

ntopng 安装和基本使用教程

ntopng 安装和基本使用教程.....	1
1. 简介.....	3
2. 版本说明.....	4
3. 安装 influxdb.....	4
3.1. ubuntu/CentOS 安装.....	4
4. 安装 ntopng.....	5
4.1. 在 ubuntu 18.04 LTS 上安装 ntopng.....	5
4.2. 在 CentOS 上安装.....	5
4.3. 启动 ntopng.....	6
4.4. 在 windows 上安装.....	9
4.4.1. ntopng 安装.....	9
4.4.2. Redis 安装.....	13
4.4.3. 启动 ntopng.....	18
4.4.4. 设置 ntopng 服务（开机自启动）.....	20
4.4.5. 安装 influxDB(可选).....	20
5. 配置文件.....	22
6. Web GUI（ntopng Enterprise）.....	23
6.1. 登录.....	23
6.2. 仪表盘.....	23
6.3. 流量报告.....	24
6.4. 流量.....	24
6.5. 主机划分.....	26
6.6. 历史图表.....	29
6.7. 获取 license 并激活.....	31
6.8. 设置.....	31
6.8.1. 首选项.....	31
6.8.2. 数据删除.....	32
6.8.3. 流数据存储时间.....	33
6.8.4. 定义私有协议.....	33
7. 在 nprobe 上使用 ntopng 示例.....	34

7.1. nprobe 简介.....	34
7.2. 多个 nProbe 到一个 ntopng.....	35
7.3. NAT.....	36
7.4. 在同一个设备上监视某个接口流量示例.....	37
7.5. 大流量监控.....	37
7.5.1. RRS 负载均衡.....	37
7.5.2. nProbe 和 ntopng 配置.....	38
8. 在 n2disk 上使用 ntopng 示例.....	38
8.1. 流量记录简介.....	38
8.2. 启动流量记录.....	39
8.3. 下载 pacp 文件.....	39
9. 连续流量记录.....	40
10. nProbe agent 中使用 ntopng.....	41
11. 监控 Netflow/SPAN/TAP 流量.....	41
12. ntopng 时间序列和流的磁盘要求.....	42
13. 购买 license.....	43
14. 关注我们.....	43

1. 简介

ntopng 是原始 ntop 的下一代版本，ntop 是监视网络使用情况的网络流量探测器。ntopng 基于 libpcap，并且以可移植的方式编写，以便实际上可以在每个 Unix 平台，MacOSX 和 Windows 上运行。

ntopng（是的，都是小写字母）提供了直观的，加密的 Web 用户界面，用于浏览实时和历史流量信息。

主要特点如下：

- 根据多种标准对网络流量进行排序，包括 IP 地址、端口、L7 协议、吞吐量、自治系统(AS)
- 显示实时网络流量和活动主机
- 针对多个网络指标生成长期报告，包括吞吐量和应用协议
- 顶级发言人（发送者/接收者），顶级自治系统，顶级 L7 应用
- 监视并报告实时吞吐量，网络 and 应用程序延迟，往返时间（RTT），TCP 统计信息（重传，乱序数据包，数据包丢失）以及已传输的字节和数据包
- 将持久流量统计数据存储在磁盘上，以便将来进行探索和事后分析
- 在地理地图中对主机进行地理定位和叠加
- 利用 nDPI 和 ntop 深度数据包检测（DPI）技术发现应用程序协议（Facebook，YouTube，BitTorrent 等）
- 通过利用 Google 和 HTTP 黑名单提供的特征化服务来表征 HTTP 流量
- 分析 IP 流量并根据源/目的对其进行分类
- 报告 IP 协议使用情况（按协议类型分类）
- 生成 HTML5 / AJAX 网络流量统计信息
- 完全支持 IPv4 和 IPv6
- 完全的第 2 层支持(包括 ARP 统计信息)
- GTP/GRE 去隧道
- 支持 MySQL，ElasticSearch 和 LogStash 导出监控数据
- 交互式历史浏览的监控数据导出到 MySQL
- 警报引擎以捕获异常和可疑主机
- SNMP v1 / v2c 支持和连续监控 SNMP 设备
- 身份管理，包括 VPN 用户与流量的关联

2. 版本说明

ntopng 软件有四个版本：Community，Professional，Enterprise M，Enterprise L，每个版本都针对较小的版本解锁附加功能。

ntopng [产品页面](#)中提供了功能的完整列表和比较表。

- ntopng Community

社区版本是免费使用的开源软件。完整的源代码可以在 [Github](#) 上找到。

- ntopng Professional

专业版提供了一些有关社区的额外功能，这些功能对于中小企业特别有用，包括图形报告，流量配置文件和 LDAP 身份验证。

- ntopng Enterprise M

Enterprise M 版本相对于 Professional 版本提供了一些额外的功能，这些功能对于大型组织特别有用，包括 SNMP 支持，快速 MySQL 导出，高级警报管理，高性能流索引。

- ntopng Enterprise L

与 Enterprise M 版本相比，Enterprise L 版本提供了一些额外的功能，包括身份管理（使用户与流量相关联的能力）。此版本还可以解锁 n2disk 1 Gbit（连续记录）和 nProbe Pro（Flow Collection），而无需其他许可证。

3. 安装 influxdb

ntopng 支持从 InfluxDB 服务器写入和获取时间序列数据。由于数据库通信是通过网络进行的，因此服务器也可以位于外部主机上。**注意：InfluxDB 不是必须的但是建议使用，它能为你提供更好的服务。**

3.1. ubuntu/CentOS 安装

```
sudo apt-get install influxdb
```

```
sudo apt-get install influxdb-client
```

```
//设置开机启动
```

```
sudo systemctl enable influxdb
```

```
//启动
```

```
influxd
```

```
mp@ubuntu:~$ influxd
88888888      .d888 888      88888888b. 8888888b.
888      d88P" 888      888  "Y88b 888  "88b
888      888  888      888  888 888 .88P
888 888888b. 888888 888 888 888 888 888 88888888K.
888 888 "88b 888 888 888 888 Y8bd8P' 888 888 888 "Y88b
888 888 888 888 888 888 888 X88K 888 888 888 888
888 888 888 888 888 Y88b 888 .d8" "8b. 888 .d88P 888 d88P
88888888 888 888 888 888 "Y88888 888 888 88888888P" 88888888P"

2020-12-11T06:53:08.849537Z info InfluxDB starting {"log_id": "0R0927S0000", "version": "1.5.1", "branch": "1.5", "commit": "cdae4ccde4c67c3390d8ae8a1a06bd3b4cdce5c5"}
2020-12-11T06:53:08.849662Z info Go runtime {"log_id": "0R0927S0000", "version": "go1.9.2", "maxprocs": 2}
run: open server: listen: listen tcp 127.0.0.1:8088: bind: address already in use
```

安装完成后需要在 ntopng Web 界面中设置启用 influxDB

4. 安装 ntopng

4.1. 在 ubuntu 18.04 LTS 上安装 ntopng

- 安装 ntop 存储库

```
sudo apt-get install software-properties-common wget
```

```
sudo add-apt-repository universe
```

```
sudo wget http://apt-stable.ntop.org/18.04/all/apt-ntop-stable.deb
```

```
sudo apt install ./apt-ntop-stable.deb
```

注(启用 root 权限)

- 安装软件包

```
sudo apt-get clean all
```

```
sudo apt-get update
```

```
sudo apt-get install pfring-dkms nprobe ntopng n2disk cento
```

```
sudo apt-get install pfring-drivers-zc-dkms
```

4.2. 在 CentOS 上安装

- 安装库和依赖项

```
cd /etc/yum.repos.d/
```

```
wget http://packages.ntop.org/centos-stable/ntop.repo -O ntop.repo
```

- CentOS/RedHat 8

```
rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

```
rpm -ivh http://rpms.remirepo.net/enterprise/remi-release-8.rpm
```

```
yum install dnf-plugins-core
```

```
dnf config-manager --set-enabled PowerTools
```

```
dnf config-manager --set-enabled remi
```

- **CentOS/RedHat 7**

```
rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- **CentOS/RedHat 6**

```
rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm
```

```
wget https://copr.fedoraproject.org/coprs/saltstack/zeromq4/repo/epel-6/saltstack-zeromq4-epel-6.repo
```

```
rpm -ivh http://packages.ntop.org/rpm6/extra/hiredis-0.10.1-3.el6.x86_64.rpm
```

- **安装软件包**

```
yum erase zeromq3
```

```
yum clean all
```

```
yum update
```

```
yum install pfring-dkms n2disk nprobe ntopng centos
```

如果需要用 PF_RING ZC，还需安装如下驱动：

```
yum install pfring-drivers-zc-dkms
```

4.3. 启动 ntopng

- **Ubuntu/CentOS**

启动 ntopng：

```
systemctl start ntopng
```

查看启用状态：

```
systemctl status ntopng
```

```
mp@ubuntu:~$ systemctl start ntopng
mp@ubuntu:~$ systemctl status ntopng
● ntopng.service - ntopng high-speed web-based traffic monitoring and analysis t
   Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset: e
   Active: active (running) since Fri 2020-09-04 02:21:32 PDT; 2s ago
     Process: 2314 ExecStartPre=/bin/sh -c /bin/sed "/^[ ]*-e.*$\|^[ ]*-G.*$\|^[ ]*-
     Process: 2283 ExecStartPre=/bin/sh -c /usr/bin/ntopng-utils-manage-config -a c
   Main PID: 2318 (ntopng)
      Tasks: 10 (limit: 2295)
     CGroup: /system.slice/ntopng.service
             └─2318 /usr/local/bin/ntopng /run/ntopng.conf

Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [NtopPro.cpp:714] [LIQ
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:842] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:842] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:851] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:873] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:883] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:873] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:883] Adding
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [PeriodicActivities.cp
lines 1-20/20 (END)
```

以服务启动:

`systemctl enable ntopng`

关闭服务启动:

`systemctl disable ntopng`

● windows 启动

您只能从 cmd.exe 启动 ntopng 以便进行调试或处理服务设置。在这种情况下，您可以启动 cmd.exe（即 Windows 命令提示符）并导航到 ntopng 安装目录（如 C:\Program Files\ntopng）。

查看帮助: `ntopng /h`

```
D:\Program Files\ntopng>ntopng /h

Unrecognized option: /h
Available options:
/i [ntopng options] - Install ntopng as service
/c                  - Run ntopng on a console
/r                  - Deinstall the service
/h                  - Prints this help

Usage: type ntopng /c -h
```

查看命令选项和可用接口: `ntopng /c -h`


```
Usage: type ntopng /c -h

D:\Program Files\ntopng>ntopng /c -h
Starting ntopng
Running ntopng.
ntopng x64 v. 4.3.201103 - (C) 1998-20 ntop.org

Usage:
  ntopng <configuration file path>
  or
  ntopng <command line options>

Options:
[--dns-mode|-n] <mode>          DNS address resolution mode
                                0 - Decode DNS responses and resolve
                                  local numeric IPs only (default)
                                1 - Decode DNS responses and resolve all
                                  numeric IPs
                                2 - Decode DNS responses and don't
                                  resolve numeric IPs
                                3 - Don't decode DNS responses and don't
                                  resolve numeric IPs
[--interface|-i] <interface|pcap> Input interface name (numeric/symbolic),
                                view or pcap file path
[--httpdocs-dir|-1] <path>       HTTP documents root directory.
                                Default: httpdocs
[--scripts-dir|-2] <path>       Scripts directory.
                                Default: scripts
[--callbacks-dir|-3] <path>     Callbacks directory.
```

在最后页面最后可以查看可用接口序号：

```
Available interfaces (-i <interface index>):
  1. Microsoft
     {B1C9C693-BE3D-4BF9-A4AB-CBC8C7B387B1}
  2. VMware Virtual Ethernet Adapter
     {3AE92A11-6407-4EDD-9E06-262DA14C2A21}
  3. Microsoft
     {8E00BEA2-66EF-43EA-B213-BE51D9C45A50}
  4. Microsoft
     {D8CEB99A-0DAE-4786-85B4-E50BCD872C03}
  5. VMware Virtual Ethernet Adapter
     {9A3172A6-D5DD-4A25-BA65-539EF8B569B4}
  6. Microsoft
     {61392BE8-9B8C-40E1-B935-0BEAB3D35C52}
```

打开特定接口： `ntopng /c -i 2`


```
D:\Program Files\ntopng>ntopng /c -i 1
Starting ntopng
Running ntopng.
11/Dec/2020 15:57:46 [Ntop.cpp:2336] Setting local networks to 127.0.0.0/8, fe80::/10
11/Dec/2020 15:57:46 [Redis.cpp:162] Successfully connected to redis 127.0.0.1@0
11/Dec/2020 15:57:46 [Redis.cpp:162] Successfully connected to redis 127.0.0.1@0
11/Dec/2020 15:57:46 [NtopPro.cpp:297] [LICENSE] Reading license from Redis
11/Dec/2020 15:57:46 [NtopPro.cpp:425] [LICENSE] Unable to validate license [Empty license file]
11/Dec/2020 15:57:46 [NtopPro.cpp:493] WARNING: [LICENSE] Invalid license [Empty license file]
11/Dec/2020 15:57:46 [NtopPro.cpp:510] WARNING: [LICENSE] ntopng will now run in Enterprise L edition for 10 minutes
11/Dec/2020 15:57:46 [NtopPro.cpp:512] WARNING: [LICENSE] before returning to community mode
11/Dec/2020 15:57:46 [NtopPro.cpp:514] WARNING: [LICENSE] You can buy a permanent license at http://shop.ntop.org
11/Dec/2020 15:57:46 [NtopPro.cpp:516] WARNING: [LICENSE] or run ntopng in community mode starting
11/Dec/2020 15:57:46 [NtopPro.cpp:517] WARNING: [LICENSE] ntopng --community
11/Dec/2020 15:57:46 [PcapInterface.cpp:93] Reading packets from 1 [id: 1]
```

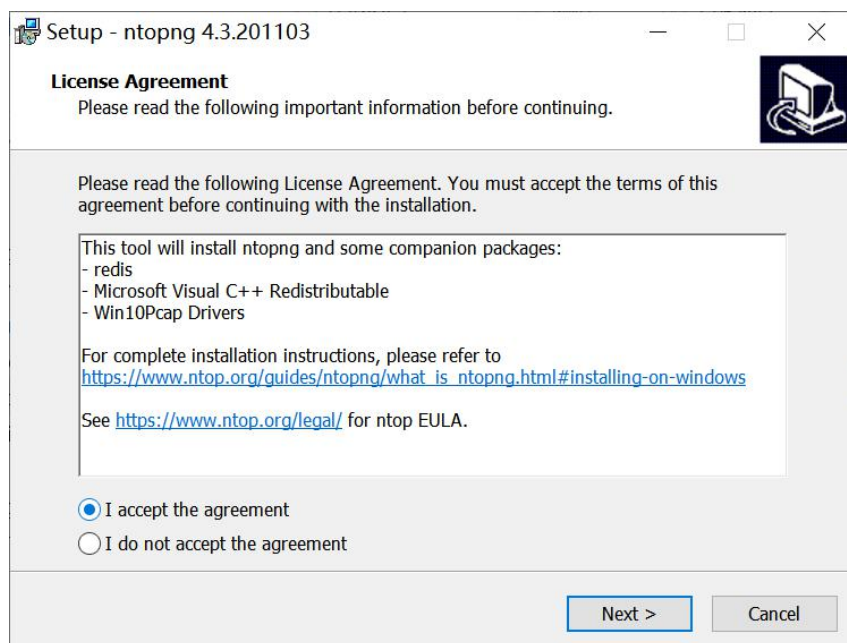
4.4. 在 windows 上安装

windows 安装参照：https://www.ntop.org/guides/ntopng/what_is_ntopng.html#installing-on-windows

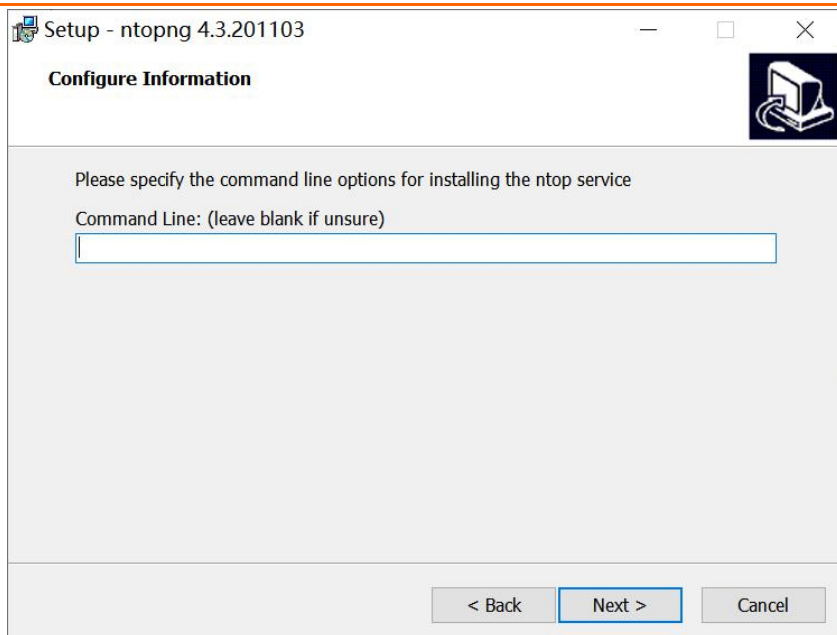
4.4.1. ntopng 安装

在压缩包中找到 ntopng 安装包或者自行下载安装。下载地址：[ntopng](https://www.ntop.org/guides/ntopng/what_is_ntopng.html#installing-on-windows)

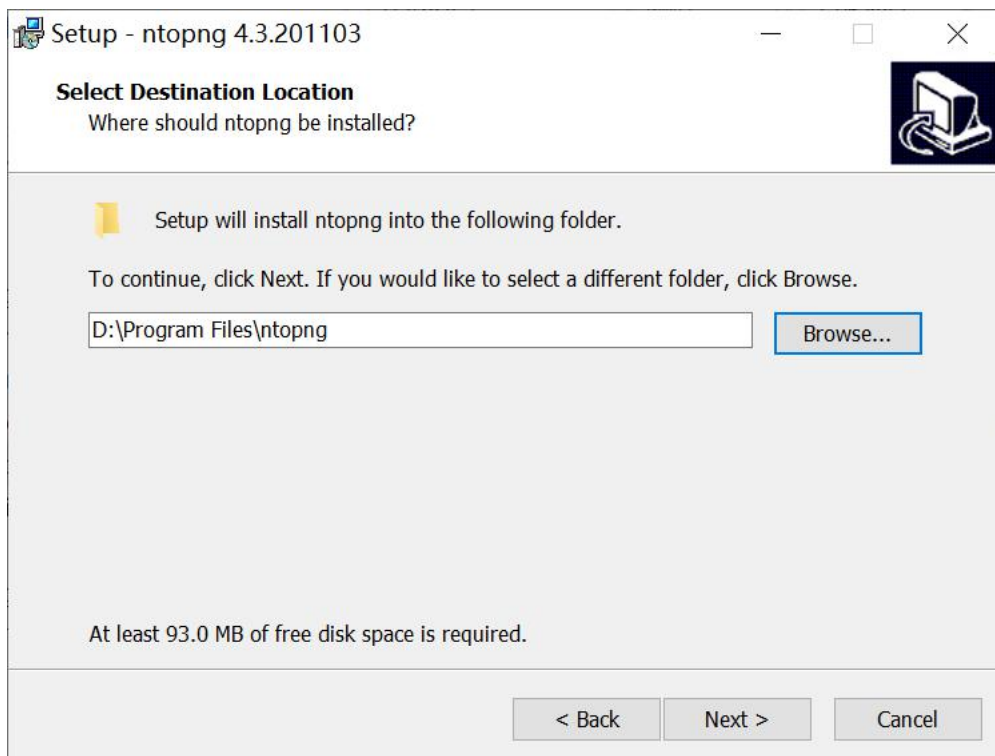
(1) 接收协议

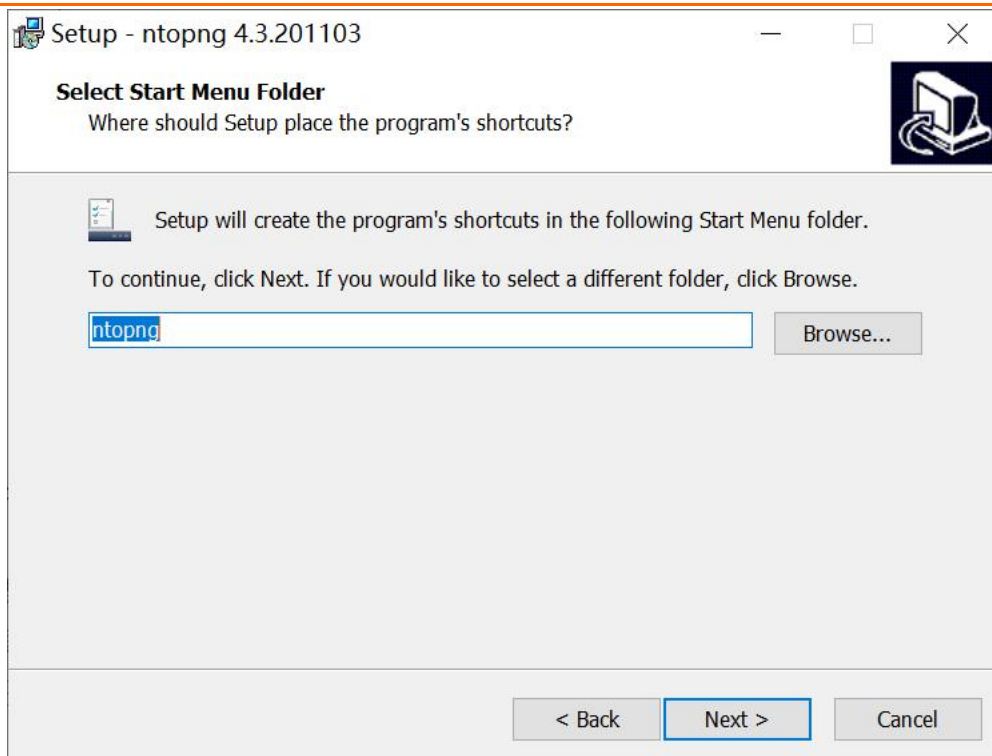


(2) 空置命令

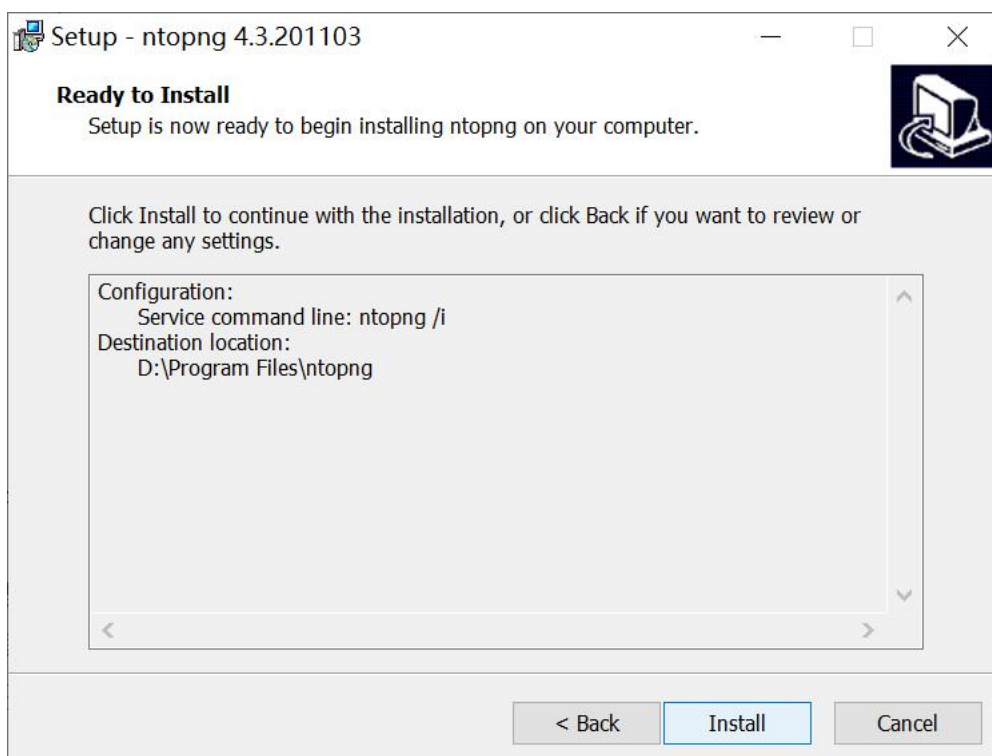


(3) 选择目录

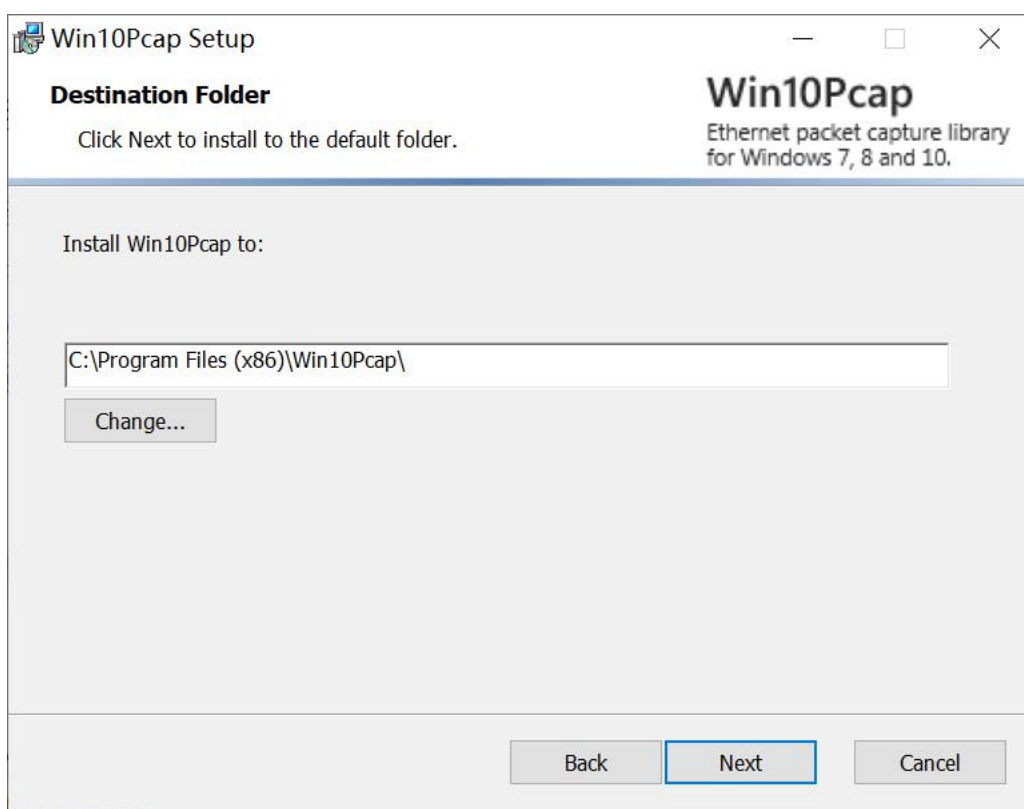
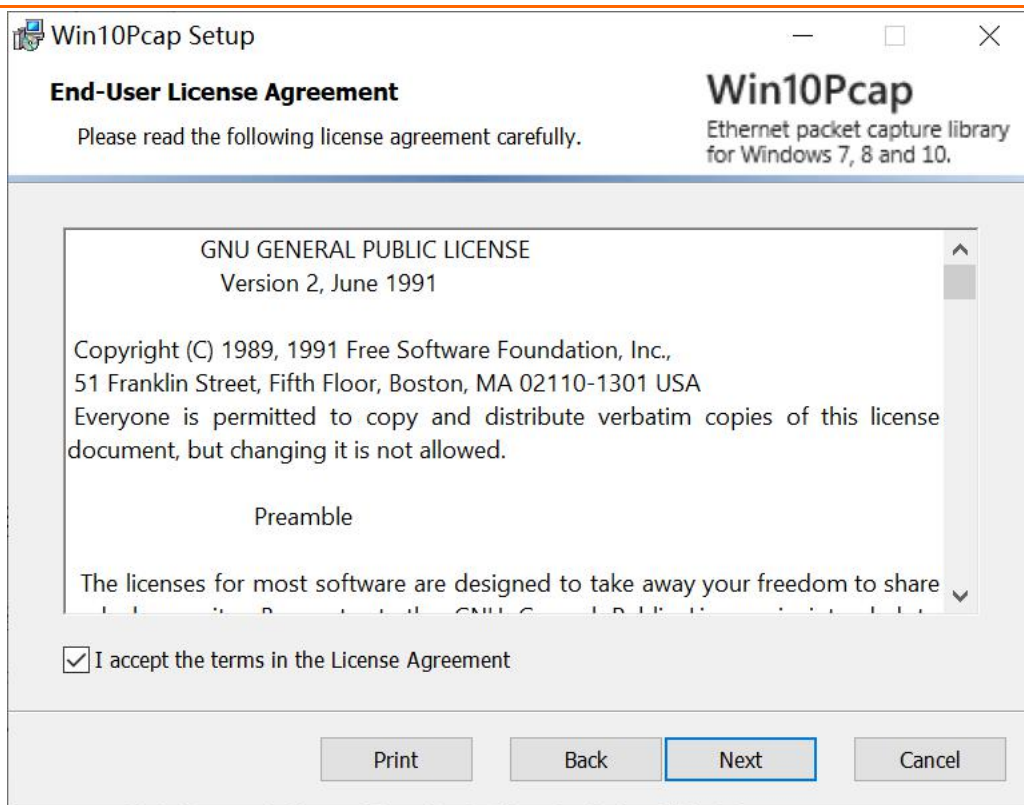




(4) 安装



(5) 安装 win10Pcap，如果 Windows 上已经安装了 Wireshark，无需进行此步骤。



(6) 安装 Microsoft Visual C++ Redistributable，如果已安装该组件可以跳过

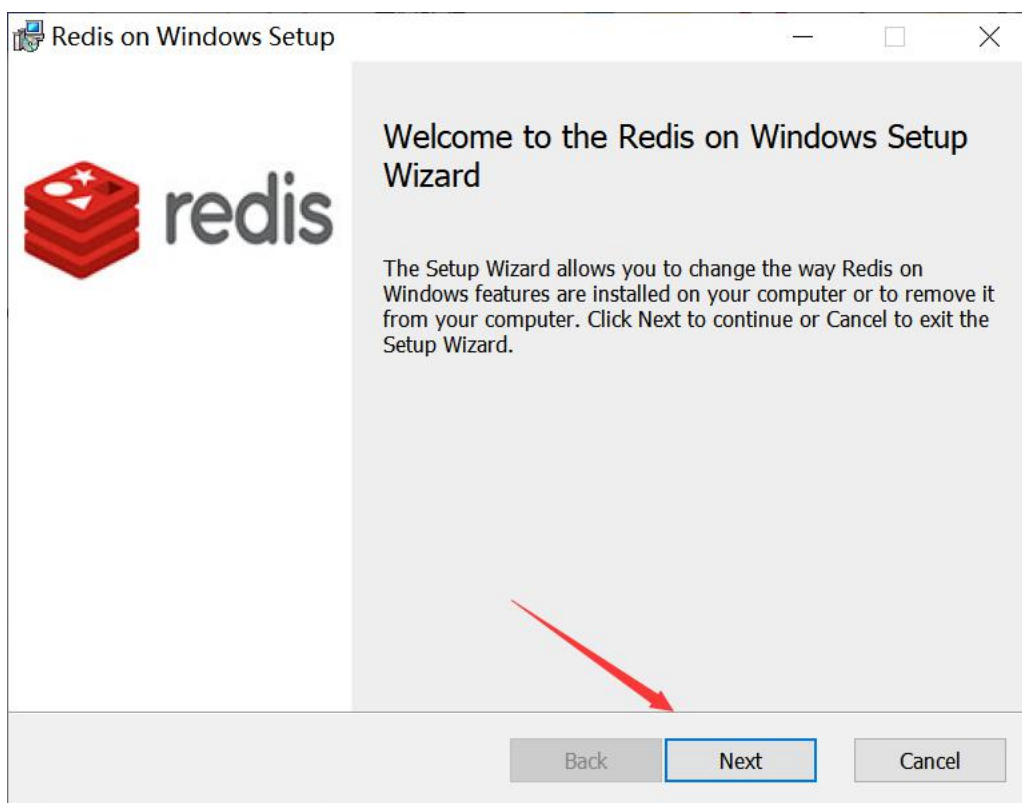
www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233



4.4.2. Redis 安装

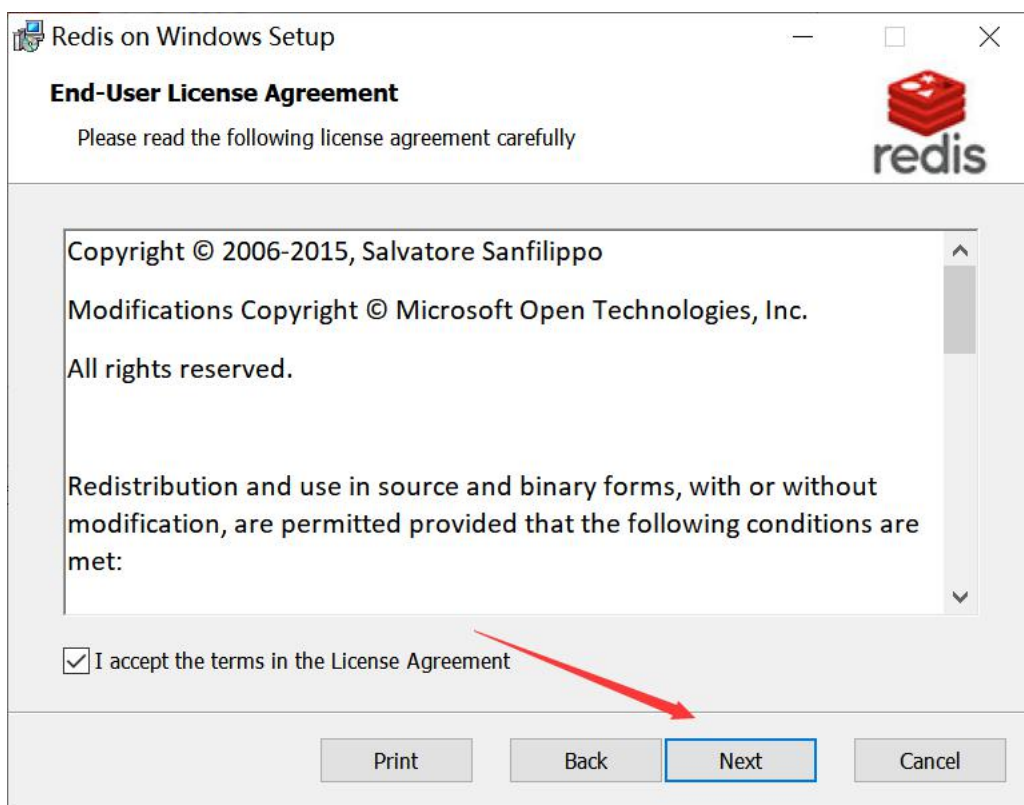
(1) 开始安装，点击 next



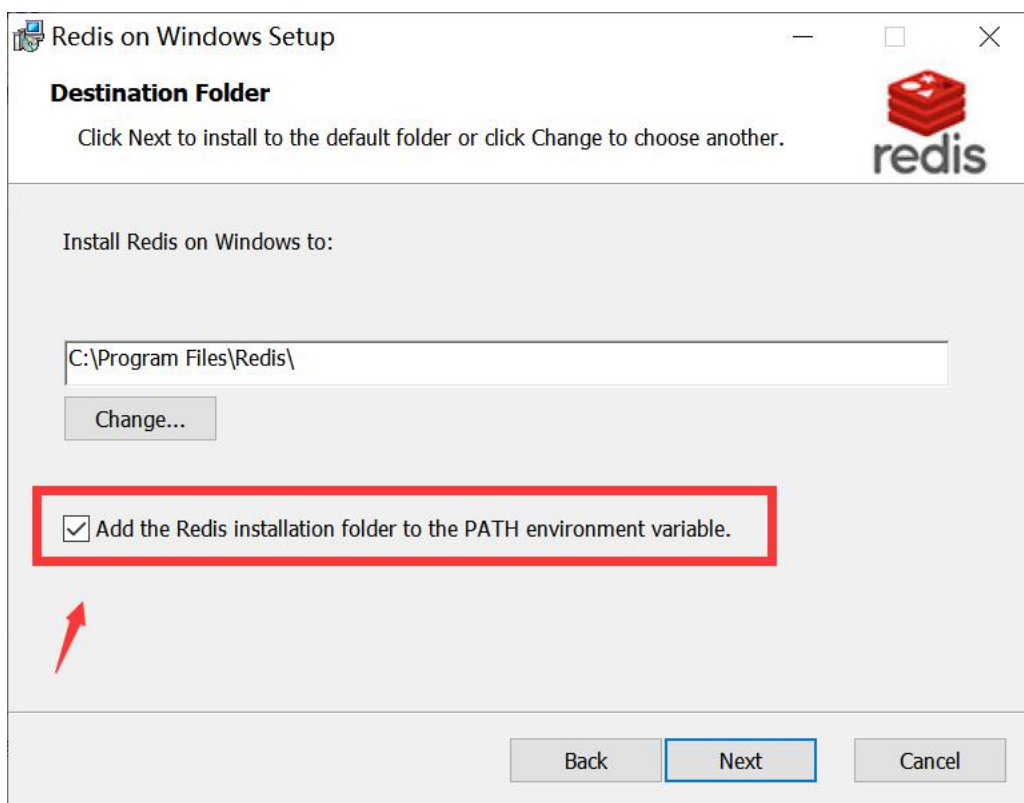
(2) 选择“同意协议”，点击 next

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233



(3) 勾选 Redis 注册到系统环境变量中



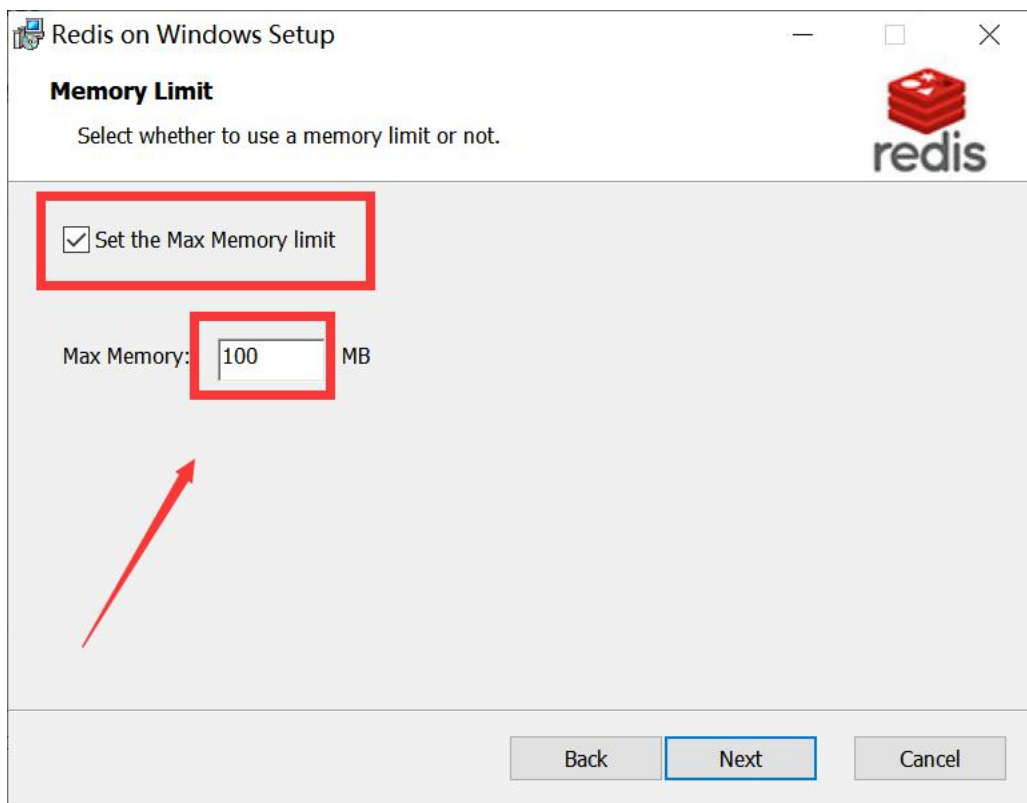
(4) 选择端口默认 6379，并勾选选择防火墙例外。

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233



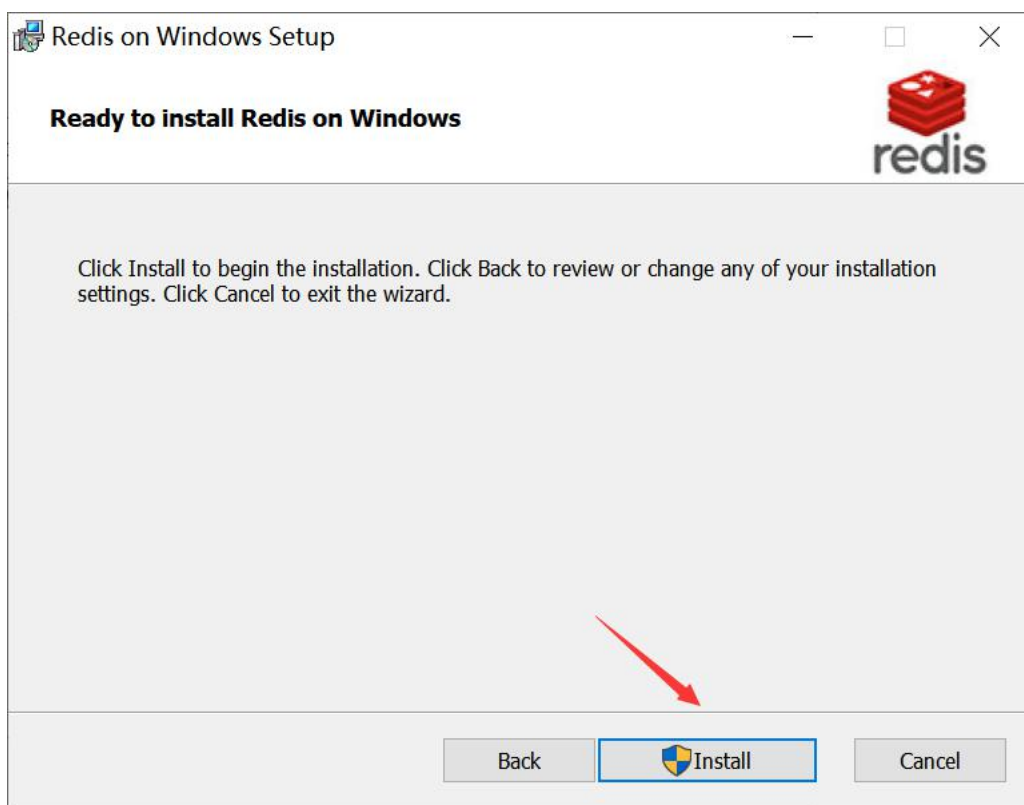
(5) 勾选最大内存限制，设置为 100M，点击 next



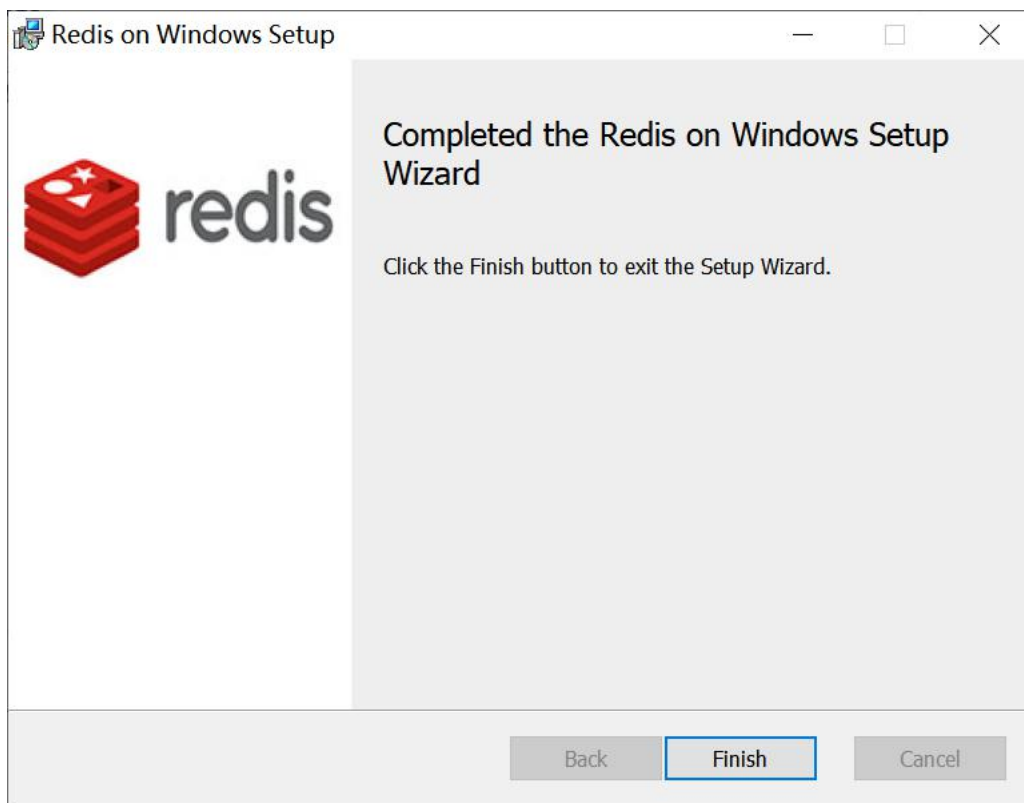
(6) 点击 install

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233



(7) Finish

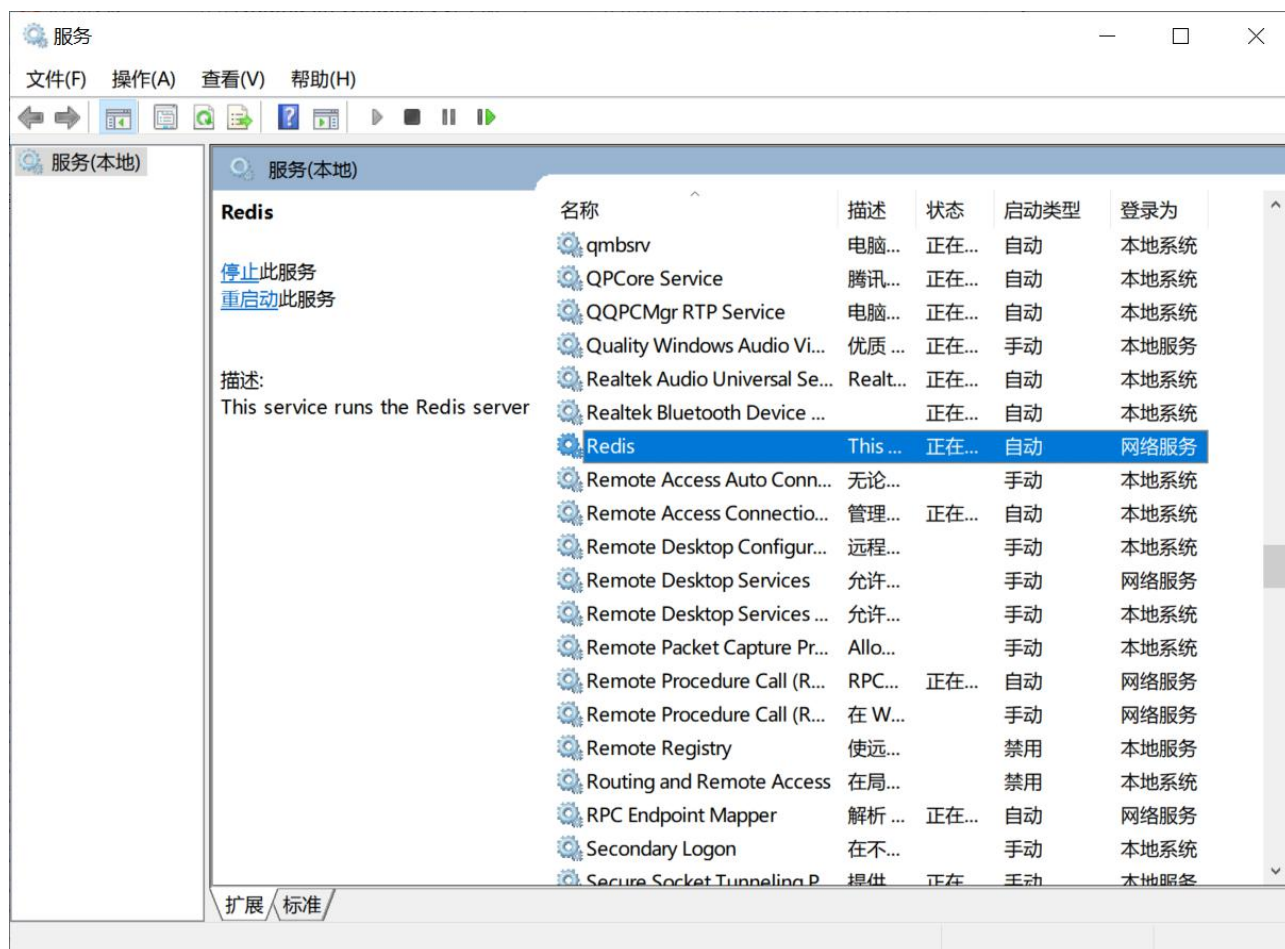


(8) 配置 Redis 的密码, 通过命令窗口进入 Redis 安装目录下, 输入命令 `redis-cli.exe` (也可双击 `redis-cli.exe`),
www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848
sales@hkaco.com support@hkaco.com 电话: 020-38743030, 38743032 传真: 020-38743233

命令 config set requirepass <mypasswd> 设置密码

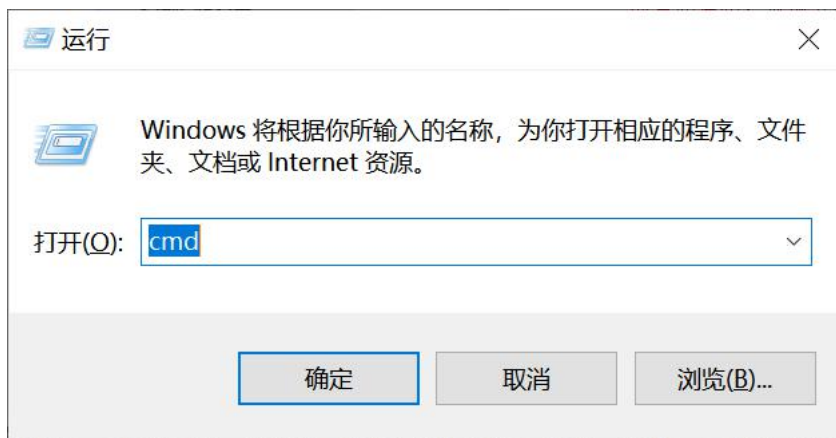
```
C:\Program Files\Redis>
C:\Program Files\Redis>redis-cli.exe 1
127.0.0.1:6379> config set requirepass 123456 2
OK
127.0.0.1:6379> _
```

(9)打开服务：再在右侧找到 Redis 名称的服务，启动 Redis。

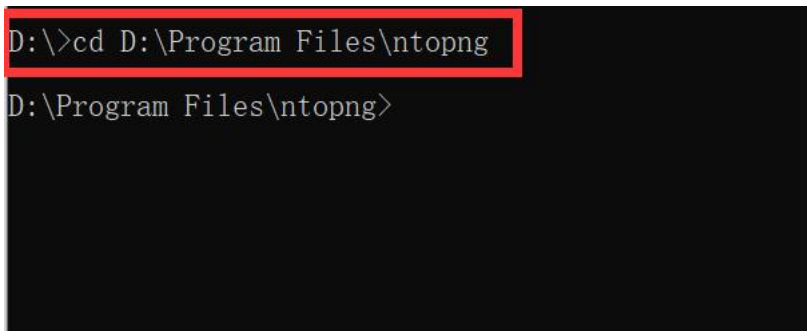


4.4.3. 启动 ntopng

- (1) Win+R 输入 cmd 打开命令窗口

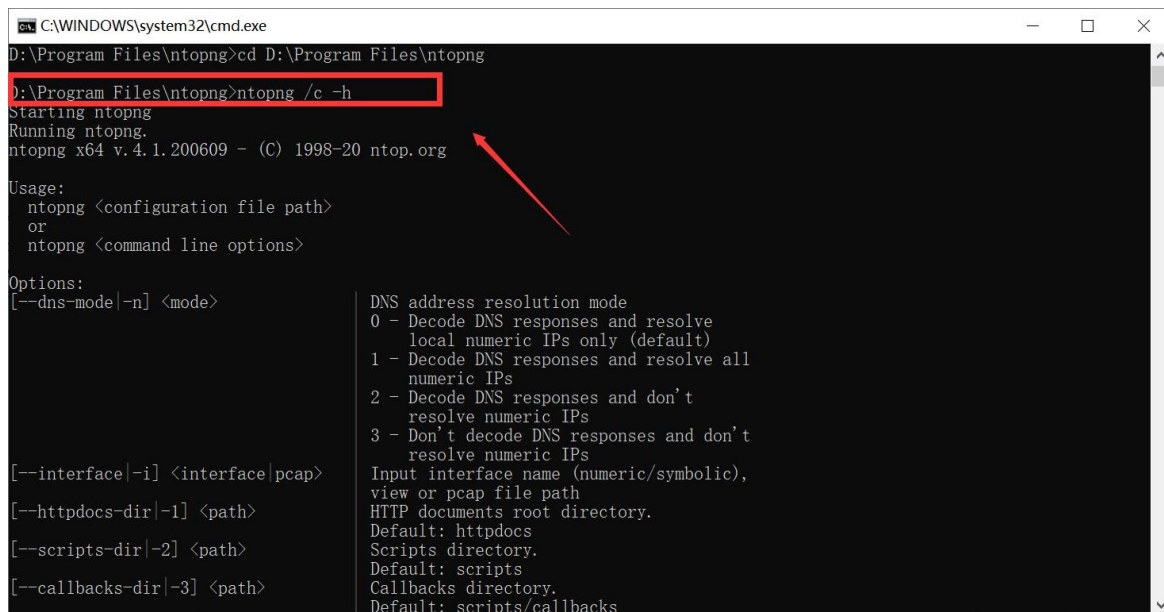


- (2) 导航到 ntopng 安装目录下



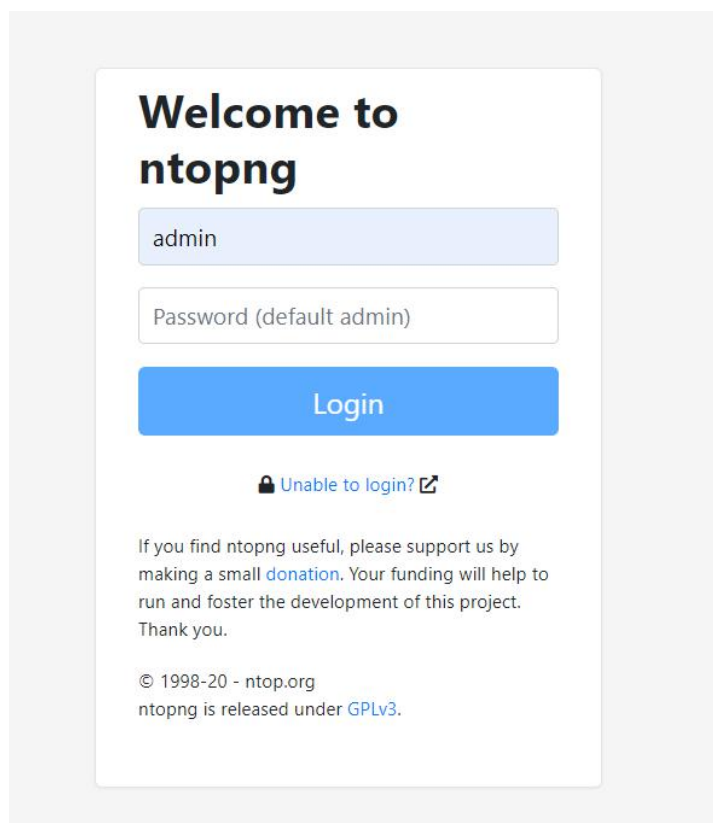
- (3) 输入命令启动 ntopng

ntopng /c -h (默认打开所有接口, 如需打开特定接口: ntopng /c -i <interface name>)

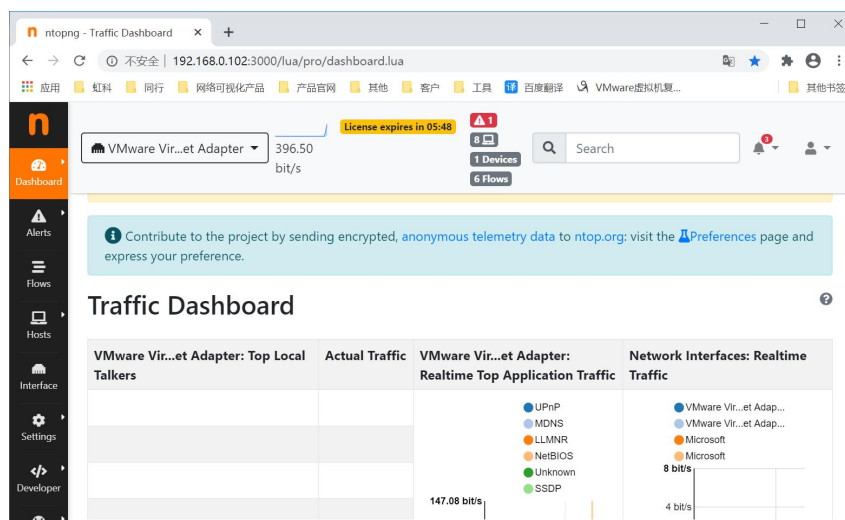


(4) 任意打开 web 浏览器输入如下命令，进入登录界面，初次登陆需重设密码：

http://127.0.0.1:3000



(5) 输入密码和登录到 web 界面



4.4.4. 设置 ntopng 服务（开机自启动）

- (1) 以管理员身份打开命令窗口
- (2) 输入：ntopng /h 可查看帮助
- (3) 输入：ntopng /i 即以服务方式运行 ntopng（输入：ntopng /r 结束本服务）

```
选择管理员: 命令提示符
Unrecognized option: /h
Available options:
/i [ntopng options] - Install ntopng as service
/c                  - Run ntopng on a console
/r                  - Deinstall the service
/h                  - Prints this help

Usage: type ntopng /c -h

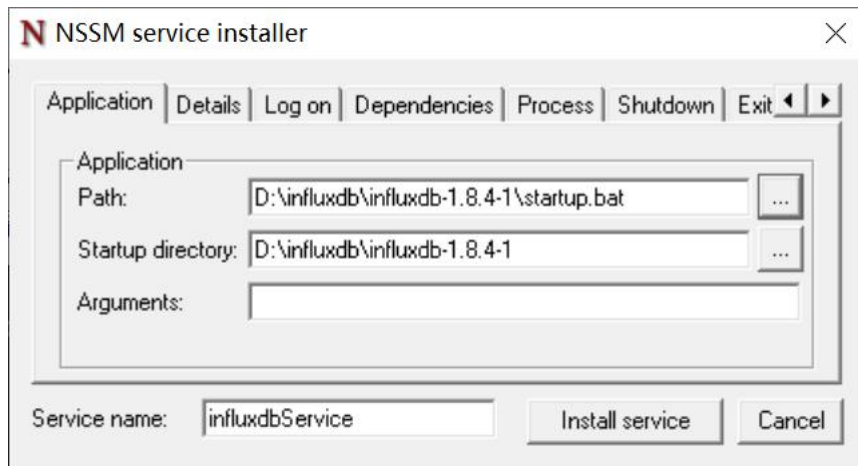
D:\Program Files\ntopng>ntopng /i
ntopng installed.
NOTE: the default password for the 'admin' user has been set to 'admin'.
D:\Program Files\ntopng>
```

4.4.5. 安装 influxDB(可选)

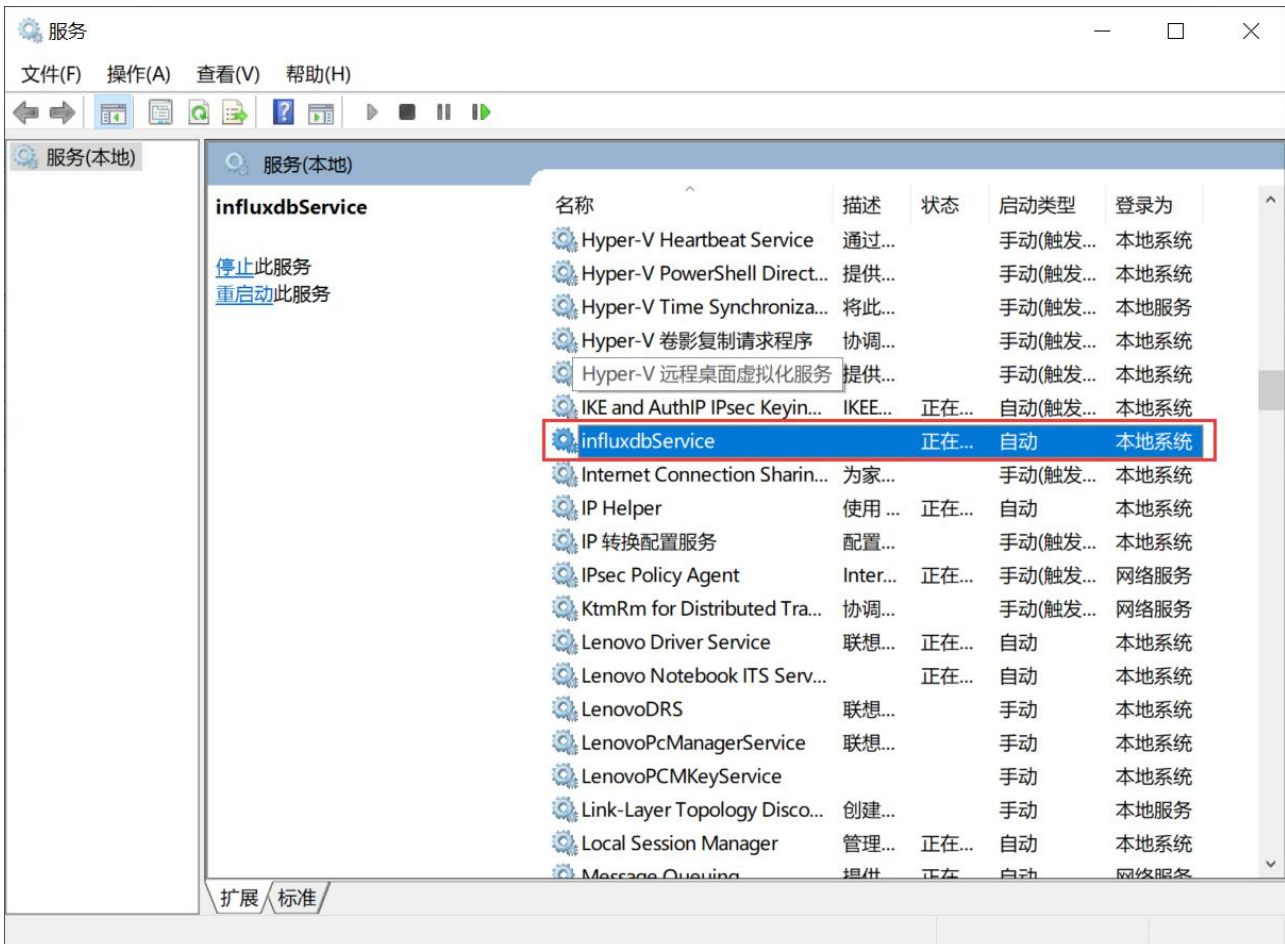
- (1) 在文件包内找到 influxdb 安装包，复制到希望的安装目录，如：D:\Program Files\influxdb\
- (2) 在命令窗口导航到该目录下执行：nssm.exe install influxdbService

```
D:\influxdb\influxdb-1.8.4-1>nssm.exe install influxdbService
```

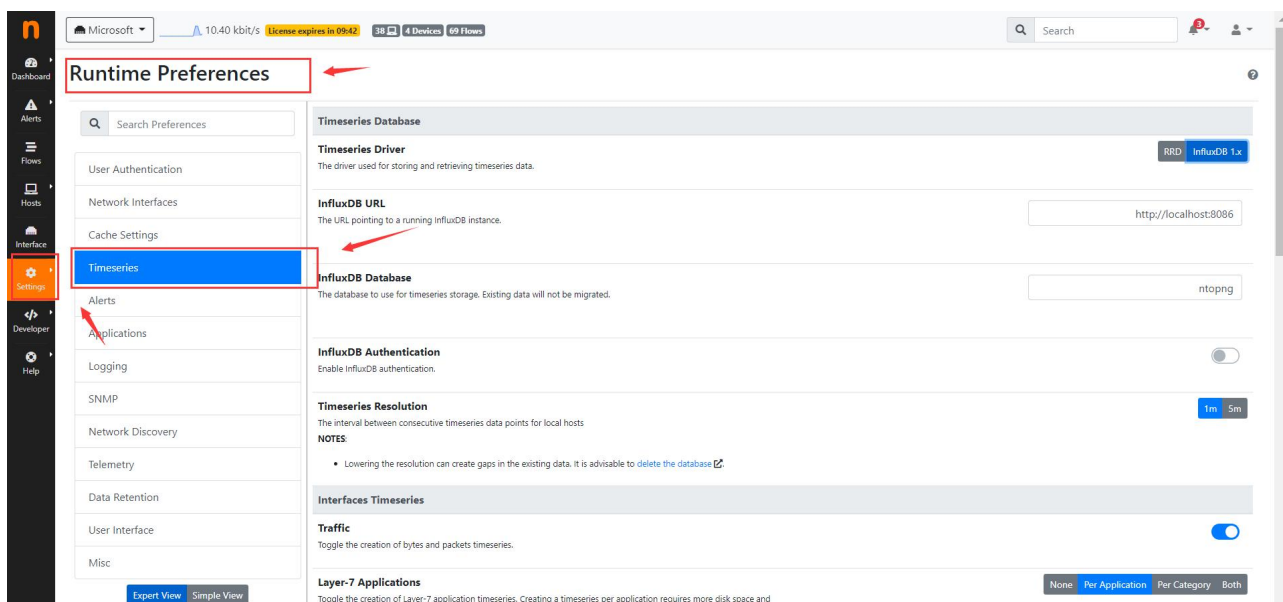
- (3) 选择 startup.bat 完成服务注册



(4) 在服务里启动 influxdbService:



(5) ntopng 配置时间序列, 在 Setting->Preferences->timeseries 选择 influxDB 数据库, 点击底部 Save 然后重启服务。



5. 配置文件

ntopng 作为守护程序启动时需要 ntopng 配置文件，文件目录为：/etc/ntopng/ntopng.conf，安装完成后会自动生成该文件，无需任何更改就能正常启用 ntopng 但是有的时候我们需要更改一些配置时必须修改配置文件。

文件的编写格式为：option=value(注意等号前后不要随便添加空格)，以-w 命令选项为设置 ntopng 所指定的端口(默认为:3000)，如需更改则可以在配置文件中新的一行添加：-w=3000 即可，一个常用的简单的配置文件示例如下：

```
#####
```

```
#监控 ens33 接口
```

```
-i=ens33
```

```
#设置 ntopng 端口为 3001，浏览器输入：127.0.0.1:3001 打开 ntopng
```

```
-w=3001
```

```
#启用流转储功能，可进行历史回溯分析（只有企业版可用）
```

```
-F=nindex
```

```
#启用编辑自定义协议功能
```

```
-p=/var/lib/ntopng/protos.txt
```

```
#设置本地网段
```

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233

```
-m="192.168.0.0/24"
```

```
#以服务运行
```

```
-G=/var/run/ntopng.pid
```

```
#####
```

6. Web GUI (ntopng Enterprise)

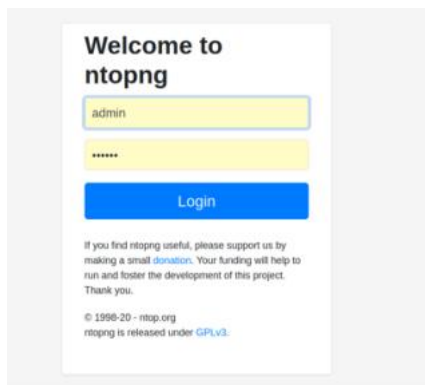
(注意：本教程后续部分均在 ubuntu 18.04 上进行，其他系统使用方法类似)

6.1. 登录

启动 ntopng 之后，您可以查看 GUI。默认情况下，可以从任何 Web 浏览器访问 GUI。在 ntopng 启动期间，可以将其他端口指定为命令行选项。始终弹出的第一页包含登录表单-前提是用户尚未决定在启动过程中关闭身份验证。http://127.0.0.1:3000/，初始账号密码均为：admin，首次登录需重置密码。

- 浏览器打开 web 界面

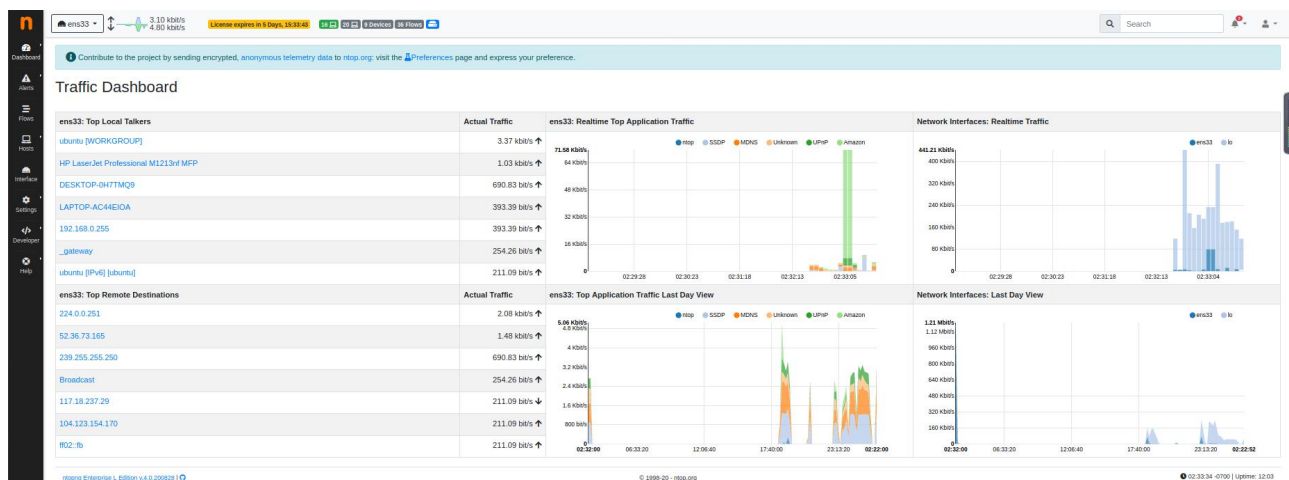
```
http://127.0.0.1:3000/
```



6.2. 仪表盘

仪表板是一个动态页面，它为 ntopng 监视的所选接口或接口视图提供当前流量的更新快照。专业版中的仪表板可提供大量信息，包括实时流量-每个受监视的界面和每个应用程序-本地本地通话者和热门目的地。仪表板将动态刷新。表格和图表由 ntopng 保持更新。仪表板的右侧部分显示了“主要应用程序和网络流量”的实时和最新图表。如果选择了网络接口视图，则将按每个物理接口显示网络流量。只需单击图表键中相应的彩色点，即可动态切换每个图表中显示的项目。

位置：Dashboard->Traffic Dashboard

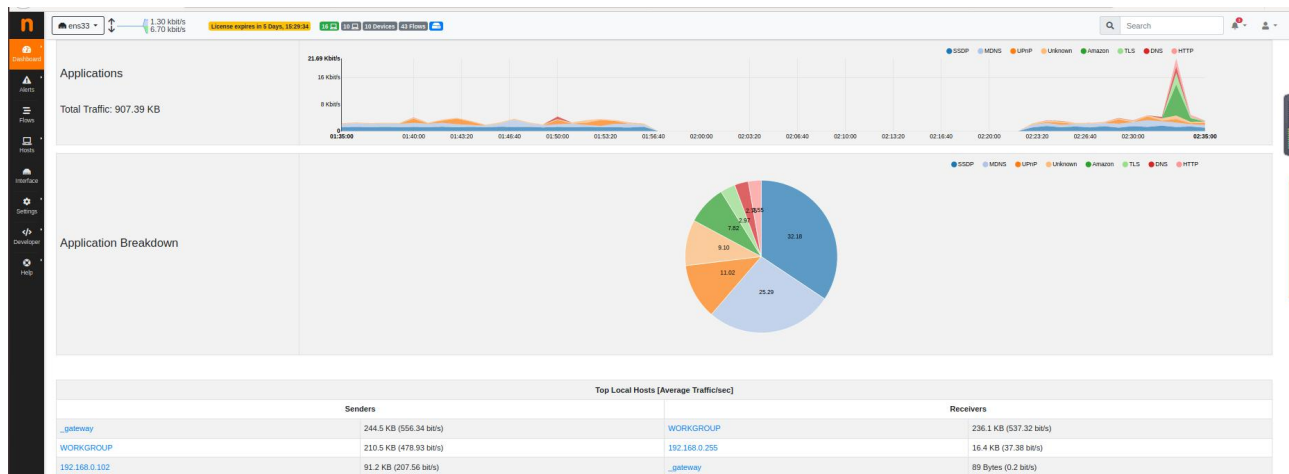


6.3. 流量报告

专业版的 ntopng 允许为受监视的一个或多个接口生成自定义流量报告。可从主工具栏的下拉主菜单访问“**Traffic Report**”页面，该页面为用户提供了多个配置选项。

左侧有固定宽度的时间间隔。它们分别是 1h（一个小时），1d（一天），1w（一周），1M（一个月），6M（六个月）和 1Y（一年）。单击这些间隔中的任何一个都会生成一个自动报告，该报告的时间范围从当前开始，并且时间倒退直到达到间隔。

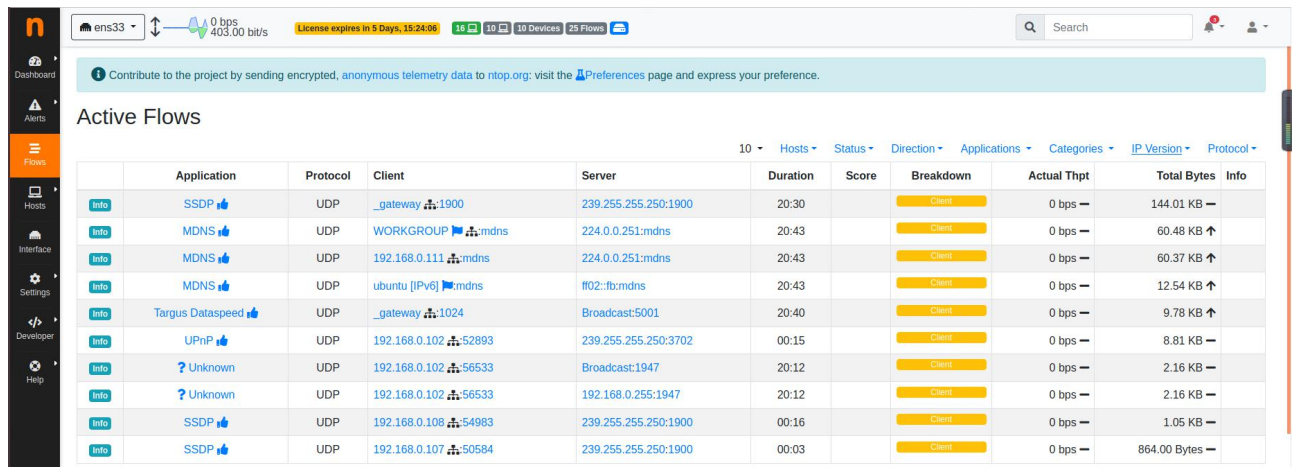
位置：Dashboard->Traffic Report



6.4. 流量

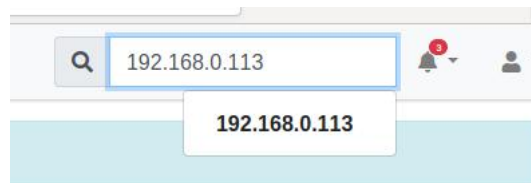
可以选择顶部工具栏中的“流”条目，以可视化当前活动流的实时交通信息。可以将流视为两个主机之

间的逻辑双向通信通道。同一对主机之间可以存在多个并发流。

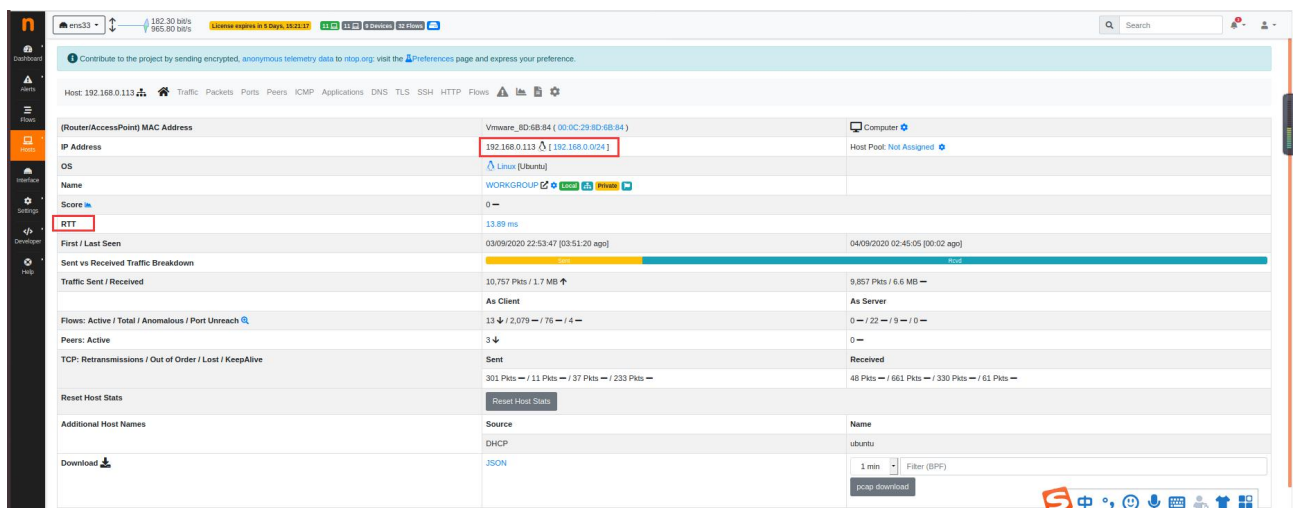


	Application	Protocol	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
Info	SSDP	UDP	_gateway 1900	239.255.255.250:1900	20:30		Client	0 bps	144.01 KB	
Info	MDNS	UDP	WORKGROUP mdns	224.0.0.251:mdns	20:43		Client	0 bps	60.48 KB	
Info	MDNS	UDP	192.168.0.111 mdns	224.0.0.251:mdns	20:43		Client	0 bps	60.37 KB	
Info	MDNS	UDP	ubuntu [IPv6] mdns	:::fb:mdns	20:43		Client	0 bps	12.54 KB	
Info	Targus Dataspeed	UDP	_gateway 1024	Broadcast:5001	20:40		Client	0 bps	9.78 KB	
Info	UPnP	UDP	192.168.0.102 52893	239.255.255.250:3702	00:15		Client	0 bps	8.81 KB	
Info	? Unknown	UDP	192.168.0.102 56533	Broadcast:1947	20:12		Client	0 bps	2.16 KB	
Info	? Unknown	UDP	192.168.0.102 56533	192.168.0.255:1947	20:12		Client	0 bps	2.16 KB	
Info	SSDP	UDP	192.168.0.108 54983	239.255.255.250:1900	00:16		Client	0 bps	1.05 KB	
Info	SSDP	UDP	192.168.0.107 50584	239.255.255.250:1900	00:03		Client	0 bps	864.00 Bytes	

● IP 搜索

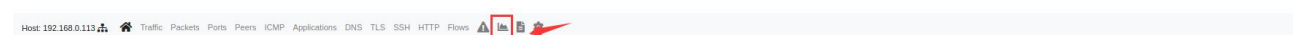


搜索后可以知道特定 ip 的详细信息如下：



Host: 192.168.0.113	
(Router/AccessPoint) MAC Address	Vmware_R0D-84 (00:0C:29:8D:6B:84)
IP Address	192.168.0.113 (192.168.0.0/24)
OS	Linux (Ubuntu)
Name	WORKGROUP
Score	0
RTT	13.89 ms
First / Last Seen	03/09/2020 22:53:47 [03:51:20 ago] 04/09/2020 02:45:05 [00:02 ago]
Sent vs Received Traffic Breakdown	
Traffic Sent / Received	10,757 Pkts / 1.7 MB 9,857 Pkts / 6.6 MB
Flows: Active / Total / Anomalous / Port Unreach	13 / 2,079 / 76 / 4
Peers: Active	3
TCP: Retransmissions / Out of Order / Lost / KeepAlive	301 Pkts / 11 Pkts / 37 Pkts / 233 Pkts
Reset Host Stats	Reset Host Stats
Additional Host Names	Source: DHCP Name: ubuntu
Download	JSON

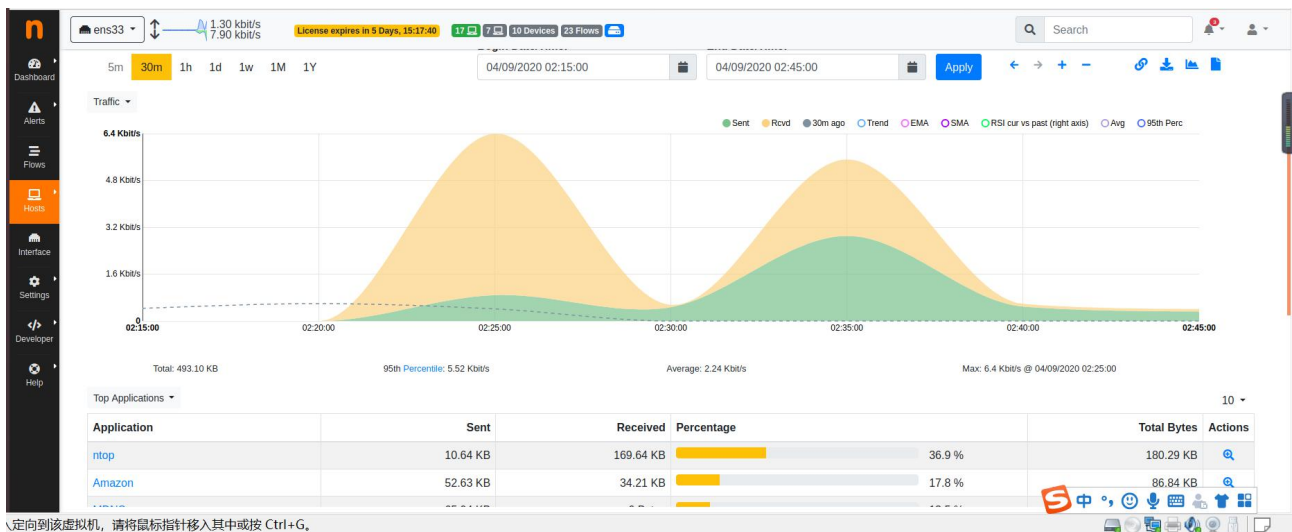
点击  可查看历史流信息



如下表：

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233



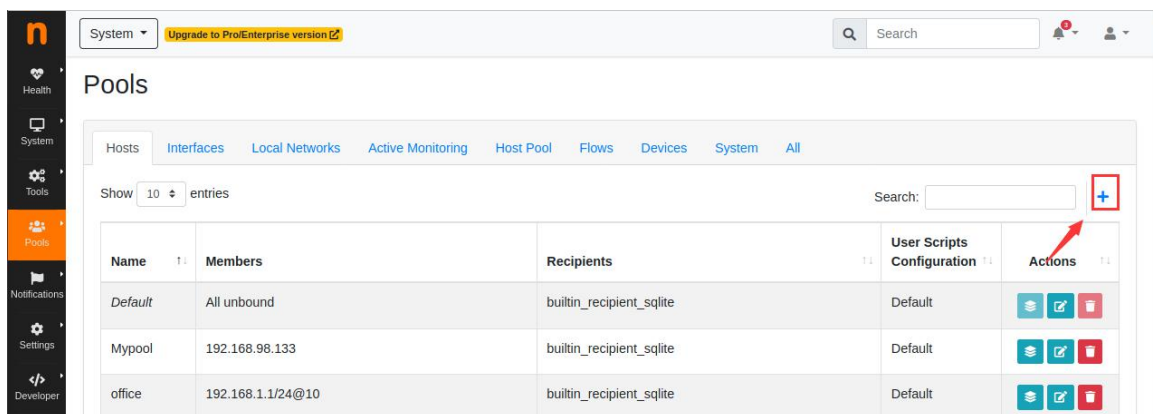
6.5. 主机划分

在 ntopng 中，主机池提供了一种将不同主机组合在一起的有效方法。主机池是基于网络接口定义的。主机池可以包含以下实体：

- 单个 IP 地址，通过 IPv4 / IPv6 地址与单个主机匹配
- MAC 地址，通过 MAC 地址匹配单个主机
- 网络地址，与 IPv4 / IPv6 地址属于给定网络的所有主机匹配（以 CIDR 格式指定）。
- 还可以指定 VLAN ID 以匹配特定 VLAN 的主机。

通过主机池对主机进行分组后，可以查看分组的统计信息和时间序列。

首先定位到 **system->pools->hosts**，点击增加主机池：



设置主机池的名称，配置等：

Add Host Pool

Name

IOT

The name must be longer than 1 character and it can't be empty.

User Scripts Configuration

Default

Recipients

builtin_recipient_sqlite

SQLite

builtin_recipient_sqlite (built-in)

Add

点击编辑主机成员：

System

Upgrade to Pro/Enterprise version

Search

Pools

Hosts

Interfaces

Local Networks

Active Monitoring

Host Pool

Flows

Devices

System

All

Show 10 entries

Search:

Name	Members	Recipients	User Scripts Configuration	Actions
Default	All unbound	builtin_recipient_sqlite	Default	
IOT		builtin_recipient_sqlite	Default	
Mypool	192.168.98.133	builtin_recipient_sqlite	Default	
office	192.168.1.1/24@10	builtin_recipient_sqlite	Default	

Showing 1 to 4 of 4 rows

Manage Configuration

点击添加主机成员

System

Upgrade to Pro/Enterprise version

Search

Host Pool Members

Current Host Pool

IOT

Show 10 entries

Member Type

Search:

Member Address	VLAN	Actions
No data available in table		

Showing 0 to 0 of 0 entries

可以用 ip, mac 和 network 三种划分方式。这里以 network 为例

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030, 38743032 传真:020-38743233

Add Host Pool Member

Member Type

IP AddressNetworkMAC Address

Network

192.168.98.1 / 24

VLAN

14

Add

添加完成后可以在主机池中看到划分的结果

Hosts

Interfaces

Local Networks

Active Monitoring

Host Pool

Flows

Devices

System

All

Show

10

entries

Search:

+

Name	Members	Recipients	User Scripts Configuration	Actions
Default	All unbound	builtin_recipient_sqlite	Default	
IOT	192.168.98.1/24@14	builtin_recipient_sqlite	Default	
Mypool	192.168.98.133	builtin_recipient_sqlite	Default	
office	192.168.1.1/24@10	builtin_recipient_sqlite	Default	

Showing 1 to 4 of 4 rows

«

<

1

>

»

最后可以在选择特定的接口，打开定位到 Hosts-Hosts pools,可以看到主机池的流量情况。

ens33

1.70 kbit/s
1.80 kbit/s

License expires in 08:16

3 8 3 Devices 24 Flows

Search

Host Pool List

Pool Name	Chart	Hosts	Seen Since	Breakdown	Throughput	Traffic
office		0	02:14	Rcvd	0 bit/s	0 Bytes
Mypool		1	02:15	Rcvd	3.8 kbit/s	141.24 MB
IOT		0	02:13	Rcvd	0 bit/s	0 Bytes
Default		11	02:13	Sent Rcvd	1.13 kbit/s	1.18 GB

Showing 1 to 4 of 4 rows

ntopng Enterprise L v.4.1.201010 | © 1998-20 - ntop.org 11:21:33 +0800 | Uptime: 02:21

6.6. 历史图表

ntopng 可以将流数据转储到持久性存储中，并提供视图以浏览过去记录的流数据。

传统上，为了提供历史数据，ntopng 需要连接的 MySQL 数据库。传统上，为了提供历史数据，ntopng 需要连接的 MySQL 数据库。请查看 Flows Dump 文档，以获取有关如何设置连接的更多详细信息以及此模式可用的历史视图。

但是，由于用户对 MySQL 的低性能和高流插入率的反馈，ntopng 现在集成了一个称为 nindex 的专用流转储数据库，它克服了 MySQL 的限制。当前仅在 Linux / x86_64 体系结构的 ntopng 企业版中可用。

为了将流转储到磁盘，ntopng 要求指定 **-F nindex** 选项。

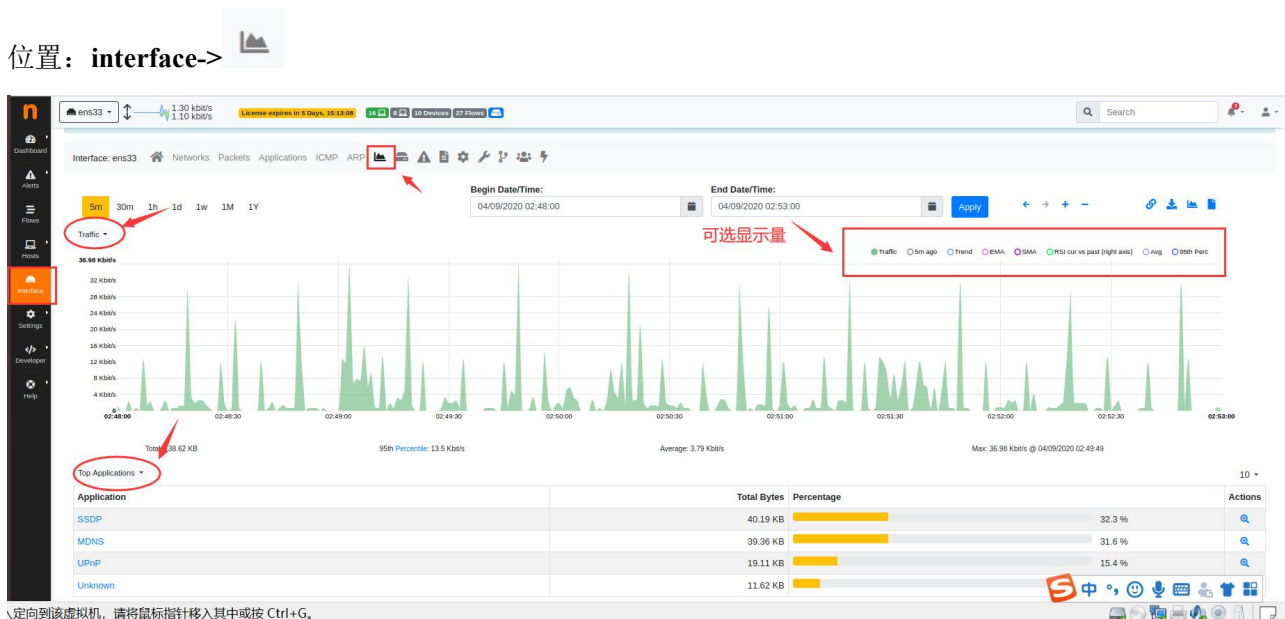
使用命令行启动：

```
sudo ntopng -i ens33 -F nindex
```

或者更改配置文件（/etc/ntopng/ntopng.conf）添加：

```
-F=nindex
```

位置：interface->



通过单击该  图标，可以选择特定的通信或主机并分析原始流。

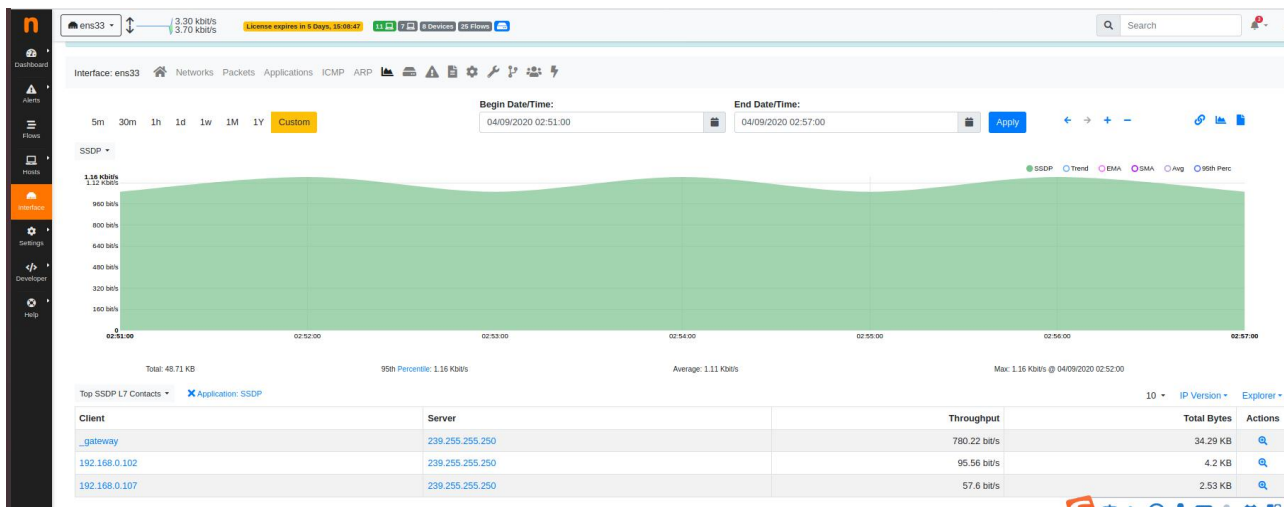
Top Applications

Application	Total Bytes	Percentage	Actions
SSDP	41.0 KB	45.1 %	
MDNS	19.99 KB	22.0 %	
Unknown	11.31 KB	12.4 %	
UPnP	9.49 KB	10.4 %	
DNS	2.51 KB	2.8 %	
Targus Dataspeed	2.33 KB	2.6 %	
UbuntuONE	2.07 KB	2.3 %	
ICMPv6	1.06 KB	1.2 %	
IGMP	917.0 Bytes	1.0 %	
NetBIOS	245.08 Bytes	0.3 %	

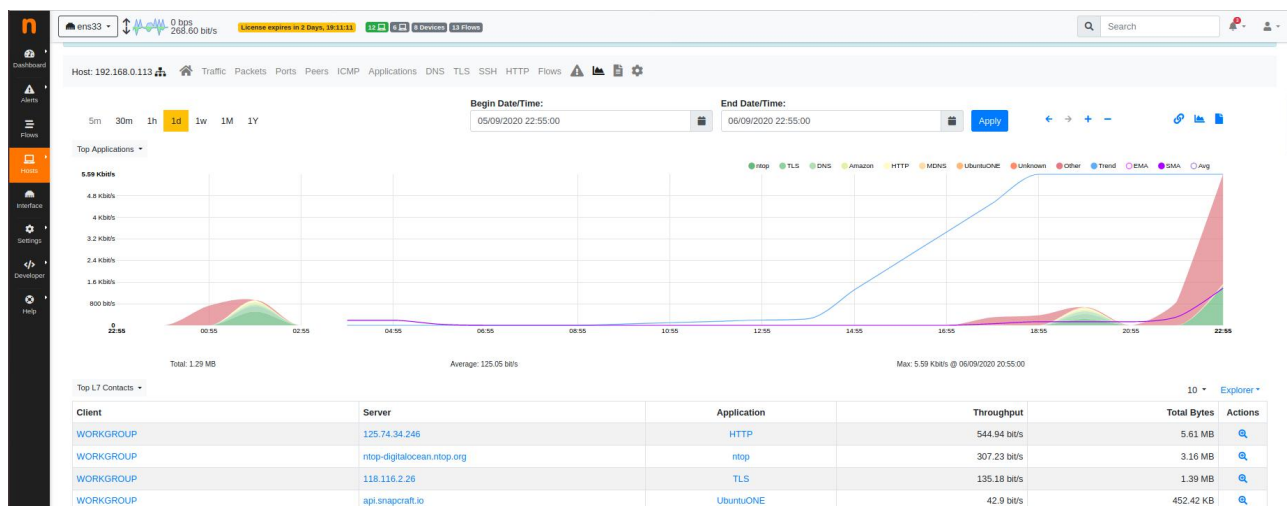
Showing 1 to 10 of 10 rows

NOTES:

点击后，何以看到每个用户的使用情况



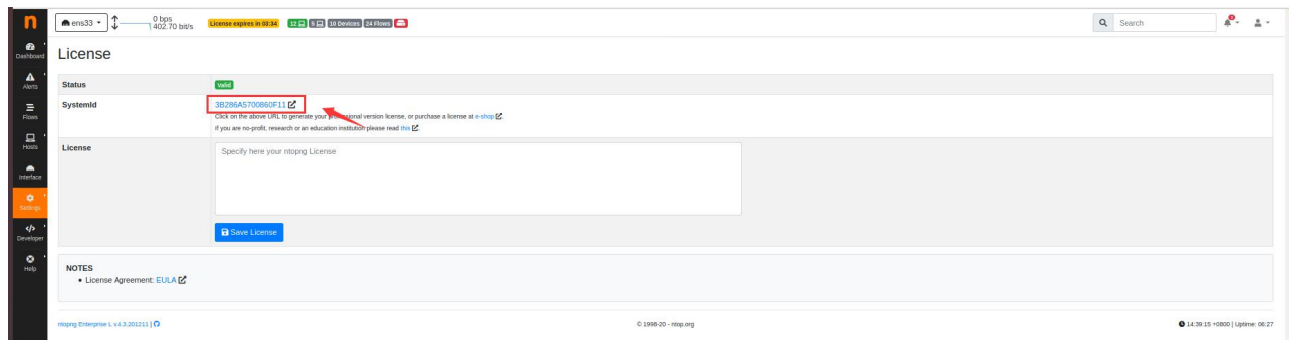
再次点击 图标可以看到特定用户的流量使用情况:



6.7. 获取 license 并激活

在 **Setting->License** 下查看软件 system ID，点击图中所示位置。

点击后会跳转到生成 license 生成界面：



ntopng License Generator	
Required Information	Description
System Id:	3B90718600860F11
Order Id:	
Email:	
ntopng Version:	4.0.200828
ntopng Edition:	Enterprise L (x64)
NOTE • The Enterprise L edition, creates a single license that also unlocks n2disk and nProbe. This means that with a single license you can unlock all products without the need to generate an individual product license.	
Create ntopng License Reset	

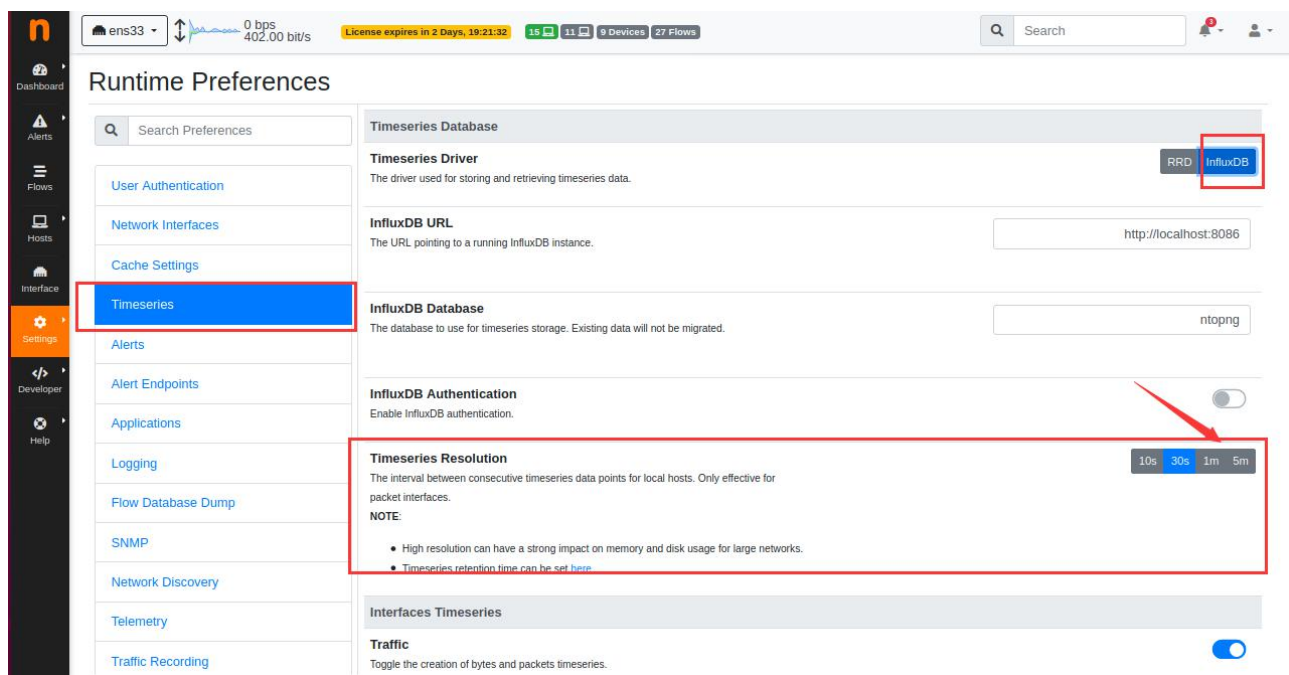
在上图中输入购买 license 得到的 Order id 和 Email 再点击 Create ntopng License 即可生成 License，依据生成 License 后界面提示信息即可完成激活。

6.8. 设置

6.8.1. 首选项

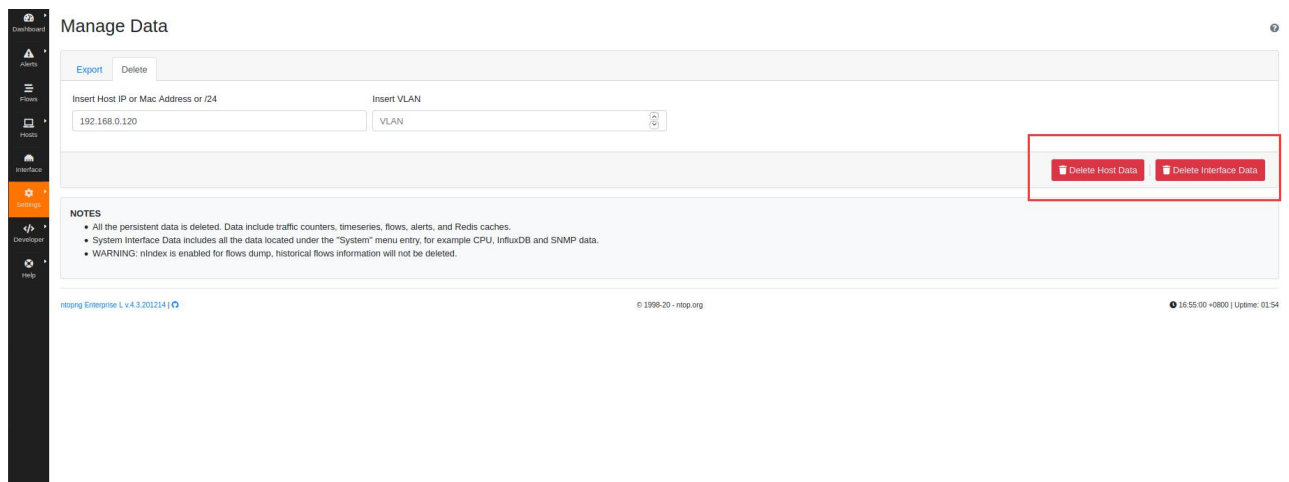
在 **Settings->Preferences** 中可以对 ntopng 进行许多配置如 SNMP、警告、时间序列等等，例如我们可

以设置时间序列为 influxDB，并设置它的分辨率，注意使用 influxDB 需要单独安装，并且版本要求高于 1.5。



6.8.2. 数据删除

在 **Setings->Manage Data** 中可以删除指定主机或者接口的数据。



主意：

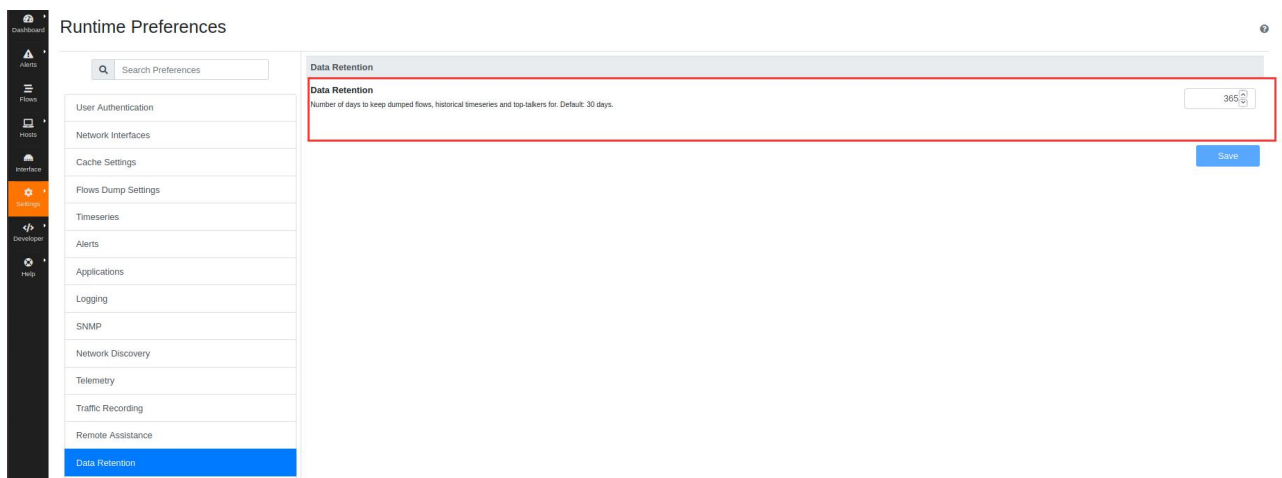
所有的持久数据删除：数据包括流量计数器、时间序列、流量、警报和 Redis 缓存。

系统接口数据包括：位于 "系统" 菜单项下的所有数据，例如 CPU、InfluxDB 和 SNMP 数据。

警告：nindex 为流量转储启用，历史流量信息将不会被删除。

6.8.3. 流数据存储时间

在 **Setings->Preference** 中选择 Data Retention 可以配置最大流量转储时间。



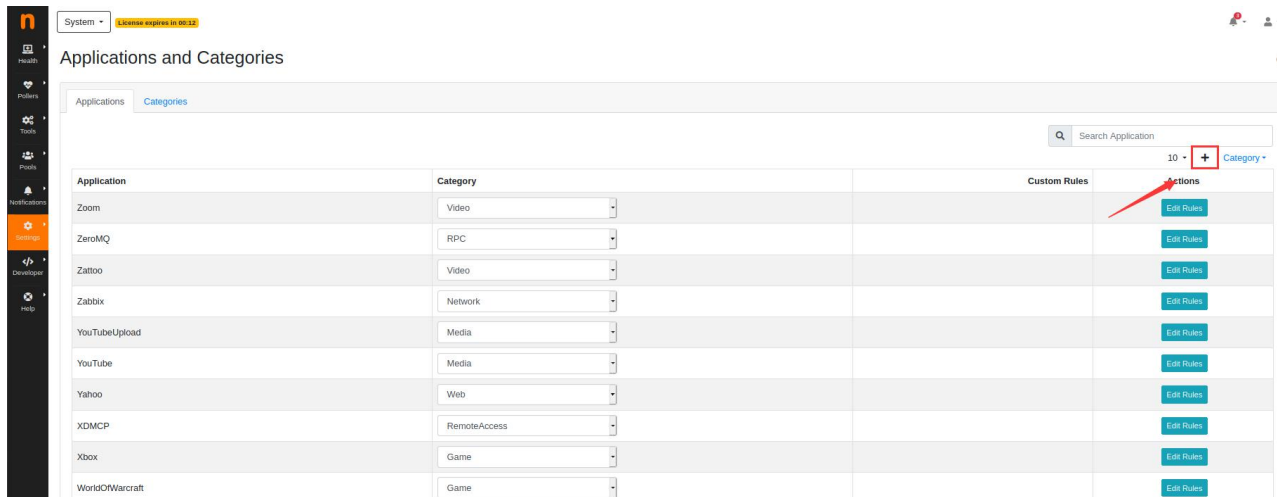
6.8.4. 定义私有协议

ntopng 可以基于 IP 地址、域名和端口定以自己的私有协议。要启用这一功能，

1) 你首先需要在/var/lib/ntopng 文件夹下新建一个 protos.txt 文件。

2) 在 etc/ntopng/ntopng.conf 文件中添加配置: -p=/var/lib/ntopng/protos.txt

3) 重新启动 ntopng，定位到 **Setings->Applications and Categories->Applications**，点击添加按钮，添加自定义协议



4) 配置私有协议，这里以域名定义私有协议。

Add Custom Application

Application Name

YOUKU

Custom Rules

youku.com

NOTES

- Each rule must be put on a separate line
- Rules can be either domain names, IPv4 addresses or TCP/UDP port ranges.
- Port range examples: "udp:443", "tcp:1230-1235"
- Domain names are interpreted as substring to be matched.
E.g. "ntop.org" will match "mail.ntop.org" and "ntop.org.example.com"

Add Application

5) 配置完成重新 ntopng 即可使用。
当我们访问优酷时就能识别该协议了。

ems33

96.40 kbit/s
6.10 kbps

Upgrade to Pro! Enterprise version 6.11.2

11.2

24.2

0 Devices

134 Flows

Search

Active Flows

10

Hosts

Status

Severity

Direction

Applications

Categories

IP Version

Protocol

	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
	IGMP	IGMP	192.168.0.106	239.255.255.250	< 1 sec	Client	0 bps	60 Bytes	
	IGMP	IGMP	192.168.0.106	239.255.255.250	< 1 sec	Client	0 bps	60 Bytes	
	IGMP	IGMP	192.168.0.100	224.0.0.252	< 1 sec	Client	0 bps	60 Bytes	
	TLS	TCP	192.168.0.106	203.119.169.88 :https	00:01	Client Server	0 bps	17.38 KB	6q6oft.tdum.alibaba.com
	TLS	TCP	192.168.0.106	14.116.143.187 :https	00:01	Client Server	0 bps	6.21 KB	
	TLS	TCP	192.168.0.106	203.119.169.141 :https	< 1 sec	Client Server	0 bps	18.28 KB	
	TLS.YOUKU	TCP	192.168.0.106	106.11.43.215 :https	00:01	Client Server	0 bps	10.13 KB	pc.pay.youku.com
	TLS	TCP	192.168.0.106	118.112.19.48 :https	< 1 sec	Client Server	0 bps	6.15 KB	liangcang-material.alicd...
	TLS	TCP	192.168.0.106	182.140.143.251 :https	< 1 sec	Client Server	0 bps	362 Bytes	
	TLS	TCP	192.168.0.106	118.112.19.48 :https	< 1 sec	Client Server	0 bps	6.09 KB	liangcang-material.alicd...

Showing 1 to 10 of 154 rows. Idle flows not listed.

ntopng Community v4.3.202114

© 1998-20 - ntop.org

17:45:15 +0800 | Uptime: 11:23

对于基于 IP 和端口自定义协议的方法类似，这里不再详述。
在我们定义完以后可以在 /var/lib/ntopng/protos.txt 中看到生成的配置。

```
# YOUKU
host: "youku.com"@YOUKU
```

因此你也可以通过直接编辑 protos.txt 文件的方法添加私有协议，编写方法参考[这里](#)。

7. 在 nprobe 上使用 ntopng 示例

7.1. nprobe 简介

ntopng 可用于可视化 nProbe 生成或收集的流量数据。在几种情况下，将 ntopng 与 nProbe 一起使用很方便，包括：

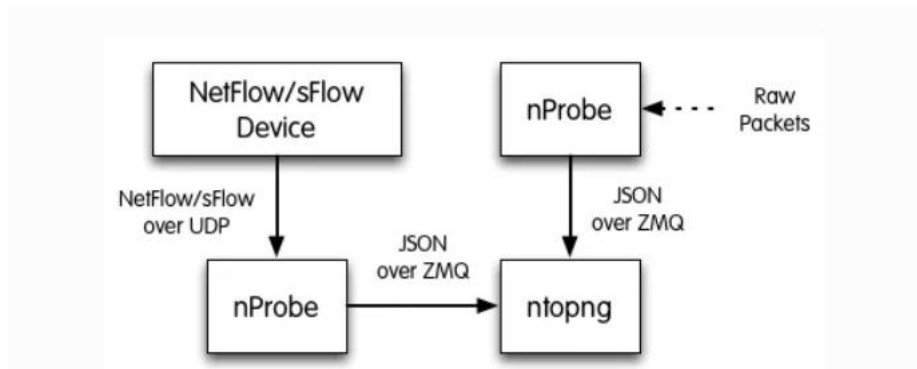
www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233

通常由路由器，交换机和网络设备产生的 NetFlow / sFlow 数据的可视化。在这种情况下，nProbe 从设备收集并解析 NetFlow / sFlow 流量，并将结果流发送到 ntopng 以进行可视化。

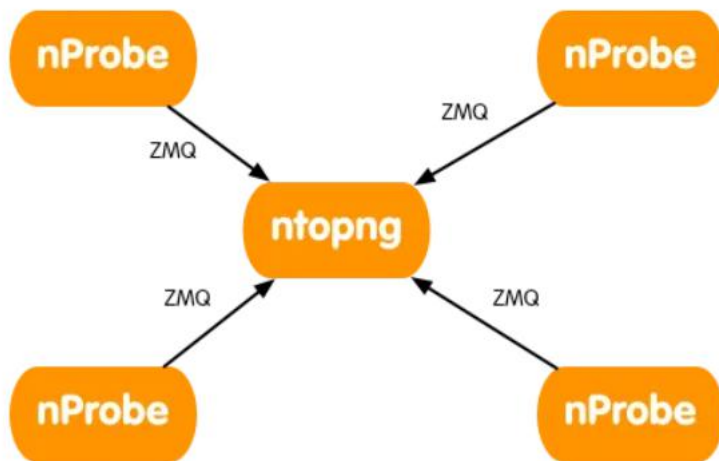
监视连接到远程系统的物理网络接口。在这种情况下，ntopng 无法直接监视网络接口，也无法看到其数据包。一个或多个 nProbe 可用于捕获远程网络接口流量并将结果流发送到中央 ntopng，以进行分析和可视化。

下图总结了上面突出显示的两种情况，并说明了它们也可以组合在一起。



7.2. 多个 nProbe 到一个 ntopng

使用单个 ntopng 从多个 nProbe 收集流对于单个位置负责可视化和存档流量数据很有用。



要从多个 nProbe 收集流，ntopng 必须以额外的开始 C（为收集器）在 ZMQ 端点的末尾，而每个 nProbe 都需要选择--zmq-probe-mode。在这种配置中，nProbes 会启动与充当服务器的 ntopng 的连接，反之亦然。因此，您必须确保 ntopng 正在侦听 ANY 地址（即通配符）* 在 ZMQ 端点地址中）或在各种 nProbe 可以访问的另一个地址上。

以下是这种配置的示例

```
ntopng -i tcp://*:5556c
```

www.hkaco.com 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

sales@hkaco.com support@hkaco.com 电话:020-38743030 , 38743032 传真:020-38743233

```
nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i eth1 -n none -T "@NTOPNG@"
```

```
nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i none -n none --collector-port 2055 -T "@NTOPNG@"
```

```
nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i none -n none --collector-port 6343 -T "@NTOPNG@"
```

7.3. NAT

nProbe 和 ntopng 的 IP 可达性不能总是被认为是理所当然的。有时，ntopng 可能有必要从单独网络中的 nProbe 收集流，该网络可能位于 NAT 之后，甚至被防火墙屏蔽。同样，NAT 后的 ntopng 可能有必要从另一个网络中的 nProbe 收集流。幸运的是，要处理这些情况，可以将 ntopng（和 nProbe）配置为可互换地充当 JSON-Over-ZMQ 通信的客户端或服务器。这样就避免了在网络设备中插入冗长，耗时且可能不安全的规则，因为这足以确保客户端可以访问服务器，而 NAT 将自动处理通信中返回的服务器到客户端部分。

当 nProbe 和 ntopng 都在同一网络上，或者当 ntopng 在另一个网络中但可以到达 nProbe 时，应使用以下配置



```
ntopng -i tcp://<ip address of nProbe>:5556
```

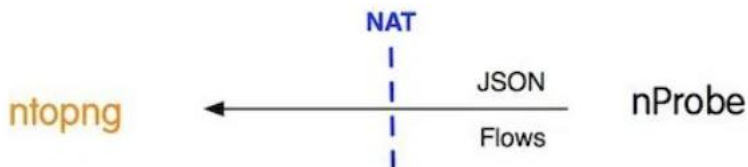
```
nprobe --zmq "tcp://*:5556" -i eth1 -n none -T "@NTOPNG@"
```

下述是最简单 nprobe 和 ntopng 的示例如：

```
ntopng -i tcp://127.0.0.1:5556
```

```
nprobe --zmq "tcp://*:5556" -i eth1 -n none -T "@NTOPNG@"
```

当 ntopng 无法达到 nProbe，但 nProbe 可以达到 ntopng 时，应使用的配置为



```
ntopng -i tcp://*:5556c
```

```
nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i eth1 -n none -T "@NTOPNG@"
```

请注意，更改 ntopng 和 nProbe 的客户端/服务器角色不会影响后续的流收集，因此两种配置可以互换

使用。

7.4. 在同一个设备上监视某个接口流量示例

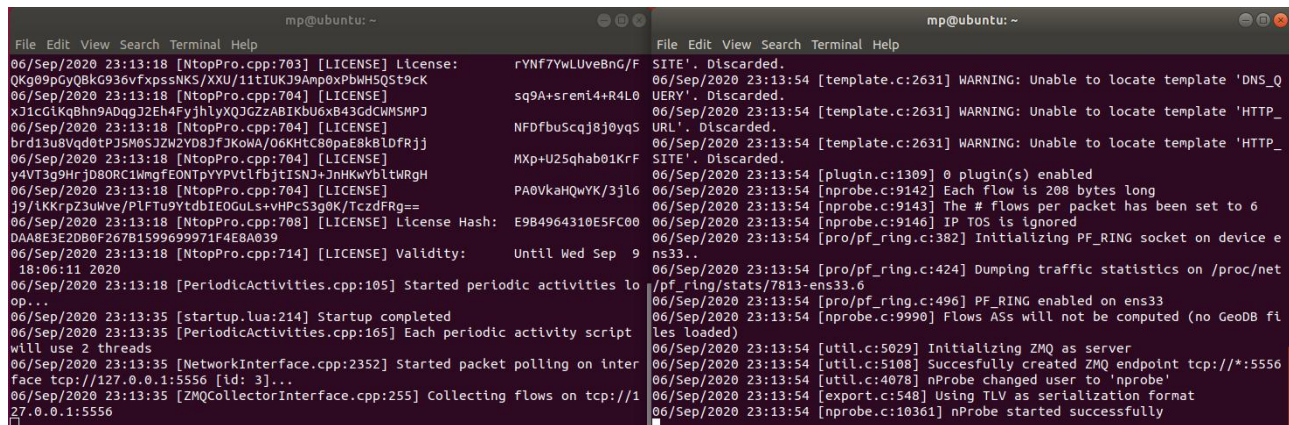
配置 ntopng:

```
sudo ntopng -i tcp://127.0.0.1:5556
```

配置 nprobe:

```
sudo nprobe --zmq "tcp://*:5556" -i ens33 -n none -T "@NTOPNG@"
```

配置完成后即可打开 web 界面:



打开 Web GUI 界面以后可以看见此时的接口变为 `tcp://127.0.0.1:5556`



7.5. 大流量监控

在监控大型网络时，流量过大，不能直接使用 ntopng 进行收集原始数据流量，而是使用 pfring ZC 和 nProbe 配合使用。

7.5.1. RRS 负载均衡

当流量较大时我们无法一次性完成流量的处理，这是需要的使用负载均衡的方法进行多线程的流量处理，最好的方法是使用 RSS，几乎所有英特尔（和其他供应商）NIC 都具有 RSS 支持，这意味着它们能够对硬件中的数据包进行哈希处理，以便将负载分配到多个 RX 队列中。

RSS 配置方法参考：https://www.ntop.org/guides/pf_ring/rss.html

7.5.2. nProbe 和 ntopng 配置

完成 RSS 配置后,使用 nProbe 在 ZC 的模式下处理流量。假设 nProbe 和 ntopng 在同一台设备上,nProbe 配置示例如下:

```
#####  
#假设配置了两个 RSS 队列  
-i=zc:ens33@0  
-i=zc:ens33@1  
-n=none  
--zmq="tcp://*:5556"  
--zmq-probe-mode=  
-T="@NTOPNG@"
```

```
#####
```

ntopng 配置示例如下:

```
#####  
-i=tcp://127.0.0.1:5556  
-m=192.168.0.0/24, 192.168.1.0/24  
#最大活动流  
-X=1000000  
最大活动主机  
-x=200000  
-F=nindex  
-G=/var/run/ntopng.pid  
#####
```

8. 在 n2disk 上使用 ntopng 示例

8.1. 流量记录简介

当需要解决网络问题或分析安全事件时,及时回溯并深入到数据包级别对于找到导致问题的确切网络活动至关重要。连续流量记录提供了进入网络历史记录关闭窗口,使您可以检索和分析该时间段内的所有原始流量。

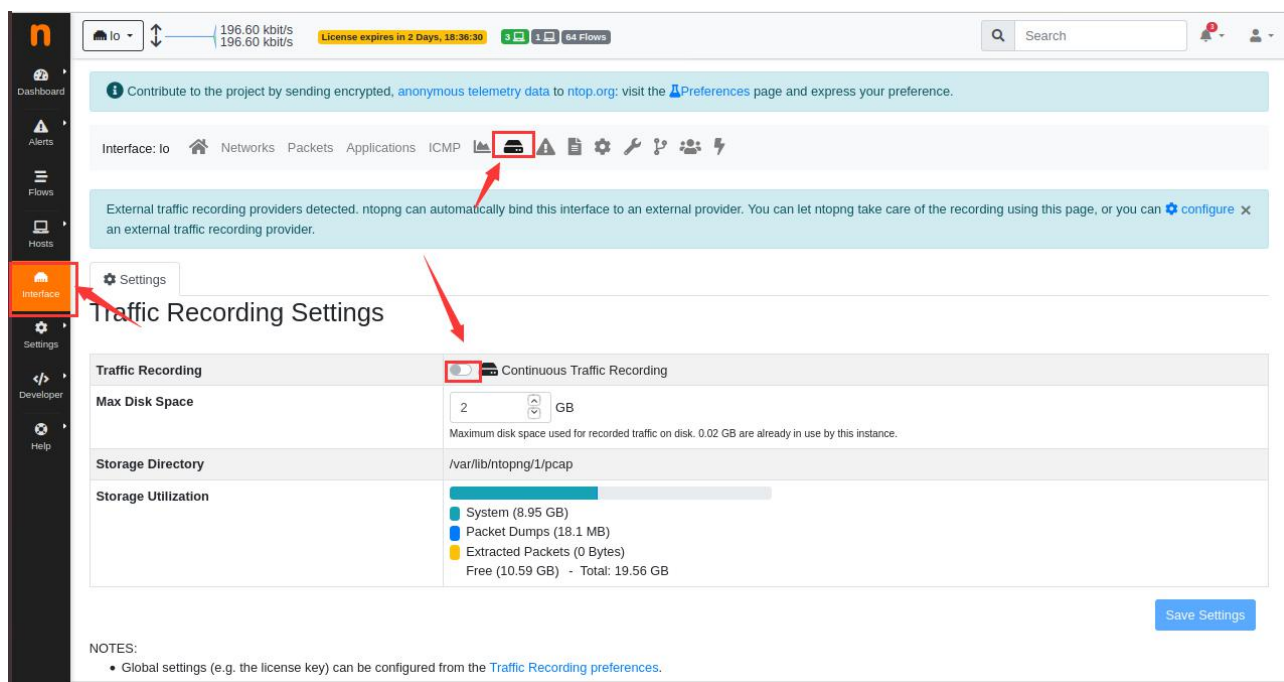
注意:

ntopng Enterprise L 已经包含一个 n2disk 1 Gbit 许可证, 如果安装了 ntopng Enterprise L 许可证, 则无需购买 n2disk 许可证。

8.2. 启动流量记录

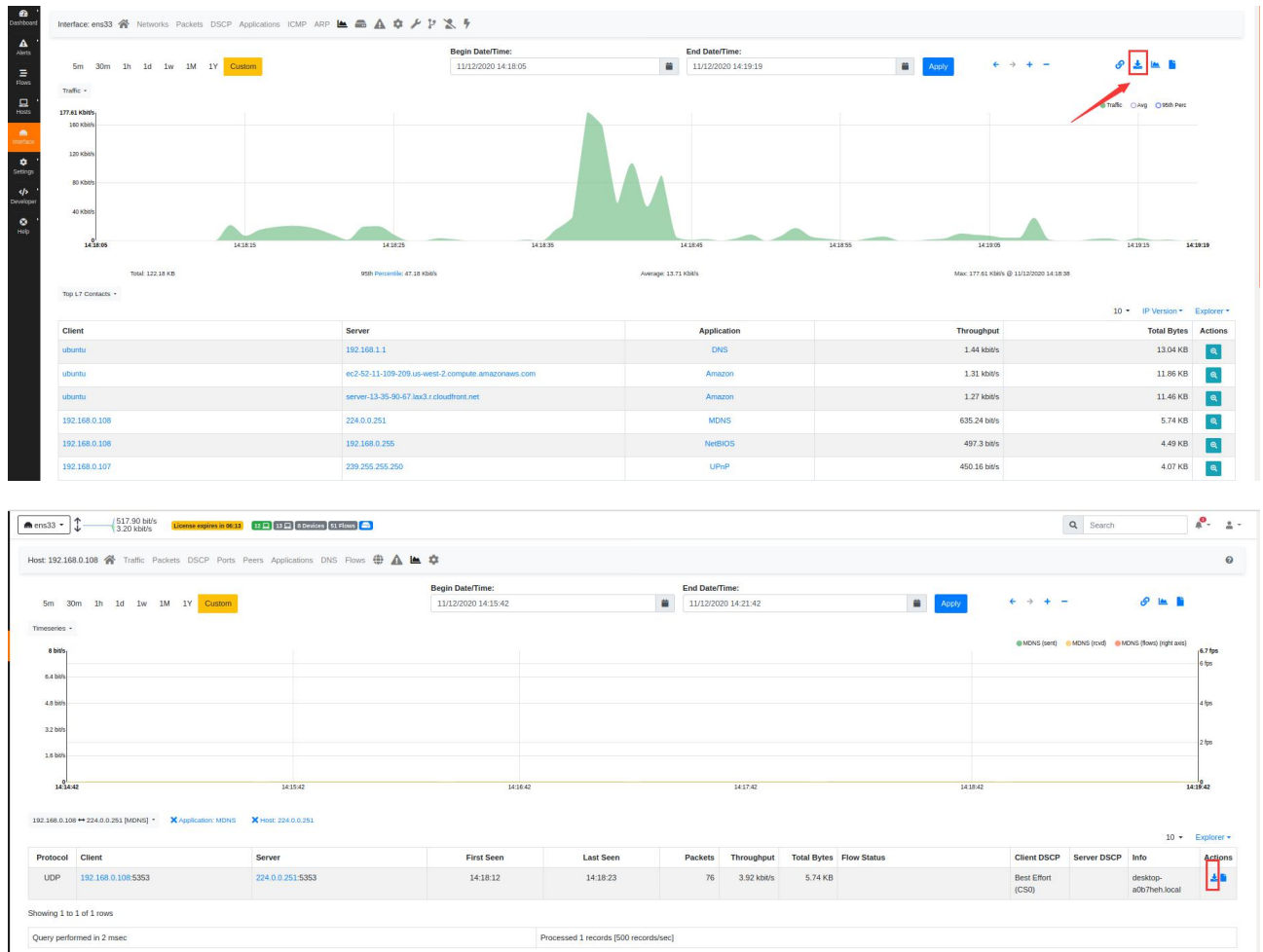
为了实际开始记录流量, 您需要从“Interface”菜单中选择一个接口, 单击  图标, 然后配置记录实例:

1. 选择“Traffic Recording”
2. 配置所需的“Max Disk Space”值。这使您可以控制用于 pcap 文件的最大磁盘空间, 这也会影响数据保留时间(超过最大磁盘空间时, 最早的 pcap 文件将被覆盖)。请注意, 数据保留时间还取决于被监视网络的流量吞吐量。
3. 按“Save Setting”按钮实际开始记录。



8.3. 下载 pcap 文件

当你启用连续流量存储记录以后, 可以在 Interface 或者 Hosts 的历史流量图界面选择特定的时间段的流量点击  进行下载:



9. 连续流量记录

使用 n2disk 连续记录流量，并提取元数据到 ntopng。

n2disk 配置示例如下：

```
#####
#捕获配置
--interface=ens33
--max-file-len=1024
--buffer-len=4096
#--reader-cpu-affinity=0
#索引配置
--index
#--indexer-cpu-affinity=1,2,3
```

#存储配置

--dump-directory=/storage

#--writer-cpu-affinity=4

--disk-limit=80%

--zmq=tcp://127.0.0.1:5556

--zmq-export-flows

#####

ntopng 配置如下:

#####

#接口配置

-i=tcp://*:5556c

#配置 web 服务端口

-w=3001

#配置本地网段

-m="192.168.0.0/24, 192.168.1.0/24"

-G=/var/run/ntopng.pid

#####

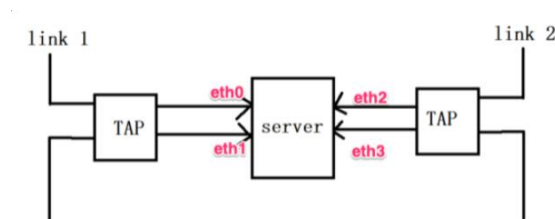
10. nProbe agent 中使用 ntopng

详细内容可查看: https://www.ntop.org/guides/ntopng/using_with_other_tools/nprobeagent.html

11. 监控 Netflow/SPAN/TAP 流量

详解示例可见: [监控 Netflow/SPAN/TAP 流量](#)

这里以 ntopng 来监控来自的 TAP 的示例: 假设我们的拓扑图如下:

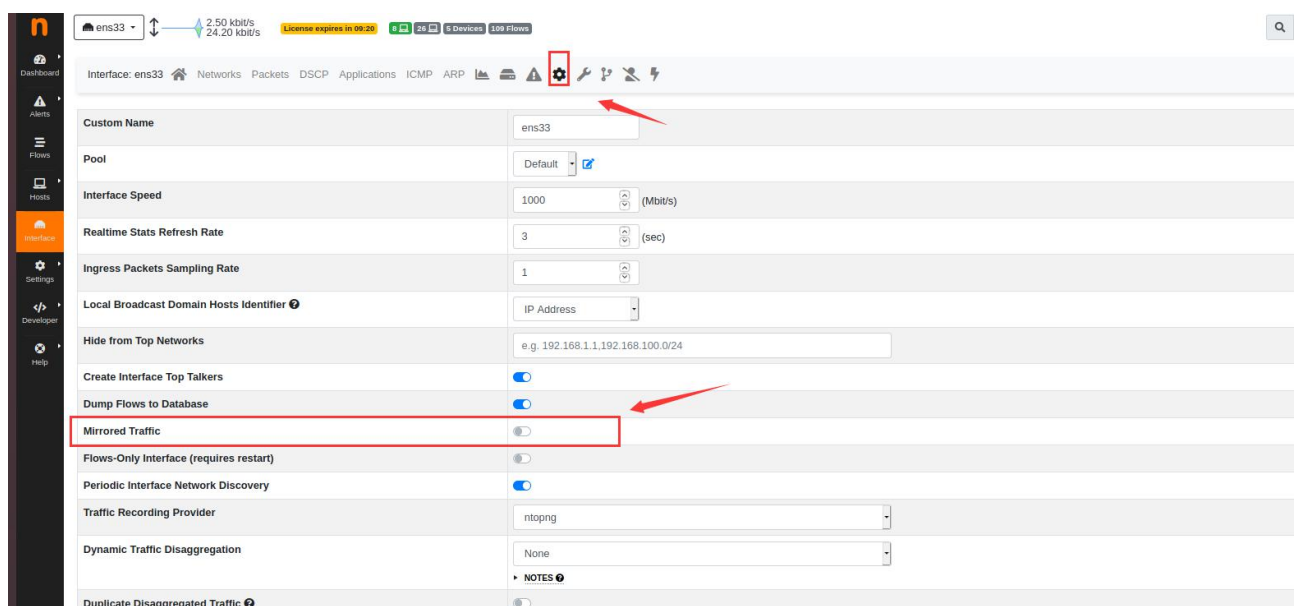


需要在配置文件（/etc/ntopng/ntopng.conf）中进行如下配置：

```
#####
#配置流量镜像接口
-i=eth0,eth1
-i=eth2,eth3
#配置流转储
-F=nindex
#配置本地网段
-m="192.168.0.0/24,172.16.1.0/24"
#以守护程序运行
-G=/var/run/ntopng.pid
#####
```

此外，由于流量是通过镜像得到，因此需要增加一个配置。

定位到 **Interface->** ，启用 Mirrored Traffic 选项。



12. ntopng 时间序列和流的磁盘要求

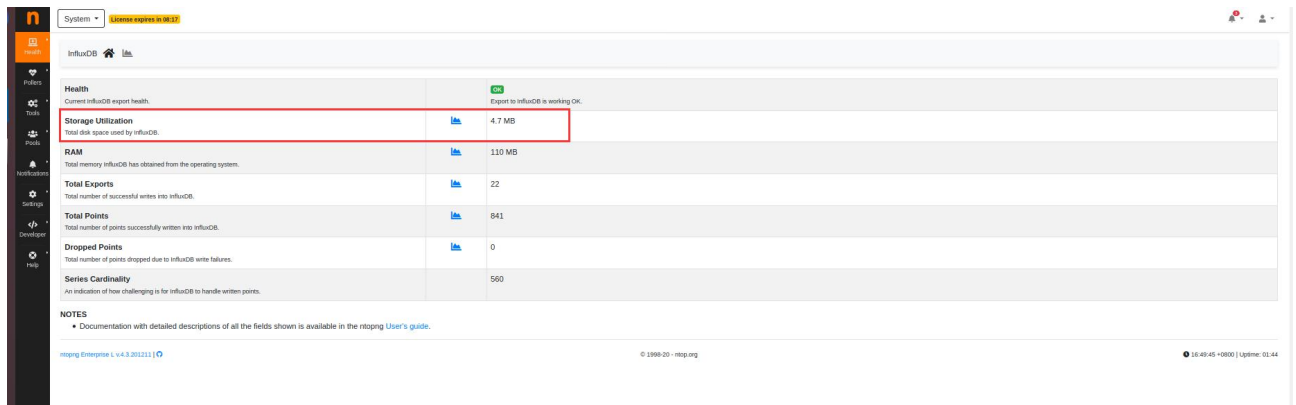
详解计算网址：

<https://www.ntop.org/ntopng/ntopng-disk-requirements-for-timeseries-and-flows/>

nindex 存储利用率在 health->system 界面下可查看特定接口的内存占用。



InfluxDB 数据库不计算在内，因为它可能是一个潜在的远程数据库。如果是本地数据库，空间可以通过查看系统和可用空间来监控，或者在 health->influxdb 界面下查看：



13. 购买 license

可在如下网址联系我们购买：

<https://hongwangle.com/ntop/traffic-analysis-and-enforcement/>

14. 关注我们

想了解跟多信息，可扫描下方二维码关注&联系我们。



网络安全与可视化

网络可视化，网络监控，时间服务器 |



☎ 400-999-3848

✉ support@hkaco.com

🌐 hongwangle.com

📍 广东省广州市高新技术产业开发区科学大道99号科汇金谷三街2号701室