

# NetFlow Analyzer

## 快速用户手册

NetFlow Analyzer 用户快速使用指南



技术支持部

本文档旨在帮助用户快速熟悉产品使用的方法。

## 目录

目录 .....	2
简介 .....	3
一、 系统安装.....	4
二、 启动 NetFlow Analyzer.....	8
三、 关闭 NetFlow Analyzer.....	10
四、 登录 NetFlow Analyzer.....	11
五、 设置接口导出 flow 包.....	12
六、 在资源清单列表中查看流量信息 .....	15
七、 分组管理.....	17
八、 告警 .....	17
产品文档.....	21

## 简介

ManageEngine NetFlow Analyzer 分析仪是一个基于 web 的流量监控工具，利用导出的 NetFlow 数据执行深入的流量分析。它支持 NetFlow、Netstream、cflowd、J-Flow、sFlow、IPFIX 等协议。

这些 Flow 协议能够提供流经某个接口的网络流量相关的详细信息。基于这些信息，NetFlow Analyzer 分析仪显示哪些应用在使用带宽，谁在使用，以及何时使用。广泛的图表和报表有助于信息分析，并加快故障诊断过程。

NetFlow Analyzer 的功能：

1. 流量分析
2. 安全分析
3. 带宽管理
4. 容量规划

## 一、 系统安装

### 1. 最小系统需求

- 2.4GHz, Pentium 4 处理器
- 4GB 内存
- 50 GB 磁盘
- 数据库 PostgreSQL ( 内置 ) MSSQL
- Windows 和 Linux

### 2. 下载安装包 ( 测试阶段推荐使用在 Windows 下安装的 64 位标准版 ) :

Windows :

<https://www.manageengine.cn/products/netflow/download.html>

下载完成后，运行下载的文件，然后按照安装画面的提示，即可完成 NetFlow 分析仪的安装。

Linux :

<https://www.manageengine.cn/products/netflow/download.html>

- 下载 BIN 文件，执行命令: `chmod a+x ManageEngine_NetFlowAnalyzer_64bit.bin` 修改文件权限
- 执行命令: `./ManageEngine_NetFlowAnalyzer_64bit.bin` ( 如果没有图形界面请加上命令 `-console` )
- 按照安装的提示进行安装

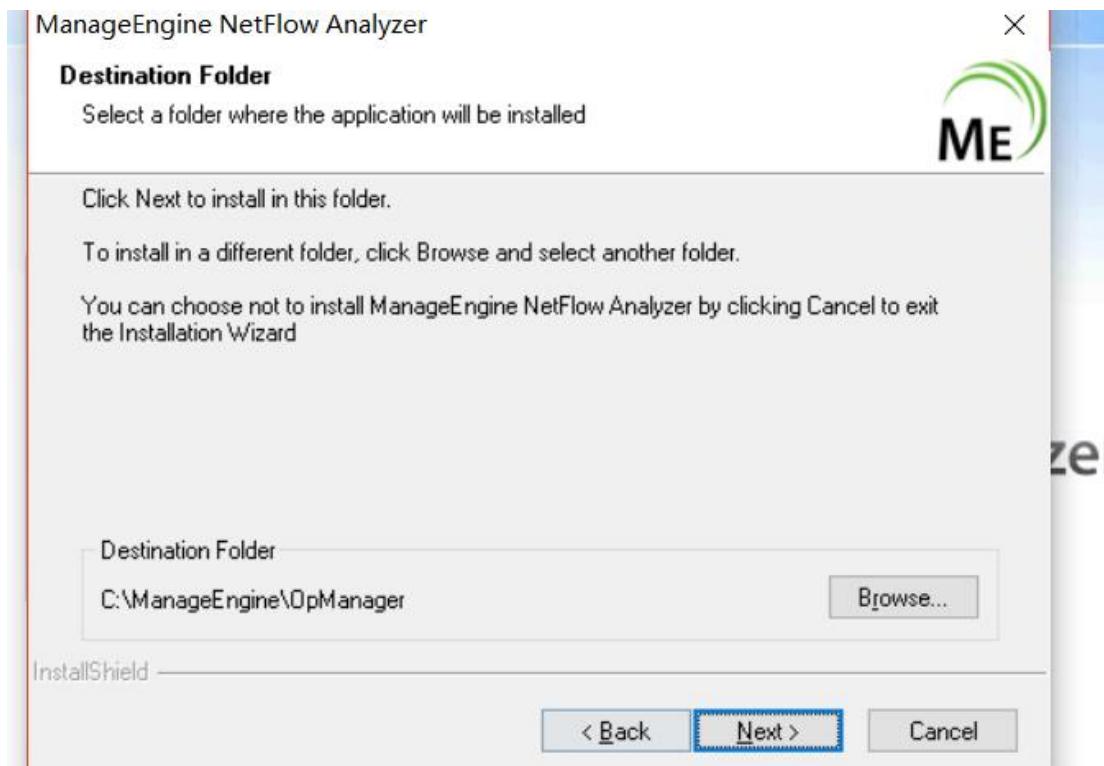
### 3. 版本选择 : NetFlow Analyzer 安装的过程中需要选择版本，默认有三种可选：

- 标准版
- 分布式版
- 高性能引擎版

Windows			Linux		
标准版	32位	64位	标准版	32位	64位
分布式版	64位		分布式版	64位	
高性能引擎	64位		高性能引擎	64位	

#### 4. 安装产品的关键步骤：

- 选择关键的路径



- 选择端口号 (一个是 web 访问端口号，一个是监听端口号 )

## ManageEngine NetFlow Analyzer

X

**Port Selection Panel**

Enter the Web Server and NetFlow Listener port



NetFlow Analyzer uses 8060 as the default web server port and 9996 as the default port to listen for NetFlow packets. If you want to run it on a different port please specify the same here

WebServer NetFlow 

InstallShield

&lt; Back

Next &gt;

Cancel

➤ 选择使用本身自带的 POSTGRESQL 还是 MSSQL 数据库。

## ManageEngine NetFlow Analyzer

X

**Select the backend database for NetFlow Analyzer**

NetFlow Analyzer supports SQL Server version 2008 and above



Click next to continue

 POSTGRESQL (Bundled with the Product) MSSQL

InstallShield

&lt; Back

Next &gt;

Cancel

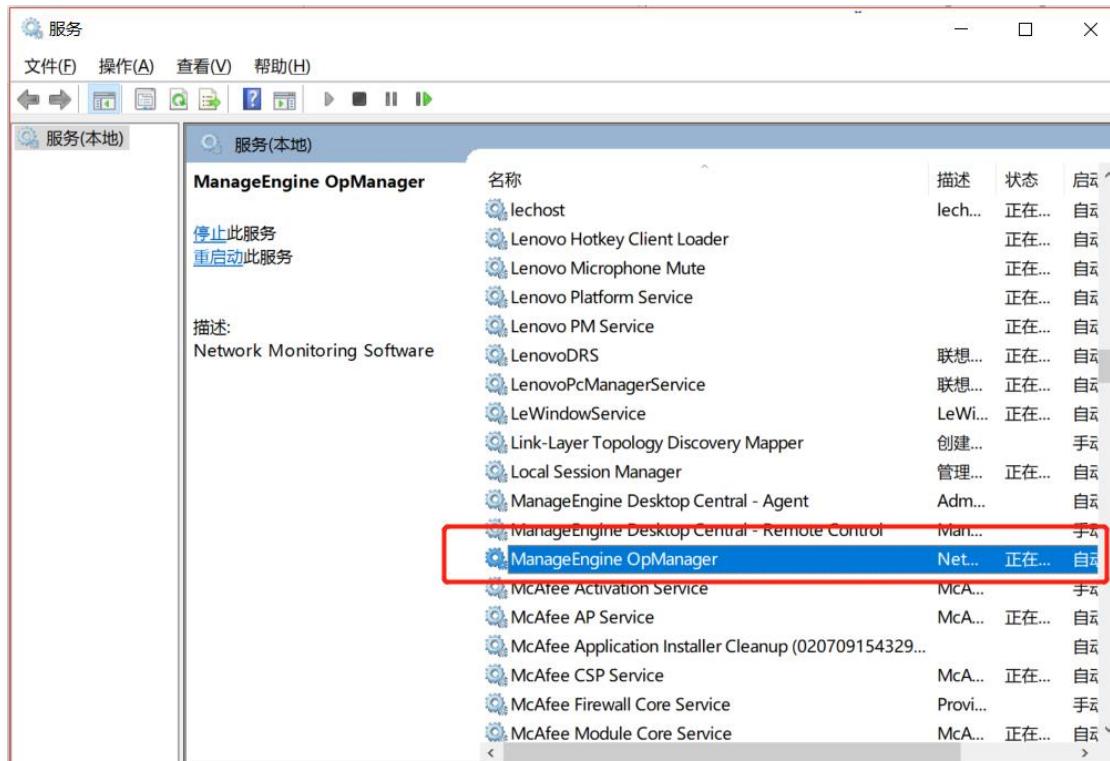
- 按照以上步骤可以安装完成。

## 二、启动 NetFlow Analyzer

NetFlow Analyzer 可以通过如下三种方式启动：

对于 Windows：

1. 桌面图标启动：双击桌面上的 NetFlow Analyzer 图标启动；
2. 服务启动：打开 windows 的服务，在服务列表中找到 “ManageEngine OpManager” 服务，打开其属性并点击 “启动”；



3. 进入到 NetFlow Analyzer 的安装根目录，进入 bin 文件夹，双击 run.bat 或者通过命令提示符运行 run.bat，在弹出如下信息后完成启动：

```

PS D:\netflow12200\OpManager\bin> .\run.bat
十二月 18, 2018 9:25:05 上午 com.adventnet.persistence.ConfigurationParser$1 resolveEntity
信息: D:\netflow12200\OpManager\bin\null\conf\customer-config.xml doesnt exists, hence it is skipped

电 Port Availability Module
80 Yes Client
13306 Yes postgres
22 Yes SSHD
69 Yes TFTP
514 Yes Syslog
=====
.
.
.
SERVER_HOME: D:\netflow12200\OpManager\bin\..
JAVA: D:\netflow12200\OpManager\bin\..\jre\bin\java
.
JAVA_OPTS: -Xms512m -Xmx1024m -XX:PermSize=128m -XX:MaxPermSize=256m -XX:+HeapDumpOnOutOfMemoryError -Dcatalina.home=D:\netflow12200\OpManager\bin\.. -Dserver.home=D:\netflow12200\OpManager\bin\.. -Djava.util.logging.config.file=D:\netflow12200\OpManager\bin\..\conf\logging.xml -Dlog.dir=D:\netflow12200\OpManager\bin\.. -Ddb.home=D:\netflow12200\OpManager\bin\..\lib -Duser.language=en -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager" -Djava.util.logging.config.file=D:\netflow12200\OpManager\bin\..\conf\logging.properties" -Duser.home=D:\netflow12200\OpManager\bin\.. -Dlogs -DStartedAsCmdPrompt="true"
.
.
.
=====
.
Check webServerPort http value : 80 https Port : null
PortCheckerUtil.getPort : serviceName :NETFLOW_LISTENER_PORT Flag : true
NFAPropfile :D:\netflow12200\OpManager\bin\..\conf\netflow\nfa.properties
PortValue is : 9996
Check for NetFlow Port with value :9996
PortCheckerUtil.checkPorts :9996

```

如果采用第三种方式启动，该命令窗口则保持当前状态，如果该窗口被关闭或者用户使用 **ctrl+c** 来中断操作，那么 NetFlow Analyzer 会自动关闭。

对于 Linux：

<NetFlow Home>/bin 目录，然后执行 **run.sh** 文件

最后启动完成的界面

```

WebService [ CREATED ]
Starting Services
StartupControllerService [ STARTED ]
CacheService [ STARTED ]
AuthenticationService [ STARTED ]
AuthorizationService [ STARTED ]
TaskEngineService [ STARTED ]
OpManagerService [ STARTED ]
WorkEngineService [ STARTED ]
ClientFrameworkService [ STARTED ]
TpTablePopulator [ STARTED ]
TemplateTablePopulator [ STARTED ]
SnmpService [ STARTED ]
CliService [ STARTED ]
NCMFTPRAService [ STARTED ]
NCMFTPService [ STARTED ]
MailService [ STARTED ]
StatusPropagationService [ STARTED ]
DiscoveryService [ STARTED ]
NCMSSHDService [ STARTED ]
ServerStartupNotify [ STARTED ]
SysLogMonitoringService [ STARTED ]
NetFlowService [ STARTED ]
OpUtilsService [ STARTED ]
DataManagement [ STARTED ]
LeaService [ STARTED ]
DService [ STARTED ]
FWASSHDService [ STARTED ]
WebService [ STARTED ]

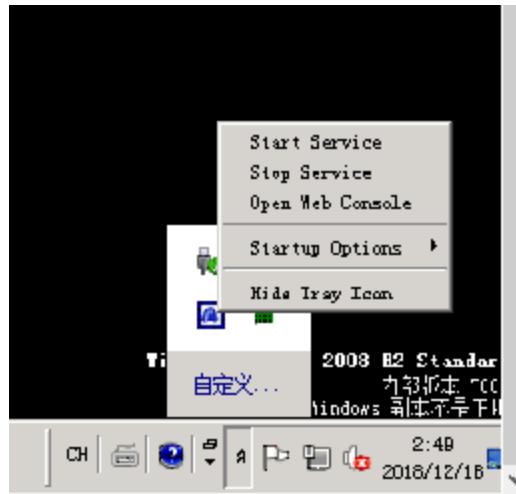
Server started in :: [487168 ms]
Connect to: [ http://localhost:8060 ]

```

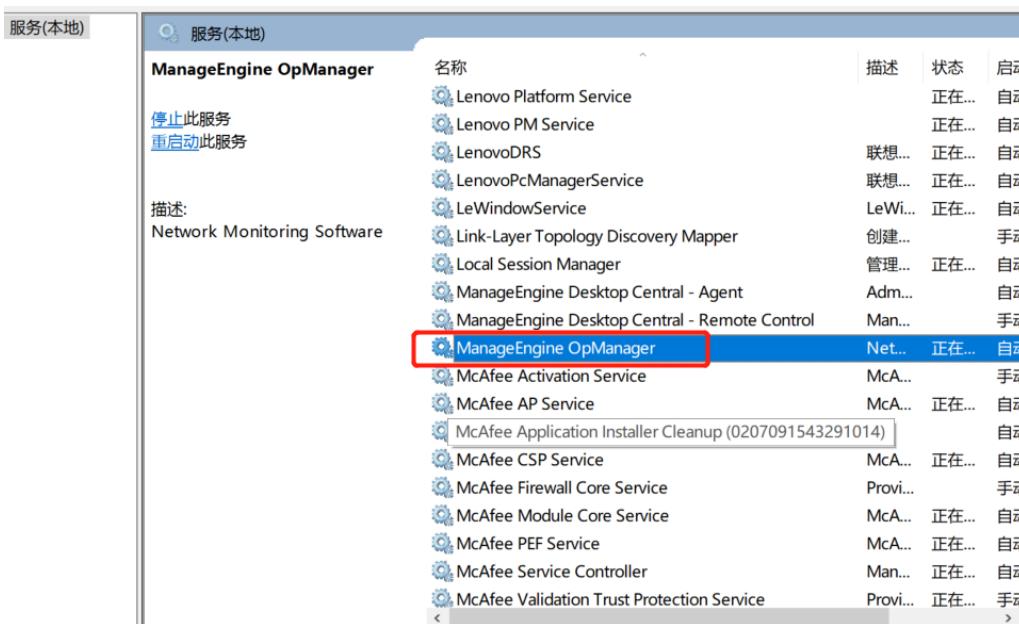
### 三、关闭 NetFlow Analyzer

NetFlow Analyzer 可以通过如下方式关闭：

1. 右击系统托盘中 NetFlow Analyzer 的图标，在弹出的选项中选择“关闭”



2. 打开 windows 系统的服务列表，关闭 NFA 的服务；



对于 Linux 系统：

<NetFlow Home>/bin 目录，然后执行 **shutdown.sh** 文件

#### 四、 登录 NetFlow Analyzer

在启动完成后用户便可以访问客户端登录 NetFlow Analyzer。NetFlow Analyzer 基于 B/S 架构开发，所以支持基于 WEB 页面的访问，所以用户可以打开浏览器，在地址栏中输入：

<http://server:port>

来访问 NetFlow Analyzer 的客户端，其中链接中的“server”是指 NetFlow Analyzer 所安装的服务器的 DNS 名称或者 IP 地址，端口就是在安装的过程中配置的 web 端口，比方说 NetFlow Analyzer 服务器的 DNS 名称叫 nfaserver，IP 地址为 192.168.1.12，web 端口使用的是 8080，那么我们可以通过访问

<http://nfaserver:8080>

或者

<http://192.168.1.12:8080>

来访问 NetFlow Analyzer 的客户端。当然，如果用户在 NetFlow Analyzer 服务器上访问 NetFlow Analyzer 的客户端，可以使用：

<http://localhost:8080>

来进行访问。

## 五、设置接口导出 flow 包

### 1. 端口设置

- Web 服务端口 : 80
- NFA 的监听端口 : 9996
- 可以自己定义

步骤 : 点击设置---再点击服务器设置



### 2. 如何配置设备输出 flow :

- 手动在设备上配置
- 使用 Network Configuration Manager
- 手动在设备上配置 : ( 华为设备为例 )

```
命令提示符

ip netstream export host 192.168.0.96 9996
ip netstream export source interface inside
ip netstream sampler fix-packet 100 inbound
ip netstream sampler fix-packet 100 outbound
ip netstream timeout active 1
ip netstream timeout inactive 15
ip netstream export version 9
ip netstream export v9-template rate 60
ip netstream template timeout 1

对于每一个接口：
interface Ethernet1/0/12
ip netstream inbound
```

## ● 使用 Network Configuration Manager 配置



使用Network Configuration Manager

添加设备 ➤ 应用凭证 ➤ 选择接口 ➤ 导出Flow

使用Network Configuration Manager的好处

- 不用在设备上输入命令
- 预定义好的配置命令模板
- 对接口进行批量设置
- 备份和还原设备配置
- 随时创建新的配置模板

选择的设备: 192.168.0.1  
 协议: TELNET - TFTP  
 选项: 主要  
 使用证书配置文件: 选择...  
 登录名称:   
 密码:   
 提示符:   
 启用用户名:   
 启用密码:   
 启用提示符: #  
 升级证书后立即备份设备

## 3. 导出 flow 后常见的问题

➤ 问题一：导出 Flow 包后，NetFlow Analyser 并没有显示数据

可能的原因：

- 1) 设备上的输出配置命令不正确
- 2) 防火墙阻断的 UDP 9996 端口

解决的方法：

- 1) 通过抓包工具 ( Wireshark ) 检查是否可以接收到 Flow 包
- 2) 检查 Windows 防火墙 , Linux 的 iptables 的设置
- 3) Flow 模板超时时间是否为 60 秒
- 4) 检查设备上的 Flow 输出配置命令
- 5) 设置活跃流的老化时间为 60 秒

➤ 问题二：我有 5 个接口，怎么少了一个接口

可能的原因：没有给那个接口配置 Flow 输出

解决的方法：

- 1) 通过抓包工具 ( Wireshark ) 检查是否可以接收到那个接口的 Flow 包
- 2) 检查 Windows 防火墙 , Linux 的 iptables 的设置
- 3) 检查外部防火墙

## 六、 在资源清单列表中查看流量信息

从设备导出 flow 后，在资源清单中可以看到以下信息：

### 1. 添加所有设备的信息

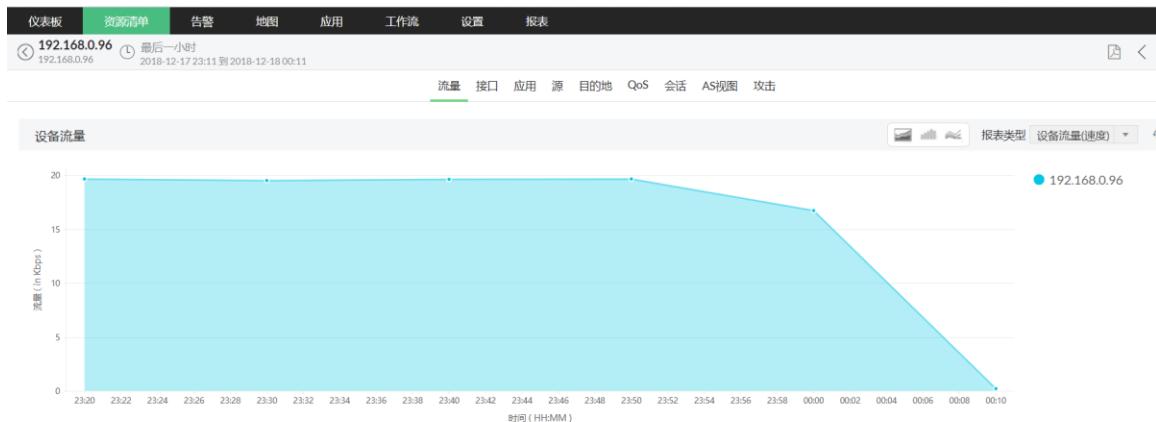
设备流量信息	接口流量信息	组流量信息
<ul style="list-style-type: none"> <li>速度</li> <li>关联的速度、流量和利用率</li> <li>应用和协议排行</li> <li>QoS排行</li> <li>源、目的和会话排行</li> <li>AS流量</li> </ul>	<ul style="list-style-type: none"> <li>按速度、流量、利用率和包数来查看</li> <li>应用和协议排行</li> <li>按DSCP和TOS的QoS排行</li> <li>源、目的、会话排行 – 可选择物理位置、网络和DNS</li> <li>SNMP/FNF NBAE、CBQoS</li> <li>组播报表</li> <li>媒体网 – 流量、RTT、包丢失</li> <li>AVC</li> </ul>	<ul style="list-style-type: none"> <li>按速度、流量、利用率和包数来查看</li> <li>关联的应用和协议</li> <li>DSCP QoS流量</li> <li>源、目的和会话</li> </ul>

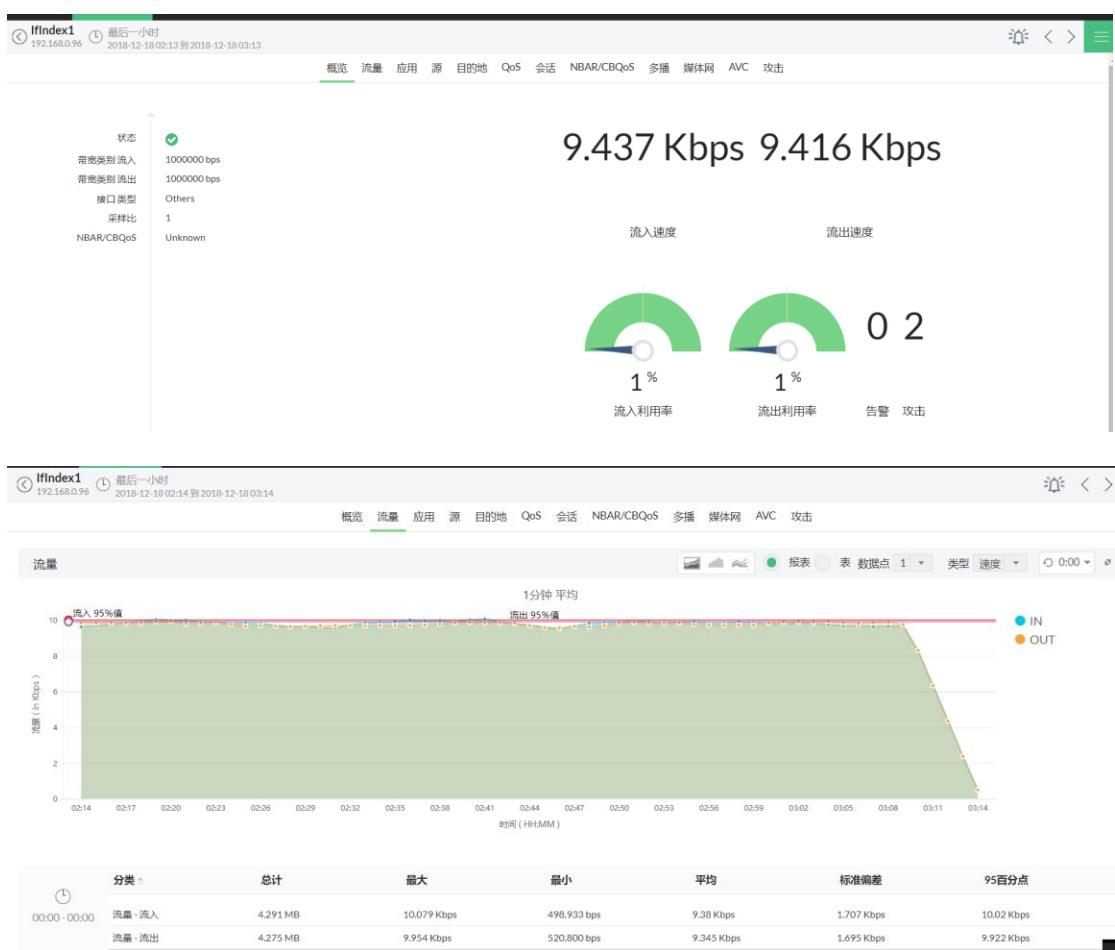
应用流量信息	QoS流量信息	WLC流量信息
<ul style="list-style-type: none"> <li>流量使用</li> <li>关联的接口</li> </ul>	<ul style="list-style-type: none"> <li>流量使用</li> <li>关联的接口</li> </ul>	<ul style="list-style-type: none"> <li>控制器的速度、流量和包数</li> <li>关联的访问点 (AP)</li> <li>应用流量</li> <li>DSCP QoS流量</li> <li>客户端IP及SSID的客户端流量信息</li> </ul>

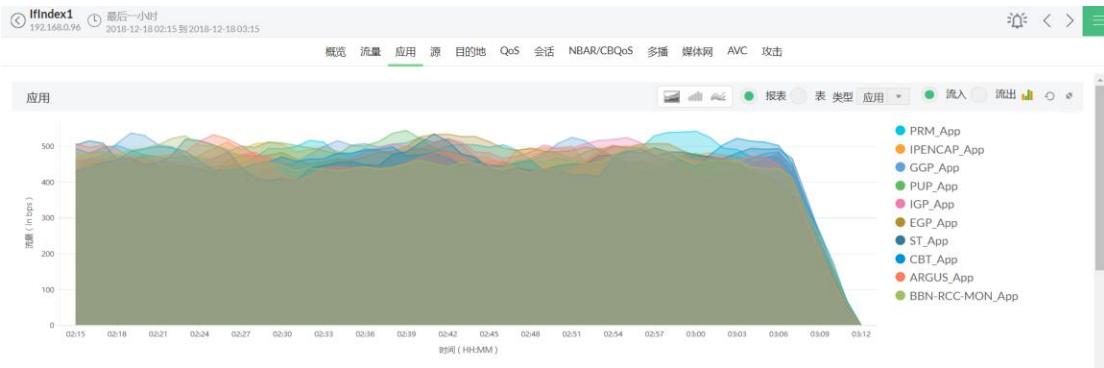
	Devices (14)	Interfaces (15)	Groups (15)	Apps (159)	QoS (32)	
	Router Name	IP Address	Type	Interface Count	Flow Count	
	▶ Data Centre AVC -IPFIX NBAR/HTTP Host	3.3.3.12	+	1	68367	
	▶ DataCenter-IPv4 ASA	3.3.3.8	■■■	1	682441	
	▶ DataCenterAVC-ART Flow	3.3.3.20	+	1	271916	
	▶ DataCenterMAINS-IPv4 ASA	3.3.3.11	■■■	1	682685	
	▶ DataCenterMAINS-IPv6 ASA	3.3.3.10	■■■	1	682443	
	▶ DataCenterMAINS-V9BASIC	3.3.3.5	+	1	683100	
	▶ DataCenterNewV9-Multicast	3.3.3.14	+	1	0	
	▶ DataCenterV9-IPv4	3.3.3.1	+	1	683599	
	▶ DatacenterV9-IPv6	3.3.3.2	+	1	683371	
	▶ DataCenterV9-Medianet	3.3.3.3	+	1	681630	
	▶ DataCenterV9-Multicast	3.3.3.6	+	1	683082	
	▶ DataCenterV9-NBAR/CBQoS	3.3.3.4	+	2	683458	

### 2. 设备流量的信息



### 3. 接口流量的信息





## 七、 分组管理

### 1. 分组的作用：

- 综合的流量分析
- 按组给操作员用户分配权限
- 为排查故障提供更好的可视化方式

### 2. 分组的方式：

- 设备
- 接口
- Ip

### 3. 分组的使用场景

- 按部门查看流量—设备或 ip 组
- VLAN 流量—接口组
- 管理客户流量—ip 分组
- 按业务管理宽带—应用分组

## 八、 告警

### 1. 内置告警 (链路断开)

- 15 分钟没有接收到 flow 包
- 5 分钟内没有 snmp 响应

### 2. 阈值告警 (通过设置阈值，当违法阈值时产生告警)

- 基于：ip 范围、ip 地址或网络、端口和协议范围、应用、DSCP

选择源:  IP组  接口组  接口

标准 定义阈值 添加

告警生成

选择全部IP组 (修改选择)

取消 下一步

➤ 告警条件：利用率、流量、速度、包数。

选择源:  IP组  标准  定义阈值  添加

告警生成

利用率  容量  速度  包

>  包  次数  分钟  要关注的  选择  None

上一步 取消 下一步

- 告警级别：严重、故障、注意
- 告警动作：邮件、短信、触发 snmp 陷阱

## 九、带宽故障排查

### 1. 配置存储数据



➤ 原始数据：从路由器接收到的每一个流都作为原始数据存储

➤ 汇聚数据：存储每十分钟的应用和会话记录。

## 2. 如何打开原始数据和汇聚数据

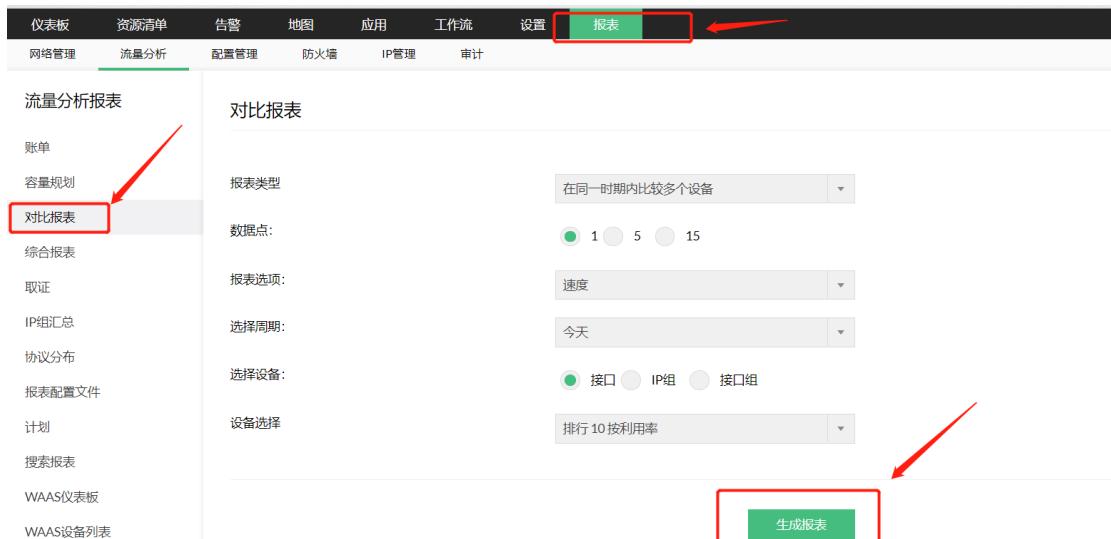


The screenshot shows the 'Raw Data' configuration page under the 'Storage' tab in the 'Settings' menu. The left sidebar lists various configuration options, with 'Storage' selected. The main area shows the 'Raw Data' tab is active. A red box highlights the 'Raw Data' tab. Another red box highlights the 'Keep Raw Data' dropdown, which is set to '1 hour'. The 'Raw Data' section also includes a table for devices that do not support raw data and a search bar for devices that do.

## 3. NetFlow Analyzer 报表

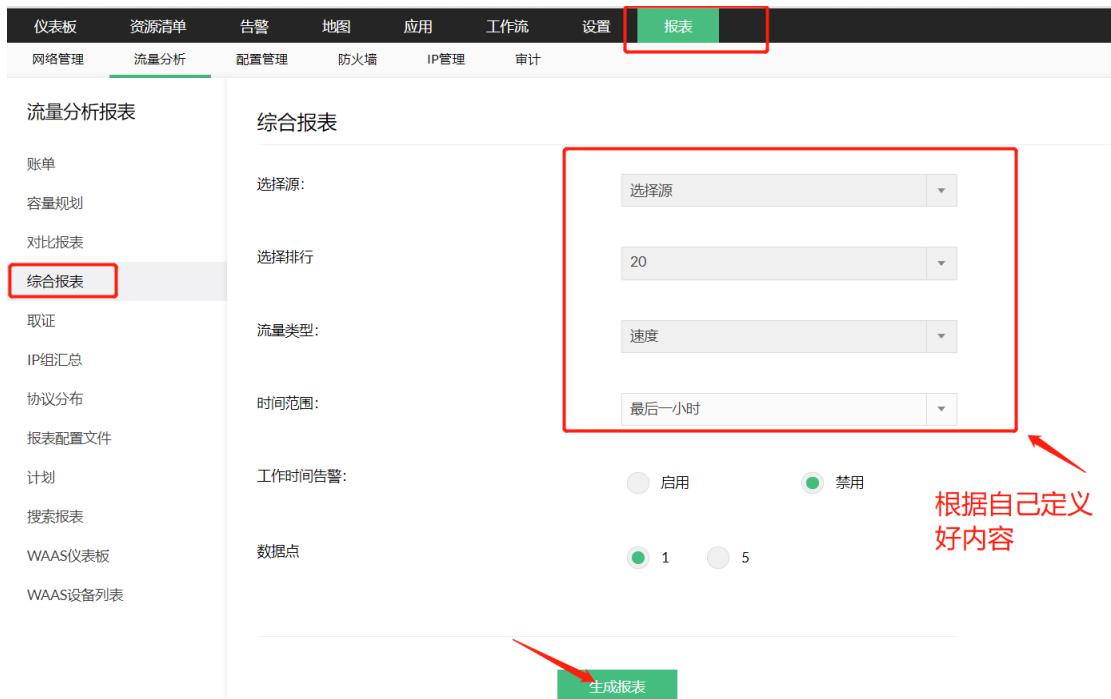
搜索/自定义报表	按照应用、协议、主机、IP搜索
对比报表	相同时段不同设备；相同设备不同时段。
综合报表	追踪流量消耗的全面信息报表
IP分组报表	IP组的综合流量信息
协议报表	按照协议来生成流量报表

1) 对比报表：既可对同一时间段内不同设备间的流量进行比较，也可以针对同一设备的不同时间段进行比较



The screenshot shows the ManageEngine interface with the '流量分析' (Traffic Analysis) tab selected. In the sidebar, the '对比报表' (Comparison Report) button is highlighted with a red box and an arrow. The main panel displays the 'Comparison Report' configuration screen, which includes fields for '报表类型' (Report Type), '数据点' (Data Points), '报表选项' (Report Options), '选择周期' (Select Period), '选择设备' (Select Device), and '设备选择' (Device Selection). The '生成报表' (Generate Report) button is also highlighted with a red box and an arrow.

2) 综合报表：了解某个接口或 IP 组的所有流量明细



仪表板 资源清单 告警 地图 应用 工作流 设置 **报表**

网络管理 流量分析 配置管理 防火墙 IP管理 审计

流量分析报表

账单 容量规划 对比报表 **综合报表** 取证 IP组汇总 协议分布 报表配置文件 计划 搜索报表 WAAS仪表板 WAAS设备列表

综合报表

选择源: 选择源

选择排行: 20

流量类型: 速度

时间范围: 最后一小时

工作时间告警:  启用  禁用

数据点:  1  5

**生成报表**

根据自己定义好内容

## 产品文档

关于更详细的说明可参见用户手册：

网站：<https://www.manageengine.cn/products/netflow/help/index.html>

在线演示：<http://demo.netflowanalyzer.com>

技术支持邮箱：[mes@zohocorp.com.cn](mailto:mes@zohocorp.com.cn)

电话：4006608680