

Dashboards & Visualizations: What's New

Nicholas Filippi | Product Management, Splunk Patrick Ogdin | Product Management, Splunk

September 2017 | Washington, DC

Welcome



splunk >

Patrick Ogdin

Product Management, Splunk

/oldlink?item

Responsible for Splunk Management
 & Deployment

//product.screen?product 1d=FL_DSH-01&JSESSIONID=S015LAFF10ADFf10ADff10AD

ISESSIONID=SD5SL9FF1ADFF3 HTTP 1.1



splunk'>

Nicholas Filippi

- Product Management, Splunk
- Responsible for Dashboards & Info Delivery



splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.



Drilldown Editor Event Annotations SearchBar Integration



Dashboard Drilldown (Default Behavior)

dunk> App: Bu	ittercup Ga	ım∨								Adr	ninistr	ator 🗸	Me	ssages		Setting	s∨	Activi	y~	Help	× (Find	_	_
arch Datasets	Report	ts	Alerts	; [Dashbo	ards																Bu	tterc	up Ga
verview																					Ed	lit	Expor	t 🕶 🛛
Overview - Numbo played all time	er of gam	es		0 pl	vervie layed	w - Nu today	umer o	of gan	nes			Overv	iew - J	Averaç	je Sco	ore			Over	rview	- Тор	Score		
67,	20)2					0	→ 0						9	.(5				6	6	i E	5.	0
# of gam	es - all tim	e				# 0	f game	s - tod	ay					avg	score						1	top sco	ire	
Leaderboard												Тор В	rowse	rs										
user.nickname 0				score	0			num	berOf	ames	0													
amaier37				1	7					1	0		_	Firef	ox iOS									
amrit					5						1		F	iretox I	Mobile Opera									
barnestim1										3	2				Edge	1	1							
birgit publikavi				2	8						0				Safari			cella 1						
brs077	•				5					4	7			F	irefox	1		7				Mobil	la Safa	4
bryanstun4				1	1					1	8		C	C Irome l	hrome Mobile	\sum		/				mooli	ie sarai	
emil V				1	4					13	0													
emma.yost					6						7													
abiolald					0						4													
					« pre	v 1	2	3	4	next »														
Play Times																								
	12AM	1AM	2AM	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	SPM	6PM	7PM	8PM	9PM	10PM	11PM
monday					•		•				•				•	•	•	•			•	•	•	
tuesday					•								•	•	•	•				•		•		
wednesday							•	•		•	•	•	•	•	•	•	•					•	•	
thursday		•		•		•			•							•		ŏ	ŏ	ŏ	•	•		•
friday			•	•			•				-				ó									
			-						-			ě	-		-	-	-				-			
c a turd au		-	-		-	•		1	-	-				-							-	•		
saturday				-			_				-	_	-	-	-		_							

Default drilldown to search uses the "intentions parser" to construct a best-effort search query

splunk'> App: Buttercup Gam		Administrator V Messages V Settings V Activity V Help V Find									
Search Datasets Reports A	lerts Dashboards	В	uttercup Games								
Q New Search			Save As ∽ Close								
index=buttercupgo eventName=ga	me_over "user.nic	kname"=amrit	All time 🗸 🔍								
→ 16 events (before 3/6/17 3:15:56.000 PM) No Event Sampling → Job → II 🔳 → 🙆 ±											
Events (16) Patterns Stat	istics Visualizat	tion									
Format Timeline ∨ — Zoom Out →	Zoom to Selection	t 20 Per Page V	1 month per column								
 Kida Fielda Eielda 	i Time	Event									
Selected Fields a bost 2 a source 1 a sourcetype 2 Interesting Fields a authenticated 1 a browsechidden 1 a browsechidden 1 a browsechidden 1 a browsechidten 1 browsechidten 1 brows	> 2/23/17 6:13:19.000 PM	<pre>{ [-] authenticated: true browser: { [-] browser: { [-] } client: { [-] } euentName: game_over game: { [+] user: { [+] version: v1.1-a7b5067-prod } Show as raw text host = demo-buttercupgo.splunkoxygen.com:8088 [source = http:buttercuppo [sourcetype = _ison</pre>									
# Drowserpoweratio 1 # browserpesh 2 # browserpesh 2 a browserpesh 2 a clientid 1 a clientid 1 a clientid 1 # game.flaps 15 a game.ld 16 # game.score 12 # game.score 13 # game.score	> 9/16/16 4:07:45:000 PM	<pre>{ [-] authentiated: true browser: { [*] } client: { [*] } eventName: game_over game: { [*] } user: { [*] yersion: v0.8-128259d-prod } Show as raw text host = http:houtercup-splunk.splunkcloud.com isource = http:buttercuppo isourcetype = http: </pre>	pevent								



Dashboard Drilldown (xml config)



/oldlink?item_id=EST-26&JSESSIONID=SDSSL9FFADF3 HTTP 1.1" 200 /oldlink?item_id=EST-26&JSESSIONID=SDSSL9FFADFF3 HTTP 1.1" 200 Optionally configure drilldown event to direct users to another dashboard, passing context in the form of token variables (XML only)



<drilldown> <link target="_blank">/app/buttercup_games/player?form.player=\$row.user.user_id\$</link> </drilldown>

1f2017

Drilldown Editor

build interactivity in your dashboard without learning XML

Objective:

- Promote more users to customize the drilldown experience
- Remove requirement to learn XML
- Default "Drill to Search" is often not the preferred behavior

Key Details

- Introduce new "Edit Drilldown" configuration dialog
- Supports common use cases
 - Link to search
 - Link to dashboard
 - Link to report
 - Link to custom URL
 - Manage tokens
- No change to Simple XML syntax
- Disable drilldown by default
 - *only affects newly created content

oduct.screen?product_id=FL-DSH-01&JSE /oldlink?item_id=FST-26&!SESSIONID=SD5

Drilldown Editor		×
On Click	Link to dashboard V	
App	No action	
	Link to search	
Dashboard	✓ Link to dashboard	
	Link to report	
	Upf Link to custom URL	
✓ Advanced Parameters	Manage tokens on this dashboard Enable in-page drilldown actions]×
	+ Add new	-
	Use parameters to set token values in the target dash For example, form.host = \$click.value2\$ or host = \$click.value2\$ Learn more 2	oard.
Preview URL	/app/search/cities	
Cancel		Apply
10n=v1ew&1tamId=€5T-6&p	splunk	°> .co



Demo

Drilldown Editor



Drilldown UI Editor – Surface Area

	Use Case
1	No action
2	Link to searchBoth default (uses intentions parser) and custom search string
3	Link to dashboardSame/different app context; pass tokens to target dashboard
4	Link to report Same/different app context
5	Link to custom URL Pass tokens to target URL
6	In-page interactivity (via token management) Set/Unset/Eval tokens on the page
7	Conditional field drilldown
8	Multiple Actions
10:57:1531 "C-	suns shopping.com/cart.do?action=view&itemid=Est-5&progues



Drilldown UI Editor – Surface Area (XML Only)

	Use Case
7	Conditional field drilldown
8	Multiple Actions

Date

+ At

ge ma

Advanced drilldown is not supported in drilldown editor. You can edit dashboard XML source code directly.

Cancel

Apply

luct.screen?product_id=FL-DSH-01&JSESS dlink?item_id=EST-26&JSESSIONID=SD5SL



Event Annotations

Add context to time-series charts by correlating against discreet events

Key use cases

- Correlate app performance metrics with code check-in events
- Overlay public/campaign events with application health

Feature details

- Supports time-series charts (line, area, column)
- Driven by a secondary search (event-driven)
- Custom Viz will need to integrate
- Optionally include categories and labels





Event Annotations

Add context to data by correlating discreet events against time-series charts

- Dashboard XML only
- Driven by a secondary search
 - <search type="annotation">
 - If <earliest> and <latest> are not specified, then it will use the primary search
- Supported fields in search results
 - <u>time</u> required field to overlay on a time-series chart
 - annotation_label optional field for display in the tooltip
 - annotation_category optional field to differentiate types of annotations, by color
 - annotation_color optional field to override color *(recommended to use charting categoryColors instead)
- XML charting options
 - charting.annotation.categoryColors Override color palette for annotation categories





Dashboard Search Bar

Improved search editing experience on dashboards

- Integrated SearchBar Component within Dashboards
 - Add Panel & Edit Search Workflows
- Improved Productivity & Consistency
- Leverage Functionality
 - Syntax Highlighting
 - Keyboard Shortcuts
 - Compact Search Assistant

Edit Search		×						
Title								
Search String	<pre>((index="main") (sourcetype="products_download")) fields "activity", "Platform", "salesforce_id", "version", " raw", "_time" fields - "_raw" eval Date=strftime('_time', "%m/%e/%Y") rename "activity" AS "Products" replace "Download" with "Enterprise" in "Products" lookup "sfdc" "salesforce_id" OUTPUT "AccountName" fields - "salesforce_id" dedup "AccountName" "Platform" "version"</pre>							
Time Range	Run Searcl stats count Command History stats count by action, host Command History stats count by host Command History stats count by src_ip,dest_ip,dest_port Command History stats first(resident_on) as resident_on Command History							
Auto Refresh Delay? Refresh Indicator	stats Learn More I2 Provides statistics, grouped optionally by field. Example: sourcetype=access_combined top limit=100 referer_domain stats							
Cancel	sum(count)	Apply						





Visualizations

Trellis Layout Result Truncation Actions for Reports



Trellis Layout

New visualization platform capability

- Introduced Splunk 6.6
- Series of similar visualizations to facilitate comparison across multiple dimensions
- Uses single query to drive many visualization
- Can be used in Search, Reports, and Dashboards



splunk>

.conf2017

Before & After

unk> App: Distributed Management Console ~					Administ	trator ~	🔛 Messages 🗸 🛛 S	iettings 🗸 🛛 Activity	rv Helpv 🎚	nd .
										gement Cons
PETVIEW Distributed Management Console monitors important de: distributed change	t aspects of your Splunk E	nterprise deployment.	Learn More 12							
5 Indexers In 5 Machines		6 Searc	h Heads			R	1 Cluste on 1 Machine	r Master		ţţţ
INDEXING RATE			CONCURI	IENT SEARCH	ES			51	ATUS	
9.49 MB/s 2.	37 MB/s	,	9 OTAL		2 AVERAGE		4 PEERS SEARCHABLE	4 INDEXES SEARCHABLE	6124 BUCKET CORIES	8.03 GB RANDATA SIZE
RESOURCE USAGE			RESO	URCE USAGE				BERGUI	INF LIRADE	
CPU	2.73 %		CPU		0.27%			081		17.5
Memory	0.64 %	Me	mory		0.28%			unu		
							Me	mory	6	45 %
1 License Master		1 Deploy on 1 Machine	yment Ser	ver		٩f	2 KV Sto on 2 Machine	ores		
SLAVES WITH WARNINGS			DEP	LOYMENT				U	SAGE	
0			1		0		N	/A		0
LICENSE USAGE					1012					
Today	465.08 / 875		RESO	URCE USAGE				RESOUR	ICE USAGE	
	GB		CPU		0.12%			CPU	0.	35 %
RESOURCE USAGE		Me	mory		0.34 %		Me	mory	0	15%
Chu	0178									
650	0.17 8									
Memory	0.45 %									
59 Alerts Enable or Disable Manage triggered alerts	Filter by Last: 24 Hours 🗸									A
Alert Name 0	Instance 0	Tim	e Triggered 0	Descriptio	in 0					
MC Alert - Saturated Event-Processing Queues	svdev-fedora14-05-p	eer-2 Nov	20, 2014 12:53 PM	One or mo	ore of your indexe	r queues is r	reporting a fill percentag	pe, averaged over the	last 15 minutes, of 9	2% or more.
MC Alert - Critical System Physical Memory Usage	svdev-fedora14-06-p	eer-3 Nov	20, 2014 12:33 PM	One or mo	ore instances has	exceeded 90	0% memory usage.			
MC Alert - Search Peer Not Responding	10.140.126.128.808	Nov	20, 2014 12:23 PM	One or mo	ore of your search	peers is cur	mently down.			
MC Alert - Critical System Physical Memory Usage	svdev-sh-demo svdev-fedora14-02-s	Nov earch-head-1	20, 2014 11:43 AM	One or mo	ore instances has	exceeded 90	0% memory usage.			
MC Alart - Saturated Event-Discussion Overas	surface/articla 14.05.0	eer.7 Nov		0.000	and a standard in data	e en en en in e	monting a fill persentar	a surround over the	last 15 minutes of 0	The normania
and refer containing french independing dagage	910011 10001014 00 p	661 E 1604	20,2014 11:43 AM	One of the	re oi your moexe	i dhenes is i	reporting a milipercentary	the averaged over the	and the summer of the latest	and the second second

uct.screen?product_id=FL-DSH-01&JSE dlink?item_id=EST-26&ISESSIONID=SD5



Benefits

- Alternative is to use series of similar queries, which causes unnecessary load on the system
- Single visualization might hide relevant outliers by over-aggregating values
- Since values often change over time, Trellis Layout can dynamically show all values that are present in the selected time range



Trellis Layout Usage

splunk > App: Search & Reporting] ∼		Administrator 🗸	$1 Messages \checkmark Settings \checkmark Activity \checkmark$	Help ✓ Find
Search Datasets Reports	Alerts Dashboards				Search & Reporting
Q New Search					Save As → New Table Close
<pre>index="energy" where (MSN="TEPRB" or MSN= eval data_total = if(MSN== eval data_renewable = if(M timechart span=1y latest(d)</pre>	"REPRB") and StateCode !="US" "TEPRB", Data, null) SN=="REPRB", Data, null) ata_total) latest(data_renewable)	by StateCode useother=false limit	t=55		All time ~ Q
✓ 4,680 events (before 4/5/17 3:35:21.0	000 PM) No Event Sampling 🗸			Job ∽ 🛛 🔳	→ ♣ 业
Events (4,680) Patterns	Statistics (45) Visualization				
	llis				
AK	AL	AR	AZ	CA	СО
5,000,000	2,000,000	2,000,000	1,000,000	5,000,000	5,000,000
CT	DC	DE	FL	GA	HI
250,000	2,500	10,000	500,000	500,000	25,000
IA	ID	μ	IN	KS	КҮ
500,000	200,000	2,500,000	1,000,000	1,000,000	5,000,000
1970 1986 2002	1970 1986 2002	1970 1986 2002	1970 1986 2002	1970 1986 2002	1970 1986 2002



di10:57/category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 322 "http://buttercup-shopping.com/category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 312 "http://buttercup-shopping.com/category_id=GIFTS&GISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 312 "http://buttercup-shopping.com/category_id=GIFTS&GISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 312 "http://buttercup-shopping.com/category_id=GIFTS&GISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 312 "GIFTS&GISESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 312 "GIFTS&GISESTIONID=SDISL4FF10ADFF10 HTTP 1.1" 405 312 "GIFTS&GISESTIONID=SDISL4F



Demo

Trellis Layout



Result Truncation

Problem

- jschart limits set low to avoid performance problems in browsers due to large result sets in charts
- Limits were not configurable

Solution

- Using combination of settings in web.conf
 - jschart_truncation_limit
 - jschart_series_limit
 - jschart_results_limit
- Customer/browser defined limits
- CAUTION: Browser Crashing Ahead

Bonus: Updated Charting Libraries



Actions For Reports

- Follow-on to Custom Alert Actions from Splunk 6.3
- Installed and enabled Alert Actions are now available to users for Alerts AND Reports
- Solves the "always alert" problem

Edit Schedule			2	×
	Report	Application Performance		
Sche	dule Report	Learn More L		
	Schedule	Run every week 🗸		
		On Monday ~ at 6:00 ~	~	
-	Time Range	Last 24 hours >		
Schedu	ule Priority?	Default 🗸		
Schedu	le Window?	No window 🗸		
Trig	ger Actions			
		+ Add Actions ~		
	E Log Eve Send log	nt event to Splunk receiver endpoint		
	Output th	results to lookup e results of the search to a CSV lookup file	Cancel Sav	/e
	Run a s Invoke a	cript custom script		
	Send en Send an	nail email notification to specified recipients		
on Privacy Policy	Beneric H	k ITTP POST to a specified URL		
	Manage Act Manage availa	ions 🖸 ble actions and browse more actions		

splunk>

.conf2017

Thank You

Don't forget to rate this session in the .conf2017 mobile app



Appendix A: Drilldown Editor



Drilldown UI Editor – Surface Area

		Use Case
	1	No action
	2	 Link to search Both default (uses intentions parser) and custom search string
	3	 Link to dashboard Same/different app context; pass tokens to target dashboard
	4	Link to report Same/different app context
	5	Link to custom URL Pass tokens to target URL
	6	In-page interactivity (via token management) Set/Unset/Eval tokens on the page
	7	Conditional field drilldown
	8	Multiple Actions
18:10	9:57.1.	Solunk

Creen?product id=FL-DSH-01&JSESSIONID



Supported via UI Editor

Drilldown UI Editor – Surface Area (XML Only)

	Use Case
7	Conditional field drilldown
8	Multiple Actions



screen?product id=FL-DSH-01&JSESSIONID=SD3



splunk>

.conf2017

Conditional Field Drilldown (XML Only)

Search	ı stri	ing	index=_i chart addtot sort ·	interi coun tals -ERRO	nal (t <mark>ove</mark> R	log_ r so	leve] urcet	l=* log_level!="W/ type <mark>by</mark> log_level	ARNING")			
	Lo	og Event	s by Sourc	etype								
		sourcety	pe 🌣					ERROR ¢	INFO 0	WARN 🌣		Total 0
	1	splunkd						18	420955	1520		422493
	2	splunk_v	veb_service					1	510	0		511
	3	schedule	er.					0	8341	0		8341
	4	splunkd_	conf					0	2	0		2
				Search	Datasets	Reports	Alerts	Dashboards		Search & Re	porting	



/product.screen?product id=FL-DSH-01&JSESSIONIL

Search string	<pre>index=_internal (log_leve chart count over source addtotals sort -ERROR</pre>	l=* log_level!="WARNING type <mark>by</mark> log_level	i")		H C	appy ase!
Log E	Events by Sourcetype					
SOL	urcetype 🗘	ERROR \$	INFO \$	WARN \$	Total 0	
1 spl	lunkd	18	420955	1520	422493	
2 spl	lunk_web_service	5	510	0	511	
3 sch	heduler	0	8341	0	8341	
4 spl	lunkd_conf	Search Datasets	Reports Alerts Dashboards	^	<u> </u>	Search & Reporting
		Log Event De	etails Hide Filters			Edit Export V
		Sourcetype	Log Level	Q v		
If user clicks	on "18".					
th dashboard ar log_level="EF	nen direct user to "Log Events De nd pass sourcetype='splunkd' & RROR"	Log Event Trend				
4		<u><u></u>8 10</u>	7:00 AM	8:00 AM	9:00 AM	10:00 AM
<pre><drilldown></drilldown></pre>	>		Tuo Mor 7			4

<link target="_blank">/app/search/log_event_details?form.sourcetype=\$row.sourcetype\$&form.log_level=\$click.name2\$</link>
</drilldown>

anseg 5. Com/oil 28.17 1 a sector removes tended est interior as a sector removes a sector removes tended est interior as a se

Search	n string	index=_int chart co addtotal sort -EF	ternal (log_level ount over sourcet Ls RROR	=* log_level!="WA ype <mark>by</mark> log_level	RNING")		Ec	lge Case
	Log Ev	vents by Sourcety	pe					
	sour	rcetype 🌣		ERROR 0	INFO 🌣	WARN 0	Total 0	
	1 splu	nkd		18	420955	1520	422493	
	2 splu	nk_web_serve		1	510	0	5	
	3 sche	eduler		0	8341	0	8341	
	4 splu	nkd_conf		0	2	0	2	

Current Behavior

If user clicks on "splunkd", then direct to "Log Event Details" and pass sourcetype='splunkd' & log_level='sourcetype' If user clicks on "422493", then direct to "Log Event Details" and pass sourcetype='splunkd' & log_level='Total'



Log Events by Sourcetypesourcetype \$ERROR \$INFO \$WARN \$Total \$splunkdsplunk_web_servee15100510	Case	Edge		RNING")	l=* log_level!="WA ype <mark>by</mark> log_level:	ternal (log_level punt over sourcet ls RROR	index=_inf chart co addtotal sort -EF	tring	earch s	Sea
sourcetype \$\2222Sourcetype \$\22222ERROR \$\22222INFO \$\222222WARN \$\222222Total \$\2222221splunkd1842095515204224932splunk_web_serve151001						/pe	nts by Sourcety	Log Eve		
1 splunkd 18 420955 1520 422493 2 splunk_web_servee 1 510 0 511		Total 0	WARN 🌣	INFO 0	ERROR 0		etype 0	source		
2 splunk_web_serve 1 510 0		422493	 1520	420955	18		d	1 splunk		
		5	0	510	1	-	_web_service	2 splunk		
3 scheduler 0 8341 0 8341		8341	0	8341	0		uler	3 schedu		
4 splunkd_conf 0 2 0 2		2	0	2	0		d_conf	4 splunk		

Desired Behavior

If user clicks on "splunkd", then direct to "Log Event Details" and pass sourcetype='splunkd' & log_level='*' If user clicks on "422493", then direct to "Log Event Details" and pass sourcetype='splunkd' & log_level='*'



Log Eve	<pre>index=_internal (log_leve chart count over source addtotals sort -ERROR</pre>	el=* log_level!="WARNI etype <mark>by</mark> log_level	NG")) So	lutio
sourc	etype 🗘	ERROR \$	INFO 0	WARN 0	Total 🗘	
			100055	1 500	400.400	
1 spluni	d	18	420955	1520	422493	
1 splun 2 splun	c_web_serve	18	420955	0	422493	
1splunl2splunl3sched	c_web_service uler	18 1 0	420955 510 8341	0	8341	

<drilldown>

<condition field="sourcetype">

luct.screen?product_id=FL-DSH-01&JS

<link target="_blank">/app/search/test_bug?form.sourcetype=\$row.sourcetype\$&form.log_level=*</link>
</condition>

<condition field="Total">

<link target="_blank">/app/search/test_bug?form.sourcetype=\$row.sourcetype\$&form.log_level=*</link>
</condition>

<condition>

<link target="_blank">/app/search/test_bug?form.sourcetype=\$row.sourcetype\$&form.log_level=\$click.name2\$</link>
</condition>

Multiple Actions (XML Only)

Purchase History	
Customer 🗘	Amount 🌣
Susan Smith - ID:12345	\$400
John Stand - ID:67890	\$300

Desired Behavior

If user clicks on "Susan Smith – ID:12345" then direct to "Customer Details" dashboard and pass ID='12345' (effectively, extract the ID from the customer field, and use that token)



Multiple Actions (XML Only)

Amount 0	
\$400	
\$300	
	Amount \$400 \$300



luct.screen?product_id=FL-DSH-01&JSESSIONID=SD3



Appendix B: Event Annotations



How To Configure Event Annotations?

Dashboard XML only

Driven by a secondary search

- <search type="annotation">
- If <earliest> and <latest> are not specified, then it will use the primary search

Supported fields in search results

- _time required field to overlay on a time-series chart
- annotation_label optional field for display in the tooltip
- annotation_category optional field to differentiate types of annotations, by color
- annotation_color optional field to override color *(recommended to use charting categoryColors instead)

XML charting options

• charting.annotation.categoryColors – Override color palette for annotation categories



Scenario #1: Basic Overlay w/ Event Annotations

Correlate Search Workload with User Logins *Example:* Correlate search workload with user activity. Set 100 login by admin label to include the login username. 75 count 50 <chart> <title>Correlate Search Workload with User Logins</title> 25 <!-- Base search that drives the visualization --><search> <query>index= audit action=search result count="*" | timechart count</g 12:00 PM 12:00 AM 6:00 PM 6:00 AM <earliest>-24h@h</earliest> Thu Aug 10 Fri Aug 11 <latest>now</latest> 2017 </search> time <!-- Secondary search that drives the annotations --> <search type="annotation"> <query>index= audit action="login attempt" | eval annotation label = "login by " . user</query> <earliest>-24h@h</earliest> <latest>now</latest> </search> <option name="charting.chart">line</option> <option name="charting.drilldown">none</option> <option name="charting.legend.placement">none</option> <option name="charting.lineWidth">1</option> </chart>

Screen?product id=FL-DSM-01&J

Scenario #2: Multiple Categories of Event Annotations

Example: Correlate search run time with various warning and error log events. Use category to differentiate log level, and label to display the log message.

```
avgRunTime
^
<chart>
  <title>Average Search Run Time with WARN/ERROR event annotations</title>
   <!-- Base search that drives the visualization -->
   <search>
      <query>index= audit action=search result count="*" | timechart avg(total ru
avgRunTime</guery>
      <earliest>-24h@h</earliest>
                                                                                                                        12:00 AM
                                                                                             12:00 PM
                                                                                                          6:00 PM
                                                                                                                                     6:00 AM
      <latest>now</latest>
                                                                                             Thu Aug 10
                                                                                                                       Fri Aug 11
   </search>
                                                                                             2017
                                                                                                                   time
  <!-- Secondary search that drives the annotations -->
  <search type="annotation">
      <query>index= internal (log level="WARN" OR log level="ERROR") | eval annotation label = message| eval
annotation category = log level</query>
      <earliest>-24h@h</earliest>
      <latest>now</latest>
   </search>
  <!-- Customize the event annotation colors based on category name -->
  <option name="charting.annotation.categoryColors">{"ERROR":"0xff3300","WARN":"0xffcc00"}</option>
  <option name="charting.chart">line</option>
  <option name="charting.drilldown">none</option>
  <option name="charting.legend.placement">none</option>
  <option name="charting.lineWidth">1</option>
                                                                                                                     splunk
  <option name="charting.seriesColors">[0x339933]</option>
</chart>
```

Average Search Run Time with WARN/ERROR event annotations

WARN

Spent 12561ms reaping search processes

Aug 10, 2017 6:43:23.180 PM

"Cas "Seis "M/nin, VC "n. 43.17 14 sec. "CM_10=EST.26&JSESSIUNIU=DUDJE." Cas creen(54) Tree:1891 "Cas 55:10/1., "GET (51) Sec.1081 "Cas creen(54) "Cas creen(54

Important Details

- Currently, integrated with dashboard XML only
- Does not yet support "user" annotations
 - Search-driven annotations only

duct.screen?product_id=FL-DSH-01&JSESS

- Supports discreet events
 - Does not support "duration" event (ex. maintenance windows, etc)

Performance

Does run an additional search on dashboard load time

Result limit of 1000





End End



Thank You

Don't forget to rate this session in the .conf2017 mobile app

