

# ntopng 安装和基本使用教程

ntopng 安装和基本使用教程.....	1
1. 简介.....	2
2. 版本说明.....	3
3. 安装 ntopng.....	3
3. 1. 在 ubuntu 18.04 LTS 上安装 ntopng.....	3
3. 2. 在 CentOS 上安装.....	4
3. 3. 启动 ntopng.....	4
4. Web GUI (ntopng Enterprise ) .....	5
4. 1. 登录.....	5
4. 2. 仪表盘.....	5
4. 3. 流量报告.....	6
4. 4. 流量.....	7
4. 5. 主机划分.....	8
4. 6. 历史图表.....	11
4. 7. 首选项.....	13
4. 8. 获取 license 并激活.....	13
5. 在 nprobe 上使用 ntopng 示例.....	15
5. 1. nprobe 简介.....	15
5. 2. 多个 nProbe 到一个 ntopng.....	15
5. 3. NAT.....	16
5. 4. 在同一个设备上监视某个接口流量示例.....	17
6. 在 n2disk 上使用 ntopng 示例.....	17
6. 1. 流量记录简介.....	17
6. 2. 启动流量记录.....	18
7. ntopng 时间序列和流的磁盘要求.....	18
8. 购买 license.....	19
9. 关注我们.....	19

## 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，网络和应用程序延迟，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 ntopng

### 3. 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
```

### 3. 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 cento
```

如果需要用 PF\_RING ZC , 还需安装如下驱动:

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

### 3. 3. 启动 ntopng

```
systemctl start ntopng
```

```
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] [LIC
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: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)
```

## 4. Web GUI (ntopng Enterprise )

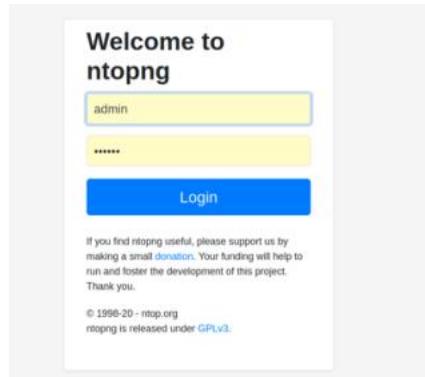
(注意：本教程后续部分均在 ubuntu 18.04 上进行，其他系统使用方法类似)

### 4. 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/>

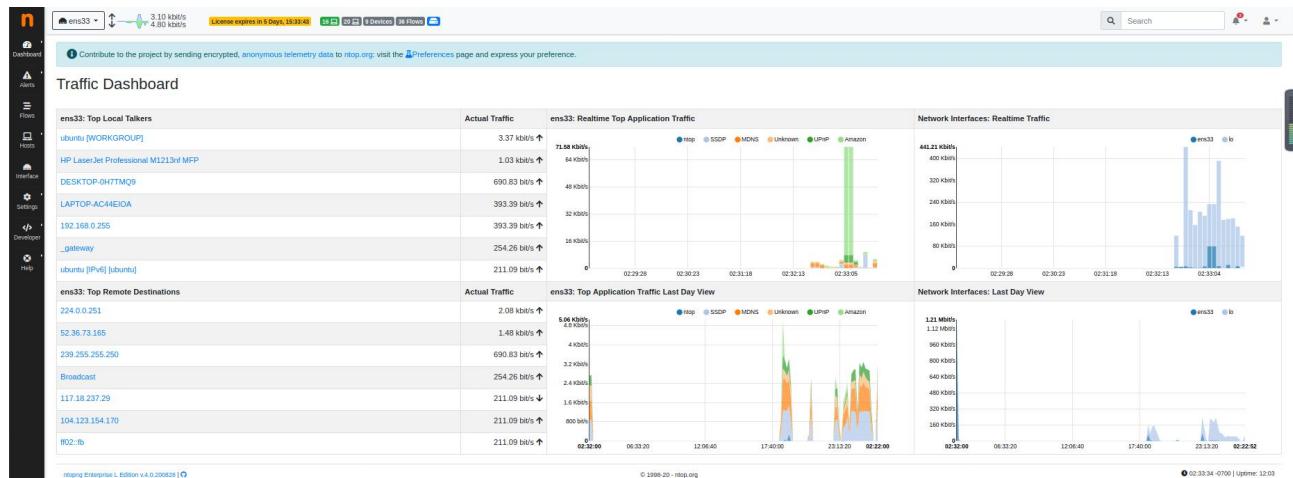


### 4. 2. 仪表盘

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  
[www.hkaco.com](http://www.hkaco.com) 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

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

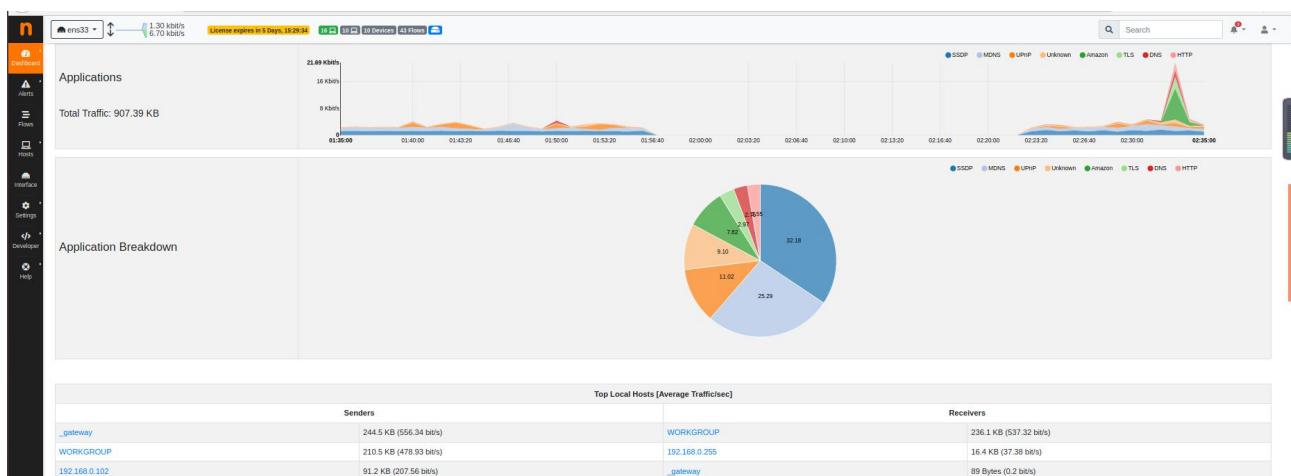


## 4. 3. 流量报告

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。

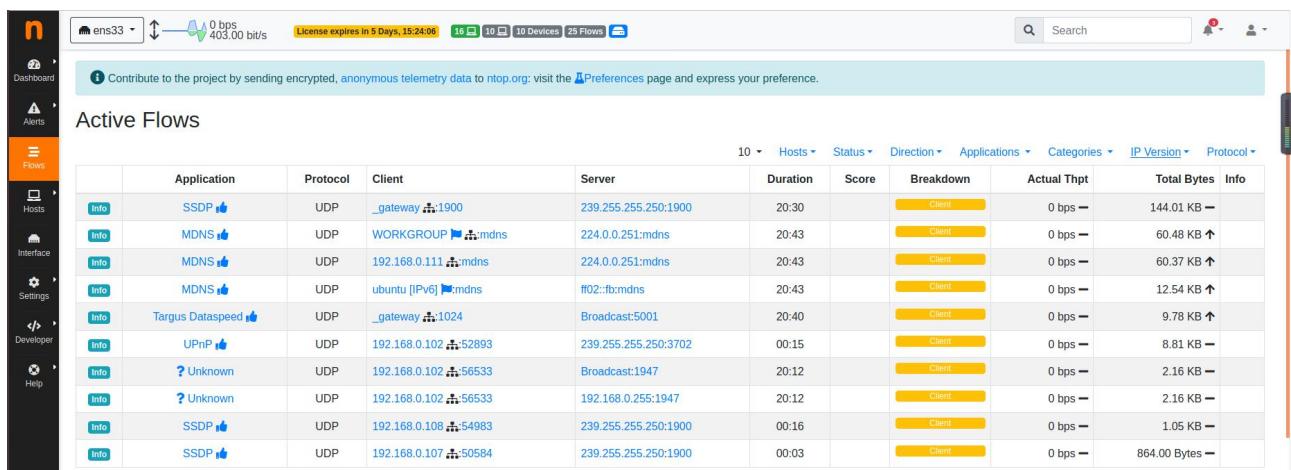
左侧有固定宽度的时间间隔。它们分别是 1h (一个小时)，1d (一天)，1w (一周)，1M (一个月)，6M (六个月) 和 1Y (一年)。单击这些间隔中的任何一个都会生成一个自动报告，该报告的时间范围从当前开始，并且时间倒退直到达到间隔。

位置： Dashboard->Traffic Report

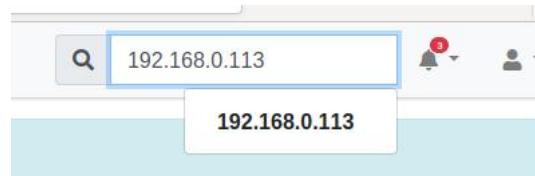


## 4.4. 流量

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。



### ● IP 搜索



搜索后可以知道特定 ip 的详细信息如下：

点击  可查看历史流信息

如下表：

指向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

## 4.5. 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。

[www.hkaco.com](http://www.hkaco.com) 广州 | 深圳 | 武汉 | 成都 | 上海 | 西安 | 北京 | 台湾 | 香港 400-999-3848

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:

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

设置主机池的名称，配置等:

Add Host Pool

Name: IOT

User Scripts Configuration: Default

Recipients:   
 builtin\_recipient\_sqlite  
 SQLite  
 builtin\_recipient\_sqlite (built-in)

Add

点击编辑主机成员:

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	

点击添加主机成员

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

Add Host Pool Member

Member Type	IP Address	Network	MAC Address
Network	192.168.98.1 / 24		
VLAN	14		
<b>Add</b>			

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								
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

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。

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

## 4. 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。

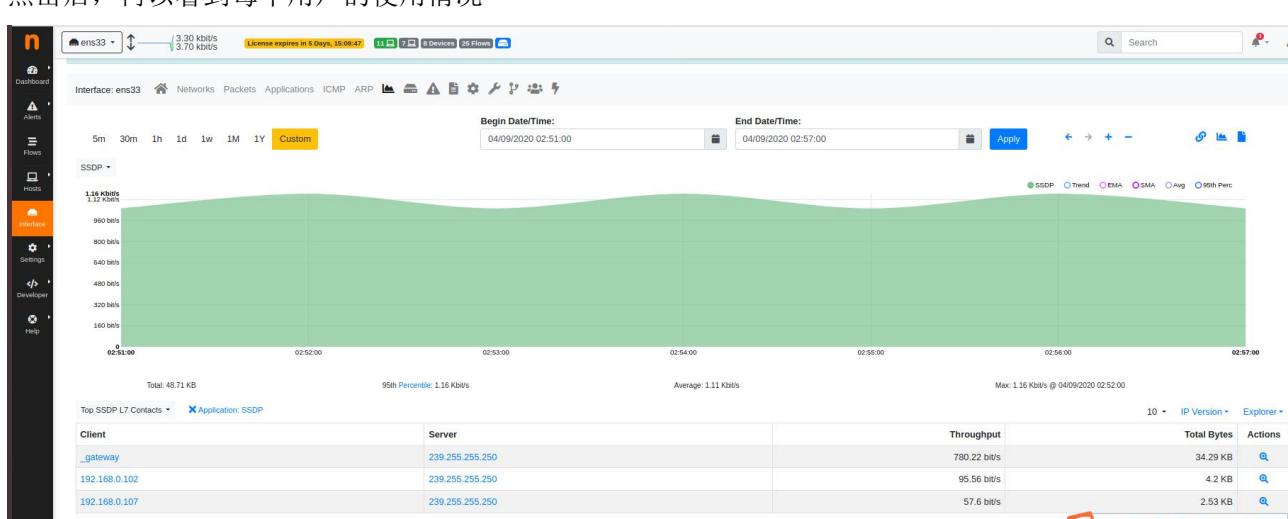
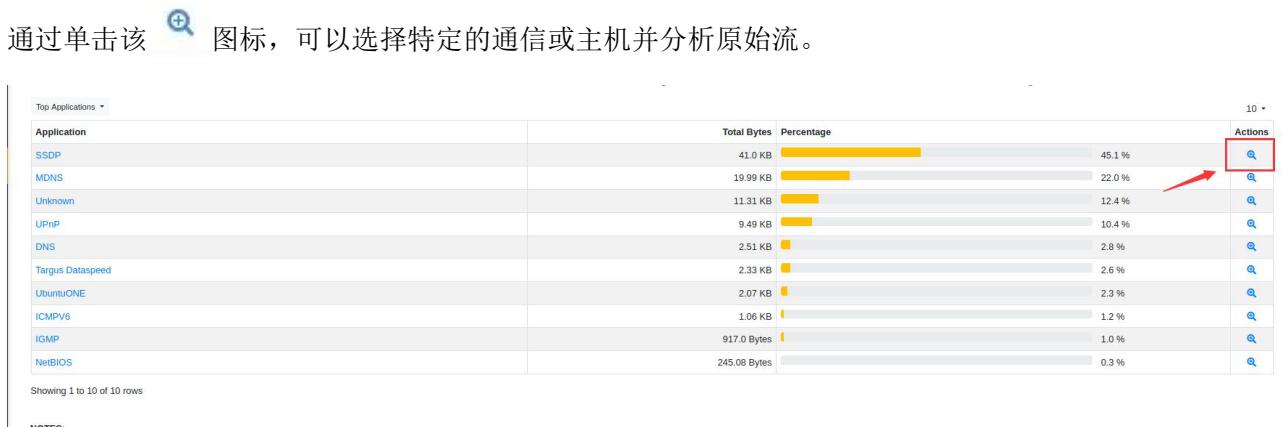
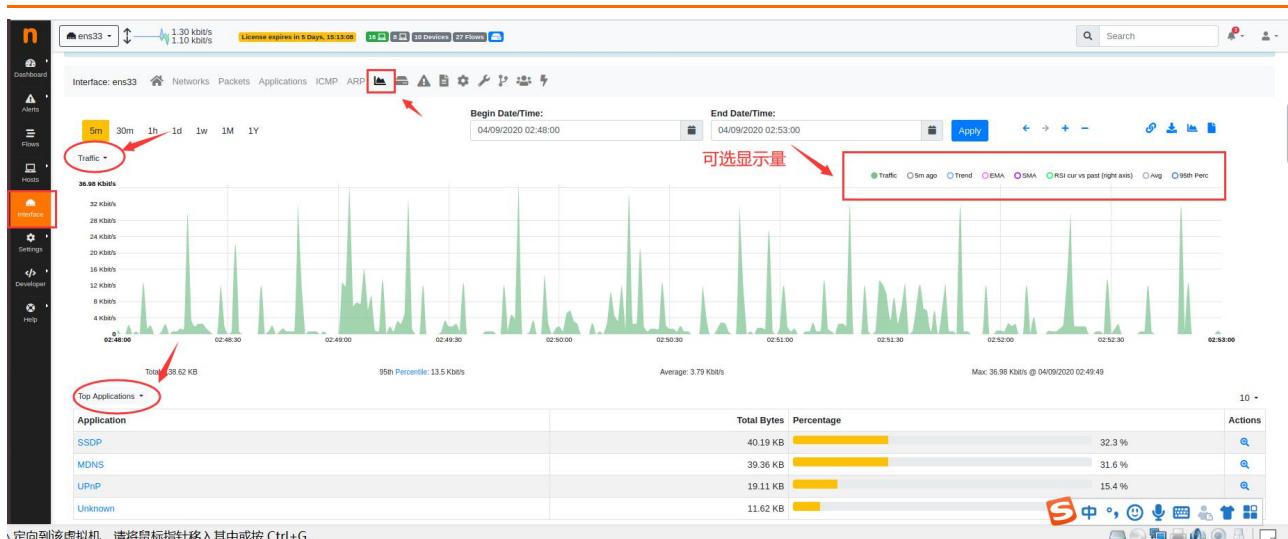
传统上，为了提供历史数据，ntopng 需要连接的 MySQL 数据库。传统上，为了提供历史数据，ntopng 需要连接的 MySQL 数据库。请查看 Flows Dump 文档，以获取有关如何设置连接的更多详细信息以及此模式可用的历史视图。

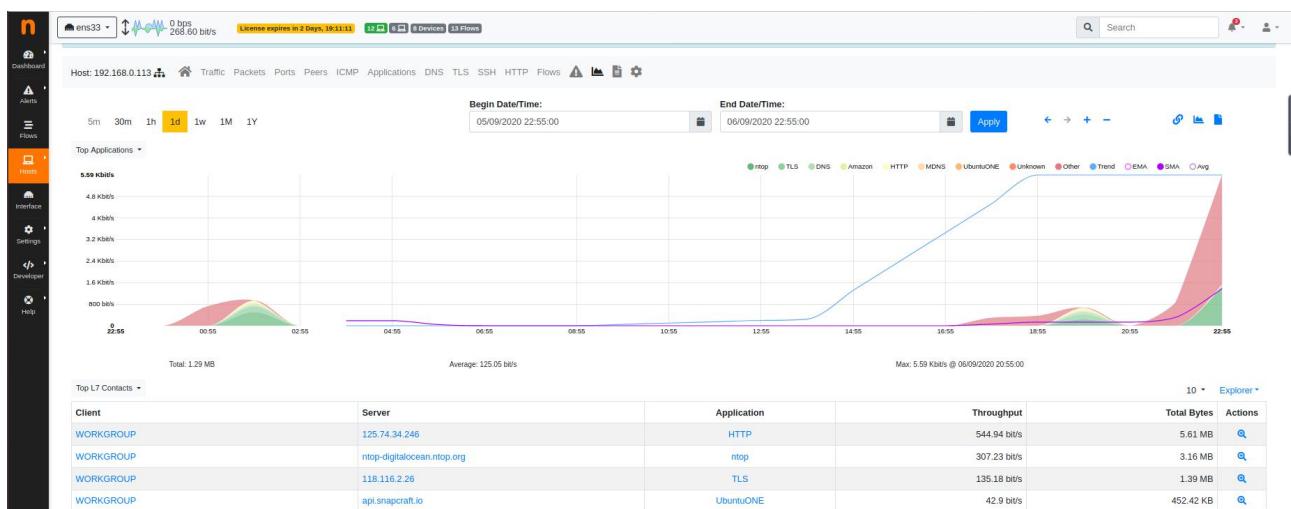
但是，由于用户对 MySQL 的低性能和高流插入率的反馈，ntopng 现在集成了一个称为 nIndex 的专用流转储数据库，它克服了 MySQL 的限制。当前仅在 Linux / x86\_64 体系结构的 ntopng 企业版中可用。

为了将流转储到磁盘，ntopng 要求指定-F nindex 选项。

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

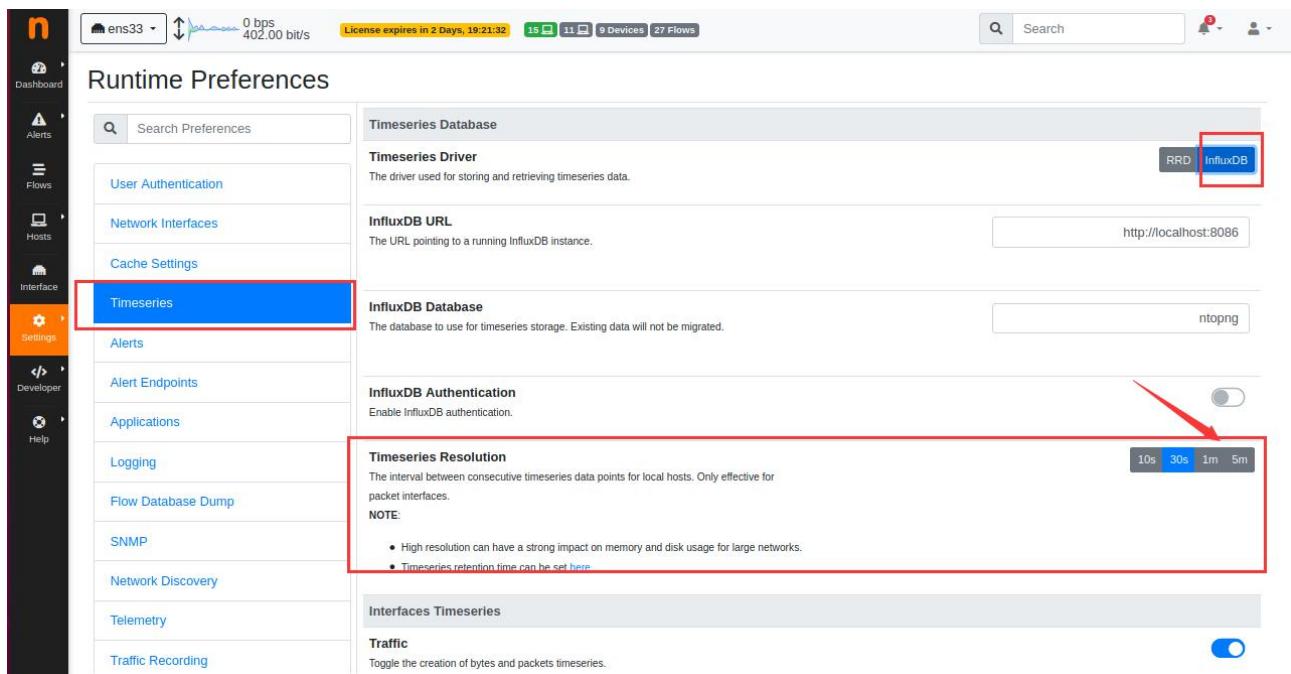
位置： interface->





## 4. 7. 首选项

在 **Settings->Preferences** 中可以配置 ntopng，例如我们可以设置时间序列的分辨率，注意使用 influxDB 需要单独安装，并且版本要求高于 1.5。



## 4. 8. 获取 license 并激活

在 **Help->About** 查看软件版本获取 License，点击图中所示位置。

About ntopng

Copyright	© 1998-20 - ntop.org
License	<a href="#">EULA [ Systemic: 3B90718600860F11 ]</a> <span style="color: red;">点击</span>
Version	4.0.200828 (11284) - Enterprise L Edition
Built on	Ubuntu 18.04.5 LTS
Platform	Debian buster/sid [x86_64][Ubuntu 18.04.5 LTS] - 64 bit
Startup Line	ntopng --dump-flows [hidden]
nDPI	3.2.0-2220-6735bb35
cURL	7.58.0
Twitter Bootstrap	4.4.0
Font Awesome	5.11.2
RRDtool	1.7.0
nIndex	1.2
Timeseries Resolution	5m
Redis Server	4.0.9
Mongoose web server	3.7

点击后会跳转到生成 license 生成界面：

ntopng License Generator

Required Information		Description
System Id:	3B90718600860F11	You can print this information within ntopng. Go to menu Home / About and you will find a URL to click on. It will bring you to this web page with all the licensing information pre-filled.
Order Id:	<input type="text"/>	This is the 10 digit order id you have placed when shopped on the ntopng site.
Email:	<input type="text"/>	This is the email associated with the order id.
ntopng Version:	4.0.200828	Example: 1.0.171098-0993-5C67-7105A-182
ntopng Edition:	Enterprise L (x64)	ntopng edition type.
<b>NOTE:</b> • 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.		
<input style="border: 1px solid red; border-radius: 5px; padding: 5px 10px; margin-right: 10px;" type="button" value="Create ntopng License"/> <input type="button" value="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。

## 5. 在 nprobe 上使用 ntopng 示例

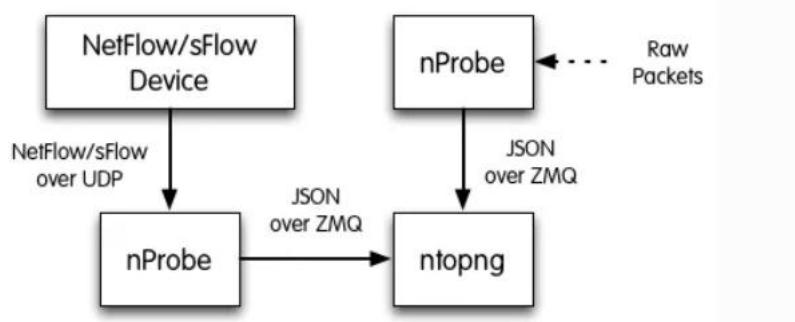
### 5.1. nprobe 简介

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

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。

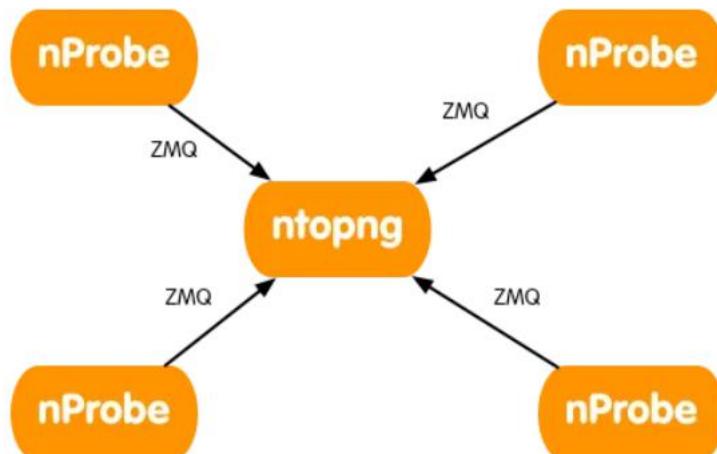
监视连接到远程系统的物理网络接口。在这种情况下，ntopng 无法直接监视网络接口，也无法看到其数据包。一个或多个 nProbe 可用于捕获远程网络接口流量并将结果流发送到中央 ntopng，以进行分析和可视化。

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。



### 5.2. 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

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@"
```

### 5. 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@"
```

上述是最简单 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。

## 5. 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:

```

File Edit View Search Terminal Help
File Edit View Search Terminal Help
06/Sep/2020 23:13:18 [NtopPro.cpp:703] [LICENSE] License: rYNf7YwLUveBnG/F SITE'. Discarded.
QKg09pgy0BkG936vfxpssNKS/XXU/11tIUk9J9Amp0xbWHSQSt9cK 06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template 'DNS_Q
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE] sq9A+sremi4+R4L0 UERY'. Discarded.
x31cG1kqBhn9AdqgJ2Eh4FyjhlyxQjGzAB1kbu6xB43GdCMMSMPJ 06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template 'HTTP_
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE] brd13u8Vqd0tP5M05JZM2YD8Jf3KoWA/06KHTc89p0E8k8l0dfRjj 06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template 'HTTP_
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE] y4V73g9Hrj0BORCiWngtEONTpYYVt1fbjtisNj+JnHKWvbtWRgH 06/Sep/2020 23:13:54 [plugin.c:1309] 0 plugin(s) enabled
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE] PA0VkaHQwYK/3j16 06/Sep/2020 23:13:54 [nprobe.c:9142] Each flow is 208 bytes long
06/Sep/2020 23:13:18 [NtopPro.cpp:714] [LICENSE] J9/LKRpz3uWve/PLfTu9YtdbIEOGULs+HPC53gOK/TczdFrq== 06/Sep/2020 23:13:54 [nprobe.c:9143] The # flows per packet has been set to 6
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE] DAABE3E2DB0F267B1599699971F4E8A039 06/Sep/2020 23:13:54 [nprobe.c:9146] IP TOS is ignored
06/Sep/2020 23:13:18 [NtopPro.cpp:714] [LICENSE] 06/Sep/2020 23:13:54 [nprobe.c:9143] Initializing PF_RING socket on device e
18:06:11 2020 06/Sep/2020 23:13:54 [pro/pf_ring.c:424] Dumping traffic statistics on /proc/net
06/Sep/2020 23:13:18 [PeriodicActivities.cpp:105] Started periodic activities lo /pf_ring/stats/7813-ens33.6
op... 06/Sep/2020 23:13:54 [pro/pf_ring.c:496] PF_RING enabled on ens33
06/Sep/2020 23:13:35 [startup.lua:214] Startup completed 06/Sep/2020 23:13:54 [nprobe.c:9990] Flows A5s will not be computed (no GeoDB fi
will use 2 threads 06/Sep/2020 23:13:54 [util.c:5029] Initializing ZMQ as server
06/Sep/2020 23:13:35 [NetworkInterface.cpp:2352] Started packet polling on inter 06/Sep/2020 23:13:54 [util.c:5108] Successfully created ZMQ endpoint tcp://*:5556
face tcp://127.0.0.1:5556 [id: 3]... 06/Sep/2020 23:13:54 [util.c:4078] nProbe changed user to 'nprobe'
06/Sep/2020 23:13:35 [ZMQCollectorInterface.cpp:255] Collecting flows on tcp://1 06/Sep/2020 23:13:54 [export.c:548] Using TLV as serialization format
27.0.0.1:5556 06/Sep/2020 23:13:54 [nprobe.c:10361] nProbe started successfully

```

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`



## 6. 在 n2disk 上使用 ntopng 示例

### 6. 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

[www.hkaco.com](http://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](mailto:sales@hkaco.com) [support@hkaco.com](mailto:support@hkaco.com) 电话:020-38743030 , 38743032 传真:020-38743233

活动至关重要。连续流量记录提供了进入网络历史记录的窗口，使您可以检索和分析该时间段内的所有原始流量。

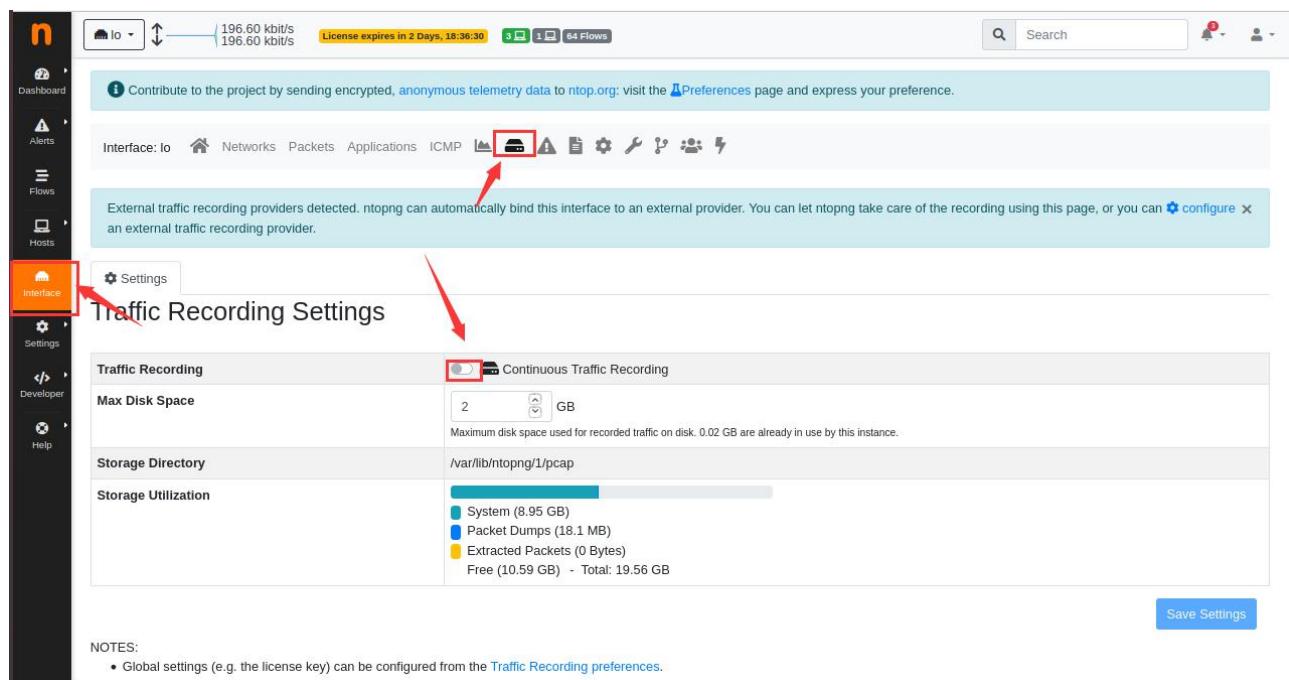
注意：

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。

## 6. 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。



The screenshot shows the ntopng web interface. The left sidebar has a 'Interface' menu item highlighted with a red box. The main content area shows the 'Traffic Recording Settings' page. At the top, there is a message about external traffic recording providers. Below that, the 'Traffic Recording' section has a checkbox for 'Continuous Traffic Recording' which is checked. The 'Max Disk Space' field is set to 2 GB. The 'Storage Directory' is set to '/var/lib/ntopng/1/pcap'. The 'Storage Utilization' section shows disk usage: System (8.95 GB), Packet Dumps (18.1 MB), Extracted Packets (0 Bytes), and Free (10.59 GB) - Total: 19.56 GB. At the bottom right, there is a 'Save Settings' button highlighted with a red box.

## 7. 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/>

[www.hkaco.com](http://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](mailto:sales@hkaco.com) [support@hkaco.com](mailto:support@hkaco.com) 电话:020-38743030 , 38743032 传真:020-38743233

## 8. 购买 license

可在如下网址联系我们购买：

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

## 9. 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