NetFlow Preprocessor

Software Version: 3.00

HP Performance Insight 5.40

User Guide

February 2009

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Overview 9
Collecting and Processing Flow Data 9
NetFlow Preprocessor Functions 10
Sources for Additional Information 10

2 Package Installation 13
Installation Prerequisites 13
Router Configuration 13
DetailCallRecord Format 13
Collector Configuration 13
Perl Installed and Running 14
Installing the Preprocessor 14
Testing for Correct Installation 14
Package Contents 15
Removing the NetFlow Preprocessor 15

3 Preprocessor Configuration 17
Master Configuration File 17
Master Configuration File Defaults 18
Parameters in the Master Configuration File 20
Domain Lookup File 23
Protocol Lookup File 24
Application Lookup File 24
Configuring Flow Collector Applications 24
Configuring Cisco's FlowCollector 25
Configuring Cisco's FlowCollector Version 5.x and Later 25
Configuring HP's Internet Usage Manager 26

4 Troubleshooting 27
Identifying the Cisco NetFlow FlowCollector User 27
Error Messages and Warnings 27
Perl Not Installed Correctly at /usr/local/bin 31
Files in the Bin Directory Will Not Run 31
Output File Is Empty 31

Index 33

1 Overview

Tracing congestion to specific applications, servers, and clients is now easier and faster thanks to a suite of NetFlow reporting packages available from HP. This suite consists of the following products:

- NetFlow Preprocessor
- NetFlow Interface Report Pack/NetFlow Interface Datapipe
- NetFlow Global View Report Pack/NetFlow Global View Datapipe

The NetFlow Preprocessor is a prerequisite for both report packs. You will install the NetFlow Preprocessor on the same system where the flow collector application resides. You will install the report packs and datapipes on your Performance Insight server.

Collecting and Processing Flow Data

A flow is a group of packets moving between source and destination devices. The packets in this group are moving in the same direction, they share the same protocol, and they use the same transport-layer information. The traffic generated by a browser on a PC, using HTTP to request information from a web site, is one flow; the response from the web site to the PC is a second flow.

Devices that support NetFlow record data about flows and send UDP datagrams to a configured destination. The destination runs a collector application, such as Cisco's NetFlow FlowCollector or HP's Internet Usage Manager (IUM). The collector application accepts the datagram, performs decoding and aggregation, and then writes a new file in one of two formats, CallRecord format or DetailCallRecord format.

The NetFlow FlowCollector application performs these tasks:

- Receives flow statistics from Cisco devices
- Aggregates and stores data
- Produces an output file in a format (CallRecord or DetailCallRecord) defined by Cisco
- Calls the NetFlow Preprocessor when the delimited ASCII file is ready for processing

The call from the flow collector application to the NetFlow Preprocessor is possible only when the flow collector application and the NetFlow Preprocessor reside on the same system.

The NetFlow Preprocessor supports DetailCallRecord format and CallRecord format. If you are running the NetFlow Interface Report Pack, you want the collector application to output records in DetailCallRecord format. If you are running the NetFlow Global View Report Pack, you want the flow collector application to output records in CallRecord format.

Although the NetFlow Global View Datapipe will accept records in DetailCallRecord format, this format is not suitable for the NetFlow Global View Report Pack and may produce undesirable results.

2 Package Installation

This chapter covers the following topics:

- Installation prerequisites
- Installing the preprocessor
- Testing for correct installation
- Package contents
- Removing the preprocessor

Installation Prerequisites

Install the NetFlow Preprocessor on the system where the flow collector application is running. When the NetFlow Preprocessor and the flow collector application are running on the same system, the flow collector application can call the preprocessor automatically. The automatic call is not possible when the preprocessor and NetFlow FlowCollector are running on different systems. If you do not use an automatic call from the collection software, you are responsible for launching the preprocessor using some other means.

Router Configuration

The devices you want to monitor must be configured to use NetFlow. They must export NetFlow datagrams to the address and port that your collector software is configured to listen to. Refer to your hardware vendor's documentation for more information about configuring devices to export NetFlow datagrams to a particular address and port.

DetailCallRecord Format

Your flow collector application must be configured to export records in DetailCallRecord format or CallRecord format. If records are exported in any other format, the NetFlow Preprocessor will be unable to process the file, and reports will not contain any data.

Collector Configuration

It is important that you do not enable any additional processes available in the collector application that map or aggregate data. These processes will conceal data that the preprocessor needs to see. If this data is concealed, your reports will be incomplete or misleading.

3 Preprocessor Configuration

This chapter covers:

- Master configuration file
- Domain lookup files
- Protocol lookup file
- Application lookup file
- Configuring the flow collector application to call the preprocessor

Master Configuration File

The NetFlow Preprocessor includes a master configuration file. Although the parameters in this file are set to defaults, we strongly recommend that you enter information appropriate to your environment and your needs. Doing so will greatly enhance the value of the output from the preprocessor.

The master configuration file is named `netflow.cfg`. By default, it is looked for in a directory named `cfg`, below the directory where the preprocessor is installed. This file contains a list of parameter/value pairs separated by an equals sign (=). The rules are:

- Comments are supported.
- Anything following a hash mark (#) on a line is ignored.
- White space is ignored unless it is embedded in a parameter.

The default configuration contains no information about domains. If a domain is unresolvable, the value for DEFAULT will be used and all addresses will resolve to OTHER_DOMAINS. In addition, application and interface will be the only differentiating factors in DetailCallRecord files, and the only way that the data will roll up is by application and interface.

The following stipulations apply to default settings:

- At most, only the top 100 records (by total traffic) will be output.
- Only records that contribute a maximum of 90% of the total traffic will be output.
- Any aggregated flows with less than 1000 bytes per second will be ignored.

5. PROTOCOLS

Contains the name and path of the lookup file for protocols. Relative paths are relative to the directory in which the preprocessor is invoked. (See “Protocol Lookup File” later in this chapter for details about the contents of this file.) Since the numbering of protocols is much more strictly governed than ports, needing to modify protocol mappings is not likely.

6. APPLICATIONS

Contains the name and path of the lookup file for applications. Relative paths are relative to the directory in which the preprocessor is invoked. (See “Application Lookup File” later in this chapter for details about the contents of this file.) You are strongly advised to add any additional applications you have installed to the application lookup file.

7. DOMAINS

Contains the name and path of the lookup file for protocols. Relative paths are relative to the directory in which the preprocessor is invoked. (See “Domain Lookup File” later in this chapter for details about the contents of this file.) Make sure that you add domain information appropriate to your environment to the source-domain lookup file.

8. LOG

Defines the name of the file to which warning and error messages will be written. The format of error messages is consistent with PI standards; errors can be written to the standard `trend.log` file.

9. AUDIT

Defines the name of the file to which standard PI audit messages will be written. If not specified (the default), no audit records will be produced. The format of audit records is consistent with PI standards; records can be written to the standard `audit.log` file.

10. WORK

Defines the directory to which temporary files will be written. If output files are being saved locally (an FTP URL is not being used for OUT), this directory should be on the same file system as the output directory to avoid problems associated with spooling output.

11. SAVE

Defines what to do with the input data after it is processed. The options are:

SAVE=	A null value; no action is taken on input files
save=/dev/null	Input files are deleted
SAVE=<dir>	Input files are moved to the directory indicated by <dir>

The preprocessor does not manage processed input data. If you do not remove the data after processing, you must do this using some other mechanism, for example, PI’s age_files program.

4 Troubleshooting

This chapter discusses:

- Identifying the Cisco NetFlow FlowCollector user
- Error messages and warnings
- Corrective actions
- Perl not installed correctly
- Files in the bin directory will not run
- Output file is empty

Identifying the Cisco NetFlow FlowCollector User

To identify the user running NetFlow FlowCollector, run the following command:

```
ps -deaf    awk '/NFCollector/ {print $0}' -
```

You should see output similar to the following:

```
bin   498   493   0     Sep 12 ?   3:37 NFCollector
```

The user “bin” is running NetFlow FlowCollector.

Error Messages and Warnings

The following table contains a list of messages generated by the NetFlow Preprocessor. Causes and corrective actions are included where appropriate.

Message	Type	Recommended Action
Application resolution file (<file>) does not exist	FATAL	The application lookup file does not exist. Relative paths are relative to the directory from which the preprocessor is called. If the default shell script is used, paths are relative to the directory above the shell script itself. Check the setting for APPLICATIONS in the master configuration file.
Can’t open config file (<file>): <reason>	FATAL	The master configuration file could not be opened for the reason given.
Can’t open log file (<file): <reason>	FATAL	The log file could not be opened for the reason given.

Index

A

addr2name utility, 22

application lookup file, 24

APPLICATIONS, 18, 21

AUDIT, 18, 21

audit.log file, 21

automatic call of preprocessor, 9, 24

B

bin directory
- contents, 15
- files will not run, 31

C

call preprocessor automatically, 9, 24

cfg directory, 15, 17

configuration files, list of, 15

D

data flow, defined, 9

DEFAULT_APP, 18, 20

DEFAULT_DOM, 18, 20

defaults, master configuration file, 18

DetailCallRecord format, 9
- differentiating factors in files, 17

directories
- bin, 15
- cfg, 15, 17

domain, unresolvable, 17

domain lookup file, 23

DOMAINS, 18, 21

E

empty output file, 31

error messages, 27

F

flow, defined, 9

I

IANA file, 24

IGNORE option, problems with, 31

installation
- prerequisites, 13
- procedure, 14
- verifying, 14

Interface Reporting Report Pack, 10

Internet Usage Manager, 9
- configuring to call preprocessor, 26

L

LOG, 18, 21

lookup files
- application, 24
- domain, 23
- protocol, 24

M

master configuration file, 17
- editing or moving, 15
- parameters
  - details about, 20
  - listed with defaults, 18
- read/write access, 15

messages, 27

MIN_BPS, 19, 23

MIN_INTERVAL, 19, 23

N

netflow.cfg file, 17

NetFlow FlowCollector
- automatically calls preprocessor, 9
- functions of, 9
- identifying user, 27

NetFlow Global View Report Pack, 9

NetFlow Interface Report Pack, 9
netrc file, 22
nf.resources file, 25
nfc-config.xml file, 25

O

OUT, 19, 22
output, default number of records, 17
output file, empty, 31

P

package contents, 15
PASS, 19, 22
PCT_INCLUDE, 19, 23
Perl
    installed incorrectly, 31
    prerequisite for preprocessor, 14
port numbers, in IANA file, 24
PREFIX, 19, 22
preprocessor
    automatically called, 9, 24
    contents of package, 15
    functions of, 10
    installing, 14
    location of archive file, 14
    uninstalling, 15
prerequisites for installation, 13
protocol lookup file, 24
protocol numbers, 24
PROTOCOLS, 18, 21

R

removing the preprocessor, 15
report packs
    Interface Reporting, 10
resolution action parameters, 31
rules
    application lookup file, 24
    domain lookup files, 23
    protocol lookup file, 24

S

SAVE, 18, 21
shell script, 15

T

temporary files, 21
TOP_X, 19, 23
trend.log file, 21

U

uninstalling the preprocessor, 15
UNKNOWN_APP, 18, 20, 31
UNKNOWN_DOM, 18, 20, 31
USER, 19, 22

V

verifying installation, 14

W

warning messages, 27
WORK, 18, 21

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback:


invent


Java™
COMPATIBLE