

nBox 2.1 - User's Guide Open Source ntop software web management

Version 2.1 April 2014

© 2002-14

nBox contact	<u>nbox@nmon.net</u>
nBox web	
ntop site	www.ntop.org
nProbe web	www.ntop.org/nProbe

Table of Contents

1. Introduction	4
2. Using the nBox 2.1 web interface	6
2.1 Usage Guidelines	6
2.2 System	8
2.3 Application	19
2.4 Admin	25

1. Introduction

Traffic measurements are necessary to operate all types of IP networks. Network admins need a detailed view of network traffic for several reasons and some of these could be security, accounting and management. The traffic compositions have to be analyzed accurately when estimating traffic metrics or when finding network problems. All of these measurements have to be made by inspecting all the packets flowing into the network trunk analyzed (such as router and/or switches). This analysis could be done on the fly or by logging all the packets and than post-processing them. But with the increasing network capacities and traffic volumes this kind of approach is not suitable for the most cases. Instead similar packets (packets with a set of common properties) can be grouped together composing what are called "flow". As an example, a flow can be composed of all packets that share the same source and destination address so a flow can be derived using only some fields of a network packet. On this way, similar types of traffic can be stored in a more compact format without loosing the information we are interested in. This information can be aggregated in a flow datagram and exported to a collector able to report network metrics in a user-friendly format.

When collected this information provides a detailed view of the network traffic.

Precise network metric measurements are a challenging task so hard work has been done in this field. In commercial environments, NetFlow is probably the de-facto standard for network traffic accounting and billing. NetFlow is a technology which was originally created by Cisco in 1996 and is now standardized as Internet Protocol Flow Information eXport (IPFIX — RFC 3917). NetFlow is based on the probe/collector paradigm. The probe, usually part of network appliance such as a router or a switch, is deployed on the measured network segment, it sends traffic information in NetFlow format towards a central collector.

nProbe is a software NetFlow v5/v9/IPFIX probe able to collect and aggregate network traffic, and export it using the standard Cisco NetFlow v5/v9/IPFIX format. It is available for most of the OSs on the market (Windows, Solaris, Linux, MacOSX). When installed on a PC, nProbe turns it into a Network-aware monitoring appliance.

Many users, who used nProbe, realised that running a network probe on a PC is not always the best choice for several reasons:

- 1. PCs have moving parts that can break making the probe unavailable.
- 2. PCs are large, need monitors and keyboards, whereas probes often need to be deployed on places where there is not much space available.
- 3. Administering PCs is not cheap and they require the purchase of an OS, its installation and maintenance.
- In large networks divided in several trunks it is necessary to have several probes each analysing a trunk. This requires that multiple PC running nProbe are deployed across the network.

- 5. The cost (for both hardware and maintenance) of a PC+nProbe is not neglectable in particular if several probes need to be deployed.
- 6. In many cases, no technician are available at the monitored site and sometimes plug and play is needed.

To face these matters and to provide an All-in-One high-performance and reliable solution, nBox has been designed and developed.

nBox is based on Linux OS, and thanks to an optimized Linux kernel with the PF_RING module that significantly improves the packet capture process, nBox is able to monitor and analyze network trunks at full speed without the need of a hardware accelerated card.

The nProbe application installed in the nBox server has been optimized and extended compared to the version of the very popular open-source software. The new nProbe contains some features not included in the open version and the software has been carefully optimized to run on the nBox server.

If you are a user that does not want to bother with installing nProbe on a PC or you need to use a high performance and reliable network probe solution then you are probably an nBox user.

In some environments it would be nice to distribute light network probes on the network that send traffic information towards a central traffic analysis console such as ntopng or any other NetFlow/IPFIX compliance collector. In order to satisfy the above requirements nProbe and ntopng can be used together.

nBox includes both a NetFlow probe (nProbe) and a collector (ntopng) for v5/v9/IPFIX NetFlow flows.

Based on your network speed and traffic volumes different nBox server could be used.

nBox can be effectively used:

- To analyze NetFlow flows generated by your border gateway.
- To replace the embedded, low-speed NetFlow probe available on your router/ switch
- As a NetFlow probe that sends flows towards one or more collectors either ntopng or a commercial one (e.g. Cisco NetFlow Collector or HP-OV).
- Both as a probe and collector at the same time. ntopng can be used as collector and analyzer for nProbe-generated flows.

Finally it is worth saying that nBox is quite easy to administer using the very intuitive embedded web interface. nBox is easy to setup and it is immediately ready to use with little configuration effort. Throughout this document we are going to describe the main components of the nBox web interface.

This manual mostly describes the nbox web interface composition and it is divided chapters, one of each menu item System, Application and Admin.

2. Using the nBox 2.1 web interface

Nbox 2.1 is a web based management interface used to configure and run ntop team developed software such as ntopng, nProbe, n2disk, disk2n, cluster and the kernel module PF_RING as well.

It allows the user to create his own custom configuration file and run the application in the preferred way. Nbox 2.1 web interface is available in packaged form (.deb or .rpm package) and can be downloaded and installed directly from the ntop web site.

It is also available in appliance format, known as nBox and nBox Recorder, where the end user just needs to plug-in the power cord and start playing with. It already contains ntopng, PF_RING and the selected software (depending on the model): nBox has nProbe as main software, whereas nBox Recorder has n2disk.

2.1 Usage Guidelines

Starting using nBox 2.1 is very simple. Startup the box, plug an Ethernet cable to its management interface and connect it to a network. From another PC connected on the same network, open a web browser and visit http://192.168.160.10/ (the default IP address of your nBox).



Clicking on the login button the system will as for credentials as follows:



The default nBox configuration is the following:

- IP address 192.168.160.10
- Default SSH user is "root" with password "nbox"
- Default Web user is "nbox" with password "nbox"

All of those could be changed using the web interface.

Upon the completion of the login process, the user is redirected to the dashboard page where most valuable parameters are shown. Processors, memory and storage usage indicators and network interface state indicators are displayed and updated in real time.

À Unux kernel 2 ⊕ Intel® Corpo ∴, Intel Corpo ∴, Restaix So …, Mel Corpo	8.32-431.11.2.4 e(TM\$2 Quad CF ration 1350 Giga miconductor Co ration 82574L C	45x80,54 x86,54 U G8200 & 2 33GHz (2010) (111) bit Network Connection , Ltd. RTL8111/8168/8411 PCI Express (igast Network Connection	Ggabit Ethernet Controller
Network Inte	rfaces		
dha0 dha1	eth0	with 1	
Cores		Memory	Storage
	_	3756.0 3756.0 3756.0	HAN THE STR

The page header displays the main characteristics of the nBox 2.1: the running kernel, the Cpu type and the number of Cpu cores, the controller raid type and how many network card are installed and their media type. An animated icon displays their link status. More information are provided via tooltip function as follow:



Each nBox 2.1 web page comes in a three section format: header, where a menu bar is available to jump from a single configuration page to all the others in an easy and quick way, the body, where the most important fields are displayed, and the footer with additional infos. No hidden sections have to be discovered by the end user. Its web 2.1 flavour requires a javascript enabled browser.

2.2 System

The "System" menu presents to the end user a sub menu where he can choose which section configure.

rs	timezone and ssh proc	cess as displayed in the following image:
vork RING	All of these values	
epages	can be chanaed by	Configuration General
nload Configuration	the end user and	Timestree Europe/Rome 1
nses	saved into the	594 Finational Desatered Enclose/Desater memore 504 access to your ribox 2.0. In any case your ribox 2.0 will stil be accessible via http://tipu.
	system using the	Elses charges Reset
e Changes"	available button.	
Well done! Contra estimation	annual account.do	
then durine consignation	and accessing	
	phose .	
Host Name	TIMAK	
Host Name Timezone	Europe/Rome	8
Host Name Timezone	Europe-Rome	8

On a successful save. a green boxed message is returned on top of the page.

Save changes Reset

With the following additional packages available on the nBox package repository (and on the internet as well)

-libapache2-mod-auth-xradius

-libpam-radius-auth

and enabling the apache radius module (issuing the command "a2enmod auth_xradius") the system enables radius authentication support.

Adding also ntp packages (ntp and ntpdate) and MySql packages general page changes as follows:

-	In maria to	Carlos and a second sec
mup:	Dentsond	Bysters Accounts Accounts
System	General	
	Host Neme	rbox
	Timezone	Europe/None 1
	NTP Server	di caentos, post. Hip org. 1 caentos, post. Hip org.2 caentos, post. Hip org.3 caentos, post. Hip org.
		Last of servers for remote time synchronization. Leave this field empty for no time synchronization. Time is synchronized at boot, every day, or whenever you realize the inputse service.
	NTP	Enables Deathed
		Activate ritp instead of repolare service.
	Radius	Enabled DataSed
		Enable-Ideable remote RADLIS authentication. Warning: a wrong configuration might prevent further users login.
	Server	
	Secret	
	TITNEOUT	
	55H	Enabled Deabled
		Enable/Deable remote SBH access to your ribox 2.1. In any case your ribox 2.1 wit still be accessible via http://ttps.
Myd	Q. Denibere	Enabled Deabled
		Enable this service if you want to start a local database for storing flows and other data. Unless you modified II the default DB user is not with no password.
		See charges . Read

A couple of additional controls are added where user can specify his preferred ntp server and settings, and if enable or not the radius authentication.

Please take care while enabling radius because misconfigured parameters may prevent further logins on the web interface and/or the whole system.

Required parameters for radius configuration are:

-server ip or hostname

-shared secret

-radius request timeout

Max one radius server per time can be configure (out of two max).

Once configured or removed radius authentication, apache web server must be restarted and a new browser session should be started (closing and reopening the browser).

The "Users" page should be used to perform an access control on the system, handling local system users and web users as well.

The administrator switches from the system users to the web users using the available tabbed view, just below the breadcrumbs.

On listed users, the administrator can perform some actions (such as removing or changing password) or create a newer one.

	Configuration	Users			
	System Users	Web Users			
		Users root Users			
		Add User	Delete User Change Pwd		
Configuration / Users	Change Pw		Configuration / Users	Add User	
Login	nbax		Login	user	
Password			Password		
Password (retype)	*****		Password (retype)		
	Change Pw			Add User	
	Configurat	ion / Users / D	elete User		
	Are you su	re you want to de	lete user nbox?		
			Delete User		

The network administration of the nBox 2.1 has to be performed on the "Network" submenu.

Applications +
s
Configuration

The administrator switches from the management interfaces to the other available network interfaces using the available tabbed view, just below the breadcrumbs.

The "Management" tab gives the possibility to change the management ip address, using either static ip or dynamic (DHCP). User can also add to the primary network interface a secondary address (Interface Alias). By default network routing through the available interfaces is disabled, but its status can also be changed on this page.

Custom DNS server could be specified by the administrator.

System / Network		
Management ethi	4	
Management Interface	and .	
DHCP Client	Enabled Deabled	
	If you enable DHCP support the above address fields are not used.	
IP Address	192.168.1.129 255.255.0	
Default Gateway	1021108.1.254	
Interface Aliae (ethi0:1)	Accreas	
	This field allows you to specify a secondary IP address on the withD interface.	
IP Forwarding	Crubied Disabled	
	Bruthe this facility if you want to use your as a network router.	
Primary DNS	82.101.83.101	
Secondary DNS	43.105.25.250	
Domain Name	Stativestimet.8	
	Seve thinges Reset	

For all the other network interfaces available on the system, the end user can decide to use this interface as management or if apply an address on one or more of them.

Dentoord	Bysters Applications Admini-	
System Network		
Management eth1		
Interface	altr.	
DHCP Clert	Enabled Disabled	
	f you anable DHCP support the above address fields are not used.	
IP Address	192.168.1.130 255.255.0	
Default Gateway	182.168.1.254	
Interface Alias (eth1))	Access	
	The field allows you to specify a secondary IP address on the eth1 interface.	
Management Interface	÷	
	Set this network interface as notice management interface.	
	Serve changes Pleaset	
18:30:52 up 1/18, 1 uses it	everage: 0.32, 0.11, 0.10	Back to t
© 2002-14 - rtop.org		
Documentation		

In standard implementation of the nBox, it is not suggested to apply any ip addresses on interfaces unless management ones.

In the nBox 2.1 we introduced the ability to manage the bounding interface.

Config	uration:	Bonding	Bridge		

By the "+" tab the administrator can create a new bounding and customize it by the new tab that will be automatically created.

	terment Computers - Robert Semantik resp og mer - Insissifie, verserik, merken opfit-likssele-t
Dentord	byters Approximes America
Management ett.1	+ Obnod
interfaces	ennG editri i
	Nativols interfaces where bonding is active. If you select the management interface, this bonding will become the management interface. If you will anable the driver DNA for selected network interfaces, the bonding will not be apply. Please remove the bonding before enable the driver DNA.
DHCP Clerit	Frabled Disalized
	If you enable DHCP support the above address fields are not used.
IP Address	Address Notress
Default Gateway	Address
Bonding Mode	active-backup [
	Specifying the bonding mode to use for the selected network interfaces.
Primary DNS	42.101.83.101
Secondary DNS	83.103.25.250
Domain Name	Sashwebrer, R
Management Interface	Sat this network interface as office management interface.
	Save charges Pearst Coarts

The "Bond" tab gives the possibility to choose the Network interfaces where bonding is active, using either static ip or dynamic (DHCP). User can also choose the bounding mode. Custom DNS server could be specified by the administrator. Any changes in these settings require a reboot of the nBox 2.1 to take effect.

System -	Applications -
General	
Users	
Network	
PF_RING	
Hugepage	S
Download	Configuration
Licenses	

PF_RING could be loaded and customized as requested on the "PF_RING" entry in "System" menu

This page is divided in three or more section (depends of your network card type) in tabbed form, where the administrator can customize the configuration of PF_RING kernel module, the DNA driver, if enabled, and the Aliases interface.

Any changes in these sections require a reboot of the nBox 2.1 to take effect.

PF_RING configuration contains the Enable/Disable button for automatic startup and module load upon system boot, the number of the ring slots (min_num_slots module param) and the transparent mode type (transparent_mode module param) as displayed in the picture below. As in the other pages, "Save Changes" is needed to commit the modified parameters.

System / PE,RNG.		
Plasas reboot your relia	x 2.1 wherever you sharing these settings	20 C
General DNA Ale	55495	
Enable PF_RING	Drabled Deabled	
	Enable/Deable PF_RING packet captur	n acceleration.
	Number of ring slots and Transperent	t mode settings are for standard PF_RMHG only. they will not affect DNAAlisees.
Min number of ring slots	4000	2
Transparent mode	1 - Deect Theraparent	1
	Please note that if you set Transpanent this will prevent such interface from rec	mode to 2, then you better not start any monitoring application (e.g. rProblem) design the management implices a aving packets.
	Seve charges Reset	

The DNA section can be used to enable or disable the DNA driver, if licensed, on each network card with the exception of the management interface, normally eth0. Loading the driver, user MTU size, the number of slots int the RX and TX ring and RSS behaviour can be chosen. The first with a numeric value, the second simply choosing from the suggested option and the last simply enabling or disabling RSS.

Dentoerd	System • Applications • Admin •	
System / PF,RNG		
Please reboot your ritio	e 2.1 whereas you, charge these settings.	
General DNA Alle		
MAC Address	40.96 # 20.02.30	
Family	fle	
Name	and	
Enable DNA	Grable Daable	
	Enable/Disable the DNA driver for this interface.	
MITU	1500	
PK Slota	85	
	Number of slots in the RX ring, increasing the number of slots usually helps handling network peaks and system activities.	
TK Skota	ac.	
	humber of alots in the TX ring.	
Receive-Side Scaling	Single-Queue Mutt-Queue	
	stratile theater a rolo queues on the interface.	
	No starse configured for the starters. Places sectory your This instance in Sustain Conven-	

System -	Applications -
General	
Users	
Network	
PF_RING	
Hugepage	s
Download	Configuration

Licenses

Nbox 2.1 can exploit the advantage of the modern CPU/memory with the configuration of the HugePages¹.

The presented menu allows the nBox administrator to configure and load the requested number of 2MB each hugepages.

Dentoard	System • Applications • Ameri*	
System / Hugepages		
Enable Hugepages	Erebind Deadled	
	Enable/Disable Hugspages.	
Page Size	2048 KByle	
Number of Pages	206 5	
	Bystem does not have evaluable pages on node D now.	
	Serve changes Reset	

To do this, it is needed to "Enable" hugepages support, select the number of pages required and commit the changes using "Save Changes".

0 0 + (G)(2) + 0++	Mappages Californitien Markit.map.org.mae.ini.initia, happages (al	c 0
Dertseard	System* Applications* Acres*	
System / Hugepages		
Well doned Configuration	served successfully	х
Enable Hugtpages	Enabled Disabled Enablet/Otable Hugspages.	
Page Size	2048 KByte	
Number of Pages	256 2 216 of 256 pages available now.	
_		

The unload of huge pages is done by clicking on "Disable" button and saving changes.

¹ More informations on Hugepages on http://en.wikipedia.org/wiki/Page_(computer_memory)#Huge_pages



NBox 2.1 comes with all software installed but it is enabled upon user request. Normally, whenever the nBox is delivered to the customer, it does not need to be licensed because it has already been done by nTop team. Just in case, after a factory reset for example, the user needs to enable its software.

Under the "Licenses" menu, administrators can add their licenses to nBox components: nProbe, nProbe plugins, n2disk, DNA, Libzero. All of these licenses are System ID (nProbe, nProbe plugins, n2disk,disk2n) or mac address (DNA, Libzero) based.

Licensing a nBox 2.1 allows to update custom software for 1 year since first registration. After this period software will continue working but any further update can be installed.

Licenses page brings the user to the displayed page where the nbox 2.1 system ID is available. On the other tabs, users can add their licenses as follows.



On nProbe tab, the software version and the system ID is available. Users will find the license field already filled with their licenses or it can be reinstalled if needed.

e (= () (2) (+) n imar a formavali	Laurentes Cardiguestion Mag.org man-in laurity, January	e
Dashbord	System* Applications* Advan*	
System / Licenses		
nillox 2.1 nProbe	nProbe Plugine n2idiak diak2m DNA Libbero	
Wild License found.		
Version	6.16.140429	
System ID	2ADE102C11B1BBAB	
License	P226358052089051631F1EE07C14831F1401400798258F8E32	
	Reset Loonse	

15

nProbe behavior can be extended using nProbe plugins. They increase the decoding and storing features of the original software and are available for purchase on the ntop shop website. Plugins come in single license (e.g. dns plugin) or in bundle license (e.g. VoIP that contains both RTP and SIP plugin).

0 0 + + _ ==== + tempet	Litement Configuration	6) I (
Dashboard	System* Applications* Admin*	
System / Licenses		
nillox 2.1 nProbe	nProbe Plugins n2idisk disk2n DNA Libzero	
nProbe Version	0.16.140429	
System ID	2ADE102C11B1B8AG	
Plugin	dns (DNS Protocol) \$	
License		
	See Lawrence Resat	

n2disk is licensed on speed capability. In this way the end the user can reduce the TCO acquiring only the license for the required capturing. Different flavours are for 1 Gbit/s, 5 Gbit/s and 10 Gbit/s. nBox 2.1 appliances have their components chosen with several years of experience and they are optimized for the requested speed. This means that a 10 Gbit/s license does not guarantee the wire speed capture unless on top of adequate hardware.

	unde see annu-training January	c 0
Luc J Dishbord	System* Applications* Advan*	
System / Licenses		
nillas 2.1 niProbe	nProbe Plugins n2disk disk2m DNA Libzero	
Version	2.3.145429	
System ID	2ADE102C11B108AG	
Dump Speed	100 1	
License		
	Carve LCOURS TREES.	

On n2disk tab, the software version and the system ID is available. The original software and are available for purchase on the ntop shop website.

	n mara, formaneli	Neot tod	d'alear sh					6	-
ntep	Dishbord	System*	upications.	Adm	6°				
Syste	m / Licenses								
nillas :	2.1 nProbe	nProbe Plugins	n2disk	diek2n	DNA	Librero			
	Version	2.3.140429							
	System ID	2ADE102C11	108A9						
	License								
		See Livere	Beast						
					_				

The following license tab is for DNA driver. DNA licensing model is on a per-mac-address basis hence each network card that supports this kind of technology might be enabled In the same way as nProbe plugins, DNA licenses can be purchased upon user request and added to nBox 2.1 during all its life cycle.

000 * * 0 0 2 + 0 mm + tomavel.	Livenues Configuration	6 0
Clasthoord	System* Applications* Admin*	
System / Licenses		
nBox 2.1 nProbe	nProbe Plugine n2diak diak2m DNA Libzero	
Interface	draß	
Family	igb	
MAC Address	A0.36.9F.38.82.32	
License		

Last licensing tab is for Libzero. Its licensing structure is equal to DNA driver model. Libzero technology extends and increases the packet capture and forward-to-application speed, giving each captured packet available to user application without extra copies from and to the memory.

* * (A) (2) + 0 mm * Amarel	Disenses Configuration	c 0
Dishboard	System* Applications* Advise*	
System Ucenses		
nBax 2.1 nProbe	nProbe Pugins n2disk disk2n DNA Ubsero	
Interface	dra0	
Family	lgb	
MAG Address	A0.36.9F.28.E2.32	
License		
- 00330		

Last available menu in "General" configuration tab is "Download Config" and it is usually needed in case of a support request or for backup purposes. From this page a compressed file with the most valuable configuration will be download and it has to be attached to the support request. In such way nTop team may reproduce and analyse the support request in a complete form and try to help end user as fast as possible.

2.3 Application



Application menu permits to customize and control all the ntop team's installed and licensed application.

This group is composed by ntopng, nProbe, n2disk, disk2n, cluster, the subgroup "Utility" composed by pfsend traffic generator and nBox activity scheduler.

"ntopng" menu permits to enable and configure an ntopng instance on nBox 2.1. A few parameters are customizable directly from the web interface, but due to the high customization level ntopng is provided, not all of them are available on the GUI.

The page is provided to the user in a tabbed form, where its first tab is the status of the application. A page like this one is available on all the applications' pages.

A grey box with the interface name is displayed in the status tab for each enabled instance. The presence of the grey box means that at least an instance of the application is configured. A button "on - off" is available and it is used to start or stop the instance.

000 (*) - (() + ()	Maging Status 12. million col	c)()
Destinent Symmit Applications*	Advent.*	
Appa ritoping		
Well danel moping is running		
Status Configuration		
Once reteping to started you can access it at https://192.	188.1.129-3000/	
eth0		

In the configuration tab, administrator can select the automatic startup ntopng upon reboot, the interface where ntopng will listen to incoming packets. All the physical interfaces will be prompted to user, but also a "no interface" can be chosen. This selection

	http://iscahov.IBBE/wop-bin/confg_ntop_initance.cg
Dushboard	Bystem+ Applications+ Admin+
Appa ritop	
Statue Configuration	
Automatic Startup	Enabled Deabled
	Enable/Disable micp at startup.
Interface	eno t
	Newsex interface where stop is active. Note: You can configure map on the management reachase andy, as the activitient interfaces (if any) are designed for off-state.
IP Address Resolution	Olastie — Enable Local Hosts — Enable Remote Hosts @ Enable Erableideade numero IP address to symbolic address resolution.
Local Network Address	Indiano/s/indianaix (e.g. 1987-1988-0.0/258-256-205-0)
	Set his field if you want to specify additional retwork addresses other than the one specified with the selected network interface from which not p is capturing traffic. If unsure, leave this field bank,
Further Options	
	Advanced wers can add further command line options that are passed to ritio al startup is g, you can specify " r 10"). Please don't add "-m" option here, use "Local Network Address" instead. Unless you know what you're doing, leave this field enoty.

is normally used whenever ntopng is used as a netflow collector, when ntopng does not need to capture packets directly from the network card.

The administrator can also control the DNS resolution thread in ntopng. The resolution can be selected among full resolution, local or remote resolution or completely disabled.

Local Network Address and its mask (the "-m" option) can be selected on the gui.

An additional input box is available where administrator can customize ntopng configuration with all the other parameters.

"Save" button allows to store the configuration into nBox 2.1.



"Nprobe" menu has several option that can be tweaked by administrators.

As in ntopng menu, nProbe is available in tabs. The first is the status tab and the following are for each available network interface. The last one is for the netflow proxy configuration.

nProbe has also many customizable options but not all of them are on the web interface.

Advanced users may optimize their nprobe configuration, editing the configuration file or running a nprobe instance from the command line.

A DECEMBER OF THE OWNER OWNE	in Continuenting - shart	and the second se	Canada Translate	
Therefore and the second	Southern Applements Appl		Calify Frankin	
Mary 1	alline the second second			
Appe rProbe				
Status shaD shaT	eth/1 Phony File			
Valid relice 2.1 Science fouri	1			
General				
Automatic Startup	Enabled Disabled			
	Enable/Disable nProbe on interface of	dned et sterlup.		
interface	mat			
	SNMP merface kt 8			
Snapien	128			
instances	Single Instance			
Collector(s) IP				
	Specify the test of collector(s) that will multiple addresses are specified (in 1 unspecified, the default transport pro protocole other than UCPS, thus can tops/1722/32.8.28.2016, ecrp./1182.1	Il receive the Alethow flows emitted by ribo this case Hbor 2.1 will send flows in round: oncool is UDP atthough TCP and SCTP are specify protocols prepending -protocol nan 48.0.1 2007.	x 2.5. The format of the list is "ip addressiport" obin; Exemple: 182-186.180.23.3005,182.185. also supported please check whether your coll- esc/haddress-sports. For instance, udp/7121	separated by commas if 160.22066 if Infor can support 7.0.0.1 (2056,
Hash Size	128000			

Several sections permit the customization of nprobe in terms of flow export type and policy, disk based flow dump or database based flow dump. Some sections are dedicated to the customization of some plugins.

Name Name Apple Interve Apple Apple Interve Interve Apple Interve Interve Apple Interve Interve Status Interve Interve Valid inflore 2.1 tourses found Interve Interve General Interve Interve Files Export Formal Interve Interve Files Export Formal Interve Interve Interve Interve	6
Network System Aggeboardes Astronomic Aggeboarde InPute InPute Status dred dred dred Free Sport Formal dred dred dred Free Sport Sporte dred dred dred Status dred dred	+
Apps mProte Status shall ethil Provy File Vestimbles 2.1 Scenee Status General Files Export Format Files Export Format Files Export Format <t< td=""><td></td></t<>	
Statut shall	
Valii nBox 2.1 Some Source Oumani Oumani Fele Export Format Fele Export Format Fele Export Palaja Options OTPV2 Palja Options OTPV2 Palja Options OTPV2 Palja Options Des Feles Dump MyGQ, DD Reas Dump	
Baranal Fee Export Fornal Fee Export Policy HTTP Plugin Options 07P-rd Plugin Options 07P-rd Plugin Options 07P-rd Plugin Options Data Fees Dump	
Fee Export Fornal Fee Export Fornal Fee Export Follow FUTP Flugs Options GTPV: Plugs Options GTPV: Plugs Options GTPV: Plugs Options Date Flows Durp MyGQ, DB Flows Durp	
Fee Export Pelay HTTP Pelayin Options GTP-of Pelayin Options GTP-of Pelayin Options GTP-of Pelayin Options Date Feese Dump Mydidl, ddi Feese Dump	
HTTP Plugin Options GTP-cPlugin Options GTP-v1 Plugin Options GTP-v2 Plugin Options Date Revel Durp MyRQL, DB Revel Durp	
GTP-40 Pugin Options GTP-47 Pugin Options GTP-42 Pugin Options Date Revel Dump MyRQL 08 Revel Dump	
GTPv1 Puge Options GTPv2 Puge Options Das Revis Dung MyRQL 08 Revis Dung	
GTPv2 Pugin Options Date Flows Dump MyGQ, D0 Flows Dump	
Das Pows Dump MyRQL 00 Revis Dump	
MySQL D8 Flaves Dump	
Advanced	
Seve changes Done from drief 2 Factory Result	

"Save Changes" button to commit changes is on the bottom of the page as in all other pages. In addition to the standard ones, nBox 2.1 gives to the administrators the ability to easily deploy configuration among all the available interfaces, using the "Clone from" button and selecting the configuration source.

Please refer to the nProbe user manual for further informations on nProbe configuration.

"n2disk" menu is the one used to customize the configuration of n2disk software. In this section, user can tweak n2disk parameters in a graphical way

Buffer and pcap file size, snapshot length, SMP affinity are just some of the options available. The above figure displays all the configurable sections. As in nProbe, deploy configuration on several interfaces it is pretty easy using the clone button and selecting the source interface.



Traffic Generator (pfsend)

🛆 🖄 🛨 🖪 Inner & formanetik recep. org	na halanta dalar mana gitir dal		6
Addità Canfiguration	- mag	Dangle Translate	
Dentord System A	coloations + Admit+		
Apps / n2dek			
Status dhaD shall whit stur	ter-180 cluster-181 etcl etcl		
Warningi Invalid or missing loanes			
General			
Processor Attivity			
Timestamp			
Fiters			
Storage Data Layout			
Index and Timeline			
Advanced			
Save charge	Clone from dha1 2 Factory Reset		

N2disk configuration file could be edited directly by the administrator. In such way all the tweak-able parameters can be modified.

"disk2n" menu is the one used to customize the configuration of disk2n software. In this section, user can show the disk2n instance configured or create a new one by the "+" tab.

Namec	instance N	lame	
Configuration:	Detault	Clone	

Applications ntopng nProbe Deploy configuration n2disk on several interfaces it disk2n is pretty easy using the cluster clone button and selecting the source Utility

In the instance tab, user can tweak disk2n parameters in a graphical way. Egress interfaces, timeline path and time, buffer, SMP affinity are just some of the options available. The above figure displays all the configurable sections.

interface.

000	disk2+ Configuration - Inst		
distant and a formation reading on a statement of the sta	and wate more stored	Dangle Translate	s 0
Dentori System Appleato	es• Amm+		
Acce dek2n			
Statue Test +			
Warning/ Invalid or instating loanse.			
General			
Processor Attivity			
Packet Reforging			
Advanced			
	Give changes		

disk2n configuration file could be edited directly by the administrator. In such way all the tweak-able parameters can be modified.

The traffic generator pfsend is a tool used to inject packets into the network from the selected interface. It is able either to forge packets or send packets from

pcap file. Emitted packets are sent with the original speed or they can be sent at wire speed or even with a

selected bit rate.

The process can be tuned also in terms of cpu affinity, dedicating a precise cpu core to the program itself.





A green led on the bottom of the page shows that an instance of pfsend is running.

The activity scheduler is a tool used to scheduler more n2disk extraction tasks from the existing index and timeline.

Applications •	
ntopng	
nProbe	
n2disk	
disk2n	
cluster	
Utility	Traffic Generator (pfsend)
	Activity Scheduler

In this section, user can see all the scheduled task, show the log, the pcap file extracted, the configuration or delete the task and the relative file in a graphical way.

The above figure displays all the scheduler component.

Apps UNI	N ADVID	heduler				
Activi	ty Scł	neduler				
T Filter *	Create Nev	task.				
(31 (1) He	cords per page					
Sulu: -	Printly	Task Creation Date .	Duration 1	Application Scheduler	Act	ien .
O Dane	Normal	Tue Apr 29 12:45:17 2014	0 second	n2dak Extract Packets		/ 8
O Done	Normal	Mon Apr 28 17:53:38 2014	56 seconds	nždak Extract Packets		1.8
O Dave	Normal	Mon Apr 28 17:30:15 2014	C second	ribbak Extract Packets		1.8
O Done	Normal	Mon Apr 28 17:28:45 2014	0 second	nždak Extract Packets		
O Done	Normal	Mon Apr 28 17:22:43 2014	8 second	nždisk Extract Packets		1.1
O Done	Normal	Mon Apr 28 17:16:28 2014	E second	12dak Extract Packets		
O Done	Normal	Tue Apr 22 11:15:25 2014	1 ancord	rödek Extract Packets		11
Showing 1 to 7	of 7 antres				+ Provina	1 Vest

cn Or Q Y Extract Files Stats E Logs The user can create a new extraction task form an existing n2disk instance and using the extraction configuration page the user can customised the extraction in a graphical way.

Interfaces, task priority, timeline date and time, bpd filter, Output directory are just some of the options available as displayed in the picture below.

n I Coli 21 (+ n hours forsarel respo	a ma sicolara perataritat	white the same	All Shares and			d
States Configuration	and the second se		added another	1	Congle Francesson	[+]
ting a Destand	Tyriner Appleators+	dame.				a de se
Appe come both	a					
Extract Pa	ackets					
Indatos	charter, 1,0 charter, 1,1 denat denat denat enat tratemose of closes from which	ethar patien.				
Task Promy	Low Normal Hight					
Prom	274-04-29	17:52:00	0			
	2014-04-28	1732.00	D			
Fiter	DPT-Live Titler for selecting pace	ats jama format	used by the popular hopdump tools.	*		
Max File (kee	16 Milyree - Bit Milyree Smarth the mermute size of se	256 Millylee	112 Millytee 1 Gillytee 2 Gillytee	Fpane		
Max File Packate		SM 10M	Rome			
File Tag			Second The benefit of the Second of	hall die namber /		
Output De	Accesses and a second second	- And the first				
	Specify where the supplifie will	the stored, if the p	with down not paint, it will be created.			

2.4 Admin

The admin menu contains the pages to handle nBox 2.1. Services can be started, stopped or restarted.

Nbox services appear as in the following figure. Simply toggling the On/Off button user can control the service status.



Admin -			
Services			
Storage			
Reboot			
Shutdown			

In case of maintenance or if necessary, Nbox 2.1 can be remotely powered off or rebooted remotely using the specific menus.

Dashboard System * Applications * Admin *	Dashboard System - Applications - Admin -
Shut Down	Admin / Reboot
own nBox 2.0 Are you sure you want to Shut Down this nBox 2.0?	Reboot nBox 2.0 Are you sure you want to Reboot this nBox
Yes, Shut Down	Yes, Reboot

NBox 2.1 is in a continuous development. New feature and bug fixing are done day by day. We suggest all the user to perform regular updates on the nBox. In case of issue please file a bug on ntop bugzilla system (https://bugzilla.ntop.org) to keep a trace on the problem found.

Follow nTop team products on http://www.ntop.org/