

INTRODUCTION

Network traffic is an important component of the information needed to investigate and troubleshoot a network when an intrusion event occurs. Since analyzing intrusion detection events are such an important aspect of network security, it is important to understand the Monitoring tools used to view, monitor and analyze data from network traffic that is generated by intrusion detection systems. We compare seven, open source network monitoring tools used to analyze network traffic in the event of an intrusion. The tools include Wireshark, Cacti, Linux Dash, Observium, Icinga, Sysstat and Sarg. There are many more tools developed to analyze network traffic. However, the tools we chose are a starting point for the discussion of monitoring tools designed for network traffic analysis.

Wireshark – Network Protocol Analyzer

Wireshark is an analyzer desktop program which is used to analyze network packets and to monitor network connections. It's written in C with the GTK+ library and released under the GPL license. **Features of Wireshark:**

- Cross-platform: it works on Linux, BSD, Mac OS X and Windows. • Command line support: there's a command line based version from Wireshark to analyze data.
- Ability to capture VoIP calls, USB traffic, network data easily to analyze it. • Available in most Linux distributions repositories.

Applications Places Sys	tem 🥑 🙆			🛛 🌻 🥵 📑	ा
2	Capturi	ng from eth0 - Wiresh	ark	and the state	
Eile Edit View Go Capture	Analyze Statistics Telephon	ny Tools Help	ht	tp://www.t	eci
	a 🗄 x 🖉 📥 🗚	* * ? * ±			-
Filter:		► Expression Clear	Apply		
No Time	Source	Destination	Protocol	Info	
3078 48.418535	4.2.2.2	192.168.0.2	DNS	Standard que	гу п
3079 48.418546	4.2.2.2	192.168.0.2	DNS	Standard que	
3080 48.419849	192.168.0.2	4.2.2.2	DNS	Standard que	
3081 48.420510	4.2.2.2	192.168.0.2	DNS	Standard que	ry n
3082 48.420536	4.2.2.2	192.168.0.2	DNS	Standard que	гу п
3083 48.421262	192.168.0.2	4.2.2.2	DNS	Standard que	
3084 48.421597	192.168.0.2	4.2.2.2	DNS	Standard que	
3085 48.423526	192.168.0.2	4.2.2.2	DNS	Standard que	
3086 48.435100	4.2.2.2	192.168.0.2	DNS	Standard que	
3087 48.684223	4.2.2.2	192.168.0.2	DNS	Standard que	
3088 48.684272	4.2.2.2	192.168.0.2	DNS	Standard que	
3089 48.688907	4.2.2.2	192.168.0.2	DNS	Standard que	
3090 48.761231	4.2.2.2	192.168.0.2	DNS	Standard que	
ε.	-	1			
> Frame 1 (71 bytes on win	re, 71 bytes captured)				
▷ Ethernet II, Src: Vmware	e b4:da:21 (00:0c:29:b4:da:	21), Dst: Vmware c0:0	0:01 (00:50:5	i6:c0:00:01)	
Internet Protocol, Src:	192.168.0.2 (192.168.0.2),	Dst: 4.2.2.2 (4.2.2.)	2)		
	Src Port: 43101 (43101), D		82		
> Domain Name System (que					
9000 00 50 56 c0 00 01 00	0c 29 b4 da 21 08 00 45 0	90 .PV)!E.			
	11 70 dc c0 a8 00 02 04 0	YAR TIME PERSON AND A THE REPORT			
	25 a2 b0 2f 2c 01 00 00 0				
<	25 GE DO ET EC OL 00 00 1				
					_

Monitor Local Network Traffic

Cacti – Network and System Monitoring

Cacti is nothing more than a free & open-source web interface for RRDtool, it is used often to monitor the bandwidth using SNMP (Simple Network Management Protocol), it can be used also to monitor CPU usage. Features of Cacti:

- Free & open-source, released under GPL license.
- Written in PHP with PL/SOL.

You do not have Wilware Tools installe

- A cross-platform tool, it works on Windows and Linux.
- User management; you may create different users accounts for Cacti.

		the second s	Morille Firelox						
Eile <u>E</u> olt <u>V</u> ew <u>Go</u> <u>B</u> ookman	is ∐ools <u>H</u> elp								
😸 + 🛞 - 😥 🔅 🕲 🚺	http://web/cacti/cacti-0.	8.6/graph_view.php?acti	omtread/rea_id=16ik	af_id=10			× KL		
console graphs	1		L			setti		20	
racka -> Tres Made								a - magnine spectra	
	-				the life year of	Bannan Jan 199			
Articiptor, MA		fort: HOU-52-STRESSS	12		8 - 8 - 9 3	i 🖏 🔒 the from treamy	a para da terretaria da ter	of the second state	
Charlotte, MC	Data Query: S/212	- Enterface Statistics			Scott.	C set			_
Charlottesulle, VA	Port 1/1				Contraction (Spring				
CHURDUS, GA	[100-52-5650	6.2 × 1 m	Catally of Ballins	1			
Dates TX			100-26-2002	9.2 - 119	tina la	derelana -			
O Setures		3		- 44	The strange on a set	Miller by heat recruptation . Any		2 1	Search:
		N 00 K	المقدى ا	1000	Straph Receptored	diti Pensilaan		iii	ing Room
- Health HOU-52-5W3549-1			and the stand	TY YORK	Graph Frence Entry Stations	Reservation.	The second	The local data	
Hudi HOU-92-9300049-2		1	A		Berdens.	ABADE BRIDDER CONCAST		101.00.0.0	1
R-Data Center Cire		2			Coloradore Martinesia Colora Galerines			170.00.000.0	20
Heats HOU-A4-A799-5					Data Inpa Matura	Industry and the second		171.04.8.05	10
Hould: MOU-84-8798-0		0 00 00	04:00 00:00 00:00	10:00 10:	Annapities Graph Parapisies		100	170.00.0.00	100
Heats HOU AL ATM 3		E Depend - Correcti	2.54 H staropet	2,98,91,98	Hard Tampates	12140303	in the second se	170.00.0.02	
Hadi HOU-M-ATH-6		Contrast:	3.68 H Average	5.30 H H	Bala Subplates	0404710	-	100000-0.07	10
	[Internet Constants	ARTICLE ARTICLE	ine a	171.00.0.0	10
Dayton, OH			100-52-595305-2	- Enicest	Search Party Series	15.07.00001.00	10	12103.3.31	1
District, NE		2.0 8			Sector Contemporation	10.01,0000.001		17106-0.05	
Herrisburg, PA					and the second s	10 10 10 10 10 10 10 10 10 10 10 10 10 1	ing and the second s	1210.1.1	
8-web Hosting Farm		1.0 1.0	1. 1. 0.02	with.	Surface Internet	15.05.0000.000.00	the second s	12103-0-04	
Hete HAR-CLIST WIRWS		-	a water a		Logist Class	10-10-10-10-10-10-1		12100.0.00	10
Hereit is ad-clubit monoral		1.0 1.0			~		iner.	170.003.00	
		-				The set of		100.00	
Heats HAR CUST WINVO		0.0 00 00	04:00 X:00 00 X	10:00 10:			10	100000.000	10
Hueld: NAR-CUST/WIRW3				ELECTRON LAND	74	*** **********************************	2	170.00.001.00	11.1
Houte HAR-OUST-WINWI		Pricest Peckets Out		APC/2401	-			17114-00120	10
Hada HAN-CUST WINWS							14	171.0.00.00	10
Pountar, TX	Port 1/2					19-101103-0071-0-001	1.0	17134.301.00	
Marmi, PL	[100-52-5450	0-2 - Tra				171.01.001.70	10
B Public Printing						Karley Bridge Fil	10	198.07.76200	35
		1				Rectaul Bridge IV	10	100.37.74.340	100
- Hold: NGA48-07299-3		10 K		1.0		No. of Concession (Con-	Contractor of	10110-0-0-0	
Phoenix, AZ		2 Bullion	Will a helt and	U. ANNA			10	670.003.00	10
Sature City, UT		- 200 K YWY - YY	Manua	the h		NA PAINT DOM 1		12104.0.0	10
San Diegs, CA		200 K			(here)				
San freedox, CA		·	والمت بموصف ا	at a bush		and the second	- 10		
Santa Pe. INI		0.00	04:00 36:00 09:30	10:00 12:	00 14:00 19:0	0 10100 20100 2210	0		
Dyracuse, W		Debugal Convert: Outloand Convert: :							
		Sectores contests	early a manufal a	and the second	And a state of the	 Second control with the second se second second sec	~		
Tampo, R.			HIC-52-595109-2	- Had over	Inclusive - 14	1			
Treaton, NJ						•	1		

Cacti Network Monitoring

Monitoring Network Traffic From Intrusion Detection Systems

Supported by NSF LUCID: A Spectator Targeted Visualization System to Broaden Participation at Cyber Defense Competitions (Grant ID: NSF-DUE 1303424) Mahfoudh M. Batarfi, Department of Computer Science, Bowie State University **Dr. Jie Yan**, Department of Computer Science, Bowie State University







MONITORING TOOLS

Linux Dash – Linux Server Performance Monitoring From its name, "Linux Dash" is a web dashboard that shows you the most important information about your Linux systems such as RAM, CPU, file-system, running processes, users, bandwidth usage in real time, it has a nice GUI and it's free & open-source.

							Acim	aple		h da	cht		C d to	o moni	te
							A SIII	ipie	evve	u ua	ISTIL	JUai	uit	mon	
0	General I	nfo	C	×		🖵 Lo	ad aver	age		0		٢			
	CentOS rele		nal)" 2.6.	32-				Ν	lumber	of cor	es: 1				
	.2.0.1.el6.i6 1e: 36 days		5						_						
	r Time: Tue			T 2014			nin			min			15 r		
Hostn	ame: locali	nost.localde	omain				4%			4%				%	
						0	.14		().04			0.	01	
														-	
	Disk Usa	-	2	×										Soft	wai
FILESY:		SIZ		USED 66M	AV/	9M	USE%		MOUNT /boot	IED				ava	
/dev/s		97		74G	19		81%		/data					ava apache2	
/dev/s		97		39G	53		43%		/home					nginx	
/dev/s				13G	82		14%		1					/sftpd	
tmpfs		2.0		0	2.0		0%		/dev/s	hm				node	
													V	/im	
	DHCP Lea	ases	C	×										IP	
EXPIRE			ADDRESS			IP ADDRESS			HOSTNA	ME			I	NTERFACE	
No da	ita available	e in table											e	external ip	
															Prev
NUMB 7	ER OF CONNI	ECTIONS		IP ADDRESS		25		HOST wikip	edia.orį	g				1ME (IN MS) 264.331	
1				172.16.25.1	25			gnu.o	rg						
1 1				8.8.8.8	25				org b.com				3	22.958	
			1			207				First	Previo	ous <u>1</u>			
1	Firs	t Previous	:	8.8.8.8 ::ffff:103.21		207				First	Previo	ous <u>1</u>			
1			: <u>1</u> Next	8.8.8.8 ::ffff:103.21		207		githul	b.com		Previo		Next		
1	Firs Users USER	C	:	8.8.8.8 ::ffff:103.21		207		githul				ous <u>1</u>			r
1 1	Users	Ю	i <u>1</u> Next	8.8.8.8 ::ffff:103.21 t Last		207		githul	b.com Onlir	FROM		2	Next	Last	r
1 1 ***	Users	HO /ho	1 Next	8.8.8.8 ::ffff:103.21 t Last day		207		githul Second	b.com Onlir	FROM 172.	116.25.	2 125	Next	Last LOGIN AT 00:00	r
1 1 TYPE USET	Users USER midday	HO /hc	i <u>1</u> Next	8.8.8.8 ::ffff:103.21 t Last day ios		207		githul Second	b.com Onlir	FROM 172.	116.25.	2	Next	Last LOGIN AT 00:00	r
1 1 TYPE User	USER midday nagios	HO /ho /ho	i <u>1</u> Next	8.8.8.8 ::ffff:103.21 t Last day ios	.187.2			githul Second	b.com Onlir	FROM 172.	116.25.	2 125	Next	Last LOGIN AT 00:00	r
1 1 TYPE User User	USER Midday nagios tecmint	Ho /ho /ho ita /da	i <u>1</u> Next	8.8.8.8 ::ffff:103.21 t Last day ios nint	.187.2			githul Second	b.com Onlir	FROM 172.	116.25.	2 125	Next	Last LOGIN AT 00:00	r
1 1 TYPE User User User	USER USER midday nagios tecmint imageda nfsnobor	HO /ho /ho hta /da dy /va	i <u>1</u> Next	8.8.8.8 ::ffff:103.21 t Last day ios nint	.187.2			githul Second	b.com Onlir	FROM 172.	116.25.	2 125	Next	Last LOGIN AT 00:00	r
1 1 TYPE USET USET USET USET	Users Midday nagios tecmint imageda nfsnobou First Pre	Ho ho ho ta /ho ta /da ta /da ty /va vious 1 2	i 1 Next ME ome/nagi ome/tecn ata/httpd ar/lib/nfs : 3 4 5	8.8.8.8 ::ffff:103.21 t Last day ios nint /htdocs/ima Next Last	.187.2			githul Second	b.com Onlir	FROM 172.	116.25.	2 125	Next	Last LOGIN AT 00:00	r
1 1 TYPE USET USET USET USET	USER USER midday nagios tecmint imageda nfsnobor	HO ho ho ho ho ho ho ho ho ho ho ho ho ho	A the second sec	8.8.8.8 stifff:103.21 t Last day ios nint /htdocs/ima Next Last	ageda	ta		githul Second	Onlir ay	FROM 172. FIrst	116.25.	2 125	Next	Last LOGIN AT 00:00 Last	r
1 1 TYPE USET USET USET USET	Users Midday nagios tecmint imageda nfsnobou First Pre	Ho ho ho ta /ho ta /da ta /da ty /va vious 1 2	i 1 Next ME ome/nagi ome/tecn ata/httpd ar/lib/nfs : 3 4 5	8.8.8.8 ::ffff:103.21 t Last day day ios nint Next Last Next Last PU	.187.2	ta v		githul Second	onlir ay R	FROM 172.	116.25.	2 125 us 1	Next	Last LOGIN AT 00:00	r
1 1 TYPE USER USER	Users Midday nagios tecmint imageda nfsnobou First Pre	HO HO Mata Mata And Mata Mata Mata Mata Mata Mata Mata Mata	ME me/mide ome/mide ome/nage ome/teen ata/httpd ata/httpd ata/httpd ata/httpd ata/httpd ata/httpd ata/httpd ata/httpd ata/httpd ata/httpd	8.8.8.8 ::ffff:103.21 t Last day ios nint Next Last Next Last PU 0 0 0 0 0 0 0 0 0 0 0 0 0	ageda	ta V		githul Second	Onlir ay	First	116.25.	2 125 τηγ	Next	Last LOGIN AT O0:00 Last STAT	r
1 1 TYPE USET USET USER 058	USER INIDAL	HO HO Mata /da dy /va vious 1 2 PID 1543	i i i <td>8.8.8.8 ::ffff:10.3.21 t Last day ios nint Next Last PU 4 0 0 0 0 0 0 0 0 0 0 0 0 0</td> <td>.187.2 ageda : :</td> <td>ta v 1 3</td> <td>×z 7432</td> <td>githul Second</td> <td>Onlir ay R R 3 1</td> <td>First SS</td> <td>116.25.</td> <td>2 125 5 5 125 7 7 7 7</td> <td>Next</td> <td>Last</td> <td>r</td>	8.8.8.8 ::ffff:10.3.21 t Last day ios nint Next Last PU 4 0 0 0 0 0 0 0 0 0 0 0 0 0	.187.2 ageda : :	ta v 1 3	×z 7432	githul Second	Onlir ay R R 3 1	First SS	116.25.	2 125 5 5 125 7 7 7 7	Next	Last	r
1 1 TYPE USET USET USER 68 68	USER INIDAL	HO Mo	i 1 Next MME Dome/middi Dome/nagigo Dome/tecn ata/httpd Dome/tecn ata/httpd C 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	8.8.8.8 ::ffff:10.3.21 t Last day ios nint /htdocs/ima Next Last PU	.187.2 ageda : : :	ta 1 3 1	sz 7432 6640	githul Second	Onlir ay R R 3 1 1 8	FROM 172. First	116.25.	2 125 us 1 7 7 7 7	Next	Last LOGIN AT O0:00 Last Salat	r
1 1 TYPE USET USET USET USER 68 68 68	USER USER Indiday	Image: Provide state sta	i 1 i 1 i 1 i 1 i 1 i 1 i 1 i 1 i 1 i 3	8.8.8.8 ::fff:103.21 t Last day ios nint Next Last PU 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ageda : : : : : : : : : : : : : : : : : : :	ta v 1 3 1 3	52 57 7432 181192	githul Second	Onlin ay R ay R ay ay	ne FROM 172. First 55 708 072	116.25.	 την <liτην< li=""> <liτην< li=""> την την</liτην<></liτην<>	Next	Last LogIN AT 00:00 Last Salat	r
1 1 TYPE USET USET USET USER 68 68 68 68 68	USER USER midday nagios tecmint imageda nfsnobou First Pre Processe	HO ho ho ho ho ho ho ho ho ho ho	i i Next i i Next MME MME MME MME MME MME MME MM	8.8.8.8 i:fff:103.21 t Last day los nint Next Last PU PU 0 0 0 0 0 0 0 0 0 0 0 0 0	.187.2 ageda : : : : : : : : : : : : : : : : : : :	ta 1 3 1 3 1	52 52 7432 181192 1144	githul Second	Onlir ay R ay	RROM 172. FIrst SS 708 072 1824 004	116.25.	2 125 125 125 127 2 2 2 2 2 2 2 2 2 2 2 2 2	Next	LUGIN AT 00:00 LUGIN AT 55 55 55 51 55 51 55	r
1 TYPE USER USER 68 68 68 68 68 68 68 68 68 68	USER USER Midday nagios tecmint imageda nfsnobou First Pre Processe	HO ho ho ho ho ho ho ho ho ho ho	i i 1 Next i i 1 Next MME MME MME MME MME MME MME MM	8.8.8.8 i:fff:103.21 it Last iday ios inint Vhtdocs/ima	.187.2 ageda : : : : : : : : : : : : : : : : : : :	ta 1 1 3 1 3 1 5	SZ 7432 2660 181192 1144 2024	githul Second	Onlir ay R ay	E FROM 172. FITST SS V V V V V V V V V V V V V V V V V	116.25.	 2 12 3 5 4 7 7	Next	Last A CGRN AT COGRN AT	r
1 TYPE USER USER 68 68 68 68 68 68 68 68 68 68 68 68 68	USER USER midday nagios tecmint imageda nfsnobor Processe av av	Image: Constraint of the second se	i 1 Next ME me/mid x x x x x x x x x	8.8.8.8 ::fff:103.21 : Last : day :	ageda 3000 3000 2000 3000 3000 3000 3000 300	ta v 1 3 1 3 3 1 5 3 3 3	sz 7432 1640 181192 181192 1244 2024 1260	githul Second	Normalize Right Right	E FROM 172. FIrst SS SS 70 8072 1824 004 608 716 136 120	116.25.	TTY 125 125 125 126 127 128 129	Next	Last 	r
1 TYPE user user user user USER 68 68 68 68 68 68 midda midda midda midda midda	USER USER Midday Anglos tecmint Imageda Afsnobol First Pre Processe	Image: Constraint of the second se	i 1 Next ME ME Come/mag	8.8.8.8 Second	All 187.2 Ageda MMEM 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	ta 1 1 3 1 3 3 3 3 3 3 3 3 3 3 2 2	52 7432 181192 1144 12024 6200 0040 0040	githul Second	Conlir ay 8 8 8 8 3 1 1 8 8 1 1 1 1 1 1 1 1 9	FROM 172. FIrst SS 708 702 1824 004 608 716 136 120 55	116.25.	Image: 100 km s and 1	Next	Last	r
1 TYPE USER USER 68 68 68 68 68 68 68 68 68 68 68 68 68	USER USER Midday Anglos tecmint Imageda Afsnobol First Pre Processe	Image: Constraint of the second se	i 1 Next ME me/mid x x x x x x x x x	8.8.8.8 Second	ageda 3000 3000 2000 3000 3000 3000 3000 300	ta 1 1 3 1 3 3 3 3 3 3 3 3 3 3 2 2	sz 7432 1640 181192 181192 1244 2024 1260	githul Second	Onlir ay R 8 3 1 1 8 8 1 1 1 1 1 1 1 1 1 1 9 8	RECONTRACTOR CONTRACTOR CONTRACTO	1 16.25. Previo	 ТТУ TТУ TТУ TТУ TТУ	Next Next	Last 	

linux-dash: Server Monitoring Tool

Observium – Network Management and Monitoring

Observium is also a network monitoring tool, it was designed to help you manage your network of servers easily, there are 2 versions from it; Community Edition which is free & open-source and Commercial version which costs £150/year. **Features of Observium :**

Written in PHP with MySQL database support. Has a nice web interface to output information and data. Ability to manage and monitor hundreds of hosts worldwide. The community version from it is licensed under QPL license. Works on Windows, Linux, FreeBSD and more.

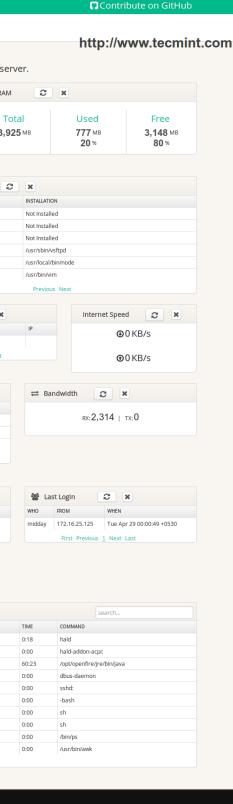
Overview § D	evices @Services	Locations	# Ports	♣Health a	# BGP Seasi
alpha.r	nemetic.org				
Overview	Graphs 🔺 Health	Apps >+ Co	illectó 🥖 Por	ts 🚳 Invento	y 🌐 Se
them about more	tio.org 3.4.32-32-3		to the first first	11 P	rocessor
20:38:33 UTC 201			an sine find date		Core i7 9
Hanfware	General v85.64	-bit		Inte	Core i7 9
Operating System		2-server (Utuentu	10.00)	Inte	Core 17 9
Contact	Adam Armstron	ng cadama@meme	tic.org>	Inte	Core i7 9
Location	Ovh, Paris, Ha	PICE .			Core i7 9
Uptime	23 days, 10h i	im 5.24			
					i Core i7 9
50 AT					Core i7 9
40.77			1	Inte	Core 17 9
8 90.00		1		- 1 BD N	lemory P
-25 8	20:00 22:00 00:00 02:0		you ho	Phys	sical mem
10.00 10.00	20.00 22.00 00.00 02.0		00 20.00 22.00		al memor
# 43	# 20	21	#22	2 2000	p space
lo, eth0, eth1, virbr1	, virbr0, cisco0, vaet0,	vnet4, vset1, m	13, vnet3		
in Freedom				E S	torage
Services				1	
0.5	0.5	0.0	00	/hor	
des, http, map, pop,	sale			/ mm	*

Observium: Linux Network Monitoring

Icinga – Next Generation Server Monitoring

Unlike the other tools, **Icinga** is a network monitoring program, it shows you many options and information about your network connections, devices and processes, it's a very good choice for those who are looking for a good tool to monitor their networking stuffs.

- Features of Icinga
- Icinga is also free and open-source.
- Very functional in monitoring everything you may have in networking.
- Support for MySQL and PostgreSQL is included.
- Real-time monitoring with A nice web interface.
- Very expendable with modules and extensions. Icinga supports applying services and actions to hosts.
- A lot more to discover...



Devices 177 (12 up 3 down 2 ignored 2 divolded) Parts : 140 (97 up 3 down 5 ignored 43 shutdown 3	Parte : 140 (00 up 3 down 5 ignored 43 shutdows 3 m System Acces : Events Systeg : Settings 0 0 2.67GHz			Logget'rs as adama	Empire() via (Perf
Alexandre Series System Second Second Secon	Aces Events Syslog Settings 0 0 2.67GHz	De		the second states of the	
0 0 2.67GHz	0 0 2.67GHz	mić.			/ System
0 0 2.67GHz 11% 0 0 2.67GHz 11% 0 0 2.67GHz 14% 10 0 2.67GHz 14%	0 0 2.67GHz				
0 0 2.67GHz 11%	0 0 2.67GHz	vices 11 Events	Syslog	2 Settings	
0 0 2.67GHz	0 0 2.67GHz				
0 0 2.67GHz 1111 0 0 2.67GHz 11111 0 0 0 2.67GHz 111111 0 0 0 0 0 0 0 0 0	0 0 2.67GHz	0 0 2.67GHz		Contraction of the local division of the loc	31%
0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 0 2.67GHz 2155 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 2.67GHz 1115 0 0 2.67GHz 2115 1 0 0 0 1 2115 1 0 0 0 1 2115 1 0 0 0 1 2115 1 0 0 0 1 2115 1 0 0 0 1 2115 1 0 0 0 1 2115 1 0 0 0 1 2115 1 0 0 0 1 2115	0 @ 2.67GHz	manual		31%
0 0 2.67GHz 2555 0 0 2.67GHz 2555 0 0 2.67GHz 2557 0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 0 2.67GHz 2155 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 2.67GHz 2555 0 0 2.67GHz 2555 0 0 2.67GHz 2557 0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 2.67GHz 2155 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 @ 2.67GHz			34%
0 0 2.67GH2 1155 0 0 0 2.67GH2 1155 0 0 0 2.67GH2 1155 0 0 0 2.67GH2 1155 0 0 0 2.67GH2 1155 0 0 0 0 2.67GH2 1155 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 2.67GHz 1155 0 0 2.67GHz 1155 0 0 2.67GHz 1155 ols 7.09GB / 7.01GB 98.4556 1.1156 / 7.01GB 98.4556	0 @ 2.67GHz			41%
0 0 2.67GHz 14% 0 0 2.67GHz 14% ools 77 7.61GB 77.61GB 18.45% 141 10 H17 21.34GB 2.55% 141 10 H17 21.34GB 2.55%	0 0 2.67GHz 1115 0 0 2.67GHz 1115 ols 7.69GB / 7.81GB Y 2.67GHz 10 0 2.67GHz 1115 ols 7.69GB / 7.81GB Y 2.67GHz 10 0 2.67GHz 1115 11 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 @ 2.67GHz			36.96
0 0 2.67GH2	0 0 2.67GHz 3156 ols 7.69G8 / 7.61G8 98.4556 9 2.000 / 7.61G8 98.4556	0 @ 2.67GHz	instant .	1000	2556
eeks 7.6968 / 2.8168 18.45% 8.1268 2.28168 18.45% 8.1268 2.28168 21.19% 4.1178 47.11.3468 21.19% 25.7168 / 38.7568 12.96% 20.9568 / 38.4068 81%	els 7.0968 / 2.0168 10.45% 8.1008 2.0168 21.19% 4.0008 2.0168 21.19% 35.7168 / 30.7568 128.456 30.9568 / 38.4568 1896	0 @ 2.67GHz	in statements		18%
7.6968 / 7.8168 98.45% 2.10968 / 7.8168 98.45% 2.1096 / 31.3468 2.84% 35.7168 / 38.7568 92% 30.9568 / 38.4568 83%	7.6968 / 7.8168 98.45% 8.1008 / 7.8168 98.45% 8.1008 / 7.8168 71.116 8.1008 / 71.1460 71.116 9.57168 / 71.1460 71.116 9.57168 / 71.1460 92% 90.9568 / 38.4068 81%	0 @ 2.67GHz			11%
25.7368 / 36.7568 21.656 26.120 m / 31.3468 31.656 35.7368 / 30.7568 92% 30.9568 / 38.4568 83%	1.1568 / 36.2568 21.556 1.611099 / 31.3668 21.659 35.7168 / 30.7568 92% 30.9568 / 38.4568 83%	ols			
14/4 201498 / 21 24008 2 2444 25.74GR / 20.75GR 92% 20.95GR / 28.45GR 82%	1441 2004 / 211 2400 - 21 8454 25.71GR / 30.75GR - 9256 30.95GR / 38.45GR - 8856	ny .		7.6968 / 7.8168	35.45%
25.73GB / 38.75GB 92% 30.95GB / 38.45GB 83%	35.73GR / 36.75GR 92% 30.95GR / 38.45GR 83%			8.3358 / JAMPER	10.004
30.95GB / 38.45GB 8356	30.95GB / 38.45GB 8356			SAUSTINE / TELEVIS	# 3.54W
30.95GB / 38.45GB 8356	30.95GB / 38.45GB 8356				
30.95GB / 38.45GB 8356	30.95GB / 38.45GB 8356			35,2108 / 38,2508	925
	1.1310/21.0310				

CA 192.168.1.55/icin/ rituated Service

Sysstat – All-in-One System Performance Monitoring Another monitoring tool for your Linux system. **Sysstat** is not a real command in fact, it's just the name of the project, Sysstat in fact is a package that includes many performance monitoring tools like iostat, sadf, pidstat beside many other tools which shows you many statistics about your Linux OS. **Features of Sysstat**

- for IPv6.
- as well.
- Many other features.

tecmint@t	ecmin	- \$ pic	istat -p i	ALL					
Linux 3.1	1.0-2	3-generio	c (tecmin	t.com)	Thursd	ay 04 Sep	tember 2	2014	_1686
12:51:55	IST	UID	PID	%usr	%system	%guest	%CPU	CPU	Command
12:51:55	IST	0	1	0.01	0.11	0.00	0.12	1	init
12:51:55	IST	0	2	0.00	0.00	0.00	0.00	0	kthreadd
12:51:55	IST	0	3	0.00	0.01	0.00	0.01	0	ksoftird
12:51:55	IST	0	5	0.00	0.00	0.00	0.00	0	kworker,
12:51:55	IST	0	7	0.00	0.00	0.00	0.00	0	migratio
12:51:55	IST	0	8	0.00	0.00	0.00	0.00	0	rcu bh
12:51:55	IST	0	9	0.00	0.04	0.00	0.04	1	rcu sche
12:51:55	IST	0	10	0.00	0.00	0.00	0.00	0	watchdo
12:51:55	IST	0	11	0.00	0.00	0.00	0.00	1	watchdo
12:51:55	IST	0	12	0.00	0.00	0.00	0.00	1	migrati
12:51:55	IST	0	13	0.00	0.01	0.00	0.01	1	ksoftir
12:51:55	IST	0	15	0.00	0.00	0.00	0.00	1	kworker
12:51:55	IST	0	16	0.00	0.00	0.00	0.00	1	khelper
12:51:55	IST	0	17	0.00	0.00	0.00	0.00	0	kdevtmp
12:51:55	IST	0	18	0.00	0.00	0.00	0.00	0	netns
12:51:55	IST	0	19	0.00	0.00	0.00	0.00	0	writeba
12:51:55	IST	0	20	0.00	0.00	0.00	0.00	1	kintegr.

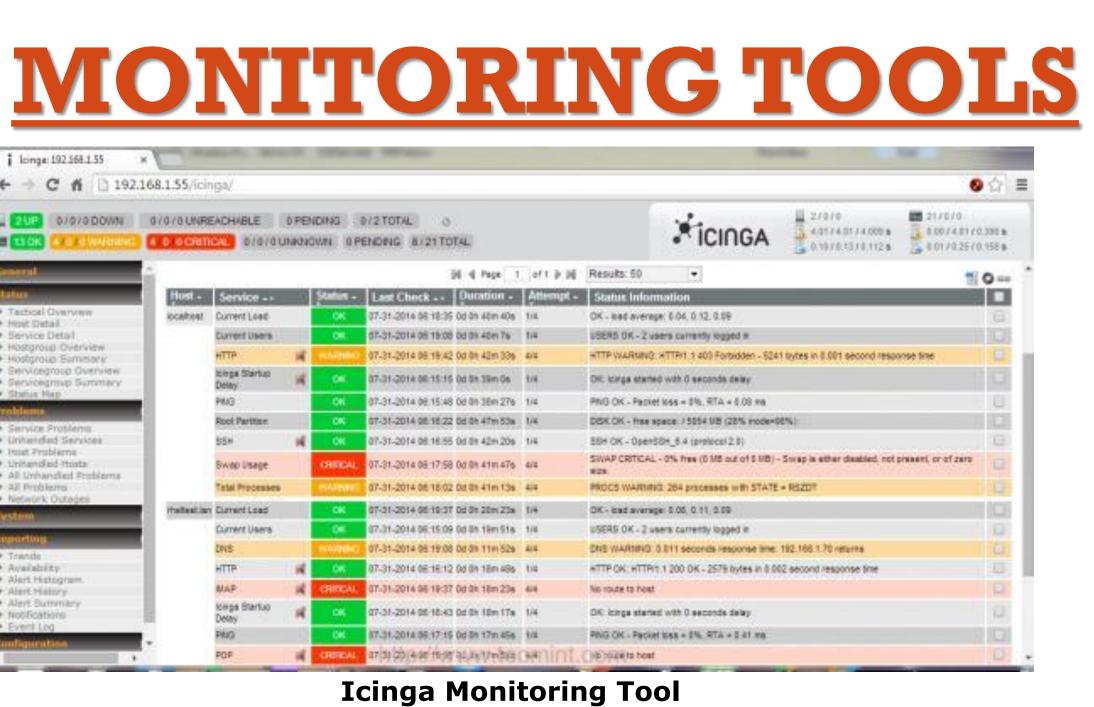
Sarg (Squid Analysis Report Generator) is a free & open-source tool which act as a monitoring tool for your Squid proxy server, it creates reports about your Squid proxy server users, IP addresses, the sites they visit beside some other information.

Features of Sarg

Licensed under GPL 2 and available in many languages. Works under Linux & FreeBSD. Generates report in HTML format. Very easy to install & use.







Available in many Linux distributions repositories by default. Ability to create statistics about RAM, CPU, SWAP usage. Beside the ability to monitor Linux kernel activity, NFS server, Sockets, TTY and filesystems. Ability to monitor input & output statistics for devices, tasks...etc. Ability to output reports about network interfaces and devices, with support

Sysstat can show you the power statistics (usage, devices, the fans speed.. etc)

Sysstat: Linux Statistics Monitoring

Sarg – Squid Bandwidth Monitoring

			SA	RG report	for 2014	Jan 21			10010
G 🛊 🖷	http://loca	/host/squid-re	ports/2014	ijan21-2014j	an21/index.	html	10	Duck Duck Go	8
rt for 2 ×									
		S/A	RC				Generator		
			Squid	d User /	CCESS A		5		
					tes, revers				
				тор p://wv	users				
				Sites	p sites & Users mloads				
USERI	D	CONNECT	BYTES	Denied Authentic	l accesses ation Failu		ELAPSED TIME	MILLISEC	%TIME
	D	20000000000000000000000000000000000000	BYTES 3.29G	Denied Authentic	l accesses ation Failu		ELAPSED TIME 725:57:08		and the second se
Pe pg		A CONTRACTOR OF		Denied Authentic %BYTES 91.57%	accesses ation Failu IN-CACI	HE-OUT	the second s	2,613,428,253	99.55%
Pg pg	.18.204	126.35K	3.29G 48.20M	Denied Authentic %BYTES 91.57%	accesses ation Failu IN-CACI 5.21%	HE-OUT 94.79%	725:57:08	2,613,428,253 1,125	99.55% 0.00%
• • • • pg • • • • 172.16 • • • • 172.16	.18.204	126.35K 31.24K	3.29G 48.20M	Denied Authentic %BYTES 91.57% 1.34%	accesses ation Failu IN-CACI 5.21% 100.00%	HE-OUT 94.79% 0.00%	725:57:08 00:00:01	2,613,428,253 1,125 575,937	99.55% 0.00% 0.02%
1 172.16 172.16 172.16 172.16 172.16	.18.204	126.35K 31.24K 2.01K	3.29G 48.20M 34.10M	Denied Authentic %BYTES 91.57% 1.34% 0.95% 0.85%	In-caci 5.21% 100.00% 3.87%	94.79% 0.00% 96.13%	725:57:08 00:00:01 00:09:35	2,613,428,253 1,125 575,937 513,197	99.55% 0.00% 0.02% 0.02%
pg 172.16 172.16 172.16 172.16 172.16	.18.204 .21.231 .21.153 .235.102	126.35K 31.24K 2.01K 1.81K	3.29G 48.20M 34.10M 30.61M	Denied Authentic %BYTES 91.57% 1.34% 0.95% 0.85% 0.80%	accesses ation Failu IN-CACI 5.21% 100.00% 3.87% 3.20%	94.79% 0.00% 96.13% 96.80%	725:57:08 00:00:01 00:09:35 00:08:33	2,613,428,253 1,125 575,937 513,197 1,278,828	99.55% 0.00% 0.02% 0.02% 0.05%
 pg 172.16 172.16 172.16 172.16 172.16 172.31 172.31 	.18.204 .21.231 .21.153 .235.102 .144.195	126.35K 31.24K 2.01K 1.81K 2.33K	3.29G 48.20M 34.10M 30.61M 28.89M	Denied Authentic %BYTES 91.57% 1.34% 0.95% 0.85% 0.80%	accesses ation Failu IN-CACI 5.21% 100.00% 3.87% 3.20% 5.85%	HE-OUT 94.79% 0.00% 96.13% 96.80% 94.15%	725:57:08 00:00:01 00:09:35 00:08:33 00:21:18	2,613,428,253 1,125 575,937 513,197 1,278,828 607,122	99.55% 0.00% 0.02% 0.02% 0.05% 0.02%
 pg 172.16 172.16 172.16 172.16 172.31 172.16 172.16 172.16 	.18.204 .21.231 .21.153 .235.102 .144.195 .23.66	126.35K 31.24K 2.01K 1.81K 2.33K 1.52K	3.29G 48.20M 34.10M 30.61M 28.89M 21.46M	Denied Authentic %BYTES 91.57% 1.34% 0.95% 0.85% 0.80% 0.80%	accesses ation Failu IN-CACC 5.21% 100.00% 3.87% 3.20% 5.85% 6.45%	HE-OUT 94.79% 0.00% 96.13% 96.80% 94.15% 93.55%	725:57:08 00:00:01 00:09:35 00:08:33 00:21:18 00:10:07	2,613,428,253 1,125 575,937 513,197 1,278,828 607,122 267,226	99.55% 0.00% 0.02% 0.02% 0.05% 0.02% 0.01%
USERI 172.16 172.16 172.16 172.16 172.16 172.16 172.16 172.16 172.16 172.16 172.16 172.16 172.16	.18.204 .21.231 .21.153 .235.102 .144.195 .23.66 .23.207	126.35K 31.24K 2.01K 1.81K 2.33K 1.52K 998	3.29G 48.20M 34.10M 30.61M 28.89M 21.46M 15.12M	Denied Authentic %BYTES 91.57% 1.34% 0.95% 0.85% 0.80% 0.60% 0.42%	accesses ation Failu IN-CACI 5.21% 100.00% 3.87% 3.20% 5.85% 6.45% 5.84%	HE-OUT 94.79% 0.00% 96.13% 96.80% 94.15% 93.55% 94.16%	725:57:08 00:00:01 00:09:35 00:08:33 00:21:18 00:10:07 00:04:27	2,613,428,253 1,125 575,937 513,197 1,278,828 607,122 267,226 198,418	99.55% 0.00% 0.02% 0.02% 0.05% 0.02% 0.01%

Sarg Monitors Squid Logs