

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

# HongKe

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 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



广州虹科电子科技有限公司

mp@ubunt	J:~\$	inf	luxd									
8888888			.d888	888					8888	888b.	8888	888b.
888			d88P"	888					888	"Y88b	888	"88b
888			888	888					888	888	888	.88P
888	8888	38b.	888888	888	888	888	888	888	888	888	8888	8888K.
888	888	"88b	888	888	888	888	Y8b	d8P'	888	888	888	"Y88b
888	888	888	888	888	888	888	X8	8K	888	888	888	888
888	888	888	888	888	Y88b	888	.d8"	"8b.	888	.d88P	888	d88P
8888888	888	888	888	888	"Y88	3888	888	888	8888	888P"	8888	8888P"
2020-12-	11T06	5:53:0	08.8495	37Z	in "com	nfo nit"	In "cd	fluxi	DB st	arting	adgae	{"log_id": "0R0927S0000", "version
2020-12-	11T06	5:53:0	98.8496	627	i	fo	. CO	run	time	101000	100	id": "08092750000" "version": "ao1.
9.2", "ma	ахрго	ocs":	2}							a Nasta		
run: oper	n ser	ver:	listen	: 11	sten 1	сср	127.0	.0.1	:8088	: Dind	: ado	dress 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

# HongKe

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

# 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 1
Loaded: loaded (/etc/svstemd/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] [LIG
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.cg
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



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

在最后页面最后可以查看可用接口序号:

Availa	able interfaces (-i <interface index):<="" th=""></interface>
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] ntopngcommunity
11/Dec/2020 15:57:46 [PcanInterface cnp:93] Reading packets from 1 [id: 1]

## 4.4. 在 windows 上安装

windows 安装参照: <u>https://www.ntop.org/guides/ntopng/what is ntopng.html#installing-on-windows</u>

### 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

### (1) 接收协议

🛃 Setup - ntopng 4.3.201103	-		×
License Agreement Please read the following important information before continuing.			
Please read the following License Agreement. You must accept the tern agreement before continuing with the installation.	n <mark>s o</mark> f th	ils	
This tool will install ntopng and some companion packages: - redis - Microsoft Visual C++ Redistributable - Win10Pcap Drivers For complete installation instructions, please refer to <u>https://www.ntop.org/guides/ntopng/what_is_ntopng.html#installing-</u> See <u>https://www.ntop.org/legal/</u> for ntop EULA.	<u>on-win</u>	dows	
<ul> <li>I accept the agreement</li> <li>I do not accept the agreement</li> </ul>			
Next	>	Ca	ncel

### (2) 空置命令



广州虹科电子科技有限公司

🕼 Setup - ntopng 4.3.201103		5 <del></del> 6		×
Configure Information				
Please specify the command line options for installing th	e ntop s	ervice		
Command Line: (leave blank if unsure)				
<u>p</u>				
				2
< Back		Next >	Ca	incel

(3) 选择目录





🕼 Setup - ntopng 4.3.201103		() <del>,</del> )		×
Select Start Menu Folder Where should Setup place the program's shor	tcuts?		(	
Setup will create the program's shortcu	uts in the following S	Start Menu f	older.	
To continue, click Next. If you would like to s	elect a different fold	er, click Bro	wse.	
			100030	
[	< Back	Next >	Car	ncel

#### (4) 安装

Setup is now ready to begin inst	talling ntopng	on your com	outer.		C
Click Install to continue with the	installation, o	or click Back if	you want to i	review or	
change any settings.					
Configuration: Service command line: nto Destination location: D:\Program Files\ntopng	png /i				^
					~
<				>	

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



SWINTUPcap Setup			
End-User License Agreement		Win10P	cap
Please read the following license a	agreement carefully.	Ethernet pack for Windows	et capture library 7, 8 and 10.
GNU GENERAL PUE Version 2, June 1	BLIC LICENSE 991		^
Copyright (C) 1989, 1991 Free 5 51 Franklin Street, Fifth Floor, B Everyone is permitted to cop document, but changing it is no	Software Foundation, In Boston, MA 02110-1301 py and distribute verb pt allowed.	uc., USA atim copies of th	is license
Preamble The licenses for most software	e are designed to take a	away your freedom	n to share 🗸
$\checkmark$ I accept the terms in the License	e Agreement		
Pri	int Back	Next	Cancel
Pri	int Back	Next	Cancel
Pri	int Back	Next	Cancel
Pri Win10Pcap Setup Destination Folder	int Back	Next — Win10P	Cancel

Destination Folder Click Next to install to the default folder.	Win10Pcap Ethernet packet capture libra for Windows 7, 8 and 10.
Install Win10Pcap to:	
C:\Program Files (x86)\Win10Pcap\ Change	
	Back Next Cancel

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





### 4.4.2. Redis 安装

(1) 开始安装, 点击 next

HongKe

🛃 Redis on Windows Setup	- 🗆 X
<b>et in the second secon</b>	Welcome to the Redis on Windows Setup Wizard The Setup Wizard allows you to change the way Redis on Windows features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel

(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



	tup		() <del>,</del> ()		>
End-User License Agi	reement			2	3
Please read the followin	g license agreement carefully	1		red	is
Copyright © 2006-2	2015, Salvatore Sanfilip	ро			^
Modifications Copy	right © Microsoft Ope	n Technologies,	Inc.		
All rights reserved.					
Redistribution and	use in source and bina	ry forms, with o	r witho	ut	
modification, are po met:	ermitted provided that	the following co	onditio	ns are	~
modification, are point and met:	ermitted provided that	the following co	onditio	ns are	~

#### (3) 勾选 Redis 注册到系统环境变量中

Fredis on Windows Setup		() <del>,</del> ()		$\times$
Destination Folder			2	
Click Next to install to the default fold	ler or click Change to choose anothe	r.	red	is
Install Redis on Windows to:				
C:\Program Files\Redis\				
Add the Dedic installation folder to	the DATH environment variable			
Add the Redis installation folder to	the PATH environment variable.			
1				
/				

(4) 选择端口默认 6379,并勾选择防火墙例外。
 www.hkaco.com
 广州|深圳|武汉|成都|上海|西安|北京|台湾|香港
 400-999-3848

<u>sales@hkaco.com</u> <u>support@hkaco.com</u> 电话:020-38743030 , 38743032 传真:020-38743233



🚜 Redis on Windows Setup	19 19		×
Port Number and Firewall Exception		2	
Select whether to add an exception to the Windows Firewall for Redis.		red	is
Port to run Redis on: 6379			
Add an exception to the Windows Firewall.			
Back Next		Cance	2l

(5) 勾选最大内存限制,设置为100M,点击 next

	9 <del></del> 0		<
JL.		redis	
	ot.	ot.	ot.

(6) 点击 install





#### (7) Finish

Redis on Windows Setup		-	1	×
redis on windows Setup	Completed the Redis on Wi Wizard Click the Finish button to exit the Setup V	indow. Wizard.	s Setup	×
	Back Finish		Cance	1

(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



命令 config set requirepass <mypasswd> 设置密码



(9)打开服务:再在右侧找到 Redis 名称的服务,启动 Redis。

🔍 服务						- 0	×
文件(F) 操作(A) i	查看(V) 帮助(H)						
(+ +) 🖬 🗐	) 📑 🚺 🖬 🕨 🔳 🕪						
🥝 服务(本地)	⑤ 服务(本地)						
	Redis	名称	描述	状态	启动类型	登录为	^
		🤹 qmbsrv	电脑	正在	自动	本地系统	
	停止此服务	QPCore Service	腾讯	正在	自动	本地系统	
	重启动此服务	QQPCMgr RTP Service	电脑	正在	自动	本地系统	
		Quality Windows Audio Vi	优质	正在	手动	本地服务	
	描述:	🤹 Realtek Audio Universal Se	Realt	正在	自动	本地系统	
	This service runs the Redis server	🧟 Realtek Bluetooth Device		正在	自动	本地系统	
		🙀 Redis	This	正在	自动	网络服务	
		🤹 Remote Access Auto Conn	无论		手动	本地系统	
		Remote Access Connectio	管理	正在	自动	本地系统	
		🎑 Remote Desktop Configur	远程		手动	本地系统	
		🤹 Remote Desktop Services	允许		手动	网络服务	
		Remote Desktop Services	允许		手动	本地系统	
		🤹 Remote Packet Capture Pr	Allo		手动	本地系统	
		Remote Procedure Call (R	RPC	正在	自动	网络服务	
		Remote Procedure Call (R	在W		手动	网络服务	
		Remote Registry	使远		禁用	本地服务	
1		Routing and Remote Access	在局		禁用	本地系统	
		RPC Endpoint Mapper	解析	正在	自动	网络服务	
		Secondary Logon	在不		手动	本地系统	
	11日(日本)	C Secure Socket Tunneling P	提供	正在	王动	木地昭名	•
	11 11 11 11 11 11 11 11 11 11 11 11 11						



#### 4.4.3. 启动 ntopng

(1) Win+R 输入 cmd 打开命令窗口

🜌 运行				×
	Windows 夹、文档回	将根据你所输入! 戊 Internet 资源。	的名称,为你打开	相应的程序、文件
打开(Q):	cmd			~
	[	确定	取消	浏览( <u>B</u> )

(2) 导航到 ntopng 安装目录下

D:\>cd D:\H	Program Files\ntopng	
D:\Program	Files\ntopng>	

(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

ntop	ng
admin	
Password	(default admin)
	Login
	🔒 Unable to login? 🗹
f you find nto making a sma run and foster Thank you.	png useful, please support us by Il donation. Your funding will help to the development of this project.
© 1998-20 - n ntopng is rele	top.org ased under GPLv3.

(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 )

om 选择管理员: 命令提示符		-	$\times$
Unrecognized option: /h> Available options: /i [ntopng options] - Install stopng as service /c - Run stopng on a console /r - Deinstall the service /h - Prints this help	以管理员身身份打开 ·		^
Usage: type ntopng /c -h			
):\Program Files\ntopng>ntopng /i ntoping 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



(3) 选择 startup.bat 完成服务注册





pplication Detail	s   Log on   Dependencies	Process Shutdown	Exit_
Application			
Path:	D:\influxdb\influxdb-1.8.4-	1\startup.bat	
Startup directory	D:\influxdb\influxdb-1.8.4-	1	
Arguments:			

(4) 在服务里启动 infuxdbService:

🔍 服务					<u>~</u>	- 🗆	×
文件(F) 操作(A) 計	查看(V) 帮助(H)						
( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	🕽 📑 🛛 🖬 🕨 🖬 🕪						
服务(本地)	◎ 服务(本地)						
	influxdbService	名称	描述	状态	启动类型	登录为	^
		🎑 Hyper-V Heartbeat Service	通过		手动(触发	本地系统	
		🍓 Hyper-V PowerShell Direct	提供		手动(触发	本地系统	
	里后动此的交牙	🍓 Hyper-V Time Synchroniza	将此		手动(触发	本地服务	
		🖳 Hyper-V 卷影复制请求程序	协调…		手动(触发	本地系统	
		A Hyper-V 远程桌面虚拟化服务	提供…		手动(触发	本地系统	
		🖳 IKE and AuthIP IPsec Keyin	IKEE	正在	自动(触发	本地系统	
		influxdbService		正在	自动	本地系统	
		internet Connection Sharin	为家		手动(触发	本地系统	
		🎑 IP Helper	使用	正在	自动	本地系统	
		🔍 IP 转换配置服务	配置		手动(触发	本地系统	
		🎑 IPsec Policy Agent	Inter	正在	手动(触发	网络服务	
		🎑 KtmRm for Distributed Tra	协调		手动(触发	网络服务	
		🎑 Lenovo Driver Service	联想	正在	自动	本地系统	
		🎑 Lenovo Notebook ITS Serv		正在	自动	本地系统	
		🎑 LenovoDRS	联想		手动	本地系统	
		🎑 LenovoPcManagerService	联想		手动	本地系统	
		🎑 LenovoPCMKeyService			手动	本地系统	
		🖏 Link-Layer Topology Disco	创建		手动	本地服务	
		🖏 Local Session Manager	管理	正在	自动	本地系统	
		Massage Queuing	担/計	正左	白动	网纹服冬	~
	\扩展 \ 标准 /						

(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。

<u>www.hkaco.com</u> 广州 深圳 武汉 成都 上海 西安 北京 台湾 香港 400-999-3848

<u>sales@hkaco.com</u> <u>support@hkaco.com</u> 电话:020-38743030, 38743032 传真:020-38743233



Microsoft 10.40 kbit/s ticen	eespires in 0942 [38 🖵 (4 Devices) (49 Flows	Q 9	Search	•	L _	<u>h</u> -
Runtime Preferences	<b>_</b>					0
Alerts Q Search Preferences	Timeseries Database					
Flows User Authentication	Timeseries Driver The driver used for storing and retrieving timeseries data.			RRD Int	fluxDB 1	×
Hosts Network Interfaces	InfluxDB URL			http://localhos	st:8086	
Cache Settings	ine one pointing to a futting interde ristance.					
timeseries	InfluxDB Database			r	ntopng	
Alerts	i i is senere to es te initiativa antigo antengo en initiati a inglitare.					
Logging	InfluxDB Authentication Enable InfluxDB authentication.					)
SNMP	Timeseries Resolution				1m Sr	m
Network Discovery	The interval between consecutive timeseries data points for local hosts NOTES					
Telemetry	Lowering the resolution can create gaps in the existing data. It is advisable to delete the database					
Data Retention	Interfaces Timeseries					
User Interface	Traffic Toggle the creation of bytes and packets timeseries.				C	)
Misc Expert View Simple View	Layer-7 Applications Toggle the creation of Layer-7 application timeseries. Creating a timeseries per application requires more disk space and	I	None Per Applicati	on Per Catego	ny Bot	:h

# 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

<u>sales@hkaco.com</u> <u>support@hkaco.com</u> 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



广州虹科电子科技有限公司

ens33      Conse expires in 5 Days, 1533:43	县 😰 🚍 🖲 Devices 🛛 36 Flows 🚍		Q Search
Contribute to the project by sending encrypted, anonymous telemetry data	to ntop.org: visit the APreferences page and express your pr	ice.	
Traffic Dashboard			
ens33: Top Local Talkers	Actual Traffic	33: Realtime Top Application Traffic Network	< Interfaces: Realtime Traffic
ubuntu [WORKGROUP]	3.37 kbit/s ↑	entop © SSDP  MDNS  Unknown  UPnP  Anzon	ero33 0
HP LaserJet Professional M1213nf MFP	1.03 kbit/s 🛧	64 Kbits 400 Kb	its
DESKTOP-0H7TMQ9	690.83 bit/s 🛧	48 Kbits 320 Kb	ids.
LAPTOP-AC44EIDA	393.39 bit/s 🛧	240 Kb	
192.168.0.255	393.39 bit/s 🛧	100 Kb	in a state of the
_galeway	254.26 bit/s 🛧	26 KB/S	25
ubuntu (IPv6) (ubuntu)	211.09 bit/s 🛧	022928 023023 023118 023213 0233.05	0 022928 023023 023118 023213 023304
ens33: Top Remote Destinations	Actual Traffic	33: Top Application Traffic Last Day View Network	Interfaces: Last Day View
224.0.0.251	2.08 kbit/s 个	teop SSDP MDNS Unknown UPnP Amazon     121 Mb	itis, erass 💿
52.36.73.165	1.48 kbit/s 🛧	1.12 Mb	(#5.
239.255.255.250	690.83 bit/s 🛧	32 Kisto	205
Broadcast	254.26 bit/s <b>↑</b>	2.4 K0055	205
117.18.237.29	211.09 bit/s 🗸	480 K2	492
104.123.154.170	211.09 bit/s 🛧	800 bits	**
ff02::fb	211.09 bit/s 个	02.12:00 06:33:20 12:06:40 17:40:00 23:13:20 02:12:00 0	0 32:32:00 06:33:20 12:06:40 17:40:00 23:13:20

### 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 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



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。

n	nens33	• \$ 0 bps 403.00 bit/s	License expires	in 5 Days, 15:24:06 16 🖵 10 🖵 10 Dev	ices 25 Flows 🚍				Q Search		₽. ≗.
Dashboard	Cont	tribute to the project by sending	g encrypted, ano	nymous telemetry data to ntop.org: vi	sit the APreferences page and expr	ess your preference.					
Alerts '	Active	e Flows									
Elour						10 - Hosts -	Status -	Direction - Applica	ations - Categories	IP Version - I	Protocol -
- Cons		Application	Protocol	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Byte	s Info
Hosts	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	4
Interface	Info	MDNS 💼	UDP	192.168.0.111 <b></b> :mdns	224.0.0.251:mdns	20:43		Client	0 bps —	60.37 KB	4
Settings	Info	MDNS 💼	UDP	ubuntu (IPv6) 🝽:mdns	ff02::fb:mdns	20:43		Client	0 bps —	12.54 KB	4
	Info	Targus Dataspeed 💼	UDP	_gateway 🚓:1024	Broadcast:5001	20:40		Client	0 bps —	9.78 KB	4
Developer	Info	UPnP 👍	UDP	192.168.0.102 🚓:52893	239.255.255.250:3702	00:15		Client	0 bps —	8.81 KB -	-
O ·	Info	? Unknown	UDP	192.168.0.102 🚓:56533	Broadcast:1947	20:12		Client	0 bps —	2.16 KB -	-
neib	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 <del>-</del>	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

۹	192.1	68.0.113	<b>*</b> ••	*	*
		192.168.0.113			

#### 搜索后可以知道特定 ip 的详细信息如下:

n	(ms33 • )			Q, Search	<b>P</b> - ±-
Dashboard	Contribute to the project by sending encrypted, anonymous telemetry data to ntop org: visit the APreferences page a	nd express your preference.			
Aletts	Host 192.168.0.113 🚠 🌴 Traffic Packets Ports Peers ICMP Applications DNS TLS SSH HTTP Fig	** A 🗠 B 🌣			
Flows	(Router/AccessPoint) MAC Address	Vmware_8D:6B:84 ( 00:0C:29:8D:6B:84 )	Computer 🗘		
Hosts	IP Address	192.168.0.113 [ 192.168.0.0/24 ]	Host Pool: Not Assigned 🌼		
	os	👌 Linux (Ubuntu)			
Interface	Name	WORKGROUP 🗹 🛊 🚥 🔐 Phane 🚬			
Settings	Score in	0 -			
	RTT	13.89 ms			
Developer	First / Last Seen	03/09/2020 22:53:47 [03:51:20 ago]	04/09/2020 02:45:05 [00:02 ago]		
e '	Sent vs Received Traffic Breakdown	Sector Sect	Rod		
	Traffic Sent / Received	10,757 Pkts / 1.7 MB 🛧	9,857 Pkts / 6.6 MB -		
		As Client	As Server		
	Flows: Active / Total / Anomalous / Port Unreach Q	13 4 / 2,079 - / 76 - / 4 -	0-/22-/9-/0-		
	Peers: Active	34	0		
	TCP: Retransmissions / Out of Order / Lost / KeepAlive	Sent	Received		
		301 Pkts -/ 11 Pkts -/ 37 Pkts -/ 233 Pkts -	48 Pkts = / 661 Pkts = / 330 Pkts = / 61 Pkts =		
	Reset Host Stats	Reset Host Stats			
	Additional Host Names	Source	Name		
		DHCP	ubuntu		
	Download 🛃	350N	1 min Piter (BPF) pcap download	°, 🙂 🎙 📟 🛻 1	

# 点击 🖿 可查看历史流信息

Host: 192.168.0.113 🚓 🌴 Traffic Packets Parts Peers ICMP Applications DNS TLS SSH HTTP Flows 🛦 🖿 🖆 🀲

如下表:



广州虹科电子科技有限公司

nens33 •	1	1.30	kbit/s kbit/s		License expires in 5 Days, 15:17:40	17 🖵 7 🖵 10 Devices	23 Flows 🔚				Q	Search			₽.
5m 30	m 1h	1d	1w	1M	1Y	04/09/2020 02	:15:00	64/09/2020 02:45:	00	Apply	← →	+ -	. 8	Ø 🛓 🖿	
Traffic 💌								Sant Roud	30m ann			t (right avis)	O Aug	0 05th Derc	
6.4 Kbit/s											in to pass	(ingrit data)	Only	<b>O</b> Souri de	
4.8 Kbit/s															
3.2 Kbit/s															
1.6 Kbit/s															
02:15:0	00				02:20:00	02:25:00	02:3	0:00	02:35:00	(	)2:40:00			02:4	.5:00
	Total: 493.1	0 KB			95th Percentile:	5.52 Kbit/s	Ą	verage: 2.24 Kbit/s		Max: 6.4 Kb	it/s @ 04/	/09/2020 0:	2:25:00		
Application	ins •					Sent	Received	Percentage						Total Bytes	10 Acti
ntop						10.64 KB	169.64 KB			36.9 %				180.29 KB	e
Amazon						52.63 KB	34.21 KB	_		17.8 %		a.		86.84 KB	e
												- 4	」。, 🙂	) 🖳 🔜 🧳	6 🔳

# 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->hoots,点击增加主机池:

n	System - Upgra	de to Pro/Enterprise version 🕑	٩	Search	<b>Å</b> •- <b>±</b> -
♥ ' Health	Pools				
Ç ' System	Hosts Inter	faces Local Networks Active Monitoring Host F	Pool Flows Devices System All		
tools	Show 10 ¢	entries		Search:	+
Pools	Namo	Mombara	Bosinianto	User Scripts	10000
Notifications	Name 1	Allumbers	Recipients	Defects	Actions
۰ ت	Delaun	All unbound	buintn_recipient_squite	Delauit	
Settings	Mypool	192.168.98.133	builtin_recipient_sqlite	Default	s 🕑 🥫
</ </ </t	office	192.168.1.1/24@10	builtin_recipient_sqlite	Default	s C 💼

设置主机池的名称,配置等:



Add Host Pool		3
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:

Hosts	Interf	aces Local Networks Active Monitoring H	Host Pool Flows Devices System All			
Show	10 ¢ e	ntries		S	Search:	
Name	ţ.	Members	Recipients		User Scripts Configuration	Actions
Defaul	t	All unbound	builtin_recipient_sqlite		Default	\$ C î
IOT			builtin_recipient_sqlite		Default	801
Mypoo	d	192.168.98.133	builtin_recipient_sqlite		Default	\$ C 1
office		192.168.1.1/24@10	builtin_recipient_sqlite		Default	s c 🚺

### 点击添加主机成员

n	System  Vpgrade to Pro/Enterprise version			Q Search	# <sup>0</sup> * ±*
♥ . Health	Host Pool Members				
⊊. System	Current Host Pool				
tools	ТОТ	• 🗷			
Pools	Show 10 + entries			Member Type - Search:	+
Notifications	Member Address			Ť.	VLAN TA Actions
¢ . Settings			No data available in table		
Developer	Showing 0 to 0 of 0 entries				« < > »
Help					
	ntopng Community v.4.1.201010   🔿		© 1998-20 - ntop.org		10:58:45 +0800   Uptime: 39:48

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



Member Type	IP Address Network MAC Address	
Network	192.168.98.1 / 24 🕅	
VLAN	14 🔊	

#### 添加完成后可以在主机池中看到划分的结果

lame 💷	Members	Recipients	User Scripts Configuration	Actions
Default	All unbound	builtin_recipient_sqlite	Default	s 🛛 🚺
от	192.168.98.1/24@14	builtin_recipient_sqlite	Default	s 7
lypool	192.168.98.133	builtin_recipient_sqlite	Default	s 🛙 🚺
office	192.168.1.1/24@10	builtin_recipient_sqlite	Default	s 🗹 💼

### 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。

Host Pool	List 💠	cense expires in 08:16	3 🖵 8 🖵 3 Devices 24 Flow	15	Q Search	<u></u>
rts						10 - +
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
ΙΟΤ	<b>L</b>	0	02:13	Rcvd	0 bit/s	0 Bytes
Default	<b>E</b>	11	02:13	Sent Rovd	1.13 kbit/s	1.18 GB
gs Showing 1 to 4 of 4 m	ows		© 1998-20 - n	top org	<b>0</b> 11:2:	1:33 +0800   Uptime: 02:2



# 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

或者更改配配置文件(/etc/ntopng/ntopng.conf)添加:

-F=nindex

位置: interface->



通过单击该 塑 图标,可以选择特定的通信或主机并分析原始流。



#### 广州虹科电子科技有限公司

Application	Total Bytes	Percentage		Actions
SSDP	41.0 KB		45.1 %	Q
NDNS	19.99 KB		22.0 %	<b>a</b>
Jnknown	11.31 KB		12.4 %	Q
JPnP	9.49 KB		10.4 %	Q
DNS	2.51 KB	1 <mark>-</mark>	2.8 %	Q
argus Dataspeed	2.33 KB		2.6 %	Q
JbuntuONE	2.07 KB		2.3 %	Q
CMPV6	1.06 KB		1.2 %	Q
GMP	917.0 Bytes	1 <b>1</b>	1.0 %	Q
VetBIOS	245.08 Bytes		0.3 %	Q

NOTES:

### 点击后,何以看到每个用户的使用情况

n ens33 - 3.30 kbit 3.70 kbit	S License expires in 5 Days, 15:08:47	7 🔜 8 Devices 25 Flows 🚍			Q Search	<b>₽</b> -
Interface: ens33   Network	s Packets Applications ICMP ARP 🖿					
5m 30m 1h 1d 1w	1M 1Y Custom	Begin Date/Time: 04/09/2020 02:51:00	End Date/Tim	e: 12:57:00 🗯 App	y ← → + − - Ø 🖿	
SSDP -					SSDP OTrend OEMA OSMA OAva O99th Perc	
1.16 Kbits 1.12 Kbits 960 bit/s						
800 bis/s 640 bis/s						
480 bit/s						
100 bit/s						
02:51:00	02:52:00	02:53:00	02:54:00	02.55:00	02:56:00	02:57:00
Total: 48.71 KB	951	h Percentile: 1.16 Kbit/s	Average: 1.11 Kbit/s	Max	1.16 Kbit/s @ 04/09/2020 02:52:00	
Top SSDP L7 Contacts • X App	lication: SSDP				10 • IP Version •	Expl
Client		Server		Throughput	Total Bytes	Act
_gateway		239.255.255.250		780.22 bit/s	34.29 KE	3 0
192.168.0.102		239.255.255.250		95.56 bit/s	4.2 KE	3 6

# 再次点击 <sup>④</sup> 图标可以看到特定用户的流量使用情况:

ens33 • 0 bps 268.60 bit/s	ee expires in 2 Days, 19:11:11 12 🔲 🛛 💷 🚳 Devices 13 Flows		a	. Search	₽.
Host: 192.168.0.113 🚠 🔗 Traffic Packe	ts Ports Peers ICMP Applications DNS TLS SSH HTTP Flows 🛕	- E D ¢			
	Begin Date/Time:	End Date/Time:			
5m 30m 1h 1d 1w 1M 1Y	05/09/2020 22:55:00	6/09/2020 22:55:00	🗰 Apply 🗧 🦮 🕇	- 🕜 🖿 🖥	
Top Applications *					
5.59 Kbit/s		ntop     TLS     DNS     Am	azon HTTP MDNS OUbuntuONE OUhrown Other	Trend OEMA SMA OAvg	
4.8 Kbit/s					
4 Kbib's					
3.2 Kbit/s					
2.4 Kbb/s					
1.6 Kbb/s					
800 bit/s					
0 22:55 00:55	02:55 04:55 06:55 08:5	5 10.55 12.55 14.5	5 16:55 18:55	20.55 22	55
Total: 1.29 MB	Average: 125.05 bit/s		Max: 5.59 Kbit/s () 06/09/2020 20:55:00		
Top L7 Contacts -				10 · E	Explo
Client	Server	Application	Throughput	Total Bytes	Acti
WORKGROUP	125.74.34.246	НТТР	544.94 bit/s	5.61 MB	G
WORKGROUP	ntop-digitalocean.ntop.org	ntop	307.23 bit/s	3.16 MB	G
WORKGROUP	118.116.2.26	TLS	135.18 bit/s	1.39 MB	Q
WORKGROUP	api.snapcraft.io	UbuntuONE	42.9 bit/s	452.42 KB	œ



# 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:

cense		
itus		
stemId	BR286457006690F11 [2] Siki on the above URL is generate your from ginnal version locence, or purchase a locence at e-shop [2]. You are no root, research or an education installized places and this [2].	
ense	Specify here your stoppg License	
	B Stee License	
• License Agreement: EULA 🛛		
ng Enterprise L x43.201211   O	6 1999-20 - titipung	6 14 39
	ntopng License Generator	
Required Information		Description
System Id:	3B90718600860F11	You can print this informati on within nto png. Go to m enu Home / A bout and you will find a UR L to cick on. It will bring y ou to this we b page with a II the licensin g information pre-filled. Example: 1F E7/1088-0882 -5:607-7105A
Order Id:		This is the 10 digit orderId you have plac ed when shoppe d on the htop site. Example: 129 8838443
Email:		This is the e mal associate d with the or der id. Example: me @company.co
ntopng Version:	4.0.200828	Example: 2.0.
ntopng Edition:	Enterprise L (x64)	ntopng editio n type,
NOTE		
The Enterprise L e uct license.	dition, creates a single license that also unlocks n2disk and nProbe. This means that with a single mense you can unlock	all products without the need to generate an individual prod

在上图中输入购买 license 得到的 Order id 和 Email 再点击 Creat 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 Setings->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 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



#### 广州虹科电子科技有限公司

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。

Runtime Preference	ces	
Q Search Preferences	Timeseries Database	_
User Authentication	Timeseries Driver The driver used for storing and retrieving timeseries data.	
Network Interfaces	InfluxDB URL	http://localhost:80
Cache Settings	The one powers to a fulling minuted instance.	
Timeseries	InfluxDB Database	ntop
Alerts	The udiabase to use for unreseries storage. Existing udia will not be migrated.	
Alert Endpoints	InfluxDB Authentication	
Applications	Enable InfluxDB authentication.	
Logging	Timeseries Resolution The interval between consecutive timeseries data points for local hosts. Only effective for	105 <mark>305</mark> 1m
Flow Database Dump	packet interfaces.	
SNMP	High resolution can have a strong impact on memory and disk usage for large networks.	
Network Discovery	Timeseries releation time can be set here	
Telemetry	Interfaces Timeseries	
Traffic Recording	Traffic Toggle the creation of bytes and packets timeseries.	

### 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。

Manage Data					6
Export Delete					
Elows Insert Host IP or Mac Address or /24	Insert VLAN				
192.168.0.120	VLAN	8	_		
					_
sortace				Telete Host Data	Data
CODE			L		_
All the persistent data is deleted. Data include traffic System Interface Data includes all the data located u WARNING: Inindex is enabled for flows dump, histori	counters, timeseries, flows, alerts, and Redis caches. under the "System" menu entry, for example CPU, InfluxDB and St ical flows information will not be deleted.	NMP data.			
ntoping Enterprise L v.4.3.201214 [ O		© 1998-20 - ntop.org		<b>0</b> 16:55:00 +0800	Uptime: 01:5

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。

Runtime Preferences		
Q Search Preferences	Data Retention	
User Authentication	Data Retention Number of days to keep dumped tooks, hotorical timeseries and top-talkers for. Default: 30 days.	365
Network Interfaces		
Cache Settings		Save
Flows Dump Settings		
Timeseries		
Alerts		
Applications		
Logging		
SNMP		
Network Discovery		
Telemetry		
Traffic Recording		
Remote Assistance		
Data Retention		

### 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

n	System + License expires in 00.12		R- 2-
Health *	Applications and Categories		0
Pollers *	Applications Categories		
tools			Q Search Application
Pools	Application	Category	Custom Rules
Notifications	Zoom	Video -	Edit Rules
Settings	ZeroMQ	RPC •	Edt Rules
<b>/&gt;</b> Developer	Zattoo	Video -	Edt Rules
e · Help	Zabbix	Network -	Edt Rules
	YouTubeUpload	Media	Edt Rules
	YouTube	Media	Edt Rules
	Yahoo	Web	Edd Rules
	XDMCP	RemoteAccess -	Edit Rules
	Xbox	Game	Edd: Rules
	WorldOfWarcraft	Game -	Edit Rules

4) 配置私有协议,这里以域名定义私有协议。





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。

n	<b>e</b> ns33 •	\$ 96.40 kbit/s 6.10 kbit/s	Upgrade to Pro/Enterprise v	ersion 🕑 🛛 👥	💂 24 🖳 8 Device	s 154 Flows					Q Search
Dashboard	Active F	lows									6
Alerts		Application	Protocol	Client		Server	Duration	10 • Hosts • Breakdown	Status • Severity • Actual Thpt	Direction - Application	s • Categories • IP Version • Protocol •
Flows	Q	IGMP 💼	IGMP	192.168.0	0.106	239.255.255.250	< 1 sec	Cient	0 bps	60 Bytes	
Hosts '	Q	IGMP 📫	IGMP			239.255.255.250	< 1 sec	Client	0 bps	60 Bytes	
nterface	Q	IGMP 👍	IGMP	168.0	0.100	224.0.0.252	< 1 sec	Client	0 bps	60 Bytes	
•	ଷ	TLS 🔒	TCP	100	57642	203.119.169.88 🖬 :https	00:01	Server	0 bps	17.38 KB	6q6o6t.tdum.alibaba.com
Settings	Q	TLS 🔒	TCP		57284	14.116.143.187 📟 :https	00:01	Client Server	0 bps	6.21 KB	
Developer	Q	TLS 🔒	TCP		<b>1</b> :57134	203.119.169.141 🖬 :https	< 1 sec	Server	0 bps	18.28 KB	
e . Help	۹	TLS.YOUKU 🟚	TCP	i i i	.52910	106.11.43.215 🗰 :https	00:01	Server	0 bps	10.13 KB	pc.pay.youku.com
	୍	TLS 🔒	тср	1	46920	118.112.19.48 🔤 :https	< 1 sec	Clem Server	0 bps	6.15 KB	liangcang-material.alicd
	ଭ	TLS 🔒	тср		<b>5</b> 4988	182.140.143.251 🐸 :https	< 1 sec	Cient Server	0 bps	362 Bytes	
	્	TLS 🔒	TCP	1 an 1 1	46922	118.112.19.48 📟 :https	< 1 sec	Gient Server	0 bps	6.09 KB	liangcang-material.alicd
	Showing 1 to 1	0 of 154 rows. Idle flows not	listed.								« < 1 2 3 4 5 > »
	ntoping Community	v x4.3.201214   O					© 1998-20 - ntop.org				0 17:45:15 +0800   Uptime: 11:2

对于基于 IP 和端口自定以协议的方法类似,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。



# 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

<u>www.hkaco.com</u> 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@"

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。

# 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:

mp@ubuntu: ~		mp@ubuntu: ~	
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.	
OKg09pGv0BkG936vfxpssNKS/XXU/11tIUKJ9Amp0xPbWH50St9cK		06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template	'DNS O
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE]	sa9A+sremi4+R4L0	UERY'. Discarded.	
xJ1cGiKaBhn9ADaaJ2Eh4FvihlvX0JGZzABIKbU6xB43GdCWMSMPJ		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]	NFDfbuScai8i0vaS	URL'. Discarded.	
brd13u8Vqd0tPJ5M0SJZW2YD8JfJKoWA/06KHtC80paE8kBlDfRjj		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]	MXp+U25ghab01KrF	SITE'. Discarded.	-
y4VT3g9HrjD80RC1WmgfE0NTpYYPVtlfbjtISNJ+JnHKwYbltWRgH		06/Sep/2020 23:13:54 [plugin.c:1309] 0 plugin(s) enabled	
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE]	PA0VkaHQwYK/3jl6	06/Sep/2020 23:13:54 [nprobe.c:9142] Each flow is 208 bytes long	
j9/iKKrpZ3uWve/PlFTu9YtdbIEOGuLs+vHPcS3g0K/TczdFRg==		06/Sep/2020 23:13:54 [nprobe.c:9143] The # flows per packet has been set t	0 6
06/Sep/2020 23:13:18 [NtopPro.cpp:708] [LICENSE] License Hash:	E9B4964310E5FC00	06/Sep/2020 23:13:54 [nprobe.c:9146] IP TOS is ignored	
DAA8E3E2DB0F267B1599699971F4E8A039		06/Sep/2020 23:13:54 [pro/pf ring.c:382] Initializing PF RING socket on de	vice e
06/Sep/2020 23:13:18 [NtopPro.cpp:714] [LICENSE] Validity:	Until Wed Sep 9	ns33	
18:06:11 2020		06/Sep/2020 23:13:54 [pro/pf ring.c:424] Dumping traffic statistics on /pr	oc/net
06/Sep/2020 23:13:18 [PeriodicActivities.cpp:105] Started period	ic 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 ASs will not be computed (no Ge	oDB fi
06/Sep/2020 23:13:35 [PeriodicActivities.cpp:165] Each periodic	activity script	les loaded)	
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] Succesfully 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



### 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: <u>https://www.ntop.org/guides/pf\_ring/rss.html</u>

### 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://127.0.0.1:5556" --zmq-probe-mode= -T="@NTOPNG@" ntopng 配置示例如下: -i=tcp://\*:5556c -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的窗口,使您可以检索和分析该时间段内的所有原 始流量。

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 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 <sup>▲</sup> 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。

n	■ lo • 196.60 kbit/s License e	pires in 2 Days, 18:36:30 3 2 1 64 Flows		Q Search	<i>₽</i> -	*
hboard	Contribute to the project by sending encry	sted, anonymous telemetry data to ntop.org: visit the $\underline{\mathbb{A}}$ Preferences page and expr	ress your preference.			
Alerts	Interface: Io 🔏 Networks Packets App	lications ICMP 🛎 🖴 🛦 皆 🌣 ≁ 🎖 🛎 🖡				
lows	External traffic recording providers detected, r an external traffic recording provider.	topng can automatically bind this interface to an external provider. You can let ntop	png take care of the record	ling using this page, or yo	ou can 🌣 configure	×
•	Settings					
¢ ·	Traffic Recording Setting	s				
<> '	Traffic Recording	Continuous Traffic Recording				
veloper	Max Disk Space	2 GB Maximum disk space used for recorded traffic on disk. 0.02 GB are already in use by	this instance.			
neib	Storage Directory	/var/lib/ntopng/1/pcap				
	Storage Utilization	System (8.95 GB) Packet Dumps (18.1 MB) Extracted Packets (0 Bytes) Free (10.59 GB) - Totai: 19.56 GB				
	NOTES				Save Settin	igs

# 8.3. 下载 pacp 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:

 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



广州虹科电子科技有限公司

		Begin Date/Time:		End Date/Time:				
5m 30m 1h 1d 1w 1M 1Y Custom		11/12/2020 14:18:05		11/12/2020 14:19:19		Apply	← → + -	8 🛓 🖿 🗎
Traffic •								
77.61 Kbith.								Traffic O Avg O s5th Perc
160 Kbiłs								/
120 Khiti								
80 Kbk/s								
40 Kbids								
0 <sup>1</sup> 1418:05 1418:15	14:18:25	14:18:35		418.45	14185	5 14	19.05	14 19 15
Total 122.15 KB	95th Percentile: 47.1	to status	Average: 13.71	Kbilis		Max 177.6	1 Kbills @ 11/12/2020 14:18:2	38
Top L7 Contacts -								
								10 • IP Version •
Client	Server			Application		Through	iput	Total Bytes
ubuntu	192.168.1.1			DNS		1.44 k	bit/s	13.04 KE
ibuntu	ec2-52-11-109-209.u	is-west-2.compute.amazonaws.com		Amazon		1.31 k	bit/s	11.86 KE
ubuntu	server-13-35-90-67.k	ax3.r.cloudfront.net		Amazon		1.27 k	bit/s	11.46 KE
				dan terrete				
192 168.0.108	224.0.0.251			MDNS		635.24	Dif/S	5.74 Kb
192:168.0.108	192.168.0.255			NetBIOS		497.3	bit/s	4.49 KE
192.168.0.107	239.255.255.250			UPnP		450.16	bit/s	4.07 KE
\$17.90 bWs         Comme regime in 36.33           \$12.0 kab/s         Comme regime in 36.33           \$168.0.108         # Traffic	rs Applications DNS Rows 🖨 🛕	* *						Q Search
(517,90 bits immersion mix)     (517,90 bits immersion mix)     (60.000	In The Torston Titling -	Begin Date/Time:		End Date/Time:				Q Search
(517.90 bd/s (1000110000000000000000000000000000000	rs Applications DNS Rows 🕀 🛕 🖢	Begin Date/Time: 11/12/2020 14:15:42		End Date/Time: 11/12/2020 14:21:42		a Auty	← → + -	Q Search
(517.90 bits 1000000000000000000000000000000000000	s Applications DNS Flows 🕀 🛕 🛓	Begin Date/Time: 11/12/2020 14-15-42		End Date/Time: 11/12/2020 14:21:42		a Apply	← → + - @MDNS (seri)	Q Search  -  -  -  -  -  -  -  -  -  -  -  -  -
(517.90 bel's 1.00000-200000 10 (80.32) (3.20 bell's 1.00000-200000 10 (80.32) 1680.0108 ∰ Traffic Packets DSCP Ports Pee 300m 3h 1d 1w 1M 1Y Custom	1 (19) (1900) (1900) - Is Applications DNS Flows 🕀 🛕 🛓	Compared and a second sec		End Date/Time: 11/12/2020 14:21:42		a A507	← → + - ⊕MDNS (sert)	Q Search
(517.90 bWs         Linescourses in M33         (680.108 mm f ratio         (680.108 mm f ratio)         (	IS Applications DNS Flows 🕀 🛕 🖿	Compared and a second and		End Date/Time: 11/12/2020 14:21:42		a Agery	€ → + - ⊕MDNS (sert)	C Search
(517,90 bits Unmarrayments MAX)     (3.20 bits Unmarrayments MAX)     (680.108	IS Applications DNS Flows 🕀 🛕 🖿	Compared Figure 2014     Segin Date/Time:     11/12/2020 14-115-42		End Date/Time: 11/12/2020 14:21:42		a Aury	€ → + - ⊕MDNS (sert)	Q Search
(517.90 bd/s 30mstagens m M33) ( 3.20 bd/s 30mstagens m M33) ( 1680.108 A Traffic Packets DSCP Parts Pec 30m 1h Id 1w 1M 1Y Contom	In Contract Classifier ( )	Compared and a second and		End Date/Time: 11/12/2020 14:21:42		a Autor	← → + - ⊕NDHS (pert)	Sourch     Sourch     Sourch     Sourch     Source (not see (
(517.90 bd/s (1000000000000000000000000000000000000	s Applications DNS Flows 🕀 🛕 🖿	Compared and a second and		End DeterTime: 11/12/2020 14:21:42		a 200	← → + - ⊕MDHS (bert)	Search     Search
(517.90 bWs         Linestages 1.9133         (1680.108 ms/rages 1.9133         (1680.108 ms/rages 1.9133)         (1680.108 ms/rages 1.913	IS Applications DNS Flows	Compared Technology     C		End Date/Time: 11/12/2080 14:21:42		a A507	← → + - ⊕MONS (sert)	Q Search
(517.90 bits Unmarrayments 2022     (517.90 bits 202     (517.90 bits 2022     (517.90 bits 202     (517.90 bits 202     (517.90 bits 202     (517.90 bits 202     (517.90 bits 202	IS Applications DNS Flows	Compared Time:     11/12/2020 14-115-42		End DateTime: 1)1/12/2020 14:21:42		<ul> <li>Retty</li> </ul>	← → + - excrusional	Q Search
(517,90 bils insertagens in M33      (3.20 bil	IS Applications DNS Flows I A I	Begin Date/Time:           13/12/2020 14:15:42		End Date/Time: 11/12/2020 14:21:42 11/12/2020 14:21:42		Retry 14142	+ → + - exceded	Sourch     Sourch     Sourch     Sourch     Source (non-g) Image (non-g) Image (non-g)     Source (non-g) Image (non-g) Ima
(517,90 bd/s         3.00 bd/s	In a contra contra contra a la	Brgin Date/Time:           13/12/2020 14/15/42	•	End DateFilme: 11/12/2020 14:21:42 14:17:42		B A007	♦ → + - ØHD06 (per)	Search     Search
(517.90 bd/s         Linescreption 1.0133         E           (53.20 bd/s         Linescreption 1.0133         E           (660.108 %)         Traffic Packets DSCP Ports Pec           300 3h 1d 1w 3M 3Y         Outcom           (-         -           (-		■      Compare 1     Compare	•	End Date/Time: 11/12/2020 14/21/42 14/17/42		Aggr	¢ → + - excreption	C Search
(517,30 bills Linescopers 1, 3133     (517,30 bills Linescopers 1, 3133     (540,108 ↔ Traffic Packets DSCP Parts Per     30m 3h 3d 3w 3M 3Y Comm	IL EL GEORGE ELEMA   IS Applications DNS Powe	Eegin Date/Time:     11/12/2020 14:15:42      16:564      First Seen	Last Seen	End DateTime: 11/12/2020 14:21:42 14:17:42 14:17:42 Packets Throughput	Total Bytes F	Actor Actor Active Acti	+ -> + - evons perg	Search     Search     Search     Search     Search     Search     Into     Into

cessed 1 records (500 re

### 9. 连续流量记录

Showing 1 to 1 of 1 rows Query performed in 2 msec

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

# 10. nProbe agent 中使用 ntopng

详细内容可查看: <u>https://www.ntop.org/guides/ntopng/using\_with\_other\_tools/nprobeagent.html</u>

## 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。

n	ens33 - \$\$ 25.0 kbit/s License expires in 09.20 0 = 26 = 6 Devices 109	Flows	Q					
Dashboard	Interface: ens33 🛠 Networks Packets DSCP Applications ICMP ARP 🖮 📾 🛦 🏚 $\not \succ  \not \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \!$							
Alerts	Custom Name	ens33						
Flows	Pool	Default - 🕼						
Hosts	Interface Speed	1000 (Mbit/s)						
Interface.	Realtime Stats Refresh Rate	3 (sec)						
🔅 • Settings	Ingress Packets Sampling Rate							
	Local Broadcast Domain Hosts Identifier 🚱	IP Address -						
O ·	Hide from Top Networks	e.g. 192.168.1.1,192.168.100.0/24						
	Create Interface Top Talkers							
	Dump Flows to Database							
	Mirrored Traffic							
	Flows-Only Interface (requires restart)							
	Periodic Interface Network Discovery							
	Traffic Recording Provider	ntopng -						
	Dynamic Traffic Disaggregation	-						
		NOTES O						
	Duplicate Disaggregated Traffic 🚱							

### 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。

m CPU Load 🖿	1
CPU States	iowait: 0%6 / active: 21%6 / idle: 80%6
RAM	Used: 82.22% / Available: 694.96 MB / Total: 3.82 GB
g PID (Process ID)	5259
RAM 🖿	Used: 252.27 MB
Alerts 🖿	Queries: 16 / Stored: 7 / Dropped: 0
Storage Utilization	Volume: Nar/Ibhntopng (/devisda1)
	€ ens33 (6.96 MB) ● 10 (7.76 MB) ● system (9.81 GB) Available (9.92 GB) - Total: 19.56 GB
Last Log Trace	11/90/2008 14:04:14 [Neurostinor/fac.up:100] [MMC in one and without .4 in yes off gas off tas off 11/90/2008 14:04:14 [Neurostinor/fac.up:100] [MMC in yes and without A to yes off gas off tas off 11/90/2009 14:04:14 [Neurostinor/fac.up:100] [Neurostinor structure attributes and the face structure in the 11/90/2009 14:04:04 [Neurostinor/fac.up:100] [Neurostinor structure attributes and [Adv 30] 11/90/2009 14:04:04 [Neurostinor/fac.up:100] [Startd gases regulating an interface structure attributes a

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:

System • License expressin 01:17			4 <sup>0</sup> - ±		
infac08 🛠 📠					
CD Health Current InfluxOII export health.		OK Expert to InflueDB is working OK.			
Storage Utilization Total disk space used by influiDB.		4.7 MB			
RAM Total memory influxDB has obtained from the operating system.		110 MB			
Total Exports Total rumber of successful writes into InfluxD8.	L	22			
Total Points Total number of points successfully written into influxDB.	<b>1</b>	841			
Dropped Points Total number of points dropped due to InfluxDB write failures.	100.	0			
Series Cardinality An indication of how challenging is for influxDB to handle written points.		560			
NOTES • Documentation with detailed descriptions of all the fields shown is available in the r	ntopng User's guide.				
ntoprg Enterprise L v.4.3.201211 ] O		© 1998-20 - ntop.org	<b>0</b> 16.49-45 +0800   Uptime: 01		

### 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

bongwangle.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