HITACHI
Inspire the Next

JP1 Version 11

网络管理 基础指南

3021-3-C05-10(E)

引言

■ 适用产品

JP1/Network Node Manager i（支持的 OS：Windows）

P-2942-82BL JP1/Network Node Manager i11-10

P-2942-83BL JP1/Network Node Manager i Advanced11-10

P-2942-89BL JP1/Network Node Manager i Developer's Toolkit11-00

JP1/SNMP System Observer（支持的 OS：Windows）

P-2942-8RBL JP1/SNMP System Observer11-10

JP1/SNMP System Observer - Agent for Process（支持的 OS：Windows）

P-2A42-8JBL JP1/SNMP System Observer - Agent for Process11-00

JP1/Network Element Manager（支持的 OS：Windows）

P-2942-8CB4 JP1/Network Element Manager for Cisco11-10

P-2942-8DB4 JP1/Network Element Manager for AX Series11-10

JP1/Extensible SNMP Agent for Windows（支持的 OS：Windows）

P-2A42-8BBL JP1/Extensible SNMP Agent for Windows11-00

JP1/Network Node Manager i（支持的 OS：Linux）

P-8242-82BL JP1/Network Node Manager i11-10

P-8242-83BL JP1/Network Node Manager i Advanced11-10

P-8242-89BL JP1/Network Node Manager i Developer's Toolkit11-00

JP1/SNMP System Observer（支持的 OS：Linux）

P-8242-8RBL JP1/SNMP System Observer11-10

JP1/SNMP System Observer - Agent for Process（支持的 OS：Linux）

P-8142-8JBL JP1/SNMP System Observer - Agent for Process11-00

JP1/Extensible SNMP Agent（支持的 OS：Linux）

P-8142-8ABL JP1/Extensible SNMP Agent11-00

JP1/SNMP System Observer - Agent for Process（支持的 OS：UNIX）

P-1M42-8JBL JP1/SNMP System Observer - Agent for Process11-00（支持的 OS：AIX）

P-1J42-8JBL JP1/SNMP System Observer - Agent for Process11-00（支持的 OS：HP-UX (IPF)）

P-9D42-8JBL JP1/SNMP System Observer - Agent for Process11-00（支持的 OS：Solaris）

JP1/Extensible SNMP Agent（支持的 OS：UNIX）

P-1M42-8ABL JP1/Extensible SNMP Agent11-00（支持的 OS：AIX）

P-1J42-8ABL JP1/Extensible SNMP Agent11-00（支持的 OS：HP-UX (IPF)）

P-9D42-8ABL JP1/Extensible SNMP Agent11-00（支持的 OS：Solaris）

■ 商标等

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

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

(http://www.bouncycastle.org)

This product includes software developed by Trantor Standard Systems Inc.

(http://www.trantor.ca)

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

■ 关于微软产品的屏幕截图的使用

已获得微软公司的许可。

■ 发行

2017 年 3 月 3021-3-C05-10(E)

■ 版权

This software and documentation are based in part on software and documentation under license from Hewlett-Packard Company.

变更内容

■ 变更内容（3021-3-C05-10(E)）

添加及变更内容	变更章节
在应用 OS 中，添加了 Windows Server 2016。	—
不支持以下版本的浏览器。 • Internet Explorer 9	1.2.1
更新了 Firefox 的支持版本。	1.2.1，C.4

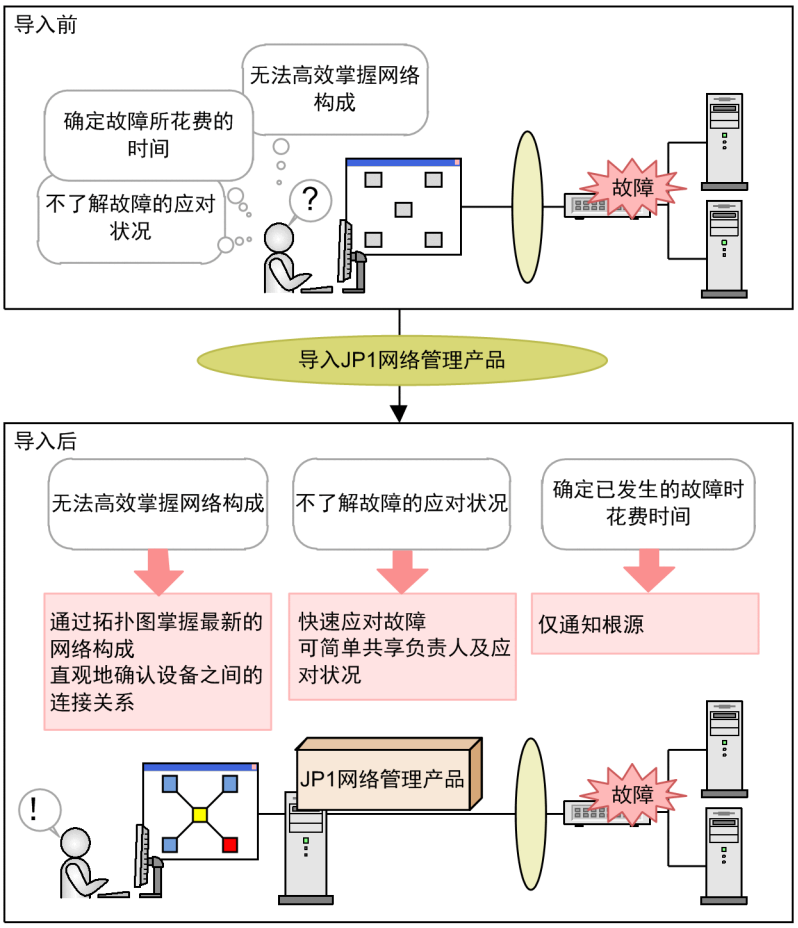
单纯性别字或少字已经更正，恕不另行通知。

请首先阅读本节

■ JP1 网络管理产品能够为您提供的功能

为了提供稳定的环境或服务，网络管理是不可或缺的。但是网络日益复杂，其规模不断扩大，管理员的操作负担也一直增大。

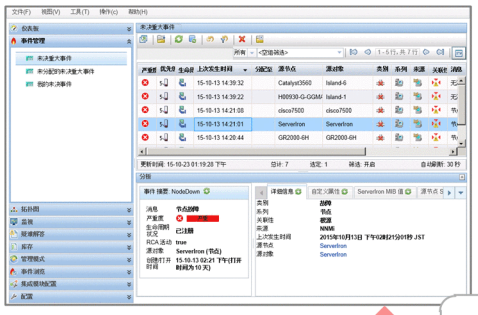
如果您有如下烦恼，请重新评估以往的网络管理及运行方法，导入 JP1 网络管理产品。导入 JP1 网络管理产品，将有助于高效掌握网络构成，迅速确定并解决故障。



另外，JP1 网络管理产品为您展示可直观地掌握网络构成或资源状况的丰富画面，全力支持网络管理员的日常业务。

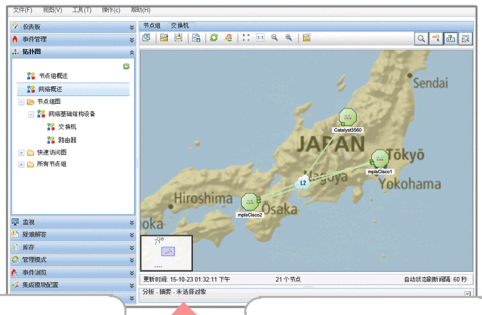
事件管理

仅将根源作为事件进行通知



节点组图

对网络设备进行分类和可视化管理

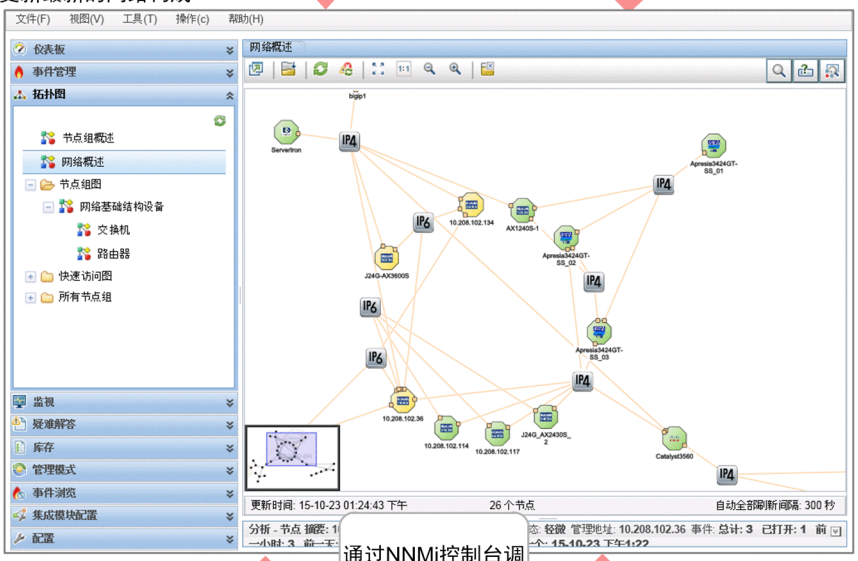


相互切换拓扑图与事件管理

通过自定义节点组图更易于了解拓扑图

拓扑图

自动更新最新的网络构成

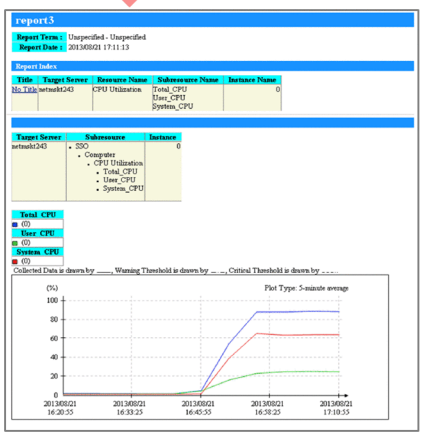


通过NNMi控制台调用SSO的画面

资源浏览器

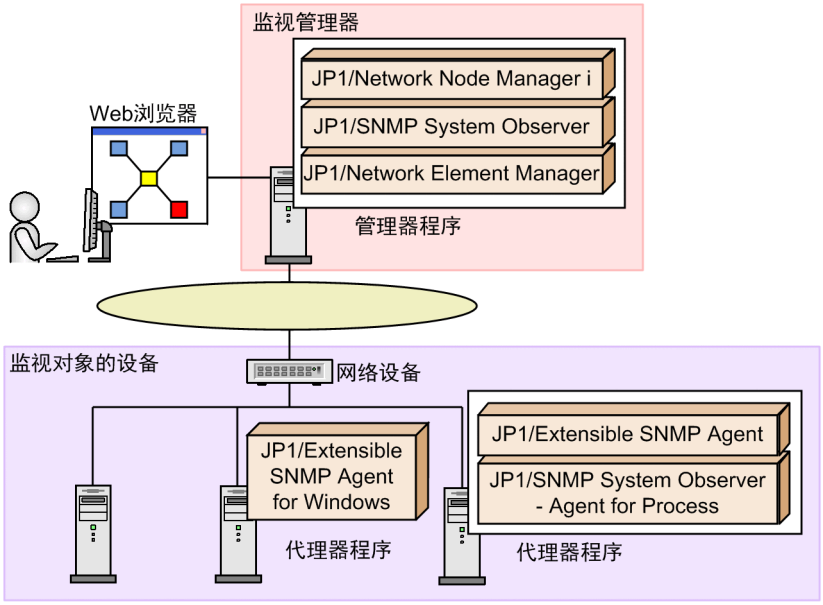
按服务器分别收集资源

报告显示



以易于理解的图表显示资源状况

JP1 网络管理产品由两个程序构成：监视管理器中安装的管理器程序；监视对象服务器中安装的代理器程序。JP1 网络管理产品的基本系统构成如下所示。



JP1/Network Node Manager i（以下简称为 NNMi）

NNMi 是一种管理器程序，采用工业标准的 SNMP 以实现网络构成管理及故障管理。可自动找出 IP 网络上的节点并管理其构成。另外，还可检测网络故障并向管理员发出警告。

JP1/SNMP System Observer（以下简称为 SSO）

SSO 是一种管理器程序，以支持 SNMP 的服务器及网络设备为对象，收集资源并监视进程的存活状况或 Windows 服务状况。可在不考虑网络设备供应商及服务器代理器类型的情况下进行监视。

JP1/Network Element Manager（以下简称为 NEM）

NEM 是一种管理器程序，通过 GUI 面板画面（使用各网络设备的外观图像）对端口状况、插槽构成、有无存储卡等详细信息进行管理。可直观地了解网络设备的状态，因此易于掌握网络设备的状况。另外，仅可在 Windows 的日文环境中使用 NEM。

JP1/Extensible SNMP Agent for Windows 或 JP1/Extensible SNMP Agent（以下简称为 ESA）

ESA 是一种代理器程序，可通过 SNMP 获取 CPU、内存、文件系统等信息。可获取无法通过操作系统标配的 SNMP 代理器获取的信息。JP1/SNMP System Observer - Agent for Process 的前提程序。

JP1/SNMP System Observer - Agent for Process（以下简称为 SSO - AP）

SSO - AP 是一种代理器程序，通过 SNMP 对服务器上运行的进程及服务进行管理。

管理器程序的主要功能如下表所示。

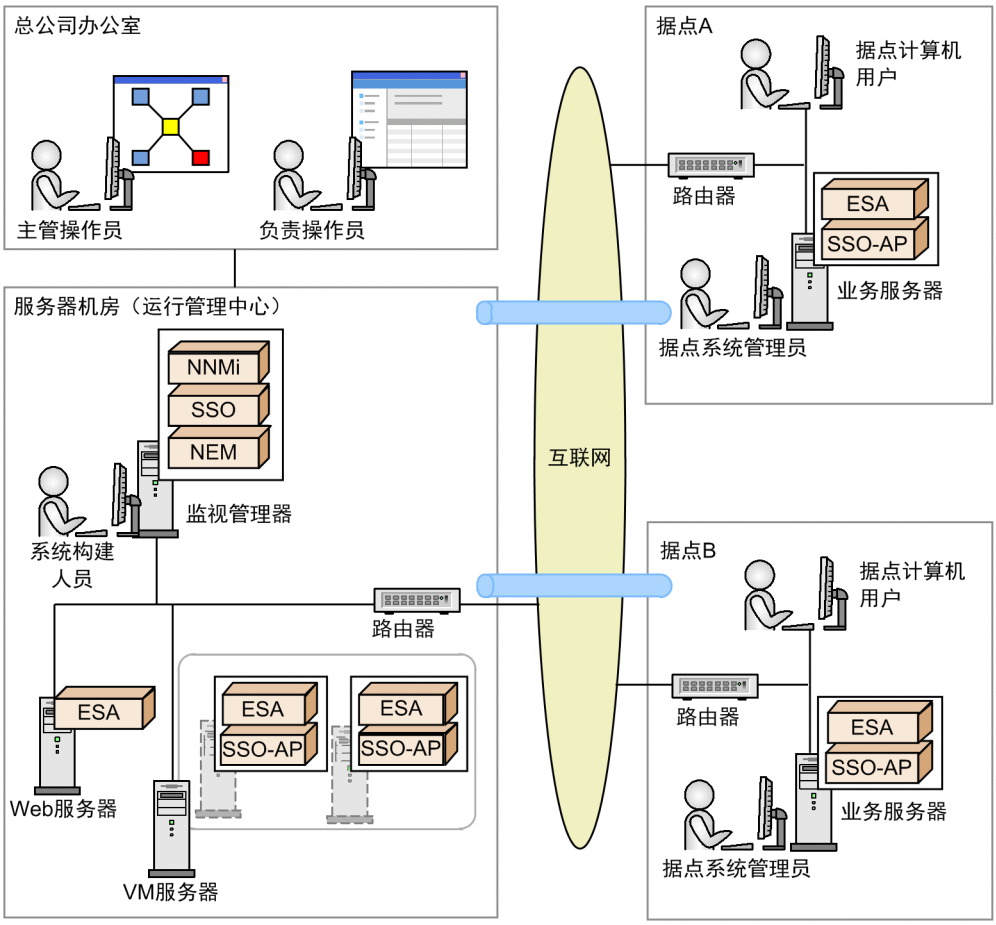
产品名称	功能名称	功能说明
NNMi	节点的发现	根据配置的规则自动发现节点。另外，也可以手动添加节点。

产品名称	功能名称	功能说明
	拓扑的发现与显示	除了层 3 拓扑（逻辑网络构成）之外，还会自动发现层 2 拓扑（物理接线的网络构成），并将其显示在图中。
	通过 ICMP/SNMP 轮询或 SNMP 陷阱进行的监视	通过 ICMP/SNMP 轮询监视对象的状况。另外，通过 SNMP 陷阱监视故障。
	根源分析	根据发现的层 2 拓扑及层 3 拓扑分析故障根源。
	事件管理	将通过轮询或 SNMP 陷阱发现的故障作为事件进行通知。
	自动操作	可根据事件的状况，作为自动操作执行任意命令。
SSO	资源收集	监视各种系统资源（如 CPU 使用率、内存使用率等服务器运行信息以及线路使用率等网络性能信息）。
	进程及服务监视	可通过进程或服务的状况监视任意应用程序的运行状况。
NEM	面板操作	打开显示网络设备（开关与路由器）外观图像的窗口。通过选择菜单，可进行各设备的状况监视及操作。

■ 本说明书的内容

本说明书对 JP1 网络管理产品的基本构建方法及运行方法进行说明。本说明书的目的在于：用户在阅读本说明书后，可通过 JP1 网络管理产品进行日常的网络管理以及迅速解决网络故障。

本说明书根据下述系统及组织构成对运行步骤进行说明。

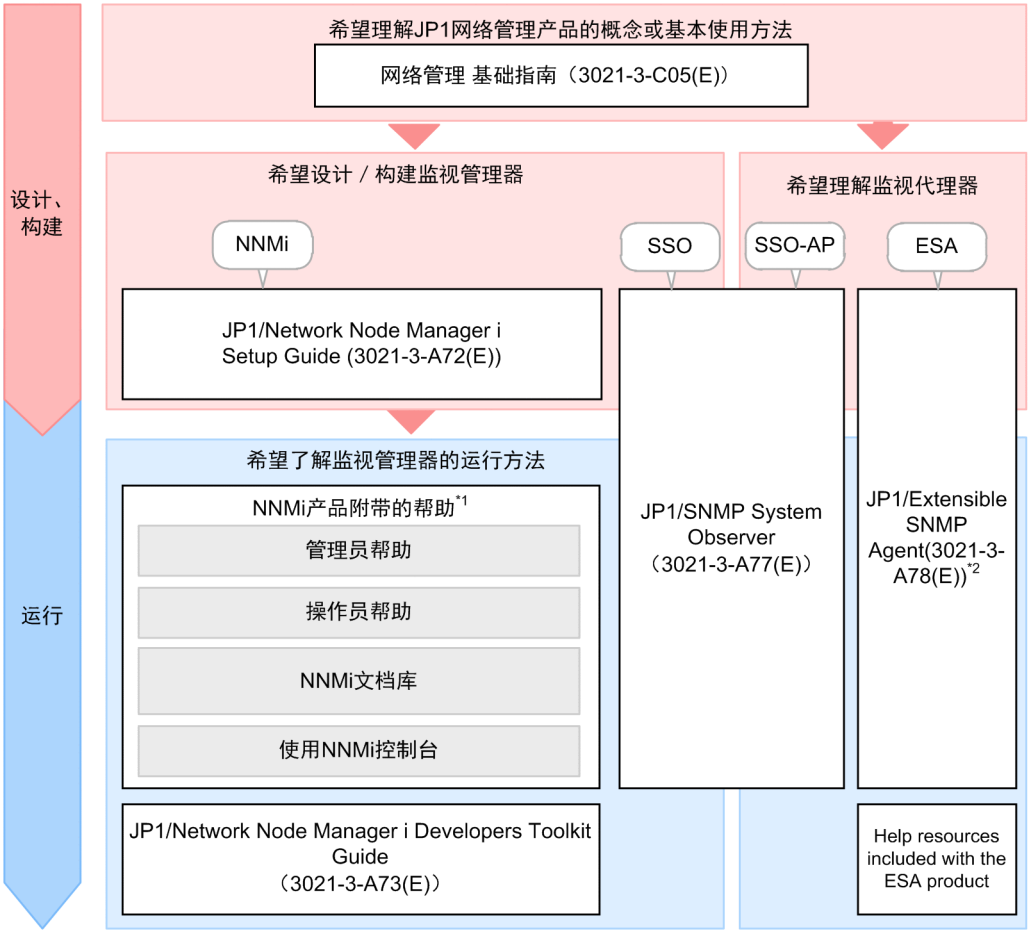


本说明书说明的构建步骤

1. 主管操作员委托系统构建人员进行 JP1 网络管理产品的环境构建。
2. 系统构建人员准备作为监视管理器的服务器，构建管理器环境。
3. 系统构建人员委托据点系统管理员进行代理器环境的构建。
4. 据点系统管理员构建代理器环境，并告知系统构建人员。
5. 接到通知的系统构建人员对 JP1 网络管理产品进行配置。
6. 完成 JP1 网络管理产品的配置后，系统构建人员将此事宜告知主管操作员。
7. 接到通知的主管操作员将负责操作员注册为用户，开始运行 JP1 网络管理产品。

■ 本说明书的使用方法

除了本说明书之外，JP1 网络管理产品还提供多种说明书及帮助。如要进一步了解应用功能或操作，请根据目的阅读如下说明书和帮助。



注*1　可从NNMi控制台的［帮助］显示帮助。
注*2　没有Windows版本的“JP1/Extensible SNMP Agent（3021-3-A78(E)）”。
关于产品的详细情况，请参照帮助或发布说明。

需要参阅其他说明书时，本说明书采用‘关于……，请参照《△△》中“○○”的说明’的句式进行记述。请以‘○○’为关键词在《△△》内进行检索并阅读相关说明。

本说明书以下列环境为前提进行说明。

监视管理器及监视代理器的操作

Windows 环境：使用 Windows Server 2008 R2 的环境

Linux 环境：使用 Linux 6.1 (x64)的环境

Web 浏览器的操作

使用 Internet Explorer 10 的环境

本说明书中刊载的画面可能会因产品改进等而与实际使用产品的画面存在部分差异，敬请谅解。

目录

1

JP1 网络管理产品的构建

安装 JP1 网络管理产品，构建网络监视环境。

1.1 JP1 网络管理产品的构建流程

如要构建 JP1 网络管理产品，需要构建监视管理器及监视代理器。在 Windows 与 Linux 中构建监视管理器及监视代理器时，其构建步骤各不相同。

监视管理器的构建流程如下所示。

操作概述	顺序	操作内容	参照章节	
			Windows	Linux
安装前的准备	1	确认服务器环境	1.2.1	
	2	确认监视管理器的前提条件	1.2.2	1.2.3
监视管理器的构建	3	安装 NNMi	1.3.1	1.4.1
	4	安装 SSO	1.3.2	1.4.2
	5	安装 NEM	1.3.3	-
	6	设置 NNMi	1.3.4	1.4.3
	7	设置 SSO	1.3.5	1.4.4

监视代理器的构建流程如下所示。构建监视代理器时，根据据点的监视代理器数量重复下述操作。

操作概述	顺序	操作内容	参照章节	
			Windows	Linux
安装前的准备	1	确认服务器环境	1.2.1	
监视代理器的构建	2	确认监视代理器的前提条件	-	1.6.1
	3	安装 ESA	1.5.1	1.6.2
	4	安装 SSO - AP	1.5.2	1.6.3
	5	设置 ESA	1.5.3	1.6.4
	6	设置 SSO - AP	-	1.6.5
	7	重新启动监视代理器	-	1.6.6

提示

请委托各据点的系统管理员构建监视代理器。如果未完成监视代理器的构建，则不能配置 JP1 网络管理产品。

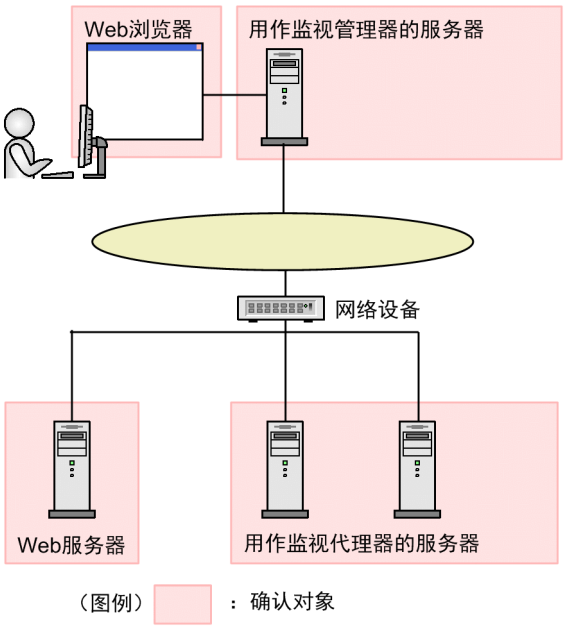
1.2 安装前的准备

1.2.1 确认服务器环境

在安装 JP1 网络管理产品前，确认用于运行的服务器环境是否适当。

前提条件

在本说明书中设想的系统构成如下所示。



操作步骤

1. 检查用作监视管理器的服务器的规格是否符合下列条件：

   - 操作系统：

     Windows 环境：Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 或 Windows Server 2016

     Linux 环境：CentOS 6.1（x64）、CentOS 7.1、Linux 6.1（x64）、Linux 7.1、Oracle Linux 6.1（x64）、Oracle Linux 7.1 或 SUSE Linux 12

     另外，本说明书对 Windows Server 2008 R2 及 Linux 6.1（x64）的构建步骤进行说明。

   - 硬盘可用空间：

     Windows 环境：不少于 14.5GB

     Linux 环境：不少于 14.0GB

   - 内存：

     Windows 环境：不少于 4.5GB

     Linux 环境：不少于 6.0GB

2. 检查用作监视代理器的服务器的规格是否符合下列条件：

- 操作系统：

  Windows 环境：Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 或 Windows Server 2016

  Linux 环境：CentOS 6.1（x64）、CentOS 7.1、Linux 6.1（x64）、Linux 7.1、Oracle Linux 6.1（x64）、Oracle Linux 7.1 或 SUSE Linux 12

  UNIX 系统：HP-UX（IPF）、AIX V6.1、AIX V7.1、Solaris 10 或 Solaris 11

  另外，本说明书对 Windows Server 2008 R2 及 Linux 6.1（x64）的构建步骤进行说明。

- 硬盘可用空间：

  Windows 环境：不少于 65.0MB

  Linux 环境：不少于 150.0MB

- 内存：

  Windows 环境：不少于 15.0MB

  Linux 环境：不少于 70.0MB

3. 确认用作监视管理器的服务器的语言配置。

在 Windows 环境中，配置如下区域设置。

- 日文环境：日文
- 英文环境：英文
- 中文环境：中文

在 Linux 环境中，配置如下区域设置。

- 日文环境：ja_JP.UTF-8
- 英文环境：C
- 中文环境：zh_CN.utf8

4. 确认 Web 服务器的端口号。

安装 NNMi 时，使用 Web 服务器的端口号。默认值为 80。

5. 确认使用的 Web 浏览器符合下列条件：

- Web 浏览器：

  Windows 环境：Internet Explorer 10、11 或 Firefox ESR 45

  Linux 环境：Firefox ESR 45

- Adobe Flash Player：

  应备有 NNMi 所需的 Adobe Flash Player。关于详细情况，请参照发布说明。

- Java Plug In：

  应备有 SSO 所需的 Java Plug In。关于详细情况，请参照发布说明。

下一步操作

确认服务器环境没有问题后，确认前提条件。

相关项目

- 《JP1/Network Node Manager i Setup Guide》中“Preinstallation Checklists”的说明
- 1.2.2　确认监视管理器的前提条件（Windows 环境）
- 1.2.3　确认监视管理器的前提条件（Linux 环境）

1.2.2　确认监视管理器的前提条件（Windows 环境）

在 Windows 环境中使用监视管理器时，确认下述配置后，开始安装 JP1 网络管理产品。关于前提条件的详细情况，请参照《JP1/Network Node Manager i Setup Guide》中“Preinstallation Checklists”的说明。

操作步骤

1. 确认监视管理器的主机名。

   配置陷阱目标机器或登录时，使用该主机名。

2. 确认没有使用监视管理器的端口号。

   通过命令提示符执行“netstat -an”后，可确认当前使用的端口号。

   关于端口号的详细情况，请参照《JP1/Network Node Manager i Setup Guide》中“List of Ports Used by NNMi”的说明。关于 SSO，请参照发布说明中的“Port Number Settings”。

3. 将固定 IP 地址分配给监视管理器。

   请将 IP 地址设为固定分配，不要设为 DHCP 动态分配。

4. 事先准备 NNMi 安装目标文件夹。

   安装时，使用 NNMi 安装目标文件夹。默认文件夹如下所示。

   - 用于程序：C:\Program Files (x86)\Hitachi\Cm2NNMi\
   - 用于数据：C:\ProgramData\Hitachi\Cm2NNMi\

5. 事先准备 SSO 的安装目标文件夹。

   安装时，使用 SSO 安装目标文件夹。默认文件夹如下所示。

   - C:\Program Files\HITACHI\JP1SSO\

6. 将防病毒软件设为无效。

   仅在安装 JP1 网络管理产品期间禁用防病毒软件。

7. 禁用 Windows 的 SNMP 相关服务的 SNMP Trap 服务。

8. 如要使用 SNMP 对监视管理器进行监视，请导入 SNMP 服务。

9. 确认 Windows 防火墙已配置为允许对监视管理器的端口进行访问。

   关于访问端口号的详细情况，请参照《JP1/Network Node Manager i Setup Guide》中“Firewall pass-through direction”的说明。

10. 检查环境变量 TEMP 及 TMP 的设定值是否相同。

    如果环境变量 TEMP 及 TMP 的值不同，可能导致 NNMi 安装失败。如果设有不同的值，请设定相同的值。另外，安装时将使用 500.0MB 的%TEMP%文件夹。

11. 依次点击［管理工具］-［远程桌面服务］-［远程桌面会话主机构成］，配置远程桌面如下所示。

    - 结束时不删除临时文件夹
    - 不对各会话分别使用临时文件夹

下一步操作

确认前提环境没有问题后，进至监视管理器的构建。

相关项目

- 1.3　监视管理器的构建（Windows 环境）

1.2.3　确认监视管理器的前提条件（Linux 环境）

在 Linux 环境中使用监视管理器时，确认下述配置后，开始安装 JP1 网络管理产品。关于前提条件的详细情况，请参照《JP1/Network Node Manager i Setup Guide》中“Preinstallation Checklists”的说明。

操作步骤

1. 确认监视管理器的主机名。

   配置陷阱目标机器或登录时使用主机名。

2. 确认未使用监视管理器所用端口号。

   通过命令提示符执行“netstat -an”后，可确认当前使用的端口号。

   关于端口号的详细情况，请参照《JP1/Network Node Manager i Setup Guide》中“List of Ports Used by NNMi”的说明。

3. 将固定 IP 地址分配给监视管理器。

   请将 IP 地址设为固定分配，不要设为 DHCP 动态分配。

4. 禁用防病毒软件。

   仅在安装 JP1 网络管理产品期间禁用防病毒软件。

5. 确认已安装下列软件包及库文件。

   - kernel-2.6.32-220.4.2.el6.x86_64.rpm 或更新的版本

- kernel-firmware-2.6.32-220.4.2.el6.noarch.rpm 或更新的版本
- /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)

另外，请安装各种存在依赖关系的库文件。所需的软件包及库文件可能因操作系统的类别或版本而异。关于详细情况，请参照发布说明。

6. 打开/etc/sysctl.conf 文件，配置内核参数。

请在/etc/sysctl.conf 文件中添加下述条目。

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

本说明书中的配置如下：将共享内存（kernel.shmmax）设为 64.0GB；将 UDP 接收缓存（net.core.rmem_max）设为 8.0MB；将 UDP 发送缓存（net.core.wmem_max）设为 2.0MB。使用嵌入式数据库时，需要配置共享内存（kernel.shmmax）。

下一步操作

确认前提环境没有问题后，进至监视管理器的构建。

相关项目

- 1.4　监视管理器的构建（Linux 环境）

1.2.4　各产品的命令保存位置

各产品的命令保存位置如下所示。

NNMi 命令保存位置

- Windows 环境
  NNMi 安装目标文件夹\bin\
- Linux 环境
  /opt/OV/bin/

SSO 命令保存位置

- Windows 环境
  SSO 安装目标文件夹\bin\
- Linux 环境
  /opt/CM2/SSO/bin/

SSO - AP 命令保存位置

- Windows 环境
  SSO - AP 安装目标文件夹\bin\
- Linux 环境
  /opt/CM2/APM/bin/

ESA 命令保存位置

- Windows 环境
  ESA 安装目标文件夹\bin\
- Linux 环境
  /opt/CM2/ESA/bin/

1.3 监视管理器的构建（Windows 环境）

安装并设置 NNMi、SSO 及 NEM，在 Windows 环境中构建监视管理器。

1.3.1 安装 NNMi（Windows 环境）

在 Windows 环境中使用监视管理器时，通过 Hitachi Integrated Installer 跟随向导安装 NNMi。

操作步骤

1. 以 Administrators 身份登录用作监视管理器的服务器，并装入附带的介质。
2. 选择“JP1/Network Node Manager i”。
   将显示 NNMi 设定值的确认画面。
3. 指定 Web 服务器的端口号并按下［Enter］键。
   如果不输入值，直接按下［Enter］键，将自动指定默认值。默认值为 80。
4. 指定 NNMi 安装目标文件夹。
   如果不输入值，直接按下［Enter］键，将自动指定默认文件夹。默认文件夹如下所示。
   - 用于程序：C:\Program Files (x86)\Hitachi\Cm2NNMi\
   - 用于数据：C:\ProgramData\Hitachi\Cm2NNMi\

   安装目标文件夹（用于数据）中保存有 NNMi 的配置文件、数据库与日志文件等。
5. 输入“yes”并按下［Enter］键。
   将开始安装 NNMi。完成后，命令提示符将自动关闭。

下一步操作

接下来，安装 SSO。

相关项目

- 1.3.2 安装 SSO（Windows 环境）

1.3.2 安装 SSO（Windows 环境）

在 Windows 环境中使用监视管理器时，通过 Hitachi Integrated Installer 跟随向导安装 SSO。

操作步骤

1. 以 Administrators 身份登录用作监视管理器的服务器，并装入附带的介质。

2. 选择“JP1/SNMP System Observer”。

3. 根据安装器的指示，安装 SSO。

下一步操作

使用 NEM 支持的交换机或路由器时，安装 NEM。无需安装 NEM 时，进至 NNMi 的设置步骤。

相关项目

- 1.3.3　安装 NEM（Windows 环境）
- 1.3.4　设置 NNMi（Windows 环境）

1.3.3　安装 NEM（Windows 环境）

在 Windows 环境中使用监视管理器的情况下，使用 NEM 支持的交换机或路由器时，安装 NEM。请通过 Hitachi Integrated Installer 跟随向导安装 NEM。

操作步骤

1. 以 Administrators 身份登录用作监视管理器的服务器，并装入附带的介质。

2. 选择“JP1/Network Element Manager”。

3. 根据安装器的指示，安装 NEM。

下一步操作

接下来，设置 NNMi。

相关项目

- 1.3.4　设置 NNMi（Windows 环境）

1.3.4　设置 NNMi（Windows 环境）

在 Windows 环境中使用监视管理器时，停止 NNMi 服务，并设定系统账号。如要注册其他成员，请在登录 NNMi 控制台后注册用户。

前提条件

如果已在安装前打开命令提示符，请在关闭后重新打开。

操作步骤

1. 通过命令提示符执行 ovstop -c，停止 NNMi 服务。

   NNMi 服务将停止。安装后，NNMi 服务暂时处于停止状态。

2. 执行 nnmchangesyspw.ovpl，设定密码。
   输入“y”后，按照消息指定密码。

3. 执行 ovstart -c，启动 NNMi。

4. 执行 ovstatus -c，确认 NNMi 的状态。
   如果所有状态处于执行状态，则属正常。

下一步操作

接下来，设置 SSO。

相关项目

- 1.2.4　各产品的命令保存位置
- 2.2.3　注册用户
- 1.3.5　设置 SSO（Windows 环境）

1.3.5　设置 SSO（Windows 环境）

在 Windows 环境中使用监视管理器时，配置团体名或 SSO 定义信息后，设置 SSO。

(1)　添加从 SSO 连接 NNMi 的信息

执行 SSO 的 ssonnmsetup 命令，配置用于与 NNMi 连动的连接信息。

操作步骤

1. 执行下列命令。
   ssonnmsetup -add -user 用户名 -password 密码 -port 端口号 -ssl
   指定系统账号的用户名及密码。将 Web 服务器的端口号指定为端口号。仅在通过 https 进行通信时指定-ssl 选项。

相关项目

- 1.2.4　各产品的命令保存位置
- 1.3.4　设置 NNMi（Windows 环境）
- 1.2.1　确认服务器环境

(2)　在 NNMi 中配置 SSO 定义信息

执行命令，在 NNMi 中配置 SSO 定义信息。

操作步骤

1. 执行 NNMi 的 nnmconfigimport.ovpl 命令，配置事件定义。
   nnmconfigimport.ovpl -u 用户名 -p 密码 -f SSO 安装目标文件夹\incident\ssoincident.def
   指定系统账号的用户名及密码。
   在将不使用 TCP 通信进行事件通知的 APM 作为进程及服务监视对象时，还需要配置下述事件定义。
   nnmconfigimport.ovpl -u 用户名 -p 密码 -f SSO 安装目标文件夹\incident\apmtrap.def
2. 执行 NNMi 的 nnmconfigimport.ovpl 命令，配置 URL 操作定义。
   nnmconfigimport.ovpl -u 用户名 -p 密码 -f SSO 安装目标文件夹\urlaction\ssourlaction.def
   指定系统账号的用户名及密码。
3. 执行 SSO 的 ssoauth 命令，将用户注册到 SSO 中。
   ssoauth -add -user 用户名 -password 密码
   配置用于通过 SSO 控制台登录的用户名及密码。
4. 执行 SSO 的 ssostart 命令，启动 SSO。
5. 执行 SSO 的 ssostart 命令，确认 SSO 的状态。
   如果所有状态处于执行状态，则属正常。

相关项目

- 1.2.4 各产品的命令保存位置

(3) 配置团体名

团体名是指使用 SNMP 协议访问 MIB 对象的密码。收集资源时，需要使监视代理器与监视管理器的 get 团体名一致；监视进程及服务时，需要使监视代理器与监视管理器的 set 团体名一致。

操作步骤

1. 打开 SNMP 定义文件（SSO 安装目标文件\conf\ssosnmp.conf）。
2. 编辑 SNMP 定义文件。
3. 如下所示，执行 ssoapcom 命令，重新读入定义文件。
   ssoapcom -r
4. 如下所示，执行 ssocollectd 命令，重新读入定义文件。
   ssocollcetd -r

下一步操作

监视管理器的构建至此结束。请确认已构建据点的监视代理器。已构建据点的监视代理器时，进至 JP1 网络管理产品的配置步骤。

相关项目

- 1.2.4　各产品的命令保存位置
- 1.3.4　设置 NNMi（Windows 环境）
- 1.5　监视代理器的构建（Windows 环境）
- 2.　JP1 网络管理产品的配置

1.4 监视管理器的构建（Linux 环境）

安装并设置 NNMi 及 SSO，在 Linux 环境中构建监视管理器。

1.4.1 安装 NNMi（Linux 环境）

在 Linux 环境中使用监视管理器时，通过 Hitachi Integrated Installer 跟随向导安装 NNMi。

操作步骤

1. 以 root 身份登录用作监视管理器的服务器。
2. 在环境变量“LC_ALL”中配置如下区域设置。
   - 日文环境

     # LC_ALL=ja_JP.UTF-8

     # export LC_ALL
   - 英文环境

     # LC_ALL=C

     # export LC_ALL
   - 中文环境

     # LC_ALL=zh_CN.utf8

     # export LC_ALL
3. 装入 NNMi 附带的介质，并执行下列命令。

   /附带的介质的安装目录名/X64LIN/setup /附带的介质的安装目录名
4. 在 Hitachi PP Installer 的初始画面上输入“I”。
5. 选择“JP1/Network Node Manager i”并输入“I”。

   将显示确认是否继续安装的信息。
6. 输入“Y”。
7. 根据安装器的指示，输入信息。

   如果不输入值，直接按下［Enter］键，将指定默认值。

   将 NNMi 安装到下列文件夹中。
   - 用于程序：/opt/OV/
   - 用于数据：/var/opt/OV/

下一步操作

接下来，安装 SSO。

相关项目

- 1.4.2　安装 SSO（Linux 环境）

1.4.2　安装 SSO（Linux 环境）

在 Linux 环境中使用监视管理器时，通过 Hitachi Integrated Installer 跟随向导安装 SSO。

操作步骤

1. 以 root 身份登录用作监视管理器的服务器，并装入附带的介质。
2. 执行下列命令。
   /附带的介质的安装目录名/X64LIN/setup /附带的介质的安装目录名
3. 在 Hitachi PP Installer 的初始画面上输入“I”。
4. 选择“JP1/SNMP System Observer”并输入“I”。
   将显示确认是否继续安装的信息。
5. 输入“Y”。
   将安装 SSO。

下一步操作

接下来，设置 NNMi。

相关项目

- 1.4.3　设置 NNMi（Linux 环境）

1.4.3　设置 NNMi（Linux 环境）

在 Linux 环境中使用监视管理器时，配置语言环境及系统账号，并设置 NNMi。

(1)　配置语言环境

NNMi 的安装结束后，需要在/etc/init.d/netmgt 文件中添加语言配置。

操作步骤

1. 打开/etc/init.d/netmgt 文件。

2. 在“/opt/OV/bin/ovstart”的前一行添加下列 2 行。

   - 日文环境

     LANG=ja_JP.UTF-8

     export LANG
   - 英文环境

     LANG=C

     export LANG
   - 中文环境

     LANG=zh_CN.utf8

     export LANG

3. 覆盖保存/etc/init.d/netmgt 文件。

   语言环境配置至此结束。

(2) 配置系统账号

配置 NNMi 的系统账号。配置方法与 Windows 环境相同。

系统账号的配置结束后，设置 SSO。

相关项目

- 1.2.4 各产品的命令保存位置
- 1.3.4 设置 NNMi（Windows 环境）
- 1.4.4 设置 SSO（Linux 环境）

1.4.4 设置 SSO（Linux 环境）

在 Linux 环境中使用监视管理器时，配置语言环境及定义信息后，设置 SSO。

(1) 配置语言环境

SSO 的安装结束后，需要在/etc/rc.d/init.d/sso 文件中添加语言配置。

操作步骤

1. 打开/etc/rc.d/init.d/sso 文件。
2. 在“/etc/rc.d/init.d/functions”前一行添加下列 2 行。

   - 日文环境

     LANG=ja_JP.UTF-8

export LANG

- 英文环境

  LANG=C

  export LANG

- 中文环境

  LANG=zh_CN.utf8

  export LANG

3. 覆盖保存/etc/rc.d/init.d/sso 文件。

   语言环境配置至此结束。

(2) 添加从 SSO 连接 NNMi 的信息

配置用于与 NNMi 连动的连接信息。配置方法与 Windows 环境相同。

相关项目

- 1.3.5(1) 添加从 SSO 连接 NNMi 的信息

(3) 在 NNMi 中配置 SSO 定义信息

执行命令，在 NNMi 中配置 SSO 定义信息。

操作步骤

1. 执行 NNMi 的执行 nnmconfigimport.ovpl 命令，配置事件定义。

   nnmconfigimport.ovpl -u 用户名 -p 密码 -f /etc/opt/CM2/SSO/incident/ssoincident.def

   指定系统账号的用户名及密码。

   在将不使用 TCP 通信进行事件通知的 APM 作为进程及服务监视对象时，还需要配置下述事件定义。

   nnmconfigimport.ovpl -u 用户名 -p 密码 -f SSO 安装目标文件夹\incident\apmtrap.def

2. 执行 NNMi 的 nnmconfigimport.ovpl 命令，配置 URL 操作定义。

   nnmconfigimport.ovpl -u 用户名 -p 密码 -f /etc/opt/CM2/SSO/urlaction/ssourlaction.def

   指定系统账号的用户名及密码。

3. 执行 SSO 的 ssoauth 命令，将用户注册到 SSO 中。

   ssoauth -add -user 用户名 -password 密码

   配置用于通过 SSO 控制台登录的用户名及密码。

4. 执行 SSO 的 ssostart 命令，启动 SSO。

5. 执行 SSO 的 ssostart 命令，确认 SSO 的状态。

   如果所有状态处于执行状态，则属正常。

相关项目

- 1.2.4　各产品的命令保存位置

(4)　配置团体名

团体名是指使用 SNMP 协议访问 MIB 对象的密码。收集资源时，需要使监视代理器与监视管理器的 get 团体名一致；监视进程及服务时，需要使监视代理器与监视管理器的 set 团体名一致。

操作步骤

1. 打开 SNMP 定义文件（/etc/opt/CM2/SSO/conf/ssosnmp.conf）。
2. 编辑 SNMP 定义文件。
3. 如下所示，执行 ssoapcom 命令，重新读入定义文件。

   ssoapcom -r
4. 如下所示，执行 ssocollectd 命令，重新读入定义文件。

   ssocollcetd -r

下一步操作

配置团体名后，确认已构建据点的监视代理器。已构建据点的监视代理器时，进至 JP1 网络管理产品的配置步骤。

相关项目

- 1.2.4　各产品的命令保存位置
- 1.3.5(2)　在 NNMi 中配置 SSO 的定义信息
- 1.6　监视代理器的构建（Linux 环境）
- 2.　JP1 网络管理产品的配置

1.5 监视代理器的构建（Windows 环境）

在 Windows 的监视代理器中安装并设置 ESA 及 SSO - AP，构建监视代理器。

> **提示**
>
> 建议在不影响业务的时间段安装监视管理器。

1.5.1 安装 ESA（Windows 环境）

在 Windows 环境中使用监视代理器时，请通过 Hitachi Integrated Installer 跟随向导安装 ESA。

操作步骤

1. 确认已安装 Windows 的 SNMP 服务。

   未安装 Windows 的 SNMP 服务时，请进行安装。关于 Windows 的 SNMP 服务的安装，请参照 Windows 的说明书。

2. 在安装代理器的机器的 hosts 文件（系统根文件夹\system32\drivers\etc\hosts）中配置下列主机名。
   - 监视管理器的主机名
   - 监视代理器的主机名

3. 以 Administrators 身份登录用于安装代理器的机器，并装入附带的介质。

4. 选择“JP1/Extensible SNMP Agent”。

5. 根据安装器的指示，安装 ESA。

6. 启动 Windows 的 SNMP 服务。

7. 执行 ESA 的 snmpcheck 命令，确认 ESA 的状态。

   如果 hismsmib 以外的所有状态处于执行状态，则属正常。

8. 停止 Windows 的 SNMP 服务。

下一步操作

接下来，安装 SSO - AP。

相关项目

- 1.2.4 各产品的命令保存位置
- 1.5.2 安装 SSO - AP（Windows 环境）

1.5.2　安装 SSO - AP（Windows 环境）

在 Windows 环境中使用监视代理器时，请通过 Hitachi Integrated Installer 跟随向导安装 SSO - AP。

操作步骤

1. 以 Administrators 身份登录用于安装代理器的机器，并装入附带的介质。
2. 选择“JP1/SNMP System Observer - Agent for Process”。
3. 根据安装器的指示，安装 SSO - AP。
4. 启动 Windows 的 SNMP System Observer - Agent for Process 服务。
5. 执行 SSO - AP 的 apmcheck 命令，确认 SSO - AP 的状态。
   如果所有状态处于执行状态，则属正常。

下一步操作

接下来，设置 ESA。

相关项目

- 1.2.4　各产品的命令保存位置
- 1.5.3　设置 ESA（Windows 环境）

1.5.3　设置 ESA（Windows 环境）

在 Windows 环境中使用监视代理器时，在 Windows 的 SNMP 服务中配置团体名及陷阱目标机器。

(1)　在 Windows 的 SNMP 服务中配置团体名

团体名是指使用 SNMP 协议访问 MIB 对象的密码。收集资源或监视进程及服务时，需要使监视代理器与监视管理器的团体名一致。

配置团体名时，需从 Windows 的［服务］画面显示［SNMP Service］属性。关于详细情况，请参照 Windows 的说明书。

(2)　在 Windows 的 SNMP 服务中配置陷阱目标机器

陷阱目标机器用于确定 SNMP 陷阱的发送目标，并确认接收监视代理器陷阱的管理器。如要将陷阱发送至监视管理器，需要在监视代理器中配置陷阱目标机器。

操作步骤

1. 从 Windows 的［服务］画面显示［SNMP Service］属性后，配置陷阱目标机器。

关于详细情况，请参照 Windows 的说明书。

下一步操作

接下来，进行通过 JP1 网络管理产品监视网络的配置。

相关项目

- 2. JP1 网络管理产品的配置

1.6 监视代理器的构建（Linux 环境）

在 Linux 的监视代理器中安装并设置 ESA 及 SSO - AP，构建监视代理器。

> **提示**
>
> 建议在不影响业务的时间段安装监视管理器。

1.6.1 确认监视代理器的前提条件（Linux 环境）

在 Linux 环境中使用监视代理器时，确认下述配置后，开始安装监视代理器。

操作步骤

1. 确认已将下列软件包或后续补丁应用于操作系统。
   - 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

   所需的软件包可能因操作系统的类别或版本而异。关于应用的软件包的详细情况，请参照发布说明。
2. 确认已安装用于获取 MIB 值的下列命令。
   - /usr/bin/vmstat
   - /bin/ps
   - /usr/bin/uptime
   - /usr/bin/free
   - /usr/bin/mpstat
3. 确认已安装原生代理器。

   未安装原生代理器时，请进行安装。关于原生代理器的安装，请参照《JP1/Extensible SNMP Agent》中“Notes about installation”的说明。

下一步操作

确认监视代理器的前提条件后，安装 ESA。

相关项目

- 1.2.4　各产品的命令保存位置
- 1.6.2　安装 ESA（Linux 环境）

1.6.2　安装 ESA（Linux 环境）

在 Linux 环境中使用监视代理器时，请通过 Hitachi Integrated Installer 跟随向导安装 ESA。

1. 在/etc/hosts 文件中配置与监视代理器主机名相应的 IP 地址。
   （例）11.22.33.44 esahost
2. 以 root 身份登录安装代理器的机器，并装入附带的介质。
3. 执行下列命令。
   /附带的介质的安装目录名/linux/setup /附带的介质的安装目录名
4. 在 Hitachi PP Installer 的初始画面上输入“I”。
5. 选择“JP1/Extensible SNMP Agent”并输入“I”。
   将显示确认是否继续安装的信息。
6. 输入“Y”。
7. 根据安装器的指示，输入信息。
   如果不输入值，直接按下［Enter］键，将指定默认值。

下一步操作

ESA 的安装至此结束。接下来，安装 SSO - AP。

相关项目

- 1.6.3　安装 SSO - AP（Linux 环境）

1.6.3　安装 SSO - AP（Linux 环境）

在 Linux 环境中使用监视代理器时，请通过 Hitachi Integrated Installer 跟随向导安装 SSO - AP。

操作步骤

1. 以 root 身份登录安装代理器的机器，并装入附带的介质。
2. 执行下列命令。
   /附带的介质的安装目录名/linux/setup /附带的介质的安装目录名

3. 在 Hitachi PP Installer 的初始画面上输入“I”。

4. 选择“JP1/SSO - Agent for Process”并输入“I”。

   将显示确认是否继续安装的信息。

5. 输入“Y”。

6. 根据安装器的指示，安装 SSO - AP。

下一步操作

SSO - AP 的安装至此结束。接下来，设置 ESA。

相关项目

- 1.6.4　设置 ESA（Linux 环境）

1.6.4　设置 ESA（Linux 环境）

在 Linux 环境中使用监视代理器时，在构成定义文件（/etc/SnmpAgent.d/snmpd.conf）中配置团体名与陷阱目标机器。在已安装代理器的机器中保存有构成定义文件。

(1)　配置团体名

团体名是指使用 SNMP 协议访问 MIB 对象的密码。收集资源时，需要使监视代理器与监视管理器的 get 团体名一致；监视进程及服务时，需要使监视代理器与监视管理器的 set 团体名一致。

操作步骤

1. 打开构成定义文件（/etc/SnmpAgent.d/snmpd.conf）。

2. 检索构成定义文件的下一行。

   get-community-name: public

   get 团体名的默认置为“public”。

3. 更改 get 团体名。

   （例）get-community-name: private

4. 检索构成定义文件的下一行。

   #set-community-name: # enter community name

5. 更改为如下。

   set-community-name:

6. 在 set-community-name:标记后配置 set 团体名。

   （例）set-community-name: private

7. 保存并关闭构成定义文件（/etc/SnmpAgent.d/snmpd.conf）。

(2) 配置陷阱目标机器

陷阱目标机器用于确定 SNMP 陷阱的发送目标，并确认接收监视代理器陷阱的管理器。如要将陷阱发送至监视管理器，需要在监视代理器中配置陷阱目标机器。

操作步骤

1. 打开构成定义文件（/etc/SnmpAgent.d/snmpd.conf）。
2. 检索构成定义文件的下一行。

   #trap-dest: # enter trap destination
3. 更改为如下。

   trap-dest:
4. 在 trap-dest:标记后面输入监视代理器发送陷阱的目标管理器的主机名或 IP 地址。

   （例）trap-dest: 15.2.113.223
5. 保存并关闭构成定义文件（/etc/SnmpAgent.d/snmpd.conf）。

下一步操作

设置 SSO - AP。

相关项目

- 1.6.5 设置 SSO - AP（Linux 环境）

1.6.5 设置 SSO - AP（Linux 环境）

在 Linux 环境中使用监视代理器时，更改 hosts 文件及端口号。

(1) 在 hosts 文件中配置自己 IP 地址

在/etc/hosts 文件的自己服务器 IP 地址中已定义“127.0.0.1”时，不能通过 SSO - AP 进行进程监视。需要在/etc/hosts 文件的自己服务器 IP 地址中配置自己 IP 地址。

操作步骤

1. 打开/etc/hosts 文件。
2. 检索下列行。

   127.0.0.1 自己服务器名 localhost. localdomain localhost

3. 更改为如下。

   127.0.0.1 localhost. localdomain localhost

   自己服务器 IP 地址 自己服务器名

   （配置示例）

   127.0.0.1 localhost. localdomain localhost

   172.16.49.18 linux01

4. 保存并关闭/etc/hosts 文件。

(2) 更改 apmstart 文件的端口号

如要通过 SSO - AP 进行进程监视，需要使 SNMP 代理器的默认启动端口号与 apmstart 文件的端口号一致。

前提条件

需要使在 SSO 的 SNMP 定义文件（ssosnmp.conf）中配置的监视代理器端口号需与在 apmstart 文件中配置的端口号一致。

请在 SSO 的 SNMP 定义文件（ssosnmp.con）中更改“# 1. Specific Hosts”或“# 2. IP Address Wildcards”下面的范畴名“process”或“sso”的监视代理器端口号。

操作步骤

1. 打开/opt/CM2/APM/bin/apmstart 文件。

2. 检索下列行。

   SR_SNMP_TEST_PORT=221161

3. 更改为如下。

   SR_SNMP_TEST_PORT=要更改的端口号

   SNMP 代理器的默认启动端口号为 22161。

4. 保存并关闭/opt/CM2/APM/bin/apmstart 文件。

下一步操作

重新启动监视代理器。

相关项目

- 1.4.4(4) 配置团体名
- 1.6.6 重新启动监视代理器（Linux 环境）

1.6.6　重新启动监视代理器（Linux 环境）

在 Linux 环境的监视代理器中完成 SSO - AP 的设置后，重新启动 ESA 及 SSO - AP，以应用配置内容。

操作步骤

1. 执行 SSO - AP 的 apmstop 命令，停止 SSO - AP。
2. 执行 ESA 的 snmpstart 命令，重新启动 ESA。
3. 执行 SSO - AP 的 apmstart 命令，启动 SSO - AP。
4. 执行 ESA 的 snmpcheck 命令，确认 ESA 的状态。
   如果所有状态处于执行状态，则属正常。
5. 执行 SSO - AP 的 apmcheck 命令，确认 SSO - AP 的状态。
   如果所有状态处于执行状态，则属正常。

下一步操作

接下来，进行监视网络的配置。

相关项目

- 1.2.4　各产品的命令保存位置
- 2.　JP1 网络管理产品的配置

2 JP1 网络管理产品的配置

访问 NNMi 及 SSO，进行开始网络管理的配置。

2.1 JP1 网络管理产品的配置流程

JP1 网络管理产品的配置流程如下所示。

操作概述	顺序	操作内容	参照章节
NNMi 的配置	1	访问 NNMi	2.2.1
	2	注册用户	2.2.3
	3	配置通信协议	2.2.4
	4	发现网络	2.2.5
	5	配置节点组	2.2.6
	6	配置监视	2.2.7
	7	配置事件	2.2.8
SSO 的配置	8	访问 SSO	2.3.1
	9	配置资源收集	2.3.2
	10	配置进程及服务监视	2.3.3

2.2 NNMi 的配置

2.2.1 访问 NNMi

通过 Web 浏览器访问 NNMi 并开始配置。

前提条件

请对 Web 浏览器进行以下配置。

- 允许弹出（禁用弹出窗口阻止程序）。
- 启用活动脚本的执行以及 Cookie 的保存。
- 启用 IE 的 IE ESC 构成时，在［可信站点］中添加“about:blank”。

操作步骤

1. 通过 Web 浏览器访问 NNMi。

   URL：http://主机名:端口号/nnm/

   - **主机名**：安装有 NNMi 的服务器主机名 （FQDN）。也可指定 IP 地址。
   - **端口号**：指定安装 NNMi 时选择的 Web 服务器的端口号。

   将显示 NNMi 的登录画面。

2. 输入用户名及密码。

   使用系统账号登录。

   用户名：system

   密码：系统账号的密码

3. 点击［登录］。

   将显示 NNMi 控制台。

   > **重要**
   >
   > 系统账号的用户名“system”为固定值。系统账号是用于进行初始配置及运维操作的账号。由于可使用命令更改密码，不建议在通常运行时使用。

下一步操作

NNMi 的登录至此结束。请一边配置 NNMi，一边学习基本操作。

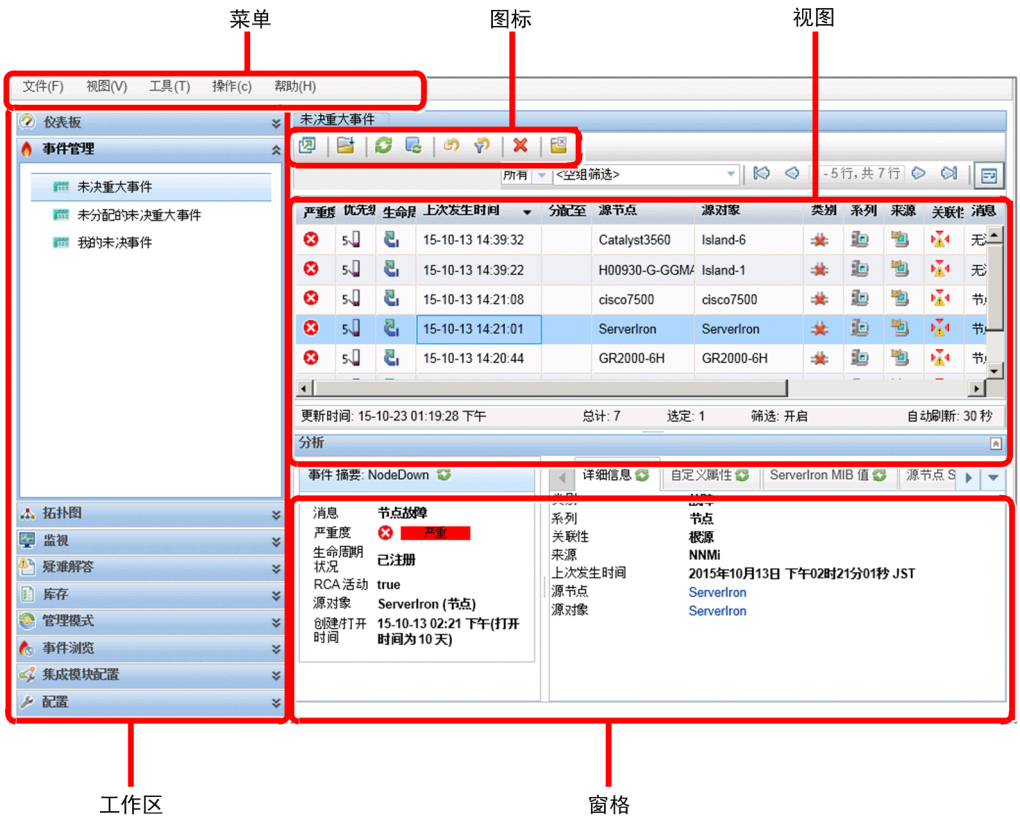
相关项目

- 1.3.4 设置 NNMi（Windows 环境）
- 1.4.3 设置 NNMi（Linux 环境）

2.2.2 关于 NNMi 控制台

访问 NNMi 后，将显示 NNMi 控制台。请使用 NNMi 控制台，熟练基本操作。除非点击 （保存）、 保存并关闭 或 （删除），也不更改配置。请随意进行操作。

可通过 NNMi 控制台操作图标、参照信息或配置定义。如果将光标放在图标上，则显示图标说明。



如果选择了［帮助］，则显示与正在操作的画面相关的说明。参照该说明，即可随时确认可指定字符数、字符类型等配置项目，非常方便。

相关项目

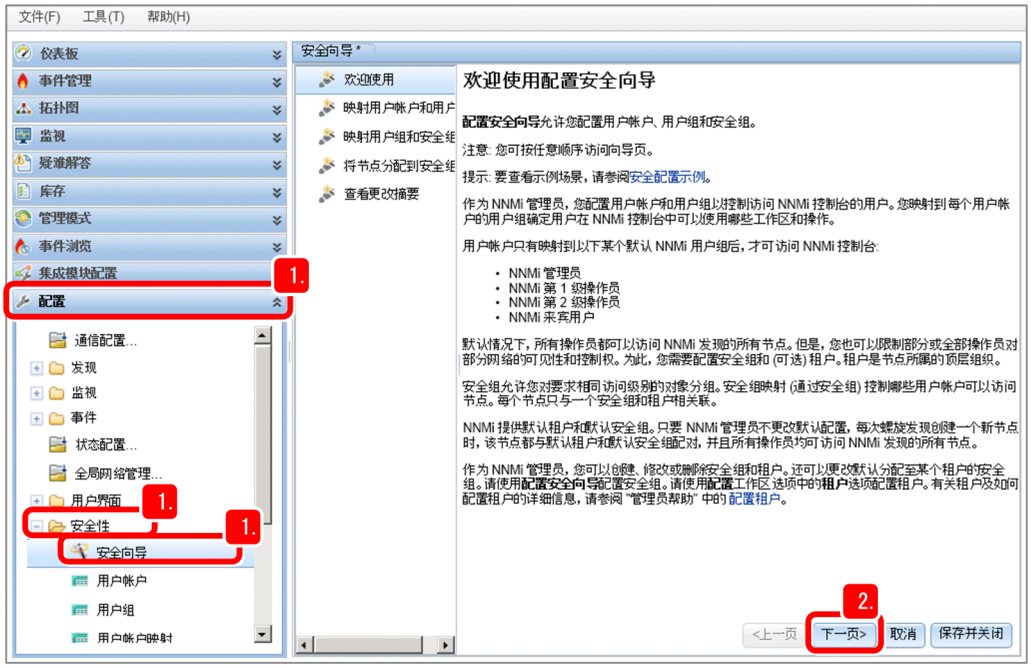
- 帮助“管理员帮助”中“随时随地使用 NNMi 帮助”的说明

2.2.3 注册用户

创建系统管理员及主管操作员的用户帐户并注册用户。首先，创建系统管理员的用户帐户，并使用该帐户重新登录。之后，创建主管操作员的用户帐户。

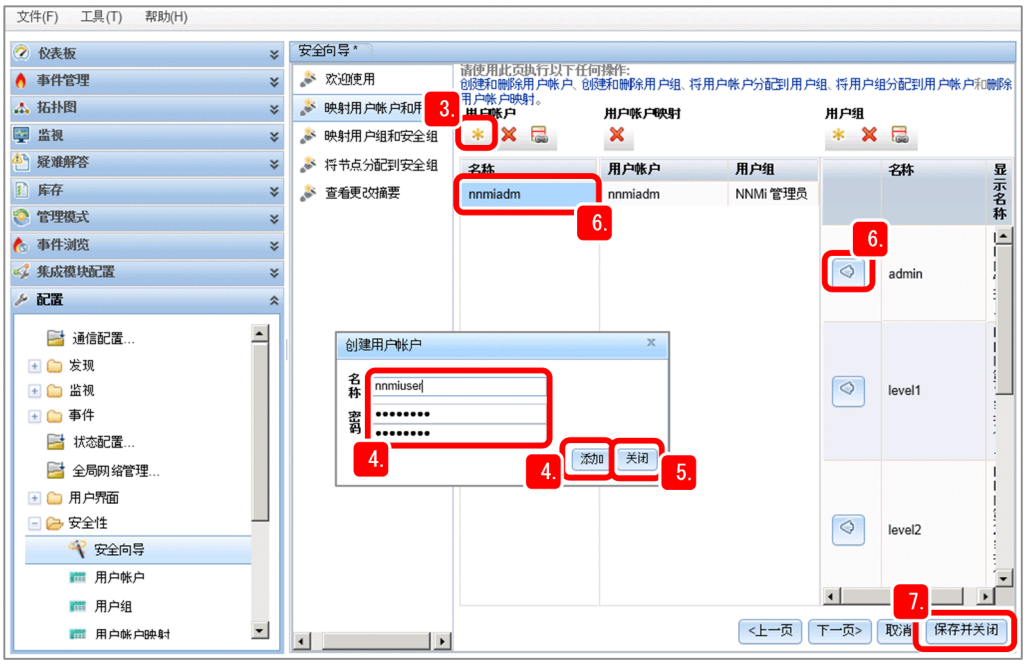
操作步骤

1. 依次选择［配置］-［安全］-［安全向导］。



2. 阅读［欢迎使用安全配置向导］的说明后，点击画面下方的［下一页>］。

3. 点击用户帐户栏中的 （创建用户帐户）。



4. 输入用户的［名称］及［密码］后，点击［添加］。

   将创建用户帐户。

   （例）

系统管理员　名称：nnmiadm、密码：password

主管操作员　名称：nnmiope、密码：password

5. 完成添加用户后，点击［关闭］。

6. 选择已创建的用户帐户，并点击要相应的用户组的  。

（例）

nnmiadm：系统管理员

nnmiope：主管操作员

7. 点击［保存并关闭］。

8. 弹出确认对话框时，点击［OK］。

将配置用户帐户。

参考

忘记密码时

关于用户帐户的密码的重新配置，请参照帮助“管理员帮助”中“更改密码和名称”的说明。

使用 nnmchangesyspw.ovpl 命令重新配置系统账号的密码。如要更改用户帐户的密码，依次选择［文件］-［更改密码］，即可更改自己用户的密码。

下一步操作

用户注册至此结束。依次选择［配置］-［安全］-［用户帐户映射］，确认已显示创建的用户帐户。

相关项目

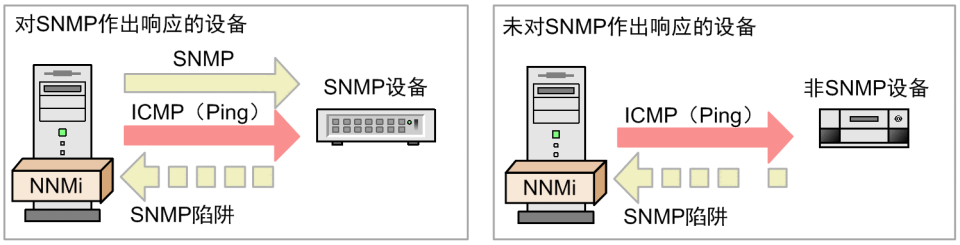
- 1.3.4　设置 NNMi（Windows 环境）
- 1.4.3　设置 NNMi（Linux 环境）
- 2.2.4　配置通信协议

2.2.4　配置通信协议

NNMi 使用 SNMP 及 ICMP（Ping）发现并监视设备，接收 SNMP 陷阱（事件通知）。

前提条件

设备可分为响应 SNMP 的 SNMP 设备及不响应 SNMP 的非 SNMP 设备。。



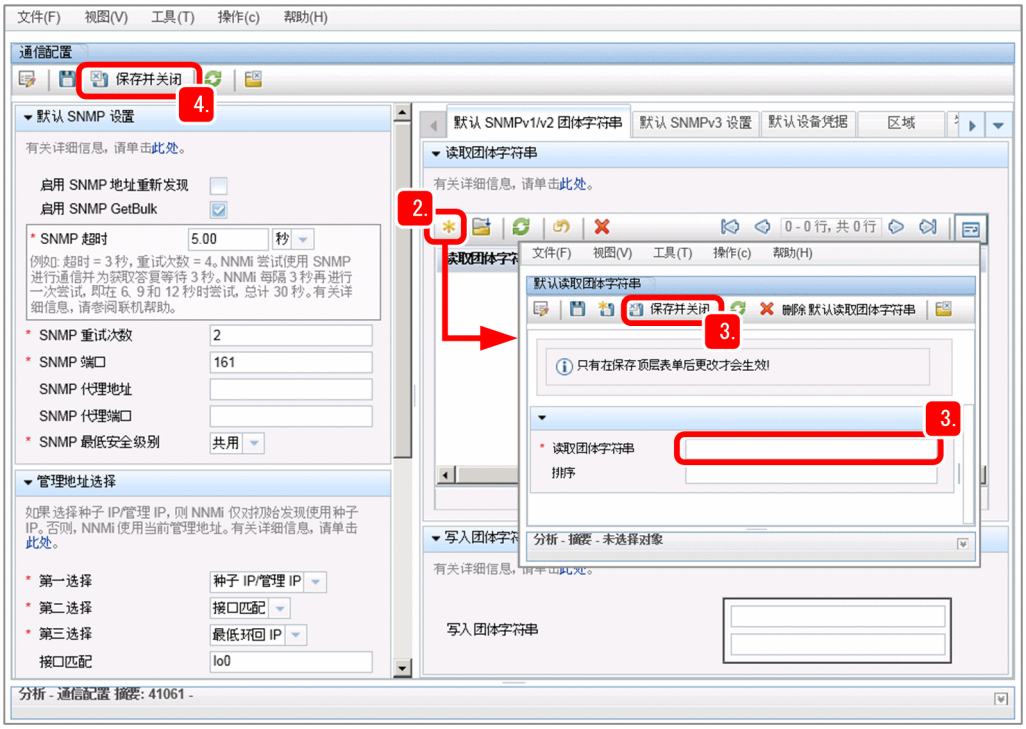
本说明书对通信协议“SNMP”（用于 NNMi 的网络发现及监视）“ICMP（Ping）”的操作配置进行说明。以下述配置内容为例进行说明。请根据需要更改设定值。

- SNMP 及 ICMP 的超时及重试次数配置：默认值（不更改）
- SNMP 最低安全级别：默认值（不更改）
- 读取团体字符串：public

操作步骤

1. 依次选择［配置］-［通信配置］。

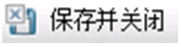
2. 点击［默认 SNMPv1/v2 团体字符串］的 （新建）。



3. 输入［读取团体字符串］并点击 保存并关闭 。

（例）读取团体字符串：public

监视的网络使用多个团体字符串时，请重复步骤 2～步骤 3，配置多个团体字符串。NNMi 对网络配置的团体字符串进行并行检查，并使用适当的值。

4. 确认已在［通信配置］中显示配置内容，并点击  。

将保存配置内容。

下一步操作

通信协议的配置至此结束。接下来，发现监视的网络。

相关项目

- 2.2.5　发现网络

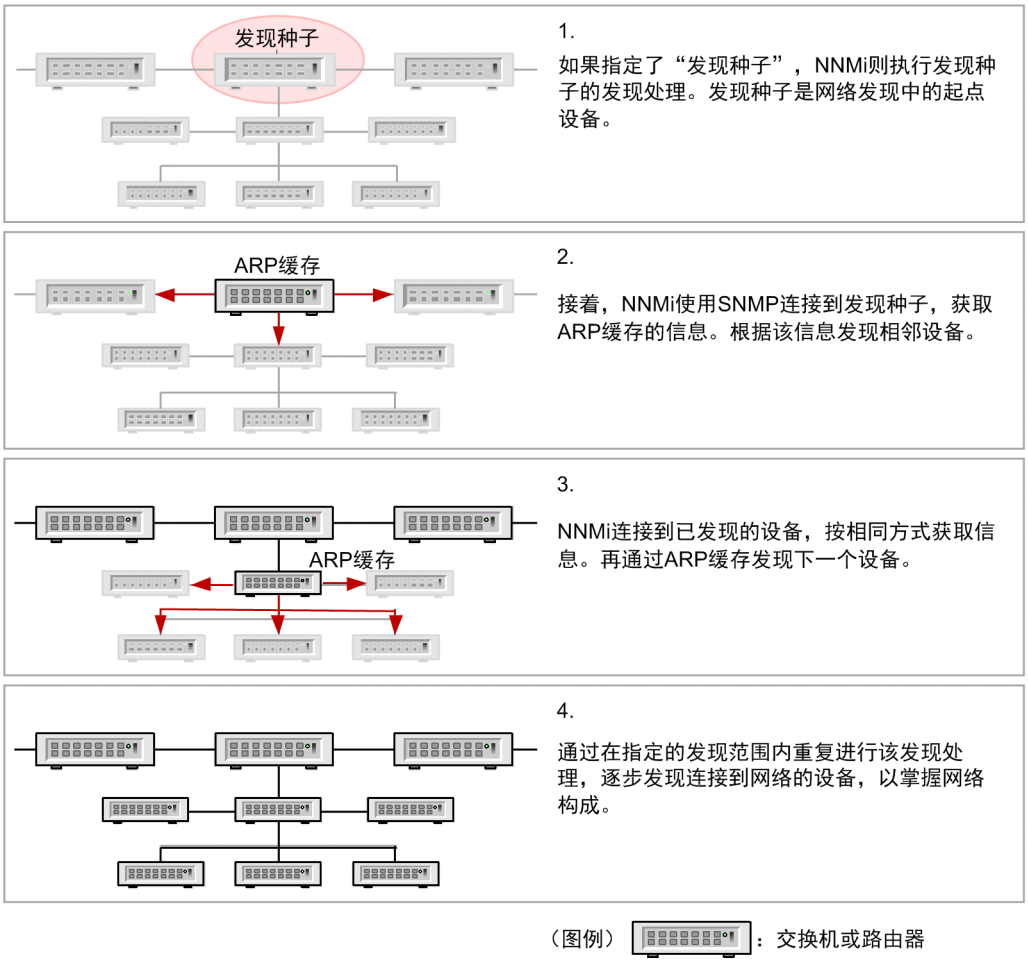
2.2.5　发现网络

NNMi 收集网络上的设备信息，以掌握各设备的详细情况及网络构成（拓扑）。

(1)　什么是发现网络？

NNMi 通过使用 SNMP 收集各设备拥有的 ARP 缓存信息及相邻设备信息（通过 LLDP 等协议识别），可发现全体网络。

在本说明书中，以使用 ARP 缓存的发现为例进行说明。

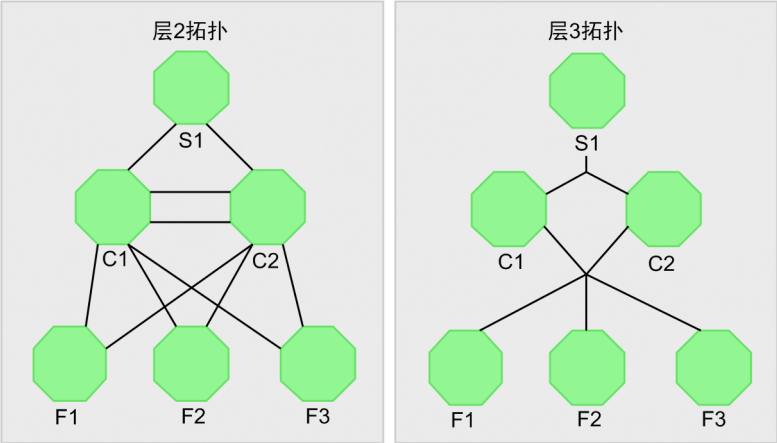


参考

NNMi 还可通过 Ping 扫描进行发现。Ping 扫描是指，使用 ICMP（Ping）监视指定的 IP 地址范围并发现已响应的设备的方法。虽然可迅速发现指定网络范围内的设备，但可能增大对网络的负荷。请根据具体运行状况使用 Ping 扫描。使用 Ping 扫描时，建议缩小对象范围。

(2) 层 2 拓扑与层 3 拓扑

针对网络的拓扑（网络构成），NNMi 可识别并显示层 3 拓扑及层 2 拓扑。如果识别层 2 拓扑（物理接线），即可对造成网络问题的原因进行更详细地分析。



层 2 拓扑

以物理接线显示网络构成。

如要确认末端的交换机与终端之间的接线，则通过层 2 拓扑进行确认。通过与层 3 拓扑并用，可确认发生故障时的情况或直观地掌握影响范围。

层 3 拓扑

使用 IP 地址显示网络的逻辑构成。

如要确认主干网的逻辑构成，则通过层 3 拓扑进行确认。

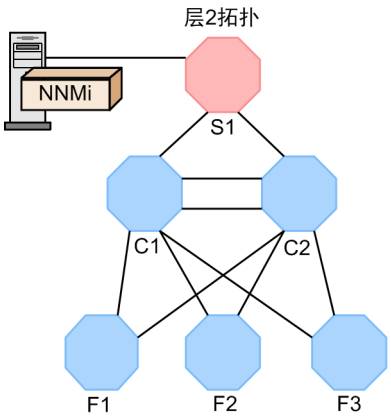
提示

层 2、层 3 的名称来自于 OSI 七层模型。

- 层 2（数据链路层）：使用 MAC 地址控制物理链路之间的数据传输等。
- 层 3（网络层）：使用 IP 地址控制网络的路由选择等。

进行 IP 网络的通信或 NNMi 的配置操作时，使用 IP 地址指定目标机器，通常无需考虑到物理接线。NNMi 通过对有关相邻设备的 MIB 信息进行收集与分析，识别物理接线的层 2 拓扑。

例如，如果因 NNMi 连接的交换机（S1）发生故障而导致无法与目标网络进行通信，将通过层 2 拓扑显示如下。



如果仅通过经由IP地址的通信（层3拓扑）进行判断，则不能与多数设备进行通信，因此，将辨别为广范围的网络故障。
如果可识别类似层2拓扑图这样的物理接线，则可通过发生故障的交换机及其影响判断不能进行通信的设备。

(3) 配置网络的发现方法

发现当前监视的网络上的网络设备。请在完成监视代理器的构建后，发现网络。

前提条件

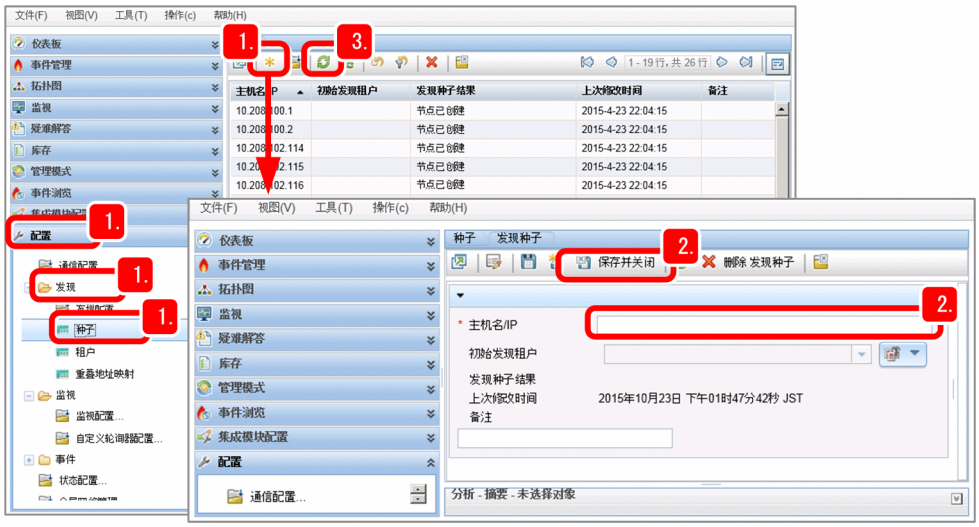
网络的发现包括自动发现方法及显式指定方法，也可以组合这两种方法进行配置。自动发现方法及显式指定方法的说明与运行例如下所示。

发现方法	描述	运行例
自动发现	通过指定自动发现规则，NNMi 可自动发现设备。	• 想要自动发现网络更改 • 在大规模网络中存在大量设备
显式指定	将特定设备显式指定为发现种子。	• 想要严格指定管理对象 • 网络构成固定

下面对显式发现网络的方法进行说明。

操作步骤

1. 依次点击［配置］-［发现］-［种子］，并点击 （新建）。



2. 在“主机名 / IP”栏中输入发现种子的 IP 地址后，点击 保存并关闭 。

   将立刻对指定的发现种子开始发现。

   请将支持 SNMP 的路由器（拥有较多相邻设备信息）指定为用作发现种子的设备。

3. 点击 （刷新）。

   确认已创建指定的发现种子。

参考

使用下列 nnmloadseeds.ovpl 命令，也可统一注册发现种子。

直接指定种子时

（例）nnmloadseeds.ovpl -n 192.168.8.82 192.168.100.24

指定种子列表文件时

（例）nnmloadseeds.ovpl -f c:\jp1\seeds.txt

种子文件的填写例

192.168.8.82 # node1

192.168.100.24 # node2

关于 nnmloadseeds.ovpl 命令，请参照［帮助］-［NNMi 文档库］-［参考页］-［nnmloadseeds.ovpl］的说明。

提示

如要自动发现，依次点击［配置］-［发现配置］-［自动发现规则］后，进行配置。指定［IP 范围］时，如果指定不发现的 IP 地址并将范围类型设为［被规则忽略］，该 IP 地址则不属于发现对象。

仅在从已发现的节点中排除特定 IP 地址时，依次选择［发现配置］-［排除的 IP 地址］。如果用于指定不监视的节点，IP 地址可能在保留节点的状态下消失。因此，请根据用途进行操作。

关于自动发现的详细情况，请参照《JP1/Network Node Manager i Setup Guide》中“Configuring auto-discovery rules”的说明。

相关项目

- 1.2.4　各产品的命令保存位置

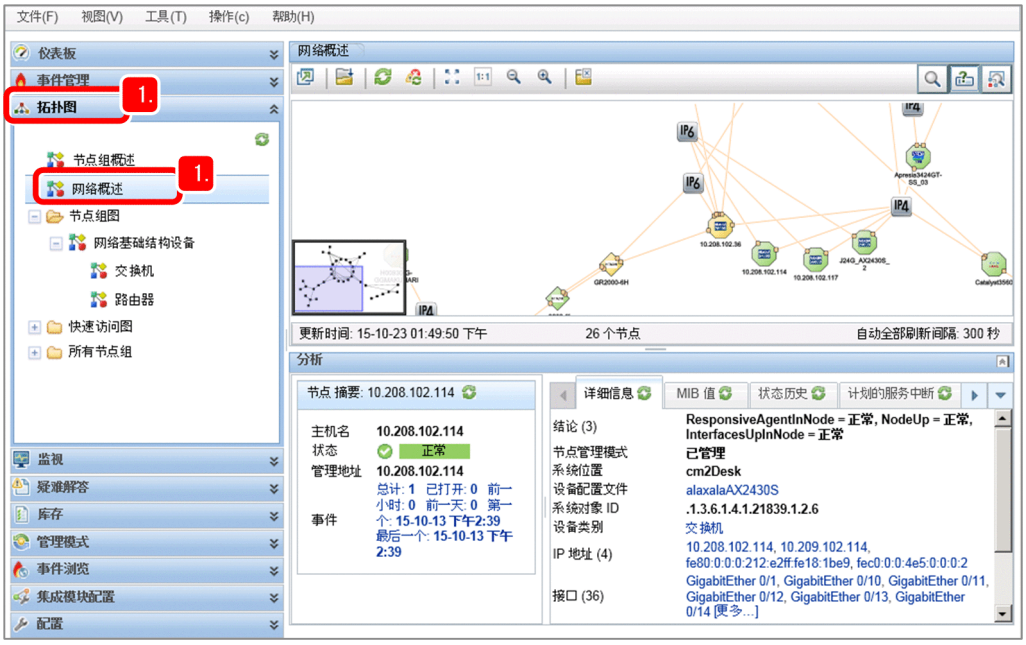
(4)　确认已发现的网络与设备

通过拓扑图参照已发现的网络。配置发现后，可暂时参照发现节点的过程。

操作步骤

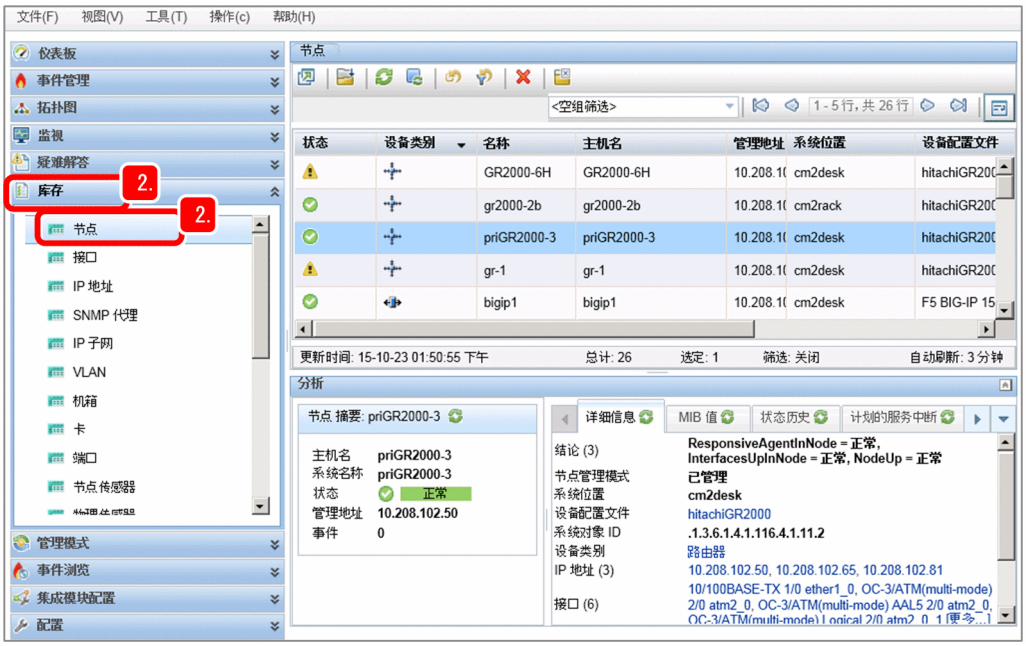
1. 依次点击［拓扑图］-［网络概述］。

   在［网络概述］中确认网络状况。



2. 依次点击［库存］-［节点］。

将确认是否正确发现并注册设为发现对象的设备。如果显示已配置的设备，则表示已正常实施网络发现。请查看［设备类别］或［设备配置文件］等，确认已发现的设备。



提示

如果在监视对象中存在群集系统的节点，请设为“排除的 IP 地址”，以免监视逻辑 IP 地址。如果未进行该配置，逻辑 IP 地址移动时，将发生删除节点或反映其它节点状态等现象。关于详细情况，请参照发布说明。

参考

如果发现了不需要监视的节点，可从监视对象中删除该节点或将其设为非监视对象。

从监视对象中删除的方法

依次点击［拓扑图］-［网络概述］，选择要删除的节点图标，即可进行删除。但对于指定为发现种子的节点，即使删除，也不会从［种子］上显示的列表中删除。请删除发现种子。

不设为监视对象的方法

依次点击［库存］-［节点］选择对象节点后，选择［操作］-［管理模式］-［未管理］。在不希望将节点从图中删除或要暂时将其设为非监视对象等情况下使用。

相关项目

- 2.2.5(5)　删除已完成发现的发现种子

(5)　删除已完成发现的发现种子

完成网络发现后，删除发现种子。

操作步骤

1. 依次点击［配置］-［发现］-［种子］。
2. 选择所有发现种子后，点击  （删除）。

   选择多个行时，在按住［Ctrl］键的同时点击行。
3. 确认已删除发现种子。

下一步操作

网络发现至此结束。接下来，配置节点组。

相关项目

- 2.2.6　节点组的配置

2.2.6　节点组的配置

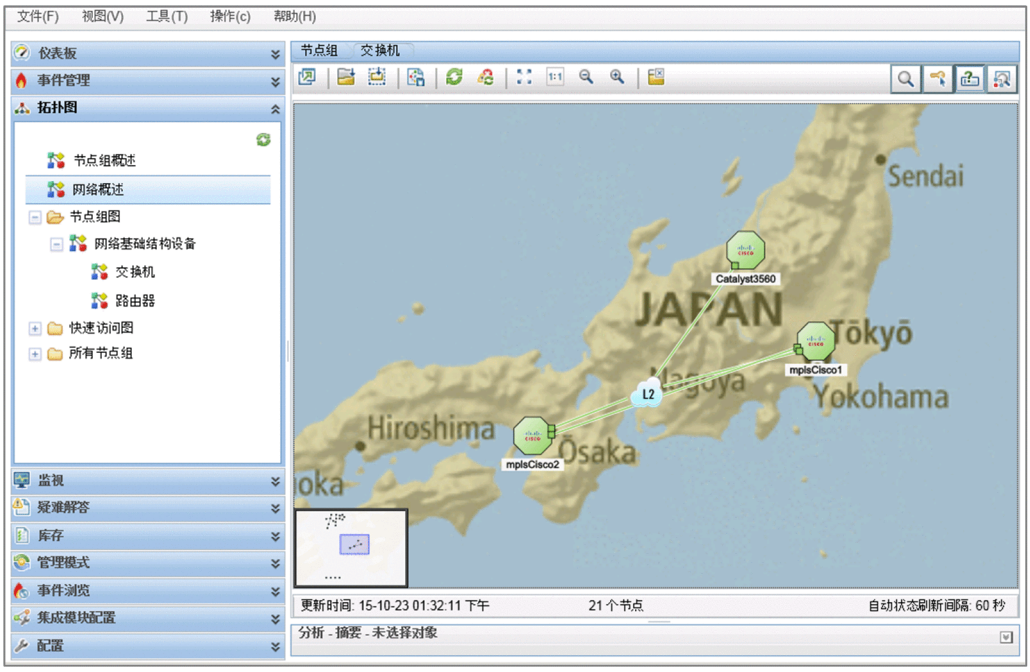
如果定义节点组，即可分别配置各节点组的监视，或按节点组进行过滤。另外，还可在 NNMi 控制台的初始画面中显示任意节点组。

(1) 什么是节点组？

节点组是指，按 IP 地址或设备类别等条件将已发现的网络设备分组及分层后的组。NNMi 标配有 Windows 或路由器等已按基本类型进行了配置的节点组。通过定义子节点组，可将节点组分层（最多 6 层）。

另外，对所检测出的网络设备进行分类并创建显示图（节点组图）。通过创建该节点组图，与拓扑图相比，更能重点把握网络构成。因此便于查找问题发生位置，可迅速确认详细情况。

节点组图



可使用图像文件自由配置节点组图的背景图。通过根据目的对显示方法进行自定义（配置平面布置图等），支持更有效的网络管理。

“重要节点”节点组的使用方法

NNMi 标配有“重要节点”节点组。该“重要节点”节点组用于注册重要的服务器或网络设备。

如果“重要节点”没有响应，设备将发行“节点故障（NodeDown）”事件通知。如果即使节点不是无响应的根本原因，但是仍然希望发行事件通知，请将该节点注册到“重要节点”。

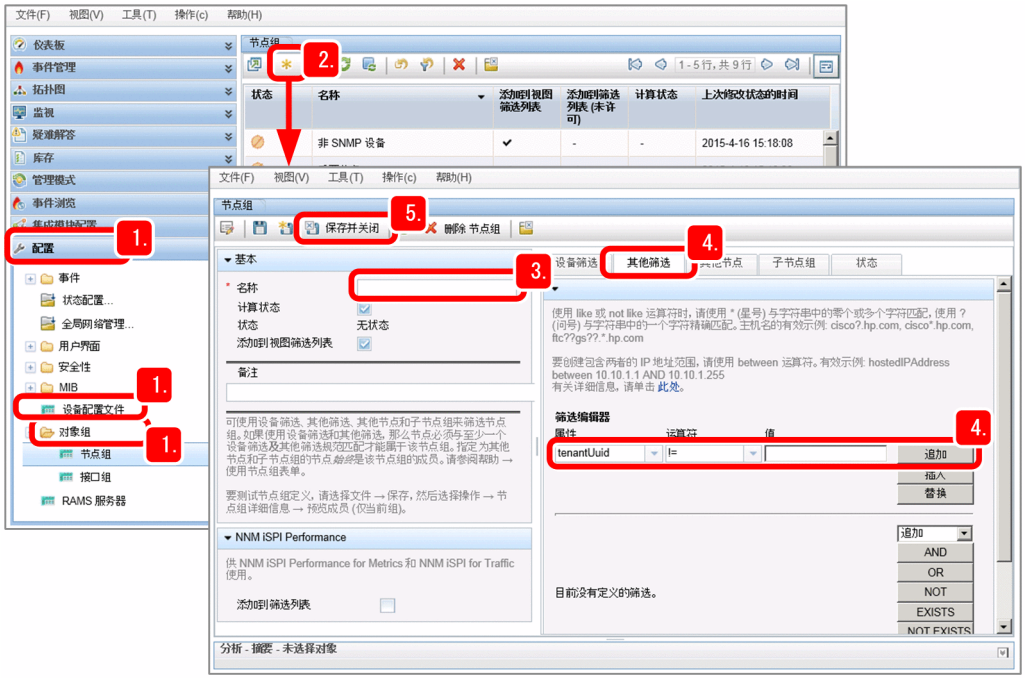
如果在“重要节点”节点组中对子节点分层后进行配置，或添加包含在其它节点组中的节点，也可发行事件。

(2) 配置节点组

配置节点组后，可在不依赖于网络构成的情况下对已发现的节点进行自由分组。本说明书对指定属性值来配置组的步骤进行说明。

操作步骤

1. 依次点击［配置］-［对象组］-［节点组］。



2. 点击 （新建）。

3. **配置节点组的名称。**

（例）名称：系统部

勾选［添加到视图筛选列表］，便在［节点］或［事件］的［<空组筛选>］中显示创建的节点组名称。

4. **在［其他筛选］，指定要在节点组中添加的节点条件。**

选择［属性］及［运算符］后，在［值］中输入适当的值，然后点击［添加］。

（例）属性：hostedIPAddress，运算符：between，值：10.208.102.2～10.208.102.254

将指定的条件表达式添加到［筛选字符串］。如要删除条件表达式，则选择条件表达式并点击［删除］。

提示

分组条件可用于指定 IP 地址的范围、设备类别及设置位置等。此外，还可使用 SQL 的运算符（between、in、like 等）灵活地配置条件。节点组最多为 6 层。节点组的使用方法如下所示：

- 定义节点组图：［节点组图］
- 分别调整各节点组的监视方法：［监视配置］-［节点设置］
- 按节点组进行性能监视：依次点击［监视］-［自定义轮询器配置］-［策略］。

5. 点击 保存并关闭 。

将关闭［节点组］并创建节点组。

6. **选择已创建的节点组的行并右击鼠标，然后依次选择［节点组详细信息］-［显示成员（包括子组）］。**

确认节点组包含了被指定为对象的节点。

7. 右键点击目标节点组，并依次选择［图］-［节点组图］。

将以图形式显示节点组。

参考

除了使用运算符的配置之外，NNMi 还备有各种分组条件。配置分组条件的标签与运行例如下所示。

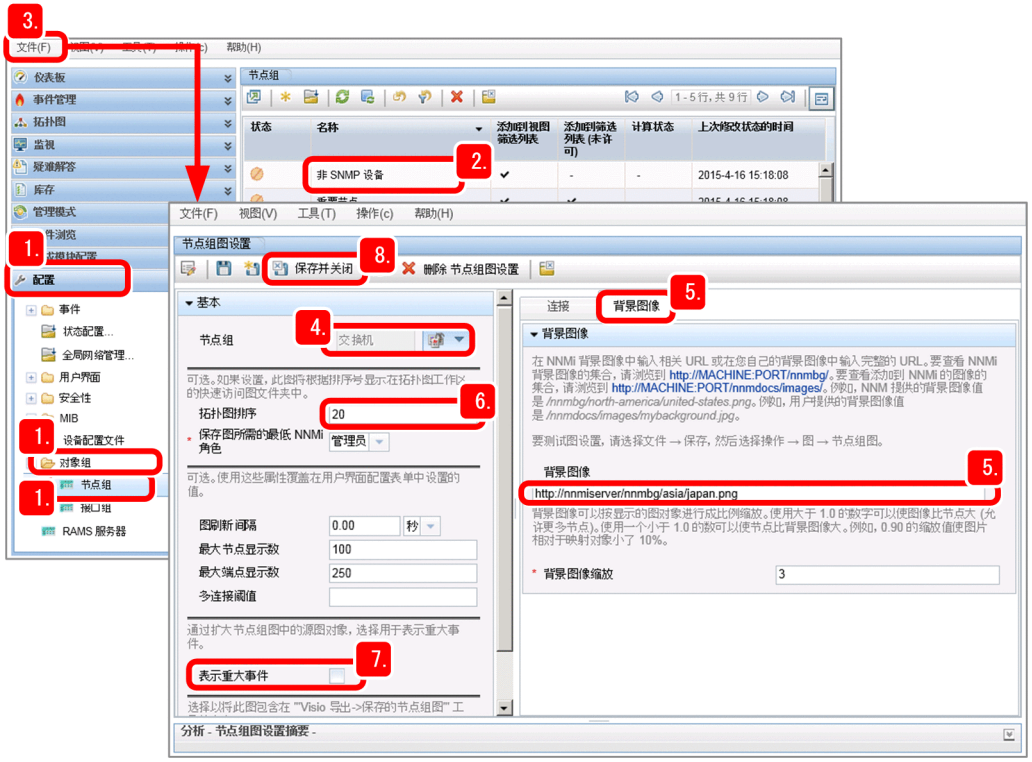
标签	配置项目	运行例
［设备筛选］	• 设备类别 • 设备供应商 等	• 根据设备的重要度进行监视。 • 按机型分别配置适当的监视方法。 • 通过对条件进行筛选（如仅显示路由器等），尽快掌握情况。
［其他筛选］	• hostedIPAddress（IP 地址） • sysLocation（位置） 等	按设置位置或组织配置监视条件或过滤显示。
［其他节点］	主机名	• 单独配置特别重要的节点等。 • 配置难以指定条件的节点。
［子节点组］	子节点组（按分层顺序依次配置）	按工作场所或地区分别将节点组分层。

(3) 配置节点组图

配置节点组图，即可将任意图像指定为背景图像。另外，也可在［拓扑图］的图名列表中显示已创建的节点组图。

操作步骤

1. 依次点击［配置］-［对象组］-［节点组］。



2. 选择要配置图的节点组，右键点击显示菜单后，依次点击［图］-［节点组图］。

3. 依次点击［文件］-［打开节点组图设置］。

4. 从［节点组］下拉菜单中选择将配置的节点组。

5. 在［背景图像］中，将图的背景图像设为［背景图像］。

   在［背景图像］中进行如下输入。

   （例）/nnmdocs/images/图像文件名

   可指定通过 Web 浏览器显示的 gif、png、jpg 等。将在监视管理器的下列文件夹中保存图像文件。

   - Windows 环境

     安装目标数据文件夹\shared\nnm\www\htdocs\images

   - Linux 环境

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

6. 指定［拓扑图排序］。

   指定后，可设定为在［拓扑图］的［快速访问图］文件夹中显示已创建的节点组。配置后重新登录，即可显示。

7. 勾选［表示重大事件］。

   勾选后，如果发生重大事件，则放大显示图上的图标。由此，便于找到问题发生位置。

8. 配置结束后，点击 保存并关闭 。

9. 调整图标位置后，点击  （保存图）。

将保存图标位置。

下一步操作

节点组图的配置至此结束。接下来，配置监视定义。

相关项目

- 2.2.7　监视配置

2.2.7　监视配置

NNMi 以通过网络发现功能发现的设备为对象，周期性地对其进行监视。

(1)　什么是监视？

监视是指，对在网络上发现的各节点进行周期性监视，以确认是否正常运行。NNMi 使用 SNMP 或 ICMP（Ping）对监视对象设备进行监视。在默认配置下，以 5 分钟为周期进行监视，确认监视对象的状态。

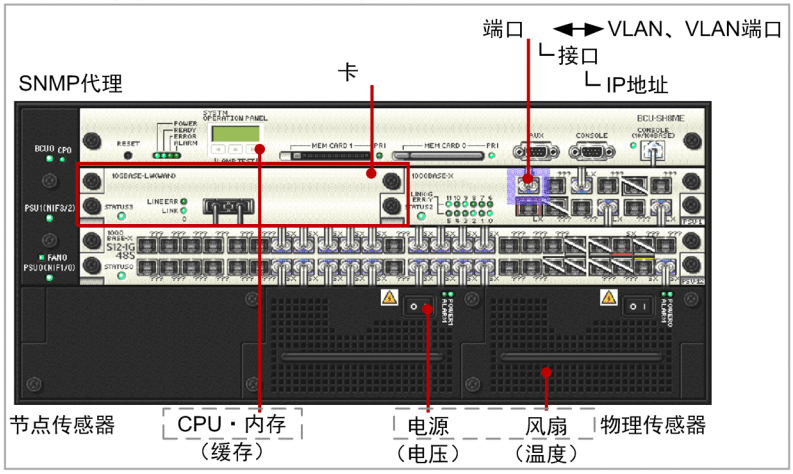
通信、发现及监视配置与通信协议 SNMP 及 ICMP（Ping）的关系如下所示。

配置对象	描述	配置位置	配置项目	默认值
协议的运作	配置使用 SNMP 或 ICMP（Ping）协议每次通信时的超时及重试次数。根据该配置进行用于发现及监视的通信。	［配置］-［通信配置］	SNMP	5 秒钟（重试 2 次）
			ICMP (ping)	
发现网络时的运作	通常不会频繁地更改构成，因此配置时确保按天进行重新发现。	［配置］-［发现］-［发现配置］	重新发现间隔	1 天
监视网络状态时的运作	将监视周期缩短，以便迅速发现故障。为了将监视负荷设为适当值，配置时确保按分钟进行轮询。	［配置］-［监视］-［监视配置］	故障轮询周期	5 分钟

将在［库存］中显示可通过 NNMi 监视的项目。NNMi 的监视项目与设备之间的对应关系如下所示。

NNMi监视项目的显示例

［节点］：在状态中反映最严重的未解决结果。



通过SNMP监视［接口］、［SNMP代理］、［卡］、［节点传感器］、［物理传感器］。通过ICMP(Ping)监视［IP地址］。
其它项目为管理构成的信息或分组信息等。

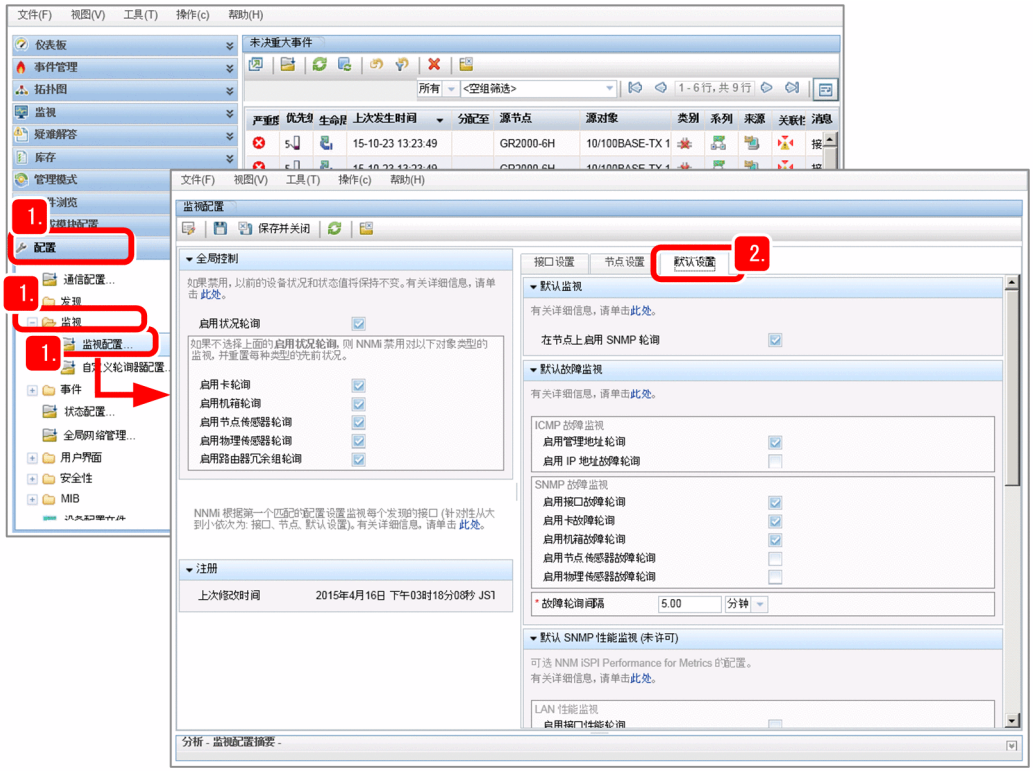
(2)　参照监视定义以确认监视方法

NNMi 标配有监视定义，以便立刻开始监视。因此，如果未对监视方法或轮询周期进行客户化，则无需更改配置。

接下来，参照标配的监视定义来确认监视方法，以便了解监视机制。

操作步骤

1. 依次选择［配置］-［监视］-［监视配置］。



2. 选择［默认设置］。

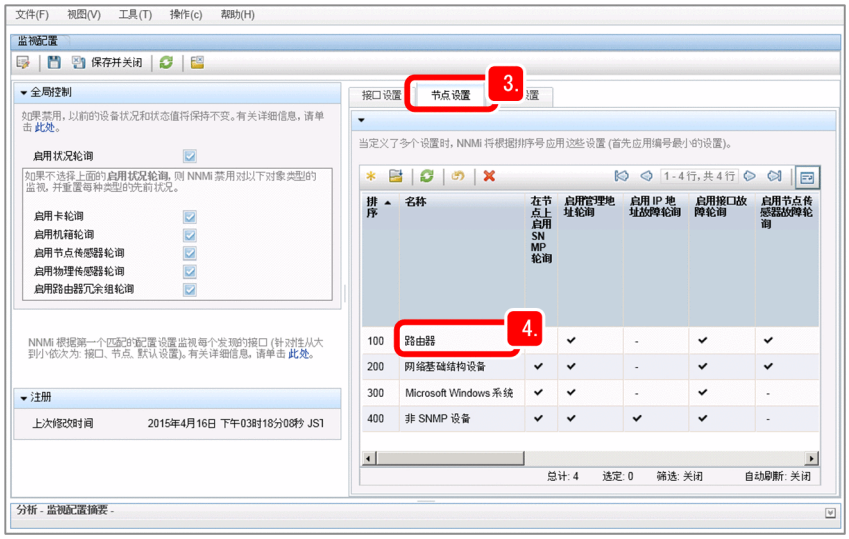
将显示监视的默认配置。

请确认已设置的监视内容及监视间隔等。

3. 选择［接口设置］或［节点设置］，以参照监视定义。

在［节点设置］中定义的监视定义如下所示。

- 路由器
- 网络基础结构设备
- Microsoft Windows 系统
- 非 SNMP 设备



4. 双击监视定义项目。

将显示各个监视定义。

按节点类型定义有适当的监视方法。浏览时，请对各个监视对象及监视间隔等进行比较。

下一步操作

默认监视定义的确认至此结束。接下来，配置事件。

相关项目

- 2.2.7(3)　监视定义的配置项目
- 2.2.8　事件配置

(3)　监视定义的配置项目

NNMi 标配有适当的监视定义，可用作监视网络的配置。监视定义用于定义监视时执行的轮询类型或周期。可通过该监视定义，在导入 NNMi 后立即按适当的方法开始网络监视。

可在［监视配置］中配置监视方法。可定义的主要监视定义项目如下所示。

配置位置	监视定义项目	描述
［全局控制］	启用状况轮询	监视 SNMP 代理器、接口及 IP 地址的运行状况。 · SNMP 代理器：使用 SNMP 进行监视 · 接口：使用 SNMP 进行监视 · IP 地址：通过 ICMP（Ping）进行监视
	启用卡轮询*	使用 SNMP 监视“卡”的状况。
	启用机箱轮询*	使用 SNMP 监视“机箱”的状况。
	启用物理传感器轮询*	使用 SNMP 监视“物理传感器”的状况。
［默认设置］	启用管理地址轮询	通过 ICMP（Ping）监视划分为管理地址的“IP 地址”。 管理地址是指，NNMi 与其节点的 SNMP 代理器通信时使用的 IP 地址。
	启用 IP 地址故障轮询	通过 ICMP（Ping）监视“IP 地址”。
	启用接口故障轮询	使用 SNMP 监视“接口”的状况。
	启用接口故障轮询*	使用 SNMP 监视“卡”的状况。
	启用机箱故障轮询*	使用 SNMP 监视“机箱”的状况。
	启用物理传感器故障轮询*	使用 SNMP 监视“物理传感器”的状况。
	故障轮询间隔	指定监视状况的周期。
［节点设置］	网络基础结构设备	以网络的核心设备为对象。除 SNMP 设备之外，也将组件（风扇、电源等）设为监视对象。
	非 SNMP 设备	自动将对 SNMP 没有响应的设备作为非 SNMP 设备进行管理。由于设为通过 ICMP（Ping）进行监视，因此,可进行存活监视。如果对 SNMP 作出响应，则使用 SNMP 开始管理。

注* 关于卡、机箱及物理传感器，仅可对 NNMi 支持的特定型号进行监视。

2.2.8 事件配置

NNMi 通过根源分析功能对问题（通过监视发现）及 SNMP 陷阱进行分析。确定根源后，将作为事件进行通知。

(1) 什么是事件？

事件是指，与网络有关且需要通知管理员的重要性较高的信息。NNMi 监视网络并检测发生的情况（事件），通过利用根源分析功能进行分析，筛选为需要管理员掌握的“事件”进行通知。

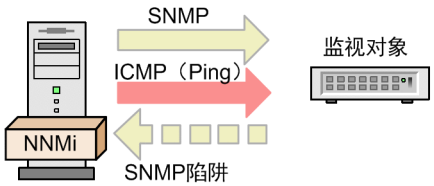
根据使用 SNMP 或 ICMP（Ping）监视网络的信息及使用 SNMP 陷阱通知问题的信息进行根源分析后，通知事件。

［管理事件］

持续监视网络并分析发现的问题，将根源作为事件进行通知。

［SNMP陷阱］

如果从监视对象收到以SNMP陷阱形式发出的问题发生通知，则作为事件进行通知。



作为对应于该网络监视的事件定义，NNMi 标配有［管理事件］及［SNMP 陷阱］等约 150 种事件定义。由于这些定义对应于各种情况，因此可直接用于运行。

例如，已将下列内容设为［管理事件］，作为发生节点故障时发生的事件。其中，通过根源分析功能分析状况并通知适当的事件。

- NodeDown（节点故障）
- NodeOrConnectionDown（节点或连接故障）

将节点加入“重要节点”节点组的操作为运行方法之一。如果“重要节点”无响应，则发行 NodeDown 事件。请监视该事件。

事件发行例

网络设备因节点故障停止时发生的事件例如下所示。通过根源分析功能，仅通知作为事件的根源情况。

为了最大限度地降低网络运行中的故障影响，NNMi 提供下列机制，毫无遗漏地对事件进行适当的处理。

功能	描述	参照章节
事件的自动操作	可进行根据事件的生命周期状况执行自动操作的配置。	2.2.8(4)
事件的故障监视	如果发生事件，则在 NNMi 控制台上通知并显示。浏览拓扑图及事件时，可切换画面以确认内容。	3.1
事件的生命周期管理	NNMi 将事件的对应进展状况作为生命周期状况进行管理。	4.2

为了使用这些功能，请配置事件。

相关项目

- 2.2.6　节点组的配置
- 2.2.8(4)　对事件配置自动操作
- 3.1　JP1 网络管理产品的网络监视
- 4.2　故障对应机制

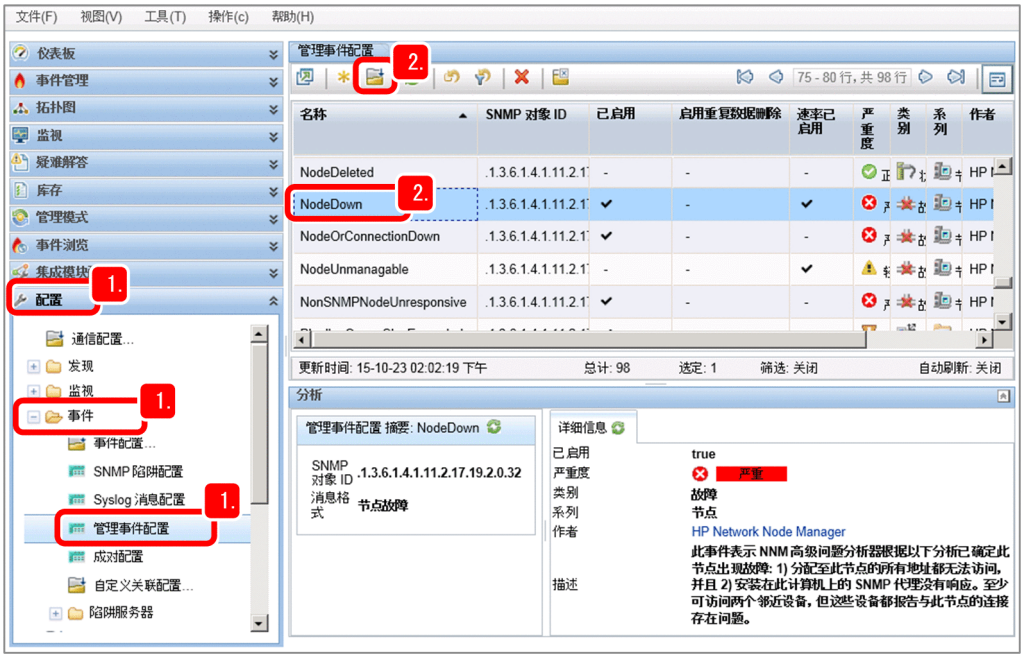
(2)　确认事件配置内容

JP1 网络管理产品中预先配置有运行时使用的标准事件。请查看标配的事件配置，并确认基本项目。

操作步骤

1. 依次点击［配置］-［事件］-［SNMP 陷阱配置］或［管理事件配置］。

   如要确认 SNMP 陷阱的事件，请选择［SNMP 陷阱配置］；如要确认 NNMi 监视网络时发现的事件，请选择［管理事件配置］。



2. 点击要浏览的事件行后，点击  （打开）。

   将显示事件的配置内容。例如，查看节点故障时发生的下列［管理事件］。

   - NodeDown（节点故障）
   - NodeOrConnectionDown（节点或连接故障）

   在［描述］中显示事件的含义。

确认事件内容以加深理解。请根据需要配置 SNMP 陷阱的事件或对事件配置自动操作。

相关项目

- 帮助“操作员帮助”-“解释根源事件”的说明

(3) 配置 SNMP 陷阱的事件

为了使网络设备等通过 SNMP 陷阱通知故障发生，可能以扩展 MIB 文件形式提供 SNMP 陷阱的定义。NNMi 标配有多种 SNMP 陷阱的事件定义，还可加载网络设备供应商特有的扩展 MIB 文件，并配置设备独有的 SNMP 陷阱的事件定义。

在一般 MIB 文件中都记述有 MIB 定义及 SNMP 陷阱定义。关于各设备供应商 MIB 文件的详细情况，请参照各设备供应商的说明书。

安装 NNMi 时，可同时加载多种 MIB（标准配置）。关于已加载的 MIB 的列表，依次选择［配置］-［MIB］-［加载的 MIB］进行参照。

前提条件

如要传入 SNMP 陷阱，需符合下列条件。如果不符合下列条件，将丢弃该陷阱。

- 配置有与 SNMP 陷阱相应的事件。并且已勾选该配置的［已启用］。
- 已发现发行 SNMP 陷阱的源节点。并且已将该节点的管理模式设为“管理对象”。

关于详细情况，请参照“管理员帮助”中“管理传入 SNMP 陷阱”的说明。另外，如要传入由未发现的节点发行的 SNMP 陷阱，请参照“管理员帮助”中“处理未解析的传入陷阱”的说明。

操作步骤

1. 执行 NNMi 的 nnmloadmib.ovpl 命令。

   指定例：nnmloadmib.ovpl -load MIB 文件名

   将 MIB 文件内容加载到 NNMi。请在-load 选项中指定要加载的 MIB 文件。

2. 执行 NNMi 的 nnmincidentcfg.ovpl 命令。

   指定例：nnmincidentcfg.ovpl -loadTraps MIB 模块名

   从 NNMi 的 MIB 数据库创建事件构成。

   请在-loadTraps 选项中指定 MIB 文件中定义的 MIB 模块名。

3. 依次点击［配置］-［事件］-［SNMP 陷阱配置］。

   可确认 SNMP 陷阱的状况。

> **参考**
>
> 也可使用 nnmtrapdump.ovpl 命令确认 SNMP 陷阱的状况。
>
> （例）
>
> nnmtrapdump.ovpl -source IPaddr
>
> 显示从 IPaddr 传入的陷阱。
>
> nnmtrapdump.ovpl -t
>
> 连续显示传入陷阱。用于配置时的确认等。
>
> 关于详细情况，请参照“操作员帮助”中“［SNMP 陷阱］”的说明以及依次点击［帮助］-［NNMi 文档库］-［参考页］-［nnmtrapdump.ovpl］后显示的内容。

> **参考**
>
> 打开 MIB 文件并查看文件的开头部分，即可确认 MIB 模块名。在“DEFINITIONS ::= BEGIN”前定义的名称则为 MIB 模块名。

（例）

MIB 模块名示例

------ MIB Simple Sample

SAMPLE-MIB DEFINITIONS ::= BEGIN

上述中的 SAMPLE-MIB 则为 MIB 模块名。

相关项目

- 1.2.4　各产品的命令保存位置

(4)　对事件配置自动操作

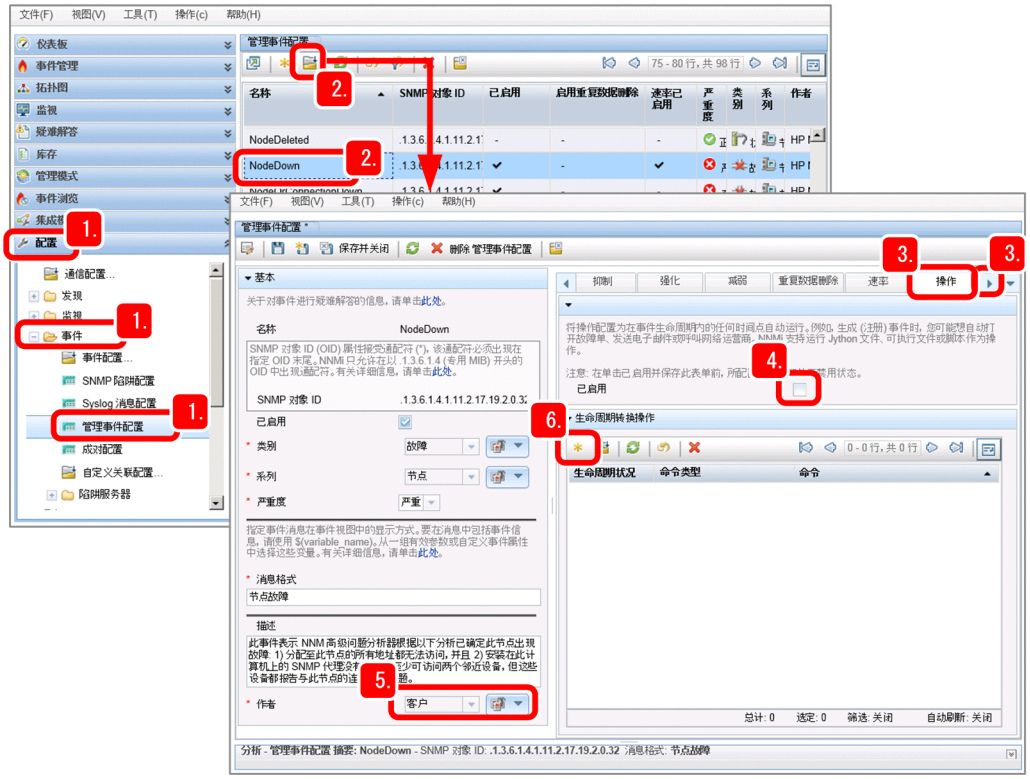
如果对事件配置自动操作，即可在特定的生命周期状况执行指定的命令。

> **参考**
>
> 如果与 JP1/IM 连动，发生故障时可发送邮件并使用警示灯。

操作步骤

1. 依次点击［配置］-［事件］-［SNMP 陷阱配置］或［管理事件配置］。

   如要将自动操作设为 SNMP 陷阱的事件，请选择［SNMP 陷阱配置］；如要将自动操作设为 NNMi 监视网络时发现的事件，请选择［管理事件配置］。



2. 点击要配置自动操作的事件行后，点击  （打开）。

3. 点击  切换标签显示，显示［操作］后点击该标签。

> **提示**
>
> 如要通过节点更改自动操作配置，可通过用于配置的标签分别指定各节点的条件。
>
> - 在［接口配置］中的［操作］……对象：以接口组指定条件
> - 在［节点设置］中的［操作］……对象：以节点组指定条件
> - ［操作］……对象：无指定
>
> 优先度顺序为［接口配置］＞［节点设置］＞普通的［操作］。由于优先度较高的操作配置将覆盖其他配置，因此只执行 1 次操作。由此，可在所有节点中配置自动操作，并仅对特定节点组执行其他自动操作等。
>
> 关于详细情况，请参照“管理员帮助”中“配置事件”的说明。

4. 勾选［已启用］。

如果未进行该配置，即使发生事件，也不执行自动操作。

5. 将作者设为“客户”。

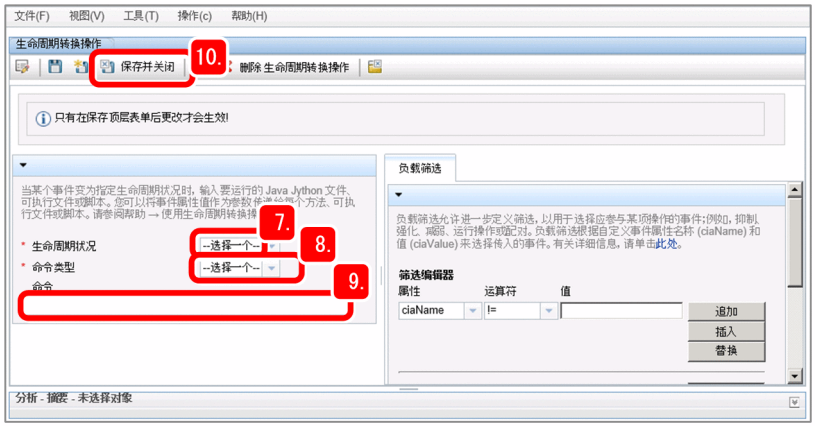
用户如要更改事件配置，需将作者更改为“客户”。

6. 在［操作］的［生命周期切换操作］中，点击  （新建）。

7. 从［生命周期状况］中选择执行自动操作的时序。

根据要执行自动操作的时序，进行如下配置：

- 已注册：检测故障并发行事件后，执行自动操作。
- 正在进行：因对事件分配负责人或正在调查事件等情况，［生命周期状况］变为“正在进行”状态时，执行自动操作。
- 已完成：故障处理完成后，［生命周期状况］变为“已完成”时，执行自动操作。
- 已关闭：NNMi 检测到已解决故障后，［生命周期状况］变为“已关闭”时，执行自动操作。例如，如要“在节点停止后恢复和启动时与通报系统连动”，则指定“已关闭”。



8. 选择［命令类型］。

   如要指定 Jython 命令，则选择“Jython”；如要指定执行文件或补丁，则选择“ScriptOrExecutable”。

9. 输入［命令］。

   命令类型为“ScriptOrExecutable”时，输入可在指定有所需参数的操作系统上执行的命令。

   （配置示例）

   msg.exe Administrator “以$sourceNodeName 的形式发生了事件$name。”

   关于命令类型为“Jython”时的输入方法，请参照“管理员帮助”中“为管理事件配置操作”的说明。

10. 点击 保存并关闭 。

11. 点击［SNMP 陷阱配置］或［管理事件配置］中的 保存并关闭 。

    将保存配置内容。

> **提示**
>
> 依次选择［工具］-［事件操作日志］后，确认自动操作的执行状况。另外，可通过下列日志文件进行确认。
>
> - Windows 环境
>
>   NNMi 的安装目标数据文件夹\log\nnm\incidentActions.*.*.log
>
> - Linux 环境
>
>   /var/opt/OV/log/nnm/public/incidentActions.*.*.log
>
> 如果未勾选操作配置中的“已启用”，则不执行自动操作，也不生成日志记录。未能执行时，请先确认是否启用。关于详细情况，请参照“管理员帮助”中“配置事件”的说明。

下一步操作

对事件的自动操作配置至此结束。接下来，访问并配置 SSO。

相关项目

- 2.3　SSO 的配置

2.3 SSO 的配置

为了稳定地运行系统，服务器的状况检查是不可或缺的。SSO 可使用资源收集功能、进程及服务监视功能极其细致地检查服务器的状况。

2.3.1 访问 SSO

登录 SSO 并开始配置。

前提条件

- 如要使用 32 位版的 Web 浏览器，请使用 32 位版 Java Plug-in。如要使用 64 位版 Web 浏览器，请使用 64 位版 Java Plug-in。
- 如要使用 Java 8，请参照 SSO 的发布说明进行配置。
- 如果未能启动 SSO 画面，请按下述步骤更改 Internet Explorer 的配置。
  1. 启动 Internet Explorer。
  2. 依次点击［工具］-［Internet 选项］-［安全］，在安全区域中选择［本地 Intranet］或［可信站点］。
  3. 将安全区域的安全级别更改为［中上］以下。
  4. 点击［站点］。
  5. 将以 URL 指定的监视管理器的主机名（或 IP 地址）添加到［Web 站点］中。
  6. 重新启动 Web 浏览器。
  7. 依次选择［工具］-［ActiveX 筛选］，取消［ActiveX 筛选］的勾选。
  8. 重新启动 Web 浏览器。

操作步骤

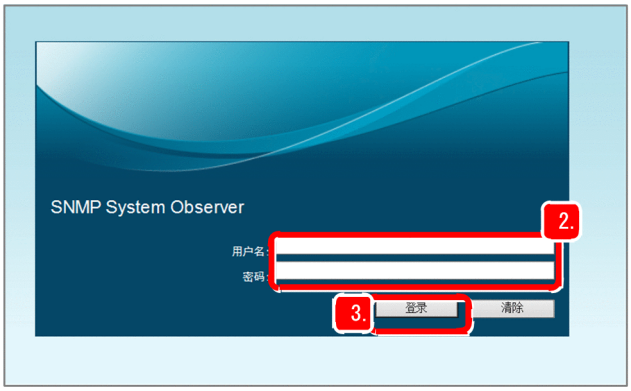
1. 通过 Web 浏览器访问 SSO。

   http://**主机名**:**端口号**/SSOConsole/

   在**主机名**中输入监视管理器的主机名。默认端口号为“20393”。

2. 输入用户名及密码。

   请按 SSO 定义信息中的设定值输入**用户名**及**密码**。



3. 点击［登录］。

将显示 SSO 控制台。

> **参考**
>
> 也可从 Windows 的［开始］依次选择［程序和功能］-［SNMP System Observer］-［SSO］进行显示。

下一步操作

SSO 的登录至此结束。接下来，进行通过 SSO 收集资源的配置。

相关项目

- 1.3.5(2)　在 NNMi 中配置 SSO 的定义信息
- 2.3.2　资源的收集

2.3.2　资源的收集

将 SNMP 代理器（ESA）导入到监视对象服务器后，SSO 可通过服务器收集系统资源。配置收集的时区、间隔、期间等后，则可定期收集并参照资源。

(1)　什么是资源收集？

资源收集是指，收集网络上的服务器系统资源或用户任意配置的监视资源。

SSO 可收集支持操作系统（Windows 及 Linux）与 SNMP 的各种服务器产品及网络设备的系统资源（性能信息、统计信息、运行信息）以及用户资源（用户可独自定义的资源），进行实时监视。例如，CPU 使用率超出 90%时，可进行发行事件等的监视。发行事件时，可同时自动执行任意操作。

SSO 可收集下列资源：

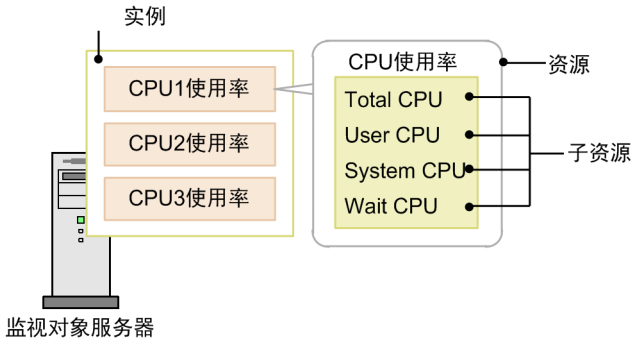
- 与 CPU 有关的资源：CPU 使用率、运行队列的长度、系统调用次数等
- 与内存有关的资源：内存使用率、交换区使用率等

- 与文件系统有关的资源：文件系统使用率、文件系统可用空间等
- 与网络有关的资源：线路使用率、界面流量等

配置收集对象的资源时，由于收集对象的选项已事先注册到 SSO 中，因此只需选择在 GUI 中显示的资源，即可简单地进行配置。可使用命令执行收集的开始及结束，因此也可实现操作自动化。

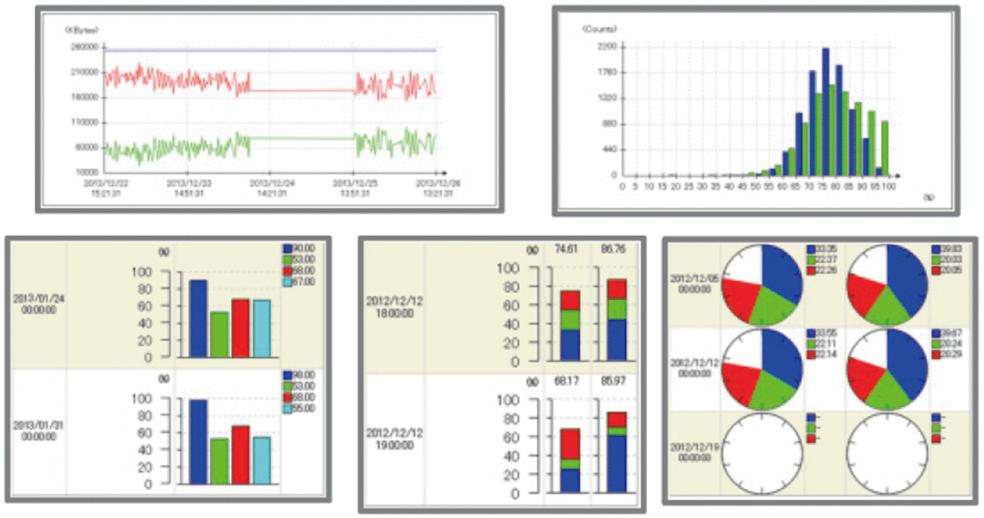
提示

在 SSO 的资源收集功能中，将资源收集源的实体定义为实例；将可从 SNMP 代理器获取的资源的最小项目定义为子资源；将多个子资源的分组定义为资源。



参考

使用收集的资源，即可按任意期间（月份或时间）创建报告。确认报告，即可掌握服务器的运作趋势，便于制定系统运行计划。可以 CSV 格式或 HTML 格式输出报告。可选择各种样式的图表，因此可输出适合用途的报告。



相关项目

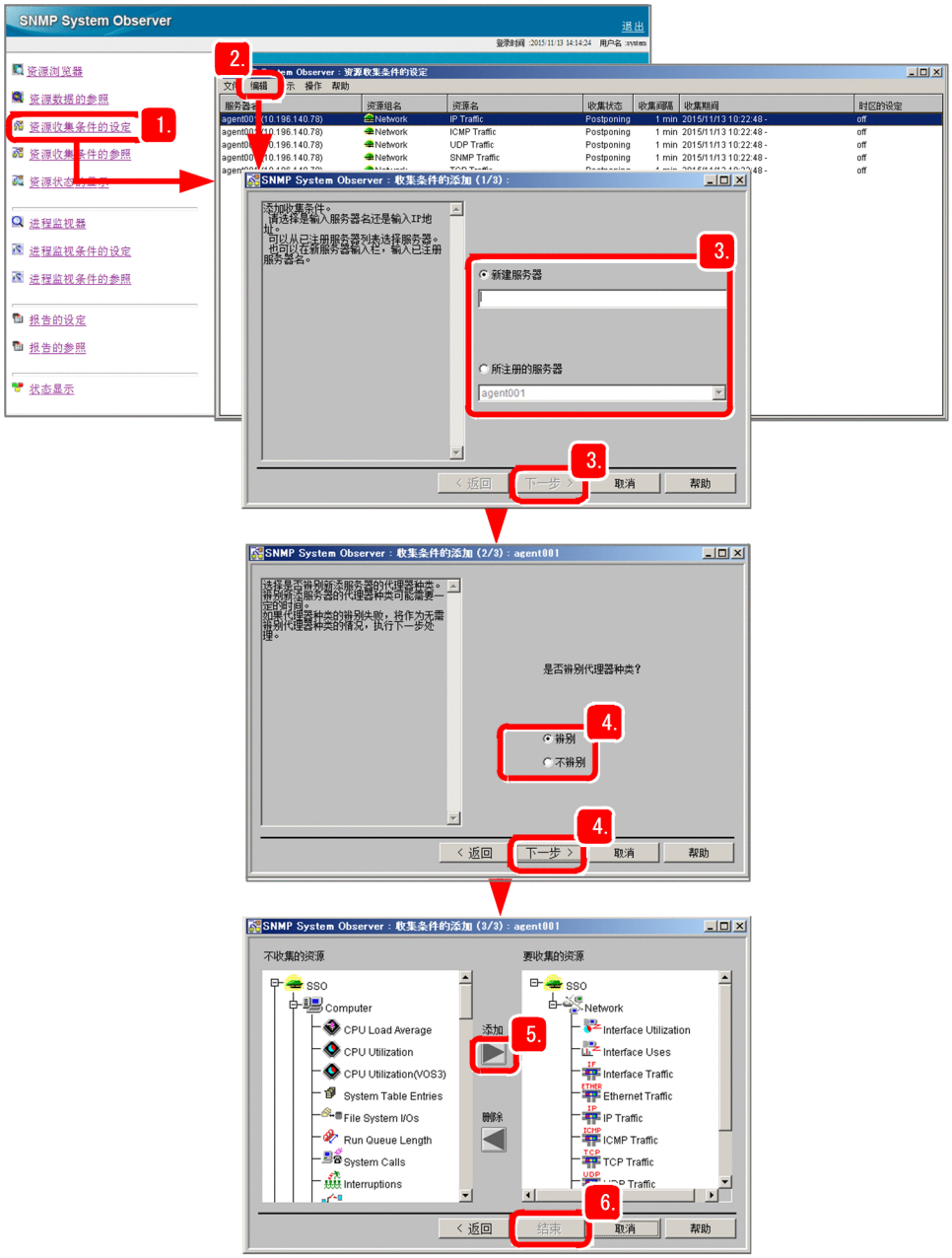
- 《JP1/SNMP System Observer》中“Resource IDs”的说明

(2) 开始收集资源

进行通过 SSO 收集资源的配置，开始收集资源。

操作步骤

1. 点击 SSO 控制台中的［资源收集条件的设定］。



2. 依次选择［编辑］-［收集条件的添加］。

3. 选择监视对象服务器后，点击［下一步］。

   直接在［新建服务器］栏位中指定服务器，或从［所注册的服务器］中选择已注册的服务器。

4. 选择是否自动辨别监视对象服务器的代理器类别后，点击［下一步］。

   可收集的资源因代理器类别而异。在［收集条件的添加（2/3）］向导中选择［辨别］后，将在［收集条件的添加（3/3）］向导中仅显示可根据代理器类别收集的资源。

5. 从［不收集的资源］中选择设为收集对象的资源，并点击［添加］。

   将选中的资源添加到［要收集的资源］中。

6. 点击［完成］。

将配置设为收集对象的资源。

7. 选择要配置收集条件的资源并依次选择［编辑］-［收集条件的更改］后，选择实例名、子资源名、收集模式。

   未配置收集条件时，所有实例均为收集对象。在收集模式下，可配置是否保存已收集的数据以及是否监视阈值。如要监视阈值，配置阈值以及超出阈值时执行的命令。

8. 点击［确定］。

   将配置资源收集条件。

9. 依次选择［编辑］-［收集时区的设定］。

   如要按每天指定的时区收集资源，配置资源的收集时区。

10. 勾选需要指定的时区编号的复选框，指定开始时间及结束时间。

    例如，如要每天在 8：00～18：00 的时区收集资源，将“08：00：00”指定为开始时间，将“18：00：00”指定为结束时间。

11. 点击［确定］。

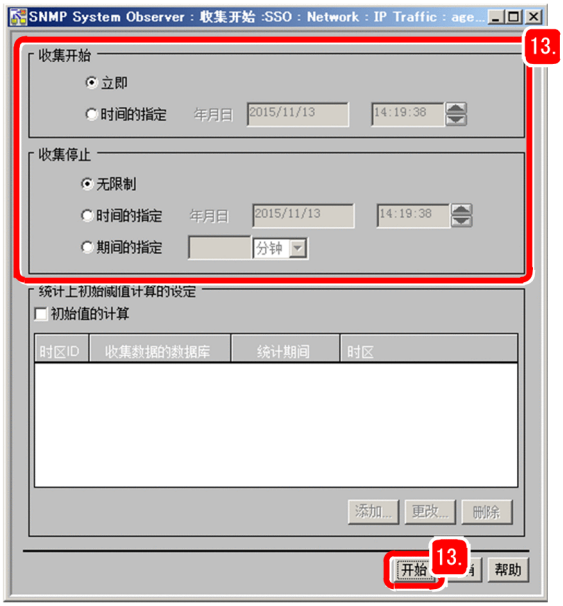
    将配置资源的收集时区。

> **提示**
>
> 也可根据用途配置收集间隔。配置收集间隔，即可减轻系统负荷。依次选择［编辑］-［收集间隔的变更］配置收集间隔。
>
> - 如要检测资源使用量及使用率的急剧上升状况，则配置较短的收集间隔。
> - 如要长期监视资源的使用情况，则配置较长的收集间隔。

12. 依次选择［操作］-［收集开始］。

13. 指定收集开始及收集停止来配置收集期间后，点击［开始］。

    将开始收集资源。



如果配置了收集时区，请在配置时确保［收集开始］窗口中的收集开始及收集停止的期间包括收集时区。

参考

- 如要手动结束收集资源，请在［资源收集条件的设定］窗口中选择要停止收集的资源，并依次选择［操作］-［收集停止］。
- 如要了解资源的收集状况，请确认［资源收集条件的设定］窗口中的收集状况。将显示当前的收集状况（［Deferred］、［Collecting］、［Completed］等）。

操作结果

资源收集至此开始。参照已收集的资源或将其输出到报告中，开始监视资源。

下一步操作

接下来，进行通过 SSO 监视进程及服务的配置。

相关项目

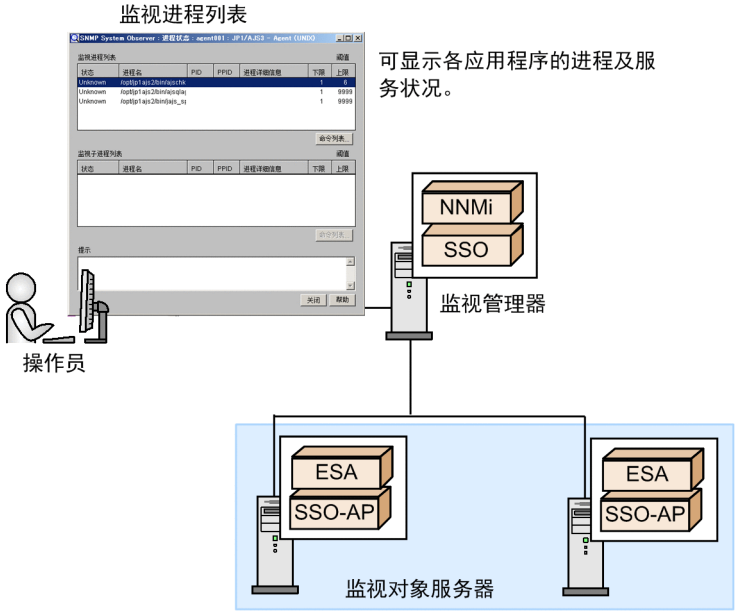
- 3.1.4　监视资源
- 2.3.3　进程及服务的监视

2.3.3　进程及服务的监视

以支持 SNMP 的服务器及网络设备为对象，可监视进程的存活状态及 Windows 服务的状况。由于 SNMP 属于工业标准协议，因此可在不考虑网络设备供应商及服务器代理器类型的情况下进行监视。

(1) 什么是进程及服务监视？

可集中 1 个以上的进程及服务，将其定义为应用程序，并通过进程的存活状态或 Windows 服务的状况监视应用程序是否正常运行。另外，可根据进程及服务的状况发行事件，或对监视对象服务器自动执行任意操作。因为通过筛选项目进行监视，所以便于监视整个系统的服务水平是否降低。



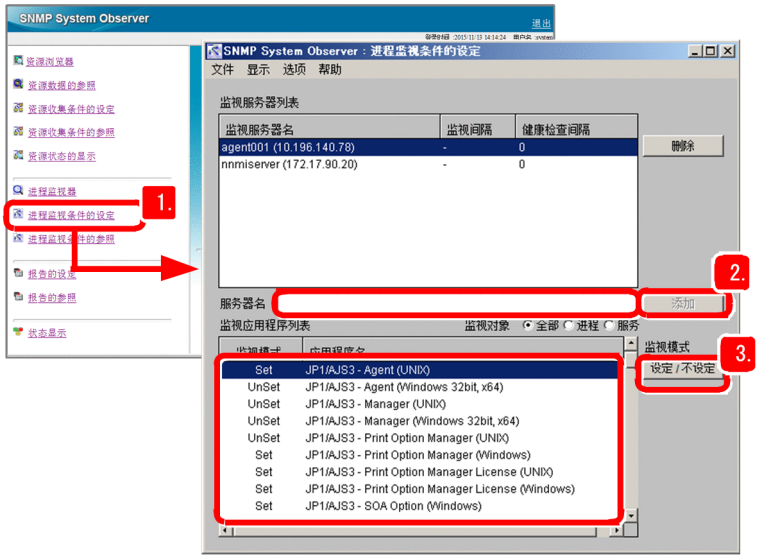
另外，通过将 SSO - AP 导入到监视对象服务器，可使用 SSO 定期监视该服务器的进程及服务的运行状况。即使监视对象服务器位于远程地点，也可及时发现运行的异常状况，因此可迅速加以对应，提高在业务中所使用服务器的效率。

(2) 配置监视的进程及服务

进行使用 SSO 监视进程及服务的配置并开始监视。

操作步骤

1. 点击 SSO 控制台中的［进程监视条件的设定］。



2. 在服务器名栏位中输入监视对象服务器的主机名或 IP 地址后，点击［添加］。

   将监视对象服务器添加到监视服务器列表中。

3. 从监视应用程序列表中选择监视对象应用程序后，点击［设定 / 不设定］。

   将切换监视应用程序列表的监视模式。

   请将监视对象应用程序的所有监视模式设为“设定”。

> **提示**
>
> 在监视应用程序列表中，已注册有各 JP1 产品的进程及服务。因此，可立即开始 JP1 产品的监视。如要监视 JP1 产品以外的应用程序，通过［进程监视条件的设定］窗口的［选项］-［应用程序的注册］注册应用程序。

4. 依次选择［选项］-［监视服务器］-［监视间隔的设定］。

5. 在监视间隔栏位中，按分钟输入监视对象服务器的监视间隔后，点击［确定］。

6. 依次选择［选项］-［监视服务器］-［健康检查间隔的设定］。

7. 在健康检查间隔栏位中，按分钟输入对监视对象服务器执行健康检查的间隔后，点击［确定］。

   将检查监视对象服务器的运行状况以及在监视对象服务器及管理器中分别配置的监视条件是否一致。

> **参考**
>
> 健康检查是用于检查是否正常监视进程及服务的功能。为了稳定地运行系统，建议实施定期健康检查。

8. 依次选择［选项］-［监视应用程序］-［自动操作］。

9. 分别选择是否在运行状况发生变化时自动执行命令后，点击［确定］。

   如果选择了［设定］，则在命令名中输入自动执行的命令。

> **参考**
>
> 运行状况发生变化时，也可在监视对象的远程服务器上执行命令。如要远程执行命令时，在［进程监视条件的设定］窗口中，依次选择［选项］-［监视应用程序］-［远程命令］进行配置。

10. 依次选择［文件］-［保存］。

将开始监视应用程序（已将监视应用程序列表的监视模式设为“设定”）的进程及服务。

> **参考**
>
> 如要结束进程及服务的监视，从［进程监视条件的设定］窗口的监视应用程序列表中选择结束监视的应用程序并点击［设定 / 不设定］，将监视模式切换为“不设定”。如果选择了［文件］-［保存］，则结束进程及服务的监视。

操作结果

进程及服务的监视至此开始。请点击 SSO 控制台中的［进程监视器］，参照进程及服务的运行状况。

下一步操作

JP1 网络管理产品的配置至此结束。请使用 JP1 网络管理产品开始监视网络。

相关项目

- 《JP1/SNMP System Observer》中“Register Application window”的说明
- 《JP1/SNMP System Observer》中“Remote Command window”的说明
- 3. JP1 网络管理产品的日常运行
- 4. JP1 网络管理产品的故障对应

3

JP1 网络管理产品的日常运行

JP1 网络管理产品开始定期监视网络。显示掌握全体网络状况的图画面或已收集的资源，开始监视网络。另外，为了持续管理网络，请定期进行运维操作。

3.1 JP1 网络管理产品的网络监视

3.1.1 网络监视的类型

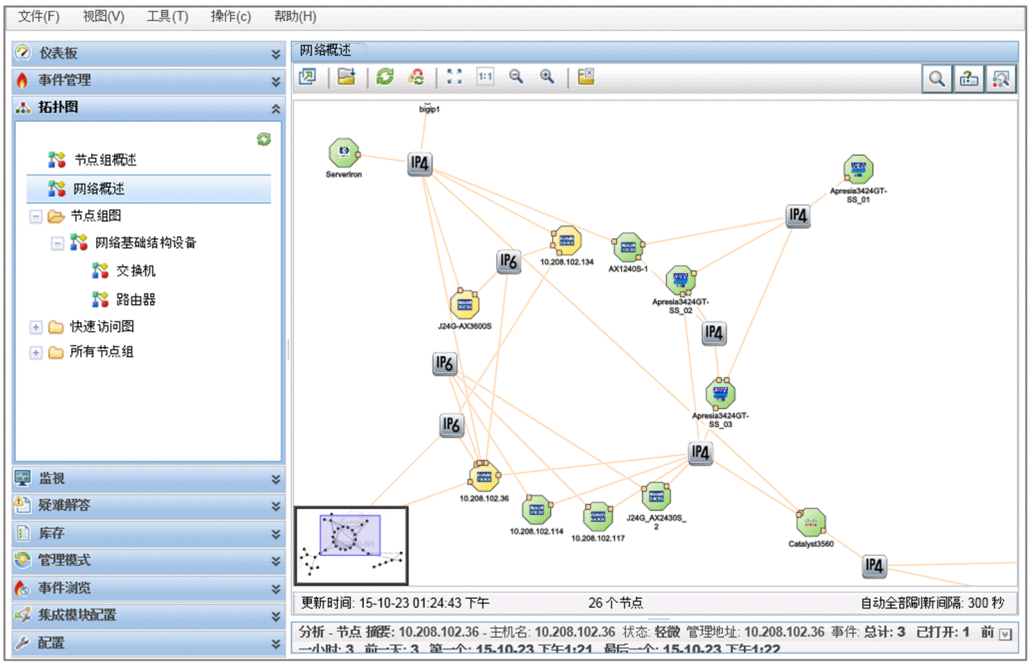
JP1 网络管理产品的网络监视方法有几种。下面通过图画面介绍运行方法及资源的确认方法。

> **参考**
>
> 通过使用 NEM，与服务器的资源监视操作一样，可对网络交换机进行资源监视。关于详细情况，请参照 NEM 的说明书。

(1) 拓扑图的监视（NNMi）

NNMi 根据已发现的网络设备自动生成网络构成图（拓扑图）。因此，开始运行后，可立即通过可视化画面掌握网络情况。

拓扑图



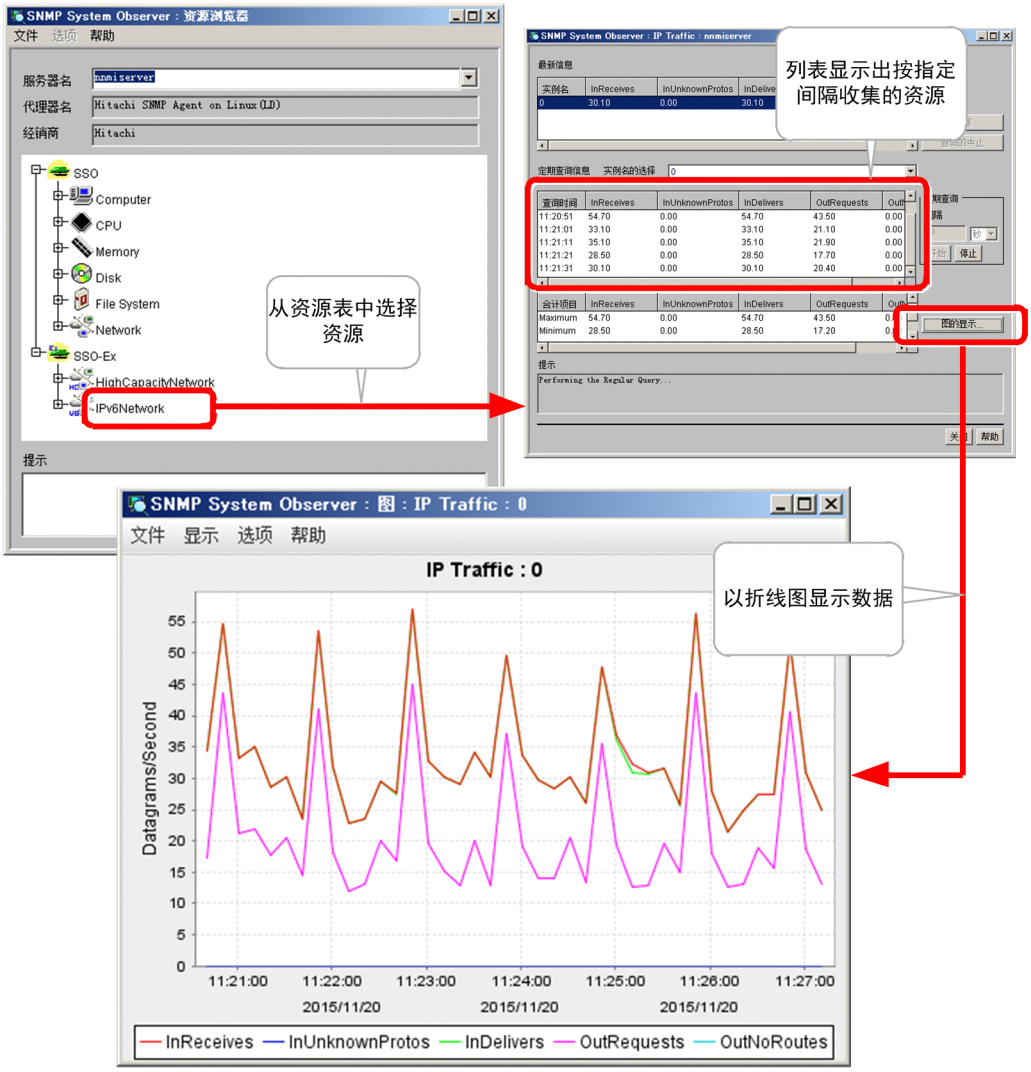
通过在拓扑图中使用图标，便于用户了解路由器或计算机等网络设备的类型。另外，可通过图标的颜色掌握是否发生故障等网络设备的状态。由于可显示网络的层 3 拓扑和层 2 拓扑以进行确认，因此可直观地掌握故障发生状况及影响范围。

相关项目

- 3.1.3 开始监视网络

(2) 资源监视（SSO）

SSO 可收集支持操作系统（Windows、Linux）及 SNMP 的各类服务器与网络设备的系统资源（性能信息、统计信息、运行信息）以及用户资源（用户可独自定义的资源），进行实时监视。例如，CPU 使用率超出 90% 时，可进行发行事件等的监视。



发行事件时，可同时自动执行任意操作。

相关项目

- 3.1.4 监视资源

3.1.2 什么是轮询？

轮询是指，使用 SNMP 或 ICMP（Ping）周期性地进行网络设备的发现或监视的操作。NNMi 通过基于 SNMP 或 ICMP 协议的轮询来监视已发现的网络设备。除了网络设备的状况之外，还包括风扇、电源电压等网络设备组件的状况，因此，可实现广泛的故障监视。

通过配置周期（按秒、分钟、小时、天），自动定期执行轮询。如要在解决故障后立即进行轮询，可以手动实施。由于可按网络设备、节点组等针对多个范围配置各不相同的轮询条件，因此可根据监视对象的重要度更改轮询实施周期等。

参考

轮询大致包括 2 种类型。

- 用于发现的轮询
- 用于监视的轮询

实际上包括上述 2 种类型，但根据目的或状况进行如下标示。

用于发现的轮询

- 发现轮询
  依次选择［操作］-［轮询］-［配置轮询］，可立即进行轮询。
- 重新发现轮询（定期重新发现的轮询，用于检查已发现的节点是否更改了构成）
- 配置轮询（用于发现配置的轮询）
- 找出轮询（用于找出节点的轮询）

用于监视的轮询

- 状态轮询（用于监视状态的轮询）
  依次选择［操作］-［轮询］-［状态轮询］，可立即进行轮询。
- 状况轮询（用于监视状况的轮询）
- 故障轮询（用于监视是否发生故障的轮询）
- 按需轮询（根据手动操作等立即进行监视的轮询）

3.1.3 开始监视网络

下面介绍显示网络构成的图画面（拓扑图）监视网络的方法。通过 NNMi 进行网络监视。例如，在运行管理中心等，始终在大型显示器上显示最重要的图进行监视等。配置发现后，可暂时参照发现节点的过程。

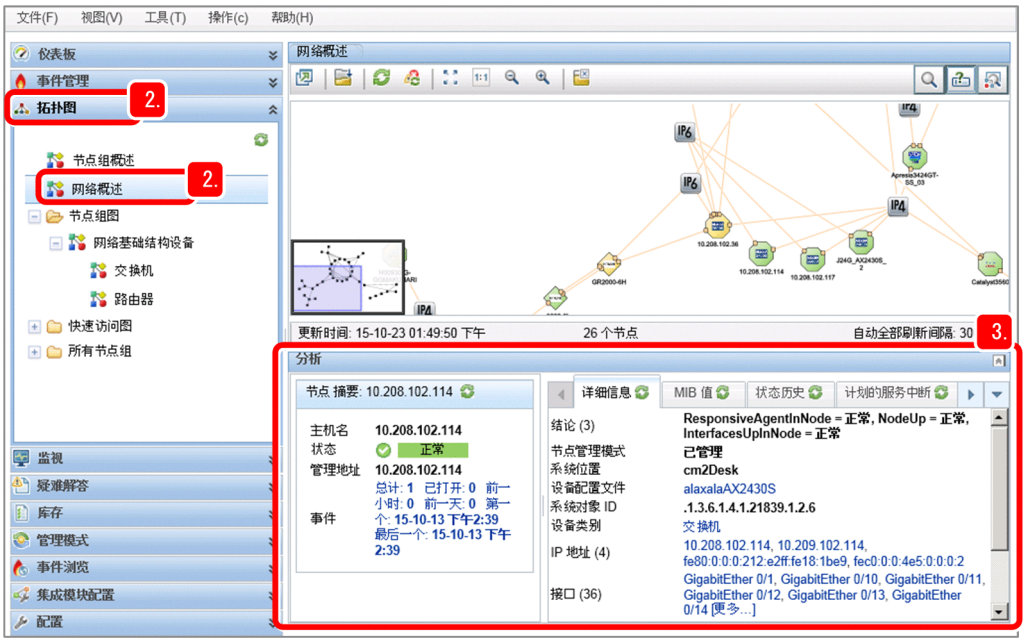
前提条件

开始监视网络前，请将监视业务负责人（操作员）注册为用户。

操作步骤

1. 访问 NNMi 控制台。

2. 依次点击［拓扑图］-［网络概述］。



3. 通过图标颜色或详细情况确认节点状态。

如果选择图上的图标，则在画面下方的［分析］窗格中显示详细情况。点击 ，则可切换［分析］窗格的显示 / 不显示。

> **提示**
>
> 如要确认节点拥有的 MIB 信息，可使用 nnmsnmpwalk.ovpl 命令进行确认。

图标的颜色与含义

通过 6,000 种以上的设备信息（注册到［配置］-［设备配置文件］中）自动辨别设备类型。确定设备配置文件后，按分类（设备范畴）确定图上的图标形状。图中的图标颜色与含义如下所示。

图标颜色	含义	图标颜色	含义
绿色	正常	红色	严重
浅蓝色	警告	蓝色	未知
黄色	轻微	灰色	已禁用
橙色	重大	米色	无状态

关于图标的详细情况，请参照帮助“使用 NNMi 控制台”中“关于图符号”的说明。

参考

在运维期间暂停监视时

如果在拓扑图等中选择节点并依次选择［操作］-［管理模式］-［服务中断］，则停止监视或重新发现。如果使用 nnmmanagementmode.ovpl 命令将管理模式设为服务中断，则可停止监视。

重新开始监视时

如果在拓扑图等中选择节点依次选择［操作］-［管理模式］-［管理］，则重新开始监视。另外，如果使用 nnmmanagementmode.ovpl 命令将管理模式设为管理对象，则重新开始监视。

以列表显示设为非管理对象的节点时

参照［管理模式］-［非被管节点］。

提示

如果未在一定时间内操作常规画面，则发生超时。可在［配置］-［用户界面］-［用户界面配置］的控制台超时中配置超时时间。默认值为 18 小时。

另外，指定 URL 打开的画面不发生超时。如要始终显示拓扑图进行监视，请指定 URL。

- 网络概述

  http://主机名:端口号/nnm/launch?cmd=showNetworkOverview

- 节点组图

  http://主机名:端口号/nnm/launch?cmd=showNodeGroup&name=节点组名*

注* 如果 URL 包括多字节字符，需要进行 URL 编码。请使用字符代码 UTF-8 进行节点组名称的 URL 编码和记述。

（例）重要节点

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

另外，如要打开多个画面（如拓扑图及事件画面等）进行监视，点击  （通过新窗口显示视图），则弹出新的画面。另外，在输入 URL 打开画面的情况下，也可弹出多个画面。

提示

如要配置登录时的初始画面，可在［用户界面配置］的初始视图中指定。例如，如要查看事件，则指定“未决重大事件”；如要查看图，则指定“网络概述”。另外，也可将用户创建的节点组图制成初始视图，但只能指定图列表的最初或最后。因此，请调整节点组图配置的［拓扑图排序］。关于详细情况，请参照帮助“管理员帮助”中“配置 NNMi 用户界面”的说明。

下一步操作

拓扑图的显示至此结束。请开始监视网络。

相关项目

- 2.2.3　注册用户

3.1.4　监视资源

参照监视对象的资源。通过 SSO 进行资源监视。

前提条件

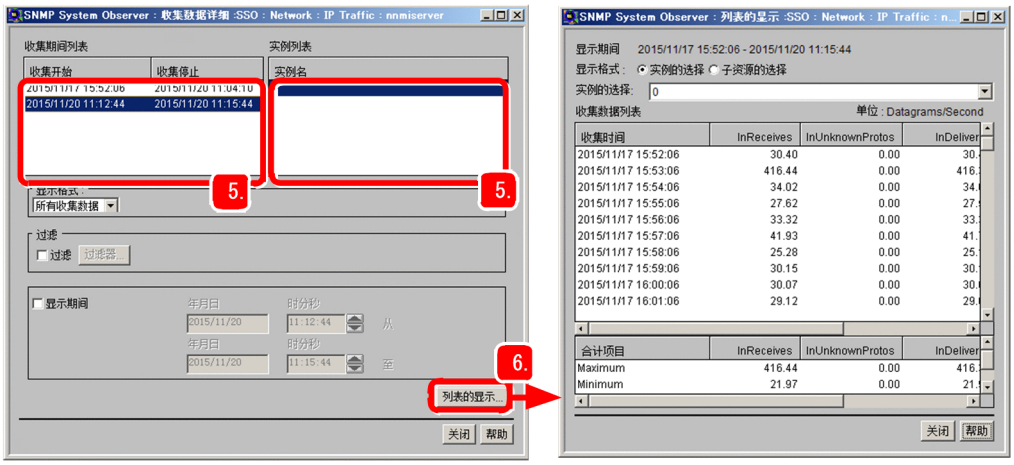
请配置资源收集条件。

操作步骤

1. 访问 NNMi 控制台。
2. 依次点击［拓扑图］-［网络概述］。
3. 选择参照资源的服务器，依次点击［操作］-［SNMP System Observer］-［资源数据的参照］。

> **提示**
>
> 点击  （检索），即可检索要参照的服务器名。

4. 选择参照的资源，并依次选择［显示］-［收集数据详细］。
5. 从“收集期间列表”及“实例列表”中分别选择要参照的期间及实例。



6. 点击［列表的显示］。

   可参照收集数据列表。

提示

可在［资源数据的参照］窗口中复制及删除已收集资源的数据。

例如，只要复制并保留发生问题期间的资源，以及删除其他不需要的资源，即可确保数据库的可用空间。

下一步操作

已收集的资源的参照至此结束。请根据需要将已收集的资源输出到报告等，掌握服务器的操作趋势，制定系统运行计划。

参考

可将收集对象的资源输出到报告。可通过 SSO 控制台的［报告的参照］输出报告。如要输出报告，需要事先进行报告配置。关于报告输出的详细情况，请参照《JP1/SNMP System Observer》中“Report Configuration window”的说明。

相关项目

- 2.3.2　资源的收集
- 《JP1/SNMP System Observer》中“Copy Collection Condition window”的说明

3.2 JP1 网络管理产品的定期运维

为了持续管理网络，平时的运维操作是至关重要的。下面对 JP1 网络管理产品的运行操作进行说明。

3.2.1 检查 NNMi 运行状况

首先，需要确保 NNMi 正常运行，以便管理网络。请确认 NNMi 正常运行。

操作步骤

1. 依次点击［帮助］-［系统信息］。
2. 确认［产品］的状态。
   确认状态为“正常”。
3. 在［健康］中确认 NNMi 的详细状况。
4. 在［状况轮询器］中确认运行状况。
5. 在［数据库］中确认已发现的对象数量等。

操作结果

NNM 正常运行的确认至此结束。

> **提示**
>
> NNMi 本身发生问题时，NNMi 控制台下部将显示黄色警告，并发行 NnmHealthOverallStatus 事件。如果在运行期间接到了该事件的通知，请在［事件］的“自定义属性”中进行确认。

相关项目

- 帮助“管理员帮助”中“检查 NNMi 运行状况”的说明

3.2.2 导出或导入 NNMi 配置

按重要性保存系统配置和管理更改内容均为在运行中重要的操作。可通过 NNMi 导出或导入系统配置。由此，可获取当前系统配置的快照，以便在配置出错时通过导入进行恢复。

操作步骤

1. 执行 nnmconfigexport.ovpl 命令或 nnmconfigimport.ovpl 命令。
   nnmconfigexport.ovpl 命令及 nnmconfigimport.ovpl 命令的执行示例如下所示。

目的	命令
导出所有配置	nnmconfigexport.ovpl -c all -f c:\nnmiconf
导入所有配置	nnmconfigimport.ovpl -f c:\nnmiconf
导入节点组配置	nnmconfigimport.ovpl -f c:\nnmiconf\nodegroup.xml

操作结果

NNMi 配置的导出或导入至此结束。

相关项目

- 1.2.4 各产品的命令保存位置
- 帮助“管理员帮助”中“导出和导入配置设置”的说明

3.2.3 备份或恢复 NNMi

为了防止因系统故障或操作失误而导致数据损失等意外事故，定期进行备份是在运行中重要的操作。由于 NNMi 可在持续监视网络的状态下进行在线备份，因此请按计划实施备份。

操作步骤

1. 执行 nnmbackup.ovpl 命令或 nnmrestore.ovpl 命令。

   nnmbackup.ovpl 命令及 nnmrestore.ovpl 命令的执行示例如下所示。

目的	命令
对整个 NNMi 进行在线备份	nnmbackup.ovpl -type online -scope all -force -target c:\nnmi 在指定为-target 的文件夹中创建带有日期及时间的文件夹（如“nnm-bak-20150922002454”）。
恢复备份	nnmrestore.ovpl -force -source c:\nnmi\nnm-bak-20150922002454

操作结果

NNMi 的备份或恢复至此结束。

相关项目

- 1.2.4 各产品的命令保存位置
- 帮助“管理员帮助”中“备份和恢复 NNMi”的说明

3.2.4 存档和删除 NNMi 事件

NNMi 可在数据库中记录最多 10 万条 SNMP 陷阱事件信息。另外，为了避免因数据条数增加而影响性能，可进行存档或自动删除（修剪）旧数据。

(1) 确认 SNMP 陷阱事件的条数

确认 SNMP 陷阱事件的条数。

操作步骤

1. 打开［事件浏览］-［SNMP 陷阱］。
   将在事件列表下面的“总计”中显示条数。

操作结果

SNMP 陷阱事件条数的确认至此结束。

> **参考**
>
> 如果 SNMP 陷阱事件的条数接近上限，则通知下列事件。
>
> - 上限的 90%：SnmpTrapLimitWarning
> - 上限的 95%：SnmpTrapLimitMajor
> - 上限：SnmpTrapLimitCritical

相关项目

- 帮助“管理员帮助”中“存档和删除事件”的说明

(2) 启用自动修剪功能

启用自动修剪功能后，如果 SNMP 陷阱事件数超出指定值，则自动删除（修剪）旧数据，或在修剪时自动创建存档文件。在默认配置中，已禁用自动修剪功能。建议启用该功能后进行运行。

相关项目

- 《JP1/Network Node Manager i Setup Guide》中“Configuring the auto-trim oldest SNMP trap incidents feature”的说明

3.2.5 定期删除 SSO 的收集数据

SSO 的收集数据库没有保存期间，数据不断增加。因此，如果持续收集，数据库将膨胀并变大，可能导致显著降低数据库的收集或删除性能。为了确保收集数据库的性能，建议定期对数据库进行备份或删除数据。运行时，请将收集数据的保存期间最长设为 1 年。

操作步骤

1. 执行 ssodbdel 命令。

   删除超出保存期间的收集数据的命令执行示例如下所示。

   ssodbdel -all -stop BMONTH 13

   如果执行了该命令，则从收集数据库中删除保存期间超出 1 年的数据。通过在每个月的第一天执行该命令，在收集数据库中仅保留最近 1 年的数据。

操作结果

SSO 的收集数据删除至此结束。

相关项目

- 1.2.4　各产品的命令保存位置
- 《JP1/SNMP System Observer》中“ssodbdel”的说明

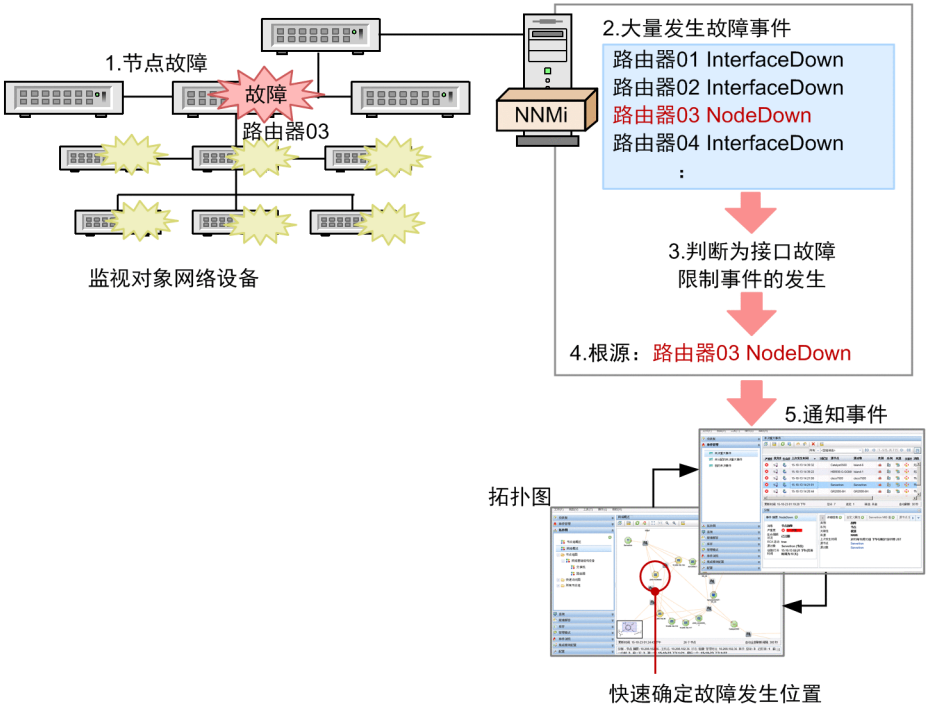
4 JP1 网络管理产品的故障对应

通过 JP1 网络管理产品的事件管理迅速确定并解决故障。

4.1 故障根源分析

在发生故障时，监视管理器通过根源分析功能调查大量发生的事件的相关关系，并对其进行筛选。通过基于层 2 拓扑与层 3 拓扑的故障分析确定根源，作为事件进行通知。在问题发生至解决期间对事件的对应进展状况（生命周期状况）进行管理。

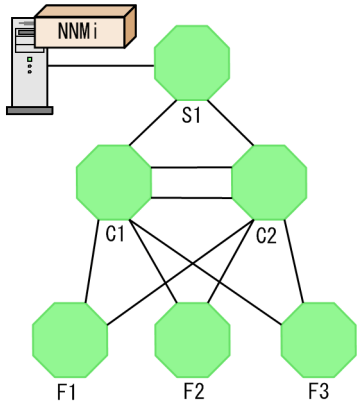
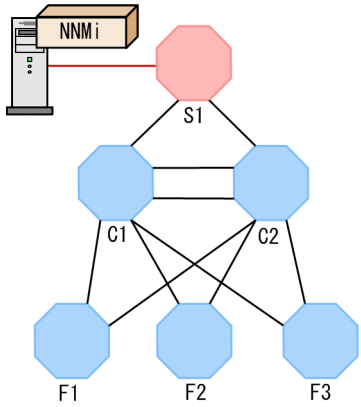
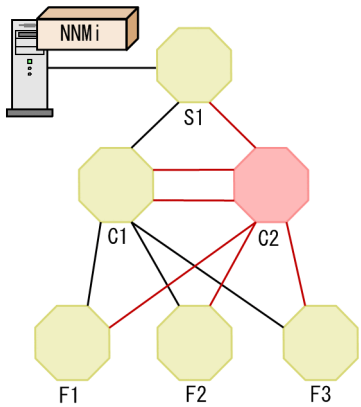
以网络设备（路由器）的监视为例，下面对观察根源分析的操作进行说明。



1. 如果路由器 03 发生节点故障，路由器 03 拥有的多个接口或 IP 地址则变为无响应状态。
2. 因接口故障或 IP 地址无响应等而大量发生故障事件。
3. 监视管理器判断为因接口故障而发生 IP 地址无响应，并限制事件的发生。
4. 根据相邻节点的通信中断状态，判断路由器 03 的节点故障为根源。监视管理器判断接口故障由上述状况所导致并与路由器 03 发生的节点故障有关。
5. 作为根源的事件，通知路由器 03 的节点故障。

另外，监视管理器也会有效使用层 2 拓扑信息对构成网络的多个节点进行根源分析。使用层 2 拓扑的网络构成进行根源分析的示例如下所示。

层 2 拓扑分析	描述
平时	监视管理器连接到最上层的交换机“S1”，当前监视的所有网络处于正常状态。

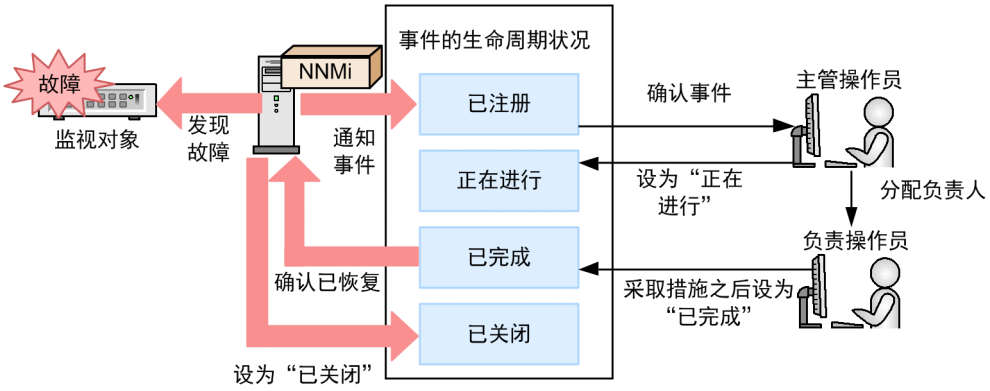
层 2 拓扑分析	描述
	
最上层交换机发生故障时 	故障内容：最上层交换机“S1”发生宕机 发生事件： • 不可与“S1”进行通信 • 不可与经由“S1”的其它交换机进行通信 监视管理器对上述状况进行如下对应： • 检测出“S1”的节点故障。 • 监视管理器判断“S1”的连接目标因受到“S1”故障的影响而无法通信后，限制事件的发生并视为状况不明。 作为最后结论，仅将“S1”故障作为根源事件进行通知。
中间交换机发生故障时 	故障内容：中间交换机“C2”发生宕机 发生事件： • 不可与“C2”进行通信 • 连接到各节点的“C2”的接口处于宕机状态 监视管理器对上述状况进行如下对应： • 发现“C2”的节点故障。 • 监视管理器判断连接“C2”的各接口受该故障影响，并限制事件的发生。 作为最后结论，仅将“C2”故障作为根源事件进行通知。

监视管理器可对其它许多情况及根源的对应方法进行分析。

4.2 故障对应机制

监视管理器在［事件］中管理事件对应进展状况，将其作为生命周期状况。由多人分担管理时，由于可指定自己以外的运行负责人（分配目标），因此开始故障的解决操作时，可在 GUI 上分担操作。

如下图所示，通过更改事件对应负责人的分配及生命周期状况，可适当地对应已发生的故障。



在通知事件之后，监视管理器仍会继续监视状况。检测出恢复时，事件将自动变为“已关闭”。例如，如果已通知“节点故障”的节点重新开始操作，事件则自动变为“已关闭”。

提示

为操作练习制造模拟故障，以此为例对通知的事件的确认方法进行说明。

1. 通过在监视对象节点上拔下 LAN 电缆或停止节点，制造模拟故障。
   请注意不要影响到业务。
2. 在图画面中选择节点后，依次选择［操作］-［轮询］-［状态轮询］。
   将进行状态轮询，并检测故障。

4.3 对应网络故障

对应网络故障的方法包括几种。下面对两种方法进行说明：对应网络设备节点故障的方法；对应进程及服务运行状况异常的方法。

4.3.1 对应网络设备的节点故障

发行通知网络设备节点故障的事件后，确认有问题的位置并采取措施。

操作步骤

1. **在 NNMi 控制台的拓扑图中确认故障位置。**

   如果检测出故障，图中的图标颜色则发生变化。

   如果已对图进行分层，则打开子节点组确认状况。节点组反映最关键的状况。子节点组的状况也反映到父节点组。

2. **打开［事件浏览］，确认作为根源通知的事件。**

   打开［未决重大事件］或［所有事件］，浏览事件内容，并确认问题位置。选择对象节点并打开［事件］，即可按时序确认事件的发生。首先，对源节点、源对象及自定义属性进行确认。

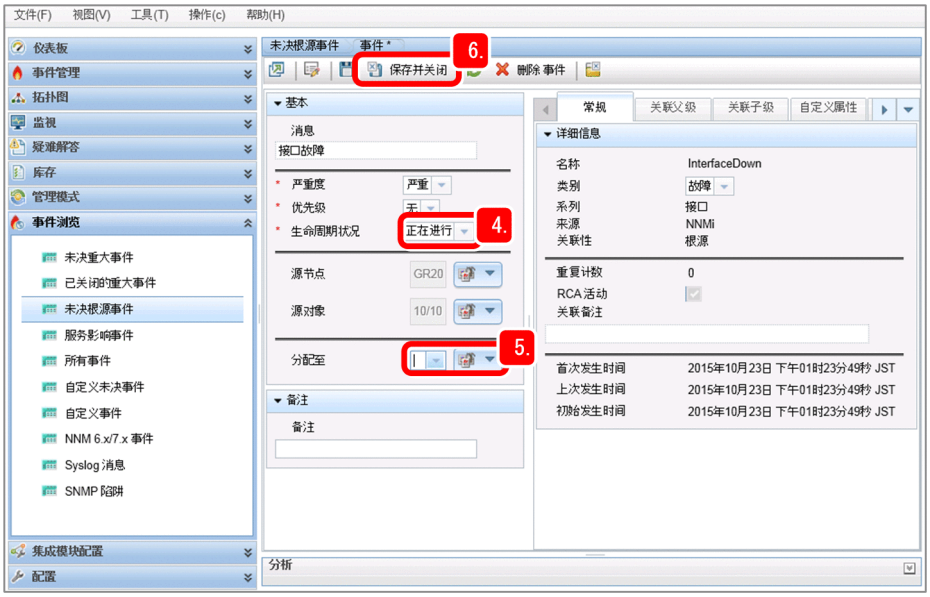
3. **双击事件，确认事件的详细信息。**

   将显示［事件］。确认“消息”及“名称”栏位中显示的已发生的事件的类型、“源节点”栏位中显示的发生位置以及“日期与时间”栏位中显示的时间。

   > **参考**
   >
   > 属于 SNMP 陷阱事件时，在［自定义属性］中确认详细信息。在自定义属性中显示通过 SNMP 陷阱通知的信息。因此，请参照发行 SNMP 陷阱的设备的说明书，确认内容。

4. **将事件的［生命周期状况］设为［正在进行］。**

   掌握问题状况后，从［生命周期状况］的下拉菜单中选择状况。注册事件后，暂时处于［已注册］状态。



5. 从［分配至］的下拉菜单中选择自己的帐户。

   如要分配自己以外的操作员，请确认操作员可访问分配的事件。

6. 点击 保存并关闭 。

   将保存已更改的配置。

7. 确认相关部分的状况。

   网络故障经常影响到通信路径的相关部分。因此，除了确认根源之外，也要确认相关部分。

   - 在图画面中确认相关部分，掌握状况。
   - 在［监视］中掌握有无问题部分。

8. 采取措施。

> **提示**
>
> 如果事先对事件配置自动操作，即可自动执行指定的命令。

9. 采取措施后，将事件的［生命周期状况］设为［已完成］。

   识别到系统没有问题时，自动设为［已关闭］。

10. 点击 保存并关闭 。

    将保存已更改的配置。

11. 确认已更改的事件的状况。

    确认在［事件浏览］中的［生命周期状况］处于［已关闭］状态。

操作结果

对应网络设备节点故障的措施至此结束。

相关项目

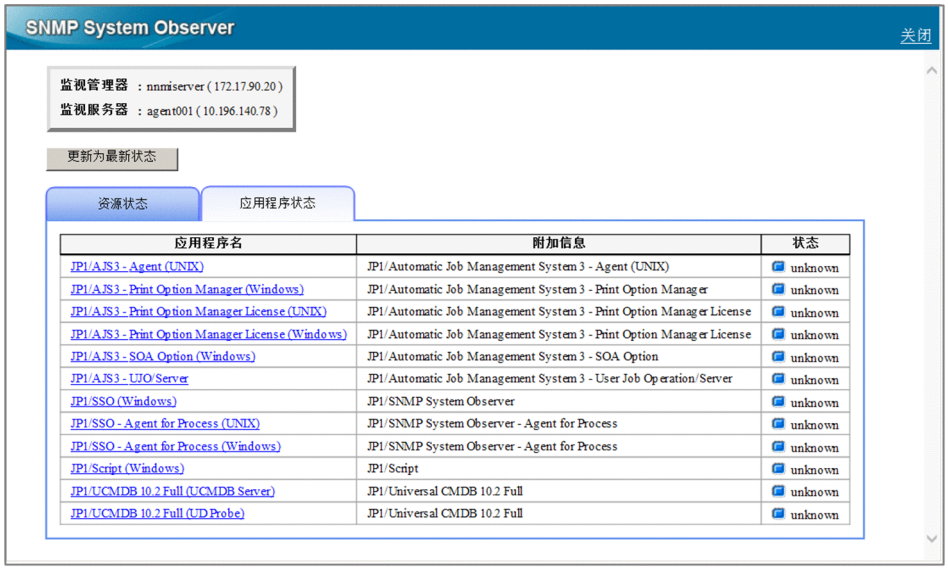
- 帮助“操作员帮助”中“解释根源事件”的說明
- 2.2.8(4)　对事件配置自动操作
- 3.1.3　开始监视网络
- 4.2　故障对应机制

4.3.2　对应进程及服务运行状况的异常

发行通知进程及服务异常的事件后，确认有问题的位置并采取措施。

操作步骤

1. 打开 NNMi 控制台的［事件浏览］，确认通知进程及服务异常的事件的内容。
2. 依次点击［拓扑图］-［网络概述］。
3. 选择确认故障的监视对象后，依次点击［操作］-［SNMP System Observer］-［监视状态的显示］。
   将弹出监视状况显示画面，用于显示资源状态及应用程序状态。
4. 选择［应用程序状态］。
   可根据图标颜色识别应用程序的状态。
   - 绿色：正常
   - 黄色：警戒
   - 红色：危险
   - 蓝色：未知



5. 针对有问题的进程及服务采取措施。

6. 采取措之后，将事件的［生命周期状况］更改为［已完成］。

操作结果

对应进程及服务异常的措施至此结束。

相关项目

- 4.3.1　对应网络设备的节点故障

附录

附录 A　如何能更有效地使用本产品？

下面介绍更有效地使用 JP1 网络管理产品的参考信息。

NNMi Advanced 的介绍

作为 NNMi 的上层产品，JP1 网络管理产品提供的 NNMi Advanced 实现了支持高级网络技术的监视。NNMi Advanced 的主要功能如下所示。

功能	描述
全局网络管理	可通过区域管理器（用于监视各据点）及全局管理器（用于统一该区域管理器）进行集中网络管理。全局管理器可管理最多 65,000 个节点。
IPv6 网络的管理	由于可同时对 IPv6 及 IPv4 进行管理，可对下一代网络及现有网络进行有效的一体化管理。
VMware ESX 服务器的管理	按自动识别路由器或交换机的方式，自动识别 ESX 主机及虚拟机，并以列表形式管理库存信息。
链路聚合的管理	自动识别聚合的链路构成。另外，在图上用粗线显示聚合的链路。
冗余路由器的管理	自动识别冗余路由器组的构成。另外，可监视路由器组是否适当地路由数据包。

关于详细情况，请参照说明书《JP1/Network Node Manager i Setup Guide》。

运行方法介绍

下面介绍使用 JP1 网络管理产品的运行例。关于详细情况，请确认参照章节。

情况	说明	参照章节
总之想先试用本产品。是否有最简单步骤？	请按下列 3 个步骤开始运行。 1. 在［通信配置］中配置 SNMP 团体字符串。 2. 在［发现配置］中指定自动发现的 IP 地址的范围，并启用 Ping 扫描以及 SNMP 节点的发现。 3. 打开［拓扑图］-［网络概述］，开始运行。	2.2.4 2.2.5 3.1.3
未发现任何节点。	请在［发现配置］中指定发现对象的 IP 地址范围及作为发现起点的发现种子。在［拓扑图］或［库存］中确认发现状况。另外，依次选择［帮助］-［系统信息］-［状况轮询器］，则可确认发现的处理状况。	2.2.5
仅发现路由器或交换机。	在默认配置时，仅发现路由器或交换机。 请在［发现配置］-［自动发现规则］中启用［发现所有 SNMP 设备］或［发现非 SNMP 设备］。	2.2.5
如果定义了节点组，则显示过多的拓扑图名，难以浏览。	如果将节点组图的［拓扑图排序］设为空白，则不在［拓扑图］的［快速访问图］文件夹中显示。	2.2.6
虽然无法与节点进行通信，但问题并不严重，变成不能识别（图标为蓝色）。	例如，网络路径上的交换机发生故障，无法与某个节点进行通信时，NNMi 将交换机作为故障的根源通知事件。另外，将受其影响而无法	2.2.6 2.2.8

情况	说明	参照章节
	通信的节点辨别为“未知”。无法通信时，如要通知事件，请使用“重要节点”。	
SNMP 管理器（NNMi）的 IP 地址如何配置?	根据操作系统的网络路由配置，区别使用与通信目标 IP 相应的 IP 地址。因此，如要在 SNMP 代理器侧的 SNMP 配置中指定（允许连接）SNMP 管理器的 IP 地址，请配置 NNMi 管理器的所有 IP 地址。 如要固定 IP 地址，请在 ov.conf 文件的 NNM_INTERFACE 处指定 IP 地址。请调整操作系统的路由配置，以便使用固定 IP 地址进行通信。	发布说明
发行了 SNMP 陷阱，但未能作为事件进行通知。	如要在 NNMi 接收到 SNMP 陷阱时，将其作为事件进行通知，启用已发现节点以及已定义相应 SNMP 陷阱事件时进行通知的功能。如要将出自未发现的节点的陷阱形作为事件，则关闭［事件配置］中的［丢弃未解析的 SNMP 陷阱和 Syslog 消息］。	帮助“管理员帮助”中“处理未解析的传入陷阱”的说明
希望创建服务器列表或事件列表等。	在以表格形式显示数据列表的画面（库存画面等）中，以 CSV 格式将数据输出到文件中。例如，依次打开［库存］-［节点］，进行如下操作。 1. 选中输出的行。 2. 右键点击显示菜单，并选择［导出到 CSV］。 3. 按照显示内容进行操作。 请将其读入到试算表软件中，以创建列表等。可创建［节点］的节点列表或［管理事件配置］的事件列表等。	帮助“使用 NNMi 控制台”中“导出表信息”的说明

附录 B　各版本的变更内容

附录 B.1　11-10 的变更内容

(1)　资料号（3021-3-C05-10(E)）的变更内容

- 在应用 OS 中，添加了 Windows Server 2016。
- 不支持以下版本的浏览器。
  - Internet Explorer 9
- 更新了 Firefox 的支持版本。

附录 C　本说明书的参考信息

下面介绍阅读本说明书时的参考信息。

附录 C.1　相关说明书

相关说明书如下所示。请根据需要阅读。

- JP1 Version 11 JP1/Network Node Manager i Setup Guide（3021-3-A72(E)）
- JP1 Version 11 JP1/Network Node Manager i Developer's Toolkit Guide（3021-3-A73(E)）
- JP1 Version 11 JP1/SNMP System Observer（3021-3-A77(E)）
- JP1 Version 11 JP1/Extensible SNMP Agent（3021-3-A78(E)）

在说明文中，将“JP1 Version 11 JP1/Network Node Manager i Setup Guide”表示为“JP1/Network Node Manager i Setup Guide”；将“JP1 Version 11 JP1/SNMP System Observer”表示为“JP1/SNMP System Observer”；将“JP1 Version 11 JP1/Extensible SNMP Agent”表示为“JP1/Extensible SNMP Agent”。

附录 C.2　微软产品名称的表示方法

在本说明书中，按下表所示名称表示微软产品名称。

表示方法			产品名称
Internet Explorer			Microsoft(R) Internet Explorer(R)
			Windows(R) Internet Explorer(R)
Windows	Windows Server 2008 R2		Microsoft(R) Windows Server(R) 2008 R2 Datacenter
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
			Microsoft(R) Windows Server(R) 2008 R2 Standard
	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

附录 C.3　本说明书中使用的书写格式

本说明书中使用的符号如下所示。

书写格式	描述
文字列	表示变量值。 （例）以 YYYYMMDD 的格式指定日期。
［　］	表示窗口、对话框、标签、菜单、键等画面上的要素名。
［　］-［　］	表示依序选择菜单。 （例）依序选择［文件］-［帮助］。 在上例中，表示选择［文件］菜单内的［帮助］。

附录 C.4　产品名称的标示方法

在本说明书中，按下表所示名称表示产品。

本说明书中的表示方法		正 式 名 称
Adobe Flash Player		Adobe(R) Flash(R) Player
ESA		JP1/Extensible SNMP Agent
Firefox	Firefox ESR 45	Mozilla Firefox(R) ESR 45
IPF		Itanium(R) Processor Family
JP1/IM		JP1/Integrated Management - Manager
Linux	CentOS 6.1 (x64)	CentOS 6 (x64)（6.1 或更新的版本）
	CentOS 7.1	CentOS 7（7.1 或更新的版本）
	Linux 6.1 (x64)	Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)（6.1 或更新的版本）
	Linux 7.1	Red Hat Enterprise Linux(R) Server 7（7.1 或更新的版本）
	Oracle Linux 6.1 (x64)	Oracle Linux(R) Operating System 6 (x64)（6.1 或更新的版本）
	Oracle Linux 7.1	Oracle Linux(R) Operating System 7（7.1 或更新的版本）
	SUSE Linux 12	SUSE Linux(R) Enteprise Server 12
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 V6.1

本说明书中的表示方法			正 式 名 称
			AIX V7.1
	HP-UX (IPF)		HP-UX 11i V3 (IPF)
	Solaris	Solaris 10	Solaris 10 (SPARC)
		Solaris 11	Solaris 11 (SPARC)
VMware			VMware(R)

附录 C.5　英文缩写

本说明书中使用的英文缩写如下所示。

英文缩写	英文全称
ARP	Address Resolution Protocol
CPU	Central Processing Unit
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
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

英文缩写	英文全称
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

附录 C.6　KB（千字节）等单位的标示方法

1KB（千字节）、1MB（兆字节）、1GB（千兆字节）、1TB（万亿字节）分别为 1,024 字节、$1{,}024^2$ 字节、$1{,}024^3$ 字节、$1{,}024^4$ 字节。

附录 D　术语解释

C

层 2 拓扑

从 OSI 七层模型的数据链路层观察到的网络连接关系。表示末端交换机与终端之间的接线等。

层 3 拓扑

从 OSI 七层模型的网络层观察到的网络连接关系。表示逻辑网络构成。

F

发现种子

发现监视对象节点时的起点节点。自动发现时，使用发现种子的 ARP 缓存以发现相邻的设备。将拥有较多相邻设备信息的路由器等指定为发现种子。

G

根源分析（RCA）

调查并过滤因网络故障而发生的各种事件的相关关系后，根据层 2 拓扑分析故障，确定故障的原因。

J

节点

通过 NNMi 监视的设备。

节点组

按 IP 地址或设备类别等条件将已发现的网络设备分组及分层后的组。

节点组图

按业务与地区等各节点组对网络设备进行分类和显示的图。

M

MIB（Management Information Base）

使用 SNMP 的服务器产品或网络设备为了将其状态通知外部而公开的信息。

MIB 对象

MIB 中的各个管理信息。MIB 对象采用分层的树结构，各层带有独特的名称以及用数值表示名称的标识符。另外，将 MIB 对象的特定值称为实例。

S

设备

路由器、交换机、计算机及打印机等 IT 设备。

生命周期状况

用于确认事件进展状况的属性。状况中包括“已注册”、“正在进行”、“已完成”及“已关闭”，根据事件的措施状况进行更新。

实例

资源收集源的实体。例如，资源“CPU 使用率”的实例为各 CPU 的 CPU 使用率。

事件

网络中发生的各种情况（事件）中需要通知管理员的重要性较高的信息。NNMi 对网络中发生的事件的根源进行分析并作为事件进行通知。

SNMP 陷阱

SNMP 代理器发生故障时由 SNMP 代理器向 SNMP 管理器通知信息的处理。

T

拓扑图

对发现的网络设备的状况及连接关系进行可视化的网络构成图。

Z

资源

SSO 通过 SNMP 代理器收集的信息的集合体。例如，包括“CPU 使用率”及“运行队列的长度”等。

索引

K

L

M

N

O

P

Q

R

S

T

V

W

X

Y

Z

Hitachi, Ltd.

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan