NEC

MasterScope Network Management
Web Console
Reference Manual

Copyrights

Trademarks

Preface

Thank you for choosing MasterScope network management products. MasterScope network management products enable users to seamlessly integrate and operate the information and controls of multiple products on one Web Console by using the MasterScope Integrated Management Server component (hereafter referred to as IMS component).

This document describes the Web Console functions using the IMS component (version 1.0) and how to operate the functions. Use this document to enable efficient networking operations by using Web Console.

Configuration of This Manual

This manual consists of the following chapters. Read the chapters relevant to you according to your "Target reader" classification in the table below.

: Administrators 

: All users of Web Console

Configuration of This Manual

Title	Content	Target reader
"Chapter 1. Overview and Basic Operations of Web Console (page 1)"	Describes an overview and basic operations of the Web Console.	User
"Chapter 2. Environment Settings Before Operations (page 28)"	Describes how to configure the environment before using and operating the Web Console.	Admin
"Chapter 3. Environment Settings During Operations (page 53)"	Describes how to configure the environment as needed while using and operating the Web Console.	Admin
"Chapter 4. Operations (page 68)"	Describes how to use the Web Console during operation.	User
"Chapter 5. System Maintenance (page 111)"	Describes how to maintain in the Web Console usage environment.	Admin
Appendix	Describes supplementary information on operation using the Web Console.	Admin
Glossary ("A - Z (page 139)")	Describes the functions of the Web Console and the terms and abbreviations that are used in this manual.	User

Notations and Text Conventions

In this manual, the following notations are used to indicate items that require special attention and supplementary information.

Notations of Items Requiring Attention and Supplementary Information

Notation	Description
Caution	Indicates important points that the user should observe to configure and use the product properly.

Notation	Description
Tip	Indicates useful information.

In this manual, the following text conventions are used.

Text Conventions

Notation	Description	Example
name	Indicates graphical user interfaces such as menus, items, and buttons.	**Dashboard** menu, **OK**button
<userinput>	Indicates items that change depending on the user environment or items that the user must specify.	*<%INSTPATH%>*, *<filepath>*
`configuration file`	Indicates the contents of the configuration file.	Set the following value: `port = 27120`
`command line`	Indicates command line operations.	Run the following command: `> Setup.exe`

In this manual, the following abbreviations are used.

Abbreviations

Formal Name	Abbreviation
MasterScope Integrated Management Server	Integrated Management Server, IMS
MasterScope Network Manager	Network Manager
MasterScope Network Flow Analyzer	NFA

To use Web Console, you need to install the component named IMS. The default installation path of the IMS component is as follows:

Default installation path: Windows

C:\Program Files\NEC\IMS

Default installation path: Linux

/opt/nec/ims

In this manual, the above installation path is referred to as *<%INSTPATH%>*. If you installed in another path, please replace this path name with the appropriate path name.

In addition, when you install IMS, you can specify a different path to store the data that will be managed by the IMS component. In this manual, the data storage path is referred to as *<%DATAPATH%>*. If you install this component and store the data in the same path, *<%DATAPATH%>* and *<%INSTPATH%>* indicate the same path.

In this manual, regardless of OS type, there are places where "\" is used as a directory symbol. For a Linux environment, read "/".

Contents

Chapter 1. Overview and Basic Operations of Web Console

This chapter describes an overview of functions and the basic operations of the Web Console.

Contents

1.1 Overview of Web Console

This chapter describes an overview and the purpose of the Web Console.

1.1.1 The Usage of Web Console

Web Console provides the mechanism to remotely operate from any terminal using a Web browser. In addition, it seamlessly integrates the operation of individual products for network monitoring, analysis and control, and provides a mechanism for streamlining network operation lifecycle management..

Web Console is useful when operating as follows.

- When checking the network status from an arbitrary terminal

  Installation of client software is not necessary because Web Console is used on a web browser. Therefore, in the case of emergency, it is possible to check the network status using web browser on an arbitrary terminal.

  For example, when using the Network Manager, in an environment where web communication is permitted, it is possible to check the status of each node and the scope of impact of the failure by accessing the Web Console remotely.

- When integrating operations of multiple MasterScope network management products

  Web Console integrates the management information of multiple products into one place and displays it. When grasping the overall status of the network, you do not need to check the individual views provided by each product, and you can efficiently perform management tasks.

  For example, It is possible to integrate management information of multiple Network Managers and integrate information of Network Manager and NFA.

Tip

Web Console can be used for routine operation such as checking the occurrence status of events, checking or analyzing the performance information of each node. However, not all functional operations provided by each product can be performed. If necessary, also use the management console provided by each product together.

1.1.2 Functional overview of Web Console

The following describes the functions on Web Console.

Dashboard

- The current network performance and event occurrence status can be grasped promptly.
- Multiple display contents can be defined for each viewpoint. This enables the status to be viewed from various viewpoints by selecting the defined contents from a pull-down menu.
- A **Widget**, which is an element use to display a chart or list, can be freely located on the dashboard page by the intuitive drag-and-drop operation. Therefore, a dashboard definition according to the operations can be created easily.

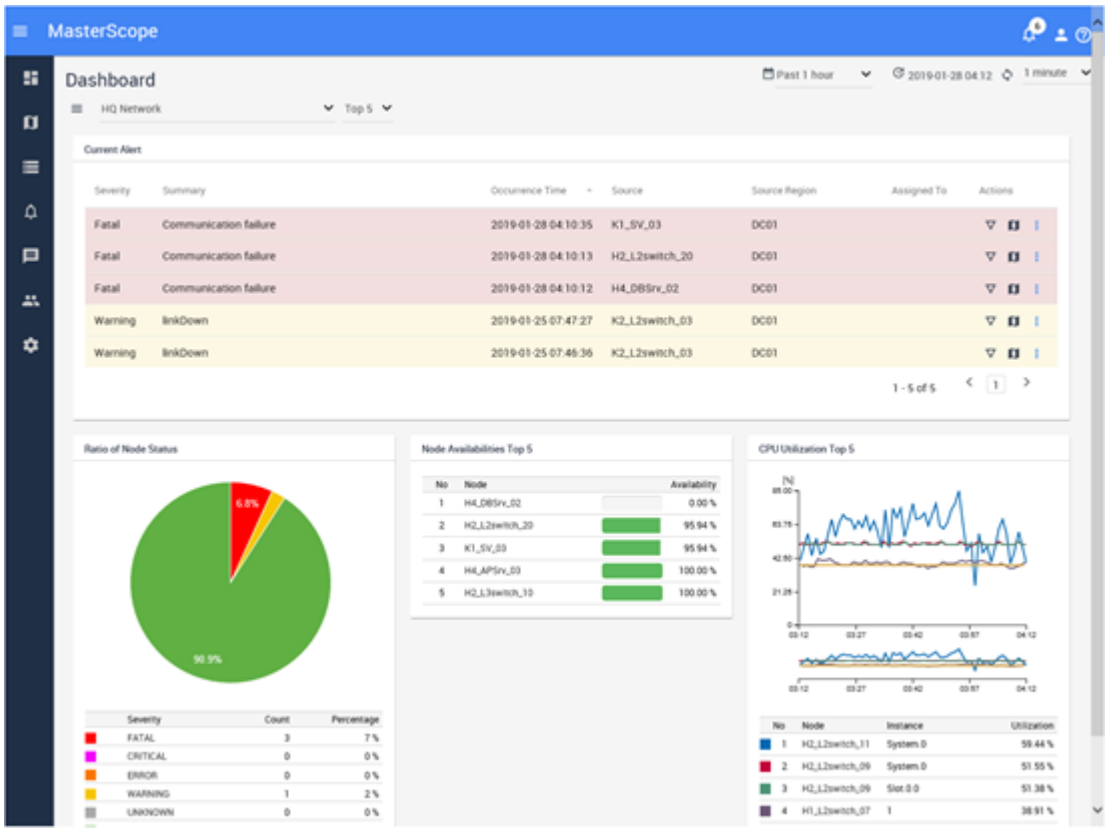

Figure 1-1 Dashboard

Node management and analysis

- Nodes managed by Network Manager and exporters of NFA are managed as a *"Node"*. Information of nodes that can be assumed to be the same in multiple products is integrated and managed in a single node.
- It is possible to search nodes that match a certain condition among all managed nodes, and also check and compare the property information.
- The dashboard (Node Detail page) of each node can be used to check and analyze the property information and load status of the specified node in detail. The dashboard (Network Interface Detail page) of each network interface can be used to check the property information and communication status of the specified network interface in detail.

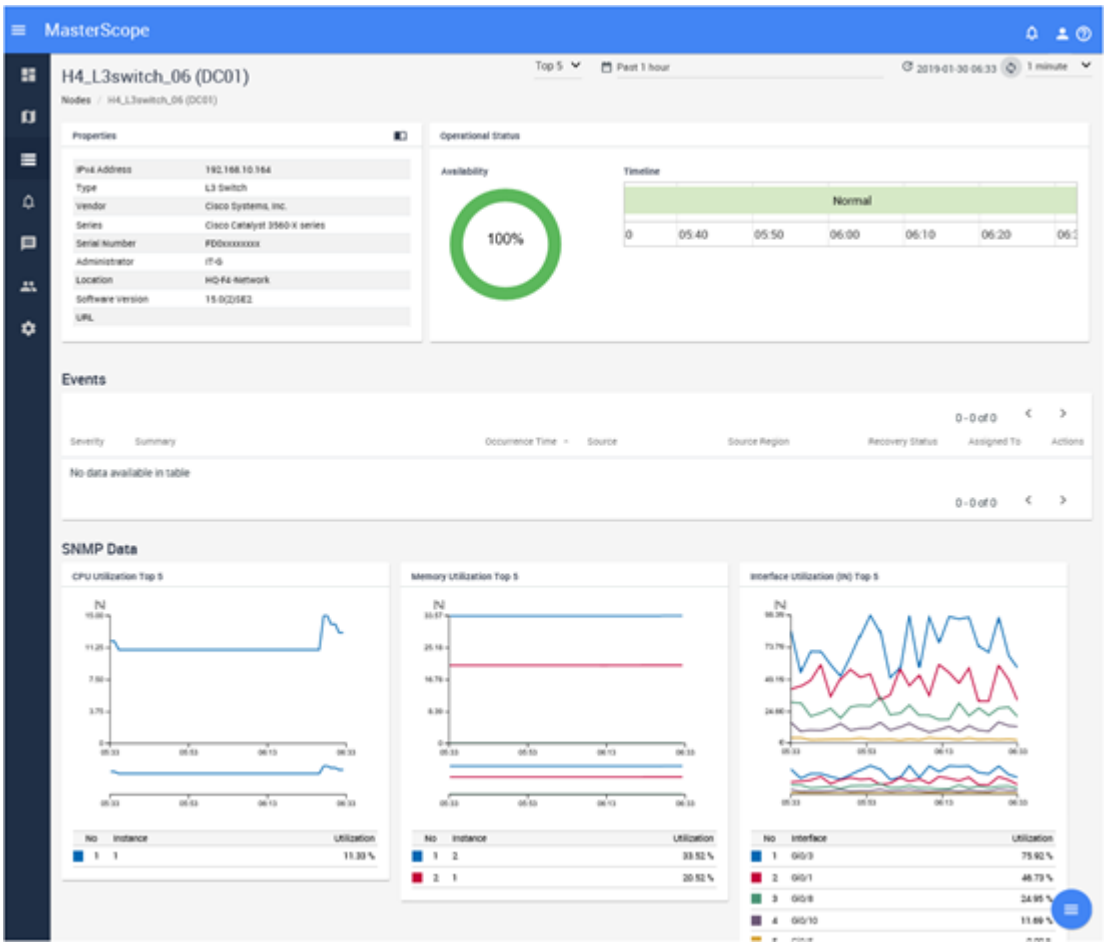

Figure 1-2 Node Detail

Topology Map (when using Network Manager)

- As the topology map, it is possible to show the physical connections among the nodes, node placement in the building or on the floor, and so on. The topology map is helpful for operations such as checking the influence range when a fault occurs. The topology map provides various editing functions that make it easy to grasp network configuration such as insertion of background image.
- A mechanism (Side Panel) is provided to check the property and performance information of nodes while looking at the topology map. It can be used to investigate nodes, which are related to each other, one by one on the topology map.
- Displaying the topology map in **analysis mode** enables users to check the event severity of each node for a certain period in the past. This is called the Timeline function. For example, if an event that occurred last night has currently recovered, this function supports the situation grasping at the time of the event occurred by going back to the event occurrence time of the previous night and visualizing the event influence range on a topology map.

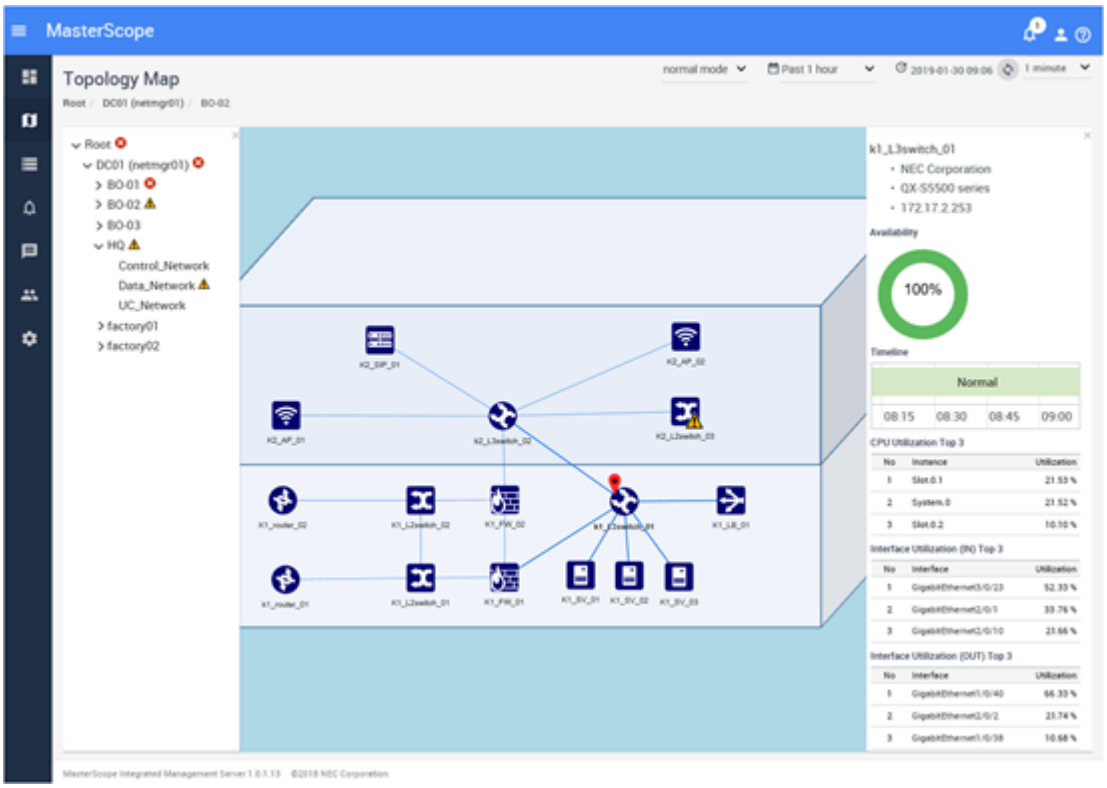

Figure 1-3 Topology Map

Event monitoring

- Alerts detected by Network Manager and events exceeding the threshold of traffic volume detected by NFA are managed as an *"event"* integrally. Also, it is possible to investigate the cause smoothly from the event; for example, checking detailed information of the relevant node and jumping to the topology map.
- The occurred events can be checked the summary information in the event list. Also, it is possible to check only necessary information by narrowing down the display events by specifying a condition. Placing the **Current Alert** widget on the Dashboard page enables to grasp current fault events promptly.
- An action such as sending an Email or running a command can be executed when an event occurs by specifying a condition for events. This function can be used to send notifications to the person involved and to control automatic recovery.

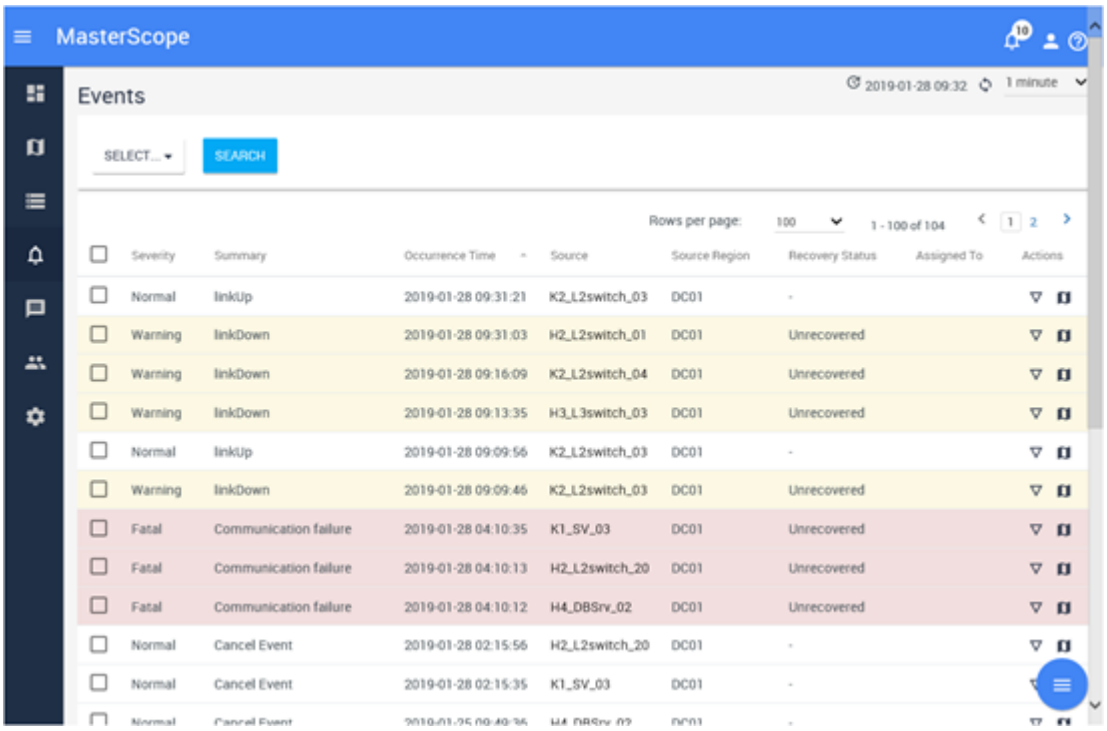

Figure 1-4 Events

1.1.3 System configuration

The following describes the system configuration when using Web Console.

To use Web Console, set up the IMS component and connect the IMS component to the MasterScope network management products. When connecting the IMS component with multiple products, products managing the same node are grouped into the region group.

For example, if Network Manager managing Nodes 1 to 45 and NFA managing Nodes 40 to 45 as exporters exist in the same environment, these two products manage Nodes 40 to 45 redundantly. In this case, the two products are grouped into the region group. Information of Nodes 40 to 45 managed by the two products can be viewed in an integrated manner on Web Console.

"Figure 1-5 System Configuration Diagram (page 7)" shows a system configuration example consisting of multiple region groups.

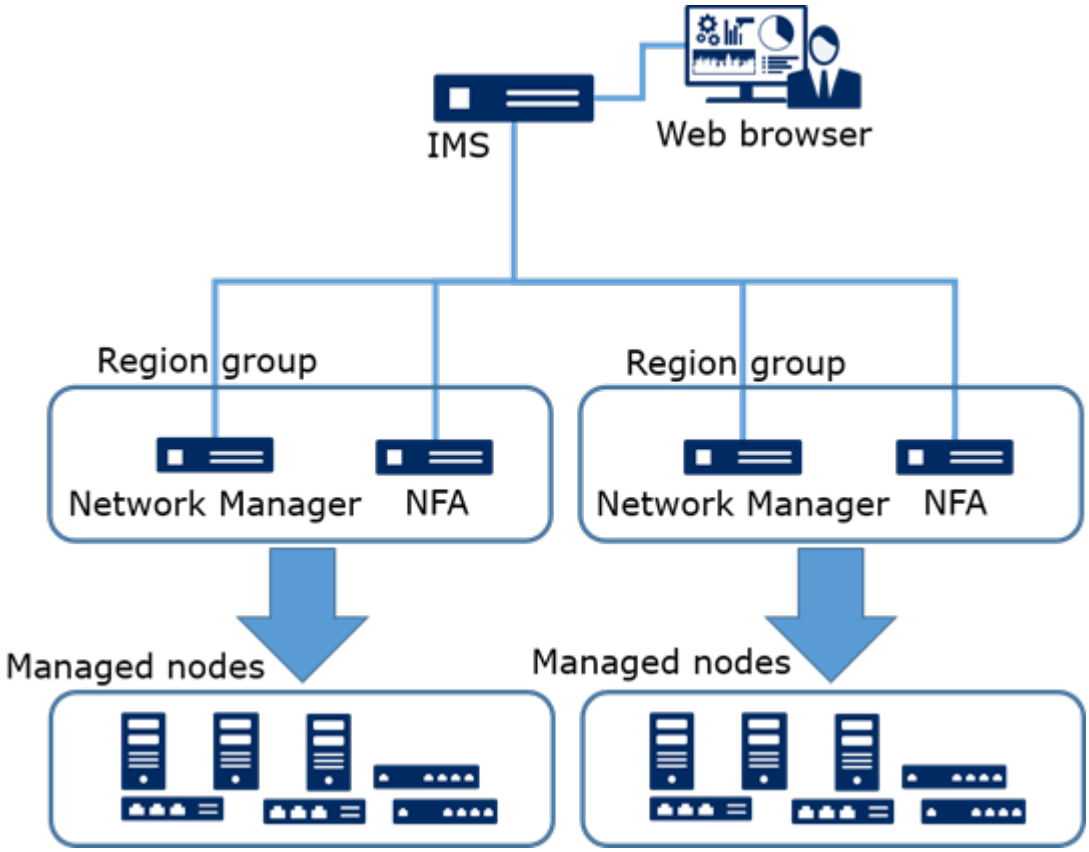

Figure 1-5 System Configuration Diagram

Tip

- A system can be built by installing the IMS component and MasterScope network management products, such as Network Manager, on the same server.
- Note that installing the IMS component and multiple products on the same server may cause problems such as slow operational response of Web Console. Therefore, thoroughly assess the system configuration before starting operations. If possible, it is recommended that products be installed separately on multiple servers.

1.2 Basic Operations of Web Console

This section describes how to access the Web Console and the basic operations of the Web Console.

1.2.1 Preparations for Using Web Console

This section describes preparations for using the Web Console.

Before using the Web Console, configure your web browser. This only needs to be configured once.

1.2.1.1 Checking the web browser security settings

This section describes the web browser security settings required to use the Web Console.

JavaScript and Cookies must be enabled for the web browser to access the Web Console.

JavaScript and Cookies are enabled by default for supported browsers. Therefore, it is not necessary to specify a particular setting. If you have changed the security settings, check whether the changed settings are appropriate to use the Web Console.

For Windows Server, if **Enhanced Security Configuration** is set to *"Enabled"*, the setting described in "Configuring settings on a Windows Server OS (page 9)" is required.

Checking the Internet Explorer settings

Check the Internet Explorer settings on the Internet Options dialog box. Press the Alt+T key on the Internet Explorer window, and then select **Internet Options** from the displayed menu. For details about the setting on each tab, refer to the help of Internet Explorer.

- **Security** tab
  - Registering the URL to *"Trusted sites"*

    Register the URL of the server where the IMS component is installed to *"Trusted sites"*.

    Tip

    If you do not want to register the URL to *"Trusted sites"*, configure the setting so that the server where the IMS component is installed is classified into other than the *"Restricted sites"*.

  - Enabling JavaScript

    Confirm that **Active scripting** is set to *"Enable"* on **Custom Level** of *"Trusted sites"*.
- **Privacy** tab

  If the server where the IMS component is installed is the *"Internet"* zone, confirm that Cookies are allowed.

  Tip

  - If the server where the IMS component is installed is the *"Trusted sites"* or *"Local Intranet"* zone, Cookies are not blocked.
  - If the server where the IMS component is installed is in the *"Restricted sites"* zone, Cookies are always blocked and the Web Console cannot be used.

Checking the Mozilla Firefox settings

Check the settings on the Options page of Mozilla Firefox. For details about the settings, refer to the help of Mozilla Firefox.

- **Privacy & Security** panel

  Confirm that the **History** setting is configured to keep Cookies from the visited websites.

Checking the Google Chrome settings

Check the settings on the Settings page of Google Chrome. Click **Advanced** at the bottom of the page, and then click the **Content settings** button under **Privacy and security**. You can check the settings on the displayed Content settings dialog box. For details about the settings, refer to the help of Google Chrome.

- **Cookie**

  Confirm that the setting is configured to keep Cookies.
- **JavaScript**

  Confirm that JavaScript is permitted.

Configuring settings on a Windows Server OS

If **Enhanced Security Configuration** is set to *"Enabled"*, add *"about:blank"* to *"Trusted sites"* on the Internet Options dialog box.

1.2.1.2 Importing the SSL server certificate into the web browser

The SSL server certificate required to be imported to the web browser to access the Web Console via HTTPS.

If you select a self-signed type SSL server certificate, you can access the Web Console safely by importing the certificate into the web browser.

Tip

Even for a certificate issued by a certificate authority, some certificate authorities may instruct you to import a root certificate to the web browser. In this case, follow the instructions of the certificate authority.

⚠ Caution

If you use Internet Explorer without importing the certificate and if the warning continues to be displayed, aberrant behavior might occur such as a page being unable to be displayed or operations being unable to be performed on the web browser. It is therefore strongly recommended to import a certificate when using a web browser.

- For Internet Explorer and Google Chrome, perform the following procedure.
  1. Place the certificate (.cer file) output by the `exportcert` command of "A.1 ims-ssl-keytool (page 132)" on the terminal where the Web browser operates.
  2. Double-click the certificate file.
  3. On the displayed Certificate dialog box, click the **Install Certificate** button.

     Certificate Import Wizard is displayed. Click the **Next** button.
  4. Select **Place all certificates in the following store** and then click the **Browse** button.
  5. On the Select Certificate Store dialog box, select *"Trusted Root Certification Authorities"*, and then click the **OK** button.
  6. Click the **Next** button.
  7. Click the **Finish** button.
  8. Although Security Warning is displayed because of a self-signed certificate, click the **Yes** button.

  When the dialog message "`The import was successful.`" is displayed, the certificate is successfully imported.
- For Mozilla Firefox, perform the following procedure.
  1. Access the following URL by using the web browser.

     https://<domain name (FQDN) of IMS sever>/ims/

     ### Tip

     It is necessary to be able to resolve the domain name (FQDN) of the IMS server specified for the URL.

The warning is displayed indicating that it is not a secure connection.

2. Click the **Advanced** button, and then click the displayed **Add Exception** button.
3. On the Add Security Exception dialog box, confirm that **Permanently store this exception** is selected, and then click the **Confirm Security Exception** button.

⚠ Caution

When adding a security exception, be sure to check that the contents of the certificate to be added are correct in advance.

The certificate is successfully imported if the login page is displayed.

1.2.2 Accessing Web Console.

This section describes how to access the Web Console from a web browser.

Perform the following procedure to access the Web Console.

1. Specify the URL of Web Console on a web browser.
   - URL for HTTP communication

     http://<domain name (FQDN) of IMS sever>/
   - URL for HTTPS communication

     https://<domain name (FQDN) of IMS sever>/

     <domain name (FQDN) of IMS sever> must be the same as the name specified when creating an SSL server certificate. Otherwise, the certificate is regarded as invalid and a warning is displayed.

Tip

- To access Web Console, it is necessary to be able to resolve the <domain name (FQDN) of the IMS server> specified for the URL.
- If you changed the communication port number for accessing the Web Console, add the changed port number to the above URL and specify it.

  For example: http://webconsole.co.jp:8080/

When access to the Web Console is successful, the login page is displayed.

2. Enter the user name and password to log in to the Web Console.

When login to the Web Console is successful, the Dashboard page that is individually set to each user is displayed.

⚠ Caution

- The following are cautions on logging in to the Web Console and operations.
  - It is recommended to change the password after the initial login.

    To change the password, click on  in the upper right of the page and display the Profile Edit page from **Profile Edit** menu.
  - If it detects more than five login failures in 30 minutes, the user is locked and can not log in for 30 minutes.

    If you want to immediately release the locked state, you can unlock it by the user belonging the group who has the role of Account Manager.

  - It is possible to operate (add, change, delete, etc.) the setting information from multiple Web Console instances at the same time. However, in the case of operate on the same page, in order to maintain consistency of data, the operation performed later may be made to fail.

- The following are cautions when enabling single sign-on behavior to the Web Console of the connected products.
  - Users with the same name must be registered with the IMS component and the connected products. Single sign-on works only for users with the same name.
  - With the IMS component stopped, you may not be able to access the Web Console of the connected product. In this case, specify the URL to access the login page of the connected product directly, and access the Web Console.

1.2.3 Structure of Web Console

This section describes the structure of the Web Console.

The Web Console consists of four areas described in "Figure 1-6 Structure of Web Console (page 11)".

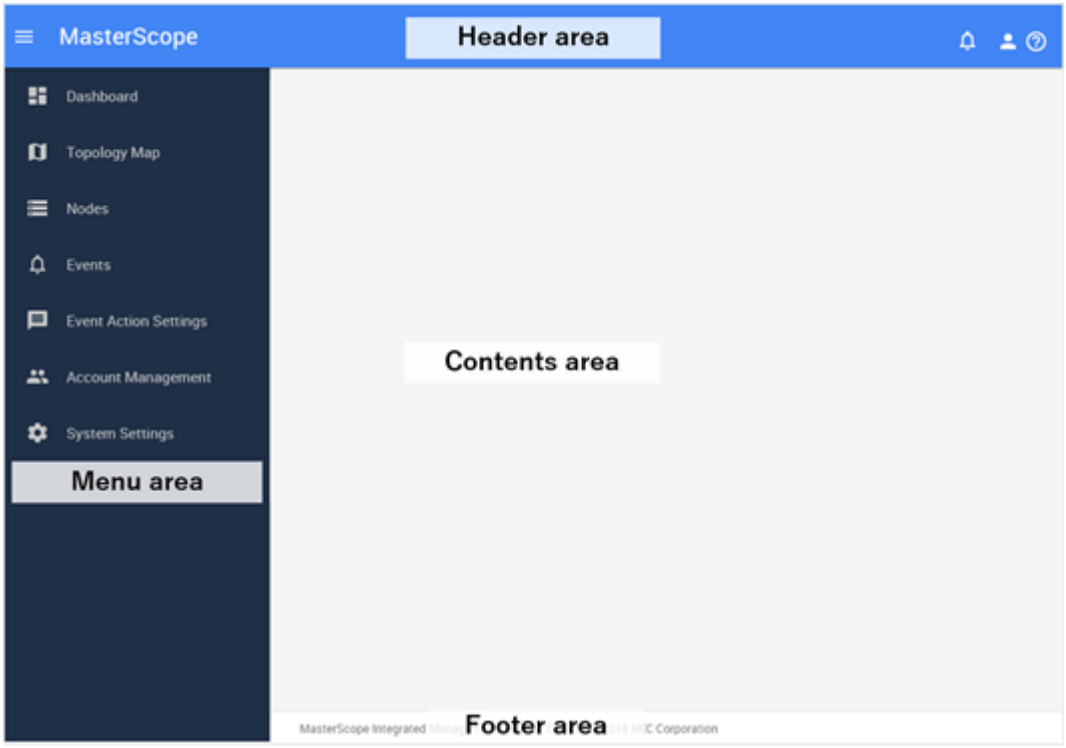

Figure 1-6 Structure of Web Console

Header area

Displays the logged-in user name, the state of new notifications and the like.

- icon

  Maximize or minimize the width of the menu area.

- **Notifications** icon

  Displays the status of new events and messages that occurred after logging in to the Web Console.

  The displayed number indicates the number of new events or messages.

Tip

A message is a notice such as an error on the operation or processing of the Web Console.

-  icon

  Clicking this icon displays the following.

  - User name

    Displays the logged-in user name (Display Name).

  - **Edit Profile** menu

    Displays the Edit Profile page. The Edit Profile page allows users to change their own user information such as **Password** for login.

    Tip

    After the initial login, be sure to change the password.

  - **Logout** menu

    Logs out from the Web Console.

-  **Help** icon

  Displays the help of the Web Console.

Menu area

Displays the menus of the functions that can be operated on the Web Console.

Caution

The menu contents to be displayed vary depending on the role of the logged-in user or the products constructing the system.

-  **Dashboard** menu

  Displays the Dashboard page. You can check the current network status.

-  **Topology Map** menu (displayed when using the Network Manager)

  Displays the Topology Map page. You can check the network topology configuration.

-  **Nodes** menu

  Displays the Nodes page. You can check the information on all the managed nodes.

-  **Events** menu

  Displays the Events page. You can check the information on the event that occurred.

-  **Event Action Settings** menu

  Clicking this menu displays the sub menu related to the event action (notification).

  Tip

  Only users belonging to a group with Administrator role can display and select menus.

  - **Event Actions** menu

Displays the Event Actions page. You can configure the notification processing triggered by event occurrence.

- **Email Servers** menu

  Displays the Email Servers page. You can configure the server settings for the Email notification.

- **Action Logs** menu

  Displays the Action Logs page. You can check the execution log of the Event Action.

- **Account Management** menu

Clicking this menu displays the sub menu related to the account management of Web Console.

Tip

Only users belonging to a group with Account Manager role can display and select menus.

- **Users** menu

  Displays the Users page. You can manage the user information.

- **Groups** menu

  Displays the Groups page. You can manage groups that define user roles.

- **System Settings** menu

Clicking this menu displays the sub menu related to the system settings.

Tip

Only users belonging to a group with Administrator role can display and select menus.

- **Node Mappings** menu

  Displays the Node Mappings page. It determines and manages whether the nodes managed by multiple products are physically identical or not.

- **Configuration Sync** menu

  Displays the Configuration Sync page. Synchronize configuration information between IMS component and the connected products.

Contents area

Displays the operation page corresponding to the selected menu.

Footer area

Displays the version and copyright information of the IMS component.

1.2.4 Updating own user information

This section describes the procedure to be used by the user logged in to Web Console to update own user information including the login password.

Tip

User Name and **Group** cannot be changed.

1. Display the Edit Profile page.

   Click  icon at the upper right of the page and select the **Edit Profile** menu.

2. Change own user information on the Edit Profile page.

   On the Edit Profile page, you can change the two settings of display information and password in the Web Console.

   - Display information
     - **Display Name**

       Specify the display user name on the page with arbitrary characters. The maximum number of characters is 128 characters.

       If omitted, also use the name specified by the **User Name** as the display name.

     - **Default Dashboard**

       By checking the check box in the list, select the definition of the first dashboard displayed after the user logs in.

       Tip

       If you have not added the definition of dashboard in advance, select from the built-in dashboards provided by the connected products.

   - Password
     - **Password (Old)**

       Specify the current password.

     - **Password**

       Specify a new password. The password must be specified at least 8 characters and consisted of a combination of single-byte alphanumeric characters and the symbol *“!"#$%&'()*+,./:;<=>?@[\]^_`{|}~ -”*.

     - **Password (Confirm)**

       For confirmation of input, specify the same password as specified by **Password**.

3. Save the changes.

   Confirm the changes and then click the **SAVE** button corresponding to the changes.

   A message indicating that the user information has been updated with the specified content is displayed.

1.2.5 Checking the newly occurred events

In the Web Console, even if you are viewing a page other than the Dashboard and Events pages, you can grasp whether there is a newly occurred event.

The following describes how to grasp a newly occurred event and confirm its contents.

1. Check whether there is a new notification.

   Check the state of the  **Notifications** icon at the upper right of the page.

   The displayed number indicates the number of events or messages that have newly occurred.

Tip

A message is a notice such as an error on the operation or processing of the Web Console.

2. Click the **Notifications** icon.

   The Notification list is displayed.

3. Check whether there is an event.

   If an event has occurred, a notification indicating the occurrence of the event is displayed in the Notification list. Also, in addition, the occurrence time and severity information for the events are displayed. From the notified severity information, you can grasp the urgency of the event.

4. Confirm the details of the event.

   To confirm the details of the event, click on the **Events** menu to display the Events page.Confirm the details of the event by comparing the event occurrence time with the display information on the Events page.

5. Delete the event whose contents have been confirmed from the list of notifications.

   By clicking the ✕ icon for the notification in the Notification list, you can delete the notification from the list. By clicking the **Clear all notifications** icon in the Notification list, you can delete all notifications in the Notification list.

Tip

- Up to 10 notifications will be made on the Notification list. If it exceeds 10, the oldest notification is deleted.
- If two or more events with the same severity occur at the same time, they are notified in one form.

1.2.6 Widget types

On the pages such as the Dashboard and Node Detail pages, various information, including the data traffic status, load of each node, and event occurrence status, is displayed in a chart or list by using the component called a widget. This section explains the widget types that are displayed on the Web Console.

The supported widgets are roughly classified into the following four types depending on the contents to display.

Line chart widgets

The temporal transition of the values of the target items within the specified period is displayed in a line chart. The ranks of the items within the specified period are displayed in a list.

For example, on the **Interface Utilization (IN) Top5** widget, the change in the utilization (%) of the top five network interfaces with high input utilization (%) is displayed in a line chart. In the list, the top five of the average utilization for network interfaces within the specified period is displayed in descending order.

"Figure 1-7 Line chart widget (page 16)" shows a sample line chart widget.

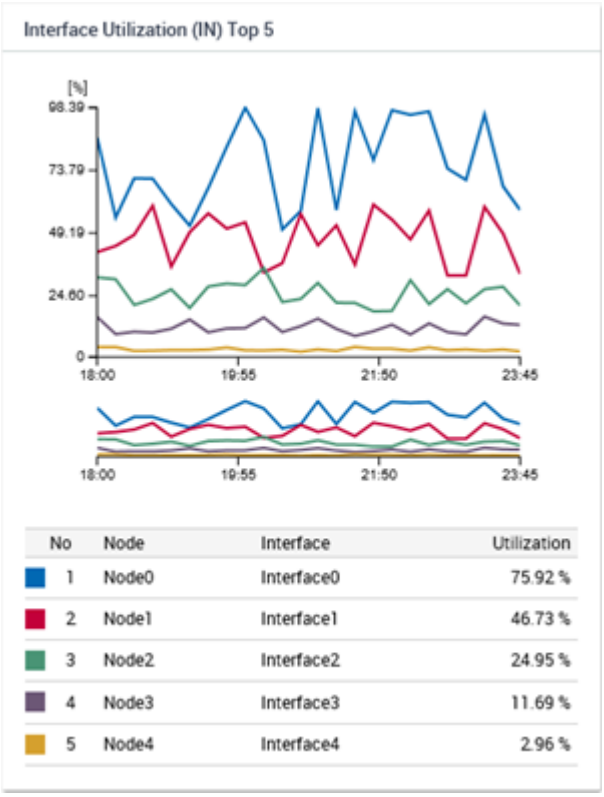

Figure 1-7 Line chart widget

The following display operations can be performed on the line chart widget.

- Zooming in on a line chart by using the **Range Selector**

  You can zoom in a line chart by narrowing down the time width with the **Range Selector** between the line chart and the list.

- Narrowing the display items by using the filtering settings

  You can narrow down the display items of the chart by clicking the mark showing the chart color to be placed on the left side of each item in the list.

Pie chart widgets

The proportion of the values of the target items within the specified period is displayed in a pie chart. Also, the ranks of the items within the specified period are displayed in the list.

For example, on the **Applications Top5** widget, among the flow information collected on the specified network interface, the traffic volume proportion of the top five applications with high traffic volume and other applications is displayed in a pie chart. In the list, the top five traffic volumes for network interfaces within the specified period are displayed in descending order.

"Figure 1-8 Pie chart widget (page 17)" shows a sample pie chart widget.

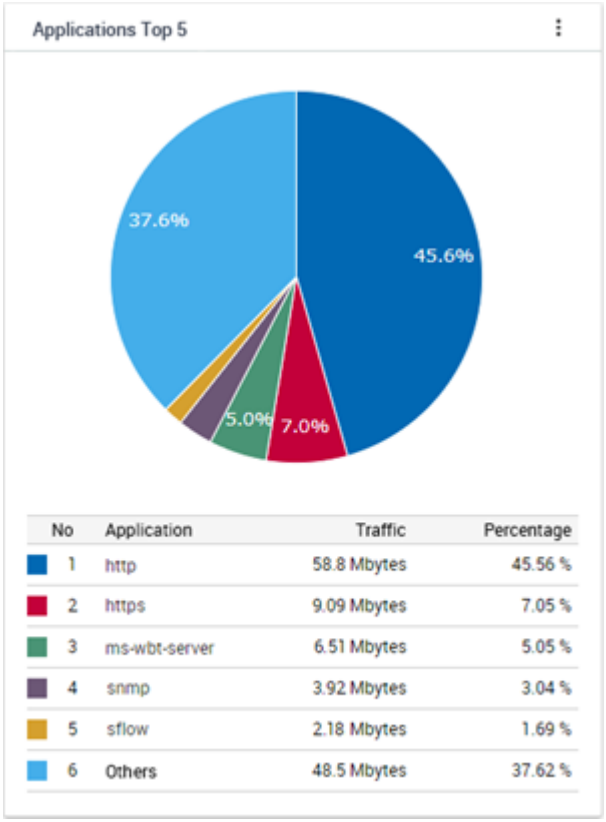

Figure 1-8 Pie chart widget

The following display operations can be performed on the pie chart widget.

- Switching to the line chart

  By clicking the ⋮ icon on the widget and operating, you can switch the display from a pie chart to a line chart, or from a line chart to a pie chart.

- Narrowing the display items by using the filtering settings

  You can display the pie chart excluding specific items by clicking the mark showing the chart color to be placed on the left side of each item in the list.

Tip

The above operations may not be performed for some target items. For example, on the **Ratio of Node Status** widget, the above two operations cannot be performed.

List widgets

Event information, node availabilities, etc. are displayed in a list.

For example, on the **Current Alert** widget, a list of fault events that have not yet been recovered is displayed.

"Figure 1-9 List widget (page 18)" shows a sample list widget.

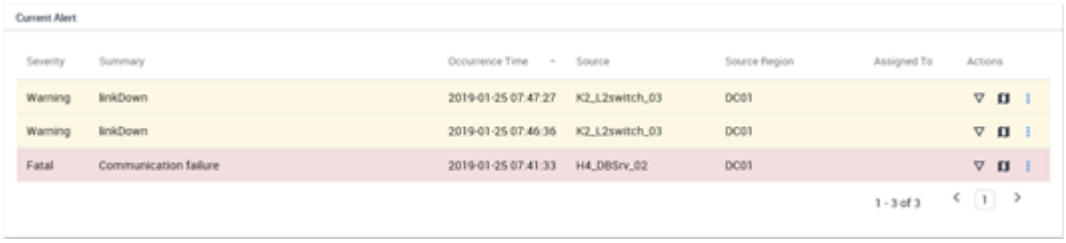

Figure 1-9 List widget

Other widgets

Depending on the features of individual pages, special types of widgets may be displayed.

On the Node Detail page, the **Operational Status** widget for the node that Network Manager is monitoring is displayed. This **Operational Status** widget displays a donut chart showing the availability of the node and a chart showing the change of the node status (severity) for time transition.

"Figure 1-10 Other widget (page 18)" shows a sample other widget.

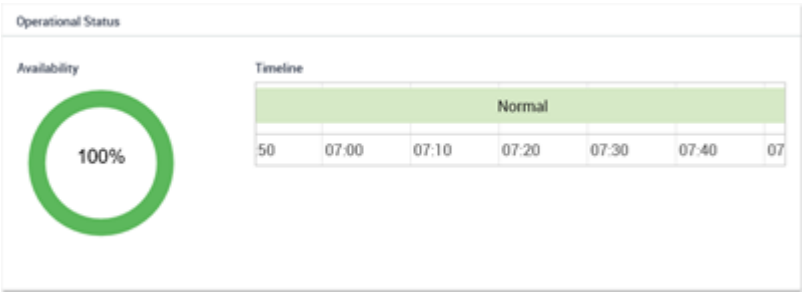

Figure 1-10 Other widget

1.2.7 Widget display contents

This section describes the information range that can be displayed on each widget and the behavior of the widget for various parameters of the page.

Range of the data to be aggregated for one widget

For the widgets displayed on the Dashboard page, the data is aggregated each region group and displayed in ranking (Top N). It does not display the ranking by aggregating the data of multiple region groups.

Tip

The following three widgets related to the occurrence status of fault events are exceptionally able to display data of all nodes that span multiple region groups in one widget.

- **Current Alert** widget
- **Ratio of Node Status** widget
- **Node Availabilities** widget

The Node Detail page displays data for the range of one selected node and the Network Interface Detail page displays data for the range of one selected network interface.

Specification of Period

For each page displaying the widget, specify the data range in **Period**. The granularity of data to be displayed varies depending on the time width of the specified period or the specified past time.

Tip

The following widgets always display the current status regardless of the specified value of **Period**.

- **Ratio of Node Status** widget

Specification of Top N (rank)

For each page displaying the widget, specify the data range with **Top N**. The specified number of the data is displayed in ascending or descending rank order (Top N) of the values within the specified period. In Web Console, data up to Top 20 can be displayed.

Tip

The following widgets display regardless of the specified value of **Top N**.

- **Events** widget
- **Current Alert** widget
- **Ratio of Node Status** widget

1.2.8 Basic operation of widgets

Clicking the link of listed items on each widget displays the page to check the details of the clicked item. Furthermore, each widget provides a mechanism to check the details of the displayed contents.

The following sections describes the basic operations of widgets.

1.2.8.1 Checking the details of the node

From the link of the node name displayed by the widget, you can easily display the Node Detail page for the node.

If the Node Detail page is displayed from a widget, **Period** specified on the previous page is kept.

Tip

On all pages including widgets, when clicking the node name link indicating the managed node, the Node Detail page for the node is displayed.

The specific procedure is described below using an example to display the Node Detail page from the **Node Availabilities** widget displayed on the Dashboard page.

1. Display the Dashboard page.

   Click **Dashboard** menu.

2. Specify **Period** on the Dashboard page.

   In this description, select **Past 24 hours** from the pull-down menu.

3. Check the contents of the **Node Availabilities** widget.

   Search for the nodes with low availability in the past 24 hours.

4. Select the node whose details you want to check.

   Click the node name link displayed on the **Node Availabilities** widget.

The Node Detail page for the node is displayed by specifying **Past 24 hours** for **Period**.

5. Identify the cause of low availability by referring to Events widget on the Node Detail page.

   The availability decreases if an event whose severity is **Fatal** occurs.

1.2.8.2 Checking the details of the network interface

From the link of the network interface name displayed by the widget, you can easily display the Network Interface Detail page for the network interface.

If the Network Interface Detail page is displayed from a widget, **Period** specified on the previous page is kept.

Tip

On all pages including widgets, when clicking the link of the network interface name, the Network Interface Detail page for the network interface is displayed.

The specific procedure is described below using an example to display the Network Interface Detail page from the **Interface Utilization (IN)** widget displayed on the Dashboard page.

1. Display the Dashboard page.

   Click **Dashboard** menu.

2. Specify **Period** on the Dashboard page.

   In this description, select **Past 24 hours** from the pull-down menu.

3. Check the contents of the **Interface Utilization (IN)** widget.

   Search for network interfaces with high input utilization in the past 24 hours.

4. Select the network interface whose details you want to check.

   Click the link of the network interface name displayed on the **Interface Utilization (IN)** widget.

   The Network Interface Detail page for the network interface is displayed by specifying **Past 24 hours** for **Period**.

5. Identify the cause of high utilization by referring to **Flow Data** on the Network Interface Detail page.

   It is possible to identify the cause of an increase in the utilization from the information of the **Applications** and **Conversations** widgets.

If you want to investigate the communication traffic in more detail, click the **FLOW ANALYZE** button to access to Web Console of the NFA.

1.2.8.3 Checking the details of the flow information

The Exporter Analysis page of the NFA can be displayed easily by clicking the link of the flow information displayed in the widget, such as the IP address of the endpoint or the application name.

If the Exporter Analysis page of the NFA is displayed from a widget, **Period** specified on the previous page is kept. In addition, the contents of the clicked item and the like are automatically set to **Filter Conditions** when Exporter Analysis page is displayed.

The specific procedure is described below using an example to display the Exporter Analysis page of the NFA from the **Applications** widget displayed on the Node Detail page.

1. Display the Node Detail page.

   Click **Nodes** menu. On the displayed Nodes page, click the node name link of the node for which you want to check the details.

2. Specify **Period** on the Node Detail page.

   In this description, select **Past 24 hours** from the pull-down menu.

3. Check the contents of the **Application** widget.

   Check the applications with high communication traffic in the past 24 hours.

4. Select the application for which you want to check the details.

   Click the link of the application name displayed on the **Applications** widget.

   In this case, Exporter Analysis page of the NFA is displayed by specifying the node in **Target Exporter** and the application in **Filter Conditions**. and **Period** is specified as **Past 24 hours**.

5. Identify the cause of high communication traffic by referring to each widget of the Exporter Analysis page.

   It is possible to identify the cause of an increase in the communication traffic from the information such as the **Conversations** widget.

1.2.8.4 Filtering the items displayed on a chart

For line chart and pie chart widgets, the filtering function allows you to exclude some of the items currently being displayed from the display targets.

Filtering is useful if you want to make a chart more visible by temporarily hiding some items so that you can focus on the desired items.

For example, if you want to compare the 10th to 20th items of the Top 20, you can make a chart more visible by excluding the 1st to 9th items. The specific steps are shown below.

Tip

When operating the following, it is recommended to specify **Nothing** for **Update interval** of the displayed page. Updating the displayed page resets the filter settings described later.

1. On the target widget, set the filtering of display items.

   It is possible to be excluded the display items of the chart by clicking the mark showing the chart color to be placed on the left side of each item in the list on the widget.

2. Check that the selected item has been excluded on the chart.

If you want to exclude multiple items, repeat the above steps.

Click the mark of the exclusion item again to return the chart of that item to the display target.

1.2.8.5 Zooming in on a line chart

For line chart widgets, a chart can be zoomed in on by reducing the the time width of the line chart that shows the entire specified period.

To narrow down the time width from the range specified in **Period** on the display page and check the details of communication traffic, perform the following operations.

Tip

When operating the following, it is recommended to specify **Nothing** for **Update interval** of the displayed page. Updating the displayed page resets the setting of **Range Selector** that is described later.

1. Select the time width to display using the lower line chart (called the **Range Selector**) that shows the overall period.

   Specify the display range with drag-and-drop.

   The display of the upper line chart is switched to the range selected by the **Range Selector**.

2. Specify the display range in detail.

   When specifying the display range in detail, perform the following operations.

   - Adjust the time width by drag-and-drop the left and right border lines in the range specified by the **Range Selector**.
   - Drag-and-drop the area specified by the **Range Selector**, and change the displayed area itself.
   - Cancel the display range by clicking outside of the area specified by the **Range Selector** and specify a new display range by drag-and-drop.

     ### Tip

     It is possible to specify the display range simply by dragging the area outside the display range without canceling the display range.

The operation of the **Range Selector** is reflected only in the display of the line chart. The display content of the list does not change.

1.2.8.6 Changing the IP address display to the hostname

When the IP address of the endpoint in the flow information is displayed, it is possible to change to the display of the corresponding hostname.

To change the IP address that indicates an endpoint to the corresponding hostname, the NFA that receives flow information must be able to inquire about the hostname to the Domain Name System (DNS) that manages hostnames and IP addresses of endpoints via the network.

Tip

- For an endpoint that is not registered to the DNS, the IP address will be displayed as is because inquiries about hostnames will fail.
- The hostname to be displayed instead of an IP address by executing the following procedure is the hostname that is obtained from the DNS when the NFA receives the analysis target flow information, not the hostname obtained by executing this procedure. Therefore, when analyzing the past communication status, if the previous hostname at reception of the analysis target flow information differs from the current hostname, the previous hostname is displayed.

The following steps show how to change an IP address of an endpoint for flow information to a hostname.

1. Click the ⋮ icon of the target widget.

   When clicking on the ⋮ icon, a check box of the display items is displayed.

2. Select the check box of the **Show Hostname**

   The IP address of the endpoint changes to the hostname.

To display the IP address again, clear the **Show Hostname** check box according to the above steps.

1.2.8.7 Changing the chart type

For a pie chart widget, it is possible to change the display from a pie chart to a line chart and vice versa.

With this operation, it is possible to check both the proportion and the temporal transition for the communication traffic of each item within the specified period from the information of one widget. The specific steps are shown below.

⚠ Caution

The **Ratio of Node Status** widget is a pie chart widget, but it is impossible to change the chart type.

1. Click the ⋮ icon of the target widget.

   When clicking on the ⋮ icon, a check box of the display items is displayed.

2. Clear the check box of the **Show Pie Chart**.

   The pie chart of the widget changes to a line chart. In changing the chart type in this procedure, if you move to another page or update the entire page by pressing F5 key, you will return to the default chart type.

When defining a line chart widget as the default graph type, you can change the chart type to a pie chart by checking the **Show Pie Chart** check box with the same procedure.

1.2.9 Operations of specific widgets

Some widgets provide a mechanism to display unique links and icons according to the type of widget so that widget specific operations can be performed.

This section describes specific operations that can be performed only for specific widgets.

1.2.9.1 Performing operations related to the event

For **Current Alert** and **Events** widgets, it is possible to perform specific operations on occurred events.

The following describes the details of the operation for the events.

Checking the details of an event

For **Current Alert** and **Events** widgets, it is possible to check the details of an event by displaying the Event Detail dialog box.

In the list of events displayed by the **Current Alert** and **Events** widgets, since it is the primary purpose to grasp the state of failure occurrence, only the summary information of the event that occurred is displayed. To check the details of a specific event, display the Event Detail dialog box.

The specific procedure is described below using an example operation of the **Current Alert** widget.

1. Display the Dashboard page.

   Click **Dashboard** menu.

2. Check the contents of the **Current Alert** widget.

   The **Current Alert** widget displays the currently occurring fault events.

3. Display the Event Detail dialog box of the event to be checked.

   Click the **Event Detail** icon in the **Actions** column of the target event.

4. Check the contents of the Event Detail dialog box.

   The Event Detail dialog box displays the following information.

   - **Summary**

     Displays summary information of the event.

   - **Severity**

     Displays the severity of the event. For details about the severity of events displayed in Web Console, refer to "4.2.1.3 Event severity levels (page 89)".

   - **Recovery Status**

     Displays the recovery status of the event. **Unrecovered** is displayed for currently occurring events.

   - **Occurrence Time**

     Displays the occurrence time of the event.

   - **Source**

     Displays the name of the node and network interface as the source of the event. Also, the IP address of the relevant node and the region group to which the node belongs are displayed.

     Caution

     The value of the IP address to be notified as the source of the event is the value of the IP address managed by the product that detected the event. Therefore, depending on the environment, it may be different from the IP address value managed by the IMS component displayed on the Node Detail page of the Web Console.

     Clicking the **Topology Map** icon displays the topology map in which the node where the event occurred is placed.

     Tip

     - The **Topology Map** icon is displayed when using the Network Manager.
     - In case of the Event Detail dialog box activated from the **Current Alert** widget, the Topology Map page is displayed in the **normal mode** displaying the current situation. Otherwise, the Topology Map page is displayed in the **analysis mode** which can display the situation at the time of the event occurrence, and the **Period** is set a period centered on the occurrence time of the event.
     - If the node is located on multiple maps, a dialog box to select the map to be displayed is displayed.

   - **Assigned To**

     The user name (display name) responsible for handling the event is displayed. If no one is assigned, it will be blank.

   - **Detail**

     Displays the detail of the event.

   - **Action**

Displays the action for the event.

- **Application Name**

  Displays the application name that detected the event. This application name indicates the name of the product connected to the IMS component.

Performing operations on the event

For **Current Alert** and **Events** widgets, the operations can be performed for the event displayed in the list.

In the Web Console, the following operations are possible for the notified events.

- Assign yourself as responsible for event handling
- Cancel assignments responsible for event handling
- Recover the state of the event
- Delete the event

The specific procedure is described below using an example operation of the **Current Alert** widget.

1. Display the Dashboard page.

   Click **Dashboard** menu.

2. Check the contents of the **Current Alert** widget.

   The **Current Alert** widget displays the currently occurring fault events.

3. Check the details of the event as necessary.

   Click on the **Event Detail** icon to display the Event Detail dialog box and check the details of the event.

4. Perform the operation on the event.

   Click the icon for the event to display the following menu.

   - **Assign me** menu

     Assign yourself as responsible for event handling. When selected, your user name is registered in the **Assign To** field for the event. also, it is possible to perform the operation for the assigned event.

   - **Unassign** menu

     Cancel assignments responsible for event handling. When selected, The **Assign To** field for the event is blank. It is also possible to cancel assignment other than yourself.

   - **Recover event** menu

     Recover the state of the event. When selected, the **Recovery Status** of the event changes from **Unrecovered** to **Recovered** and The display of the event on the **Current Alert** widget disappears.

     Tip

     Depending on the specification of the product that detected the event, there are events where the recovery operation cannot be performed. For such the event, the recovery state is automatically detected and recovery processing is performed

   - **Delete event** menu

Delete the event. When selected, the event is deleted and the display of the event in the list disappears.

When the above menu is selected, the Confirmation dialog box will be displayed. After confirming the contents, processing is executed by clicking the **OK** button.

5. Check the contents of the **Current Alert** widget after the operation.

   Confirm that the operation of the selected menu is being processed properly in the list of events.

Checking the influence of the event on the topology map

For **Current Alert** and **Events** widgets, you can easily display the Topology Map page where the source node is registered from the displayed event.

On the Topology Map page, the influence range of the occurred event can be checked directly by referring to the connections among nodes.

The specific procedure is described below using an example of a Topology Map page that is displayed on the **Current Alert** widget on the Dashboard page.

1. Display the Dashboard page.

   Click **Dashboard** menu.

2. Check the contents of the **Current Alert** widget.

   The **Current Alert** widget displays the currently occurring fault events.

3. Display the Topology Map page for the event whose influence range is to be checked.

   Click the **Topology Map** icon in the **Actions** column of the target event.

   If the node where the event occurred is registered in a single map, the Topology Map page to which the node is registered is displayed.

   If the node where the event occurred is registered in multiple maps, a list of display candidate maps is displayed. Click the link of the map to display the Topology Map page.

   Tip

   - From the **Current Alert** widget, the Topology Map page is displayed in **normal mode**.
   - From the **Events** widget, the Topology Map page is displayed in **analysis mode** and the **Period** is set a period centered on the occurrence time of the event. This enables users to check the state of the map where the event occurred.

4. Check the nodes around the relevant node on the Topology Map page.

   Investigate the influence on the entire network by checking the nodes adjacent to the node in which the event occurred and nodes next to the adjacent nodes.

1.2.9.2 Checking the nodes with the specified status in a list

The **Ratio of Node Status** widget allows users to easily search for the nodes with the specified state.

On the **Ratio of Node Status** widget, the current state of the managed nodes is shown by the number and percentage of nodes to severity. The following describes how to check the nodes in each severity level.

1. Check the contents of the **Ratio of Node Status** widget on the Dashboard page.

The **Ratio of Node Status** widget displays the current severity states of the managed nodes.

2. Click the link with the severity you want to check for the specific node name.

   When clicking on the severity link of **Ratio of Node Status** widget, the Nodes page is displayed with severity specified for the **Search Conditions**.

   The displayed node list shows the specific node name currently in the state of the specified severity.

Chapter 2. Environment Settings Before Operations

This chapter describes how to configure the environment before using and operating the Web Console.

Contents

2.1 Managing users

The following describes how to manage users who log in to the Web Console.

2.1.1 Groups and users

This section describes the relationship between and operation authorities of groups and users in user management.

Users who operate the Web Console must belong to a group. The users can operate the Web Console within the scope of the role assigned to that group. The operation range of users can be managed by creating multiple groups that have different roles and assigning users to an appropriate group.

There are the following three roles to be assigned to groups.

- Administrator
- Operator
- Observer

Details about each role and authority are as follows:

Administrator

It has the role for all operations and management using the Web Console. And it has the authority of reference, operation, and definition on all pages.

In addition, it is possible to be assigned **Account Manager** role. When **Account Manager** is assigned, it is possible to perform operations for group and user management.

Operator

It has the role of performing network monitoring operation using the Web Console. And it has the authority of reference and operation on each page.

Tip

The *"operation"* in the above description means execution of processes on each page. For example, event checking and recovery processing can be executed.

Observer

It has the role of observing the status of the network using the Web Console. And it only has the authority of reference on each page.

2.1.2 Managing the group information

This section describes the page that manages the information of the group to which the user belongs, and the operation on that page.

Tip

Only users belonging to a group with Account Manager role can manage the group information.

2.1.2.1 Groups page

The Groups page is described below.

The Groups page allows users to check the information of groups, and operate (add, edit, and delete) the groups.

Click **Account Management**>**Groups** to display the Groups page.

Tip

Only users belonging to a group with Account Manager role can display the Groups page.

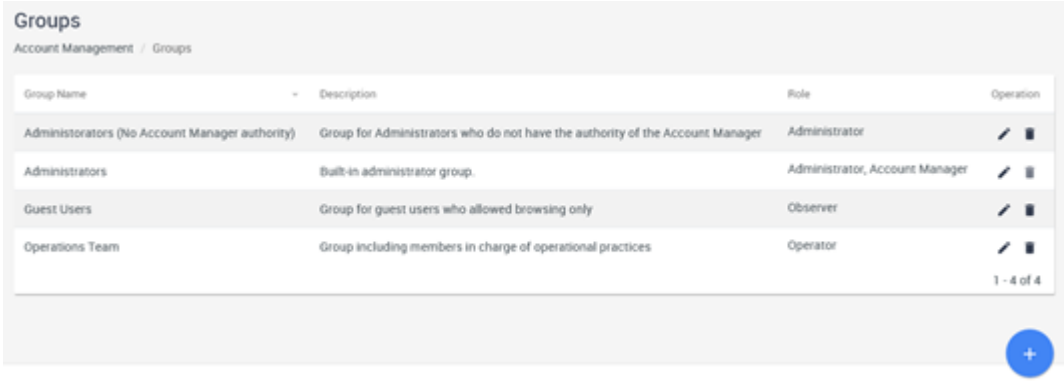

Figure 2-1 Groups page

- **NEW GROUP** button

  Adds a new group. Clicking the **NEW GROUP** button displays the New Group page. For details, refer to "2.1.2.2 Adding a group (page 31)".

Group list

- **Group Name**

  Displays the group name.

- **Description**

  Displays the description of the group.

- **Role**

  Displays the roles assigned to the group.

- **Operation**

  Clicks each icon to operate the group.

  - **Edit** icon

    Changes the group information. Clicking the **Edit** icon displays the Edit Group page. For details, refer to "2.1.2.3 Updating the group (page 31)".

  - **Delete** icon

    Deletes the group information. For details, refer to "2.1.2.4 Deleting the group (page 32)".

    ### Caution

    Group *"Administrators"* registered from the initial state can not be deleted.

2.1.2.2 Adding a group

The following describes how to add a new group.

The specific procedure is described below using an example of how to add a group named *"Operations team"* as a group for members in charge of operational practices.

1. Display the Groups page.

   Click **Account Management**>**Groups**.

2. Click the **NEW GROUP** button.

   The New Group page is displayed.

3. On the New Group page, specify the following appropriately.

   - **Group Name**

     Specify a unique group name. Up to 128 characters are available. It is impossible to specify a duplicate name as an existing group name.

     In this example, *"Operations team"* is specified.

   - **Description**

     Specify the description of the group. Up to 512 characters are available.

     In this example, *"Group including members in charge of operational practices"* is specified.

   - **Role**

     Select one of the following role to be assigned to the group.

     - **Administrator**
     - **Operator**
     - **Observer**

     For details about the roles, refer to "2.1.1 Groups and users (page 29)".

     In this example, *" **Operator** "* is selected.

     Tip

     When **Administrator** is selected, it is possible to select whether to assign **Account Manager**.

4. Save the group information.

   Confirm the settings and then click the **SAVE** button.

   The group is newly added with the specified contents.

On the Groups page, check that *"Operations team"* has been added as a group.

2.1.2.3 Updating the group

The following describes how to update the contents of the registered group.

The specific procedure is described below using an example of how to change the description of *"Operations team"*.

1. Display the Groups page.

Click **Account Management**>**Groups**.

2. Click the **Edit** icon of *"Operations team"* to be updated.

   The Edit Group page for *"Operations team"* is displayed.

3. Change the contents of the target item on the Edit Group page.

   All of the following items can be changed the contents.

   - **Group name**

     Specify a unique group name. Up to 128 characters are available. It is impossible to specify a duplicate name as an existing group name.

     This item is not changed in this example.

   - **Description**

     Specify the description of the group. Up to 512 characters are available.

     In this example, the contents to *"Group including members in charge of network management operation"* are changed.

   - **Role**

     Select one of the following role to be assigned to the group.

     - **Administrator**
     - **Operator**
     - **Observer**

     For details about the roles, refer to "2.1.1 Groups and users (page 29)".

     This item is not changed in this example.

     Tip

     When **Administrator** is selected, it is possible to select whether to assign **Account Manager**.

4. Save the changed contents.

   Confirm the changes and then click the **SAVE** button.

   The group is updated with the specified contents.

On the Groups page, check that the **Description** of *"Operations team"* has been updated with the specified contents.

2.1.2.4 Deleting the group

The following describes how to delete the registered group.

1. Display the Groups page.

   Click **Account Management**>**Groups**.

2. Click the **Delete** icon of the group to be deleted.

   The Confirmation dialog box for the deletion is displayed.

Caution

If users are registered in the group specified to be deleted, the group cannot be deleted. Move all users registered in the group to another group and then delete the group.

3. Check the contents on the Confirmation dialog box.
4. Perform the deletion.

   Click the **OK** button on the Confirmation dialog box.

   The specified group information is deleted from the group list of the Groups page.

2.1.3 Managing the user information

This section describes the page to manage information of users and how to operate user information.

Tip

Only users belonging to a group with Account Manager role can managing the user information.

2.1.3.1 Users page

The Users page is described below.

The Users page allows users to check the information of users, and operate (add, edit, and delete) the users.

Click **Account Management**>**Users** to display the Users page.

Tip

Only users belonging to a group with Account Manager role can display the Users page.

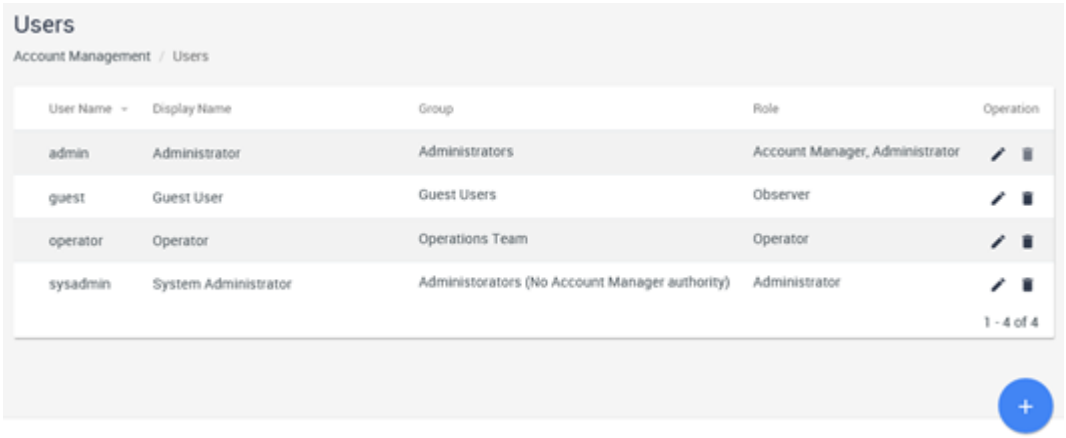

Figure 2-2 Users page

- **NEW USER** button

  Adds a new user. Clicking the **NEW USER** button displays the New User page. For details, refer to "2.1.3.2 Adding a user (page 34)".

User list

- **User Name**

  Displays the name to identify the registered user.

- **Display Name**

  Displays the setting value of the user display name to be displayed at login.

- **Group**

  Displays the name of the group to which the user belongs.

- **Role**

  Displays the roles assigned to the group to which the user belongs.

- **Operation**

  Click each icon to operate the user.

  - **Edit** icon

    Changes the user information. Clicking the **Edit** icon displays the Edit User page. For details, refer to "2.1.3.3 Updating the user information (page 35)".

  - **Delete** icon

    Deletes the user information. For details, refer to "2.1.3.4 Deleting the user (page 36)".

    Caution

    User *"admin"* registered from the initial state can not be deleted.

Tip

If it detects more than five login failures in 30 minutes, the user is locked and can not log in for 30 minutes.

The icon is displayed at the left of the name for users who are in locked state. Locking of user information is automatically release after 30 minutes, but you can immediately release the locked state by clicking the icon.

2.1.3.2 Adding a user

The following describes how to add a new user.

The specific procedure is described below using an example of how to add *"tyamada"* to *"Operations team"*.

1. Display the Users page.

   Click **Account Management**>**Users**.

2. Click the **NEW USER** button.

   The New User page is displayed.

3. On the New User page, specify the following appropriately.

   - **User Name**

     Specify a unique user name by using single-byte alphanumeric characters. Up to 64 characters are available. It is impossible to specify a duplicate name as an existing user name.

     In this example, *"tyamada"* is specified.

   - **Display Name**

     Specify a user name to be displayed on the page. Up to 128 characters are available.

If this is omitted, the name specified for **User Name** is used as the display name.

In this example, *"Taro Yamada"* is specified.

- **Password**

  Specify the initial password of the user to be registered. The password must be specified at least 8 characters and consisted of a combination of single-byte alphanumeric characters and the symbol *"!"#$%&'()*+,./:;<=>?@[\]^_`{|}~ -"*.

- **Password (Confirm)**

  Specify the same password as specified by **Password**.

- **Group**

  From the created groups, select the group to which the user will belong.

  In this example, *"Operations team"* is selected.

- **Default Dashboard**

  Select the definition of the first dashboard displayed after the user logs in.

  Tip

  If you have not added the definition of dashboard in advance, select from the built-in dashboards provided by the connected products.

4. Save the user information.

   Confirm the settings and then click the **SAVE** button.

   The user is newly added with the specified contents.

On the Users page, Check that the user *"tyamada"* belonging to the group *"Operations team"* has been added.

2.1.3.3 Updating the user information

The following describes how to update the contents of the registered user.

The specific procedure is described below using an example of how to change the group to which *"tyamada"* belongs to *"Administrators"*.

Tip

User Name cannot be changed.

1. Display the Users page.

   Click **Account Management**>**Users**.

2. Click the **Edit** icon of *"tyamada"* whose information is to be updated.

   The Edit User page for *"tyamada"* is displayed.

3. Change the contents of the update target items on the Edit User page.

   - **Display Name**

     Specify a user name to be displayed on the page. Up to 128 characters are available.

     If this is omitted, the name specified for **User Name** is used as the display name.

   - **Password**

Specify the initial password of the user to be registered. The password must be specified at least 8 characters and consisted of a combination of single-byte alphanumeric characters and the symbol *"!"#$%&'()*+,./:;<=>?@[\]^_`{|}~ -"*.

- **Password (Confirm)**

  Specify the same password as specified by **Password**.

- **Group**

  From the created groups, select the group to which the user will belong.

  In this example, *"Administrators"* is selected as a new group to which the user will belong.

- **Default Dashboard**

  Select the definition of the first dashboard displayed after the user logs in.

  Tip

  If you have not added the definition of dashboard in advance, select from the built-in dashboards provided by the connected products.

4. Save the changed contents.

   Confirm the changes and then click the **SAVE** button.

   The user information is updated with the specified contents.

On the Users page, check that the group to which *"tyamada"* belongs has been changed to *"Administrators"*.

2.1.3.4 Deleting the user

The following describes how to delete the registered user.

1. Display the Users page.

   Click **Account Management**>**Users**.

2. Click the **Delete** icon of the user to be deleted.

   The Confirmation dialog box for the deletion is displayed.

3. Check the contents on the Confirmation dialog box.

4. Perform the deletion.

   Click the **OK** button on the Confirmation dialog box.

   The specified user information is deleted from the user list of the Users page.

2.2 Setting the action when an event is detected

Some action can be executed when an event occurs. This section describes the environment settings that must be configured in advance to execute actions, the conditions of events subject to the actions, and how to set the actions.

Define the following two elements in the action (event action) definition for an event.

- Event condition to execute the corresponding action

  Define the condition for filtering event information, such as a severity, occurrence time, and node name, to determine whether to execute the action.

- Contents of the action to be executed

  Define the contents of the action such as notification of the event contents by email and execution of the command on the server where the IMS component is installed.

2.2.1 Configuring the environment settings prior to definition of event actions

This section describes the environment setting to be configured before defining event actions.

To perform notification by email as an action, the mail server to be used must be registered before defining the event action. The following sections describe how to manage information of the mail server to be used by the action.

2.2.1.1 Email Servers page

The Email Servers page is described below.

The Email Servers page allows users to check the contents of the mail servers to be used, and operate (register, edit, and delete) the mail servers.

Click **Event Action Settings**>**Mail Server** to display the Email Servers page.

Tip

Only users with the Administrator authority can display the Email Servers page.

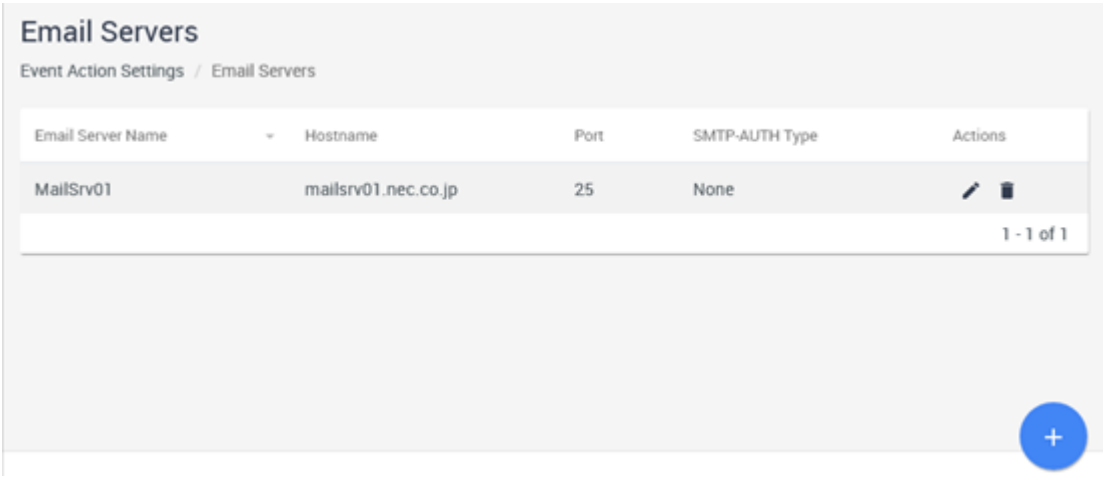

Figure 2-3 Email Servers Page

- **NEW EMAIL SERVER** button

  Click this icon to register a new mail server. Clicking the **NEW EMAIL SERVER** button displays the New Email Server page. For details, refer to "2.2.1.2 Adding an mail server (page 38)".

Email server list

- **Email Server Name**

  Displays the mail server name.

- **Hostname**

  Displays the domain name (FQDN) or IP address of the mail server.

- **Port**

  Displays the port number to be used in mail transmission

- **SMTP-AUTH Type**

  Displays the SMTP authentication method of the mail server.

- **Actions**

  Click each icon to operate the mail server.

  - **Edit** icon

    Click this icon to change the registered mail server information. Clicking the **Edit** icon displays the Edit Email Server page. For details, refer to "2.2.1.3 Updating the mail server (page 39)".

  - **Delete** icon

    Click this icon to delete the mail server information. For details, refer to "2.2.1.4 Deleting the mail server (page 40)".

2.2.1.2 Adding an mail server

The following describes how to register a new mail server.

1. Display the Email Servers page.

   Click **Event Action Settings**>**Email Servers**.

2. Click the **NEW EMAIL SERVER** icon.

   The New Email Server page is displayed.

3. On the New Email Server page, specify the following appropriately.

   - **Email Server Name**

     Specify a unique mail server name. Up to 64 characters are available.

   - **Hostname**

     Specify the domain name (FQDN) or IP address of the mail server. Up to 128 characters are available.

   - **Port**

     Specify the port number to be used in mail transmission from 1 to 65,535.

   - **Source Email Address**

     Specify the sender's e-mail address used for e-mail notification. Up to 64 characters are available.

   - **SMTP-AUTH Type**

     Select the authentication method from the following:

     - **None**

       SMTP authentication is not used to access the mail server.

     - **LOGIN**

       LOGIN authentication is used to access the mail server.

- **PLAIN**

  PLAIN authentication is used to access the mail server.

The following information for authentication is required when **LOGIN** or **PLAIN** is selected.

- **Username**

  Specify the account name to be used for authentication of the mail server. Up to 36 characters are available.

- **Password**

  Specify the password of the account name to be used for authentication of the mail server. Up to 64 characters are available.

4. Save the mail server information.

   Confirm the settings and then click the **SAVE** button.

   The mail server is newly registered with the specified contents.

On the Email Servers page, check that the mail server information has been added.

2.2.1.3 Updating the mail server

The following describes how to update the information of the registered mail server.

1. Display the Email Servers page.

   Click **Event Action Settings**>**Email Server**.

2. Click the **Edit** icon of the mail server to be updated.

   The Edit Email Server page for the relevant mail server is displayed.

3. Change the contents of the update target items on the Edit Email Server page.

   The contents of the following items can be changed.

   - **Email Server Name**

     Specify a unique mail server name. Up to 64 characters are available.

   - **Hostname**

     Specify the domain name (FQDN) or IP address of the mail server. Up to 128 characters are available.

   - **Port**

     Specify the port number to be used in mail transmission from 1 to 65,535.

   - **Source Email Address**

     Specify the sender's e-mail address used for e-mail notification. Up to 64 characters are available.

   - **SMTP-AUTH Type**

     Select the authentication method from the following:

     - **None**

       SMTP authentication is not used to access the mail server.

     - **LOGIN**

LOGIN authentication is used to access the mail server.

- **PLAIN**

  PLAIN authentication is used to access the mail server.

The following information for authentication is required when **LOGIN** or **PLAIN** is selected.

- **Username**

  Specify the account name to be used for authentication of the mail server. Up to 36 characters are available.

- **Password**

  Specify the password of the account name to be used for authentication of the mail server. Up to 64 characters are available.

4. Save the changes.

   Confirm the changes and then click the **SAVE** button.

   The mail server information is updated with the specified contents.

Display the Edit Email Server page to check that the changes have been reflected correctly.

2.2.1.4 Deleting the mail server

The following describes how to delete the information of the registered mail server.

Caution

The mail server that is used in the event definition cannot be deleted.

1. Display the Email Servers page.

   Click **Event Action Settings**>**Email Server**.

2. Click the **Delete** icon of the mail server to be deleted.

   The Confirmation dialog box for the deletion is displayed.

3. Check the contents on the Confirmation dialog box.

4. Start the deletion.

   Click the **OK** button on the Confirmation dialog box.

   The specified mail server information is deleted from the user list of the Users page

2.2.2 Setting the event action definition

This section describes event conditions to execute an action and an event definition that defines the contents of the action.

In an event definition, multiple event conditions to execute an action and contents of the actions can be defined. For the event conditions to execute an action, for example, the severity and occurrence time can both be specified. For the actions to be executed, for example, e-mail report and execution of a command can both be defined.

Multiple event action definitions can be registered. An action specific to each event can be defined. If multiple event action definitions are registered, it is determined which event action definition is to be executed by comparing the occurred event with the event action definitions in order from the one with the highest execution priority.

The event action definitions are managed on the Event Actions page.

2.2.2.1 Event Actions page

The Event Actions page is described below.

The Event Actions page allows users to check the contents of event action definitions, and operate (register, edit, and delete) the event action definitions.

Click **Event Action Settings**>**Event Actions** to display the Event Actions page.

Tip

Only users with the Administrator authority can display the Event Actions page.

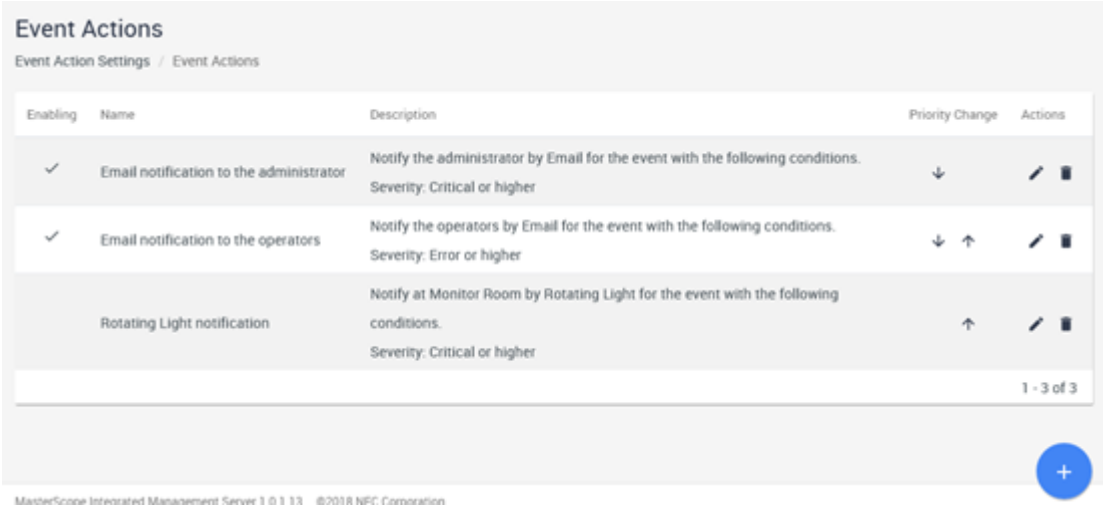

Figure 2-4 Event Actions Page

- **NEW EVENT ACTION** button

  Click this icon to register an event action definition. Clicking the **NEW EVENT ACTION** icon displays the New Event Action page. For details, refer to "2.2.2.2 Adding an event action definition (page 42)".

Event action definition list

- **Enabling**

  Displays whether the event action definition is enabled. The ✓ mark is displayed for the enabled event action.

  Enable or disable event actions on the Edit Event Action page.

- **Name**

  Displays the event action definition name.

- **Description**

  Displays the description of the event action definition.

- **Priority Change**

  Change the processing priority of event action definitions. Event action definitions are processed in order from the top of the list.

- **Increase Priority** icon

  Increases the priority of this event action by one.

- **Decrease Priority** icon

  Decreases the priority of this event action by one.

- **Actions**

  Click each icon to operate the event action definition.

  - **Edit** icon

    Click this icon to change the registered event action definition information. Clicking the **Edit** icon displays the Edit Event Action page. For details, refer to "2.2.2.3 Updating the event action definition (page 48)".

  - **Delete** icon

    Click this icon to delete the event action definition. For details, refer to "2.2.2.4 Deleting the event action definition (page 52)".

2.2.2.2 Adding an event action definition

The following describes how to add an event action definition.

The specific procedure is described below using an example to create a definition to execute the following event actions.

- Send a report of events with **Severity** of **Warning** or higher to the operators' mailing list at *"nw_operator_ml@xx.zz.com"*.
- If there are events with **Severity** of **Critical** or higher, also send a report of events to the administrators' mailing list at *"nw_admin_ml@xx.zz.com"*.

1. Display the Event Actions page.

   Click **Event Action Settings**>**Event Actions**.

2. Click the **NEW EVENT ACTION** icon.

   The New Event Action page is displayed.

3. On the New Event Action page, specify the appropriate values as below.

   Create an event action definition to send a report of events with **Severity** of **Warning** or higher to the operators' mailing list at *"nw_operator_ml@xx.zz.com"*.

   a. Specify the basic information of the event action definition.

      - **Name**

        Specify a unique event action name. Up to 64 characters are available.

      - **Description**

        Specify the description of the event action definition. Up to 1,024 characters are available.

      - **Enable this event action.** check box

        - When selected

          The event action definition becomes enabled. Usually, select this check box.

- When not selected

  The event action definition becomes disabled. When disabled, this event action is not processed. It is useful when you want to disable the event action temporary.

- **If the condition of this event match, the following event action will be stopped.** check box
  - When selected

    After the action is executed because it matches the specified event conditions, the event conditions will not be checked against other event action definitions and the process will stop.
  - When not selected

    Even after the action is executed because it matches the specified event conditions, the event conditions will be checked against other event action definitions.

In this example, specify the summary information as follows.

- **Event Action Name**

  "Email report (for operators)"
- **Description**

  "Definition to report operators by sending e-mail of events with the severity of Warning or higher."
- **Enable this event action.** check box: Select
- **If the condition of this event match, the following event action will be stopped.** check box: Select

b. Specify the event conditions to execute the corresponding action.

- How to add or remove event conditions

  A new condition can be added from the pull-down menu by clicking the **Select** button.

  To remove the added condition, click the − icon displayed at the beginning of it.
- How to specify event conditions

  Set the conditions to the items in the event data by using the following two methods. The setting method differs depending on the selected item.
  - Specification by selecting a check box

    Set the condition by using the check box displayed according to the selected item. This specification method is available for the following items.
    * Target items:

      Severity
  - Specification by using a keyword

    Specify a keyword and collation method for the selected item. This specification method is available for the following items.
    * Target items:

Summary, **Detail**, **Action**, **Source Node**, **Source Interface**, **Source Region**, **IPv4 Address**, **IPv6 Address**, **Application Name**

The following collation methods are available.

* Collation methods:

  is (match), **is not** (not match), **contains** (included), **does not contain** (not included), **starts with** (forward match), **ends with** (backward match)

  In **IPv4 Address** and **IPv6 Address**, you can only specify **is** (match) and **is not** (not match).

Tip

If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

In this example, the event condition is specified with the following settings.

- **Severity**

  Select the following check boxes.

  Fatal, **Critical**, **Error**, **Warning**

c. Specify the contents of the action to be executed.

Select the action type from the followings.

- **Email**

  The contents of the event that matches the event condition are sent to the specified destination by e-mail. Click the + icon on the side of **Email** and then specify the following items.

  - **Action Name**

    Specify the name to identify the action. Up to 128 characters are available.

    Action Name is used as identification information of the execution content in the action log.

  - **Email Server Name**

    Select a mail server from the pre-set mail servers.

  - **To**, **Cc**

    Specify the destination to which to send e-mail. To specify multiple destinations, separate them with a comma (,).

    Tip

    It is recommended to use mailing lists for sending e-mails to multiple destinations.

  - **Subject**

    Specify the subject of the e-mail to be sent. Up to 128 characters are available.

  - **Body**

    Specify the body of the e-mail to be sent.

Tip

The character code of the e-mail is UTF-8.

- **Command**

  Run a command on the server where the IMS component is installed. Click the + icon on the side of **Command** and then specify the following items.

  - **Action Name**

    Specify the name to identify the action. Up to 128 characters are available.

    Action Name is used as identification information of the execution content in the action log.

  - **Command**

    Specify the command by absolute path to be executed when the event condition matches.

  - **Command Arguments**

    Specify options or arguments for the command.

  - **Working Directory**

    Specify the working directory of the specified command.

To delete the added action content, click the **DELETE IT** button for each action.

The following replacement strings can be used for specifying **Subject** and **Body** of **Email**, and **Command Arguments** of **Command**. The replacement string is converted to an appropriate character string when the command is executed.

Table 2-1 Replacement Strings

Replacement string	Description
{occurTime}	Converted to the event occurrence date.
{severity}	Converted to the event severity.
{sourceName}	Converted to the name of the node or interface where the event occurred.
{sourceIpv4Address}	Converted to the IPv4 address of the node where the event occurred.
{sourceIpv6Address}	Converted to the IPv6 address of the node where the event occurred.
{sourceRegion}	Converted to the name of the region group to which the node where the event occurred belongs.
{summary}	Converted to the summary information of the event.
{detail}	Converted to the detailed information of the event.
{action}	Converted to the action information of the event.
{applicationName}	Converted to the name of the application (product name connected to the IMScomponent) that detected the event.
{eventDetailUrl}	Converted to the URL of the details page of the event.

Replacement string	Description

	Caution
	Beforehand, it is necessary to set the URL for accessing the Web Console to the following configuration file.
	• Configuration file
	`<%DATAPATH%>\conf\ims-conf.ini`
	• Format
	`noms.core.url.external-base-url = <URL>`
	Restart the services to reflect the contents of the configuration file.

The following environment variables can be used in the command to be executed.

Table 2-2 Environment Variables

Environment variable	Description
NEC_IMS_OCCUR_TIME	Converted to the event occurrence date.
NEC_IMS_SEVERITY	Converted to the event severity.
NEC_IMS_SOURCE_NAME	Converted to the name of the node or interface where the event occurred.
NEC_IMS_SOURCE_IPV4_ADDRESS	Converted to the IPv4 address of the node where the event occurred.
NEC_IMS_SOURCE_IPV6_ADDRESS	Converted to the IPv6 address of the node where the event occurred.
NEC_IMS_SOURCE_REGION	Converted to the name of the region group to which the node where the event occurred belongs.
NEC_IMS_SUMMARY	Converted to the summary information of the event.
NEC_IMS_DETAIL	Converted to the detailed information of the event.
NEC_IMS_ACTION	Converted to the action information of the event.
NEC_IMS_APPLICATION_NAME	Converted to the name of the application (product name connected to the IMScomponent) that detected the event.

In this example, the action is specified with the following settings.

- **Action Type**: **Email**
  - **To**: nw_operator_ml@xx.zz.com
  - **Subject**:

    ```
    Severity: {severity} event occurred.
    ```

  - **Body**:

```
This e-mail is sent automatically.

The following event occurred in {occurTime}.
====================================
Severity: {severity}
Origin: {sourceName} ({sourceIpv4Address})
Region: {sourceRegion}
Summary: {summary}
Details: {detail}
Action: {action}
Detected by: {applicationName}
URL: {eventDetailUrl}
====================================
```

4. Save the event action definition.

   Confirm the settings and then click the **SAVE** button.

   The event action definition *"E-mail report (for operators)"* is registered to the Event Actions page.

5. Click the **NEW EVENT ACTION** icon.

   The New Event Action page is displayed.

6. On the New Event Action page, specify one more event action definition.

   Create an event action definition to send a report events with **Severity** of **Critical** or higher to the Administrator's mailing list at *"nw_operator_ml@xx.zz.com"*.

   - Summary information of the event action definition:
     - **Event action name**

       "E-mail report (for administrators)"
     - **Description**

       "Definition to report administrators by sending e-mail of events with the severity of Critical or higher."
     - **Enable this event action.** check box: Select
     - **If the condition of this event match, the following event action will be stopped.** check box: Do not select
   - Event conditions:
     - **Severity**

       Select the following check boxes.

       Fatal, **Critical**
   - Action to be executed:
     - **Action Type**: **E-mail report**
       * **To**: nw_admin_ml@xx.zz.com
       * **Subject**

         ```
         Severity: {severity} event occurred.
         ```
       * **Mail text**:

```
This e-mail is sent automatically.

The following event occurred in {occurTime}.
====================================
Severity: {severity}
Origin: {sourceName} ({sourceIpv4Address})
Region: {sourceRegion}
Summary: {summary}
Details: {detail}
Action: {action}
Detected by: {applicationName}
URL: {eventDetailUrl}
====================================
```

7. Save the event action definition.

   Confirm the settings and then click the **SAVE** button.

   The event action definition *"E-mail report (for administrators)"* is registered to the Event Actions page.

8. On the Event Actions page, change the execution order of the event actions.

   When adding a new event action definition, decide the execution order of the added event action so that the event action will not affect existing event action definitions by using the **Increase Priority** and **Decrease Priority** buttons.

   In this example, the execution priority of *"E-mail report (for administrators)"* is higher than that of *"E-mail report (for operators)"*.

2.2.2.3 Updating the event action definition

The following describes how to update the registered event action definition.

The specific procedure is described below using an example of how to add the e-mail address of the IT system manager *"it_gm@xx.zz.com"* as the destination to which the event action definition *"Late night and early morning e-mail report (for administrators)"* is to be sent.

1. Display the Event Actions page.

   Click **Event Action Settings**>**Event Actions**.

2. Click the **Edit** icon of the event action definition *"Late night and early morning e-mail report (for administrators)"* that is to be updated.

   The Edit Event Action page for the event action definition *"Late night and early morning e-mail report (for administrators)"* is displayed.

3. Change the contents of the target item on the Edit Event Action page.

   The contents of the following items can be changed.

   - Basic information of the event action definition:
     - **Name**

       Specify a unique event action name. Up to 64 characters are available.

     - **Description**

       Specify the description of the event action definition. Up to 1,024 characters are available.

- **Enable this event action.** check box
  * When selected

    The event action definition becomes enabled. Usually, select this check box.
  * When not selected

    The event action definition becomes disabled. When disabled, this event action is not processed. It is useful when you want to disable the event action temporary.
- **If the condition of this event match, the following event action will be stopped.** check box
  * When selected

    After the action is executed because it matches the specified event conditions, the event conditions will not be checked against other event action definitions and the process will stop.
  * When not selected

    Even after the action is executed because it matches the specified event conditions, the event conditions will be checked against other event action definitions.

• Event conditions to execute the corresponding action
- How to add or remove event conditions

  A new condition can be added from the pull-down menu by clicking the **Select** button.

  To remove the added condition, click the − icon displayed at the beginning of it.
- How to specify event conditions

  Set the conditions to the items in the event data by using the following two methods. The setting method differs depending on the selected item.
  * Specification by selecting a check box

    Set the condition by using the check box displayed according to the selected item. This specification method is available for the following items.
    + Target items:

      Severity
  * Specification by using a keyword

    Specify a keyword and collation method for the selected item. This specification method is available for the following items.
    + Target items:

      Summary, **Detail**, **Action**, **Source Node**, **Source Interface**, **Source Region**, **IPv4 Address**, **IPv6 Address**, **Application Name**

    The following collation methods are available.
    + Collation methods:

      is (match), **is not** (not match), **contains** (included), **does not contain** (not included), **starts with** (forward match), **ends with** (backward match)

In **IPv4 Address** and **IPv6 Address**, you can only specify **is** (match) and **is not** (not match).

Tip

If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

- Action contents to be executed

  Select the action type from the followings.

  - **Email**

    The contents of the event that matches the event condition are sent to the specified destination by e-mail. Click the + icon on the side of **Email** and then specify the following items.

    * **Action Name**

      Specify the name to identify the action. Up to 128 characters are available.

      Action Name is used as identification information of the execution content in the action log.

    * **Email Server Name**

      Select a mail server from the pre-set mail servers.

    * **To**, **Cc**

      Specify the destination to which to send e-mail. To specify multiple destinations, separate them with a comma (,).

      Tip

      It is recommended to use mailing lists for sending e-mails to multiple destinations.

    * **Subject**

      Specify the subject of the e-mail to be sent. Up to 128 characters are available.

    * **Body**

      Specify the body of the e-mail to be sent.

    Tip

    The character code of the e-mail is UTF-8.

  - **Command**

    Run a command on the server where the IMS component is installed. Click the + icon on the side of **Command** and then specify the following items.

    * **Action Name**

      Specify the name to identify the action. Up to 128 characters are available.

      Action Name is used as identification information of the execution content in the action log.

    * **Command**

      Specify the command by absolute path to be executed when the event condition matches.

* **Command Arguments**

  Specify options or arguments for the command.

* **Working Directory**

  Specify the working directory of the specified command.

To delete the added action content, click the **DELETE IT** button for each action.

The following replacement strings can be used for specifying **Subject** and **Body** of **Email**, and **Command Arguments** of **Command**. The replacement string is converted to an appropriate character string when the command is executed.

Table 2-3 Replacement Strings

Replacement string	Description
{occurTime}	Converted to the event occurrence date.
{severity}	Converted to the event severity.
{sourceName}	Converted to the name of the node or interface where the event occurred.
{sourceIpv4Address}	Converted to the IPv4 address of the node where the event occurred.
{sourceIpv6Address}	Converted to the IPv6 address of the node where the event occurred.
{sourceRegion}	Converted to the name of the region group to which the node where the event occurred belongs.
{summary}	Converted to the summary information of the event.
{detail}	Converted to the detailed information of the event.
{action}	Converted to the action information of the event.
{applicationName}	Converted to the name of the application (product name connected to the IMScomponent) that detected the event.

{eventDetailUrl}	Converted to the URL of the details page of the event.
	Caution
	Beforehand, it is necessary to set the URL for accessing the Web Console to the following configuration file.
	• Configuration file
	`<%DATAPATH%>\conf\ims-conf.ini`
	• Format
	`noms.core.url.external-base-url = <URL>`
	Restart the services to reflect the contents of the configuration file.

The following environment variables can be used in the command to be executed.

Table 2-4 Environment Variables

Environment variable	Description
NEC_IMS_OCCUR_TIME	Converted to the event occurrence date.

Environment variable	Description
NEC_IMS_SEVERITY	Converted to the event severity.
NEC_IMS_SOURCE_NAME	Converted to the name of the node or interface where the event occurred.
NEC_IMS_SOURCE_IPV4_ADDRESS	Converted to the IPv4 address of the node where the event occurred.
NEC_IMS_SOURCE_IPV6_ADDRESS	Converted to the IPv6 address of the node where the event occurred.
NEC_IMS_SOURCE_REGION	Converted to the name of the region group to which the node where the event occurred belongs.
NEC_IMS_SUMMARY	Converted to the summary information of the event.
NEC_IMS_DETAIL	Converted to the detailed information of the event.
NEC_IMS_ACTION	Converted to the action information of the event.
NEC_IMS_APPLICATION_NAME	Converted to the name of the application (product name connected to the IMScomponent) that detected the event.

In this example, the e-mail address of the IT system manager *"it_gm@xx.zz.com"* is specified into the **Cc** field of **Email** action. Other items are not changed.

4. Save the changes.

   Confirm the changes and then click the **SAVE** button.

   The event action definition is updated with the specified contents.

Some updated contents of the event action definition may affect the behavior of existing event action definitions. Therefore, if necessary, change the execution order of the event action definitions on the Event Actions page.

2.2.2.4 Deleting the event action definition

The following describes how to delete the registered event action definition.

1. Display the Event Actions page.

   Click **Event Action Settings**>**Event Actions**.

2. Click the **Delete** icon of the event action definition to be deleted.

   The Confirmation dialog box for the deletion is displayed.

3. Check the contents on the Confirmation dialog box.

4. Start the deletion.

   Click the **OK** button on the Confirmation dialog box.

   The specified event action definition is deleted from the Event Actions page.

Chapter 3. Environment Settings During Operations

This chapter describes how to configure the environment as needed while using and operating the Web Console.

Contents

3.1 Managing the dashboard definitions

This section describes the dashboard definition that is used to grasp the current network performance and event occurrence status.

The dashboard is provided as the home page to grasp the network status promptly from various viewpoints. When logging in to Web Console, the dashboard that is individually set to each user is displayed. By defining multiple dashboards on which information of each task is collected, it is possible to toggle between the dashboard display for each task.

The Dashboards page allows users to create and manage dashboard definitions corresponding to individual tasks.

3.1.1 Dashboards page

The Dashboards page is described below.

The Dashboards page allows users to check the information of dashboard definitions, and operate (register, edit, and delete) the dashboard definitions.

The Dashboards page is displayed by clicking the **Dashboard list** icon on the Dashboard page that is displayed by clicking the **Dashboard**.

Tip

In the Dashboard page, **Dashboard list** icon is displayed only for users with the Administrator authority. Therefore, these users can display the Dashboards page.

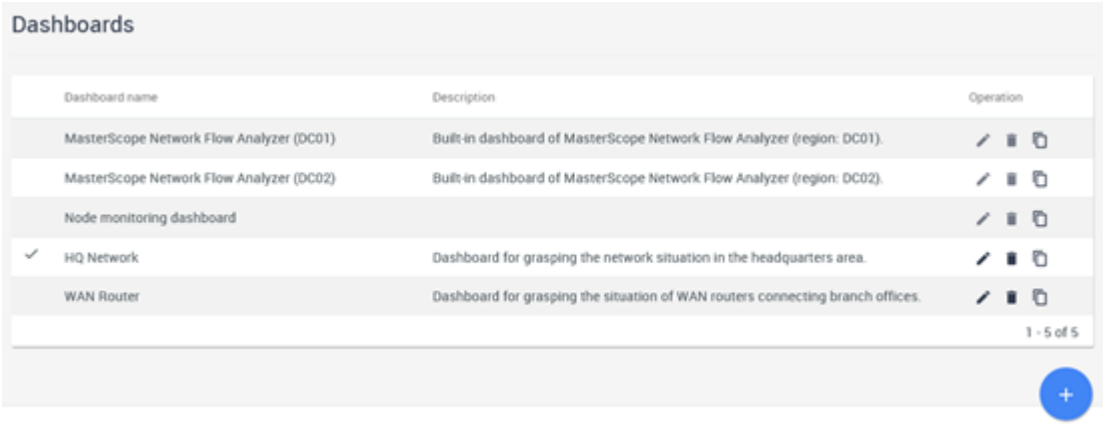

Figure 3-1 Dashboards Page

- **NEW DASHBOARD** icon

  Click this icon to register a new dashboard definition. Clicking the **NEW DASHBOARD** icon displays the New Dashboard page. For details, refer to "3.1.2 Adding a dashboard definition (page 55)".

Dashboard definition list

- **Dashboard name**

  Displays the dashboard definition name.

Tip

The ✓ mark indicates that the relevant dashboard is set as the dashboard to be displayed first after a login.

- **Description**

  Displays the description of the dashboard definition.

- **Operation**

  Click each icon to operate the dashboard definition.

  - **Edit** icon

    Click this icon to change the dashboard definition. Clicking the **Edit** icon displays the Edit Dashboard page. For details, refer to "3.1.3 Updating the dashboard definition (page 58)".

    Caution

    The built-in dashboards cannot be edited.

  - **Delete** icon

    Click this icon to delete the dashboard definition. For details, refer to "3.1.4 Deleting the dashboard definition (page 60)".

    Caution

    The built-in dashboards cannot be deleted.

  - **Copy** icon

    Register a new dashboard definition by using the registered contents of the existing dashboard definitions. Clicking the **Copy** icon displays the New Dashboard page on which the registered contents of the existing dashboard definitions are displayed.

    Use this icon to create a new dashboard definition by changing some contents of the existing dashboard definition. For details, refer to "3.1.2 Adding a dashboard definition (page 55)".

3.1.2 Adding a dashboard definition

The following describes how to register a dashboard definition.

1. Display the Dashboards page.

   Click **Dashboard** to display the Dashboard page. Next, click the **Dashboard list** icon on the Dashboard page.

2. Click the **NEW DASHBOARD** icon.

   Tip

   If you want to add a new dashboard definition by using the registered contents of the existing dashboard definitions, click the **Copy** icon of the dashboard definition to be used instead of the **NEW DASHBOARD** icon.

The New Dashboard page is displayed.

3. Specify the basic information of the dashboard definition.

   Specify the following items on the New Dashboard page.

   - **Dashboard Name**

     Specify a unique dashboard name. Up to 32 characters are available.

   - **Description**

     Specify the description of the dashboard definition. Up to 1,024 characters are available.

   - **Widget columns**

     Specify the number of widgets that can be displayed horizontally on a widget. You can specify 1 to 12 columns. The default is *"three columns"*.

   - **Default settings**

     Specify the default display settings to be adopted immediately after a dashboard is displayed.

     - **Period**

       Select the period of data to be displayed on each widget from the pull-down menu (**Past 15 minutes**, **Past 30 minutes**, **Past 1 hour**, **Past 6 hours**, **Past 24 hours**, **Past 48 hours**, or **Past 72 hours**). The default is **Past 1 hour**.

     - **Top N**

       Select the number of ranked data items to be displayed on each widget from the pull-down menu (**Top 5**, **Top 10**, or **Top 20**). The default is **Top 5**.

     - **Update interval**

       Select the refresh interval of data to be displayed on each widget from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**). The default is **1 minute**.

4. Add widgets.

   Add widgets one by one according to the following procedure.

   Tip

   Up to 16 widgets can be located on a dashboard definition.

   a. Click the **ADD WIDGET** button on the New Dashboard page.

      The Add Widget page is displayed.

   b. Select the type of the widget to be added on the New Widget page.

      Select a product name from the pull-down menu. The widget types provided by the selected product are displayed under the **Widget Type**.

      Next, select the type of the widget to be added from the displayed widget types.

      Setting items are shown according to the selected widget type.

   c. Configure widget settings.

      - **Title**

        Specify the title of the widget to be added. Up to 32 characters are available. The default title is the widget type name.

Specify the following items depending on the widget type.

- **Top N**

  Specify this item to set the number of items to be displayed by rank for each widget. Select the number of ranked data items to be displayed on each widget from the pull-down menu (**Same as Dashboard settings**, **Top 5**, **Top 10**, or **Top 20**). The default is **Same as Dashboard settings**.

  The **Top N** pull-down menu is not displayed for the widgets that display data regardless of the number of items specified for **Top N**.

- **Chart Type**

  For the widgets that can display both a pie chart and line chart, select the initial chart type (**Pie Chart** or **Line Chart**) to be displayed when the Dashboard page is displayed. The default is **Line Chart**.

- **Unit**

  For the widgets provided by NFA that display the data traffic, select the display unit of the data traffic from **bps/bytes** or **pps/packets**. The default is **bps/bytes**.

- Selection of the range of the targets (nodes and interfaces)

  For the widgets for which the data aggregation range can be specified, specify the target range as follows:

  i. Specify **Region**.

     Select the target region group from the pull-down menu.

  ii. Specify **Filter Source**.

     Next, select the data aggregation range displayed on a widget from **All**, **Node**, and **Interface**. The available choices vary depending on the widget type.

     When **Node** or **Interface** is selected, select a specific node or interface.

d. Register the widget.

   Confirm the settings and then click the **OK** button.

   The configured widget is registered to the New Dashboard page.

Repeat the above steps as many times as the number of widgets to be added.

If you want to change the contents of the added widget, click the **Edit** icon of the widget to display the Edit Widget page. On the Edit Widget page, all the items specified after selecting the widget type can be changed.

5. Adjust the widget display position.

   - Changing the widget display position

     Place the cursor on the widget whose display position is to be changed, and drag and drop it in the desired position.

   - Deleting unnecessary widgets

     Click the **Delete** icon of the widget.

6. Register the dashboard definition.

Confirm the settings and then click the **OK** button.

The configured dashboard is registered to the Dashboards page.

3.1.3 Updating the dashboard definition

The following describes how to update the contents of the registered dashboard definition.

1. Display the Dashboards page.

   Click **Dashboard** to display the Dashboard page. Next, click the **Dashboard list** icon on the Dashboard page.

2. Click the **Edit** icon of the dashboard definition to be updated.

   The Edit Dashboard page for the relevant dashboard definition is displayed.

3. Update the basic information of the dashboard definition.

   On the Edit Dashboard page, all of the following items can be changed.

   - **Dashboard Name**

     Specify a unique dashboard name. Up to 32 characters are available.

   - **Description**

     Specify the description of the dashboard definition. Up to 1,024 characters are available.

   - **Widget columns**

     Specify the number of widgets that can be displayed horizontally on a widget. You can specify 1 to 12 columns.

   - **Default settings**

     Specify the default display settings to be adopted immediately after a dashboard is displayed.

     - **Period**

       Select the period of data to be displayed on each widget from the pull-down menu (**Past 15 minutes**, **Past 30 minutes**, **Past 1 hour**, **Past 6 hours**, **Past 24 hours**, **Past 48 hours**, or **Past 72 hours**).

     - **Top N**

       Select the number of ranked data items to be displayed on each widget from the pull-down menu (**Top 5**, **Top 10**, or **Top 20**).

     - **Update interval**

       Select the refresh interval of data to be displayed on each widget from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**).

4. Add a widget.

   When adding a new widget, perform the following procedure.

   Tip

   Up to 16 widgets can be located on a dashboard definition.

   a. Click the **ADD WIDGET** button on the Edit Dashboard page.

      The Add Widget page is displayed.

b. Select the type of the widget to be added on the New Widget page.

Select a product name from the pull-down menu. The widget types provided by the selected product are displayed under the **Widget Type**.

Next, select the type of the widget to be added from the displayed widget types.

Setting items are shown according to the selected widget type.

c. Configure widget settings.

- **Title**

  Specify the title of the widget to be added. Up to 32 characters are available. The default title is the widget type name.

Specify the following items depending on the widget type.

- **Top N**

  Specify this item to set the number of items to be displayed by rank for each widget. Select the number of ranked data items to be displayed on each widget from the pull-down menu (**Use the default**, **Top 5**, **Top 10**, or **Top 20**). The default is **Use the default**.

  The **Top N** pull-down menu is not displayed for the widgets that display data regardless of the number of items specified for **Top N**.

- **Chart Type**

  For the widgets that can display both a pie chart and line chart, select the initial chart type (**Pie Chart** or **Line Chart**) to be displayed when the Dashboard page is displayed. The default is **Line Chart**.

- **Unit**

  For the widgets provided by NFA that display the data traffic, select the display unit of the data traffic from **bps/bytes** or **pps/packets**. The default is **bps/bytes**.

- Selection of the range of the targets (nodes and interfaces)

  For the widgets for which the data aggregation range can be specified, select the target range as follows:

  i. Specify **Region**.

     Select the target region group from the pull-down menu.

  ii. Specify **Data Aggregation Range**.

     Next, select the data aggregation range displayed on a widget from **All**, **Node**, and **Interface**. The available choices vary depending on the widget type.

     When **Node** or **Interface** is selected, select a specific node or interface.

d. Register the widget.

Confirm the settings and then click the **OK** button.

The configured widget is registered to the Edit Dashboard page.

Repeat the above steps as many times as the number of new widgets to be added.

5. Update the contents of the registered widget.

If you want to change the contents of the added widget, click the **Edit** icon of the widget to display the Edit Widget page. On the Edit Widget page, all the items specified after selecting the widget type can be changed.

6. Delete unnecessary widgets.

   Click the **Delete** icon of the widget to be deleted.

7. Change the widget display position.

   Place the cursor on the widget whose display position is to be changed, and drag and drop it in the desired position.

8. Register the changes.

   Confirm the changes and then click the **OK** button.

   The dashboard definition is updated with the specified contents.

3.1.4 Deleting the dashboard definition

The following describes how to delete the registered dashboard definition.

1. Display the Dashboards page.

   Click **Dashboard** menu to display the Dashboard page. Next, click the **Dashboard list** icon on the Dashboard page.

2. Click the **Delete** icon of the dashboard definition to be deleted.

   The Confirmation dialog box for the deletion is displayed.

3. Check the contents on the Confirmation dialog box.

4. Start the deletion.

   Click the **OK** button on the Confirmation dialog box.

   The specified dashboard definition is deleted from the Dashboards page.

Caution

Even if the dashboard is set in the user settings as the initial **Dashboard** to be displayed after a login, its definition can be deleted. If the definition of the initial dashboard is deleted, it is necessary for users to set **Dashboard** again on the Personal Information Settings page after a login.

3.2 Editing the network map displays

This section describes how to display and edit a network map on Web Console.

Web Console incorporates the following configuration information registered to Network Manager Map View and creates network map data for Web Console.

- Network configuration (Layered structure of the map)
- Node information
- Connections among nodes

Web Console displays a network map on the Topology Map page using this information.

Tip

When the IMS component connects to Network Manager, the IMS component incorporates the above information automatically and creates network map data for Web Console.

Since information from Network Manager other than the above is not incorporated in Web Console, graphics and background images placed on each Network Manager Map View are not reflected in the Topology Map page of Web Console. Edit the network map displayed on the Topology Map page on Web Console to insert graphics and background images to the network map or to change the position of the icon indicating a node.

When editing a network map, change the mode of the Topology Map page from **View mode** to **Edit mode**.

3.2.1 Edit mode and Editing Tool

This section describes **Edit mode** and **Editing Tool** of the Topology Map page.

On the Topology Map page, a network map can be edited in various ways by switching **View mode** to **edit mode**.

Click **Topology Map** menu to display the Topology Map page. Select **edit mode** from the mode selection pull-down menu to switch **View mode** to **edit mode**.

Tip

Only users with the Administrator authority can change the mode to **edit mode**.

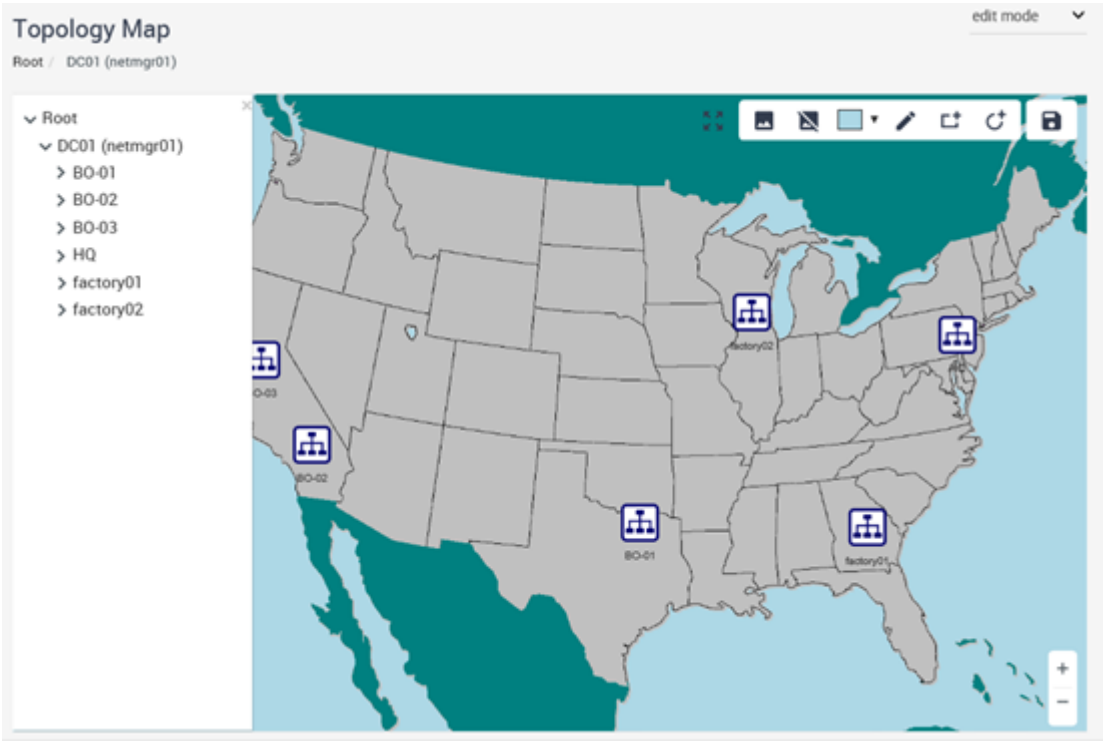

Figure 3-2 Topology Map Page (Edit Mode)

Editing Tool is displayed by switching **View mode** to **edit mode**. Positions of node icons and map icons on a **Map View** can also be changed.

Tip

Connection lines between nodes are displayed based on the connection information of the Network Manager. To edit connection lines, edit connection lines (**Connection-line**, **Simple Line**) on the Map View of the Network Manager.

Editing Tool

Click each icon of **Editing Tool** to insert a shape, image, and text to the background of the network map. The details of **Editing Tool** are provided below.

- **Change Background** icon

  Click this icon to insert an image to the background on a network map. The file formats that can be specified for a background image are *"JPG"*, *"GIF"*, and *"PNG"*.

- **Remove Background** icon

  Click this icon to cancel insertion of an image to the background on a network map.

- **Change Background Color** icon

  Click this icon to change the background color of a network map.

- **Add Line** icon

  Click this icon to draw a straight line on a **Map View**. The line width and color can be specified.

- **Add Rectangle** icon

  Click this icon to draw a rectangle on a **Map View**. The line width and color, and the fill color can be specified. It is also possible to input text in the rectangle.

- **Add Ellipse** icon

  Click this icon to draw a circle on a **Map View**. The line width and color, and the fill color can be specified.

- **Save** icon

  Click this icon to save the changed node icon positions and edited network map background.

  ### Caution

  If the changes and edits are not saved, they will be discarded when changing the display map or transitioning from the page. Therefore, be sure to save the changes and edits before changing the display map or transitioning from the page.

Graphic Editing Tool

When you select a shape on the **Map View**, the **Graphic Editing Tool** is displayed. To edit shapes, click each icon of the **Graphic Editing Tool**.

- **Change Color** icon

  Click this icon to specify the fill color of the selected shape. Clicking the **Change Color** icon displays the widget to specify a color. Use the left **Slider** to specify a color and the right **Slider** to specify the transparency.

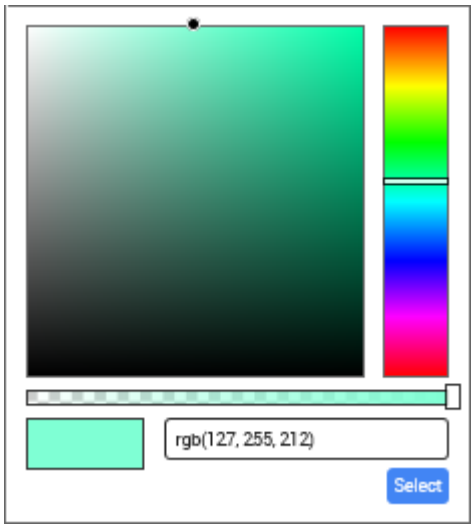

Figure 3-3 Color Specification

- **Change Border Color** icon

  Click this icon to specify a line color of the selected shape. Clicking the **Change Border Color** icon displays a dialog box to specify a color. Choose a color and then click the **Select** button to specify a border color. By moving the lower **Slider**, you can specify the color transmission rate.

- **Change Text Color** icon

  Click this icon to specify the font color of the text input to the selected shape. Clicking the **Change Text Color** icon displays a dialog box to specify a color. Choose a color and then click **Select** to specify a text color.

- **Edit Line Width** icon

  Click this icon to specify the line width of the selected shape. Clicking the **Edit Line Width** icon displays a dialog box to specify a line width. Move **Slider** to the right to make the line thicker.

Figure 3-4 Edit Line Width Dialog Box

- **Edit Text** icon

Click this icon to input a text in the rectangle placed on a network map. Clicking the **Edit Text** icon displays the Edit Text dialog box. On this dialog box, operations to enter text are available.

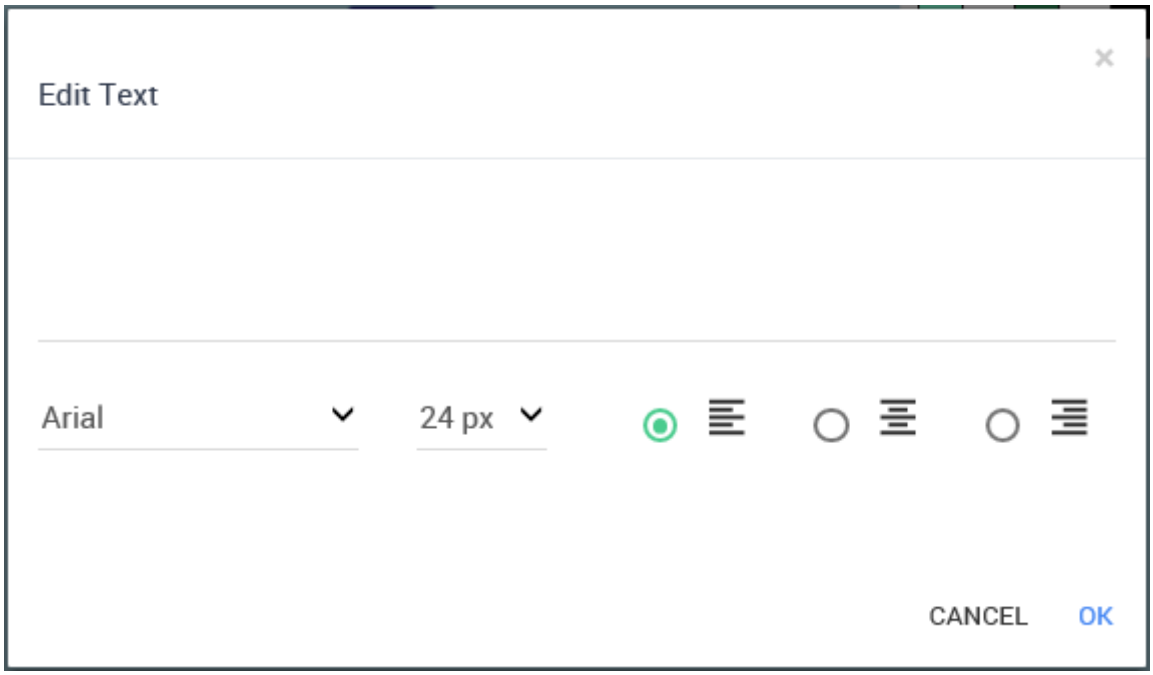

Figure 3-5 Edit Text Dialog Box

- **Bring Forward** icon

  Click this icon to move the shape placed on a network map to the front.

- **Send Backward** icon

  Click this icon to move the shape placed on a network map to the back.

- **Delete** icon

  Click this icon to delete the shape placed on a network map.

3.2.2 Changing the icon position on a network map

The following describes how to change the positions of node icons and map icons on a network map.

1. Display the Topology Map page.

   Click **Topology Map** menu.

2. Change the mode of the Topology Map page from **View mode** to **edit mode**.

   Select **edit mode** from the pull-down displaying **View mode**.

3. Display the network map to be edited.

   From Tree View of the Topology Map page, select the **Map** icon to be edited.

   The network map corresponding to the selected **Map** icon is displayed on Map View of the Topology Map page.

4. Change the position of the node or map icon.

   Drag the icon to be moved and drop it in a desired position.

Repeat this step to change the positions of all node or map icons to be moved.

5. Save the changes of the network map.

   Check the changes and then click the **Save** icon.

   Caution

   If the changes are not saved, they will be discarded when moving a map or transitioning from the page.

   The changes of the network map are saved.

Tip

- Network maps are edited one at a time.
- Editing the background along with changing the icon positions makes the configuration of a network map easier to understand. For details, refer to "3.2.3 Editing a network map to make it easier to understand by using the editing tool (page 65)".

3.2.3 Editing a network map to make it easier to understand by using the editing tool

The following describes how to edit the background of a network map to make it easier to understand.

Editing a network map as follows makes the network configuration of the map easier to understand.

- Inserting an image indicating the construction of a building and floor.
- Inserting a border (rectangle) presenting a group of devices constructing a cluster
- Inserting text supplementing a network configuration

1. Display the Topology Map page.

   Click **Topology Map** menu.

2. Change the mode of the Topology Map page from **normal mode** to **edit mode**.

   Select **edit mode** from the pull-down displaying **View mode**.

3. Display the network map to be edited.

   From Tree View of the Topology Map page, select the **Map** icon to be edited.

   The network map corresponding to the selected **Map** icon is displayed on Map View of the Topology Map page.

4. Edit the background of the network map.

   Edit the background of the network map by using **Editing Tool**.

   - Inserting an image to the background.

     a. Click the **Change Background** icon of **Editing Tool**.

        The Open Files dialog box is displayed.

     b. Select an image file to be inserted to the background of the network map.

        The image file formats that can be selected are *"JPG"*, *"GIF"*, and *"PNG"*.

     c. Check that the selected image is inserted in the background of the network map.

Here, select the image indicating the construction of a building and floor.

- Inserting a shape to the background

  a. From **Editing Tool**, click one of the icons to insert a shape.

  The icons to insert a shape are **Add Line**, **Add Rectangle**, and **Add Ellipse**.

  b. Insert a shape.

  Place the mouse pointer in the position where the shape is to be inserted.

  Click the inserted shape and drag to adjust the size of the shape then drop to confirm the size.

  The inserted shape can be moved by dragging and dropping.

  c. Change the color of the inserted shape.

  Select the shape and then click the **Change Background Color** icon of **Editing Tool** to change the fill color. Similarly, the **Change Border Color** and **Edit Line Width** icons to change the line color and line width, respectively.

  Here, enclosing the node icons forming the cluster configuration in a rectangle by using **Add Rectangle**, and then make the fill color transparent by using **Change Background Color**.

- Inserting text to the background

  a. Select a rectangle in which to enter text.

  The rectangle must be created in advance.

  b. Click the **Edit Text** icon of **Graphic Editing Tool**.

  c. Input characters.

  Tip

  If you want to insert only text to the background of the network map, after entering the text, set the line and fill color of the relevant shape to *"Transparent"*.

  Here, select the rectangle that encloses the node icons in the cluster configuration, and then insert *"Cluster configuration"* as text.

5. Save the changes of the network map.

   Check the changes and then click the **Save** icon.

   Caution

   If the changes are not saved, they will be discarded when moving a map or transitioning from the page.

   The changes of the network map are saved.

Tip

- Network maps are edited one at a time.

- Changing the icon positions along with editing the background makes the configuration of a network map easier to understand. For details, refer to "3.2.2 Changing the icon position on a network map (page 64)".

Chapter 4. Operations

This chapter describes how to use the Web Console during operation.

Contents

4.1 Checking the current network status

This section describes how to use Web Console to grasp the current network status promptly.

Web Console provides the following three pages to grasp the current network status promptly.

- Dashboard page

  This page is used to grasp the status of the entire network. Check whether there is a problem in the load or communication status of each node by referring to data displayed by rank (Top N),

- Topology Map page (displayed in **normal mode**)

  This page is used to grasp the network configuration, identify the fault locations, and check the influence of the faults. Check the configuration around the faulty node by drilling down and investigating a hierarchical map.

- Nodes page

  This page is used to check the property information and current status (severity) of the managed node. Specify search conditions and check the status and information of the node that matches the specified conditions.

4.1.1 Checking the overall situation on the dashboard

The Dashboard page displays various information by rank (TopN) or other formats, allowing users to check the current status. The Dashboard page operation procedure is described below.

The following information can be checked on the Dashboard page.

- Usage rates of resources such as CPU and memory of the managed nodes
- Information (usage rate, packet loss rate, and error rate) of network interfaces of the managed nodes
- Information of communication flow through a network
- Information of the failure occurrence status and node usage rate

On the Dashboard page, the overall situation can be grasped by checking the values of the ranked data. For example, when the top 10 nodes whose CPU usage rate is higher among all the managed nodes are displayed, if there is no problem in the displayed CPU usage rates, it can be decided that there is also no problem in the CPU usage rates of the entire network.

4.1.1.1 Dashboard page

The Dashboard page is described below.

The Dashboard page is used to grasp the status of the entire network from various information by rank (Top N).

Click **Dashboard** to display the Dashboard page.

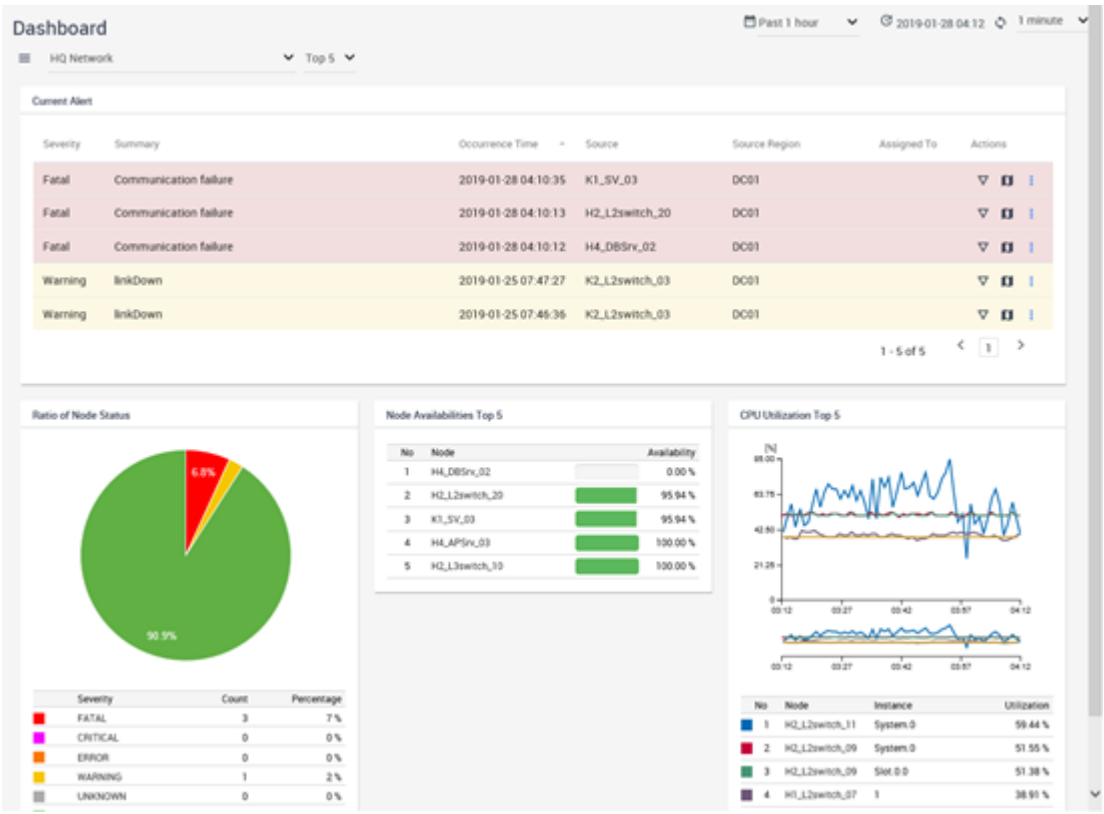

Figure 4-1 Dashboard Page

Screen operation area

- **Dashboard list** icon

  Click this icon to display the Dashboards page. The Dashboards page allows users to check the information of dashboard definitions, and operate (register, edit, and delete) the dashboard definitions. For details, refer to "3.1.1 Dashboards page (page 54)".

  Tip

  Dashboard list icon is displayed only for users with the Administrator authority.

- **Dashboard**

  Information to be displayed on the Dashboard page can be changed by selecting the registered dashboard name from the pull-down menu.

- **Top N**

  Select the number of ranked data items to be displayed on each widget of a dashboard from the pull-down menu (**Top 5**, **Top 10**, or **Top 20**).

- **Period**

  Select the period of data to be displayed on a dashboard from the pull-down menu (**Past 15 minutes**, **Past 30 minutes**, **Past 1 hour**, **Past 6 hours**, **Past 24 hours**, **Past 48 hours**, or **Past 72 hours**).

- **Last Updated**

  Displays the last update date.

- **Update** icon

  Click this icon to refresh the display of the page.

- **Update interval**

  Select the refresh interval of the display of the page from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**).

Widget display area

Displays widgets. For how to operate widgets displayed on the dashboard, refer to "1.2.8 Basic operation of widgets (page 19)" or "1.2.9 Operations of specific widgets (page 23)".

4.1.1.2 Changing the display of the dashboard

The network status can be checked from various viewpoints by changing the parameters of the Dashboard page.

The specific procedure is described below using an example to check the status of the entire network by switching between the *"Head office network"* and *"Branch office network"* dashboards.

These two dashboards are described as follows in the operation example.

- Head office network

  Past 1 hour is selected for **Period** and **Top 5** is selected for **Top N**. The following widgets are displayed.

  - CPU usage rates of backbone switches
  - Bandwidth utilization for input interfaces of backbone switches

- Branch office network

  Past 1 hour is selected for **Period** and **Top 5** is selected for **Top N**. The following widgets are displayed.

  - CPU usage rates of WAN routers of branches
  - Bandwidth utilization for output interfaces of WAN router of branches

1. Display the Dashboard page.

   Click **Dashboard** menu.

   The contents of the dashboard definition that is registered as the initial dashboard are displayed on the Dashboard page.

   In this operation example, the *"Head office network"* dashboard is displayed initially.

2. Set **Update interval** to **Nothing**.

   If you want to check the network status in detail, select **Nothing** from the **Update interval** pull-down menu so that the page display is not refreshed unintentionally.

3. Check the contents of each widget.

   Determine whether there is any problem on the network according to the highly ranked data displayed on each widget.

   For example, suppose that, on the *"CPU usage rates of backbone switches"* widget, the highest CPU usage rate is *"60%"*. In this case, it can be seen that the CPU usage rates of all

other switches are *"60% or less"*, and it can be determined that the CPU usage rates of all target switches are not high.

As another example, suppose that, the usage rate of the 5th ranked input interface exceeds *"90%"* when checking the *"Bandwidth utilization for input interfaces of backbone switches"* widget. It can be seen that all of five network interfaces displayed on the widget are heavily loaded. In such a case, change **Top N** to a value larger than the default value such as **Top20** to check how many network interfaces are heavily loaded.

Check the influence of the heavily loaded network interfaces and investigate the causes as necessary on the Node Detail, Network Interface Detail, or Topology Map page.

4. Switch to another dashboard.

   When checking the network status has been complete, select another dashboard name from the pull-down menu to check the status from another point of view. Information of the selected dashboard is displayed on the Dashboards page.

   Here, switch to the *"Branch office network"* dashboard and check the network status of the branch offices.

5. Set **Update interval** to **Nothing**.

   When the dashboard is switched, the default values of the selected dashboard are set to the parameters of the Dashboard page. Therefore, select **Nothing** from the **Update interval** pull-down menu again.

6. Check the contents of each widget.

   Determine whether there is any problem on the network according to the highly ranked data displayed on each widget.

   For example, suppose that according to *"Bandwidth utilization for output interfaces of WAN router of branches"*, the network load from 30 minutes ago to the current time is normal, but that earlier than 30 minutes ago tended to be heavy. In such a case, change **Period** to a value larger than the default value such as **Past 6 hours** to check from when the load is heavy.

   Investigate the cause of the heavy load on the Network Interface Detail page of the relevant network interface as necessary.

   Tip

   When NFA is used, on the Network Interface Detail page, it is possible to check the application and conversation (information being communicated between two points) of the communication flow through the relevant network interface.

As described above, the status of the entire network can be grasped by switching between the dashboard definitions on the Dashboard page. To check the details, move from each widget to the corresponding page displaying the details.

4.1.2 Checking the status on the network map (Normal mode)

The Topology Map page can be displayed in two types of **View mode**: **normal node** displaying the current status and **analysis mode** displaying the past node status (severity). When checking the network status, distinguish between these two modes. This section explains the operation in **normal node** displaying the current status.

The Topology Map page allows users to check how nodes are connected physically and where in a building or on a floor the nodes are installed. If network maps are hierarchized, the lower-level network maps can be displayed by drilling down. In **normal node**, the current status (severity) of

each nod can be checked. By using the Side Panel, not only the network configuration but also the current load of each node can be checked.

4.1.2.1 Network Map page (Normal mode)

The Topology Map page in **Normal mode** is described below.

The Topology Map page allows users to check the network configuration, and the status (severity) and load of each node.

Click **Topology Map** menu to display the Topology Map page.

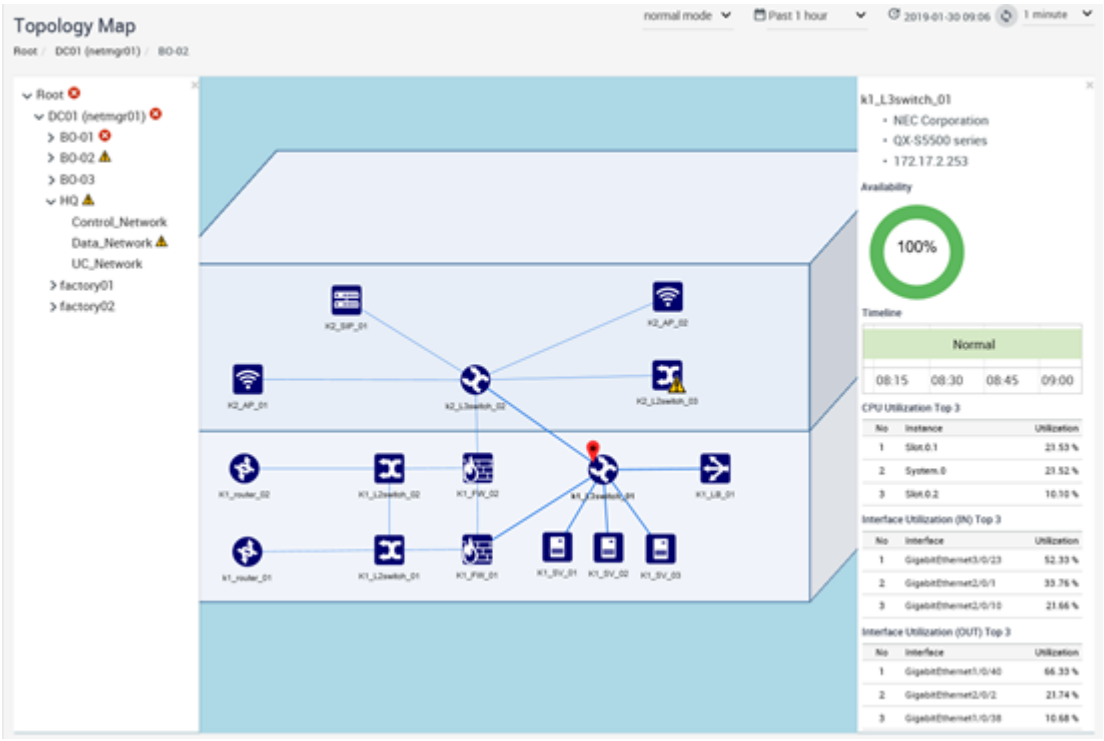

Figure 4-2 Topology Map Page (Normal Mode)

Screen operation area

- **View mode**

  View mode can be switched between the following modes by selecting from the pull-down menu.

  - **normal mode**

    Select this mode to check the current status (severity) of a network. When the Topology Map page is displayed by using the **Topology Map** menu, this page is always in **normal mode**.

  - **analysis mode**

    Select this mode to check the past status (severity) of a network. When the Topology Map page is displayed from the Node Detail page displaying the past period or from the Events page, this page is always in **analysis mode**.

  - **edit mode**

    Select this mode to edit the display contents of a network.

Tip

Only users with the Administrator authority can change the mode to **edit mode**.

- **Period** (Normal mode)

  Select the period of data to be displayed on the Side Panel from the pull-down menu (**Past 15 minutes**, **Past 30 minutes**, **Past 1 hour**, **Past 6 hours**, **Past 24 hours**, **Past 48 hours**, or **Past 72 hours**). The default is **Past 1 hour**.

- **Last Updated**

  Displays the last update date.

- **Update** icon

  Click this icon to refresh the display of the page.

- **Update interval**

  Select the refresh interval of the display of the page from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**). The default is **1 minute**.

Tree View

Displays the hierarchical configuration of network maps in a tree. Tree View is collapsed usually.

Click the icon on Map View to expand it.

Like Tree View of Network Manager, if a fault occurs on a node of the network map, the severity information of the fault is reflected in the **Map** icon. The information is also reflected in the **Map** icon above the relevant **Map** icon.

Map View

A network map corresponding to the **Map** icon selected in Tree View is displayed. A network map displayed in Map view displays **Node** icons showing the managed nodes, **Connection line** showing the connections between the managed nodes, and **Map** icons showing lower-level network maps.

Tip

If nodes are connected via multiple physical lines, Map View represents connections between the nodes as a single line. Details of physical connections can be checked on the Side Panel that is displayed by selecting **Connection line**.

The following operations are available on Map View.

- Zooming in and zooming out

  Click the **Zoom In** icon to zoom in on a network map. Click the **Zoom Out** icon to zoom out a network map.

  You can also zoom in or zoom out on a network map by scrolling the mouse wheel.

- Moving the display position

  The display position can be moved by dragging a network map. This operation is available when a network map is zoomed in.

- Adjusting the position and scale

Click the **Fit** icon to adjust the position and scale of the Map View to display all the **Node** and **Map** icons on the Map View.

- Moving to an upper- or lower-level network map page

  A path link indicating a tree position of a **Map** icon selected in Tree View is displayed at the top of Map View. Clicking this link switches a Map View page to an upper-level network map page. Clicking a **Map** icon indicating a lower-level network map on Map View switches a Map View page to the page of the selected lower-level network.

  The above operations allow users to switch and operate the display of network maps only with Map View.

Side Panel

The Side Panel is displayed by selecting a **Node** icon, **Map** icon, or **Connection line** displayed on Map View. The Side Panel displays the details of the load and connection lines of the node. For details, refer to "4.1.2.2 Side Panel on the map view (page 75)".

4.1.2.2 Side Panel on the map view

The Side Panel is described below.

The Side Panel is available to check the load and connection lines of the node with checking the network configuration.

The Side Panel is displayed by selecting a **Node** icon, **Map** icon, or **Connection line** on Map View. This pane shows the information of the selected node or connection line.

The contents to be displayed on the Side Panel vary greatly depending on a selected icon.

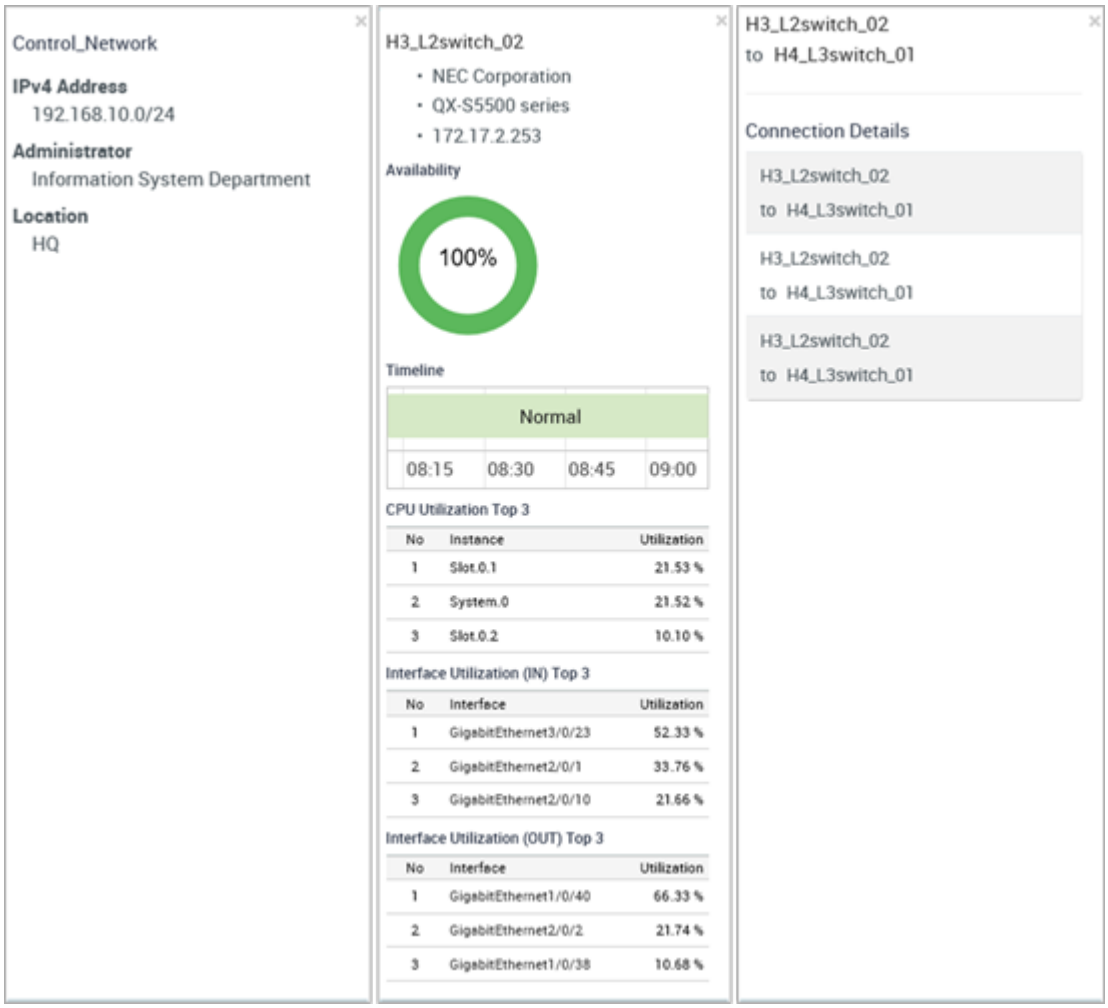

Figure 4-3 Side Panels

Display contents for a node

When selecting a **Node** icon, the Side Panel displays the following information.

- **Node Name**

  Clicking a node name link displays a Node Detail page for the relevant node.

- **Vendor Name**

  Displays information of a node vendor.

- **Series Name**

  Displays information of a node model.

- **IPv4 Address**

  Displays information of the IPv4 address used in the monitoring process.

- **IPv6 Address**

  Displays information of the IPv6 address used in the monitoring process.

This pane also shows the following information corresponding to the **Period** value on the Topology Map page. Top 3 items are displayed.

- **Availability**

Displays changes in the usage rate and status (severity) of the node.

- **CPU Utilization**

  Displays the CPU usage rate.

- **Interface Utilization (IN)**

  Displays the input usage rate of network interfaces.

- **Interface Utilization (OUT)**

  Displays the output usage rate of network interfaces.

Tip

To display **CPU usage rate**, **Interface Utilization (IN)**, and **Interface Utilization (OUT)**, it is necessary to set to collect information of these items in the Network Manager data collection function in advance.

Display contents for a map

When selecting a **Map** icon, the Side Panel displays the following information.

- **Map Name**

  Displays a map name.

- **IPv4 Address**

  Displays information of the IPv4 address set in this map.

- **IPv6 Address**

  Displays information of the IPv6 address set in this map.

- **Administrator**

  Displays information of the administrator set in this map.

- **Location**

  Displays information of the location set in this map.

- **URL**

  Displays the URL set in this map.

Display contents for a connection line

When selecting a **Connection line**, the Side Panel displays the following information.

- Connection information

  Connected two nodes are displayed in the following format;

  ```
  <Node name 1>
  to <Node name 2>
  ```

- Network interface information

  Network interfaces that are used to connect the nodes of "Connection information" are displayed in the following format:

  ```
  <Interface name 1>(<Line speed>)
  to <Interface name 2>(<Line speed>)
  ```

Tip

- A network interface of <*Node name 1*> is displayed on the left, and that of <*Node name 2* is displayed on the right.
- <*Line speed*> displays a bandwidth speed of the network interface obtained from each node.
- If multiple network interfaces are used for connection, information of all network interfaces is displayed in the same format.

4.1.2.3 Checking a fault location on a network map

It is possible to identify a fault location and check the situation around the fault by drilling down network maps.

The following describes how to identify a fault location by drilling down network maps from the upper-level network map displaying the entire network.

1. Display the Topology Map page.

   Click **Topology Map**.

2. Check a **Map** icon indicating a fault occurrence on Map View.

   The top Map View is displayed immediately after displaying the Topology Map page . If a fault has occurred in a node of a map, the fault severity is reflected and displayed in the corresponding **Map** icon.

   Tip

   The top Map View displays a **Map** icon indicating Network Manager to be connected to the IMS component.

3. Click the **Map** icon indicating a fault occurrence.

   The network map corresponding to the clicked **Map** icon is displayed on Map View.

4. Check an icon indicating a fault occurrence on Map View.

   If the icon is a **Map** icon, click it and drill down the map.

   If the icon is a **Node** icon, a fault has occurred in the relevant node.

5. Check the configuration around the **Node** icon indicating a fault occurrence.

   The influence range can be checked by checking the configuration around the faulty node.

6. Check the state of the node indicating a fault occurrence.

   Click the **Node** icon indicating a fault occurrence to display the Side Panel. Check the current load status and the changes in state (severity) according to the information displayed on the Side Panel.

If you want to check the node in more detail, for example, checking the occurred events, click the node name link displayed on the Side Panel to display the Node Detail page corresponding to the relevant node.

4.1.3 Checking the node status in a list

This section describes how to use the Nodes page to list property information and status (severity) of the nodes that match the specified search conditions.

The Nodes page is available to specify search conditions and check the property information (such as an IP address, vendor, series, version) and current status (severity) of the nodes that match the specified conditions.

For example, only nodes of a specific model can be displayed by specifying **Vendor** and **Series** for search conditions. This enables to check the nodes of the same model whether they are the same version or whether any of them has not been upgraded.

As described above, node information can be checked efficiently by searching under various conditions for all the managed nodes.

4.1.3.1 Nodes page

The Nodes page is described below.

The Nodes page is used to check and investigate information of the managed nodes from various viewpoints.

Click **Nodes** to display the Nodes page.

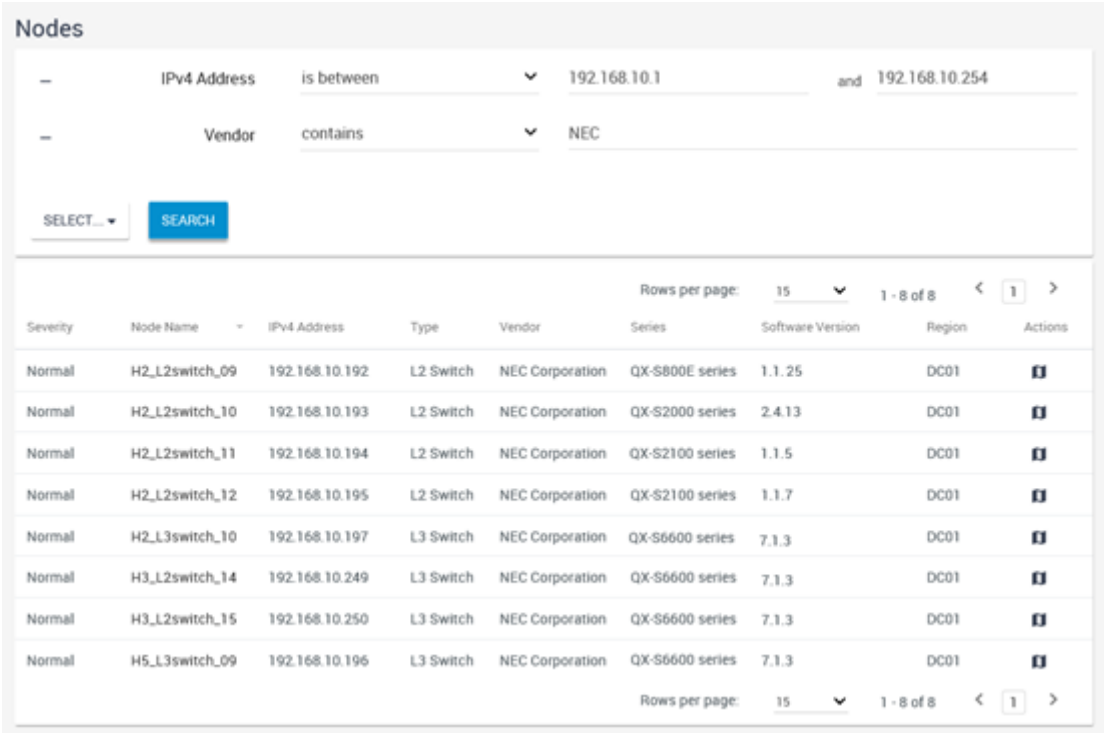

Figure 4-4 Nodes Page

Specifying search conditions

Nodes to be displayed can be narrowed down by specifying conditions for items displayed in the node list.

- How to add or remove search conditions

  A new search condition can be added from the pull-down menu by clicking the **Select** button.

  To remove the added search condition, click the − icon displayed at the beginning of it.

- How to specify search conditions

  There are the following three methods to specify search conditions for items displayed in the node list. The search condition specification method differs depending on the selected item.

- Specification by selecting a check box

  Specify a search condition by selecting the corresponding check box. This specification method is available for the following items.

  * Target items:

    Severity

- Specification by using a keyword

  Specify a keyword and collation method for the selected item. This specification method is available for the following items.

  * Target items:

    Node Name, **Type**, **Vendor**, **Series**, **Software Version**, **Region**

  The following collation methods are available.

  * Collation methods:

    is (match), **is not** (not match), **contains** (included), **does not contain** (not included), **starts with** (forward match), **ends with** (backward match)

- Specification of a value range

  Specify a value or value range as a search condition. This specification method is available for the following items.

  * Target items:

    IPv4 Address

  * Collation methods:

    is (match), **is between** (within the range)

Tip

If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

After specifying the conditions, click the **SEARCH** button to display a list of nodes that match the specified search conditions.

Node list

- **Severity**

  Displays the current status (severity) of the node.

- **Node Name**

  Displays the node name. Click the node name link to display the Node Detail page for the relevant node.

- **IPv4 Address**

  Displays the IPv4 address used in the node monitoring process.

- **Type**

  Displays node classification information. **Type** is determined by information of **Icon type** specified by Network Manager or **sysObjectId** (ID indicating the model) that Network Manager obtained from MIB.

- **Vendor**

  Displays the manufacturer company name of the node. **Vendor** is determined by **sysObjectId** (ID indicating the model) that Network Manager obtained from MIB.

  Tip

  Vendor is displayed according to the vendor ID and company name that are defined by the Internet Assigned Numbers Authority (IANA).

- **Series**

  Displays the node model series. **Series** is determined by **sysObjectId** (ID indicating the model) that Network Manager obtained from MIB.

- **Software Version**

  Displays the software version of the node.

- **Region**

  Displays the name of the region group to which the node belongs.

- **Actions**

  Click the following icon to perform an operation for the node.

  - **Topology Map** icon

    Displays the network map where the relevant node is placed, in **normal mode**.

    Tip

    * The **Topology Map** icon is displayed when using the Network Manager.
    * If the node is located on multiple maps, a dialog box to select the map to be displayed is displayed.

Select the number of node information items to be displayed on one page from the pull-down menu (**15**, **50**, or **100**). The default is **15**.

If whole of the node information that matches the search conditions cannot be displayed on one page, switch pages to check the information.

4.1.3.2 Checking the faulty nodes in a list

The Nodes page is available to specify search conditions and check information of the nodes that match the specified conditions.

The specific procedure to use the Nodes page is described below using an example to search for the nodes whose status (severity) is *"Warning or higher"*.

1. Display the Nodes page.

   Click **Nodes**.

2. Select the item to be searched.

   Select the item to be searched from the pull-down list (**Severity**, **Node Name**, **IPv4 Address**, **Type**, **Vendor**, **Series**, **Software Version**, **Region**).

   Here, select **Severity** from the pull-down menu.

3. Specify a search condition for the selected item.

When **Severity** is selected, the check box of each severity is displayed. Select the check boxes of the severity levels to be used as a condition.

Here, to search for nodes whose severity is *"Warning or higher,"* select the check boxes of **Fatal**, **Critical**, **Error**, and **Warning**.

4. Click the **SEARCH** button.

   Information of the nodes that match the specified search condition is displayed in the node list.

5. Check the search result.

   Check the information displayed in the node list. If whole of the search result is not displayed on one page, switch pages to check the result.

   Narrow down the information further by adding a search condition from the pull-down menu by clicking the **Select** button as necessary.

If you want to check the details of the node displayed in the node list, display the Node Detail page by clicking the node name link. The Node Detail page is available to check the property information and load status of the relevant node in detail.

4.2 Checking the event occurrence status

The section describes how to check the event occurrence status by using Web Console.

Web Console uses the following two pages to check the event occurrence status.

- Events page

  This page is used to check information of the occurred event in chronological order and detailed information of the event. It is possible to check the past event occurrence status by specifying the event occurrence time period as a search condition.

- Topology Map page (displayed in **Analysis mode**)

  This page is used to check the influence range of events that occurred in the past and the load status at that time. On the Timeline page, the status (severity) of each node at the time of the event can be reproduced as a network map by specifying a desired time period.

Tip

See the state of the **Notifications** icon to check whether an event occurred or not while operating Web Console. Clicking the **Notifications** icon shows summary information of the occurred event. For details, refer to "1.2.5 Checking the newly occurred events (page 14)".

4.2.1 Checking the contents of the occurred events

The contents of all occurred events can be checked on the Events page of Web Console.

The following operations can be performed for the occurred events on the Events page.

- Searching for events that match a certain condition

  By specifying a search condition, only the events that match the specified condition can be displayed in the list.

  If you want to check unrecovered events or events in charge of your investigation, preform this search operation.

- Checking the details of an event

By displaying the Event Detail page corresponding to the specified event from Events page, you can check the details of the event.

- Assigning an investigator

  An investigator can be assigned to the occurred events. If multiple operators manages a network, assign someone of the operator a role to correspond faults or a role to notify other operators that the event has been checked.

- Recovering an event

  If a fault (with the severity of Warning or higher) occurred in an event, a recovery operation can be performed for the event. After investigating the fault cause and restoring the environment, recover the faulty event.

Tip

Depending on the specifications of the product detecting an event, recovery of events may not be performed.

4.2.1.1 Events page

The Events page is described below.

The Events page allows users to check the contents of the occurred event, and operate (assign a person in charge, recover, and delete) the event.

Click **Events** menu to display the Events page.

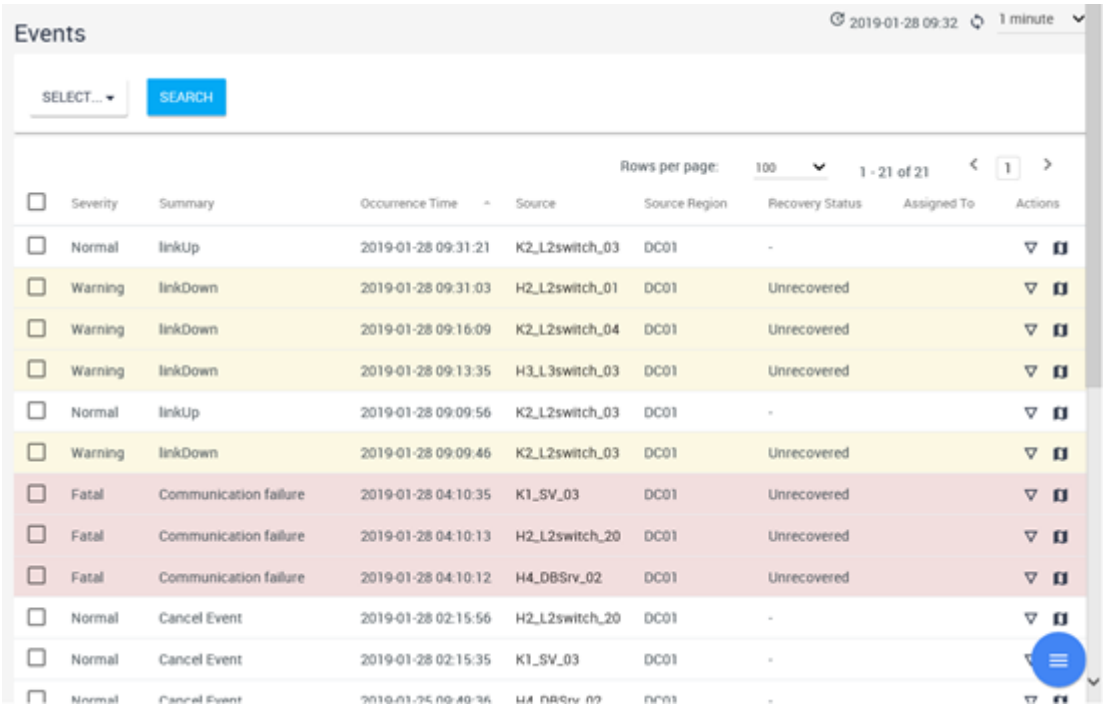

Figure 4-5 Events Page

Screen operation area

- **Last Updated**

  Displays the last update date.

- **Update** icon

Click this icon to refresh the display of the page.

- **Update interval**

  Select the refresh interval of the display of the page from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**). The default is **1 minute**.

Specifying search conditions

Event information to be displayed can be narrowed down by specifying conditions for items displayed in the event list.

- How to add or remove search conditions

  A new search condition can be added from the pull-down menu by clicking the **Select** button.

  To remove the added search condition, click the − icon displayed at the beginning of it.

- How to specify search conditions

  There are the following three methods to specify search conditions for items displayed in the event list. The search condition specification method differs depending on the selected item.

  - Specification by selecting a check box

    Specify a search condition by selecting the corresponding check box. This specification method is available for the following items.

    * Target items:

      Severity, **Recovery Status**

  - Specification by using a keyword

    Specify a keyword and collation method for the selected item. This specification method is available for the following items.

    * Target items:

      Summary, **Source**, **Source Region**, **Assigned To**

    The following collation methods are available.

    * Collation methods:

      is (match), **is not** (not match), **contains** (included), **does not contain** (not included), **starts with** (forward match), **ends with** (backward match)

      In **Source** and **Assigned To**, you can also specify **is not defined**.

  - Specification of a time range

    Specify the time range in *YYYY-MM-DD hh:mm* format for the selected item. This specification method is available for the following items.

    * Target items:

      Occurrence Time

Tip

If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

After specifying the conditions, click the **SEARCH** button to display a list of events that match the specified search conditions.

Caution

When searching for **Source**, pay attention to the followings.

- If the **Name** of the node from which the event occurred is changed, the **Source** of the event that had occurred is not changed.
- Events issued by the IMS component do not have **Source** information. To search events issued by the IMS component, use the collation method: **is not defined** for the **Source**.

Event list

- **Check box**

  Selects the operation target events of each button popped up when the mouse cursor is over the **CHOOSE ACTION FOR SELECTED EVENTS:** button.

  For the events whose **check box** is selected, the following operations can be performed.

  Tip

  The **CHOOSE ACTION FOR SELECTED EVENTS:** button is not displayed to users who belong only to observer groups.

  - **ASSIGN ME** button

    Assigns the currently logged in user to the person in charge for the selected events.

  - **UNASSIGN** button

    Releases the assigned users for the selected events. You can also perform for events assigned to other users.

  - **RECOVER EVENT** button

    Recovers the events.

  - **DELETE EVENT** button

    Deletes the events.

- **Severity**

  Displays the severity of the event. For details about the severity of events displayed in Web Console, refer to "4.2.1.3 Event severity levels (page 89)".

- **Summary**

  Displays summary information of the event.

- **Occurrence Time**

  Displays the occurrence time of the event.

- **Source**

  Displays the names of the node or interface where the event occurred.

- **Source Region**

  Displays the name of the region group to which the node where the event occurred belongs.

- **Recovery Status**

Displays the recovery status of the event. **Unrecovered** is displayed for currently occurring events.

- **Assigned To**

  The user name (display name) responsible for handling the event is displayed. If no one is assigned, it will be blank.

- **Actions**

  Click the following icons to display the operation screens for the event.

  - **Event Detail** icon

    Displays the Event Detail dialog box of the event.

  - **Topology Map** icon

    Displays the topology map where the source node is located. The topology map is displayed in the **analysis mode**

    Tip

    * The **Topology Map** icon is displayed when using the Network Manager.
    * If the node is located on multiple maps, a dialog box to select the map to be displayed is displayed.

Select the number of events to be displayed on one page from the pull-down menu (**50**, **100**, or **250**). The default is **100**.

If all of node information that matches the search conditions cannot be displayed on one page, switch pages to check the information.

Tip

The maximum number of events that can be held is 1,000,000. When the number of events exceeds 1,000,000, old events are deleted in order.

4.2.1.2 Event Detail dialog box and page

The Event Detail dialog box and Event Detail page are described below.

The Event Detail dialog box and the Event Detail page allow users to check the details of the selected event.

Click the **Event Detail** icon of the event on each page displaying event information to display the Event Detail dialog box.

The Event Detail page can be displayed from the URL in the e-mail body that is sent by the event action.

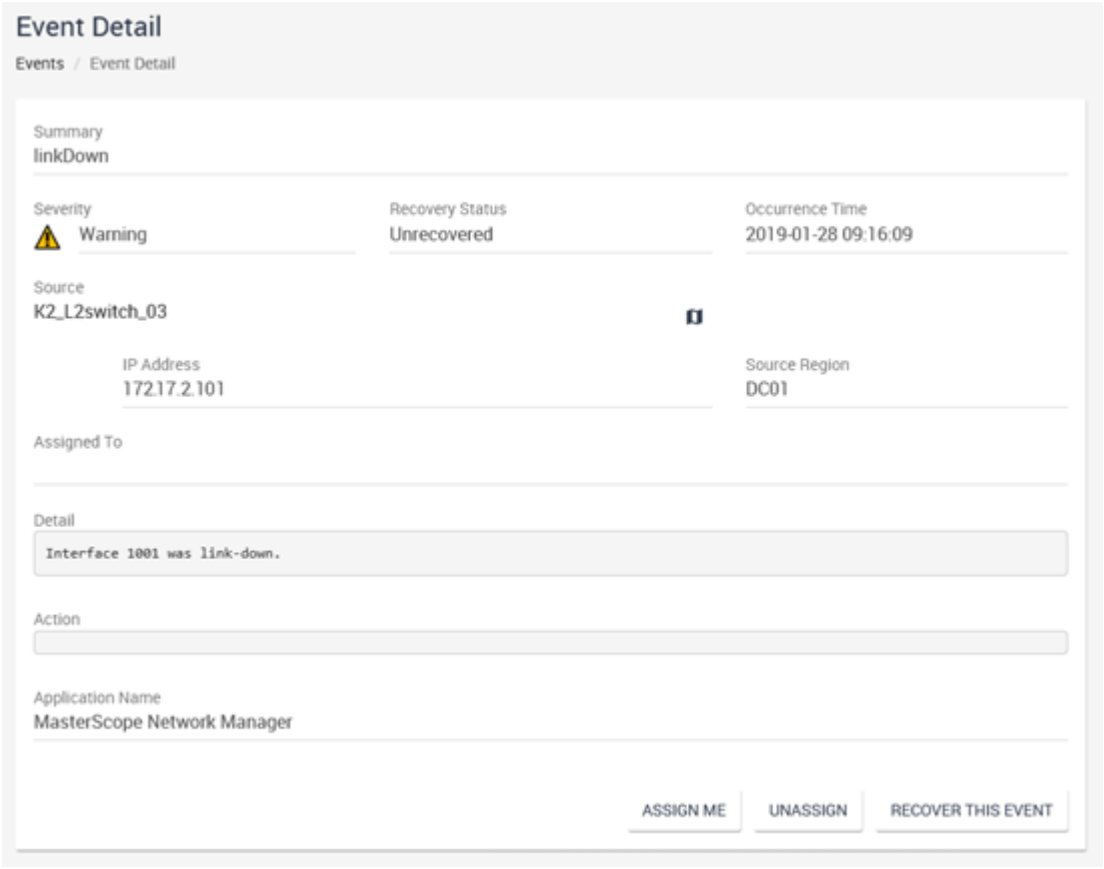

Figure 4-6 Event Detail Dialog Box

Tip

The display contents of event information are the same for the Event Detail dialog box and the Event Detail page. It is possible to manipulate events with operation buttons only in the Event Detail page.

- **Summary**

  Displays summary information of the event.

- **Severity**

  Displays the severity of the event. For details about the severity of events displayed in Web Console, refer to "4.2.1.3 Event severity levels (page 89)".

- **Recovery Status**

  Displays the recovery status of the event. **Unrecovered** is displayed for currently occurring events.

- **Source**

  Displays the name of the node and network interface as the source of the event. Also, the IP address of the relevant node and the region group to which the node belongs are displayed.

  ### Caution

  The value of the IP address to be notified as the source of the event is the value of the IP address managed by the product that detected the event. Therefore, depending on the environment, it may be different from the IP address value managed by the IMS component displayed on the Node Detail page of the Web Console.

Clicking the **Topology Map** icon displays the topology map in which the node where the event occurred is placed.

Tip

- The **Topology Map** icon is displayed when using the Network Manager.
- In case of the Event Detail dialog box activated from the **Current Alert** widget, the Topology Map page is displayed in the **normal mode** displaying the current situation. Otherwise, the Topology Map page is displayed in the **analysis mode** which can display the situation at the time of the event occurrence, and the **Period** is set a period centered on the occurrence time of the event.
- If the node is located on multiple maps, a dialog box to select the map to be displayed is displayed.

- **Occurrence Time**

  Displays the occurrence time of the event.

- **Assigned To**

  The user name (display name) responsible for handling the event is displayed. If no one is assigned, it will be blank.

- **Detail**

  Displays the detail of the event.

- **Action**

  Displays the action for the event.

- **Application Name**

  Displays the application name that detected the event. This application name indicates the name of the product connected to the IMS component.

Event operation buttons

The following buttons are provided on the Event Detail page to operate events.

Tip

Users only with the Observer authority cannot use the event operation buttons.

- **ASSIGN ME** button

  Assigns the currently logged in user as a person in charge for the event.

- **UNASSIGN** button

  Releases the assigned user for the event.

- **RECOVER THIS EVENT** button

  Recovers the event.

  ### Tip

  Depending on the specifications of the product detecting an event, some event may not be recovered. For such events, the recovery state is automatically detected and recovery of them is performed.

4.2.1.3 Event severity levels

The following event severity levels are reported to Web Console.

Event severity levels of Web Console

On Web Console, the following six severity levels are assigned to the events detected by each product and reported. The following severity levels are listed from the highest.

- **Fatal**

  Indicates that a fatal problem such as a system down occurred.

  Tip

  The usage rate displayed on the Web Console is calculated by assuming that *"a node is stopped"* during the duration of a **Fatal** event.

- **Critical**

  Indicates that a problem that is not fatal such as a system down but requires urgent action occurred.

- **Error**

  Indicates that a general error that may affect system operations occurred.

- **Warning**

  Indicates that an event that requires attention or confirmation occurred.

- **Unknown**

  Indicates that an event whose severity is unknown occurred. **Unknown** is reported if the severity is not defined on the product that detected the relevant event.

- **Normal**

  Indicates that information about operations was reported. For example, this severity is assigned to an event indicating the change in the system status or an event indicating that the occurred event has been recovered.

Severity correspondence among the products

The expressions of some severity levels are different between Web Console and other product. "Table 4-1 Severity Correspondence Among the Products (page 89)" shows the severity correspondence.

Table 4-1 Severity Correspondence Among the Products

Web Console	Network Manager	NFA
Fatal	FATAL	-
Critical	MAJOR	FATAL
Error	MINOR	-
Warning	Warning	Warning

Web Console	Network Manager	NFA
Unknown	Unknown	-
Normal	Normal	Normal

4.2.1.4 Narrowing down the event contents to be displayed

The Events page allows users to narrow down the events by specifying various conditions.

The following specific procedure to operate the Events page uses an example to search for events occurred at night (2018/10/01 22:00:00 to 2018/10/02 03:00:00).

1. Display the Events page.

   Click **Events** menu.

2. Enter the search condition.

   Select the item subject to the condition from the pull-down menu. Then, the input box corresponding to the selected item is displayed.

   Here, select **Occurrence time** from the pull-down menu, and specify *"2018-10-01 22:00:00"* to *"2018-10-02 03:00:00"* in the input box.

   Tip

   - A new search condition can be added from the pull-down menu by clicking the **Select** button.

     To remove the added search condition, click the icon displayed at the beginning of it.
   - If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

3. Click the **SEARCH** button.

   Search results are displayed on the Events page.

4.2.1.5 Assigning a person in charge of an event

The following describes how to manage the events that you are responsible for.

By assigning a person in charge of the events notified to Web Console, you can manage the events that you are responsible for on the Events page.

Tip

Users only with the Observer authority cannot perform this operation.

1. Display the Events page.

   Click **Events** menu.

2. Select the event that you will be responsible for.

   Select the check box of the event that you will be responsible for on the Events page.

3. Assign you as a person in charge of events.

   a. Move the mouse cursor over the **CHOOSE ACTION FOR SELECTED EVENTS:** button.

      The **ASSIGN ME** button pops up.

b. Click the **ASSIGN ME** button.

The Confirmation dialog box is displayed.

4. Check the contents on the Confirmation dialog box.
5. Assign yourself as a person in charge of the event.

Click the **OK** button on the Confirmation dialog box.

Then, your user name is registered to the **Assigned To** column of the event whose check box is selected.

6. Narrow down the events by a person in charge.

a. Select the search item.

Select **Assigned To** from the pull-down menu.

b. Select the collation method.

Select **is** from the pull-down menu.

c. Specify the search keyword.

Specify your user name (display name).

d. Start the search.

Confirm the specified setting and then click the **SEARCH** button.

The events that your are in charge of are displayed in the event list.

Take appropriate action for the events by checking the events that you are in charge of according to the above procedure.

Tip

- Use the **UNASSIGN** button to release assigned users.
- If using **ASSIGN ME** button for events to which users are already assigned are selected, assigned users are changed to you.

4.2.1.6 Recovering an event

The following describes how to recover an event.

After the response to the occurred event is complete, recover the relevant event.

The specific procedure is described below using an example to recover a *"fan fault"* (SNMP trap) event of *"router 01"* detected by Network Manager.

Tip

- Users only with the Observer authority cannot perform this operation.
- Depending on the specifications of the product detecting an event, some event may not be recovered.
- If the recovery operation is performed for the event, the recovery operation is also performed on the product that detected the event.

1. Display the Events page.

Click **Events** menu.

2. Select the event to be recovered.

Select the check box of the event to be recovered on the Events page.

Narrow down the display contents of the event as necessary, and select the event.

Here, select the check box of the *"fan fault"* event of *"router 01"* detected by Network Manager.

3. Execute **Restore**.

   a. Move the mouse cursor over the **CHOOSE ACTION FOR SELECTED EVENTS:** button.

      The **RECOVER EVENT** button pops up.

   b. Click the **RECOVER EVENT** button.

      The Confirmation dialog box is displayed.

4. Check the contents on the Confirmation dialog box.
5. Restore the event recovery.

   Click the **OK** button on the Confirmation dialog box.

   The *"fan fault"* alert of *"router 01"* is recovered on Network Manager.

   Then, on the Events page of Web Console, **Recovery state** of the selected *"fan fault"* event of *"router 1"* changes to **Recovered**.

4.2.1.7 Deleting the event

The following describes how to delete the event.

The events not requiring management or response, notified by a task such as changing a network configuration, can be deleted manually.

Tip

Users only with the Observer authority cannot perform this operation.

1. Display the Events page.

   Click **Events** menu.

2. Select the event to be deleted.

   Select the check box of the event to be deleted on the Events page.

   Narrow down the display contents of the event as necessary, and select the event.

3. Execute **Delete**.

   a. Move the mouse cursor over the **CHOOSE ACTION FOR SELECTED EVENTS:** button.

      The **DELETE EVENT** button pops up.

   b. Click **DELETE EVENT** button.

      The Confirmation dialog box is displayed.

4. Check the contents on the Confirmation dialog box.
5. Start the deletion.

Click the **OK** button on the Confirmation dialog box.

The events whose check box is selected on the Events page are deleted.

4.2.2 Checking the events on the network map (Analysis mode)

The Topology Map page can be displayed in two types of **View mode**: **normal mode** displaying the current status and **analysis mode** displaying the past node status (severity). When checking the network status, distinguish between these two modes. This section explains the operation in **analysis mode** displaying the past node status.

The Timeline page is displayed by displaying the Topology Map in **Analysis mode**. The past status of each node is reflected and displayed on the network map by using this Timeline page and specifying **Period**. On the Side Panel, the past load status of the specified node is displayed.

For example, if it is confirmed the next morning that a fault that occurred at midnight was already recovered by automatic recovery, **analysis mode** is available to visually check the midnight situation at the time of the fault occurrence by reproducing it on the Topology Map page.

4.2.2.1 Topology Map page (Analysis mode)

The Topology Map page in **Analysis mode** is described below.

The Topology Map page allows users to check the network configuration, and the status (severity) and load of each node. By switching **View mode** to **analysis mode**, the past status of each node is reflected in the network map, enabling to investigate the situation at that time.

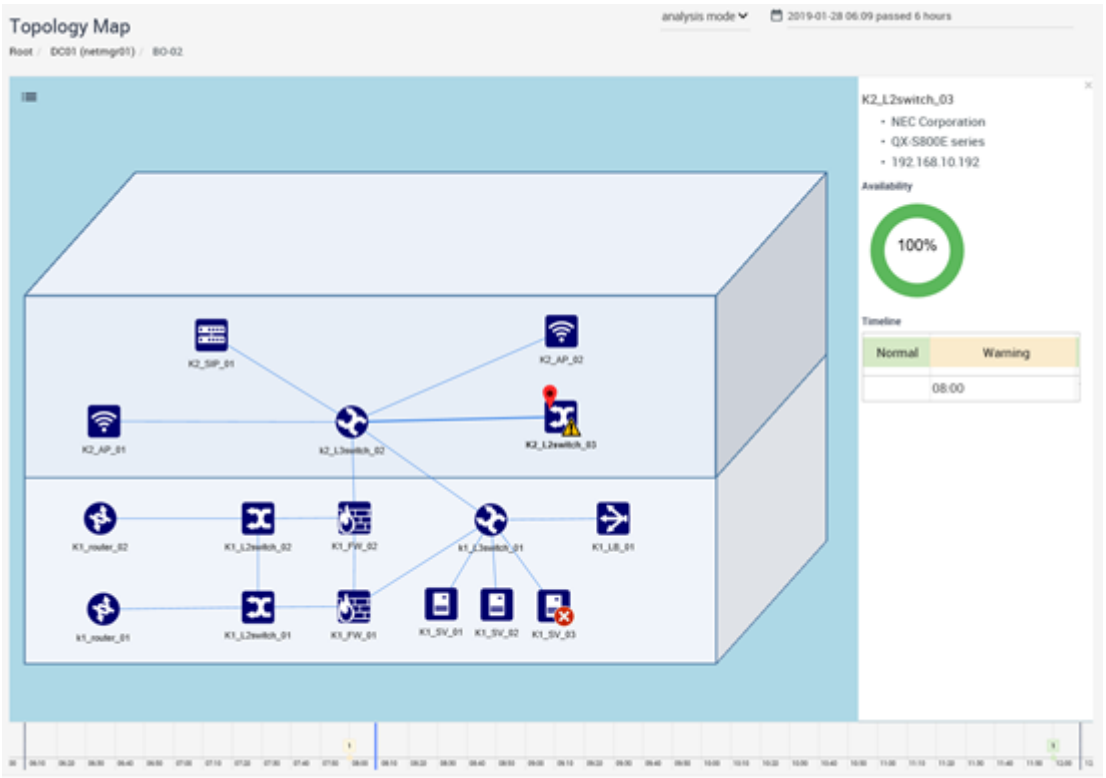

Figure 4-7 Topology Map Page (Analysis mode)

Screen operation area

Switching **View mode** to **analysis mode** stops automatic updating of the page display, and the data within the range specified for **Period** is displayed.

- **Period** (Analysis mode)

  From the pull-down menus to select the start date and period, select the display period of the data to be displayed on the Topology Map page on which the Timeline and Side Panel are displayed. By default, **Start Time** is *"1 hour ago from now"* and **Period** is *"1 hour"*.

Timeline page

The changes of the status (severity) of each node displayed on Map View are displayed in chronological order. The display range is the range specified for **Period**. By moving **Slider**, the status of each node at that time is reflected in then network map. The status (severity) of the **Map** icon on Tree View is also changed.

The map and node status in case of a past fault can be reproduced visually, enabling to check the influence range at that time and to investigate the relevance of fault occurrence.

⚠ Caution

In the Timeline, pat severity status of nodes is displayed based on the event occurrence history. On the other hand, the map configuration displays only the current state and does not manage changes from past. Therefore, if the map configuration has been changed, the timeline contents and map contents may not match.

Other displays

The display contents and operation methods of Tree View, Map View, and Side Panel are the same as those of **normal mode**. For details, refer to "4.1.2.1 Network Map page (Normal mode) (page 73)".

4.2.2.2 Checking the past event occurrence status by using a network map

The following describes how to visually check past event occurrence status by using a network map.

By displaying the Topology Map page in **analysis mode**, the network status and relevance of event occurrence of the past event can be checked on the network map.

The following specific procedure to operate the Topology Map page (Analysis mode) uses an example to check the influence of the events occurred around *"2018/10/01 00:00:00"* on the network map.

1. Display the Events page.

   Click **Events** menu.

2. Enter the search condition.

   Here, select **Occurrence Time** from the pull-down menu. To search for the events that occurred around *"2018/10/01 00:00:00"*, specify *"2018-09-30 23:00:00"* and *"2018-10-01 01:00:00"* for the input boxes.

3. Click the **SEARCH** button.

   Search results are displayed on the Events page.

4. Check the search results on the Events page.

   Check the event contents and relevance of event occurrence from the contents displayed in the event list.

5. Display the network map from the event.

   Clicking the **Topology Map** icon of the event displays the network map in which the node where the event occurred is placed.

   Here, click the **Topology Map** icon of the event whose severity is the highest among the occurred events.

   Clicking the **Topology Map** icon displays the Topology Map page in **analysis mode**.

6. Review the value set to **Period** as necessary.

   When the Topology Map page is displayed from an event, the display period including the event occurrence time is automatically set. If the display period is not appropriate, specify **Period** again.

   In this example, *"2018-09-30 23:00:00"* is specified for **Start Time** and *"2 hours"* is specified for **Period**. Then, the period *"2018-09-30 23:00:00 ~ 2018-10-01 01:00:00"* to be investigated is displayed.

7. Check the changes in the node status (severity) during the specified period.

   On the Timeline page, check the time zone in which the status of each node changed and the nodes whose status changed.

8. Check the changes over time in the node status.

   Move **Slider** on the Timeline page to reflect the status to the network map and check the status of each node when the event occurred and examine the influence on peripheral systems.

   Tip

   - By using **Slider** with displaying Tree View, it is also possible to check whether the statuses of the nodes on another network map were changed.
   - If you want to check the details of the status change, specify **Period** as short as possible.

If the occurred event affected the load of the node, click the node icon on the network map to display the Side Panel. The status can be checked on this page. If you need to check a specific node in more detail, click the node name link displayed on the Side Panel to display the Node Detail page corresponding to the relevant node.

4.3 Checking the node status in detail

The Node Detail page displays the dashboard specific to the specified node.

The Node Detail page is available to check the following information of the specified node, understanding the detailed node status promptly.

- Property information
- Usage rate information
- Event list
- Flow information by rank (TopN)
- Load information of CPU, memory, and network interfaces by rank (TopN)

4.3.1 Node Detail page

The following describes Node Detail page that displays the dashboard specific to the specified node.

The Node Detail page is used to grasp the detailed node status based on information in various viewpoints.

The Node Detail page is displayed by clicking the node name link displayed on each page.

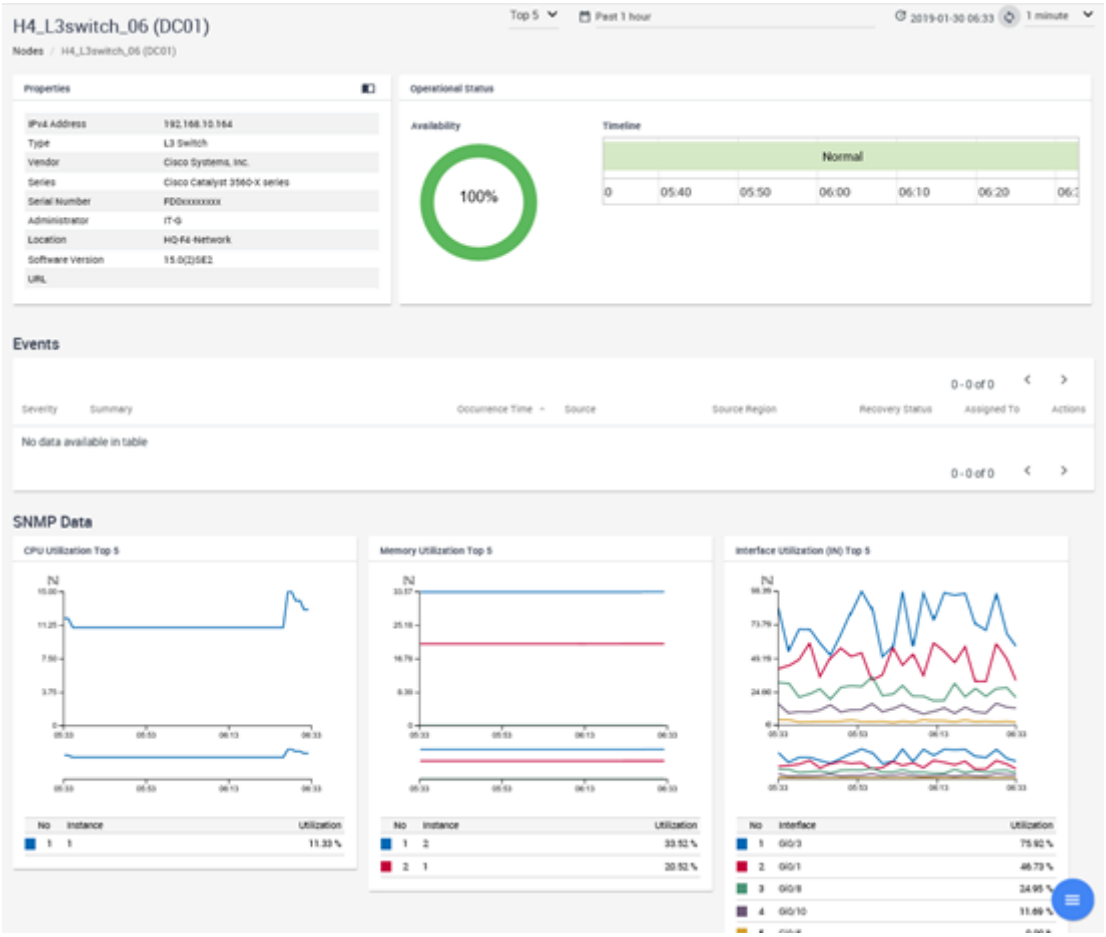

Figure 4-8 Node Detail Page

The following buttons are popped up when the mouse cursor is over the **MENU** button on the Node Detail page. You can display each page for this node by clicking the following buttons.

- **FLOW ANALYZE** button

  Displays the Exporter Analysis page of the NFA where this node is registered as an exporter. This button is displayed when using the NFA.

- **TOPOLOGY MAP** button

  Displays the topology map where this node is located. This button is displayed when using the Network Manager.

  Tip

  If the node is located on multiple maps, a dialog box to select the map to be displayed is displayed.

- **IPV6 ADDRESSES** button

Displays the IPv6 Addresses page for this node. This button is displayed when using the Network Manager.

- **NETWORK INTERFACES** button

  Displays the Network Interfaces page for this node.

Screen operation area

- **Top N**

  Select the number of ranked data items to be displayed on each widget from the pull-down menu (**Top 5**, **Top 10**, or **Top 20**). The default is **Top 5**.

- **Period**

  Specify the display period of data to be used on a widget by using either of the following two methods.

  - **Select from Default Periods** (Default)

    Select the data display period from the pull-down menu (**Past 15 minutes**, **Past 30 minutes**, **Past 1 hour**, **Past 6 hours**, **Past 24 hours**, **Past 48 hours**, or **Past 72 hours**). The default is **Past 1 hour**.

  - **Specify Starting Time and Period**

    Specify the start date and time and the data display period by selecting from the pull-down menu and so on. By default, **Start Time** is *"1 hour ago from now"* and **Period** is *"1 hour"*.

- **Last Updated**

  Displays the last update date.

- **Update** icon

  Click this icon to refresh the display of the page.

- **Update interval**

  Select the refresh interval of the display of the page from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**). The default is **1 minute**.

Widget display area

Displays widgets related to the specified node. The following widgets are displayed on the Nodes page.

- **Properties** widget

  Displays property information of a node. Clicking the icon displays the Property Details dialog box.

  Information registered to Network Manager or NFA is integrated and displayed for the property information of a node.

  ### Tip

  - If **URL** of the node properties is registered to Network Manager, the registered URL information is displayed in link format in Web Console. This enables to access the corresponding site only by clicking the URL.

- The Property Details dialog box displays the following information that Network Manager collects from the MIB of the node.
  * **Description**

    Displays the description of model information obtained from sysDescr (1.3.6.1.2.1.1.1) of the node.
  * **sysObjectId**

    Displays the ID to identify the model obtained from sysObjectId (1.3.6.1.2.1.1.2) of the node.

- **Operational Status** widget

  Displays the node usage rate and the timeline indicating state changes.

  This widget is displayed if Network Manager is used.
- **Events** widget

  Displays a list of the events that occurred on the relevant node. Clicking the ▽**Event Detail** icon displays the Event Detail page for the relevant node.
- Flow data

  The following flow data widgets are displayed if NFA is used.
  - **Applications** widget

    Displays ranking data for the data traffic of each application within the communication flow via the relevant node.
  - **IP Protocols** widget

    Displays ranking data for the data traffic of each IP protocol within the communication flow via the relevant node.
  - **DSCP** widget

    Displays ranking data for the data traffic of each DSCP value (IP packet priority setting) within the communication flow via the relevant node.
  - **Conversations** widget

    Displays ranking data for the data traffic of conversation (information between two communication points) within the communication flow via the relevant node.
- SNMP data

  The following SNMP data widgets are displayed if Network Manager is used.
  - **CPU Utilization** widget

    Displays ranking data for the CPU usage rate of a node.
  - **Memory Utilization** widget

    Displays ranking data for the memory usage rate of a node.
  - **Interface Utilization (IN)** widget

    Displays ranking data for the input usage rate of network interfaces kept by a node.
  - **Interface Utilization (OUT)** widget

    Displays ranking data for the output usage rate of network interfaces kept by a node.
  - **Packet Loss Rate (IN)** widget

Displays ranking data for the input packet loss rate of network interfaces kept by a node.

- **Packet Loss Rate (OUT)** widget

  Displays ranking data for the output packet loss rate of network interfaces kept by a node.

- **Packet Error Rate (IN)** widget

  Displays ranking data for the input packet error rate of network interfaces kept by a node.

- **Packet Error Rate (OUT)** widget

  Displays ranking data for the output packet loss rate of network interfaces kept by a node.

Caution

If the settings to collect data has not been configured for Network Manager and NFA, the SNMP data and flow data widgets are not displayed.

4.3.2 Checking the past status of nodes

The following describes how to check the past status of a specific node from the Node Detail page.

The Node Detail page displays widgets of the past statuses of a node by specifying the target past period for **Period**.

The following describes the specific procedure based on the example to check the past statuses of *"router 01"* according to the event that occurred in *"router 01"* around *"23:00"* last night.

1. Display the Events page.

   Click **Events**.

2. Search for the nodes to be checked for failure.

   a. Select **Source** from the pull-down menu.

   b. Select **is** as the collation method.

   c. Enter the name of the node to be checked for failure.

      Here, enter *"router 01"*.

   d. Click the **SEARCH** button.

   A list of the events that occurred in *"router 01"* is displayed on the Events page.

3. Check the event contents.

   For example, suppose that an event of *"CPU Usage Rate Threshold Excess"* occurred around *"23:00"* last night. In the steps below, the procedure to inspect an event of *"CPU Usage Rate Threshold Excess"*.

4. Display the Node Detail page for the node on which the target event occurred.

   Click the link of the node name displayed in **Source**.

   Here, click the link of *"router 01"*.

   Then, the Node Detail page for *"router 01"* is displayed. **Period** displays the past period containing *"23:00"* last night when the event of *"CPU Usage Rate Threshold Excess"* occurred.

5. Check the node status during the specified period.

   The **CPU Utilization** widget is available to check the CPU behavior at that time.

The **Interface Utilization (IN)** and **Interface Utilization (OUT)** widgets are available to check the data traffic at that time.

The **Applications** and **Conversations** widgets are available to the communication contents through *"router 01,"* enabling to inspect whether there is any event that affected the CPU load.

If no problem is found in the checked communication statuses, check **Software Version** displayed on the **Properties** widget and ask the support desk of *"router 01"* for whether the router has any known issue.

If the communication status might have caused to increase the CPU usage rate, the detailed flow analysis using NFA is effective. The Exporter Analysis page of the NFA can be displayed easily by clicking a link in the **Applications** or **Conversations** widgets, or the **FLOW ANALYZE** button.

4.4 Checking the network interface status

Web Console provides the mechanism to check detailed information of network interfaces that the specified node keeps.

The following pages are provided as the specific procedures to check detailed information of network interfaces.

- Network Interfaces page

  This page displays property information of all network interfaces that a node keeps. For a device that keeps many network interfaces, information to be displayed can be narrowed down by specifying search conditions.

- IPv6 Addresses page

  This page displays property information of IPv6 addresses assigned to network interfaces of a node.

- Network Interface Detail page

  This page displays various data of the specified network interface to check its communication status.

4.4.1 Network Interfaces page

The Network Interfaces page is described below.

The Network Interface page is available to check the property information of all network interfaces that a node keeps.

The Network Interface page is displayed by clicking the **NETWORK INTERFACES** button on the Node Detail page. The Node Detail page is displayed by clicking the node name link displayed on each page.

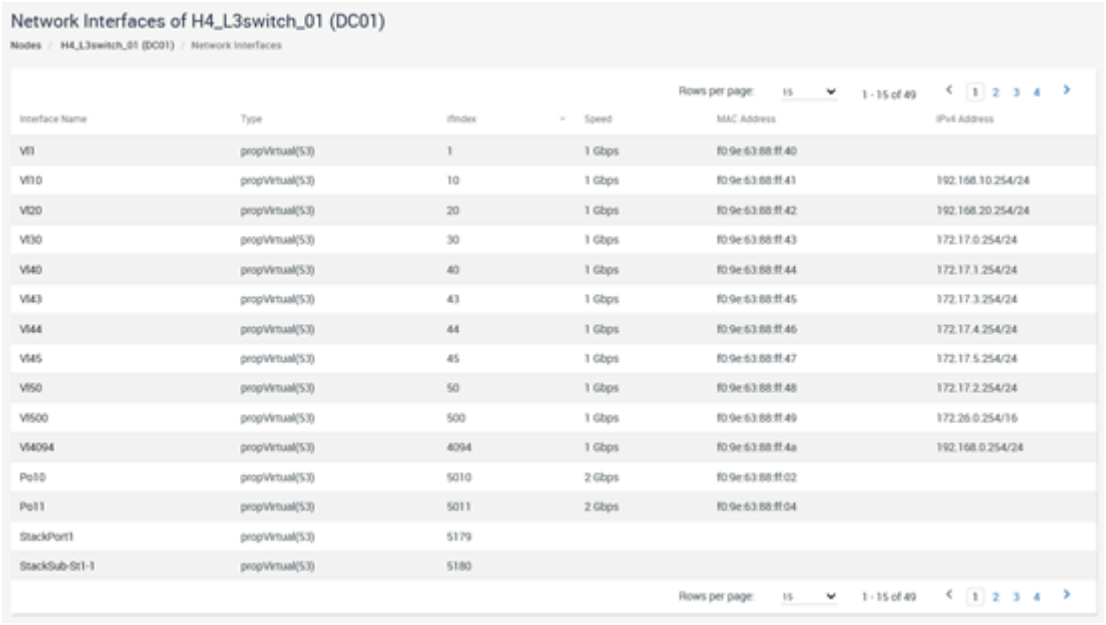

Figure 4-9 Network Interfaces Page

Network interface list

- **Interface Name**

  Displays the network interface name. Click the network interface name link to display the Network Interface Detail page for the relevant network interface.

- **Type**

  Displays the network interface type information.

  Tip

  The value obtained from MIB ifType (1.3.6.1.2.1.2.2.1.3) is displayed according to the notation defined by Internet Assigned Numbers Authority (IANA).

- **ifIndex**

  Displays the ID for uniquely identifying a network interface.

- **Speed**

  Displays the line speed of a network interface.

- **MAC Address**

  Displays the MAC address assigned to a network interface.

- **IP Address**

  Displays the IPv4 address assigned to a network interface.

Select the number of network interface information items to be displayed on one page from the pull-down menu (**15**, **50**, or **100**). The default is **15**.

If whole of the network interface information that matches the search conditions cannot be displayed on one page, switch pages to check the information.

4.4.2 IPv6 Addresses page

The IPv6 Addresses page is described below.

The IPv6 Addresses page is available to check information of the IPv6 addresses assigned to a node.

The IPv6 Addresses page is displayed by clicking the **IPV6 ADDRESSES** button on the Node Detail page. The Node Detail page is displayed by clicking the node name link displayed on each page.

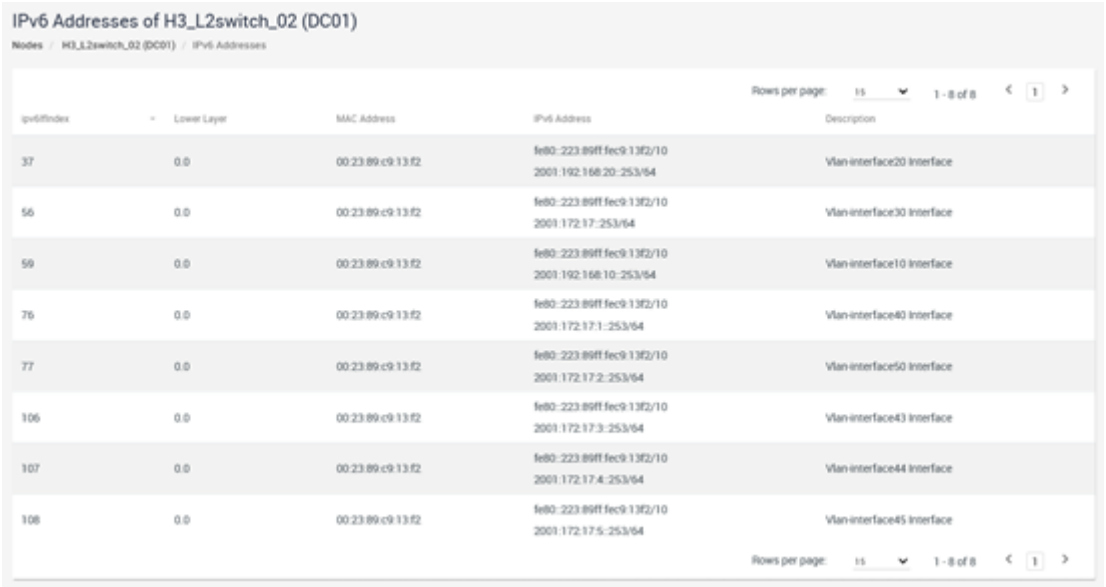

Figure 4-10 IPv6 Addresses Page

IPv6 address list

- **ipv6ifIndex**

  Displays the ID for uniquely identifying an IPv6 interface.

- **Lower Layer**

  Displays the ID for identifying a protocol layer in which a network interface operates.

- **MAC Address**

  Displays the MAC address assigned to an IPv6 network interface.

- **IPv6 Address**

  Displays the IPv6 address assigned to an IPv6 network interface.

- **Description**

  Displays the description of an IPv6 interface.

4.4.3 Checking the IPv6 address assigned to a node

The following describes how to check the IPv6 address assigned to a node.

The specific procedure is described below using an example to check the IPv6 address assigned to *"router 01"*.

1. Display the Nodes page.

   Click **Nodes** menu.

2. Select the item to be checked.

   Here, click the link of *"router 01"* in the **Node Name** box.

The Node Detail page for *"router 01"* is displayed.

3. Check the IPv6 address used in the monitoring process.

   Click the ▽ icon of the **Properties** widget to display the Property Details dialog box. On the Property Details dialog box, the IPv6 address used in the monitoring process is displayed in the **IPv6 Address** box.

4. Display the IPv6 Addresses page.

   To check the assignment status of other IPv6 addresses, display the IPv6 Addresses page following the steps below.

   Click the **IPV6 ADDRESSES** button on the Node Detail page.

5. Check the contents displayed on the IPv6 Addresses page.

   The IPv6 Addresses page displays information of all IPv6 addresses assigned to a node including the IPv6 address used in the monitoring process.

4.4.4 Network Interface Detail page

The following describes the Network Interface Detail page that displays various data indicating the communication status the specified network interface.

The Network Interface Detail page is used to grasp the detailed network interface status based on information in various viewpoints.

The Network Interface Detail page is displayed by clicking the network interface name link displayed on each page.

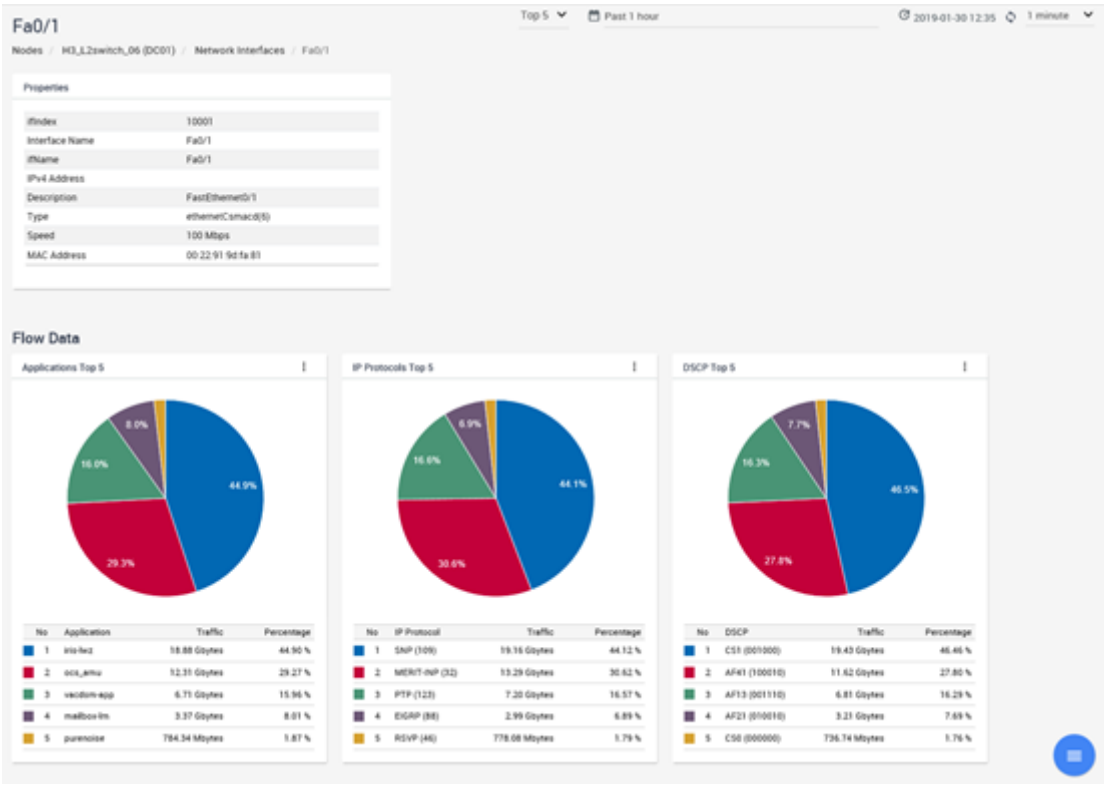

Figure 4-11 Network Interface Detail Page

The following buttons are popped up when the mouse cursor is over the **MENU** button on the Network Interface Detail page.

- **FLOW ANALYZE** button

  Displays the Exporter Analysis page of the NFA where this network interface is registered. This button is displayed when using the NFA.

Screen operation area

- **Top N**

  Select the number of ranked data items to be displayed on each flow information widget from the pull-down menu (**Top 5**, **Top 10**, or **Top 20**). The default is **Top 5**.

  Tip

  If NFA is not used, **Top N** is not displayed.

- **Period**

  Specify the display period of data to be used on a widget by using either of the following two methods.

  - **Select from Default Periods** (Default)

    Select the data display period from the pull-down menu (**Past 15 minutes**, **Past 30 minutes**, **Past 1 hour**, **Past 6 hours**, **Past 24 hours**, **Past 48 hours**, or **Past 72 hours**). The default is **Past 1 hour**.

  - **Specify Starting Time and Period**

    Specify the start date and time and the data display period by selecting from the pull-down menu and so on. By default, **Start Time** is *"1 hour ago from now"* and **Period** is *"1 hour"*.

- **Last Updated**

  Displays the last update date.

- **Update** icon

  Click this icon to refresh the display of the page.

- **Update interval**

  Select the refresh interval of the display of the page from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**). The default is **1 minute**.

Widget display area

Displays widgets related to the specified network interface. The following widgets are displayed on the Network Interface Detail page.

- **Properties** widget

  Displays property information of a network interface.

- Flow data

  The following flow data widgets are displayed if NFA is used.

  - **Applications** widget

    Displays ranking data for the data traffic of each application within the communication flow via the relevant network interface.

- **IP Protocols** widget

  Displays ranking data for the data traffic of each IP protocol within the communication flow via the relevant network interface.

- **DSCP** widget

  Displays ranking data for the data traffic of each DSCP value (IP packet priority setting) within the communication flow via the relevant network interface.

- **Conversations** widget

  Displays ranking data for the data traffic of conversation (information between two communication points) within the communication flow via the relevant node.

• SNMP data

  The following SNMP data widgets are displayed if Network Manager is used.

- **Interface Utilization (IN)** widget

  Displays the input usage rate of a network interface.

- **Interface Utilization (OUT)** widget

  Displays the output usage rate of a network interface.

- **Packet Loss Rate (IN)** widget

  Displays the input packet loss rate of a network interface.

- **Packet Loss Rate (OUT)** widget

  Displays the output packet loss rate of a network interface.

- **Packet Error Rate (IN)** widget

  Displays the input packet error rate of a network interface.

- **Packet Error Rate (OUT)** widget

  Displays the output packet loss rate of a network interface.

Caution

If the settings to collect data has not been configured for Network Manager or NFA, the SNMP data or flow data widgets are not displayed.

4.4.5 Checking the past status of network interfaces

The following describes how to check the past status of a specific network interface from the Network Interface Detail page.

The Network Interface Detail page displays widgets of the past statuses of a network interface by specifying the target past period for **Period**.

The specific procedure is described below using an example to check the past statuses of *"GigabitEthernet1/0/1"* according to the event that occurred in *"switch 01"* around *"23:00"* last night.

1. Display the Events page.

   Click **Events** menu.

2. Search for the nodes to be checked for failure.

   a. Select **Source** from the pull-down menu.

b. Select **is** as the collation method.

c. Enter the name of the node to be checked for failure.

Here, enter *"switch 01"*.

d. Click the **SEARCH** button.

A list of the events that occurred in *"switch 01"* is displayed on the Events page.

3. Check the event contents.

For example, suppose that an event of *"Interface Utilization (IN) Threshold Excess"* occurred around *"23:00"* last night. In the steps below, the procedure to inspect an event of *"Interface Utilization (IN) Threshold Excess"*.

4. Display the Node Detail page for the node on which the target event occurred.

Click the link of the node name displayed in **Source**.

Here, click the link of *"switch 01"*.

Then, the Node Detail page for *"switch 01"* is displayed. **Period** displays the past period containing *"23:00"* last night when the event of *"Interface Utilization (IN) Threshold Excess"* occurred.

5. Check the node status during the specified period.

The **Interface Utilization (IN)** widget is available to check the name of the network interface exceeding the threshold and its behavior before and after the threshold excess occurred. The **CPU Utilization** and **Memory Utilization** widgets are available to check whether an abnormal network interface load has occurred.

6. Display the Network Interface Detail page for the network interface whose load status is abnormal.

Click the network interface name link displayed on the **Interface Utilization (IN)** widget.

Here, click the link of *"GigabitEthernet1/0/1"* that is ranked number 1.

The Network Interface Detail page for *"GigabitEthernet1/0/1"* is displayed. **Period** of the Network Interface Detail page takes over the setting configured on the Node Detail page.

7. Checking the network interface status during the specified period.

On the **Packet Loss Rate (IN)** and **Packet Error Rate (IN)** widgets, it is possible to check whether packet loss or an error occurred, in addition to the usage rate of the input interface of *"GigabitEthernet1/0/1"*.

If NFA is used, it is possible to investigate the application communication increasing the network interface load on the **Applications** widget. The **Conversions** widget is available to check the IP addresses that frequently communicates with each other.

If you want to investigate the communication flow contents in more detail, click the **FLOW ANALYZE** button on the Network Interface Detail page to display the Exporter Analysis page of NFA.

4.5 Checking the event action execution status

The execution results of the pre-defined event actions are all recorded in a log. This section describes how to check event action logs.

By checking event action logs, you can check that the defined event action has been executed properly and that the processes called in the executed event action have been complete normally.

4.5.1 Action Logs page

The Action Logs page is described below.

The Action Logs page allows uses to check the status of the action executed according to the event action definition.

The Action Logs page is displayed by clicking **Event Action Settings**>**Action Logs**.

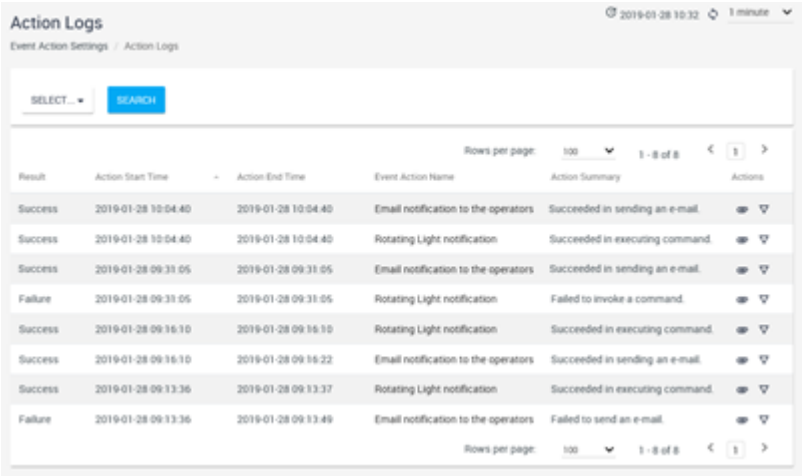

Figure 4-12 Action Logs Page

Screen operation area

- **Last Updated**

  Displays the last update date.

- **Update** icon

  Click this icon to refresh the display of the page.

- **Update interval**

  Select the refresh interval of the display of the page from the pull-down menu (**1 minute**, **5 minutes**, **15 minutes**, or **Nothing**). The default is **1 minute**.

Specifying search conditions

Events to be displayed can be narrowed down by specifying conditions for items displayed in the action log list.

- How to add or remove search conditions

  A new search condition can be added from the pull-down menu by clicking the **Select** button.

  To remove the added search condition, click the − icon displayed at the beginning of it.

- How to specify search conditions

  There are the following three methods to specify search conditions for items displayed in the action log list. The search condition specification method differs depending on the selected item.

- Specification by selecting a check box

  Specify a search condition by selecting the corresponding check box. This specification method is available for the following items.

  * Target items:

    Result

- Specification by using a keyword

  Specify a keyword and collation method for the selected item. This specification method is available for the following items.

  * Target items:

    Event Action Name, **Action Summary**

  The following collation methods are available.

  * Collation methods:

    is (match), **is not** (not match), **contains** (included), **does not contain** (not included), **starts with** (forward match), **ends with** (backward match)

- Specification of a time range

  Specify the time range in *YYYY-MM-DD hh:mm* format for the selected item. This specification method is available for the following items.

  * Target items:

    Action Start Time, **Action End Time**

Tip

If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

After specifying the conditions, click the **SEARCH** button to display a list of action logs that match the specified search conditions.

Action log list

- **Result**

  Display the event action execution results.

  ### Tip

  When command is executed as an action, the result of the action is interpreted as *"Success"* if the command return value is *"0"*, otherwise it is interpreted as *"Failure"*.

- **Action Start Time**

  Displays the date and time when action processing started.

- **Action End Time**

  Displays the date and time when action processing ended.

- **Event Action Name**

  Displays the definition name of the executed event action. Click the event action name link to display the Edit Event Action page in which you can edit the event action definition.

- **Action Summary**

Displays the summary of the action execution status.

- **Actions**

  Click the following icons to display the operation screens for the action.

  - **Action Log Detail** icon

    Clicking this icon displays the Action Log Detail dialog box of the action called by the event action.

  - **Event Detail** icon

    Clicking this icon displays the Event Detail dialog box for the event that triggered the relevant event action.

Select the number of action logs to be displayed on one page from the pull-down menu (**50**, **100**, or **250**). The default is **100**.

If all action logs that match the search conditions cannot be displayed on one page, switch pages to check the action logs.

Tip

The maximum number of action logs that can be held is 10,000. When the number of action logs exceeds 10,000, old logs are deleted in order.

4.5.2 Action Log Detail dialog box

The Action Log Detail dialog box is described below.

Action Log Detail dialog box allows users to check the detailed log showing the processing contents of the event action.

Click the **Action Log Detail** icon in the Action Logs page to display the Action Log Detail dialog box. To display the Action Logs page, click **Event Action Settings**>**Action Logs**.

Figure 4-13 Action Log Detail Dialog Box

- **Action Summary**

  Displays the summary of the action execution status.

- **Action Start Time**

  Displays the date and time when action processing started.

- **Action End Time**

Displays the date and time when action processing ended.

- **Result**

  Display the event action execution results.

  Tip

  When command is executed as an action, the result of the action is interpreted as *"Success"* if the command return value is *"0"*, otherwise it is interpreted as *"Failure"*.

- **Event Action Name**

  Displays the definition name of the executed event action.

- **Action Name**

  Displays the executed action name that is defined in the event action definition.

- **Action Detail**

  In command execution, the contents of standard output and standard error output are displayed. In the case of e-mail notification, error log information on sending e-mail is displayed.

4.5.3 Checking the event action execution results in detail

The following describes how to check the event action execution results in detail.

If the **Result** of the event action is **Failure**, you may be able to investigate the execution status of the action by checking the details of the action log.

The specific procedure is described below using an example to check the executed contents of event action definition *"Contact output command execution"*.

1. Display the Action Logs page.

   Click **Event Action Settings**>**Action Logs**.

2. Search for the action logs to be investigated.

   a. Select **Event Action Name** from the pull-down menu.

   b. Select **is** as the collation method.

   c. Specify the name of the event action to be investigated.

      Here, enter *"Contact output command execution"*.

   d. Click the **SEARCH** button.

   Action logs for *"Contact output command execution"* are displayed on the action log list.

3. Specify the executed contents of the action.

   Click the **Action Log Detail** icon of the action log whose **Result** is **Failure**.

   The Action Log Detail dialog box is displayed.

4. Check the log contents.

   The standard output and standard error output of the executed command are output to the **Action Detail**.

   Check whether there is a problem in the command execution result according to the command specifications by referring to the standard output and standard error output of the called *"contact output command"*.

Chapter 5. System Maintenance

This chapter describes how to maintain in the Web Console usage environment.

Contents

5.1 Managing the mapping status of node management information

If multiple products are registered in one region group, nodes managed by each product are automatically judged on whether or not they are physically the same then registered to the IMS component. The following describes how to check the result for determining whether nodes are physically the same and how to fix any invalid processes that are detected.

5.1.1 Mapping node information

Nodes managed by the products in the same region group are subject to judgment as to whether or not they are the same The following describes in detail the process to determine whether or not the nodes are the same.

If multiple products are registered in one region group, nodes managed by each product are registered to the IMS component after determining whether the nodes are the same according to the following node information managed by each product.

- IP address of the node (IPv4 and IPv6 addresses)
- sysName(1.3.6.1.2.1.1.5) value obtained from the MIB of the node

For example, as shown in "Figure 5-1 Process to Determine Whether or Not Nodes are the Same (page 112)", if nodes managed by Network Manager and NFA are the same, which is determined by checking the IP address and sysName value from the management information of each product, they are registered as the same to the IMS component.

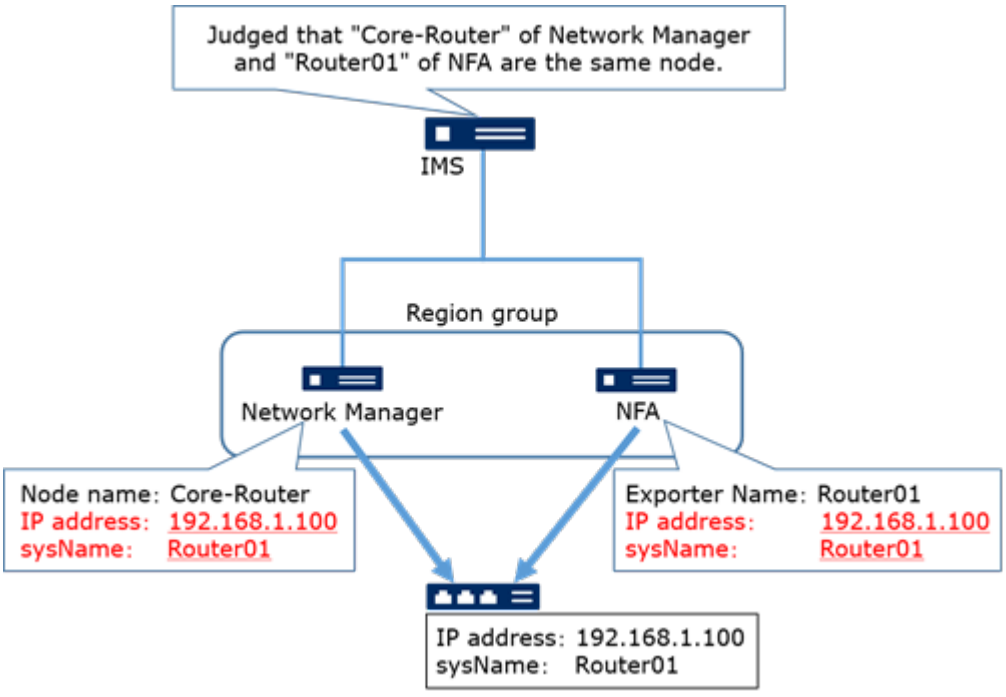

Figure 5-1 Process to Determine Whether or Not Nodes are the Same

Tip

If nodes are determined to be the same, their information is integrated and they are registered as one node in the IMS component. At this time, as shown in "Figure 5-1 Process to Determine Whether or Not Nodes are the Same (page 112)", if the node names of Network Manager and NFA are different, the node name (*"backbone router"*) of Network Manager is registered to the IMS component.

The Node Mappings page is available to check the result of determining whether the nodes are the same. If the result of determining whether the nodes are the same is invalid, correct the node information on the Node Mappings page.

5.1.1.1 Node Mappings page

The Node Mappings page is described below.

The Node Mappings page is available to check the result for determining whether a node managed on multiple products is the same, and to make modifications as necessary.

Click **System Settings**>**Node Mappings** to display the Node Mappings page.

Tip

- Only users with the Administrator authority can display the Node Mappings page.
- It is not necessary to operate on this page when you do not register multiple products in the same region group.

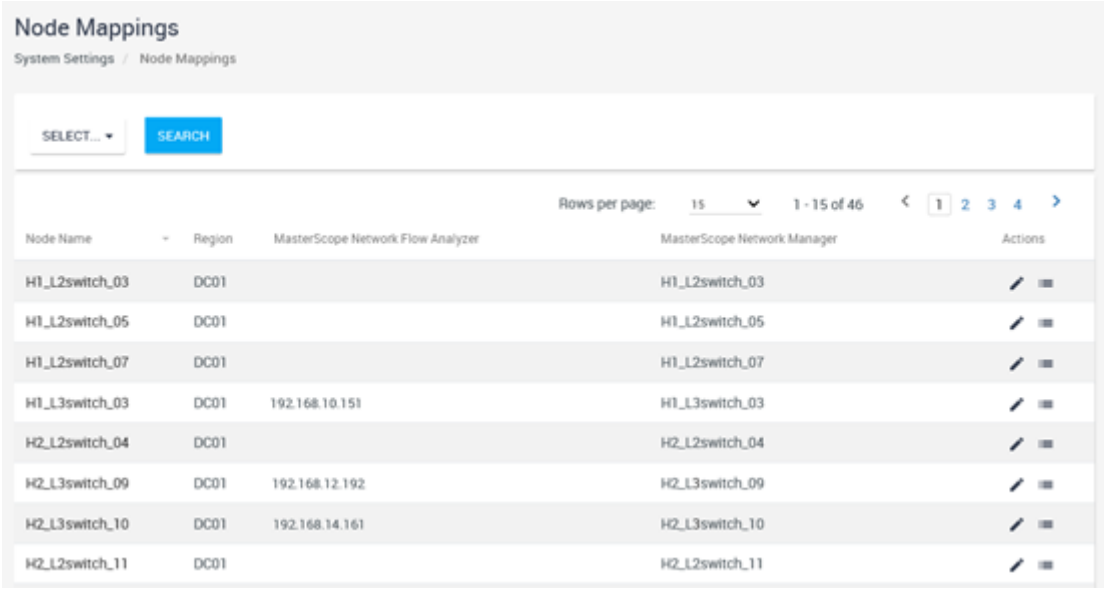

Figure 5-2 Node Mappings Page

Specifying search conditions

Nodes to be displayed can be narrowed down by specifying conditions for items displayed in the node mapping list.

- How to add or remove search conditions

  A new search condition can be added from the pull-down menu by clicking the **Select** button.

  To remove the added search condition, click the − icon displayed at the beginning of it.

- How to specify search conditions

  Specify a keyword and collation method for each item to be displayed in the node mapping list.

  - Target items:

    Node name, **Region**, **<*Product name*>: Node Name**

  - Collation methods:

is (match), **is not** (not match), **contains** (included), **does not contain** (not included), **starts with** (forward match), **ends with** (backward match)

Tip

If conditions are added for different items, they are handled as an AND condition. If multiple conditions are added to the same item, they are handled as an OR condition.

After specifying the conditions, click the **SEARCH** button to display a list of node mappings that match the specified search conditions.

Caution

When searching for ***<Product name>*: Node Name**, nodes matching the conditions are displayed from the names managed by the specified product (<*Product name*>). Nodes that are not managed by the specified product (<*Product name*>) will not be displayed.

Node mapping list

- **Node name**

  Displays the node name used on Web Console.

- **Region**

  Displays the name of the region group to which the node belongs.

- ***<Product name>*: Node Name**

  Displays the node name used on each product. Node names managed by Network Manager are displayed in the **Network Manager: Node Name** column, and node names managed by NFA are displayed in the **NFA: Node Name** column.

- **Actions**

  Click the following icons to display the operation pages for node interface mapping information.

  - **Edit** icon

    Click this icon to modify the result of determining whether the nodes are the same.

    Clicking the **Edit** icon displays the Edit Node Mapping page. For details, refer to "5.1.1.2 Changing the node mapping status (page 114)".

  - **Network interface mappings** icon

    Click this icon to display the result for determining whether the network interface retained by the nodes are the same. Clicking the **Network interface mappings** icon displays the Network Interface Mappings page. For details, refer to "5.1.2.1 Network Interface Mappings page (page 116)".

Select the number of node mapping information items to be displayed on one page from the pull-down menu (**15**, **50**, or **100**). The default is **15**.

If all the node mapping information matching the search conditions cannot be displayed on one page, check the subsequent pages.

5.1.1.2 Changing the node mapping status

The following describes how to modify the result of determining whether the nodes corresponding to the node information displayed on Web Consoleare the same.

If the result of determining whether the nodes are the same is invalid, be sure to correct the result manually.

The specific procedure is described below using an example to correct the determination result if nodes that are not physically the same are determined to be the same.

Caution

If an event has occurred at the node before updating the mapping of the node, the source information of the event does not change even after the mapping update operation. Therefore, the situation may be as follows.

- When separating the mapped nodes:

  If the mapping of the node where the event occurred changes and the name on the IMS component of that node changes, it is treated as if the event occurred in the other node whose name has not changed.

- When manually mapping to one node:

  If the name of the node where the event occurred is changed by the mapping operation, the event is treated as an event not related to the mapped node.

When editing the mapping of nodes, consider this specification and properly read and replace the source of the event.

1. Display the Node Mappings page.

   Click **System Settings**>**Node Mappings**.

2. Search for the node to be updated.

   a. Select **Region** from the pull-down menu.

   b. Select **is** as the collation method.

   c. Enter the name of the region group to which the node to be updated belongs.

   d. Select **Node Name** from the pull-down menu.

   e. Select **is** as the collation method.

   f. Enter the name of the node to be updated.

   g. Click the **SEARCH** button.

   The search results are displayed in the node mapping list.

3. Click the **Edit** icon of the node to be updated.

   The Edit Mapping of Node page for the relevant node is displayed.

4. Update the node mapping information.

   Click the following buttons corresponding to the node information of each product to update the mapping information.

   - **Edit** icon

     Click this icon to display the Select Mapping Node screen. The Select Mapping Node screen displays a list of the nodes managed by the selected product among the nodes in the region group to which the relevant node belongs. On the Select Mapping Node screen, select the changed node and click the **OK** button. Then, information of the selected node is reflected in the Edit Mapping of Node page.

   - **Delete** icon

     Click this icon to unmap the node.

Here, select the node that has been determined as a different node by mistake on the Select Mapping Node screen.

On the Edit Node Mapping page, mapping set to the relevant node is corrected.

5. Register the changes of node mapping.

   Confirm the changes and then click the **OK** button on the Edit Node Mapping page.

   The updates are reflected in the Edit Node Mapping page.

5.1.2 Mapping network interfaces

After determining whether the nodes are physically the same, when information of the nodes managed by multiple products is integrated and registered to the IMS component, whether the network interface information of the nodes are the same is also determined and registered.

Whether the network interfaces are the same is determined by the value of ifIndex(1.3.6.1.2.1.2.2.1.1) that each product obtained from the MIB of the relevant node, and then registered.

The Network Interface Mappings page is available to check the result of determining whether the network interfaces are the same. If the result of determining whether the network interfaces are the same is invalid, correct the network interface information on the Network Interface Mappings page.

Tip

- Since a network interface name and ifIndex value normally have a one-to-one correspondence, network interfaces are identified correctly except when the result of determining whether the nodes are the same is incorrect.

  However, depending on the device specifications, the ifIndex value may be changed by restarting the device. This greatly affects management of network interfaces, including monitoring of each product. For devices with such specifications, be sure to configure the devices so that the ifIndex value is fixed (persistent).
- NFA provides the mechanism to group multiple physical network interfaces on NFA and collect flow information so as to manage devices that cannot be configured to send flow information directly from the network interfaces logically combined in a Link Aggregation Group (LAG). Since NFA manages the ifIndex value for grouped network interfaces, it is not possible to determine whether the network interfaces are the same if Network Manager obtains the ifIndex value of the LAG interface. In this case, manually register the network interfaces as the same by using this function.

5.1.2.1 Network Interface Mappings page

The Network Interface Mappings page is described below.

The Network Interface Mappings page is available to check the result of determining whether the network interfaces are the same after determination of whether the nodes managed by multiple products are the same, and modify the configuration, if necessary.

The Network Interface Mappings page is displayed by clicking the **Network interface mappings** icon for each node displayed on the Node Mappings page. Click **System Settings**>**Node Mappings** to display the Node Mappings page.

Tip

Only users with the Administrator authority can display the Network Interface Mappings page.

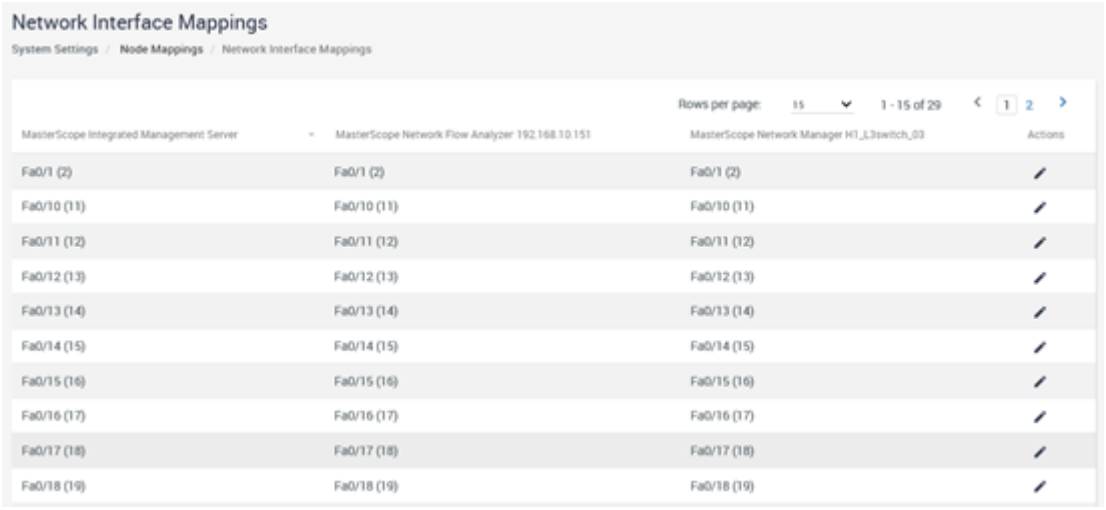

Figure 5-3 Network Interface Mappings Page

Network interface mapping list

- **MasterScope Integrated Management Server**

  Displays the network interface name of IMS.

- ***<Product name><Node name>***

  Displays the network interface name of each product. The column header consists of the product name and the node name in that product.

- **Actions**

  Click the following icon to display the operation page for network interface mapping information.

  - **Edit** icon

    Click this icon to modify the result of determining whether the nodes are the same.

    Clicking the **Edit** icon displays the Edit Network Interface Mapping page. For details, refer to "5.1.2.2 Changing the network interface mapping (page 117)".

Select the number of network interface information items to be displayed on one page from the pull-down menu (**15**, **50**, or **100**). The default is **15**.

If all the network interface mapping information matching the search conditions cannot be displayed on one page, check the subsequent pages.

5.1.2.2 Changing the network interface mapping

The following describes how to modify the result of determining whether the network interfaces are the same as the network interface information displayed on Web Console.

If the result of determining whether the network interfaces are the same is invalid, be sure to correct the result manually.

The specific procedure is described below using an example to show how to register information of network interfaces grouped in NFA and the network interface managed as a Link Aggregation Group (LAG) interface on Network Manager as the same network interface.

1. Display the Node Mappings page.

Click **System Settings**>**Node Mappings**.

2. Search for the node containing the network interface to be updated.
   a. Select **Region** from the pull-down menu.
   b. Select **is** as the collation method.
   c. Enter the name of the region group to which the node to be updated belongs.
   d. Select **Node Name** from the pull-down menu.
   e. Select **is** as the collation method.
   f. Enter the name of the node to be updated.
   g. Click the **SEARCH** button.

   The search result is displayed in the node mapping list.

3. Click the **Network interface mappings** icon corresponding to the name of the node containing the network interface to be updated.

   The Network Interface Mappings page for the relevant node is displayed.

4. Display the Edit Mapping of Network Interface page for the network interface to be updated.

   Click the **Edit** icon of the network interfaced grouped on NFA or the **Edit** icon of the network interface managed as a Link Aggregation Group (LAG) interface on Network Manager.

   Here, click the **Edit** icon of the network interfaced grouped on NFA.

   The Edit Mapping of Network Interface page for the network interfaced grouped on NFA is displayed.

5. Update the mapping information of the network interface.

   Click the following buttons corresponding to the network interface information of each product to update the mapping information.

   - **Edit** icon

     Click this icon to display the Select Mapping Network Interface screen. In the Select Mapping Network Interface screen, information of the network interfaces that match the specified search condition is displayed in the network interface list. On the Select Mapping Network Interface screen, select the changed network interface and click the **OK** button. Then, information of the selected node is reflected in the Edit Mapping of Network Interface page.

   - **Delete** icon

     Click this icon to unmap the network interface.

   Here, click the **Edit** icon corresponding to the network interface information managed by Network Manager. On the displayed Select Mapping Network Interface screen, select the network interface managed as the corresponding Link Aggregation Group (LAG) interface.

   The network interfaces grouped in NFA and the network interface managed as a Link Aggregation Group (LAG) interface on Network Manager are set as the same network interface on the Edit Mapping of Network Interface page.

6. Register the changes of the network interface mapping.

Confirm the changes and then click the **OK** button on the Edit Mapping of Network Interface page.

The updates are reflected in the Network Interface Mappings page.

5.2 Maintaining the system environment

This section describes how to maintain the system environment.

5.2.1 Checking the versions of the related components

The following describes how to check the versions of the IMS component and integrated plug-in modules of each product.

When asking NEC Customer Support Center about the operations of Web Console, or when applying the update module obtained from NEC Customer Support Center to the operations, it is necessary to know the correct versions of the IMS component in use and integrated plug-in modules of the related products.

The version of the IMS component can be checked from Web Console or by using a command. The versions of integrated plug-in modules can be checked by using a command.

- Checking the version of the IMS component from Web Console.
  1. Access Web Console.
  2. Check the version displayed in the footer area at the bottom of each page.

     The display format is as follows:

     MasterScope Integrated Management Server <version>.<revision>.<release>
- Checking the versions of the IMS and applications by using a command.
  1. Log in to the server where the IMS component is installed.
  2. For a Windows environment, start the command prompt.
  3. Move to the current directory.

     ```
     > cd <%INSTPATH%>/bin
     ```
  4. Run the command to check the version.

     ```
     > ims-app list
     ```
  5. Check the version in the displayed result.

     The display format is as follows:

     ```
     MasterScope Integrated Management Server version 1.0.1.15

       ID  | Application Name                  | Version
       ----------------------------------------------
       nvp | MasterScope Network Manager       | 1.0.1.15
       nfa | MasterScope Network Flow Analyzer | 1.0.1.15
     ```

5.2.2 Starting and stopping the services

The following describes how to manually start or stop the IMS component services.

The IMS component service starts or stops automatically along with the start or stop of the OS.

When maintaining the IMS component, only the IMS component services need to be stopped or restarted while the OS is running according to the following procedure.

For a Windows environment

Control the services by using **Administrative Tools** of Windows OS.

1. Open the Control Panel and then select **Administrative Tools**.
2. Select **Services** on the Administrative Tools page.
3. Execute the following steps.
   - Before starting the services, check that all the services have stopped. Then, select the following services in this order from the service list in the Services page, and execute **Start**.
     a. MasterScope IMS System Database
     b. MasterScope IMS Key Store
     c. MasterScope IMS Message Queue
     d. MasterScope IMS Event Manager
     e. MasterScope IMS Web Server
   - When stopping the services, select the following services in this order from the list in the Services page, and execute **Stop**.
     a. MasterScope IMS Web Server
     b. MasterScope IMS Event Manager
     c. MasterScope IMS Message Queue
     d. MasterScope IMS Key Store
     e. MasterScope IMS System Database

For a Linux environment

Control the services by using the following command provided by the IMS component.

- For Red Hat Enterprise Linux 6

  `/etc/init.d/`nec-ims {start | stop}
- For Red Hat Enterprise Linux 7

  systemctl {start | stop} nec-ims

Tip

To use this command, log in to the server where the IMS component is installed as the root user.

- Run this command with the `start` argument to start the services.

  If all daemon processes of IMS started successfully, the command returns 0 as the return value.
  - For Red Hat Enterprise Linux 6

```
# /etc/init.d/nec-ims start
```

```
Starting systemdb:                [  OK  ]
Starting key store:               [  OK  ]
Starting message queue:           [  OK  ]
Starting event manager:           [  OK  ]
Starting web server:              [  OK  ]
```

- For Red Hat Enterprise Linux 7

```
# systemctl start nec-ims

Starting nec-ims (via systemctl):  [  OK  ]
```

- Run this command with the `stop` argument to stop the services.

  If all daemon processes of IMS stopped successfully, the command returns 0 as the return value.

  - For Red Hat Enterprise Linux 6

```
# /etc/init.d/nec-ims stop

Stopping web server:              [  OK  ]
Stopping event manager:           [  OK  ]
Stopping message queue:           [  OK  ]
Stopping key store:               [  OK  ]
Stopping systemdb:                [  OK  ]
```

  - For Red Hat Enterprise Linux 7

```
# systemctl stop nec-ims

Stopping nec-ims (via systemctl):  [  OK  ]
```

- Run the `ims-ctl` command with the `status` argument to check the service status.

```
# <%INSTPATH%>/bin/ims-ctl status
```

  When the services have started, the following messages are displayed. The command returns 0 as the return value.

```
systemdb (pid 12341) is running...
key store (pid 12342) is running...
message queue (pid 12343) is running...
event manager (pid 12344) is running...
web server (pid 12345) is running...
```

  When the services have stopped, the following messages are displayed. The command returns 3 as the return value.

```
systemdb is stopped
key store is stopped
message queue is stopped
event manager is stopped
web server is stopped
```

5.2.3 Changing the communication port numbers to be used

The following describes how to change the port numbers used by the IMS component.

For the port numbers that the IMS component uses, refer to "B.1 Port number list (page 138)".

Tip

The following procedure must be performed by a user with OS administrator privileges.

Change the port numbers used by the IMS component according to the procedure below.

1. Log in to the server where the IMS component is installed.
2. Stop the IMS component services.
3. Change and save the content of the configuration file.

   Refer to "Table 5-1 Communication Port Numbers (page 122)" for the specification format of each communication protocol

Table 5-1 Communication Port Numbers

Communication type	Specification format

HTTP communication	• Configuration file
	`<%DATAPATH%>\conf\ims-conf.ini`
	`<%DATAPATH%>` /conf/ims-conf.ini
	• Specification format
	`noms.tomcat.http.port = <Port number>`
	By setting the following property in the configuration file to *"true"* , the above setting becomes to enable.
	If *"false"*, the port is nor opened.
	`noms.tomcat.http.enabled = true`

HTTPS communication	• Configuration file
	`<%DATAPATH%>\conf\ims-conf.ini`
	• Specification format
	`noms.tomcat.https.port = <Port number>`
	By setting the following property in the configuration file to *"true"* , the above setting becomes to enable.
	If *"false"*, the port is nor opened.
	`noms.tomcat.https.enabled = true`

Message Queue communication	• Configuration file
	`<%DATAPATH%>\conf\ims-conf.ini`
	• Specification format
	By adding the following property in the configuration file, a port number can be set.
	`amqphub.amqp10jms.remote-url = amqps://localhost:<Port number>?transport.trustAll=true`
	On the Products connected to the IMScompornent , it is needed to change the setting according to the above changed port number.
	In the case of Network Manager
	• Configuration file
	`Network Manager<%DATAPATH%>\Manager\sg\NvPRO\NvPROIms.ini`
	• Specification format

Communication type	Specification format
	[NOMS] MessageQueuePort=<*Port number*> You have to restart the services when you have changed the configuration file. In the case of NFA • Configuraion file NFA<*%DATAPATH%*>/controller/conf/controller.properties • Specification format ims.msgqueue.port = <*Port number*> You have to restart the services when you have changed the configuration file.
System Database communication	• Configuration file <*%DATAPATH%*>\conf\ims-conf.ini • Specification format By adding the following property in the configuration file, a port number can be set. noms.tomcat.jndi.port = <*Port number*> Also update the following setting file according to the above setting. • Configuration file <*%DATAPATH%*>\conf\systemdb-extra.conf • Specification format port = <*Port number*>
Key Store communication	• Configuration file <*%DATAPATH%*>\conf\ims-conf.ini • Specification format By adding the following property in the configuration file, a port number can be set. spring.redis.port = <*Port number*> Also update the following setting file according to the above setting. • Configuration file <*%DATAPATH%*>\conf\redis-extra.conf • Specification format port = <*Port number*>

⚠ Caution

If a port is described and set up in multiple configuration files, edit all the configuration files at the same time and specify the same port number. If the port numbers are different between the related configuration files, communication cannot be performed properly.

4. Review the firewall setting if necessary.

Especially, the port numbers for external communication are often blocked by a firewall. Therefore, when changing the port numbers, check whether the firewall setting is appropriate.

5. Start the IMS component services.

   After the services start, the changed port numbers are reflected in the IMS component.

5.2.4 Changing the domain name (FQDN)

This section describes the procedures required when changing the domain name (FQDN) of the server where the IMS component is installed.

5.2.4.1 Changing the URL for notification

You need to update the URL setting for notification when changing the domain name (FQDN) of the server where the IMS component is installed.

In notification of event actions, the Event Detail page URL relevant to the event can be embedded in the e-mail body, etc. The embedded URL is based on the URL specified in the configuration file (ims-conf.ini). Thefore, you need to update the contents of the configuration file (ims-conf.ini) when changing the domain name (FQDN) of the server where the IMS component is installed.

Tip

The following procedure must be performed by a user with OS administrator privileges.

1. Log in to the server where the IMS component is installed.
2. Stop the IMS component services.
3. Edit the configuration file and save it.
   - Configuration file

     `<%DATAPATH%>\conf\ims-conf.ini`
   - Format

     ```
     noms.core.url.external-base-url = <URL>
     ```

     Example:

     ```
     noms.core.url.external-base-url = http://ims.nec.com:8080/
     ```
4. Restart the IMS component services.

   After the restarting the services, the updated URL is reflected in the IMS component.

5.2.4.2 Changing the domain name in the SSL server certificate

If you are accessing the Web Console using HTTPS, you need to update the SSL server certificate when changing the domain name (FQDN) of the server where the IMS component is installed.

Since the SSL server certificate contains the domain name, you need to update it according to the domain name (FQDN) of the server where the IMS component is installed.

Tip

When HTTP is used to access Web Console, the following procedure is unnecessary.

Use the `ims-ssl-keytool` command provided by the product for operations related to the SSL server certificate. For details, refer to "A.1 ims-ssl-keytool (page 132)".

Tip

The following procedure must be performed by a user with OS administrator privileges.

1. Log in to the server where the IMS component is installed.
2. Run the following command to check the Owner information in the output message.

   ```
   > <%INSTPATH%>/bin/ims-ssl-keytool list -v
   ```

   Execution example for Windows:

   ```
   > cd C:\Program Files\NEC\IMS/bin
   > ims-ssl-keytool list -v | findstr Owner
   Owner: CN=ims.nec.com, OU=IT Operation Division, O=NEC Corporation,
    L=Minato-ku, ST=Tokyo, C=JP
   ```

3. Run the `ims-ssl-keytool selfcert` command with the `-dname` option to update the identification name.

   ```
   > <%INSTPATH%>/bin/ims-ssl-keytool selfcert -dname <dname>
   ```

   Change the CN value indicating the domain name in the checked Owner information and run the command.

   Execution example for Windows:

   ```
   > ims-ssl-keytool selfcert -dname "CN=new-ims.nec.com,
    OU=IT Operation Division, O=NEC Corporation, L=Minato-ku,
    ST=Tokyo, C=JP"
   ```

4. If the certificate was issued by a public certificate authority, ask the certificate authority to issue the certificate again.

   a. Run the following command to output a certificate signing request (CSR) to send to a certificate authority to a file.

      ```
      > <%INSTPATH%>/bin/ims-ssl-keytool certreq -dns <FQDN> <filename>
      ```

      The contents of CSR are output in the specified file in text format.

   b. Submit a certificate signing request (CSR) to a certificate authority.

      Submit the CSR file output by using the `ims-ssl-keytool certreq` command to a certificate authority.

      The certificate authority signs a certificate according to the contents of the CSR file and returns the signed certificate to the requester. Some certificate authorities may take several days to return the signed certificate.

   c. Import the signed certificated issued by the certificate authority.

      Run the `ims-ssl-keytool importcert` command without the `-alias` option.

      ```
      > <%INSTPATH%>/bin/ims-ssl-keytool importcert <filename>
      ```

      If the message `Failed to establish chain from reply` is displayed during execution of the above command, the certificate chain could not be resolved. The root certificate of the certificate authority or the intermediate certificate may not be imported. For the certificates to be imported, ask the relevant certificate authority.

5. Restart the IMS component services.
6. In the case of a self-signed certificate, run the `ims-ssl-keytool exportcert` command to output the certificate to import into web browsers to a file.

```
> <%INSTPATH%>/bin/ims-ssl-keytool exportcert <filename>
```

Distribute and import the certificate file output by using the `ims-ssl-keytool exportcert` command into all web browsers that you will use to access Web Console. Importing a certificate into a web browser prevents problems such as a phishing attack pretending to be the web browser that can be used to access the IMS component.

For how to import the certificate to a web browser, refer to "1.2.1.2 Importing the SSL server certificate into the web browser (page 9)".

5.2.4.3 Changing single sign-on settings

You need to change single sign-on settings on the product side when changing the domain name (FQDN) of the server where the IMS component is installed.

The Web console of NFA can be launched from the Web Console of IMS component with single sign-on. Before launching Web consoles with single sign-on, it is necessary to register the Web Console URL of the IMS component on the product side. For this reason, you need to update the single sign-on settings on the product side when changing the domain name (FQDN) of the server where the IMS component is installed.

The following explains the procedure for changing in the NFA as an example.

Tip

The following procedure must be performed by a user with OS administrator privileges.

1. Log in to the server where the NFA component is installed.
2. Stop the NFA services.
3. Edit the configuration file (controller.properties) and save it.
   - Configuration file

     On NFA, `<%DATAPATH%>/controller/conf/controller.properties`
   - Format

     ```
     ims.webserver.base-url = <ims web url>
     ```

     Example:

     ```
     ims.webserver.base-url = http://chg-ims.nec.com/
     ```
4. Restart the NFA services.

   After the restarting the services, the updated URL is reflected in the NFA.

5.2.5 Changing the IP address

This section describes how to change the IP address of the server where the IMS component is installed.

Before changing the IP address of the server where the IMS component is installed, be sure to stop all services of the IMS component.

Also, when changing the IP address of the server where the IMS component is installed, it is necessary to change the setting on each product side that is connected the IMS component.

The following explains how to change the settings of the Network Manager and NFA that are connected to the IMS component.

Tip

The following procedure must be performed by a user with OS administrator privileges.

1. Log in to the server where the IMS component is installed.
2. Stop the services of the connected product.
3. Edit the configuration file and save it.
   - For Network Manager
     - Configuration file

       `On Network Manager, <%DATAPATH%>\Manager\sg\NvPRO\NvPROIms.ini`

     - Format

       ```
       [NOMS]
       MessageQueueIP=<IP address>
       ```

   - For NFA
     - Configuration file

       `On NFA, <%DATAPATH%>/controller/conf/controller.properties`

     - Format

       ```
       ims.msgqueue.host = <ims ip address>
       ```

4. Restart the service of the connected product.

   After the restarting the services, the updated IP address is reflected.

5.2.6 Synchronizing the configuration information

The configuration information may become inconsistent between the IMS component and products.

For example, the following cases cause configuration inconsistency.

- When the IMS component services have stopped, the properties of the managed node are changed on Network Manager, or a new exporter is added on NFA.
- Old backups are restored in the IMS component.

In these cases, synchronize the configuration with the product instance with a different configuration from the Configuration Sync page.

5.2.6.1 Configuration Sync page

The Configuration Sync page is described below.

The Configuration Sync page allows users to synchronize the configuration information of this product with the specified product instance.

Click **System Settings**>**Configuration Sync** to display the Configuration Sync page.

Tip

Only users with the Administrator authority can display the Configuration Sync page.

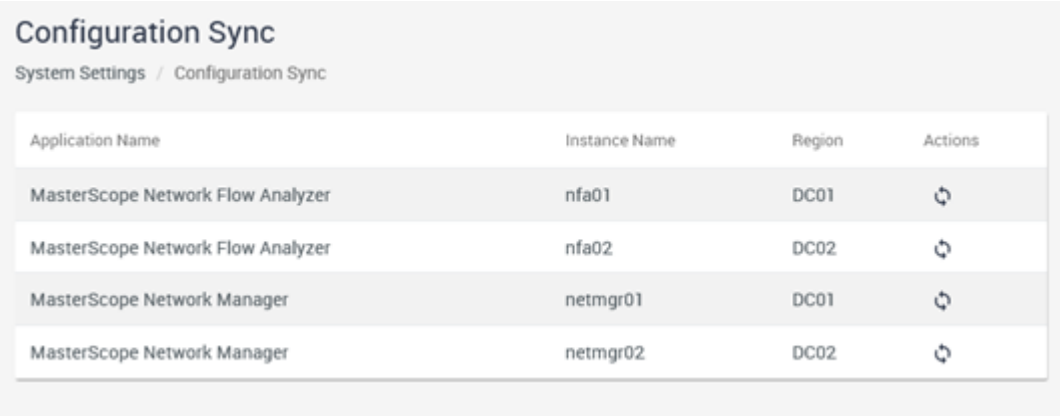

Figure 5-4 Configuration Sync Page

Product instance list

- **Application Name**

  Displays the product name that connects to the IMS component.

- **Instance Name**

  Displays the name of the product instance that connects to the IMS component.

- **Region**

  Displays the name of the region group to which the product instance belongs.

- **Actions**

  Click the icon to operate the product instance.

  - **Synchronize this instance** icon

    Click this icon to obtain the configuration information of the product and register the obtained information to the IMS component again. This eliminates the configuration inconsistency.

5.2.6.2 Eliminating the configuration inconsistency

The following describes how to eliminate the configuration inconsistency between the IMS component and the products caused by maintenance and other tasks.

If the configuration of each product is operated while the IMS component services are stopped, inconsistency may occur in the configuration information managed by them, causing problems in operation. In this case, eliminate the inconsistency by synchronizing their configuration information and obtaining the configuration information of each product from the IMS component again.

The specific procedure is described below using an example showing how the configuration of product instance *"NetMgr01"* of Network Manager belonging to region group *"Head Office"* was changed while the IMS component services were stopped,

1. Display the Configuration Sync page.

   Click **System Settings**>**Configuration Sync**.

2. Synchronize the inconsistent configuration with the managed product instance.

   Select the relevant product instance from the product instance list and click the **Synchronize this instance** icon.

   Here, click the **Synchronize this instance** icon of product instance *"NetMgr01"* of Network Manager belonging to region group *"Head Office"* whose configuration was changed.

   Caution

   When displaying the Configuration Sync page, the **Synchronize this instance** icon can be clicked again even if the synchronization is not complete. However, do not perform another synchronization of information in parallel because the synchronization places burden on the products from where configuration information is obtained.

3. Check the completion report of the synchronization.

   The result of the synchronization is reported as an event. Search for the event indicating the completion of the synchronization from the new arrival event report or the Events page, and check the contents of the event.

4. Check that the configuration information has been synchronized properly.

   By referring to the information displayed on the Nodes page, the **Properties** widget of the Node Detail page, or the Topology Map page, check that the updated configuration information has been reflected in the IMS component and can be referenced on Web Console.

5.3 Backing up and restoring the operation environment

This section describes how to back up and restore the environment settings and accumulated data of the IMS component.

In the IMS component, the environment settings and all the accumulated data are subject to backup and restoration.

The backup operation can be performed either while the IMS component services are running or stopped. When restoring from backup data, the services should be stopped.

5.3.1 Backing up all data

The following describes how to back up both the environment settings and accumulated data.

The backup operation can be performed either while the IMS component services are running or stopped.

Caution

- The size of backup data may be about the same as the disk consumption of <*%DATAPATH%*>. Therefore, ensure a sufficient free disk space in the destination to which the backup data will be output.
- The backup processing may take several minutes to complete depending on the backup data size.

Tip

The following procedure must be performed by a user with OS administrator privileges.

1. Log in to the server where the IMS component is installed.

2. Check the current size of the data to be backed up.

   - For a Windows environment

     Display and check the Properties dialog boxes of the following two folders. Sum the values displayed for **Size**.

     - <*%DATAPATH%*>\conf
     - <*%DATAPATH%*>\db

   - For a Linux environment

     Run the following command to check the size.

     ```
     # du -sm <%DATAPATH%>/{conf,db}
     ```

     Individual directory sizes are displayed in units of MB. Sum the displayed values.

3. For a Windows environment, start the command prompt.

   You need to start the command prompt in the **Run as Administrator** menu.

4. Run the backup command.

   ```
   > <%INSTPATH%>/bin/ims-backup <path>
   ```

   For the <*path*> argument, specify the directory in which to output the backup. Before specifying a directory, ensure that the directory has a free space enough for saving the data to be backed up.

   For details on the `ims-backup` command, refer to "A.2 ims-backup (page 135)".

   When this command ends normally with no error message displayed, a backup file is created in the specified output directory.

5.3.2 Restoring the backup of all data

The following describes how to restore the backup of both the environment settings and accumulated data.

When restoring the backup, be sure to stop the IMS component services.

Before starting the restoration, place the backup directory generated in "5.3.1 Backing up all data (page 129)" in the server where the IMS component is installed.

⚠ Caution

Restoration may take several hours to complete depending on the backup size.

Tip

The following procedure must be performed by a user with OS administrator privileges.

1. Log in to the server where the IMS component is installed.
2. Stop the IMS component services.
3. For a Windows environment, start the command prompt.

   You need to start the command prompt in the **Run as Administrator** menu.

4. Restore the backup of the IMS component.

   Run the following restore command.

```
> <%INSTPATH%>/bin/ims-restore -full <path>
```

For the <*path*> argument, specify the directory in which the backup is stored.

For details on the `ims-restore` command, refer to "A.3 ims-restore (page 135)".

When this command ends normally with no error message displayed, the restoration is complete.

5. Update the SSL server certificate as necessary.

   This step should be performed when using HTTPS and the domain name (URL to access the web server) of the environment where the data is backed up differs from that of the environment to which the data is restored.

   For the procedure, refer to "5.2.4.2 Changing the domain name in the SSL server certificate (page 124)".

6. Start the IMS component services.

If a configuration inconsistency occurs between the IMS component and the connected products after the restoration, synchronize the configuration. For details, refer to "5.2.6 Synchronizing the configuration information (page 127)".

Appendix A. Command Reference

The following describes the commands that are provided by IMS.

A.1 ims-ssl-keytool

This command creates and manages an SSL server certificate to be used in HTTPS communication.

This command is a wrapper command that provides the functions of the Java keytool command in an easy-to-use format for this product. Note that this command can use only some functions of the Java keytool command. The names and meanings of the argument of this command are the same as those of the Java keytool command.

For details on the Java keytool command, refer to the following URL.

- http://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html *1

The differences from the Java keytool command are as follows:

- A subcommand name such as `genkeypair` is specified for the first argument. `-` is not attached at the beginning of the argument name of the subcommand.
- For this command, the keystore path is fixed to *<%DATAPATH%>*`\conf\server.keystore`.
- By running the `genkeypair` subcommand, the password of the keystore and aliases of entries in the keystore are saved in the following file.

  <%DATAPATH%>`\conf\ims-conf.ini`

  Information saved in the above file are used automatically when the `-storepass` and `-alias` options are omitted when running each subcommand. This enables to run this command by specifying minimal options.
- The default values of the `-keyalg` and `-validity` options are different from those of the Java keytool command.
- This command implements its own subcommand, `initstore`.

Caution

This command requires OS administrator privileges.

Path

<%INSTPATH%>`\bin\ims-ssl-keytool`

Syntax

```
ims-ssl-keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
ims-ssl-keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-sigalg SIGALG] [-validity DAYS] [-dname DNAME]
```

*1 This URL is current as of January 2019.

```
ims-ssl-keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
    [-dns DNS] FILE

ims-ssl-keytool importcert [-help] [-storepass PASS] [-alias ALIAS]
    FILE

ims-ssl-keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE

ims-ssl-keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]

ims-ssl-keytool delete [-help] [-storepass PASS] [-alias ALIAS]

ims-ssl-keytool initstore [-help]

ims-ssl-keytool -help
```

Description

The subcommands are described below.

- `genkeypair`

  Creates and stores a pair of keys (public key and associated private key) in the keystore. In addition, this subcommand writes Information to use keys generated by a web server to the following files.

  <%DATAPATH%>`\conf\ims-conf.properties`

  Caution

  The value of noms.tomcat.https.enabled in the ims-conf.ini is updated to *"true"* by this command.

- `selfcert`

  Creates a self-signed certificate for the key of the keystore entry.

- `certreq`

  Generates a certificate signing request (CSR) in the PKCS#10 format.

- `importcert`

  Reads a certificate or certificate chain from a file and stores it to the keystore.

- `exportcert`

  Reads a certificate from the keystore and stores it in a file in binary encoding format.

- `list`

  Displays the contents of a certain keystore entry or of the entire keystore.

- `delete`

  Deletes a certain entry from the keystore.

- `initstore`

  Deletes the keystore file.

Arguments

-storepass *PASS*

Specify the password of the keystore.

If this argument is omitted when running the `genkeypair` subcommand, you will be prompted to enter your password while the subcommand is running. If this argument is omitted when running other subcommands, the value read from the ims-conf.properties file is used.

-alias *ALIAS*

Specify an alias for the entry in the keystore.

If this argument is omitted when running the `genkeypair` subcommand, the default value *"tomcat"* is used. If this argument is omitted when running the `list` subcommand, an alias is specified for all entries. If this argument is omitted when running other subcommands, the value read from the ims-conf.properties file is used.

-keyalg *KEYALG*

Specify the encryption algorithm for the key. For example, *"RSA"*, *"DSA"*, and *"EC"* can be specified. The default is *"RSA"*.

For the algorithms that can be specified for `-keyalg` and `-sigalg`, refer to Java Cryptography Architecture Specification and Reference. *2

-keysize *KEYSIZE*

Specify the size of the key to be generated.

The setting range and default value comply with the Java keytool specifications.

-sigalg *SIGALG*

Specify the algorithm to be used to sign a self-signed certificate.

Be sure to specify the algorithm that is compatible with `-keyalg`. The setting range and default value comply with the Java keytool specifications.

-validity *DAYS*

Specify the valid period of a self-signed certificate in days. Values from 0 to 365000 can be specified. The default is 3650 (Approx. 10 years).

-dname *DNAME*

Specify the X.500 identification name to be used as the issuer and subject fields of a self-signed certificate.

If the identification name is not specified, you will be prompted to enter the identification name while the command is running.

-dns *DNS*

Specifies the FQDN for Subject Alternative Name (SAN) extension.

In `genkeypair` subcommand, if this argument is omitted, Common Name of a certificate is used as SAN.

-rfc

This option is used to specify the output format of the `list` subcommand. The contents of a certificate will be output in the specified encoding format.

This option cannot be specified together with the `-v` option.

-v

*2 This URL is current as of October 2018.

This option is used to specify the output format of the `list` subcommand. The detailed contents of a certificate will be output in the human readable format.

This option cannot be specified together with the `-rfc` option.

-help

Displays the usage of all or each of the commands.

Return values

Upon success, 0 is returned. In case of failure, a value other than 0 is returned.

A.2 ims-backup

This command backs up the environment settings and accumulated data of the IMS component.

This command is run to back up the environment settings of the IMS component.

⚠ Caution

- This command requires OS administrator privileges.
- This command may take several minutes to complete depending on the size of backup target.

Path

<%INSTPATH%>\bin\ims-backup

Syntax

```
ims-backup PATH
```

```
ims-backup -help
```

Description

When this command ends normally with no error message displayed, a backup file is created in the specified output directory.

Arguments

PATH

Specify the directory in which to output a backup file.

-help

Displays the usage of the command.

Return values

Upon success, 0 is returned. In case of failure, a value other than 0 is returned.

A.3 ims-restore

This command restores the backup of the environment settings and accumulated data of the IMS component.

This command is run to restore the backup of the environment settings of the IMS component.

⚠ Caution

- This command requires OS administrator privileges.
- Before running this command, be sure to stop the IMS component services.
- This command may take several minutes to complete depending on the backup size.

Path

`<%INSTPATH%>\bin\ims-restore`

Syntax

```
ims-restore PATH
```

```
ims-restore -help
```

Description

When this command ends normally with no error message displayed, restoration of the backup is complete.

Arguments

PATH

Specify the directory in which the backup is stored.

-help

Displays the usage of the command.

Return values

Upon success, 0 is returned. In case of failure, a value other than 0 is returned.

A.4 ims-app

This command manages the applications incorporated in the IMS component

This command is used to perform the following three tasks.

- Conforms versions of the IMS component and incorporated applications.
- Installs applications into the IMS component.
- Uninstalls applications incorporated in the IMS component.

⚠ Caution

- This command requires OS administrator privileges.
- Before installing or uninstalling applications, you need to stop the services of the IMS component.

Path

`<%INSTPATH%>\bin\ims-app`

Syntax

```
ims-app list
```

```
ims-app install [-help] [-silent] [-overwrite] [-ignore-dependencies]
        WAR_FILE
```

```
ims-app uninstall [-help] [-silent] ID
```

```
ims-app -help
```

Description

The subcommands are described below.

- `list`

  Displays the IMS version, and applications that are incorporated in the IMS component.

- `install`

  Installs the application file (WAR file) specified as *WAR_FILE* and enables it on the IMS component.

- `uninstall`

  Uninstalls the application the IMS component by specifying the application *ID*.

Arguments

-silent

Specify it to run the command in non-interactive mode (silent mode).

-overwrite

It is enabled in the `install` subcommands with non-interactive mode.

Overwrites the application without confirmation even if the application is already installed.

-ignore-dependencies

It is enabled in the `install` subcommands

Ignores dependencies between applications and performs installation.

-help

Displays the usage of all or each of the commands.

Return values

Upon success, 0 is returned. In case of failure, a value other than 0 is returned.

Appendix B. System Resources to Use

The following describes the system resources used by IMS.

B.1 Port number list

This section describes the default port numbers that the IMS component uses.

The port numbers that the IMS component uses for external communication and internal communication are described in "Table B-1 Communication Port Number List (for External Communication) (page 138)" and "Table B-2 Communication Port Number List (for Internal Communication) (page 138)".

Table B-1 Communication Port Number List (for External Communication)

Name	Port number	Protocol	Direction	Application
HTTP communication port	80	TCP	IN	Port for HTTP communication
HTTPS communication port	443	TCP	IN	Port for HTTPS communication
Message Queue communication port	28110	TCP	IN	Port for message send and receive communication

Table B-2 Communication Port Number List (for Internal Communication)

Name	Port number	Protocol	Direction	Application
System Database communication port	28120	TCP	IN	Port for communication with a system database
Key Store communication port	28130	TCP	IN	Port for communication with a key store

You can change these port numbers. For how to change the port number, refer to "5.2.3 Changing the communication port numbers to be used (page 121)".

Glossary

A - Z

A

AS

AS stands for autonomous system. This is an RFC 1930 compliant autonomous network that is owned and operated by an organization within a large-scale TCP/IP network, such as the Internet.

An AS number is used to identify this autonomous network. AS numbers are managed by the Network Information Center (NIC) of each country.

C

Conversation

For Web Console and NFA, this means a mutual communication between two specific points.

D

DNS

DNS stands for domain name system. This is a system that manages the mapping between host names or domain names on a network and IP addresses.

DSCP

DSCP stands for Differentiated Services Code Point. This is a method to prioritize packets. DSCP uses 6 bits of the ToS field (8 bits) in the IP header. This makes it possible to prioritize in 64 levels.

E

Endpoint

This is a generic name for network terminals such as personal computers that connect to a network and perform various types of communication.

Exporter

For NFA, this is a generic name for devices such as switches and routers, and software, that can send packets in a flow (sFlow, NetFlow, IPFIX).

F

Flow

This indicates a communication flow between endpoints, or information (sFlow, NetFlow, IPFIX) generated by monitoring this communication flow by an exporter.

FQDN

FQDN stands for fully qualified domain name. This is a full domain name that includes the domain name, subdomain names, and host name.

I

IANA

IANA stands for Internet Assigned Numbers Authority. This is an organization that manages various numbers related to the Internet, such as IP addresses, protocol numbers, port numbers.

ifIndex

This is one of the most frequently used identifiers in SNMP network management and indicates a unique identification number that is associated with a physical or logical interface.

ifName

This is the name of the MIB object to which the name of the physical or logical interface of a device is recorded.

IP protocol

For Web Console and NFA, this refers to the protocol that is indicated by the protocol number (IP Protocol Number) in the IP header. In particular, this is a generic name for TCP, UDP, and ICMP.

IPFIX

IPFIX stands for IP Flow Information Export. This is a technology used to monitor the network communication status. This is an expanded IETF standard technology based on NetFlow version 9.

L

LAG

LAG means link aggregation groups. This technology treats multiple physical interfaces as one interface by virtually bundling them. LAG is defined by IEEE P802.3ad.

M

MIB

MIB stands for management information base. This is management information that is issued externally by a network device that can be managed by SNMP to report its own state. The MIB information can be referenced externally by specifying the target object name by using SNMP.

N

NetFlow

This technology has been developed by Cisco Systems, Inc. in the United States to monitor the communication status of a network. The specifications of version 9 have been published as RFC3954.

NetFlow targets only IP-based communication information, and offers two communication packet monitoring methods: full mode and sampling mode.

P

PHB

PHB stands for Per Hop Behavior. This indicates the packet forwarding behavior corresponding to the DSCP value.

Port number

This is a number to identify the communication destination program in TCP/IP communication.

S

sFlow

This technology was developed by InMon Corp. in the United States to monitor the communication status of a network. The specifications of version 4 were published as RFC3176.

sFlow offers a mechanism to sample communication packets in a specific ratio and calculate the total communication traffic by analyzing the sampled information statistically.

SNMP

This stands for Simple Network Management Protocol. This is a protocol for network management, and is defined by RFC1157.

SNMP enables network devices connected to a TCP/IP network to be monitored and managed via the network.

SNMP Trap

This is a mechanism provided by SNMP to enable an agent to report its own status by way of an unsolicited message.

sysDescr

This is the name of the MIB object in which a description about the device is recorded.

sysName

This is the name of the MIB object in which a device host name is recorded. The sysName value can be set in the device configuration.

sysObjectId

This indicates a unique identification number associated with the device model, or the name of the MIB object that records it.

T

ToS

ToS stands for Type of Service. It is one of the fields in IP header and is used to tell each packet forwarding device how to forward the packet.

W

Widget

This is a component of the Dashboard and Node Detail page. Graphs and lists are displayed as widgets.

MasterScope Network Management
Web Console
Reference Manual

IMS00ME0100-01

January, 2019 01 Edition

NEC Corporation