

Visual Exploration and Analysis of Routing Events

Davide Ceneda Marco Di Bartolomeo Valentino Di Donato Maurizio Patrignani Maurizio Pizzonia **Massimo Rimondini**

RoutingWatch

Visual Exploration and Analysis of Routing Events

Davide Ceneda Marco Di Bartolomeo Valentino Di Donato Maurizio Patrignani Maurizio Pizzonia **Massimo Rimondini**

RoutingWatch



RoutingWatch



RoutingWatch



RoutingWatch



RoutingWatch



RoutingWatch



RoutingWatch







Management &	Inference	Visualization
Monitoring Tools	Algorithms	Systems















SInferenceVisualizationIsAlgorithmsSystems
--



Embedded

CISCO Event Manager

event manager applet interface_Shutdown
event syslog pattern "Interface FastEthernet1/0, changed
 state to administratively down"
action 1.0 cli command "enable"
action 1.5 cli command "config t"
action 2.0 cli command "interface fa1/0"
action 2.5 cli command "no shutdown"
action 3.0 cli command "end"
action 3.5 cli command "who"
action 4.0 mail server "192.168.1.1" to
 ".engineer@cisco.com." from ".EEM@cisco.com."
 subject ".ISP1_Interface_fa1/0_SHUT." body "Current
 users \$_cli_result"





Weather OK: No watches or warning

OK - load average: 0.29, 0.49, 0.56

USERS OK - 0 users currently logg HTTP OK: HTTP/1.1 200 OK - 218

PING OK - Packet loss = 0%, RTA

DISK OK - free space: / 20300 MB

SSH OK - OpenSSH_4.3 (protocol

SWAP OK - 100% free (255 MB ou

PROCS OK: 147 processes with ST

area

response time

Management & Inference Visualization **Monitoring Tools** Algorithms **Systems** 11 11 11 Embedded OS® Monitoring CISCO Event Inspecto event manager ap Managerface_Shutdown event syslog pattern "Interface FastEthernet1/0, changed state to administratively System down action 1.0 cli command "enable" action 1.5 cli command "config t" action 2.0 cli command "interface fa1/0" action 2.5 cli command "no shutdown" action 3.0 cli command "end" Nagios' **Current Network Status Host Status Totals** Service Status Totals action 3.5 cli command "who" Last Updated: Fri Oct 17 18:51:18 UTC 2014 Up Down Unreachable Pending Ok Warning Unknown Critical Pending action 4.0 mail server "192.168.1.1" to Updated every 90 seconds .engineer@cisco.com." from 11 0 0 0 33 1 1 4 0 Nagios® Core™ 4.0.8 - www.nagios.org ".EEM@cisco.com." subject General Logged in as naglosadmin All Problems All Types All Problems All Types .ISP1_Interface_fa1/0_SHUT." body 0 11 6 39 Home "Current users \$_cli_result" View History For all hosts Documentation View Notifications For All Hosts View Host Status Detail For All Hosts Current Status Service Status Details For All Hosts Tactical Overview Map Limit Results: 100 V Hosts Service ** Attempt ** Status Information Services Host ** Status ★★ Last Check ★★ Duration ★★ Host Groups Aurora OK: Activity level is 2 NOAA × Auroral Activity 10-17-2014 18:51:09 535d 4h 28m 6s 1/3 Summary Grid Weather Carteret North WARNING 10-17-2014 18:43:15 Od Oh 46m 57s 3/3 Weather Warning: Beach Hazards Service Groups Carolina Summary Weather King Weather OK: No watches or warning Grid 10-17-2014 18:45:25 737d 1h 52m 46s 1/3 Washington Problems area Services (Unhandled) Weather Ramsey Weather OK: No watches or warning 10-17-2014 18:46:45 59d 20h 47m 12s 1/3 OK Hosts (Unhandled) Minnesota area Network Outages Weather Quick Search San Weather OK: No watches or warning • 10-17-2014 18:41:45 Od 0h 48m 40s 1/3 Bernardino area California Weather Reports Strafford Weather OK: No watches or warning -10-17-2014 18:43:45 Od 0h 46m 51s 1/3 Availability New area

Hampshire

Oklahoma

Current

Load

HTTP

PING

SSH

localhost

Weather Tulsa

Current Users

Root Partition

Swap Usage

Total Pro

-

OH

OH

10-17-2014 18:45:53 737d 1h 53m 51s

10-17-2014 18:48:25 1019d 2h 7m 58s

10-17-2014 18:51:02 1710d 15h 36m 24s 1/4

10-17-2014 18:50:20 1710d 15h 35m 9s 1/4

10-17-2014 18:48:32 938d 2h 32m 35s 1/4

10-17-2014 18:46:38 1704d 7h 35m 15s 1/4

10-17-2014 18:48:54 1710d 15h 33m 17s 1/4

10-17-2014 18:50:49 1706d 8h 22m 2s

10-17-2014 18:49:08 Od Oh 46m 9s

1/3

1/4

1/4

Trends

Alerts

History

Summary Histogram

Notifications

Event Log

Comments

Downtime

Process Info Performance Info

Configuration

Scheduling Queue

System





Management & Inference Vis Monitoring Tools Algorithms S

Visualization Systems



event manager ap Man agerface_shutdown event syslog pattern "Interface FastEthernet1/0, changed state to administratively down" action 1.0 cli command "enable" action 2.0 cli command "interface fa1/0" action 2.5 cli command "end"

action 3.5 cli command "who" action 4.0 mail server "192.168.1.1" to ".engineer@cisco.com." from ".EEM@cisco.com." subject ".ISPl_Interface_fal/0_SHUT." body "Current users &_cli_result"

					-	-		ng	
Nagios'	Current Network Last Updated Price	Status	18 970 2014	U	Hout St.	dus Totals	OK Yhanny U	Status Total	in Pending
	Repuel Cor" 41		qua.wy			* *	M •		
	collector and other				ATALLA	Al Types	ALTO	CARL AT THE	
Plane Documentation	View History For all View Scotloations Fo	NORS PORT							-
AVAILABLE STATES						and a faster l	And the Part of the		
Tactical Overview Map	und femile 200					Service coattle I	Jeuris Por Jul	10090	
Services	19141 **		Service **		Males **	Last Check **	Duration **	Allowed **	Status information
Heat Groupe	10/104	*	Annual a list.		100	10.15.254 01.17.26	STATUS TRANSPORT	12	Annual Co. Adult Red & 7
Orid Rervice Groups			theber Carbon 75x0		INTER	10-11-021H 18:K0.15	N 24 404 175	30	Andrew Variety, Beach-Halande
Dela Problema			Vasher Keg Vashington		OK	10-17-2214 10-45-25	1212 11 520 404	15	Vasiliar OC his webles or ware area.
Services (Unhandled) Hosts (Unhandled)			Vester fors	10	ox	15.17.2014 18.46.45	10x 20x 41m 12s	13	Vester OR No watches or wart also.
Sumon Conspin			Vesther Zan Bernandens California		OR.	10-13-2014 10-41-40	00 01 401 40s	15	Vasilier DC für unlichen im andre 979.
and a local la			Vester						
Analobility Trends			20uffield Here Herendez		08	10-17-2214 10-42-45	der din wähn Site	15	Vealer OC 10 withtet or wait
Alerta History Summary			Vester Tube Chattons		ок	10.07.2014 19.45.53	TITLE IN STREETING	13	Vester OI, to wat tes or wart and
Hatoptam Notificationa	notes		Current		OR	10 17 2014 10 40 00	00 01 40m 34	14	CK- Kel aways 5.21 5.41 5.1
EventLog			Ourset itsets		06	10-17-2014 10-51 02	1710015n.00m.04s	58	USERS DK- I seen currents by
and a second			HTTP		ox	10.11.2014 18 48 28	101 N 2h 7m 58a	14	HTTP OR HETRIG \$ 200-DK-24 response the
Conments			9990		04	10-17-2014 10:50:20	171001012000	54	PING OK - Pathet Ball + 2%, 871
Document Info			Post Parties		04	10-17-2014 10-40-22	9080 2h 30h 354	14	OTH DK - New space / 20000 rm
Parksmance Info			591		01	10-17-2014 10-40-20	17540 In 25n 154	54	55H DK - Open55H1.4.3 (ph/200
Scheduling Queue			Sweet-Annes		06	10-17-2214 104054	17130155-555113	54	554P (H-1075 Not (255-10)
Consputation			Table Income		1000		a bild of the follow for		debut a data and second and it

Raise alarms based on unexpected changes in:

- performance levels (bandwidth)
- health flags (interface status)
- configurations





Management & Inference Visualization **Monitoring Tools** Algorithms 11 111 11 Embedded



Event event manager ap Managerface_Shutdown event syslog pattern "Interface FastEthernet1/0, changed state to administratively down action 1.0 cli command "enable"

action 1.5 cli command "config t" action 2.0 cli command "interface fa1/0" action 2.5 cli command "no shutdown" action 3.0 cli command "end" action 3.5 cli command "who" action 4.0 mail server "192.168.1.1" to

.engineer@cisco.com." from .EEM@cisco.com." subject .ISP1_Interface_fa1/0_SHUT." body "Current users \$_cli_result"

	-			-			ng	
Nagios'	Current Network Stat Lett Upsteel Price 1718 Upsteel Party ID Manuals	IST NEWYO 2014	-	Hout St.	itus Totals muhatris Pending	Cit Wanning D	Status Tota	A Pending
General	Looped P. es nertisatives	a reported		4150.00	and Talant	47.00		a contract of the second
Hone Documentation	View History For all holds View Soldcattures For ALP	odu			-	-	н	1
CALIFIER MODILE	Vew Hod Status Detail Po	APPER						
Tactical Overview					fervice Status I	petails For All	190905	
Map								
House a	Und results 17.0							Dates internation
Heat Groups	10.00	Annual		And the owned	LINE CORES - +	Contrast	And and a second second	
Symnets		The first states		~				
Revice Groups		Called 75x8 Call/Mil		INTERS	10-11-2014 18:K0.15	N 28 400 275	99	Zouthe Vanity, Booth-Aca
Citid Excidence		Vester Kry Vestington		OK	10-17-2014 10-40-20	7270 11 521-404	10	Vasilier OC No webdes or at 979.
Services (Unhandled) Heats (Unhandled)		Vester for termoots	90	ox	15.17.2014 18.46.45	10x 20x 41m 12s	13	Vestler OK No watches or an area.
Out Seest		Vester San Bernardes California		OR	10-13-2014 10-41-40	00 01 401 40s	15	Vasifier OC for unit-feet or an area.
Analadaliy Timah		Vester Stuffed Here Herestes		04	10-17-2214 104040	de de vider dira	55	Vestler OK 16 sublet ir as
Alerta Hatary Sumnary		Vester Tub Chahona		os	10.07.2014 1848.63	Title in film file	13	Vester OI: No withteo or we area.
Hatoptan Notificatione	nated	Current		OR	10-11-2014 10-48-08	00 25 40m 34	14	CK- Kel aways 521 541
EventLog		Current inset		06	10-17-2014 10-51 02	1710/151.50m.041	58	USERS DC- I seen our with it
lystem		HTTP		ox	10.17.2014 10.48.21	101 N 2h Ter Sh	14	HTTP OR HETRR & 200-DK-
Conments		-		-		alla be alla bila da		response and
Downtime Countries Info		these Description		0	10.12. MAA ST.AT.ST.	star in the Ma	-	Print Fill - New Holds - Children
Curleymance Info		1001		0	VALUE AND ADDRESS	riting in the ris	14	Statute - Countries a 3 years
Scheduling Opeum		funded have		08	VALUE ANALYS	17101150.000170	14	SAND FRI , 1975 Bay (155 urb
Configuration		TableTown		100				debut a data and second and

Systems

Raise alarms based on unexpected changes in:

- performance levels (bandwidth)
- health flags (interface status) ____
- configurations
- Require polling and/or agents
- Must support many technologies





Management &	Inference	Visualization	Part Part
Monitoring Tools	Algorithms	Systems	

- J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network". Proc. NSDI, 2005
 - Online BGP route analysis to find and correlate events
- G. Comarela, G. Gürsun, and M. Crovella, "Studying Interdomain Routing over Long Timescales". Proc. IMC, 2013
 - Evolution of the Routing State Distance
- G. Comarela and M. Crovella, "Identifying and Analyzing High Impact Routing Events with PathMiner". Proc. IMC, 2014
 - Next-hop tensor factorization





Management &	Inference	Visualization
Monitoring Tools	Algorithms	Systems

- J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network". Proc. NSDI, 2005
 - Online BGP route analysis to find and correlate events
- G. Comarela, G. Gürsun, and M. Crovella, "Studying Interdomain Routing over Long Timescales". Proc. IMC, 2013
 - Evolution of the Routing State Distance
- G. Comarela and M. Crovella, "Identifying and Analyzing High Impact Routing Events with PathMiner". Proc. IMC, 2014
 - Next-hop tensor factorization
- Focus on BGP
- Long-term Internet evolution studies
- Limited information about each event (typically, cause AS)





Managem	ent &	Inference	Visualization	
Monitoring	Tools	Algorithms	Systems	a The State of The

- J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network". Proc. NSDI, 2005
 - Online BGP route analysis to find and correlate events
- G. Comarela, G. Gürsun, and M. Crovella, "Studying Interdomain Routing over Long Timescales". Proc. IMC, 2013
 - Evolution of the Routing State Distance
 - Future work envisions combined investigation of <u>space and time</u>, assessment of the <u>type of routing</u> <u>change</u>, <u>event inference</u>
- G. Comarela and M. Crovella, "Identifying and Analyzing High Impact Routing Events with PathMiner". Proc. IMC, 2014
 - Next-hop tensor factorization
- Focus on BGP
- Long-term Internet evolution studies
- Limited information about each event (typically, cause AS)





Management &	Inference	Visualization
Monitoring Tools	Algorithms	Systems

- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Discovering High-impact Routing Events using Traceroutes". Proc. ISCC, 2015
- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Mining Network Events using Traceroute Empathy". Tech. Rep., 2015 http://arxiv.org/abs/1412.4074v2.pdf
 - Event inference





_			
	Management &	Inference	Visualization
	Monitoring Tools	Algorithms	Systems

- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Discovering High-impact Routing Events using Traceroutes". Proc. ISCC, 2015
- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Mining Network Events using Traceroute Empathy". Tech. Rep., 2015 http://arxiv.org/abs/1412.4074v2.pdf
 - Event inference

Lots of inferred events





Management & Monitoring ToolsInference AlgorithmsVisualization Systems	Management & Monitoring Tools	ference orithms Systems
---	----------------------------------	----------------------------

 M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Discovering High-impact Routing Events using Traceroutes". Proc. ISCC, 2015



- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, "Mining Network Events using Traceroute Empathy". Tech. Rep., 2015 http://arxiv.org/abs/1412.4074v2.pdf
 - Event inference

Lots of inferred events











Visual exploration tool for a large number of routing events





Visual exploration tool for a large number of routing events

Target users: high-level administrators in a NOC, interested in highly informative aggregate reports







- Visual exploration tool for a large number of routing events
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require agents running on devices







- Visual exploration tool for a large number of routing events
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require agents running on devices
- (Partial) visibility of events in external networks









- Visual exploration tool for a large number of <u>routing events</u>
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require agents running on devices
- (Partial) visibility of events in external networks









RIPE Atlas

Sam Knows





RIPE NCC 1 d Sam Knows RIPE NETWORK COORDINATION CENTRE **RIPE** Atlas ARCHIPELAGO **RIPE NCC** Leaflet | Tiles © Esri - Esri, DeLorme, NAVTEQ



























Event






















































Display events that satisfy the following conditions:

5	10	15	20	AND	

MA

	<nor< th=""></nor<>
Target is:	<nor< th=""></nor<>
	<nor< td=""></nor<>

 ∇



	Edge count cap	(max: 35532)
Compute similarity betwee	n events consideri	.ng:
Sets of probes		
0 50 100	0 50 100	None 🔻
Sets of causes		similarity panel









































































filtering panel



filtering panel



filtering panel
























similarity panel































continuous interaction





Edge_count cap (max:17292) 2000 4000 Ó Compute similarity between events considering: Sets of probes Recurrence: Time: Time of day 🔻 50 50 100 100 Sets of causes 0 50 100









User study



User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)





User study



User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results: 5





User study



User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results:

events are a useful aggregation of routing dynamics





User study



User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results:



 events are a useful aggregation of routing dynamics
 comparing events by probes/geography/time is useful to find related events





User study

User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results:



the tool supports it effectively





User study



 events are a useful aggregation of routing dynamics
 comparing events by probes/geography/time is useful to find related events
 the tool supports it effectively

finding related events is useful





User study



 events are a useful aggregation of routing dynamics
 comparing events by probes/geography/time is useful to find related events
 the tool supports it effectively

- finding related events is useful
 - the tool supports it effectively





ilters

User study

User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results:

 events are a useful aggregation of routing dynamics
 comparing events by probes/geography/time is useful to find related events
 the tool supports it effectively

- finding related events is useful
 - the tool supports it effectively





ilters

User study

User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results:

 events are a useful aggregation of routing dynamics
 comparing events by probes/geography/time is useful to find related events

the tool supports it effectively

- finding related events is useful
 - the tool supports it effectively







Filters

User study

User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
 Questionnaire results:

 events are a useful aggregation of routing dynamics
 comparing events by probes/geography/time is useful to find related events

 the tool supports it effectively

- finding related events is useful
 - the tool supports it effectively



"A tool for mining traceroutes"

Scalability of the user interface (e.g., clustering leaders)

 Scalability of the user interface (e.g., clustering leaders)
 Other notions of similarity (e.g., geography-based)

 Scalability of the user interface (e.g., clustering leaders)
 Other notions of similarity (e.g., geography-based)
 Real-time analysis (streaming data analytics)

Scalability of the user interface (e.g., clustering leaders) Other notions of similarity (e.g., geography-based) Real-time analysis (streaming data analytics) **Exploration** session (to build a knowledge base)