address, whichever is enabled), and Host Name registered in the repository management feature in order and identifies the matching node as the send destination node. Further, when performing system log monitoring in a Windows 2003 (IPv6) environment, the computer name in that environment must be 15 characters or less.

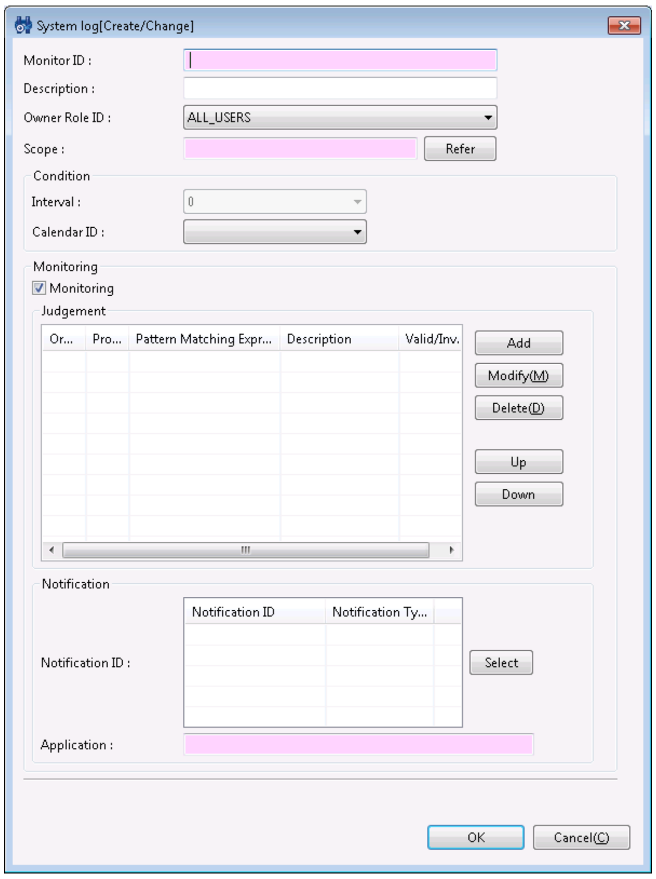
Pattern matching is performed on the MSG section with the regular expression specified in the "Pattern Matching Expression".

The System Log Monitor is set up in the System Log [Create/Change] dialog. The System Log [Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select System Log Monitor (String) from the Monitor Type dialog and click the "Next" button.
3. The System Log [Create/Change] dialog opens.

Refer to the set up process in HTTP Monitor (String) in HTTP Monitor for the set up process from here.

Copyright (c) 2013 NTT DATA CORPORATION



System log[Create/Change]

Monitor ID :

Description :

Owner Role ID : ALL_USERS

Scope :

Condition

Interval : 0

Calendar ID :

Monitoring

☑ Monitoring

Judgement

Notification

Notification ID :

Application :

Figure 7-24 System Log [Create/Change] Dialog

Table 7-25 Configuration Items of System Log Monitor (String)

Configuration item			Input type	Description
Monitor ID			Text	Enter an ID to identify the monitor setting which output the notification information.
Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope or node as object for monitoring.
Condition	Interval		Select from list	This monitoring is performed during log acquisition so the monitor interval cannot be selected.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If selected, the monitor setting will operate in the time zone specified in the calendar operation time.
Monitor	Monitor		Checkbox	Check to perform monitoring by string matching.
	Judge	Order	Change the order with the "Up" button or the "Down button	String matching is checked in order from the one with the smallest order number.
		Edit	Edit string matching with the "Add" button, the "Modify" button, or the "Delete" button	Edit the pattern matching expression to be used for string matching.
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.

Copyright (c) 2013 NTT DATA CORPORATION

7.15 Logfile Monitor

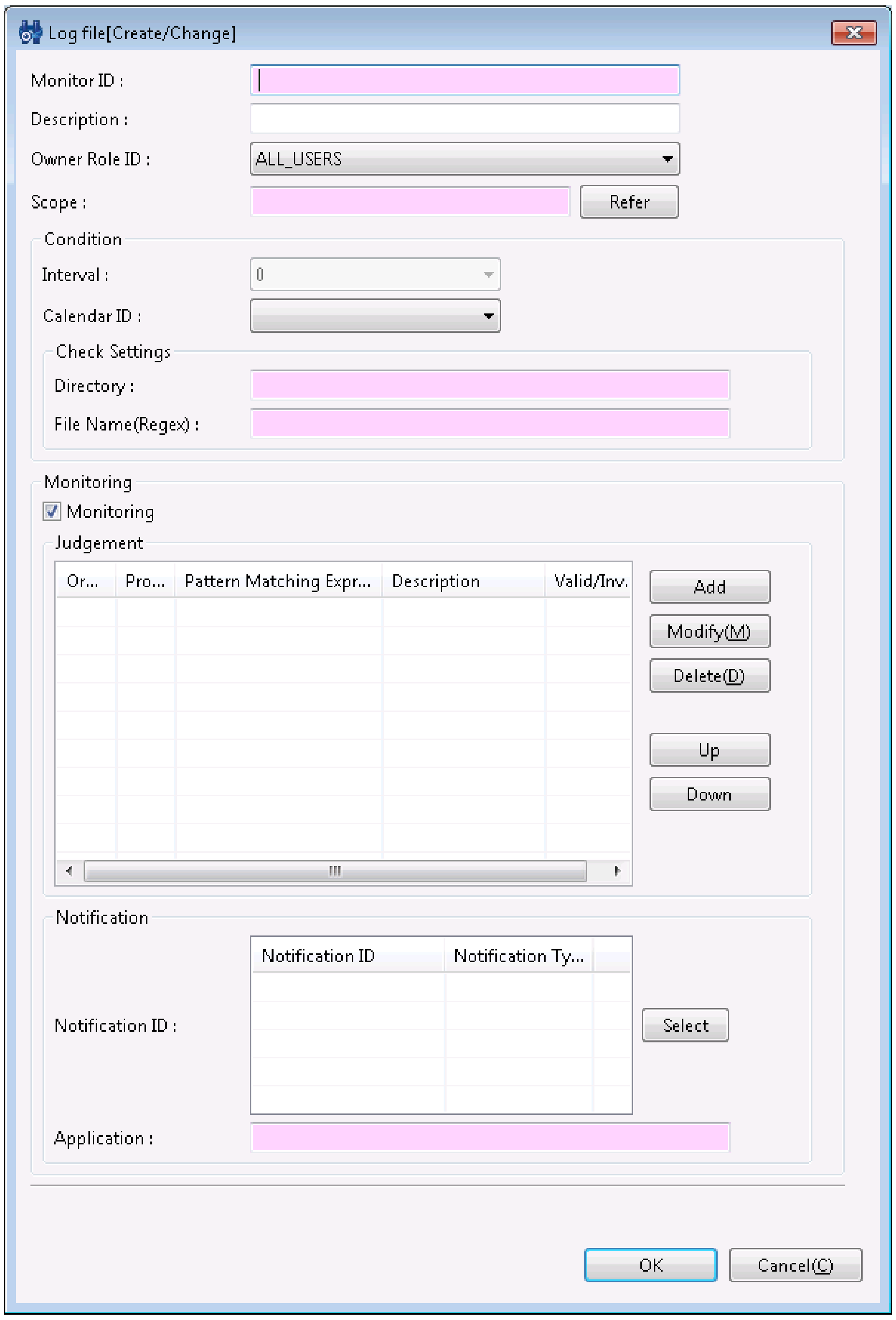
The Logfile Monitor feature is where file processing is performed on the log file output to a discretionary path by the monitored node, and provides notification if the output log file matches the specified matching conditions. The Logfile Monitor feature belongs to the String monitoring category.

Further, when using Logfile Monitor, the Hinemos Agent must be operating on the target node.

The Logfile Monitor is set up in the Log file[Create/Change] dialog. The Log file[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Logfile Monitor (String) from the Monitor Type dialog and click the "Next" button.

Refer to the set up process in HTTP Monitor (String) in HTTP Monitor for the set up process from here.



Owner Role ID : ALL_USERS

Interval : 0

☑ Monitoring

Figure 7-25 Log file [Create/Change] Dialog

Table 7-26 Configuration Items of Logfile Monitor (String)

Configuration item	Input type	Description
Monitor ID	Text	Enter an ID to identify the monitor setting which output the notification information.

Copyright (c) 2013 NTT DATA CORPORATION

Description			Text	Enter a description of the monitoring setting.
Owner Role ID			Select from list	Select an Owner Role ID for the monitoring setting.
Scope			Select from the scope tree	Select a scope or node as object for monitoring.
Condition	Interval		Select from list	This monitor interval indicates the file check interval (*1) on Hinemos Agent, so it cannot be selected.
	Calendar ID		Select from list	Select the calendar setting assigned in the monitor setting. If selected, the monitor setting will operate in the time zone specified in the calendar operation time.
	Check Settings	Directory	Text	Indicate the file path of the monitored log file.
		Filename (Regular Expression)	Text	Indicate the file name of the monitored log file. Enter the file name using regular expression. (*2)
Monitor	Monitor		Checkbox	Check to perform monitoring by string matching.
	Judge	Order	Change the order with the "Up" button or the "Down button	String matching is checked in order from the one with the smallest order number. When the corresponding pattern matching expression is found, follow the settings in "Process if matched" or "Do not process if matched", and notify the monitoring results. (Further matching with a string as the pattern matching expression will not be performed)
		Edit	Edit string matching with the "Add" button, the "Modify" button, or the "Delete" button	Edit the pattern matching expression to be used for string matching.
	Notification	Notification ID	Select from list	Select the notification setting assigned to the monitor setting.
		Application	Text	Enter an application name that is assigned as the notification information.

*1 For more details of file check interval in Logfile Monitor, see Chapter 13, List of Hinemos Manager's Configuration Settings, of the Administrator's Guide.

*2 A regular expression can match multiple log files. However, note that the file number is limited. The default maximum number of monitoring file is 500.

Start position for reading a file

The start position for reading a file depends on whether the file exists at the time the monitor is set to be valid.

- Read from the end of the file

  At the time the monitor setting becomes valid after the agent started (all existing settings are load and new settings are registered), if the target file exists, it will be read from the end.

- Read from the beginning of the file

  At the time the monitor setting becomes valid after the agent started (all existing settings are load and new settings are registered), if the target file does not exist, it will be created (*) and read from the beginning.

*** If the directory in the check setting of monitor configuration does not exists, both the directory and the target file will not be created.**

(For instance, if a log file is placed in a shared disk storage, all the directories and files will be switched when a failover occurred at the source of log output.)

7.16 Resource Monitor

Resource Monitor performs threshold judgement for the collected values acquired from the monitored node. The collected values are calculated based on the values acquired by polling using SNMP (default) or WBEM (WBEM is only for Linux). The resource monitor feature belongs to the Numeric monitoring category.

- When SNMP (default) is used

  SNMP is the default for accumulation of the collected values in a Linux or Windows environment. The SNMP service must be set up on the monitored device. This is net-snmp for Linux and SNMP Service for Windows. Refer to 7.8, "Polling Protocol Settings" in the Administrator's Guide regarding the method for setting up the resource monitor device's SNMP service.

  To connect to SNMP for the managed node, the SNMP port number, community name, version, time out and retry count must be set in the Repository registration information. Refer to Creating/Changing/Deleting a Node for details.

  - However, if the Windows managed node is SNMP version 1, disk I/O cannot be acquired. This occurs on the Windows due to the constraints of the SNMP Service extension module included in the Hinemos Agent for Windows. There is no other resource information that cannot be obtained because the collection item entered by default is SNMP version 1.

- If using WBEM

  Part of the accumulation of collection values in a UNIX environment uses WBEM. Accumulation of the collection values is also possible in a Linux environment by changing the settings.

  The CIM server must be set up on the monitored device. This is OpenPegasus for Linux. Refer to 7.8, "Polling Protocol Settings" in the Administrator's Guide regarding the method for setting up the resource monitor device's CIN server.

  To connect to WBEM for the managed node, the WBEM user name, user password, port number, protocol, version, time out and retry count must be set in the Repository registration information. Refer to Creating/Changing/Deleting a Node for details.

The Resource Monitor is set up in the Resource[Create/Change] dialog. The Resource[Create/Change] dialog is opened with the following process.

1. Click the "Create" button from the Monitor Setting[List] view.
2. Select Resource Monitor (Numeric) from the Monitor Type dialog and click the "Next" button.
3. The Resource[Create/Change] dialog opens.

Registering Monitoring Setting

Refer to the Process Monitor feature for the Resource Monitor setting process.

Table 7-27 Configuration Items of Resource Monitor

Configuration item	Input type	Description
Monitor ID	Text	Enter an ID to identify which notification setting generated the notification.
Description	Text	Enter a description of the monitoring setting.
Owner Role ID	Select from list	Select an Owner Role ID for the monitoring setting.
Scope	Select from the scope tree	Select a scope subject for monitoring.

Condition	Interval		Select from list	Specify the monitoring interval.
	Calendar ID		Select from list	Select the calendar ID for the calendar to set up. Monitoring will be enabled only during the time when configured as working hours on the calendar.
	Check Setting	Monitor Item	Select from list	Specify the collection value of the monitoring subject. When you specify a "Scope" for the monitored target, a list of the collection items that can be acquired in common for nodes included in that scope is displayed.
		Collect all including specification data when collecting		**If there is a check** For items with specifications, if "Collect" is valid, those specification items will also be collected. In this way, it can be virtualized along with the specification items when displayed as a graph by the performance management feature. There is no effect on the operation if this check "Monitor" is valid. **If there is no check** For items with specifications, if "Collect" is valid, the items will not be collected.
Monitor	Monitor		Checkbox	When checked, the monitoring setting is enabled. If unchecked, the setting is disabled. The setting will be saved, but the monitoring process will not be executed.
	Judge **Information /** Warning	Greater than or equal to Acquired value	Text (numeric)	Enter the lower limit for the acquired value. (To judge "More than" the lower limit)
		Less than Acquired value	Text (numeric)	Specify the upper limit value for the acquired value. (To judge "Less than" the upper limit)
Notification	Notification ID		Select from list	Select a notification ID to be used as a notification method.
	Application		Text	Enter an application name to be displayed as the notification information.
Collection	Collection		Checkbox	Check to acquire the value of the monitor target.
	Collected Item Name		Text	Enter the display name for the collected value.
	Collected value units		Text	Enter the units for the collected value.

- Specify the Monitor Items

  The "Collection Items" that can be set in the "Monitor Items" differ depending on the scope set for the monitored target. When you set the "Scope" for the monitored target, the items that can be acquired in common for nodes included in that scope are displayed in a list. Refer to the chapter on the Performance Management Feature for a list of collection value items that can be set.

  The collection value items that can be set as monitored items largely have the following characteristics.

- Specification items

  There are collection value items set as monitored items that have a parent and child relationship. In this case, the item specifications are displayed from parent to child. Specifications will be displayed with "()".

  Refer to Table 7-3, List of Collection Values of the Specification Items and the Specification Items Included in the Collection Values for details on the specifications.

Copyright (c) 2013 NTT DATA CORPORATION

Example) "Packet count" specifications

Packet Count (received)

Packet Count (sent)

If "Collect along with Specification Data When Collecting" is checked, collect to match the specification items if "Collect" is valid for items with specifications. In this way, they can be virtualized along with the specification items when displayed as a graph by the performance management feature. There is no effect on the operation if this check "Monitor" is valid.

- Device Specific Items

The collection values for each device (CPU, Memory, Disc, NIC, File system) can be monitored. The device will be displayed with "[]".

Example) The following items are for disk device sda0, sda1.

Device specific disk I/O count [sda0]

Device specific disk I/O count [sda1]

[Devices that can be specified]

Devices that can be specified as monitored items are devices that exist in common in the node included the monitored target's "Scope". For example, the default device naming rules are different for Linux and Windows nodes, therefore, you cannot select device specific items in a scope that includes both.

You can distinguish whether or not a device is common in the "Display Name" for each device in the node properties. Therefore, for example, even if it is a device where the actual device name is different, editing the "Device Name" property enables it to be treated as the same device.

```
(Example)

- Scope S
  Node A
  Node B

  - Node A
    NIC information
    Display Name: hoge
    Device Name: eth0

  - Node B
    NIC information
    Display Name: hoge
    Device Name: eth2
```

With these settings, if Scope S is set, device specific collection value items can be selected in Resource Monitor for device [hoge].

[All Device Settings]

Only one collection value item can be specified for one setting in Resource Monitor. For scopes that include nodes that have multiple devices and nodes that have different devices, all of the devices can be monitored with one setting by specifying [ALL] devices.

```
(Example)

- Scope S
  Node A
  Node B

  - Node A
    File System Information
    Display Name:/
    File System Information
    Display Name: /home

  - Node B
    File System Information
    Display Name:/
    File System Information
    Display Name: /home
    File System Information
    Display Name:/var

  - Collection Item
    |File System Usage [*ALL*]
```

If Scope S is specified in these type of settings, monitoring of the specified threshold value operates for all of the file system information registered in Node A and Node B Delete devices that do not need monitoring from the node properties.

Changing the Monitor Setting

Refer to the Process Monitor feature for the Resource Monitor setting change process.

1. Select the object to change from the monitor setting list displayed in the Monitor Settings[List] dialog, then click the "Modify" button. The Resource[Create/Change] dialog opens.

2. Edit the setting details, and then click the "OK" button. (Refer to "Adding Monitor Settings" in the previous chapter for the procedures for entering settings).

Deleting Monitor Settings

Select the object to delete from the monitor setting list displayed in the Monitor Settings[List] dialog, then click the "Delete" button.

Changing the Valid/Invalid Setting in the Monitor Settings

You can collectively change the valid/invalid settings in the monitor settings. Select the setting to change from the setting list (can select multiple). Then click the "Valid" ("Invalid") button. A confirmation dialog is displayed. Click the "OK" button.

8 Performance Management Feature

8.1 Overview

The Performance Management feature provides features for displaying data collected through numeric monitoring with graphs and file output (download).

- Collection value graph display

  The value acquired by numeric value monitoring is displayed as a graph. The display type can be converted to by node, by collection item or by device. The display period, time, days, weeks, months, etc. can be selected. The graph types can be specified as line graphs or stack area graphs and collected values can be viewed and analyzed from various angles.

- Collection Value Download

  The numerical value of the monitoring target is output (downloaded) to a file. The download target can be specified by node and scope unit and the output is in CSV format by node.

8.2 Interface Composition

8.2.1 Default Interface

Interface Composition of the performance management feature is composed of the following views.

- Performance[List] view
- Performance[Graph] view

The Performance[Graph] view is not displayed with the initial screen display configuration. The Monitor ID specified in the Performance[List] view can be displayed by clicking the "Add Graph" button. Refer to the next section for more information.

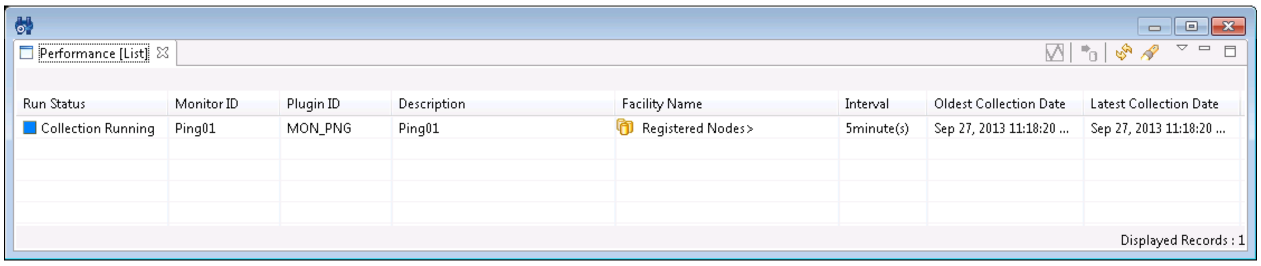
8.2.2 Performance[List] View

From the Monitor Setting (numeric value monitoring) created in the Performance[List] view, the accumulation status of the value acquisition for the monitor setting where the collection of monitor results is enabled is shown.

The status of collection of each monitor setting is shown in the Run Status.

- Collection Running: "Collection" is enabled for numeric value monitoring.
- Stopped: Other than collecting

* If there is not even one collection value, the oldest date and latest date will be blank.



Run Status	Monitor ID	Plugin ID	Description	Facility Name	Interval	Oldest Collection Date	Latest Collection Date
🟦 Collection Running	Ping01	MON_PNG	Ping01	Registered Nodes>	5minute(s)	Sep 27, 2013 11:18:20 ...	Sep 27, 2013 11:18:20 ...

Displayed Records : 1

Figure 8-1 Performance[List] View

Table 8-1 Toolbar

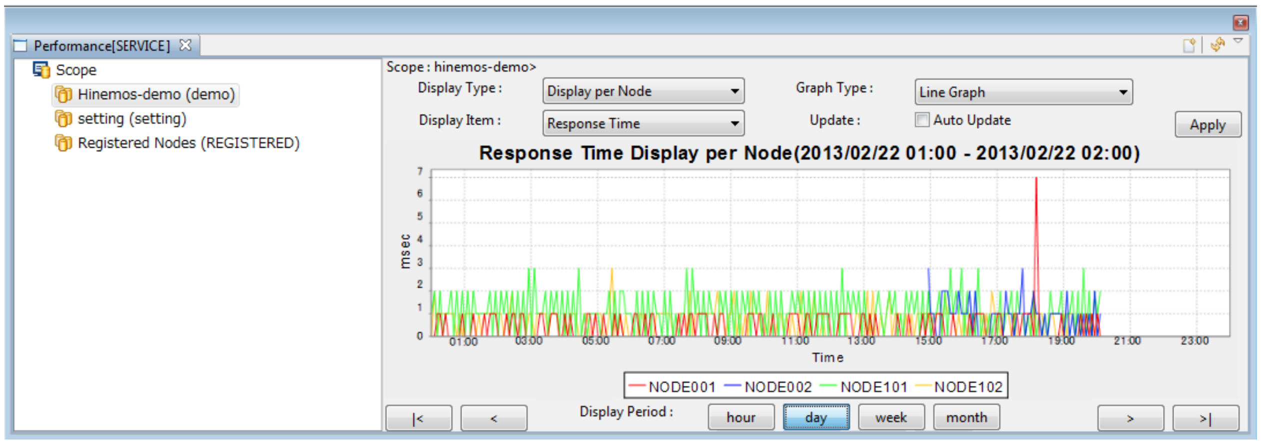
Icon	Button name	Description
	Add graph	A graph is displayed of the values collected by the specified monitor setting The graph displays 1 monitor setting in 1 view.

Copyright (c) 2013 NTT DATA CORPORATION

	Download	The value collected with the monitor setting is output to a file.
	Update	The contents of the table are updated with the latest information.
	Filter	Performs filter setting for the performance list.

8.2.3 Performance[Graph] View

View the collected values in a graph display. When you specify the monitor setting in the Performance[List] view and click the "Add Graph" button, a new Performance[Graph] view is displayed. The view name is Performance[Monitor ID].



Scope : hinemos-demo>

Display Type : Display per Node

Graph Type : Line Graph

Display Item : Response Time

Update : □ Auto Update

Display Period : day

Figure 8-2 Performance[Graph] View

Table 8-2 Toolbar

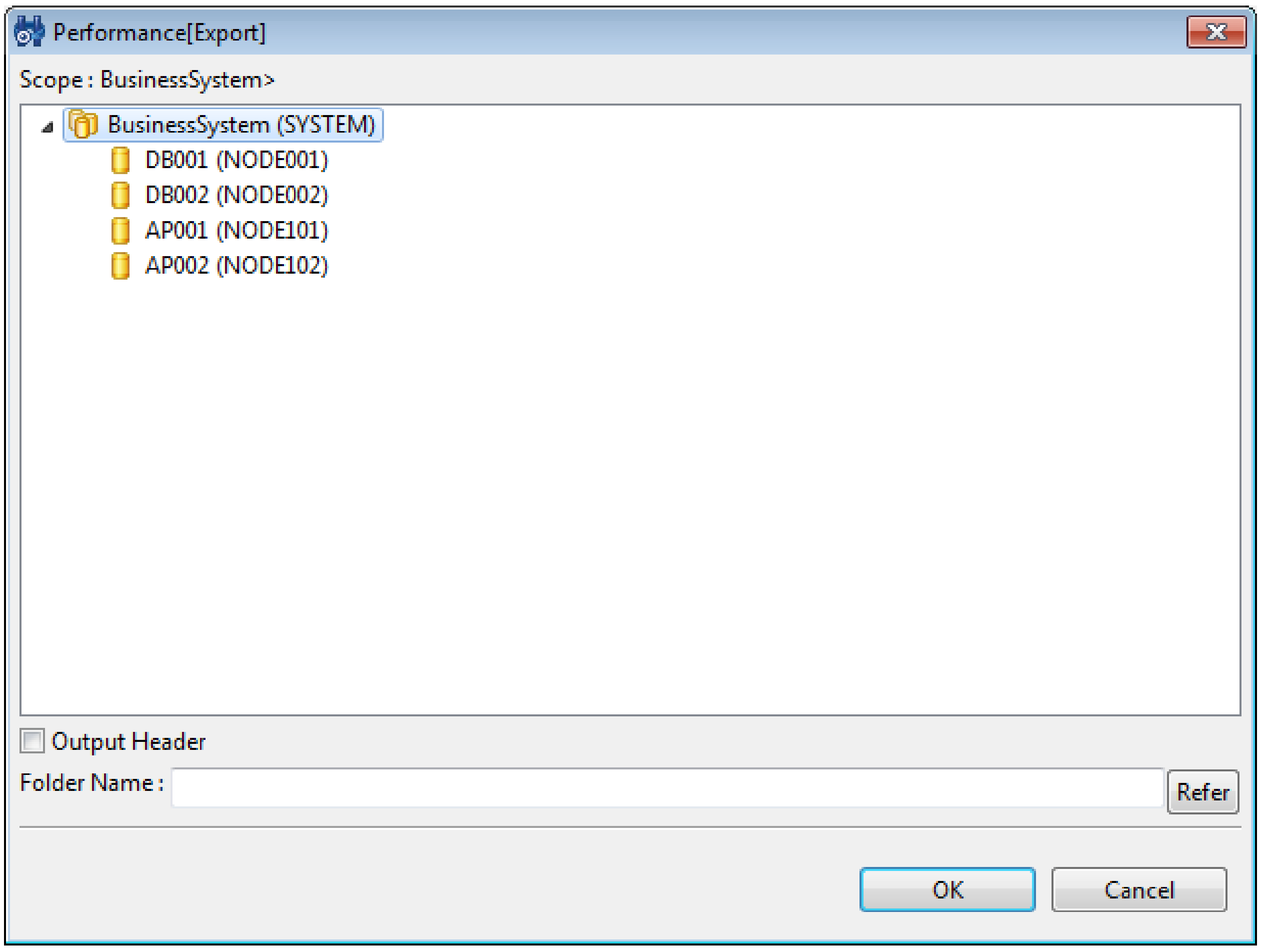
Icon	Button name	Description
	Save graph	A graph of the values collected by the specified monitor setting is displayed.
	Update	Update the graph.

8.3 Collection Value Download

You can export the collected values in CSV format by following the procedures below.

For the specified Monitor ID, specify the node and scope included under the scope for that monitored target and download. The download file will be a CSV file compressed in a zip format.

1. Select the Monitor ID to export from the table in the Performance[List] view. Then click the "Download" button. The Performance[Export] dialog is displayed.



Performance[Export]

Scope : BusinessSystem>

- BusinessSystem (SYSTEM)
  - DB001 (NODE001)
  - DB002 (NODE002)
  - AP001 (NODE101)
  - AP002 (NODE102)

□ Output Header

Folder Name :

Figure 8-3 Performance[Export] Dialog

2. Select the scope or node targeted for download from the scope tree, and specify the directory path for the ou tput destination.
3. To attach a header to the CSV file and output, enter a check in the "Output Header" box. The information belo w is added to the top of the output file as a header.
   - Monitor ID
   - Facility ID
   - Oldest Date
   - Latest Date
   - Column name
4. Click the "OK" button to start the download. Click the "Cancel" button to cancel the download. The name of th e download file is as follows.

   [Monitor ID]_[Facility ID specified in 2]_[Serial number].zip

   The serial number is a 14 digit numeric value string starting from the download time (YYYYmmddMMHHSS).

   After expanding the zip file, a data file of the collected data in CSV format is created for each node.

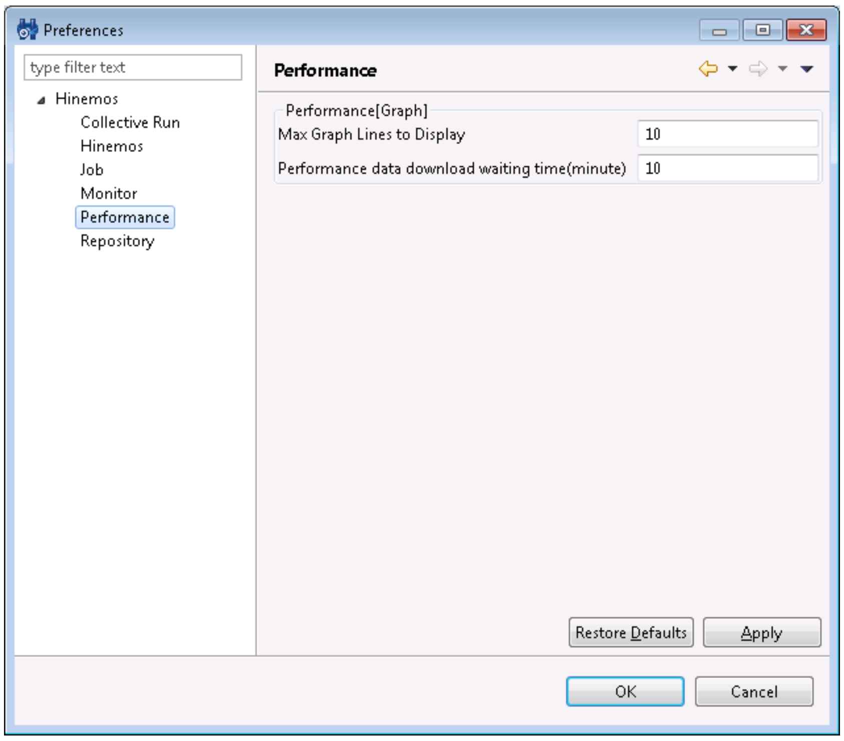
- Precautions

The download file is created and compressed by the Hinemos Manager server. For the Hinemos Client to download the file, the Hinemos Manager server must have sufficient free space to temporarily write the collected data in the following directory.

The location for temporary files on the Hinemos Manager server:

```
/opt/hinemos/var/export
```

A log time is required to download collection values that accumulated for a long time. In this case, in the "Preferences" dialog displayed by selecting "Client Settings" - "Preferences", change the Performance Download Waiting Time (minutes).



Performance[Graph]

Max Graph Lines to Display: 10

Performance data download waiting time(minute): 10

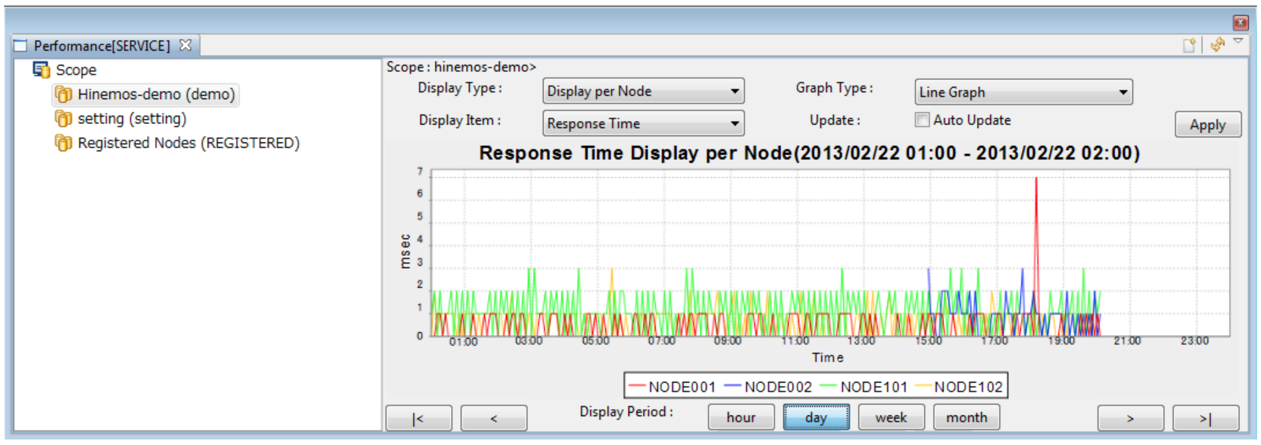
Figure 8-4 Change the Performance Download Waiting Time (minutes)

When you download collection values that have accumulated for a long time, it will place a large burden on the Hinemos Manager server, so be careful.

8.4 Collection Value Graph Display

You can display the collected values as a graph with the following procedures.

1. Select the Monitor ID to display as a graph from the table in the Performance[List] view, and click the "Add Graph" button. The Performance[Graph] view is displayed. The view name is Performance[Monitor ID].



Performance[SERVICE]

Scope
- Hinemos-demo (demo)
- setting (setting)
- Registered Nodes (REGISTERED)

Scope : hinemos-demo>

Display Type : Display per Node

Graph Type : Line Graph

Display Item : Response Time

Update : □ Auto Update

Figure 8-5 Performance[Graph] View Display Example

The facility tree that is the root of the facility ID specified by the monitor settings is displayed in the let pane of the view. This facility tree displays the latest repository information when the "Add Graph" button is clicked.

The graph is displayed in the right plane.

2. Change the scope/node that is the monitor target of the graph

A graph is displayed of collected values for the scope and node specified in the left pane. If a scope is specified, a graph is displayed targeting all nodes under that scope. If a node is specified, a graph is displayed targeting just that node.

The node or scope that is specified in the left pane is reflected in the graph.

3. Changing the Content Displayed in the Graph

In the Performance[Graph] view you can specify and switch the display type, graph type and display items that is the content displayed in the graph. Clicking the "Apply" button will apply the action in the graph.

[Display Type]

You can select from the next 3 types of display items.

- Display per Node The graph is displayed by node.
- Display per Collecting Item There are collection items that have the classification of resource monitor only. You can display these items at the same time.

  For example, if you specify CPU usage in the collection item, the CPU usage for each node, and the CPU usage subordinate items. are displayed.

  Example) Items displayed by Display per Collecting Item

  * Since these are subordinate items, they cannot be selected outside of CPU usage.

  - CPU Usage
  - CPU Usage(User)
  - CPU Usage (System)
  - CPU Usage (Nice Process)
  - CPU Usage (IO Wait)
- Display per device: Resource monitor and custom monitor can collect the same collection item from multiple devices that have those items. You can display these items for each device at the same time.

  For example, if disk I/O count [*ALL*] per disk is specified as a collection item, the items specified as display items are displayed for each disk.

  Example) Items displayed by Display per device

  - Disk I/O count per device

If scope is specified in the left pane, only "Display per Node" can be selected. If node is specified in the left pane then you can select all of the above display types.

[Graph Type]

- Line Graph: The graph is displayed as a line.
- Stack Area Graph: The graph is displayed as a stacked area.

[Display Item]

The collection items specified in the Monitor Setting are displayed as a list. Only Resource Monitor and Custom Monitor will have lists with multiple items.

Copyright (c) 2013 NTT DATA CORPORATION

4. Changing the Graph Display Period

   In the Performance[Graph] view, you can switch the period to display with the buttons. Clicking the button will apply the action in the graph.

Table 8-3 Changing the Display Period

Button name	Description
hour	Makes 1 hour the display period. The graph's horizontal axis will have a range of N:00 - N:59. (*)
day	Makes 1 day the display period. The graph's horizontal axis will have a range of 0:00 - 23:59.
week	Makes one week the display period. The graph's horizontal axis will have a range of Sunday - Saturday.
month	Makes one month the display period. The graph's horizontal axis will have a range of 1st - last day of the month.

   * The graph is not displayed if the collection interval is 60 minutes.

   If you change the period, normally the time will be the left side of the time axis. If you widen the time period (such as changing from the "day" button to the 'week" button), normally the period will change to include the time. If you narrow the time period (such as changing from the "week" button to the 'day" button), normally the time will be fixed to the left axis.

5. Moving the Graph Display Period

   In the Performance[Graph] view, you can move the period to display with the buttons. Clicking the button will apply the action in the graph.

Table 8-4 Moving the Display Period

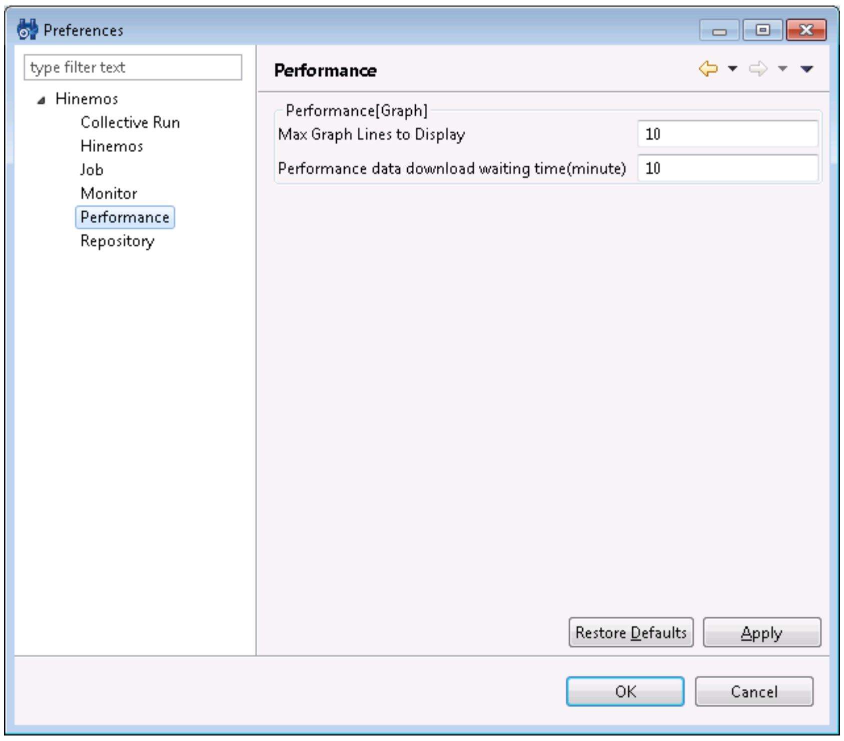
Button name	Description
|<	The display period moves to display the oldest collection time.
<	Moves to the prior display period. **Example)** If the graph is displaying 4/25, it would move to 4/24.
<	Moves to the next display period. **Example)** If the graph is displaying 4/25, it would move to 4/26.
>|	The display period moves to display the latest collection time.

6. Auto Update of the Graph Display

   If you check "Auto Update", the graph automatically updates the displayed monitor period of the Monitor Setting. If you do not want the graph to automatically update, remove the check from "Auto Update".

7. Precautions

The default Graph Max Display Lines displayable at the same time in the Performance[Graph] view is 10. To change this, in the "Preferences" dialog displayed by selecting "Client Settings" - "Preferences", change the Graph Max Display Lines.



Performance[Graph]

Max Graph Lines to Display: 10

Performance data download waiting time(minute): 10

Figure 8-6 Changing the Graph Max Display Lines

However, an extreme amount of memory resources is consumed when the Graph Max Display Lines is large, so be careful when changing this. After changing Graph Max Display Lines, close the Performance[Graph] view and again press the "Add Graph" button to display.

The maximum number of plots for each line can be defined in the Hinemos settings. The Hinemos Manager must be restarted to reflect the change in this setting.

/opt/hinemos/etc/hinemos.properties

```
performance.graph.max.plot=10000
```

When the Graph Max Display Lines is large an extreme amount of memory resources is consumed, so be careful when changing this.

9 Job Management Feature

9.1 Overview

Job management feature executes scheduled processes in order.

Mainly, the following features are provided.

- Job management by GUI

  You can register/change/delete a job by screen operation.

  Also, you can execute operations of the registered job listed below.

  - Run a job
  - Start a job
  - If a job (JobNet) is composed of multiple jobs, start from any job
  - Pause a JobNet
  - Stop a job
  - Resume a paused job

  You can confirm the progress of running jobs and completed jobs from the screen.

- Detailed job control

  You can perform detailed control of the job execution.

  - Run a command with command line arguments
  - Specify the Effective User for the job
  - Serial execution of a job

    You can specify whether or not to run a succeeding job based on the process result value (end status or end value) for the previous job. Multiple jobs can be specified to start when a single job ends.

  - Specify the job run condition

    A job can be run with Job (End Status), Job (End Value) or time as the evaluation criterion for a wait rule. If time is specified in the wait rule, the wait rule will be judged to have been met when the specified time has elapsed.

  - Specify the Job Run Target

    You can specify the job run target node by scope unit.

    - You can execute the same job for all nodes in a scope.
    - You can run (retry) on nodes that belong to the scope until start is successful for at least one node in the scope.

9.1.1 Starting the Hinemos Agent

The Hinemos Agent must be running on the target node to execute a job.

- Refer to the following manuals for more information.

- For Linux

  Chapter 6.2.1, "Hinemos Agent Startup" in the Installation Manual

- For Windows

  Chapter 5.2.1, "Hinemos Agent Startup" in the Installation Manual

Copyright (c) 2013 NTT DATA CORPORATION

9.1.2 Composition of a Job

In Hinemos, you can create a hierarchy structure in a job. A job hierarchy is composed of the following elements.

- Job unit

  The Job unit is the top element of the job hierarchy. All JobNets and jobs are configured as the elements of a job unit. When registering a job, it is necessary to first create a job unit.

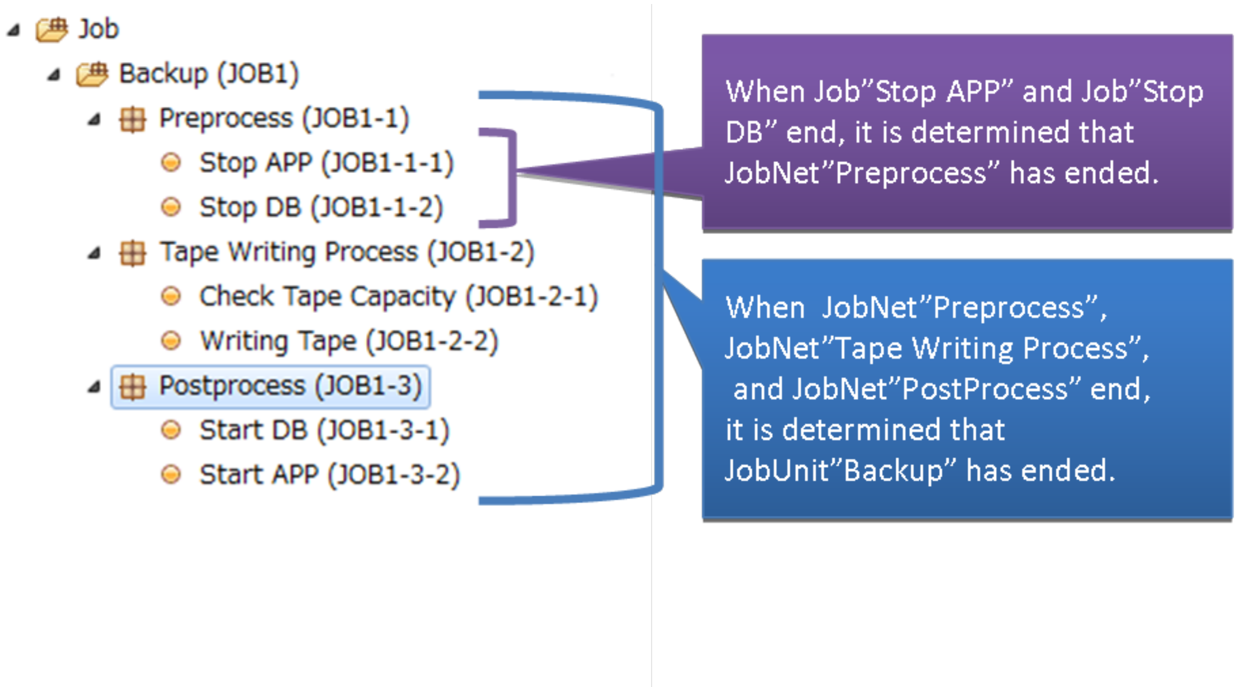
- JobNet

  JobNet is an element that lumps and operates JobNets and jobs. Along with jobs, JobNets can also be combined. Thus, a JobNet is composed of multiple JobNets and jobs. Multiple JobNets and jobs can be registered.

  When a JobNet is executed, the job (or the JobNet) registered in the lower hierarchy of that JobNet is executed. A JobNet ends when all jobs (or JobNets) in the lower hierarchy finish execution.

- Job

  A job is the smallest unit. Set up the command to run on a node.



Job
Backup (JOB1)
Preprocess (JOB1-1)
Stop APP (JOB1-1-1)
Stop DB (JOB1-1-2)
Tape Writing Process (JOB1-2)
Check Tape Capacity (JOB1-2-1)
Writing Tape (JOB1-2-2)
Postprocess (JOB1-3)
Start DB (JOB1-3-1)
Start APP (JOB1-3-2)

When Job"Stop APP" and Job"Stop DB" end, it is determined that JobNet"Preprocess" has ended.

When JobNet"Preprocess", JobNet"Tape Writing Process", and JobNet"PostProcess" end, it is determined that JobUnit"Backup" has ended.

Figure 9-1 Determining Job, JobNet, and Job Unit

- Refer Job

  Jobs that can be specified in the form of referring to another job that belongs to the same Job Unit where the definitions are complete.

- File transfer job

  This job runs the file transfer. For a file transfer job, configure the file transfer settings instead of the command settings. Similar to the configuration of a job, you can configure the wait rule and the end value, and control it within the JobNet.

9.1.3 End Status and End Value

All job units, JobNets, and jobs have an end status and end value when executed. There are three statuses as an end status: "Normal", "Warning", and "Error". The end value is determined by the end status. You can configure which end value applies to which end status.

The end status of a job and a JobNet (or a job unit) will be different.

The end status of a job is specified by the range of the return code when a command is executed. (For example, set "Normal" if the return code is 0. Set "Warning" if the return code is 1~9. Otherwise, set "Error"). The return code of the command must be between -2147483648 - +2147483647.

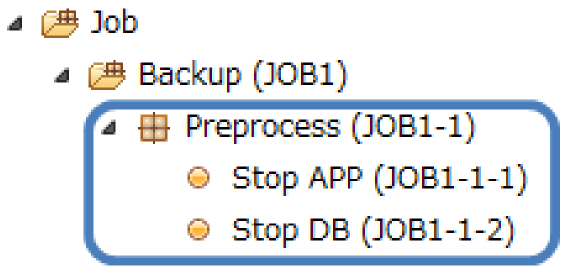
The end status of a JobNet is specified by the range of the end value of all jobs (or JobNets) included in the JobNet. (However, jobs that have wait rule specified are excluded from the end value evaluation. Since a job specified as wait rule has a succeeding job, the end value of the succeeding job will be the target for evaluation Even if jobs spe

Copyright (c) 2013 NTT DATA CORPORATION

cified as wait rule continue, the end value of the last executed job will be the target for the evaluation).

If the end value of all jobs included in the JobNet (excluding those specified as wait rule) are within the range specified as "Normal" end status, then the end status is "Normal". If the end status of all jobs are within the range specified as "Warning", then the end status is "Warning". If the end status of a job does not meet the conditions of both "Normal" and "Warning", it is an "Error".

Example) Explanation of the end status using the example of JobNet "Preprocess" (JOB1-1) below.

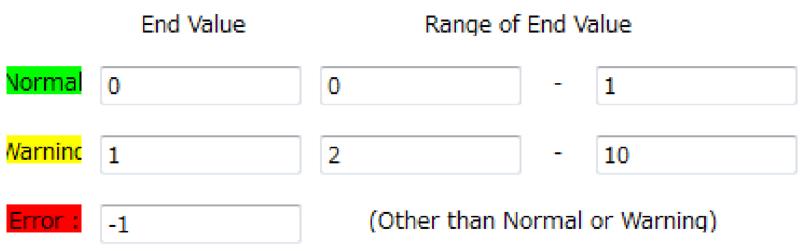


- Job
  - Backup (JOB1)
    - Preprocess (JOB1-1)
      - Stop APP (JOB1-1-1)
      - Stop DB (JOB1-1-2)

Figure 9-2 JobNet "Preprocess" (JOB1-1)

You must make the following settings, for example, when it is set as normal end in JobNet "Preprocess" (JOB1-1) when both Job"Stop APP" (JOB1-1-1) and Job"Stop DB" (JOB1-1-2) end normally.

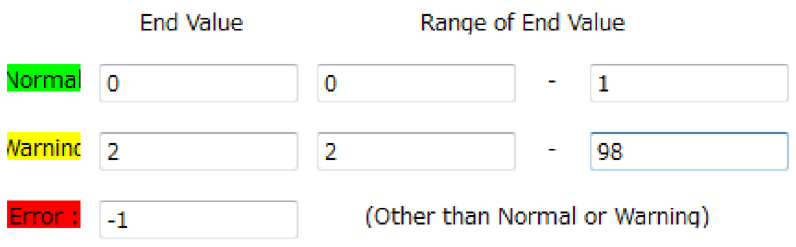
- Configuring the End Value of JobNet "Preprocess" (JOB1-1):



	End Value	Range of End Value		
Normal	0	0	-	1
Warninc	1	2	-	10
Error :	-1	(Other than Normal or Warning)		

Figure 9-3 End Value of JobNet "Preprocess"

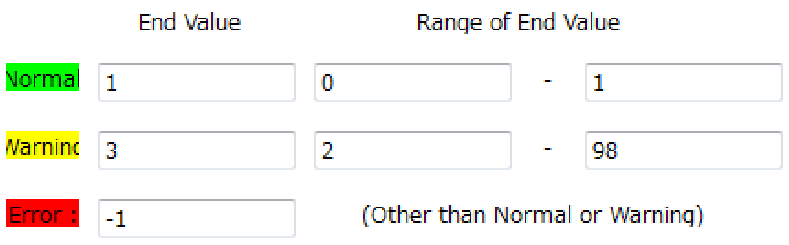
- Configuring the end value of Job"Stop APP" (JOB1-1-1):



	End Value	Range of End Value		
Normal	0	0	-	1
Warninc	2	2	-	98
Error :	-1	(Other than Normal or Warning)		

Figure 9-4 End Value of Job"Stop APP"

- Configuring the end value of Job"Stop DB" (JOB1-1-2):



	End Value	Range of End Value		
Normal	1	0	-	1
Warninc	3	2	-	98
Error :	-1	(Other than Normal or Warning)		

Figure 9-5 End Value of Job"Stop DB"

If the return code of the command is within the range 0-1, the job has ended successfully. The end value of Job"Stop APP" is set to 0. Also, if the return code of the command is within the range 0-1, the job has ended successfully. The end value of Job"Stop DB" is set to 1. Therefore, if Job"Stop APP" (end value 0) and Job"Stop DB" (end value 1)

Copyright (c) 2013 NTT DATA CORPORATION

ended successfully, "JobNet[Preprocess]" is evaluated as a successful end because it is within the range 0~1 (set "Normal"). The end value of "JobNet[Preprocess]" itself is 0, with the end value set as success.

Next, consider the case when the result of Job"Stop APP" is "Warning" (if the return code of the command is 2-98), and Job"Stop DB" has successfully ended. In this case, the end value of Job"Stop APP" is 2, and the end value of Job"Stop DB" is 1. Since the end value of Job"Stop APP" (2) is not included within the range of the end value determined as "Normal" in "JobNet[Preprocess]", it is "Warning". Also, since the end value of Job"Stop DB" (1) is included within the range of the end value determined as "Normal" in "JobNet[Preprocess]", it is "Normal". In this case, the end value of "JobNet[Preprocess]" itself is 1, and the end value configured as "Warning".

9.1.4 Running a JobNet (job unit)

When a JobNet (or a job unit) is run, out of all jobs/job units included in the JobNet the one without a configured wait rule is executed first (if there are multiple, they will be executed concurrently). A JobNet or job unit with a configured wait rule starts running when the condition is fulfilled.

When all jobs/JobNets included in the JobNet are complete, the JobNet itself is complete.

9.1.5 Notification Feature of the Job Execution Time and End Time

During the start and end of a job (or a JobNet or a job unit) run, you can notify the status using the notification feature. You can set the execution priority ("Info", "Warning", "Critical", "Unknown") for the start time or end time ("Normal", "Warning", "End") for a job (or a JobNet or a job unit) in notification.

- You can set a job notification to a job (or a JobNet or a job unit). However, this setting is not recommended. Apply a "Wait Rule" in the job configuration to use the end value or end status of a job as a trigger to run another job. Refer to section Creating/Changing a JobNet for the Wait Rule settings.

9.1.6 Job Variable

You can configure a job variable for each job unit.

By describing the command configuration (start command, stop command) of a job as "#[job variable name]", you can replace these strings and run the job at the job run time.

The following two types for job variables exist.

- System job variable

  The system job variable is a job variable that is reserved in the system in advance. When executing a job triggered by a notification, you can transfer the notification contents as a variable.

Table 9-1 List of System Job Variables

Variable name	Trigger	Value transferred to the job
FACILITY_ID	Notification of monitoring management feature	"Facility ID" of a scope or a node that generated the notification
PLUGIN_ID	Notification of monitoring management feature	"Plugin ID" of the monitoring feature
MONITOR_ID	Notification of monitoring management feature	"Monitor ID"
MESSAGE_ID	Notification of monitoring management feature	"Message ID"
APPLICATION	Notification of monitoring management feature	"Application"
PRIORITY	Notification of monitoring management feature	"Priority"(numeric)(Critical:0 Unknown:1 Warning:2 Info:3)
MESSAGE	Notification of monitoring management feature	"Message"

Copyright (c) 2013 NTT DATA CORPORATION

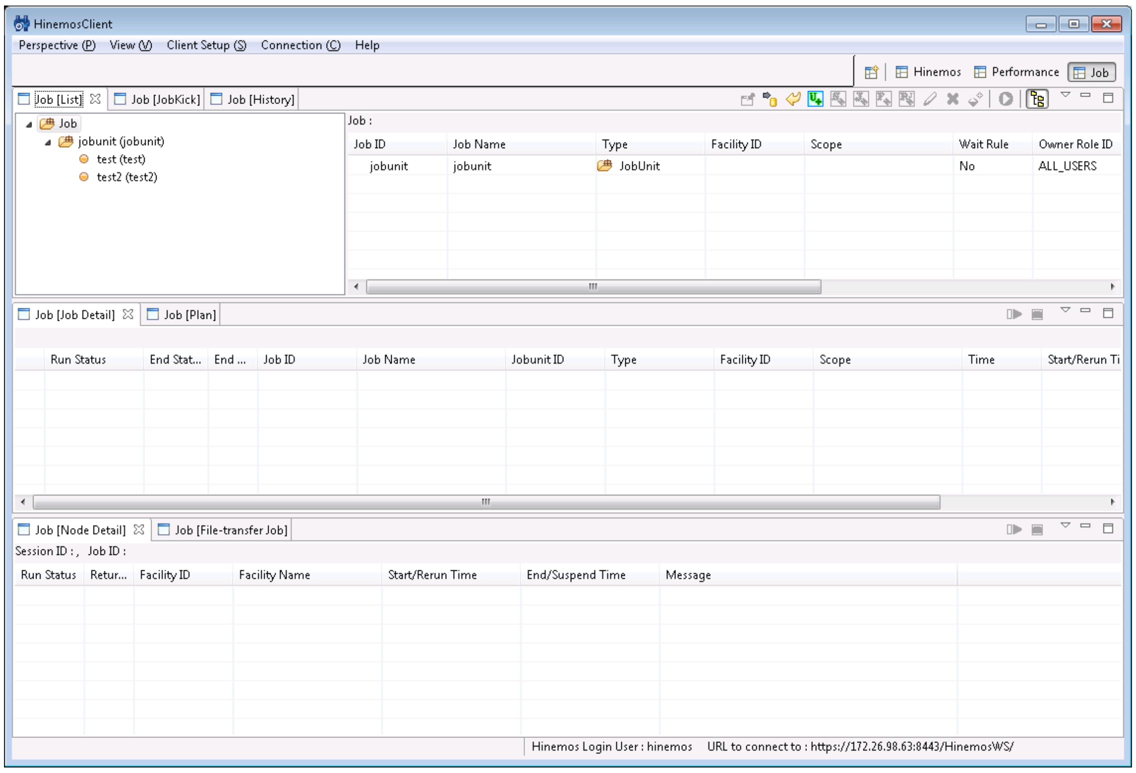
ORG_MESSAGE	Notification of monitoring management feature	"Original Messages"
FILENAME	Job execution	File Name to check when a job runs when there is a Job[FileCheck]
START_DATE	Job execution	"Time" when a job is executed (Example:2009/04/13 18:30)
SESSION_ID	Job execution	"Session ID" during job execution (Example:20090413183000-000)
TRIGGER_TYPE	Job execution	"Trigger Type" of a job (Example:Schedule)
TRIGGER_INFO	Job execution	"Trigger Type" of a job (details are as follows) JobKick ID when the job's JobKick Type is Schedule/FileCheck. (Example:schedule001) If the trigger type is a manual execution, it is the "User Name" (Example:hinemos) If the trigger type is an interlocking monitoring, it is the "Monitor ID" (Example:PING001)

- User job variable

  You can configure any string as a user job variable. The job unit is a unit in a valid range. When a user job variable is configured to a job unit, jobs assigned below the job unit can use the configured user job variable.

9.2 Interface Composition

9.2.1 Default Interface


HinemosClient
Perspective (P) View (V) Client Setup (S) Connection (C) Help
Hinemos Performance Job
Job [List] Job [JobKick] Job [History]
Job
jobunit (jobunit)
test (test)
test2 (test2)
Job [Job Detail] Job [Plan]
Job [Node Detail] Job [File-transfer Job]
Session ID : , Job ID :

Job :

Job ID	Job Name	Type	Facility ID	Scope	Wait Rule	Owner Role ID
jobunit	jobunit	JobUnit			No	ALL_USERS

Run Status	End Stat...	End ...	Job ID	Job Name	Jobunit ID	Type	Facility ID	Scope	Time	Start/Rerun Ti

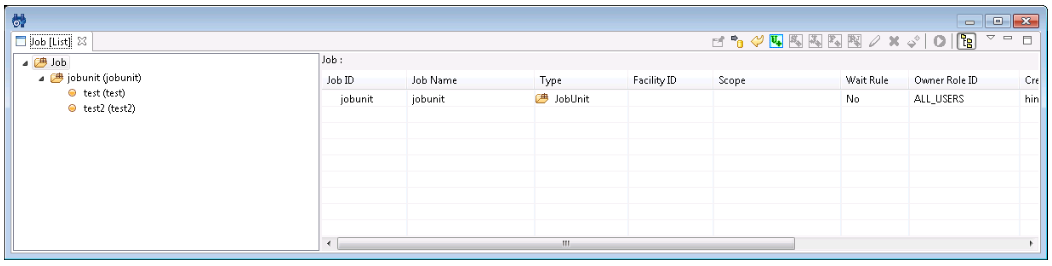
Run Status	Retur...	Facility ID	Facility Name	Start/Rerun Time	End/Suspend Time	Message

Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 9-6 Default Interface of Job Management Feature

9.2.2 Job[List] View

A list of Jobs, Refer Jobs, File Transfer Jobs, JobNets, and JobUnits is shown. In this view, you can create, change, delete, and manually run Jobs, Refer Jobs, File Transfer Jobs, JobNets, and JobUnits.



Job :

Job ID	Job Name	Type	Facility ID	Scope	Wait Rule	Owner Role ID	Cre
jobunit	jobunit	JobUnit			No	ALL_USERS	hin

Figure 9-7 Job[List] View

Table 9-2 Job Tree Icons

Icon	Description
📂	Display job units.
⊞	Display JobNets.
●	Display jobs.
📄	Display file transfer jobs.

Table 9-3 Toolbar

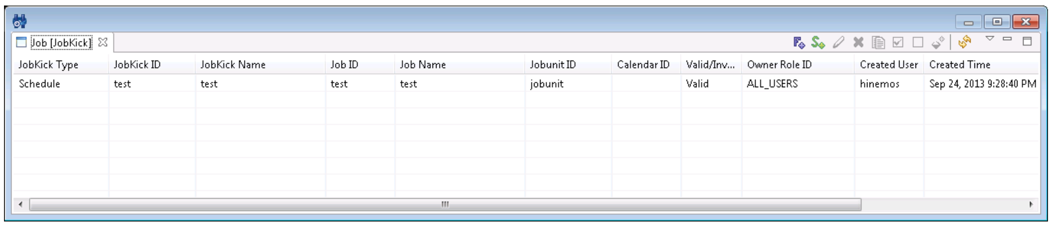
Icon	Button name	Description
📝	Edit Mode	Status (Edit Mode) where the job tree information can be edited as JobUnit units.

Copyright (c) 2013 NTT DATA CORPORATION

	Register	Register information to the manager for the job tree edited on the client.
	Cancel	Clear information for the job tree edited on the client.
U+	Create JobUnit	Create a new JobUnit.
N+	Create JobNet	Create a new JobNet.
J+	Create Job	Create a new Job.
RJ+	Create Refer Job	Create a new Refer Job.
F+	Create File-transfer Job	Create a new file transfer job.
✎	Change	Change the element (job unit, JobNet, job, file transfer job) selected in the job tree.
✖	Delete	Delete the element (job unit, JobNet, job, file transfer job) selected in the job tree.
	Object Privilege Settings	Configure object privilege for the JobNet.
▶	Run	Immediately run the element (job unit, JobNet, job, file transfer job) selected in the job tree.
	Show Scope Tree Pain	Select display/nondisplay of the job tree.

9.2.3 Job[JobKick] view

Displays a list of the Job Triggers Also, you can create, modify, and delete Triggers. You can select Schedule Run and FileCheck (create, delete, and modify files to check) as Triggers. Refer to the section, Running a Job Schedule for more details.



JobKick Type	JobKick ID	JobKick Name	Job ID	Job Name	Jobunit ID	Calendar ID	Valid/Inv...	Owner Role ID	Created User	Created Time
Schedule	test	test	test	test	jobunit		Valid	ALL_USERS	hinemos	Sep 24, 2013 9:28:40 PM

Figure 9-8 Job[JobKick] view

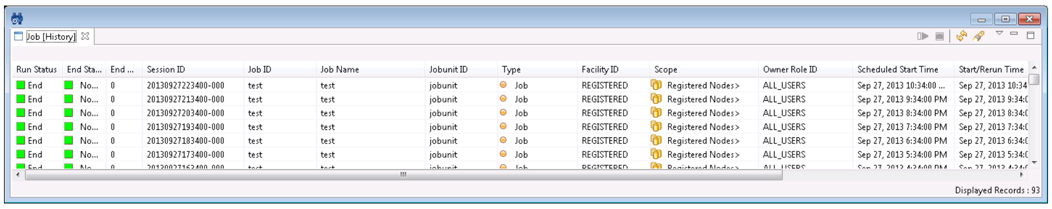
Table 9-4 Toolbar

Icon	Button name	Description
	Create FileCheck	Create the FileCheck Setting for the Job.
	Create Schedule	Create the Job Schedule Setting.
✎	Change	Change a Job Trigger.
✖	Delete	Delete a Job Trigger.
	Copy	Copy a Job Trigger.
☑	Valid	Enable the Job Trigger.
□	Invalid	Disable the Job Trigger.
	Object Privilege Settings	Configure object privilege for the Job Trigger.
	Update	Update the Job Trigger.

Copyright (c) 2013 NTT DATA CORPORATION

9.2.4 Job[History] View

A history of the Jobs that have run, Refer Jobs, File Transfer Jobs, JobNets, and JobUnits is shown. In this view, you can display filtered histories, and resume or stop jobs displayed in the history. Refer to the section, List of Job Execution History for more details.



Job [History]

Run Status	End Sta...	End ...	Session ID	Job ID	Job Name	Jobunit ID	Type	Facility ID	Scope	Owner Role ID	Scheduled Start Time	Start/Rerun Time
🟩 End	🟩 No...	0	20130927223400-000	test	test	jobunit	● Job	REGISTERED	Registered Nodes>	ALL_USERS	Sep 27, 2013 10:34:00 ...	Sep 27, 2013 10:34
🟩 End	🟩 No...	0	20130927213400-000	test	test	jobunit	● Job	REGISTERED	Registered Nodes>	ALL_USERS	Sep 27, 2013 9:34:00 PM	Sep 27, 2013 9:34:(
🟩 End	🟩 No...	0	20130927203400-000	test	test	jobunit	● Job	REGISTERED	Registered Nodes>	ALL_USERS	Sep 27, 2013 8:34:00 PM	Sep 27, 2013 8:34:(
🟩 End	🟩 No...	0	20130927193400-000	test	test	jobunit	● Job	REGISTERED	Registered Nodes>	ALL_USERS	Sep 27, 2013 7:34:00 PM	Sep 27, 2013 7:34:(
🟩 End	🟩 No...	0	20130927183400-000	test	test	jobunit	● Job	REGISTERED	Registered Nodes>	ALL_USERS	Sep 27, 2013 6:34:00 PM	Sep 27, 2013 6:34:(
🟩 End	🟩 No...	0	20130927173400-000	test	test	jobunit	● Job	REGISTERED	Registered Nodes>	ALL_USERS	Sep 27, 2013 5:34:00 PM	Sep 27, 2013 5:34:(

Displayed Records : 93

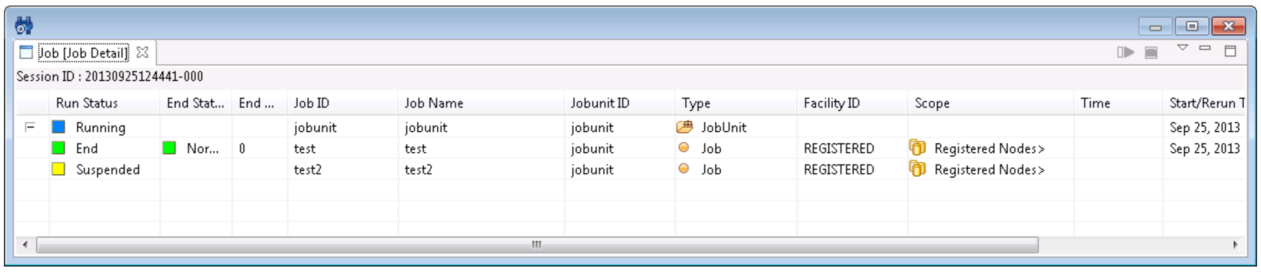
Figure 9-9 Job[History] View

Table 9-5 Toolbar

Icon	Button name	Description
▶	Start	Start a job.
🟥	Stop	Stop a job.
⟳	Update	Update job histories.
✎	Filter	Filter the list of job histories.

9.2.5 Job[Job Detail] View

The Job[History] view displays the job hierarchy and the execution status of the selected Jobs, Refer Jobs, File Transfer Jobs, JobNets and JobUnits. Also, you can resume or stop jobs, JobNets, and job units in this view. Refer to the section, List of Job Execution History for more details.



Job [Job Detail]

Session ID : 20130925124441-000

Run Status	End Stat...	End ...	Job ID	Job Name	Jobunit ID	Type	Facility ID	Scope	Time	Start/Rerun T
🟦 Running			jobunit	jobunit	jobunit	JobUnit				Sep 25, 2013
🟩 End	🟩 Nor...	0	test	test	jobunit	● Job	REGISTERED	Registered Nodes>		Sep 25, 2013
🟨 Suspended			test2	test2	jobunit	● Job	REGISTERED	Registered Nodes>		

Figure 9-10 Job[Job Detail] View

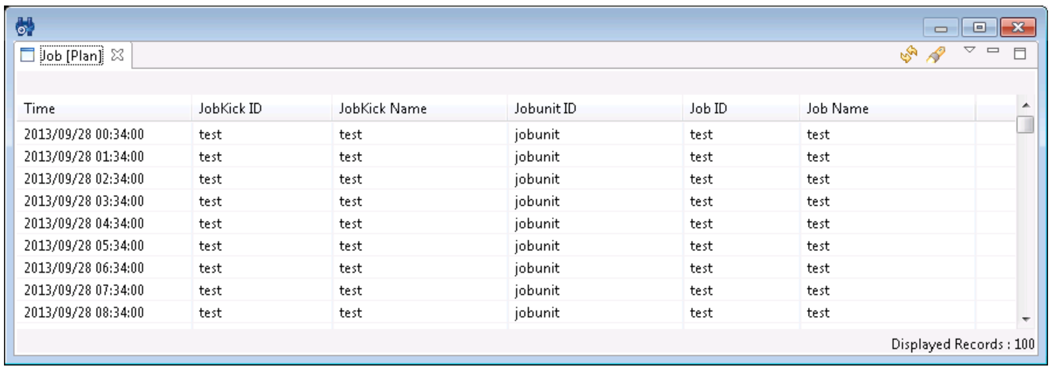
Table 9-6 Toolbar

Icon	Button name	Description
▶	Start	Start a job.
🟥	Stop	Stop a job.

9.2.6 Job[Plan] view

Displays a list of the job schedules planned for execution based on the job schedule specifications created in the Job[JobKick] view.

The default status for the Job[Plan] view shows the most recent 100 run plans.



Time	JobKick ID	JobKick Name	Jobunit ID	Job ID	Job Name
2013/09/28 00:34:00	test	test	jobunit	test	test
2013/09/28 01:34:00	test	test	jobunit	test	test
2013/09/28 02:34:00	test	test	jobunit	test	test
2013/09/28 03:34:00	test	test	jobunit	test	test
2013/09/28 04:34:00	test	test	jobunit	test	test
2013/09/28 05:34:00	test	test	jobunit	test	test
2013/09/28 06:34:00	test	test	jobunit	test	test
2013/09/28 07:34:00	test	test	jobunit	test	test
2013/09/28 08:34:00	test	test	jobunit	test	test

Displayed Records : 100

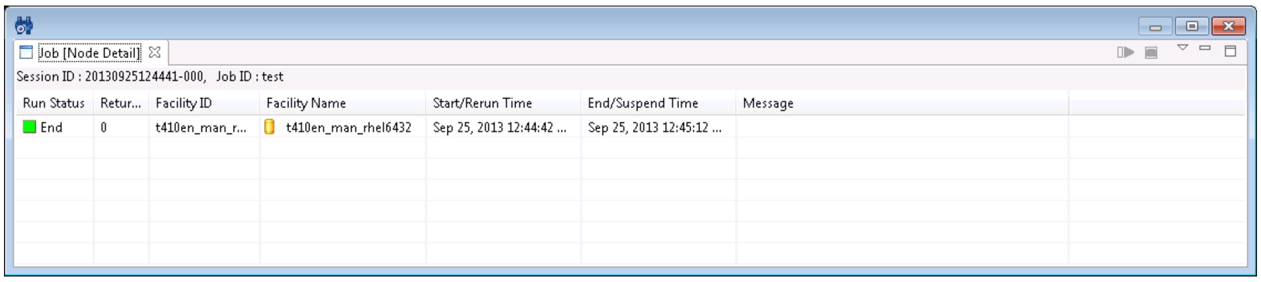
Figure 9-11 Job[Plan] view

Table 9-7 Toolbar

Icon	Button name	Description
🔄	Update	Updates the job schedule plan to the most recent.
🖊	Filter	Filters the job schedule plans.

9.2.7 Job[Node Detail] View

Job[Node Detail] view displays the selected nodes that are running jobs and the execution status of each job. In this view, you can resume or stop jobs per node. Refer to the section, List of Job Execution History for more details.



Session ID : 20130925124441-000, Job ID : test

Run Status	Retur...	Facility ID	Facility Name	Start/Rerun Time	End/Suspend Time	Message
🟩 End	0	t410en_man_r...	t410en_man_rhel6432	Sep 25, 2013 12:44:42 ...	Sep 25, 2013 12:45:12 ...	

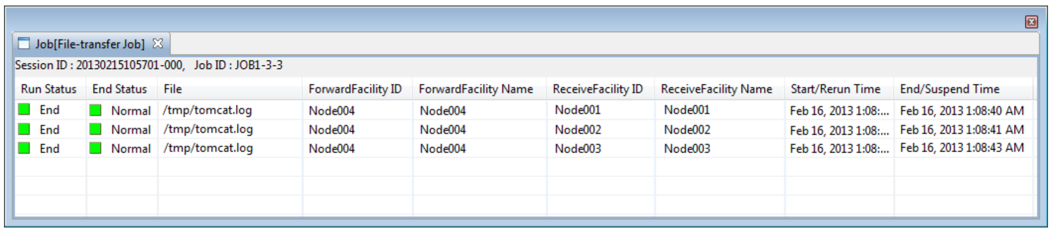
Figure 9-12 Job[Node Detail] View

Table 9-8 Toolbar

Icon	Button name	Description
▶	Start	Start a job.
🟥	Stop	Stop a job.

9.2.8 Job[File-transfer Job] View

Job[File-transfer Job] view displays the run history of the file transfer job. Refer to the section, File Transfer Job f or more details on the file transfer job.



Session ID : 20130215105701-000, Job ID : JOB1-3-3

Run Status	End Status	File	ForwardFacility ID	ForwardFacility Name	ReceiveFacility ID	ReceiveFacility Name	Start/Rerun Time	End/Suspend Time
🟩 End	🟩 Normal	/tmp/tomcat.log	Node004	Node004	Node001	Node001	Feb 16, 2013 1:08:...	Feb 16, 2013 1:08:40 AM
🟩 End	🟩 Normal	/tmp/tomcat.log	Node004	Node004	Node002	Node002	Feb 16, 2013 1:08:...	Feb 16, 2013 1:08:41 AM
🟩 End	🟩 Normal	/tmp/tomcat.log	Node004	Node004	Node003	Node003	Feb 16, 2013 1:08:...	Feb 16, 2013 1:08:43 AM

Figure 9-13 Job[File-transfer Job] View

Copyright (c) 2013 NTT DATA CORPORATION

9.3 Prerequisites for Feature Usage

The following settings must be made beforehand to use the job management feature.

- The node targeted for job execution must be registered in repository feature, and must be assigned to one of the scopes
- The notification method must be configured and registered in the notification configuration of the common features when generating a notification to the Monitor Settings feature during job execution.
- The calendar must be registered in the calendar configuration of the common features beforehand when configuring the valid period of the job execution based on the calendar configuration.

9.4 Registering a job

9.4.1 Creating/Changing a Job Unit

Edit Mode

You must switch to Edit Mode to Edit (create, modify or delete) JobUnits or Jobs or JobNets in the subordinate hierarchy. You can only inspect the settings of JobUnits that haven't switched to Edit Mode.

Switching to Edit Mode is done in JobUnit units. "[Edit Mode]" is shown at the end of the Job Name in the job tree in the Job[List] view for JobUnits that are in Edit Mode.

Switching to and releasing Edit Mode

1. Select the JobNet to switch from the job tree in the Job[List] view. Click the "Edit Mode" button at the top right of the Job[List] view.
2. Select the JobUnit for Edit Mode and click the "Edit Mode" button once again to release Edit Mode.

When you release Edit Mode, the status of the JobUnit returns to the status prior to switching to Edit Mode.

Further, switching to and releasing Edit Mode is not just for JobUnits; you can also select jobs, etc. in the subordinate hierarchy and perform it as well. Even in that case, switching to Edit Mode is done by JobUnit units.

Important Points about Edit Mode

- If a different user wants to switch a JobUnit to Edit Mode,

  only one user can switch the JobUnit to Edit Mode. If another user wants to switch a JobUnit to Edit Mode and they click on the "Edit Mode" button, the following message will be displayed.

  ```
  An Edit Lock on the JobUnit "(JobUnit ID)" has been obtained by another user ((User Name), (IP Address of the connecting client)).
  Do you want to obtain an Edit Lock?
  ```

  In that case, when you click the "Yes" button, the Edit Mode for the JobUnit that had been switched to Edit Mode by the other user will change from the other user to yourself.

  - If the Job's settings differ from the manager

    To switch the Job to Edit Mode, the settings for the JobUnit maintained by the Hinemos Client and the settings for the JobUnit registered with the Hinemos Manager must match.

    If another user has changed the JobUnit settings and the setting information maintained by the Hinemos Client is different than that registered with the Hinemos Manager, the following message is displayed when the "Edit Mode" button is clicked.

    ```
    The job tree is not the latest (Last Change Time: (Last change time for the JobUnit)).
    ```

    In this case, to edit the JobUnit, you must click on the "Cancel" button at the top right of the Job[List] view and obtain the latest JobUnit setting information.

Creating a Job Unit

1. Select "Job" located at the top of the job tree in the Job[List] view.

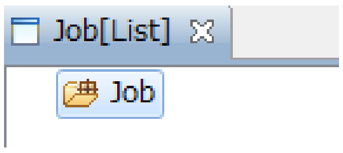
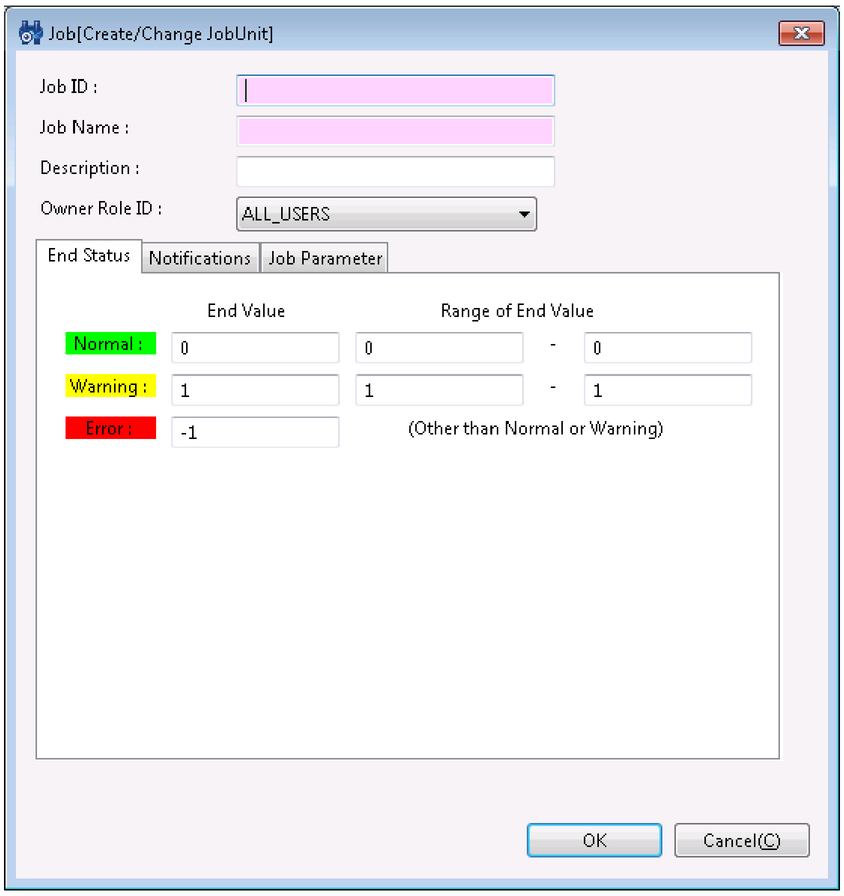


Figure 9-14 Selecting a Job Unit From the Job Tree

2. Click the "Create JobUnit" button in the Job[List] view. The Job[Create/Change JobUnit] dialog is displayed.
3. Configure "Job ID", "Job Name", and "Description". Always be sure to enter the "Job ID" and "Job Name", since b oth are mandatory fields. The "Job ID" of the job unit must be unique on the system.
4. To change the End Status from the default setting, select the "End Status" tab and make the change. The range of the end values for "Normal" and "Warning" cannot overlap (Refer to the section, End Status and End Value for more details relating to the end status and end value).



Job ID :
Job Name :
Description :
Owner Role ID : ALL_USERS

	End Value	Range of End Value		
Normal :	0	0	-	0
Warning :	1	1	-	1
Error :	-1	(Other than Normal or Warning)		

Figure 9-15 Job[Create/Change JobUnit] Dialog (End Status tab)

5. Configure "Notifications". Select the "Notifications" tab. Configure the following items.

- Start:

  Configure the notification that is generated during the start of a job unit.
- Normal:

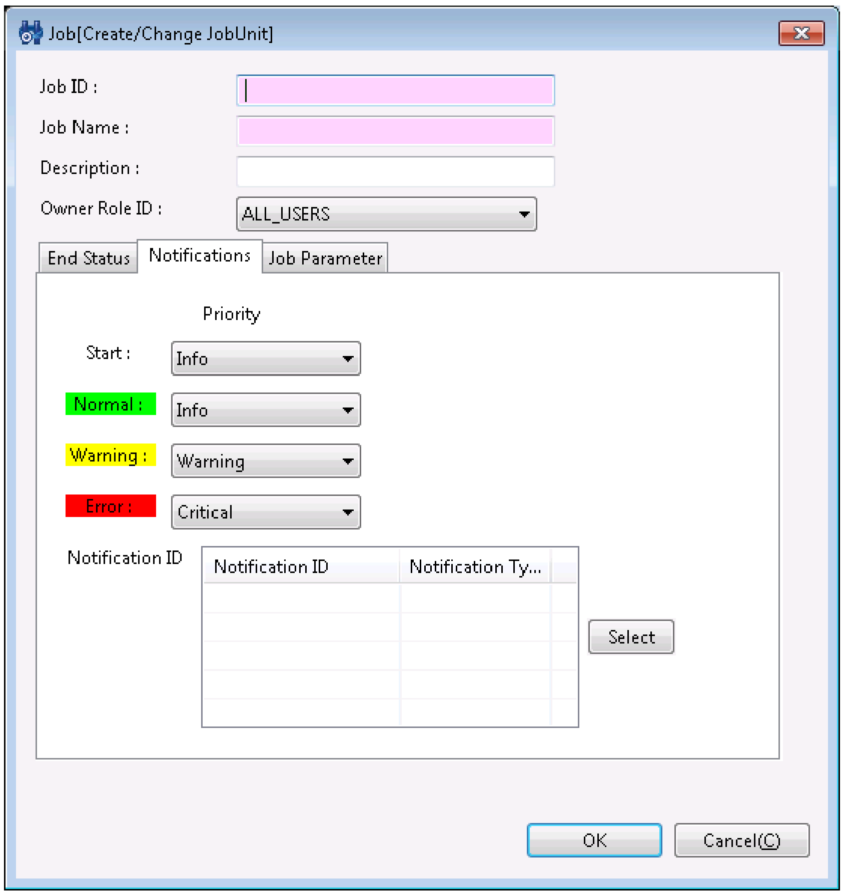
  Configure the notification that is generated when the end status of a job unit is "Normal".
- Warning:

  Configure the notification that is generated when the end status of a job unit is "Warning".
- Error:

  Configure the notification that is generated when the end status of a job unit is "Error".

- Notification ID:

  Select from the list the Notification ID that is the notification method used in the notification setting. (Refer to the section `Notification Feature`_ regarding notification settings) When you click the "Select" button on the right, the Notification[List] dialog is displayed. Select the notification method.



Job[Create/Change JobUnit]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

Priority

Start : Info

Normal : Info

Warning : Warning

Error : Critical

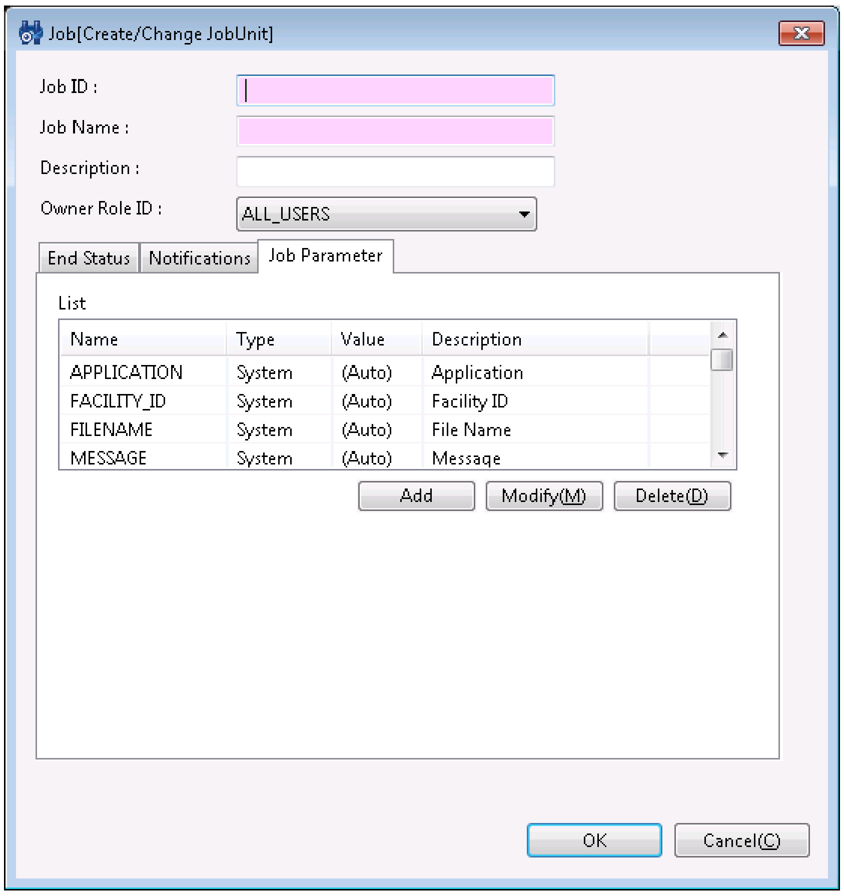
Notification ID

Notification ID	Notification Ty...

Figure 9-16 Job[Create/Change JobUnit] Dialog (Notifications tab)

Copyright (c) 2013 NTT DATA CORPORATION

6. Setup Job Parameter. Select the "Job Parameter" tab.



Job[Create/Change JobUnit]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

List

Name	Type	Value	Description
APPLICATION	System	(Auto)	Application
FACILITY_ID	System	(Auto)	Facility ID
FILENAME	System	(Auto)	File Name
MESSAGE	System	(Auto)	Message

Figure 9-17 Job[Create/Change JobUnit] Dialog (Job Parameter tab)

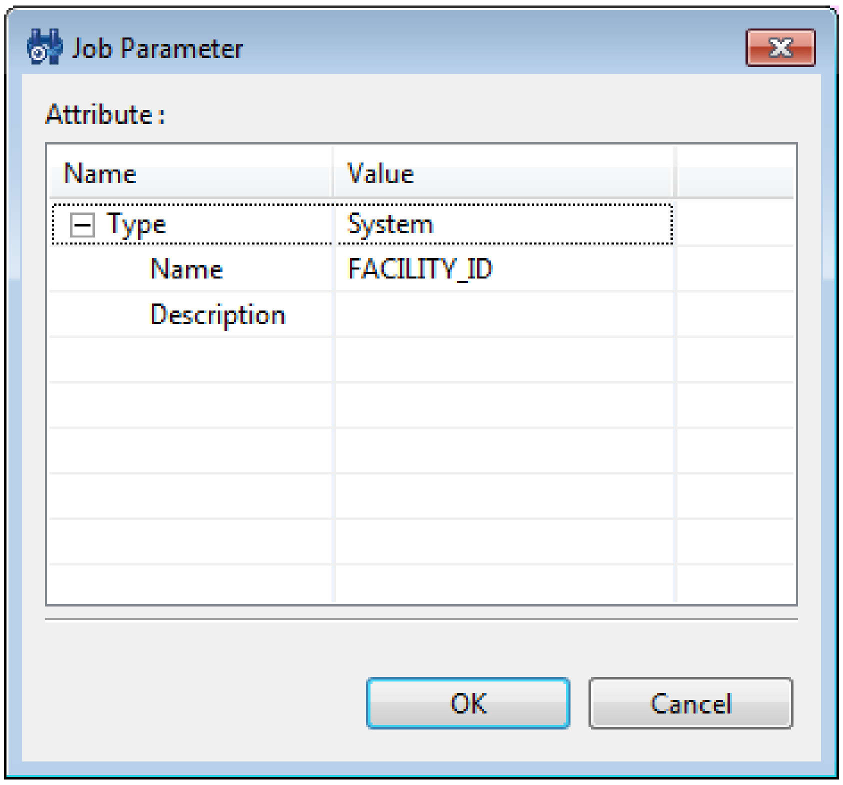
Configure by the following procedures.

- Adding a job variable

  When the "Add" button is clicked, the Job Parameter dialog is displayed.

  Select either the system job variable or the user job variable as "Type", and then configure the following.

  System job variable



Job Parameter

Attribute :

Name	Value
⊟ Type	System
Name	FACILITY_ID
Description	

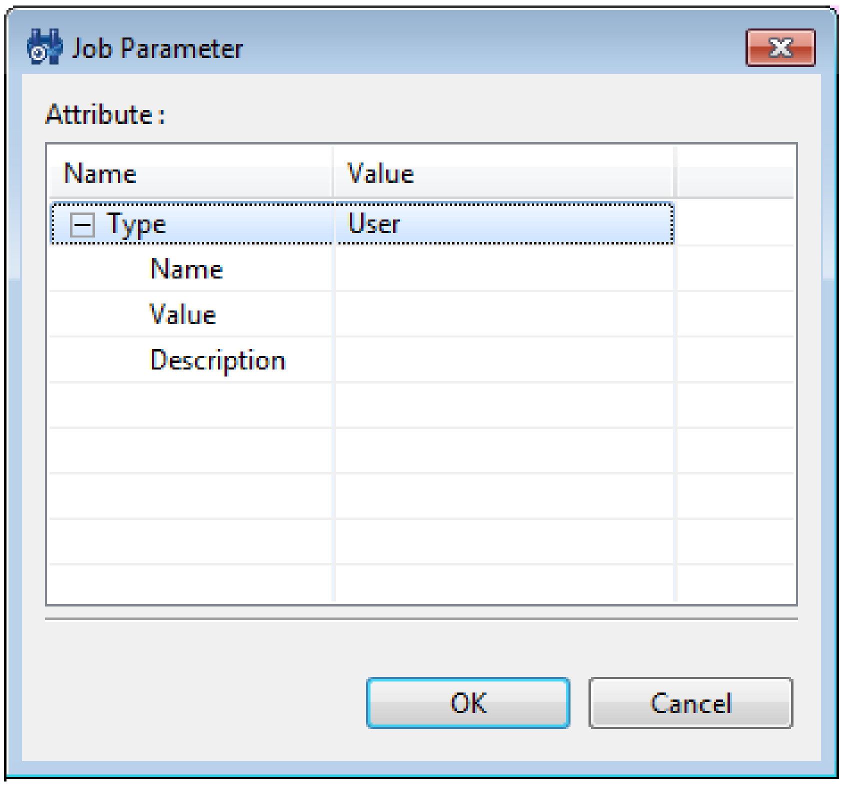
Figure 9-18 Job Count Dialog (When System is Selected as the Type)

- Name:

  Select the system job variable to add from the list.
- Description:

  Enter a description of the job variable.

User job variable



Job Parameter

Attribute :

Name	Value
⊟ Type	User
Name	
Value	
Description	

Figure 9-19 Job Count Dialog (When User is Selected as the Type)

- Name:

  Enter a variable name. User job variable can be referred by #[variable name] at the command field of a job.

  Only the characters "_" or "-" can be used as the text for the variable name.
- Value:

  Enter a value assigned to the job variable.
- Description:

  Enter a description of the job variable.

  Click the "OK" button.

- Changing a job variable

  Select the job variable to change from the list, and then click the "Modify" button. The Job Parameter dialog is displayed. Change the contents, and then click the "OK" button.
- Deleting a job variable

  Select the job variable to change from the list, and then click the "Delete" button.

7. Click the "OK" button. The Job[Create/Change JobNet] dialog closes. The newly created job unit is added to th e job tree in the Job[List] view.

   Note) The operations described above are made in the client. Information of the editing job tree is not reflect ed in the manager until the "Register" button is clicked and it has processed.

Changing a Job Unit

- To change the JobUnit, the JobUnit must be in Edit Mode.

1. Select the job unit to change from the job tree in the Job[List] view.
2. Click on the "Modify" button in the Job[List] view. The Job[Create/Change JobUnit] dialog is displayed.
3. Modify the parameter of the job unit

Copy a Job Unit

1. From the job tree in the Job[List] view, right click on the JobUnit to be copied and then click "Copy".
2. From the job tree in the Job[List] view, right click on the copy destination and then click "Paste".
3. From the job tree in the Job[List] view, select the JobUnit that was copied.
4. Click on the "Modify" button in the Job[List] view. The Job[Create/Change JobUnit] dialog is displayed.
5. Change the temporarily defined Job ID (Copy_Of_xxx) as necessary.

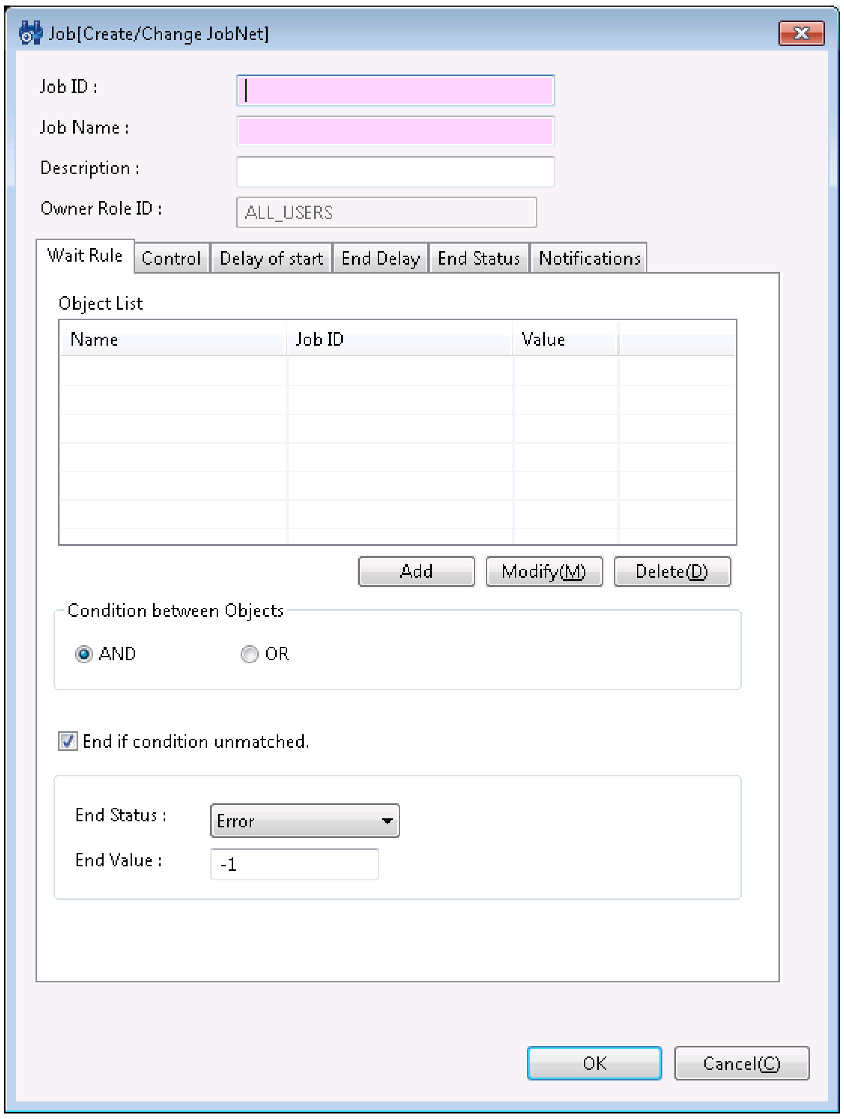
9.4.2 Creating/Changing a JobNet

Creating a JobNet

- To create a JobNet, the JobUnit that is the destination for creating the JobNet must be in Edit Mode.

1. From the job tree in the Job[List] view, select the JobUnit or JobNet that is to be the source for creating the JobNet.

2. Click on the "Create JobNet" button in the Job[List] view. The Job[Create/Change JobNet] dialog is displayed.



Job[Create/Change JobNet]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

Object List

Name	Job ID	Value

Condition between Objects

● AND ○ OR

☑ End if condition unmatched.

End Status : Error

End Value : -1

Figure 9-20 Job[Create/Change JobNet] Dialog

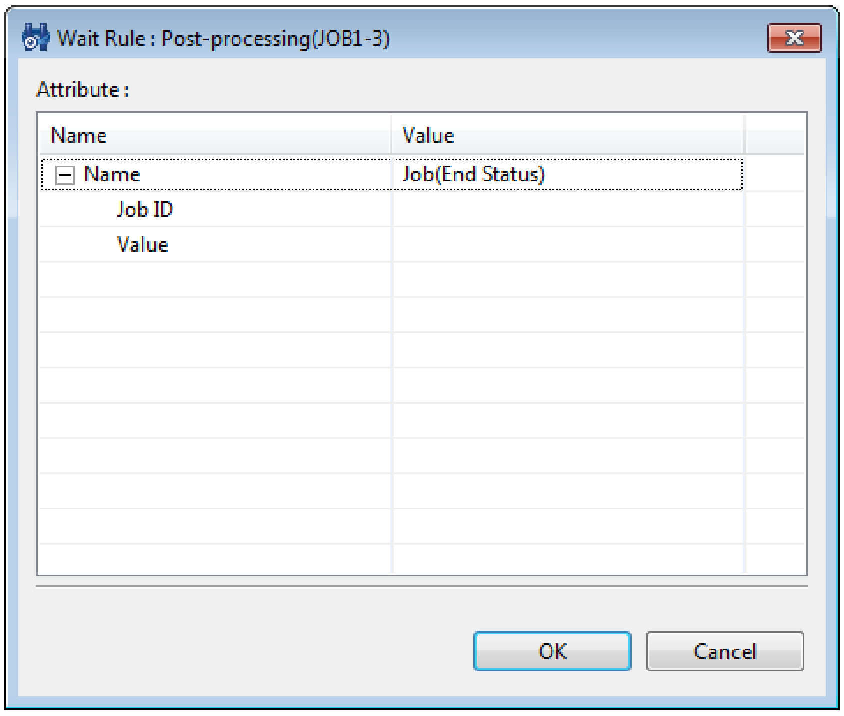
3. Configure "Job ID", "Job Name", and "Description". Always be sure to enter the "Job ID" and "Job Name", since b oth are mandatory fields. "Job ID" of the job unit must be unique within the same job unit.

4. Enter "Wait Rule". Select the "Wait Rule" tab. First, configure the "Object".

- Add a wait rule

  You can specify the status when the preceding job ended (end status or end value) and time as the wait rule. For example, by specifying the End condition of the preceding job as a wait rule, you can make a setting that executes the JobNet when the preceding job Ends with an error.

  Click on the "Add" button located at the bottom of "Object List". The Wait Rule dialog is displayed.



Wait Rule : Post-processing(JOB1-3)

Attribute :

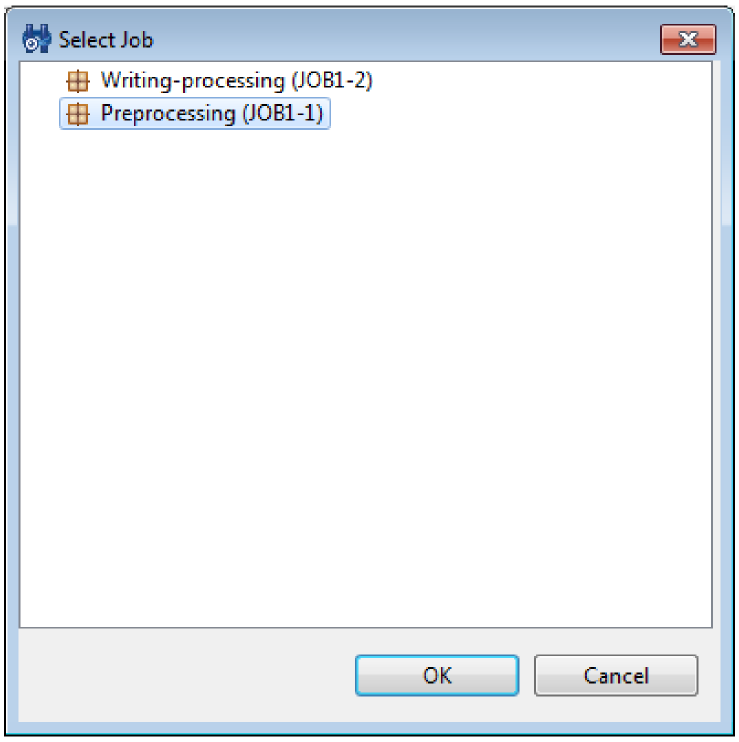
Name	Value
⊟ Name	Job(End Status)
Job ID	
Value	

Figure 9-21 Wait Rule Dialog

When making the end status of the preceding job a wait rule:

a. Click on the record value for the table property "Name". From the combo box, select "Job(End Status)".

b. Configure the preceding job. a. Click on the record value for the table property "Name-Job ID". Then click on the button that appears on the far right of the field. The Select Job dialog is displayed.



Select Job

- Writing-processing (JOB1-2)
- Preprocessing (JOB1-1)

Figure 9-22 Select Job Dialog

c. Select the preceding job from the scope tree, and then click the "OK" button. The Select Job dialog closes. "Job ID" will be added to the Wait Rule dialog.

Copyright (c) 2013 NTT DATA CORPORATION

d. Select the End Status (Normal, Warning or Error). Click the value field of the "Value". A Combo box is displayed. Select the End Status (Normal, Warning or Error).

   You can specify the final status as * (asterisk), in addition to Normal, Warning or Error. If set as *, regardless of the end status (Normal, Warning or Error) of the prior job specified as a Wait Rule, the Wait Rule will be judged to be met when the prior job status is "End".

   An arbitrary end status can be set in the Wait Rule.

e. Click the "OK" button. The Wait Rule dialog closes. The configured wait rule will be added to the "Object List" table.

When making the end value of the preceding job a wait rule:

a. Click on the record value for the table property "Name". From the combo box, select "Job(End Value)".

b. Configure the preceding job. a. Click on the record value for the table property "Name-Job ID". Then click on the button that appears on the far right of the field. The Select Job dialog is displayed.

c. Select the preceding job from the scope tree, and then click the "OK" button. The Select Job dialog closes. "Job ID" will be added to the Wait Rule dialog.

d. Click the value field for the record of the property "Value" in the table. Enter the End Value.

e. Click the "OK" button. The Wait Rule dialog closes. The configured wait rule will be added to the "Object List" table.

When making time a wait rule:

a. Click on the record value for the table property "Name". From the combo box, select "Time".

b. Configure the time. Select the time to start the JobNet in the value field for the record of the property "Time" in the table Enter hours and minutes in the "hh:mm:ss" format. The range of time that can be set as a Wait Rule is 00:00:00～48:00:00.

- Changing a wait rule

  a. Select the wait rule to change from the "Object List" table.

  b. Click on the "Modify" button located at the bottom of "Object List". The Wait Rule dialog is displayed. Change the parameter.

  c. Click the "OK" button. The Wait Rule dialog closes. Changes will be reflected. Click the "Cancel" button to cancel the modification.

- Deleting a wait rule

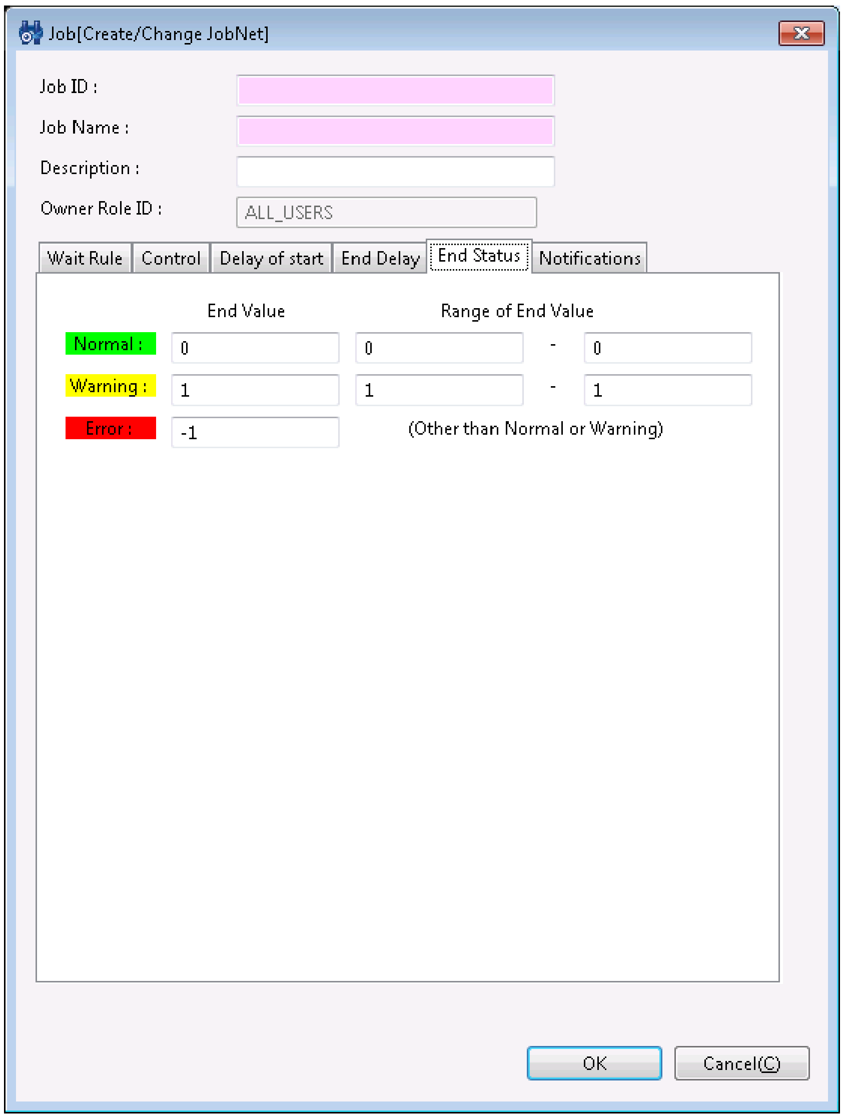
  a. Select the Wait Rule to delete from the "Object List" table, and then click the "Delete" button.

5. Configure "Condition between Objects". Select the "AND" or "OR" radio button. If "AND" is selected, the JobNet starts when all configured wait rules are met. If "OR" is selected, the JobNet starts when any one of the wait rule is met.

6. You can configure an operation to process when it is determined that all wait rules will not be met. Wait conditions are checked during the JobNet execution. JobNet execution can be configured to end when it is determined that all wait rules will not be met. Check the "End if condition unmatched." button to apply this operation, and then configure the End Status and End Value.

Copyright (c) 2013 NTT DATA CORPORATION

7. Next, set up the End Status. When changing the End Status from the default setting, select the "End Status" tab and make the change. The range of the end values for "Normal" and "Warning" cannot overlap (Refer to the section, End Status and End Value for more details relating to the end status and end value).



Job[Create/Change JobNet]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

	End Value	Range of End Value		
Normal :	0	0	-	0
Warning :	1	1	-	1
Error :	-1	(Other than Normal or Warning)		

Figure 9-23 Job[Create/Change JobNet] Dialog (End Status Tab)

8. Configure "Notifications". Select the "Notifications" tab. Configure the following items.

- Start:

  Configure the notification that is generated during the start of a JobNet.

- Normal:

  Configure the notification that is generated when the end status of a JobNet is "Normal".

- Warning:

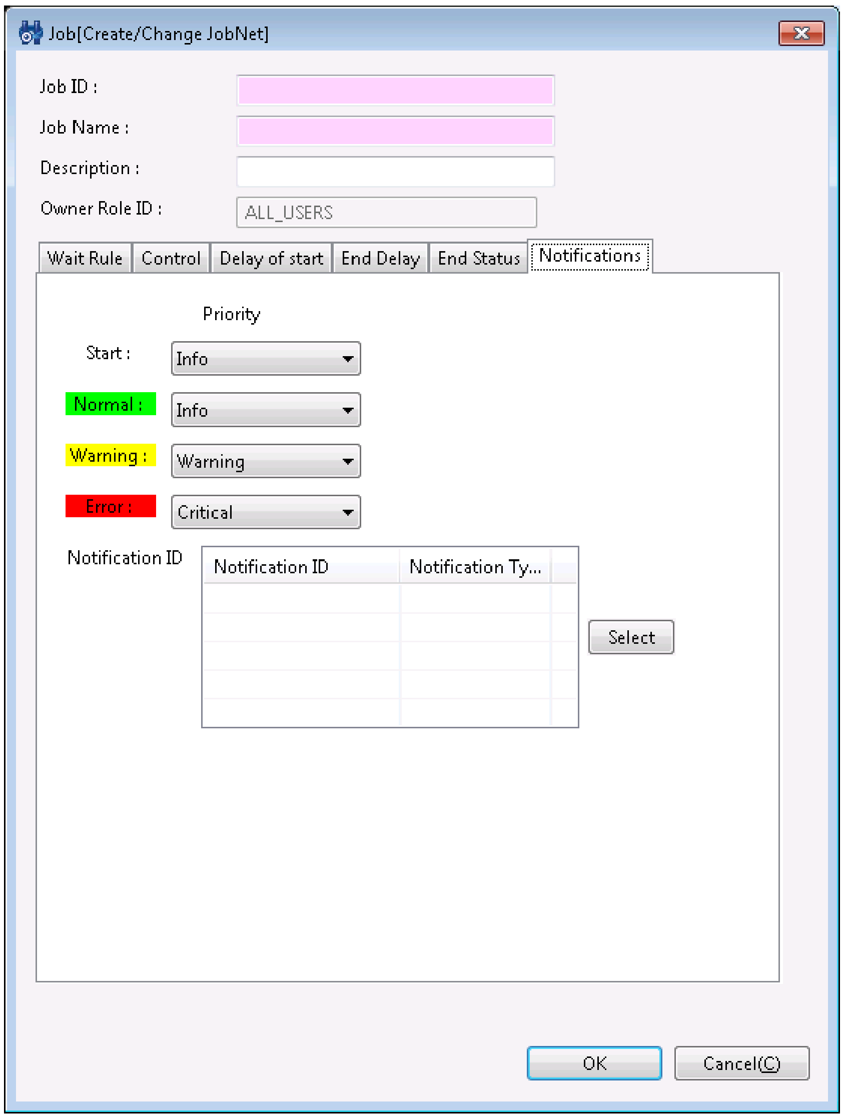
  Configure the notification that is generated when the end status of a JobNet is "Warning".

- Error:

  Configure the notification that is generated when the end status of a JobNet is "Error".

- Notification ID:

  Select from the list the Notification ID that is the notification method used in the notification setting. (Refer to the section `Notification Feature`_ regarding notification settings) When you click the "Select" button on the right, the Notification[List] dialog is displayed. Select the notification method.



Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

Start : Info

Normal : Info

Warning : Warning

Error : Critical

Notification ID

Figure 9-24 Job[Create/Change JobNet] Dialog (Notifications)

9. **Click the "OK" button. The Job[Create/Change JobNet] dialog closes.**

   The newly created JobNet will be added to the job tree in the Job[List] view.

   Note) The operations described above are made in the client. Information of the editing job tree is not reflected in the manager until the "Register" button is clicked and it has processed.

Changing a JobNet

- To change a JobNet, the JobUnit to which the JobNet you want to change belongs must be in Edit Mode.

1. Select the JobNet to change from the job tree in the Job[List] view.
2. Click on the "Modify" button in the Job[List] view. The Job[Create/Change JobNet] dialog is displayed.
3. Modify the parameter of the JobNet.

Copy a JobNet

1. From the job tree in the Job[List] view, right click on the JobNet to be copied and then click "Copy".
2. From the job tree in the Job[List] view, right click on the copy destination and then click "Paste".

- The JobUnit that is the paste destination must be in Edit Mode when you paste the copied JobNet.

3. From the job tree in the Job[List] view, select the JobNet that was copied.

Copyright (c) 2013 NTT DATA CORPORATION

4. Click on the "Modify" button in the Job[List] view. The Job[Create/Change JobNet] dialog is displayed.
5. Change the temporarily defined Job ID (Copy_Of_xxx) as necessary.

9.4.3 Items to Consider when Creating/Changing a JobNet

Controlling a JobNet

You can control the execution of a JobNet with the following settings.

- Configure a calendar
- Suspend the execution status of a job in advance
- Skip the execution status of a job in advance

1. Select the "Control" tab in the Job[Create/Change JobNet] dialog.

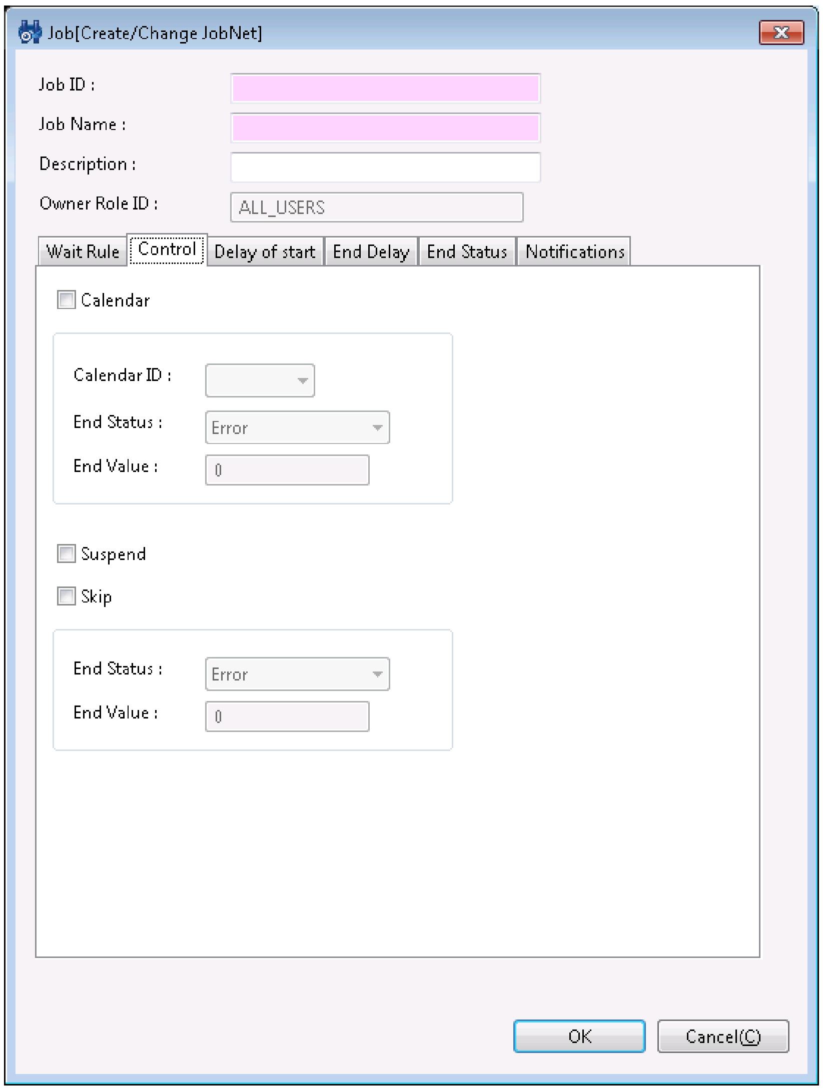


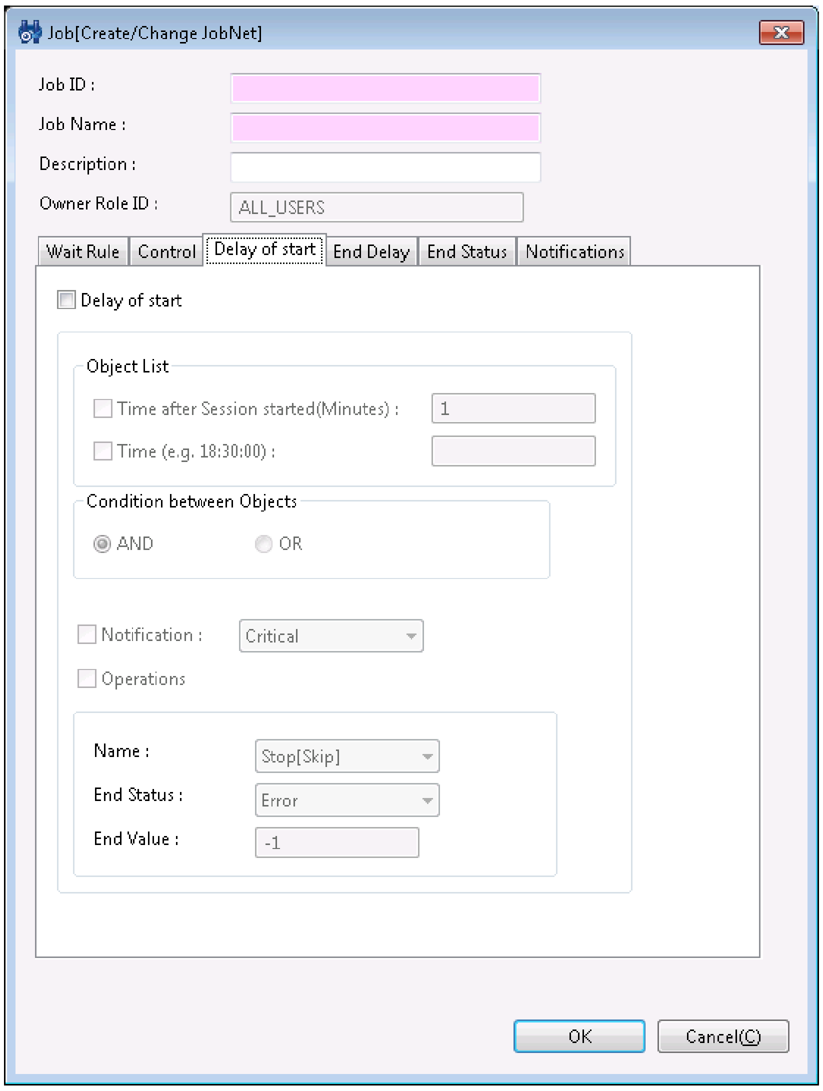
Figure 9-25 Job[Create/Change JobNet] Dialog (Control Tab)

2. If configuring a calendar, check on the "Calendar" check box. Select the calendar ID for the calendar you want to set up. When setting a calendar, it can only be run when the job session start time is within the operation period range of the specified calendar. (Refer to the section, `Calendar Feature`_ for more details on the calendar). When a JobNet can't be run due to calendar conditions, enter the setting value as the JobNet end value for the value in "End Value".
3. Check on the "Suspend" check box Enter a check in the "Suspend" checkbox. Similarly, to advance skip a run status, enter a check in the "Skip" checkbox and enter the end value.

Delay of Start Monitoring

Check if the start of JobNet execution has been delayed. It is possible to configure control if it is delayed.

1. Select the "Delay of start" tab in the Job[Create/Change JobNet] dialog.



Job[Create/Change JobNet]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

☐ Delay of start

Object List

☐ Time after Session started(Minutes) : 1

☐ Time (e.g. 18:30:00) :

Condition between Objects

● AND ○ OR

☐ Notification : Critical

☐ Operations

Name : Stop[Skip]

End Status : Error

End Value : -1

Figure 9-26 Job[Create/Change JobNet] Dialog (Delay of Start Tab)

2. Check on the "Delay of start" check box, and then set the following items.

- Object List:
  - Time after Session started (Minutes)

    Execute delayed monitoring by the time elapsed since the job session started. A job session is a unit used for running a job unit (or the JobNet). A job session is created each time job unit (or JobNet) is run. When a series of job units (or JobNets) end, the job session itself ends as well. (The history displayed in the Job[History] view is a job session unit).

    When a currently set JobNet is run, if the time set as the delay time has elapsed since the job session started, it is judged to be delayed.

  - Time

    You can run delay monitoring by time. When a currently set JobNet is run, it is judged to be delayed when the specified time has elapsed.

    If you do Delay of Start Monitoring by time, the delay will be determined using the same evaluation method as the Wait Rule time. Confirm the Wait Rule time evaluation method for details.

- Condition between Objects:

  Set the Condition between Objects set for the Object List.

  If "AND" is selected and the conditions of both the Time after Session started (Minutes) and Time are met, the JobNet execution is judged to be delayed.

  If "OR" is selected, JobNet execution is judged as delayed when either one of the conditions are met.

Copyright (c) 2013 NTT DATA CORPORATION

- Notification:

  To perform notification when the job Delay of start occurs, check the check box and select the priority of the notification.

  Further, notification due to Delay of start does not affect the Priority above the "Notification ID" field in the "Notifications" tab, and the notification is made with the specified priority.

- Operations:

  To run an operation for a job where a Delay of start occurred for that job, check the check box and select the operation to run.

  The following two operations can be selected.

  - Stop[Skip]

    The run status of the JobNet is Skip. Enter the end value when the run status is Skip.

  - Stop[Suspend]

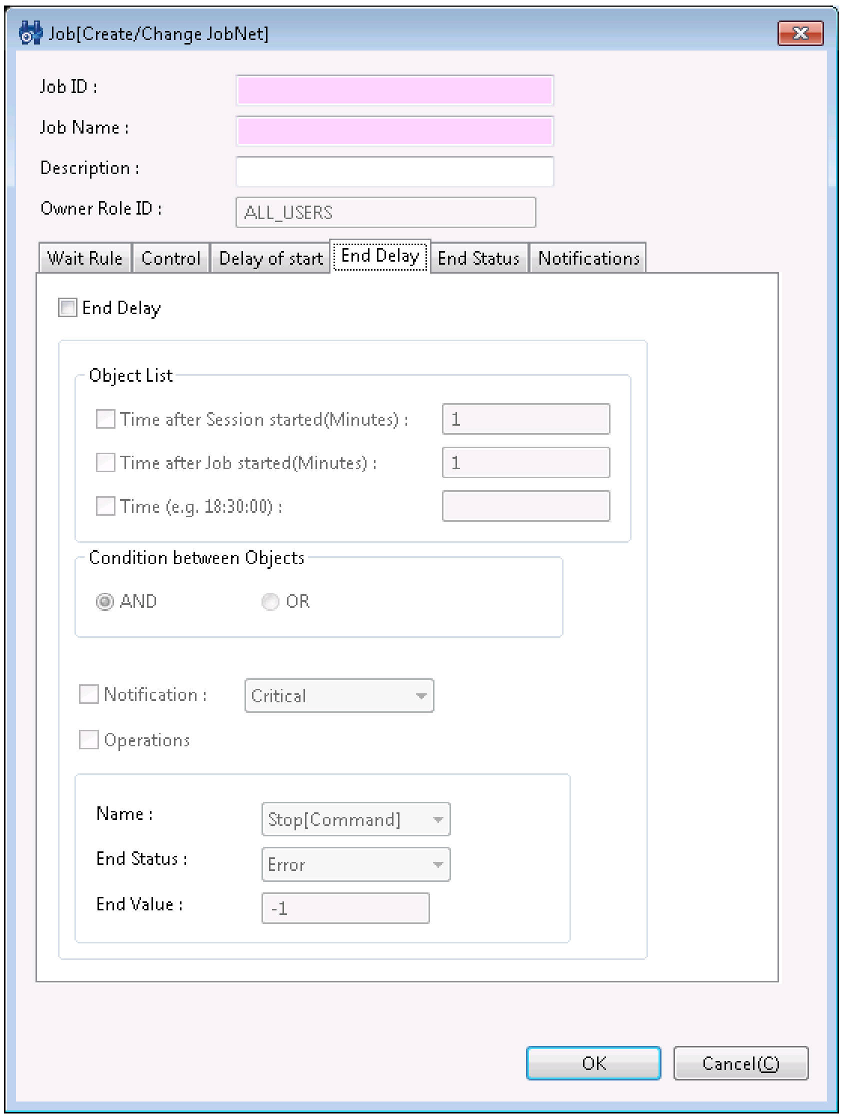
    The run status of the job is Suspend.

  Note) When running a JobNet (Job), the settings for the wait rule, delayed monitoring (delayed start/delayed End), and control (calendar, suspend, skip) of the job net (job) at the top are disabled when a JobNet (job) is run.

When Running End Delay Monitoring

Check if the end of a JobNet has been delayed. You can configure the control if it is delayed.

1. Select the "End Delay" tab in the Job[Create/Change JobNet] dialog.



Job[Create/Change JobNet]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

□ End Delay

Object List

□ Time after Session started(Minutes) : 1

□ Time after Job started(Minutes) : 1

□ Time (e.g. 18:30:00) :

Condition between Objects

● AND ○ OR

□ Notification : Critical

□ Operations

Name : Stop[Command]

End Status : Error

End Value : -1

Figure 9-27 Job[Create/Change JobNet] Dialog (End Delay Tab)

2. Check on the "End Delay" check box, and then set the following items.

Copyright (c) 2013 NTT DATA CORPORATION

- Object List:
  - Time after Session started (Minutes)

    Execute delayed monitoring by the time elapsed since the job session started.

    If the specified time has already passed since the start of the session and the JobNet being configured does not end, it is judged as a delay.
  - Time after Job started(Minutes)

    Execute delayed monitoring by the time elapsed since the job net started. Even if the specified time has already passed and the JobNet has not ended, it is evaluated as a delay.
  - Time

    You can run delay monitoring by time. If the configuring JobNet does not end after the specified time, and the JobNet being configured does not end, it is evaluated as a delay.

    If you do End Delay Monitoring by time, the delay will be determined using the same evaluation method as the Wait Rule time. Confirm the Wait Rule time evaluation method for details.
- Condition between Objects:

  Set the Condition between Objects set for the Object List.

  If "AND" is selected. it is evaluated as job execution has been delayed when all three conditions, "Time after Session started(Minutes)", "Time after Job started(Minutes)", and "Time" are met.

  If "OR" is selected, it is evaluated that the JobNet end has been delayed when either one of the condition are met.
- Notification:

  When notification is performed when the job End Delay occurs, check the check box and select the priority of the notification.
- Operations:

  To run an operation for a job where an End Delay occurred for a job, check the check box and select the operation to run.

  The following three operations can be selected.
  - Stop[Command]:

    The run status of the job is Command Stop.
  - Stop[Pause]

    The run status of the job is Pause.
  - Stop[Set End Value]

    The run status of the job is End. Enter the end value when the run status is End.

  Note) When running a JobNet (Job), the settings for the wait rule, delayed monitoring (delayed start/delayed End), and control (calendar, suspend, skip) of the job net (job) at the top are disabled when a JobNet (job) is run.

Wait Rules for Copy Operation Time

If a JobNet is copied,

the Wait Rules of that JobNet, and of some JobNets/Jobs subordinate to that JobNet which are controled by "End Status" and "End Value", will be deleted.

- If the Wait Rule is "Time",

  all of the Wait Rules are copied.
- If the Wait Rule is "End Value" or "End Status",

  only the Wait Rules subordinate to the copied JobNet are copied.

Wait Rule Time Evaluation Method

If Time is selected as the Wait Rule, the range of time that can be set as the Wait Rule is 00:00:00～48:00:00.

The Wait Rule evaluates conditions based on the following formula.

(The Wait Rule is judged to be met if the following formula is met.)

The job session start date + Wait Rule time <= the current date and time.

(Example 1) The job (Job2) operates when the Wait Rule is set as the end of the prior Job (Job1) and time (26:00:00).

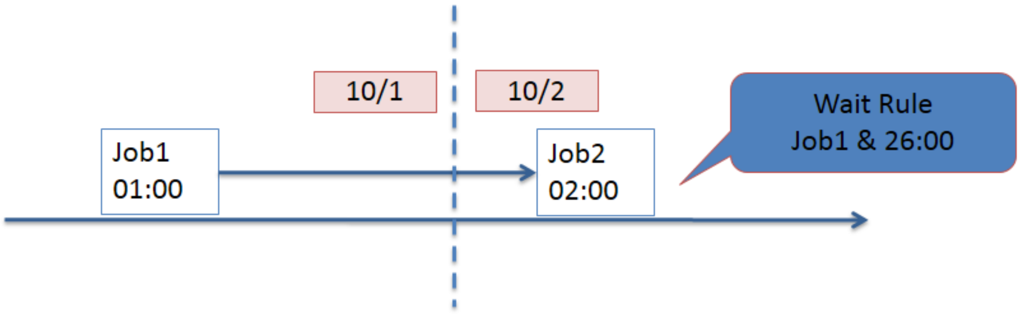


Figure 9-28 Operation Example (1) When Time Is Specified as the Wait Rule

(Example 2) When the Wait Rule is set as the end of the prior Job (Job1) and time (23:50:00),

the Job (Job2) will operate if Job1 has not ended by 23:50:00.

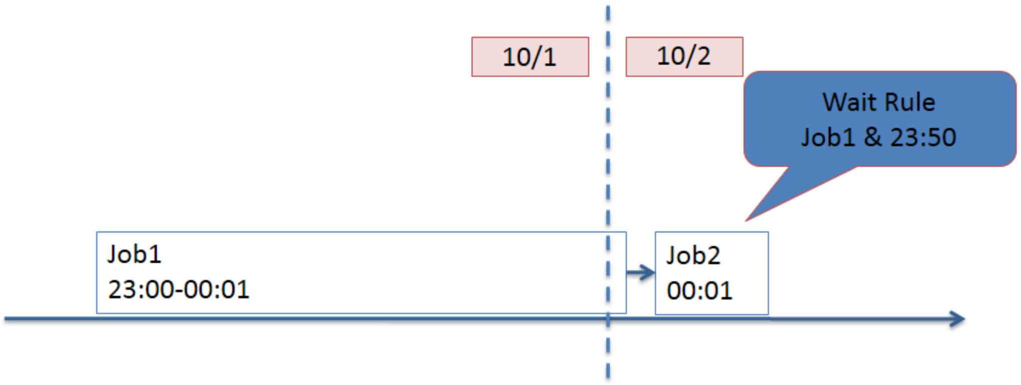


Figure 9-29 Operation Example (2) When Time Is Specified as the Wait Rule

9.4.4 Creating/Changing a Job

A job is the smallest unit that can be executed. A command that will be issued to the node during job execution must be configured. Configuration procedures of the end status and the wait rules are similar to the procedures for creating a job net.

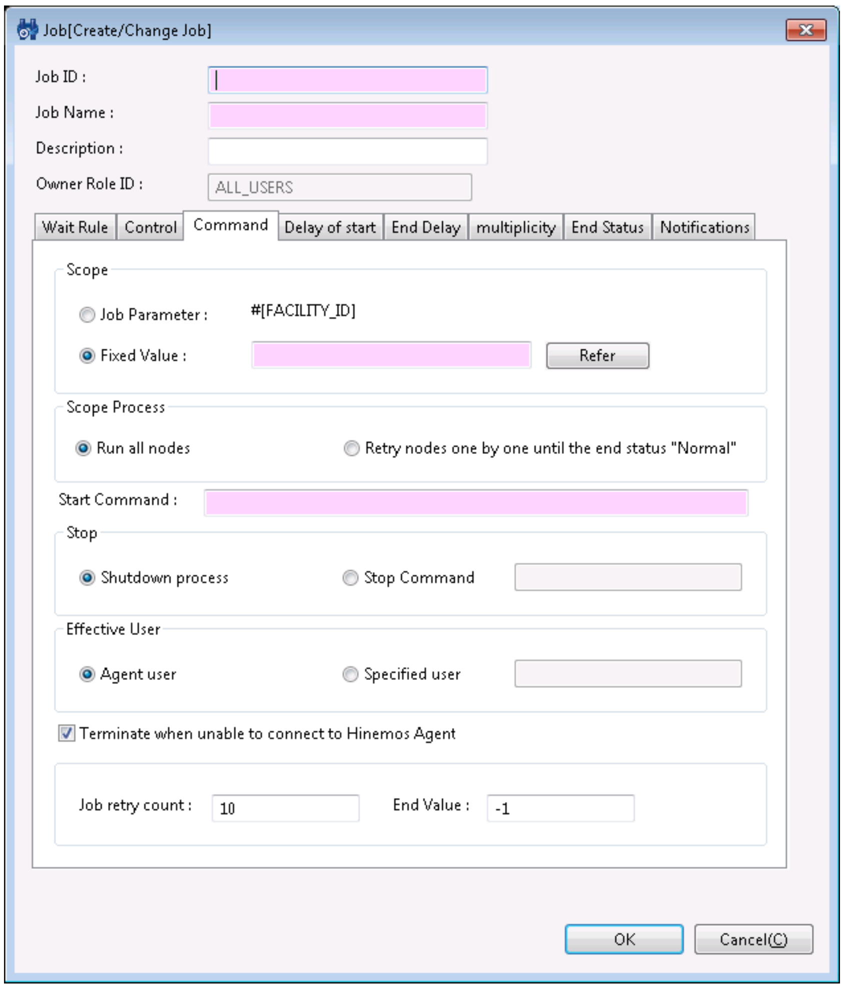
Creating a Job

- To create a Job, the JobUnit that is the destination for creating the Job must be in Edit Mode.

1. From the job tree in the Job[List] view, select the new job to be added to a JobNet (or JobUnit).
2. Click the "Create Job" button in the Job[List] view. The Job[Create/Change Job] dialog is displayed.
3. Configure "Job ID", "Job Name", and "Description". Always be sure to enter the "Job ID" and "Job Name", since both are mandatory fields. The "Job ID" of the job must be unique within the same job unit.
4. Select the "Wait Rule" tab, and then configure the wait rule (Refer to Creating/Changing a JobNet for the Wait Rule entry method.)

Copyright (c) 2013 NTT DATA CORPORATION

5. Configure the command executed in the node during job execution. Select the "Command" tab, and set the following items. (Refer to Job Execution Using a Script if registering a script in the command field)



Job[Create/Change Job]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

Scope

○ Job Parameter : #[FACILITY_ID]

● Fixed Value :

Scope Process

● Run all nodes ○ Retry nodes one by one until the end status "Normal"

Start Command :

Stop

● Shutdown process ○ Stop Command

Effective User

● Agent user ○ Specified user

☑ Terminate when unable to connect to Hinemos Agent

Job retry count : 10 End Value : -1

Figure 9-30 Job[Create/Change Job] Dialog (Command Tab)

Copyright (c) 2013 NTT DATA CORPORATION

- Scope:
  - Job Parameter

    The job selected in this setting is valid only for Job execution triggered by job notification. The scope (or the node) that issued the notification is the subject for job execution.

    Note) "FACILITY_ID" for the "Job Parameter" must be registered during job unit creation if configuring scope specification by the job variable.

  - Fixed Value

    In "Fixed Value" field, specify the scope (or the node) subject for job execution.

    Click the "Refer" button and the Select Scope dialog is displayed; Select the scope subject for command execution, and then click on the "OK" button.

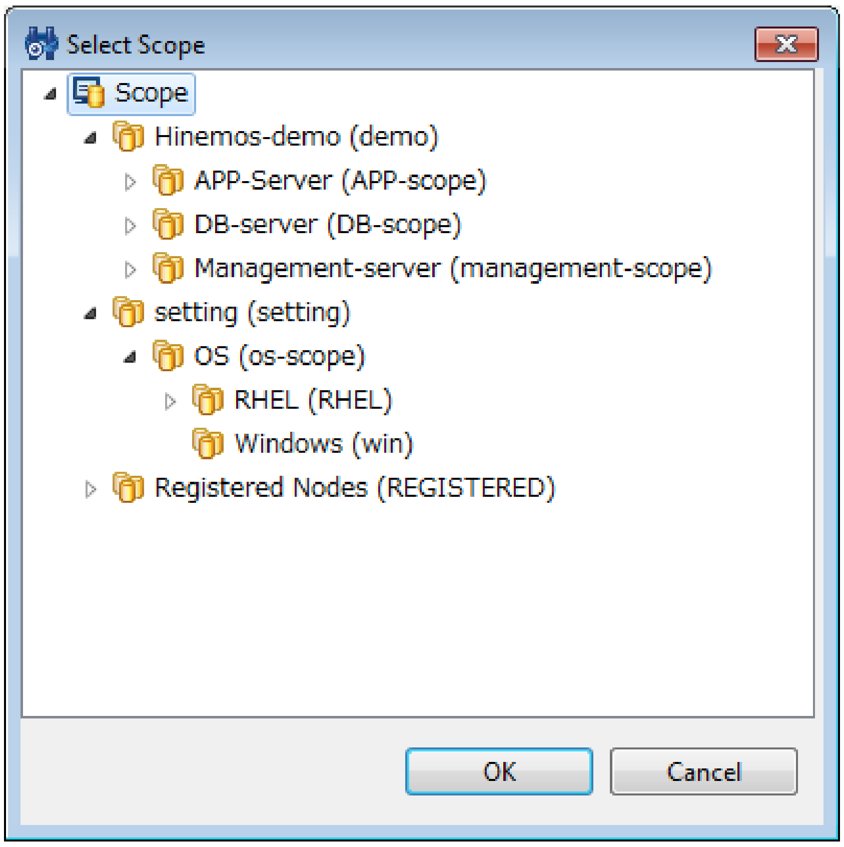


Figure 9-31 Select Scope Dialog

- Scope Process:

  Select one from the following.

  - Run all nodes

    Process will be executed concurrently in all nodes.

  - Retry nodes one by one until the end status 'Normal'

    Jobs will execute in order in the node included in the scope until one of the jobs has a normal end.

    When a job has a normal end in one of the nodes, operation will end for jobs in that scope.

    In this case, nodes that are execution targets for the job are evaluated and determined in the following order.

    1. Node where the Hinemos Agent is operating
    2. On the node with the highest "Job Priority" setting value (default is 16) out of the nodes registered with the Repository function.
    3. Node Facility ID (ascending order)

- Start Command:

  Enter a command issued to the node during job execution.

  - A wild card character cannot be used in the start command.
  - Return code of the Start command
  - Another Job execution result (return code) from the same job session can be included as a variable in the start command.

    Variable description method

    ```
    #[RETURN:jobId:facilityId]
    ```

- Stop:

  Specify the process to run at the time of the job stop process.

  - Shutdown process

    This is selected when you want to issue a system call to end a process in the job process at the time of the job stop process.

  - Stop Command:

    This is selected when you want to run a prescribed command at the time of the job stop process.

    If the stop command is selected, select the command to run at the time of the job stop process.

    - A wild card character cannot be used for the stop command.
    - Another Job execution result (return code) from the same job session can be included as a variable in the stop command.

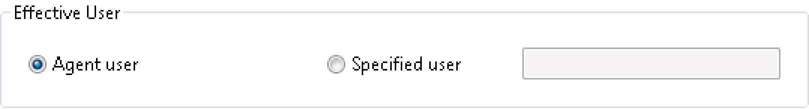
      (The method for describing the variable when another Job execution result (return code) from the same job session is included in the start command

      is the same.)

- Effective User:

  Enter the effective user of the command.

  Be careful because the environment variable of each user (those configured by the specific file of the home directory) is not reflected.



Effective User

● Agent user ○ Specified user

Figure 9-32 Effective User

  - Agent user

    The user that started the Hinemos Agent that is the destination for job execution becomes the Effective User.

  - Specify the user:

    Manually enter the Effective User.

  Refer to 'Start Command Operation'_ for important points about the Agent User and Effective User.

- Terminate when unable to connect to Hinemos Agent

  If you want to end a job when it can't connect to the Agent that is the job execution destination when the job runs, enter a check in the "Suspend" checkbox.

  If you enter a check in "Terminate when unable to connect to Hinemos Agent", set the following as well.

  - Number of retries:

    Specifies the number of times it will attempt to connect to the agent.

  - End Value

    Specifies the End Value if the job ends being unable to connect to the agent.

6. Select the "End Status" tab, and then configure the end status (Refer to Creating/Changing a JobNet for the End Status entry method.)
7. Select the "Notifications" tab, and then configure the notification (Refer to `Creating/Changing a JobNet`_ for the Notification setting method.)
8. Select the "Multiplicity" tab and specify the operation when the number of job executions on the same node exceeds the prescribed multiplicity.

   - Notify when the multiplicity of jobs reaches limit:

     When the number of job executions exceeds the multiplicity on the same node and the message "Exceeded the upper limit for simultaneous execution multiplicity." is notified in the Job[Node Details] view, enter a check and select the priority for notification.

   - Behavior when notifying when the multiplicity of jobs reaches limit:

     If the number of jobs running on the same node exceeds the prescribed multiplicity, select the behavior of new jobs attempting to run from the following.

     - Wait

       Have execution of jobs wait till the number of jobs running on the target node drops below the prescribed multiplicity.

     - End

       Abort running jobs attempting to run on the target node and end. Also, specify the end value for jobs where job execution is aborted.

9. **Click the "OK" button. The Job[Create/Change Job] dialog closes.**

   The newly created job is added to the job tree in the Job[List] view.

   Click the "Cancel" button to cancel the job creation.

   Note) The operations described above are made in the client. Information of the editing job tree is not reflected in the manager until the "Register" button is clicked and it has processed.

Changing a job

1. Select a job from the job tree in the Job[List] view.
2. Click on the "Modify" button in the Job[List] view. The Job[Create/Change Job] dialog is displayed.
3. Modify the parameter of the Job.

Copying a Job

1. From the job tree in the Job[List] view, right click on the job to be copied and then click "Copy".
2. From the job tree in the Job[List] view, right click on the copy destination and then click "Paste".
3. From the job tree in the Job[List] view, select the Job that was copied.
4. Click on the "Modify" button in the Job[List] view. The Job[Create/Change Job] dialog is displayed.
5. Change the temporarily defined Job ID (Copy_Of_xxx) as necessary.

9.4.5 Items to Consider when Creating/Changing a Job

Controlling a Job

You can control the execution of a JobNet with the following settings. Refer to Creating/Changing a JobNet for the setting method.

- Configure a calendar
- Suspend the execution status of a job in advance
- Skip the execution status of a job in advance

Delay of Start Monitoring

Check if the start of job execution has been delayed. If it is delayed, you can configure the control (Refer to Creating/Changing a JobNet for the setting method.)

End Delay monitoring

Check if the end of a job has been delayed. If it is delayed, you can configure the control. (Refer to Creating/Changing a JobNet for the setting method.)

Multiplicity of Running Jobs

The number of jobs running simultaneously on the same node can be controlled. The number of jobs that can run on the same node (multiplicity of running jobs) is specified for each node in the Repository[Node View].

By default, the value for "Job Multiplicity" is 16. (Refer to 'Changing Node Information'_ for the process to change the node information.)

Action when Registering a Job

Job (job unit, JobNet) creation and modification are performed with an editing operation on the client. Information of the editing job tree is not reflected in the manager until the "Register" button is clicked on and processed. By creating a "Registration", the edited JobUnit (and JobNets subordinate to the JobUnit, Jobs, File Transfer Jobs and Refer Jobs) information is reflected as a batch in the Manager.

To register a job, click on the "Register" button in the Job[List] view.

- To clear the modified contents on the client

  click the "Cancel" button. The modified information is canceled, and the job tree registered in the manager will return.

  Similarly, if you click the "Edit" button when the "Registration" is not created, Edit Mode is released and the job tree can return to the state prior to editing.

Wait Rules for Copy Operation Time

If a job is copied, the same job's Wait Rules will be partially deleted unless the Wait Rule is controlled by "time". This is differnt from copying a JobNet. For informations about copying a JobNet, please refer to Items to Consider when Creating/Changing a JobNet .

- If the Wait Rule is "Time",

  all of the Wait Rules are copied.
- If the Wait Rule is "End Value" or "End Status",

  all of the Wait Rules are deleted.

9.5 Deleting a Job

- To delete a Job, the JobUnit to which the JobNet you want to delete belongs must be in Edit Mode.

1. Select the job to be deleted (File Transfer Job, Refer Job, JobNet, JobUnit) from the job tree in the Job[List] view.
2. Click the "Delete" button in the Job[List] view.

When a JobNet (job unit) is deleted, jobs, file transfer jobs and JobNets included in the deleted job net (job unit) are also deleted.

When a job subject to delete is specified as the wait rule in the other job, review the wait rule because the configuration will remain.

- Important point The job setting content has a job session ID assigned and a copy saved at the job run start time, so even if you change the setting content, the changed content won’t be applied to jobs that are already started because a job is run based on that information.

9.6 Executing/Starting/Stopping a job

9.6.1 Job Status/Operation

According to the current execution status, the status of job unit, JobNet, and job is classified into two types: "Status during session execution", and "Status when session stopped".

- [Status during session execution]

  Waiting: Status when the job unit has started and the session information is created

  Running: Status when the command execution is notified to the agent

  Suspended: Status when the command execution is pending

  Skip: Status when the command execution is skipped

  Pause: Status when the command execution is paused

  Stopping: Status when the stop command is executed, until the end notification is returned from the agent

  Command Stop: Status when the stop command is executed, and the end notification is returned from the agent

- [Status when session is stopped]

  End: Status when the end notification of command execution is returned.

  Changed: Status when the end value is set at the Stop[Change End Value].

Status changing operations executed for the JobNet/job in the Job[Job Detail] view and the node in the Job[Node Detail] view are listed below.

Table 9-9 Operations Executed on the JobNet, Job and Node

Operation	JobNet	Job	Node	Description
Stop[Suspend]	○	○	・	Change from [Stop] status to [Suspend] status.
Start[Cancel Suspend]	○	○	・	Cancel [Suspend] status.
Stop[Skip]	○	○	・	Change from [Stop] status to [Skip] status.
Start[Cancel Skip]	○	○	・	Cancel [Skip] status.
Stop[Pause]	○	○	・	Change from [Running] status to [Pause] status.
Start[Cancel Pause]	○	○	・	Cancel [Pause] status.
Stop[Command]	○	○	○	Run the stop command.
Start[Start]	○	○	○	Immediately start a job per JobNet/job/node.
Stop[Change End Value]	○	○	○	Change the end value of the startup failure.
Stop[Force]	○	○	○	Kill when the status does not change.

Copyright (c) 2013 NTT DATA CORPORATION

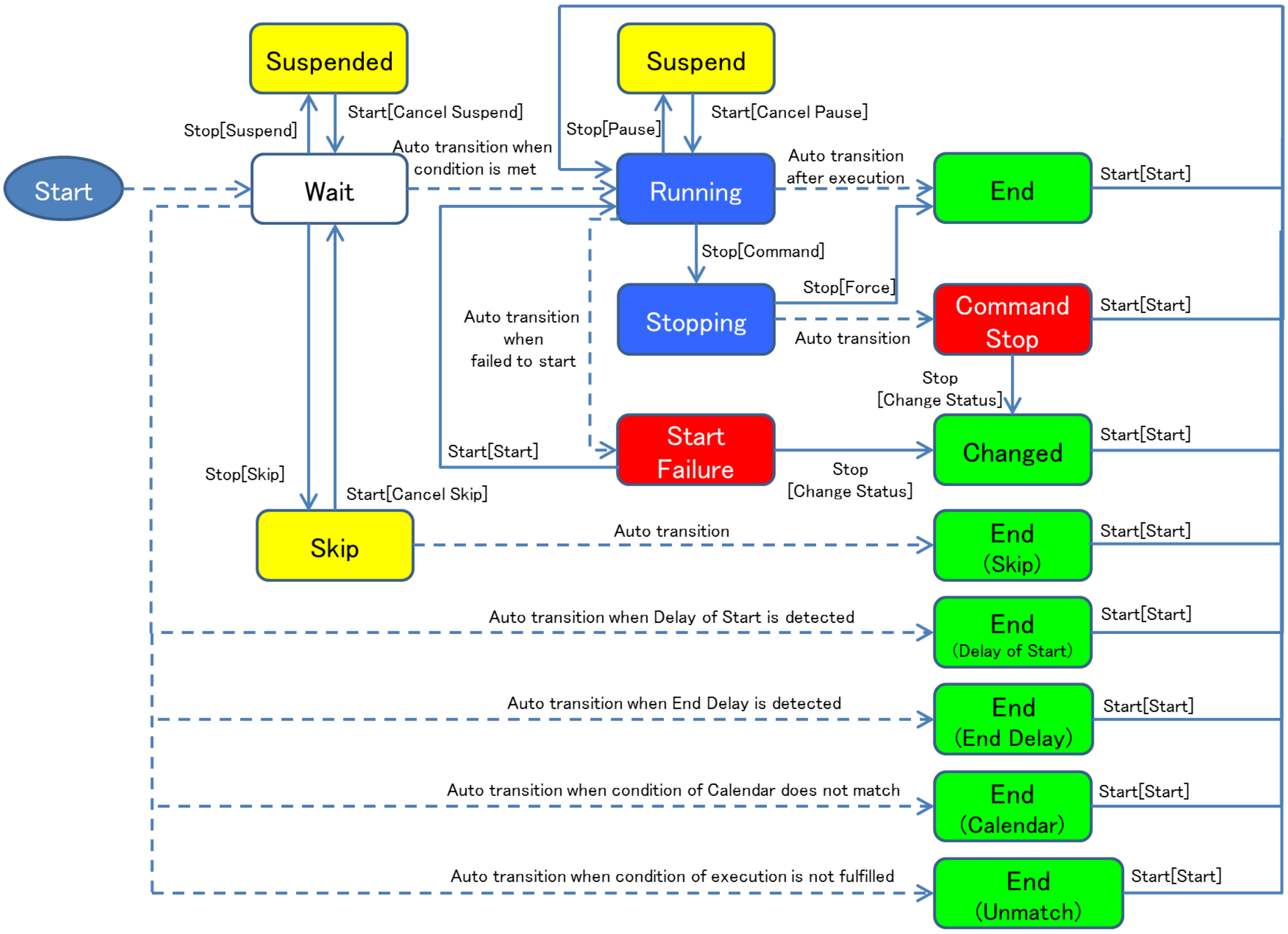


Figure 9-33 Status Transition Diagram

9.6.2 Running a Job

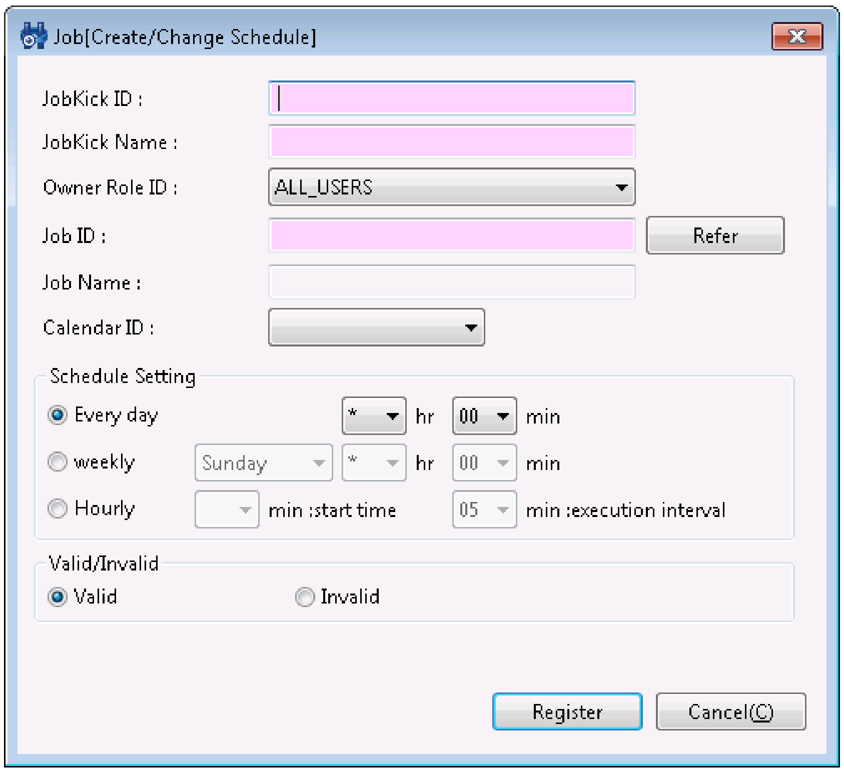
Select the job to run from the job tree in the Job[List] view or from the table of job lists. Click the "Run" button.

Note) The job will not be run when "Run" is operated before the "Register" operation. Information about the editing job tree is registered in the manager when the registration process is complete. You can run a job once it is register ed in the manager.

9.6.3 Running a Job Schedule

Set (Scheduling) the currently registered Job (JobNet, JobUnit) to run at a prescribed time. The scheduled job will b e run on the configured date and time (when the calendar is applied to the Schedule Setting, the scheduled job will r un only when the job session start time is within the range of the configured operating period of the specified cale ndar).

1. Click the "Create Schedule" button in the Job[JobKick] view. The Job[Create/Change Schedule] dialog is displayed.



Job[Create/Change Schedule]

JobKick ID :

JobKick Name :

Owner Role ID : ALL_USERS

Job ID : Refer

Job Name :

Calendar ID :

Schedule Setting

● Every day * hr 00 min

○ weekly Sunday * hr 00 min

○ Hourly min :start time 05 min :execution interval

Valid/Invalid

● Valid ○ Invalid

Register Cancel(C)

Figure 9-34 Job[Create/Change Schedule] Dialog

2. Enter the JobKick ID and the JobKick Name. Always be sure to enter both the "JobKick ID" and the "JobKick Name", since both are mandatory fields. The "JobKick ID" must be unique on the system.
3. Configure the Job ID (or JobNet or JobUnit) for the schedule run target job. Always be sure to enter the Job ID, since it is a mandatory field. Click the "Refer" button located on the side of the "Job ID:". The Select Job dialog is displayed.

Select the schedule run target job from the job tree, and then click on the "OK" button.

Job ID and Job Name are configured.

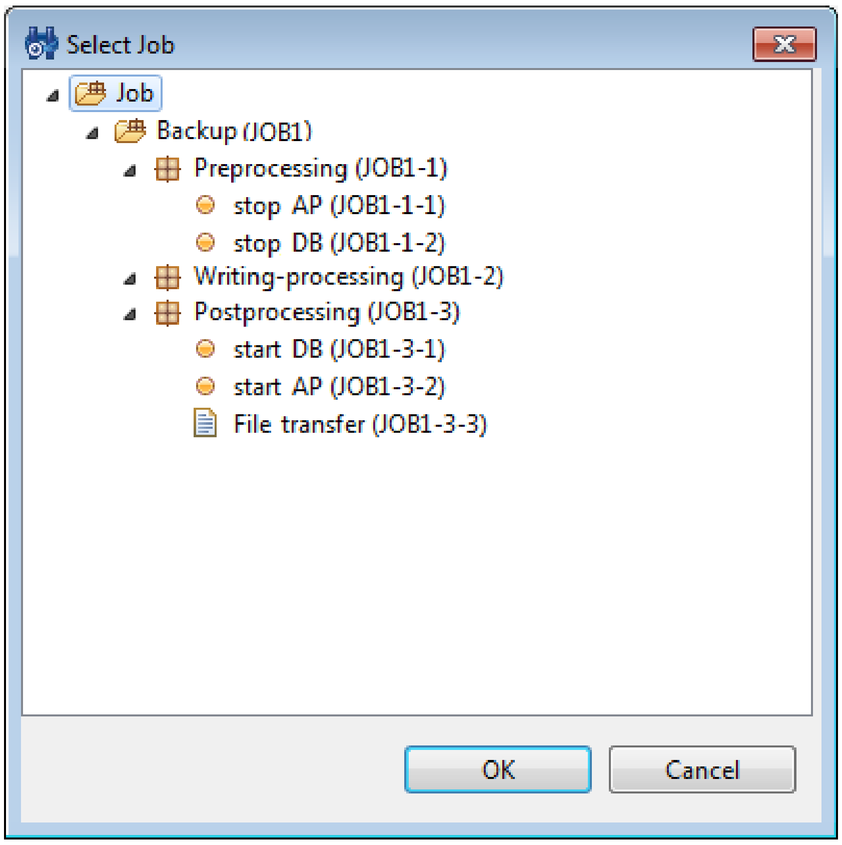


Figure 9-35 Select Job Dialog

4. Configure the calendar. Select the calendar ID for the calendar you want to set up. (Refer to the section, `Cale ndar Feature`_ for more details on the calendar).
5. Configure the schedule. Schedule setting can be configured with the following three methods.

- Every day

  Configure so that the job is executed every day at the specified time. Select the "Hour", and "minute(s)" from the combo boxes.

  If there is an * (asterisk) for the "Hour", and a specific time is set for "Minutes", then the job run is scheduled

  every day at the specified time.

- Weekdays

  Schedule job execution by specified day of the week. Select "Weekday", "Hour", and "minute(s)" from each comb o box.

  If there is an * (asterisk) for the "Hour", and a specific time is set for "Minutes", then the job run is scheduled

  every hour at the prescribed time (Minutes) on the set day of the week.

- Hourly

  Job execution is scheduled to repeat hourly at the prescribed minutes. Select the "min :start time" and "min :e xecution interval" values from each combo box. Set the minutes to start running each hour from the "min :star t time" combo box to schedule running of repeat jobs. Set the minutes for the execution interval from the "min :execution interval" combo box to schedule running of repeat jobs.

6. Configure whether to enable the configured schedule. Select the "Valid" or "Invalid" radio button. When "Invalid" is selected, the schedule configuration is saved, but the schedule run target job is not executed.
7. Click the "Register" button. The Job[Create/Change Schedule] dialog is closed. The Successful dialog is displaye d.
8. Click the "OK" button. The created schedule is added to the schedule list table in the Job[JobKick] view.

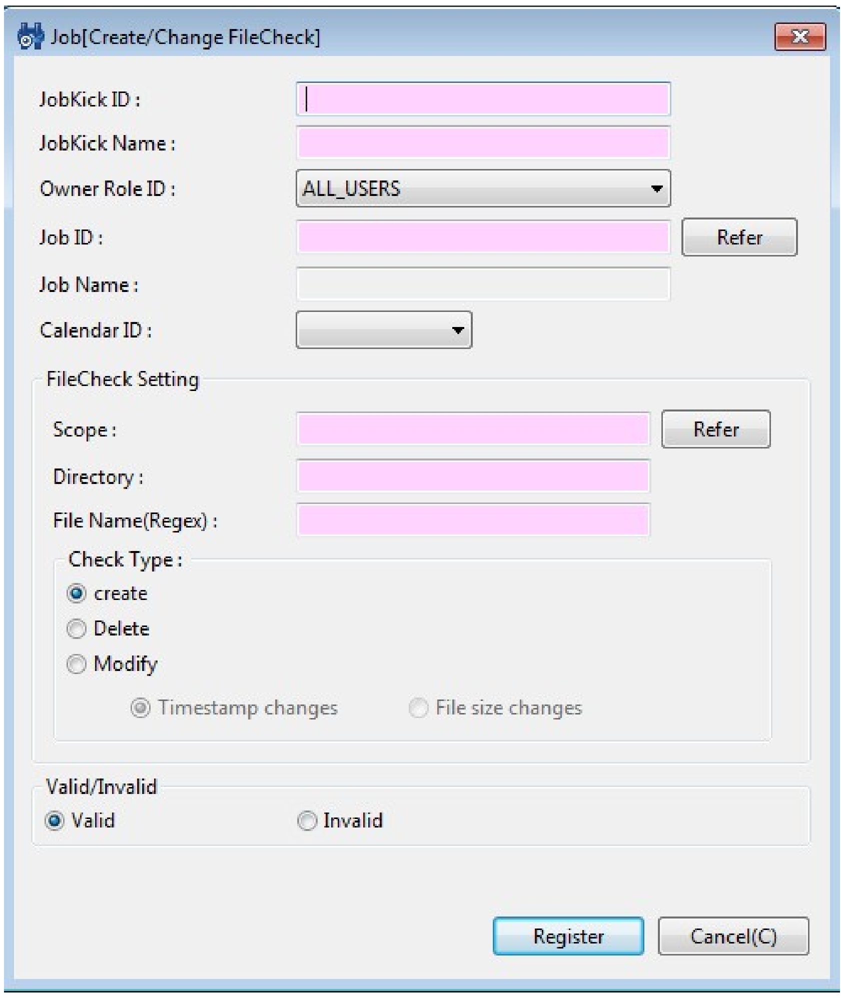
   Note) The system date of the Hinemos Manager Server OS becomes the standard for schedule execution.

Copyright (c) 2013 NTT DATA CORPORATION

9.6.4 Run FileCheck for the Job

Set the currently registered Job (JobNet, JobUnit) to run at the FileCheck opportunity. The job set as a FileCheck execution Trigger runs when there is an opportunity to check, delete or change the check target file.

1. Click the "Create Schedule" button in the Job[JobKick] view. The Job[Create/Change Schedule] dialog is displayed.



Owner Role ID : ALL_USERS

Check Type : ● create

● Timestamp changes

● Valid

Figure 9-36 Job[Create/Change FileCheck] Dialog

2. Enter the JobKick ID and the JobKick Name. Always be sure to enter both the "JobKick ID" and the "JobKick Name", since both are mandatory fields.

   The "JobKick ID" must be unique on the system.

3. The job that is run at the FileCheck (check the creating, deleting and editing of the check target file) opportunity,

   (or the JobNet or JobUnit) has its Job ID set.

   Always be sure to enter the Job ID, since it is a mandatory field.

   Click the "Refer" button located on the side of the "Job ID:". The Select Job dialog is displayed.

Copyright (c) 2013 NTT DATA CORPORATION

Select the Job to run at the FileCheck opportunity from the job tree, and then click the "OK" button.
Job ID and Job Name are configured.

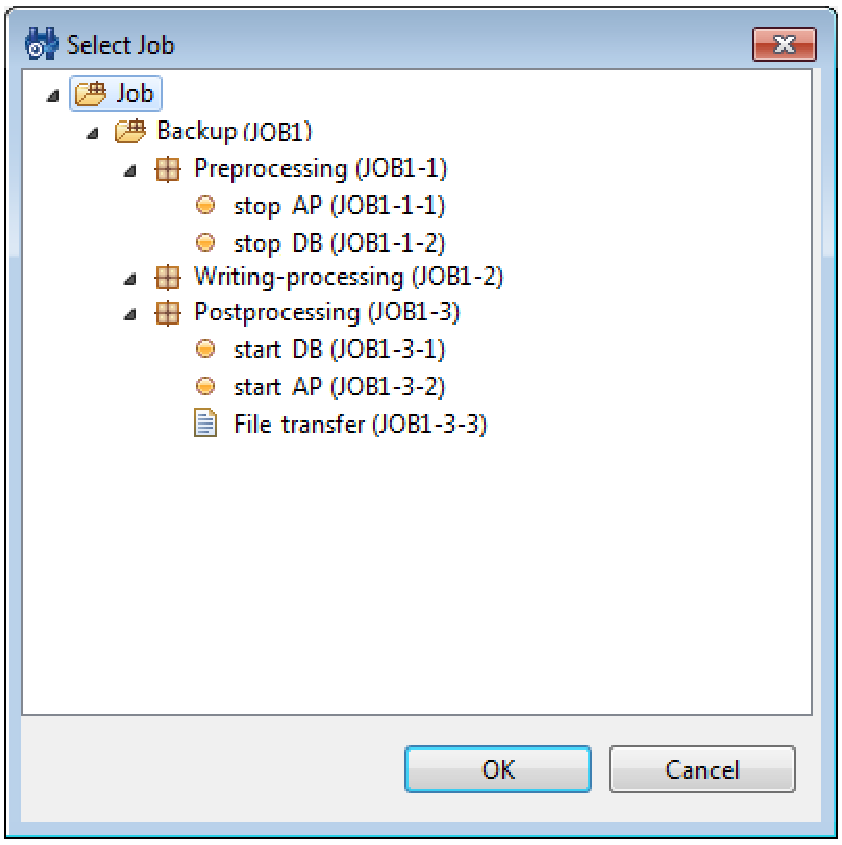


Figure 9-37 Select Job Dialog

4. Configure the calendar. Select the calendar ID for the calendar you want to set up. (Refer to the section, `Cale ndar Feature`_ for more details on the calendar).
5. Configure the FileCheck Setting.

- Scope:

  Configure the run target scope for FileCheck. Run FileCheck for all nodes included in the specified scope.

  Click the "Refer" button located on the side of the "Scope". The "Select Scope" dialog is displayed. Select the target scope for FileCheck from the scope tree, and then click the "OK" button.

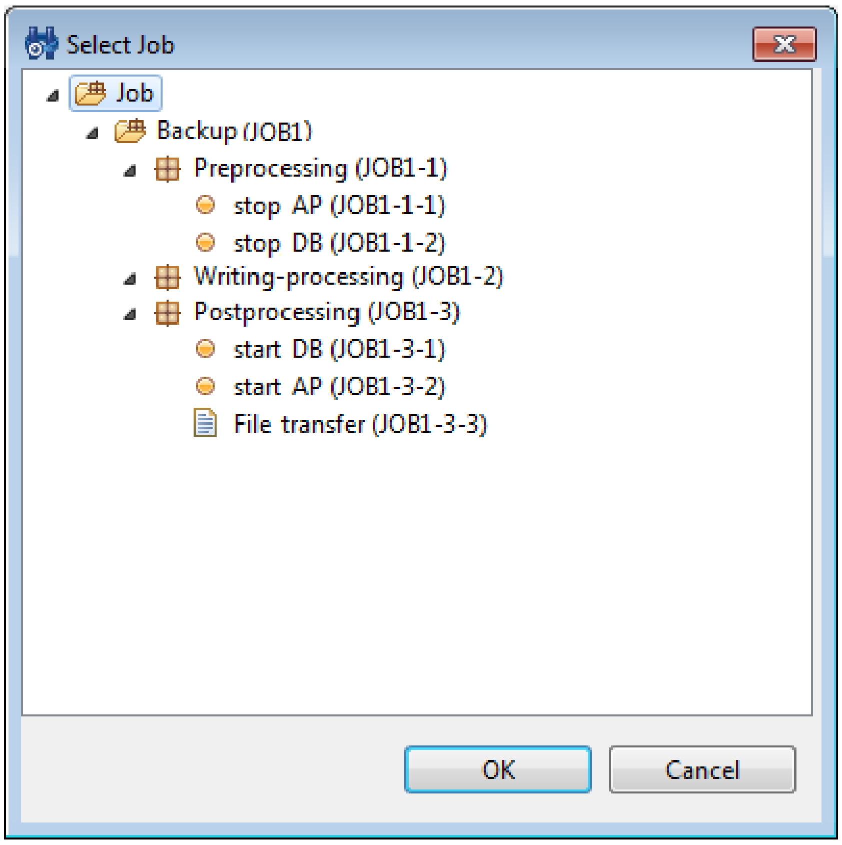


Figure 9-38 Select Scope Dialog

- Directory

  Configure the run target directory for FileCheck.

- File Name:

  Configure the run target File Name for FileCheck.

  Regex can be used for the File Name. (Refer to http://docs.oracle.com/javase/jp/6/api/java/util/regex/Pattern.html regarding Regex)

- Check Type:

  Select the FileCheck type. Create, Modify and Delete can be selected as the FileCheck type.

  - Create

    Checks whether the check target file is created.

  - Delete(D)

    Checks whether the check target file is deleted.

  - Modify(M)

    Checks whether the check target file is changed. Select the method to check whether it has changed from the following.

    - Timestamp changes
    - File size changes

6. Configure whether to enable the configured FileCheck settings. Select the "Valid" or "Invalid" radio button. When "Invalid" is selected, the FileCheck Setting will be saved, but the FileCheck will not be run.
7. Click the "Register" button. The Job[Create/Change FileCheck] dialog closes. The Successful dialog is displayed.
8. Click the "OK" button. The created schedule is added to the schedule list table in the Job[Schedule] view.

Copyright (c) 2013 NTT DATA CORPORATION

FileCheck Run Interval

The default FileCheck Run Interval is 10 seconds.

To change the FileCheck Run Interval, in the Hinemos Agent setting file, change the following parameter.

- /opt/hinemos_agent/conf/Agent.properties

```
## sleep after file check (msec)
filecheck.run.interval=10000
```

Trigger Assignment Frequency by FileCheck

- Check Type: "Modify(M)" operation

  The job will run at the FileCheck opportunity with the latest update as long as updates continue to be detected at each FileCheck opportunity.

  Example) If the FileCheck interval is 10 seconds and a file update is detected as follows

  - Update → Update → Update → Update → No Update

    In this case, the job will run at the timing of Update → No Update.

- Check Type: "Create" operation

  There is a check whether a file is created at each FileCheck opportunity, and when it detects that a file is created,

  the job will run at the FileCheck opportunity.

  Example) If the FileCheck interval is 10 seconds and file creation and file update is detected as follows

  - No File → File → Update → Update → No Update

    In this case, the job will run at the timing of No File → File.

9.6.5 Operational Differences by the Method of Job Execution

"Wait Rule", "Control", "End Delay", and "End Status" configurations are enabled when they are executed from the above JobNet or the job unit.

Operations are described using the structure below.

```
JobUnit1
    - JobNet1
        - Job1
        - Job2 (wait condition = time 12:00).
        - Job3 (wait condition = time 18:00).
```

When "JobUnit1" or "JobNet1" is executed by clicking the "Run" button or because of a scheduled run, the wait rule identified in "Job2" and "Job3" is enabled, and the corresponding job is executed when the specified time has passed.

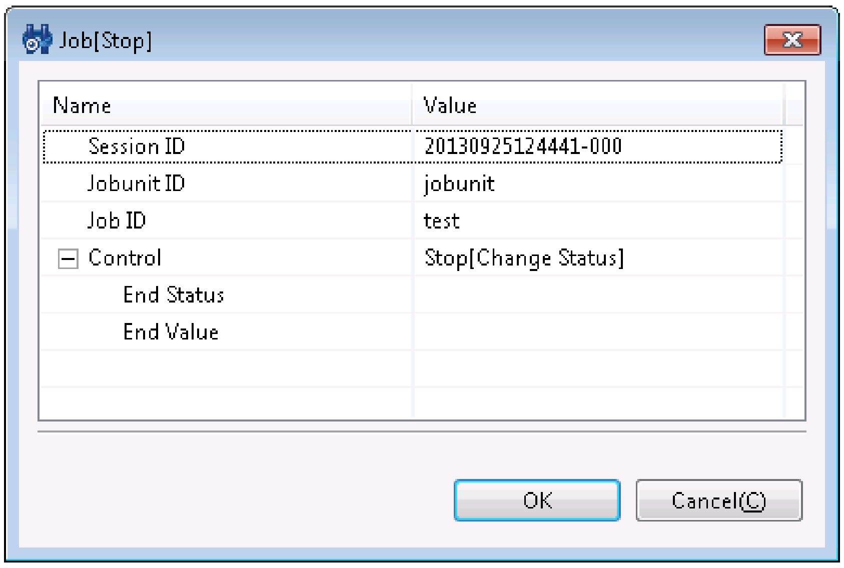
However, if "Job2" or "Job3" is selected and executed, the wait rule is disabled, and the corresponding job is executed immediately.

9.6.6 Stopping a Job

The running job (JobNet, job unit) can be stopped. When a job is stopped, you can rerun the stopped job.

1. Select the job to be stopped from the list of job execution histories in the Job[History] view.

2. Click on the "Stop" button in the Job[History] view. Job[Stop] dialog opens.



Job[Stop]

Name	Value
Session ID	20130925124441-000
Jobunit ID	jobunit
Job ID	test
⊟ Control	Stop[Change Status]
End Status	
End Value	

Figure 9-39 Job[Stop] Dialog

3. Select "Stop[Command]" in the "Control" field.
4. Click the "OK" button. The Job[Stop] dialog closes. The configured stop command is executed, and the job is stopped immediately.

   Note) If a Stop[Command] is run for a JobNet, the Stop[Command] specified in the Job[Create/Change Job] "Command" tab is run for the subordinate running job or JobNet.

   Click the "Cancel" button to cancel the job stoppage.

9.6.7 Pausing a JobNet

Running JobNets (job unit) can be paused. When a JobNet (job unit) is paused, you can rerun it or cancel the pause.

Pausing a JobNet

1. Select the JobNet to be paused from the list of job execution histories in the Job[History] view.
2. Click on the "Stop" button in the Job[History] view. Job[Stop] dialog opens.
3. Select "Stop[Pause]" in the "Control" field.
4. Click the "OK" button. The Job[Stop] dialog closes. Wait for the job included in the currently running JobNet to end, and then the JobNet will be paused.

Click the "Cancel" button to cancel the JobNet pause.

Pausing a JobNet at a job detail level

Select the JobNet to be pause from the list of job execution histories in the Job[Job Detail] view. Click on the "Pause" button. The procedure hereafter is similar to the procedure to pause the JobNet.

9.6.8 Resuming JobNet

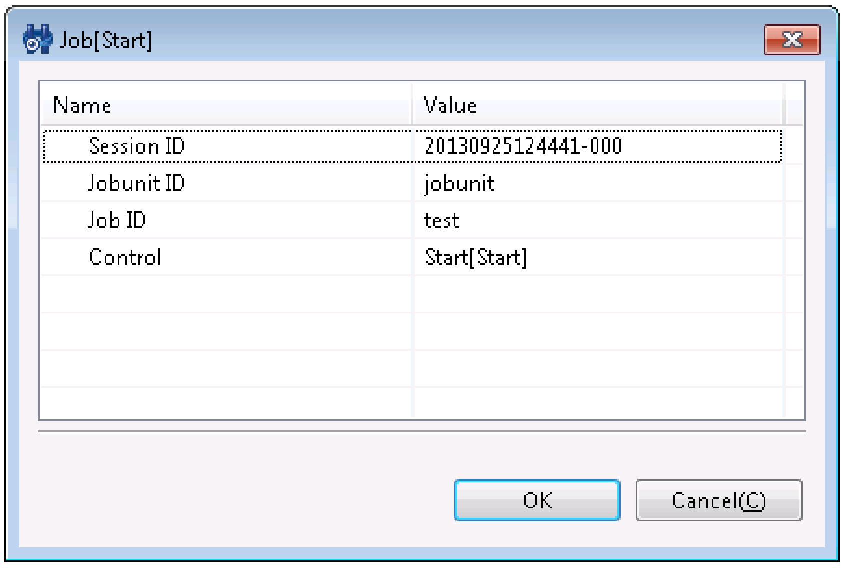
Paused JobNets (job units) can be resumed.

Resuming JobNets

1. Select the paused JobNet to be resumed from the list of job execution histories in the Job[History] view.

Copyright (c) 2013 NTT DATA CORPORATION

2. Click the "Start" button in the Job[History] view. The Job[Start] dialog opens.



Job[Start]

Name	Value
Session ID	20130925124441-000
Jobunit ID	jobunit
Job ID	test
Control	Start[Start]

Figure 9-40 Job[Stop] Dialog

3. Select Start[Cancel Pause] in Control.
4. Click the "OK" button. The Job [Start] dialog closes. Wait for the job included in the currently paused JobNets to end, and then the JobNet will be rerun.

Resuming a job in a detailed level

Select the paused JobNet to be resumed from the list of job execution histories in the Job[Job Detail] view. Click the "Start" button. The following process, is the same as the procedure to restart the JobNet.

9.7 List of Job Execution History

Job history is displayed in the following three views by changing the display level.

- Job[History] view

  Manually executed jobs, scheduled executions, and interlocking monitoring executions are displayed in the Job[History] view.

- Job[Job Detail] view

  Details of a job selected in the Job[History] view are displayed in the Job[Job Detail] view. The Job unit, JobNet, and Job that comprise the job are displayed at the element level. You can confirm to which job the process has progressed.

- Job[Node Detail] view

  The node level status of a job selected in the job execution history list of the Job[History] view is displayed.

To determine the trigger of a job

The "Trigger Type" and "Trigger Info" in the Job[History] view is displayed in the following format.

- When Job is triggered by Schedule

  Trigger Type: Schedule

  Trigger Info: JobKick Name (JobKick ID)

- When Job is triggerd by Filecheck

  Trigger Type: Filecheck

  Trigger Info: JobKick Name (JobKick ID)

- When Job is triggered by Monitoring Result (Job Notification)

  Trigger Type: Monitor

  Trigger Info: Monitor ID (Plugin ID)

- When Job is triggered manually

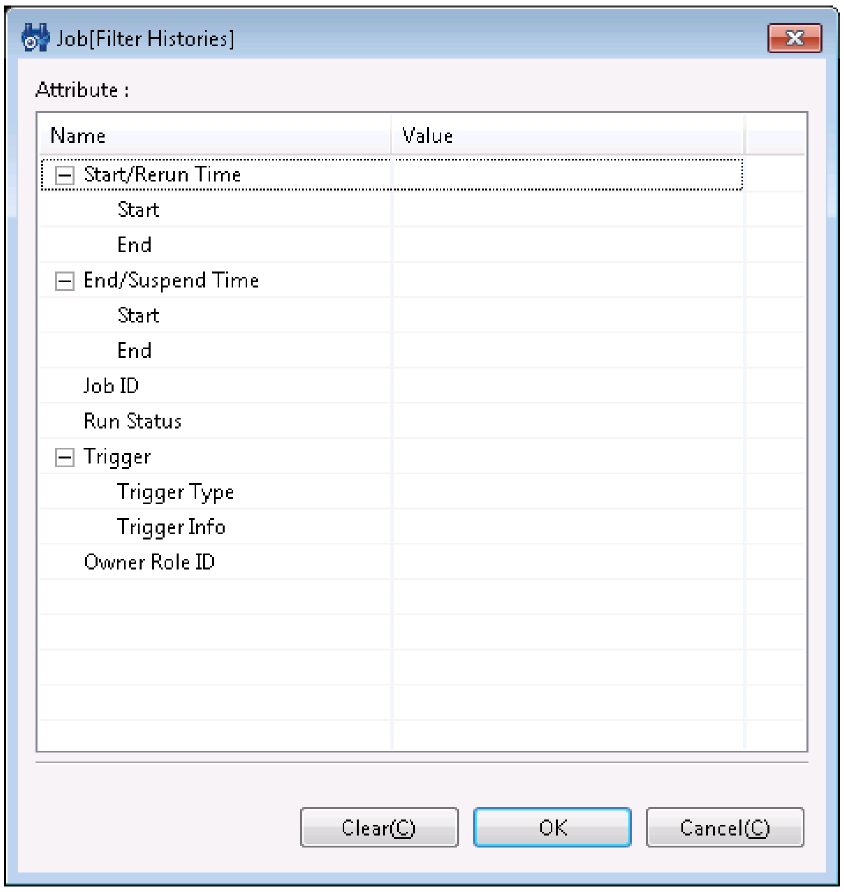
  Trigger Type: Manual

  Trigger Info: Manual Hinemos User Name

To refine the displaying job histories

Click the "Filter" button in the Job[History] view. The Job[Filter Histories] dialog is displayed. Configure the refiner.

Leave blank for items not used as the refiner.



Job[Filter Histories]

Attribute :

Name	Value
⊟ Start/Rerun Time	
Start	
End	
⊟ End/Suspend Time	
Start	
End	
Job ID	
Run Status	
⊟ Trigger	
Trigger Type	
Trigger Info	
Owner Role ID	

Figure 9-41 Job[Filter Histories]

** To confirm the standard output and standard error output of the job execution results**

In the Job[Node Detail] view, the standard output and standard error output of the job execution results are displayed.

9.8 Job Plan List View

The schedule for planned executions is displayed in the Job[Plan] view.

By default, the most recent 100 Job execution plans are displayed. Refer to 'Job Screen Change Cycle - Changing the History Display Limits' for the method for changing the Job execution plan count that is displayed.

9.8.1 Plan Filter

By using the "Filter" button, you can display only the plans that meet a condition.

1. Click the "Filter" button in the Job[Plan] view. The Job[Filter Schedule Plan] dialog is displayed.

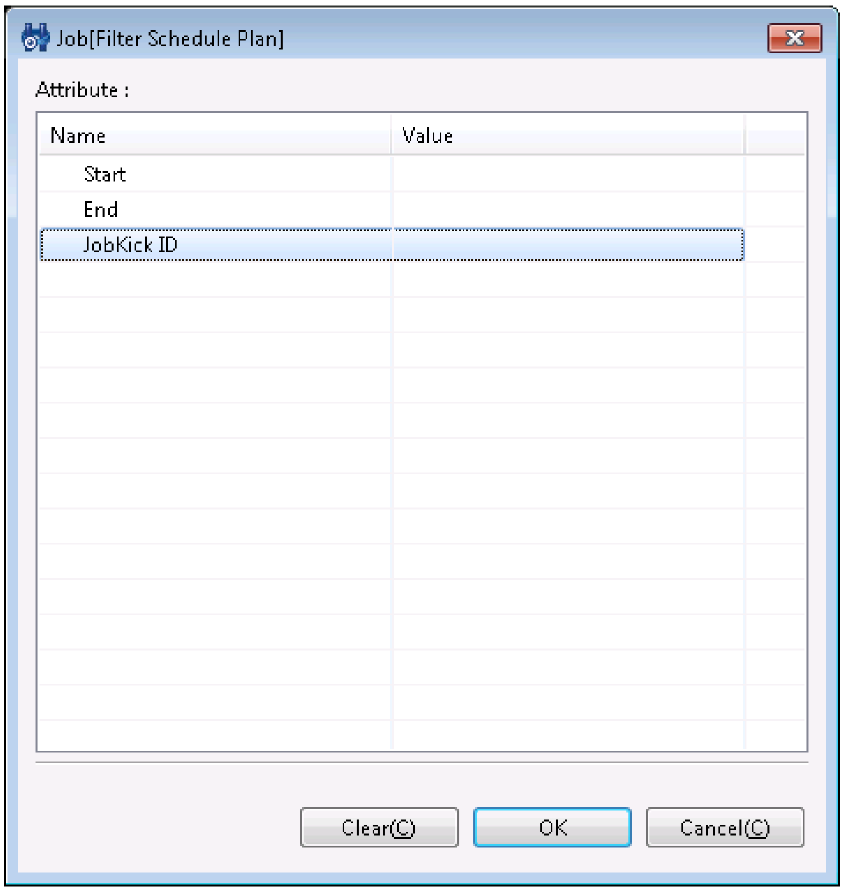


Figure 9-42 Job[Filter Schedule Plan]

2. Configure the filter condition. Leave the field blank when an item is not included in the conditions. (Please click on the "Clear" button to change the filtering conditions back to the default conditions).

   - Start, End Make "Time" a filtering condition. Future plans can be displayed by specifying a time in the future. Also, you can display past plans by specifying a past time. The Time dialog can be opened by clicking the button next to the input field. Please select the time in the dialog. Select the date and time from the combo box.
   - Include, Exclude Make JobKick ID a filtering condition. Multiple JobKick IDs can be used as conditions by delimiting them with commas.

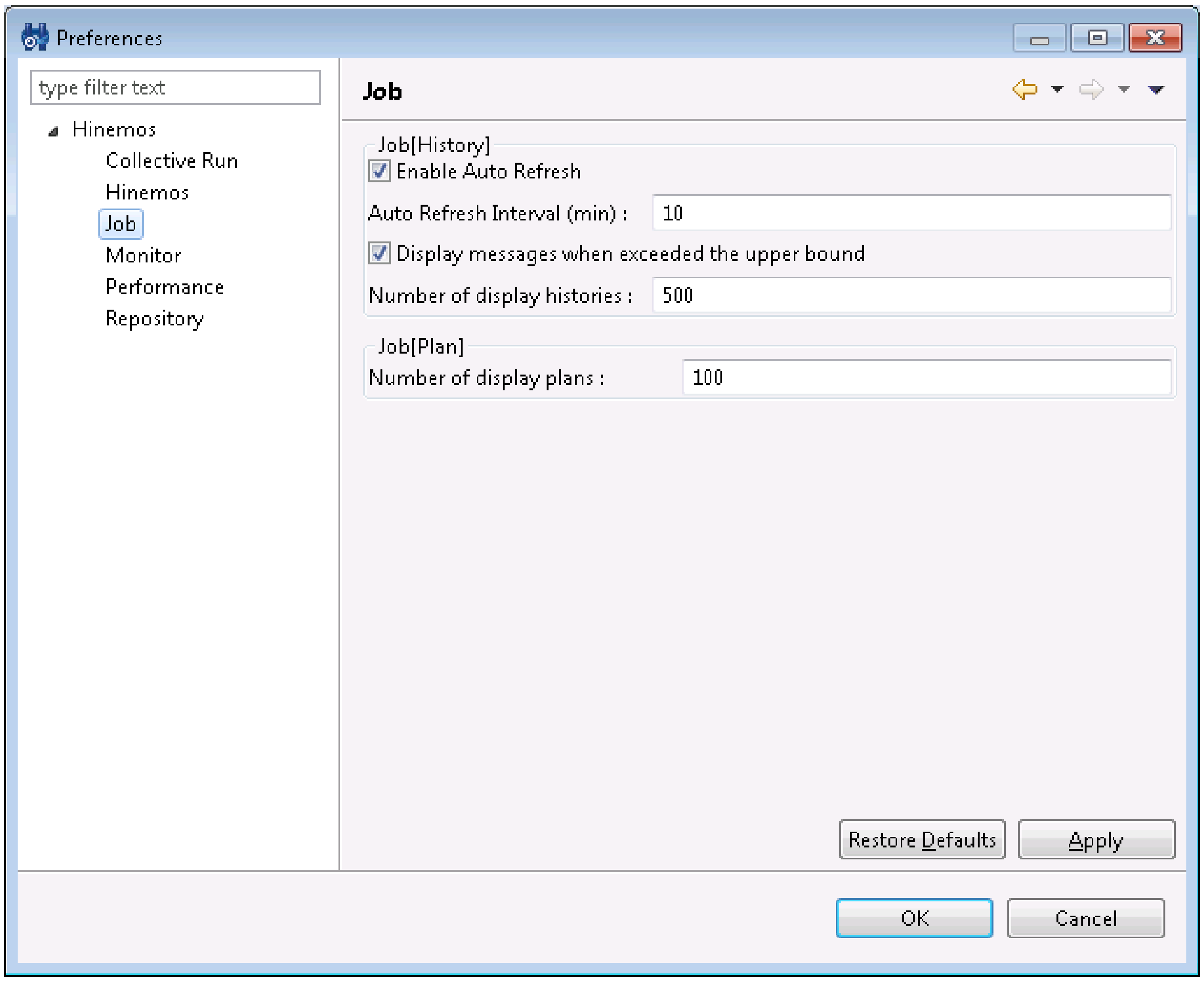
3. Click the "OK" button. The Job[Filter Schedule Plan] dialog closes and only the plans that meet the specified conditions are displayed in the Job[Plan] view.
4. The filter process can be released by once again clicking on the "Filter" button in the Job[Plan] view.

9.9 Changing the Job Screen Update Interval and History Display Control

The screen information is updated regularly by obtaining manager information from the client at regular intervals. The restriction on the displayed update interval and the history can be changed by the following procedures.

Copyright (c) 2013 NTT DATA CORPORATION

1. Select [Client Setup] - [Setup] from the menu bar. The Preferences dialog is displayed.



Job[History]
☑ Enable Auto Refresh
Auto Refresh Interval (min) : 10
☑ Display messages when exceeded the upper bound
Number of display histories : 500

Job[Plan]
Number of display plans : 100

Figure 9-43 Preferences Dialog

2. Select Hinemos - Job Management in the tree pane on the left side.
3. The following configurations can be made for the Job[History] view.

- Enable Auto Refresh:

  The contents of the view will be updated at the specified auto refresh interval when this check box is checked. If unchecked, the contents will not be updated unless the "Update" button is clicked.

- Auto Refresh Interval (min):

  If auto refresh is enabled, specify the update interval in minutes (from 1 to 32767 can be set).

- Display messages when the upper bound is exceeded:

  Output message if this check box is checked and if the accumulated number of events exceeds the specified nu mber of displayed events. If unchecked, message is not output even if the history count exceeds the display hi story count.

- Number of display histories:

  Specify the history cases to display at one time (from 1 to 32767 can be set).

4. The following configurations can be made for the Job[Plan] view.

- Number of display plans

  Specify the number of Job plans that are displayed at one time. (Can be specified from 1 to 32767).

Copyright (c) 2013 NTT DATA CORPORATION

9.10 Refer Job

A Refer Job is a job that can be set with the form where it refers to another job (or File Transfer Job) with completed definitions in the same JobUnit.

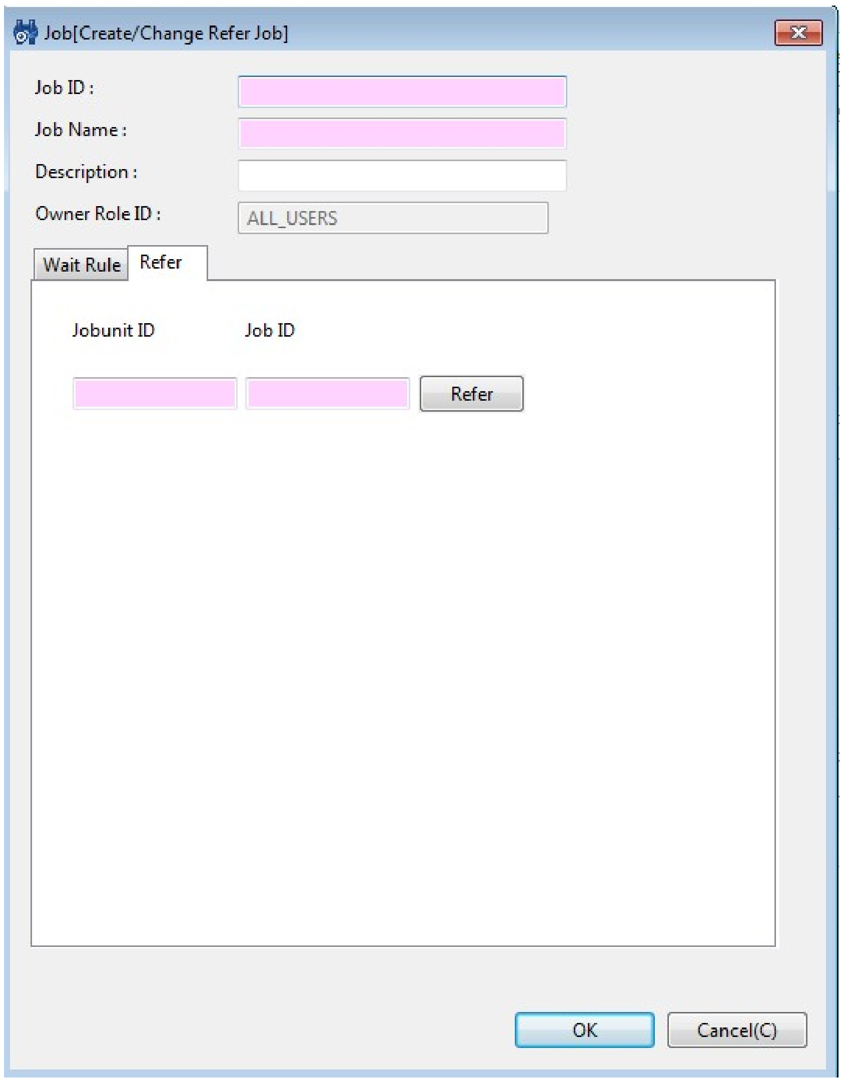
A Refer Job can only be defined as a Wait Rule or refer job, and you can register it and run it based on the setting information (setting information set in the various Control, Command, Delay of Start, End Delay, Multiplicity, End Status and Notifications tabs) for the refer destination job. for the refer destination job.

Configuration procedures for the Wait Rule settings are the same as the procedures for creating a Job.

Create Refer Job

To create a Refer Job, the JobUnit that is the destination for creating the Refer Job must be in Edit Mode.

1. From the job tree in the Job[List] view, select the new Refer Job to be added to a JobNet (or JobUnit).
2. Click the "Create Refer Job" button in the Job[List] view. The Job[Create/Change Refer Job] dialog is displayed.
3. Configure Job ID, Job Name, and Description. Always be sure to enter the "Job ID" and "Job Name", since both are mandatory fields. The "Job ID" of the Refer Job must be unique within that job unit.
4. Select the "Wait Rule" tab, and then configure the Wait Rule (Refer to Creating/Changing a JobNet for the Wait Rule entry method.)
5. Configure the refer settings. Select the "Refer" tab.



Job[Create/Change Refer Job]

Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

Figure 9-44 Job[Create/Change Refer Job] Dialog (Refer Tab)

6. Configure the job to refer. Click on the "Refer" button and the Select Job dialog is displayed. Select the job to refer from the scope tree, and then click the "OK" button.
7. **Click the "OK" button. The Job[Create/Change Refer Job] dialog closes.**

   The newly created job is added to the job tree in the Job[List] view.

Copyright (c) 2013 NTT DATA CORPORATION

9.11 File Transfer Job

The File Transfer Job is for transferring files. The specified command is run when a normal job is run, but file trans fer is run for the specified scope (or node) for file transfer jobs.

You can transfer to multiple nodes from a single node.

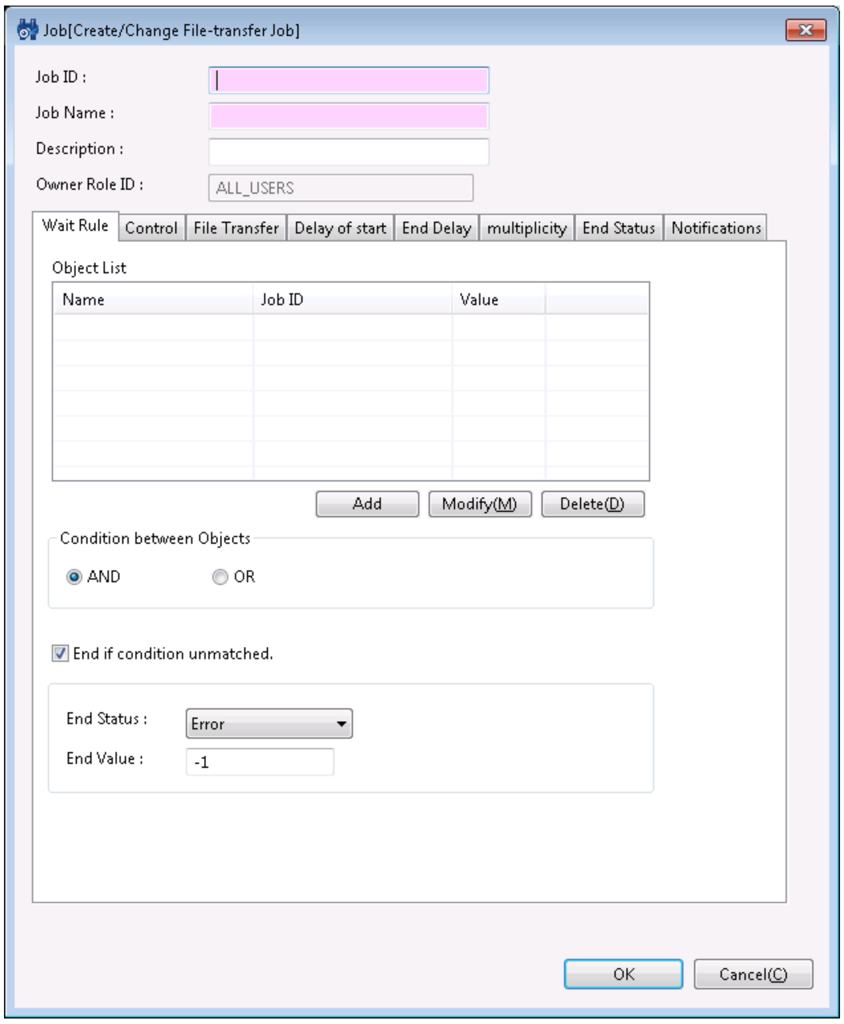
The configuration procedures for the End Status and Wait Rules are similar to the procedures for creating a Job.

Note) ssh setup is required to execute the File Transfer Job. When using the Collective Run feature to perform a se tup, and `Collective Run Feature`_ is set up manually, refer to Chapter 6, Collective Run in the Administrator's Guide.

Creating File Transfer Job

To create a File Transfer Job, the JobUnit that is the destination for creating the Refer Job must be in Edit Mode.

1. From the job tree in the Job[List] view, select the new File Transfer Job to add to a JobNet (or JobUnit).
2. Click on the "Create File-transfer Job" button in the Job[List] view. The Job[Create/Change File-transfer Job] dialog is displayed.
3. Configure "Job ID", "Job Name", and "Description". Always be sure to enter the "Job ID" and "Job Name", since b oth are mandatory fields. "Job ID" of the file transferring job must be unique within the same job unit.
4. Select the "Wait Rule" tab, and then configure the wait rule (Refer to Creating/Changing a JobNet for the Wait Rule entry method.)
5. Configure "File Transfer". Select the "File Transfer" tab.



Job ID :

Job Name :

Description :

Owner Role ID : ALL_USERS

Object List

Name	Job ID	Value

Condition between Objects

● AND ○ OR

☑ End if condition unmatched.

End Status : Error

End Value : -1

Figure 9-45 Job[Create/Change File-transfer Job] Dialog (File Transfer Tab)

6. Configure the source. Enter the following settings.

- Scope:

  Click the "Refer" button and the Select Scope dialog is displayed; Select the source node, and then click the "Register" button (you cannot select "Scope", which is the root node of the job tree).

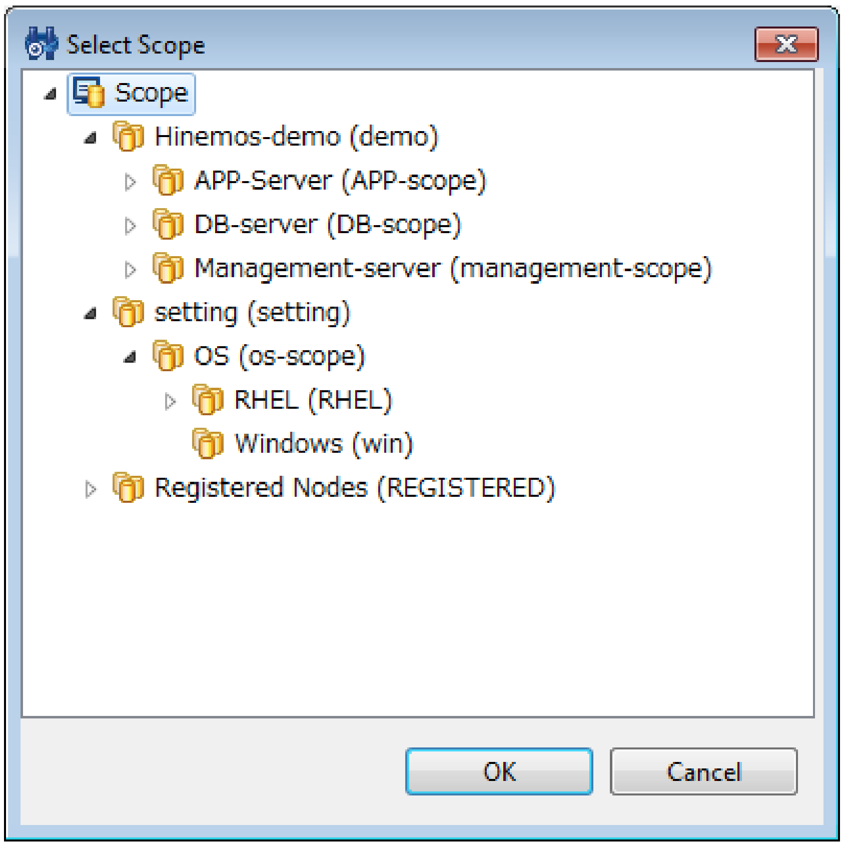


Figure 9-46 Select Scope Dialog

- File:

  Enter the subject file. You can specify a wild card character in the file name.

  The directory can also be specified. In that case, all files included in that directory will be transferred.

  Note) You cannot transfer the system file (for Linux, it is the file starting with a dot (.)).

7. Configure the recipient. Enter the following settings.

- Scope:

  Click the "Refer" button and the Select Scope dialog is displayed; Select the destination scope, and then click on the "OK" button.

- Processing method:

  - Received by All Nodes

    If a scope is configured in the recipient, execute file transfer to all nodes included in that scope.

  - Received by One Node

    If a scope is configured in the recipient, and if file transfer succeeds in one of the node included in that scope, then the file will not be transferred to other nodes.

8. Configure the transferring method. Check on the check box to enable the following configuration.

- Compress at the time of Transfer

  Transfer compressed file during file transfer. It will be extracted after the file transfer.

- Check Transferred Files

  Check the integrity of the source file and the destination file. If there is no match, then the End state is "Error".

9. Configure "Effective User". Enter the effective user of the file transfer command (the owner of the transferred file is the user specified by the effective user).
10. Select the "End Status" tab, and then configure the end status (Refer to Creating/Changing a JobNet for the End Status entry method.)
11. Select the "Notifications" tab, and then configure the notification (Refer to Creating/Changing a JobNet for the Notification setting method.)
12. Click the "OK" button. The Job[Create/Change File-transfer Job] dialog closes. The newly created job is added to the job tree in the Job[List] view.

    Note) The operations described above are made in the client. Information of the editing job tree is not reflected in the manager until the "Register" button is clicked and it has processed.

If configuring control in more details

The following settings are possible (Refer to Creating/Changing a JobNet for the setting method.)

- Configure a calendar
- Make the execution status of a job as hold, in advance
- Skip the execution status of a job in advance

When Running Delayed Start Monitoring

Check if the start of job execution has been delayed. If it is delayed, you can configure the control (Refer to Creating/Changing a JobNet for the setting method.)

When Running End Delay Monitoring

Check if the end of a job has been delayed. If it is delayed, you can configure the control. (Refer to Creating/Changing a JobNet for the setting method.)

Changing File Transfer Job

1. Select the file transferring job to change from the job tree in the Job[List] view.
2. Click on the "Modify" button in the Job[List] view. The Job[Create/Change File-transfer Job] dialog is displayed.
3. Change the parameter of the "File Transfer Job"

End value of the File Transfer Job

The end value of the File Transfer Job is the value shown in Table 9-10 End Value of the File Transfer Job.

Table 9-10 End Value of the File Transfer Job

Status	End value	End status(default)
No source file	-1	Warning
Have source file Transferring process ends successfully	0	Normal
Have source file Transferring process ends with an error	9	Error

9.12 Job Execution Using a Script

You can specify scripts for "Start Command" and "Stop Command" during job registration. The following are notes when using scripts.

1. Current directory

- For the Windows Agent

  The current directory is "C:\WINDOWS\system32".

- For the Linux Agent (default install)

  The current directory is "/opt/hinemos_agent/var/log".

During script creation, it is recommended that the script is not dependent on the current directory (all directories that move to the directory at the beginning of the script startup must be described in absolute paths).

2. Standard output and standard error

   Scrip must release the standard output and the standard error when it ends. The job will not be in end status when the standard output and the standard error is not released.

   - **Example:** pg_ctl (Start command of PostgreSQL)

     In this case, pg_ctl does not release the standard output or the standard error after the startup. Therefore, by making the standard output and the standard error as /dev/null, the job will be in end status.

     ```
     /usr/local/sbin/pg_ctl -w start > /dev/null 2>&1
     ```

   Even if the standard output and the standard error is released, the job will not be in end status when command executed inside the script is not releasing standard output and standard error.

3. Condition to end job by the completion of the parent shell (not waiting for the child shell to complete the process)

   If a (background) process holds the standard output and the standard error in the shell script (command which was started as a job), that control will not return to the Hinemos Job Agent, and the job will remain as the running status. Perform any of the following (switching the output destination) for the section that handles the standard output and the standard error of the parent output.

   - Output the standard output and the standard error in the /dev/null (discard all output data)
   - Output the standard output and the standard error contents in a log file

     Redirection of the output destination will differ by the environment where the bash/csh is executed. Make configurations according to the environment.

   - For csh / tcsh :command >& [log file path or /dev/null]
   - For sh / bash :command > [log file path or /dev/null] 2>&1

Job sample (sleep.sh)

The following section shows a job sample (sleep.sh). When sleep.sh exists in the home directory of the user name "job", execute

```
/home/job/sleep.sh start 10
```

When it is executed, "sleep" is executed for 10 seconds, and returns 0 (successful End). Also, if /home/job/sleep.sh stop 5 is executed, the running sleep.sh process is killed. After the processed is killed, "sleep" is executed for 5 seconds, then returns 0 (successful End).

```
############################################################
###                                                  ###
###                    sleep.sh                        ###
###                                                  ###
############################################################

#!/bin/sh
##############################
# Parameter
##############################
# Work name
gyomu="Sleep"
# Work program
```

Copyright (c) 2013 NTT DATA CORPORATION

```
prg_home="/home/job"
prg_name="${prg_home}/${gyomu}"
# PID file
prg_pid="${prg_home}/${gyomu}.pid"
# Log file
log="${prg_home}/${gyomu}.log"

###################################
# Argument
###################################
# $1 ${action} # start/stop specification
# $2 ${sleep} # sleep time
action=$1
sleep=$2

###################################
# Process
###################################
start() {
        cd ${prg_home}
        echo "Starting : ${gyomu}" >> ${log}
        echo "${action}" >> ${log}
        echo "${sleep}" >> ${log}

        ifif [ -f ${prg_pid} ]; then
                echo "${gyomu} is already running" >> ${log}
                exit 1
        fi

        touch ${prg_pid}
        rval=$?
        if [ $rval != 0 ]; then
                echo "failed to create the status file" >> ${log}
                exit 1
        fi

        # At this time, obtain pid and write in the pid file.
        echo "$$" >> ${prg_pid}
        sleep ${sleep}
        rval=$?
        if [ $rval != 0 ]; then
                echo "${gyomu} program ended with an error ret=${rval}" >> ${log}
                rm -f ${prg_pid}
                rval2=$?
                if [ ${rval2} != 0 ]; then
                        echo "failed to delete the status file" >> ${log}
                        exit ${rval2}
                fi
                exit ${rval}
        fi

        echo "${gyomu} program ended successfully" >> ${log}
        rm -f ${prg_pid}
        rval2=$?
        if [ ${rval2} != 0 ]; then
                echo "failed to delete the status file" >> ${log}
                exit ${rval2}
        fi
        return ${rval}
}

stop() {
        echo "Stopping : ${gyomu}" >> ${log}
        kill `cat ${prg_pid}`
```

Copyright (c) 2013 NTT DATA CORPORATION

```
        rval=$?
        if [ ${rval} != 0 ]; then
                echo "${gyomu} failed to end the program" >> ${log}
                exit ${rval}
        fi
      sleep ${sleep}
        rval=$?
        if [ ${rval} != 0 ]; then
                echo "${gyomu} failed to end the program" >> ${log}
                exit ${rval}
        fi

        echo "${gyomu} program paused successfully" >> ${log}
        rm -f ${prg_pid}
        rval2=$?
        if [ ${rval2} != 0 ]; then
                echo "failed to delete the status file" >> ${log}
                exit ${rval2}
        fi
        return ${rval}
}


case ${action} in
  start)
        start
        ;;
  stop)
        stop
        ;;
  *)
        echo "argument to specify the operation is wrong."  >> ${log}
        exit 1
esac

exit $?
# End of file.
```

** Due to Hinemos specifications, the end code range is 0-255. **

9.13 Operation of the Start Command

Operation of the "Start Command" during job registration differs by the running OS platform and the "Effective User". The agent acts to send a command like that shown below to each platform.

- Windows platform

  If the agent starting the user = Effective User : {Start Command}

  If the agent starting the user ≠ Effective User : execution error

- Linux platform

  If the agent starting the user ＝ Effective User : sh -c {Start Command}

  If the agent starting the user ≠ Effective User : sudo -u {Effective User} sh -c {Start Command} (* The agent's effective user must have the sudo permission. Comment out the corresponding section of the following configuration file.)

  sudoers configuration : /etc/sudoers

  ```
  Before the edition:
  Defaults   requiretty

  After the edition:
  # Defaults   requiretty
  ```

Identification of the OS platform is performed automatically by the agent. Refer to Chapter 8.1, Start Command Action Change in the Administrator's Guide regarding changing the settings.

Start Command for the Windows Platform

With Hinemos 4.1, the specifications for the command passed to the OS have changed.

- Hinemos 4.0 or prior
  - CMD /C {Start Command}
- Hinemos 4.1
  - {Start Command}

Therefore, some of the commands created in versions prior to Hinemos 4.0 will not operate in Hinemos 4.1. (i.e.: If just the script file name for some of the scripts such as VB script, etc. are to be a Start Command. In this case, in order to have the same Start Command operation as in versions prior to Hinemos 4.0:

```
Use CMD /C {Start Command entered
```

in Hinemos 4.0}

10 Collective Run Feature

10.1 Overview

This feature allows for concurrent batch processing for multiple nodes at once.

You can access this feature using a graphical interface. You can perform batch processing of all nodes registered in a scope by specifying that scope.

By default, the following processes can be run by scope.

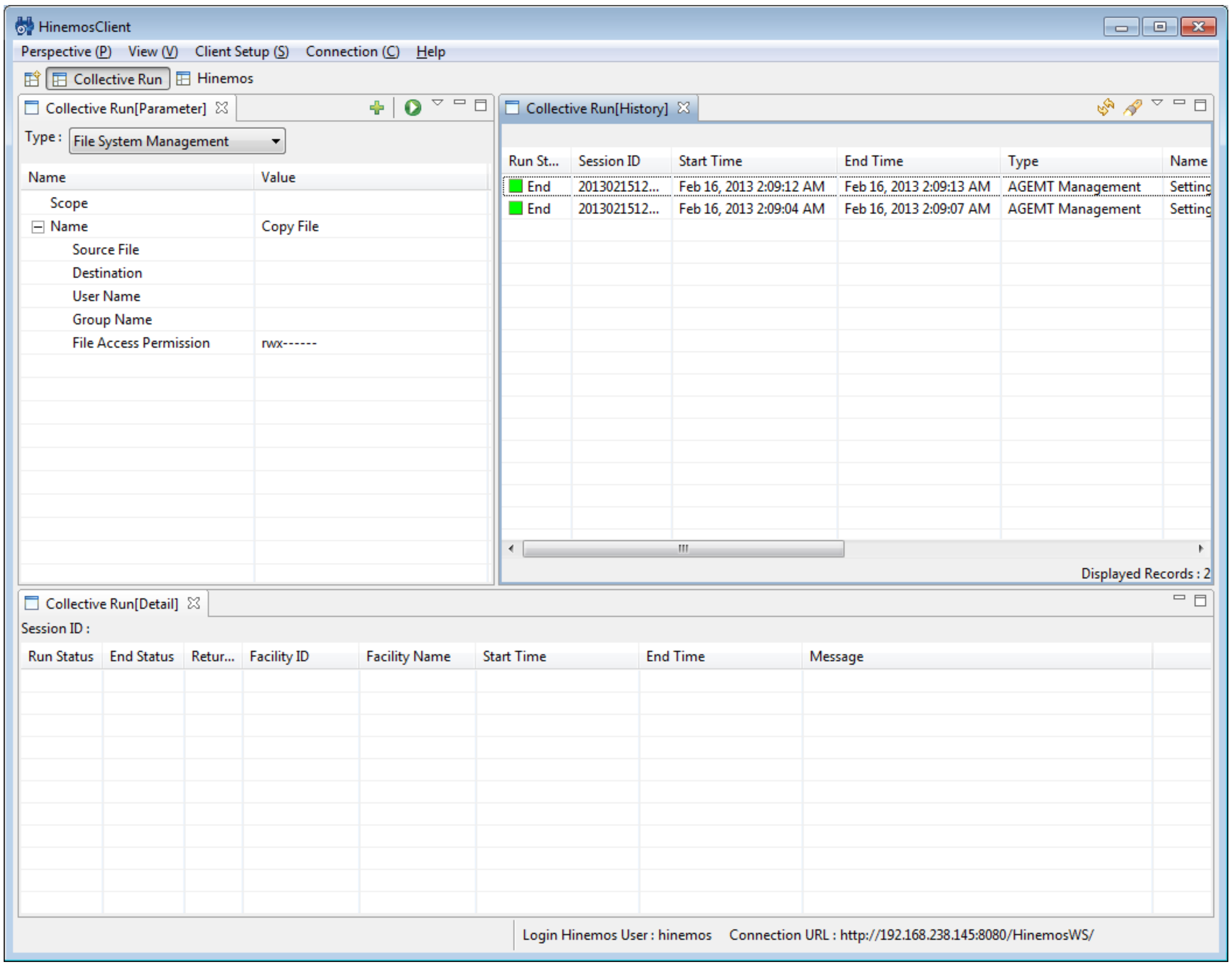
- Installation of the rpm package
- Reboot/Stop Linux
- Start/Stop apache
- Add/Change/Delete the OS account
- Make a Directory
- Copy a file
- Remove a file/directory
- Installation of the Hinemos Agent
- Configure the file transfer job

You can create and edit the processing of new batches on the managed node.

Copyright (c) 2013 NTT DATA CORPORATION

10.2 Interface Composition

10.2.1 Default Interface


HinemosClient
Perspective (P) View (V) Client Setup (S) Connection (C) Help
Collective Run
Hinemos
Collective Run[Parameter]
Collective Run[History]
Collective Run[Detail]

Type : File System Management

Name	Value
Scope	
⊟ Name	Copy File
Source File	
Destination	
User Name	
Group Name	
File Access Permission	rwx------

Run St...	Session ID	Start Time	End Time	Type	Name
🟩 End	2013021512...	Feb 16, 2013 2:09:12 AM	Feb 16, 2013 2:09:13 AM	AGEMT Management	Setting
🟩 End	2013021512...	Feb 16, 2013 2:09:04 AM	Feb 16, 2013 2:09:07 AM	AGEMT Management	Setting

Displayed Records : 2

Session ID :

Run Status	End Status	Retur...	Facility ID	Facility Name	Start Time	End Time	Message

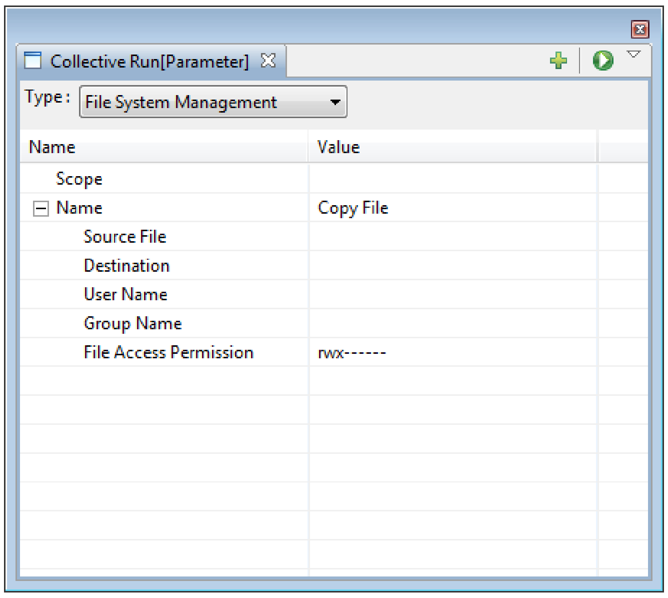
Login Hinemos User : hinemos Connection URL : http://192.168.238.145:8080/HinemosWS/

Figure 10-1 Default Interface of Collective Run Feature

10.2.2 Collective Run[Parameter] View

This view is for selecting operations for running the collective run feature and configuring the parameters.

Copyright (c) 2013 NTT DATA CORPORATION



Collective Run[Parameter]

Type : File System Management

Name	Value
Scope	
⊟ Name	Copy File
Source File	
Destination	
User Name	
Group Name	
File Access Permission	rwx------

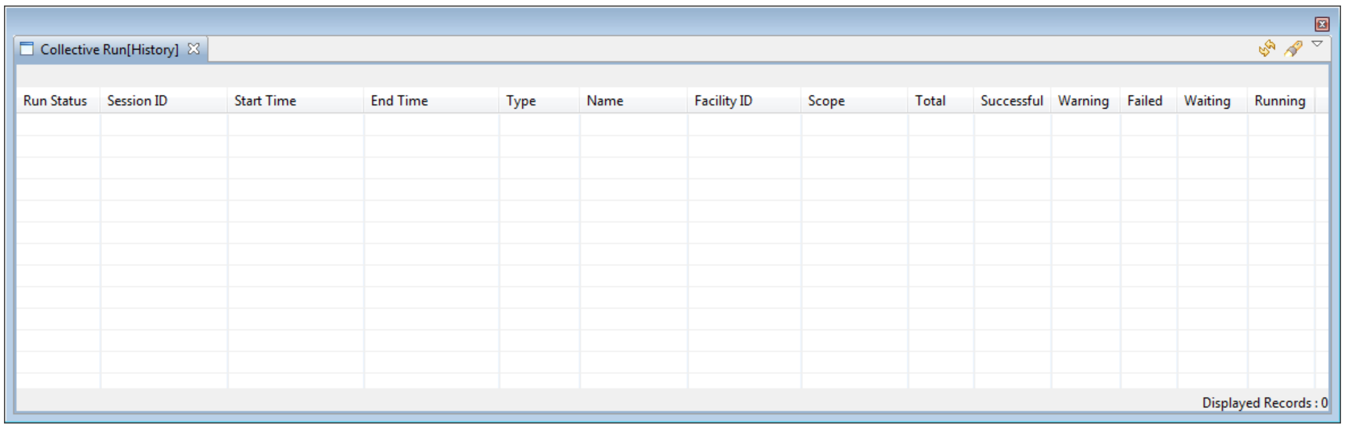
Figure 10-2 Collective Run[Parameter] View

Table 10-1 Toolbar

Icon	Button name	Description
✚	Create	Create commands to run by collective run
▶	Run	Run configured process.

10.2.3 Collective Run[History] View

This view displays the execution results of the collective run feature. It displays the results of the executed operations. When a result is selected from the list, details of the execution results for each node are displayed in the Collective Run[Detail] view.



Collective Run[History]

Run Status	Session ID	Start Time	End Time	Type	Name	Facility ID	Scope	Total	Successful	Warning	Failed	Waiting	Running

Displayed Records : 0

Figure 10-3 Collective Run[History] View

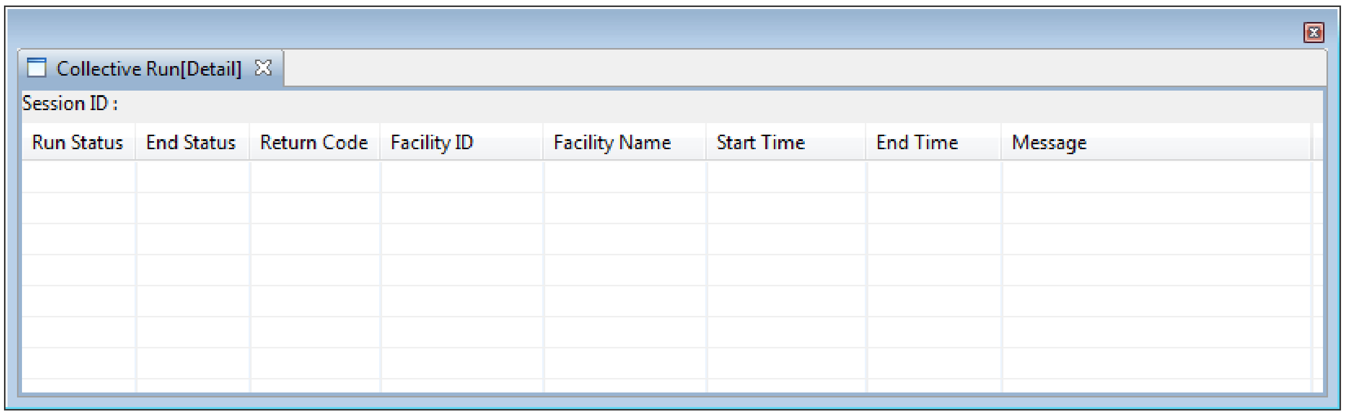
Table 10-2 Toolbar

Icon	Button name	Description
⟳	Update	Update information on the table.
🖉	Filter	Configure filter of execution result list.

10.2.4 Collective Run[Detail] View

This view displays the execution result by node.

Copyright (c) 2013 NTT DATA CORPORATION



Collective Run[Detail]

Session ID :

Run Status	End Status	Return Code	Facility ID	Facility Name	Start Time	End Time	Message

Figure 10-4 Collective Run[Detail] View

10.3 Prerequisites for Feature Usage

The following configuration must be made beforehand to use the collective run feature.

- Node that is subject to operation must be registered in the repository feature and assigned to any of the scopes
- You can run a command on the monitored node from the manager with ssh or rsh.

  Refer to the following manuals for more information.

  Chapter 6, "Collective Run Feature" in the Administrator's Guide

10.4 Procedures for Processing the Collective Run

You can execute "Installation Management", "Start/Stop Management", "User Management", and "File System Management" in the collective run feature. These operations are executed by common procedures; the procedure is described below (for detailed procedures of each operation, please refer to the section described below).

Execution procedures for the collective run feature are as follows.

1. From the Type select combo box in the Collective Run[Parameter] view, select the management feature to run. The parameter configuration of the selected feature will be displayed on the property table.
2. Select the scope subject to operation. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The Select Scope dialog box is displayed. Scope can be selected from this dialog box.
3. Select the operation to execute. Click on the value field in the table's Property "Name". From the combo box, select the operation to execute.
4. Configure the parameter. Enter a value in the value field of "Property". The setting value items selected from the states are in the combo box, so select the setting items from the list. There is a text box to directly enter the necessary items.
5. Click the "Run" button in the Collective Run[Parameter] view.
6. The "Confirmed" dialog is displayed. Confirm the contents, and click the "Run" button.
7. The process is executed. The status of the running collective run feature will be displayed in the Collective Run[History] view.

10.5 Installation Management

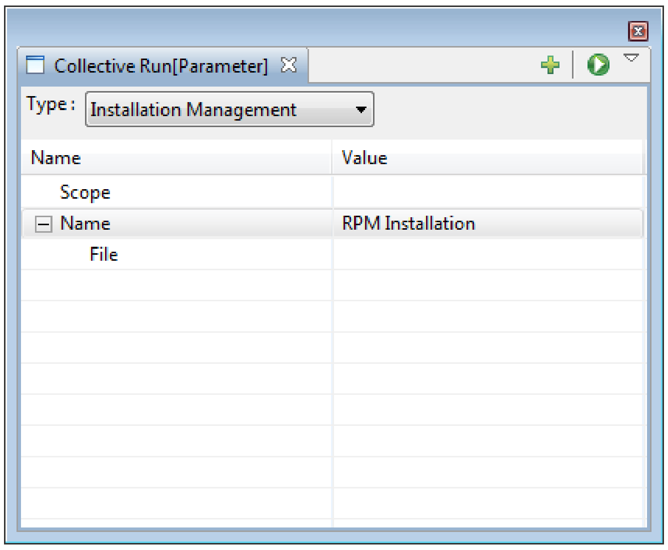
10.5.1 rpm Installation

Installation Management collectively installs the rpm package to all nodes in the specified scope.

1. Place the rpm package file (***. rpm file) on the FTP server configured for the Hinemos file transfer. Configure the settings of the FTP user so that the rpm package file can be read.

   * Refer to Chapter 6.1.3, "FTP Server Startup" in the Administrator's Guide regarding the method for setting up the FTP server and the FTP user.

2. From the Type select combo box in the Collective Run[Parameter] view, select "Installation Management".



Type: Installation Management

Name	Value
Scope	
⊟ Name	RPM Installation
File	

Figure 10-5 Collective Run[Parameter] View

3. Configure the scope to perform batch installation. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.

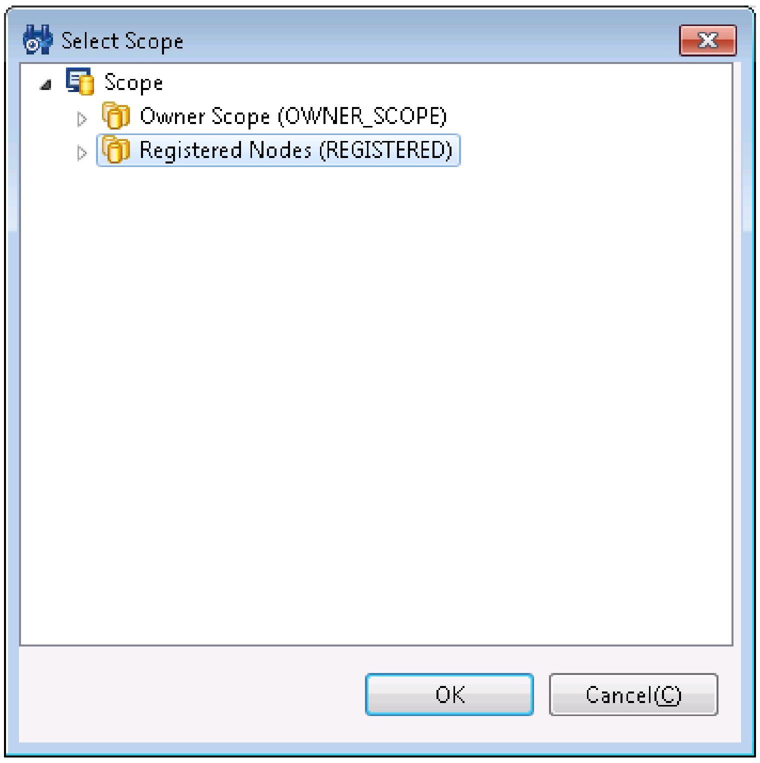
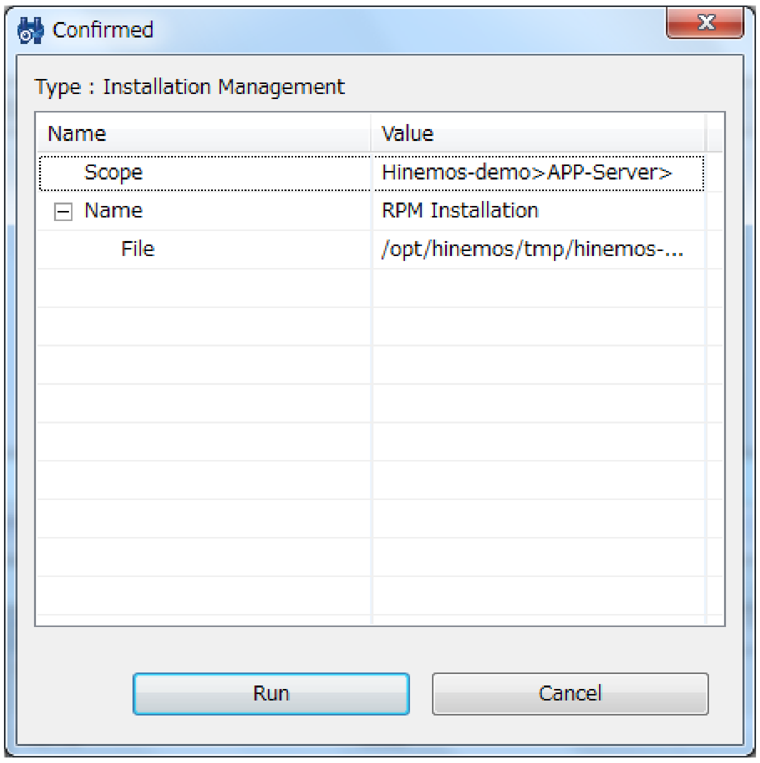


Figure 10-6 Select Scope Dialog

4. Select the scope to be installed from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".

5. Enter the RPM package file name to install. Enter the full path (path on the FTP server) where the rpm package file is located.

6. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Type : Installation Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	RPM Installation
File	/opt/hinemos/tmp/hinemos-...

Figure 10-7 Confirmed Dialog

7. Confirm that the scope targeted for install and the set parameters for installation are correct. Then click the " Run" button.

   When canceling the rpm installation, click the "Cancel" button.

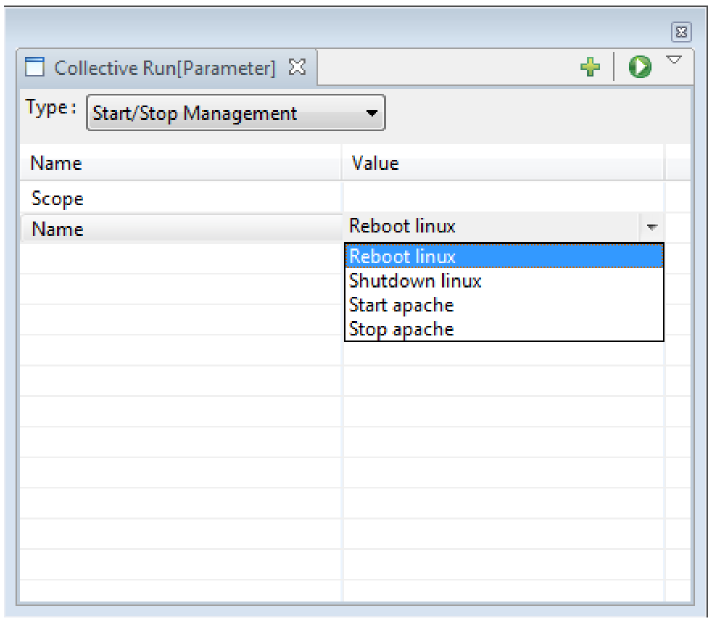
10.6 Start/Stop Management

The following functions are provided for managing startup and stop.

- Reboot Linux
- Stop Linux
- Start apache
- Stop apache

1. From the Type select combo box in the Collective Run[Parameter] view, select "Start/Stop Management".
2. Configure the subject scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.
3. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".

4. Select the operation to run. Click on the value field in the table's Property "Name" record. Select the operation to execute from the combo box that is displayed.



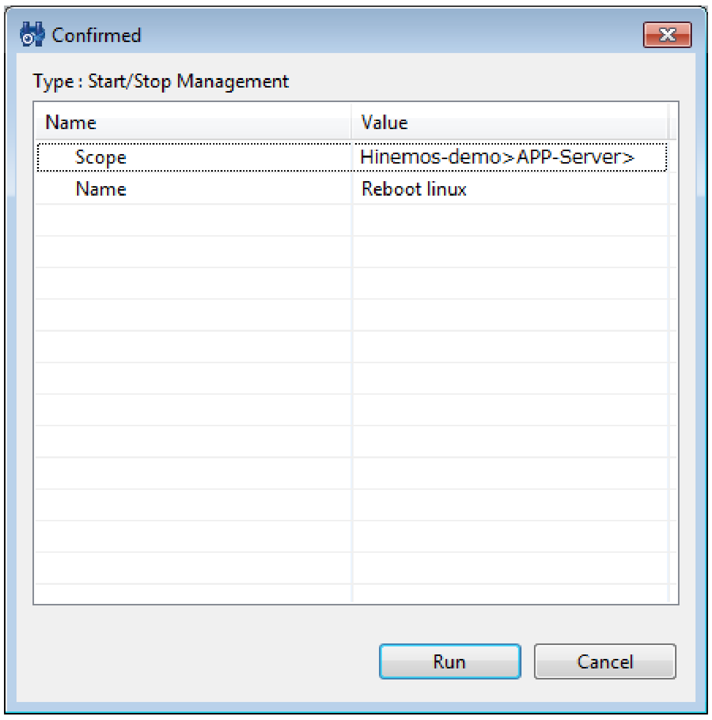
Collective Run[Parameter]

Type : Start/Stop Management

Name	Value
Scope	
Name	Reboot linux

Figure 10-8 Selecting the Operation to Run

5. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Confirmed

Type : Start/Stop Management

Name	Value
Scope	Hinemos-demo>APP-Server>
Name	Reboot linux

Figure 10-9 Confirmed Dialog

6. Confirm that the specified parameter is correct and click the "Run" button.

When canceling the executing operation, click the "Cancel" button.

10.7 User Management

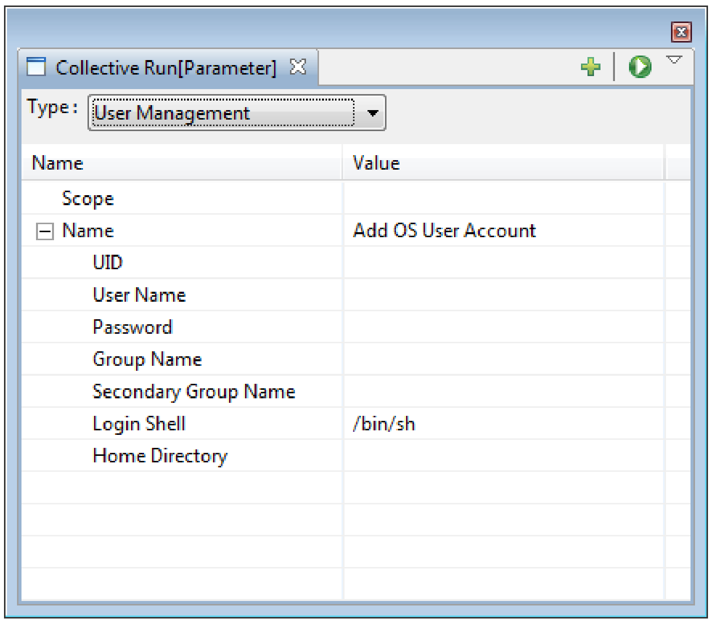
The following features are provided by user management.

- Add OS User Account
- Change OS User Account
- Delete OS User Account

Copyright (c) 2013 NTT DATA CORPORATION

10.7.1 Add OS User Account

1. From the Type select combo box in the Collective Run[Parameter] view, select "User Management" in the "Type" combo box.



Type : User Management

Name	Value
Scope	
Name	Add OS User Account
UID	
User Name	
Password	
Group Name	
Secondary Group Name	
Login Shell	/bin/sh
Home Directory	

Figure 10-10 Collective Run[Parameter] View

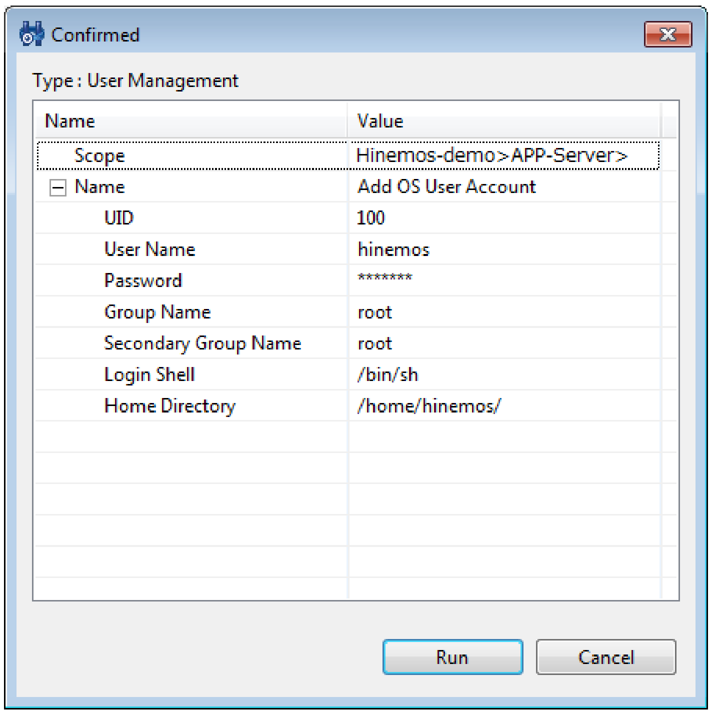
2. Configure the subject scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.
3. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".
4. Click on the value field in the table's Property "Name" record. Select "Add OS User Account" from the combo box.
5. Enter the parameter. Configure "UID", "User Name", "Password", "Group Name", "Secondary Group Name", and "Home Directory". Enter the value in the text box. A combo box is displayed when the value field of "Login Shell" is clicked; please select the parameter from the list.

   "Group Name", "Secondary Group Name", and "Home Directory" can be blank. When the item is blank

- "Group Name" ... will belong to the same primary group as the user name
- "Secondary Group Name" ... will not belong to any group other than the primary group
- "Home Directory" ... will be /home/ (user name)

Copyright (c) 2013 NTT DATA CORPORATION

6. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Confirmed

Type : User Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	Add OS User Account
UID	100
User Name	hinemos
Password	*******
Group Name	root
Secondary Group Name	root
Login Shell	/bin/sh
Home Directory	/home/hinemos/

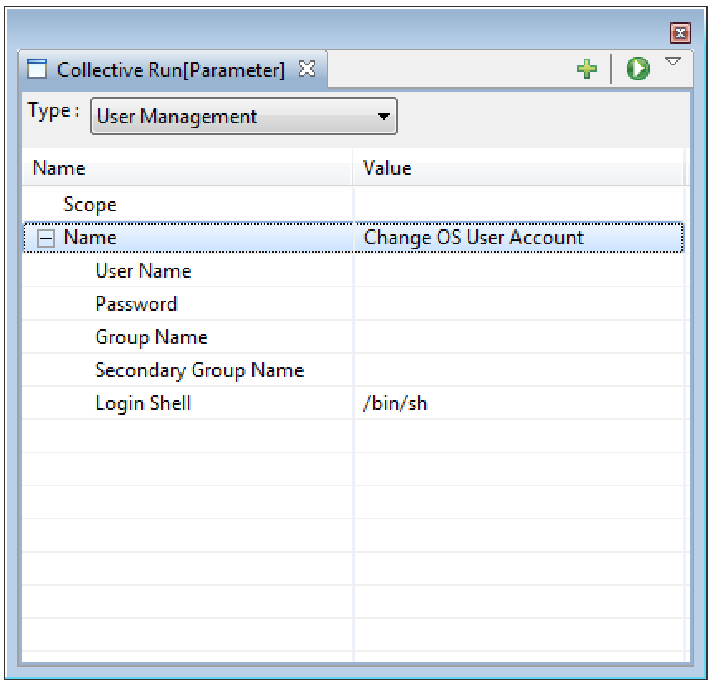
Figure 10-11 Confirmed Dialog

7. Confirm that the configured parameters are correct. Then click the "Run" button.

When canceling "Add OS User Account", click on the "Cancel" button.

10.7.2 Change OS User Account

1. From the Type select combo box in the Collective Run[Parameter] view, select "User Management" in the "Type" combo box.



Collective Run[Parameter]

Type : User Management

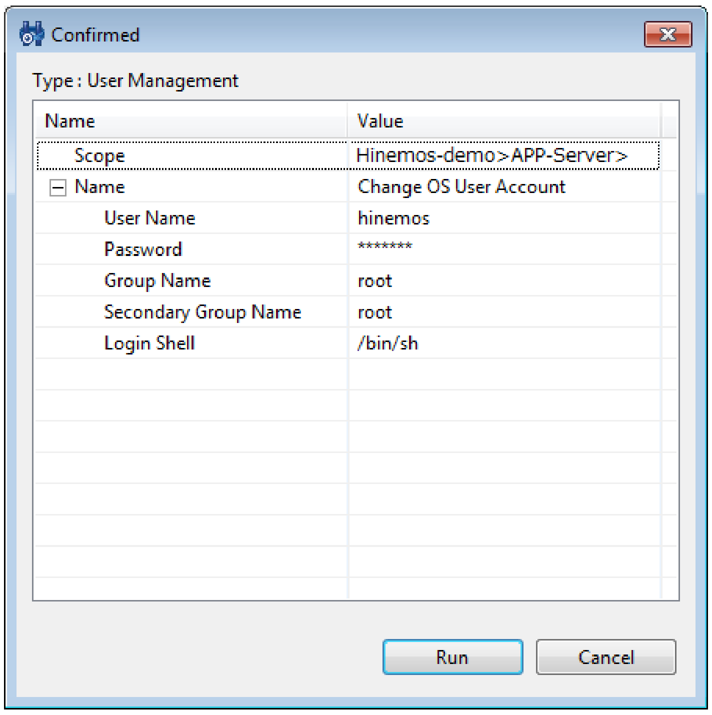
Name	Value
Scope	
⊟ Name	Change OS User Account
User Name	
Password	
Group Name	
Secondary Group Name	
Login Shell	/bin/sh

Figure 10-12 Collective Run[Parameter] View

2. Configure the subject scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.
3. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".

Copyright (c) 2013 NTT DATA CORPORATION

4. Click on the value field in the table's Property "Name" record. Select "Change OS User Account" from the comb o box.
5. Enter the parameter. Configure "User Name", "Password" and "Group Name", "Secondary Group Name", and "Logi n Shell". Enter the value in the text box. A combo box is displayed when the value field of "Login Shell" is click ed; please select the parameter from the list. If making no changes, please leave the subject parameter blank.
6. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Type : User Management

Name	Value
Scope	Hinemos-demo>APP-Server>
Name	Change OS User Account
User Name	hinemos
Password	*******
Group Name	root
Secondary Group Name	root
Login Shell	/bin/sh

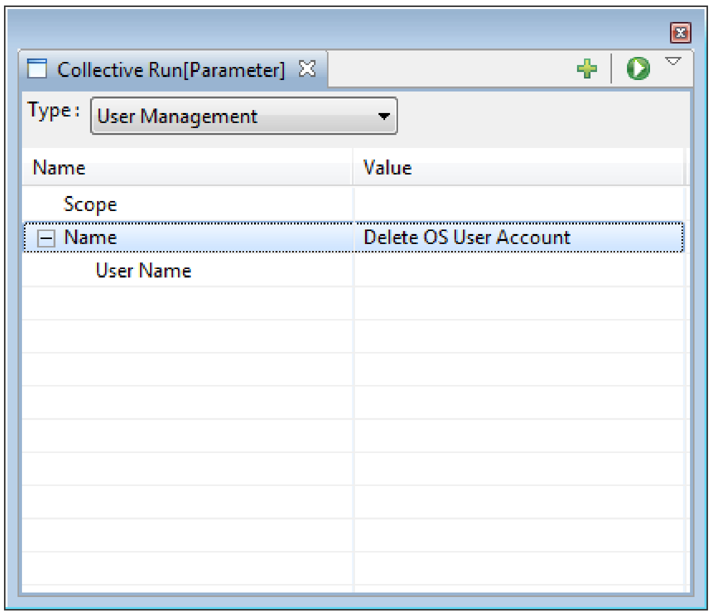
Figure 10-13 Confirmed Dialog

7. Confirm that the configured parameters are correct. Then click the "Run" button.

When canceling "Change OS User Account", click the "Cancel" button.

10.7.3 Delete OS User Account

1. From the Type select combo box in the Collective Run[Parameter] view, select "User Management" in the "Type" combo box.

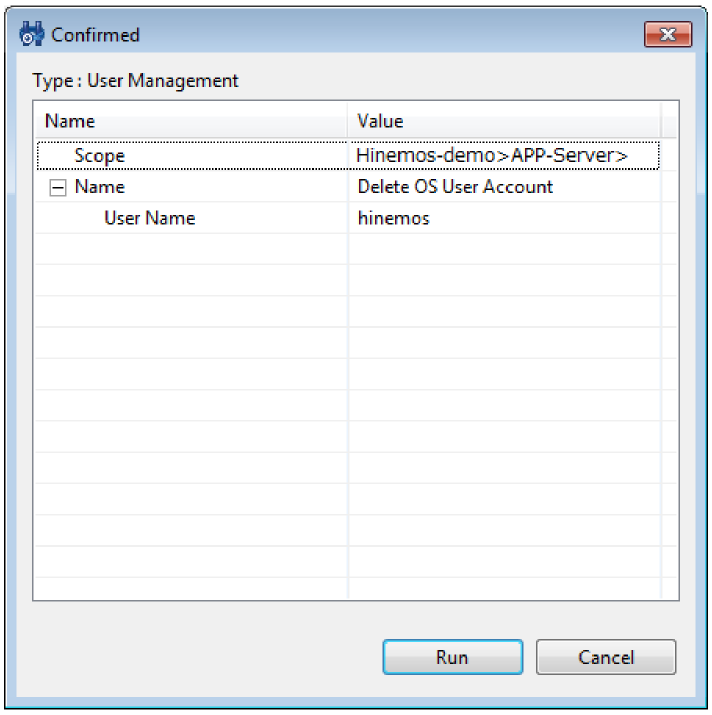


Type : User Management

Name	Value
Scope	
Name	Delete OS User Account
User Name	

Figure 10-14 Collective Run[Parameter] View

2. Configure the subject scope. Click on the record value field in the table's Property scope. Then click the butto n that appears on the far right of the field. The "Select Scope" dialog is displayed.
3. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".
4. Select the operation to run. Click on the value field in the table's Property "Name" record. Select "Delete OS U ser Account" from the combo box.
5. Enter the user name. Enter the user name in the "User Name".
6. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Confirmed

Type : User Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	Delete OS User Account
User Name	hinemos

Figure 10-15 Confirmed Dialog

7. Confirm that the specified parameter is correct and click the "Run" button.

When canceling "Add OS User Account", click on the "Cancel" button.

10.8 File System Management

The following functions are provided for file system management.

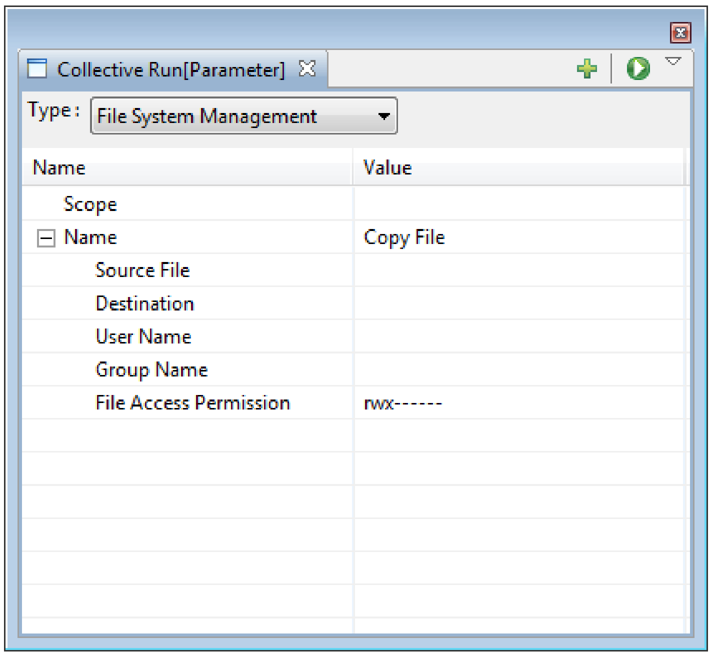
- Copy File
- Make Directory
- Remove File/Directory

10.8.1 Copy File

1. Place the file to copy on the FTP server configured for the Hinemos file transfer. Configure the copy target fi le so that it can be read by the FTP user using Hinemos.

   * Refer to Chapter 6.1.3, "FTP Server Startup" in the Administrator's Guide regarding the method for setting u p the FTP server and the FTP user.

2. From the Type select combo box in the Collective Run[Parameter] view, select "File System Management" in the "Type" combo box.



Type : File System Management

Name	Value
Scope	
⊟ Name	Copy File
Source File	
Destination	
User Name	
Group Name	
File Access Permission	rwx------

Figure 10-16 Collective Run[Parameter] View

3. Configure the subject scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.

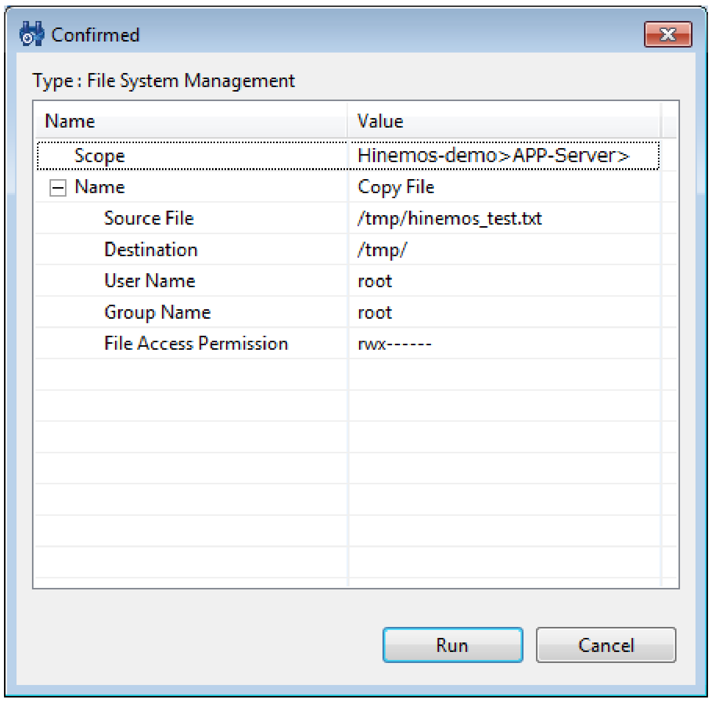
4. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".

5. Click on the value field in the table's Property "Name" record. Select "Copy File" from the combo box.

6. Enter the file name target to copy in "Source File". Enter the full path where the file is placed (the path on the FTP server).

7. Configure "Destination", "User Name" and "Group Name" and "File Access Permission" of the file owner after it is copied. Enter "Destination", "User Name", and "Group Name" values in the appropriate text box. A combo box is displayed when the value field of "File Access Permission" is clicked; please select the parameter from the list.

8. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Type : File System Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	Copy File
Source File	/tmp/hinemos_test.txt
Destination	/tmp/
User Name	root
Group Name	root
File Access Permission	rwx------

Figure 10-17 Confirmed Dialog

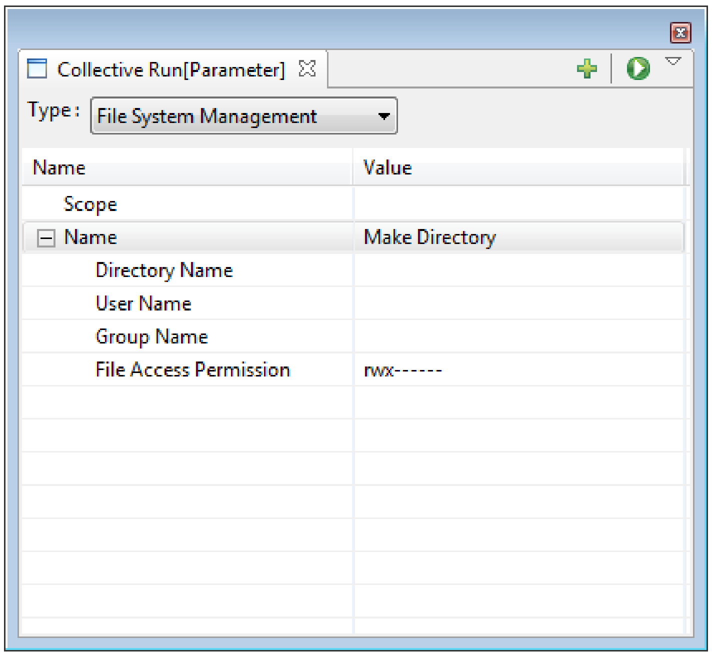
9. Confirm that the specified parameter is correct and click the "Run" button.

Copyright (c) 2013 NTT DATA CORPORATION

To cancel "Copy File", click the "Cancel" button.

10.8.2 Make Directory

1. From the Type select combo box in the Collective Run[Parameter] view, select "File System Management" in the "Type" combo box.



Type : File System Management

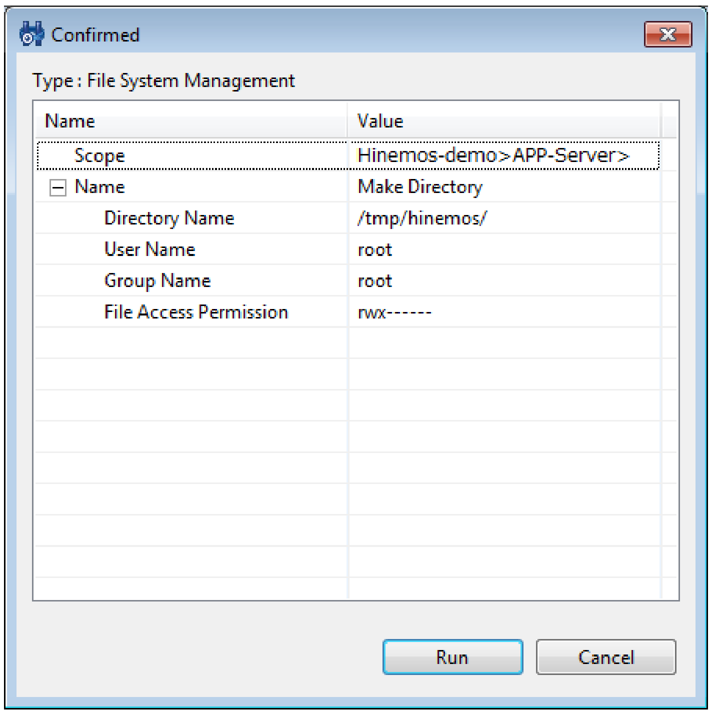
Name	Value
Scope	
⊟ Name	Make Directory
Directory Name	
User Name	
Group Name	
File Access Permission	rwx------

Figure 10-18 Collective Run[Parameter] View

2. Configure the subject scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.
3. Select the target scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".
4. Click on the value field in the table's Property "Name" record. Select "Make Directory" from the combo box.
5. Specify the directory name of the directory to create and the User Name and Group Name of the directory owner, and File Access Permission. Enter "Directory Name", "User Name", and "Group Name" in the appropriate text box. A combo box is displayed when the value field of "File Access Permission" is clicked; please select the parameter from the list.

Copyright (c) 2013 NTT DATA CORPORATION

6. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Confirmed

Type : File System Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	Make Directory
Directory Name	/tmp/hinemos/
User Name	root
Group Name	root
File Access Permission	rwx------

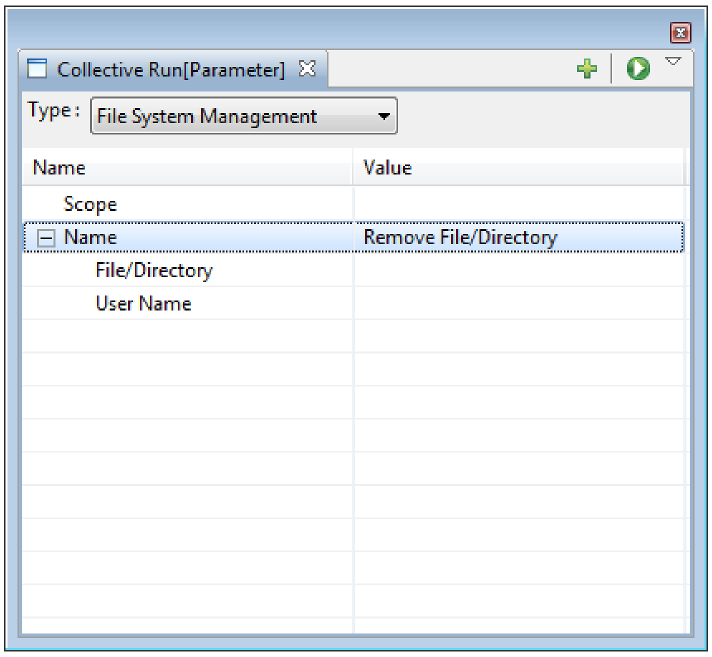
Figure 10-19 Confirmed Dialog

7. Confirm that the specified parameter is correct and click the "Run" button.

To cancel directory creation, click the "Cancel" button.

10.8.3 Remove File/Directory

1. From the Type select combo box in the Collective Run[Parameter] view, select "File System Management" in the "Type" combo box.



Type : File System Management

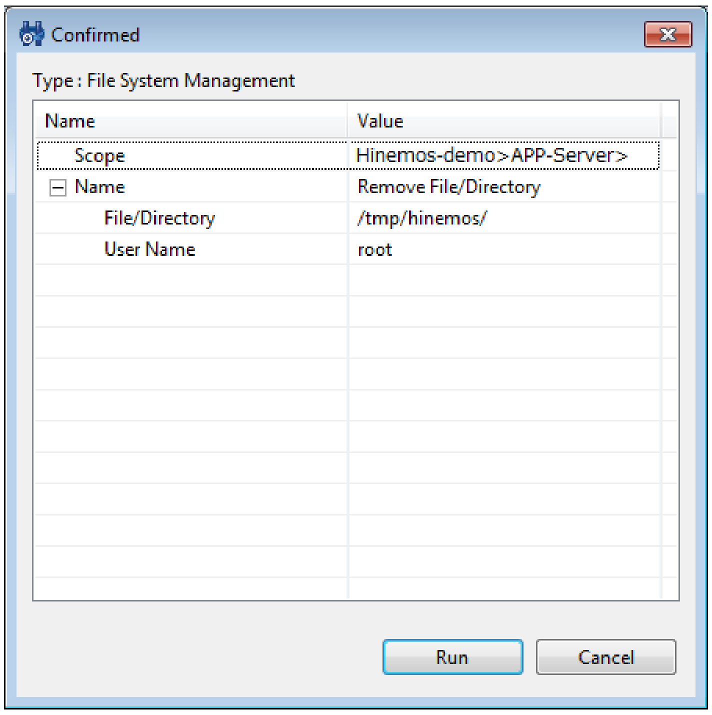
Name	Value
Scope	
⊟ Name	Remove File/Directory
File/Directory	
User Name	

Figure 10-20 Collective Run[Parameter] View

2. Configure the operation target scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.
3. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".

Copyright (c) 2013 NTT DATA CORPORATION

4. Select the operation to run. Click on the value field in the table's Property "Name" record. Select "Remove File/ Directory" from the combo box.
5. Enter the path of the file (directory) to delete and the user name that will execute the delete command. Enter the value in the text box.
6. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Type : File System Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	Remove File/Directory
File/Directory	/tmp/hinemos/
User Name	root

Figure 10-21 Confirmed Dialog

7. Confirm that the specified parameter is correct and click the "Run" button.

To cancel "Remove File/Directory", click the "Cancel" button.

10.9 AGENT Management

The following features are provided for agent management.

- Installation of the Agent
- Configure the file transfer job

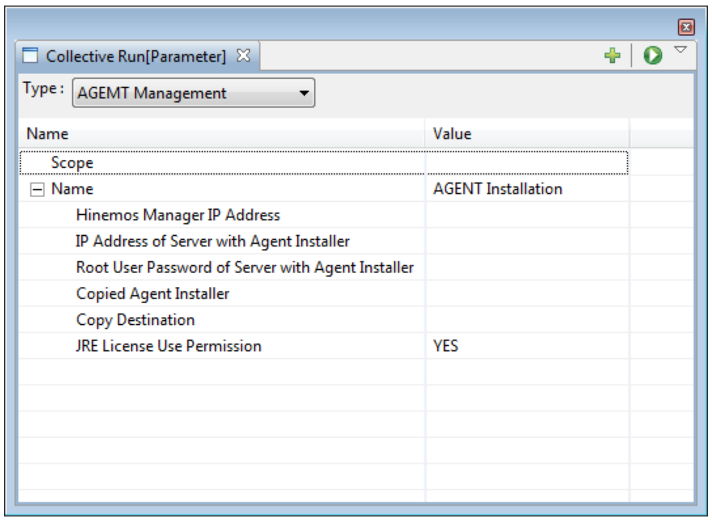
10.9.1 AGENT Installation

1. Place the Hinemos Agent installer for the installation on the SCP server. Configure the hinemos user so that t he installer can be read.

   * The public key for the SCP server must be registered in the known_hosts file of the server where the agent is installed.

Copyright (c) 2013 NTT DATA CORPORATION

2. From the Type select combo box in the Collective Run[Parameter] view, select "AGENT Management" in the "Type" combo box.

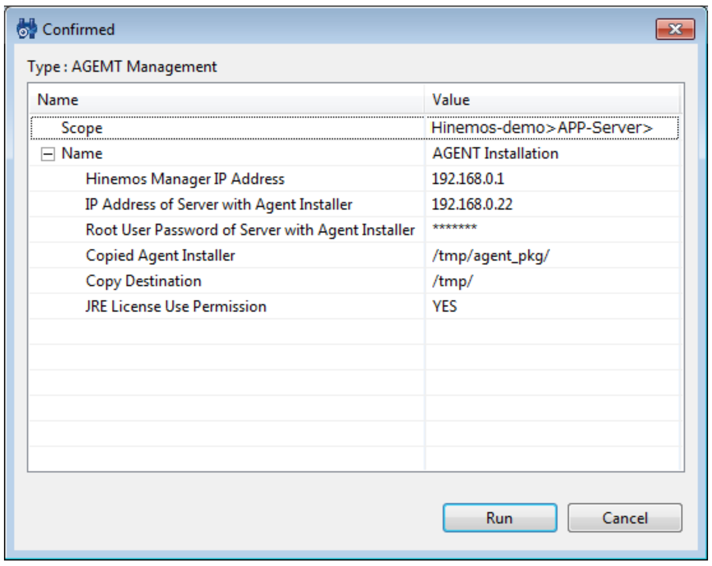


Type : AGEMT Management

Name	Value
Scope	
⊟ Name	AGENT Installation
Hinemos Manager IP Address	
IP Address of Server with Agent Installer	
Root User Password of Server with Agent Installer	
Copied Agent Installer	
Copy Destination	
JRE License Use Permission	YES

Figure 10-22 Collective Run[Parameter] View

3. Configure the operation target scope. Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.
4. Select the subject scope from the scope tree, and then click on the "OK" button. The selected scope name will be entered as the value for "Scope".
5. Click on the value field in the table's Property "Name" record. Select "AGENT Installation" from the combo box.
6. Enter the "Hinemos Manager IP Address". Enter the value in the text box.
7. Enter the "IP Address of Server with Agent Installer" and the "Root User Password of Server with Agent Installer". Enter the value in the text box.
8. Enter the full path (the path on the SCP server) of the Hinemos Agent installer in the "Copied Agent Installer" field.
9. Enter the full path (the path on the agent machine) in the "Copy Destination" field for the Hinemos Agent installer (path on the server where the agent is installed).
10. Configure the "JRE License Use Permission". Combo box is displayed when the value field is clicked: please select the parameter from the list.
11. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Type : AGEMT Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	AGENT Installation
Hinemos Manager IP Address	192.168.0.1
IP Address of Server with Agent Installer	192.168.0.22
Root User Password of Server with Agent Installer	*******
Copied Agent Installer	/tmp/agent_pkg/
Copy Destination	/tmp/
JRE License Use Permission	YES

Figure 10-23 Confirmed Dialog

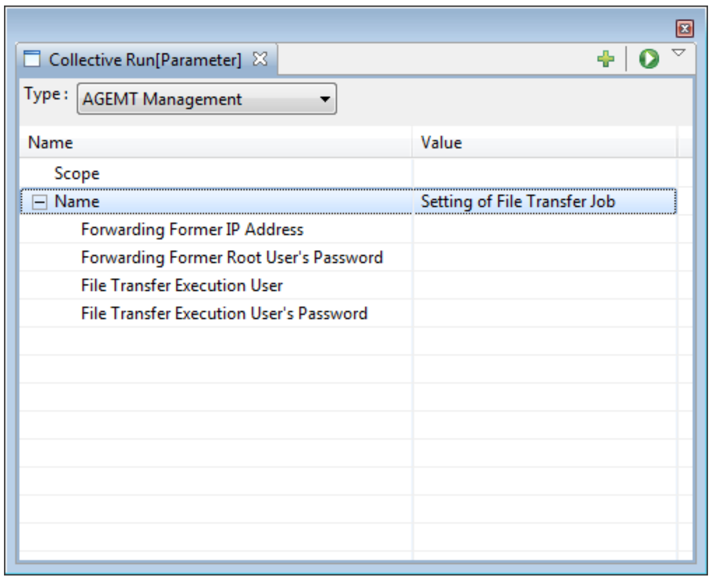
12. Confirm that the specified parameter is correct and click the "Run" button.

When canceling the agent installation, click the "Cancel" button.

10.9.2 Setting of File Transfer Job

1. On the node that performs the settings for File Transfer Job (Refer to the section File Transfer Job for more details on the file transfer job) create the user for executing the file transfer in advance and install the Hinemos Agent (refer to Chapter 6, "Monitored Node (Linux Agent)" in the Installation Manual for the installation method).

2. From the Type select combo box in the Collective Run[Parameter] view, select "AGENT Management" in the "Type" combo box.



Collective Run[Parameter]

Type : AGEMT Management

Name	Value
Scope	
⊟ Name	Setting of File Transfer Job
Forwarding Former IP Address	
Forwarding Former Root User's Password	
File Transfer Execution User	
File Transfer Execution User's Password	

Figure 10-24 Collective Run[Parameter] View

3. Configure the subject scope (scope that is the transfer destination). Click on the record value field in the table's Property scope. Then click the button that appears on the far right of the field. The "Select Scope" dialog is displayed.

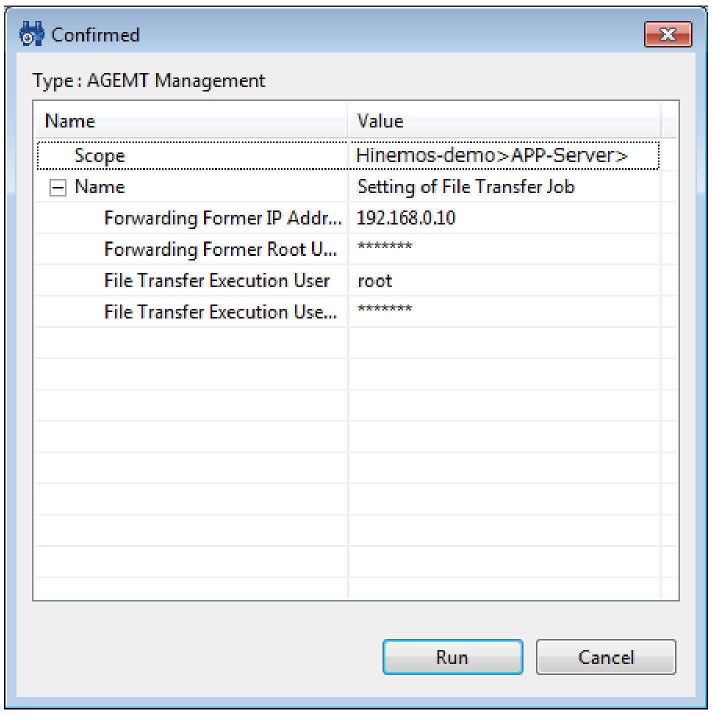
4. Select the subject scope from the scope tree, and then click the "OK" button. The selected scope name will be entered as the value for "Scope".

5. Click on the value field in the table's Property "Name" record. Select "Setting of File Transfer Job" from the combo box.

6. Enter "Forwarding Former IP Address", "Forwarding Former Root User's Password", "File Transfer Execution User", and "File Transfer Execution User's Password". Enter the value in the text box.

Copyright (c) 2013 NTT DATA CORPORATION

7. Click the "Run" button in the Collective Run[Parameter] view. The "Confirmed" dialog is displayed.



Type : AGEMT Management

Name	Value
Scope	Hinemos-demo>APP-Server>
⊟ Name	Setting of File Transfer Job
Forwarding Former IP Addr...	192.168.0.10
Forwarding Former Root U...	*******
File Transfer Execution User	root
File Transfer Execution Use...	*******

Figure 10-25 Confirmed Dialog

8. Confirm that the specified parameter is correct and click the "Run" button.

To cancel "Setting of File Transfer Job", click the "Cancel" button.

* After configurations are made, restart the Hinemos Manager to enable the configuration.

10.10 History of the Collective Run

The history of executed operation is displayed in the Collective Run[History] view. When an operation is selected from the history list, the execution status of each node selected in the Collective Run[Detail] view is displayed.

- To rerun the same operation

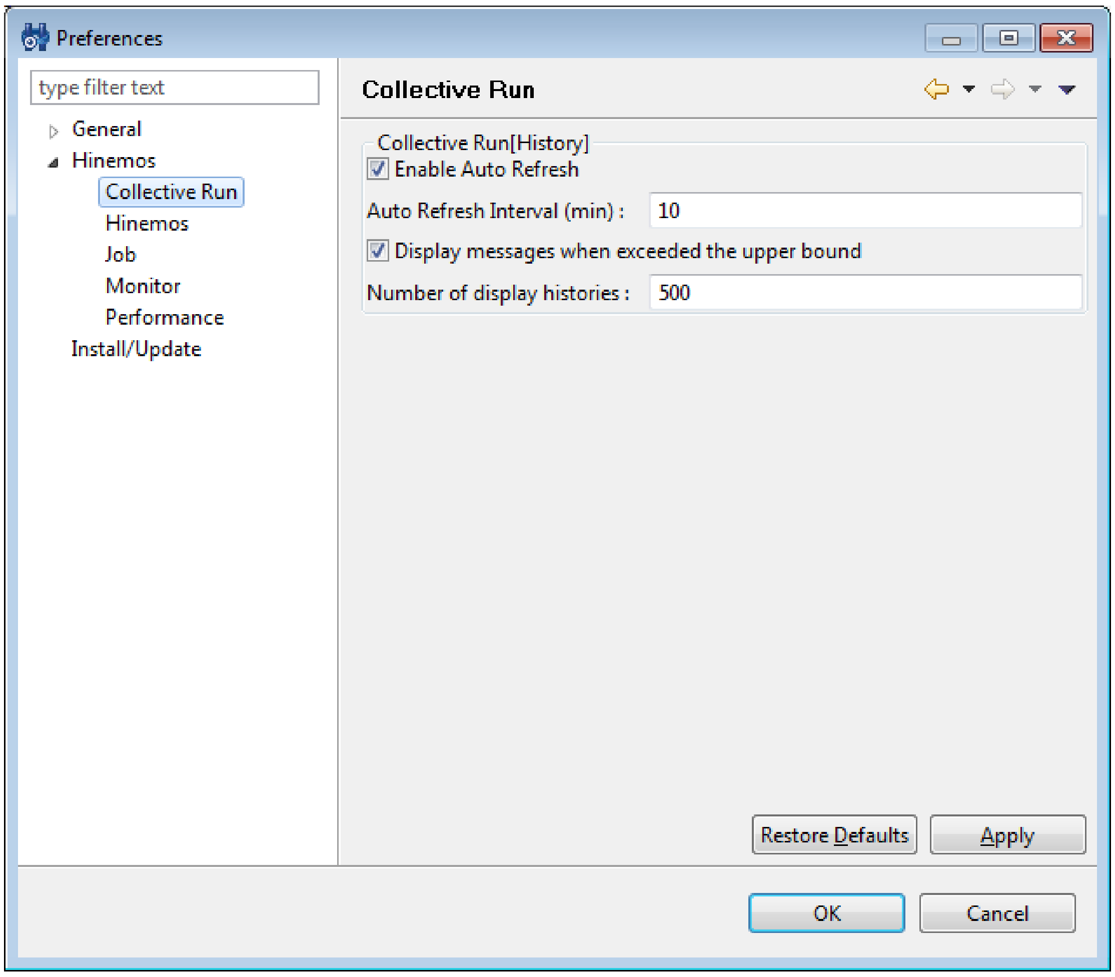
The operation can be executed again based on the past execution.

1. Select the operation to rerun from the run history in the Collective Run[History] view.
2. The configuration from the last run is displayed in the Collective Run[Parameter] view. If there is a need to change the configuration, modify the parameter in the Collective Run[Parameter] view.
3. Click the "Run" button in the Collective Run[Parameter] view.

10.11 Changing the Screen Update Interval and History Display Control of Collective Run Feature

The screen information is updated regularly by obtaining manager information from the client at regular intervals. The restriction on the displayed update interval and the history can be changed by the following procedures.

1. Select [Client Setup] - [Setup] from the menu bar. The Preferences dialog is displayed.



Collective Run

Collective Run[History]

☑ Enable Auto Refresh

Auto Refresh Interval (min) : 10

☑ Display messages when exceeded the upper bound

Number of display histories : 500

Figure 10-26 Preferences Dialog

2. Select Hinemos - Collective Run in the tree pane on the left side.
3. The following configurations relating to the Collective Run[History] view can be made.

- Enable Auto Refresh:

  The contents of the view will be updated at the specified auto refresh interval when this check box is checked. If unchecked, the contents will not be updated unless the "Update" button is clicked.

- Auto Refresh Interval (min):

  If auto refresh is enabled, specify the refresh interval in minutes. (Can be specified from 1 to 32767)

- Display messages when the upper bound is exceeded:

  A message will be output if this check box is checked and if the number of displayed histories exceeds the spe cified "Number of display histories". If unchecked, message will not be output even if the history count exceed s the display history count.

- Number of display histories:

  Specify the number of histories displayed at once. (Can be specified from 1 to 32767)

10.12 Modifying the Master Information

You can modify the executed command during the collective run feature.

The registered master information is composed of "Type", "Command", and "Parameter".

To configure a new command to execute in the collective run feature, first create the "Type". The "Type" is used to classify the type of control.

The "Type" created here is added to the "Type" in the Collective Run[Parameter] view. "File System Management", "I nstallation Management", "Start/Stop Management", and "User Management" are registered by default.

Next, create the "Command". The collective run feature is a feature for command execution from the GUI, but this "Command" names the control to be executed and defines the actual executing command (Script can be executed as well. When executing a script, first transfer the script file on the manager to the managed node then execute on the managed node). For example, the commands "Copy File", "Make Directory", and "Remove File/Directory" are registered in "Type: File System Management" by default.

You can configure the parameter for the "Command". To configure the parameter, register the ID as "Parameter" and make the parameter ID reference. When the parameter is configured correctly, it can be used in multiple "Commands". Input type of the "Parameter" is either "Edit" or "Select". Use "Edit" to enter the text and use "Select" to select from the list.

10.12.1 Create a Command

1. Click on the "Create" button in the Collective Run[Parameter] view. The Collective Run[Create/Change] dialog box is displayed.

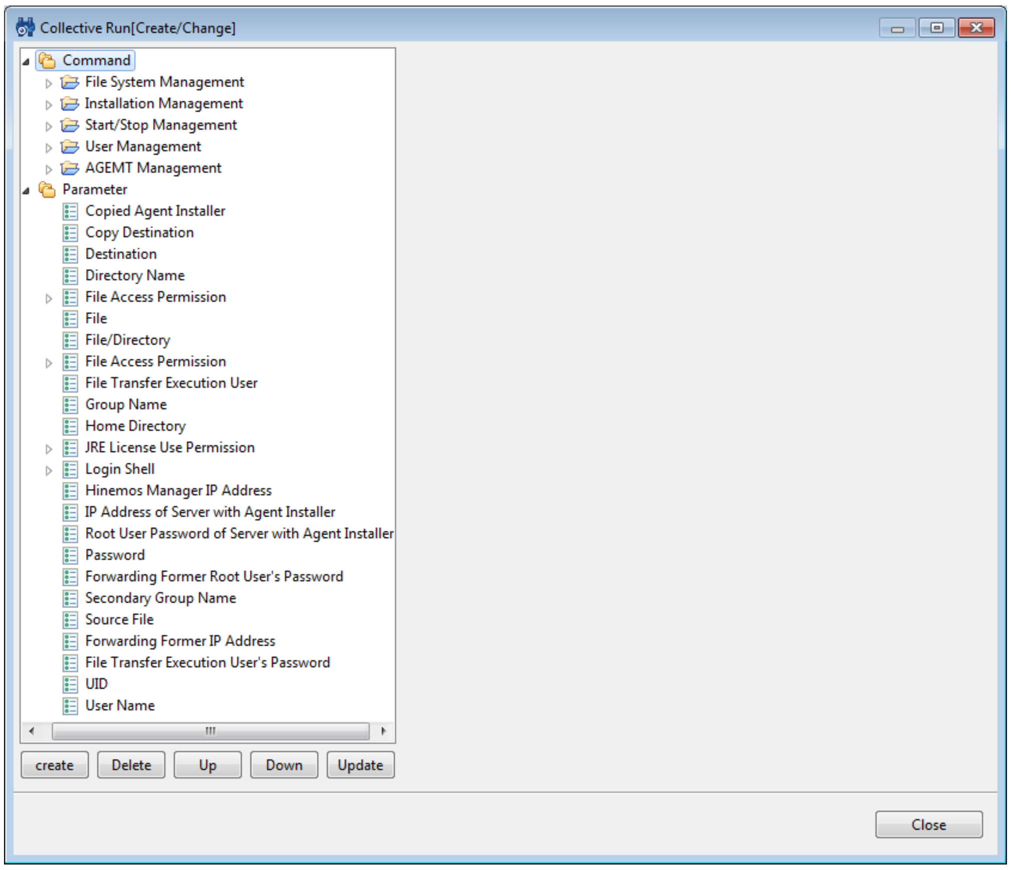


Figure 10-27 Collective Run[Create/Change] Dialog

First create the "Type" by the following procedure.

1. Select the "Command" from the tree pane on the left side, then click the "Create" button. The name "Create" is created as a "Type".
2. Enter the following items in the area on the right side, then click the "Apply" button.

- Type ID;

  Enter the ID to uniquely identify the type.
- Name:

  The name entered here is displayed on the selection candidate list as the "Type" in the Collective Run[Parameter] view.

Next, create the "Command".

1. Select the "Type" from the tree pane on the left side, then click the "create" button. "Create" is newly created.

2. Enter the following items in the area on the right side, then click the "Apply" button.

Copyright (c) 2013 NTT DATA CORPORATION

- Command ID:

  Enter ID to uniquely identify the command.

- Name:

  The name entered here is displayed on the selection candidate list as a selectable command in the Collective Run[Parameter] view.

- Type:

  Select a command or a script.

- Command:

  Enter the actual command or the scrip to be executed during the collective run feature. If it is a command, please specify a command that can be executed as the root user on the managed node.

  If it is a script, please make sure that it is registered on the manager side and enter the script file name with a full path.

- End Status:

  Exit status of the command is determined by the return code during the command or the script execution. Please specify the return code range for "Normal" and "Warning" exit status. Return codes outside of the "Normal" and the "Warning" range are "Errors".

The registration is now complete if the command line argument is not specified for the registering command (script).

When specifying the command line argument, please create and assign the "Parameter" by following the procedures below.

Create the "Parameter" by following the procedures below.

1. Select the "Parameter" in the tree pane on the left side, then click on the "Create" button. A parameter with the name "New" is created.
2. Enter the following items in the area on the right side, then click the "Apply" button.

- Parameter ID:

  Enter an ID to uniquely identify the parameter.

- Name:

  The name entered here is displayed as the parameter in the Collective Run[Parameter] view.

  For example, "Make Directory" in the "Type: File System Management" (this is configured by default) is registered with the name "Directory Name", "User Name", "Group Name", and "File Access Permission".

- Input Type:

  Edit/Select

  Choose either "Edit" or "Select" for the parameter input type.

  - If "Edit" is selected

    The parameter must be entered in alphanumeric text; A text box will appear in the Collective Run[Parameter] view. If Edit is selected, choose either "Appear as text" or "Appear as asterisks". If "Appear as text" is selected, the entered strings will output on screen as entered. If "Appear as asterisks" is selected, the entered strings will be displayed with asterisks "*" (Use "Appear as asterisks" for passwords, when the entered string should not be displayed on screen).

  - If "Select" is selected

    The parameter at the time of collective run can be selected from the list. A list of selections must be registered. Please register a list of selections by the following procedures.

If the "Input Type" of the parameter is "Select", it is necessary to register options by the following procedures (multiple selections can be registered).

1. Select the parameter from the tree pane on the left side, then click the "create" button. An "Option" with the name "Create" is created.
2. Edit the following items in the area on the right side, then click the "Apply" button.

- Name:

  The name entered here is displayed on the selection candidate list as the parameter of the Collective Run[Parameter] view.

- Value: Configure the value when relevant option is selected from the selection list.

  Click the "Close" button, and close the Collective Run[Create/Change] dialog.

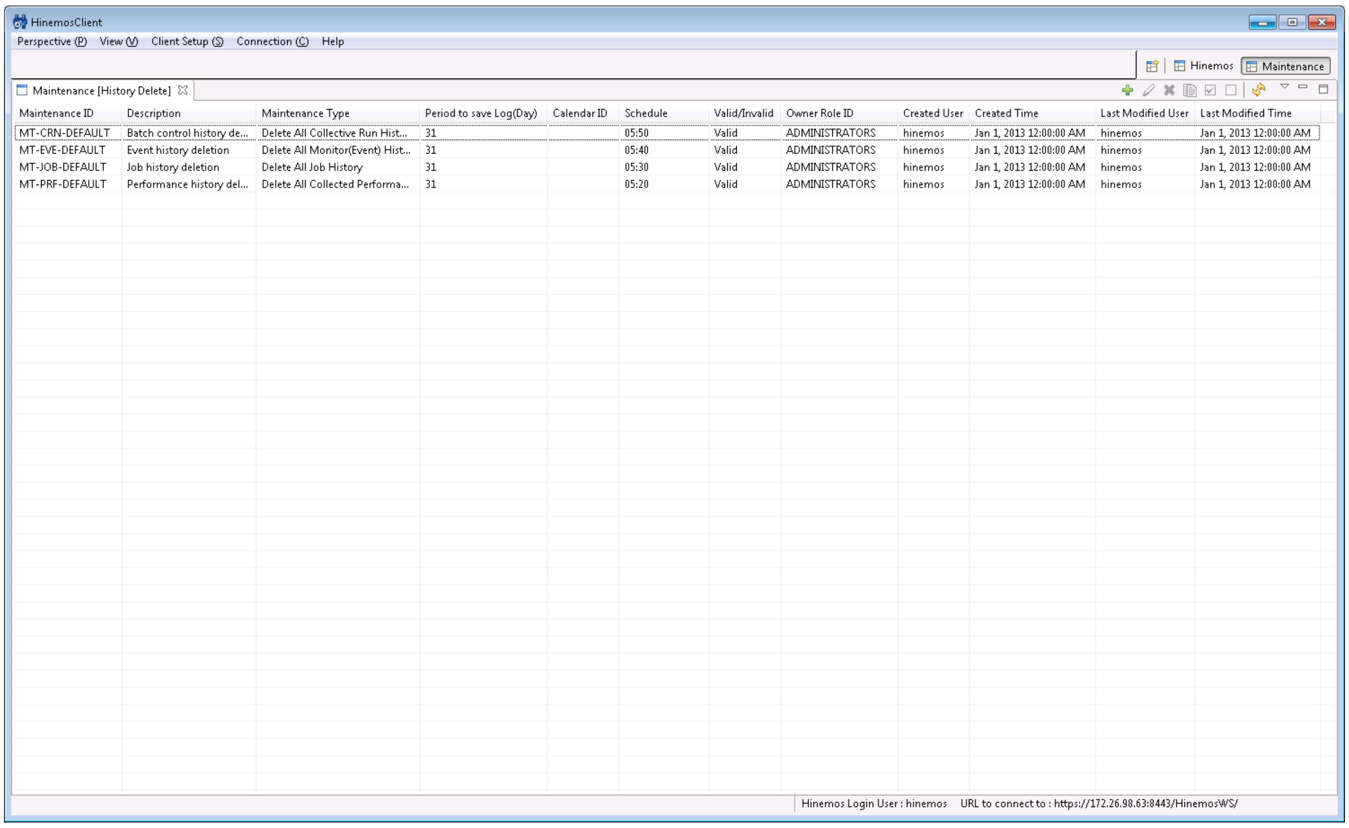
11 Maintenance Feature

11.1 Overview

This feature is used in the administration of Hinemos itself, and is necessary for the operation of Hinemos. This feature is used when deleting historical data stored in Hinemos's internal database.

11.2 Interface Composition

11.2.1 Default Interface



Maintenance ID	Description	Maintenance Type	Period to save Log(Day)	Calendar ID	Schedule	Valid/Invalid	Owner Role ID	Created User	Created Time	Last Modified User	Last Modified Time
MT-CRN-DEFAULT	Batch control history de...	Delete All Collective Run Hist...	31		05:50	Valid	ADMINISTRATORS	hinemos	Jan 1, 2013 12:00:00 AM	hinemos	Jan 1, 2013 12:00:00 AM
MT-EVE-DEFAULT	Event history deletion	Delete All Monitor(Event) Hist...	31		05:40	Valid	ADMINISTRATORS	hinemos	Jan 1, 2013 12:00:00 AM	hinemos	Jan 1, 2013 12:00:00 AM
MT-JOB-DEFAULT	Job history deletion	Delete All Job History	31		05:30	Valid	ADMINISTRATORS	hinemos	Jan 1, 2013 12:00:00 AM	hinemos	Jan 1, 2013 12:00:00 AM
MT-PRF-DEFAULT	Performance history del...	Delete All Collected Performa...	31		05:20	Valid	ADMINISTRATORS	hinemos	Jan 1, 2013 12:00:00 AM	hinemos	Jan 1, 2013 12:00:00 AM

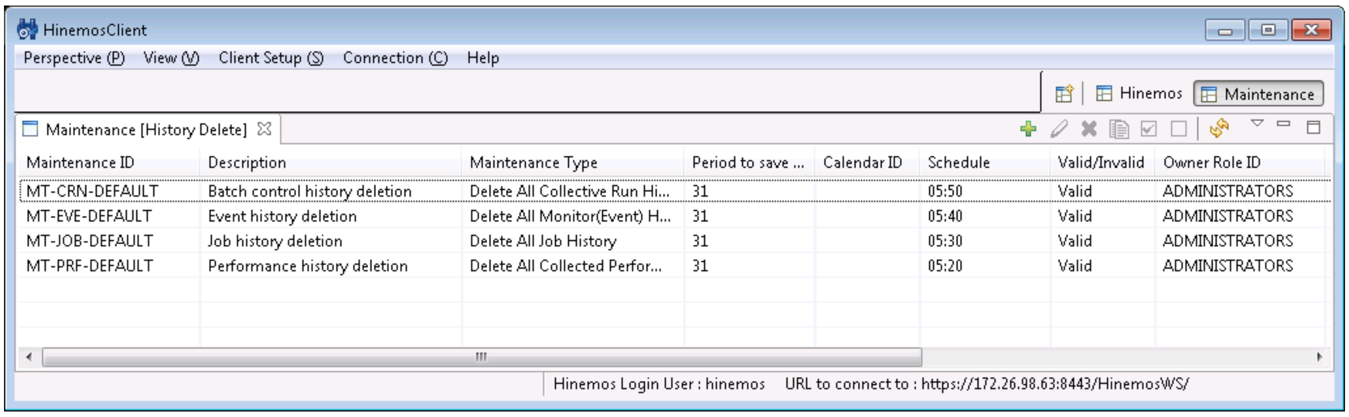
Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 11-1 Default Interface of Maintenance Feature

11.2.2 Maintenance[History Delete] View

This view displays a list of registered history delete settings. History data delete settings can be registered and deleted and operations related to history data delete settings can be performed in this view.

Copyright (c) 2013 NTT DATA CORPORATION


HinemosClient
Perspective (P) View (V) Client Setup (S) Connection (C) Help
Hinemos
Maintenance
Maintenance [History Delete]

Maintenance ID	Description	Maintenance Type	Period to save ...	Calendar ID	Schedule	Valid/Invalid	Owner Role ID
MT-CRN-DEFAULT	Batch control history deletion	Delete All Collective Run Hi...	31		05:50	Valid	ADMINISTRATORS
MT-EVE-DEFAULT	Event history deletion	Delete All Monitor(Event) H...	31		05:40	Valid	ADMINISTRATORS
MT-JOB-DEFAULT	Job history deletion	Delete All Job History	31		05:30	Valid	ADMINISTRATORS
MT-PRF-DEFAULT	Performance history deletion	Delete All Collected Perfor...	31		05:20	Valid	ADMINISTRATORS

Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 11-2 Maintenance[History Delete] View

Table 11-1 Toolbar

Icon	Button name	Description
✚	Create	Create the Delete History Settings.
✎	Change	Change the Delete History Settings.
✖	Delete	Delete the Delete History Settings.
📄	Copy	Copy the Delete History Settings.
☑	Valid	Enable the Delete History Settings. Multiple Delete History Settings can be selected and collectively enabled.
□	Invalid	Disable the Delete History Settings. Multiple Delete History Settings can be selected and collectively disabled.
⟳	Update	The content of the Maintenance[History Delete] view is updated.

11.3 History Data Delete Feature

11.3.1 Feature Summary

The History Data Delete feature periodically deletes the history stored in the Hinemos DB. When history data delete is run, the delete process run date used as a standard to delete the history data older than the retention date.

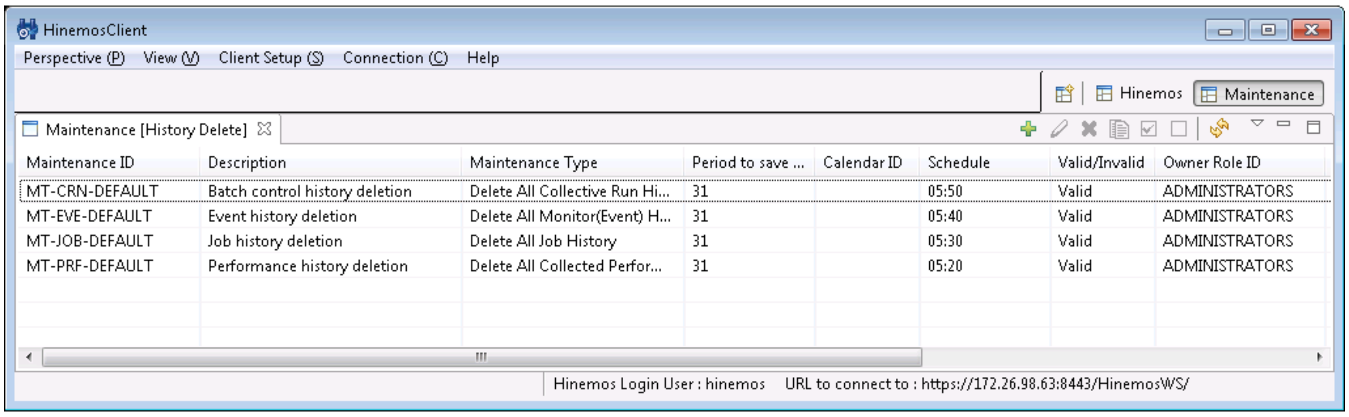
The following 4 histories are subject to deletion.

- Monitor (Event) history ... Information displayed in the Monitor[Event] view
- Job history ... Information displayed in the Job[History] view
- Collective Run history ... Information displayed in the Collective Run[History] view
- Performance Results... Information displayed in the Performance[List] view

11.3.2 Registering History Data Delete Settings

You can register the history data delete settings using the procedure below.

1. Click the "Create" button in the Maintenance[History Delete] view.


HinemosClient
Perspective (P) View (V) Client Setup (S) Connection (C) Help
Hinemos
Maintenance
Maintenance [History Delete]

Maintenance ID	Description	Maintenance Type	Period to save ...	Calendar ID	Schedule	Valid/Invalid	Owner Role ID
MT-CRN-DEFAULT	Batch control history deletion	Delete All Collective Run Hi...	31		05:50	Valid	ADMINISTRATORS
MT-EVE-DEFAULT	Event history deletion	Delete All Monitor(Event) H...	31		05:40	Valid	ADMINISTRATORS
MT-JOB-DEFAULT	Job history deletion	Delete All Job History	31		05:30	Valid	ADMINISTRATORS
MT-PRF-DEFAULT	Performance history deletion	Delete All Collected Perfor...	31		05:20	Valid	ADMINISTRATORS

Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 11-3 Maintenance[History Delete] View

2. The History Delete[Create/Change] dialog will be displayed.

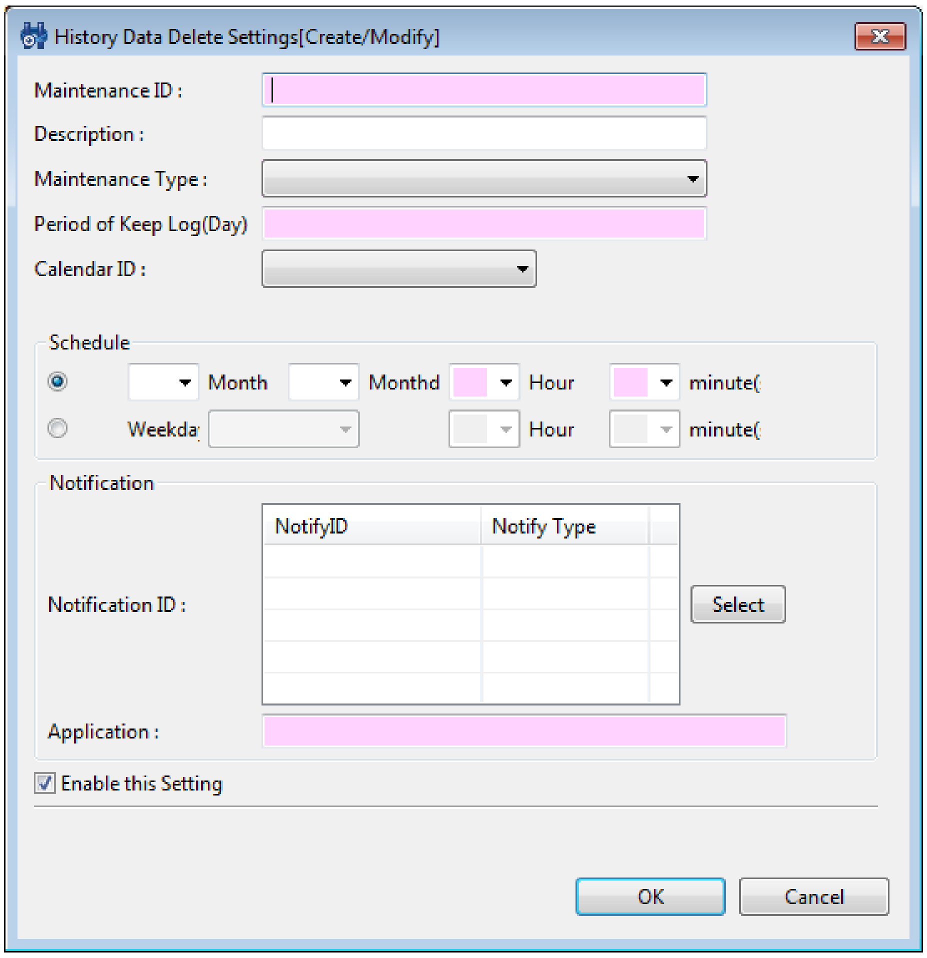


Figure 11-4 History Delete[Create/Change] Dialog

3. Configure the following items.

- Maintenance ID:

  The history data delete settings are specified in a list. Enter the Maintenance ID text.

- Description:

  Enter a description of the history data delete settings as alphanumeric text.

4. Specify the process to run using the history data delete settings.

- Maintenance Type:

  Select the process content from the list below.

Table 11-2 Maintenance Type

Copyright (c) 2013 NTT DATA CORPORATION

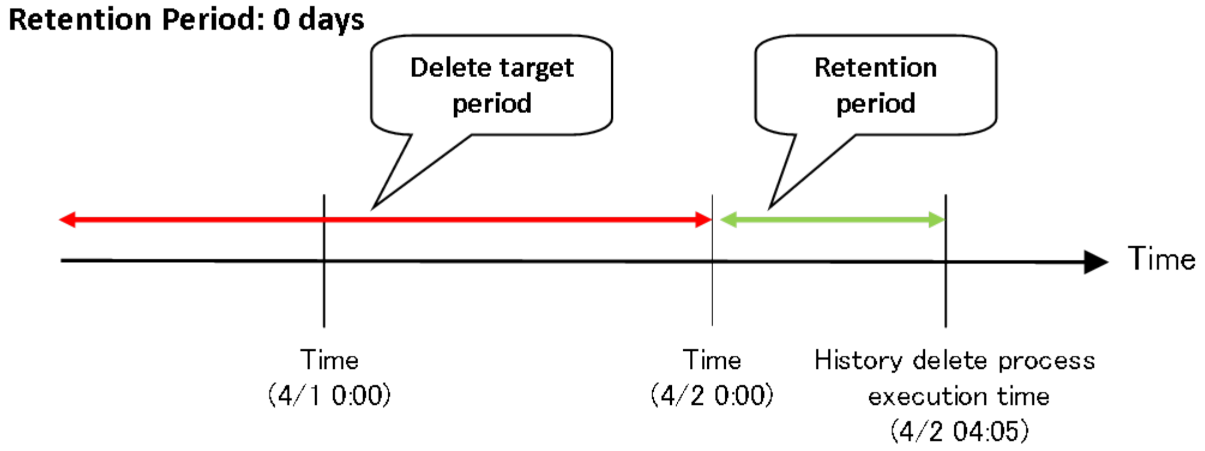
Maintenance Type	Process contents
Delete All Monitor(Event) History	Delete event history
Delete Confirmed Monitor(Event) History	Delete "Confirmed" event history
Delete All Job History	Delete job history
Delete Job History	Delete job history with "End"/"Changed" execution status
Delete All Collective Run History	Delete collective run history
Delete Executed Collective Run History	Delete collective run history with "End" as the execution status
Delete All Collected Performance Data	Delete all collected performance data
Delete Running Performance Data	Delete performance data that is "Collection Running"

- Retention Period:

  You can configure a retention period (a period not subject to deletion) when deleting the history. The retention period is set in 1 day units.

  This setting uses the time the history data delete process is run as a base and deletes the history data that was output at a time outside the retention period.

  Further, if the retention period is "0", all history data prior to 0:00:00 of the day the history data delete process is run is deleted.



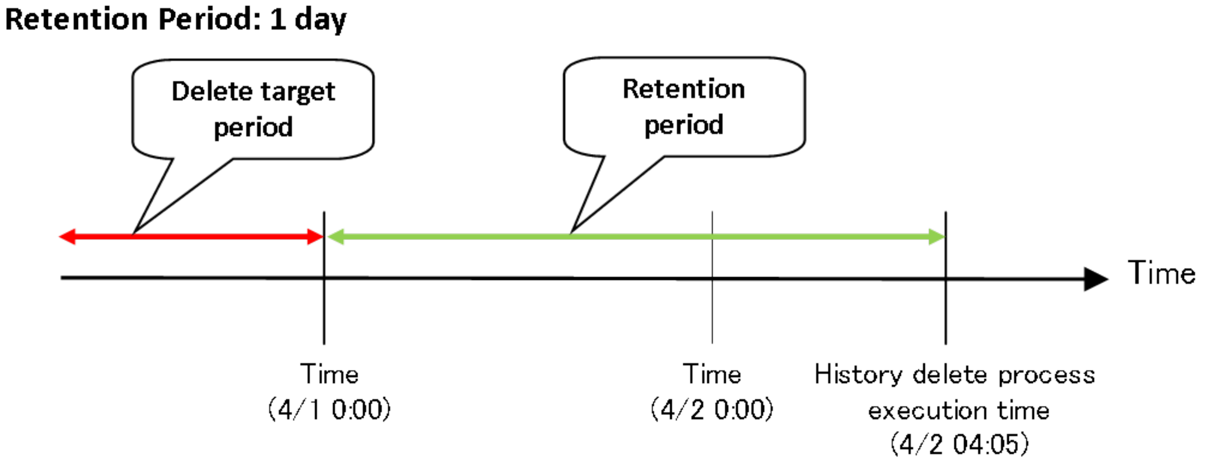


Figure 11-5 Retention Period

- Calendar ID:

  Select the calendar ID for the calendar you want to set up. The history data delete setting will be enabled only during the period configured as working hours on the calendar (Refer to the section, Calendar Feature for more details on the calendar). If Calendar ID is not selected, the filter configuration is enabled throughout the day.

5. Configure the schedule.

   Schedule configuration can be configured with the following two methods.

- Specify "Time"

  The history data delete process is run on the specified date and time. Select "Month", "Day", "Hour", and "minute(s) from each combo box.

- Specify "Weekday"

  The history data delete process execution is scheduled for weekdays. Select "Weekday", "Hour", and "minute(s)" from each combo box.

6. Configure the notification details.

- Notification ID:

  Select from the list the Notification ID that is the notification method used in the notification setting. (Refer to the section Notification Feature regarding notification settings) When you click the "Select" button on the right, the Notification[List] dialog is displayed. Select the notification method.

- Application:

  Enter an application name in alphanumeric text. This is displayed as the notification information.

7. Specify whether to enable this setting. Set it with the check box below.

- Enabling this Setting:

  When checked, the setting is enabled. If unchecked, and it is specified as disabled, the setting is saved, but the history data delete process will not run.

11.3.3 Changing History Data Delete Settings

You can change the history data delete settings with the procedure below.

1. Select the subject to change from the configuration list, and then click the "Modify" button. The History Data Delete Settings[Create/Modify] dialog opens.
2. Edit the setting details, and then click the "OK" button. (Refer to the section, Registering History Data Delete Settings for the procedures for entering settings)

11.3.4 Deleting the History Data Delete Settings

Select the object to delete from the setting list, and then click the "Delete" button.

Copyright (c) 2013 NTT DATA CORPORATION

12 Account Feature

12.1 Overview

The User and Role Management, and the Access Permission Management Feature are offered in the Account Feature.

12.2 User and Role Management

With Hinemos, a user must be registered in advance to operate Hinemos. Also, the registered users are grouped by role and access permission is controlled by group unit. These groups are called Roles.

12.2.1 User Management

With Hinemos, you can control logins to Hinemos by group unit. Also, access permissions are managed flexibly by assigning roles to the users.

Refer to Access Permission Management regarding managing access permissions.

Users (1) and (2) exist under Users.

1. System User A system user is a user registered n advance in Hinemos. The following users exist.

Table 12-1 List of System Users

User Name	Description	Assigned Role
hinemos	Hinemos Super User Must be assigned to a system role and cannot be released	Hinemos Administrator Role All users Role Hinemos internal Role

2. General User A general user is a user registered to use Hinemos. Register in the Account Feature.

12.2.2 Role Management

With Hinemos, registered users are divided into groups and access permissions are controlled by group unit. These groups are called Roles.

Roles (1) and (2) exist under Roles.

1. System Role A system role is a role registered in advance in Hinemos. The following roles exist.

Table 12-2 List of System Roles

Role Name	Initial Setting System Privileges	Whether System Privilege can be changed	Whether Assigned Users can be changed	Description
Hinemos Administrator role (ADMINISTRATORS)	All	No	Yes	Role that can operate all of the settings without conditions The settings that can be changed by this role are just for the users assigned to this role
All users role (ALL_USERS)	All	Yes	No	Role assigned to all Hinemos users Automatically assigned when a user is created Cannot be released from this role
Hinemos internal role (INTERNAL)	All	Yes	No	Role to refer to INTERNAL events

2. General Role A general role is a role registered to Hinemos users. Register in the Account Feature.

Role specific scope

A role specific scope is a scope that is created automatically when the role is created. The role name and scope name are created under the "Owner specific scope" when the role is created. This scope is used when creating a node. The node registered to the owner role and the scope with the same name that is specified when the node is created is automatically assigned.

12.3 Access Permission Management

12.3.1 Privilege Types and Roles

With Hinemos, access can be flexibly controlled by specifying the System Privileges and Object Privileges for each group. The various privileges are described in the next section.

12.3.2 Management by System Privileges

System Privileges manage the Access Permissions for the features of the Repository feature and the Job Management feature.

The four types of system privileges are "Create", "Update", "Refer" and "Run".

- Create... Create configuration information.
- Update... Update or delete configuration information.
- Refer... Refer configuration information.
- Run... Run an operation.

The operations that are controlled by each system privilege for each feature are as follows.

Table 12-3 List of System Privileges

Feature	Privilege	Description
Repository	Create	Can create a node or scope
	Update	Can update or delete a node or scope Assigns/releases a node to a scope Can set the Object Privilege to a scope
	Refer	Can refer a node or scope
	Run	Restarts or updates an agent
Account	Create	Can create a user or role
	Update	Can update or delete a user or role Assigns/releases System Privileges to a role Assigns/releases a user to a scope
	Refer	Can refer a user or role
Monitor results	Update	Deletes the status from the Monitor[Status] view Can change the status of the confirmation flag for the event from the Monitor[Event] view Can edit the comments for the monitor results in the Monitor[Event] view
	Refer	Can refer monitor results
Monitor Setting	Create	Can create the various monitor settings (Ping Monitor or System Log Monitor, etc.)
	Update	Can update or delete the various monitor settings Can change the validity of the various monitor settings Can set the Object Privileges for the various monitor settings
	Refer	Can refer the various monitor settings

Job	Create	Can register a JobUnit, JobNet or Job Can create a FileCheck or Schedule
	Update	Can update or delete a JobUnit, JobNet or Job Can update or delete a FileCheck or Schedule Can set the Object Privileges for a JobUnit Can set the Object Privileges for a FileCheck or Schedule
	Refer	Can refer a JobUnit, JobNet or Job Can refer the execution history of a JobUnit, JobNet or Job Can refer a FileCheck or Schedule
	Run	Can immediately run a JobUnit, JobNet or Job Can operate from the job execution history
Information	Refer	Can refer performance information
Collective Run (*1)	Create	Can create collective run settings
	Update	Can update or delete the collective run settings
	Refer	Can refer the collective run settings
	Run	Can run a collective run
Calendar	Create	Can create a calendar or calendar pattern
	Update	Can update or delete a calendar or calendar pattern Can set the Object Privileges for a calendar or calendar pattern
	Refer	Can refer a calendar or calendar pattern
Notification	Create	Can create various notifications or mail templates
	Update	Can update or delete various notifications or mail templates Can change the validity of various notifications Can set the Object Privileges for various notifications or mail templates
	Refer	Can refer various notifications or mail templates
Maintenance (*1)	Create	Can create maintenance settings
	Update	Can update or delete maintenance settings
	Refer	Can refer maintenance settings

(*1) Can only be operated by users assigned the system administrator role.

12.3.3 Management by the Owner Role

The owner role manages the settings for the Access Permissions for the scope and JobUnit and the various monitor settings. You can control referring and updating from users assigned to other roles by specifying the role as "Owner" when creating the scope and JobUnit and the various monitor settings Further, the user assigned to the role specified as the owner role can perform all operations for the corresponding settings. Specify the system role "All Users Role (ALL_USERS)" if you want all users to be able to operate.

The settings that can be specified for the owner role are as follows.

Table 12-4 List of Settings Specified for Owner

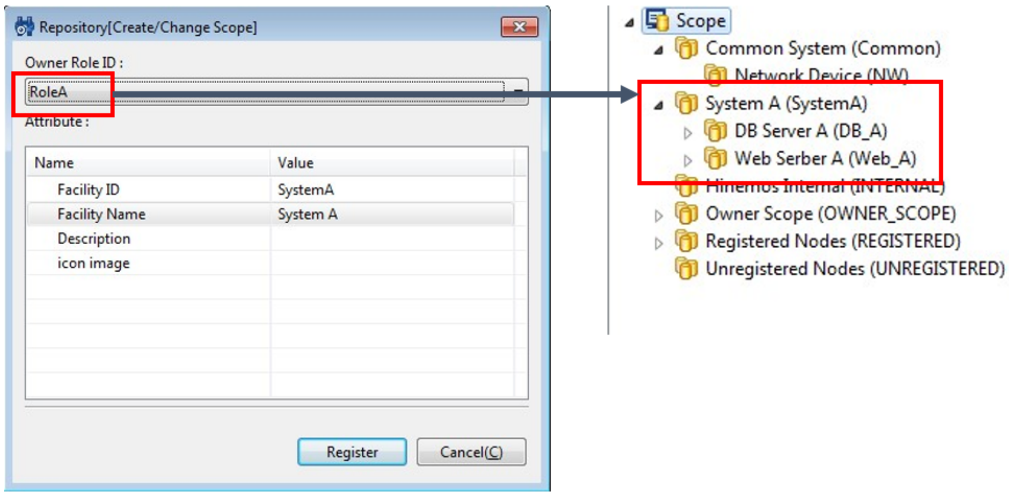
Feature	Settings that can be specified
Repository	Node Scope
Account	—
Monitor results	(Inherits the monitor setting owner)
Monitor Setting	All types of monitor settings
Job	JobUnit (the JobNet and Job inherit the owner role of the JobUnit) FileCheck Job schedule

Performance	(Inherits the monitor setting owner)
Collective Run	—
Calendar	Calendar Calendar Pattern
Notification	All types of notification settings Mail template
Maintenance	—

You can perform the following Access Permissions by specifying the owner role.

Example 1) Access Permissions for a scope

If the RoleA role is specified as the owner role for SystemA scope then users assigned to RoleA can Refer and Update, but other users can't Refer.



Repository[Create/Change Scope]

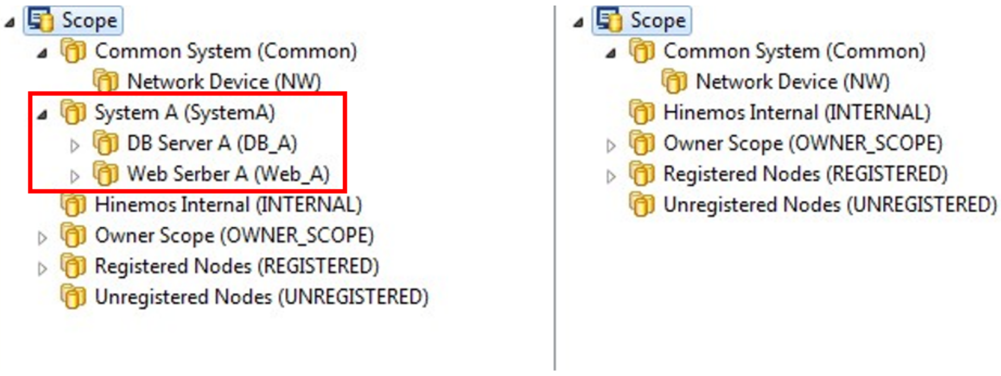
Owner Role ID : RoleA

Attribute :

Name	Value
Facility ID	SystemA
Facility Name	System A
Description	
icon image	

Figure 12-1 Specify an Owner Role for a Scope

By specifying in this manner, you can limit the Refer range of the scope to users assigned to a particular role. (The System Role "All Users Role" (ALL_USERS) is specified as the owner role for the Common scope in the middle of the figure.)



Scope
Common System (Common)
Network Device (NW)
System A (SystemA)
DB Server A (DB_A)
Web Serber A (Web_A)
Hinemos Internal (INTERNAL)
Owner Scope (OWNER_SCOPE)
Registered Nodes (REGISTERED)
Unregistered Nodes (UNREGISTERED)
Scope
Common System (Common)
Network Device (NW)
Hinemos Internal (INTERNAL)
Owner Scope (OWNER_SCOPE)
Registered Nodes (REGISTERED)
Unregistered Nodes (UNREGISTERED)

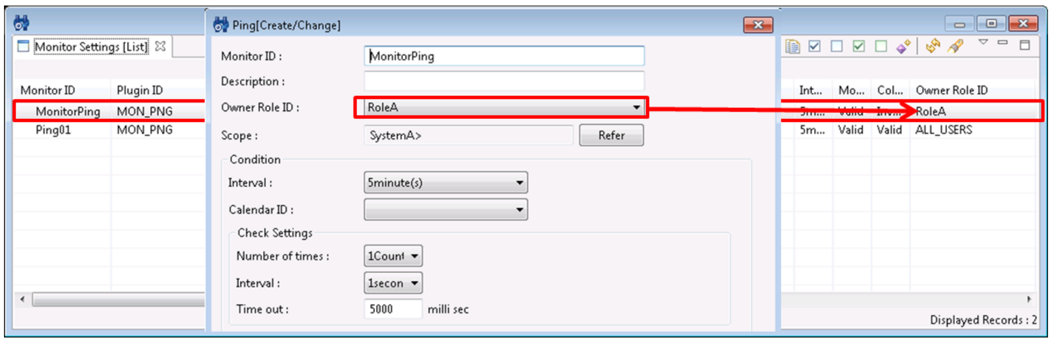
Method of Viewing the Monitor of the Assigned Users for the RoleA Role

Method of Viewing the Monitor of the Unassigned Users for the RoleA Role

Figure 12-2 Method of Viewing Scopes for Each Role

Example 2) Access Permissions for a Monitor Setting

If the RoleA role is specified as the owner role for Monitor Setting MonitorPingA then users assigned to RoleA can Refer and Update, but other users can't Refer.



Monitor Settings [List]

Monitor ID	Plugin ID
MonitorPing	MON_PNG
Ping01	MON_PNG

Ping[Create/Change]

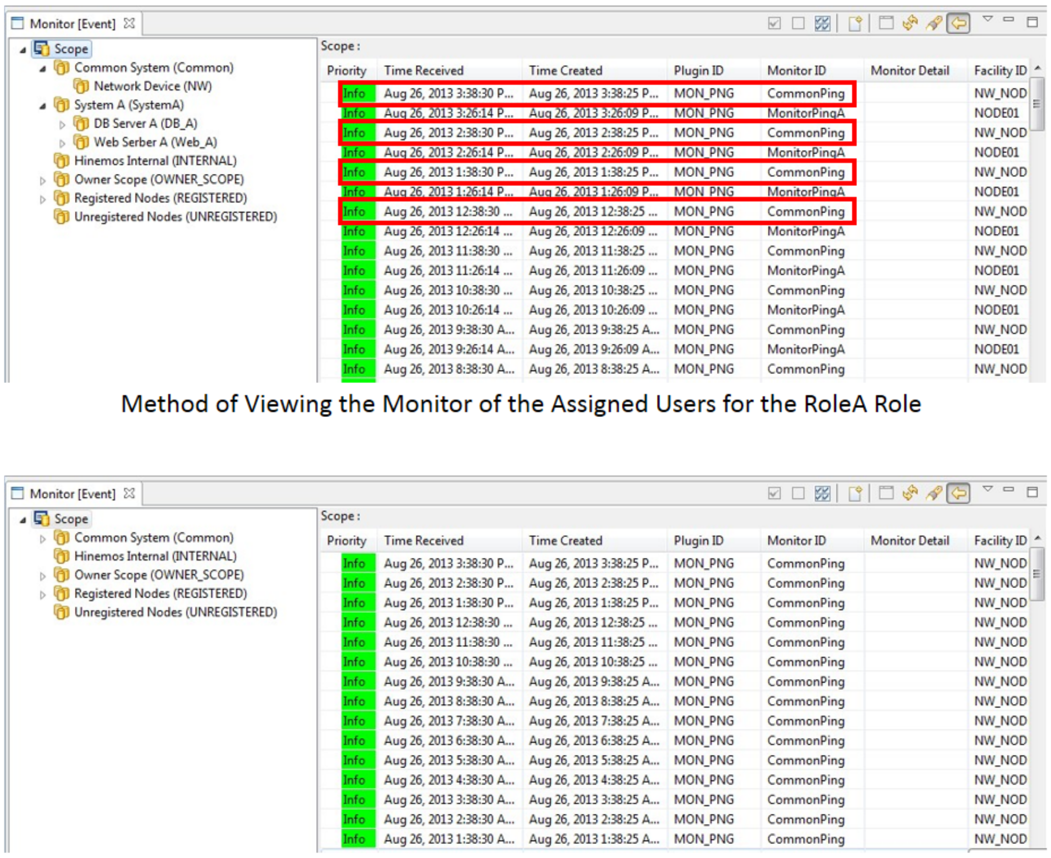
Monitor ID : MonitorPing
Description :
Owner Role ID : RoleA
Scope : SystemA>
Condition
Interval : 5minute(s)
Calendar ID :
Check Settings
Number of times : 1Count
Interval : 1secon
Time out : 5000 milli sec

Int...	Mo...	Col...	Owner Role ID
5m...	Valid	Inv...	RoleA
5m...	Valid	Valid	ALL_USERS

Displayed Records : 2

Figure 12-3 Specify an Owner Role for a Monitor Setting

Also, the monitor results (Status Notification, Event Notification, Job Notification results) for MonitorPing will inherit the same owner role as the Monitor Setting, so you can also limit the Refer range of the monitor results to users assigned to a particular role. (The System Role "All Users Role" (ALL_USERS) is specified as the owner role for the Monitor Setting CommonPing in the middle of the figure.)



Monitor [Event]

- Scope
  - Common System (Common)
    - Network Device (NW)
  - System A (SystemA)
    - DB Server A (DB_A)
    - Web Serber A (Web_A)
  - Hinemos Internal (INTERNAL)
  - Owner Scope (OWNER_SCOPE)
  - Registered Nodes (REGISTERED)
  - Unregistered Nodes (UNREGISTERED)

Scope :

Priority	Time Received	Time Created	Plugin ID	Monitor ID	Monitor Detail	Facility ID
Info	Aug 26, 2013 3:38:30 P...	Aug 26, 2013 3:38:25 P...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 3:26:14 P...	Aug 26, 2013 3:26:09 P...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 2:38:30 P...	Aug 26, 2013 2:38:25 P...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 2:26:14 P...	Aug 26, 2013 2:26:09 P...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 1:38:30 P...	Aug 26, 2013 1:38:25 P...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 1:26:14 P...	Aug 26, 2013 1:26:09 P...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 12:38:30 ...	Aug 26, 2013 12:38:25 ...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 12:26:14 ...	Aug 26, 2013 12:26:09 ...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 11:38:30 ...	Aug 26, 2013 11:38:25 ...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 11:26:14 ...	Aug 26, 2013 11:26:09 ...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 10:38:30 ...	Aug 26, 2013 10:38:25 ...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 10:26:14 ...	Aug 26, 2013 10:26:09 ...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 9:38:30 A...	Aug 26, 2013 9:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 9:26:14 A...	Aug 26, 2013 9:26:09 A...	MON_PNG	MonitorPingA		NODE01
Info	Aug 26, 2013 8:38:30 A...	Aug 26, 2013 8:38:25 A...	MON_PNG	CommonPing		NW_NOD

Method of Viewing the Monitor of the Assigned Users for the RoleA Role

Monitor [Event]

- Scope
  - Common System (Common)
  - Hinemos Internal (INTERNAL)
  - Owner Scope (OWNER_SCOPE)
  - Registered Nodes (REGISTERED)
  - Unregistered Nodes (UNREGISTERED)

Scope :

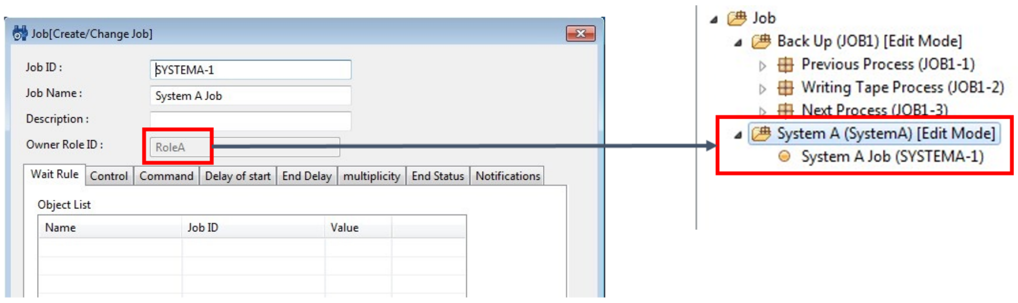
Priority	Time Received	Time Created	Plugin ID	Monitor ID	Monitor Detail	Facility ID
Info	Aug 26, 2013 3:38:30 P...	Aug 26, 2013 3:38:25 P...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 2:38:30 P...	Aug 26, 2013 2:38:25 P...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 1:38:30 P...	Aug 26, 2013 1:38:25 P...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 12:38:30 ...	Aug 26, 2013 12:38:25 ...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 11:38:30 ...	Aug 26, 2013 11:38:25 ...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 10:38:30 ...	Aug 26, 2013 10:38:25 ...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 9:38:30 A...	Aug 26, 2013 9:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 8:38:30 A...	Aug 26, 2013 8:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 7:38:30 A...	Aug 26, 2013 7:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 6:38:30 A...	Aug 26, 2013 6:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 5:38:30 A...	Aug 26, 2013 5:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 4:38:30 A...	Aug 26, 2013 4:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 3:38:30 A...	Aug 26, 2013 3:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 2:38:30 A...	Aug 26, 2013 2:38:25 A...	MON_PNG	CommonPing		NW_NOD
Info	Aug 26, 2013 1:38:30 A...	Aug 26, 2013 1:38:25 A...	MON_PNG	CommonPing		NW_NOD

Method of Viewing the Monitor of the Unassigned Users for the RoleA Role

Figure 12-4 Method of Viewing Monitor Results for Each Role

Example 3) Access Permissions for a JobUnit

If the RoleA role is specified as the owner role for SystemAJob JobUnit then only the users assigned to RoleA can Refer, Update and Run, but other users can't Refer. Further, Access Permissions for Job settings can only be done for JobUnit units.



Job[Create/Change Job]

Job ID : SYSTEMA-1
Job Name : System A Job
Description :
Owner Role ID : RoleA

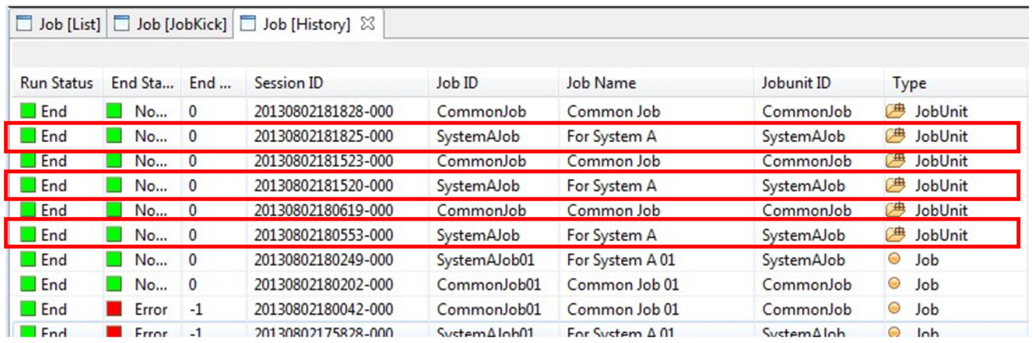
Object List

Name	Job ID	Value

- Job
  - Back Up (JOB1) [Edit Mode]
    - Previous Process (JOB1-1)
    - Writing Tape Process (JOB1-2)
    - Next Process (JOB1-3)
  - System A (SystemA) [Edit Mode]
    - System A Job (SYSTEMA-1)

Figure 12-5 Specify an Owner Role for a JobUnit

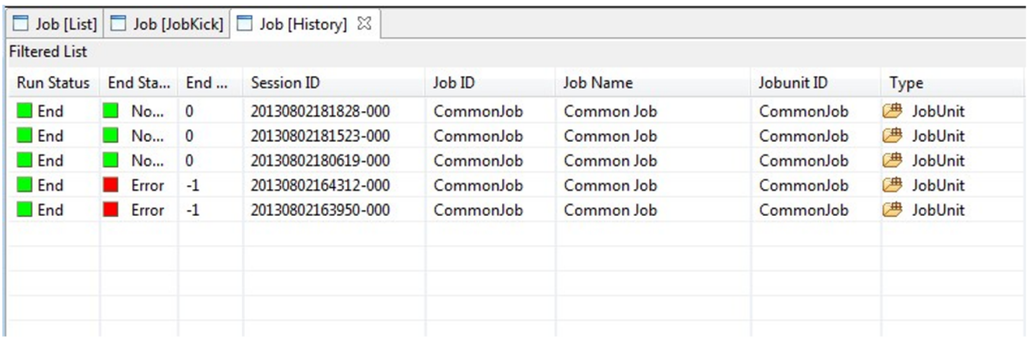
Also, the run history for the SystemAJob JobUnit inherits the same owner role as the JobUnit, so you can also limit the Refer range of the job run history to users assigned to a particular role. (The System Role "All Users Role" (ALL _USERS) is specified as the owner role for the Common JobUnit in the middle of the figure.)



Job [List] | Job [JobKick] | Job [History]

Run Status	End Sta...	End ...	Session ID	Job ID	Job Name	Jobunit ID	Type
🟩 End	🟩 No...	0	20130802181828-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟩 No...	0	20130802181825-000	SystemAJob	For System A	SystemAJob	JobUnit
🟩 End	🟩 No...	0	20130802181523-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟩 No...	0	20130802181520-000	SystemAJob	For System A	SystemAJob	JobUnit
🟩 End	🟩 No...	0	20130802180619-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟩 No...	0	20130802180553-000	SystemAJob	For System A	SystemAJob	JobUnit
🟩 End	🟩 No...	0	20130802180249-000	SystemAJob01	For System A 01	SystemAJob	Job
🟩 End	🟩 No...	0	20130802180202-000	CommonJob01	Common Job 01	CommonJob	Job
🟩 End	🟥 Error	-1	20130802180042-000	CommonJob01	Common Job 01	CommonJob	Job
🟩 End	🟥 Error	-1	20130802175828-000	SystemAJob01	For System A 01	SystemAJob	Job

Method of Viewing the Job History of the Assigned Users for the RoleA Role



Job [List] | Job [JobKick] | Job [History]

Filtered List

Run Status	End Sta...	End ...	Session ID	Job ID	Job Name	Jobunit ID	Type
🟩 End	🟩 No...	0	20130802181828-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟩 No...	0	20130802181523-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟩 No...	0	20130802180619-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟥 Error	-1	20130802164312-000	CommonJob	Common Job	CommonJob	JobUnit
🟩 End	🟥 Error	-1	20130802163950-000	CommonJob	Common Job	CommonJob	JobUnit

Method of Viewing the Job History of the Unassigned Users for the RoleA Role

Figure 12-6 Method of Viewing Job Run History for Each Role

12.3.4 Managing by Object Privileges

The Object Privileges manage the Access Permissions for the settings in the scope and JobUnit and the various monitor settings. You can specify Access Permissions for roles other than owner roles described in the prior item. "Update", "Refer" and "Run" are the three types of settings that can be specified for the settings (excluding nodes) for owner roles for Object Privileges.

- Update... Update or delete configuration information.
- Refer... Refer configuration information.
- Run... Run an operation.

The Object Privileges that can be specified are as follows.

Table 12-5 List of Object Privileges

Feature	Object Privileges	Privileges	Description
Repository	Node	—	(Cannot set)
	Scope	Update	Can update or delete the scope settings Assigns/releases a node of a scope Can set the Object Privilege of a scope
		Refer	Can Refer the scope tree contained under the corresponding scope
Account	—	—	—

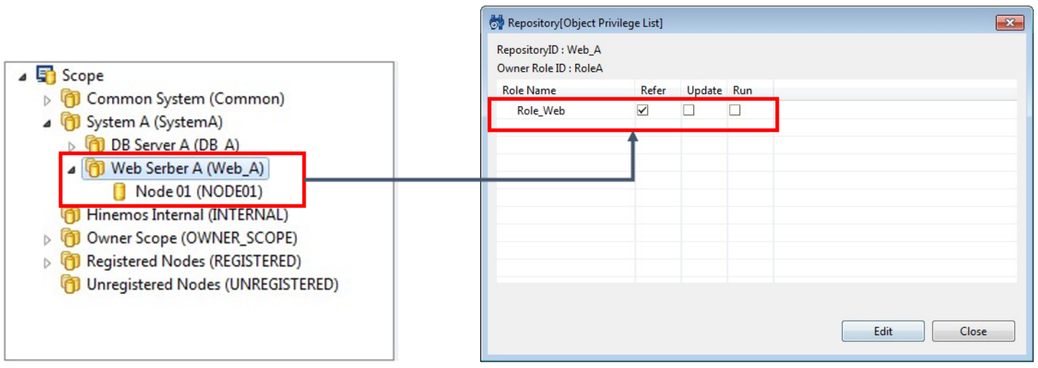
Copyright (c) 2013 NTT DATA CORPORATION

Monitor results	Monitor results (Inherits the Object Settings of the Monitor Setting)	Update	Deletes the status from the Monitor[Status] view Can change the status of the confirmation flag for the event from the Monitor[Event] view Can edit the comments for the monitor results in the Monitor[Event] view
		Refer	Can refer monitor results
Monitor Setting	Monitor Setting	Update	Can update or delete the monitor settings Can change the validity of the monitor settings Can set the Object Privileges for the monitor settings
		Refer	Can refer monitor settings
Job	JobUnit	Update	Can update or delete a JobUnit, JobNet or Job Can set the Object Privileges for a JobUnit
		Refer	Can refer a JobUnit, JobNet or Job Can refer the execution history of a JobUnit, JobNet or Job
		Run	Can immediately run a JobUnit, JobNet or Job Can operate from the job execution history
	FileCheck Schedule	Update	Can update or delete a FileCheck or Schedule Can set the Object Privileges for a FileCheck or Schedule
		Refer	Can refer a FileCheck or Schedule
Performance	Performance information (Inheritance the Object Privileges of the Monitor Setting)	Refer	Can refer performance information
Collective Run	－	－	－
Calendar	Calendar Calendar Pattern	Update	Can update or delete a calendar or calendar pattern Can set the Object Privileges for a calendar or calendar pattern
		Refer	Can refer a calendar or calendar pattern
Notification	Notification setting Mail template	Update	Can update or delete various notifications or mail templates Can change the validity of the notification settings Can set the Object Privileges for notification settings or mail templates
		Refer	Can refer notification settings or mail templates
Maintenance	－	－	－

You can perform access control for roles other than the owner role by setting the Object Privileges as follows. Further, refer to Object Privilege Settings for the method of setting Object Privileges.

Example 1) Access Permission when you only want to Refer subordinate to a particular scope.

When there is a scope structure (the owner role is all of RoleA roles) for WebA scope and DB_A scope under the SystemA scope, only users who belong to RoleA role can Refer and Update. At this time, if you want to Refer to the RoleWeb role to manage the Web server only under the WebA scope, set the "Refer" Object Privileges of the RoleWeb role for the WebA scope.

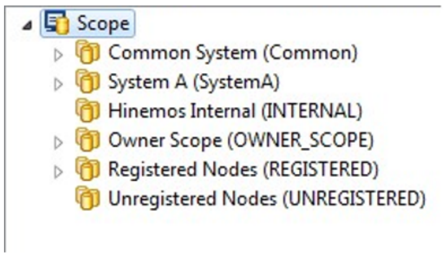

Scope
Common System (Common)
System A (SystemA)
DB Server A (DB_A)
Web Serber A (Web_A)
Node 01 (NODE01)
Hinemos Internal (INTERNAL)
Owner Scope (OWNER_SCOPE)
Registered Nodes (REGISTERED)
Unregistered Nodes (UNREGISTERED)
Repository[Object Privilege List]
Edit
Close

RepositoryID : Web_A
Owner Role ID : RoleA

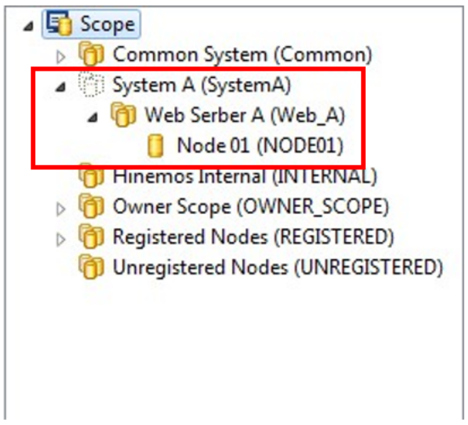
Role Name	Refer	Update	Run
Role_Web	☑	□	□

Figure 12-7 Setting "Refer" Object Privileges for a Particular Scope

You can Refer to just things under a particular scope (WebA scope) and not the entire SystemA scope by performing settings in this manner.


Scope
Common System (Common)
System A (SystemA)
Hinemos Internal (INTERNAL)
Owner Scope (OWNER_SCOPE)
Registered Nodes (REGISTERED)
Unregistered Nodes (UNREGISTERED)

Method of Viewing the Monitor of the Assigned Users for the RoleWeb Role (Before the Object Privilege Settings)


Scope
Common System (Common)
System A (SystemA)
Web Serber A (Web_A)
Node 01 (NODE01)
Hinemos Internal (INTERNAL)
Owner Scope (OWNER_SCOPE)
Registered Nodes (REGISTERED)
Unregistered Nodes (UNREGISTERED)

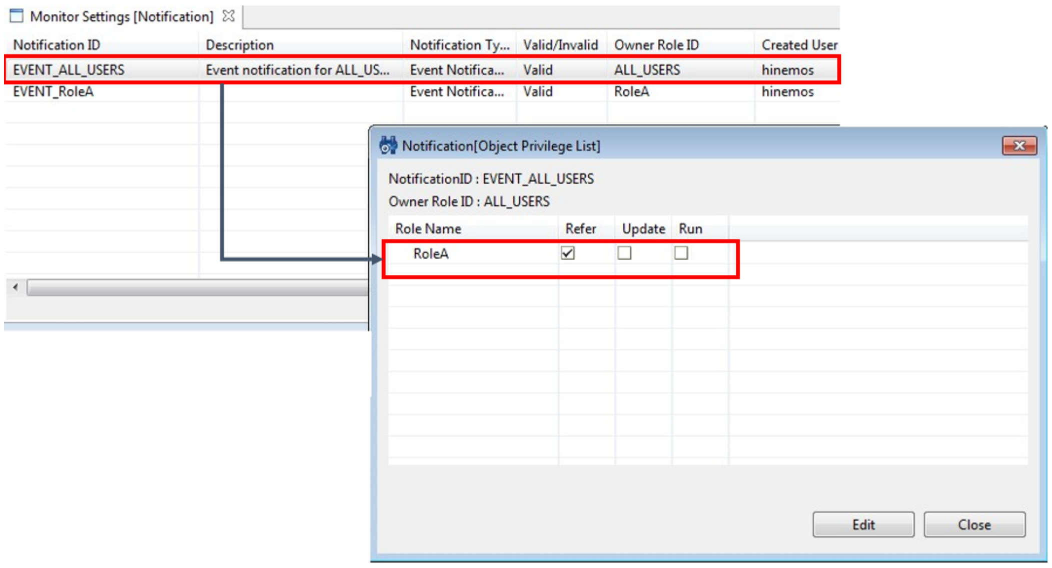
Method of Viewing the Monitor of the Assigned Users for the RoleWeb Role (Following the Object Privilege Settings)

Figure 12-8 Method of Viewing the Scope of the Assigned Users for the RoleWeb Role

Further, scopes such as SystemA shown with a dotted line, like in the above figure, can be specified at the time of various monitor settings or job settings.

Example 2) Access Permissions for common settings (Repository, Notification, Calendar) referred to when regis tering monitor settings.

If the RoleA role is specified as the owner role for Monitor Setting MonitorPing then the owner role is RoleA and only common settings can be selected when setting. If you want to select common settings when setting MontiorP ing, where a role other than RoleA is the owner role, set the "Refer" Object Privileges of the RoleA role for the t arget common settings.


Monitor Settings [Notification]

Notification ID	Description	Notification Ty...	Valid/Invalid	Owner Role ID	Created User
EVENT_ALL_USERS	Event notification for ALL_US...	Event Notifica...	Valid	ALL_USERS	hinemos
EVENT_RoleA		Event Notifica...	Valid	RoleA	hinemos

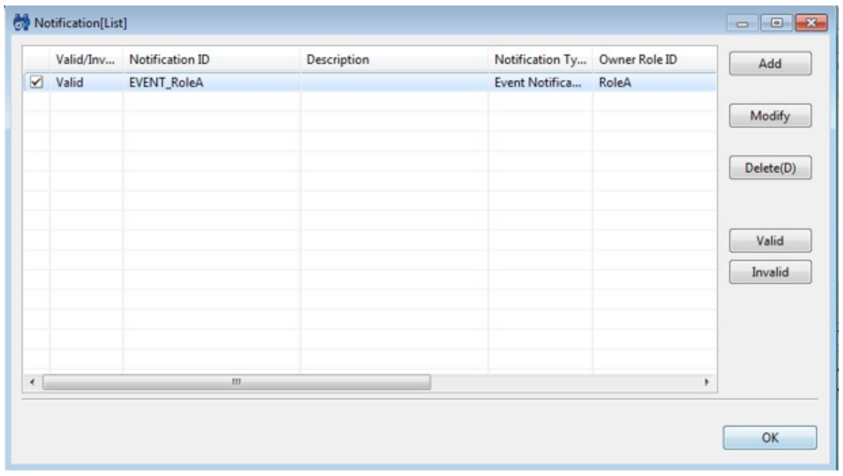
Notification[Object Privilege List]

NotificationID : EVENT_ALL_USERS
Owner Role ID : ALL_USERS

Role Name	Refer	Update	Run
RoleA	☑	□	□

Figure 12-9 Setting "Refer" Object Privileges for the Notification Settings

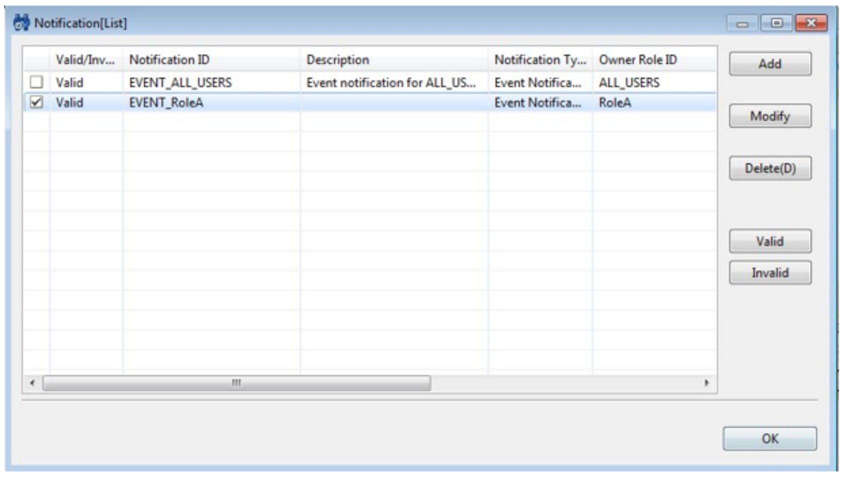
With these settings, you can refer to common settings of a different owner role when setting MonitorPing.



Notification[List]

	Valid/Inv...	Notification ID	Description	Notification Ty...	Owner Role ID
☑	Valid	EVENT_RoleA		Event Notifica...	RoleA

Notification Settings for MonitorPingA
(Before the Object Privilege Settings)



Notification[List]

	Valid/Inv...	Notification ID	Description	Notification Ty...	Owner Role ID
☐	Valid	EVENT_ALL_USERS	Event notification for ALL_US...	Event Notifica...	ALL_USERS
☑	Valid	EVENT_RoleA		Event Notifica...	RoleA

Notification Settings for MonitorPingA
(Before the Object Privilege Settings)

Figure 12-10 Method to View the Notification Settings Following the Object Privilege Settings

Object Privilege settings of Built-in Scope

Right after installing Hinemos Manager, Owner Role and Object Privilege settings of Built-in Scopes are as listed below.

Table 12-6 Object Privilege of Built-in Scope

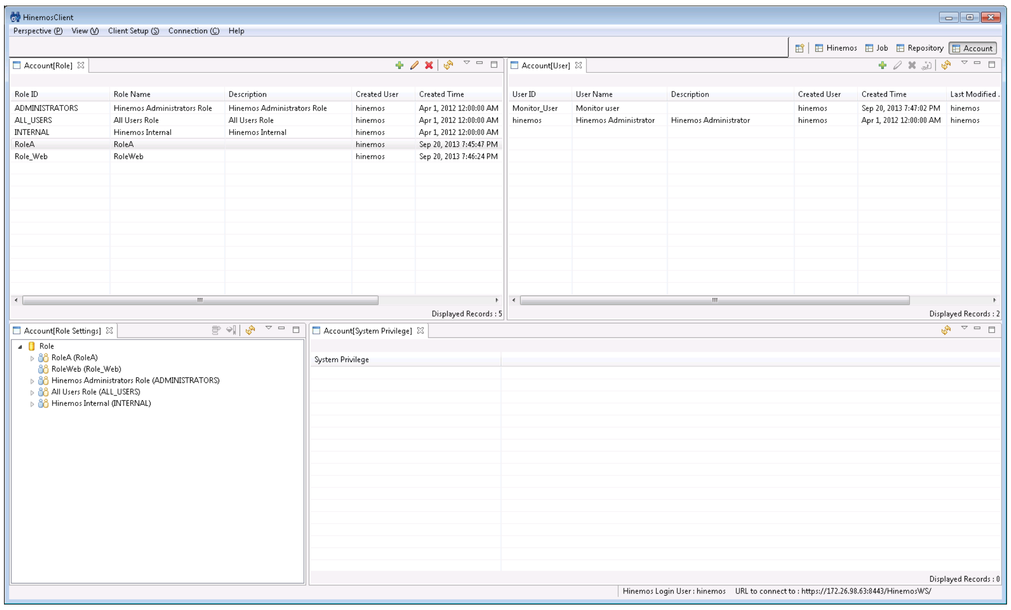
Built-in Scope Name	Owner Role Name	Role with Object Privilege
Owner Scope (OWNER_SCOPE)	Hinemos Administrators Role (ADMINISTRATORS)	—
Hinemos Internal (INTERNAL)	Hinemos Internal (INTERNAL)	All Users Role (ALL_USERS)
Registered Nodes (REGISTERED)	Hinemos Administarotrs Role (ADMINISTRATORS)	All Users Role (ALL_USERS)
Unregistered Nodes (UNREGISTERED)	Hinemos Administartors Role (ADMINISTRATORS)	All Users Role (ALL_USERS)

Right after installing Hinemos Manager, in order to make all node accessible without considering the belonging role, all the Built-in Scope except Owner Scope is set with an Object Privilege of "All Users Role".

Because of this, in order to use "Role" to restrict READ-Privileges of scopes, remove object privileges of buil-in scopes, especially Registered Nodes scope.

12.4 Interface Composition

12.4.1 Default Interface


HinemosClient
Perspective (P) View (V) Client Setup (S) Connection (C) Help
Hinemos Job Repository Account
Account[Role]
Account[User]
Account[Role Settings]
Account[System Privilege]

Role ID	Role Name	Description	Created User	Created Time
ADMINISTRATORS	Hinemos Administrators Role	Hinemos Administrators Role	hinemos	Apr 1, 2012 12:00:00 AM
ALL_USERS	All Users Role	All Users Role	hinemos	Apr 1, 2012 12:00:00 AM
INTERNAL	Hinemos Internal	Hinemos Internal	hinemos	Apr 1, 2012 12:00:00 AM
RoleA	RoleA		hinemos	Sep 20, 2013 7:45:47 PM
Role_Web	RoleWeb		hinemos	Sep 20, 2013 7:46:24 PM

Displayed Records : 5

User ID	User Name	Description	Created User	Created Time	Last Modified ...
Monitor_User	Monitor user		hinemos	Sep 20, 2013 7:47:02 PM	hinemos
hinemos	Hinemos Administrator	Hinemos Administrator	hinemos	Apr 1, 2012 12:00:00 AM	hinemos

Displayed Records : 2

- Role
  - RoleA (RoleA)
  - RoleWeb (Role_Web)
  - Hinemos Administrators Role (ADMINISTRATORS)
  - All Users Role (ALL_USERS)
  - Hinemos Internal (INTERNAL)

System Privilege

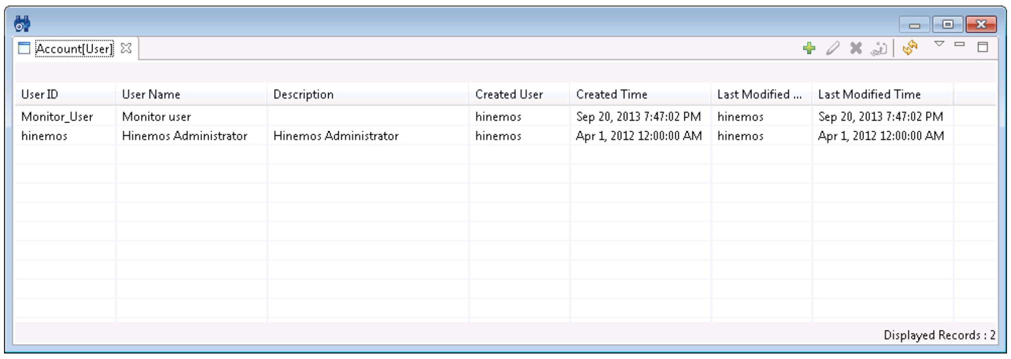
Displayed Records : 0

Hinemos Login User : hinemos URL to connect to : https://172.26.98.63:8443/HinemosWS/

Figure 12-11 Default Interface of Account Feature

12.4.2 Account[User] View

This is the view to manage Hinemos users. The view displays a list of users. If there is no permission for "Account - READ" then only the user login information will be displayed. Users can be created/deleted and configuration inform ation can be changed.



User ID	User Name	Description	Created User	Created Time	Last Modified ...	Last Modified Time
Monitor_User	Monitor user		hinemos	Sep 20, 2013 7:47:02 PM	hinemos	Sep 20, 2013 7:47:02 PM
hinemos	Hinemos Administrator	Hinemos Administrator	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM

Displayed Records : 2

Figure 12-12 Account[User] View

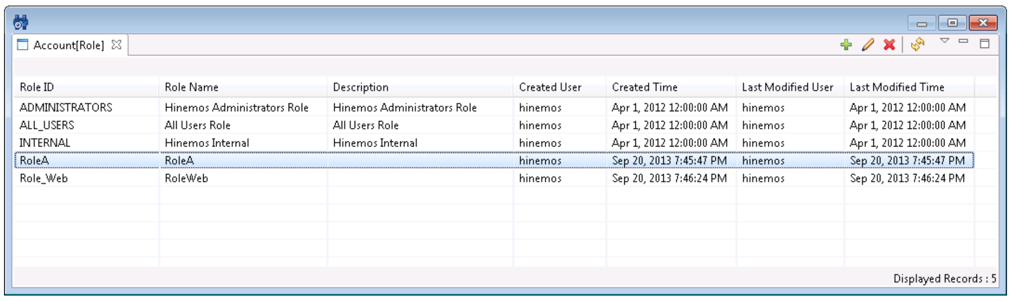
Table 12-7 Toolbar

Icon	Button name	Description
✚	Create	Create user information.
✎	Modify	Modify user information.
✖	Delete	Delete user information.
🔒	Change Passwor d	Change user password.
⟳	Update	Update the contents of the Account[User] view.

Copyright (c) 2013 NTT DATA CORPORATION

12.4.3 Account[Role] View

This is the view to manage roles. The view displays a list of roles. Roles can be created/deleted and configuration information can be changed.



Role ID	Role Name	Description	Created User	Created Time	Last Modified User	Last Modified Time
ADMINISTRATORS	Hinemos Administrators Role	Hinemos Administrators Role	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
ALL_USERS	All Users Role	All Users Role	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
INTERNAL	Hinemos Internal	Hinemos Internal	hinemos	Apr 1, 2012 12:00:00 AM	hinemos	Apr 1, 2012 12:00:00 AM
RoleA	RoleA		hinemos	Sep 20, 2013 7:45:47 PM	hinemos	Sep 20, 2013 7:45:47 PM
Role_Web	RoleWeb		hinemos	Sep 20, 2013 7:46:24 PM	hinemos	Sep 20, 2013 7:46:24 PM

Displayed Records : 5

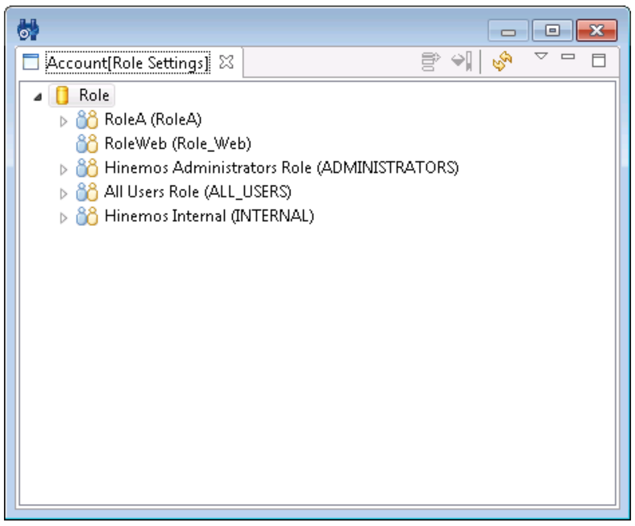
Figure 12-13 Account[Role] View

Table 12-8 Toolbar

Icon	Button name	Description
✚	Create	Create role information.
✎	Modify	Modify role information.
✖	Delete	Delete role information.
⟳	Update	Update the contents of the Account[Role] view.

12.4.4 Account[Role Settings] View

This is the view to manage the user information and System Privilege information for the roles. The roles and users who are assigned to the roles are shown in a tree structure. System Privileges can be allocated/released from roles and users can be assigned/released.



- Role
  - RoleA (RoleA)
  - RoleWeb (Role_Web)
  - Hinemos Administrators Role (ADMINISTRATORS)
  - All Users Role (ALL_USERS)
  - Hinemos Internal (INTERNAL)

Figure 12-14 Account[Role Settings] View

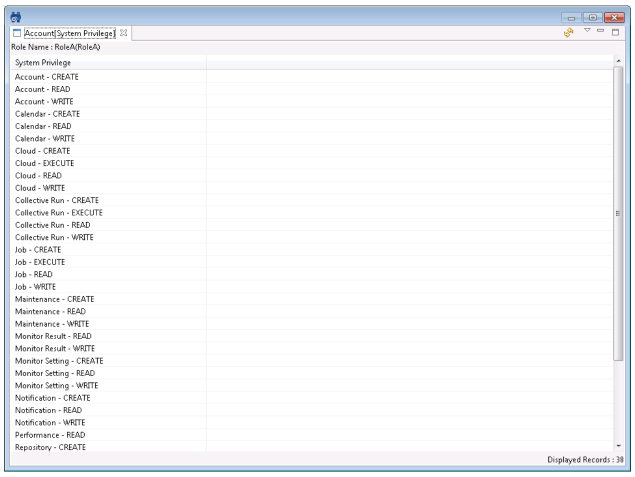
Table 12-9 Toolbar

Icon	Button name	Description
☰	User assignment settings	Change the user information assigned to a role.
◆	System Privilege settings	Change the System Privilege information allocated to a role.
⟳	Update	Update the contents of the Account[Role Settings] view.

Copyright (c) 2013 NTT DATA CORPORATION

12.4.5 Account[System Privilege] View

This is the view to confirm the System Privileges allotted to roles and users. This displays the System Privileges allocated to the roles and users selected in the Account[Role Settings] view. This displays the applied details of the information for all roles that are assigned when displaying the information related to a user.



Role Name : RoleA(RoleA)

System Privilege
Account - CREATE
Account - READ
Account - WRITE
Calendar - CREATE
Calendar - READ
Calendar - WRITE
Cloud - CREATE
Cloud - EXECUTE
Cloud - READ
Cloud - WRITE
Collective Run - CREATE
Collective Run - EXECUTE
Collective Run - READ
Collective Run - WRITE
Job - CREATE
Job - EXECUTE
Job - READ
Job - WRITE
Maintenance - CREATE
Maintenance - READ
Maintenance - WRITE
Monitor Result - READ
Monitor Result - WRITE
Monitor Setting - CREATE
Monitor Setting - READ
Monitor Setting - WRITE
Notification - CREATE
Notification - READ
Notification - WRITE
Performance - READ
Repository - CREATE

Displayed Records : 38

Figure 12-15 Account[System Privilege] View

Table 12-10 Toolbar

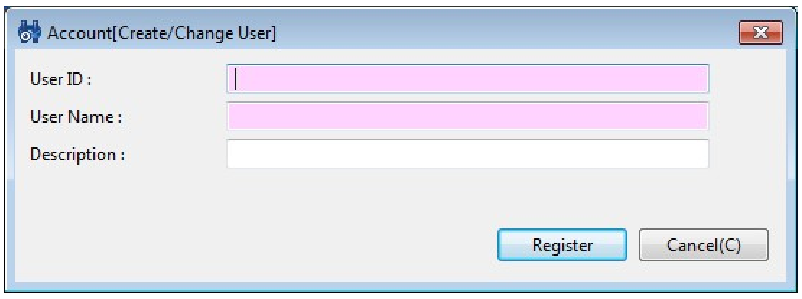
Icon	Button name	Description
↻	Update	Update the contents of the Account[System Privileges] view.

12.5 User Set Up

12.5.1 User Registration

Users with "Account - CREATE" privileges can create users. Create a user with the procedure below.

1. Click the "Create" button in the Account[User] view. This opens the Account[Create/Change User] dialog.



User ID :

User Name :

Description :

Figure 12-16 Account[Create/Change Calendar] Dialog

2. Enter the attribute information. User ID and User Name are required attribute information and must be entered. (Specify them with up to 64 single byte alphanumeric characters or symbols "-", "_". Multi byte characters are not permitted.) In addition, make the user ID unique on the system. You cannot register duplicate user IDs.
3. Click the "Register" button. Password set up is required for the created user to login. The password setup is done with Change Password.

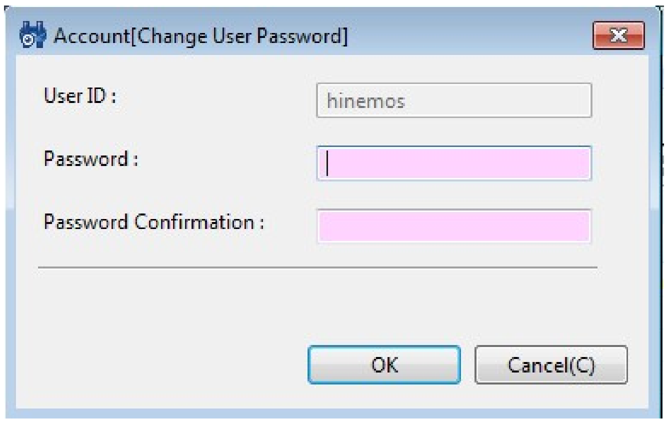
12.5.2 Changing Password

Users with "Account - WRITE" permission can change passwords. Also, login users can change their own passwords. Login users who change their own password will be automatically logged out. Re-login with the changed password.

Password can be changed with the procedures below.

Copyright (c) 2013 NTT DATA CORPORATION

1. Select the user to change from the user list table in Account[User] view and then click the "Change Password" button. This opens the Account[Change User Password] dialog.



Account[Change User Password]

User ID : hinemos

Password :

Password Confirmation :

Figure 12-17 Account[Change User Password] Dialog

2. Enter a password in the Password field. (Up to 64 characters can be specified. Multi byte characters are not permitted.)
3. Re-enter the password in the Password Confirmation field.
4. Click the "OK" button.

12.5.3 Changing User Information

Users with "Account - WRITE" permission can change user information. Also, login users can change their own user information.

User information can be changed with the procedure below.

1. Select the user to change from the user list table in Account[User] view and then click the "Modify" button. This opens the Account[Create/Change User] dialog.
2. Edit the attribute information.
3. Click the "Modify" button.

12.5.4 Deleting a User

Users with "Account - WRITE" permission can delete users. Further, login users cannot delete themselves.

Delete a user by following the procedures bellow.

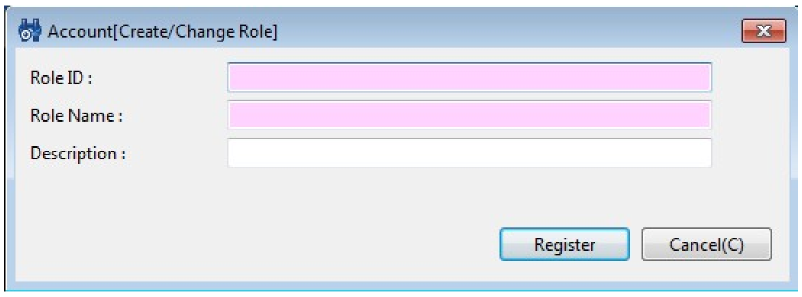
1. Select the user to delete from the user list table in Account[User] view and then click the "Delete" button. A confirmation dialog opens.
2. Click the "OK" button.

12.6 Role Set Up

12.6.1 Role Registration

Users with "Account - CREATE" permission can create roles. Create a user with the procedure below.

1. Click the "Create" button in the Account[Role] view. This opens the Account[Create/Change Role] dialog.



Account[Create/Change Role]

Role ID :

Role Name :

Description :

Figure 12-18 Account[Create/Change Role] Dialog

2. Enter the attribute information. Role ID and Role Name are required attribute information and must be entered. (Specify them with up to 64 single byte alphanumeric characters or symbols "-", "_". Multi byte characters are not permitted.) In addition, make the Role ID unique on the system. Also you can't register duplicate Node, Sco pe or Facility IDs.
3. Click the "Register" button. Specify the assigned users for the created role and assign System Privileges in the Account[Role Settings] view.

12.6.2 Changing Role Information

Users with "Account - WRITE" permission can change role information.

Role information can be changed with the procedure below.

1. Select the role to change from the role list table in Account[Role] view and then click the "Modify" button. Thi s opens the Account[Create/Change Role] dialog.
2. Edit the attribute information.
3. Click the "Modify" button.

12.6.3 Delete Role

Roles with "Account - WRITE" permission can delete roles. Further, roles that have assigned users and roles specifie d as owner roles can't be deleted.

Delete roles by following the procedure below.

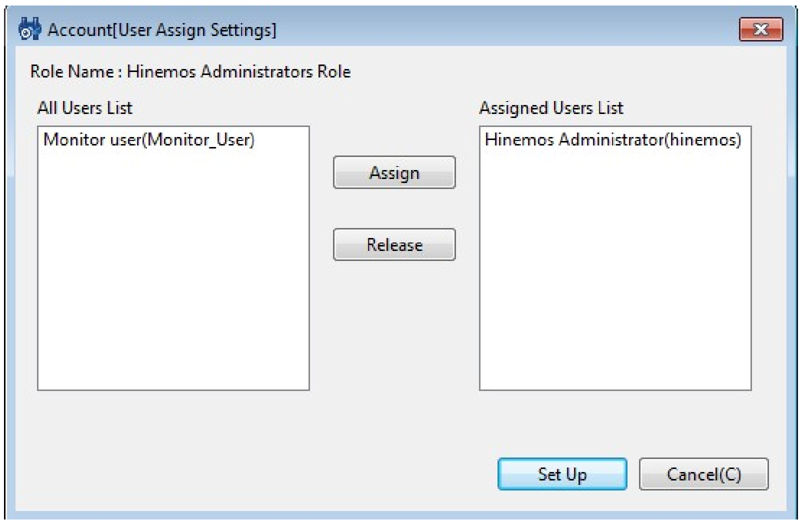
1. Select the role to delete from the role list table in Account[Role] view and then click the "Delete" button. A c onfirmation dialog opens.
2. Click the "OK" button.

12.6.4 User Assign Settings

Users with "Account - WRITE" permission can delete user assign settings.

Specify users assigned to a role with the following procedure.

1. Select the role you want to assign users to from the role tree in the Account[Role Settings] view. Then click t he "User Assign Settings" button. This opens the Account[User Assign Settings] dialog.



Account[User Assign Settings]

Role Name : Hinemos Administrators Role

All Users List

Monitor user(Monitor_User)

Assigned Users List

Hinemos Administrator(hinemos)

Figure 12-19 Account[User Assign Settings] Dialog

2. Select the user to be assigned from the All Users List and click the "Assign" button. Or, select the user to be assigned from the Assigned Users List and click the "Assign" button.

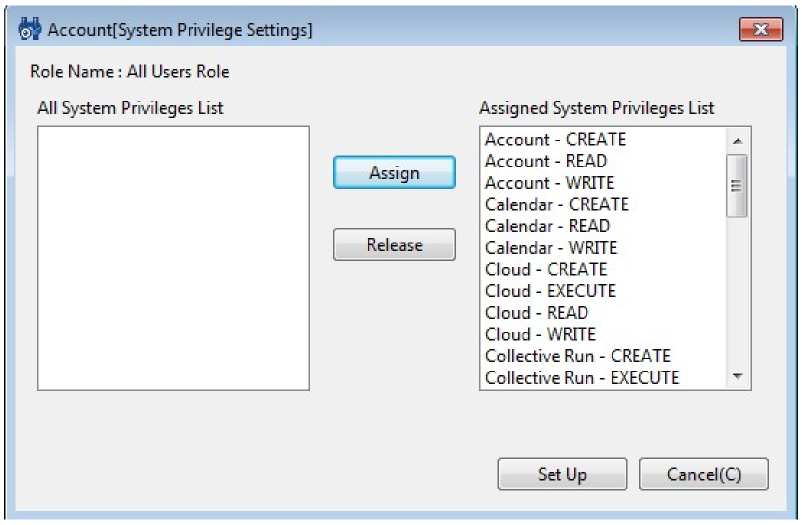
3. Click the "Set Up" button to confirm the users that have been assigned in the Assigned Users List.

12.6.5 System Privileges Settings

Users with "Account - WRITE" permission can set up System Privileges.

System Privileges are assigned to Roles with the following procedure.

1. Select the role you want to set System Privileges for from the role tree in the Account[Role Settings] view. Then click the "System Privilege" button. This opens the Account[System Privilege Settings] dialog.



Account[System Privilege Settings]

Role Name : All Users Role

All System Privileges List

Assigned System Privileges List

Account - CREATE
Account - READ
Account - WRITE
Calendar - CREATE
Calendar - READ
Calendar - WRITE
Cloud - CREATE
Cloud - EXECUTE
Cloud - READ
Cloud - WRITE
Collective Run - CREATE
Collective Run - EXECUTE

Figure 12-20 Account[System Privilege Settings] Dialog

2. Select the System Privilege you want to assign from the All System Privileges List and click the "Assign" button. Also, you can select the System Privileges you want to release from the All System Privileges List and click the "Release" button.
3. Click the "Set Up" button to confirm all of the System Privileges that are assigned in the Assigned System Privileges List.

12.7 Owner Role Set Up

The Owner role is set up when a Scope, JobUnit or Monitor Setting, etc. is registered. The owner role can't be changed once it is registered. Roles that can be specified as owner roles become roles that are assigned to the login user. (All roles can be specified if the login user is assigned the "Hinemos administrator role (ADMINISTRATORS)")

Refer to Table 12-4 List of Settings Specified for Owner regarding settings specified for the owner role.

12.8 Object Privilege Settings

Set object settings to allow for existing Scope or JobUnit or various monitor settings to operate for roles other than the owner role. The following conditions must be met to set up Object Privileges.

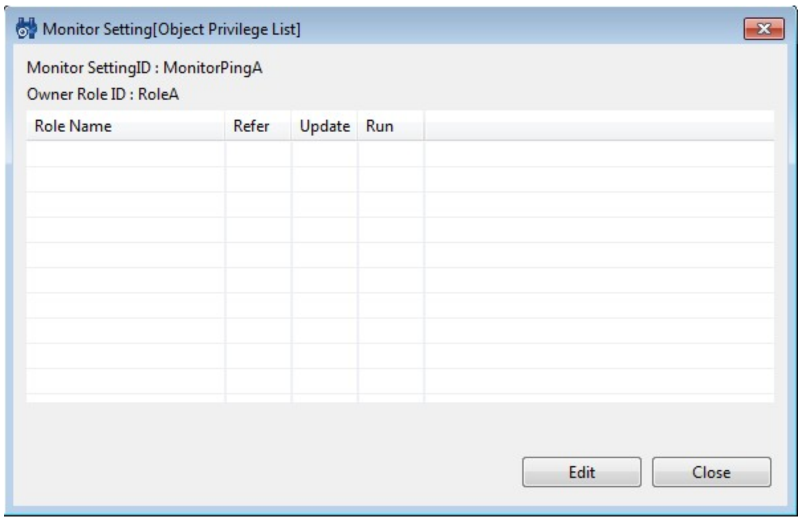
- They are assigned to the owner role of the corresponding setting
- They are assigned to a role where Object Privilege "Update" is valid for the corresponding setting

Refer to Table 12-5 List of Object Privileges regarding the settings that are possible for Object Privileges.

12.8.1 Object Privilege Registration

An example of the procedure for setting Object Privileges when setting Object Privileges in Monitor Settings is shown below.

1. Select the Monitor Setting where you want to set the Object Privileges from the Monitor Setting List table in the Monitor Setting[List] view. Then click the "Object Privilege Settings" button. The Monitor Setting[Object Privilege List] dialog opens.



Monitor SettingID : MonitorPingA

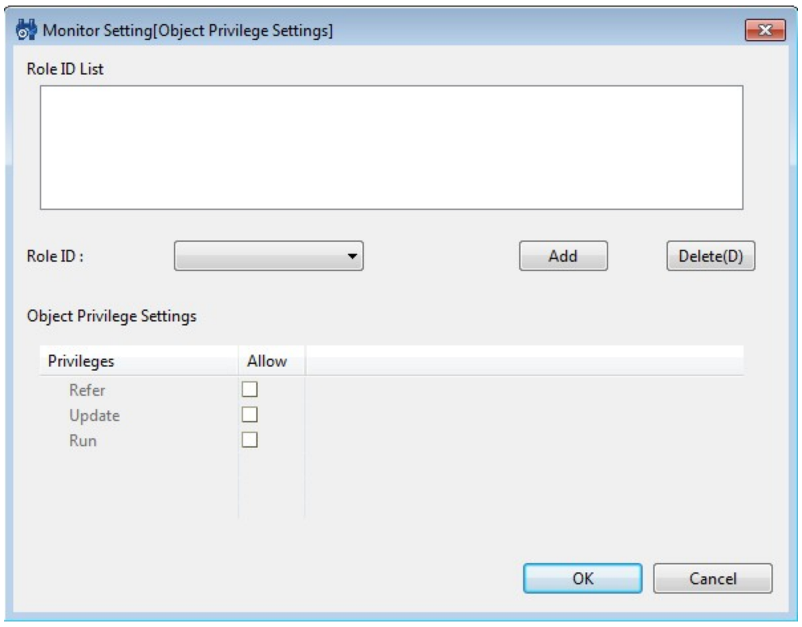
Owner Role ID : RoleA

Role Name	Refer	Update	Run

Figure 12-21 Monitor Setting[Object Privilege List] Dialog

Any Object Privileges that are already set up will be shown in this list.

2. Click the "Edit" button. The Monitor Setting[Object Privilege Settings] dialog opens.



Monitor Setting[Object Privilege Settings]
Role ID List
Role ID :
Add
Delete(D)
Object Privilege Settings
OK
Cancel

Privileges	Allow
Refer	□
Update	□
Run	□

Copyright (c) 2013 NTT DATA CORPORATION

Figure 12-22 Monitor Setting[Object Privilege List] Dialog

3. Set up the following items.

- Role ID List

  Roles with any Object Privileges set up will be shown in this list.

- Role ID:

  Select the role you would like to add the Object Privilege to from the pull down menu. Click the "Add" button. The Role ID selected in the "Role ID List" is added. Further, roles that can be selected are roles that are assigned to the login user. (If the login user is assigned the "Hinemos administrator role (ADMINISTRATORS)", then all roles except for owner role for the corresponding setting can be selected.)

- Object Privilege Settings

  Select the role from the Role ID List and set up the Object Privilege. Further, "Refer" privilege is specified by default, but this can be removed. Also, you may be able to configure privileges (such as "Run" privileges for the monitor feature) that are irrelevant for that feature, but their operation will have no effect.

4. Click the "OK" button. The Object Privilege settings are registered. The Monitor Setting[Object Privilege Settings] dialog closes, and the set details are displayed in the Monitor Setting[Object Privilege List] dialog.
5. Click the "Close" button.

12.8.2 Modify Object Privileges

An example of the procedure for modifying Object Privileges when modifying Object Privileges registered in Monitor Settings is shown below. You can't modify the corresponding Object Privilege if integrity can't be maintained when changing the Object Privilege.

1. Select the Monitor Setting where you want to modify the Object Privilege from the Monitor Setting List table in the Monitor Setting[List] view. Then click the "Object Privilege Settings" button. The Monitor Setting[Object Privilege List] dialog opens.
2. Click the "Edit" button. The Monitor Setting[Object Privilege Settings] dialog opens.
3. Edit the details of the setting, then click the "OK" button (refer to Object Privilege Registration for the entry method).
4. Click the "Close" button.

12.8.3 Delete Object Privileges

An example of the procedure for deleting Object Privileges when deleting Object Privileges registered in Monitor Settings is shown below. You can't delete the corresponding Object Privilege if integrity can't be maintained when deleting the Object Privilege.

1. Select the Monitor Setting where you want to delete the Object Privilege from the Monitor Setting List table in the Monitor Setting[List] view. Then click the "Object Privilege Settings" button. The Monitor Setting[Object Privilege List] dialog opens.
2. Click the "Edit" button. The Monitor Setting[Object Privilege Settings] dialog opens.
3. Select the role to delete in the Role ID List, then click "Delete" button.
4. Click the "OK" button.
5. Click the "Close" button.

12.8.4 Object Privilege Collective Settings

You can collectively set Object Privileges for multiple settings if they are the same kind of settings. However, use caution if there are already settings because it is set to overwrite the existing Object Privilege Settings if you perform the settings with this process.

An example of the procedure for collectively setting Object Privileges when collectively setting Object Privileges for multiple Monitor Settings is shown below.

1. Select multiple Monitor Settings where you want to set the Object Privilege from the Monitor Setting List table in the Monitor Setting[List] view. Then click the "Object Privilege Settings" button. The Monitor Setting[Object Privilege Settings] dialog opens.
2. Configure the contents you want to register, then click the "OK" button (Refer to Object Privilege Registration for the entry method).
3. A confirmation dialog is displayed. Click the "OK" button.

Copyright (c) 2013 NTT DATA CORPORATION

13 Precautions

13.1 Behaviour of Job schedules when planned execution time has passed while java porcess was stopped

Please be aware that Job schedules which were supposed to be executed, but did not because of java process stoppage, will behave as written below.

Also, when restoring database from backups, this operation will cause a time difference in between time informations stored in the database and the java process uptime.

This will cause Job schedules to act in a same way as if java process was stopped for a certain amount of time.

- When scheduled execution time of Job schedule is within threshold (time to judge scheduled job execution as failure. default:1hour) from java process start up.

  Scheduled Job will be executed immediately after the start up of java process completes.

  Example) If a schedule which executes a Job every day at 10:00 AM, is set. (Figure 13-1)

  If java process was stopped from Sunday night to Monday 10:30 AM, and java process was started on Monday 10:30 AM, scheduled job which were supposed to be executed at Monday 10:00 AM, will be executed immediately after the start up of java process.

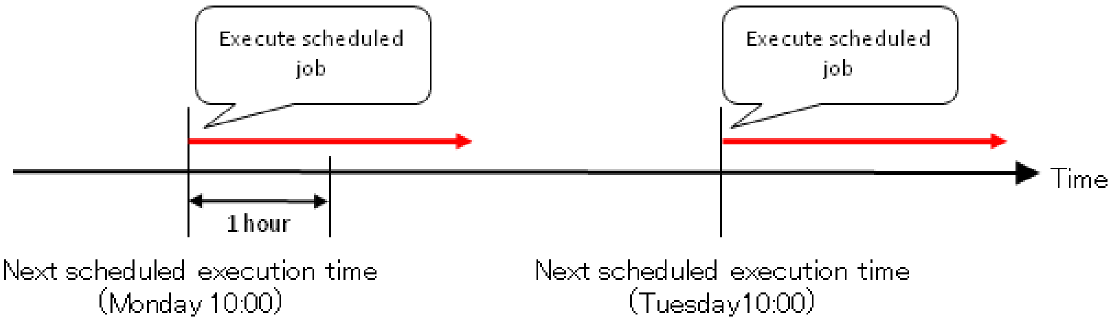

Execute scheduled job
Execute scheduled job
Time
1 hour
Next scheduled execution time (Monday 10:00)
Next scheduled execution time (Tuesday10:00)

figure 13-1 Example of Job Schedule

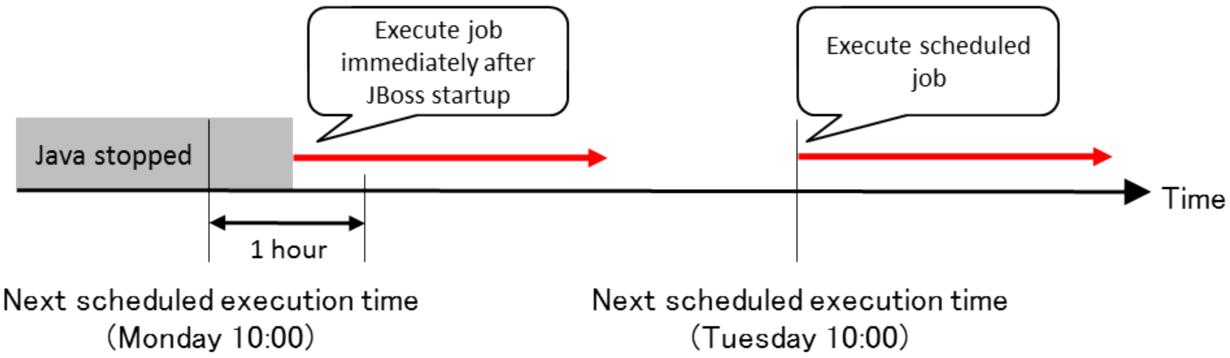

Execute job immediately after JBoss startup
Execute scheduled job
Java stopped
Time
1 hour
Next scheduled execution time (Monday 10:00)
Next scheduled execution time (Tuesday 10:00)

figure 13-2 When java process was started within threshold time to judge scheduled job execution as failure

Copyright (c) 2013 NTT DATA CORPORATION

- When scheduled execution time of Job schedule is above threshold (time to judge scheduled job execution as failure. default:1hour) from java process start up.

  Execution of scheduled Job will not occur, and will be executed in next scheduled time.

  Example) If a schedule which executes a Job every day at 10:00 AM, is set. (Figure 13-1)

  If java process was stopped from Sunday night to Monday 11:30 AM, and java process was started on Monday 11:30 AM, scheduled job which were supposed to be executed at Monday 10:00 AM, will not be executed on Monday, and will wait until next scheduled timing (Tuesday 10:00 AM). (Figure 13-3)

  In this case, when Job schedule was executed on Sunday 10:00 AM, next scheduled time (Monday 10:00 AM) will be set in the database. Because execution timing(Monday 10:00 AM) has passed while java process was stopped, and java process was started in 11:30 AM which is past the threshold time of one hour, this scheduled Job execution will be skipped at this timing and the next scheduled time (Tuesday 10:00) will be set in the database.

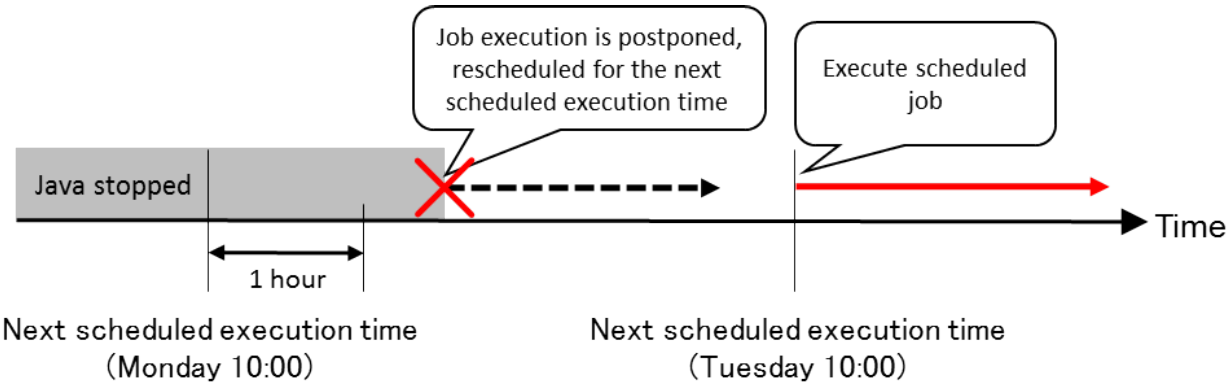

Job execution is postponed, rescheduled for the next scheduled execution time
Execute scheduled job
Java stopped
Time
1 hour
Next scheduled execution time (Monday 10:00)
Next scheduled execution time (Tuesday 10:00)

Figure 13-3 Behaviour of Job Schedule when java process was started after the threshold time.

In order to change the threshold time (time to judge scheduled job execution as failure), please refer to Administrator's Guide "8.2 Configuring the Job Schedule Control when Restarting Hinemos Manager".

13.2 Changing the system time of the Hinemos Manager OS

When changing the OS Clock of Hinemos Manager Server, please execute scheduler reset script. For more detail, please refer to Administrator's Guide "3.1.10 Scheduler Adjustment after changing the OS clock settings"

When scheduler reset script is not executed, Hinemos Manager will act as follows.

When the "OS system time" of the manager node is changed from time T2 to the past time T1 (T1 < T2), the monitor management features and jobs scheduled between T1 and T2 will not start.

Hinemos controls the startup of the monitor management features and scheduled jobs based on the "OS system time" of the manager node. Each monitoring configuration, scheduled job, and system schedule of the Hinemos Manager has its own "next scheduled execution time". When the "OS system time" reaches the "next scheduled execution time", the monitoring or job runs.

For example, assume that monitoring configuration A has a monitoring interval of 10 minutes, and it is executed on 4/25 at 10:00am. In this case, the "next scheduled execution time" for monitoring configuration A is on 4/25 at 10:10am. If the "OS system time" is changed to 3/25 at 9:00pm, monitoring configuration A does not execute between the periods of 3/25 at 9:00am to 4/25 at 10:10am.

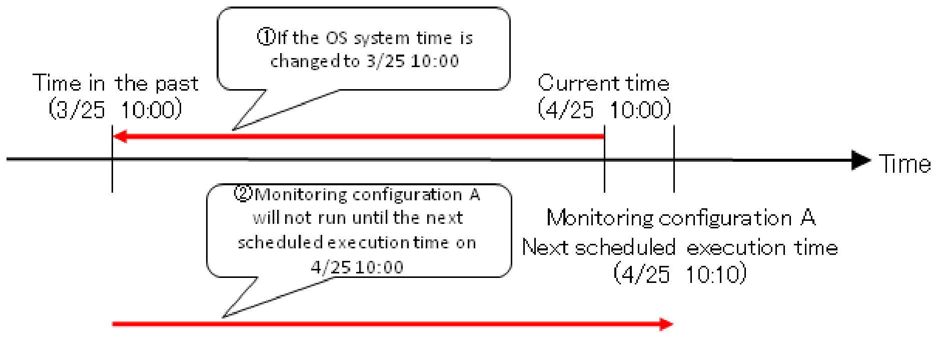

①If the OS system time is changed to 3/25 10:00
Time in the past (3/25 10:00)
Current time (4/25 10:00)
Time
②Monitoring configuration A will not run until the next scheduled execution time on 4/25 10:00
Monitoring configuration A Next scheduled execution time (4/25 10:10)

Figure 13-4 Operation when the "OS system time" is Returned to the Past

The Hinemos Manager does not operate again until it is 4/25 at 10:00am.

13.3 Restrictions on the Character Code

The OS character code for the Hinemos Manager must be UTF-8.

The following character codes are standard for the Hinemos Agent.

- Linux: UTF-8
- Windows: MS932 (sjis)

The following restrictions apply if another character code is used.

1. System Log Monitor limits

   When a Japanese log is output to the syslog of the monitor target, detection will fail if Japanese is used for pattern matching of the system log monitoring. The original message will be corrupt when a language other than Japanese is used for the pattern matching.

2. Monitor Logfile limits

   When a Japanese log is output to the log file of the monitor target, detection fails if Japanese is used for pattern matching of the system log monitoring. You can use a language other than Japanese for a pattern matching expression, but the original message will be corrupt when displayed.

3. Job feature limits

   The execution results of a job may be corrupt.

You can avoid 2 and 3 by changing the configuration of the Hinemos Agent. Refer to Chapter 4.4, "Configuring OS Locale and Character Encoding" in the Administrator's Guide for details.

13.4 Restrictions on the Windows Agent

The following section describes the restrictions on the Windows Agent.

13.4.1 Job Feature Limitations

1. File transfer is not available.

   The ssh protocol is used for file transfer in the job management feature. You can use the file transfer feature in the Linux Agent by using the ssh daemon (openssh) on the source of the file, and by executing the command on the ssh client (openssh) at the destination of the file.

   However, the file transfer feature is not available on the Windows Agent because the shh daemon and the ssh client are not provided by the Windows OS (default).

2. The effective user of the job must be the same as the service startup user.

   Make sure that the effective user and the service startup user set in the Job Register dialog of the Job feature are the same. The following log will be output if they are not the same.

   ```
   The execution user of the command and agent's user are different.
   execUser=[Effective User name], agentUser=[Service startup user name]
   ```

   Effective user and service startup user(Agent user) can be set the same by selecting "Agent user" in Job[Create/Change Job] dialog. By doing this, Job can be executed without considering the startup user(Agent user) of every managed target.

3. The service startup user cannot be specified as the SYSTEM user in Windows Server 2008 and Windows Server 2012.

   Please change the service startup user to other than SYSTEM when starting up the agent as a service in Windows Server 2008 and Windows Server 2012.

   The user name and the password are required to configure the service startup user. Therefore, when changing the password of the OS user account, please do not forget to change the password of the service startup user.

13.4.2 Monitor Setting Feature Limitations

1. Load average cannot be acquired.

   Load average cannot be retrieved due to restrictions in resource monitoring. However, the performance value is obtained by using the UCD-MIB(1.3.6.1.4.1.2021) of SNMP. Specifically, the following items cannot be retrieved.

   - 1 minute load averages
   - 5 minutes load averages
   - 15 minutes load averages

   Use SNMP monitoring to monitor the load average of Windows. The 1 minute load average (in %) can be obtained from the "HOST-RESOURCE-MIB". Please specify "hrProcessorLoad (OID：1.3.6.1.2.1.25.3.3.1.2.1)" in the SNMP Monitor feature.

2. Restart the SNMP Service required when the logical drive increases.

   The SNMP Service must be restarted when the logical drive increases due to removable disk connection etc.

13.4.3 Monitor Logfile Limits

When performing Monitor Logfile on a Windows environment, by default you can't rename or delete a log file. Therefore, the rotation method of the file will be limited.

The "copytruncate" method and "mv" method used for the "logrotate" in Linux are explained in the example.

1. "copytruncate" method

   The "copytruncate" method creates a copy of the subject log file, and then truncates the original file. The Hinemos Agent for Windows environment is compatible with this method.

2. "mv" method

   The "mv" method moves (renames) the subject log file, and then creates a new original log file. The default Hinemos Agent for Windows environment is not compatible with this method because the subject log will be moved (renamed). ("log4j" used in Java application uses the "mv" method during the rotation scheme.) Add the following to the Hinemos Agent settings file (Agent.properties) and restart the Hinemos Agent to support the mv format.

   ```
   random.access.file=windows
   ```

13.5 Method to Configure the Arguments of Process Monitoring with net-snmp

The length of the string returned as the parameter (argument) may be restricted depending on the version of net-snmp.

- Example of a restricted string length

  net-snmp-5.3.1-24.el5_2.1 : 128 characters

If the information exceeds the maximum character count, the end characters is truncated to meet the maximum character count.

Therefore, when setting the Process Monitor for processes where the arguments are extremely long, the first part of the argument must be fixed.

13.6 Behavior of Resource Monitoring when the Repository Information has Changed

Resource monitoring feature is paused when the contents of the resource monitoring has changed. When the IP address of the managed node in the repository information has changed, the resource monitoring for the corresponding node is temporarily stopped.

Resource Monitor calculates Monitor items (CPU usage, etc) that require the difference in the results of two polls. Therefore, the monitor results can't be acquired right after the update. As the start of polling is synchronized (0 seconds for each minute), acquisition of monitoring results requires a time twice the monitoring interval.

13.7 Multi-client Access

- Browsing from the Hinemos Client

  You can connect and operate the same/different user accounts from multiple Hinemos Clients. However, as the number of client connections increases, reference inquiries to the Hinemos Manager will increase as well.

  When multiple Hinemos Clients are connected, it is recommended that you reduce the inquiries to the Hinemos Manager by making the refresh interval for each client longer.

- Changing the configuration from the Hinemos Client

  You can change the configuration from multiple Hinemos Clients. However, there are no exclusive control features for Monitoring Settings. Therefore, it is recommended that a single Hinemos Client be used to carry out the configuration changes. For Job feature, you can use "edit mode" to gain exclusive control over job settings.

13.8 Setting command including whitespace character for "start command" and "stop command"

When setting a command including whitespace character for "start command" and "stop command" of Job feature, command must be quoted with double quote (").

Example 1) When designating (C:\Program Files (x86)\hoge.sh) command for

"start command" and "stop command" of Job

```
"C:\Program Files (x86)\hoge.sh"
```

When setting a command and argument of command including whitespace character for "start command" and "stop command" of Job feature, each of them must be quoted with double quote (").

Example 2) When designating (C:\Program Files (x86)\hoge.sh -cp C:\test a b c) command for

"start command" and "stop command" of Job

```
"C:\Program Files (x86)\hoge.sh" -cp C:\test "a b c"
```

13.9 Behaviour of Jobs while Hinemos Agent is stopped

Hinemos Manager sends Job execution order to Hinemos Agent on Job execution time. When Hinemos Manager tries to send Job execution order, but cannot connect to Hinemos Agent properly, Hinemos Manager retries connecting, in designated interval, for designated number of times. (Default interval:60sec, number of times to order: 10)

When this retrying fails, End Status of Job will shift from "Running" to "Error".

The number of times to retry command execution ordering can be changed from Job[Create/Change Job] dialog

For more detail, please refer Creating/Changing a Job .

Copyright (c) 2013 NTT DATA CORPORATION

14 ChangeLog

ChangeLog

Version	Date	Details
Edition 1.0	10/1/2013	First release

Hinemos ver4.1 User Manual

Not for sale
- Unauthorized duplication prohibited
- Unauthorized reproduction prohibited
- Unauthorized redistribution prohibited

"Hinemos" is a registered trademark of NTT DATA Corporation.
"Hinemos Node Map" is a registered trademark of NTT DATA Corporation.
"Hinemos Job Map" is a registered trademark of NTT DATA Corporation.
"Linux" is a trademark/registered trademark of Linus Torvalds world-wide.
In addition, companies and product names described in this document are trademarks and/or registered trademarks of the respective companies.
This holds true even when, TM and R marks are not marked in this manual.