NEC

MasterScope

Network Flow Analyzer 2.0

Getting Started Guide

Copyrights

Trademarks

Preface

Thank you for choosing MasterScope Network Flow Analyzer 2.0 (hereafter referred to as "NFA"). NFA provides the functions to analyze flow information of the communication on the network and visualize the communication status.

This manual describes how to install NFA and configure the environment, and explains the basic operations. Before configuring the environment of NFA, please read this manual carefully.

Configuration of This Manual

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

: NFA administrator. 

: all NFA users

Configuration of This Manual

Title	Content	Target reader
"Chapter 1. Product Overview (page 1)"	Provides an overview of NFA.	User
"Chapter 2. Installation (page 13)"	Describes how to set up NFA.	Admin
"Chapter 3. Post-Installation Environment Settings (page 32)"	Describes how to configure the environment before using and operating NFA	Admin
"Chapter 4. Basic Operations (page 41)"	Describes the basic operations of the web console of NFA.	User
"Chapter 6. Uninstallation (page 53)"	Describes how to uninstall NFA.	Admin
"Appendix A. Command Reference (page 55)"	Describes the commands that are used to set up NFA.	Admin
"Appendix B. Troubleshooting (page 59)"	Describes how to troubleshoot problems that occur while setting up NFA.	Admin

Notations and Text Conventions

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

Notations of Items Requiring Attention and Supplementary Information

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

Notation	Description
Tip	Indicates useful information.

In this manual, the following text conventions are used.

Text Conventions

Notation	Description	Example
	Indicates graphical user interfaces such as dialog boxes, tabs, menus, items, and buttons.	**Dashboard** tab, **OK** button
<*userinput*>	Indicates items that change depending on the user environment or items that the user must specify.	<*%installation directory%*>, <*filepath*>
`configuration file`	Indicates the contents of the configuration file.	Set the following value: `port = 27120`
`command line`	Indicates command line operations.	Run the following command: `$ rpm -q nec-nfa-controller`

In this manual, the following abbreviations are used.

Abbreviations

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

The default installation directory of this product is as follows:

Default installation directory:

`/opt/nec/nfa`

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

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

Contents

Chapter 1. Product Overview

This chapter provides an overview of NFA.

Contents

1.1 Product features

NFA provides the functions required to intuitively analyze the flow information of communications on a network using simple operations, and visualize the communication status from a variety of perspectives.

NFA performs fine-grained analysis of the source and destination of communications, the communication type, and the communication traffic, and displays the communication status, thereby enabling the network to operate stably.

Fine-grained analysis of communication status based on flow information (NetFlow and sFlow)

SNMP is widely used to check the communication status of the network. SNMP can check the communication traffic passing through interfaces such as switches and routers. However, SNMP cannot be easily used to check the details of the communication traffic.

NFA uses flow information (NetFlow and sFlow) instead of SNMP to analyze the communication status. Analysis using flow information allows fine-grained checking of communication traffic details that cannot be checked by using SNMP, such as the source and destination of the communication, the communication type, and the communication traffic. By understanding the communication status in detail, you can efficiently investigate causes of network failures and effectively manage network capacity.

Simple drill-down analysis

NFA allows you to narrow down the information on charts and lists with a single click.

For example, by performing the following intuitive and simple operation on the information displayed on the page, you can check the detailed communication status immediately.

Operation example:

1. Select an interface (for example, Ethernet1/1) from the display showing the communication traffic passing through each interface.

   (The display is narrowed down to the communication traffic on the selected Ethernet1/1.)
2. Select an application (for example, http) from the display showing the communication traffic for each application.
3. The results of analyzing the http communication traffic on Ethernet1/1 are displayed.

Free customization of display contents

NFA allows you to customize the display contents freely to improve visibility.

For example, by customizing the display and analysis contents according to your operating environment as follows, you can gain an accurate understanding of the network status.

Customization examples:

- The contents of charts and lists displayed in the Dashboard (main page) can be defined for each user who logs in to NFA.
- The analysis results can be visualized clearly by uniquely defining job application communications or specifying the target department by using an IP address range.

1.2 Functional overview

The following describes the functions that are provided by NFA.

Dashboard

- This displays the current communication status and event occurrence status of the network managed by the user who is currently logged in to NFA.
- All displayed analysis results can be exported to a CSV file.
- A **widget**, which is an element used to display a chart or list, can be freely located on the dashboard page by a drag-and-drop operation, allowing each user to define the dashboard according to their needs.

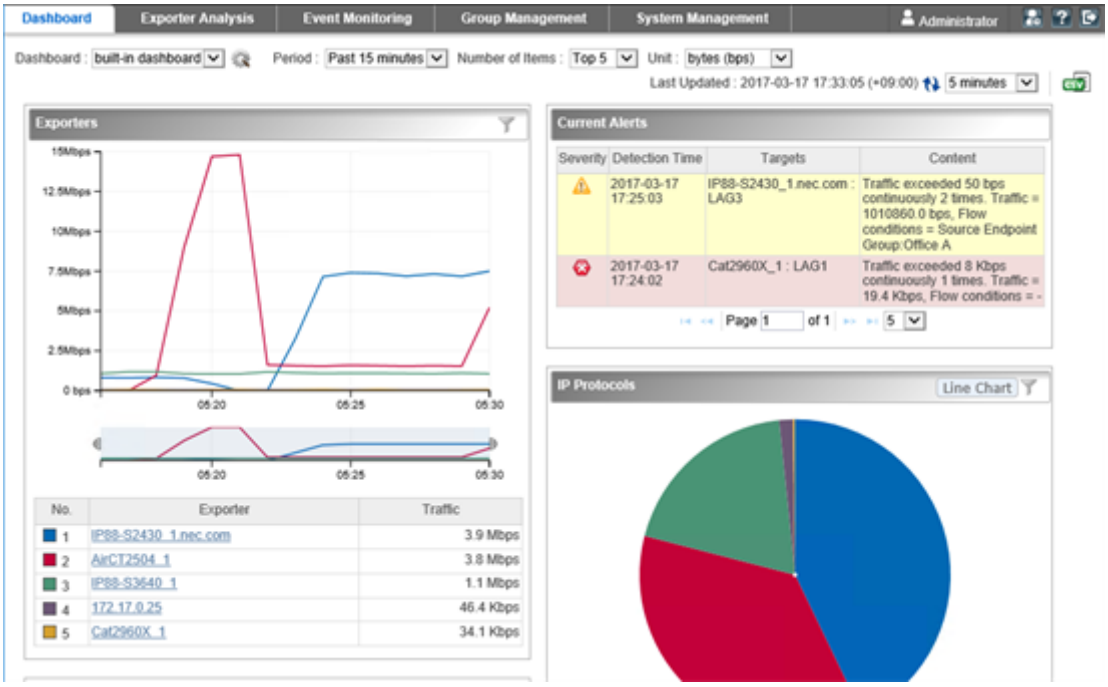


Figure 1-1 Dashboard

Exporter analysis

- Fine-grained analysis of the communication status can be performed by narrowing down the exporters that send flow information and their interfaces.
- Not only the current communication status but also previous communication status can be analyzed, allowing you to check mid-and-long-term changes in the communication status.
- All displayed analysis results can be exported to a CSV file as well as on the Dashboard page.

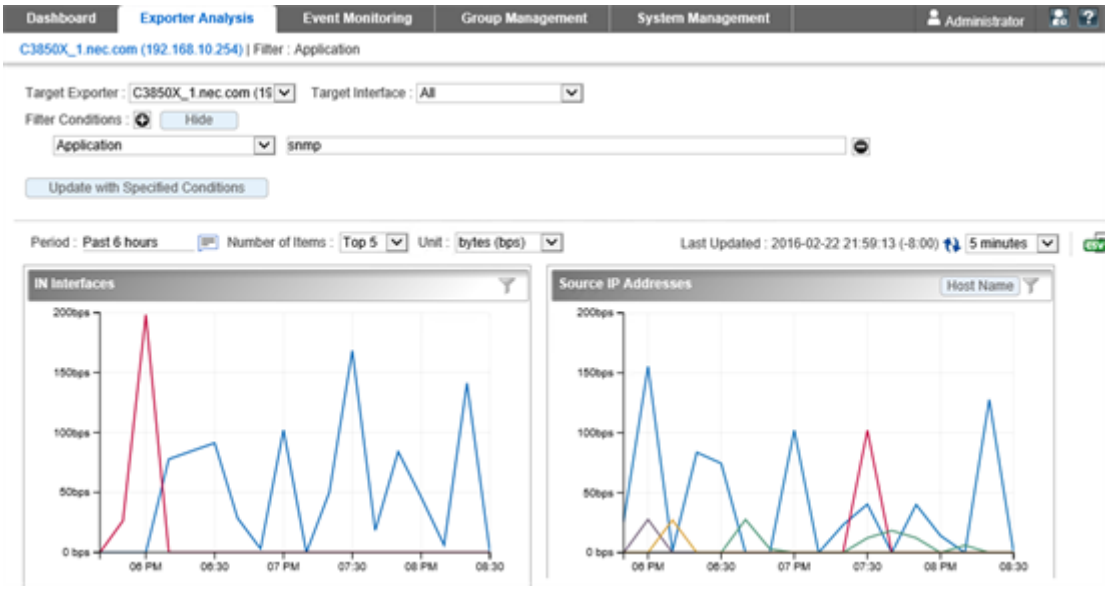


Figure 1-2 Exporter analysis

Event monitoring

- The communication traffic narrowed by conditions such as source and destination IP address or application can be monitored by specifying a threshold.
- The history of threshold violation and recovery event occurrence is displayed in a list. If a current alert widget is set up on the Dashboard page, the current event occurrence status is displayed on the Dashboard page.
- Threshold violation and recovery events can be sent to another management system by using the SNMP trap format.

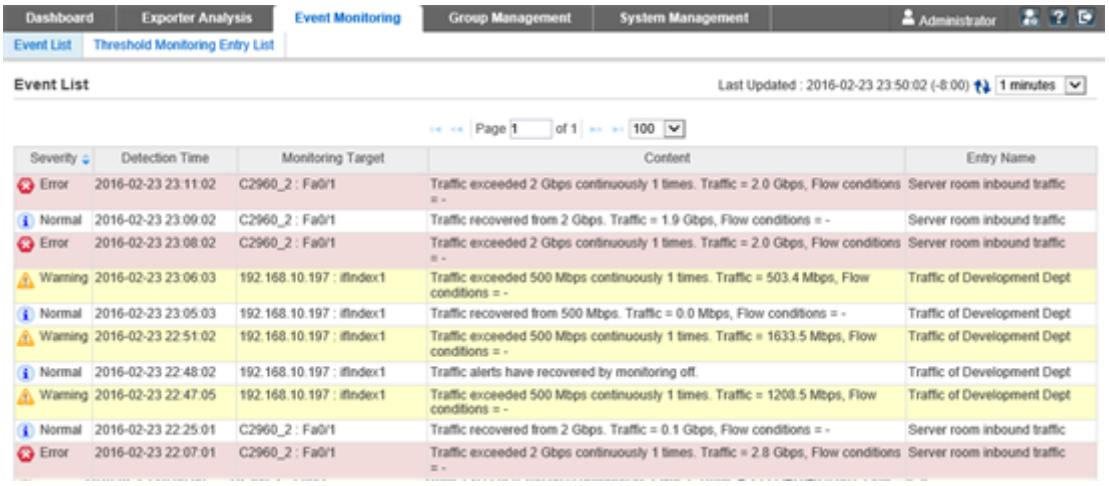


Figure 1-3 Event list

Group management

- The communication traffic can be analyzed in units of groups by grouping multiple IP addresses or network addresses that are endpoints (source or destination) of communication.
- By grouping multiple interfaces that configure a Link Aggregation (LAG), the communication traffic passing through those interfaces can be analyzed as one LAG interface.

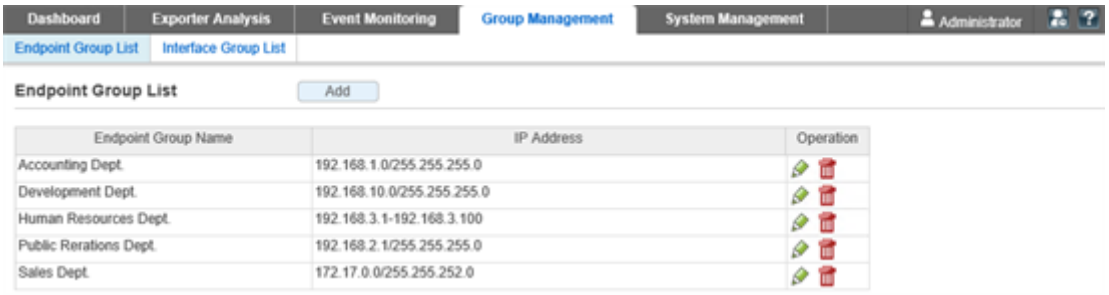


Figure 1-4 Endpoint group list

System Management

- Applications that are used to analyze the communication status can be defined. An application can be defined in detail by combining an IP protocol, port number, and a source or destination IP address.
- The exporters that send flow information, their interfaces, and license assignment status can be managed in a list.
- NFA user information, such as a password or default dashboard definition, can be managed.

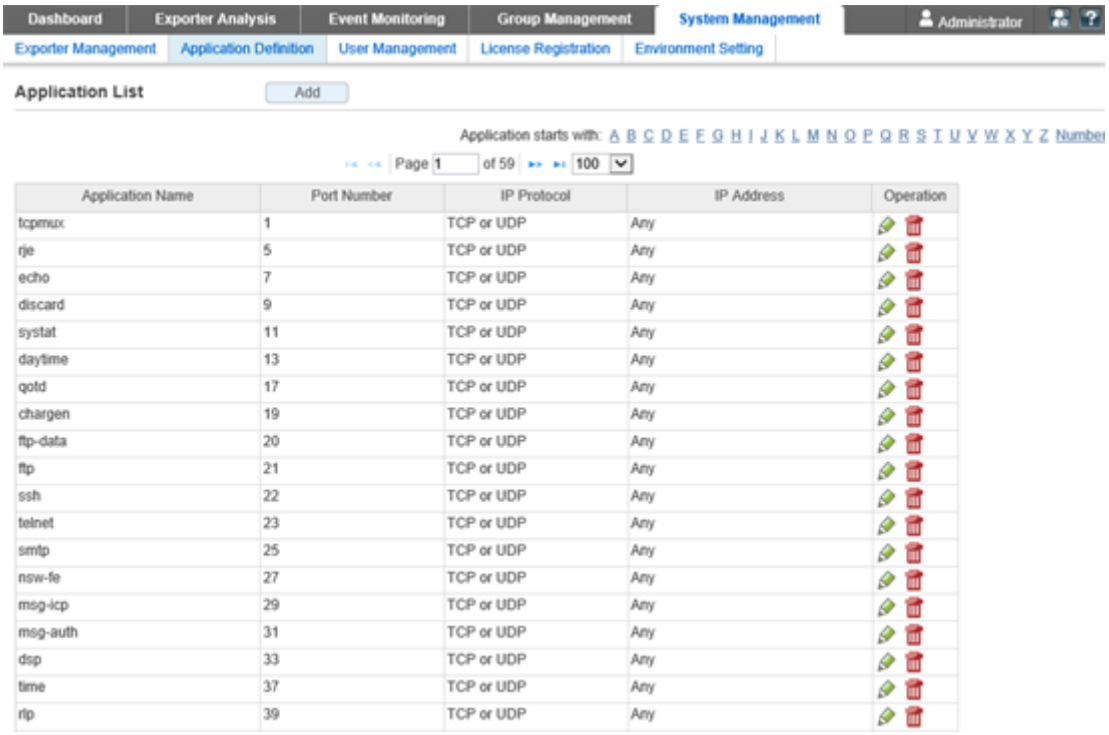


Figure 1-5 Application definitions

1.3 Operating Environment

This chapter describes the operating environment of NFA.

1.3.1 System configuration

The following describes the system configuration of NFA.

System configuration of NFA

The NFA operating environment consists of a server to which NFA is installed (NFA server), the terminals of the NFA users, exporters, and endpoints as shown in "Figure 1-6 System configuration diagram (page 6)".

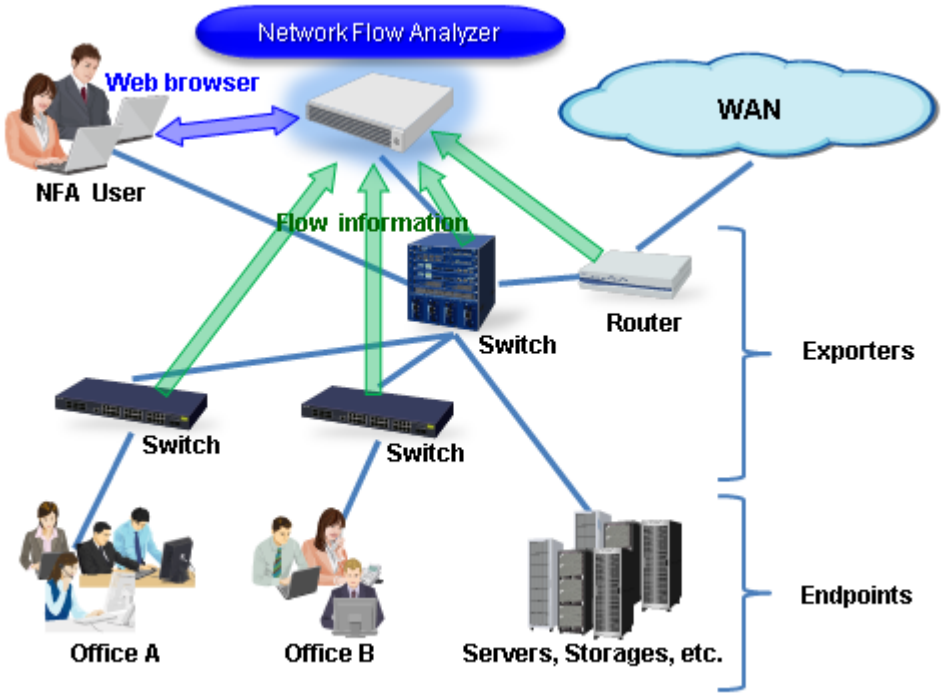


Figure 1-6 System configuration diagram

NFA has two roles: one is a flow collector that receives and accumulates flow information, and the other is a flow analyzer that analyzes the communication status according to the accumulated flow information. A web server function that provides operation pages for NFA users is also included. In NFA, the flow collector function is called *"collector"*, and the flow analyzer and web server functions are collectively called *"controller"*.

NFA users can connect to the NFA web console via a web browser from their terminals.

Tip

- In NFA, terminals and servers that connect to a network and perform communication are collectively called an endpoint.
- Switches and routers that convert communication contents between endpoints to flow information and send the information to NFA are collectively called an exporter.

System configuration when using IMS component

By using the IMS component, it is possible to integrate the operation of multiple NFAs, or NFA and Network Manager. A system configuration example at integrated operation is shown in "Figure 1-7 System configuration example at integrated operation (page 7)".

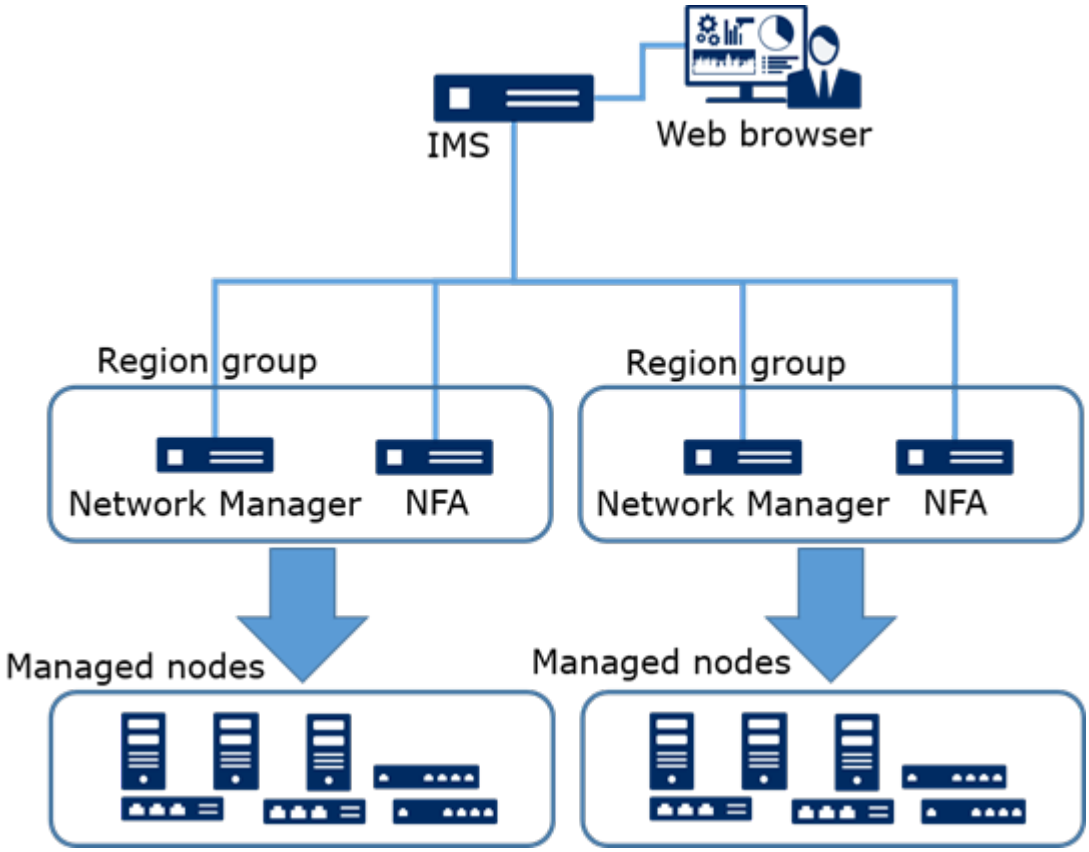


Figure 1-7 System configuration example at integrated operation

NFA and Network Manager which manage the same node (exporter) are grouped by Region group as shown in "Figure 1-7 System configuration example at integrated operation (page 7)". In the Web Console of the IMS component, information of the same node (exporter) managed by each product in the same Region group is integrated and displayed.

Tip

It is possible to install NFA and IMS component on the same server. However, it may cause problems such as slow response to the operation. Therefore, thoroughly assess the system configuration before starting operations. If possible, it is recommended to install them separately on multiple servers.

1.3.2 System requirements

The following describes the system requirements for properly operating NFA and the supported environment.

Table 1-1 Server system requirements

Item	Description
CPU	Intel Quad-Core Xeon or higher, or equivalent compatible processor recommended
System memory	4 GB or more (8 GB or more recommended)
Disk capacity	Installation directory: 5 GB or more
	Data directory: 100 GB or more [1)] For how to estimate the disk size required for a data directory, see "1.3.3.2 Estimating the required disk capacity (page 9)".
OS	• Red Hat Enterprise Linux 6 (x86_64) [2)]

Item	Description
	• Red Hat Enterprise Linux 7 (x86_64)
Flow protocol	• NetFlow (v5, v9) • IPFIX • sFlow (v4, v5) Sampling mode is supported for NetFlow and IPFIX.

Note

1. This product frequently accesses the hard disk on specifications. It is recommended to use hard disk with high access performance such as SAS 15,000 rpm according to usage environment.
2. Operation with version 6.6 or higher OS is supported.

Table 1-2 Web browser requirements

Item	Description
Supported browser	The following browsers running on Windows • Internet Explorer 11 • Mozilla Firefox 60 or later • Google Chrome 71 or later
CPU	Intel Core i3 or higher, or equivalent compatible processor recommended
System memory	1 GB or more

Tip

- It is recommended to apply the latest bug fix updates to the browser before using it. If the bug fix updates have not been applied, some functions might not work properly.
- Depending on a browser, a Unicode surrogate pair character is treated as two characters. In this case, an actual number of characters that can be input to each input field will be less.

1.3.3 Flow data management

NFA manages received data in a database. The following describes how flow data is managed.

1.3.3.1 Flow data retention periods and data aggregation

To store large amounts of data for a long period with a limited disk capacity, NFA manages received data by aggregating it every unit time shown in "Table 1-3 Data unit times and retention periods (page 8)" and changing the data granularity. In addition, NFA defines the retention periods for each data unit time and discards the data beyond the defined retention periods. You can change the retention period.

Table 1-3 Data unit times and retention periods

Data unit time	Default retention period	Available range for retention period
1 minute	24 hours	2 to 168 hours
10 minutes	72 hours	12 to 336 hours
60 minutes	14 days	4 to 60 days
6 hours	60 days	14 to 365 days
24 hours	365 days	60 to 1095 days

Data unit time	Default retention period	Available range for retention period
7 days	1095 days	365 to 2190 days

The flow data aggregation processing aggregates all flow data whose seven flow keys described below are the same for each unit time.

1. Source IP address
2. Destination IP address
3. Source port number
4. Destination port number
5. IP protocol
6. ToS byte (DSCP)
7. Input Interface

In addition, to minimize the disk capacity required to accumulate flow data, NFA also performs the following operations in the aggregation process.

- Manages data of the top 1,000 flows whose communication traffic is large per unit time as a target of detailed analysis.
- Aggregates and manages data of flows below the top 1,000 as *"other"* flows.

1.3.3.2 Estimating the required disk capacity

The following describes the procedure to estimate the disk capacity required to accumulate and manage received flows.

The disk capacity required to accumulate and manage flow data depends on the number of exporters managed by NFA and the flow occurrence frequency. As described in "1.3.3.1 Flow data retention periods and data aggregation (page 8)", NFA defines the retention periods of flow data per unit time and the maximum number of flows to be stored. Therefore, the estimated disk capacity required to accumulate the flow data can be obtained by a formula that takes into account these definitions.

⚠ Caution

The larger the number of exporters, the larger the flow data size. There is therefore a risk that the disk capacity will be exhausted. If the disk capacity is exhausted, new flow data cannot be received, and the system as a whole cannot operate properly. Therefore, we recommend assigning a slightly smaller value for the maximum number of flows.

The specific calculation method is described below.

1. Check the number of exporters managed by NFA.

   If it is possible that the number of exporters will increase in the future, clarify the final number of managed exporters.

2. Check the retention periods of flow data, and calculate the coefficient by using the following formula:

   Coefficient of retention periods: $P = P1 \times 60 + P2 \times 6 + P3 \times 24 + P4 \times 4 + P5 + P6 \div 7$

   - P1: Retention period of 1 minute unit data (unit: hour)
   - P2: Retention period of 10 minutes unit data (unit: hour)
   - P3: Retention period of 60 minutes unit data (unit: day)

- P4: Retention period of 6 hours unit data (unit: day)
- P5: Retention period of 24 hours unit data (unit: day)
- P6: Retention period of 7 days unit data (unit: day)

Round the calculation result up to zero decimal point.

If the retention periods of flow data remain at those default values, the coefficient P is equal to 2,970.

Tip

For details of the flow data retention periods, see "1.3.3.1 Flow data retention periods and data aggregation (page 8)".

3. Check the flow occurrence frequency (average number of flows per minute) in the operating environment.

   Assume that the average number of communication sessions that have occurred per minute in the operating environment is the approximate flow occurrence frequency.

4. Calculate the estimated disk capacity by using the following formula:

   Estimated disk capacity [MB] = (N + 5) × P × L × 0.000415 + A × 0.15 + 10,000 [MB]

   - N: Number of exporters managed by NFA

     Assign the value that was checked in step 1.

   - P: Coefficient of the flow retention periods in NFA

     Assign the value that was checked in step 2.

   - L: Maximum number of flows to be stored per unit time

     By default, the maximum number of flows to be sored is 1,000.

     Tip

     If the maximum number of flows has been changed, specify an appropriate value according to that number.For how to change the maximum number of flows, see "1.3.3.3 Changing the maximum number of flows that can be stored (page 11)".

   - A: Average number of flows per minute that NFA received

     Assign the value that was checked in step 3.

Calculation example:

When the number of exporters is 50, the retention periods and the maximum number of flows to be stored per unit time remain at those default values, and the average number of flows per minute is 600,000, the calculation result is as follows:

- N = 50
- P = 2,970 (24 × 60 + 72 × 6 + 14 × 24 + 60 × 4 + 365 + 1095 ÷ 7)
- L = 1,000
- A = 600,000
- Estimated = (50 + 5) × 2,970 × 1,000 × 0.000415 + 600,000 × 0.15 + 10,000 ≒ 163.9GB

1.3.3.3 Changing the maximum number of flows that can be stored

The following describes the procedure to change the maximum number of flows that can be stored.

NFA stores the top 1,000 flows for each exporter per unit time by default.

This number can be changed after installation.

⚠ Caution

Note that the larger the maximum number of flows to be stored, the larger the load on the NFA server. Therefore, the load on the server may become increasingly heavy, depending on the number of managed exporters, the number of received flows, and the machine specifications, with the result that NFA may not work properly.

After executing operations for one or more days in the actual operating environment, check the following to confirm that this product can work properly.

- No delay occurred in **Last Received** of all exporters on the Exporter Management page.
- Flow data can be viewed on the Dashboard and Exporter Analysis pages.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Specify the maximum number of flow data items that can be saved in the **Maximum Number of Flows** box.

   Specify a value from 1,000 to 10,000 for the maximum number of flows. Use the following as a guide when considering the number of exporters as an index.

   1 to 10

   Top 10,000 flows

   11 to 20

   Top 6,000 flows

   21 to 30

   Top 3,000 flows

   31 or more

   It is not recommended to increase the maximum number of flows.

Tip

- You can change the maximum number by editing the following configuration file. If no configuration file exists, create a configuration file. If you change the maximum number of data flow items from **System Management**>**Environment Settings**, this file will be overwritten.
- After editing the configuration file, restart the NFA service to enable the change.
- *<%data directory%>*/controller/conf/flowdb.properties
- Specify the same value for the following six parameters:

```
flowdb.table.record.limit.1 = 1000
flowdb.table.record.limit.2 = 1000
flowdb.table.record.limit.3 = 1000
```

```
flowdb.table.record.limit.4 = 1000
flowdb.table.record.limit.5 = 1000
flowdb.table.record.limit.6 = 1000
```

1.3.3.4 Changing the flow retention periods

The following describes the procedure to change the maximum number of flows that can be stored.

NFA defines the retention periods to store flow data in a database according to "1.3.3.1 Flow data retention periods and data aggregation (page 8)".

The procedure to change the retention periods is described below.

Tip

It takes from several to 40 minutes after the maximum number of flows or the maximum retention period is decreased until the data will be actually deleted.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Specify the retention periods of flow data items to be saved in each input field of **Maintenance Settings of Flow Data**.

   Specify a longer retention period in order from the top of the above table. For example, if the retention period of **Flow Data of 1 Minute Unit** is set to 36 hours, the retention period of **Flow Data of 10 Minutes Unit** must be longer than 36 hours.

1.4 Product license and interface license

The following describes the concept of the product license and interface license of NFA.

Product license

A product license is a license that is necessary to validate the NFA product.

After installation, NFA initially behaves as a trial version with limited available functions. For the trial version, only two interfaces for an exporter can be registered as a managed object. The function restrictions can be canceled by registering the product license, allowing the user to use the product functions according to the registered product license.

Interface license

An interface license is a license that is assigned to the interfaces of the managed exporter in order to judge whether to receive flow information. The maximum number of interfaces to which a license can be assigned depends on the registered product license.

Chapter 2. Installation

This chapter describes how to install NFA.

Contents

2.1 Product installation flow

The following describes the flow to install NFA.

The setup flow is described in "Table 2-1 Installation flow (page 14)".

Tip

When integrating the operation of multiple NFAs, or NFA and Network Manager, you need to install the IMS component. For details, refer to *"MasterScopeNetwork Management Web Console Getting Started Guide"*.

Table 2-1 Installation flow

No.	Outline	Description
1	Determine the installation parameters.	"2.2.1 Designing the installation parameters of NFA (page 15)" Check the parameters required for installation work and determine the values to specify.
2	Check the installation environment.	"2.2.2 Checking the installation environment (page 17)" Check that there is sufficient free disk space and that the OS kernel parameter values are appropriate.
3	Run the installer.	"2.3 Installing the software (page 18)" Run the installer on the installation media to install NFA.
4	Prepare the appropriate SSL server certificate.	"2.4 Preparing an appropriate SSL server certificate (page 19)" HTTPS is used to access NFA. Therefore, prepare an SSL server certificate for HTTPS communication. There are two types of certificates. One is a self-signing certificate that is signed by the user. The other is a certificate that is issued by a public certificate authority. Prepare either of these.
5	Check the port number to use.	"2.5 Checking the port numbers used in this product (page 23)" Confirm that the port number to be used by NFA does not conflict with the port number used by another software on the NFA server.
6	Configure a firewall.	"2.6 Changing a firewall configuration (page 26)" Change the firewall settings to receive NetFlow and sFlow packets and perform HTTPS communication with an outside device.
7	Configure the additional settings for the web server.	"2.7 Additional settings for the web server (page 28)" Configure the additional settings for the NFA web server, as necessary.
8	Configure for using IMS component	"2.8 Configuring for using IMS component (page 28)" Configure for the integrated operation using the IMS component. When not using the IMS component, this configuration is not necessary.
9	Start the service.	"2.9 Starting the service (page 30)" Start the NFA service and confirm that access from a web browser is enabled.

2.2 Preparations

The following describes the preparations required to install NFA.

2.2.1 Designing the installation parameters of NFA

Determine the parameters that are required for installation in advance.

Kernel parameter requirements

The following parameter requirements must be met to run NFA.

Table 2-2 Kernel parameter requirements

Parameter name	Description
kernel.shmmax	Specifies the maximum shared memory size that processes can use. The unit is bytes. For NFA, 256 MB or more must be specified for this parameter. We strongly recommend setting 2 GB or more to maximize the performance of this software.

Parameters required when running the installer

The following parameters are required when running the installer.

Table 2-3 Parameters required to run the installer

Parameter name	Description	Default
Installation directory	Specifies the directory in which the executable files of this software are installed. Up to 128 characters can be specified. The available characters are single-byte alphanumeric characters, hyphens (-), underscores (_), and dots (.).	/opt/nec/nfa
Data directory	Specifies the directory in which flow information and configuration data are stored. Up to 128 characters can be specified. The available characters are single-byte alphanumeric characters, hyphens (-), underscores (_), and dots (.). We recommend specifying a separate directory from the installation directory. All received flow data is accumulated in the data directory. Therefore, a large amount of free space might be necessary depending on the number of managed exporters. For the procedure to estimate the disk size necessary for a data directory, see "1.3.3.2 Estimating the required disk capacity (page 9)".	/opt/nec/nfa

Parameters required to create an SSL certificate

Determine the parameters related to SSL server certificates and parameters related to certificate identification names (Distinguished Name) to create the SSL server certificate that will be used in HTTPS communication with NFA.

For a certificate issued by a public certificate authority, certain conditions might be set to some parameters related to the key encryption algorithm and identification name depending on the certificate authority. Therefore, check the conditions required by the certificate authority.

Table 2-4 Parameters that must be specified to create an SSL server certificate

Parameter name	Description	Default
Keystore password	Specifies the password for the keystore that stores the SSL server certificate.	None
Private key password	Specifies the password for the private key of the SSL server certificate.	None
Entry alias	Specifies the display name for the entry that stores the SSL server certificate. We recommend using the default value unless there is a special reason not to.	tomcat
Key encryption algorithm	Specifies the encryption algorithm for the key of the SSL server certificate. For a self-signing certificate, there is no problem usually if the default value is used. For details about the specifiable values, see "A.1 nfa_ssl_keytool (page 55)".	RSA
Key size	Specifies the size of the key of the SSL server certificate. For a self-signing certificate, there is no problem usually if the default value is used. For details about the specifiable values, see "A.1 nfa_ssl_keytool (page 55)".	2048
Signature algorithm	Specifies the algorithm to sign the self-signed certificate. There is no problem if the default value is used in normal operation. For details about the specifiable values, see "A.1 nfa_ssl_keytool (page 55)". You may be able to specify the algorithm to be used when asking a public certificate authority to issue a certificate. For details, contact the public certificate authority.	SHA256withRSA
Expiration date of a self-signing certificate	Specifies the expiration date of the self-singing certificate to be used. Specify the number of days during which the self-signing certificate will be valid from the creation date. For a certificate issued by a public certificate authority, the expiration date is usually determined by the public certificate authority. Therefore, it is not necessary to specify this parameter.	3650 (10 years)

Table 2-5 Parameters that must be specified to create an SSL server certificate identification name (Distinguished Name)

Parameter name	Description	Example
Server FQDN	Specifies the fully-qualified domain name (FQDN) of the NFA server. This is equivalent to Common Name on the SSL server certificate. Because all web browsers that access NFA use this domain name in the URL specification for access, a name that can be resolved by all web browsers must be specified.	nfa.nec.com
Department name	Specifies the name of the department that possesses and uses this software. This is equivalent to Organizational Unit on the SSL server certificate.	IT Operation Division
Organization name	Specifies the name of the organization that possesses and uses this software. This is equivalent to Organizational Name on the SSL server certificate. Usually, specify the official English name.	NEC Corporation

Parameter name	Description	Example
City name	Specifies the location of the organization possessing and using this software. This is equivalent to Locality on the SSL server certificate. For example, if the relevant organization is located in Minato-ku, Tokyo, specify Minato-ku.	Minato-ku
Province name	Specifies the province of the organization possessing and using this software. This is equivalent to State on the SSL server certificate. For example, if the relevant organization is located in Tokyo, specify Tokyo.	Tokyo
Country code	Specifies the country code of the organization possessing and using this software. This is equivalent to Country on the SSL server certificate. In the case of Japan, it is usual to specify JP.	JP

Parameters required when using the IMS component

By using the IMS component, it is possible to integrate the operation of multiple NFAs, or NFA and Network Manager.

The following parameters are required in the configuration when using the IMS component.

Table 2-6 Parameters required when using the IMS component

Parameter name	Description	Default
ims.application-instance-id (manager id)	Specify the ID so that the IMS component can identify the NFA to be connected. Available characters are single-byte alphanumeric characters, underscore (_), and hyphen (-). This parameter must match the value of the configuration file (ims-conf.ini) on the IMS component.	Undefined
ims.msgqueue.host (ims ip address)	Specify the IPv4 address of the server where the IMS component is installed. If the IMS component is installed on the cluster system, specify the floating IP address of the cluster system.	127.0.0.1
ims.msgqueue.port (port number)	Specify the communication port number to be used for communication with the Message Queue of the IMS component.	28110
ims.webserver.base-url (ims web url)	Specify the URL to access the Web Console of the IMS component. For this parameter, specify URL accessible from the NFA.	http://localhost
ims.sso.enabled	Specify whether to enable single sign-on behavior with the Web Console of the IMS component as follows. • true : Enable single sign-on behavior. • false : Disable single sign-on behavior.	false

2.2.2 Checking the installation environment

The configuration of the server to which to install NFA must meet the installation requirements.

Check the following two points.

- Does the kernel parameter value meet the requirements?

- Does the disk have enough free space?

1. Check that the value of the kernel parameter kernel.shmmax meets the installation requirements.

```
# cat /proc/sys/kernel/shmmax
68719476736
```

The unit of the displayed value is bytes. In the above example, the kernel.shmmax value is 64 GB. Therefore, it is not necessary to change the value.

If a value such as 32 MB (33554432) is displayed, change the value to 256 MB or more (2 GB is recommended). For how to change the kernel parameter setting, see the manual of the OS in use.

2. Check that the installation disk has enough free space.

   a. Estimate the disk capacity that NFA needs.

   For how to estimate the disk capacity, see "1.3.3.2 Estimating the required disk capacity (page 9)".

   b. Check the current free space of the installation disk.

   Use the df command to check the free space.

```
# df -h
Filesystem            Size  Used Avail Use% Mount Position
/dev/mapper/vg_nfa-lv_root
                       22T  1.8T   19T   9% /
tmpfs                  16G     0   16G   0% /dev/shm
/dev/sda1             485M   32M  429M   7% /boot
```

   Check the free space (Avail) by referring to the displayed mount position.

   In this example, if the installation disk is /opt/nec/nfa, the free space of this disk is 19 TB.

If the free space of the installation disk is insufficient, change the installation disk or add a disk.

2.3 Installing the software

Run the installer on the installation media to install NFA.

1. Insert the installation media in the CD-ROM drive and mount it.

In the following description, the CD-ROM mount point is `/media`. If you mounted the installation media on another location, replace this mount point with the appropriate mount point.

2. Run the following command to start the installer.

```
# /media/NFA/Linux/nfa-install
```

3. A prompt to enter the install directory path is displayed. Enter the path.

```
Input installation path [default:  /opt/nec/nfa]
 >
```

The default value is displayed on the right of the first line. To use the default value, press the Enter key without entering anything.

4. A prompt to enter the data directory path is displayed. Enter the path.

```
Input data installation path [default:  /opt/nec/nfa]
 >
```

The default value is displayed on the right of the first line. To use the default value, press the Enter key without entering anything.

5. Check the entered paths and start installation.

The entered installation directory path and data directory path are displayed. If the displayed paths are correct, enter `y` and press the Enter key.

```
----- Confirmation --------------------
Installation path      : /opt/nec/nfa
Data Installation path : /opt/nec/nfa
---------------------------------------

Is it OK to install? (y/n): y
```

Entering `y` starts installation.

Entering `n` displays the prompt to enter the paths again. Correct the installation destinations.

When the following message is displayed, installation is complete.

```
Installing controller ... done
Installing collector  ... done
```

If an error has occurred during installation, an error message is displayed. If an error message is displayed, see "B.1 Installation errors and actions (page 59)" and take appropriate action.

2.4 Preparing an appropriate SSL server certificate

HTTPS is used to access NFA. It is therefore necessary to prepare an SSL server certificate for HTTPS communication.

The following two types of SSL server certificates are available:

- Self-signing certificate
- Certificate issued by a public certificate authority

In addition to the above certificates, NFA can use a certificate that was created for other purposes by using Java keytool.

The procedures to prepare these three certificates are described below.

- "2.4.1 Preparing a self-signing certificate (page 20)"
- "2.4.2 Preparing a certificate issued by a public certificate authority (page 21)"
- "2.4.3 Using a certificate created for other purposes (page 23)"

⚠ Caution

The supported certificate format is X.509, which is equivalent to the format that can be handled by Java keytool. X.509 is supported by many certificate authorities. However, make sure that the certificate authority you will use supports X.509 in advance.

2.4.1 Preparing a self-signing certificate

The following describes the procedure to create a self-signing certificate as the SSL server certificate that NFA will use.

To perform operations on the SSL server certificate, use `nfa_ssl_keytool` command provided by this software. For details, see "A.1 nfa_ssl_keytool (page 55)".

Distribute and install the created certificate to all web browsers that access NFA.

1. Run the following command to generate a pair of keys (public key and private key) and create a certificate for this key pair.

```
# <%installation directory%>/controller/bin/nfa_ssl_keytool genkeypair
```

Enter the password of the keystore to store the keys and certificate, certificate identification name, and password of the key.

- The default value is displayed in [ ]. The default value is used by pressing the Enter key without entering anything.
- For the key password entry (key password), pressing the Enter key without entering anything sets the same password as the keystore.

```
What is your server domain name? (FQDN)
  [nfa.nec.com]:
What is the name of your organizational unit?
  [Unknown]:  IT Operation Division
What is the name of your organization?
  [Unknown]:  NEC Corporation
What is the name of your City or Locality?
  [Unknown]:  Minato-ku
What is the name of your State or Province?
  [Unknown]:  Tokyo
What is the two-letter country code for this unit?
  [Unknown]:  JP
Is CN=nfa.nec.com, OU=IT Operation Division, O=NEC Corporation,
 L=Minato-ku, ST=Tokyo, C=JP correct?
  [No]:  yes
Enter key password for <tomcat>
        (RETURN if same as keystore password):
```

Tip

- For `nfa_ssl_keytool` command, arguments can be specified. If you want to change the algorithm, size, or expiration date of the key, see "A.1 nfa_ssl_keytool (page 55)" and specify appropriate arguments.

  Example of specifying ECDSA for the key algorithm and 256 bits for the key size

```
# cd /opt/nec/nfa/controller/bin
# ./nfa_ssl_keytool genkeypair -keyalg EC -keysize 256
```

- To change the key contents and then recreate a key, run `nfa_ssl_keytool delete` command and then `nfa_ssl_keytool genkeypair` command again, or run `nfa_ssl_keytool genkeypair` command with a different `-alias` from the previous one.

  For details about the commands, see "A.1 nfa_ssl_keytool (page 55)".

The created certificate has also been self-signed.

2. Run the following command to output the certificate to be imported to a web browser to a file.

```
# <%installation directory%>/controller/bin/nfa_ssl_keytool exportcert
 <filename>
```

Any name can be specified for <*filename*>. However, we strongly recommend specifying `.cer` as the file extension to enable the created file to be easily imported to a web browser.

Upon successful execution of the command, a binary encoded certificate is output to the specified file.

Distribute and import the certificate file exported by using `nfa_ssl_keytool exportcert` command to all web browsers that access NFA. This prevents security problems such as a phishing attack whereby an unauthorized server acts as a NFA web server.

For details about the procedure to import the certificate to a web browser, see "3.1.3 Importing an SSL server certificate to the web browser (page 34)".

2.4.2 Preparing a certificate issued by a public certificate authority

The following describes the procedure to ask a public certificate authority to issue a certificate as the SSL server certificate that NFA will use.

To perform operations on the SSL server certificate, use `nfa_ssl_keytool` command provided by this software. For details, see "A.1 nfa_ssl_keytool (page 55)".

The supported certificate format is X.509, which is equivalent to the format that can be handled by Java keytool. X.509 is supported by many certificate authorities. However, make sure that the certificate authority you will use supports X.509 in advance.

1. Run the following command to generate a pair of keys (public key and private key) and create a certificate for this key pair.

```
# <%installation directory%>/controller/bin/nfa_ssl_keytool genkeypair
```

Enter the password of the keystore to store the keys and certificate, certificate identification name, and password of the key.

- The default value is displayed in [ ]. The default value is used by pressing the Enter key without entering anything.
- For the key password entry (key password), pressing the Enter key without entering anything sets the same password as the keystore.

```
What is your server domain name? (FQDN)
  [nfa.nec.com]:
What is the name of your organizational unit?
  [Unknown]:  IT Operation Division
What is the name of your organization?
  [Unknown]:  NEC Corporation
What is the name of your City or Locality?
  [Unknown]:  Minato-ku
What is the name of your State or Province?
  [Unknown]:  Tokyo
What is the two-letter country code for this unit?
  [Unknown]:  JP
Is CN=nfa.nec.com, OU=IT Operation Division, O=NEC Corporation,
 L=Minato-ku, ST=Tokyo, C=JP correct?
  [No]:  yes
Enter key password for <tomcat>
        (RETURN if same as keystore password):
```

Tip

- For `nfa_ssl_keytool` command, arguments can be specified. If you want to change the algorithm, size, or expiration date of the key, see "A.1 nfa_ssl_keytool (page 55)" and specify appropriate arguments.

  Example of specifying ECDSA for the key algorithm and 256 bits for the key size

  ```
  # cd /opt/nec/nfa/controller/bin
  # ./nfa_ssl_keytool genkeypair -keyalg EC -keysize 256
  ```

- To change the key contents and then recreate a key, run `nfa_ssl_keytool delete` command and then `nfa_ssl_keytool genkeypair` command again, or run `nfa_ssl_keytool genkeypair` command with a different `-alias` from the previous one.

  For details about the commands, see "A.1 nfa_ssl_keytool (page 55)".

2. Run the following command to output the certificate signing request (CSR) to be sent to the certificate authority to a file.

   ```
   # <%installation directory%>/controller/bin/nfa_ssl_keytool
    certreq -dns <FQDN> <filename>
   ```

   The contents of the CSR are output to the specified file.

3. Submit the certificate signing request (CSR) to the certificate authority.

   Submit the CSR file contents output by `nfa_ssl_keytool certreq` command to the certificate authority.

   The certificate authority will sign the certificate according to the contents of the CSR and return to the signed certificate to you. It might take several days until you receive the signed certificate.

4. After receiving the signed certificate, import the root certificate of the certificate authority first.

   Save the root certificate as a file in the NFA server, and then import it by using the following command:

   ```
   # <%installation directory%>/controller/bin/nfa_ssl_keytool
    importcert -alias <alias> <filename>
   ```

   <alias> is arbitrary. Specify an easy-to-understand name such as the root certificate authority name.

   In addition to a root certificate, an intermediate certificate may need to be installed depending on the certificate authority. For details about the certificates to be installed, please contact the certificate authority.

5. After importing the root and/or intermediate certificates, import the the certificate signed by the certificate authority.

   Use `nfa_ssl_keytool importcert` command to import the signed certificate. Run this command without the `-alias` option specified.

   ```
   # <%installation directory%>/controller/bin/nfa_ssl_keytool
    importcert <filename>
   ```

   If `Failed to establish chain from reply` is displayed, the certificate chain could not be built. The root and/or intermediate certificates might not have been imported. Ask the certificate authority about the root and/or intermediate certificates that must be imported.

Certificate creation on the NFA server is now complete.

It may be necessary to install the certificates to the web browser depending on the certificate authority. For details, follow the instructions of the certificate authority.

2.4.3 Using a certificate created for other purposes

The following describes the procedure to use a certificate that was created for other purposes as the SSL server certificate that NFA will use.

Prepare a keystore in the Java KeyStore (JSK) format and create a valid key and certificate in the keystore. Deploy the prepared keystore file on the NFA server.

1. Open the following text file.

   `<%data directory%>/controller/conf/tomcat.properties`

   If no properties file exists, create a properties file. Use UTF-8 as the file encoding.

2. Describe the following in the tomcat.properties file.

```
nfa.tomcat.https.keyAlias = Alias of the entry including the key
nfa.tomcat.https.keyPass = Password of the key
nfa.tomcat.https.keystoreFile = Absolute path of the keystore file
nfa.tomcat.https.keystorePass = Password of the keystore
```

⚠ Caution

If a setting to use an external keystore is described in the tomcat.properties file, `nfa_ssl_keytool` command will not be able to be used. In this case, use the Java keytool command to manage the certificate.

The Java keytool command is also installed in the NFA server.

`<%installation directory%>/controller/jre/bin/keytool`

For a self-signing certificate, export a binary encoded certificate (.cer) and import it to the web browser.

2.5 Checking the port numbers used in this product

NFA uses multiple port numbers for external and internal communications.

Check that the port numbers used in the NFA server do not conflict with those used by other software.

The communication port numbers used by NFA are listed in the next section. If NFA and other software use the same port number, change the port number used by one of them.

2.5.1 Port numbers used in this product

The following describes the default port numbers used by this product.

The port numbers that NFA uses for external and internal communications are listed in "Table 2-7 Communication port numbers that NFA uses for external communication (page 23)" and "Table 2-8 Communication port numbers that NFA uses for internal communication (page 24)".

Table 2-7 Communication port numbers that NFA uses for external communication

Name	Port Number	Protocol	Direction	Purpose
HTTPS communication port	443	TCP	IN	This is an HTTPS communication port.

Name	Port Number	Protocol	Direction	Purpose
sFlow packet reception port	6343	UDP	IN	This is an sFlow packet reception port.
NetFlow packet reception port	9995	UDP	IN	This is a NetFlow packet reception port.

Table 2-8 Communication port numbers that NFA uses for internal communication

Name	Port Number	Protocol	Direction	Purpose
Flow database communication port	27100	TCP	IN	This is a communication port for a flow database.
System database communication port	27110	TCP	IN	This is a communication port for a system configuration management database.
Event database communication port	27120	TCP	IN	This is a communication port for an event database.
Controller control communication port	27200	TCP	IN	This is a communication port for controller process control.
Collector log service communication port	27210	UDP	IN	This is a communication port for a log service of a collector process.

2.5.2 Changing the port number used in this product

The following describes the procedure to change the port number that NFA uses.

If NFA and another software use a same port number, change the port number of one of them.

Execute the following procedure to change the port numbers used by NFA.

1. Log in to the server as a root user.
2. Change the content of the configuration file corresponding to the port number to be changed and save the file.

   For details about the configuration files, see "Table 2-9 Configurations for communication port numbers (external communication) (page 24)" and "Table 2-10 Configurations for communication port numbers (internal communication) (page 25)". If no configuration file exists, create a configuration file.

   The configuration files are stored in *<%data directory%>*.

Table 2-9 Configurations for communication port numbers (external communication)

Purpose	Setting items

HTTP communication	• Configuration file
	`controller/conf/tomcat.properties`
	• Specification format
	`nfa.tomcat.https.port = 443`

Reception of sFlow packets	• Configuration file
	`collector/conf/collector.conf`
	• Specification format
	`sflow.port = 6343`

Reception of NetFlow packets	• Configuration file `collector/conf/collector.conf`

Purpose	Setting items
	• Specification format `netflow.port = 9995`

The configuration files are stored in *<%data directory%>*.

Table 2-10 Configurations for communication port numbers (internal communication)

Purpose	Setting items

Flow database communication	• Configuration file
	`collector/conf/flowdb.conf`
	• Specification format
	`flowdb.port = 27100`

	• Configuration file
	`collector/conf/flowdb-extra.conf`
	• Specification format
	`port = 27100`

System database communication	• Configuration file
	`controller/conf/controller.properties`
	• Specification format
	`systemdb.port = 27110`

	• Configuration file
	`controller/conf/systemdb-extra.conf`
	• Specification format
	`port = 27110`

Event database communication	• Configuration file
	`controller/conf/event.properties`
	• Specification format
	`eventdb.port = 27120`

	• Configuration file
	`controller/conf/eventdb-extra.conf`
	• Specification format
	`port = 27120`

Controller control communication	• Configuration file
	`controller/conf/controller.properties`
	• Specification format
	`message.server.port = 27200`

	• Configuration file `collector/conf/collector.conf` • Specification format

Purpose	Setting items
	`controller.port = 27200`

Collector log service communication	• Configuration file
	`collector/conf/nfalog.conf`
	• Specification format
	`Port = 27210`

Caution

For a communication port for which one item is described in multiple configuration files, edit all the files at the same time to specify the same port number. If the specified port number differs among the relevant configuration files, this product does not work properly.

3. Review the firewall settings as required.

   The port number for external communication is often blocked by a firewall. Therefore, after changing the port number, check that the firewall settings are appropriate.

Tip

After the service is started, the changed port number is applied to the NFA.

2.6 Changing a firewall configuration

It is necessary to change the firewall configuration so that the communication ports used by NFA will not be blocked by the firewall.

The default values of the communication ports that are open and used on the NFA server are listed in "Table 2-11 Communication port numbers that NFA uses for external communication (page 26)" and "Table 2-12 Communication port numbers that NFA uses for internal communication (page 26)". The default values of the ports that NFA uses for external communication are listed in "Table 2-13 Default destination port numbers for external communication of NFA (page 27)".

Change the firewall configuration so that these communication ports will not be blocked by the firewall.

Table 2-11 Communication port numbers that NFA uses for external communication

Name	Port Number	Protocol	Direction	Purpose
HTTPS communication port	443	TCP	IN	This is an HTTPS communication port.
sFlow packet reception port	6343	UDP	IN	This is an sFlow packet reception port.
NetFlow packet reception port	9995	UDP	IN	This is a NetFlow packet reception port.

Table 2-12 Communication port numbers that NFA uses for internal communication

Name	Port Number	Protocol	Direction	Purpose
Flow database communication port	27100	TCP	IN	This is a communication port for a flow database.
System database communication port	27110	TCP	IN	This is a communication port for a system configuration management database.

Name	Port Number	Protocol	Direction	Purpose
Event database communication port	27120	TCP	IN	This is a communication port for an event database.
Controller control communication port	27200	TCP	IN	This is a communication port for controller process control.
Collector log service communication port	27210	UDP	IN	This is a communication port for a log service of a collector process.

Table 2-13 Default destination port numbers for external communication of NFA

Name	Port Number	Protocol	Direction	Purpose
SNMP Get	161	UDP	OUT	This destination port number is used for SNMP communication from the NFA server to an exporter. This port number can be changed for each exporter on the web console.
SNMP Trap	162	UDP	OUT	This destination port number is used for SNMP trap transmission from the NFA server to external network management software. This port number can be changed on the web console.

The following describes a configuration example when iptables or firewalld is used as a firewall.

For details about other firewall software and firewall devices on network paths, see the manual of the relevant product.

If the port number to be used was changed by using the procedure in "2.5.2 Changing the port number used in this product (page 24)", permit communication to the port number after the change.

- When using iptables, edit `/etc/sysconfig/iptables`.

  The following is an example of the edited file. For details about how to edit this file, see the manual of the OS in use.

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -p udp -m udp --dport 6343 -j ACCEPT
-A INPUT -p udp -m udp --dport 9995 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

  The underlined portions are the added descriptions.

  After editing the file, restart iptables service so that the changed settings will be applied.

- When using firewalld, run firewalld commands as follows.

```
# firewall-cmd --permanent --add-port=443/tcp
# firewall-cmd --permanent --add-port=6343/udp
# firewall-cmd --permanent --add-port=9995/udp
# firewall-cmd --reload
```

For details about firewalld, see the manual of the OS in use.

2.7 Additional settings for the web server

The following describes the additional settings for the NFA web server.

2.7.1 Settings for automatic deletion of the web server logs

The following describes the settings for automatic deletion of the NFA web server log files.

The access logs and process logs of the NFA web server are stored in the following directory.

<%installation directory%>/controller/tomcat/logs/

Some log files shown below in this directory are not rotated or deleted automatically. By using cron, etc., you can configure settings so that old log files will be deleted automatically.

- localhost_access_log.*yyyy-mm-dd*.txt
- catalina.*yyyy-mm-dd*.log

yyyy-mm-dd indicates the date on the NFA server. For example, localhost_access_log.2016-04-01.txt is the access log file of the web console at April 1st, 2016.

Example

The following is an example of cron setting that deletes logs older than 30 days at 1:00 a.m.

```
0 1 * * *    /usr/bin/find /opt/nec/nfa/controller/tomcat/logs/
   -type f -regex '^.*\.[0-9]+-[0-9]+-[0-9]+\.\(txt\|log\)$'
   -mtime +30 -exec /bin/rm -f {} \;
```

For details about cron, see the manual of the OS in use.

2.8 Configuring for using IMS component

The following describes the configuration when integrating multiple NFAs or NFA and Network Manager using IMS component.

Tip

When not using the IMS component, this configuration is not necessary.

When using the IMS component, configure the following three items.

- Setting up the IMS component

  Install the IMS component and configure the IMS component to allow the connection from NFA.

  For details, refer to *"MasterScope Network Management Web Console Getting Started Guide"*.
- Configuring for the connection with the IMS component

  Configure for the connection with the IMS component in the NFA.
- Configuring for single sign-on

Configure the NFA to enable access from Web Console of the IMS component to the Web Console of the NFA by single sign-on.

For configuring the NFA, update the following configuration file (controller.properties).

The configuration file:

```
<%data directory%>/controller/conf/controller.properties
```

Tip

After the service is started, the updated configuration file is applied to the NFA.

Configuring for the connection with the IMS component

Update the following parameters in the configuration file (controller.properties), overwrite it and save.

```
ims.application-instance-id = <manager id>
ims.msgqueue.host = <ims ip address>
ims.msgqueue.port = <port number>
```

<manager id>

Specify the ID so that the IMS component can identify the NFA to be connected.

This parameter must match the value of the configuration file (ims-conf.ini) on the IMS component.

<ims ip address>

Specify the IPv4 address of the server where the IMS component is installed.

If the IMS component is installed on the cluster system, specify the floating IP address of the cluster system.

<port number>

Specify the communication port number to be used for communication with the Message Queue of the IMS component.

This parameter is required to be updated when changing the default communication port number.

Example:

```
ims.application-instance-id = nfa01
ims.msgqueue.host = 192.168.1.200
ims.msgqueue.port = 28110
```

Configuring for single sign-on

Update the following parameters in the configuration file (controller.properties), overwrite it and save.

```
ims.webserver.base-url = <ims web url>
ims.sso.enabled = <true|false>
```

<base url>

Specify the URL to access the Web Console of the IMS component.

Caution

For this parameter, specify URL accessible from the NFA.

<true|false>

Specify whether to enable single sign-on behavior as follows.

- true : Enable single sign-on behavior.
- false : Disable single sign-on behavior.

Specify *"true"* to enable single sign-on behavior.

Example:

```
ims.webserver.base-url = http://ims.nec.com
ims.sso.enabled = true
```

2.9 Starting the service

The NFA service can be started when installation is complete.

The NFA service can be started by directly running the start script (System V init script) or by restarting the OS.

The following describes the procedure to start the service by running the start script.

1. Log in to the NFA server as a root user.
2. Run the following command to start the service.

   ```
   # /etc/init.d/nec-nfa-service start
   ```

   If the service started normally, the following message is displayed.

   - In Red Hat Enterprise Linux 6

     ```
     Starting systemdb...              [  OK  ]
     Starting eventdb:                 [  OK  ]
     Starting controller:              [  OK  ]
     Starting web server:              [  OK  ]
     Starting flowdb:                  [  OK  ]
     Starting log server:              [  OK  ]
     Starting collector:               [  OK  ]
     ```

     The message consists of multiple lines because the service includes multiple service processes.

   - In Red Hat Enterprise Linux 7

     ```
     Starting nec-nfa-service (via systemctl):  [  OK  ]
     ```

   `[ NG ]` instead of `[ OK ]` is displayed for a process that could not start normally.
3. Run the following command to confirm that the service processes are running normally.

   ```
   # /etc/init.d/nec-nfa-service status
   ```

   If the service processes are running normally, *name* `(pid` *process_id*`) is running` is displayed for each process.

```
systemdb (pid 12340) is running...
eventdb (pid 12341) is running...
controller (pid 12342) is running...
web server (pid 12343) is running...
flowdb (pid 12344) is running...
logserver (pid 12345) is running...
collector (pid 12346) is running...
```

4. Run the following command to confirm that the listen port of the web server is open.

```
# ss -an | grep 443
```

443 is the default listen port number of the web server.

If the web server is running normally, port 443 is LISTEN state as follows:

```
LISTEN     0      100             :::443             :::*
```

If the web server is not running normally, see "B.2 Service startup errors and actions (page 60)" and take appropriate action.

Chapter 3. Post-Installation Environment Settings

This chapter describes how to configure the environment after installing NFA.

Contents

3.1 Preparing to use web console

The following describes the preparations required to use the NFA web console from a web browser.

Configure your web browser before accessing the web console. The following web browser settings only need to be configured once.

3.1.1 Synchronizing the time with the NFA server

The time of the computer on which to run the web console must be synchronized with the NFA server clock.

If the time of the web console is not identical to the NFA server clock, the displayed time may appear fast or slow.

Therefore, before using and operating the web console, configure its time to be identical to that of the NFA server clock.

Tip

It is recommended to use an NTP service so that a time lag does not occur.

3.1.2 Checking the web browser security settings

The following describes the web browser security settings required to use the NFA web console.

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

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

For Windows Server, if **Enhanced Security Configuration** is set to *"Enable"*, the setting described in "Configuring settings on a Windows Server OS (page 34)" is required.

Checking the Internet Explorer settings

Check the Internet Explorer settings from the Internet Options dialog box. Press ALT+T on the Internet Explorer window and select **Internet Options** from the displayed menu. For details about the settings on each tab, see the help of Internet Explorer.

- **Security** tab
  - Registration to *"Trusted sites"*

    Register the URL of the NFA server to *"Trusted sites"*.

    Tip

    If you do not want to register the NFA server to *"Trusted sites"*, configure the security settings so that the server is assumed to be other than a site on *"Restricted sites"*.

  - Enabling JavaScript

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

  If the zone to which the NFA server belongs is *"Internet"*, make sure that Cookies are allowed.

Tip

- If the zone to which the NFA server belongs is *"Trusted sites"* or *"Local Intranet"*, cookies are not blocked.
- If the zone to which the NFA server belongs is *"Restricted sites"*, cookies are always blocked and the web console cannot be used.

Checking the Mozilla Firefox settings

Check the Mozilla Firefox settings from the Options page. For details about the settings, see the help of Mozilla Firefox.

- **Privacy** panel

  In the **History** setting, make sure that Cookies from sites are acceptable.

Checking the Google Chrome settings

Check the Google Chrome settings from Settings page. In this page, click **Show advanced settings** at the bottom of the page and then click **Content settings** button under the **Privacy** section. You can check the settings in the Content settings dialog box. For details about the settings, see the help of Google Chrome.

- **Cookie**

  Make sure that Cookies can be stored.

- **JavaScript**

  Make sure that JavaScript is permitted.

Configuring settings on a Windows Server OS

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

3.1.3 Importing an SSL server certificate to the web browser

The SSL server certificate required to access NFA must be imported to the web browser.

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

Tip

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

⚠ Caution

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

- Perform the following procedure for Internet Explorer and Google Chrome.

  1. Create a certificate (.cer file) that can be imported by using `exportcert` command of "A.1 nfa_ssl_keytool (page 55)".

2. Double-click the certificate file created by using `nfa_ssl_keytool exportcert` on the computer on which to run the web browser.
3. On the displayed Certificate dialog box, click the **Install Certificate** button.

   Certificate Import Wizard is displayed. Click the **Next** button.
4. Select **Place all certificates in the following store** and click the **Browse** button.
5. On the Select Certificate Store dialog box, select *"Trusted Root Certification Authorities"* and click the **OK** button.
6. Click the **Next** button.
7. Click the **Finish** button.
8. A security warning is displayed for self-signed certificates. Click the **Yes** button.

The certificate is successfully imported when a dialog message `The import was successful.` is displayed.

- Perform the following procedure for Mozilla Firefox.

  1. Access the following URL by using the web browser.

     https://<NFA server domain name (FQDN)>/nfa/

     Tip

     Name resolution needs to be available for the NFA server domain name specified in the URL.

     A security warning is displayed for self-signed certificates.
  2. Click the **Advanced** button, and then click the **Add Exception** button.
  3. In the Add Security Exception dialog box, confirm that **Permanently store this exception** is checked, and then click the **Confirm Security Exception** button.

     Caution

     Before confirming the security exception, make sure that the adding certificate is collect.

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

3.2 Accessing the web console

The following describes how to access the NFA web console from a web browser.

Configure the web browser settings described in "3.1 Preparing to use web console (page 33)" beforehand.

Execute the following to access the web console.

1. Specify the following URL on the address bar of the web browser to open the login page of the web console.

   https://<NFA server domain name (FQDN)>/nfa/

   The host name (FQDN) must be the same as the name specified when creating an SSL server certificate. Otherwise, a warning indicating an invalid certificate is displayed.

   Tip

   To access the web console, name resolution needs to be available for the NFA server domain name specified in the URL.

2. Enter a user name and password to log in to the web console.

   The initial user name is *"admin"*, and the initial password is *"password"*.

When the login to the web console is successful, the Dashboard page set for the login user is displayed.

Caution

- The following are cautions on logging in to the web console and operation.
  - After the first login, change the password of the admin user.

    To change the password, click the **(Personal Settings)** button at the upper right of the page to display the Personal Settings page.
  - The NFA settings cannot be handled (added, changed, or deleted) on multiple web consoles at the same time.
  - If no operation is performed for 30 minutes after logging in to the web console, automatic logout is executed and the login page is displayed again when the next operation is performed.

    However, automatic logout is not executed if 1 minute, 5 minutes, or 15 minutes is set as the update interval on the Dashboard, Exporter Analysis, and Event List pages.
- The following are cautions when enabling single sign-on behavior with the Web Console of the IMS component.
  - In the IMS component, register users with the same name as the NFA. Single sign-on is valid only for users with the same name.
  - Even if you specify the URL for the web console of the NFA when logging in, login page for the web console of the IMS component is displayed. When login is successful, it will automatically transition to the web console page of the NFA.
  - If the IMS component is stopped, access to the web console of the NFA may fail. In this case, specify the following URL, display the login page for the web console of NFA and login.

    https://<NFA server domain name (FQDN)>/nfa/login

3.3 Configuring the system environment

The following describes the system environment settings that must be configured before registering the managed exporter information (the exporter and its interfaces) to NFA.

By default, if NFA receives flow information from an unknown exporter, information of that exporter (the exporter and its interfaces) is automatically registered. At this time, the interface license is also assigned automatically.

Tip

You can specify a setting to prevent automatic registration of exporter information at reception of flow information. The automatic registration policy can be set on the Environment Settings page. To open the Environment Settings page, click **System Management**>**Environment Settings**.

If exporter information is automatically registered, NFA collects the following information automatically and registers it as exporter information.

- Name of the exporter used in DNS (FQDN)
- Name of the exporter used in SNMP (sysName)
- Name of the interface (ifName)

For the FQDN, the IP address of the exporter is converted and obtained according to the name resolution mechanism of the NFA server.

For sysName and ifName, information is obtained from the exporter's MIB through SNMP communication according to the default values that have been set for the SNMP information acquisition parameters.

The following describes the procedure to set default values for the SNMP information acquisition parameters.

Before executing the following procedure, check the values of the SNMP parameters that have been set to the exporters in your operating environment.

Tip

We recommend setting the same SNMP parameter values (SNMP version, port number, and SNMP community name) for all exporters to be deployed in your operating environment.

1. Open the Environment Settings page.

   Click **System Management**>**Environment Settings**.

2. Enter the same values as the values of the exporter settings in the following fields of **Parameters for Getting Exporter Information (SNMP)**.

   - **SNMP Version**

     Select the version from the pull-down menu (**1** or **2c**). The default is **2c**.

   - **Port Number**

     Specify a value from 0 to 65535 in single-byte numbers. The default is *"161"*. Generally, *"161"* is used for the SNMP port number.

   - **SNMP Community Name**

     Specify a character string consisting of up to 255 single-byte alphanumeric characters. The default is *"public"*.

3. Check the settings and click the **Save** button.

3.4 Registering a product license

The following describes the procedure to validate a product license.

Prepare the Codeword Request Form on which the license key to register is described.

Execute the following three steps to register the product license.

1. Register the license key.
2. Request the codeword issuing center to issue the codeword.
3. Register the issued codeword.

These steps are described in detail below.

1. Register the license key.
   a. Open the License Registration page.

      Click **System Management**>**License Registration**.

   b. Click the **Add License** button.

      The Add License page is displayed.

   c. Enter the product code and license key described in the Codeword Request Form.

   d. Click the **Register** button.

If registration is successful, the codeword request code is displayed in the **Request Code** text box of the Add License page.

2. Request the codeword.

   To get the codeword, send the codeword request code that was displayed. For how to send the codeword request code, see the Codeword Request Form.

   Tip

   To display the codeword request code, click the **(Show Details)** button of the target license key in the License Registration page.

   The codeword will be sent in a few days.

3. Register the codeword.

   a. In the License Registration page, click the **(Register Codeword)** button of the target license key.

      The Register Codeword page is displayed.

   b. Enter the obtained codeword in the **Codeword** text box.

   c. Check the settings and click the **Register** button.

      If registration is successful, the License Registration page is displayed again. Confirm that **Codeword is registered** is displayed in **Status** of the relevant license key in License Key List.

3.5 Configuring exporter devices

Exporter devices need to be configured so that NetFlow or sFlow information will be sent to NFA, and the information will be obtained by using SNMP.

To collect flow information from exporters in NFA, the following settings are needed on the exporter devices.

- Settings to send NetFlow or sFlow information to the NFA server
- Settings to obtain information by using SNMP

For the concrete setting procedure, see the manuals of the exporter devices in use.

The following describes an overview of the items that must be set up on the device.

1. Specify the IP address of the NFA server as the destination to which to send flow information. For the destination port number, specify 9995 in the case of NetFlow or 6343 in the case of sFlow.

   Tip

   If the reception port number of NetFlow or sFlow has been changed by using the procedure in "2.5.2 Changing the port number used in this product (page 24)", specify the device setting according to the changed port number.

2. If necessary, configure ifIndex persistence settings.

   After the exporter is restarted, the ifIndex value corresponding to the analysis target interface may change depending on the exporter specifications. If the ifIndex value changes, NFA cannot identify the analysis target interface and the analysis result may not be displayed correctly.

For such an exporter, specify the setting so that the ifIndex value of the interface will be kept after the exporter restarts.

Configuration example for Cisco IOS:

```
(config)# snmp-server ifindex persist
```

3. In the case of NetFlow, specify one minute for the cache timeout of an active flow.

   Configuration example for Cisco IOS:

   ```
   (config)# ip flow-cache timeout active 1
   ```

4. In the case of sFlow, specify one minute for the interval at which to send a counter sample.

   Configuration example for the NEC UNIVERGE IP8800/S series:

   ```
   (config)# sflow polling-interval 60
   ```

5. Specify 1 or 2c for the SNMP version of the device.
6. Specify the SNMP Get community name of the device.

3.6 Adding an user

The following describes the procedure to add a new user.

1. Open the User Management page.

   Click **System Management**>**User Management**.

2. Click the **Add** button in the User List.
3. Specify an appropriate value for each item on the displayed Add User page.

   - **User Name**

     Specify a user name that is unique in NFA. The available number of characters is 32. The available characters are single-byte alphanumeric characters, hyphens(-), underscores (_), dots (.), and apostrophes (').

   - **Display Name**

     Specify the user name to be displayed on the console page. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

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

   - **Initial Password**

     Specify the initial password of the user to be registered. Specify a character string consisting of 8 to 32 single-byte alphanumeric characters.

   - **Confirmation**

     Enter the password specified in **Initial Password**.

   - **Authority Level**

     Select **Administrator** or **Operator**.

   - **Default Dashboard**

     Select the name of the dashboard definition that is initially displayed after the user logs in.

4. Check the settings and click the **OK** button.

Chapter 4. Basic Operations

This chapter describes the basic operations of NFA.

Contents

4.1 Structure of web console

The following describes the configuration of the web console of NFA.

The NFA web console consists of the areas as shown in "Figure 4-1 Configuration of web console (page 42)".

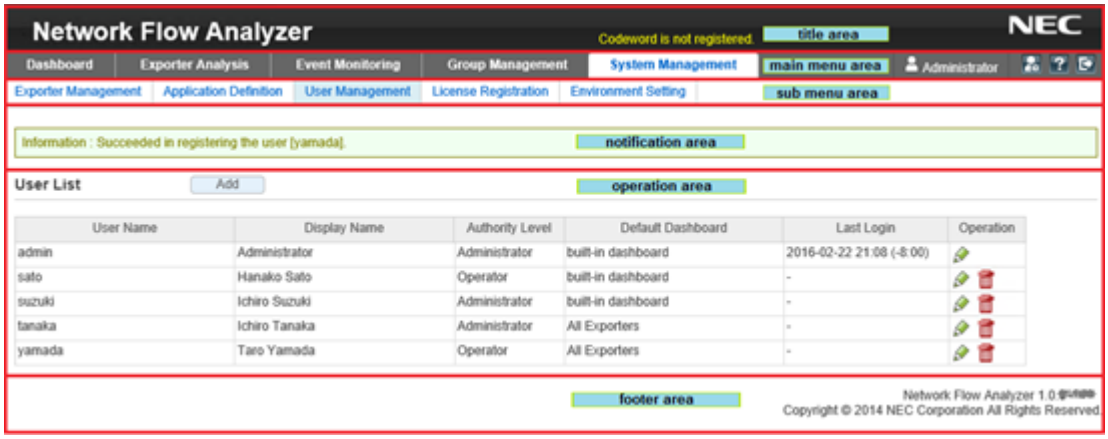


Figure 4-1 Configuration of web console

Title area

Displays the product name, and a message indicating the registration status of the product license and codeword.

Main menu area

Displays menus and operation buttons.

- Main menu (functional category of NFA)
  - **Dashboard** tab

    The operation page for displaying and setting the Dashboard page.
  - **Exporter Analysis** tab

    Displays the Exporter Analysis page where you can narrow down the exporters to be analyzed and analyze the communication traffic in detail.
  - **Event Monitoring** tab

    Displays a page to specify monitoring the communication traffic by using thresholds and to check the history of threshold violation and recovery event occurrence.
  - **Group Management** tab

    Displays a setting page to group endpoints that are used in analysis or for display on the Dashboard and Exporter Analysis tab and also to group exporter interfaces. In addition, a list page is displayed to show the current group setting status.
  - **System Management** tab

    Displays a page to configure and manage the settings related to the entire system, for example, to manage the exporters and their interfaces and to manage the users who can log in to NFA.

Tip

The **System Management** tab can be used only by a logged in user who has administrator rights.

- Display of user name
  - The logged in user name is displayed. Here, **Display Name** value of the user is displayed. If **Display Name** is not specified, the value of **User Name** is displayed.
- Buttons
  - **(Personal Settings)** button

    Clicking this button displays the page to change the personal settings of the logged in user, such as **Display Name** and **Password**.

    Tip

    We recommend changing the password after the first login.

  - **(Help)** button

    Clicking this button displays the help of NFA.

  - **(Logout)** button

    Clicking this button logs you off from the web console.

Sub menu area

If the selected main menu has sub menus, these are displayed here.

Notification area

Displays information related to the current operation or error information indicating, for example, that the input value is invalid.

Operation area

Displays the operation contents according the selected main menu or sub menu.

Footer

Displays the version and copyright of the NFA.

4.2 Widget types

On the Dashboard and Exporter Analysis pages, individual analysis results of the communication status are displayed as widgets. The following describes the widget types that NFA supports.

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

Line chart widgets

These widgets display the results of analyzing transitions in the communication traffic for each item within the specified period on a line chart. The amount of communication traffic for each item within

the specified period is also ranked in a list. The communication traffic unit can be selected from bps or pps.

The following widgets belong to this type.

- Communication traffic analysis widget

Table 4-1 Communication traffic analysis widget

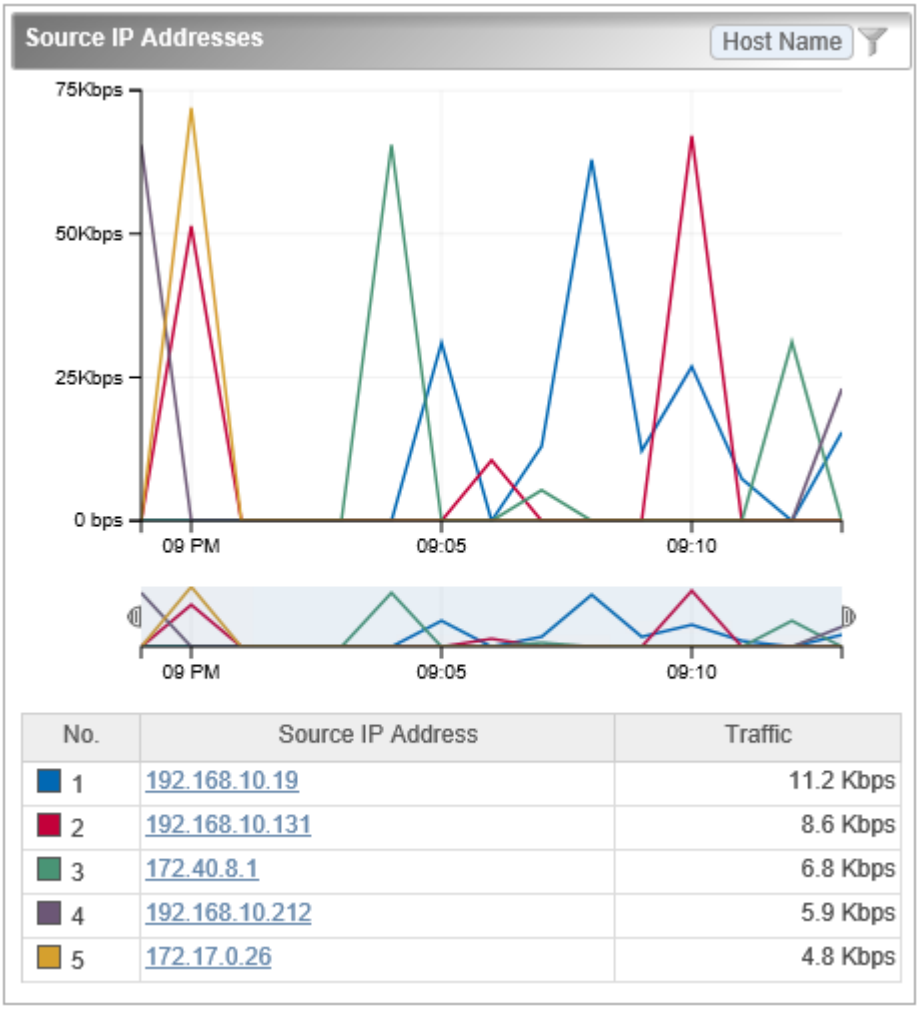
Widget type	Description
Exporters	Displays exporters with a high volume of communication traffic. The communication traffic of an exporter is the total communication traffic passing through the interfaces of the exporter.
IN Interfaces	Displays input interfaces with a high volume of communication traffic.
OUT Interfaces	Displays output interfaces with a high volume of communication traffic.

- Communication source and destination analysis widget

Table 4-2 Communication source and destination analysis widget

Widget type	Description
Source IP addresses	Displays source IP addresses with a high volume of communication traffic. In the widget display, the source IP address can be changed to the host name.
Destination IP addresses	Displays destination IP addresses with a high volume of communication traffic. In the widget display, the destination IP address can be changed to the host name.
Conversations	Displays conversations (communication between two endpoints) with a high volume of communication traffic. In the widget display, the IP addresses of the communicating endpoints can be changed to the host names.
Source Endpoint Groups	Displays source endpoint groups with a high volume of communication traffic.
Destination Endpoint Groups	Displays destination endpoint groups with a high volume of communication traffic.
Source AS	Displays source autonomous systems (AS) with a high volume of communication traffic. The AS is displayed as a number.
Destination AS	Displays destination autonomous systems (AS) with a high volume of communication traffic. The AS is displayed as a number.

"Figure 4-2 Line chart widget (page 45)" shows a sample line chart widget.



No.	Source IP Address	Traffic
1	192.168.10.19	11.2 Kbps
2	192.168.10.131	8.6 Kbps
3	172.40.8.1	6.8 Kbps
4	192.168.10.212	5.9 Kbps
5	172.17.0.26	4.8 Kbps

Figure 4-2 Line chart widget

Pie chart/line chart widgets

The analysis result can be displayed as a pie chart or line chart.

- Pie chart

  A pie chart displays the proportion of communication traffic for each item to the total communication traffic within the specified period. The amount of communication traffic for each item within the specified period is also ranked in a list. The communication traffic unit can be selected from bytes or packets.

- Line chart

  These widgets display the results of analyzing transitions in the communication traffic for each item within the specified period on a line chart. The amount of communication traffic for each item within the specified period is also ranked in a list. The communication traffic unit can be selected from bps or pps.

The following widgets belong to this type.

Table 4-3 Pie chart/line chart widgets

Widget type	Description
Applications	Displays applications with a high volume of communication traffic.

Widget type	Description
IP Protocols	Displays IP protocols with a high volume of communication traffic.
DSCP	Displays DSCP with a high volume of communication traffic.

"Figure 4-3 Pie chart/line chart widget (page 46)" shows a sample pie chart widget.

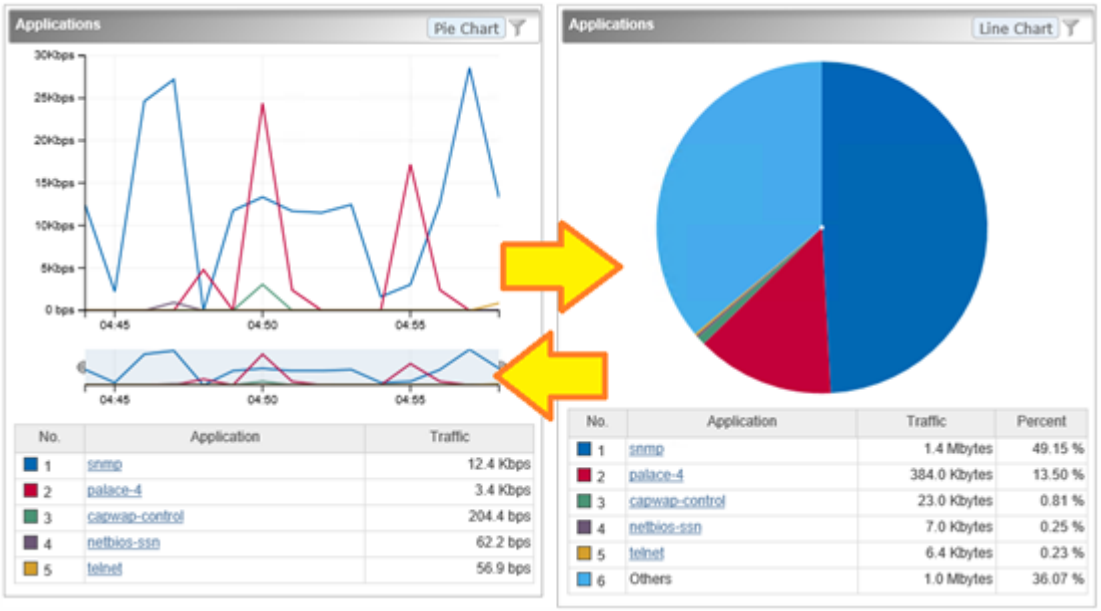


Figure 4-3 Pie chart/line chart widget

List display type

These widgets display information about the communication status in a list.

The following widgets belong to this type.

Table 4-4 List display widget

Widget type	Description
Current Alerts	Displays current alert events.

"Figure 4-4 List display widget (page 46)" shows a sample list display widget.

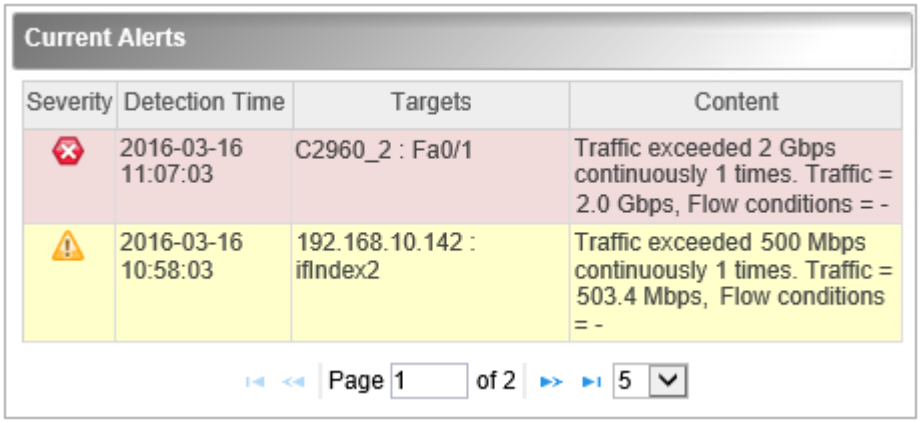


Figure 4-4 List display widget

4.3 Performing operations on widgets

For line chart and pie chart widgets, drill-down analysis can be performed and the items displayed by the widget can be filtered. Furthermore, for line chart widgets, the user can zoom in on the chart and the displayed IP address can be changed to the corresponding host name.

For a line chart widget and a pie chart/line chart widget on which a line chart is displayed, the user can zoom in on the chart.

Furthermore, for a widget that displays endpoint information by using an IP address, the displayed IP address can be changed to the corresponding host name.

For a pie chart/line chart widget, a pie chart or line chart can be displayed.

Tip

Click the **Line Chart** button to display a line chart. Click the **Pie Chart** button to change the displayed line chart to a pie chart.

4.3.1 Performing drill-down analysis

For line chart and pie chart widgets, the analysis conditions can be narrowed down by clicking the link of the item you want to analyze on the list. The procedure is shown below.

Drill-down analysis is useful if you want to perform detailed analysis from a widget displayed on the Dashboard page or intuitively add a filtering condition to the analysis results on the Exporter Analysis page.

1. Click the link of the item you want to analyze on the list of the target widget.

   Tip

   If this is performed for a widget related to multiple exporters on the Dashboard page, a page to select an exporter and the interfaces to be analyzed is displayed. In this case, select the exporter or interface you want to analyze.

2. The selected item is added to **Filter Conditions** on the Exporter Analysis page.

Confirm that the analysis results have been updated.

Operation example:

The following operation example shows how to perform drill-down analysis on the Dashboard page of the communication of the source IP address *"192.168.1.100"* that passes through interface *"0/1"* of the *"base connection router"*.

1. Click the link of the source IP address *"192.168.1.100"* of the *"Source IP Address"* widget on the Dashboard page.
2. The page transitions to the Exporter Analysis page, and **List of Analysis Candidates** is displayed.

   At this time, the source IP address *"192.168.1.100"* is set to **Filter Conditions**. In **List of Analysis Candidates**, the names and communication traffic of the exporter and interfaces that are monitoring the flow corresponding to this condition are displayed.
3. In **List of Analysis Candidates**, click interface *"0/1"* that is the *"base connection router"*.
4. Widgets that analyze the flow corresponding to the following conditions are displayed in the Exporter Analysis page.

Target Exporter

Base connection router

Target Interfaces

0/1

Filter Conditions

Source IP Address ="192.168.1.100"

4.3.2 Filtering the items displayed on a chart

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

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

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

1. Click the **(Filter Settings)** button of the target widget.
2. On the Filter Analysis Targets dialog box, clear the check box of an analysis target item to exclude it from the targets.
3. Click the **OK** button to apply the filter settings.

The contents displayed in the widget will change.

- For line chart widgets

  Only the items specified for analysis will be displayed.

- For pie chart widgets

  The proportion of the items specified for analysis to the total communication traffic will be displayed.

4.3.3 Zooming in on a line chart

For line chart widgets, a chart can be zoomed in on by reducing the the time scale of the line chart that shows the entire specified period. The procedure is shown below.

You can zoom in on a line chart by specifying the time scale, within the chart display period that is specified in the display settings. This is useful if you want to check the communication status in detail by zooming in on the chart.

1. Select the lower line chart that shows the overall period. This line chart is called the range selector.
2. Adjust the time scale by dragging and dropping the right and left cursors of the range selector.

   If you want to adjust the display position, execute the following:

   - Adjust the the time scale by dragging and dropping the right and left cursors of the range selector.
   - Move the time scale by dragging and dropping the specification area of the range selector.

- Click outside the specification area of the range selector to release the time specification and specify a new time scale by dragging and dropping.

  Tip

  - The right and left cursors of the range selector are hidden by releasing the time specification. The cursors can be displayed again by specifying the time scale in the range selector.
  - The time scale can also be specified by dragging the area outside the time axis without releasing the time specification.

The upper line chart is zoomed in on within the specified range. The amount and rank of communication traffic for each item within the specified period are also displayed in a list.

4.3.4 Changing the IP address display to the host name

For widgets that display endpoint information by using IP addresses, the displayed IP addresses can be changed to the corresponding host names. The procedure is shown below.

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

Tip

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

By seeing the displayed the host name, you can easily understand the status of communication endpoints.

1. Click the **Host Name** button of the target widget.
2. The IP addresses indicating the endpoints are changed to the corresponding host names.

   Check the list display of the target widget.

   Caution

   When the display is changed from an IP address to a host name, the link to the Exporter Analysis page will be disabled.

To return to the original IP address display, click the **IP Address** button.

4.4 Updating the personal settings

The following describes the procedure for the user who logged in to the NFA web console to change the own user information including the login password.

Tip

The **User Name** and **Authority Level** settings cannot be changed.

1. Open the Personal Settings page.

Click the **(Personal Settings)** button of the main menu area.

2. Change the settings on the displayed Personal Settings page.

   - **Display Name**

     Specify a user name to be displayed on the web console. The available number of characters is 32. A single-byte space cannot be used at the beginning and end of the name.

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

   - **Default Dashboard**

     Select the name of the dashboard definition that is initially displayed after the login.

   - **Change Password**

     Select the check box and enter the current password in the **Old Password** text box.

     Enter a new password in the **New Password** text box, and then in the **Confirmation** text box.

     Specify the password consisting of 8 to 32 single-byte alphanumeric characters.

3. Check the changes and click the **Save** button.

Chapter 5. Upgrade

This chapter describes how to upgrade NFA.

Contents

By upgrading, the software will be updated from an old version to the latest version.

5.1 Upgrading the software

Run the installer on the installation media to upgrade NFA.

1. Insert the installation media in the CD-ROM drive and mount it.

   In the following description, the CD-ROM mount point is `/media`. If you mounted the installation media on another location, replace this mount point with the appropriate mount point.

2. Stop the NFA service before upgrading.

   ```
   # /etc/init.d/nec-nfa-service stop
   ```

3. Run the following command to start the upgrade installer.

   ```
   # /media/NFA/Linux/nfa-upgrade
   ```

4. Check the displayed version number and start upgrading.

   The current version of each functional component is displayed at the left, and the version after the upgrade is displayed in [ ] at the right. If the displayed versions are correct, enter `y` and press the Enter key.

   ```
   Network Flow Analyzer version 2.0.0-2 Upgrade Installer

   ----- Confirmation ---------------------
   Controller : 1.1.0-6  -> [ 2.0.0-2 ]
   Collector  : 1.1.0-6  -> [ 2.0.0-2 ]
   ----------------------------------------

   Is it OK to upgrade? (y/n): y
   ```

   Entering `y` starts installation.

   Entering `n` stops installation.

When the following message is displayed, upgrading is complete.

```
Upgrading controller ... done
Upgrading collector  ... done
```

If an error occurs during the upgrade, an error message is displayed. If an error message is displayed, see "B.1 Installation errors and actions (page 59)" and take appropriate action.

After the upgrade has been finished, start the NFA service.

```
# /etc/init.d/nec-nfa-service start
```

Chapter 6. Uninstallation

This chapter describes how to uninstall NFA.

Contents

6.1 Notes on uninstallation

The following describes the notes on uninstalling NFA.

Mainly, use `rpm -e` command to uninstall this product.

- If this product has been installed by separating the installation directory and data directory, `rpm -e` command does not delete the data directory. Therefore, delete the data directory manually.
- If the installation directory and data directory are the same directory, `rpm -e` command deletes all data.
- `rpm -e` command does not delete the `/etc/init.d/nec-nfa-service` script. Therefore, delete this script manually during the uninstallation processing.

6.2 Uninstalling the product

The following describes how to uninstall NFA.

1. Log in to the server as a root user.
2. Run the following command to stop the NFA service.

```
# /etc/init.d/nec-nfa-service stop
```

3. Run the following command to uninstall the software.

```
# rpm -e nec-nfa-controller nec-nfa-collector
```

4. Run the following commands to delete the service start script.

```
# chkconfig --del nec-nfa-service
# rm -f /etc/init.d/nec-nfa-service
```

5. If the installation directory and data directory have been separated, delete the data directory manually.

Uninstallation is now complete.

Appendix A. Command Reference

The following describes the commands that are provided by NFA.

A.1 nfa_ssl_keytool

This command is used to create and manage SSL server certificates that are used in HTTPS communication.

This command is a wrapper command that provides the functions of the Java keytool command in an easy-to-use format for this product. The Java keytool command functions that this command can use are limited. The names and meanings of the arguments are the same as those of the Java keytool command.

For details about the Java keytool command, see the following URL.

- https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html *1

The differences between this command and the Java keytool command are described below.

- For the first argument, specify a subcommand name such as `genkeypair`. `-` is not needed at the beginning of the argument name of the subcommand.
- For this command, the path of the keystore is fixed to *<%data directory%>*`/controller/conf/server.keystore`.
- `genkeypair` subcommand records the keystore passwords, the aliases of the entries in the keystore, and key passwords in the following file:

  <%data directory%>`/controller/conf/tomcat.properties`

  The information recorded in this file is automatically used when the `-storepass`, `-alias`, and `-keypass` options are omitted in subcommands. This permits users to run the command with the minimum number of arguments specified.
- The default values of the `-keyalg` and `-validity` options differ.
- An original subcommand `initstore` is implemented.

Path

<%installation directory%>`/controller/bin/nfa_ssl_keytool`

Synopsis

```
nfa_ssl_keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
nfa_ssl_keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-sigalg SIGALG] [-validity DAYS] [-dname DNAME]
```

```
nfa_ssl_keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-dns DNS] FILE
```

*1 This URL is current as of January 2019.

```
nfa_ssl_keytool importcert [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] FILE

nfa_ssl_keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE

nfa_ssl_keytool storepasswd [-help] [-storepass PASS] [-new NEWPASS]

nfa_ssl_keytool keypasswd [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-new NEWPASS]

nfa_ssl_keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]

nfa_ssl_keytool delete [-help] [-storepass PASS] [-alias ALIAS]

nfa_ssl_keytool initstore [-help]

nfa_ssl_keytool -help
```

Description

The following describes the subcommands.

- `genkeypair`

  Generates a key pair (public key and associated private key) and stores it in the keystore. This subcommand also writes the information required to used the key generated by the web server to the following file:

  <%data directory%>`/controller/conf/tomcat.properties`

- `selfcert`

  Creates a self-signed certificate for the key of the keystore entry.

- `certreq`

  Generates a certificate signing request (CSR) in the PKCS#10 format.

- `importcert`

  Reads the certificate or certificate chain from a file and stores it in the keystore.

- `exportcert`

  Reads the certificate from the keystore and stores it in a file as a binary encoded certificate.

- `storepasswd`

  Changes the password of the keystore.

- `keypasswd`

  Changes the key password of the keystore entry.

- `list`

  Displays a specific keystore entry or the entire contents of the keystore.

- `delete`

  Deletes an entry from the keystore.

- `initstore`

  Deletes a keystore file.

Arguments

-storepass *PASS*

Specifies a password for the keystore.

If this argument is omitted when running `genkeypair` subcommand, you will be prompted to enter a password while the command is running. If this argument is omitted when running other subcommands, the value read from the tomcat.properties file will be used.

-alias *ALIAS*

Specifies an alias for an entry in the keystore.

If this argument is omitted when running `genkeypair` subcommand, *"tomcat"* will be used by default. If this argument is omitted when running `list` subcommand, all entries will be displayed. If this argument is omitted when running other subcommands, the value read from the tomcat.properties file will be used.

-keypass *KEYPASS*

Specifies a password for the key.

If this argument is omitted when running `genkeypair` subcommand, you will be prompted to enter a password while the command is running. If this argument is omitted when running other subcommands, the value read from the tomcat.properties file will be used.

-keyalg *KEYALG*

Specifies an encryption algorithm for the password. For example, *"RSA"*, *"DSA"*, *"EC"* can be specified. The default is *"RSA"*.

For the algorithms that can be specified for `-keyalg` and `-sigalg`, see Java Cryptography Architecture (JCA) Reference Guide. *2

-keysize *KEYSIZE*

Specifies the size of the key to be generated.

The specifiable value range and default value comply with the Java keytool specifications.

-sigalg *SIGALG*

Specifies the algorithm used to sign a self-signed certificate.

An algorithm that is compatible with `-keyalg` must be specified. The specifiable value range and default value comply with the Java keytool specifications.

-validity *DAYS*

Specifies the number of days a self-signed certificate is valid. A value from 0 to 365000 can be specified. The default is 3650 (10 years).

-dname *DNAME*

Specifies the X.500 identification name to be used as the issuer and the subject fields of a self-signed certificate.

If this argument is omitted, you will be prompted to enter an identification name while the command is running.

-dns *DNS*

Specifies the FQDN for Subject Alternative Name (SAN) extension.

*2 This URL is current as of March 2016.

In `genkeypair` subcommand, if this argument is omitted, Common Name of a certificate is used as SAN.

-new *NEWPASS*

Specifies a new password if you want to change the kestore or key password.

If this argument is omitted, you will be prompted to enter a new password while the command is running.

-rfc

Specifies the output format of `list` subcommand. The content of a certificate will be output in a printable encoding format.

This option cannot be specified together with the `-v` option.

-v

Specifies the output format of `list` subcommand. The detailed content of the certificate will be output in a human readable format.

This option cannot e specified together with the `-rfc` option.

-help

Displays how to use commands in general or a specific command.

Return values

Success: 0 is returned. Failure: A value other than 0 is returned.

Appendix B. Troubleshooting

The following describes the problems that might occur while setting up NFA and the suggested actions to take to resolve those problems.

B.1 Installation errors and actions

The following describes the errors that might occur during installation and the suggested actions to take to resolve those errors.

SHMMAX must be larger than 256 MB

If the following message is displayed, the value set to kernel parameter kernel.shmmax is less than 256 MB and the software installation requirements are not satisfied.

```
ERROR:  SHMMAX must be larger than 256 MB.
```

Set 256 MB (268,435,456 bytes) or more to kernel.shmmax. We strongly recommend setting 2 GB or more to maximize the performance of this software. After changing the kernel parameter value, run the installer again.

Non-root user cannot access the install path

If the following message is displayed, a non-root user does not have permission to access the installation directory.

```
ERROR: Non-root user cannot access the install path:  /opt/nec/nfa
       Check the permission of the install destination.
```

Change the setting to permit a non-root user to access the directory specified as the installation directory and directories on the path to the installation directory by using a command such as `chmod`. Then run the installer again.

installing package nec-nfa-controller-*x.y.z-n*.x86_64 needs *XXX*MB on the / file system

If the following message is displayed, the capacity of the file system specified as the installation directory is insufficient or the file system is prohibited from being written.

```
Installing controller . failed
ERROR: Failed to install controller package:  code=1
        installing package nec-nfa-controller-x.y.z-n.x86_64 needs XXXMB
        on the / filesystem.
```

Specify a file system that has sufficient free space for the installation directory. After allocating sufficient free space, run the installer again.

Failed to initialize data. Directory exists

If the following message is displayed, the directory specified as the data directory is included the directory to be created at installation.

```
Installing controller . failed
ERROR: Failed to initialize data.
        Directory exists:  /opt/nec/nfa/controller/conf
```

If `Failed to initialize data` is displayed, the recovery command shown below is displayed following the message.

```
Try to run the following command later.
        /opt/nec/nfa/controller/bin/nfa_init_controller -data /opt/nec/nfa
```

Delete the directory displayed in the message and run the above recovery command as a root user.

B.2 Service startup errors and actions

The following describes errors that might occur when the service starts and the suggested actions to take to resolve those errors.

`[ NG ]` is displayed when the service starts.

If `[ NG ]` is displayed in the service startup processing, the data directory might not have been initialized correctly.

Perform the following:

1. Stop the service.

   ```
   # /etc/init.d/nec-nfa-service stop
   ```

2. Run the following commands:

   ```
   # <%installation directory%>/controller/bin/nfa_init_controller
    -data <%data directory%>
   # <%installation directory%>/collector/bin/nfa_init_collector
    -data <%data directory%>
   ```

   If the data directory is not empty, the following message might be displayed.

   ```
   ERROR:  Directory exists:  /opt/nec/nfa/controller/conf
   ```

   If this message is displayed, delete the displayed directory and run the commands again.

3. Create an SSL server certificate.

   Perform the procedure in "2.4 Preparing an appropriate SSL server certificate (page 19)".

4. Restart the service.

   ```
   # /etc/init.d/nec-nfa-service start
   ```

Listen port 443/tcp of the web server does not exist or the port is not LISTEN state.

Even if you have confirmed the state of listen port 443/tcp of the web server by using a command such as `ss -an | grep 443`, the SSL certificate might not be created correctly if there is no open port.

Perform the following:

1. Create an SSL server certificate.

   Perform the procedure in "2.4 Preparing an appropriate SSL server certificate (page 19)".

2. Restart the service.

```
# /etc/init.d/nec-nfa-service stop
# /etc/init.d/nec-nfa-service start
```

Service does not start automatically during the OS startup.

If the service can be started manually but does not start automatically during the OS startup, the setting of the service startup might have been changed by `chkconfig` command, and so on.

To start the service automatically during the OS startup, run the following command.

```
# chkconfig nec-nfa-service on
```

MasterScope
Network Flow Analyzer 2.0
Getting Started Guide

NFA0LSE0200-01

February, 2019 01 Edition

NEC Corporation