HITACHI
Inspire the Next

JP1 Version 12

Network Management: Getting Started

3021-3-E01-30(E)

Notices

■ Relevant program products

JP1/Network Node Manager i (for Windows)
P-2942-82CL JP1/Network Node Manager i 12-60
P-2942-89CL JP1/Network Node Manager i Developer's Toolkit 12-00

JP1/SNMP System Observer (for Windows)
P-2942-8RCL JP1/SNMP System Observer 12-00

JP1/SNMP System Observer - Agent for Process (for Windows)
P-2A42-8JCL JP1/SNMP System Observer - Agent for Process 12-00

JP1/Network Element Manager (for Windows)
P-2942-8CC4 JP1/Network Element Manager for Cisco 12-00
P-2942-8DC4 JP1/Network Element Manager for AX Series 12-00

JP1/Extensible SNMP Agent for Windows (for Windows)
P-2A42-8BCL JP1/Extensible SNMP Agent for Windows 12-00

JP1/Network Node Manager i (for Linux)
P-8242-82CL JP1/Network Node Manager i 12-60
P-8242-89CL JP1/Network Node Manager i Developer's Toolkit 12-00

JP1/SNMP System Observer (for Linux)
P-8242-8RCL JP1/SNMP System Observer 12-00

JP1/SNMP System Observer - Agent for Process (for Linux)
P-8142-8JCL JP1/SNMP System Observer - Agent for Process 12-00

JP1/Extensible SNMP Agent (for Linux)
P-8142-8ACL JP1/Extensible SNMP Agent 12-00

JP1/SNMP System Observer - Agent for Process (for UNIX)
P-1M42-8JCL JP1/SNMP System Observer - Agent for Process 12-00 (for AIX)
P-1J42-8JCL JP1/SNMP System Observer - Agent for Process 12-00 (for HP-UX (IPF))
P-9D42-8JCL JP1/SNMP System Observer - Agent for Process 12-00 (for Solaris)

JP1/Extensible SNMP Agent (for UNIX)
P-1M42-8ACL JP1/Extensible SNMP Agent 12-00 (for AIX)
P-1J42-8ACL JP1/Extensible SNMP Agent 12-00 (for HP-UX (IPF))
P-9D42-8ACL JP1/Extensible SNMP Agent 12-00 (for Solaris)

■ Trademarks

HITACHI, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

AIX is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Itanium is a trademark of Intel Corporation or its subsidiaries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft is a trademark of the Microsoft group of companies.

Microsoft, Internet Explorer are trademarks of the Microsoft group of companies.

Microsoft, Microsoft Edge are trademarks of the Microsoft group of companies.

Microsoft, Windows are trademarks of the Microsoft group of companies.

Microsoft, Windows Server are trademarks of the Microsoft group of companies.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

The following program products contain some parts whose copyrights are reserved by Oracle and/or its affiliates: P-9D42-8JCL, and P-9D42-8ACL.

The following program products contain some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D42-8JCL, and P-9D42-8ACL.

This product includes software developed by the Apache Software Foundation.

(http://www.apache.org)

This product includes software developed by the Indiana University Extreme! Lab.

(http://www.extreme.indiana.edu)

This product includes software developed by The Legion Of The Bouncy Castle.

(http://www.bouncycastle.org)

JP1/SNMP System Observer includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

■ Issued

Jun. 2022: 3021-3-E01-30(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-E01-30(E)) and product changes related to this manual.

Changes	Location
Windows Server 2022 was added to the applicable OSs of servers for the Monitoring Manager and Monitoring Agents.	1.2.1, C.2
The procedure was changed so that the system account password is set during installation of NNMi.	1.2.2
Setting of the system account password was added to the procedure for installing NNMi.	1.3.1, 1.3.4, 1.4.1, 1.4.3
The locales set in the environment variables LC_ALL and LANG were changed.	1.4.1

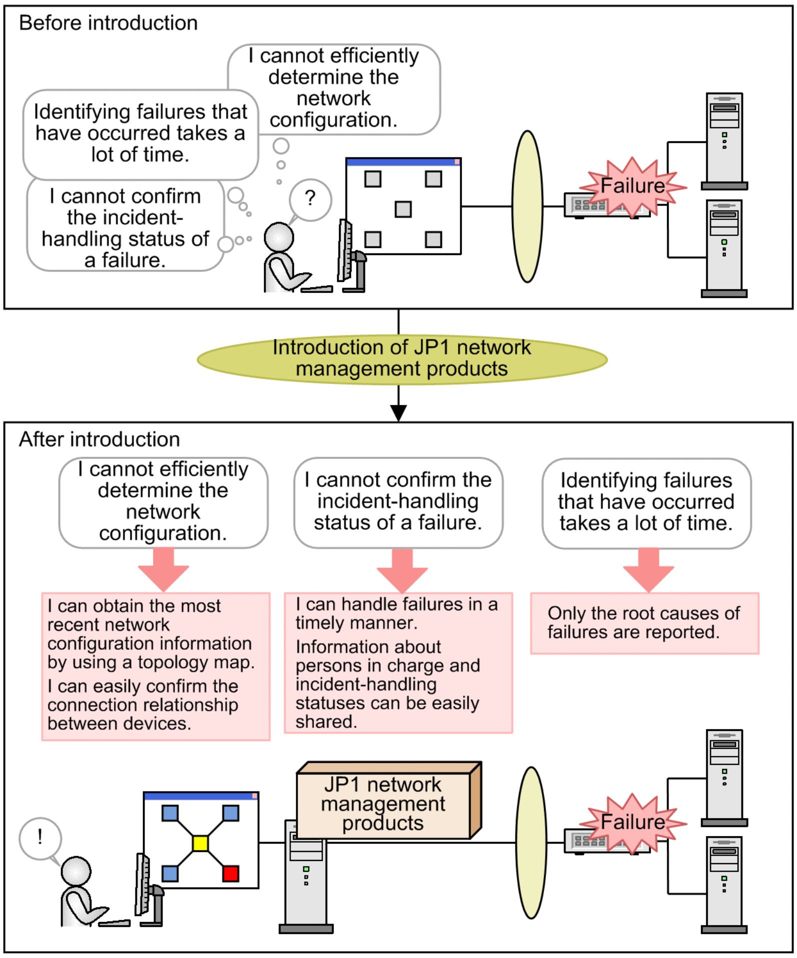
In addition to the above changes, minor editorial corrections were made.

Preface

■ What you can do with JP1 network management products

Network management is essential for providing stable environments and services, but as networks continue to become larger and more complex each day, the workload of administrators also increases.

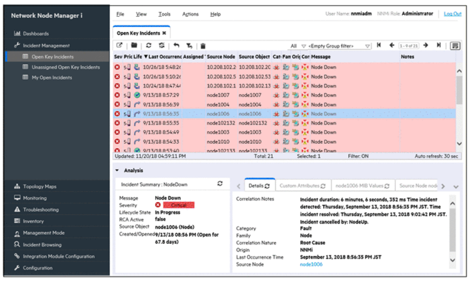
If you have encountered any of the problems shown below, take a look at your current system for network management and operation problems, and consider installing JP1 network management products. By doing so, you can efficiently monitor the status of the network to rapidly identify and solve failures.


Before introduction
I cannot efficiently determine the network configuration.
Identifying failures that have occurred takes a lot of time.
I cannot confirm the incident-handling status of a failure.
?
Failure
Introduction of JP1 network management products
After introduction
I cannot efficiently determine the network configuration.
I cannot confirm the incident-handling status of a failure.
Identifying failures that have occurred takes a lot of time.
I can obtain the most recent network configuration information by using a topology map.
I can easily confirm the connection relationship between devices.
I can handle failures in a timely manner.
Information about persons in charge and incident-handling statuses can be easily shared.
Only the root causes of failures are reported.
JP1 network management products
!
Failure

JP1 network management products provide various windows from which you can get an intuitive understanding of the configuration of networks and the statuses of resources, and provide support for the day-to-day tasks of network administrators.

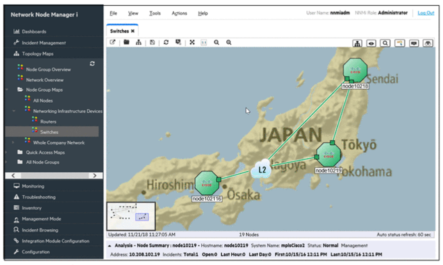
Incident management

Only root causes are reported as incidents



Node group map

Categorize and visually manage network devices

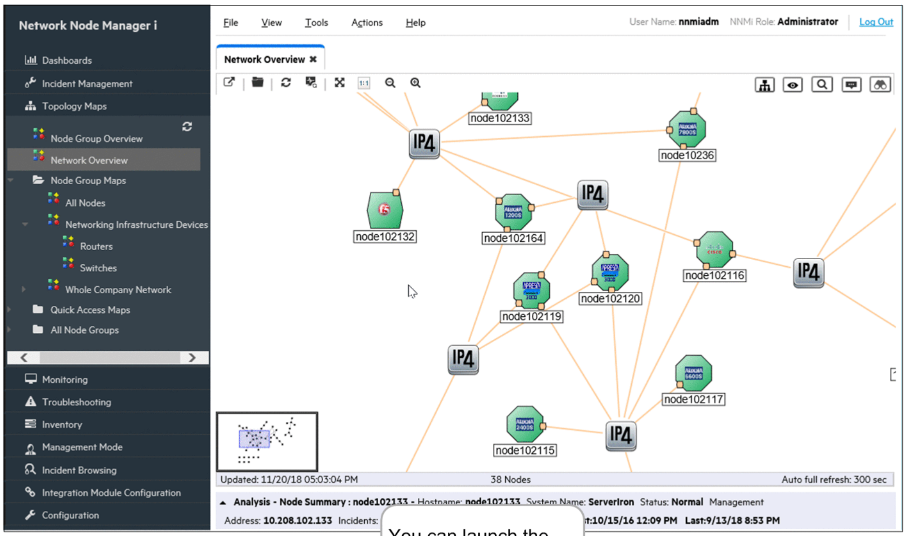


You can switch between the topology map and incident management windows.

By using a node group map, which is a customized topology map, you can obtain information about the network configuration in a form that is easier to understand.

Topology map

The network configuration is automatically updated to show the most recent information.



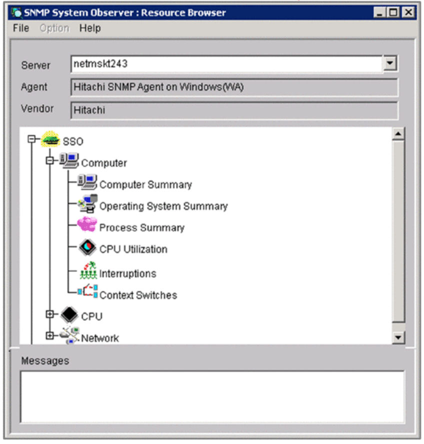
Updated: 11/20/18 05:03:04 PM 38 Nodes Auto full refresh: 300 sec

Analysis - Node Summary : node102133 - Hostname: node102133 System Name: ServerIron Status: Normal Management

Address: 10.208.102.133 Incidents: ... t:10/15/16 12:09 PM Last:9/13/18 8:53 PM

You can launch the SSO window from the NNMi console.

Resource browser



Server netmskt243

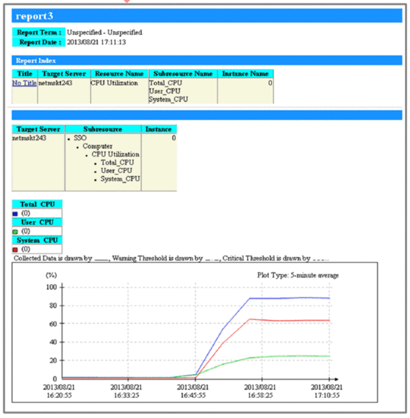
Agent Hitachi SNMP Agent on Windows(WA)

Vendor Hitachi

Messages

Collect resources for each server

Report display



report3

Report Term : Unspecified - Unspecified

Report Date : 2013/08/21 17:11:13

Report Index

Title	Target Server	Resource Name	Subresource Name	Instance Name
No Title	netmskt243	CPU Utilization	Total_CPU User_CPU System_CPU	0

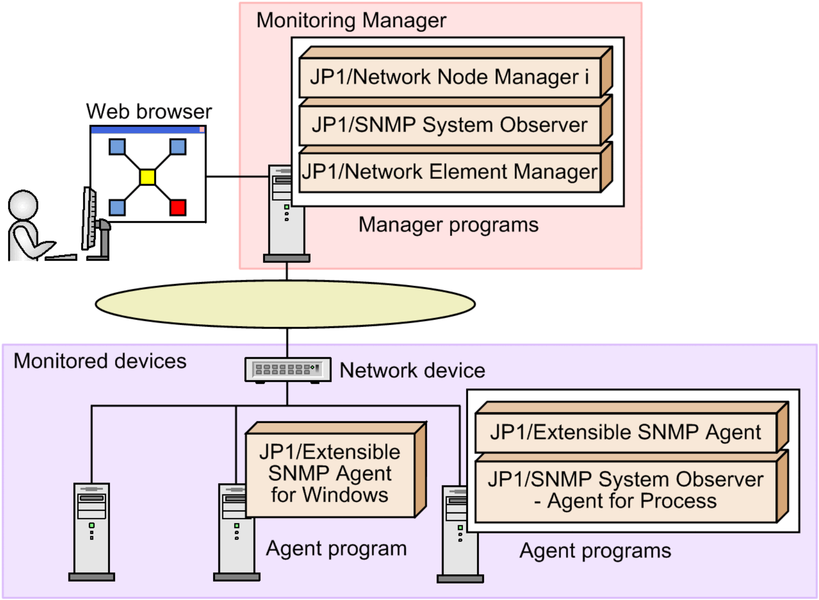
Target Server	Subresource	Instance
netmskt243	• SSO • Computer • CPU Utilization • Total_CPU • User_CPU • System_CPU	0

Total CPU
🟦 (0)
User CPU
🟩 (0)
System CPU
🟥 (0)

Collected Data is drawn by ____, Warning Threshold is drawn by _._._, Critical Threshold is drawn by _ _ _.

View the statuses of resources in easy-to-understand graphs

The JP1 network management products consist of manager programs to be installed on the Monitoring Manager, and agent programs to be installed on the monitored servers. The following figure shows the basic system configuration of JP1 network management products.


Monitoring Manager
Web browser
JP1/Network Node Manager i
JP1/SNMP System Observer
JP1/Network Element Manager
Manager programs
Monitored devices
Network device
JP1/Extensible SNMP Agent for Windows
Agent program
JP1/Extensible SNMP Agent
JP1/SNMP System Observer - Agent for Process
Agent programs

JP1/Network Node Manager i (hereinafter abbreviated to NNMi)

A manager program that uses industry-standard SNMP and that enables the management of network configurations and failures. You can use this program to automatically discover nodes in an IP network and to manage the network configuration. This program can also be used to detect network failures and issue warnings to the system administrator.

JP1/SNMP System Observer (hereinafter abbreviated to SSO)

A manager program that collects information about resources, performs alive-status monitoring of processes, and monitors the statuses of Windows services on the servers and network devices that support SNMP. By using this program, you can perform monitoring without differentiating between the vendors of network devices or between the agent types of servers.

JP1/Network Element Manager (hereinafter abbreviated to NEM)

A manager program that manages detailed information (such as port status, slot configuration, and the installation statuses of memory cards) from the GUI panel windows designed in the image of actual network devices. By using this program, you can easily and intuitively determine the statuses of network devices. Note that NEM can only be used in a Japanese environment for Windows.

JP1/Extensible SNMP Agent for Windows or JP1/Extensible SNMP Agent (hereinafter abbreviated to ESA)

An agent program that can obtain information about resources such as the CPU, memory, and file systems via SNMP. By using this program, you can obtain information that cannot be obtained by using OS-standard SNMP agents. This is a prerequisite program for JP1/SNMP System Observer - Agent for Process.

JP1/SNMP System Observer - Agent for Process (hereinafter abbreviated to SSO - AP)

An agent program that manages processes and services running on servers via SNMP.

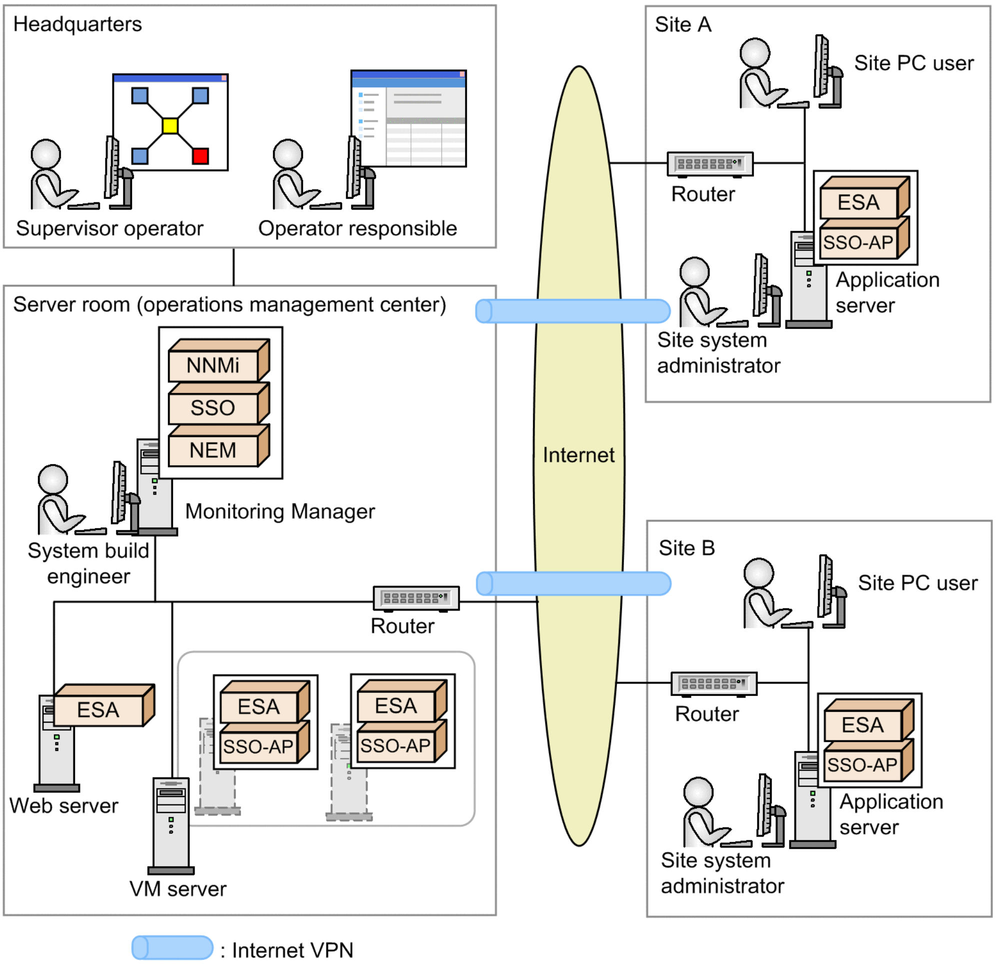
The following table describes the main functionalities of the manager programs:

Product	Functionality	Description
NNMi	Node discovery	Automatically discovers nodes according to defined rules. Nodes can also be added manually.
	Discovery and display of topologies	Automatically discovers the Layer 2 topology (network configuration using physical connection lines) in addition to the Layer 3 topology (logical network configuration), and then displays them in a map.
	Monitoring by using ICMP/SNMP polling and SNMP traps	Monitors the statuses of objects by using ICMP and SNMP polling, and monitors failures by using SNMP traps.
	Root cause analysis	Analyzes the root cause of a failure based on the Layer 2 and Layer 3 topologies that were discovered.
	Incident management	Reports failures discovered through polling and SNMP traps as incidents.
	Automatic action	Enables user-specified commands to be executed as automatic actions in response to certain incident statuses.
SSO	Resource collection	Monitors various system resources including server operational information (such as CPU usage and memory usage) and network performance information (such as line usage).
	Monitoring of processes and services	Monitors the operating status of an application through the statuses of processes and services.
NEM	Panel operation	Displays windows designed in the image of the surface panels of network devices (switches and routers). By selecting a menu, you can monitor device statuses and perform operations on each device.

■ What is explained in this manual

This manual describes the basic methods for configuring and operating JP1 network management products. The goal of this manual is to enable users who read this manual to perform day-to-day tasks for network management and to rapidly handle failures by using the JP1 network management products.

The operating procedures described in this manual are based on the system configuration and organizational structure shown in the following figure.

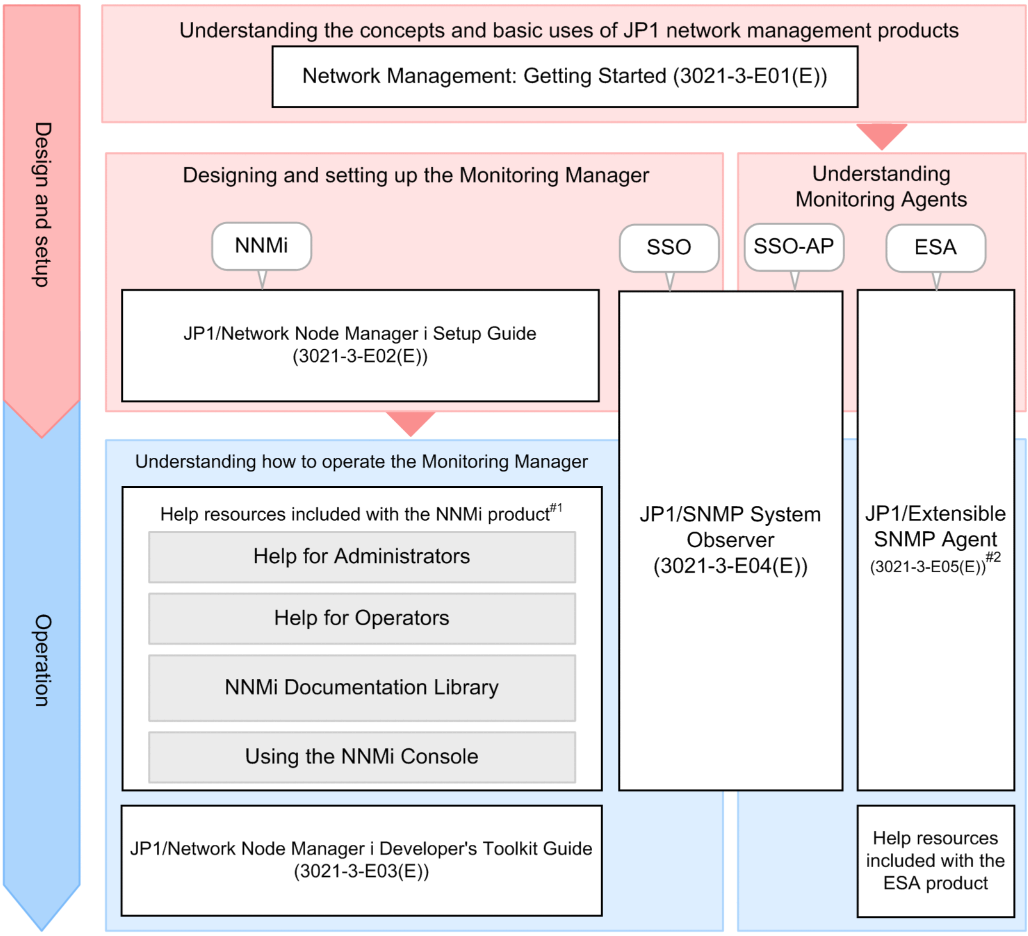


Setup procedure explained in this manual

1. The supervisor operator asks the system build engineer to set up an environment for the JP1 network management products.
2. The system build engineer prepares a server to be used as the Monitoring Manager and then sets up the Monitoring Manager environment.
3. The system build engineer asks each site system administrator to set up an environment for the Monitoring Agent.
4. Each site system administrator sets up the Monitoring Agent environment and then notifies the system build engineer.
5. After receiving notification from the site system administrators, the system build engineer configures the JP1 network management products.
6. After configuring the JP1 network management products, the system build engineer notifies the supervisor operator.
7. After receiving notification from the system build engineer, the supervisor operator registers an operator responsible as a user and starts operation using the JP1 network management products.

■ How to read this manual

In addition to this manual, the JP1 network management product provides multiple manuals and Help resources. To learn more about advanced functionality and operations, read these manuals and Help resources as shown below according to your purpose.


Design and setup
Operation
Understanding the concepts and basic uses of JP1 network management products
Network Management: Getting Started (3021-3-E01(E))
Designing and setting up the Monitoring Manager
Understanding Monitoring Agents
NNMi
SSO
SSO-AP
ESA
JP1/Network Node Manager i Setup Guide (3021-3-E02(E))
Understanding how to operate the Monitoring Manager
Help resources included with the NNMi product#1
Help for Administrators
Help for Operators
NNMi Documentation Library
Using the NNMi Console
JP1/SNMP System Observer (3021-3-E04(E))
JP1/Extensible SNMP Agent (3021-3-E05(E))#2
JP1/Network Node Manager i Developer's Toolkit Guide (3021-3-E03(E))
Help resources included with the ESA product

#1: You can access the Help resources from the **Help** menu of the NNMi console.
#2: *JP1/Extensible SNMP Agent (3021-3-E05(E))* for Windows is not available.
For details about the product, see the *Help* or *Release Notes*.

A reference to another manual is written as follows: For details about *something*, see *topic-title* in the *manual-name*. Using *topic-title* as a keyword, search for the relevant section in the target manual.

This manual assumes the use of the following environments:

For operations performed on the Monitoring Manager or Monitoring Agents

Windows: Environment where Windows Server 2012 is used

Linux: Environment where Linux 6.1 (x64) is used

For operations performed from the Web browser

Environment where Internet Explorer 11 is used

Some windows in this manual might differ from the windows of your product because of improvements made without prior notice.

■ Conventions: Fonts and symbols

The following table explains the text formatting conventions used in this manual:

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
|	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means A, or B, or C.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of A, or B, or C.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
`...`	In coding, an ellipsis (...) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify B as many times as necessary.

Contents

1 Setting Up JP1 Network Management Products

This chapter describes how you (the system build engineer) install JP1 network management products and create an environment that monitors the network.

1.1 General procedure for setting up JP1 network management products

To set up JP1 network management products, the Monitoring Manager and the Monitoring Agent need to be set up. The procedure for setting up the Monitoring Manager or the Monitoring Agent is different between Windows and Linux.

The following table shows the general procedure for setting up the Monitoring Manager.

Task overview	Step	Task details	Reference	
			Windows	Linux
Preparation before installation	1	Check the server environment.	1.2.1	
	2	Check the prerequisites of the Monitoring Manager.	1.2.2	1.2.3
Setting up the Monitoring Manager	3	Install NNMi.	1.3.1	1.4.1
	4	Install SSO.	1.3.2	1.4.2
	5	Install NEM.	1.3.3	--
	6	Set up NNMi.	1.3.4	1.4.3
	7	Set up SSO.	1.3.5	1.4.4

The table below shows the general procedure for setting up the Monitoring Agent. To set up the Monitoring Agent, repeat the following procedure according to the number of Monitoring Agents at each site:

Task overview	Step	Task details	Reference	
			Windows	Linux
Preparation before installation	1	Check the server environment.	1.2.1	
Setting up the Monitoring Agent	2	Check the prerequisites of the Monitoring Agent.	--	1.6.1
	3	Install ESA.	1.5.1	1.6.2
	4	Install SSO-AP.	1.5.2	1.6.3
	5	Set up ESA.	1.5.3	1.6.4
	6	Set up SSO-AP.	--	1.6.5
	7	Restart the Monitoring Agent.	--	1.6.6

Tip

Before setting up the Monitoring Agent, ask the system administrator of each site beforehand. Setup of the Monitoring Agent needs to be complete before you set up JP1 network management products.

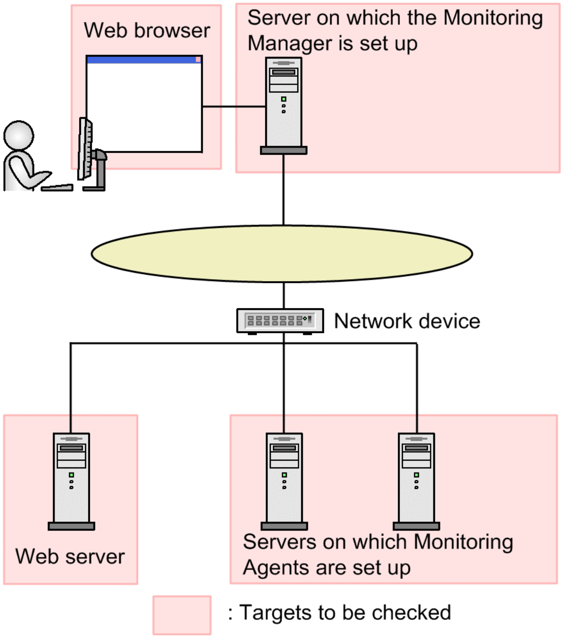
1.2 Preparation before installation

1.2.1 Checking the server environment

Before installing JP1 network management products, check whether the server environment to be used for operation is appropriate.

Before you begin

The following figure shows the system configuration that is assumed by this manual:


Web browser
Server on which the Monitoring Manager is set up
Network device
Web server
Servers on which Monitoring Agents are set up
: Targets to be checked

Procedure

1. Make sure that the specifications of the server on which the Monitoring Manager is to be set up satisfy the following conditions:
    - OS

      For Windows: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022

      For Linux: CentOS 6.1 (x64), CentOS 7.1, CentOS 8.1, Linux 6.1 (x64), Linux 7.1, Linux 8.1, Oracle Linux 6.1 (x64), Oracle Linux 7.1, Oracle Linux 8.1, or SUSE Linux 12

      Note that this manual describes the setup procedure for Windows Server 2012 and Linux 6.1 (x64).
    - Disk capacity:

      For Windows: 14.5 GB or more

      For Linux: 14.0 GB or more
    - Memory:

      For Windows: 4.5 GB or more

      For Linux: 6.0 GB or more

2. Make sure that the specifications of the server on which the Monitoring Agent is to be set up satisfy the following conditions:

   - OS

     For Windows: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022

     For Linux: CentOS 6.1 (x64), CentOS 7.1, CentOS 8.1, Linux 6.1 (x64), Linux 7.1, Linux 8.1, Oracle Linux 6.1 (x64), Oracle Linux 7.1, Oracle Linux 8.1, SUSE Linux 12, or SUSE Linux 15

     For UNIX: HP-UX (IPF), AIX V7.1, AIX V7.2, or Solaris 11

     Note that this manual describes the setup procedure for Windows Server 2012 and Linux 6.1 (x64).

   - Disk capacity:

     For Windows: 65.0 MB or more

     For Linux: 150.0 MB or more

   - Memory:

     For Windows: 15.0 MB or more

     For Linux: 70.0 MB or more

3. Check the language settings of the server on which the Monitoring Manager is to be set up.

   For Windows, set the locale as follows:

   - For a Japanese environment: Japanese
   - For an English environment: English
   - For a Chinese environment: Chinese

   For Linux, set the locale as follows:

   - For a Japanese environment: ja_JP.UTF-8
   - For an English environment: C
   - For a Chinese environment: zh_CN.utf8

4. Check the port number of the Web server.

   The port number of the Web server is used during the installation of NNMi. The default HTTP port is 80, and the default HTTPS port is 443.

5. Make sure that the Web browser to be used satisfies the following conditions:

   If the OS is Windows: Internet Explorer 11, Firefox ESR 78, Google Chrome or Microsoft Edge (Chromium version)

Next steps

After making sure that there is no problem in the server environment, proceed to the next task of checking the prerequisites.

Related topics

- Topic *Preinstallation Checklists* in the *JP1/Network Node Manager i Setup Guide*.
- 1.2.2 Checking the prerequisites of the Monitoring Manager (for Windows)
- 1.2.3 Checking the prerequisites of the Monitoring Manager (for Linux)

1.2.2 Checking the prerequisites of the Monitoring Manager (for Windows)

If the Monitoring Manager is to run on Windows, check the settings below, and then start installing the JP1 network management products.

Before you begin

For details about the prerequisites, see the topic *Preinstallation Checklists* in the *JP1/Network Node Manager i Setup Guide*.

Procedure

1. Check the host name of the Monitoring Manager.

   The host name is used when setting the trap destination and during login.

2. Make sure that the port number to be used by the Monitoring Manager is not used.

   If you execute `netstat -an` at the command prompt, you can check the currently used port numbers.

   For details about the port numbers, see the topic *List of Ports Used by NNMi* in the *JP1/Network Node Manager i Setup Guide*. For details about SSO, see *Port Number Settings*.

3. Assign a static IP address to the Monitoring Manager.

   You need to assign a static IP address, not a dynamic IP address by DHCP.

4. Check the installation folder of NNMi.

   The installation folder of NNMi is used during its installation. The default folders are as follows:

   - For the program: `C:\Program Files (x86)\Hitachi\Cm2NNMi\`
   - For data: `C:\ProgramData\Hitachi\Cm2NNMi\`

5. Consider the NNMi system account password.

   The NNMi system account is used to sign in to the NNMi console first.
   Between 1 and 40 characters can be entered for the password.
   Alphanumeric characters (A to Z, a to z, 0 to 9), and underscores (_) can be used.

6. Check the installation folder of SSO.

   The installation folder of SSO is used during its installation. The default folder is as follows:

   - `C:\Program Files\HITACHI\JP1SSO\`

7. Disable the antivirus software.

   Disable the antivirus software only during the installation of the JP1 network management products.

8. Set the SNMP Trap service, which is a Windows SNMP-related service, to **Disabled**.

9. If you monitor the Monitoring Manager by using SNMP, make sure the SNMP service is available.

10. Use Windows Firewall to make sure that access to the port number used by the Monitoring Manager is enabled.

    For details about access to the port number, see the topic *Firewall pass-through direction in the JP1/Network Node Manager i Setup Guide*.

11. Make sure that the values set for the environment variables `TEMP` and `TMP` are the same.

    If the values of the environment variables `TEMP` and `TMP` differ, the installation of NNMi might fail. If the values differ, set the same value. Note that 500.0 MB of the `%TEMP%` folder is used during the installation.

12. Click **Administrative Tools**, **Remote Desktop Services**, and then **Remote Desktop Session Host Configuration**. Specify the Remote Desktop settings as follows:
    - Do not delete temporary folders on exit
    - Do not use temporary folders per session

Next steps

After you make sure that there is no problem in the prerequisite environment, proceed to the next task of setting up the Monitoring Manager.

Related topics

- 1.3 Setting up the Monitoring Manager (for Windows)

1.2.3 Checking the prerequisites of the Monitoring Manager (for Linux)

If the Monitoring Manager is to run on Linux, check the settings below, and then start installing the JP1 network management products.

Before you begin

For details about the prerequisites, see the topic *Preinstallation Checklists* in the *JP1/Network Node Manager i Setup Guide*.

Procedure

1. Check the host name of the Monitoring Manager.

   The host name is used for setting the trap destination and during login.

2. Make sure that the port number to be used by the Monitoring Manager is not used.

   If you execute `netstat -an` at the command prompt, you can check the currently used port numbers.

   For details about the port numbers, see the topic *List of Ports Used by NNMi* in the *JP1/Network Node Manager i Setup Guide*.

3. Assign a static IP address to the Monitoring Manager.

   You need to assign a static IP address, not a dynamic IP address by DHCP.

4. Disable the antivirus software.

   Disable the antivirus software only during the installation of the JP1 network management products.

5. Make sure that the following packages and library files are installed:
    - kernel-2.6.32-220.4.2.el6.x86_64.rpm or later
    - kernel-firmware-2.6.32-220.4.2.el6.noarch.rpm or later
    - /lib64/libaio.so.1
    - /usr/lib64/libXtst.so.6
    - /usr/lib64/libXi.so.6
    - glibc (i686)

- libstdc++ (i686)
- libgcc (i686)
- ncompress (x86_64)
- tar (x86_64)
- gdb (x86_64)
- openmotif (x86_64)
- glibc (x86_64)
- glibc-common (x86_64)
- glibc-devel (i686)
- glibc-devel (x86_64)
- glibc-headers (x86_64)
- glibc-utils (x86_64)
- nscd (x86_64)
- libXtst (i686)
- libnsl (Linux 8.1 or later, CentOS 8.1 or later, Oracle Linux 8.1 or later)
- lsb_release
- net-tools
- unzip
- fontconfig
- liberation-sans-fonts (It is not necessary if fc-list command shows one or more fonts.)

In addition, install the library files that depend on each of the files above. The required packages and library files differ depending on the type or version of the OS. For details, see the *Release Notes*.

6. Open the `/etc/sysctl.conf` file, and set the kernel parameters.

Add the following entries to the `/etc/sysctl.conf` file:

```
# NNM settings for embedded database
kernel.shmmax = 68719476736
kernel.shmall = 68719476736
# NNM settings for UDP receive and send buffer sizes
net.core.rmem_max = 8388608
net.core.wmem_max = 2097152
```

In the entries above, the shared memory (kernel.shmmax, kernel.shmall) is set to 64.0 GB, the UDP receive buffer (net.core.rmem_max) is set to 8.0 MB, and the UDP send buffer (net.core.wmem_max) is set to 2.0 MB.

Next steps

After you make sure that there is no problem in the prerequisite environment, proceed to the next task of setting up the Monitoring Manager.

Related topics

- 1.4 Setting up the Monitoring Manager (for Linux)

1.2.4 Storage location of the commands of each product

The following shows the storage location of the commands of each product:

Storage location of the NNMi commands

- For Windows
  installation-folder-of-NNMi`\bin\`
- For Linux
  `/opt/OV/bin/`

Storage location of the SSO commands

- For Windows
  installation-folder-of-SSO`\bin\`
- For Linux
  `/opt/CM2/SSO/bin/`

Storage location of the SSO - AP commands

- For Windows
  installation-folder-of-SSO-AP`\bin\`
- For Linux
  `/opt/CM2/APM/bin/`

Storage location of the ESA commands

- For Windows
  installation-folder-of-ESA`\bin\`
- For Linux
  `/opt/CM2/ESA/bin`

1.3 Setting up the Monitoring Manager (for Windows)

You need to install and set up NNMi, SSO, and NEM to set up the Monitoring Manager in a Windows environment.

1.3.1 Installing NNMi (for Windows)

If the Monitoring Manager is to run on Windows, use the Hitachi Integrated installer and follow the wizard to install NNMi.

Procedure

1. As a user with Administrators permissions, log in to the server on which the Monitoring Manager is to be set up, and then insert the distribution media.
2. Select `JP1/Network Node Manager i`.
   A window to confirm the NNMi setting values appears.
3. Specify the port number of the Web server, and then press the **Enter** key.
   If you press the **Enter** key without entering a value, the default value is specified. The default value of the http port is 80, and the default value of the https port is 443.
4. Specify the installation folder of NNMi.
   If you press the **Enter** key without entering a value, the default value is specified. The default value is as follows:
   - For the program: `C:\Program Files (x86)\Hitachi\Cm2NNMi\`
   - For data: `C:\ProgramData\Hitachi\Cm2NNMi\`

   The NNMi settings file, database, and log file are stored in the installation folder for data.
5. Enter `yes`, and then press the **Enter** key.
   The installation of NNMi starts. After a while, you will be prompted to set the system account password.
6. Set the system account password.
   Follow the instructions on the screen to set a password.
   To set it after installation, enter `\quit`.
   After the configuration is complete, press Enter to close the command prompt.

Next steps

Next, install SSO.

Related topics

- 1.3.2 Installing SSO (for Windows)

1.3.2 Installing SSO (for Windows)

If the Monitoring Manager is to run on Windows, use the Hitachi Integrated installer and follow the wizard to install SSO.

Procedure

1. As a user with Administrators permissions, log in to the server on which the Monitoring Manager is to be set up, and then insert the distribution media.

2. Select `JP1/SNMP System Observer`.

3. Install SSO by following the installer instructions.

Next steps

If you are using a switch or router that is supported by NEM, install NEM. If you do not need to install NEM, proceed to the task of setting up NNMi.

Related topics

- 1.3.3 Installing NEM (for Windows)
- 1.3.4 Setting up NNMi (for Windows)

1.3.3 Installing NEM (for Windows)

If the Monitoring Manager is to run on Windows and you are using a switch or router that is supported by NEM, install NEM. Use the Hitachi Integrated installer and follow the wizard to install NEM.

Procedure

1. As a user with Administrators permissions, log in to the server on which the Monitoring Manager is to be set up, and then insert the distribution media.

2. Select `JP1/Network Element Manager`.

3. Install NEM by following the installer instructions.

Next steps

Next, set up NNMi.

Related topics

- 1.3.4 Setting up NNMi (for Windows)

1.3.4 Setting up NNMi (for Windows)

If you skip setting the system account password during installation, stop the NNMi service and set the system account. To register other members, first log in to the NNMi console, and then register users.

Before you begin

If the command prompt was opened before the installation and remains open, close it, and then open it again.

Procedure

1. Steps a. and b. are performed only if you skip setting the system account password during installation.
   a. In the command prompt, execute `ovstop -c` to stop the NNMi service.
      The NNMi service stops. Immediately after the installation, the NNMi service is stopped.
   b. Execute `nnmchangesyspw.ovpl` to set the password.
      Enter `y`, and then specify the password by following the message.

2. Execute `ovstart -c` to start NNMi.

3. Execute `ovstatus -c` to check the NNMi status.
   If all statuses are in the running status, there is no problem.

Next steps

Next, set up SSO.

Related topics

- 1.2.4 Storage location of the commands of each product
- 2.2.3 Registering users
- 1.3.5 Setting up SSO (for Windows)

1.3.5 Setting up SSO (for Windows)

If the Monitoring Manager is to run on Windows, set the community name and the SSO definition information to set up SSO.

(1) Adding information about the connection from SSO to NNMi

Execute the `ssonnmsetup` command of SSO to set the connection information for linking with NNMi.

Procedure

1. Execute the following command:
   `ssonnmsetup -add -user` *user-name* `-password` *password* `-port` *port-number* `-ssl`
   Specify the user name and password of the system account. For *port-number*, specify the port number of the Web server. Specify the `-ssl` option only if HTTPS is used for communication.

Related topics

- 1.2.4 Storage location of the commands of each product
- 1.3.4 Setting up NNMi (for Windows)
- 1.2.1 Checking the server environment

(2) Setting the SSO definition information for NNMi

Execute a command to set the SSO definition information for NNMi.

Procedure

1. Execute the `nnmconfigimport.ovpl` command of NNMi to set the incident definition.

   `nnmconfigimport.ovpl -u` *user-name* `-p` *password* `-f` *installation-folder-of-SSO*`\incident \ssoincident.def`

   Specify the user name and password of the system account.

   If an APM instance that does not use TCP communication for event notification is used to monitor processes or services, the following incident definition must also be set:

   `nnmconfigimport.ovpl -u` *user-name* `-p password -f` *installation-folder-of-SSO*`\incident \apmtrap.def`

2. Execute the `nnmconfigimport.ovpl` command of NNMi to set the URL action definition.

   `nnmconfigimport.ovpl -u` *user-name* `-p` *password* `-f` *installation-folder-of-SSO*`\urlaction \ssourlaction.def`

   Specify the user name and password of the system account.

3. Execute the `ssoauth` command of SSO to register a user in SSO.

   `ssoauth -add -user` *user-name* `-password` *password*

   Set the user name and password that are used for logging in from the SSO console.

4. Execute the `ssostart` command of SSO to start SSO.

5. Execute the `ssostatus` command of SSO to check the SSO status.

   If all statuses are in the running status, there is no problem.

Related topics

- 1.2.4 Storage location of the commands of each product

(3) Setting the community name

The community name is a password for accessing the MIB object by using the SNMP protocol. To collect resources, you need to match the `get` community names of the Monitoring Agent and the Monitoring Manager. To monitor processes and services, you need to match the `set` community names of the Monitoring Agent and the Monitoring Manager.

Procedure

1. Open the SNMP definition file (*installation-folder-of-SSO*`\conf\ssosnmp.conf`).

2. Edit the SNMP definition file.

3. Execute the `ssoapcom` command as follows to load the definition file again:

   ```
   ssoapcom -r
   ```

4. Execute the `ssocollectd` command as follows to load the definition file again:

   ```
   ssocollcetd -r
   ```

Next steps

You have now successfully completed the setup of the Monitoring Manager. Make sure that the setup of the Monitoring Agent at each site is complete. If the setup of the Monitoring Agent at each site is complete, proceed to the next task of setting up the JP1 network management products.

Related topics

- 1.2.4 Storage location of the commands of each product
- 1.3.4 Setting up NNMi (for Windows)
- 1.5 Setting up the Monitoring Agent (for Windows)
- 2. Configuring JP1 Network Management Products

1.3.6 Setting up WebGUI of SSO (for Windows)

Set up WebGUI of SSO on Windows where you use SSO Console.

Do the following by an user with Administrators permissions.

Procedure

1. Copy `ssogui_fileset.zip` file to the Windows and extract the zip file.
   File location:
   installation-folder-of-SSO`\webgui\ssogui_fileset.zip`
2. Execute the following command included in the extracted folder at command prompt.
   extracted-path`\SSOGUI\bin\webguisetup.bat` *extracted-path*`\SSOGUI`

1.4 Setting up the Monitoring Manager (for Linux)

Install and set up NNMi and SSO to set up the Monitoring Manager in a Linux environment.

1.4.1 Installing NNMi (for Linux)

If the Monitoring Manager is to run on Linux, use the Hitachi Integrated installer and follow the wizard to install NNMi.

Procedure

1. As a user with root permissions, log in to the server on which the Monitoring Manager is to be set up.
2. For the environment variable `LC_ALL`, `LANG`, set the following locale:
   - For a Japanese environment
     ```
     # LC_ALL=ja_JP.utf8
     # export LC_ALL
     # LANG=ja_JP.utf8
     # export LANG
     ```
     or
     ```
     # LC_ALL=ja_JP.UTF-8
     # export LC_ALL
     # LANG=ja_JP.UTF-8
     # export LANG
     ```
   - For an English environment
     ```
     # LC_ALL=C
     # export LC_ALL
     # LANG=C
     # export LANG
     ```
     or
     ```
     # LC_ALL=en_US.utf8
     # export LC_ALL
     # LANG=en_US.utf8
     # export LANG
     ```
     or
     ```
     # LC_ALL=en_US.UTF-8
     # export LC_ALL
     # LANG=en_US.UTF-8
     # export LANG
     ```
   - For a Chinese environment
     ```
     # LC_ALL=zh_CN.utf8
     # export LC_ALL
     # LANG=zh_CN.utf8
     # export LANG
     ```

3. Insert the distribution media of NNMi, and then execute the following command:
   `/`*mount-directory-name-of-the-provided-media*`/X64LIN/setup /`*mount-directory-name-of-the-provided-media*

4. In the initial window of Hitachi PP Installer, enter `I`.

5. Select `JP1/Network Node Manager i`, and then enter `I`.
   A message confirming that you want to continue the installation appears.

6. Enter `Y`.

7. Enter information by following the installer instructions.
   If you press the **Enter** key without entering a value, the default value is specified.
   NNMi is installed in the following folders:
   - For the program: `/opt/OV/`
   - For data: `/var/opt/OV/`

   After a while, you will be prompted to enter the password for the system account. To set it after installation, enter `\quit`.

Next steps

Next, install SSO.

Related topics

- 1.4.2 Installing SSO (for Linux)

1.4.2 Installing SSO (for Linux)

If the Monitoring Manager is to run on Linux, use the Hitachi Integrated installer and follow the wizard to install SSO.

Procedure

1. As a user with root permissions, log in to the server on which the Monitoring Manager is to be set up, and then insert the distribution media.

2. Execute the following command:
   `/`*mount-directory-name-of-the-provided-media*`/X64LIN/setup /`*mount-directory-name-of-the-provided-media*

3. In the initial window of Hitachi PP Installer, enter `I`.

4. Select `JP1/SNMP System Observer`, and then enter `I`.
   A message confirming that you want to continue the installation appears.

5. Enter `Y`.
   SSO is installed.

Next steps

Next, set up NNMi.

Related topics

- 1.4.3 Setting up NNMi (for Linux)

1.4.3 Setting up NNMi (for Linux)

If the Monitoring Manager is to run on Linux, set the system account to set up NNMi.

(1) Setting up the system account

If you skipped setting the System account password during installation, set the NNMi system account. The procedure for setting up the account is the same as that for Windows.

After setting the system account, set up SSO.

Related topics

- 1.2.4 Storage location of the commands of each product
- 1.3.4 Setting up NNMi (for Windows)
- 1.4.4 Setting up SSO (for Linux)

1.4.4 Setting up SSO (for Linux)

If the Monitoring Manager is to run on Linux, set the language environment and the definition information to set up SSO.

(1) Setting the language environment

After the installation of SSO is complete, you need to add the language setting to the `/etc/rc.d/init.d/sso` file.

Procedure

1. Open the `/etc/rc.d/init.d/sso` file.

2. Add the following two lines immediately after the line `./etc/rc.d/init.d/functions`.
   - For a Japanese environment
     LANG=ja_JP.UTF-8
     export LANG
   - For an English environment
     LANG=C
     export LANG
   - For a Chinese environment
     LANG=zh_CN.utf8

export LANG

3. Overwrite the `/etc/rc.d/init.d/sso` file.

   Now, the language environment is set.

(2) Adding information about the connection from SSO to NNMi

Set the connection information for linking with NNMi. The procedure for setting the information is the same as that for Windows.

Related topics

- (1) Adding information about the connection from SSO to NNMi

(3) Setting the SSO definition information for NNMi

Execute a command to set the SSO definition information for NNMi.

Procedure

1. Execute the `nnmconfigimport.ovpl` command of NNMi to set the incident definition.

   `nnmconfigimport.ovpl -u` *user-name* `-p` *password* `-f /etc/opt/CM2/SSO/incident/ssoincident.def`

   Specify the user name and password of the system account.

   If an APM instance that does not use TCP communication for event notification is used to monitor processes or services, the following incident definition must also be set:

   `nnmconfigimport.ovpl -u` *user-name* `-p` *password* `-f` *installation-folder-of-SSO* `\incident\apmtrap.def`

2. Execute the `nnmconfigimport.ovpl` command of NNMi to set the URL action definition.

   `nnmconfigimport.ovpl -u` *user-name* `-p` *password* `-f /etc/opt/CM2/SSO/urlaction/ssourlaction.def`

   Specify the user name and password of the system account.

3. Execute the `ssoauth` command of SSO to register a user in SSO.

   `ssoauth -add -user` *user-name* `-password` *password*

   Set the user name and password that are used for logging in from the SSO console.

4. Execute the `ssostart` command of SSO to start SSO.

5. Execute the `ssostatus` command of SSO to check the SSO status.

   If all statuses are in the running status, there is no problem.

Related topics

- 1.2.4 Storage location of the commands of each product

(4) Setting the community name

The community name is a password for accessing the MIB object by using the SNMP protocol. To collect resources, you need to match the `get` community names of the Monitoring Agent and the Monitoring Manager. To monitor processes and services, you need to match the `set` community names of the Monitoring Agent and the Monitoring Manager.

Procedure

1. Open the SNMP definition file (`/etc/opt/CM2/SSO/conf/ssosnmp.conf`).

2. Edit the SNMP definition file.

3. Execute the `ssoapcom` command as follows to load the definition file again:

   ```
   ssoapcom -r
   ```

4. Execute the `ssocollectd` command as follows to load the definition file again:

   ```
   ssocollcetd -r
   ```

Next steps

After setting the community name, make sure that the setup of the Monitoring Agent at each site is complete. If the setup of the Monitoring Agent at each site is complete, proceed to the task of setting up the JP1 network management products.

Related topics

- 1.2.4 Storage location of the commands of each product
- (2) Setting the SSO definition information for NNMi
- 1.6 Setting up the Monitoring Agent (for Linux)
- 2. Configuring JP1 Network Management Products

1.4.5 Setting up WebGUI of SSO (for Linux)

Set up WebGUI of SSO on Windows where you use SSO Console.

Do the following by an user with Administrators permissions.

Procedure

1. Copy `ssogui_fileset.zip` file to the Windows and extract the zip file.

   File location:

   ```
   /etc/opt/CM2/SSO/webgui/ssogui_fileset.zip
   ```

2. Execute the following command included in the extracted folder at command prompt.

   ```
   extracted-path\SSOGUI\bin\webguisetup.bat  extracted-path\SSOGUI
   ```

1.5 Setting up the Monitoring Agent (for Windows)

For a Monitoring Agent that is to run on Windows, install and set up ESA and SSO - AP to set up the Monitoring Agent.

> **Tip**
>
> We recommend that you (the system administrator at each site) install the Monitoring Agent at a time that will not affect your business's work.

1.5.1 Installing ESA (for Windows)

If the Monitoring Agent is to run on Windows, use the Hitachi Integrated installer and follow the wizard to install ESA.

Procedure

1. Make sure that the Windows SNMP service is installed.

   If the service is not installed, install it. For details about how to install the Windows SNMP service, see the Windows documentation.

2. For the `hosts` file (*system-root-folder*`\system32\drivers\etc\hosts`) of the computer on which you will install an agent, set the following host names:

   - Host name of the Monitoring Manager
   - Host name of the Monitoring Agent

3. As a user with Administrators permissions, log in to the computer on which you will install the agent, and then insert the distribution media.

4. Select `JP1/Extensible SNMP Agent`.

5. Install ESA by following the installer instructions.

6. Start the Windows SNMP service.

7. Execute the `snmpcheck` command of ESA to check the ESA status.

   If all statuses are running (except for `hismsmib`), there is no problem.

8. Stop the Windows SNMP service.

Next steps

Next, install SSO - AP.

Related topics

- 1.2.4 Storage location of the commands of each product
- 1.5.2 Installing SSO - AP (for Windows)

1.5.2 Installing SSO - AP (for Windows)

If the Monitoring Agent is to run on Windows, use the Hitachi Integrated installer and follow the wizard to install SSO - AP.

Procedure

1. As a user with Administrators permissions, log in to the computer on which you will install the agent, and then insert the distribution media.
2. Select `JP1/SNMP System Observer - Agent for Process`.
3. Install SSO - AP by following the installer instructions.
4. Start the Windows SNMP System Observer - Agent for Process service.
5. Execute the `apmcheck` command of SSO - AP to check the SSO - AP status.
   If all statuses are in the running status, there is no problem.

Next steps

Next, set up ESA.

Related topics

- 1.2.4 Storage location of the commands of each product
- 1.5.3 Setting up ESA (for Windows)

1.5.3 Setting up ESA (for Windows)

If the Monitoring Agent is to run on Windows, set the community name and the trap destination for the Windows SNMP service.

(1) Setting the community name for the Windows SNMP service

The community name is a password for accessing the MIB object by using the SNMP protocol. To collect resources or to monitor processes and services, you need to match the community names of the Monitoring Agent and the Monitoring Manager. To set the community name, from the Windows Services window, display the **SNMP Service** properties, and then set the name. For details, see the Windows documentation.

(2) Setting the trap destination for the Windows SNMP service

The trap destination determines where SNMP traps should be sent, and is used to check the manager that receives Monitoring Agent traps. If you want to send traps to the Monitoring Manager, you need to use the Monitoring Agent to set the trap destination.

Procedure

1. From the Windows Services window, display the **SNMP Service** properties, and then set the trap destination.
   For details, see the Windows documentation.

Next steps

Next, specify settings for monitoring the network by using the JP1 network management products.

Related topics

- 2. Configuring JP1 Network Management Products

1.6 Setting up the Monitoring Agent (for Linux)

For a Monitoring Agent that is to run on Linux, install and set up ESA and SSO - AP to set up the Monitoring Agent.

> **Tip**
>
> We recommend that you (the system administrator at each site) install the Monitoring Agent at a time that will not affect your business's work.

1.6.1 Checking the prerequisites of the Monitoring Agent (for Linux)

If the Monitoring Agent is to run on Linux, check the settings below, and then start installing the Monitoring Agent.

Procedure

1. Make sure that the following packages or subsequent patch files are applied to the OS:
   - glibc-2.12-1.25.el6.i686
   - libgcc-4.4.5-6.el6.i686
   - libstdc++-4.4.5-6.el6.i686
   - nss-softokn-freebl-3.12.7-1.1.el6.i686
   - net-snmp-5.5-31.el6
   - net-snmp-libs-5.5-31.el6
   - net-snmp-utils-5.5-31.el6

   The required packages differ depending on the type or version of the OS. For details about the packages to be applied, see the *Release Notes*.

2. Make sure that the following commands used to obtain the MIB values are installed:
   - /usr/bin/vmstat
   - /bin/ps
   - /usr/bin/uptime
   - /usr/bin/free
   - /usr/bin/mpstat

3. Make sure that the native agent is installed.

   If the native agent is not installed, install it. For details about how to install the native agent, see the topic *Notes about installation* in the manual *JP1/Extensible SNMP Agent*.

Next steps

Check the prerequisites of the Monitoring Agent, and then install ESA.

Related topics

- 1.2.4 Storage location of the commands of each product

- 1.6.2 Installing ESA (for Linux)

1.6.2 Installing ESA (for Linux)

If the Monitoring Agent is to run on Linux, use the Hitachi Integrated installer and follow the wizard to install ESA.

Procedure

1. For the `/etc/hosts` file, set the IP address that corresponds to the host name of the Monitoring Agent.
   (Example) 11.22.33.44 esahost
2. As a user with root permissions, log in to the computer on which you will install the agent, and then insert the distribution media.
3. Execute the following command:
   `/`*mount-directory-name-of-the-provided-media*`/linux/setup /`*mount-directory-name-of-the-provided-media*
4. In the initial window of Hitachi PP Installer, enter `I`.
5. Select `JP1/Extensible SNMP Agent`, and then enter `I`.
   A message confirming that you want to continue the installation appears.
6. Enter `Y`.
7. Enter information by following the installer instructions.
   If you press the **Enter** key without entering a value, the default value is specified.

Next steps

Now, you have successfully installed ESA. Next, install SSO - AP.

Related topics

- 1.6.3 Installing SSO - AP (for Linux)

1.6.3 Installing SSO - AP (for Linux)

If the Monitoring Agent is to run on Linux, use the Hitachi Integrated installer and follow the wizard to install SSO - AP.

Procedure

1. As a user with root permissions, log in to the computer on which you will install the agent, and then insert the distribution media.
2. Execute the following command:
   `/`*mount-directory-name-of-the-provided-media*`/linux/setup /`*mount-directory-name-of-the-provided-media*
3. In the initial window of Hitachi PP Installer, enter `I`.

4. Select `JP1/SSO - Agent for Process`, and then enter `I`.
   A message confirming that you want to continue the installation appears.

5. Enter `Y`.

6. Install SSO - AP by following the installer instructions.

Next steps

Now, you have successfully installed SSO - AP. Next, set up ESA.

Related topics

- 1.6.4 Setting up ESA (for Linux)

1.6.4 Setting up ESA (for Linux)

If the Monitoring Agent is to run on Linux, set the community name and the trap destination for the configuration definition file (`/etc/SnmpAgent.d/snmpd.conf`). The configuration definition file is stored on the computer on which you installed the agent.

(1) Setting the community name

The community name is a password for accessing the MIB object by using the SNMP protocol. To collect resources, you need to match the `get` community names of the Monitoring Agent and the Monitoring Manager. To monitor processes and services, you need to match the `set` community names of the Monitoring Agent and the Monitoring Manager.

Procedure

1. Open the configuration definition file (`/etc/SnmpAgent.d/snmpd.conf`).

2. Search for the following line in the configuration definition file:
   `get-community-name: public`
   For the `get` community name, `public` is set by default.

3. Change the `get` community name.
   (Example) `get-community-name: private`

4. Search for the following line in the configuration definition file:
   `#set-community-name: # enter community name`

5. Change the setting as follows:
   `set-community-name:`

6. On the right side of the label `set-community-name:`, set the `set` community name.
   (Example) `set-community-name: private`

7. Save the configuration definition file (`/etc/SnmpAgent.d/snmpd.conf`), and then close it.

(2) Setting the trap destination

The trap destination determines where SNMP traps should be sent, and is used to check the manager that receives Monitoring Agent traps. If you want to send traps to the Monitoring Manager, you need to use the Monitoring Agent to set the trap destination.

Procedure

1. Open the configuration definition file (`/etc/SnmpAgent.d/snmpd.conf`).
2. Search for the following line in the configuration definition file:
   ```
   #trap-dest: # enter trap destination
   ```
3. Change the setting as follows:
   ```
   trap-dest:
   ```
4. On the right side of the label `trap-dest:`, enter the host name or IP address of the manager to which the Monitoring Agent sends traps.
   (Example) `trap-dest: 15.2.113.223`
5. Save the configuration definition file (`/etc/SnmpAgent.d/snmpd.conf`), and then close it.

Next steps

Next, set up SSO - AP.

Related topics

- 1.6.5 Setting up SSO - AP (for Linux)

1.6.5 Setting up SSO - AP (for Linux)

If the Monitoring Agent is to run on Linux, change the `hosts` file and port number.

(1) Setting the local IP address in the hosts file

If `127.0.0.1` is defined as the local IP address in the `/etc/hosts` file, the SSO - AP process cannot be monitored. You need to define the actual local IP address.

Procedure

1. Open the `/etc/hosts` file.
2. Search for the following line:
   `127.0.0.1` *local-server-name* `localhost. localdomain localhost`
3. Change the line as follows:
   `127.0.0.1 localhost. localdomain localhost`
   IP-address-of-the-local-server local-server-name
   (Example)

```
127.0.0.1 localhost. localdomain localhost
172.16.49.18 linux01
```

4. Save the `/etc/hosts` file, and then close it.

(2) Changing the port number in the apmstart file

To perform process monitoring for SSO - AP, you need to match the default start port number of the SNMP agent and the port number in the `apmstart` file.

Before you begin

The port number of the monitoring agent that was set in the SSO's SNMP definition file (`ssosnmp.conf`) must be the same as the port number set in the `apmstart` file.

In the SSO's SNMP definition file (`ssosnmp.conf`), change the port number of the monitoring agent in the category name `process` or `sso`, under `# 1. Specific Hosts` or `# 2. IP Address Wildcards`.

Procedure

1. Open the `/opt/CM2/APM/bin/apmstart` file.

2. Search for the following line:
   ```
   SR_SNMP_TEST_PORT=221161
   ```

3. Change the line as follows:
   `SR_SNMP_TEST_PORT=`*new-port-number*
   The default start port number of the SNMP agent is 22161.

4. Save the `/opt/CM2/APM/bin/apmstart` file, and then close it.

Next steps

Next, start the Monitoring Agent again.

Related topics

- (4) Setting the community name
- 1.6.6 Restarting the Monitoring Agent (for Linux)

1.6.6 Restarting the Monitoring Agent (for Linux)

After the setup of ESA is complete on the Monitoring Agent for Linux, restart ESA and SSO - AP to apply the settings.

Procedure

1. Execute the `apmstop` command of SSO - AP to stop SSO - AP.

2. Execute the `snmpstart` command of ESA to start ESA.

3. Execute the `apmstart` command of SSO - AP to start SSO - AP.

4. Execute the `snmpcheck` command of ESA to check the ESA status.
   If all statuses are in the running status, there is no problem.

5. Execute the `apmcheck` command of SSO - AP to check the SSO - AP status.
   If all statuses are in the running status, there is no problem.

Next steps

Next, specify settings for monitoring the network.

Related topics

- 1.2.4 Storage location of the commands of each product
- 2. Configuring JP1 Network Management Products

2 Configuring JP1 Network Management Products

This chapter describes how you (the system build engineer) access NNMi or SSO to start network management.

2.1 General procedure for configuring JP1 network management products

The following table shows the general procedure for configuring JP1 network management products.

Task overview	Step	Task details	Reference
Configuring NNMi	1	Access NNMi.	2.2.1
	2	Register users.	2.2.3
	3	Configure communication protocols.	2.2.4
	4	Discover a network.	2.2.5
	5	Configure node groups.	2.2.6
	6	Configure monitoring.	2.2.7
	7	Configure incidents.	2.2.8
Configuring SSO	8	Access SSO.	2.3.1
	9	Configure resource collection.	2.3.2
	10	Configure the monitoring of processes and services.	2.3.3

2.2 Configuring NNMi

2.2.1 Accessing NNMi

In the following procedure, from the Web browser, you access NNMi and start setup.

Before you begin

Configure the following Web browser settings:

- Allow pop-up windows to open (disable the pop-up blocker).
- Enable active scripting, and allow cookies to be saved.
- If IE ESC is enabled in Internet Explorer, add `about:blank` to **Trusted sites**.

Procedure

1. From the Web browser, access NNMi.
   URL: `http://`*host-name*`:`*port-number*`/nnm/`
   - *host-name*: Specify the host name (FQDN) of the server on which you installed NNMi. You can also specify the IP address.
   - *port-number*: Specify the port number of the Web server specified during installation of NNMi.

   The NNMi Sign in window is displayed.

2. Enter the user name and password.
   Sign in by using the system account.
   User name: `system`
   Password: Password for the system account

3. Click **Sign in**.
   The NNMi console is displayed.

   > **Important**
   >
   > The user name of the system account is fixed to `system`. The `system` account is used for initial settings and maintenance work. We recommend not using this account during normal operations because the password for the account can be changed by using a command.

Next steps

You have now successfully signed in to NNMi. In the next section, you will learn basic operations while configuring NNMi.

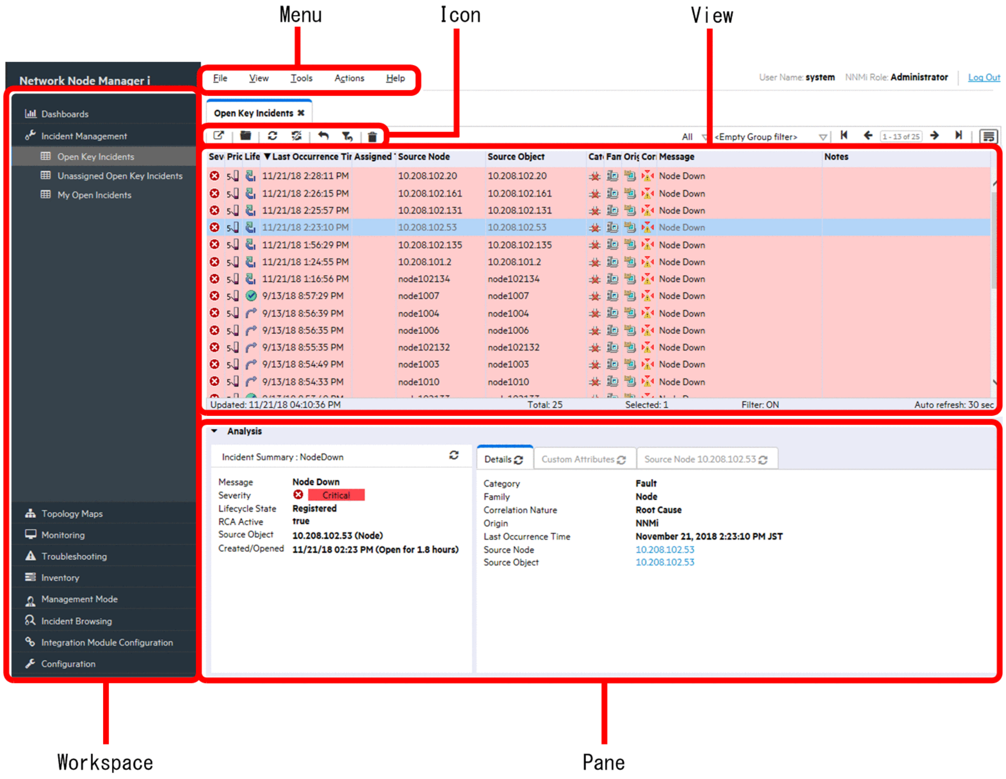
Related topics

- 1.3.4 Setting up NNMi (for Windows)
- 1.4.3 Setting up NNMi (for Linux)
- 2.1 General procedure for configuring JP1 network management products

2.2.2 About the NNMi console

If you access NNMi, the NNMi console is displayed. Use the NNMi console to become familiar with basic operations. You can use the console as you like because the settings are not changed until you click 💾 (Save), ☒ (Save and Close), or 🗑 (Delete).

From the NNMi console, you can use icons to view information and specify definitions. Place the cursor on an icon to display a description of the icon.



Sev	Pric	Life	▼Last Occurrence Tir	Assigned '	Source Node	Source Object	Cat	Fan	Orig	Cor	Message	Notes
	5		11/21/18 2:28:11 PM		10.208.102.20	10.208.102.20					Node Down	
	5		11/21/18 2:26:15 PM		10.208.102.161	10.208.102.161					Node Down	
	5		11/21/18 2:25:57 PM		10.208.102.131	10.208.102.131					Node Down	
	5		11/21/18 2:23:10 PM		10.208.102.53	10.208.102.53					Node Down	
	5		11/21/18 1:56:29 PM		10.208.102.135	10.208.102.135					Node Down	
	5		11/21/18 1:24:55 PM		10.208.101.2	10.208.101.2					Node Down	
	5		11/21/18 1:16:56 PM		node102134	node102134					Node Down	
	5	✓	9/13/18 8:57:29 PM		node1007	node1007					Node Down	
	5		9/13/18 8:56:39 PM		node1004	node1004					Node Down	
	5		9/13/18 8:56:35 PM		node1006	node1006					Node Down	
	5		9/13/18 8:55:35 PM		node102132	node102132					Node Down	
	5		9/13/18 8:54:49 PM		node1003	node1003					Node Down	
	5		9/13/18 8:54:33 PM		node1010	node1010					Node Down	

Updated: 11/21/18 04:10:36 PM Total: 25 Selected: 1 Filter: ON Auto refresh: 30 sec

Message	Node Down
Severity	Critical
Lifecycle State	Registered
RCA Active	true
Source Object	10.208.102.53 (Node)
Created/Opened	11/21/18 02:23 PM (Open for 1.8 hours)

Category	Fault
Family	Node
Correlation Nature	Root Cause
Origin	NNMi
Last Occurrence Time	November 21, 2018 2:23:10 PM JST
Source Node	10.208.102.53
Source Object	10.208.102.53

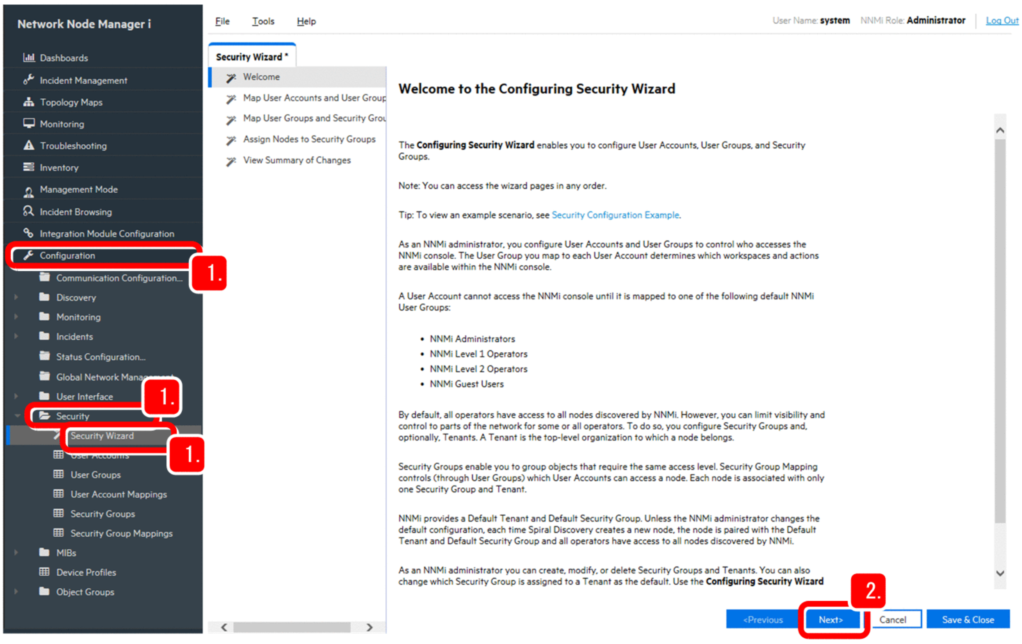
Clicking the **Help** menu displays the topic related to the window on which you are performing operations. From this topic, you can immediately check what you want to know about setup items, such as the number and type of specifiable characters.

2.2.3 Registering users

Create user accounts for the system administrator and supervisor operator to register users. First create a user account for the system administrator, and sign in again as that user. Then, create a user account for the supervisor operator.

Procedure

1. In the **Configuration** workspace, select **Security** and then **Security Wizard**.



Welcome to the Configuring Security Wizard

The **Configuring Security Wizard** enables you to configure User Accounts, User Groups, and Security Groups.

Note: You can access the wizard pages in any order.

Tip: To view an example scenario, see Security Configuration Example.

As an NNMi administrator, you configure User Accounts and User Groups to control who accesses the NNMi console. The User Group you map to each User Account determines which workspaces and actions are available within the NNMi console.

A User Account cannot access the NNMi console until it is mapped to one of the following default NNMi User Groups:

- NNMi Administrators
- NNMi Level 1 Operators
- NNMi Level 2 Operators
- NNMi Guest Users

By default, all operators have access to all nodes discovered by NNMi. However, you can limit visibility and control to parts of the network for some or all operators. To do so, you configure Security Groups and, optionally, Tenants. A Tenant is the top-level organization to which a node belongs.

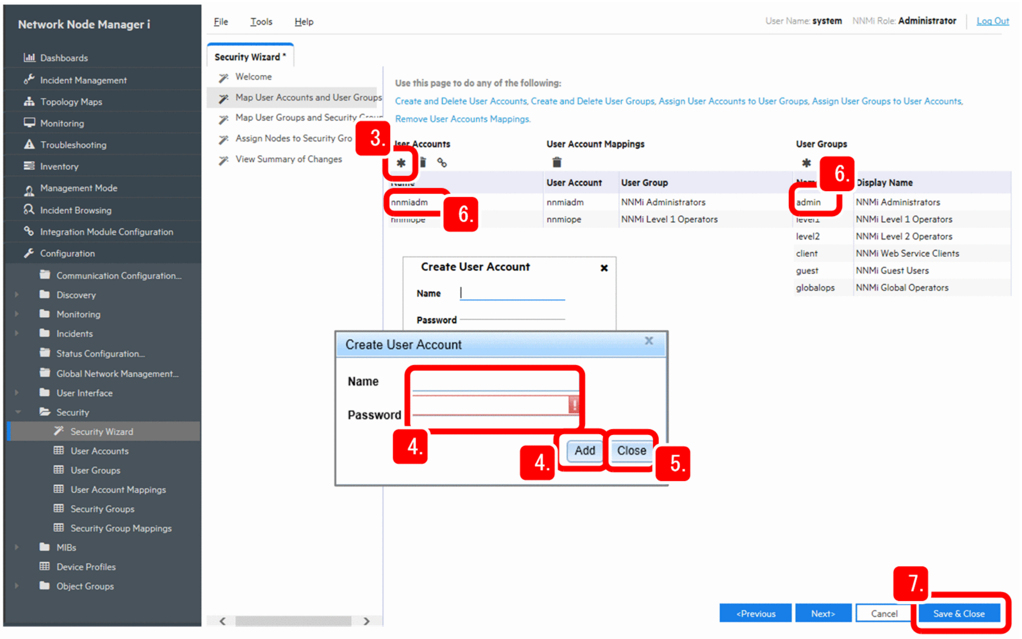
Security Groups enable you to group objects that require the same access level. Security Group Mapping controls (through User Groups) which User Accounts can access a node. Each node is associated with only one Security Group and Tenant.

NNMi provides a Default Tenant and Default Security Group. Unless the NNMi administrator changes the default configuration, each time Spiral Discovery creates a new node, the node is paired with the Default Tenant and Default Security Group and all operators have access to all nodes discovered by NNMi.

As an NNMi administrator you can create, modify, or delete Security Groups and Tenants. You can also change which Security Group is assigned to a Tenant as the default. Use the **Configuring Security Wizard**

2. Read the description under **Welcome to the Configuration Security Wizard**, and then click **Next** at the bottom of the window.

3. In the **User Accounts** field, click ✱ (Create User Account).



Use this page to do any of the following:

Create and Delete User Accounts, Create and Delete User Groups, Assign User Accounts to User Groups, Assign User Groups to User Accounts, Remove User Accounts Mappings.

User Accounts

Name
nnmiadm
nnmiope

User Account Mappings

User Account	User Group
nnmiadm	NNMi Administrators
nnmiope	NNMi Level 1 Operators

User Groups

Name	Display Name
admin	NNMi Administrators
level1	NNMi Level 1 Operators
level2	NNMi Level 2 Operators
client	NNMi Web Service Clients
guest	NNMi Guest Users
globalops	NNMi Global Operators

4. Enter the values in **Name** and **Password**, and then click **Add**.

   The user account is created.

   Example:

   System administrator Name: `nnmiadm`, password: `password`

   Supervisor operator Name: `nnmiope`, password: `password`

5. After adding the user, click **Close**.

6. Select the user account that you created, and then click the user group to which you want to assign the user.
   Example:
   nnmiadm: System administrator
   nnmiope: Supervisor operator

7. Click **Save & Close**.

8. In the confirmation dialog box, click **OK**.
   The user account is configured.

> **Note**
>
> What to do if you forgot the password:
>
> For details about how to reset the password for a user account, see the topic *Change user name and password of Configure user accounts* in the *Help for Administer*.
>
> To reset the password for the system account, use the `nnmchangesyspw.ovpl` command. If you want to change the password for a user account, you can change the password for the current user by clicking the **File** menu and then **Change Password**.

Next steps

You have now successfully registered users. In the **Configuration** workspace, select **Security**, and then **User Account Mappings,** to make sure that the created user accounts are displayed.

Related topics

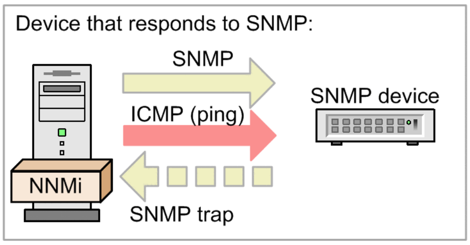
- 1.3.4 Setting up NNMi (for Windows)
- 1.4.3 Setting up NNMi (for Linux)
- 2.2.4 Configuring communication protocols

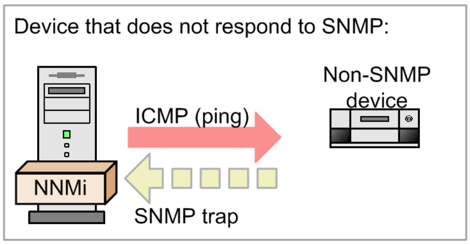
2.2.4 Configuring communication protocols

NNMi uses SNMP and ICMP (`ping`) to discover and monitor devices, and receives SNMP traps (notifications of problems).

Before you begin

Devices are classified into SNMP devices that respond to SNMP and non-SNMP devices that do not respond to SNMP.





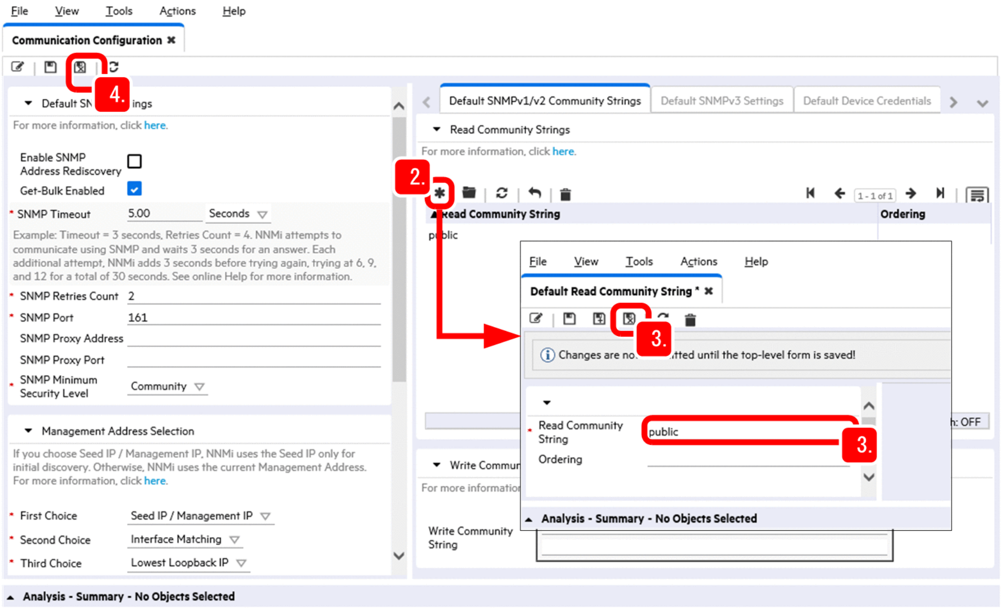
In the following procedure, you can configure the behavior of communication protocols SNMP and ICMP (`ping`) that NNMi uses to discover and monitor networks. In the procedure, the settings below are used as an example. Change the setting values as necessary.

- Settings for the timeout and the number of retries for SNMP and ICMP: Default (do not change)
- SNMP Minimum Security Level: Default (do not change)
- Read Community Strings: `public`

Procedure

1. In the **Configuration** workspace, select **Communication Configuration**.

2. In the **Default SNMPv1/v2 Community Strings** tab, click ✱ (New).


File
View
Tools
Actions
Help
Communication Configuration ✖
4.
Default SN ings
2.
Default SNMPv1/v2 Community Strings
Default SNMPv3 Settings
Default Device Credentials
Read Community Strings
1 - 1 of 1
Read Community String
Ordering
File
View
Tools
Actions
Help
Default Read Community String * ✖
3.
3.
h: OFF
Write Commun
Analysis - Summary - No Objects Selected
Analysis - Summary - No Objects Selected

For more information, click here.

Enable SNMP Address Rediscovery ☐

Get-Bulk Enabled ☑

* SNMP Timeout 5.00 Seconds

Example: Timeout = 3 seconds, Retries Count = 4. NNMi attempts to communicate using SNMP and waits 3 seconds for an answer. Each additional attempt, NNMi adds 3 seconds before trying again, trying at 6, 9, and 12 for a total of 30 seconds. See online Help for more information.

* SNMP Retries Count 2

* SNMP Port 161

SNMP Proxy Address

SNMP Proxy Port

* SNMP Minimum Security Level Community

Management Address Selection

If you choose Seed IP / Management IP, NNMi uses the Seed IP only for initial discovery. Otherwise, NNMi uses the current Management Address. For more information, click here.

* First Choice Seed IP / Management IP

* Second Choice Interface Matching

* Third Choice Lowest Loopback IP

For more information, click here.

public

Changes are no itted until the top-level form is saved!

* Read Community String public

Ordering

For more informatio

Write Community String

3. Enter the value in **Read Community Strings**, and then click (Save and Close).

   Example: Read Community Strings: `public`

   If a network to be monitored uses multiple community strings, repeat steps 2 and 3 to specify those community strings. NNMi checks the community strings configured in the network in parallel, and uses the appropriate value.

4. In the **Communication Configuration** view, make sure that the configured settings are displayed, and then click (Save and Close).

   The configured settings are saved.

Next steps

You have now successfully configured the communication protocols. Next, you will perform network discovery in the network to be monitored.

Related topics

- 2.2.5 Performing network discovery

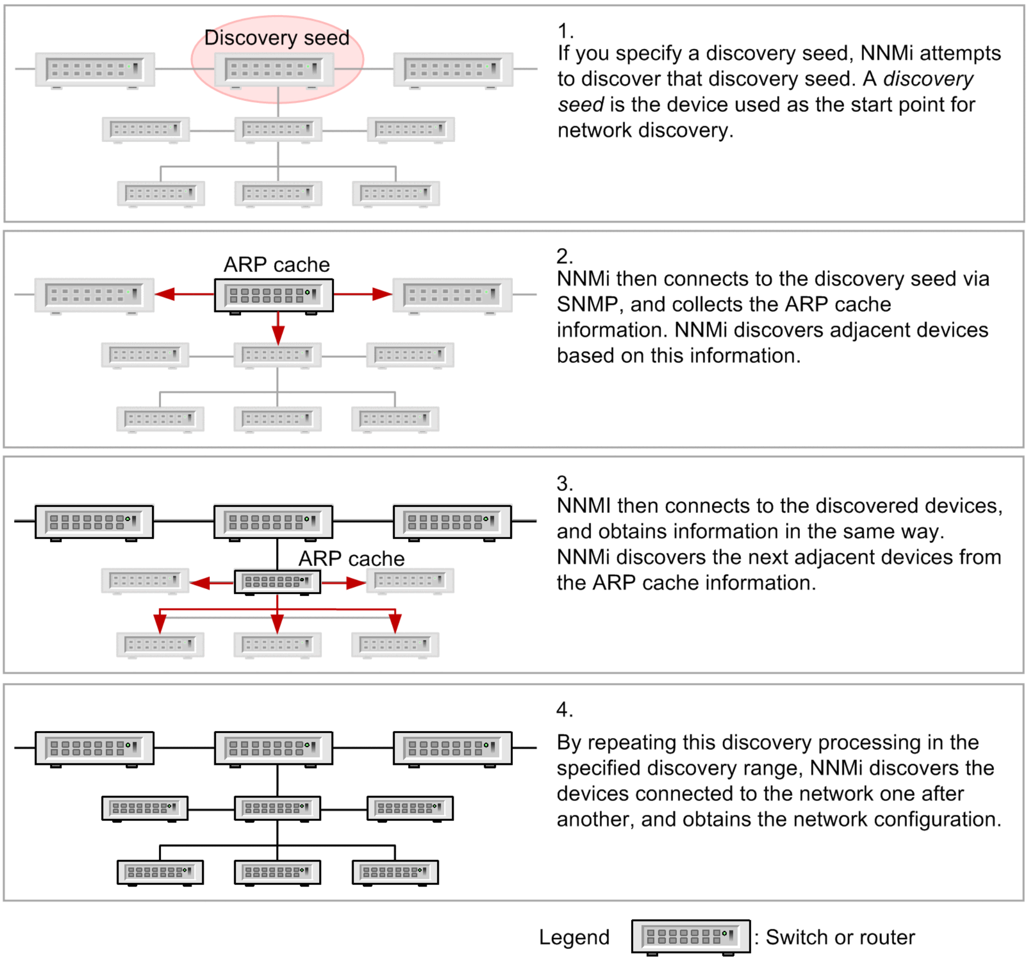
2.2.5 Performing network discovery

NNMi collects information from devices on a network, and obtains the details of individual devices and the network configuration (topology).

(1) About network discovery

NNMi discovers details of the entire network by collecting via SNMP, ARP cache information of each device and information about adjacent devices recognized by a protocol such as LLDP.

The following description uses an example of network discovery using an ARP cache.



1\.
If you specify a discovery seed, NNMi attempts to discover that discovery seed. A *discovery seed* is the device used as the start point for network discovery.

2\.
NNMi then connects to the discovery seed via SNMP, and collects the ARP cache information. NNMi discovers adjacent devices based on this information.

3\.
NNMI then connects to the discovered devices, and obtains information in the same way. NNMi discovers the next adjacent devices from the ARP cache information.

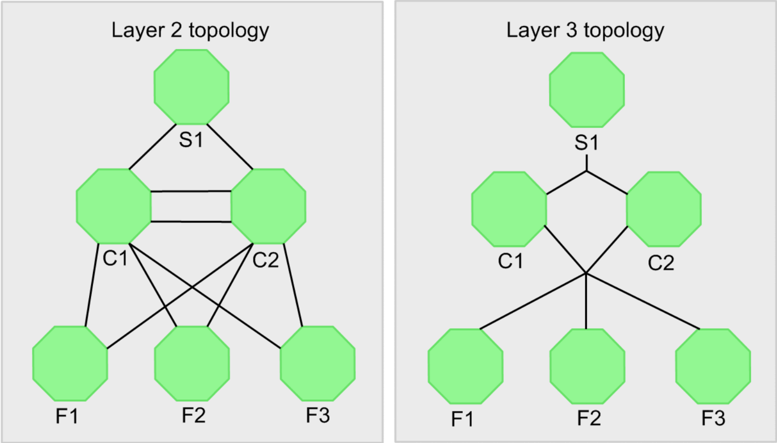
4\.
By repeating this discovery processing in the specified discovery range, NNMi discovers the devices connected to the network one after another, and obtains the network configuration.

Note

NNMi can perform network discovery by using a `ping` sweep. The `ping` sweep method monitors a specified range of IP addresses by using ICMP (`ping`), and discovers devices that return a response. This method can be used to promptly discover devices in the specified network range, but it places a load on the network. Use a `ping` sweep that matches your operations. We recommend that you limit the target range when using a `ping` sweep.

(2) Layer 2 and Layer 3 topologies

NNMi can recognize and display the network topology (the network configuration) by using not only a Layer 3 topology but also a Layer 2 topology. By recognizing a Layer 2 topology (physical connection lines), you can analyze the causes of network problems in more detail.



Layer 2 topology

This topology displays a network configuration by using physical connection lines.

To check the connection lines between switches and terminals at the ends of a network, use a Layer 2 topology. By using it together with a Layer 3 topology, you can intuitively check the situation when a failure occurs, and understand the range affected by the failure.

Layer 3 topology

This topology displays a logical network configuration by using IP addresses.

To check the logical configuration of a core network, use a Layer 3 topology.

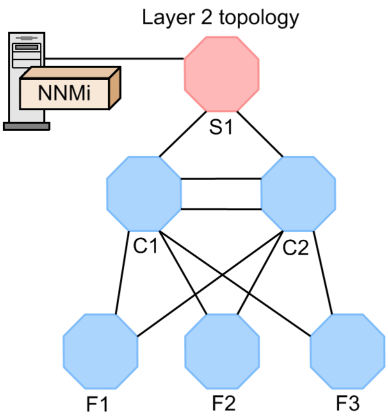
Tip

Layer 2 and Layer 3 are the terms that are used in the OSI seven-layer model.

- Layer 2 (data link layer): Controls data transfer between physical links by using MAC addresses.
- Layer 3 (network layer): Controls selection of routes in a network by using IP addresses.

For IP network communications or when configuring NNMi, you specify destinations by using IP addresses, and generally you do not need to be conscious of physical connections. NNMi recognizes physical connection lines, the Layer 2 topology, by collecting and analyzing MIB information about adjacent devices.

The following figure provides an example of displaying a Layer 2 topology when a failure occurs in the switch (S1) to which NNMi is connected to, and NNMi cannot communicate with the network beyond the switch.



If you attempt to determine the failure by using connections through IP addresses (Layer 3 topology) only, it will be determined that network failures occurred over a wide range because communication is unavailable for many devices. However, by recognizing physical connection lines provided by the Layer 2 topology map, you can determine the switch where the failure occurred, and determine the devices where communication is unavailable because of that failure.

(3) Specifying how to perform network discovery

You can discover network devices connected to the monitored network. Before you start network discovery, the system administrator needs to complete configuration of the Monitoring Agent.

Before you begin

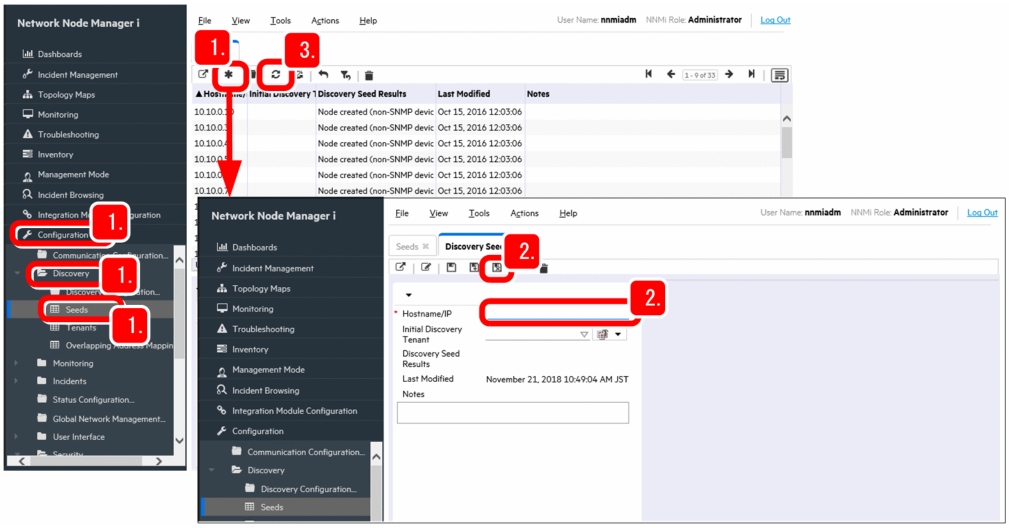
To perform network discovery, you can use a method that performs network discovery automatically, or a method that performs network discovery of explicitly specified items. You can also use these methods in combination. The following table describes these methods, and gives examples of operations.

Discovery method	Description	Example of operation
Automatic discovery	In this method, NNMi automatically discovers devices according to the auto-discovery rules you specified.	• You want to automatically discover the changes in a network. • There are many devices connected to a large-scale network.
Discovery of explicitly specified items	In this method, you explicitly specify a device as a discovery seed.	• You want to strictly specify the targets to be managed. • The network configuration is fixed.

The following procedure describes how to discover explicitly specified items.

Procedure

1. In the **Configuration** workspace, click **Discovery** and **Seeds**, and then click ✱ (New).



2. Enter the IP address of the discovery seed in **Hostname/IP**, and click ☒ (Save and Close).

   The discovery processing immediately starts for the specified discovery seed.
   For the device to be set as a discovery seed, specify a router that supports SNMP and has much information about adjacent devices.

3. Click 🔄 (Refresh).

   Make sure that the specified discovery seed has been created.

Note

You can also use the `nnmloadseeds.ovpl` command as shown below to register discovery seeds in a batch operation.

To directly specify seeds:

Example: `nnmloadseeds.ovpl -n 192.168.8.82 192.168.100.24`

To specify a list of seeds:

Example: `nnmloadseeds.ovpl -f c:\jp1\seeds.txt`

Example of describing a seed file:

```
192.168.8.82 # node1
192.168.100.24 # node2
```

For details about the `nnmloadseeds.ovpl` command, see the topic displayed by selecting the **Help** menu, **NNMi Documentation Library**, **Reference Pages**, and then **nnmloadseeds.ovpl**.

Tip

If you want to perform network discovery automatically, in the **Configuration** workspace, select **Discovery Configuration** and then **Auto-Discovery Rules**. Also, when specifying **IP Ranges**, if you specify the IP addresses that you do not want to discover and set the range type to **Ignored by rule**, the IP addresses are excluded from discovery.

Use the operation of selecting **Discovery Configuration** and then **Excluded IP Addresses** only when excluding specific IP addresses from the discovered nodes. If you use this operation to specify nodes to be excluded from monitoring, the IP addresses might disappear while the nodes still remain. Use the method appropriate for your usage.

For details about automatic discovery, see the topic *Setting up auto-discovery rules* in the *JP1/Network Node Manager i Setup Guide*.

Related topics

- 1.2.4 Storage location of the commands of each product

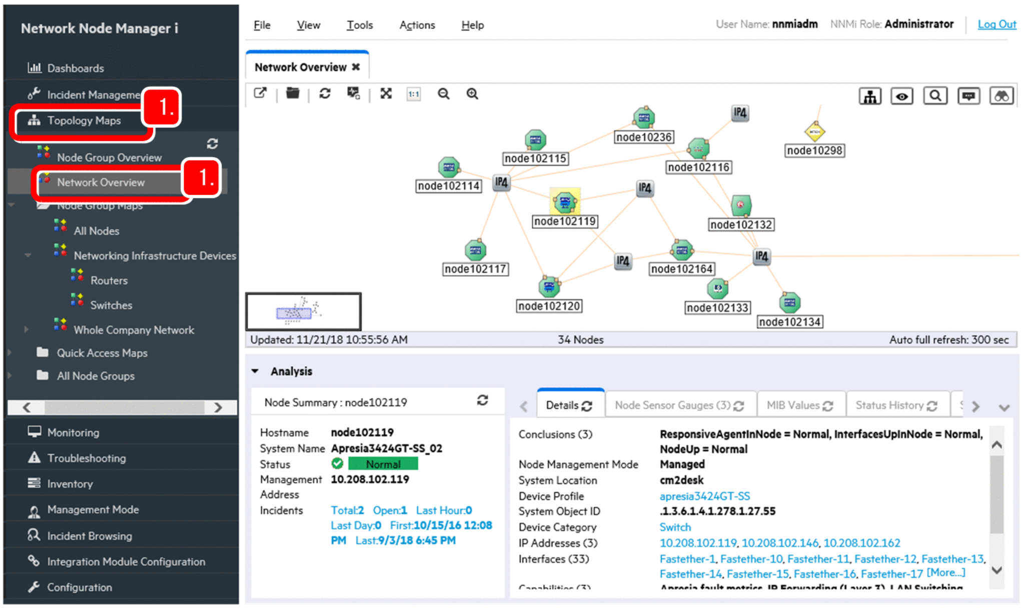
(4) Checking the discovered network and devices

You can view a discovered network by using a topology map. Immediately after you configure the discovery settings, you can view the process of node discovery.

Procedure

1. Click the **Topology Maps** workspace and then **Network Overview**.

   In the **Network Overview** view, check the network status.



Updated: 11/21/18 10:55:56 AM 34 Nodes Auto full refresh: 300 sec

Node Summary : node102119

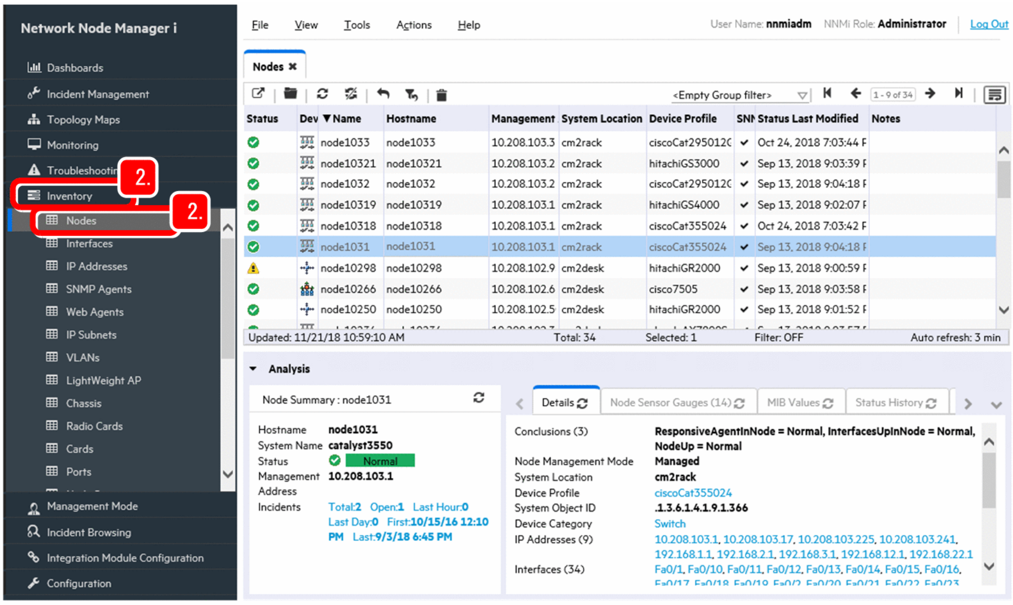
Hostname node102119
System Name Apresia3424GT-SS_02
Status Normal
Management Address 10.208.102.119
Incidents Total:2 Open:1 Last Hour:0 Last Day:0 First:10/15/16 12:08 PM Last:9/3/18 6:45 PM

Conclusions (3) ResponsiveAgentInNode = Normal, InterfacesUpInNode = Normal, NodeUp = Normal
Node Management Mode Managed
System Location cm2desk
Device Profile apresia3424GT-SS
System Object ID .1.3.6.1.4.1.278.1.27.55
Device Category Switch
IP Addresses (3) 10.208.102.119, 10.208.102.146, 10.208.102.162
Interfaces (33) Fastether-1, Fastether-10, Fastether-11, Fastether-12, Fastether-13, Fastether-14, Fastether-15, Fastether-16, Fastether-17 [More...]
Capabilities (3) Apresia fault metrics, IP Forwarding (Layer 3), LAN Switching

2. Click the **Inventory** workspace and then **Nodes**.

   Make sure that the devices that you specified as discovery targets are discovered and registered correctly. If the specified devices are displayed, the network discovery has been performed successfully.

   Check **Device Category** and **Device Profile** to check what devices have been discovered.



User Name: nnmiadm NNMi Role: Administrator

Status	Dev	▼Name	Hostname	Management	System Location	Device Profile	SNI	Status Last Modified	Notes
✓		node1033	node1033	10.208.103.3	cm2rack	ciscoCat295012C	✓	Oct 24, 2018 7:03:44 F	
✓		node10321	node10321	10.208.103.2	cm2rack	hitachiGS3000	✓	Sep 13, 2018 9:03:39 F	
✓		node1032	node1032	10.208.103.2	cm2rack	ciscoCat295012C	✓	Sep 13, 2018 9:04:18 F	
✓		node10319	node10319	10.208.103.1	cm2rack	hitachiGS4000	✓	Sep 13, 2018 9:02:07 F	
✓		node10318	node10318	10.208.103.1	cm2rack	ciscoCat355024	✓	Oct 24, 2018 7:03:42 F	
✓		node1031	node1031	10.208.103.1	cm2rack	ciscoCat355024	✓	Sep 13, 2018 9:04:18 F	
⚠		node10298	node10298	10.208.102.9	cm2desk	hitachiGR2000	✓	Sep 13, 2018 9:00:59 F	
✓		node10266	node10266	10.208.102.6	cm2desk	cisco7505	✓	Sep 13, 2018 9:03:58 F	
✓		node10250	node10250	10.208.102.5	cm2desk	hitachiGR2000	✓	Sep 13, 2018 9:01:52 F	

Updated: 11/21/18 10:59:10 AM Total: 34 Selected: 1 Filter: OFF Auto refresh: 3 min

Node Summary : node1031

Hostname	node1031
System Name	catalyst3550
Status	✓ Normal
Management Address	10.208.103.1
Incidents	Total:2 Open:1 Last Hour:0 Last Day:0 First:10/15/16 12:10 PM Last:9/3/18 6:45 PM

Conclusions (3)	ResponsiveAgentInNode = Normal, InterfacesUpInNode = Normal, NodeUp = Normal
Node Management Mode	Managed
System Location	cm2rack
Device Profile	ciscoCat355024
System Object ID	.1.3.6.1.4.1.9.1.366
Device Category	Switch
IP Addresses (9)	10.208.103.1, 10.208.103.17, 10.208.103.225, 10.208.103.241, 192.168.1.1, 192.168.2.1, 192.168.3.1, 192.168.12.1, 192.168.22.1
Interfaces (34)	Fa0/1, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/2, Fa0/20, Fa0/21, Fa0/22, Fa0/23

Tip

If a node in a cluster system is included in the monitored targets, specify the logical IP address as an excluded IP address so that it is not monitored. If you do not configure this setting, a problem occurs if the node is deleted or the status of a different node is applied when the logical IP address is moved. For details, see the *Release Notes*.

Note

If a node that does not need to be monitored is discovered, you can either delete the node from the monitored targets or exclude it from the monitored targets.

To delete the node from the monitored targets:

In the **Topology Maps** workspace, select **Network Overview** and then the icon for the node that you want to delete. Note that if the node is specified as a discovery seed, the node is not removed from the list displayed in the **Seeds** view even if you delete it. Delete the discovery seed.

To exclude the node from the monitored targets:

In the **Inventory** workspace, select **Nodes** and then the target node. Select **Actions**, **Management Mode**, and **Note Managed**. Use this method if you do not want to delete the node from a map, or want to temporarily exclude the node from monitoring.

Related topics

- (5) Deleting the discovery seeds for which discovery is complete

(5) Deleting the discovery seeds for which discovery is complete

After the network discovery is complete, delete the discovery seeds.

Procedure

1. In the **Configuration** workspace, click **Discovery** and then **Seeds**.

2. Select all discovery seeds, and then click 🗑 (Delete).

   To select multiple rows, click the rows while pressing the **Ctrl** key.

3. Verify that the discovery seeds have been deleted.

Next steps

You have now successfully performed network discovery. In the next section, you will configure node groups.

Related topics

- 2.2.6 Configuring node groups

2.2.6 Configuring node groups

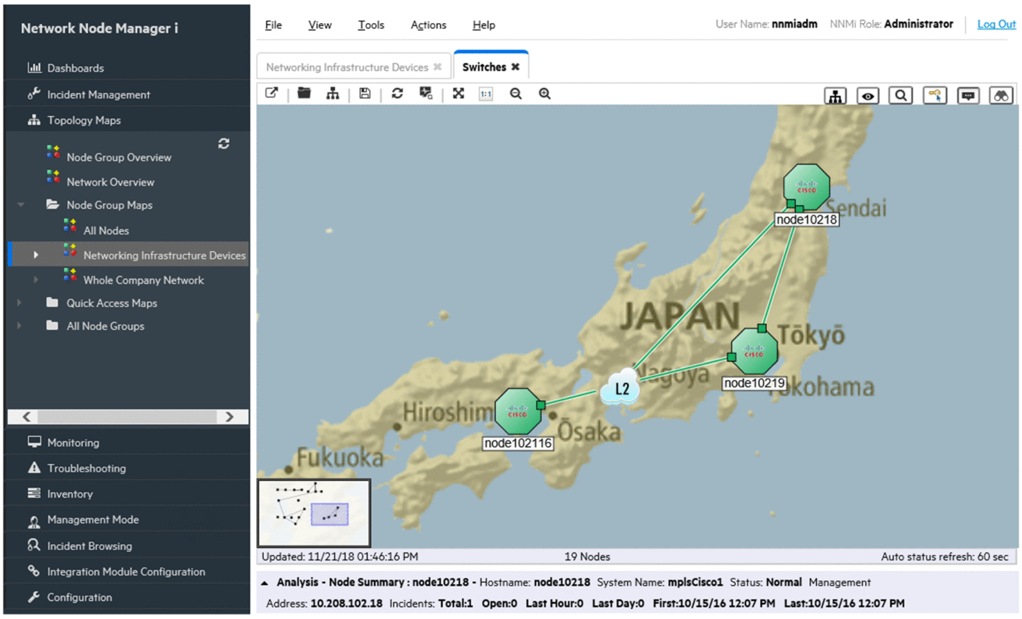
By defining node groups, you can configure monitoring settings and perform filtering for each node group. You can also display any of the defined node groups as the initial screen of the NNMi console.

(1) About node groups

A *node group* is a collection of discovered network devices that are put into a group in a hierarchy, based on conditions such as IP address or device type. NNMi provides, as standard, node groups for which appropriate settings are configured for each of basic categories, such as Windows or routers. You can classify a node group into six hierarchies by defining child node groups.

You can also create a map (a node group map) that displays discovered network devices by dividing them into categories. By creating and using a node group map, you can understand the network configuration from a more focused viewpoint than by using a topology map. You can find the location in which a problem occurred more easily, and check the details immediately.

Node Group Map



Updated: 11/21/18 01:46:16 PM 19 Nodes Auto status refresh: 60 sec

Analysis - Node Summary : node10218 - Hostname: **node10218** System Name: **mplsCisco1** Status: **Normal** Management Address: **10.208.102.18** Incidents: **Total:1 Open:0 Last Hour:0 Last Day:0 First:10/15/16 12:07 PM Last:10/15/16 12:07 PM**

You can freely configure the background image of a node group map by using an image file. By customizing the display method to suit your purpose by, for example, setting the floor layout image, you can manage networks more effectively.

How to use the Important Nodes node group

In NNMi, the *Important Nodes* node group is configured as standard. You can register important servers and network devices to the Important Nodes node group.

If no reply is received from a registered important node, a `NodeDown` incident is issued for the device. If you have particular nodes for which you want incidents reported whenever those nodes do not respond, even when they are not the root cause of a failure, register the nodes as Important Nodes.

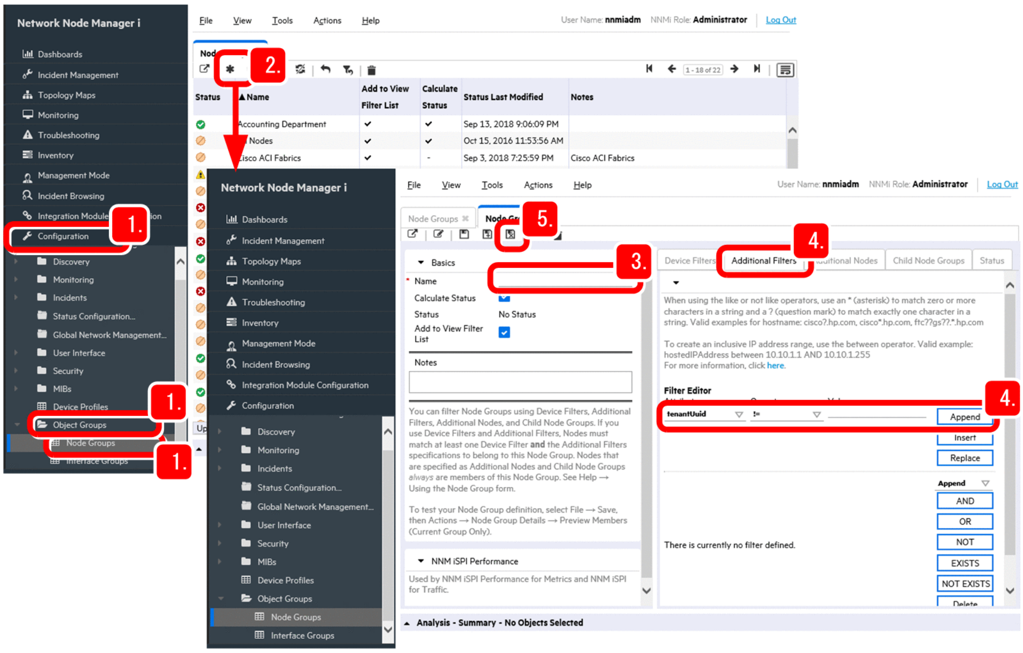
An incident is also issued when child node groups are put into a hierarchy and configured in the Important Nodes node group or a node that is included in another node group is added to the Important Nodes group.

(2) Configuring a node group

By configuring a node group, you can freely group discovered nodes regardless of the network configuration. The following procedure describes how to specify the attribute values to configure a node group.

Procedure

1. In the **Configuration** workspace, click **Object Groups** and then **Node Groups**.



Status	▲Name	Add to View Filter List	Calculate Status	Status Last Modified	Notes
✓	Accounting Department	✓	✓	Sep 13, 2018 9:06:09 PM	
⊘	Nodes	✓	✓	Oct 15, 2016 11:53:56 AM	
⊘	isco ACI Fabrics	✓	-	Sep 3, 2018 7:25:59 PM	Cisco ACI Fabrics

You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter **and** the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups *always* are members of this Node Group. See Help → Using the Node Group form.

To test your Node Group definition, select File → Save, then Actions → Node Group Details → Preview Members (Current Group Only).

Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.

When using the like or not like operators, use an * (asterisk) to match zero or more characters in a string and a ? (question mark) to match exactly one character in a string. Valid examples for hostname: cisco?.hp.com, cisco*.hp.com, ftc??gs??.*.hp.com

To create an inclusive IP address range, use the between operator. Valid example: hostedIPAddress between 10.10.1.1 AND 10.10.1.255
For more information, click here.

There is currently no filter defined.

2. Click ✱ (New).

3. Specify the name of the node group in **Name**.
   Example: Name: `System division`

   If you select the **Add to View Filter List** check box, the name of the node group to be created is displayed in the **Nodes** view, and in the **Empty Group filter** of the **Incidents** view.

4. In the **Additional Filters** tab, specify the conditions for nodes to be added to the node group.
   Select the values in the **Attribute** and **Operator** fields, and enter a value in **Value**, and then click **Append**.

   Example: Attribute: `hostedIPAddress`, Operator: `between`, Value: `10.208.102.2` to `10.208.102.254`

The specified conditional expression is added to **Filter String**. To delete a conditional expression, select it, and then click **Delete**.

Tip

You can specify the range of IP addresses, device category, and installation location as grouping conditions. You can also specify flexible conditions by using SQL operators (such as between, in, and like). A node group can have a maximum of six hierarchical levels. You can use a node group as follows:

- To define a node group map: Select **Node Group Maps**.
- To adjust the monitoring method for each node group: Select **Monitoring Configuration** and then **Node Settings**.
- To monitor performance for each node group: Select **Monitoring**, **Custom Poller Configuration**, and **Custom Poller Policy**.

5. Click (Save and Close).

   The **Node Groups** view closes, and the node group is created.

6. Select and right-click the row of the created node group, and then click **Node Group Details** and **Show Members (Include Child Groups)**.
   Make sure that the nodes that you specified as targets are included in the node group.

7. Right-click the desired node group, and select **Maps** and then **Node Group Maps**.
   The node group is displayed in a map format.

Note

NNMi provides various grouping conditions other than those that are set by using operators. The following table describes the tabs used to set grouping conditions, and provides examples of operations.

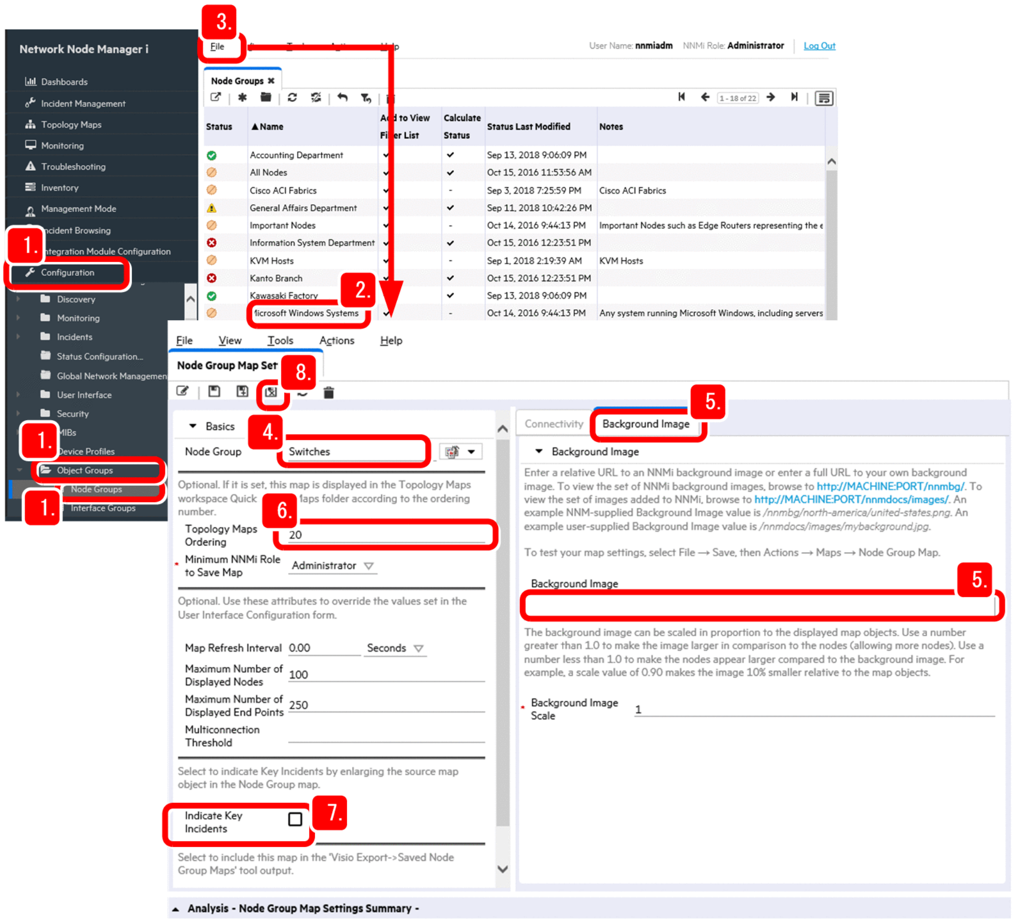
Tab for configuring the settings	Setup item	Example of operation
Device Filters	• Device Category • Device Vendor and others	• Perform monitoring according to the importance of devices. • Set an appropriate monitoring method for each model. • Understand the situation immediately by reducing conditions so that, for example, only routers are displayed.
Additional Filters	• hostedIPAddress (IP address) • sysLocation (location) and others	Set monitoring conditions and filter the displayed items for each installation location or organization.
Additional Nodes	Node Hostname	• Set particularly important nodes individually. • Set the nodes for which it is difficult to specify conditions.
Child Node Groups	Child Node Group (Set in the hierarchy order)	Put node groups into a hierarchy for each workplace or region

(3) Configuring a node group map

By configuring a node group map, you can specify an image for the background image. You can also display the created node group map in the list of map names under the **Topology Maps** workspace.

Procedure

1. In the **Configuration** workspace, click **Object Groups** and then **Node Groups**.



User Name: **nnmiadm** NNMi Role: **Administrator** Log Out

1 - 18 of 22

Status	▲Name	Add to View Filter List	Calculate Status	Status Last Modified	Notes
✓	Accounting Department	✓	✓	Sep 13, 2018 9:06:09 PM	
⊘	All Nodes	✓	✓	Oct 15, 2016 11:53:56 AM	
⊘	Cisco ACI Fabrics	✓	-	Sep 3, 2018 7:25:59 PM	Cisco ACI Fabrics
⚠	General Affairs Department	✓	✓	Sep 11, 2018 10:42:26 PM	
⊘	Important Nodes	✓	-	Oct 14, 2016 9:44:13 PM	Important Nodes such as Edge Routers representing the e
☒	Information System Department	✓	✓	Oct 15, 2016 12:23:51 PM	
⊘	KVM Hosts	✓	-	Sep 1, 2018 2:19:39 AM	KVM Hosts
☒	Kanto Branch	✓	✓	Oct 15, 2016 12:23:51 PM	
✓	Kawasaki Factory	✓	✓	Sep 13, 2018 9:06:09 PM	
⊘	licrosoft Windows Systems	✓	-	Oct 14, 2016 9:44:13 PM	Any system running Microsoft Windows, including servers

Node Group: Switches

Optional. If it is set, this map is displayed in the Topology Maps workspace Quick laps folder according to the ordering number.

Topology Maps Ordering: 20

Minimum NNMi Role to Save Map: Administrator

Optional. Use these attributes to override the values set in the User Interface Configuration form.

Map Refresh Interval: 0.00 Seconds

Maximum Number of Displayed Nodes: 100

Maximum Number of Displayed End Points: 250

Multiconnection Threshold:

Select to indicate Key Incidents by enlarging the source map object in the Node Group map.

Indicate Key Incidents □

Select to include this map in the 'Visio Export->Saved Node Group Maps' tool output.

Enter a relative URL to an NNMi background image or enter a full URL to your own background image. To view the set of NNMi background images, browse to http://MACHINE:PORT/nnmbg/. To view the set of images added to NNMi, browse to http://MACHINE:PORT/nnmdocs/images/. An example NNM-supplied Background Image value is */nnmbg/north-america/united-states.png*. An example user-supplied Background Image value is */nnmdocs/images/mybackground.jpg*.

To test your map settings, select File → Save, then Actions → Maps → Node Group Map.

Background Image:

The background image can be scaled in proportion to the displayed map objects. Use a number greater than 1.0 to make the image larger in comparison to the nodes (allowing more nodes). Use a number less than 1.0 to make the nodes appear larger compared to the background image. For example, a scale value of 0.90 makes the image 10% smaller relative to the map objects.

Background Image Scale: 1

2. Select the node group whose map you want to configure, right-click it to display the menu, and then click **Maps** and **Node Group Maps**.

3. From the **File** menu, click **Open Node Group Map Settings**.

4. From the **Node Group** pull-down menu, select the node group whose map you want to configure.

5. In the **Background Image** tab, specify the background image for the map in **Background Image**.

   Enter the value in **Background Image** as follows:

   Example: `/nnmdocs/images/`*image-file-name*

   You can specify a `.gif`, `.png`, or `.jpg` file that can be displayed in the Web browser. Store the image file in the following folder for the Monitoring Manager:

   - For Windows

     installation-data-folder`\shared\nnm\www\htdocs\images`

   - For Linux

```
/var/opt/OV/shared/nnm/www/htdocs/images
```

6. Specify a value in **Topology Maps Ordering**.

   By specifying the value, you can configure the created node group to be displayed in **Quick Access Maps** under the **Topology Maps** workspace. The created node group is displayed after you complete the setting and sign in to NNMi again.

7. Select the **Indicate Key Incidents** check box.

   If you select the check box, the icons in the map are enlarged if a key incident occurs, and you can easily find the location where the problem occurred.

8. After you complete the setting, click 💾 (Save and Close).

9. Adjust the icon positions, and then click 💾 (Save Map).

   The icon positions are saved.

Next steps

You have now successfully configured the node group map. In the next section, configure monitoring definitions.

Related topics

- 2.2.7 Configuring monitoring settings

2.2.7 Configuring monitoring settings

NNMi periodically monitors devices discovered by network discovery.

(1) About monitoring

Monitoring is a process to periodically monitor whether nodes on a discovered network work properly. NNMi monitors target devices by using SNMP or ICMP (`ping`). By default, monitoring is performed at five-minute intervals to check the status of the targets.

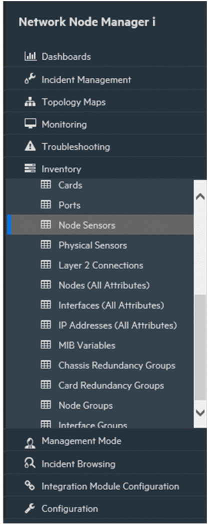
The following table describes the relationship between the settings for communication, discovery, and monitoring, and communication protocols SNMP and ICMP (`ping`).

Target of configuration	Description	Location for configuring the setting	Setup item	Default value
Protocol behavior	Configure the timeout and retry count per communication for SNMP or ICMP (`ping`). Communications for discovery and monitoring are performed based on these settings.	Select the **Configuration** workspace and then **Communication Configuration**.	SNMP	Five minutes (two retries)
			ICMP (`ping`)	
Behavior during network discovery	Configure the setting so that rediscovery is performed on a daily basis because generally the configuration of a network is not changed frequently.	Select the **Configuration** workspace, **Discovery**, and **Discovery Configuration**.	Sweep Interval	One day

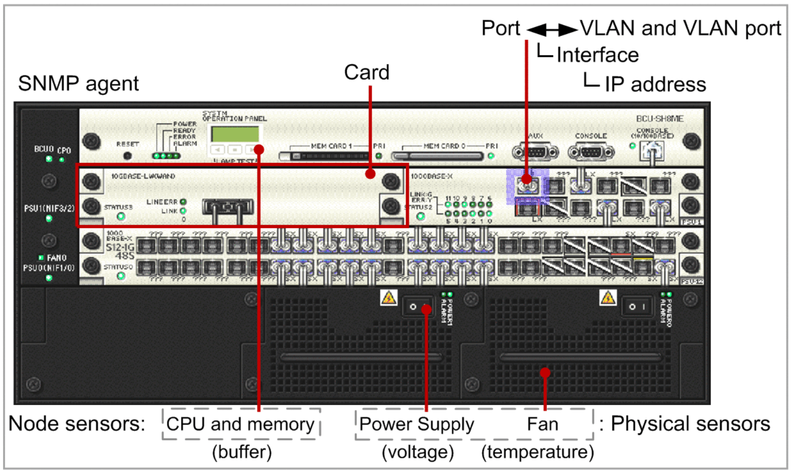
Target of configuration	Description	Location for configuring the setting	Setup item	Default value
Behavior during network monitoring	Configure the setting so that monitoring is performed in a short cycle to immediately discover a failure. However, configure the setting so that polling is performed in minutes to keep a proper monitoring load.	Select the **Configuration** workspace, **Monitoring**, and **Monitoring Configuration**.	Fault Polling Interval	Five minutes

Items that can be monitored by NNMi are displayed in the **Inventory** view. The following figure shows the correspondence between the items monitored by NNMi and a device.

Display example of the items monitored by NNMi



Nodes: The most severe outstanding result is applied to the status.



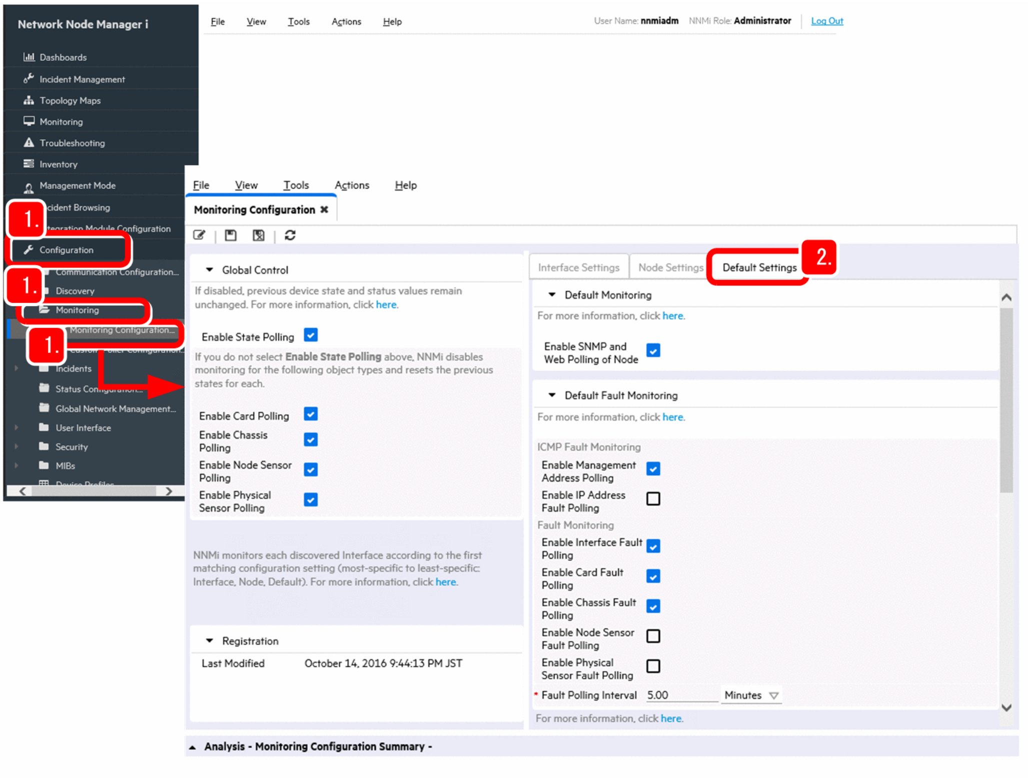
Interfaces, **SNMP Agents**, **Cards**, **Node Sensors**, and **Physical Sensors** are monitored via SNMP. **IP Addresses** are monitored via ICMP (ping).
Other items are pieces of information used to manage the configuration, and grouped information.

(2) Viewing monitoring definitions and checking the monitoring method

NNMi provides monitoring definitions as standard to help you immediately start monitoring. Therefore, you do not need to change the settings unless you want to customize the monitoring method or polling interval. In the following procedure, you will view the standard monitoring definitions, and check the monitoring method.

Procedure

1. In the **Configuration** workspace, select **Monitoring** and then **Monitoring Configuration**.



Monitoring Configuration

Global Control

If disabled, previous device state and status values remain unchanged. For more information, click here.

Enable State Polling ☑

If you do not select **Enable State Polling** above, NNMi disables monitoring for the following object types and resets the previous states for each.

Enable Card Polling ☑
Enable Chassis Polling ☑
Enable Node Sensor Polling ☑
Enable Physical Sensor Polling ☑

NNMi monitors each discovered Interface according to the first matching configuration setting (most-specific to least-specific: Interface, Node, Default). For more information, click here.

Registration

Last Modified October 14, 2016 9:44:13 PM JST

Default Monitoring

For more information, click here.

Enable SNMP and Web Polling of Node ☑

Default Fault Monitoring

For more information, click here.

ICMP Fault Monitoring
Enable Management Address Polling ☑
Enable IP Address Fault Polling □

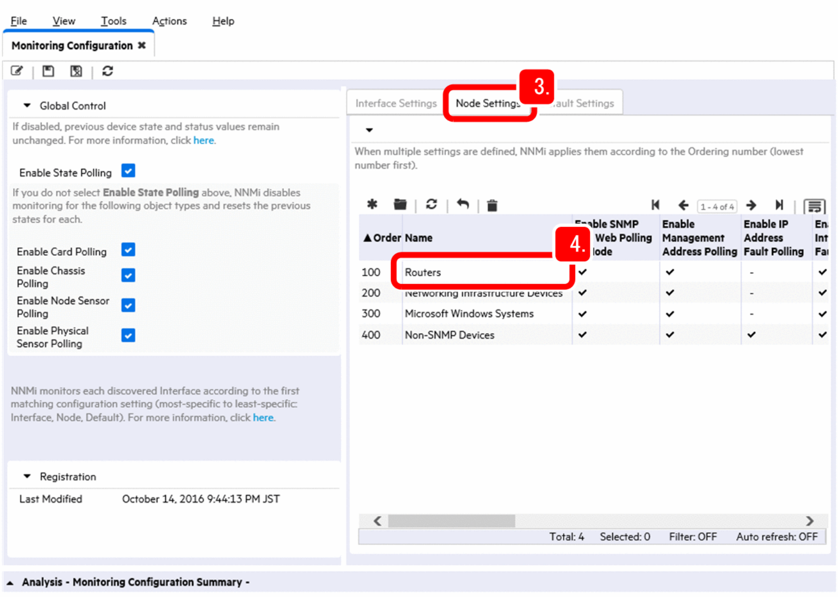
Fault Monitoring
Enable Interface Fault Polling ☑
Enable Card Fault Polling ☑
Enable Chassis Fault Polling ☑
Enable Node Sensor Fault Polling □
Enable Physical Sensor Fault Polling □
* Fault Polling Interval 5.00 Minutes

For more information, click here.

2. Select the **Default Settings** tab.
   The default monitoring settings are displayed.
   Check the settings such as the targets to be monitored and the number of minutes set for the monitoring interval.

3. Select the **Interface Settings** tab or the **Node Settings** tab to view the monitoring definitions.
   In the **Node Settings** tab, the following definitions are specified:

   - Routers
   - Networking infrastructure devices
   - Microsoft Windows systems
   - Non-SNMP devices



Global Control

If disabled, previous device state and status values remain unchanged. For more information, click here.

Enable State Polling ☑

If you do not select **Enable State Polling** above, NNMi disables monitoring for the following object types and resets the previous states for each.

Enable Card Polling ☑

Enable Chassis Polling ☑

Enable Node Sensor Polling ☑

Enable Physical Sensor Polling ☑

NNMi monitors each discovered Interface according to the first matching configuration setting (most-specific to least-specific: Interface, Node, Default). For more information, click here.

Registration

Last Modified October 14, 2016 9:44:13 PM JST

When multiple settings are defined, NNMi applies them according to the Ordering number (lowest number first).

▲Order	Name	able SNMP Web Polling lode	Enable Management Address Polling	Enable IP Address Fault Polling	En Int Fa
100	Routers	✓	✓	-	✓
200	Networking Infrastructure Devices	✓	✓	-	✓
300	Microsoft Windows Systems	✓	✓	-	✓
400	Non-SNMP Devices	✓	✓	✓	✓

Total: 4 Selected: 0 Filter: OFF Auto refresh: OFF

Analysis - Monitoring Configuration Summary -

4. Double-click a monitoring definition item.

   Monitoring definitions for the item are displayed.

   An appropriate monitoring method is defined for each node type. Check and compare the difference in monitoring targets and monitoring interval among the methods.

Next steps

You have now successfully checked the default monitoring definitions. In the next section, you will configure incidents.

Related topics

- (3) Items configured in monitoring definitions
- 2.2.8 Configuring incidents

(3) Items configured in monitoring definitions

NNMi provides, as standard, appropriate monitoring definitions as the settings for monitoring networks. Monitoring definitions define the type and cycle of polling performed during monitoring. By using these monitoring definitions, you can start network monitoring in an appropriate method immediately after installing NNMi.

You can configure the monitoring method in the **Monitoring Configuration** view. The following table describes the main monitoring definition items that can be defined.

Location for configuring the setting	Monitoring definition item	Description
Global Control field	Enable State Polling	Selecting this item monitors the operating status of SNMP agents, interfaces, and IP addresses. • SNMP agents: Monitored via SNMP • Interfaces: Monitored via SNMP • IP addresses: Monitored via ICMP (`ping`).
	Enable Card Polling#	Selecting this item monitors the status of cards via SNMP.
	Enable Chassis Polling#	Selecting this item monitors the status of the chassis via SNMP.

Location for configuring the setting	Monitoring definition item	Description
Global Control field	Enable Physical Sensor Polling#	Selecting this item monitors the status of physical sensors via SNMP.
Default Settings tab	Enable Management Address Polling	Selecting this item monitors the IP addresses that are classified as management addresses via ICMP (`ping`). A management address is used by NNMi to communicate with the SNMP agent in its node.
	Enable IP Address Fault Polling	Selecting this item monitors IP addresses via ICMP (`ping`).
	Enable Interface Fault Polling	Selecting this item monitors the status of interfaces via SNMP.
	Enable Card Fault Polling#	Selecting this item monitors the status of cards via SNMP.
	Enable Chassis Fault Polling#	Selecting this item monitors the status of the chassis via SNMP.
	Enable Physical Sensor Fault Polling#	Selecting this item monitors the status of physical sensors via SNMP.
	Fault Polling Interval	Specify the interval for status monitoring.
Node Settings tab	Networking Infrastructure Devices	Core devices in the network are monitored. Not only SNMP devices but also components (fans, power supplies, etc.) are configured as targets to be monitored.
	Non-SNMP Devices	Devices that do not respond to SNMP are automatically managed as non-SNMP devices. They are configured to be monitored via ICMP (`ping`), and therefore their active status can be monitored. If a non-SNMP device becomes able to respond to SNMP, it is managed via SNMP.

#: Cards, chassis, and physical sensors can be monitored only in specific models supported by NNMi.

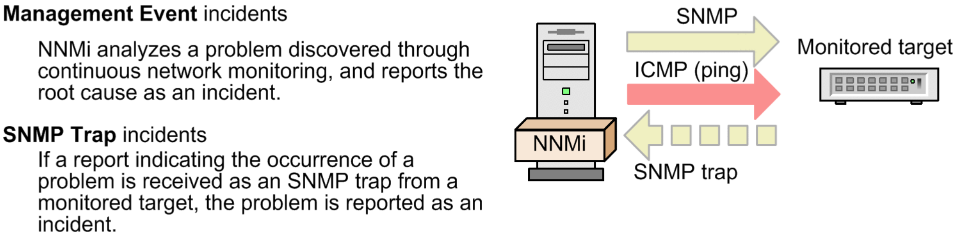
2.2.8 Configuring incidents

NNMi analyzes problems discovered during monitoring and SNMP traps by using the functionality for resolving root causes, and if the root cause is identified, NNMi reports the cause as an incident.

(1) About incidents

An incident is network-related information with high importance that needs to be reported to the administrator. NNMi monitors a network, detects events that have occurred, analyzes them by using the functionality for analyzing root causes, and then reports only the incidents that the administrator needs to know about.

An incident is reported as a result of root cause analysis performed based on the information obtained through network monitoring via SNMP and ICMP (`ping`) and from problem reports by SNMP traps.



Management Event incidents

NNMi analyzes a problem discovered through continuous network monitoring, and reports the root cause as an incident.

SNMP Trap incidents

If a report indicating the occurrence of a problem is received as an SNMP trap from a monitored target, the problem is reported as an incident.

NNMi provides, as standard, definitions for approximately 150 types of incidents, including **Management Event** incidents and **SNMP Trap** incidents, which are configured as incident definitions corresponding to this network monitoring. These incident definitions correspond to various events, and therefore you can use them without change for operation.

For example, the information below is configured in the **Management Event** incidents as incidents that occur when a node goes down. The functionality for analyzing root causes analyzes the status, and reports the appropriate one from the incidents.

- NodeDown (The node is down.)
- NodeOrConnectionDown (The node or connection is down.)

As one of the operation methods, you can include a node in the Important Nodes node group. Monitor a `NodeDown` incident that is issued if an important node does not respond.

Examples of issued incidents

The table below provides examples of incidents that are generated when the node of a network device is down and stopped. The functionality for analyzing root causes reports only the root cause events as incidents.

To minimize the impact of a failure during the operation of a network, NNMi provides the following approaches to appropriately handle all incidents without omission.

Functionality	Description	Reference
Automatic action for incidents	You can configure the setting so that actions are automatically performed according to the lifecycle state of incidents.	2.2.8(4)
Failure monitoring through incidents	If an incident is generated, it is reported and displayed on the NNMi console. You can check the details by switching the windows between Topology Maps and Incident Browsing.	3.1
Incident lifecycle management	NNMi manages the progress of handling of an incident by lifecycle states.	4.2

You need to configure incidents in order to use the above functionality.

Related topics

- 2.2.6 Configuring node groups
- (4) Configuring automatic actions for an incident
- 3.1 Network monitoring by using JP1 network management products
- 4.2 Troubleshooting mechanism

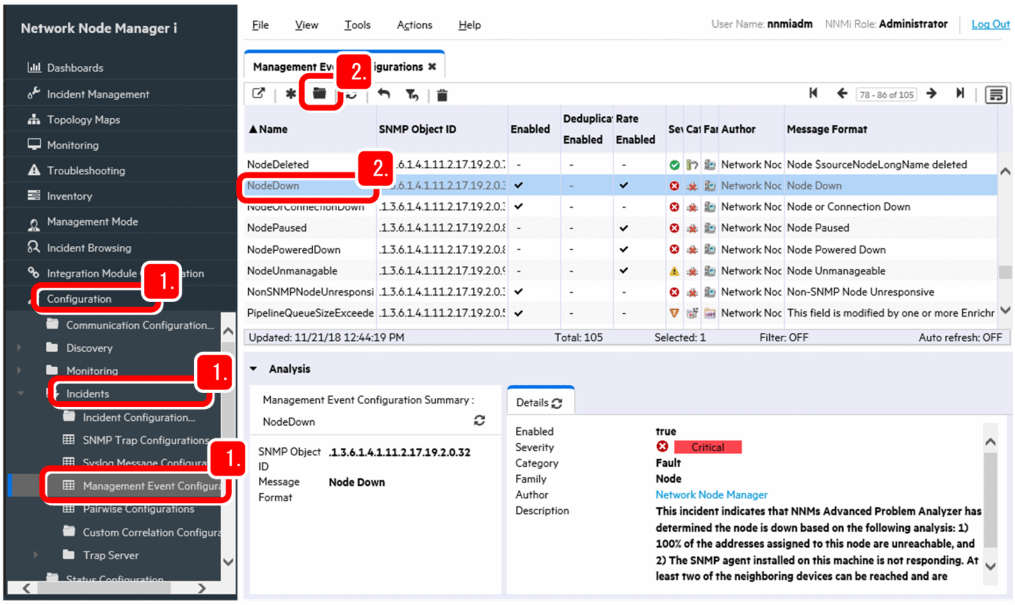
(2) Checking the details of incident settings

The JP1 network management products provide pre-configured standard incident settings usable for operations. In the following procedure, you will view the incident settings provided as standard, and check the basic items.

Procedure

1. In the **Configuration** workspace, click **Incidents** and then **SNMP Trap Configurations** or **Management Event Configurations**.

   To check the incidents caused by SNMP traps, select **SNMP Trap Configurations**. To check the incidents detected by NNMi network monitoring, select **Management Event Configurations**.



User Name: **nnmiadm** NNMi Role: **Administrator**

▲Name	SNMP Object ID	Enabled	Deduplication Enabled	Rate Enabled	Sev	Cat	Fam	Author	Message Format
NodeDeleted	.6.1.4.1.11.2.17.19.2.0.:	-	-	-	✓			Network Noc	Node $sourceNodeLongName deleted
NodeDown	.6.1.4.1.11.2.17.19.2.0.:	✓	-	✓	⊗			Network Noc	Node Down
NodeOrConnectionDown	.1.3.6.1.4.1.11.2.17.19.2.0.:	✓	-	-	⊗			Network Noc	Node or Connection Down
NodePaused	.1.3.6.1.4.1.11.2.17.19.2.0.8	-	-	✓	⊗			Network Noc	Node Paused
NodePoweredDown	.1.3.6.1.4.1.11.2.17.19.2.0.8	-	-	✓	⊗			Network Noc	Node Powered Down
NodeUnmanagable	.1.3.6.1.4.1.11.2.17.19.2.0.9	-	-	✓	⚠			Network Noc	Node Unmanageable
NonSNMPNodeUnresponsi	.1.3.6.1.4.1.11.2.17.19.2.0.:	✓	-	-	⊗			Network Noc	Non-SNMP Node Unresponsive
PipelineQueueSizeExceede	.1.3.6.1.4.1.11.2.17.19.2.0.5	✓	-	-	▽			Network Noc	This field is modified by one or more Enrichr

Updated: 11/21/18 12:44:19 PM Total: 105 Selected: 1 Filter: OFF Auto refresh: OFF

Management Event Configuration Summary :
NodeDown

SNMP Object ID **.1.3.6.1.4.1.11.2.17.19.2.0.32**
Message Format **Node Down**

Enabled **true**
Severity ⊗ Critical
Category **Fault**
Family **Node**
Author Network Node Manager
Description **This incident indicates that NNMs Advanced Problem Analyzer has determined the node is down based on the following analysis: 1) 100% of the addresses assigned to this node are unreachable, and 2) The SNMP agent installed on this machine is not responding. At least two of the neighboring devices can be reached and are**

2. Click the row of the incident that you want to check, and then click 📁 (Open).

The details of the incident configurations are displayed. As examples, check the following **Management Event** incidents that are generated when a node goes down.

- NodeDown (The node is down.)
- NodeOrConnectionDown (The node or connection is down.)

The meaning of the incident is displayed in **Description**.

Result

Check the details of incidents to deepen your understanding. If necessary, configure the incident for an SNMP trap, and set up automatic actions for the incident.

(3) Configuring SNMP trap incidents

Some network devices might provide SNMP trap definitions as an extended MIB file to report the occurrence of a failure by using an SNMP trap. NNMi provides many incident definitions for SNMP traps as standard, but you can also load a vendor-specific extended MIB file for a device such as a network device, and configure incident definitions for SNMP traps that are unique for the device. General MIB files contain MIB definitions and SNMP trap definitions. For details about MIB files for each vendor, see the vendor's manual. Many MIBs have already been loaded during installation of NNMi. You can view a list of loaded MIBs by selecting the **Configuration** workspace, **MIBs**, and **Loaded MIBs**.

Before you begin

To receive an SNMP trap, the following conditions must be met. If the conditions are not met, the trap is discarded.

- The incident that corresponds to the SNMP trap is configured. In addition, the **Enabled** check box is selected.
- The source node that issued the SNMP trap is discovered. In addition, the management mode of the node is set to **Managed**.

For details, see the topic *Manage SNMP Traps* in the *Help for Administer*. If you want to receive SNMP traps from a node that has not been discovered, see the topic *Manage unresolved incoming SNMP traps* in the *Help for Administer*.

Procedure

1. Execute the `nnmloadmib.ovpl` command of NNMi.

   Example of specification: `nnmloadmib.ovpl -load` *MIB-file-name*

   Executing this command loads the contents of the MIB file to NNMi. Specify the MIB file to be loaded for the `-load` option.

2. Execute the `nnmincidentcfg.ovpl` command of NNMi.

   Example of specification: `nnmincidentcfg.ovpl -loadTraps` *MIB-module-name*

   Executing this command creates the incident configuration from the MIB database of NNMi.

   Specify the MIB module name defined in the MIB file for the `-loadTraps` option.

3. In the **Configuration** workspace, click **Incidents** and then **SNMP Trap Configurations**.

   You can check the status of SNMP traps.

> **Note**
>
> You can also use the `nnmtrapdump.ovpl` command to check the status of SNMP traps.
>
> Example:
>
> `nnmtrapdump.ovpl -source` *IP-address*
>
> Executing this command displays traps received from the IP address.
>
> `nnmtrapdump.ovpl -t`
>
> Executing this command continuously displays received traps. Use the command when you check the configuration.
>
> For details, see the topic *SNMP Traps view* in the *Help for Operators*, and information displayed by clicking the **Help** menu, **NNMi Documentation Library**, **Reference Pages**, and **nnmtrapdump.ovpl**.

> **Note**
>
> To find the MIB module name, open the MIB file, and check the area around the top of the file. The name defined before `DEFINITIONS ::= BEGIN` is the MIB module name.
>
> Example:
>
> Example of a MIB module name
>
> ```
> ------ MIB Simple Sample
> SAMPLE-MIB DEFINITIONS ::= BEGIN
> ```
>
> In this example, the MIB module name is `SAMPLE-MIB`.

Related topics

- 1.2.4 Storage location of the commands of each product

(4) Configuring automatic actions for an incident

If you configure automatic actions for an incident, you can execute a specified command under a specific lifecycle state.

Context

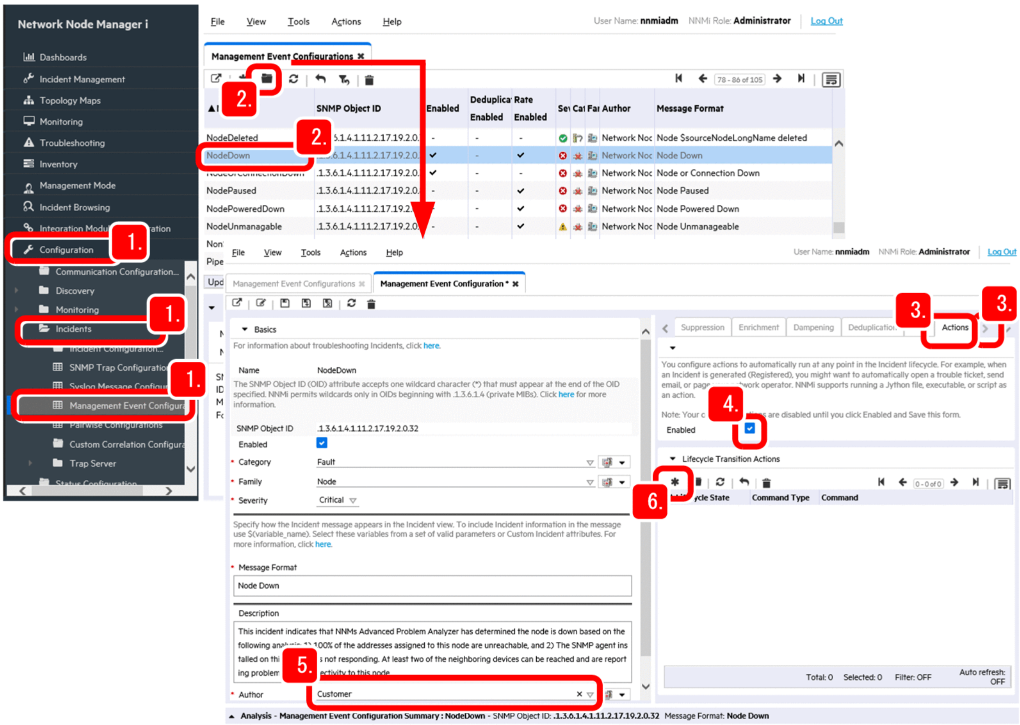
Note

By linking to JP1/IM, you can send an email when a failure occurs and use a signal light.

Procedure

1. In the **Configuration** workspace, click **Incidents** and then **SNMP Trap Configurations** or **Management Event Configurations**.

   To configure automatic actions for incidents caused by SNMP traps, select **SNMP Trap Configurations**. To configure automatic actions for incidents detected by NNMi network monitoring, select **Management Event Configurations**.



2. Click the row of the incident that you want to configure automatic actions, and then click 📁 (Open).

3. Switch the tab display by clicking >, and if the **Actions** tab is displayed, click it.

Tip

If you want to configure different automatic actions for each node, you can specify conditions for each node by configuring the settings from the following tabs:

- The **Actions** tab in the **Interface Settings** tab: You can specify conditions for each interface group.
- The **Actions** tab in the **Node Settings** tab: You can specify conditions for each node group.
- The **Actions** tab: The target is not limited.

> The order of priority is the **Interface Settings** tab, the **Node Settings** tab, and the general **Actions** tab, from highest to lowest. Actions are performed only once because the action settings configured from a tab with a higher priority overwrite the settings configured from a tab with a lower priority. Therefore, for example, you can configure automatic actions for all nodes, and then different automatic actions for a specific node group.
>
> For details, see the topic *Configure Incidents* in the *Help for Administer*.

4. Select the **Enabled** check box.

   If you omit this setting, automatic actions are not performed even if an incident occurs.

5. Set **Author** to **Customer**.

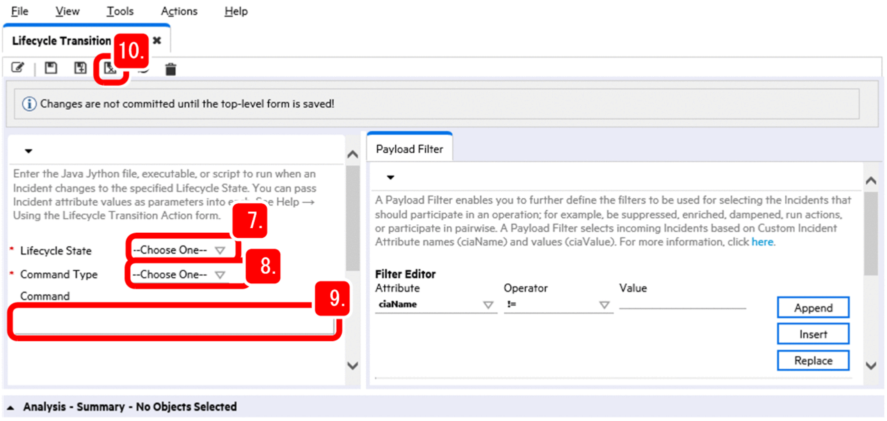
   The user needs to change the author to **Customer** before changing incident definitions.

6. Under **Lifecycle Transition Actions** on the **Actions** tab, click ✱ (New).

7. Select the timing for executing automatic actions in **Lifecycle State**.

   Specify the setting as follows, depending on the timing you want to execute automatic actions:

   - **Registered**: When a failure is detected and an incident is issued, an automatic action is executed.
   - **In Progress**: When **Lifecycle State** becomes **In Progress**, such as when a person responsible for handling is assigned to an incident, or when an incident is investigated, an automatic action is executed.
   - **Completed**: When handling of the failure is completed and **Lifecycle State** becomes **Completed**, an automatic action is executed.
   - **Closed**: When NNMi detects that the failure has been solved and **Lifecycle State** becomes **Closed**, an automatic action is executed. For example, if you want a node to link with the report system when the node restarts after recovery, specify **Closed**.



Changes are not committed until the top-level form is saved!

Enter the Java Jython file, executable, or script to run when an Incident changes to the specified Lifecycle State. You can pass Incident attribute values as parameters into [illegible] See Help → Using the Lifecycle Transition Action form.

* Lifecycle State: --Choose One--

* Command Type: --Choose One--

Command:

A Payload Filter enables you to further define the filters to be used for selecting the Incidents that should participate in an operation; for example, be suppressed, enriched, dampened, run actions, or participate in pairwise. A Payload Filter selects incoming Incidents based on Custom Incident Attribute names (ciaName) and values (ciaValue). For more information, click here.

Filter Editor

Attribute	Operator	Value
ciaName	!=	

8. Select a command type in **Command Type**.

   To specify the `Jython` command, select **Jython**. To specify an execution file or a batch file, select **ScriptOrExecutable**.

9. Enter a command in **Command**.

   If the command type is **ScriptOrExecutable**, enter a command that can be executed on the OS, and for which necessary parameters are specified.

   Example:

```
msg.exe Administrator "Incident $name occurred at $sourceNodeName."
```

For details about how to enter commands whose command type is `Jython`, see the topic *Configure an action for an incident* in the *Help for Administer*.

10. Click (Save and Close).

11. In the **SNMP Trap Configurations** view or **Management Event Configurations** view, click (Save and Close).
    The settings are saved.

> **Tip**
>
> To check the execution status of automatic actions, click the **Tools** menu and then **Incident Actions Log**. You can also check the status by using the following log file:
>
> - For Windows
>   *NNMi-installation-data-folder*`\log\nnm\incidentActions.*.*.log`
> - For Linux
>   `/var/opt/OV/log/nnm/public/incidentActions.*.*.log`
>
> If you fail to select the **Enabled** check box of the action settings, automatic actions are not executed and the history is not output to the log file. If automatic actions are not performed, make sure that the **Enabled** check box is selected. For details, see the topic *Configure Incidents* in the *Help for Administer*.

Next steps

You have now successfully configured automatic actions for incidents. In the next section, access and configure SSO.

Related topics

- 2.3 Configuring SSO

2.3 Configuring SSO

To secure stable system operation, you must check the server status. With SSO, you can check the detailed server status by using the resource collection functionality and the processes and services monitoring functionality.

2.3.1 Accessing SSO

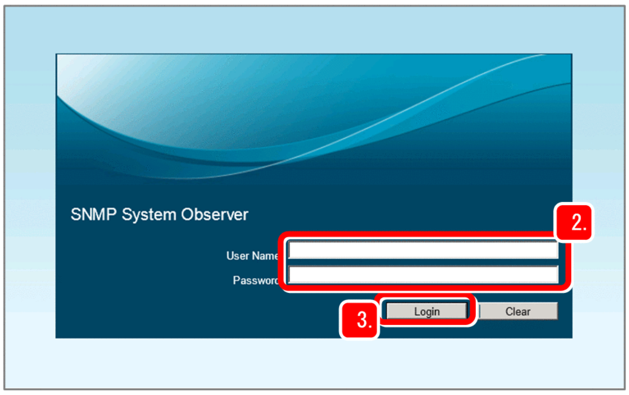
In this procedure you log in to SSO, and start configuring SSO.

Procedure

1. From the Web browser, access SSO.
   `http://`*host-name*`:`*port-number*`/SSOConsole/`

   For *host-name*, enter the host name of the Monitoring Manager. The default port number is `20393`.

2. Enter the user name and password.
   For *user-name* and *password*, enter the values that you set in the SSO definition information.



3. Click **Login**.
   The SSO console is displayed.

> **Note**
>
> You can also display the SSO console by selecting the Windows **Start** menu, **Programs and Features**, **SNMP System Observer**, and **SSO**.

Next steps

You have now successfully logged in to SSO. In the next section, configure the settings to collect resources by using SSO.

Related topics

- (2) Setting the SSO definition information for NNMi
- 2.3.2 Resource collection

2.3.2 Resource collection

By using SSO, you can collect system resources from servers by installing an SNMP agent (ESA) on monitored servers. If you configure the time zone, interval, and period, you can collect resources at regular intervals, and view them.

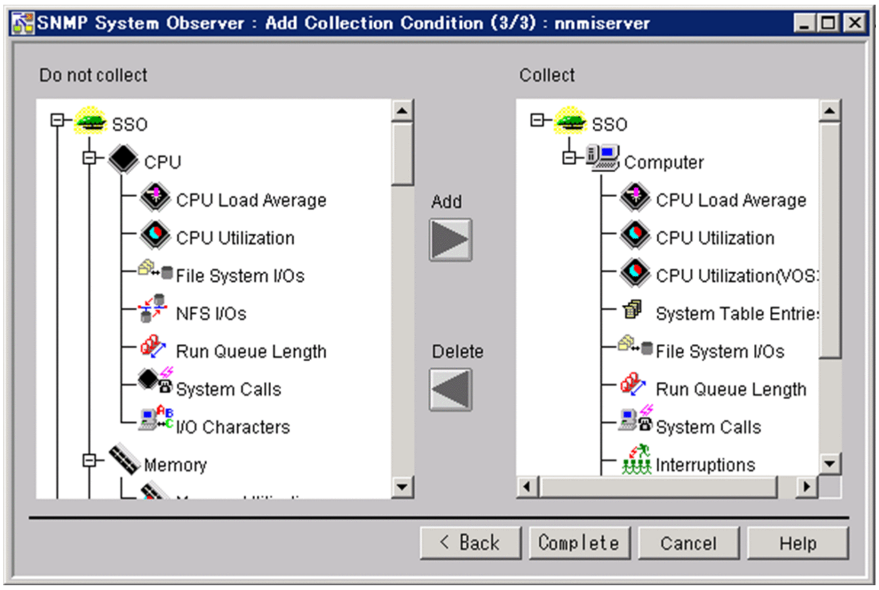
(1) About resource collection

Resource collection is a process for collecting system resources from the servers connected to a network and monitoring target resources that users arbitrarily configured.

With SSO, you can collect the user resources (resources that can be uniquely defined by a user) and system resources (performance information, statistical information, and operating information) of the network devices and various server products that are supported on the OS (Windows or Linux) and SNMP, and monitor the resources in real time. For example, you can perform monitoring by which an incident is issued when CPU usage exceeds 90%. In addition to issuing incidents, any action can be executed automatically.

You can use SSO to collect the following resources:

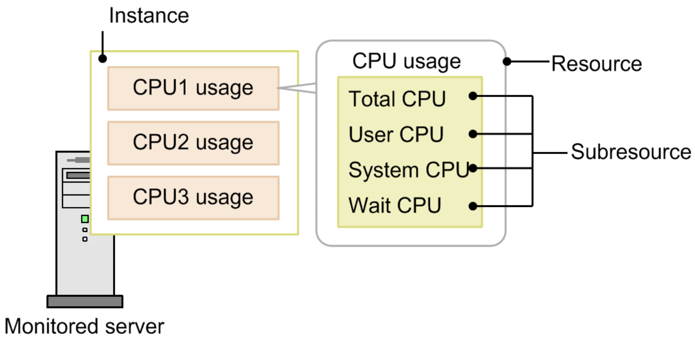
- Resources related to CPU: CPU Utilization, Run Queue Length, System Calls, etc.
- Resources related to memory: Memory Utilization, Swap Utilization, etc.
- Resources related to file systems: File System Utilization, File System Available, etc.
- Resources related to networks: Interface Utilization, Interface Traffic, etc.



You can easily configure resources to be collected by selecting resources from those displayed in the GUI because resource candidates are registered in advance in SSO. You can also automate the operation because collection can be started and ended by using the command.

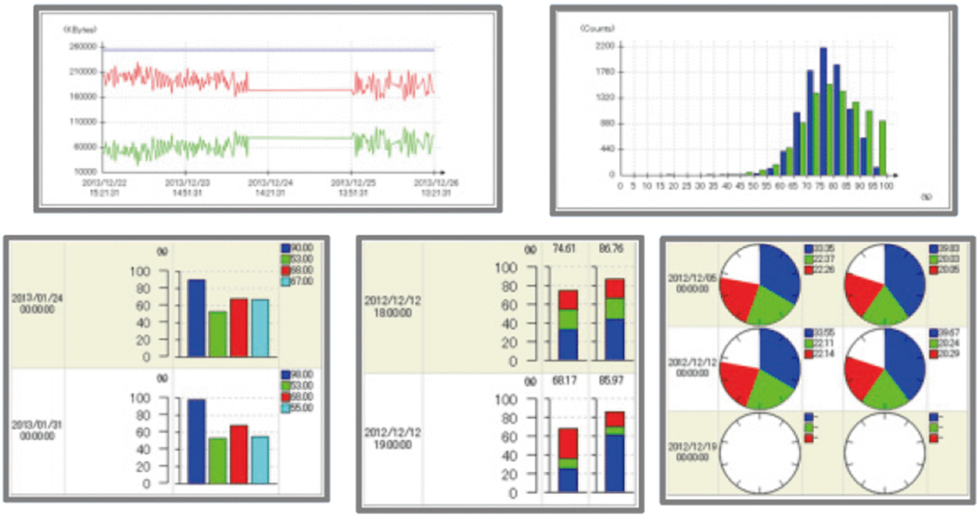
Tip

In the resource collection functionality of SSO, a substance of the source from which a resource is collected is defined as an *instance,* the smallest unit of resources that can be obtained from SNMP agents is defined as a *subresource*, and a group of multiple subresources is defined as a *resource*.



Note

You can create a report for any period such as month or hour, by using collected resources. You can check the operating trend of servers by checking the reports, and can create system operation plans more easily. You can output reports in CSV or HTML format. You can output a report that best suits your purpose because you can select various graph formats.



Related topics

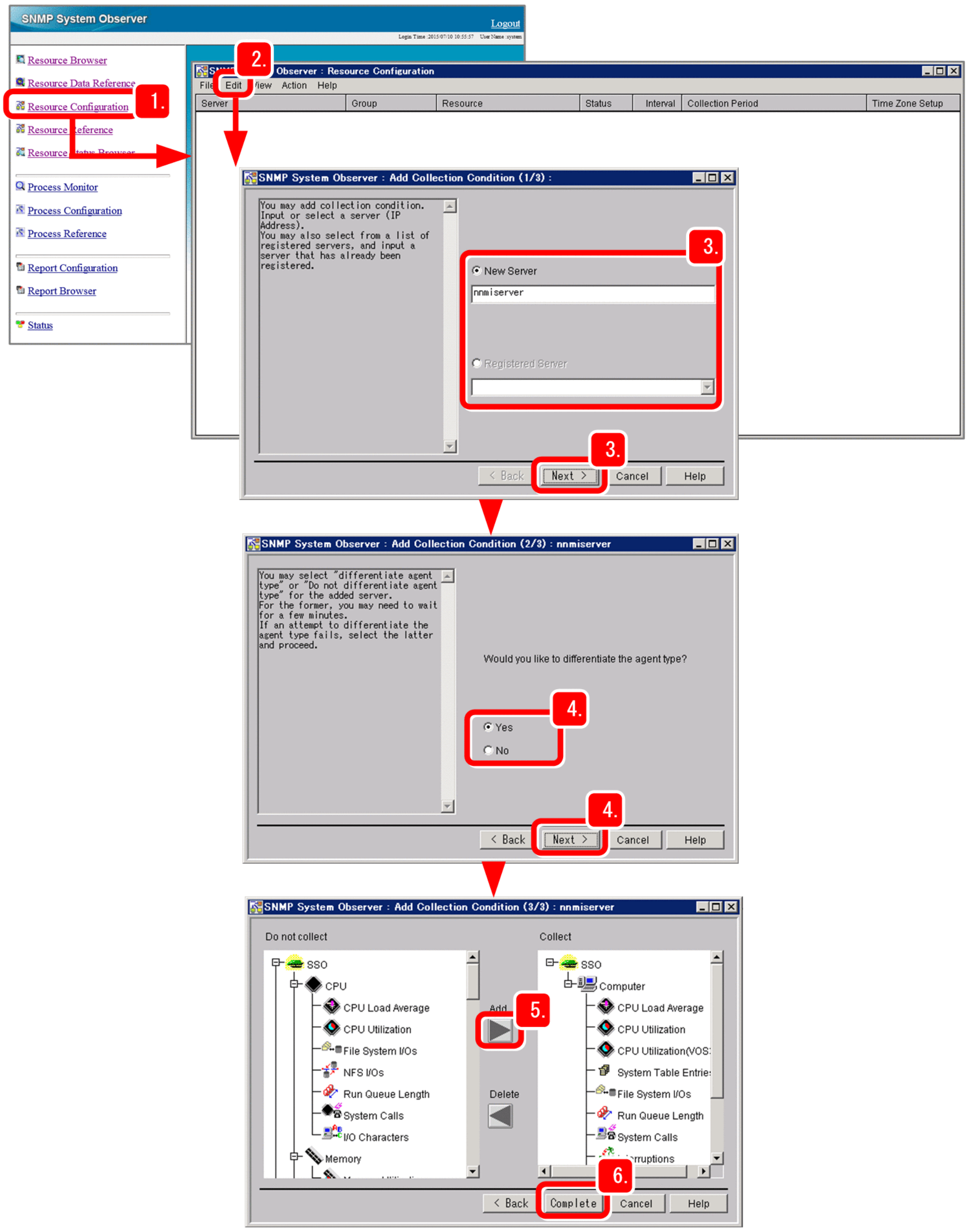
- Topic *Resource IDs* in the manual *JP1/SNMP System Observer*

(2) Starting resource collection

In this procedure, you configure the settings to collect resources by using SSO, and start resource collection.

Procedure

1. In the SSO console, click **Resource Configuration**.



You may add collection condition.
Input or select a server (IP Address).
You may also select from a list of registered servers, and input a server that has already been registered.

New Server: nnmiserver

You may select "differentiate agent type" or "Do not differentiate agent type" for the added server.
For the former, you may need to wait for a few minutes.
If an attempt to differentiate the agent type fails, select the latter and proceed.

Would you like to differentiate the agent type?

● Yes
○ No

2. Click **Edit** and then **Add Collection Condition**.

3. Select a monitored server, and then click **Next**.

   Directly specify a server in **New Server**, or select a registered server in **Registered Server**.

4. Select whether to automatically determine the agent type of the monitored server, and then click **Next**.

   Resources that can be collected differ depending on the agent type. Selecting **Yes** in the **Add Collection Condition (2/3)** wizard displays only the resources that can be collected for the agent type in the **Add Collection Condition (3/3)** wizard.

5. From **Do not Collect**, select the resources that you want to collect, and then click **Add**.

   The selected resources are added to **Collect**.

6. Click **Complete**.

   Resources to be collected are configured.

7. Select the resource for which you want to set the collection conditions, and then click **Edit** and then **Change Collection Detail Condition**. Select the instance, subresource, and collection mode.

   If you do not set the collection conditions, all instances are subject to collection. For the collection mode, you can set whether to save the collected data and whether to monitor thresholds. To monitor thresholds, you also need to set the thresholds and commands that are executed when the thresholds are exceeded.

8. Click **OK**.

   Resource collection conditions are configured.

9. Click **Edit** and then **Set Collection Time Zone**.

   Configure the resource collection time zone if you want to collect resources in a fixed time zone every day.

10. Select the check box for the number in which you want to specify a time zone, and specify the start and stop times.

    For example, to collect resources during the period between 8:00 and 18:00, specify `08:00:00` for the start time, and `18:00:00` for the stop time.

11. Click **OK**.

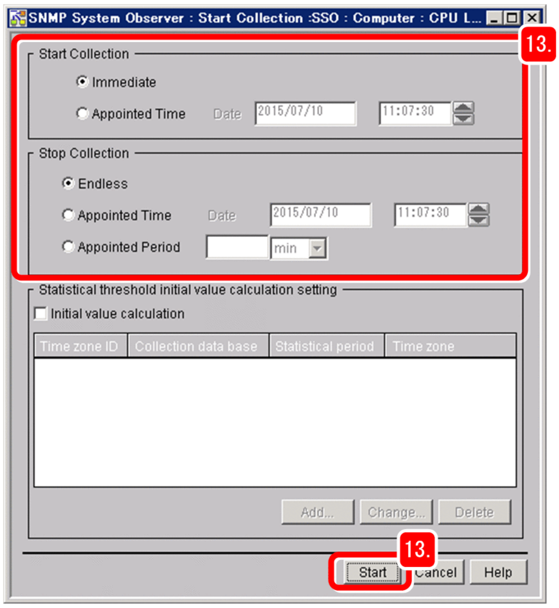
    The resource collection time zone is configured.

    > **Tip**
    >
    > You can also configure collection intervals to suit your purpose. By configuring collection intervals, you can reduce the load on the system. To configure collection intervals, click **Edit** and then **Change Collection Interval**.
    >
    > - To detect a sharp rise in the used amount or usage rate of resources, configure a short collection interval.
    > - To monitor the resource usage for a long period, configure a long collection interval.

12. From the **Actions** menu, click **Start Collection**.

13. Configure the period of time for collecting resources in **Start Collection** and **Stop Collection** fields, and then click **Start**.

    Resource collection is started.



SNMP System Observer : Start Collection :SSO : Computer : CPU L...

Start Collection

● Immediate

○ Appointed Time Date 2015/07/10 11:07:30

Stop Collection

● Endless

○ Appointed Time Date 2015/07/10 11:07:30

○ Appointed Period min

Statistical threshold initial value calculation setting

□ Initial value calculation

Time zone ID	Collection data base	Statistical period	Time zone

If you have configured the collection time zone, make sure that the time zone is within the period from the start to the stop of collection specified in the Start Collection window.

> **Note**
>
> - To manually stop resource collection, from the Resource Configuration window, select the resource that you want to stop collecting, and then from the **Actions** menu, click **Stop Collection**.
> - To check the status of resource collection, check the collection status in the Resource Configuration window. The current collection status is displayed by **Deferred**, **Collecting**, **Completed**, etc.

Result

Now resource collection has successfully started. You can start monitoring resources, such as by viewing collected resources and outputting the resources to a report.

Next steps

In the next section, configure the settings to monitor processes and services by using SSO.

Related topics

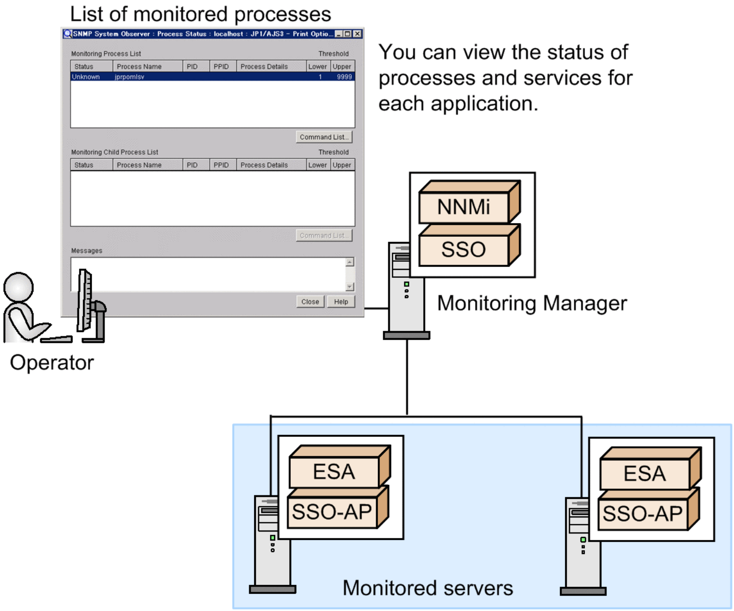
- Topic *Register Application window* in the manual *JP1/SNMP System Observer*
- Topic *Remote Command window* in the manual *JP1/SNMP System Observer*
- 3.1.4 Monitoring resources
- 2.3.3 Monitoring of processes and services

2.3.3 Monitoring of processes and services

You can monitor the active status of processes and the status of Windows services for servers and network devices that support SNMP. You can monitor without needing to be aware of the vendors of network devices or the agent types of servers because SNMP is an industry-standard protocol.

(1) About process and service monitoring

You can define a collection of one or more processes and services as an application, and monitor whether the application operates properly according to the active status of processes and the status of Windows services. You can also issue incidents according to the status of processes and services, and automatically perform actions for monitored servers. Process and service monitoring is suitable for easily and widely monitoring whether the service level of the entire system has decreased because monitoring is performed after the items to be monitored are filtered.


List of monitored processes
SNMP System Observer : Process Status : localhost : JP1/AJS3 - Print Optio...
Monitoring Process List
Threshold
Command List...
Monitoring Child Process List
Threshold
Command List...
Messages
Close
Help
You can view the status of processes and services for each application.
NNMi
SSO
Monitoring Manager
Operator
ESA
SSO-AP
ESA
SSO-AP
Monitored servers

Monitoring Process List

Status	Process Name	PID	PPID	Process Details	Lower	Upper
Unknown	jprpomlsv				1	9999

Monitoring Child Process List

Status	Process Name	PID	PPID	Process Details	Lower	Upper

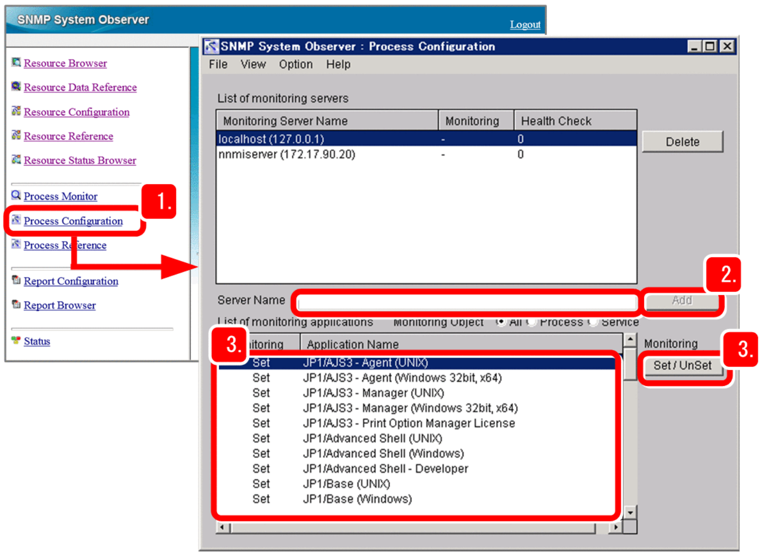
In addition, by installing SSO - AP on monitored servers, you can use SSO to monitor the operating status of processes and services on the servers at regular intervals. You can immediately find an error in the operating status even if a monitored server is located in a remote location. This enables you to quickly respond to the error, and to enhance system availability.

(2) Configuring processes and services to be monitored

In this procedure, you configure the settings for monitoring processes and services by using SSO, and start monitoring.

Procedure

1. In the SSO console, click **Process Configuration**.



List of monitoring servers

Monitoring Server Name	Monitoring	Health Check
localhost (127.0.0.1)	-	0
nnmiserver (172.17.90.20)	-	0

Server Name

List of monitoring applications Monitoring Object ● All ○ Process ○ Service

...itoring	Application Name
Set	JP1/AJS3 - Agent (UNIX)
Set	JP1/AJS3 - Agent (Windows 32bit, x64)
Set	JP1/AJS3 - Manager (UNIX)
Set	JP1/AJS3 - Manager (Windows 32bit, x64)
Set	JP1/AJS3 - Print Option Manager License
Set	JP1/Advanced Shell (UNIX)
Set	JP1/Advanced Shell (Windows)
Set	JP1/Advanced Shell - Developer
Set	JP1/Base (UNIX)
Set	JP1/Base (Windows)

Monitoring

2. In the **Server Name** field, enter the host name or IP address of the server to be monitored, and then click **Add**.
   The server is added to the list of monitoring servers.

3. From the list of monitoring applications, select the application to be monitored, and then click **Set / Unset**.
   The monitoring mode displayed in the list of monitoring applications is changed.
   Set the monitoring mode of all of the applications to be monitored to **Set**.

Tip

Processes and services of JP1 products are pre-registered in the list of monitoring applications. Therefore, you can immediately start monitoring JP1 products. To monitor an application other than a JP1 product, in the Process Configuration window, select **Option** and **Application Registration** to register the application.

4. Select **Option**, **Monitoring Server**, and **Setting the monitoring interval**.

5. In the **Monitoring Interval** field, enter the interval (in minutes) by which monitored target servers are monitored, and then click **OK**.

6. Click **Option**, **Monitoring Server**, and **Setting the health check interval**.

7. In the **Health Check Interval** field, enter the interval (in minutes) by which a health check is to be performed for monitored servers, and then click **OK**.
   Check the operating status of monitored servers, and check whether the monitoring conditions configured on the monitored server match those configured in the Manager.

Note

The health check functionality checks whether processes and services are monitored properly. We recommend that you perform a health check on a regular basis to ensure stable system operation.

8. Select **Option**, **Monitoring Application**, and **Automatic Action**.

9. Select whether to automatically execute the command when the operating status changes for each application, and then click **OK**.

   If you select **Set**, in the **Command** field, enter the command to be automatically executed.

   > **Note**
   >
   > You can remotely execute the command on a monitored server when the operating status changes. To remotely execute the command, in the Process Configuration window, click **Option**, **Monitoring Application**, and **Remote Command** to configure the settings.

10. From the **File** menu, click **Save**.

    Monitoring is started for processes and services of the applications for which the monitoring mode is set to **Set** in the list of monitoring applications.

    > **Note**
    >
    > To stop the monitoring of processes and services, from the list of monitoring applications in the Process Configuration window, select the applications that you want to stop monitoring, and click **Set / Unset** to change the mode to **Unset**. Clicking the **File** menu and then **Save** finishes the monitoring of processes and services.

Result

Now monitoring of processes and services has successfully started. In the SSO console, click Process Monitor to view the operating status of processes and services.

Next steps

You have completed setup of the JP1 network management products. Now you need to start network monitoring by using the JP1 network management products.

Related topics

- Topic *Register Application window* in the manual *JP1/SNMP System Observer*
- Topic *Remote Command window* in the manual *JP1/SNMP System Observer*
- 3. Normal Operation by Using JP1 Network Management Products
- 4. Troubleshooting by Using JP1 Network Management Products

3 Normal Operation by Using JP1 Network Management Products

After you start periodic monitoring of the network by using JP1 network management products, you can view the map windows or collected resources to get an understanding of the status of the entire network and start monitoring the network. In addition, to ensure continuous network management, periodically perform maintenance work.

3.1 Network monitoring by using JP1 network management products

3.1.1 Network monitoring types

There are several ways to monitor the network by using JP1 network management products. This subsection describes how to perform operations based on the map windows and how to check the resources.

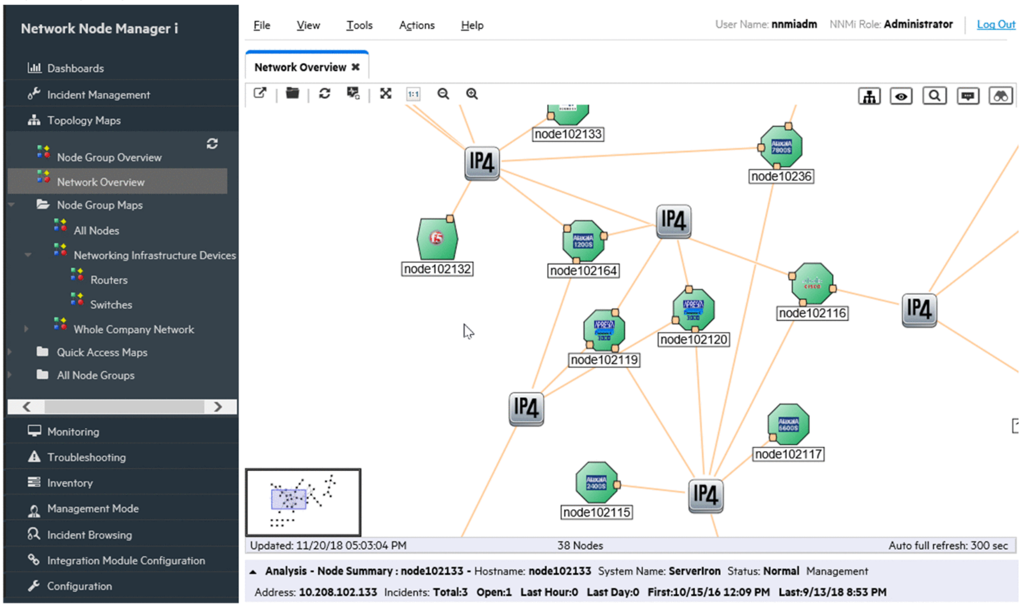
Note

By using NEM, you can monitor the resources of the network switch in the same way as monitoring of the resources of the server. For details, see the NEM manual.

(1) Monitoring by using topology maps (NNMi)

In NNMi, network configuration diagrams (topology maps) are automatically created based on the discovered network devices. For this reason, you can visually determine the status of the network immediately after starting operation.

Topology Map



Updated: 11/20/18 05:03:04 PM 38 Nodes Auto full refresh: 300 sec

Analysis - Node Summary : node102133 - Hostname: node102133 System Name: ServerIron Status: Normal Management Address: 10.208.102.133 Incidents: Total:3 Open:1 Last Hour:0 Last Day:0 First:10/15/16 12:09 PM Last:9/13/18 8:53 PM

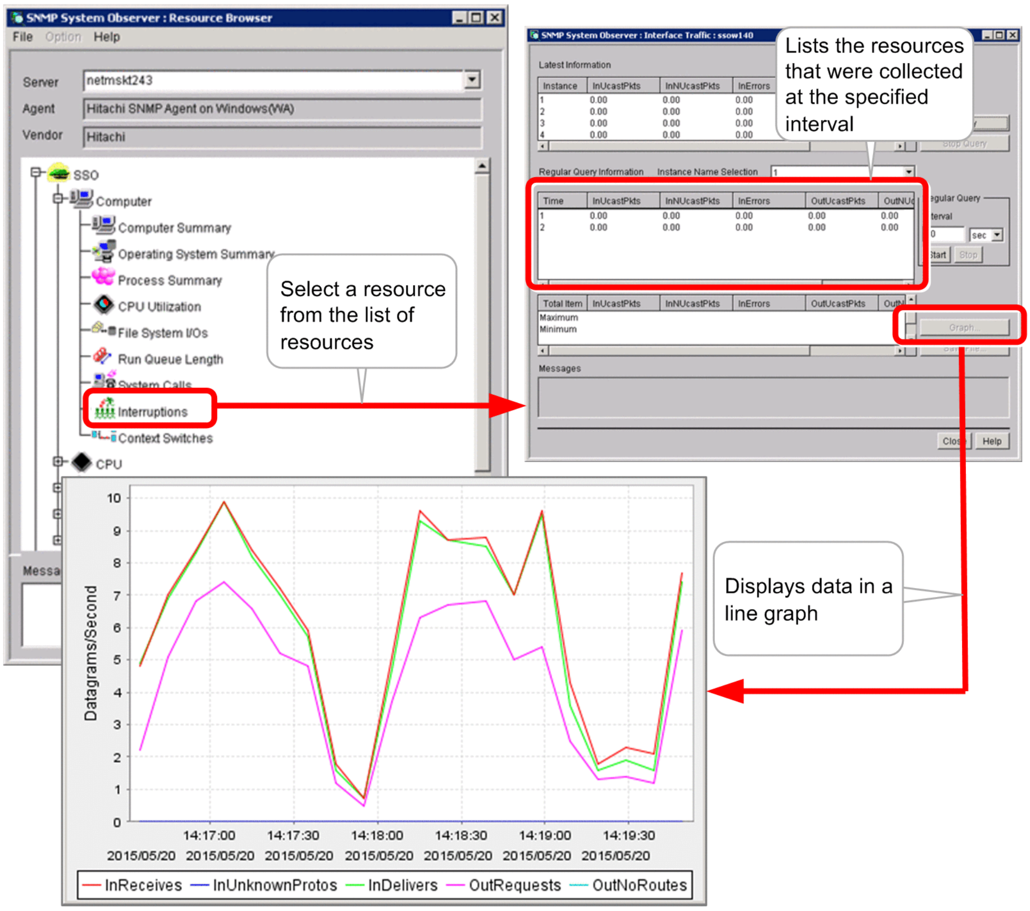
From the topology map, you can distinguish, based on the shape of the icon, the type of the network device, such as a router or computer. In addition, based on the color of the icon, you can determine the status of the network device, such as whether a failure has occurred. You can view not only the Layer 3 topology of the network, but also the Layer 2 topology. This enables you to intuitively check the status when a failure occurs and to understand the affected range.

Related topics

- 3.1.3 Starting network monitoring

(2) Resource monitoring (SSO)

With SSO, you can collect information about user resources (resources that can be uniquely defined by a user) and system resources (performance information, statistics, and operational information) of network devices and various server products that support SNMP and the OS (Windows or Linux), and monitor those resources in real time. For example, you can monitor an incident that was issued when the CPU utilization exceeded 90%.



Server: netmskt243

Agent: Hitachi SNMP Agent on Windows(WA)

Vendor: Hitachi

Select a resource from the list of resources

Lists the resources that were collected at the specified interval

Displays data in a line graph

In addition to issuing an incident, you can also specify that an action is to be automatically executed.

Related topics

- 3.1.4 Monitoring resources

3.1.2 Polling

Polling is using SNMP and ICMP (pings) to periodically discover and monitor network devices. NNMi monitors the discovered network devices by performing polling based on the SNMP and ICMP protocols. NNMi monitors not only the statuses of network devices but also the statuses of the components (such as fans, power supplies, and voltages) of those devices. This enables a wide range of failure monitoring.

If you set an interval (in seconds, minutes, hours, or days), polling can be performed automatically and periodically. You can also perform polling manually when you want to perform polling immediately, for example, immediately after resolving a failure. You can set different polling conditions for multiple ranges, such as for each network device or for each node group. This enables you to change the interval of polling depending on the severity of each monitoring target.

Note

There are two types of polling:

- Polling for discovery
- Polling for monitoring

The above two types of polling are referred to by the following names according to the purpose or situation:

Polling for discovery

- Discovery polling (polling performed immediately by selecting the **Actions** menu, **Polling**, and then **Configuration Poll**)
- Rediscovery polling (periodic polling to rediscover discovered nodes to check whether the configuration has changed)
- Setting polling (polling for discovering settings)
- Finding polling (polling for finding nodes)

Polling for monitoring

- Status polling (polling performed immediately to monitor statuses by selecting the **Actions** menu, **Polling**, and then **Status Poll**)
- State polling (polling for monitoring states)
- Fault polling (polling for monitoring whether a failure has occurred)
- Demand polling (polling for immediate monitoring when a manual operation is performed)

3.1.3 Starting network monitoring

This subsection describes how to monitor a network by displaying the map windows (topology maps) of the network configuration. NNMi performs network monitoring. For example, the operation management center always displays the most important map on a large screen to monitor the network. Immediately after specifying discovery settings, you can check the progress of node discovery.

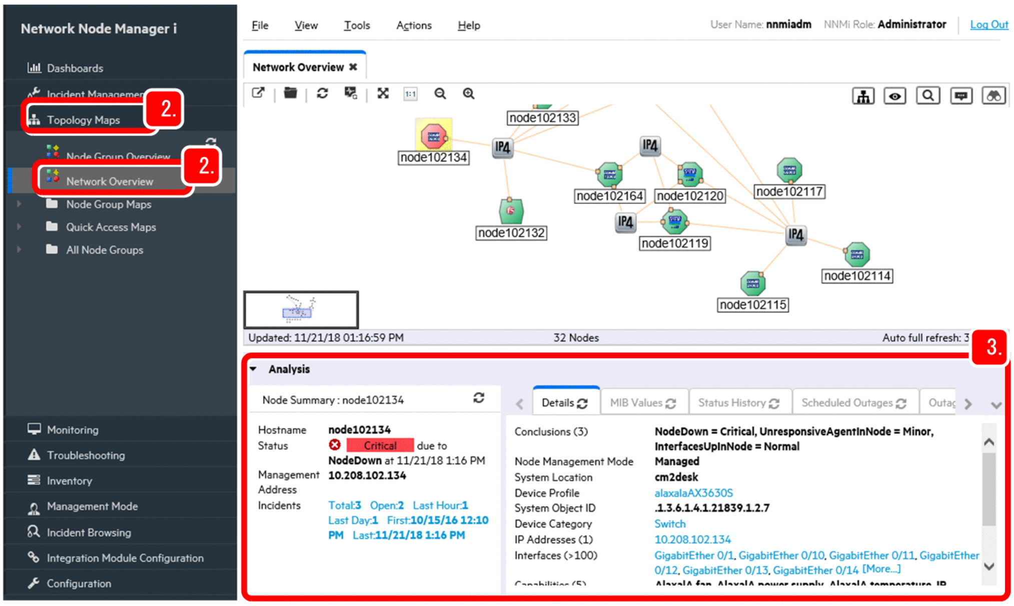
Before you begin

Before you can start monitoring the network, the person (operator) responsible for the monitoring operation must be registered as a user.

Procedure

1. Access the NNMi console.

2. In the **Topology Maps** workspace, click **Network Overview**.



Updated: 11/21/18 01:16:59 PM   32 Nodes   Auto full refresh: 3

Node Summary : node102134

Hostname node102134
Status Critical due to **NodeDown** at 11/21/18 1:16 PM
Management Address **10.208.102.134**
Incidents Total:**3** Open:**2** Last Hour:**1** Last Day:**1** First:**10/15/16 12:10 PM** Last:**11/21/18 1:16 PM**

Conclusions (3)	**NodeDown = Critical, UnresponsiveAgentInNode = Minor, InterfacesUpInNode = Normal**
Node Management Mode	**Managed**
System Location	**cm2desk**
Device Profile	alaxalaAX3630S
System Object ID	**.1.3.6.1.4.1.21839.1.2.7**
Device Category	Switch
IP Addresses (1)	10.208.102.134
Interfaces (>100)	GigabitEther 0/1, GigabitEther 0/10, GigabitEther 0/11, GigabitEther 0/12, GigabitEther 0/13, GigabitEther 0/14 [More...]
Capabilities (5)	AlaxalA fan, AlaxalA power supply, AlaxalA temperature, IP

3. Check the statuses of the nodes based on the colors and details of the icons.

If you select an icon on the map, detailed information is displayed in the **Analysis** pane at the bottom of the window. You can display or hide the **Analysis** pane by clicking ▼ .

Tip

To check the MIB information for a node, use the `nnmsnmpwalk.ovpl` command.

Icon colors and their meanings

By using the more than 6,000 types of device information registered in **Device Profiles** of the **Configuration** workspace, device types are automatically decided. When a device profile is decided, the shape of the icon used in maps is decided according to the category (device category). The following table shows the icon colors and their meanings in maps.

Icon color	Meaning	Icon color	Meaning
Green	Normal	Red	Critical
Light blue	Warning	Blue	Unknown
Yellow	Minor	Gray	Disable
Orange	Major	Beige	No Status

For details about icons, see the topic *About Map Symbols* in the Help *Use*.

Note

To temporarily stop monitoring during maintenance

You can stop monitoring and rediscovery by selecting a node from the topology map, selecting **Management Mode** from the **Actions** menu, and then selecting **OUT OF SERVICE**. Alternatively, you can stop monitoring by using the `nnmmanagementmode.ovpl` command to change the management mode to out of service.

To resume monitoring

To resume monitoring, select the node from the topology map, select **Management Mode** from the **Actions** menu, and then select **Manage**. Alternatively, you can resume monitoring by using the `nnmmanagementmode.ovpl` command to change the management mode to managed.

To list the nodes that were removed from the nodes to be managed

In the **Management Mode** workspace, click **Unmanaged Nodes**.

Tip

In general, a window times out if you do not perform any operations for a certain period of time. You can set the timeout time in the console timeout section that is displayed by clicking the **Configuration** workspace, **User Interface**, and then **User Interface Configuration**. The default is 18 hours.

Note that a window that you open by specifying a URL will not time out. If you want to continuously display a topology map for monitoring, specify the applicable URL.

- Network Overview

  `http://`*host-name*`:`*port-number*`/nnm/launch?cmd=showNetworkOverview`

- Node Group Maps

  `http://`*host-name*`:`*port-number*`/nnm/launch?cmd=showNodeGroup&name=`*node-group-name*#

#: To include a multi-byte character in a URL, you need to URL-encode the character. Use UTF-8 encoding to URL-encode the node group name, and then specify the name.

Example: Important node

%e9%87%8d%e8%a6%81%e3%81%aa%e3%83%8e%e3%83%bc%e3%83%89

In addition, to open multiple windows for monitoring, such as a topology map and an incident window, click ↗ to display the view in a new window. Alternatively, you can display multiple windows by entering a URL to open a window.

Tip

To set the initial window that is displayed when you sign in, specify the setting in the initial view section that is displayed by clicking **User Interface Configuration**. To display incidents, specify **Open Key Incidents**. To display a map, specify **Network Overview**. Note that, although you can also set a node group map created by a user for the initial window, you can specify only the first or last item in the map list. For this reason, you need to adjust the **Topology Maps Ordering** setting in the Node Group Map Settings window. For details, see the *Configure the NNMi User Interface* in the *Help for Administer*.

Next steps

You have now successfully displayed the topology map. Next, start monitoring the network.

Related topics

- 2.2.3 Registering users

3.1.4 Monitoring resources

View the resources to be monitored. SSO performs resource monitoring.

Before you begin

Set the conditions for collecting resources.

Procedure

1. Access the NNMi console.

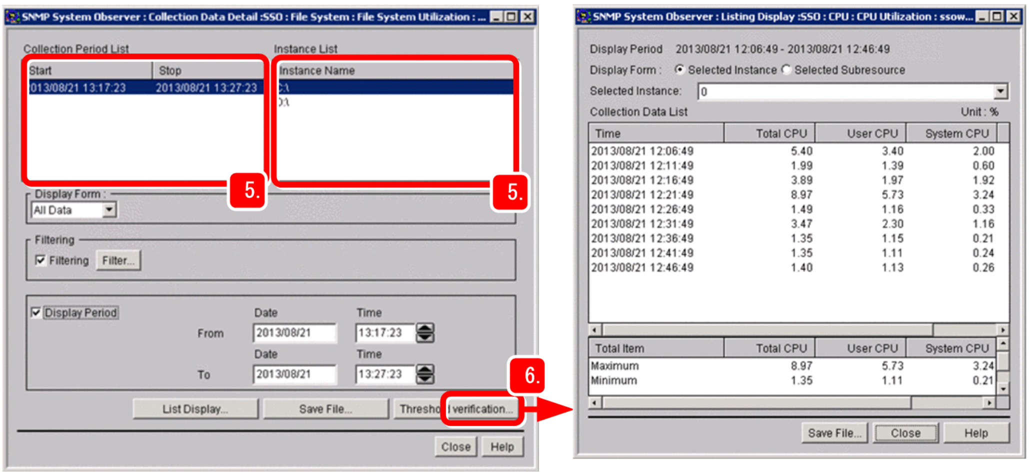
2. In the **Topology Maps** workspace, click **Network Overview**.

3. Select the server whose resources you want to view, and from the **Actions** menu, click **SNMP System Observer** and **Resource Data Reference**.

> **Tip**
>
> If you click 🔍 (Search), you can search for the server name you want to view.

4. Select the resource that you want to view, and select **View** and **Collection Data Details**.

5. From **Collection Period List** and **Instance List**, select the period and instance that you want to view, respectively.



SNMP System Observer : Collection Data Detail :SSO : File System : File System Utilization : ...

Collection Period List

Start	Stop
013/08/21 13:17:23	2013/08/21 13:27:23

Instance List

Instance Name
C:\
D:\

Display Form : All Data

Filtering: ☑ Filtering

☑ Display Period

From: Date 2013/08/21 Time 13:17:23

To: Date 2013/08/21 Time 13:27:23

SNMP System Observer : Listing Display :SSO : CPU : CPU Utilization : ssow...

Display Period 2013/08/21 12:06:49 - 2013/08/21 12:46:49

Display Form : ● Selected Instance ○ Selected Subresource

Selected Instance: 0

Collection Data List Unit : %

Time	Total CPU	User CPU	System CPU
2013/08/21 12:06:49	5.40	3.40	2.00
2013/08/21 12:11:49	1.99	1.39	0.60
2013/08/21 12:16:49	3.89	1.97	1.92
2013/08/21 12:21:49	8.97	5.73	3.24
2013/08/21 12:26:49	1.49	1.16	0.33
2013/08/21 12:31:49	3.47	2.30	1.16
2013/08/21 12:36:49	1.35	1.15	0.21
2013/08/21 12:41:49	1.35	1.11	0.24
2013/08/21 12:46:49	1.40	1.13	0.26

Total Item	Total CPU	User CPU	System CPU
Maximum	8.97	5.73	3.24
Minimum	1.35	1.11	0.21

6. Click **List Display**.
   You can view a list of collected data.

> **Tip**
>
> In the Resource Data Reference window, you can copy or delete the data of the collected resources.
>
> For example, you can secure free space in the database by copying and retaining the resources only for the period during which a problem occurred, and then deleting other unnecessary resources.

Next steps

You have now successfully viewed information about the collected resources. If necessary, you can output information about the collected resources to a report to understand the operational trends of the server and to make system operation plans.

> **Note**
>
> You can output information about the collected resources to a report by using **Report Browser** of the SSO console. To output a report, you need to configure the report settings in advance. For details about outputting reports, see the topic *Report Configuration window* in the manual *JP1/SNMP System Observer*.

Related topics

- 2.3.2 Resource collection
- Topic *Copy Collection Condition window* in the manual *JP1/SNMP System Observer*

3.2 Periodic maintenance of JP1 network management products

To continuously perform network management, periodic maintenance work is important. This section describes the operational tasks of JP1 network management products.

3.2.1 Checking the NNMi operating status

To manage the network, NNMi first needs to be operating normally. Make sure that NNMi is operating normally.

Procedure

1. From the **Help** menu, click **System Information**.
2. In the **Product** tab, check **Status**.
   Make sure the status is the normal level.
3. In the **Health** tab, check the detailed status of NNMi.
4. In the **State Poller** tab, check the operating status.
5. In the **Database** tab, check the number of discovered objects.

Result

You were able to confirm that NNMi was operating normally.

> **Tip**
>
> If a problem occurs in NNMi itself, a warning is displayed in yellow at the bottom of the NNMi console, and the NnmHealthOverallStatus incident is issued. If this incident is reported during operation, check **Custom Attributes** of **Incident**.

Related topics

- Topic *Check NNMi Health* in the *Help for Administer*

3.2.2 Exporting or importing the NNMi settings

Storing the system settings for each important point and managing changed items are important operational tasks. With NNMi, you can export and import system settings. This enables you to obtain a snapshot of the current system settings, and to restore settings that contain a mistake by importing settings.

Procedure

1. Execute the `nnmconfigexport.ovpl` command or the `nnmconfigimport.ovpl` command.

   The following table shows the execution examples of the `nnmconfigexport.ovpl` command and the `nnmconfigimport.ovpl` command.

Purpose	Command
To export all settings	`nnmconfigexport.ovpl -c all -f c:\nnmiconf`
To import all settings	`nnmconfigimport.ovpl -f c:\nnmiconf`
To import the settings of a node group	`nnmconfigimport.ovpl -f c:\nnmiconf\nodegroup.xml`

Result

You were able to export or import the NNMi settings.

Related topics

- 1.2.4 Storage location of the commands of each product
- Topic *Export and Import Configuration Settings* in the *Help for Administer*

3.2.3 Backing up or restoring NNMi

Periodically backing up NNMi in preparation for unexpected situations (such as system failure or data loss due to an operational error) is an important operational task. You can perform an online backup of NNMi while continuing to monitor the network. Thus, you can systematically back up NNMi.

Procedure

1. Execute the `nnmbackup.ovpl` command or the `nnmrestore.ovpl` command.

   The following table shows the execution examples of the `nnmbackup.ovpl` command and the `nnmrestore.ovpl` command.

Purpose	Command
To perform an online backup of NNMi as a whole	`nnmbackup.ovpl -type online -scope all -force -target c:\nnmi` In the folder specified for `-target`, a folder whose name includes the date and time (for example, `nnm-bak-20150922002454`) is created.
To restore the backed up data	`nnmrestore.ovpl -force -source c:\nnmi\nnm-bak-20150922002454`

Result

You were able to back up or restore NNMi.

Related topics

- 1.2.4 Storage location of the commands of each product
- Topic *Backup and Restore NNMi in the Help for Administer*

3.2.4 Archiving or deleting NNMi incidents

NNMi can record a maximum of 100,000 SNMP trap incidents in the database. In addition, you can use NNMi to automatically delete (trim) data starting from the oldest data, or save data to an archive to prevent an increase in data items from affecting performance.

(1) Checking the number of SNMP trap incidents

Check the number of SNMP trap incidents.

Procedure

1. In the **Incident Browsing** workspace, click **SNMP Traps**.
   At the bottom of the displayed incident list, the number of SNMP trap incidents is displayed to the right of **Total**.

Result

You were able to check the number of SNMP trap incidents.

> **Note**
>
> When the number of SNMP trap incidents is close to the upper limit, the following incidents are reported:
>
> - 90% of the upper limit: SnmpTrapLimitWarning
> - 95% of the upper limit: SnmpTrapLimitMajor
> - Upper limit: SnmpTrapLimitCritical

Related topics

- Topic *Archive and Delete Incidents* in the *Help for Administer*

(2) Enabling the automatic trimming feature

If you enable the automatic trimming feature, data can be automatically deleted (trimmed) starting from the oldest data or an archive can be automatically created during trimming when the number of SNMP trap incidents exceeds the specified number. The automatic trimming feature is enabled by default in the new installation environment. We recommend that you enable this feature for operation.

Related topics

- Topic *Configuring the auto-trim oldest SNMP trap incidents feature* in the *JP1/Network Node Manager i Setup Guide*

3.2.5 Periodically deleting SSO collection data

The amount of data in the SSO collection database monotonically increases because the database does not have a retention period. Thus, as SSO continues to collect data and the size of the database increases, the collection or deletion performance of the database might decrease significantly. For this reason, we recommend that you periodically back up the database or delete collection data to maintain the performance of the collection database. Set the retention period of the collection data to a maximum of one year.

Procedure

1. Execute the `ssodbdel` command.

   The following shows an execution example of the command to delete collection data for which the retention period has expired:

   ```
   ssodbdel -all -stop BMONTH 13
   ```

   When you execute this command, of the data in the collection database, data for which the retention period (of one year) has expired is deleted. If you execute this command on the first day of every month, the collection database will store data only for about one year.

Result

You were able to delete SSO collection data.

Related topics

- 1.2.4 Storage location of the commands of each product
- Topic *ssodbdel* in the manual *JP1/SNMP System Observer*

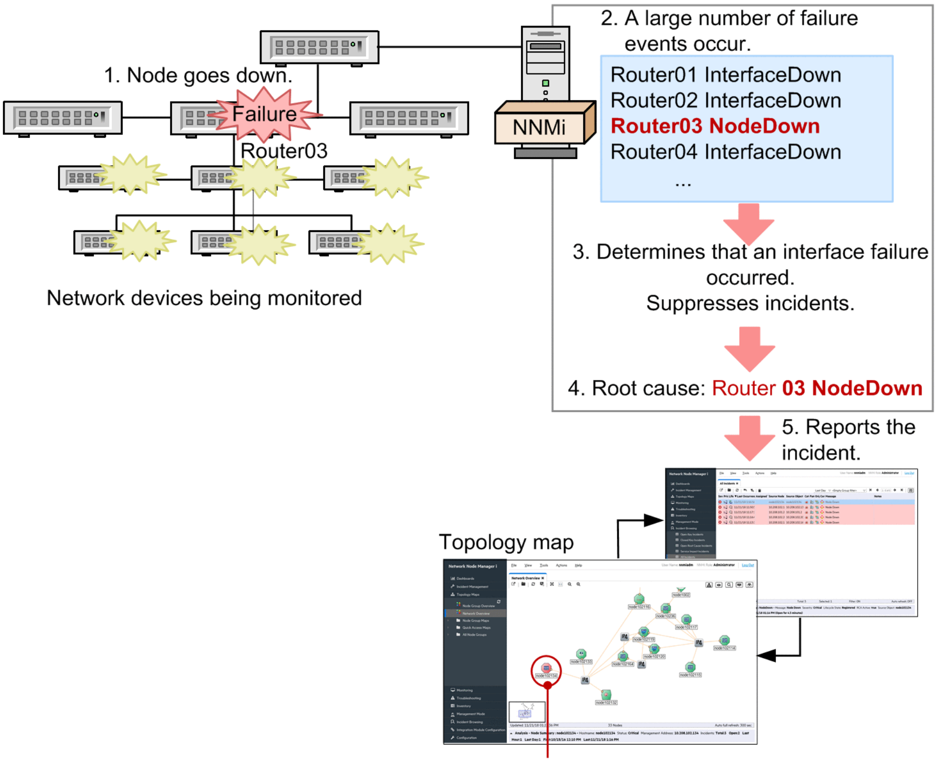
4 Troubleshooting by Using JP1 Network Management Products

This chapter describes how to use the incident management features of JP1 network management products to quickly identify and solve failures.

4.1 Analyzing the root cause of a failure

When a failure occurs, the Monitoring Manager uses the functionality for analyzing root causes to investigate and filter the correlations among the large number of events that occur. The Monitoring Manager analyzes the failure based on the Layer 2 topology and Layer 3 topology to identify the root cause, and then reports the root cause as an incident. The Monitoring Manager manages the progress of incident handling (lifecycle state), from the occurrence of the problem to its solution.

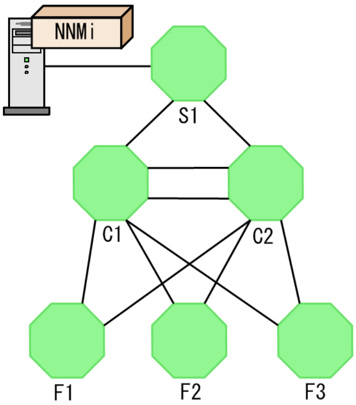
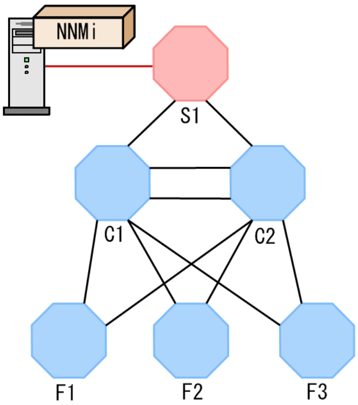
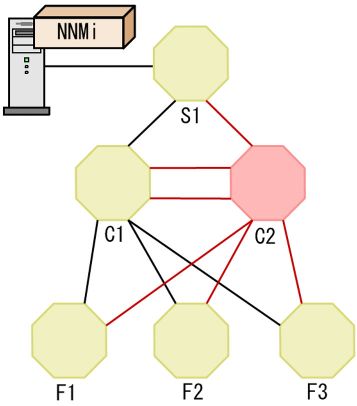
The following uses an example of monitoring a network device (router) to check how to analyze the root cause.



The location where the failure occurred can be immediately identified.

1. If the Router03 node goes down, there is no response from a large number of interfaces and IP addresses that Router03 has.
2. A large number of failure events occur due to interface failures and no response from IP addresses.
3. The Monitoring Manager decides that the lack of responses from IP addresses was caused by the interface failures, and then suppresses the corresponding incidents.
4. Based on the fact that communication was lost at neighboring nodes, the Monitoring Manager decides the root cause is the Router03 node going down. The Monitoring Manager also decides that the interface failures were caused by the node going down, and associates the interface failures with the Router03 node going down.
5. The Router03 node going down is reported as the root-cause incident.

In addition, the Monitoring Manager effectively uses Layer 2 topology information to analyze the root cause even for multiple nodes that compose a network. The following table shows examples of analyzing the root cause by using a Layer 2 topology network configuration.

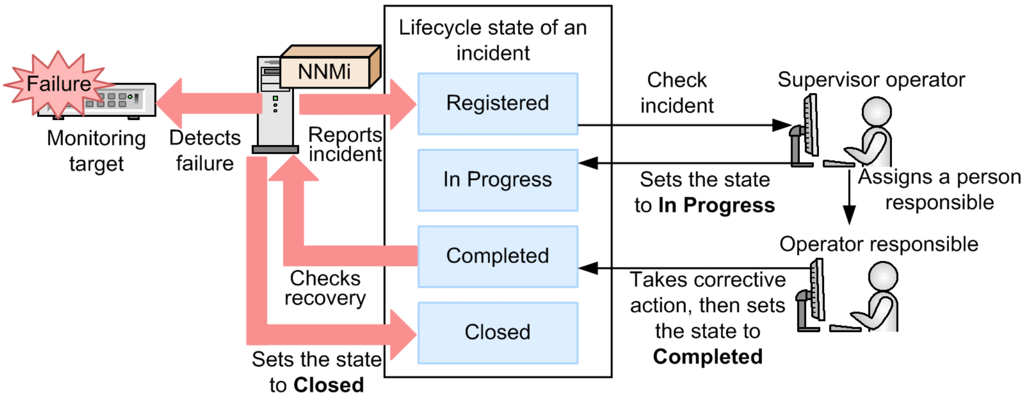
Analysis of a Layer 2 topology	Description
Normal time  	The Monitoring Manager is connected to the top-level switch `S1`, and the networks that are being monitored are all in the normal status.
When a failure occurs in the top-level switch  	Detailed failure: The top-level switch `S1` went down. Events that occur: • Communication with `S1` is unavailable. • Communication with other switches via `S1` is unavailable. The Monitoring Manager handles this situation as follows: • Detects the failure of the `S1` node. • Decides that the failure of `S1` caused communication via `S1` to be unavailable, suppresses the corresponding incidents, and then decides that the status is unclear. As a result, the Monitoring Manager reports only the failure of `S1` as the root-cause incident.
When a failure occurs in a middle-level switch  	Detailed failure: The middle-level switch `C2` went down. Events that occur: • Communication with `C2` is unavailable. • Each node interface connecting with `C2` went down. The Monitoring Manage handles this situation as follows: • Detects the failure of the `C2` node. • Decides that each interface connecting with `C2` went down because of the failure of `C2`, and then suppresses the corresponding incidents. As a result, the Monitoring Manager reports only the failure of `C2` as the root-cause incident.

The Monitoring Manager can also analyze many other correspondences between an event and a root cause.

4.2 Troubleshooting mechanism

The Monitoring Manager manages the progress of incident handling as lifecycle states in the **Incidents** view. If multiple persons share the management, you can specify a person responsible for the operation other than you (by using **Assigned To**) to share the tasks on the GUI when starting the tasks to resolve a failure.

As shown in the following figure, if you assign a person responsible for handling an incident and change the lifecycle state, you can appropriately handle a failure that occurred:


Failure
Monitoring target
Detects failure
NNMi
Reports incident
Lifecycle state of an incident
Registered
In Progress
Completed
Closed
Checks recovery
Sets the state to **Closed**
Check incident
Supervisor operator
Sets the state to **In Progress**
Assigns a person responsible
Operator responsible
Takes corrective action, then sets the state to **Completed**

After reporting an incident, the Monitoring Manager continues to monitor the state. If the Monitoring Manager detects a recovery, the state of the incident is automatically set to **Closed**. For example, when a node for which **NodeDown** was reported starts operation again, the state of the incident is automatically set to **Closed**.

Tip

As an exercise illustrating the operation, the following describes how to cause a dummy failure to occur in order to check the reported incident:

1. Cause a failure to occur by disconnecting the LAN cable from a monitoring target node or stopping the node.
   Make sure the problem will not affect your business's work.
2. After selecting the node in a map window, from the **Actions** menu, select **Polling**, and then select **Status Poll**.
   The state polling is performed, and then the failure is detected.

4.3 Troubleshooting a network failure

You can use several methods to troubleshoot a network failure. This section describes how to handle a network device node going down, and how to handle an abnormal operating status of a process or service.

4.3.1 Handling a network device node that is going down

If an incident reports a network device node going down, you need to check the location that has the problem, and then take corrective action.

Procedure

1. Use the topology map of the NNMi console to check the location in which a failure occurred.

   When a failure is detected, the color of an icon on the map changes.

   If you put maps into a hierarchy, open the child node group to check the status. For the status of a node group, the most critical status is displayed. The statuses of child node groups are applied to the parent node group.

2. Open the **Incident Browsing** workspace to check the incident that was reported as the root cause.

   Open the **Open Key Incidents** view or the **All Incidents** view to reference the content of the incident, and then check the location that has the problem. If you select the target node, and then open the **Incident** tab, you can check occurrence of the incidents in chronological order. First, check **Source Node**, **Source Object**, and **Custom Attributes**.

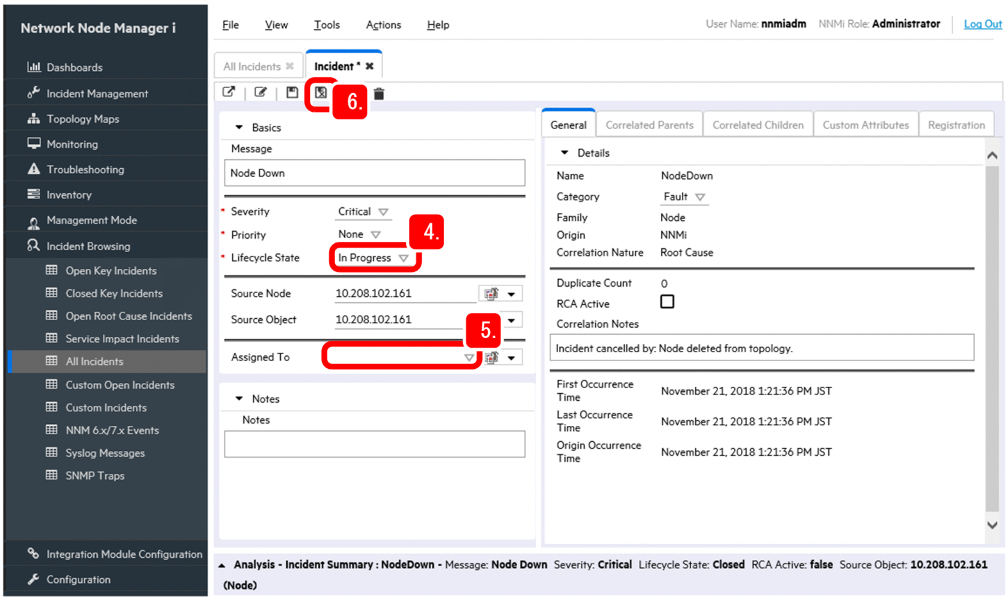
3. Double-click the incident to check detailed information about the incident.

   The **Incident** view is displayed. Use the message and name information to check the type of the incident. Use the source node information to check the location where the failure occurred. Use the date and time information to check the time when the failure occurred.

   > **Note**
   >
   > For an SNMP trap incident, use the **Custom Attributes** tab to check the detailed information. In the **Custom Attributes** tab, the information reported by an SNMP trap is displayed. Check the content by referring to the documentation of the devices that issued the SNMP trap.

4. Set **Lifecycle State** of the incident to **In Progress**.

   After you understand the details of the problem, from the **Lifecycle State** pull-down menu, select a state. Immediately after an incident is registered, the state is set to **Registered**.



User Name: **nnmiadm** NNMi Role: **Administrator**

Basics

Message: Node Down

Severity: Critical

Priority: None

Lifecycle State: In Progress

Source Node: 10.208.102.161

Source Object: 10.208.102.161

Assigned To:

Notes

Notes:

Details

Name: NodeDown

Category: Fault

Family: Node

Origin: NNMi

Correlation Nature: Root Cause

Duplicate Count: 0

RCA Active: ☐

Correlation Notes: Incident cancelled by: Node deleted from topology.

First Occurrence Time: November 21, 2018 1:21:36 PM JST

Last Occurrence Time: November 21, 2018 1:21:36 PM JST

Origin Occurrence Time: November 21, 2018 1:21:36 PM JST

Analysis - Incident Summary : NodeDown - Message: **Node Down** Severity: **Critical** Lifecycle State: **Closed** RCA Active: **false** Source Object: **10.208.102.161 (Node)**

5. From the **Assigned To** pull-down menu, select your account.

   If you want to assign an operator other than you, make sure that the operator can access the assigned incident.

6. Click (Save and Close).

   The changed setting is saved.

7. Check the situation of the related parts.

   A network failure often affects related parts of the communication routes. Therefore, check not only the root cause but also the related parts.

   - In a map window, check the related parts to understand the situation.
   - In the **Monitoring** workspace, make sure that there is no part that has a problem.

8. Take corrective action.

   If you configure automatic actions for an incident beforehand, the specified command can be automatically executed.

9. After taking corrective action, set **Lifecycle State** of the incident to **Completed**.

   Closed is automatically set when the system identifies that there is no problem.

10. Click (Save and Close).

    The changed setting is saved.

11. Check the changed state of the incident.

    In the **Incident Browsing** view, make sure that **Lifecycle State** is set to **Closed**.

Result

You have now successfully taken corrective action for a network device node going down.

Related topics

- (4) Configuring automatic actions for an incident
- 3.1.3 Starting network monitoring

4.3.2 Handling an abnormality in the operating status of a process or service

If an incident reports an abnormality in a process or service, you need to check the location that has the problem, and then take corrective action.

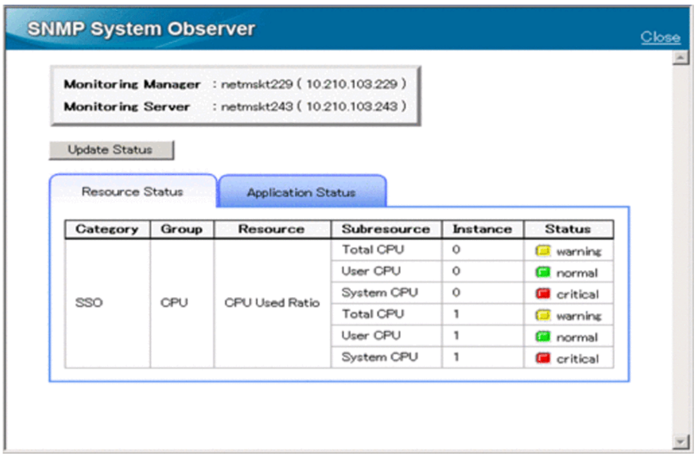
Procedure

1. Open the **Incident Browsing** workspace of the NNMi console, and then check the content of the incident that reported an abnormality in a process or service.

2. In the **Topology Maps** workspace, click **Network Overview**.

3. After selecting the monitoring target whose failure you want to check, from the **Actions** menu, click **SNMP System Observer**, and then click **View Monitoring Status**.
   The monitoring status display window that displays the resource status and the application status is displayed.

4. Select the **Application Status** tab.
   You can identify the application status from the icon color.
   - Green: Normal
   - Yellow: Warning
   - Red: Critical
   - Blue: Unrecognizable



Monitoring Manager : netmskt229 (10.210.103.229)
Monitoring Server : netmskt243 (10.210.103.243)

Category	Group	Resource	Subresource	Instance	Status
SSO	CPU	CPU Used Ratio	Total CPU	0	🟨 warning
			User CPU	0	🟩 normal
			System CPU	0	🟥 critical
			Total CPU	1	🟨 warning
			User CPU	1	🟩 normal
			System CPU	1	🟥 critical

5. For the process or service that has a problem, take corrective action.

6. After taking corrective action, change **Lifecycle State** of the incident to **Closed**.

Result

You have now successfully taken corrective action for an abnormality in a process or service.

Related topics

- 4.3.1 Handling a network device node that is going down

Appendixes

A. Advanced Use

This appendix provides reference information for making full use of JP1 network management products.

Introduction to NNMi Advanced

Among the JP1 network products, NNMi Advanced is provided as a higher-level version of NNMi and enables monitoring that supports advanced network technology. The following table describes the main functionalities of NNMi Advanced.

Functionality	Description
Global network management	Enables central management by using a regional manager to monitor each site and a global manager to control the regional managers. A global manager can be used to manage a maximum of 65,000 nodes.
NNMi IPv6 Management Feature	Enables efficient and unified management of next-generation networks and existing networks, because NNMi Advanced can manage IPv6 and IPv4 networks at the same time.
Discover and monitor VMware hypervisor-based virtual networks	Enables automatic identification of ESX hosts and virtual machines in the same way as automatic identification of routers and switches, and enables you to manage inventory information in a list.
Discovering link aggregation	Automatically recognizes aggregated link configurations. In maps, aggregated links are displayed as thick lines.
Router Redundancy Group	Automatically recognizes the configuration of a redundant router group. In addition, this functionality enables you to monitor whether a router group routes packets appropriately.

For details, see the *JP1/Network Node Manager i Setup Guide*.

Introduction to operational methods

The following table provides examples of how to use the JP1 network management products. For details, see the locations listed in the Reference column.

Case example	Description	Reference
I want to try out the product. Is it easy to start using the products immediately?	To start using the products, perform the following three steps: 1. In **Communication Configuration**, configure the SNMP community strings. 2. In **Discovery Configuration**, specify the range of IP addresses to be automatically discovered, enable ping sweeps, and then enable SNMP node discovery. 3. In the **Topology Maps** work space, open **Network Overview** to start operations.	2.2.4 2.2.5 3.1.3
No nodes were discovered.	In **Discovery Configuration**, specify the range of IP addresses to be discovered, and then specify the discovery seed used as the starting point of discovery. You can check the discovery status from **Topology Maps** or **Inventory**. You can also check the status of the discovery processing by clicking the **Help** menu, **System Information**, and then **State Poller**.	2.2.5
Only routers and switches were discovered.	By default, only routers and switches will be discovered. To change this setting, in **Discovery Configuration**, select **Auto-Discovery Rules**, and then select the **Discover Any SNMP Device** and **Discover Non-SNMP Devices** check boxes as needed.	2.2.5
After node groups were defined, the topology map became hard to read because	If you specify a blank for Topology Maps Ordering of a node group map, the topology map name of the node group map will not be	2.2.6

Case example	Description	Reference
too many topology map names were displayed.	displayed in the Quick Access Maps folder under the Topology Maps workspace.	2.2.6
It is impossible to communicate with a node, but the status is determined to be unrecognized (blue icon) instead of critical.	For example, if a failure occurs on a switch located in the middle of a network route and communication with a certain node becomes unavailable, NNMi determines the switch to be the root cause and reports an incident. In addition, the statuses of nodes with which communication has become unavailable due to the failure are determined to be unrecognized. To report an incident when communication becomes unavailable, use *important nodes*.	2.2.6 2.2.8
How can I specify the IP address of the SNMP manager (NNMi)?	To specify the IP address of the SNMP manager (to permit a connection) in the SNMP settings on the SNMP agent side, specify all IP addresses of the NNMi manager, because an IP address that corresponds to the destination IP address will be dynamically selected depending on the network routing settings of the OS. To revise the IP address, specify the IP address for NNM_INTERFACE in the `ov.conf` file. Adjust the routing settings of the OS to enable communication by using the fixed IP address.	*Release Notes*
An SNMP trap was issued, but it was not reported as an incident.	To report an SNMP trap as an incident when NNMi receives the SNMP trap, the node must have already been discovered and an incident for the relevant SNMP trap must already be defined and enabled. To change a trap issued from an undiscovered node to an incident, from **Incident Configuration**, clear the **Discard Unresolved SNMP Traps and Syslog Messages** check box.	Topic *Manager Unresolved Incoming SNMP Traps* in the *Help for Administer*
I want to create a list of servers or incidents.	In a window (such as the inventory window) where data is displayed in table format, you can output the data to a file in CSV format. To do this, for example, in the **Inventory** workspace, open **Nodes**, and then perform the following operations: 1. Select the row that you want to output. 2. Right-click the row, and then select **Export to CSV** from the displayed menu. 3. Perform operations according to the displayed information. Import the output data into a spreadsheet application to create a list. You can create a list of nodes from data in the **Nodes** view, and a list of incidents from data in the **Management Event Configuration** view.	Topic *Export Table Information of Use Table Views* in the Help *Use*

B. Version Changes

B.1 Changes in version 12-60

(1) Changes in manual 3021-3-E01-30(E)

- Windows Server 2022 was added to the applicable OSs of servers for the Monitoring Manager and Monitoring Agents.
- The procedure was changed so that the system account password is set during installation of NNMi.
- Setting of the system account password was added to the procedure for installing NNMi.
- The locales set in the environment variables LC_ALL and LANG were changed.

B.2 Changes in version 12-50

(1) Changes in manual 3021-3-E01-20(E)

- A description of the default value of the HTTPS port used by NNMi was added.
- The description about supported OSs for servers used as the Monitoring Manager or as Monitoring Agents was changed.
- The conditions on web browsers that can be used were changed.
- A description about the packages and library files required as part of the prerequisite conditions for the Monitoring Manager was added.
- A description about kernel.shmall was added.
- LANG was added as an environment variable to be specified during the installation of NNMi.
- A description about the language environment was deleted.
- The description about the automatic trimming feature was changed.

B.3 Changes in version 12-10

(1) Changes in manual 3021-3-E01-10(E)

- Windows Server 2019 was added as an applicable OS for the server on which the Monitoring Manager is to be set up.

B.4 Changes in version 12-00

(1) Changes in manual 3021-3-E01(E)

- Windows Server 2008 R2 was removed from the applicable OSs.
- The following were added to the OSs applicable for the server used as the Monitoring Agent:
  - SUSE Linux 15
  - AIX V7.2
- The following were removed from the OSs applicable for the server used as the Monitoring Agent:
  - AIX V6.1
  - Solaris 10
- Internet Explorer 10 is no longer supported.
- The supported Firefox versions for Windows were changed. Also, Firefox for Linux is no longer supported.
- The procedure for setting up JP1/SNMP System Observer was changed. Also, the descriptions about the Java Plug-in were deleted.

B.5 Changes in version 11-10

(1) Changes in manual 3021-3-A71-10(E)

- Windows Server 2016 is now supported.
- The following browser is no longer supported:
  - Internet Explorer 9
- Supported Firefox versions were changed.

C. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

C.1 Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *JP1 Version 12 JP1/Network Node Manager i Setup Guide* (3021-3-E02(E))
- *JP1 Version 12 JP1/Network Node Manager i Developer's Toolkit Guide* (3021-3-E03(E))
- *JP1 Version 12 JP1/SNMP System Observer Description, Operator's Guide and Reference* (3021-3-E04(E))
- *JP1 Version 12 JP1/Extensible SNMP Agent Description, Operator's Guide and Reference* (3021-3-E05(E))

In this manual, the *JP1 Version 12 JP1/Network Node Manager i Setup Guide* is abbreviated as the *JP1/Network Node Manager i Setup Guide*. *JP1 Version 12 JP1/SNMP System Observer Description, Operator's Guide and Reference* is abbreviated as *JP1/SNMP System Observer*. *JP1 Version 12 JP1/Extensible SNMP Agent Description, Operator's Guide and Reference* is abbreviated as *JP1/Extensible SNMP Agent*.

C.2 Abbreviations for Microsoft product names

This manual uses the following abbreviations for Microsoft product names.

Abbreviation			Full name or meaning
Internet Explorer			Windows(R) Internet Explorer(R)
Windows	Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
			Microsoft(R) Windows Server(R) 2012 Standard
		Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
			Microsoft(R) Windows Server(R) 2012 R2 Standard
	Windows Server 2016		Microsoft(R) Windows Server(R) 2016 Datacenter
			Microsoft(R) Windows Server(R) 2016 Standard
	Windows Server 2019		Microsoft(R) Windows Server(R) 2019 Datacenter
			Microsoft(R) Windows Server(R) 2019 Standard
	Windows Server 2022		Microsoft(R) Windows Server(R) 2022 Datacenter
			Microsoft(R) Windows Server(R) 2022 Standard

C.3 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation			Full name or meaning
ESA			JP1/Extensible SNMP Agent
Firefox	Firefox ESR 78		Mozilla Firefox(R) ESR 78
IPF			Itanium(R) Processor Family
JP1/IM			JP1/Integrated Management - Manager
Linux	CentOS 6.1 (x64)		CentOS 6 (x64) (version 6.1 or later)
	CentOS 7.1		CentOS 7 (version 7.1 or later)
	CentOS 8.1		CentOS 8 (version 8.1 or later)
	Linux 6.1 (x64)		Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64) (version 6.1 or later)
	Linux 7.1		Red Hat Enterprise Linux(R) Server 7 (64-bit x86_64) (version 7.1 or later)
	Linux 8.1		Red Hat Enterprise Linux(R) Server 8 (64-bit x86_64) (version 8.1 or later)
	Oracle Linux 6.1 (x64)		Oracle Linux(R) Operating System 6 (x64) (version 6.1 or later)
	Oracle Linux 7.1		Oracle Linux(R) Operating System 7 (version 7.1 or later)
	Oracle Linux 8.1		Oracle Linux(R) Operating System 8 (version 8.1 or later)
	SUSE Linux 12		SUSE Linux(R) Enterprise Server 12
	SUSE Linux 15		SUSE Linux(R) Enterprise Server 15
NEM			JP1/Network Element Manager
NNMi			JP1/Network Node Manager i
NNMi Advanced			JP1/Network Node Manager i Advanced
SSO			JP1/SNMP System Observer
SSO - AP			JP1/SNMP System Observer - Agent for Process
UNIX	AIX		AIX V7.1
			AIX V7.2
	HP-UX (IPF)		HP-UX 11i V3 (IPF)
	Solaris	Solaris 11	Solaris 11 (SPARC)
VMware			VMware(R)

C.4 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
ARP	Address Resolution Protocol
CPU	central processing unit
CSV	comma separated values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System

Acronym	Full name or meaning
ESC	Enhanced Security Configuration
FQDN	fully qualified domain name
GIF	Graphics Interchange Format
GUI	graphical user interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	local area network
LLDP	Link Layer Discovery Protocol
MAC	media access control
MIB	management information base
OS	operating system
PC	personal computer
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	uniform resource locator
UTF	Unicode Transformation Format
VPN	virtual private network
WWW	World Wide Web

C.5 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1{,}024^2$ bytes
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

Glossary

D

device

An IT device such as a router, switch, PC, or printer.

discovery seed

A node from which the discovery of the monitoring target nodes starts. If nodes are to be automatically discovered, the ARP cache of the discovery seed is used to discover neighboring devices. For the discovery seed, specify a router that has a lot of information about neighboring devices.

I

incident

Among various events that occur in a network, one with high importance for which information needs to be reported to the administrator. NNMi analyzes the root causes of events that occur in a network, and then reports those root causes as incidents.

instance

The source from which a resource is collected. For example, the instance of the resource **CPU Utilization** is the CPU utilization of each CPU.

L

Layer 2 topology

The connection relationship of a network as seen from the data link layer of the OSI Reference Model. A Layer 2 topology shows the connections between the switches and terminals in the network.

Layer 3 topology

A connection relationship of a network as seen from the network layer of the OSI Reference Model. A Layer 3 topology shows the logical configuration of the network.

lifecycle state

An attribute that is used for checking the progress of an incident. The lifecycle states are **Registered**, **In Progress**, **Completed**, and **Closed**. The state is updated according to the incident-handling status of an incident.

M

management information base (MIB)

Status information that an SNMP server product or SNMP network device releases externally.

MIB object

A unit of management information in the MIB. A MIB object consists of a hierarchical tree structure. Each level of the tree has a unique name and an identifier that indicates the unique name by using a numerical value. Note that a specific value of a MIB object is called an *instance*.

N

node

A device that is monitored by NNMi.

node group

A collection of discovered network devices that are grouped and organized into a hierarchy based on, for example, the IP address or device type.

node group map

A map that categorizes (such as by each business or region) and displays the network devices in each node group.

R

resource

A collection of information that SSO collects from SNMP agents. Examples of resources include **CPU Utilization** and **Run Queue Length**.

root cause analysis (RCA)

Identification of the cause of a failure by investigating and filtering the correlations among various events that occur because of a network failure, and then analyzing the failure based on the Layer 2 topology.

S

SNMP trap

Processing that reports information from an SNMP agent to the SNMP manager when a failure occurs on the SNMP agent.

T

topology map

A network configuration diagram that shows the statuses of discovered network devices and their connection relationships.

Index

Hitachi, Ltd.
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan