



splunk>

How Splunk Cloud Monitors Splunk Cloud with 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. © 2018 Splunk Inc. All rights reserved.

Our Speakers



ERIK CAMBRA

**Product Manager, Splunk
Cloud, Splunk**



RUSSELL UMAN

**Principal Nephelococcygist,
Cloud Monitoring, Splunk**



The Splunks We Splunk Splunk With

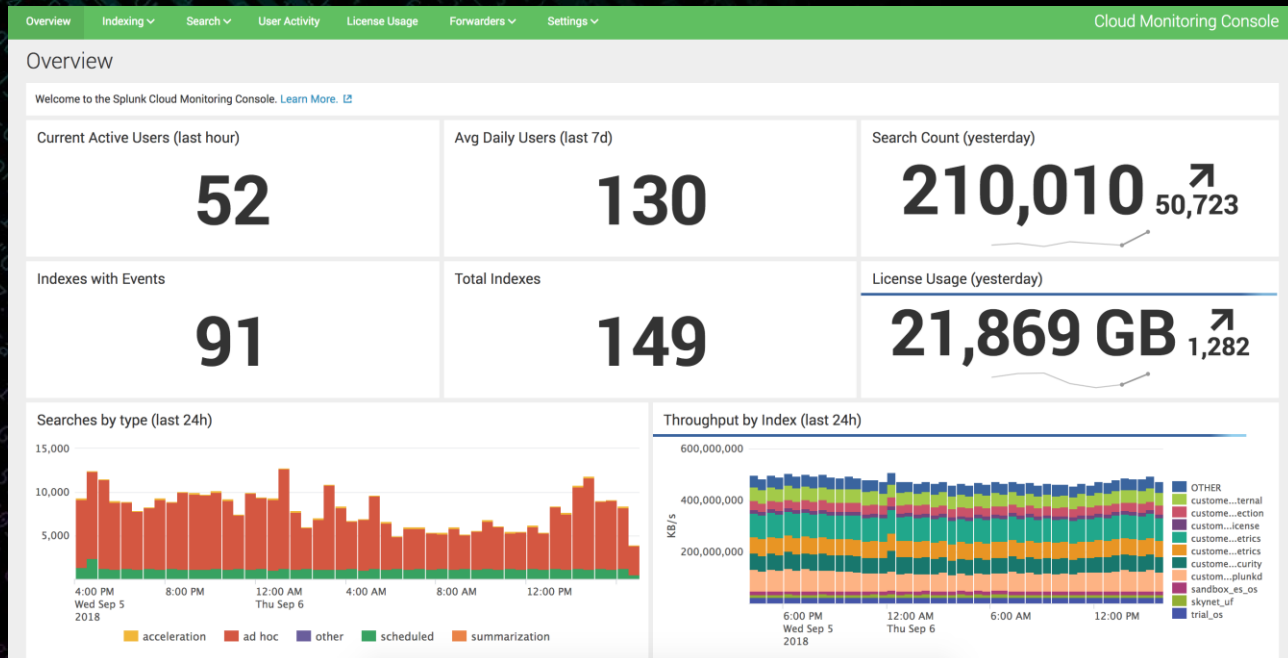
Not suitable for children under 3 years due to small parts.



My friends call me McCloud.

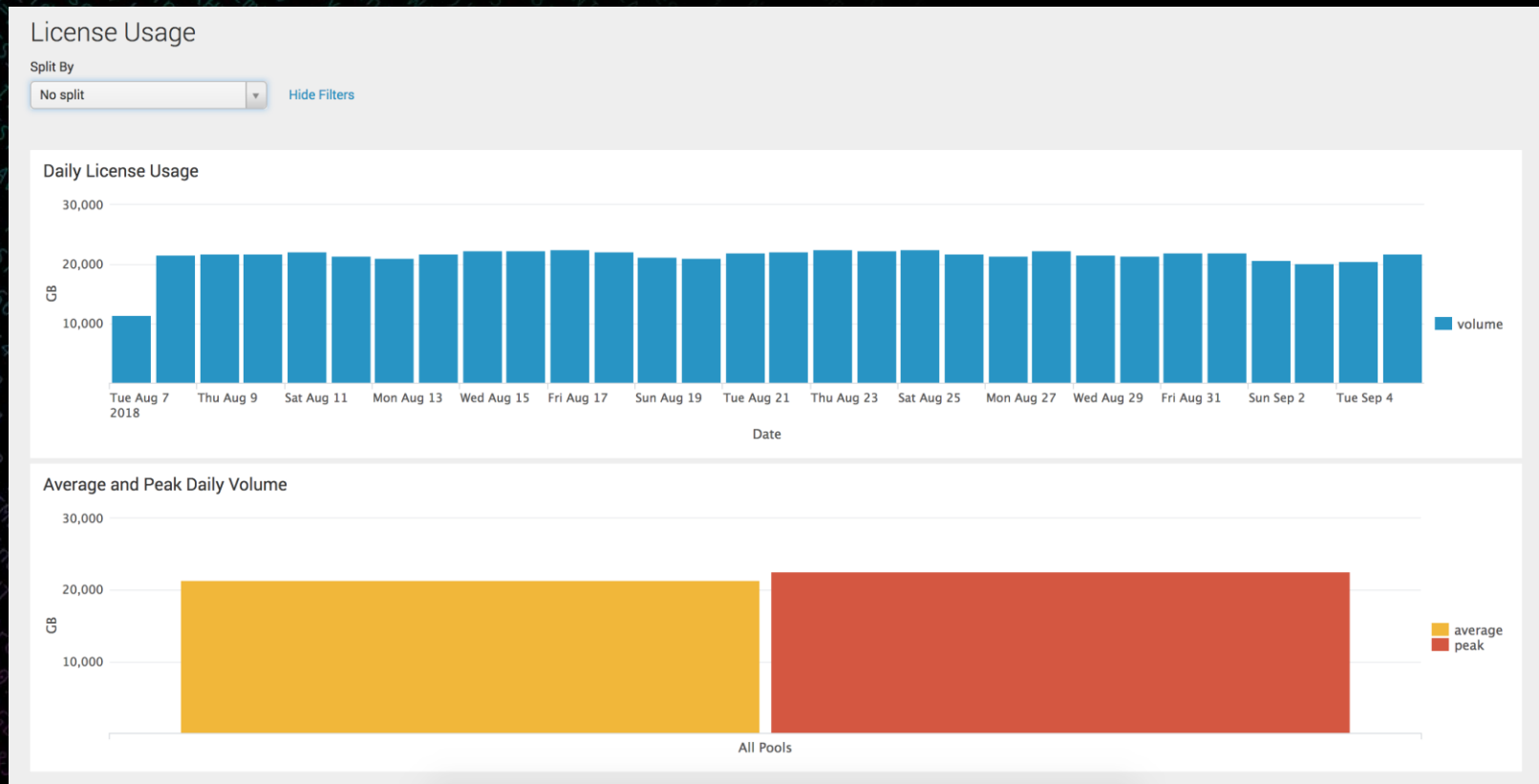
Things you can do with the CMC

- ▶ Review Daily Data Ingest
- ▶ Audit Data Storage by Index
- ▶ Understand Usage Patterns
- ▶ Troubleshoot Data Ingest
- ▶ Investigate Search Issues



Data Ingest

Do you know how much data you're sending?



Data Storage

How much data are you retaining?

Indexes and Storage

91

Indexes with Events

149

Total Configured Indexes

4884.63 TB

Total Index Size

13,967,525,088,750

Total Event Count

Indexes (91)

index	Index Size (GB)	Total Event Count	Total Bucket Count	Earliest Event	Latest Event	Retention
access_control	0.04	73018	12	2018-08-03 19:25:25	2018-09-06 16:02:15	456 Days
apps	3.61	902784	19	2018-06-18 11:21:08	2018-09-06 13:56:48	456 Days
automation_services	0.01	1016	46	2017-12-13 21:44:29	2018-09-05 17:53:16	456 Days
aws-cloudtrail	1609.79	1205872002	502	2016-03-29 19:18:34	2018-09-06 16:52:10	1095 Days
aws-cloudtrail-dev	24.30	18553043	63	2018-05-04 08:27:03	2018-09-06 16:55:07	120 Days
aws-cloudtrail-qa	7.13	6246362	30	2018-05-11 11:43:02	2018-09-06 16:52:03	90 Days
aws-cloudtrail-stg	168.99	143135230	309	2017-08-15 05:50:48	2018-09-06 16:57:51	365 Days
aws-config	169.08	18128254	1044	2015-11-03 23:46:06	2018-09-06 16:31:14	1095 Days
aws-others	1.45	1673379	90	2018-03-28 21:14:31	2018-09-06 16:39:42	150 Days
aws-vpcflow	44.61	420891886	292	2016-07-17 08:08:36	2018-09-06 16:51:57	300 Days

[« prev](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next »](#)

- **Index Usage (GB):** The amount of raw data stored for the index in GB
- **Total Event Count:** The total number of events currently stored for the index.
- **Total Bucket Count:** The total number of buckets currently stored for the index.

Search Usage Statistics

Instances: All Time Range: Last 4 hours Only Ad Hoc Searches: ☒ Yes ☐ No

[Hide Filters](#)

Search Activity by User (75)

User	Search Count	Search Head Count	Median Runtime	Cumulative Runtime	Last Search
jcutler	4656	2	0.51s	1h 25min 6.80s	09/06/2018 16:58:21 +0000
swatanabe	2455	2	0.56s	1h 5min 46.82s	09/06/2018 16:59:16 +0000
fcaneet	2335	2	0.58s	1h 8min 45.51s	09/06/2018 17:01:21 +0000
dpham	1248	2	2.49s	48min 36.62s	09/06/2018 17:02:09 +0000
internal_monitoring	1227	16	1.53s	2h 14min 35.34s	09/06/2018 17:01:55 +0000
rmorgan	772	1	1.97s	2h 3min 20.66s	09/06/2018 17:02:06 +0000
dtoledo	449	2	0.92s	11min 52.29s	09/06/2018 16:58:47 +0000
splunk-system-user	363	15	0.67s	22min 53.93s	09/06/2018 17:02:06 +0000
dcarmack	337	1	4.22s	1h 27min 34.48s	09/06/2018 17:02:09 +0000
tnerpel	288	1	0.68s	3min 10.11s	09/06/2018 17:00:50 +0000

[prev](#) 1 2 3 4 5 6 7 8 [next](#)[Click to see a list of search head names and a list of search strings.](#)

Skipped Scheduled Searches

Assess whether your scheduled searches are running as expected, quantify the fraction of your search workload that is being skipped or delayed, and find pointers for taking corrective action. [Learn More.](#)

Time Range: Last 24 hours Include Acceleration Searches: ☒ yes ☐ no

[Hide Filters](#)

Total Skipped Searches

523

Scheduled Search Skip Ratio

1.94 %

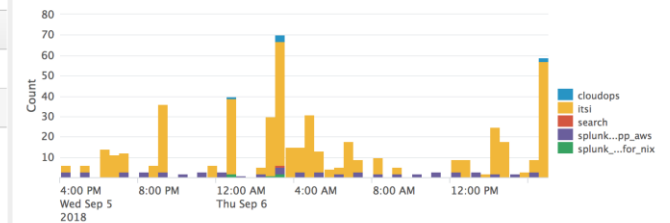
Count of Skipped Scheduled Searches

Group by: Reason

Reason	Count	Percent of Total
The maximum number of concurrent running jobs for this historical scheduled search on this instance has been reached	496	94.84 %
The maximum number of concurrent running jobs for this historical scheduled search on this cluster has been reached	27	5.16 %

Count of Skipped Searches Over Time

Group by: App

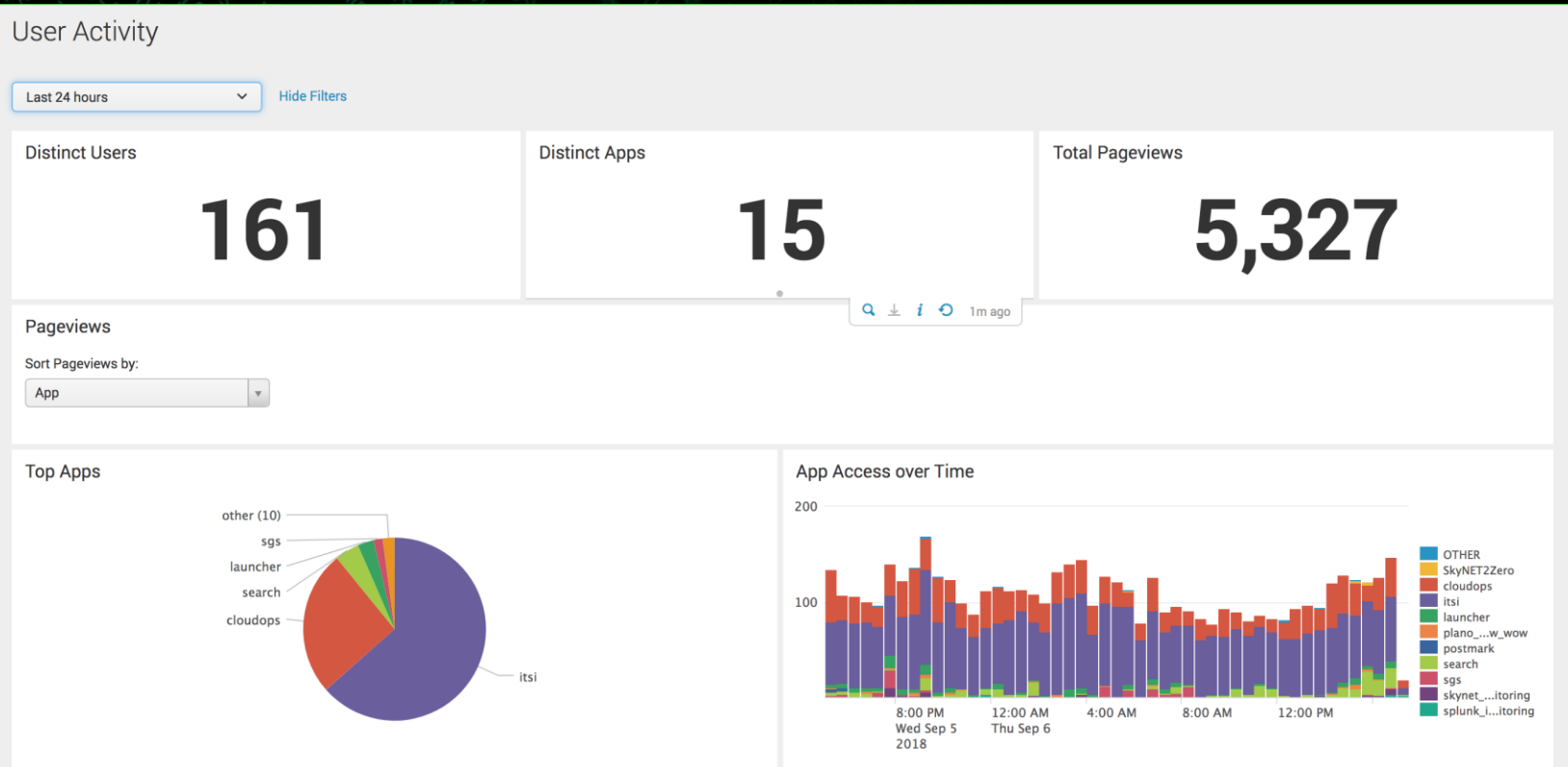


Understanding Search Performance

How many searches am I running and can they be improved?

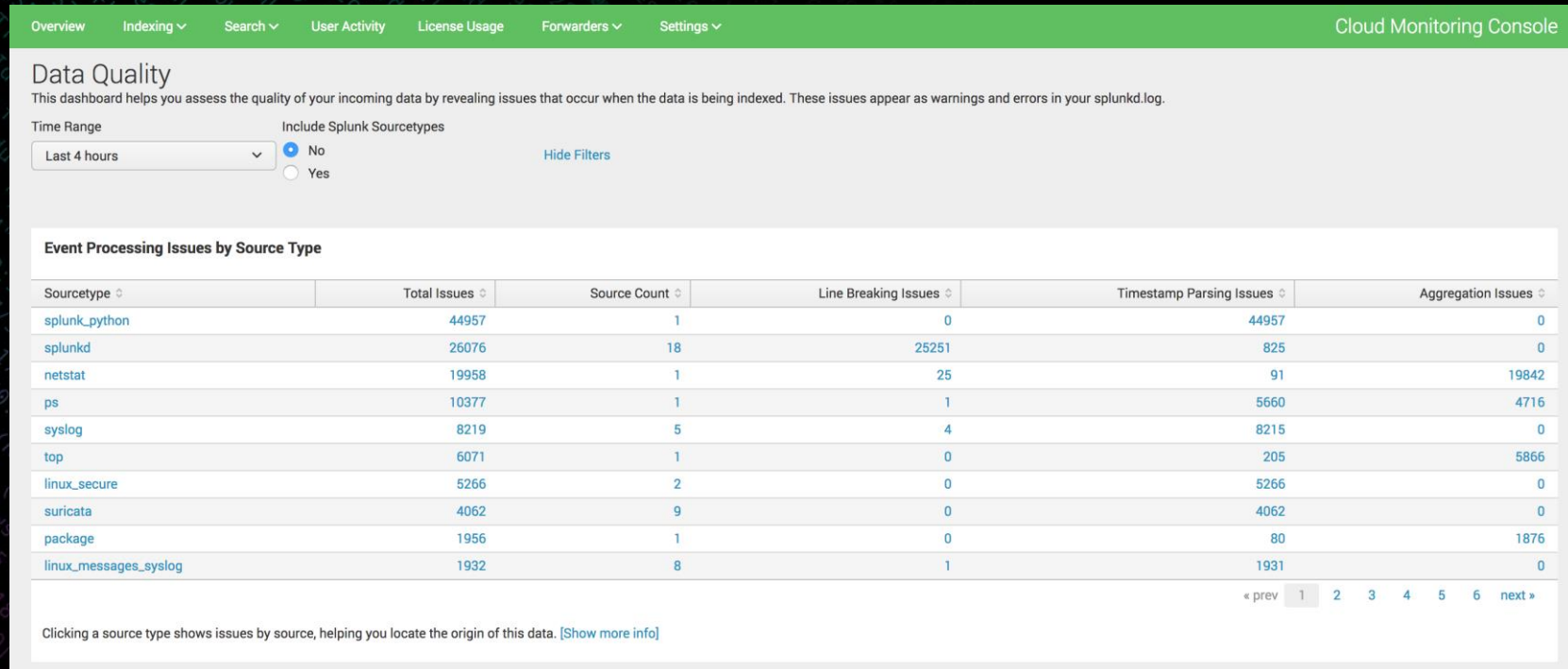
Usage Review

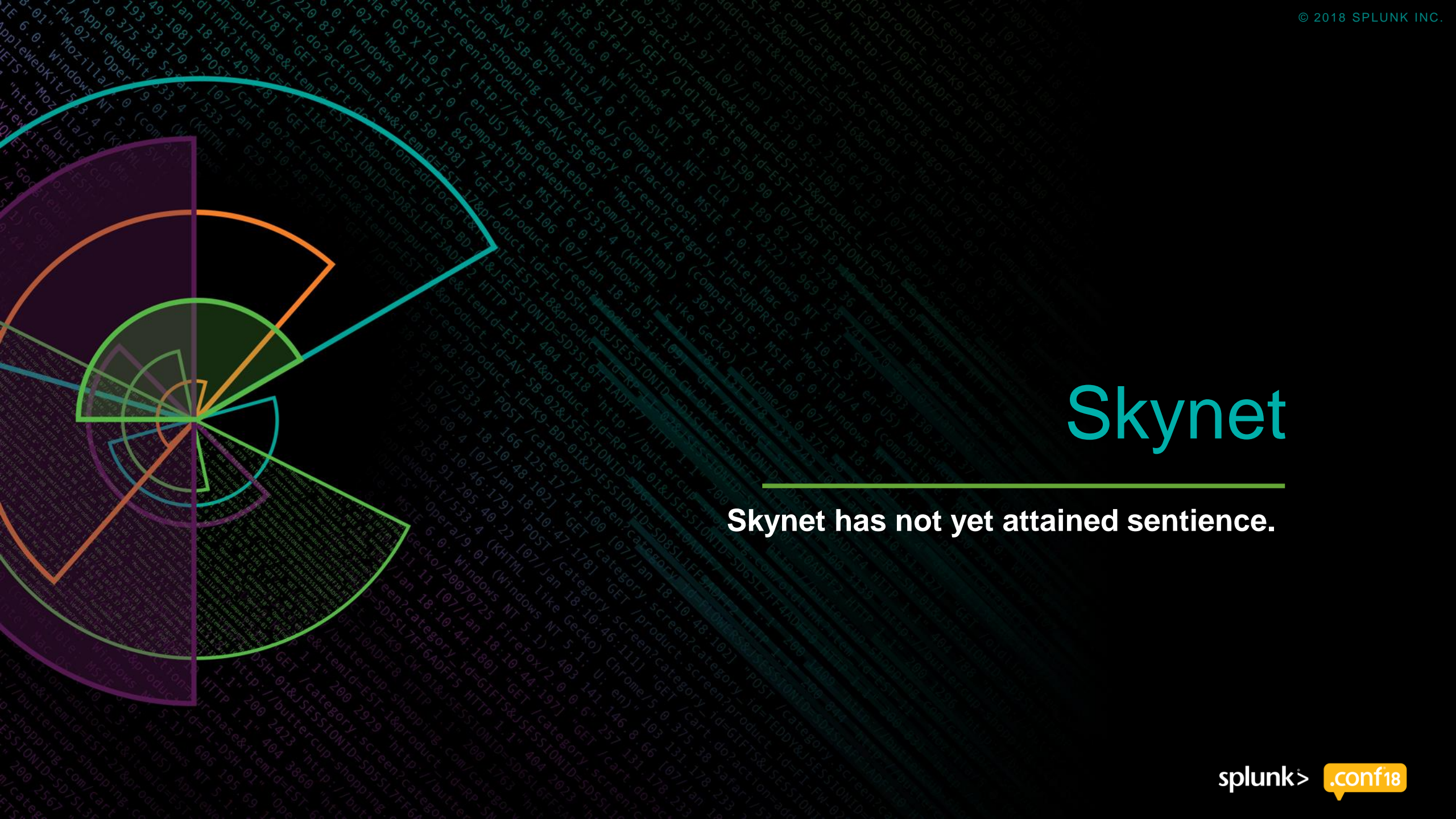
How are your users gaining value from Splunk Cloud?



Troublesome Data

Do your configs match your logs?





Skynet

Skynet has not yet attained sentence.

Skynet Architecture

- ▶ Multiple Cloud Stacks
- ▶ Regional stacks that collect data from Skynet forwarder on customer instances
- ▶ Infrastructure stack that collects data from Skynet forwarder on infra instances, and 3rd-party systems (e.g. AWS)
- ▶ Search stack that distributes over all the other stacks.
- ▶ Additional stacks for Single-Instance customers and next-generation Cloud



Skynet Architecture

- ▶ The first attempt at Skynet put everything into `_internal`. This did not work.
- ▶ The second attempt at Skynet had a separate index for each customer. This did not work!
- ▶ The current iteration has a separate index for each large source (splunkd, metrics, license, etc.)



Skynet Inventory

- ▶ Inventory lookup lets us know who we should expect to receive data from.
- ▶ One row per host, for all the ec2 instances across all Splunk Cloud AWS accounts.
- ▶ Generated from AWS TA Description inputs.
- ▶ Enriched with fields (alertable, bucket_location, cloud_flavor) based on ec2 tags.
- ▶ Inventory lookup built from a scheduled search, with counter-measures against failures to collect Description events.

[aws_inventory_lookup]

```

index=aws_description source=*:ec2_instances
| fillnull value="null" alertable aws_account_shortcode bucket_location customer_type tags.Role
tags.Stack vpc_id tags.CloudworksEnv
| stats count by alertable account_id aws_account_shortcode aws_account_name bucket_location id
instance_type ip_address launch_time private_ip_address region vpc_id tags.CloudworksEnv state
customer_type FQDN tags.Name tags.Role tags.Stack
| fields - count
| rename account_id AS aws_account_id, aws_account_shortcode AS aws_account, tags.Name AS name,
tags.Stack AS stack, tags.Role AS role, tags.CloudworksEnv AS cloudworksenv
| eval owner="CloudOps"
| eval new_event = 1
| inputlookup append=t aws_inventory
| eval old_event=if(isnull(new_event), 1, null())
| eventstats count(old_event) as old_count, count(new_event) AS new_count
| fillnull value="0" new_count old_count
| eval change_multiplier = if(old_count > 0, new_count / old_count, 1)
| where (change_multiplier >= .9 AND new_event = 1) OR (change_multiplier < .9 AND old_event = 1)
| fields - change_multiplier new_count new_event old_count old_event

```

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Opera/9.80 (Win
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&SESSIONID=5D1SL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0 (Compaq i486)
ows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SL8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FI-SW-03" "Opera/9.80 (Win
item_id=EST-16&product_id=RP-LI-02)" 468 125.17 14 189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0 (Compaq i486)
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0 (Compaq i486)"

Cloud Monitoring Alerts

splunk>

App: SkyNET Customer Monitoring

Messages

Settings

Activity

Find

Default

Indexers

Infrastructure

Other

Search

Customer SLA

Russell Uman

Support & Services

SkyNET Customer Monitoring

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

52 Alerts

AllYoursThis App'sfilter

i	Title ^	Actions	Owner	App	Sharing	Status
>	alert_blocked_index_clusters	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_bloomHomePath_set	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_buckets_s2_failed_registration	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_buckets_s2_failures_bucket_download	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_buckets_s2_failures_bucket_upload	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_cloud-administration_failed_login	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_custom_sg_missing	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_customer_stack_io_issues	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_dirty_indexer_restart	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_ebs_missing_expected_snapshots_cloudworks	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_ebs_missing_expected_snapshots_stackmakr	Open in Search Edit	nobody	skynet_customer_monit...	App	Disabled
>	alert_ebs_missing_last_snapshot_cloudworks	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_ebs_missing_last_snapshot_stackmakr	Open in Search Edit	nobody	skynet_customer_monit...	App	Disabled
>	alert_indexers_datasources_ossec	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_indexers_datasources_skynetuf	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_inventory_duplicate_fqdn	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_inventory_missing_customer_type	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_lighthouse_saml_error	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_maxDataSize_incorrect	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_mom_frozen_buckets	Open in Search Edit	nobody	skynet_customer_monit...	App	Disabled
>	alert_mom_low_inventory	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_oom_too_many_restarts_critical	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_oom_too_many_restarts_warning	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_oom_without_restart	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_pass4symmkey_mismatches	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_puppetmaster_bad_eyaml_decrypt	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_puppetmaster_data_outage	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_puppetmaster_monitor_ports	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_rainmakr_beluga_rollbacks	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_rainmakr_cartographer_not_polling_sqs	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_rainmakr_infrastructure_disk_space	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled
>	alert_rainmakr_infrastructure_missing_data	Open in Search Edit	nobody	skynet_customer_monit...	App	Enabled

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10
128.241.220.02 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD1SLAFF10
" 317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1AD
ows NT 5.1: SV1: .NET CLR 1.1.4322" 468 125.17 14.10.10.10
itemId=EST-16&product_id=RP-LI-02" "0
toaction=purchase&is.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1AD
opping.com/purchase&is.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1AD
02.2018.01.07 18:10:57.153

Cloud Monitoring Alerts IO issues

splunk> App: SkyNET Customer Monitoring Messages Settings Activity Find

Default Indexers Infrastructure Other Search Customer SLA

alert_customer_stack_io_issues Save Save As View Close

```
index=customer_quux sourcetype=linux_messages_syslog "blk_update_request" "I/O error" NOT alerttable=0
| timechart span=1m count by host
| untable _time host count
| streamstats global=false window=15 avg(count) AS avg BY host
| where avg > 1
| lookup aws_inventory FQDN AS host OUTPUT aws_account_name region
| stats latest(_time) AS _time BY aws_account_name host region
```

✓ 167 events (9/5/18 3:00:00.000 AM to 9/6/18 3:36:42.000 AM) No Event Sampling

Job II ↗ ↕ ⬇ Smart Mode

Events Patterns Statistics (5) Visualization

100 Per Page Format Preview

aws_account_name	host	region	_time
Splunk Cloud - Production	idx102.foo.splunkcloud.com	us-east-1	2018-09-05 14:08:00
Splunk Cloud - Production	idx17.bar.splunkcloud.com	us-east-1	2018-09-05 16:01:00
Splunk Cloud - Production	idx30.skyenet-virginia.splunkcloud.com	us-east-1	2018-09-05 11:07:00
Splunk Cloud - Production	idx40.bas.splunkcloud.com	us-east-1	2018-09-05 19:29:00
Splunk Cloud - Production	idx7.bat.splunkcloud.com	eu-central-1	2018-09-05 11:05:00

Cloud Ops Dashboards

Stack Overview

Stack Overview

Stack ID

skynet-search

Hide Filters

AWS Account

Splunk Cloud Prod

Stack Type

Stackmakr Classic

HEC Enabled?

Yes

	tags Stack	id	FQDN
1	skynet-search	i-0c3202d0a02098c6a	sh9.skynet-search.splunkcloud.com
2	skynet-search	i-0c45369ca8c5641b9	sh8.skynet-search.splunkcloud.com
3	skynet-search	i-0a2ca3d5294796826	sh7.skynet-search.splunkcloud.com
4	skynet-search	i-0e8d0695a3220025f	sh6.skynet-search.splunkcloud.com
5	skynet-search	i-b92d543e	sh5.skynet-search.splunkcloud.com
6	skynet-search	i-748e7eee	sh4.skynet-search.splunkcloud.com
7	skynet-search	i-090ada826bf2de257	sh3.skynet-search.splunkcloud.com
8	skynet-search	i-6602e3e1	sh2.skynet-search.splunkcloud.com
9	skynet-search	i-7c0572e7	sh1.skynet-search.splunkcloud.com
10	skynet-search	i-f9233977	lm1.skynet-search.splunkcloud.com
11	skynet-search	i-07d5b41fb7c005e2d	idx3.skynet-search.splunkcloud.com
12	skynet-search	i-0a74b8b2c0780fb22	idx2.skynet-search.splunkcloud.com
13	skynet-search	i-0801545b3580f783b	idx1.skynet-search.splunkcloud.com
14	skynet-search	i-435744d9	com1.skynet-search.splunkcloud.com

About

Support

File a Bug

Documentation

Privacy Policy

SRE Grab Bag

Stack Overview

Stack Disk Capacity

Stack Subnet Distribution

Stack Indexer Storage Distribution

Dynect Changes

Disk IO

Stack Memory Utilisation

Stack Search memory on Indexers

IP Address Details

Stack Index Settings

Stack Index Usage

Stack Indexer Throughput

License Mismatch

Stack Indexer Queues

Stack Splunkd Events

Stack CPU Utilisation

Stack Load Avg

Stack Vmmetric

Stack HEC Status

AWS Cloud Trail For Instance

AWS RateLimit Throttling

Stack HEC Throughput

SSH Credential Reconciliation

Searches Consuming Lots Of Memory

Stack Xtralife Config Backup Exceptions

Xtralife Bucket Backup Errors

Stack EBS Attachment

Stack Cluster Replication Status

Stack Configuration Comparison

Host Blocked 9997/Queue (Nagios overlay)

Stack Builder Stats

Stack Test Results

Stack Buckets Suffering From 'Skipping Freeze'

Stack-1

Splunk Version

7.0.3.2

Customer Type

Ops

Stack-2

Avg Daily Ingestion

3 GB

Licensed Ingestion

No results found.

Migration Status

Migration: TBD

sh_type	shc	machine_age_days	manual_steps	instance_status	instance_type	CPU	memGB	vpc_id	account_id
itsi	-	44	true	-	c3.4xlarge	16	30	vpc-4df91828	377580395208
adhoc	-	133	true	-	c3.2xlarge	8	15	vpc-4df91828	377580395208
adhoc	-	189	true	-	c3.2xlarge	8	15	vpc-4df91828	377580395208
adhoc	-	513	true	-	c3.2xlarge	8	15	vpc-4df91828	377580395208
adhoc	captain	190	true	-	c3.8xlarge	32	60	vpc-4df91828	377580395208
adhoc	member	853	true	-	c3.8xlarge	32	60	vpc-4df91828	377580395208
adhoc	member	49	true	-	c3.8xlarge	32	60	vpc-4df91828	377580395208
adhoc	-	883	true	-	c3.4xlarge	16	30	vpc-4df91828	377580395208
itsi	-	687	true	-	c3.8xlarge	32	60	vpc-4df91828	377580395208
-	-	638	true	-	m3.large	2	7.5	vpc-4df91828	377580395208
-	-	169	true	-	d2.2xlarge	8	61	vpc-4df91828	377580395208
-	-	119	true	-	d2.xlarge	8	61	vpc-4df91828	377580395208
-	-	169	true	-	d2.2xlarge	8	61	vpc-4df91828	377580395208
-	-	884	true	-	m3.large	2	7.5	vpc-4df91828	377580395208

© 2005-2018 Splunk Inc. All rights reserved.

Cloud Ops Dashboards App Versions

splunk> App: Cloud Operations Messages Settings Activity Find

Search Reports Alerts Dashboards Investigation Apps Ingestion SRE Grab Bag Cloudworks Migration Recovery Monitoring SRE Remediation

App Version For A Specific Stack

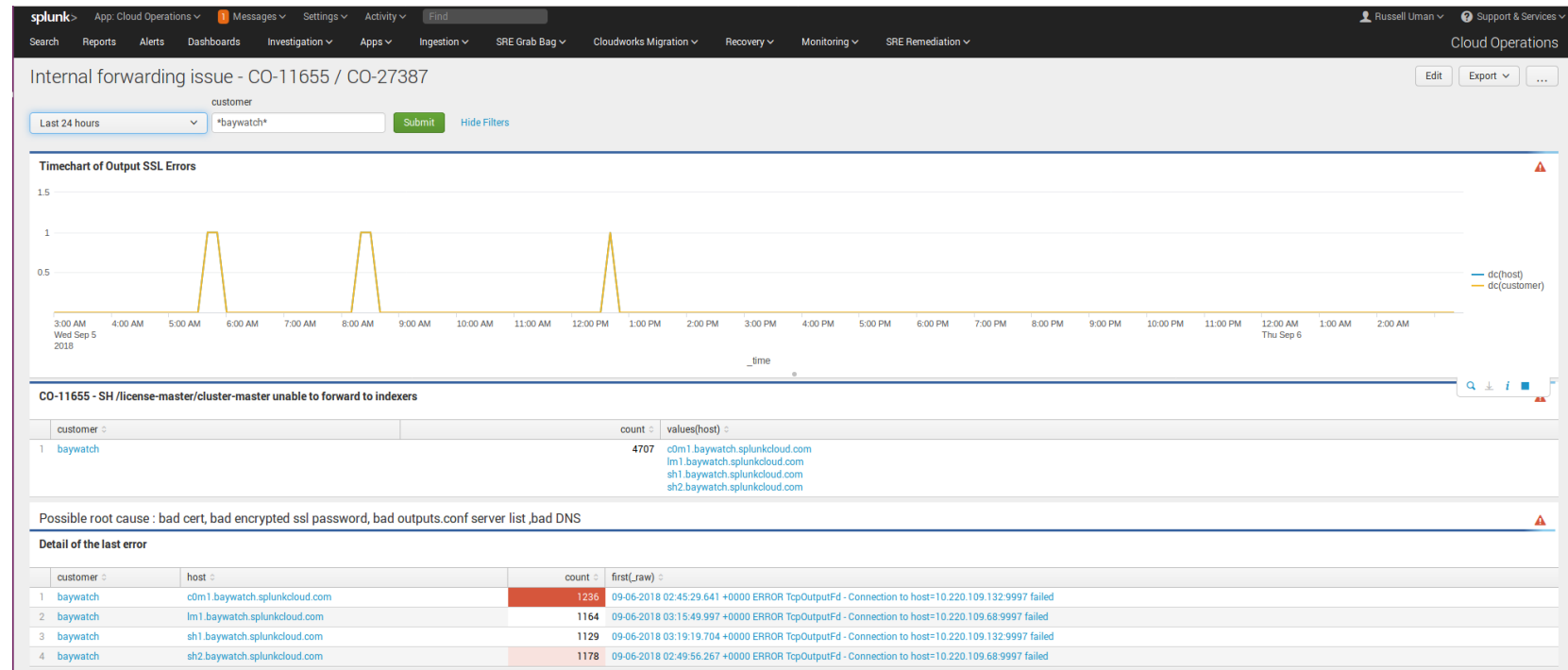
Stack ID: skynet-virginia App: Splunk_TA_aws

Apps And Version By Host

app	version	host
Splunk_TA_aws	4.4.0	fwd1.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx1.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx10.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx11.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx12.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx13.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx14.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx15.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx16.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx17.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx18.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx19.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx2.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx20.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx21.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx22.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx23.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx24.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx25.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx26.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx27.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx28.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx29.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx3.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx30.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx31.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx32.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx33.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx34.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx35.skynet-virginia.splunkcloud.com
Splunk_TA_aws	4.4.0	idx36.skynet-virginia.splunkcloud.com

Cloud Ops Dashboards

Specific Incidents





ITSI

Don't call it "ITSI".

Notable Events

ITSI

NOC Criticals

Notable Events Review | Splunk - Mozilla Firefox

https://tsi-skyline-search.splunkcloud.com/en-us/app/itsi_event_management?demo=5b3d3632b7647f737365cb4d8bae1e1e...

IT Service Intelligence

NOC Criticals

32 groups Last 24 hours Severity Critical, High, L... Status In Progress, New... Add Filter

Sort by Severity

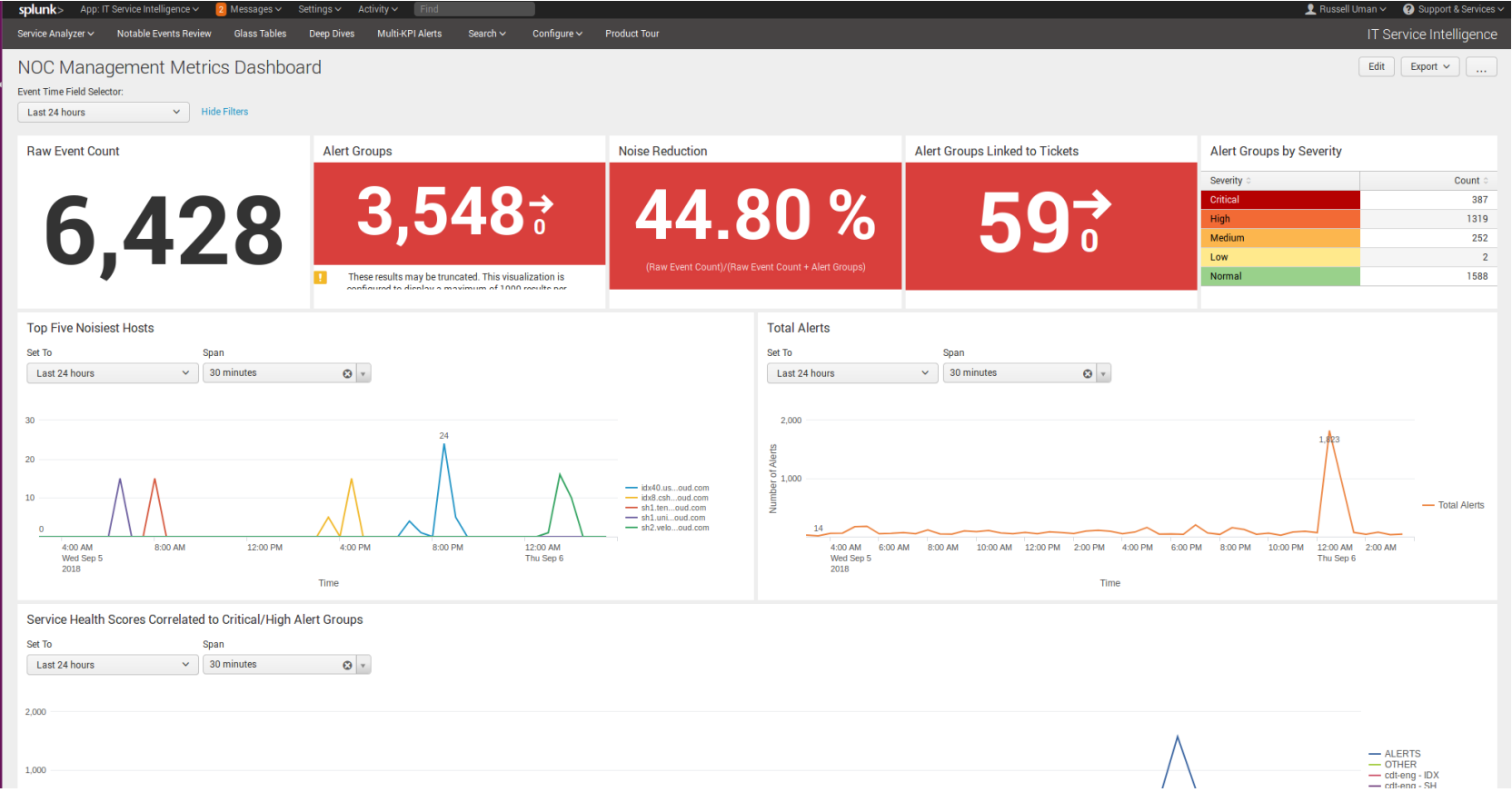
Count	customer_stack	Title	Time	Owner	Severity	Status	All Tickets
6			Fri Sep 7 09:54:02 AM - Fri Sep 7 17:58:03 PM	Unassigned	Critical	New	
6			Thu Sep 6 16:08:03 PM - Fri Sep 7 16:10:03 PM	Michael Kirkley	Critical	In Progress	
6			Thu Sep 6 16:08:03 PM - Fri Sep 7 16:10:03 PM	Michael Kirkley	Critical	In Progress	
6			Thu Sep 6 16:08:03 PM - Fri Sep 7 16:10:03 PM	Michael Kirkley	Critical	In Progress	
6			Thu Sep 6 16:08:03 PM - Fri Sep 7 16:10:03 PM	Michael Kirkley	Critical	In Progress	
6			Thu Sep 6 16:08:03 PM - Fri Sep 7 16:10:03 PM	Michael Kirkley	Critical	In Progress	
19			Thu Sep 6 09:31:02 AM - Fri Sep 7 09:58:03 AM	Gary Torres	Critical	In Progress	
2			Fri Sep 7 06:11:03 AM - Fri Sep 7 06:12:03 AM	Michael Kirkley	Critical	In Progress	JIRA-CD-50181 - 102655
3			Thu Sep 6 21:45:03 PM - Thu Sep 6 23:42:03 PM	Gary Torres	Critical	In Progress	
3			Thu Sep 6 19:05:02 PM - Thu Sep 6 19:07:03 PM	Jason Cutler	Critical	In Progress	
3			Thu Sep 6 17:43:02 PM - Thu Sep 6 17:45:03 PM	Jason Cutler	Critical	In Progress	
3			Fri Sep 7 10:03:03 AM - Fri Sep 7 10:05:03 AM	Unassigned	High	New	
6			Fri Sep 7 02:07:02 AM - Fri Sep 7 06:20:02 AM	Unassigned	High	New	
3			Fri Sep 7 06:03:03 AM - Fri Sep 7 06:05:02 AM	Unassigned	High	New	
3			Fri Sep 7 17:54:02 PM - Fri Sep 7 17:56:03 PM	Unassigned	Medium	New	
15			Thu Sep 6 07:02:02 AM - Fri Sep 7 17:42:02 PM	Unassigned	Medium	New	
14			Thu Sep 6 07:02:02 AM - Fri Sep 7 17:41:03 PM	Unassigned	Medium	New	
3			Fri Sep 7 17:39:02 PM - Fri Sep 7 17:41:03 PM	Unassigned	Medium	New	
3			Fri Sep 7 16:42:02 PM - Fri Sep 7 16:44:01 PM	Unassigned	Medium	New	
6			Fri Sep 7 09:49:02 AM - Fri Sep 7 16:16:02 PM	Unassigned	Medium	New	JIRA-CD-90219 - 1026102
6			Fri Sep 7 09:36:02 AM - Fri Sep 7 16:03:03 PM	Unassigned	Medium	New	
3			Fri Sep 7 09:42:03 AM - Fri Sep 7 09:44:02 AM	Unassigned	Medium	New	
6			Fri Sep 7 01:49:02 AM - Fri Sep 7 05:51:02 AM	Unassigned	Medium	New	
12			Wed Sep 5 21:27:02 PM - Fri Sep 7 05:24:03 AM	Michael Kirkley	Medium	In Progress	
3			Thu Sep 6 23:11:03 PM - Thu Sep 6 23:13:03 PM	Unassigned	Medium	New	
3			Thu Sep 6 23:11:03 PM - Thu Sep 6 23:13:03 PM	Unassigned	Medium	In Progress	
3			Thu Sep 6 22:04:02 PM - Thu Sep 6 22:06:02 PM	Unassigned	Medium	New	
3			Thu Sep 6 22:04:02 PM - Thu Sep 6 22:06:02 PM	Unassigned	Medium	New	
3			Thu Sep 6 21:57:03 PM - Thu Sep 6 21:59:03 PM	Unassigned	Medium	New	
1			Thu Sep 6 21:42:02 PM - Thu Sep 6 21:42:02 PM	Unassigned	Medium	New	
1			Thu Sep 6 21:42:02 PM - Thu Sep 6 21:42:02 PM	Unassigned	Medium	New	
3			Thu Sep 6 19:05:02 PM - Thu Sep 6 19:07:03 PM	Unassigned	Medium	New	
3			Thu Sep 6 19:04:03 PM - Thu Sep 6 19:06:02 PM	Unassigned	Medium	New	

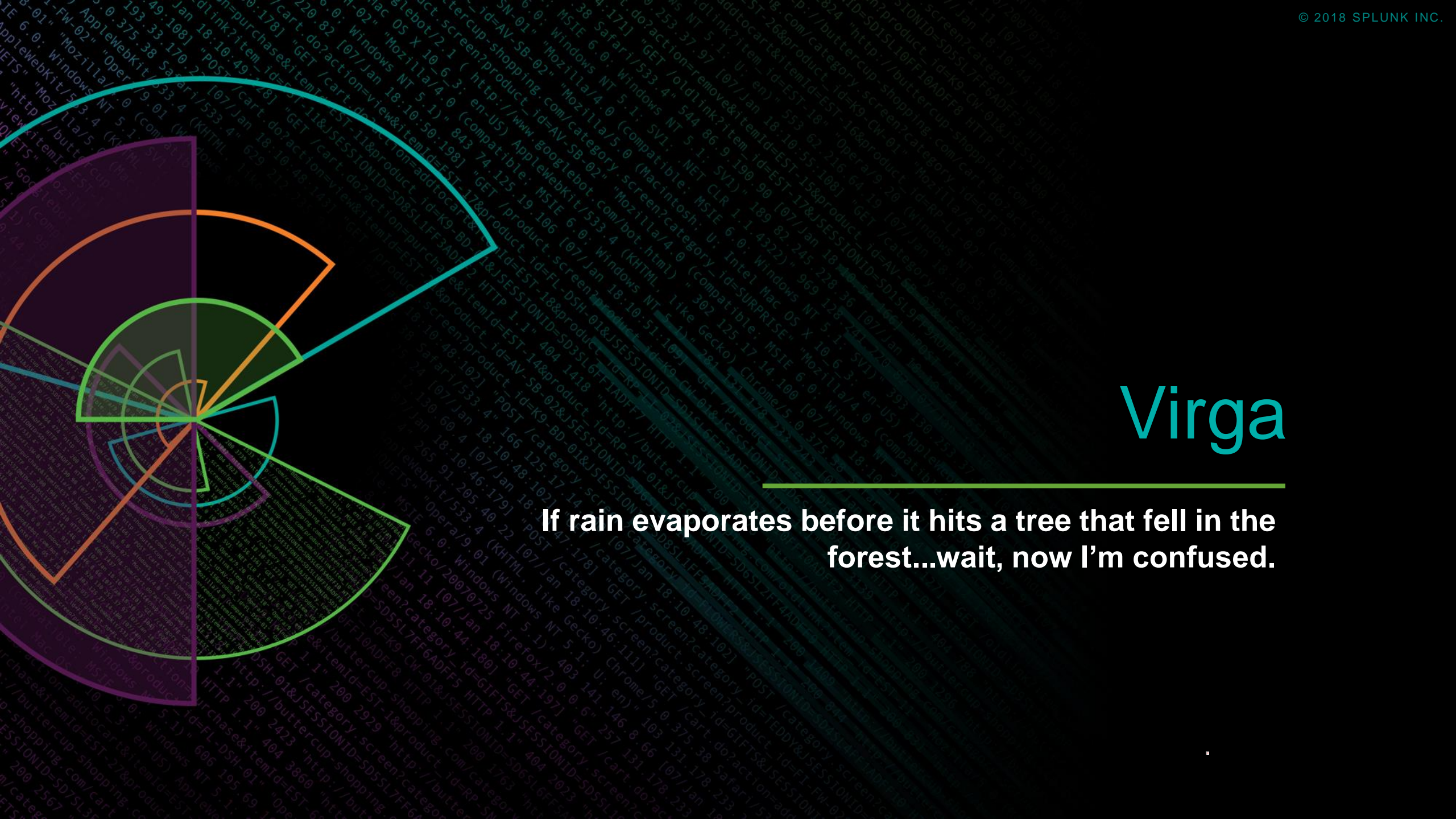
No more notable event groups.

About Support File a Bug Documentation Privacy Policy

© 2009-2018 Splunk Inc. All rights reserved.

ITSI NOC Management Metrics





Virga

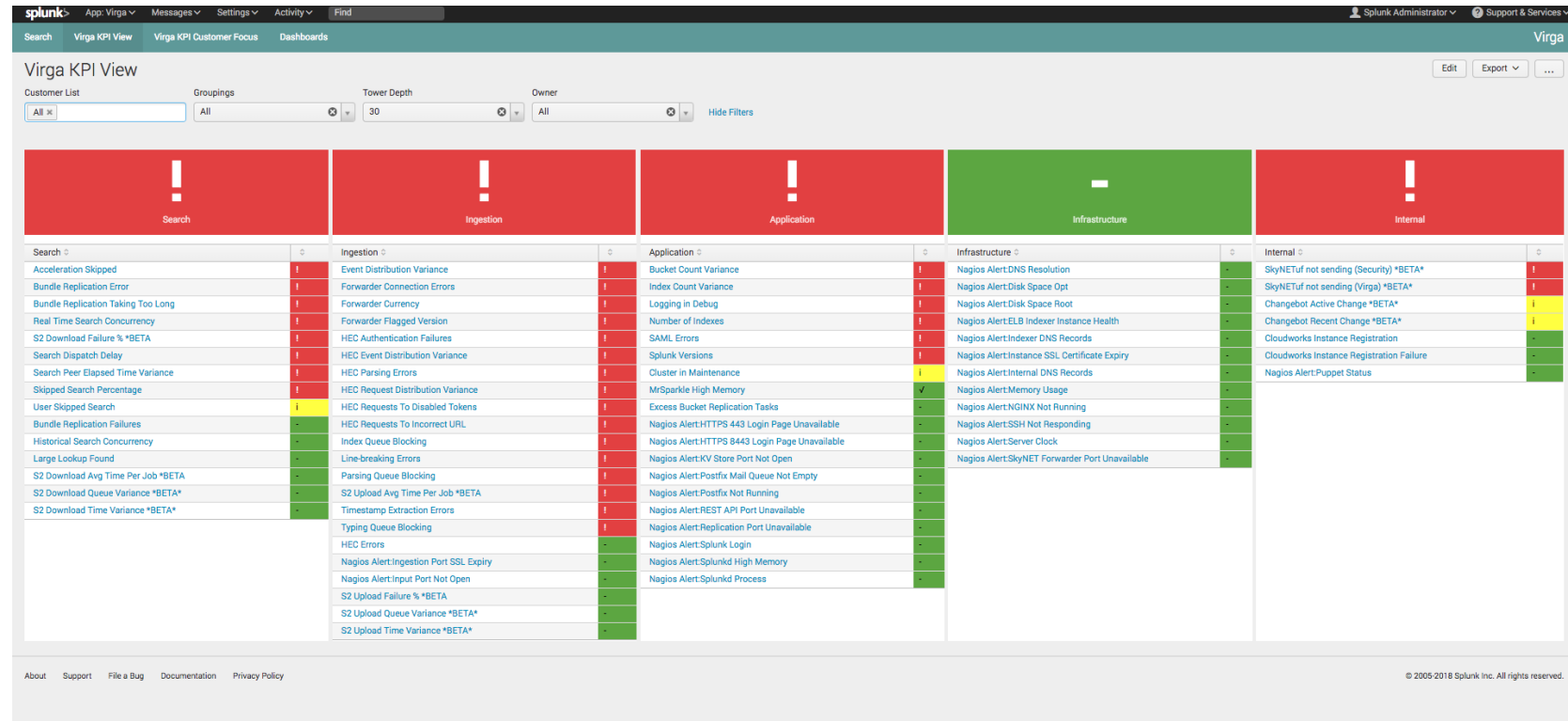
If rain evaporates before it hits a tree that fell in the forest...wait, now I'm confused.

KPIs for Support

- ▶ Many customer issues are better addressed by Support than by Cloud Ops.
- ▶ Virga leverages Skynet to help Support quickly hone in on components that need attention.

VIRGA

KPI Dashboard



Next Steps

Learn more about the Cloud Monitoring Console and find guided walkthroughs for each of these topics at:

<http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DMCoverview>

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&SESSIONID=SD1B5L8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.1.1.1 screen?category_id=FLOWERS&SESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
action=purchase&itemId=EST-26&product_id=K9-CW-01" 468 125.17 14.1.1.1 screen?category_id=FLOWERS&SESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"



Q&A

Thank You

Don't forget to **rate this session**
in the **.conf18** mobile app

.conf18

splunk>

.conf18