Event Navigation

EventLog User interface

When EventLog module is selected main screen will show the following parts:

- 1. Mode Panel choose between the Syslog and SNMP Trap mode.
- 2. Main Panel displays results of SNMP request and MIB search operations.

ayslog SNMP Tr	ap System 🎙							Last 6 Ho	urs		
P.Refresh Gear Sh	ow names										
		har = 5 minutes		9	Severity	Logs	Distribution	Exporter	Log	5	Distribution
					Emergency	0	0.0%	\$9.8.4.226		12,168	
erro				- L I 💻	1-Net	11	0.0%	10.0.4.63		8,414	
800			Contraction of the local division of the loc		2-Oitical	2	0.0%	10.8.4.26		6,501	
500 m H m m	and the second second	and the second se			3-Ener	4,475	8.8%	10.8.4.75		4,761	
and the second second					+ Warning	5,565	11/0%	10.0.6.201		3,861	
400 -					5 Notice	1,233	2,4%	20.8.7.106		2,249	
				6.1	nformational	34,024	67.3%	10.0.6.202		1,829	-
200 -					7-Debug	5,266	10.4%	20.0.2.3		1,591	
					Total	50,576		Total		50.576	
05:00 05:30	osios osiss o7ico	07:30 08:00 08:	0 09:00 09:30 10:	20 10:30							
Date	Exporter	Exporter Severity Facility Message								Alarma	
				decession - Selar	In Task Oct 10	10:47:4	3.972: %DTL-4-AR	P_ORPHANENT_DETE	CTED:		
10 2017, 10:47:38.938	10.0.6.201	4 - Warning	5 - Syslogd-Internal	dtl_met.c:1721 STA REQUEST) received Address) 91.187.15	A(Target MAC) d with invalid S S8.1	lddress) PA(Sour	[18:68:3f:82:ec:2) ce IP Address] 91.1	t, 91.187.150.40] ARF 187.158.39/TFA(Desti	(op ARP sation IP		
10 2017, 10:47:30.938	10.0.6.201	4 - Warning 4 - Warning	5 - Syslegd-Internal 5 - Syslegd-Internal	dd_set.c:1721 STA REQUEST) received Address) 91.187.15 cisco5505-L: *ddA dd_set.c:1721 STA REQUEST) received Address) 91.187.15	A(Tarpet MAC) d with invalid S SR1 krpTask: Oct 88 A(Tarpet MAC) d with invalid S SR1	iddress) PA(Sour 10:47:4 iddress) PA(Sour	[10:60:37:82:ec:2) ce IP Address) 91.1 2.371: %07L-4.48 [10:60:37:82:ec:2) ce IP Address) 91.1	4, 91, 187, 150, 40] ARF 187, 158, 39/TFA(Ded) P_OF5HAMFKT_DETE 1, 91, 187, 150, 40] ARF 187, 150, 39/TFA(Ded)	(op ARP Nation IP CTED: (op ARP nation IP		
 10 2017, 10:47:38.038 10 2017, 10:47:37.336 10 2017, 10:47:36.031 	10.8.6.201 10.8.6.201 10.8.6.201	4 - Warning 4 - Warning 4 - Warning	S - Sydogd-Internal S - Sydogd-Internal S - Sydogd-Internal	dd_met.ci721 STA REQUESTI received Address) 91.187.15 cicco53505.L: *ddA dd_met.ci721 STA REQUESTI received Address) 91.187.15 cicco5508-L: *doLl STA[Target MGC A received with invali	A(Target HAC) d with involid 5 58:1 krpTask: Oct 88 A(Target MAC) d with involid 5 59:1 LMbgTask: Oct Kidness) [10:88 Ald SPA(Source	iddress) PA(Sear 10:47:4 iddress) PA(Sear 08:10:4 CF:82:e IP Adde	[18:68:37:82:ec:2) or IP Address) 91:7 2:371: %DTL-0-AR [18:68:37:82:ec:2) or IP Address) 91:7 7:41:864: %L00-4 c:24, 92:387:358.4 ms) 91:387:358.4	6, 91, 187, 158, 39, TPA(Dest) 87, 158, 39, TPA(Dest) 9, 06594AMFKT, DETE 4, 91, 187, 158, 39, TPA(Dest) 87, 158, 39, TPA(Dest) 9, IND: 68, set, c. 17, 10, AFP (op AFP REQU TTA(Destination IP A	(op ARP sation IP CTED: (op ARP sation IP 21 EST) ddress)		
18 2817, 18+47:38,338 18 2817, 18+47:35,338 18 2817, 18+47:36,831 18 2817, 18+47:36,351	10.0.6.201 10.0.6.201 10.0.6.201 10.0.7.7	4 - Warning 4 - Warning 4 - Warning 6 - Informational	S - Syslegd-Internal S - Syslegd-Internal S - Syslegd-Internal S - Syslegd-Internal 22 - Local Use 7	dd_met.ci3721 STA REQUESTI mechined Addressly 2018/07.18 dd_met.ci3721 STA dd_met.ci3721 STA dd_met.ci3721 STA ddmessly 91.187.15 cisco5588-Li*dotL STA(Tarpet MAC Ar neoemod with mult 91.187.155.1 244641 Oct 8 09:47 30.8.128.7456552	A(Target MAC J d with invold S S8.1 IrpTask: Oct 88 A(Target MAC J d with invold S S8.1 InMogTask: Oct ddress) [10:88 Ad SPA(Source 07351 % SEC-6- 2) -> 217.28.70	Iddress) PA(Sour 10:47:4 Iddress) PA(Sour 08:10:4 IPACCE 104CE 104CS	[18:68:27:182:ec:2) ce IP Address() 91.1 2.371: %DTL-4 AP [18:68:25:82:ec:2) ce IP Address() 91.1 7:41.264: %AC000 19:142:64: %AC000 19:1377:38.4 ma) 91.287.280.79 (\$LOGP: list vian20) 1 packet	t, 91.187.150.491,AKP 187.150.39/TPA(Dext) P_OSPHANPNT_DETE (1.51.187.150.49)AKP (2.187.150.39/TPA(Dext) (2.187.09 dH_set.c17 187.150.497 REQU TPA(Dextination IP A 1-in permitted top	(op ABP sation IP CTED: (op ABP sation IP sation IP 21 EST) ddress)		
 10 2017, 10:47:20.028 10 2017, 10:47:25.0336 10 2017, 10:47:26.031 10 2017, 10:47:26.755 10 2017, 10:47:25.336 	10.8.6.201 20.8.6.201 20.8.6.201 20.8.6.201 20.8.6.201	4 - Warning 4 - Warning 4 - Warning 6 - Talarmational 4 - Warning	S - Syrlopd-Internal S - Syrlopd-Internal S - Syrlopd-Internal 23 - Local Use 7 S - Syrlopd-Internal	dfmtc. 1723 TM EQUEST / received Address) 91.187.15 ctr.07538 L * ddA. dd_mstc.1723 TM EQUEST / received dd_mstc.1723 TM EQUEST / received model / dd STATAppel MAC. As received with imal 91.97.150.1 944641 OL 8 19-47 194641 OL 8 19-47 194642 OL 8 19-47 1957 J Recieved Address 9 1187-15 EQUEST / received Address 9 1187-15 EQUEST / received	A(Target MAC J d with invalid S S8.1 VrpTask: Oct 88 A(Target MAC J d with invalid S S8.1 InffsgTask: Oct 88 A(Target MAC J Vr) SSEC-4- 2) >> 217.26.70 VrpTask: Oct 88 A(Target MAC J d with invalid S S8.1	Iddress) PA(Sour 20:47:4 (ddress) PA(Sour 08:10:4 (3f:82:e IP Addes IP Addes IPACCE 300(25) 30:47:4 Iddress) PA(Sour	[10:08/71020-cc] ce IP Address] 91. 2.371: %10TL-4.40 [10:08:27123-cc] ce IP Address] 91. 7:41.904: %10.02-4 cc]d, 91.187.150.3% int 91.187.150.3% ist.06P1 list vlav20 ist.06P1 list vlav20 ist.06P1 list vlav20 ist.06P1 list vlav20 ce IP Address] 91.1	1, 91, 132, 132, 143, 143 147, 158, 139, 174, 104 147, 158, 139, 174, 104 1, 91, 137, 139, 139, 144 1, 91, 137, 139, 149, 149 147, 150, 139, 174, 104 141, 142, 104 141, 144, 144 141, 144, 144 144, 144, 144, 144, 144 144, 144, 144, 144, 144, 144, 144, 144,	(op ARP addian IP (op ARP addian IP 21 EST) ddress) CTED: (op ARP addian IP		

For the purpose of this chapter, we will focus on the navigation in the Syslog mode.

Navigating in Syslog mode

To view syslog go to EventLog module and click Syslog tab. Here you can see Syslog messages sent from different exporters for a chosen Time Window.

- 1. Show Options
- 2. EventLog Chart
- Severity Table
 Exporter Table
- Exporter Table
 EventLog Table
- 5. LVEIILOY TADIE

Table and charts will show logs that have (1) the same severity as set in Severity Table (2) for the time set in Time Window. For these logs Exporter table will show distribution by exporters and Severity Table will show distribution by log's severity.

Active alarms for Syslog message are shown in Alarms column. Column is labeled with colour of alarm severity and number of active alarms with that severity. If there is more than one active alarm with different severities, label will be split. If there are no active alarms sign "-" is shown.

Numbers under Alarm column are clickable, and after click you will be redirected to Alarm module. There, you will be able to see the list off all active alarms within that Syslog message.

Nyskog	-	o Nysten													Last 60 Plans	lei	
, Andrea	i that the	n names 1															
				bar - bi seconda a							Generity	Loga Olub	dation 3	Ispate	Loge	Databathan	
151	1											Manupacy Infert Joghad Disea Manupacy National Contemport National	1.118 946 1.128 4.00	00233350	COMAND TUBERTI COMANDE COMAND COMAND COMAND TUBERTI COMAND TUBERTI COMAND	A PARTY AND A PART	
	10.40	20 ⁵ es	10.00 10	aa 11700	12,000 1	518	15.18	11/30	11.28	11.30	11/38						
	Deb	Exporter	Browsky	Facility						Message							Abore
	4. 10.000 AL	C2463.4D	2 College	N-Secrit/Information	This is Spaling bott messary	a sankar GDA											-
24 200	10.00-0.00	172363.002	3 - Critical	17-5aoi/Sec1	The islanders but means	e nardre 6000											1 02
e 346 201	10,000000	572.863.852	1 Collect	thricolitie 3	The is Scaleg but message	a number 600											
	100000	172343.00	1-Orient	9 - Del Darran	The islipshop lesi reasons	e nelle CDD											1 02
	5 220607-065	1214-122	2-04504	N-100/VH 7	The is Seeing Suff, many	a number 600											100
34 304	10,000,041	10143.00	1 - Oriented	4 - Lea Ponter Labouters	This is Spalsey last manage	a nambar CON											
	TO BORD A	172.04.0.002	2-040-04	20-500FU84 4	The altering but many	a turbe stat											02
36 204	6,00004342	10.14.1.VD	2 - Critical	47-Local Unit 1	This is Spalley leaf-manage	p haning 600											0 21
34 200	MCCORCE #	172.343.002	3-04604	O-Keind	This is Systep but means	a harder CER											(0)
	6, 993632342	\$2343.89	E College	8 - 2002 Subsystem	This is Spaleg but message	p hanker 605											0 000
+ 34 200	10,00,00,002	171343.00	3 - Critical	4 - Insurity/Automation	The is living induced	e nardee CD1											1 02
	5, 2206-08-345	52.443.02	1 - Collect	6 - Ene Printe Subeurlam	The is Scaleg but memory	p. surber 650											1 (3)
34 200	6,15,06,08,380	17234-578	d - Ethernalized	1 - Jystere Daarnara	Hard STATISTICS DAY and	en(200) Carros	alian Iran UDPs (1034.072)40040-	07234479344								\$0
34 220	INCOME A	172.04.5.00	1-04604	the Printer Schoutsen	The a Solid NUT HARD	a surbe kill											0.00
36 204	8, 25 (K	LO1110	2 - Gettinud	20-Lond Use 4	This is Spalsey leaf-mesoary	e nanise 600											1 000
1 24 200	10.1246.01.8	172343.00	2-046-04	T - Md-oA/Teve 3-Joychen	The altyping but making	a hundre kaan											. 02
ar 34 204	6, 003006368	60.M3.40	2 - Grifford	K2 - N79 Exhipation	This is Spalling leaf messary	p hankar (D.A											
- 24 200	10,000,000	171363.00	2 - Critical	12-100/Ver8	The B Dates had manage	a hardward 22.8											

For example, on the screenshot to the left, you can see that logs that occurred during the selected Time Window and severity 0 to 7 are shown. You can also see that there was 4433 such logs (Severity Table) of which most numerous were Critical (50.0%), Informational (27.7%) and Notice (22.2%).

You can also see the distribution of these logs by exporters in the Exporter table: exporter 172.16.2.152 generated the most logs (2218).

Continue reading about Syslog Analysis.