卓豪（北京）技术有限公司

NFA 快速用户手册

NFA 用户快速使用指南

技术支持部

2013-01-14

本文档旨在帮助用户快速熟悉产品使用的方法。

目录

简介

ManageEngine™ NetFlow 分析仪是一个基于 web 的带宽监控工具，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 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 的特点：

1. 流量分析
2. 安全分析
3. 带宽管理
4. 容量规划

使用 1:系统安装

1. 最小系统需求

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

2. 下载安装包的路径：

   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：

   http://www.netflowanalyzer.com/download.html

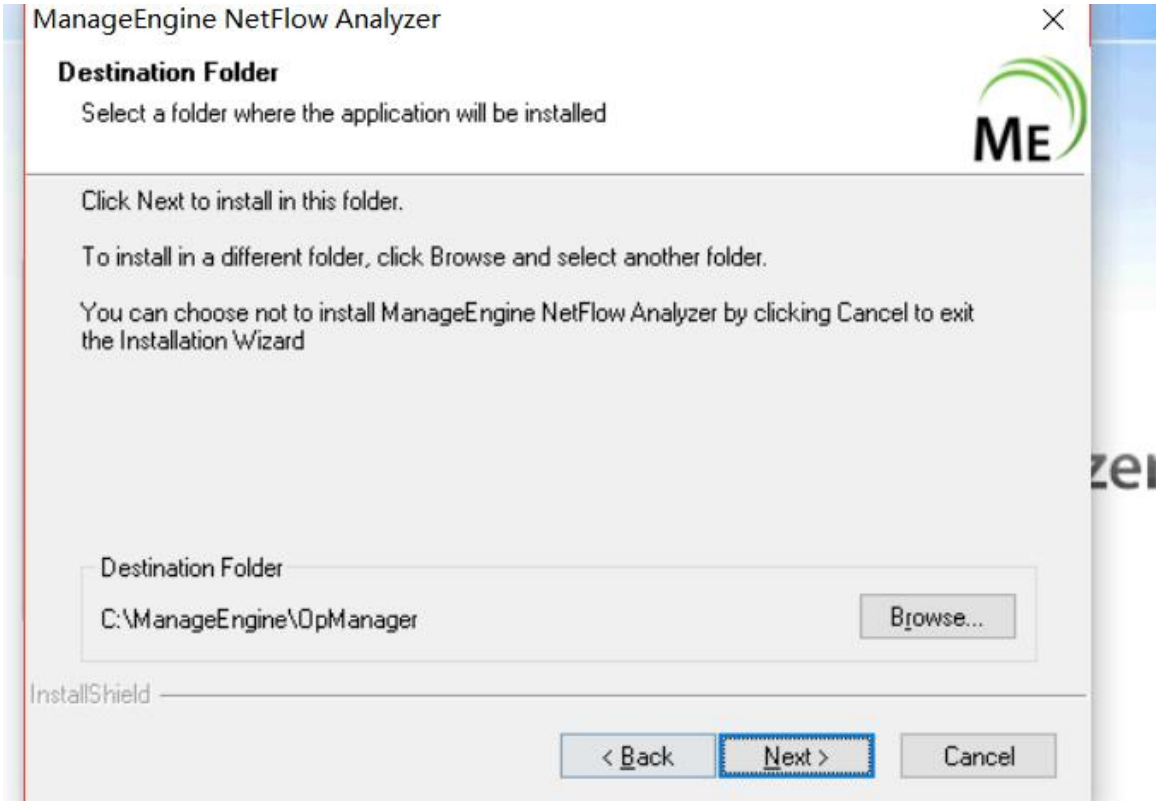
   - 下载 BIN 文件，执行命令: chmod a+x *<file_name>*.bin 修改文件权限
   - 执行命令: ./ *<file_name>*.bin -console
   - 按照安装的提示进行安装

3. 版本选择：NFA 安装的过程中需要选择版本，默认有三种可选：

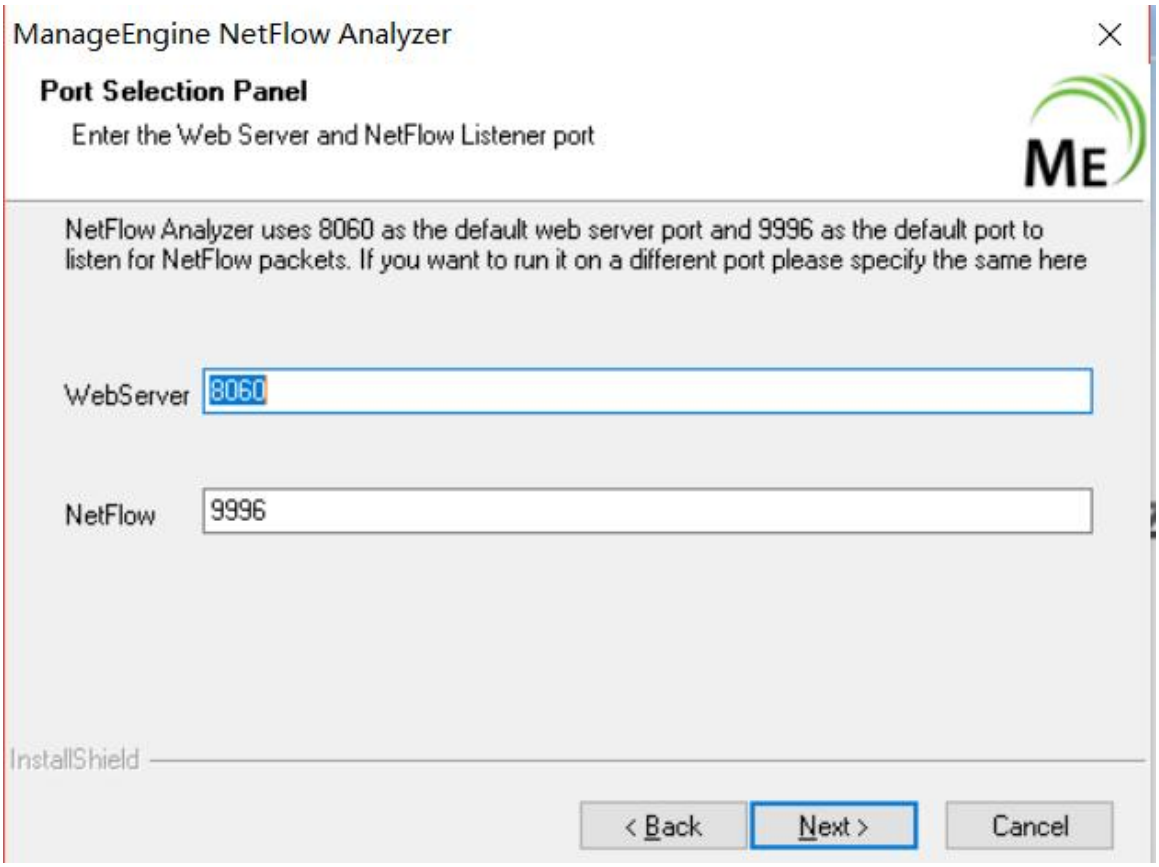
   - 标准版
   - 分布式版
   - 高性能引擎版

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	

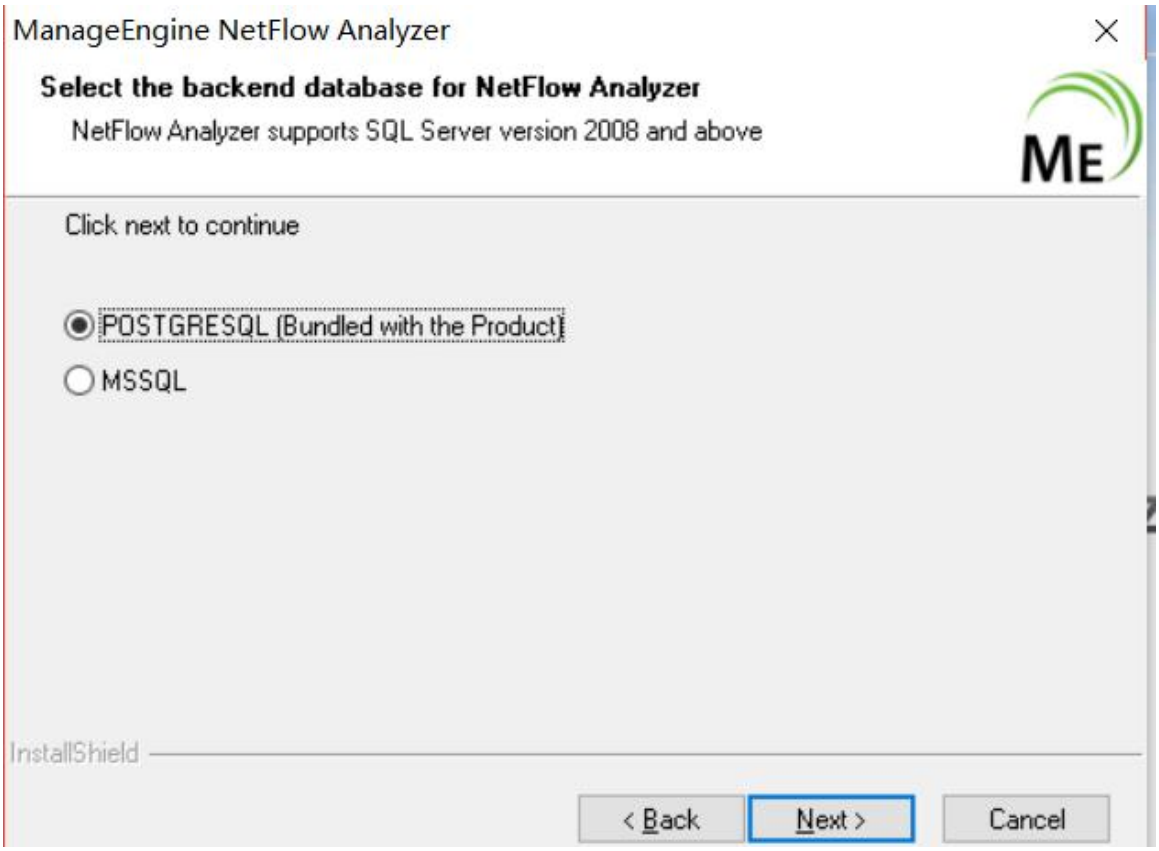
4. 选择安装的路径



5. 选择端口号



6. 选择使用本身自带的 Mysql 还是用户环境中的 MSSQL 数据库。



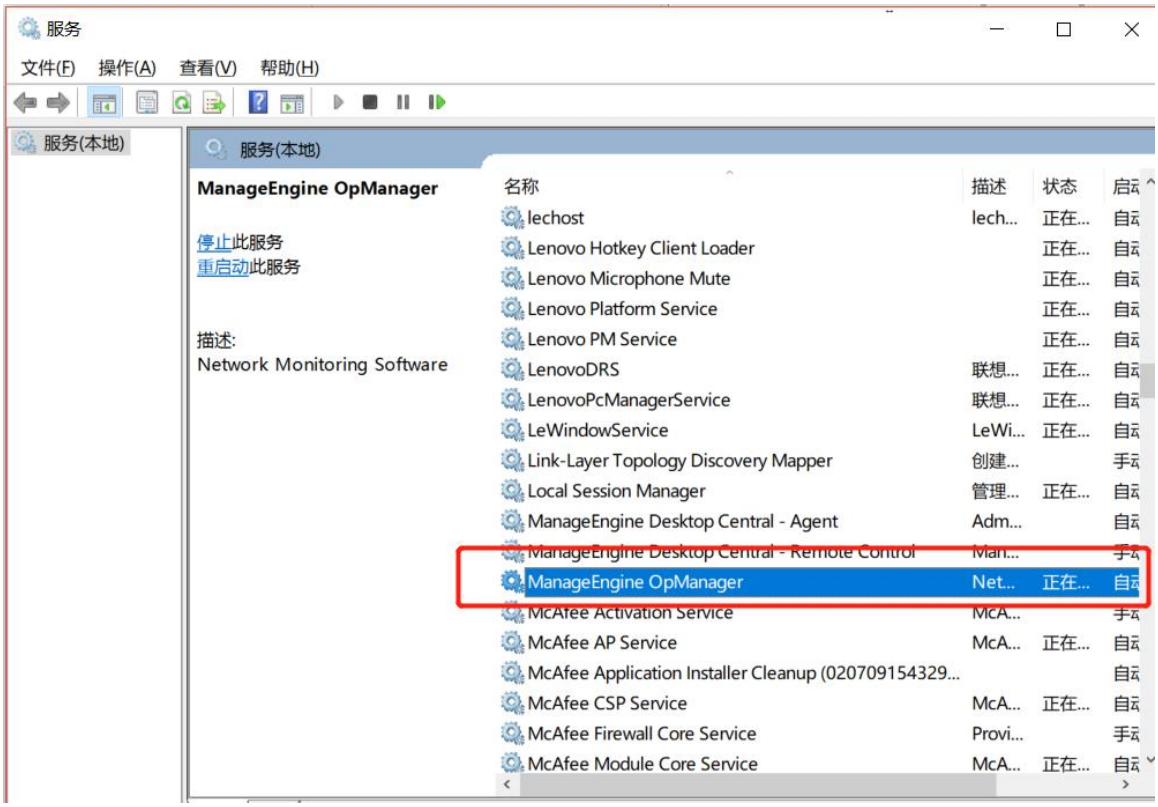
7. 以上操作完成后 NFA 便能够自行复制安装。

使用 2：启动 NFA

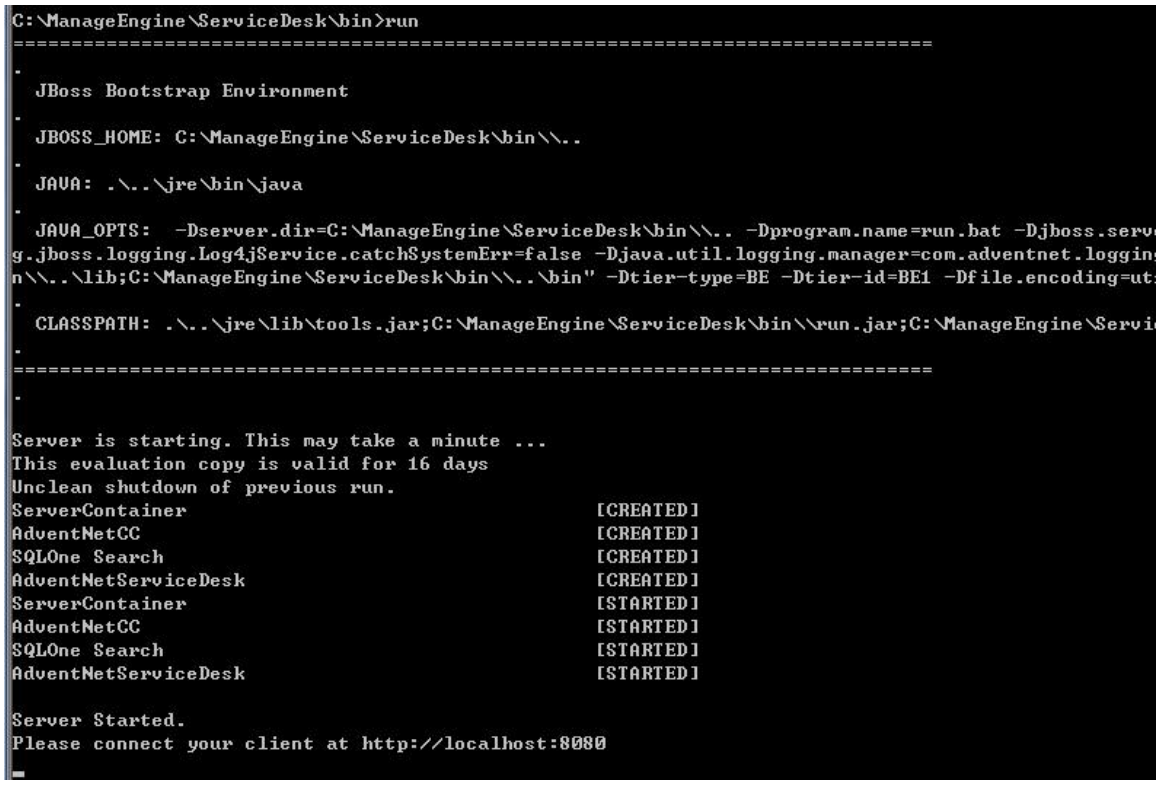
NFA 可以通过如下方式启动：

对于 Windows：

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



3. 进入到 FNA 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：

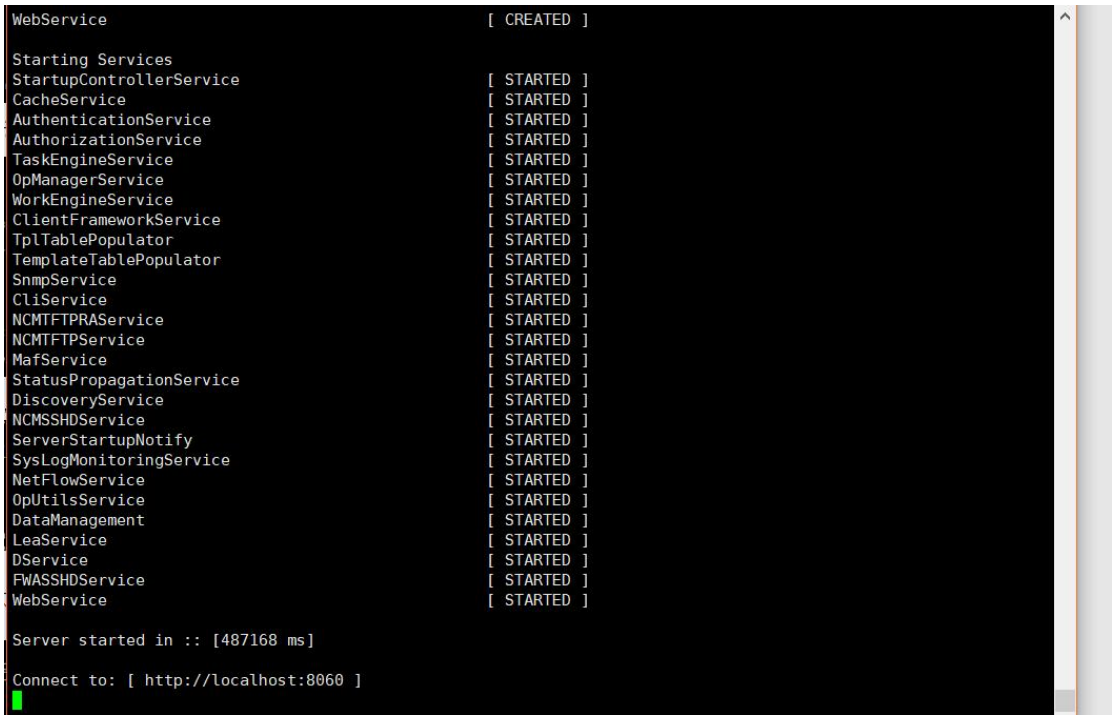


如果采用第三种方式启动，该命令窗口则保持当前状态，如果该窗口被关闭或者用户使用 ctrl+c 来中断操作，那么 NFA 会自动关闭。

对于 Linux：

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

最后安装的界面

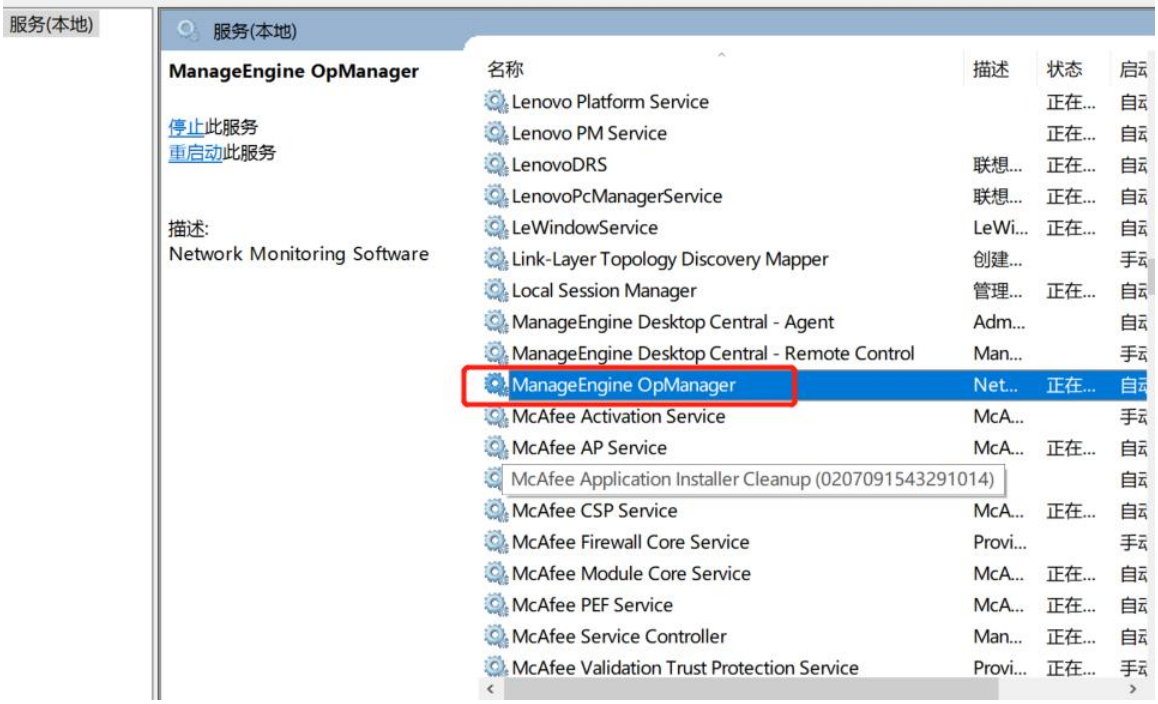

WebService [CREATED]
Starting Services
StartupControllerService [STARTED]
CacheService [STARTED]
AuthenticationService [STARTED]
AuthorizationService [STARTED]
TaskEngineService [STARTED]
OpManagerService [STARTED]
WorkEngineService [STARTED]
ClientFrameworkService [STARTED]
TplTablePopulator [STARTED]
TemplateTablePopulator [STARTED]
SnmpService [STARTED]
CliService [STARTED]
NCMTFTPRAService [STARTED]
NCMTFTPService [STARTED]
MafService [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]

使用 3：关闭 NFA

NFA 可以通过如下方式关闭：

1. 右击系统托盘中的 NFA 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

使用 4：登录 NFA

在启动完成后用户便可以访问客户端登录 NFA。NFA 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 NFA 的客户端，其中链接中的‘server’是指 NFA 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 FNA 服务器的 DNS 名称叫 sdpserver，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://sdpserver:8080

或者

http://192.168.1.12:8080

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

http://localhost:8080

来进行访问。

使用 5：设置接口导出 flow 包

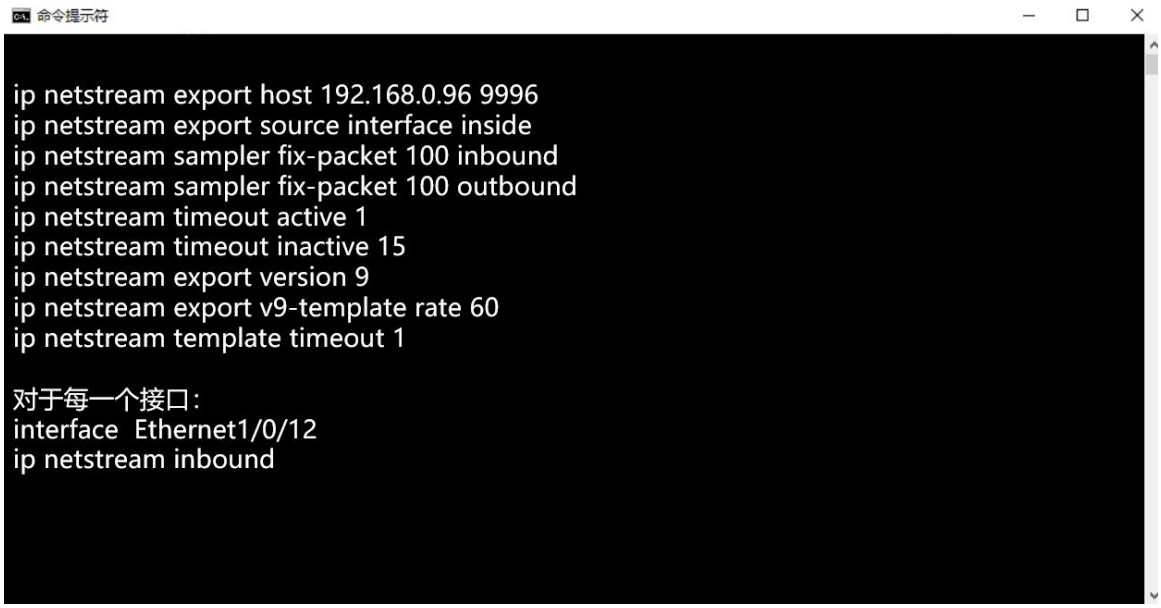
1. 端口设置

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

2. 如何配置：

    - 手动在设备上配置
    - 使用 Network Configuration Manager

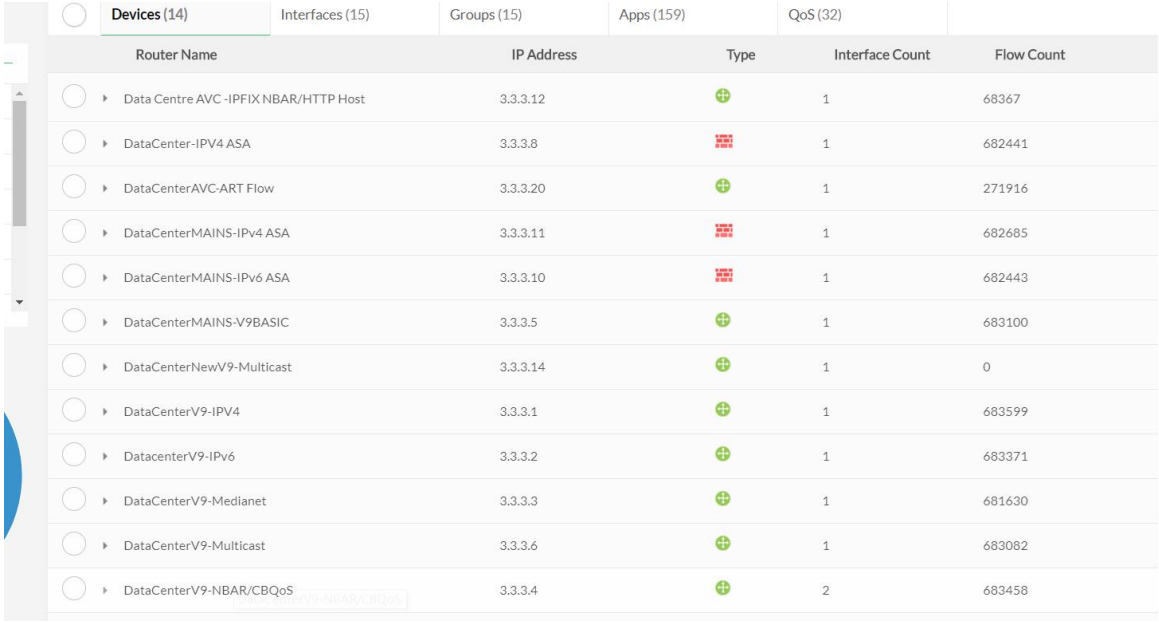
手动在设备上配置（以华为设备 NetStream 为例）：



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 Configraton 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
应用凭证
选择接口
输出流
选择的设备
192.168.0.1
协议
TELNET - TFTP
选项
主要
附加
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
ManageEngine

使用 6：在资源清单列表中查看流量信息



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

1. 资源清单的便捷使用

   - 自定义过滤器/排序
   - 编辑配置
   - 自定义视图

- 自定义搜索

2. 设备相关的定制选项

使用 7：分组管理

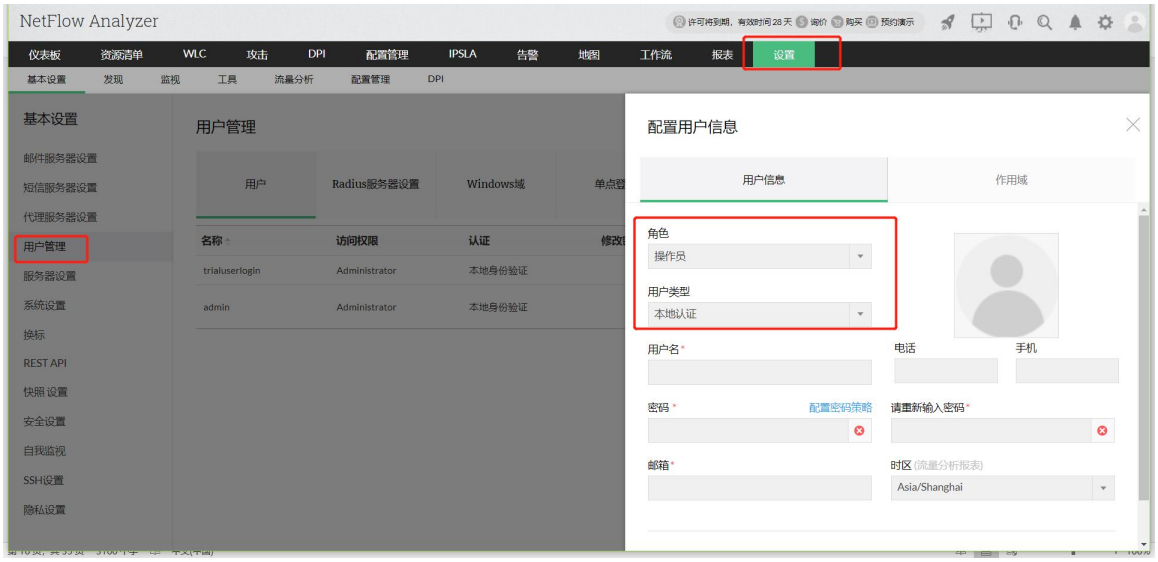
1. 分组的方式：
   - 设备
   - 接口
   - Ip
   - 应用
   - DSCP
2. 分组的作用

- 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

3. 分组的应用

- 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



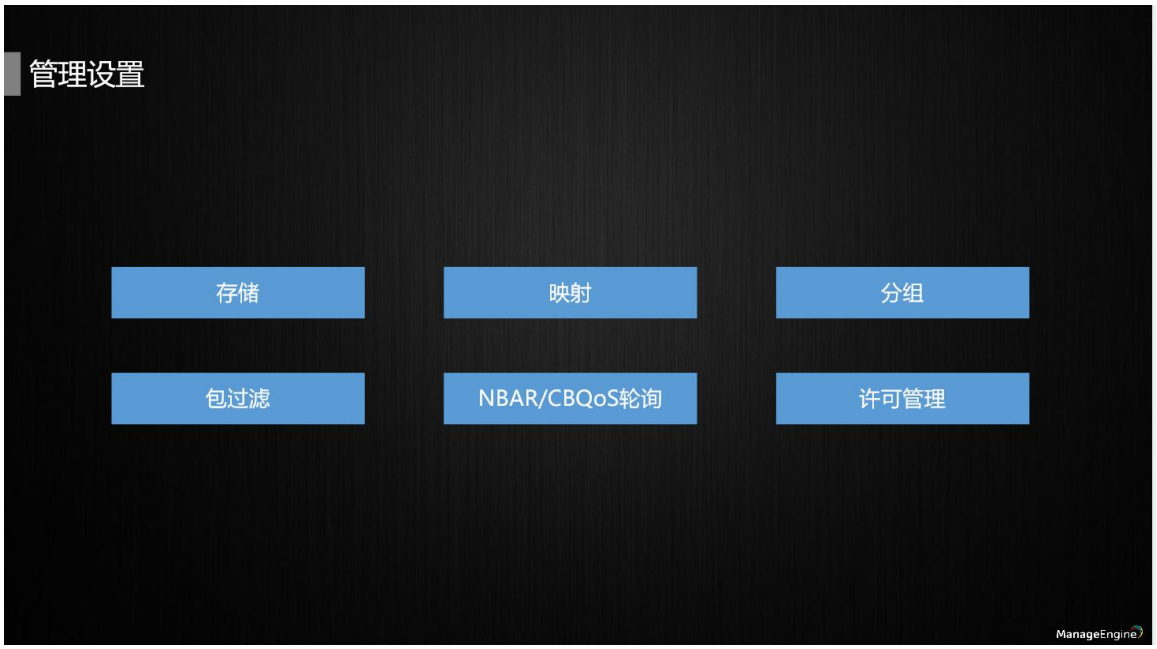
使用 8：告警

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
    - 基于：ip 范围,ip 地址或网络；端口和协议范围；应用；DSCP

- 告警条件：利用率，流量，速度，包数。

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

3. 服务器设置

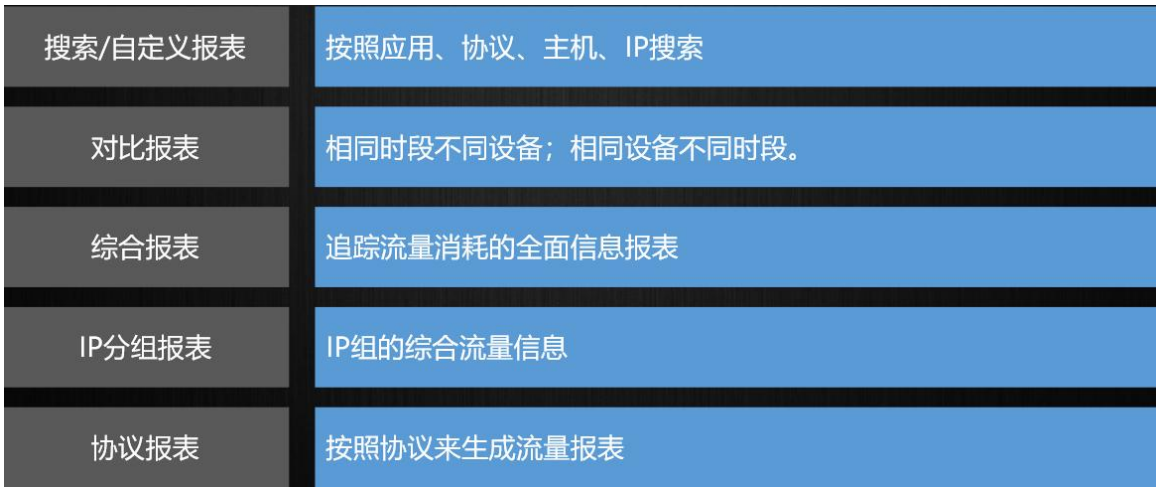


使用 9：带宽故障排查

1. 配置存储数据

2. 自定义仪表盘

3. NFA 报表和计费




NetFlow Analyzer
许可将到期，有效时间 28 天
仪表板
资源清单
WLC
攻击
DPI
配置管理
IPSLA
告警
地图
工作流
报表
设置
流量分析
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
配置管理
硬件清单报表
固件清单
设备清单
网络健康状态
设备管理状态
设备审计
启动-运行冲突
配置变更
配置变更趋势
EOL/EOS报表
合规报表
配置分析报表
DPI
取证
审计
API访问
常规

产品文档

关于更详细的说明可参见用户手册：

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