HP OpenView Performance Insight

NetFlow Preprocessor 用户指南

软件版本：3.0

Reporting and Network Solutions 7.0

2004 年 11 月

法律声明

保证

对与本文档有关的内容，包括但不限于对用于任何特定目的商销性和适应性所包含的保证，惠普公司不做任何担保。对于此处包含的错误或与本书的提供、执行或使用有关的直接、间接、附带性或后果性损失，惠普公司概不负责。

可以从当地销售和服务办事处，获取适用于您的惠普产品的具体保修条款副本。

有限权利的声明

美国政府使用、复制或公开本产品，必须符合 DFARS 252.227-7013 的技术数据和计算机软件权利条款 (c)(1)(ii) 小节中提出的限制规定。

惠普公司
美国

美国国防部之外的其他政府部门和机构的权利，应符合 FAR 52.227-19(c)(1,2) 的规定。

版权声明

商标声明

OpenView 是惠普公司的美国注册商标。

Java™ 是 Sun 公司的美国商标。

Oracle® 是加利福尼亚州雷德伍德城 Oracle 公司的美国注册商标。

UNIX® 是 Open Group 的注册商标。

Windows® 和 Windows NT® 是 Microsoft 公司的美国注册商标。

支持

请访问 HP OpenView 网站：

http://www.hp.com/managementsoftware

在此可以找到联系人信息，以及有关 HP OpenView 提供的产品和服务的细节。若要访问支持网站，请单击**支持**。使用支持网站，可以实现：

- 搜索感兴趣的文档
- 查找补丁
- 提交并追踪支持案例进展
- 管理支持合同
- 查找 HP 支持联系人
- 加入与其他客户的在线讨论
- 软件培训注册

目录

1

概述

追踪特定应用程序、服务器和客户机的拥堵情况，现在变得更加轻松快捷，应当归功于来自 HP OpenView 的 NetFlow 报告包套件。此套件由下列产品组成：

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

NetFlow Preprocessor 是两个报告包的先决条件。必须将 NetFlow Preprocessor 安装在流采集器应用程序驻留的同一系统上。必须将报告包和数据管道安装在 OVPI 服务器上。

采集和处理流数据

流是在源设备和目标设备之间移动的一组包。组中的包以同样的方向移动，共享同样的协议，使用同样的传输层信息。PC 的浏览器上生成的通信流，使用 HTTP 请求来自网站的信息，就是一种流；从网站到 PC 的应答信息也是一种流。

支持 NetFlow 的设备，可以记录有关流的数据，并将 UDP 数据包发送到配置的目标。目标必须正在运行采集器应用程序，例如 Cisco 的 NetFlow FlowCollector 或 HP 的 Internet Usage Manager （IUM）。采集器应用程序接收数据包，执行解码和汇总任务，然后以下列两种格式之一书写新文件：CallRecord 格式或 DetailCallRecord 格式。

NetFlow FlowCollector 应用程序执行下列任务：

- 接收来自 Cisco 设备的流统计数据
- 汇总和存储数据
- 以 Cisco 定义的格式 （CallRecord 或 DetailCallRecord）生成输出文件
- 限定的 ASCII 文件准备就绪可以处理时，调用 NetFlow 预处理器

只有当流采集器应用程序 NetFlow Preprocessor 驻留在同一系统上时，才有可能让流采集器应用程序调用 NetFlow Preprocessor。

NetFlow Preprocessor 支持 DetailCallRecord 格式和 CallRecord 格式。如果正在运行 NetFlow 接口报告包，那么希望采集器应用程序以 DetailCallRecord 格式输出记录。如果正在运行 NetFlow Global View Report Pack，那么希望流采集器应用程序以 CallRecord 格式输出记录。

尽管 NetFlow Global View Datapipe 将接收 DetailCallRecord 格式的记录，但是这种格式却不适用于 NetFlow Global View Report Pack，可能产生不合要求的结果。

NetFlow Preprocessor 功能

NetFlow Preprocessor 处理来自采集器应用程序的数据，然后以适合 OVPI 数据管道读取的格式创建新文件。采集 NetFlow Interface Report Pack 和 NetFlow Global View Report Pack 数据的数据管道，读取新文件的内容，并填写 OVPI 数据库中的表格。

在 NetFlow Interface 报告和 NetFlow 全局视图报告中，将看到特定类型通信量的每小时、每天、每月的趋势。您将从这些报告出发响应拥堵吗？ 可能不会。对拥堵的响应可能将从 Interface Reporting Report Pack 出发，在此可以找到利用率高的具体接口。只要知道了受影响的具体接口，马上就能使用 NetFlow Interface 和 NetFlow 全局视图报告，找出正在经历拥堵的通信量类型，以及每个通信量类型的起源。

NetFlow Preprocessor 执行下列任务：

- 在由 NetFlow FlowCollector 创建的文件中过滤数据
- 执行不同的分组和汇总任务
- 匹配单向记录对，创建双向数据
- 允许对汇总数据进一步过滤
- 以下列数据管道要求的格式创建输出文件：
  - NetFlow Interface Datapipe
  - NetFlow Global View Datapipe
- 将输出文件存储在本地或远程文件系统上

过滤与汇总是可配置的，具体取决于协议、端口和地址信息。输出可以被约束到一定数量的记录、总流量的百分比或最低传输速率。有关详情，请参见第 3 章 “预处理器配置”。

更多信息来源

下列文档与本手册有关：

- 《NetFlow Preprocessor 发布声明》
- 《NetFlow Interface Report Pack 3.0 用户指南》
- 《NetFlow Global View Report Pack 2.0 用户指南》
- 《Interface Reporting Report Pack 4.6 用户指南》

- 《NetFlow FlowCollector 安装和用户指南 [Cisco]》

此列表中最后一个文档，含有关于记录格式、CallRecord 和 DetailCallRecord 的信息。

OVPI 手册和在 OVPI 上运行的报告解决方案的手册，可以从下列网站下载得到：

http://www.hp.com/managementsoftware

选择 **Support > Product Manuals**，就可以打开 **Product Manual Search** 网页。OVPI 用户指南列举在 **Performance Insight** 之下，而报告解决方案、 NNM SPI 和 NNM 采集器的用户指南列举在 **Reporting and Network Solutions** 之下。

Reporting and Network Solutions 名下的条目标明发布的年份和月份。如果手册被修订和重新公布，即使软件版本号没有变更，发布日期也会被变更。因为我们将定期发布修订的用户指南，所以在使用较老的 PDF 之前，应当搜索本网站，而较老的 PDF 可能不是可用的最新 PDF。

2

安装预处理器

本章包括下列主题：

- 安装先决条件
- 安装预处理器
- 正确安装的测试
- 包内容
- 删除预处理器

安装先决条件

将 NetFlow Preprocessor 安装在流采集器应用程序正在运行的系统上。当 NetFlow Preprocessor 与流采集器应用程序正运行在同一系统上时，流采集器应用程序可以自动调用预处理器。当预处理器与 NetFlow FlowCollector 正运行在不同的系统上时，自动调用是不可能的。如果不使用从相关软件进行自动调用，那么就要负责使用其他手段来启动预处理器。

路由器配置

希望监视的设备必须被配置为使用 NetFlow。它们必须将 NetFlow 数据包，导出到采集器软件被配置为监听的地址和端口。有关如何配置设备将 NetFlow 数据包导出到特定的地址和端口的详情，请参见硬件厂商的技术文档。

DetailCallRecord 格式

流采集器应用程序必须被配置为可以导出 DetailCallRecord 或 CallRecord 格式的记录。如果以任何其他格式导出记录，那么 NetFlow Preprocessor 将无法处理文件，报告将没有任何数据。

采集器配置

重要的是，不要启用任何其他采集器应用程序中可用的映射和汇总数据的进程。这些进程将隐藏预处理器必须看到的数据。如果这些数据被隐藏，报告就不完整或产生误导。

有关 NetFlow FlowCollector 配置的详情，请参见 Cisco 公司出版的 《NetFlow FlowCollector 安装与用户指南》。有关配置 IUM 创建 DetailCallRecord 文件的详情，请联系 HP IUM 代表。

Perl 安装与运行

Perl 5.x 是先决条件，运行预处理器之前必须被安装。Perl 是某些软件包 （例如 OVPI）和某些操作系统携带的软件。有关如何获取和安装 Perl 的详情，请访问 http://www.perl.com 或相应操作系统厂商维护的网站。对于 MS Windows，请访问：

www.activestate.com.

应当借助用户的 PATH 环境变量，使用户可以使用 Perl。不需要任何附加的 Perl 程序库或模块。对于 UNIX 系统， Perl 可执行文件 （或指向它的符号链接）应当存放为 /usr/bin/perl。

安装预处理器

NetFlow Preprocessor 提供形式是标准压缩文件格式 （“tarball”和 zip）的存档文件。需要 NetFlow Preprocessor 的所有 OVPI 包中都包含此存档文件。存档文件可以在 OVPI 系统的 Packages 目录中数据管道下的 Preprocessor 子目录找到。例如：

```
{DPIPE_HOME}/packages/Netflow_Interfaces_Datapipe/Preprocessor
```

在回顾当前 《NetFlow Preprocessor 发布声明》并了解已知问题信息之后，就可以遵循下列步骤来安装预处理器软件：

1. 如果先前进行过预处理器安装，并建立了预处理器的自动调用，那么请禁用这些调用。
2. 删除或重命名预处理器文件与 / 或目录。
3. 若要确保正确的所有权和权限应用于 UNIX 系统上的 NetFlow Preprocessor 文件，请以将运行 NetFlow FlowCollector 应用程序的相同用户身份登录到系统上。
4. 创建安装软件包的目标目录。
5. 使用 uncompress and tar 或 unzip 实用程序，将相应的存档文件 （zip 或 tar.Z）恢复到目标目录上；确保选定保留目录 / 路径名称选项。

如果必须识别正在运行 Cisco 的 NetFlow FlowCollector 的用户，请参见第 4 章 “疑难解答”。

正确安装的测试

若要验证是否正确安装 NetFlow Preprocessor，请从安装软件包的目录下运行下列命令：

```
perl bin/Netflow_PP.pl -h
```

如果 NetFlow Preprocessor 安装正确，那么将看到下列消息：

```
Usage is:

bin/NetflowPP.pl [-c <cfg_file>] -f <file>

where:

<cfg_file> is a configuration file
```

```
   <file> is a NetFlow file
The default configuration file is ./cfg/netflow.cfg.
```

如果看不到这一消息，请参见第 4 章 “疑难解答”。

包内容

安装此存档文件，将在安装目录下创建一个 bin 目录和一个 cfg 目录。bin 目录包含预处理器可执行文件、shell 脚本和批处理文件。预处理器可执行文件、shell 脚本和批处理文件必须位于同一个目录，因此不要将它们移动到不同的目录。 cfg 目录包含下列配置文件：

- 主配置文件
- 默认域查找文件
- 默认应用程序查找文件
- 默认协议查找文件

尽管存档文件采用了恰当的目录结构，如果有必要，还是可以通过编辑主配置文件，来改变默认文件地点。除此之外，通过使用命令行选项，还可以改变主配置文件自身的地点。

主配置文件可以包含明文格式的密码。若要确保密码不能被未授权用户读取，那么只有配置文件的所有者才能读或写此文件。在 UNIX 系统上，必须拥有所使用的配置文件。当文件安装时，所需的权限是默认设置的。

删除 NetFlow Preprocessor

若要卸载 NetFlow Preprocessor，请遵循下列步骤。

1. 保存已经修改过的所有配置文件。如果删除整个目录树，那么已经修改过的所有配置文件都将丢失。
2. 如果曾把流采集器应用程序配置为自动调用预处理器，请从配置文件中删除此选项。（有关详情，请参见第 3 章 “预处理器配置”。）
3. 删除或重命名通过解压缩 zip 文件所创建的文件。

3

预处理器配置

NetFlow Preprocessor 包含一个主配置文件。尽管此文件的参数是默认设置的，我们还是强烈建议您，自己输入适合环境和需要的信息。如此设置，必将大大提升预处理器输出的价值。除了主配置文件之外，本章还将介绍下列内容：

- 域查找文件
- 协议查找文件
- 应用程序查找文件
- 配置流采集器应用程序调用预处理器

主配置文件

主配置文件名称为 `netflow.cfg`。默认情况下，它位于预处理器安装目录下的 `cfg` 目录之下。此文件包含一张用等号 （=）分隔的参数 / 值对的列表。规则为：

- 支持注释功能。
- 忽略行中散列符号 （#）后面的任何内容。
- 空白也将被忽略，除非内嵌在参数内部。

默认配置没有包含有关域的信息。如果域不可解析，那么将使用 DEFAULT 值，所有地址将解析为 OTHER_DOMAINS。除此之外，应用程序和接口将是 DetailCallRecord 文件中唯一的差分因子，数据积累的唯一方式也是通过应用程序和接口。

下列约定适用于默认设置：

- 最多只输出前 100 个记录 （对于总体通信量）。
- 将只输出最大贡献值为总体通信量的 90% 的记录。
- 任何每秒小于 1000 字节的汇总流将被忽略。

主配置文件默认设置

下表提供了主配置文件中的参数列表，在适用的地方则提供了默认值。

参数	默认	描述
UNKNOWN_APP	DEFAULT	找到协议、源和目标端口的组合不能被解析为应用程序时所采取的动作。 DEFAULT = DEFAULT_APP 中使用的值 CREATE = 创建由“lowerport:higherport:protocol”构成的名称 IGNORE = 忽略此流记录
DEFAULT_APP	OTHER_APPS	当 UNKNOWN_APP 被设置为 DEFAULT 时未知应用程序所使用的值；否则忽略此参数。
UNKNOWN_DOM	DEFAULT	找到 IP 地址不能解析为域时所采取的动作。 DEFAULT = DEFAULT_DOM 中使用的值 CREATE = 从 IP 地址创建域 IGNORE = 忽略此流记录
DEFAULT_DOM	OTHER_DOMAINS	当 UNKNOWN_DOM 被设置为 DEFAULT 时未知所使用的值；否则忽略此参数。
PROTOCOLS	./cfg/protocols.cfg	协议查找文件。
APPLICATIONS	./cfg/protocols.cfg	应用程序查找文件。
DOMAINS	./cfg/domains.cfg	IP 地址域查找文件。
LOG	./netflow.log	记录错误和警告的文件。此文件可以被打开之前遇到的错误，将被指引到 STDERR。
AUDIT		书写审计日志消息的文件。如果没有指定此参数 （默认设置），就不生成审计日志消息。
WORK	./	假脱机输出的工作目录。如果输出目录位于本地系统，那么工作目录也应当位于同一文件系统。
SAVE	NULL	输出数据的保存目录。如果设置为 /dev/null，就删除输出文件；如果设置为空值 （即 SAVE= ），那么对输出文件不采取任何动作。

参数	默认	描述
OUT	./	输出目录。也可以指定目录的 FTP URL （例如 OUT=ftp://myserver/outdir）。如果此目录位于本地系统，就应当驻留于工作目录的同一文件系统 （请参见 WORK 参数条目）。如果目录采用 FTP URL 指定，那么 USER 和 PASS 参数被用来登录到远程系统上。如果没有提供上述参数，就可以使用 .netrc 文件。如果此文件不存在，就使用匿名 FTP。显而易见，目标系统必须支持 FTP 才能使用 FTP URL。也可以使用操作系统提供的共享磁盘工具，指定存在于其他服务器上的目录。
USER	匿名	在 OUT 中指定的登录到 FTP 服务器上的用户名称 （只有 OUT 是一个 FTP URL 才需要）。
PASS	< 电子邮件地址 >	在 OUT 中指定的登录到 FTP 服务器上的密码（只有 OUT 是一个 FTP URL 才需要）。
OUT-PREFIX	NETFLOW-PP	输出文件名称将把此值作为前缀。
MIN_INTERVAL	300	PERIOD 小于此值的流文件将被拒绝。 （请注意， PERIOD 的单位是分，而此参数的单位是秒。）
PCT_INCLUDE	90	此文件输出与通信量的百分比。输出按通信量进行排序 （字节为单位），只有对通信量前 X% 做贡献的记录才被输出，其中： X = PCT_INCLUDE
TOP_X	100	只有前 X 个记录被输出。如果设置为 NULL，应当输出所有记录。
MIN_BPS	1000	当表达为整个周期内每秒字节数时，汇总输出记录的总体通信量必须至少等于这个数值速率。例如，如果输入文件覆盖 15 分钟，此值被设置为 5，那么每个输出记录必须包括的总体通信量至少为 4,500 字节： （5 字节 / 秒 * 15 分钟 * 60 秒) = 4,500 字节。

主配置文件中的参数

本节提供上表列举的参数的注释。

1. UNKNOWN_APP

当端口和协议的组合不能解析为应用程序时，就采取 UNKNOWN_APP 定义的动作。它可以是：

DEFAULT	对应用程序名称赋予定义好的默认值。
CREATE	使用源端口、目标端口和协议的串联，中间用冒号（：）分隔，创建应用程序名称
IGNORE	忽略输入流记录

与预处理器一起交付的文件包含“著名”和注册的应用程序。如果已经配置的应用程序使用了特定的端口和协议，但是没有提供相关信息，那么直到在应用程序的查找文件中输入相关信息，才可以解析此应用程序。

确保应用程序查找文件包含已安装的所有其他的应用程序。

2. DEFAULT_APP

如果 UNKNOWN_APP 参数设置为 DEFAULT，此值将被赋予任何不可解析的应用程序。

3. UNKNOWN_DOM

当 IP 地址不能被解析为域时，将采取由 UNKNOWN_DOM 定义的动作。选项有：

DEFAULT	对域名称赋予定义好的默认值。
CREATE	CREATE = 从 IP 地址创建域名称
IGNORE	忽略输入流记录

与预处理器一起提交的文件没有包含域信息，因此所有地址都不可解析。确保在更改此参数之前，将域信息添加到域查找文件。

4. DEFAULT_DOM

如果 UNKNOWN_DOM 参数设置为 DEFAULT，此值将被赋予任何不可解析的域。

5. PROTOCOLS

包含协议查找文件的名称和路径。相对路径相对于调用预处理器的目录。（有关此文件的详情，请参见本章后面的“协议查找文件”。）因为协议的编号方式比端口管理更严格，所以可能不需要修改协议的映射方式。

6. APPLICATIONS

包含应用程序查找文件的名称和路径。相对路径相对于调用预处理器的目录。（有关此文件的详情，请参见本章后面的“应用程序查找文件”。）强烈建议将已经安装的任何附加应用程序添加到应用程序查找文件。

7. DOMAINS

包含协议查找文件的名称和路径。相对路径相对于调用预处理器的目录。（有关此文件的详情，请参见本章后面的 “域查找文件”。）确保将适合于所在环境的域信息，添加到源域查找文件。

8. LOG

定义将书写警告和错误消息的文件的名称。错误消息的格式与 OVPI 标准一致；错误可以写入标准 `trend.log` 文件。

9. AUDIT

定义将书写 OVPI 审计消息的文件的名称。如果没有被指定 （默认设置），将不生成审计记录。审计记录的格式与 OVPI 标准一致；记录可以写入标准 `audit.log` 文件。

10. WORK

定义临时文件将书写的目录。如果输出文件正在被保存在本地 （FTP URL 没有被用于 OUT），那么此目录应当与输出目录处于同一系统，以免出现与假脱机输出关联的问题。

11. SAVE

定义输入数据被处理之后所实施的动作。选项有：

SAVE=	空值；对输入文件不采取任何动作
save=/dev/null	输入文件被删除
SAVE=<dir>	输入文件被移动到 <dir> 标示的目录

预处理器没有管理处理过的输入数据。如果处理之后没有删除数据，就必须使用某种其他机制，例如 OVPI 的 age_files 程序，来进行管理。

12. OUT

定义输出数据将被写入的地点。地点可以是本地系统上的目录名称，地点也可以是 FTP 样式的 URL。如果 FTP 被用来将输出数据移动到其他系统，那么 USER 和 PASS 可以用来定义登录远程系统的用户名称和密码。如果 USER 和 PASS 没有被定义，就使用 .netrc 文件。如果 .netrc 文件不存在，就尝试使用匿名 FTP。无论地点是目录名称还是 URL，数据都将假脱机到临时文件之后才移动到最终目标。

输出目录的路径，不但将取决于使用的具体 NetFlow 报告包 （NetFlow Interface 或 NetFlow Global View），而且取决于是否正在使用 addr2name mapping 实用程序。OVPI 系统的默认目录为：

NetFlow Global View addr2name 输入目录：

```
{DPIPE_HOME}/data/ImportData/NetFlowGVDP_addr2name
```

NetFlow Global View Teel 源目录：

```
{DPIPE_HOME}/data/ImportData/NetFlowGVDP
```

NetFlow Interface addr2name 输入目录

```
{DPIPE_HOME}/data/ImportData/NetFlowIFDP_addr2name
```

NetFlow Interface Teel 源目录

```
{DPIPE_HOME}/data/ImportData/NetFlowIFDP
```

如果选择将数据放到 OVPI 系统的不同目录上，就必须修改数据管道的输入目录。有关修改数据管道输入目录的详情，请参见 《NetFlow Interface 和 NetFlow Global View 的用户指南》。

13. USER

如果在 OUT 中给出 FTP 样式的 URL，定义 FTP 输出到其他服务器时所使用的用户名称。

14. PASS

如果在 OUT 中给出 FTP 样式的 URL，定义 FTP 输出到其他服务器时所使用的密码。因为配置文件中以明文格式表示密码，所以必须强加一定的约束措施，以免出现可能的安全泄密事故。因为配置文件必须被运行预处理器的用户所拥有，所以只有文件的所有者才允许读写访问文件。

15. OUT-PREFIX

定义输出文件名称使用的前缀。输出文件名称创建时，将前缀、输入文件报头的 SOURCE 地址、输入文件报头的 STARTTIME 串联起来，中间用圆点分隔。只有前缀可以被指定。

16. MIN_INTERVAL

输入文件报头中 PERIOD 的值，必须大于等于 MIN_INTERVAL 值。PERIOD 的单位是分，而 MIN_INTERVAL 的单位是秒。如果 PERIOD 为 PARTIAL，那么 ENDTIME 和 STARTTIME 之间的差必须大于等于 MIN_INTERVAL。

17. PCT_INCLUDE

此文件输出与通信量的最大百分比。输出按通信量进行排序 （字节为单位），只有对通信量前 X% 做贡献的记录才被输出 （其中 X = PCT_INCLUDE）。

18.TOP_X

被输出的记录最大数。如果设置为 NULL，可以输出所有记录。

19. MIN_BPS

当表达为整个周期内每秒字节数时，汇总输出记录的总体通信量必须至少等于这个数值速率。例如，如果输入文件覆盖 15 分钟，此值被设置为 5，那么每个输出记录必须包括的总体通信量至少为 4,500 字节，具体计算如下：

```
(5 字节 / 秒 * 15 分钟 * 60 秒) = 4,500 字节
```

域查找文件

域名查找文件包含构成每个域的 IP 地址的定义。域可以包含一个或多个 IP 地址。具体规则如下：

- 支持注释功能。
- 忽略一行中符号 （#）后面的任何内容。
- 域名之前或之后的空白被忽略。
- 域名内部允许空格。

对于 IP 域，每行都由 IP 地址或 IP 地址范围组成，后面跟着由空白分隔的域名。IP 地址范围可以用两种方式定义：

- 起始地址，后跟短划线，再接结束地址，例如：

  ```
  192.168.1.2-192.168.1.254
  ```

- CIDR 块，或无类 IP 域范围，例如：

  ```
  192.168.1.2/24
  ```

强烈建议将适合于所在环境的域信息，添加到源域查找文件。

协议查找文件

以类似的方式将协议定义成 BSD 样式 /etc/protocols。提供的默认文件的内容，来源于 Internet Authority for Number Assignments (IANA) 文件 “protocol-numbers.”它包含所有注册的协议编号。具体规则为：

- 支持注释功能。
- 忽略一行中散列符号 （#）后面的任何内容。
- 空白被忽略。
- 每行由协议名称后跟协议编号组成。
- 协议编号后续可能还有若干其他字段；这些字段将被忽略。
- 一个协议编号映射到一个协议名称；它是一对一关系。
- 当一个特定协议编号有多个定义时，使用文件中的第一个定义；后续的定义将被忽略。

协议不可能被更改。默认设置适合于大多数情形。

应用程序查找文件

以类似的方式将应用程序定义成 BSD 样式 /etc/services。提供的默认文件的内容，来源于 Internet Authority for Number Assignments (IANA) 文件 “port-numbers.”它包含所有著名和注册的应用程序。具体规则为：

- 支持注释功能。

- 忽略一行中散列符号 （#）后面的任何内容。
- 空白被忽略。
- 每行由一个应用程序名称和一个端口 / 协议对构成，中间用空白分隔。
- 端口 / 协议对用反斜杠 （/）分隔。
- 与 BSD 格式不同的是，通配符 （*）可以被用作端口号。

如果安装了其他应用程序，一定要确保将它们添加到应用程序查找文件中。如果将非标准端口用于任何应用程序，那么必须定义这些端口；否则将丢失端口在报告中的可视性。

配置流采集器应用程序

本节提供配置流采集器的帮助信息。有关详情，请参见采集应用程序的软件厂商所提供的文档。有关如何配置 NetFlow 启用的设备将 NetFlow 数据包导出到采集系统的信息，请参见硬件厂商所提供的文档。

配置 Cisco 的 FlowCollector

可能需要修改若干参数，才能生成预处理器所要求的数据。

1. 查找 NetFlow 配置目录。
2. 使用文本编辑器修改 `nf.resources` 文件。
3. 确保 OUTPUT_DOTTEDADDRESS 被设置为 yes。
4. 如果正在从来自多个时区的设备采集数据，请确保 GMT_FLAG 被设置为 yes。
5. 确保 DEVICE_DOTTEDADDRESS 被设置为 yes。
6. 确保 ACCEPT_PACKETS_FROM 块被注释掉，除非希望其来源来过滤数据。
7. 如果希望只要创建数据就自动调用预处理器 （这是推荐方式），那么将 USER_SCRIPT_LOCATION 更改为 `nf2ovpi.ksh` 的完全限定名称和路径 （它可以在安装预处理器的目录下面创建的 bin 目录下找到）。
8. 保存此文件。
9. 在 `nf.resources` 文件中查找 NFC_CONFIGFILE 条目，并使用文本编辑器进行修改。
10. 确保其中有一个部分，可以包含 Aggregation DetailCallRecord （或者如果没有运行 NetFlow Interface，可以包含 Aggregation CallRecord），并插入 Period、 Port、 DataSetPath 和 MaxUsage 的值。确保将 Compression 设置为 No，将 Binary 也设置为 No。
11. 保存此文件。
12. 在 `nf.resources` 文件中查找 NFC_KNOWNPROTOCOLS 条目，并使用文本编辑器进行修改。
13. 删除或注释掉此文件的内容。
14. 保存此文件。

15 在 nf.resources 文件中查找 NFC_KNOWNSRCPORTS 条目，并使用文本编辑器进行修改。

16 删除或注释掉此文件的内容。

17 保存此文件。

18 停止并重新启动 NetFlow Collector，以便激活更改。

配置 HP 的 Internet Usage Manager

将每个路由器添加到 IUM 采集器。确保 NotifyCommand 功能被用于调用预处理器。用来调用预处理器的文件将随系统而变化。对于 UNIX，文件是一个 shell 脚本；对于 MS Windows，文件是一个批处理文件。有关如何使用 IUM 设置适合于生成 DetailCallRecord 数据的配置的详情，请与 HP IUM 代表联系。

4

疑难解答

本章主要讨论下列内容：

- 识别 Cisco NetFlow FlowCollector 用户
- 错误消息与警告
- 更正动作
- Perl 没有正确安装
- bin 目录中的文件将不能运行
- 输出文件为空

识别 Cisco NetFlow FlowCollector 用户

若要识别运行 NetFlow FlowCollector 的用户，请运行下列命令：

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

应当看到与下列内容相似的输出：

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

用户 “bin” 正在运行 NetFlow FlowCollector。

错误消息与警告

下表包含由 NetFlow Preprocessor 生成的消息列表。适当的时候，包含原因与更正动作。

消息	类型	建议动作
应用程序解析文件 (< 文件 >) 不存在	FATAL	应用程序查找文件不存在。相对路径相对于调用预处理器的目录。如果使用默认的 shell 脚本，那么路径是相对于 shell 脚本自身上面的目录。请检查主配置文件的 APPLICATIONS 设置。
不能打开配置文件 （< 文件 >）：< 原因 >	FATAL	主配置文件由于给出的原因而不能打开。
不能打开日志文件 （< 文件 >）：< 原因 >	FATAL	日志文件由于给出的原因而不能打开。
默认值必须被设置才能被赋值（DEFAULT_APP）	FATAL	找到不可解析的应用程序时所采取的动作，是赋予一个默认设置值。此默认设置尚未被 DEFAULT_APP 参数所定义。请检查主配置文件的具体设置。
默认值必须被设置才能被赋值（DEFAULT_DOM）	FATAL	找到不可解析的域时所采取的动作，是赋予一个默认设置值。此默认设置尚未被 DEFAULT_DOM 参数所定义。请检查主配置文件的具体设置。
目标目录无效 （<dir>）	FATAL	目标系统上的目标目录无效。确保目录存在，并且用户有权进行写访问。
域解析文件 (< 文件 >) 不存在	FATAL	域查找文件不存在。相对路径相对于调用预处理器的目录。如果使用默认的 shell 脚本，那么路径是相对于 shell 脚本自身上面的目录。请检查主配置文件的 DOMAIN 设置。
重复的应用程序：< 端口 > < 协议 > < 应用程序 >	警告	找到应用程序的重复定义。将使用所找到的第一个定义。将忽略此定义。
重复的域：<IP> < 域 >	警告	找到域的重复定义。将使用所找到的第一个定义。将忽略此定义。
重复的协议：< 协议名称 > < 协议编号 >	警告	找到协议的重复定义。将使用所找到的第一个定义。将忽略此定义。
无法打开应用程序文件， < 文件 > < 原因 >	FATAL	应用程序查找文件由于给出的原因而不能打开。
无法打开域文件， < 文件 >：< 原因 >	FATAL	域查找文件由于给出的原因而不能打开。
无法打开 ftp 会话 （< 原因 >）	FATAL	FTP 会话由于给出的原因而不能启动。
无法打开输入文件 （< 文件 >）：< 原因 >	FATAL	主配置文件由于给出的原因而不能打开。

消息	类型	建议动作
无法打开协议文件， < 文件 >: < 原因 >	FATAL	协议查找文件由于给出的原因而不能打开。
无法删除目标主机上现有版本的文件	FATAL	当使用 FTP 时，在远程服务器上找到输出文件的版本。此文件不能被删除。请检查下列事项：1) 为什么产生同样的输出文件？ 预处理器不应当被用来多次处理同一输入文件。2) 它为什么不能被删除？
无法将 <workfile> 移动到 <output>	FATAL	工作文件不能被移动到最终的目标目录。请检查文件和目录的权限。
无法移动输入数据进行保存 （< 文件 > < 目标 >）：< 原因 >	FATAL	输入文件不能被移动到保存目录 （正如所配置的那样）。请检查文件和目录的权限。
无法打开审计日志 （< 文件 >) < 原因 >	FATAL	审计日志文件由于给出的原因而不能打开。
无法打开工作文件 （< 文件 >）: < 原因 >	FATAL	主配置文件由于给出的原因而不能打开。
无法删除输入数据 （< 文件 >）: < 原因 >	FATAL	输入文件在处理之后不能被删除 （正如所配置的那样）。请检查文件的权限。
FTP 登录失败 （<ftp 服务器 >）	FATAL	无法登录到 FTP 服务器。最可能的原因是使用了无效的用户名称和密码。请检查主配置文件的 USER 和 PASS 设置。如果没有使用这些设置，请检查 .netrc 文件中所使用的值，或检查服务器匿名登录的可用性。
FTP put 失败 （< 原因 >）	FATAL	FTP put 由于给出的原因而失败。
FTP rename 失败	FATAL	FTP rename 失败 输出文件首先被传输到临时文件，然后重命名为最终目标。请检查目标系统的权限。
输入文件不存在 （< 文件 >）	FATAL	输入文件已被传递给预处理器，但是现在却不存在。此文件真的不存在吗？ 如果不存在，那么为什么不存在？ 请检查调用预处理器所使用的方法。其他程序是否正在访问此输入文件？
时间间隔太小 （< 时间 >， < 文件 >）	FATAL	时间间隔小于 MIN_INTERVAL 指定的间隔，文件已经被拒绝。
无效的报头字段 （< 字段 >）	FATAL	报头字段没有数值。请检查 NetFlow FlowCollector 是否以 DetailCallRecord 格式生成文件。
无效的报头记录 （< 文件 >）	FATAL	文件中的报头记录无效。请检查 NetFlow FlowCollector 是否以 DetailCallRecord 格式生成文件。
配置文件的所有者无效 （< 文件 >）:	FATAL	正在运行预处理器的用户必须拥有主配置文件。这是一个安全措施，因为此文件可能包含明文形式的密码。
配置文件的权限无效 （< 文件 >）:	FATAL	只有主配置文件的所有者才能读或写配置文件。这是一个安全措施，因为此文件可能包含明文形式的密码。

消息	类型	建议动作
UNKNOWN_APP 的值无效（< 应用程序 >）	FATAL	此参数必须是 DEFAULT、 CREATE 或 IGNORE。请检查主配置文件的 UNKNOWN_APP 和 DEFAULT_DOM 设置。
UNKNOWN_DOM 的值无效（< 域 >）	FATAL	此参数必须是 DEFAULT、 CREATE 或 IGNORE。请检查主配置文件的 UNKNOWN_DOM 和 DEFAULT_DOM 设置。
没有指定输入文件。	FATAL	没有指定输入文件。输入文件必须使用 “-f” 选项传递给预处理器。
输出目录 （< 文件 >) 不存在	FATAL	输出目录不存在。相对路径相对于调用预处理器的目录。如果使用默认的 shell 脚本，那么路径是相对于 shell 脚本自身上面的目录。请检查主配置文件的 OUT 设置。
协议解析文件 (< 文件 >) 不存在	FATAL	协议查找文件不存在。相对路径相对于调用预处理器的目录。如果使用默认的 shell 脚本，那么路径是相对于 shell 脚本自身上面的目录。请检查主配置文件的 PROTOCOLS 设置。
对于审计日志条目，记录类型必须为 1 或 2	FATAL	这种内部编码错误不应当出现。如果出现，请与 HP 技术支持人员联系。
需要的报头字段缺失 (< 文件 >)	FATAL	需要的报头字段不存在。确保 NetFlow FlowCollector 以 DetailCallRecord 格式生成文件。
保存目录 （< 文件 >) 不存在	FATAL	保存目录不存在。相对路径相对于调用预处理器的目录。如果使用默认的 shell 脚本，那么路径是相对于 shell 脚本自身上面的目录。请检查主配置文件的 SAVE 设置。
工作目录 （< 文件 >) 不存在	FATAL	工作目录不存在。相对路径相对于调用预处理器的目录。如果使用默认的 shell 脚本，那么路径是相对于 shell 脚本自身上面的目录。请检查主配置文件的 WORK 设置。

Perl 没有正确安装到 /usr/local/bin

此问题只适用于 UNIX 系统。确保可以从 `/usr/local/bin/perl` 运行 Perl。运行此命令：

```
/usr/local/bin/perl -v
```

将看到类似下列文本的消息：

```
This is Perl, v5.6.0 built for sun4-solaris

Copyright 1987-2000, Larry Wall
```

```
Perl may be copied only under the terms of either the Artistic License or the GNU
General Public License, which may be found in the Perl 5.0 source kit.

Complete documentation for Perl, including FAQ lists, should be found on this
system using `man perl' or `perldoc perl'. If you have access to the Internet,
point your browser at http://www.perl.com/, the Perl Home Page.
```

如果没有看到这一消息，那么请求系统管理员安装 Perl，并在 /usr/local/bin 目录中创建指向 Perl 可执行文件的符号链接。

Bin 目录中的文件将不运行

此问题只适用于 UNIX 系统。确保预处理器安装目录下的 bin 目录中的文件已被授予执行权限。运行此命令：

```
ls -l bin
```

应当生成与下列内容相似的输出：

```
-rwx------   1 bin      staff       18459 Jun  1 09:30 netflow_pp.pl
-rwx------   1 bin      staff         604 Jun  1 09:30 trend_nfc.ksh
```

如果正在尝试手工运行预处理器，请确保拥有相应的权限。如果希望使用 NetFlow FlowCollector 提供的 USER_SCRIPT_LOCATION 参数来调用预处理器，那么运行 NetFlow FlowCollector 的用户必须拥有执行权限。

输出文件为空

解析动作参数是 UNKNOWN_APP 和 UNKNOWN_DOM。如果两个解析动作参数的任何一个被设置为 IGNORE, 就有可能忽略整个数据文件，特别是域查找文件没有被更新以反映环境变化时更是如此。**只有**已经将应用程序和域配置为符合环境要求时，才使用 IGNORE 选项。

索引

N

O

P

S

T

U

W

X

Y

Z