CHAPTER 2

Installing and Setting Up the NetFlow FlowAnalyzer

This chapter contains platform and system requirements, and provides instructions for installing and setting up the NetFlow FlowAnalyzer application.

Before You Begin

Before you begin installation of the NetFlow FlowAnalyzer application (the FlowAnalyzer), ensure that you have the correct version of platform software and that your workstation has enough logical memory and disk space as well as access to a browser

Platforms Supported

The NetFlow FlowAnalyzer application runs on the following platforms:

- HP-UX—Version 10.2 on a Class C machine with at least 256 MB RAM and running standard Java 1.02 (HP-UX Java 1.0.3)
- Solaris—Version 2.5.1 on an ULTRA-1 workstation with at least 256 MB RAM (Java 1.02 included)

Workstation Requirements

To ensure a successful installation of the FlowAnalyzer application, see that your workstation meets the following requirements:

- A Solaris or HP-UX workstation with 400 MB of free logical memory.
- Enough memory and 6 MB disk space available for installation of the FlowAnalyzer application.
- A browser to run the NFAnalyzer.html file. (The recommended version of Netscape browser is 3.0.1)

Note To reduce data loss during collection, install the FlowAnalyzer on a workstation separate from the FlowCollector. You get better performance when the Display user interface is not running on the same workstation as the FlowAnalyzer.

Installing the NetFlow FlowAnalyzer Application

The FlowAnalyzer application is available on CD-ROM. This section provides instructions for installing the FlowAnalyzer programs FlowAnalyzer DisplayServer and FlowAnalyzer Display. The NFADisplayServer program runs on Solaris 2.5.1 and uses Java classes and native libraries. The NFADisplay program includes a set of Java classes and an html file and should be installed on the same machine where your web server is running.

Important Notes

1. If you have installed this package on the same system before, you must remove it before you install a new one using the package remove utility:

   ```
   $ pkgrm NFA
   ```

   or

   ```
   $ pkgrm CSCOnfa
   ```

2. If you have been using a previous version of this tool and you have saved some data in the /opt/CSCOnfa/NFAServer/exported_files directory by pressing Export in the Display, you should copy this data out to a safe location, because the directory will be deleted when you do a pkgrm.
3. It is recommended that, due to system performance requirements, you do *not* run the FlowAnalyzer on the same machine as the FlowCollector.
4. This application must be installed on a machine hosting a web server.
5. If you install this application on an HP machine, you must also install Java 1.0.2 on that machine.
6. For HP_10 installations, Java 1.0.2 is required. For both HP-UX and Solaris installations, a web server is required.

Install from CD-ROM

Use the following installation procedure after installing the FlowAnalyzer software package:

Step 1 Log in as root.

```
$ su root
```

Step 2 Copy the tar file from the CD and untar the file.

For Solaris

```
$ cp NFA1_0.SOL.tar
$ tar -xvf NFA1_0.SOL.tar
```

For HP-UX

```
$ cp NFA1_0.HP_10.tar
$ tar -xvf NFA1_0.HP_10.tar
```

Step 3 Run the installation script and answer all questions.

```
$ chmod +x NFC1_0.setup.sh
$ ./NFA1_0.setup.sh NFA1_0.<platform>.Z
```

For the Solaris platform, enter the following:

```
$ ./NFA1_0.setup.sh ./NFA1_0.SOL.Z
```

For the HP-UX platform, enter the following:

```
$ ./NFA1_0.setup.sh ./NFA1_0.HPUX.Z
```

Setting Up the Display User Interface

To set up the FlowAnalyzer Display program on your workstation, use the following procedure:

Note To run the FlowAnalyzer Display, you must install the NFADisplayServer on the same machine where your http web server is running.

Step 1 Edit the NFAnalyzerB.html file located in the /opt/CSCOnfa/NFADisplay/bin directory so that NFDISPLAYSERVERPORT (6544 is the default) uses the port value that the server is listening on.

Also, the NFDISPLAYSERVERDATAPATH must point to the directory where the data is collected.

Step 2 Move the FlowAnalyzer files to a web server directory. For example:

```
$ cd /http-web-server-root-directory/docs
```

The http-web-server-root-directory is the directory where the http web server is installed.

Step 3 Create a directory for the nfa files and move to that directory.

```
$ mkdir nfa
$ cd nfa
```

Step 4 Copy the nfa files to this new directory.

```
$ cp -rf /opt/CSCOnfa/NFADisplay/bin/* .
```

Step 5 Open the NFAnalyzer.html file by clicking on the **Open** button or use the Open Location option from the File pull down menu in your browser. Enter the following:

```
http://http-web-servername/nfa/NFAnalyzer.html
```

The http-web-servername is the name of the host where the http web server is running.

Note Because browsers cache applets, you should flush the browser's cache if a pre-beta version of the FlowAnalyzer exists on your system. To flush the browser cache, use the Options->Network Preferences->Cache menu item.

Setting Up the DisplayServer

To set up the FlowAnalyzer DisplayServer program to retrieve traffic statistics from the NetFlow FlowCollector application, you can configure the DisplayServer program using the resource file or using the default parameters. Some additional setup is required for installation on the HP-UX platform.

Quick Start the DisplayServer

The following quick start procedures for the DisplayServer are provided here for your convenience.

Solaris Quick Start

Step 1 Verify that you have at least 256 MB of physical RAM and 400 MB of available swap space. If you do not, refer to the section entitled “Memory Management.”

To reduce the MaxMB value, edit the NFADS.resources file. For example:

```
MaxMB {your_value}
```

with

```
{your_value} = (physical RAM - 32) MB
```

Step 2 Start the DisplayServer program from the {DisplayServerBaseDir}/bin directory to begin listening to Port 6544.

```
$ start.DisplayServer
```

HP-UX Quick Start

Step 1 Verify that you have at least 256 MB of physical RAM and 300 MB of available swap space. Enter

```
$ /usr/sbin/swapinfo -m
```

If you do not, refer to the section entitled “Memory Management.”

To reduce the MaxMB value, edit the NFADS.resources file. For example:

```
MaxMB {your_value}
```

with

```
{your_value} = (physical RAM - 32) MB
```

Step 2 Ensure that your execution path is set with HP-UX Java Version 1.0.3. If it is not, refer to the section entitled “Configure the DisplayServer.”

Step 3 Start the DisplayServer program from the {DisplayServerBaseDir}/bin directory to begin listening to Port 6544.

```
$ start.DisplayServer
```

Customize the DisplayServer

The DisplayServer’s resource file NFADS.resource contains a variety of parameters you can use to configure the DisplayServer so that it retrieves summarized traffic statistics from the NetFlow FlowCollector.

To redefine configuration parameters from their default values in the NFADS.resources file, use the guidelines described in the following list:

- Redefine one parameter per line.

- You must use a valid parameter key word when you are starting a new line; otherwise, the line is ignored.
- If a parameter is defined more than once, the last parameter defined is used.
- Parsing stops at the first blank line of the file.

The format to use for redefining the parameters is

```
<parameter_keyword> <new_value>
```

Define Router Aliases

The DisplayServer program includes two files used to change the information displayed by the FlowAnalyzer user interface. The files are located in the NFAServer/imported_files directory. Edit the following files to define router aliases:

- RouterAliases.txt—Allows you to define
  - — A NetFlow reporting router textual alias (used instead of an IP address)
  - — An Autonomous System (AS) number for each NetFlow reporting router
- AS.txt—Allows you to define the text associated with the AS numbers in the ASMatrix aggregation schemes.

RouterAliases.txt File

The NetFlow reporting router defined in the RouterAliases.txt file has three columns:

1. The first column contains the router's IP address in decimal-byte format (a.b.c.d).
2. The second column contains the router's identifying text that is displayed in the router list of the user interface. This column can be left blank.
3. The third column contains the NetFlow reporting router's local AS number, which is substituted for AS 0 in the ASMatrix aggregation scheme. The router's textual AS description begins with "(local)" in order to show that the substitution for AS 0 has been made.

In the RouterAliases.txt file, you can leave the router's identifying text blank (second column) and still define the router's AS number in the third column. This allows you to continue to view the router and its IP address and still have the AS 0 replacement. This also implies that you cannot use a number from 0 to 65535 as a router identifying string, unless you also provide an AS number on that line. The DisplayServer's interpretation of the RouterAliases.txt file is printed near the top of the DisplayServer's log file.

AS.txt File

The AS.txt file has two columns; the first column includes the AS number, and the second column is used to create a textual description associated with the AS number.

Collection Configuration

Run the NetFlow FlowCollector application using the GMT reference. To run the FlowCollector in this mode, you must edit the nf.resources file to uncomment the line GMT_FLAG. The GMT_FLAG parameter by default is turned on (yes). If you do not uncomment the GMT_FLAG parameter, you must use a distinct DataSetPath for each local time zone in your collection of data. There can be only one time zone for each DataSetPath directory of your FlowCollector database. For example:

```
GMT_FLAG        yes
```

The NFADisplayServer can accommodate the shift to daylight saving time and will support the locally named file for a single time zone used for each DataSetPath (Data Location). The DataSetPath is defined for each thread in your nfconfig.file and is the same as the DataLocation. The FlowCollector database may contain anomalies if you collect data from different time zones from the same DataSetPath, or if you are not running the GMT reference when daylight saving time causes the local clock to be shifted back.

The router name should always be specified in decimal byte format (a.b.c.d). This prevents ambiguity, which could cause the analysis module to miss requested data. For example, the format should be

```
171.69.204.5
```

The FlowCollector uses the dot-decimal format only in order to prevent data from the same router being stored in only one location in the FlowCollector database. For example, the format should be

```
DEV_DOTTEDADDRESS     yes
```

Use a consistent router alias. If the FlowCollector cannot find the router alias, it uses the decimal byte format, DEV_DOTTEDADDRESS. To avoid inconsistencies using router identifiers, use the DEV_DOTTEDADDRESS format.

Java Note for HP-UX

Run HP-UX Java 1.0.3, which you can access using the URL:

```
http://hpcc920.external.hp.com/gsyinternet/hpjdk/productbrief.html
```

Then select "1.0.3 Release for HP-UX 10.20 or 10.10..."

Problems can arise if you use inconsistent router identifiers of HP's 1.0.2 and 1.0.3 releases. Ensure you are running the correct version:

```
$ which java
/opt/java/bin/java
bee /tmp_mnt/home/jdoe/HPUX
$ java -version
java version "1.03.01 HP-UX 10.20: 970327"
bee /tmp_mnt/home/jdoe/HPUX
$
```

Specifically, delete any /usr/bin/java script or file, and do not refer to the /usr/java directory on your disk. If you have these references, run a clean install of HP 1.0.3 only.

Additional setup is required when you are running the DisplayServer on an HP-UX platform:

Step 1 Install the Java runtime environment, Version 1.0.2 (HP-UX Version 1.0.3), on your workstation.

Step 2 Ensure that the correct Java runtime environment is in your execution path. Use one of the following methods:

Method 1: Verify that Java is in your execution path.

```
$ which java
/opt/java/bin/java
```

Verify the Java runtime version installed.

```
$ java -version
java version “1.0.3ss:08/01/96-23:00”
```

Method 2: The shell script set_path.JAVABIN returns the correct location of the Java runtime environment. If you have performed the standard installation of Java, it is not necessary to edit the set_path.JAVAVIN file. To check the location of Java, enter

```
$ set_path.JAVABIN
/opt/java/bin/java
```

If you have installed the HP-UX version of Java in the /opt/java/bin default directory, the set_path.JAVABIN script is correct and your installation of HP-UX is complete.

If you have installed the HP-UX version of Java in a different location, you must edit the set_path.JAVABIN script file to include the location of the java executable file, which is actually a wrapper shell script named “java.”

Memory Management

You use two memory management parameters to configure the DisplayServer for your workstation and the FlowAnalyzer application:

MaxMBperCommand	280	most used on one command
MaxMB	224	size of memory pool

The MaxMBperCommand parameter is automatically truncated to MaxMB.

The memory use of DisplayServer is limited primarily by the MaxMB parameter in the NFADS.resources file. When you are tuning the memory configuration, be careful not to configure the DisplayServer to use too much memory, which would exhaust your workstation system swap space. If this does happen, the operating system might terminate the DisplayServer and cause a (possibly large) core dump in the /opt/CSCOnfa/NFAServer/bin directory. You can save time and inhibit this core dump by creating an unwritable core file in the DisplayServer bin directory. Doing so creates an unwritable core file in the NFADisplayServer directory:

```
$ rm core
$ touch core
$ chmod 444 core
```

If Java runs out of memory, the message “java.lang.OutOfMemoryError” appears in your log file. If this happens, you should stop and then restart your DisplayServer using the stop and start shell scripts provided.

Recommended Memory Setup

The following memory setup procedures are required for the Solaris and HP-UX platforms. For more information about memory setup, refer to the *Release Notes for NetFlow FlowAnalyzer Release 1.0*.

Solaris Platform

This memory setup procedure runs on the Solaris platform in normal running mode with all applications other than DisplayServer active.

Step 1 Verify the amount of available logical memory on your workstation. You can run vmstat to check your available memory. (The first line of vmstat's output is not valid.)

```
$ vmstat 5

 procs     memory            page      ...
 r b w   swap  free  re  mf pi po fr de...
 0 0 0  74312 51536   0  16 64 20 46  0...
 0 0 0 420056 223296  0   1  6  0  0  0...
 0 0 0 420056 223280  0   0  4  0  0  0...
 0 0 0 420056 223272  0   0  0  0  0  0...
 0 0 0 420056 223272  0   0  0  0  0  0...
 0 0 0 420056 223264  0   0  1  0  0  0...
...
```

The column labeled swap shows the number of kilobytes of space available. Divide this number by 1024 to calculate the amount of memory available. For example, 420056 divided by 1024 is approximately 410 MB.

```
 SWAP_AVAIL = 410 MB
```

Another method of verifying the amount of swap space available is to run the "swap -s" program. For example:

```
$ swap -s
total: 117808k bytes allocated + 60160k reserved = \
       117968k used, 550152k available
```

Step 2 Configure the DisplayServer to allow a large amount of unused memory. The largest reasonable starting value for MaxMB is

```
$ SWAP_AVAILABLE - ALLOWANCE
```

The allowance should be at least 100 MB of memory. For example, a reasonable value is

```
MaxMB = (410-100) = 310 => 224
```

The value 224 is selected because this is 32 MB less than the physical memory in the workstation. The DisplayServer program may use up to 76 MB of additional memory. A cushion of 110 MB is allowed. For example:

```
410 MB available - (224 + 76)MB = 110 MB
```

For optimum performance, keep the MaxMB below the amount of actual RAM you have in your workstation. This is particularly important if you plan to process up to the MaxMB of Detail disk data in a single command. Failure to allow for some extra physical RAM can cause disk thrashing while you are accessing the dispersed locations of data over the range of flow keys. CPU utilization can drop below 2 percent and the time to get a response to a command can be exceedingly large.

For example, on a busy ULTRA-1 with 256 MB of actual RAM, extra memory of 32 MB, and MaxMB = 224, the performance is sufficient to minimize disk thrashing.

On a moderately busy ULTRA-1, the expected performance for the DisplayServer is approximately 0.6 to 3.5 MB of disk data per second. Consequently, processing and sorting 400 MB of HostMatrix data should take about 90 seconds, and 100 MB of DetailHostMatrix could require about 90 seconds. Performance varies with the amount of paging/context switching required. If you must change the maxMB setting, it is a good idea to run vmstat 60 to monitor your swap space and activity when the DisplayServer is processing large volumes of Detail* aggregation scheme data. The perfmeter program is also useful when you are tuning for the spot of maximal processing storage capacity with minimal disk thrashing.

HP-UX Platform

This memory setup procedure runs on the HP-UX platform. The assumption here is that you have the recommended 256 MB of physical RAM and at least 350 MB of free logical memory space.

Note The HP-UX shell tools top and vmstat are not available with the NetFlow FlowAnalyzer application Version 1.0.

The MaxMB parameter in the NFADS.resources file limits the amount of memory used to store data when a command is being processed. The MaxMB value should not be more than the actual amount of physical RAM in your workstation minus 32 MB. If you have 256 MB of RAM, you should keep MaxMB less than or equal to 224 in order to minimize disk thrashing and poor performance. The recommended value for the workstation is MaxMB 224.

The workstation needs to be configured so that the DisplayServer application is allowed to use the MaxMB memory space, plus about 32 MB. The system parameter maxdsize is the kernel process limit of the amount of memory a single application is allowed to use. The recommended value is maxdsize >= (MaxMB + 32)MB. Given these calculations, the maxdsize should be configured to represent at least 256 MB on our recommended platform.

Step 1 Monitor the amount of memory used and the amount of memory remaining. Run swapinfo under root access to monitor logical memory:

```
$ swapinfo
while [ 1 ]
do
/usr/sbin/swapinfo -m
sleep 3
done
```

If you run the top program while processing a large command, you may find that the "%CPU" is small; the process may be causing disk thrashing.

In the following example, the DisplayServer process is efficiently processing several commands simultaneously:

```
$ /bin/top
System: bee                                  Mon Jun 30 14:23:56 1997
Load averages: 1.03, 0.76, 0.78
101 processes: 99 sleeping, 2 running
Cpu states:
 LOAD   USER   NICE    SYS   IDLE  BLOCK  SWAIT   INTR   SSYS
 1.03  98.0%   0.0%   2.0%   0.0%   0.0%   0.0%   0.0%   0.0%

Memory: 53456K (50940K) real, 71836K (60848K) virtual, 5228K free  Page# 1/8

 TTY   PID USERNAME  PRI NI   SIZE   RES  STATE   TIME %WCPU  %CPU COMMAND
  p4 26209 jwiggins  236 20 48156K 48220K run     2:36 97.90 97.72 java
  p7 26146 jwiggins  168 20   316K   312K sleep   0:02  0.38  0.38 top
  p8 26257 jwiggins  178 20   316K   328K run     0:00  0.40  0.38 top
   ?   859 root      154 20   432K   200K sleep   1:29  0.30  0.30 automount
... other processes ...
```

Step 2 Calculate the amount of available memory. Keep MaxMB below the amount of actual RAM you have on your workstation. This is particularly important if you plan to use a single command to process up to the MaxMB of Detail disk data. Failure to allow for some extra physical RAM will cause disk thrashing while you are accessing the dispersed locations of data over the range of flow keys.

Managing Files on Solaris

The NFADisplayServer running on a Solaris host can serve data only from the host's local disks and from valid NFS mounts to that machine. An automounter may allow your NFADisplayServer's workstation to NFS mount many shared file systems that are not really valid NFS mount points.

To obtain a list of valid NFS mount points from a NetFlow database machine, log in to the database machine and type the command **showmount -e**. For example, suppose that you have data on your_database_WS:

```
$ /usr/sbin/showmount -e
 export list for your_database_WS:
/u0                                [list_of_hosts_having_permission]
/u1                                [list_of_hosts_having_permission]
```

Any of the Solaris machines on the list_of_hosts_having_permission can run the NFADisplayServer and serve any local NetFlow data they have in addition to the your_database_WS. You can also obtain the same valid list without logging in to the database workstation by typing

```
$ /usr/sbin/showmount -e your_database_WS
```

You can expect better performance if you use file structures local to the NFADisplayServer's workstation.

File Export

The files exported from the DisplayServer through the use of the Export button are located in the exported_files directory. The location for a standard installation is

```
/opt/CSCOnfa/NFAServer/exported_files
```

Running the DisplayServer

This section describes how to start and stop the DisplayServer and check the DisplayServer's status while you are running the FlowAnalyzer on the Solaris platform.

Start the Process

To start the DisplayServer, run the start.DisplayServer shell script. The DisplayServer command starts and generates a log file of sessions.

```
$ /opt/CSCOnfa/NFAServer/bin/start.DisplayServer [server_logfile]
```

If you do not include a <server_logfile>, the filename server.out is used. If a server_logfile already exists, the log file is stored in the lowest-numbered server_logfileNUM (NUM is a nonnegative integer).

Stop the Process

To stop the DisplayServer, run the stop.DisplayServer shell script:

```
$ /opt/CSCOnfa/NFAServer/bin/stop.DisplayServer
```

Check the Status

To check the status of the DisplayServer, run the check.DisplayServer shell script:

```
$ /opt/CSCOnfa/NFAServer/bin/check.DisplayServer
```