.conf18

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> .conf18

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.

splunk> .conf18

Cloud Monitoring Console

Skynet

ITSI

Virga

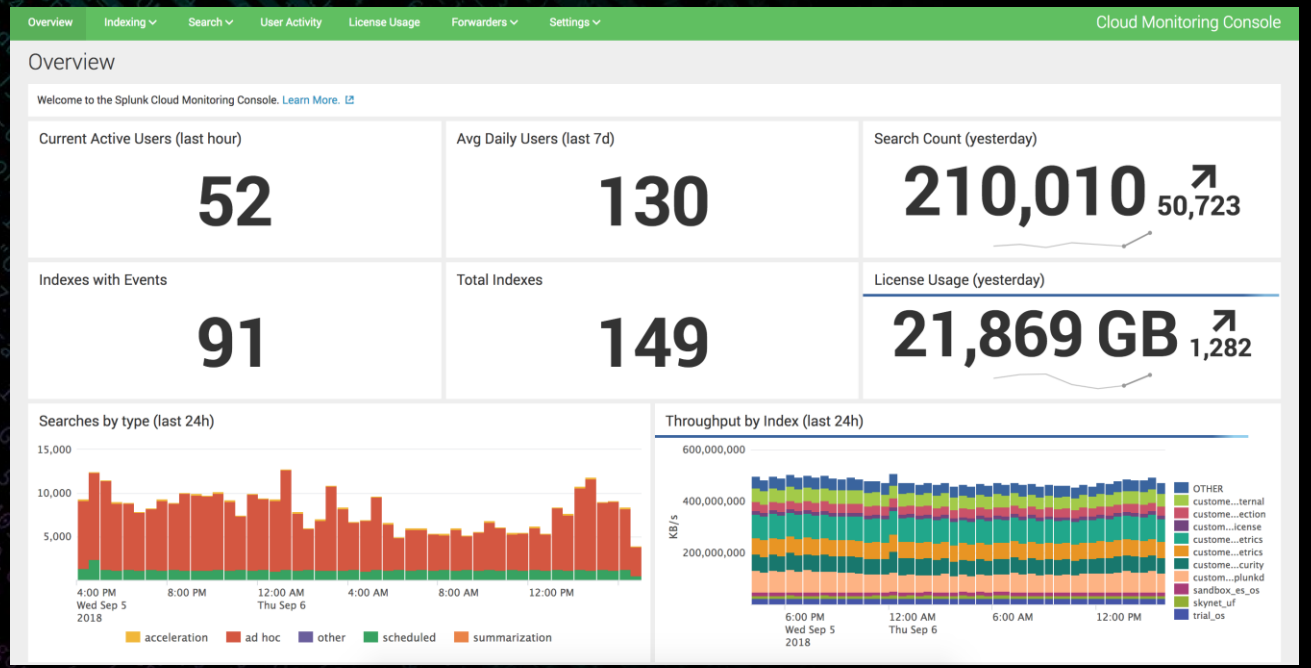
Cloud Monitoring Console

My friends call me McCloud.

splunk> .conf18

Things you can do with the CMC

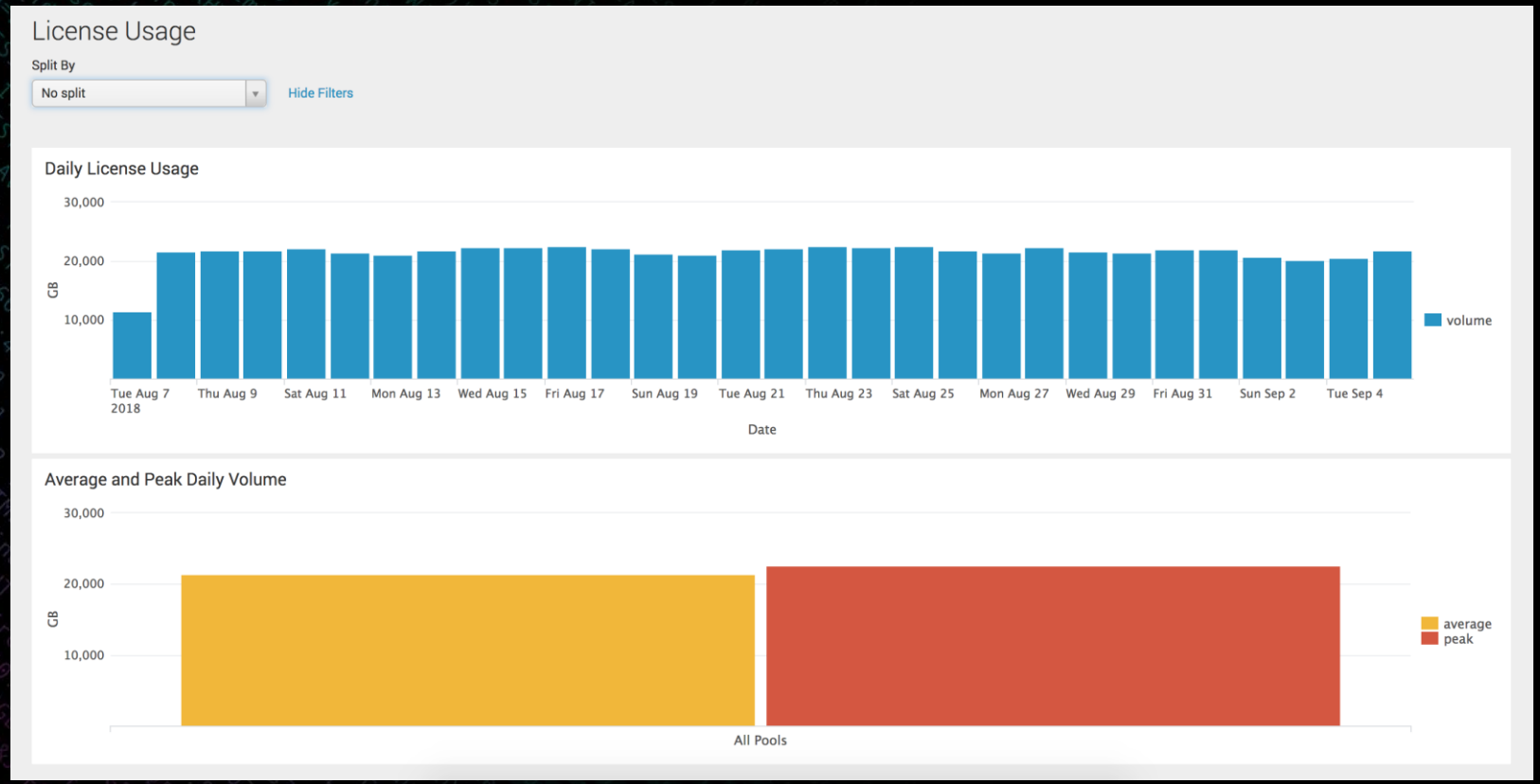
- Review Daily Data Ingest
- Audit Data Storage by Index
- Understand Usage Patterns
- Troubleshoot Data Ingest
- Investigate Search Issues



splunk> .conf18

Data Ingest

Do you know how much data you're sending?



splunk> .conf18

Data Storage

How much data are you retaining?

Indexes and Storage

91	149	4884.63 TB	13,967,525,088,750
Indexes with Events	Total Configured Indexes	Total Index Size	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

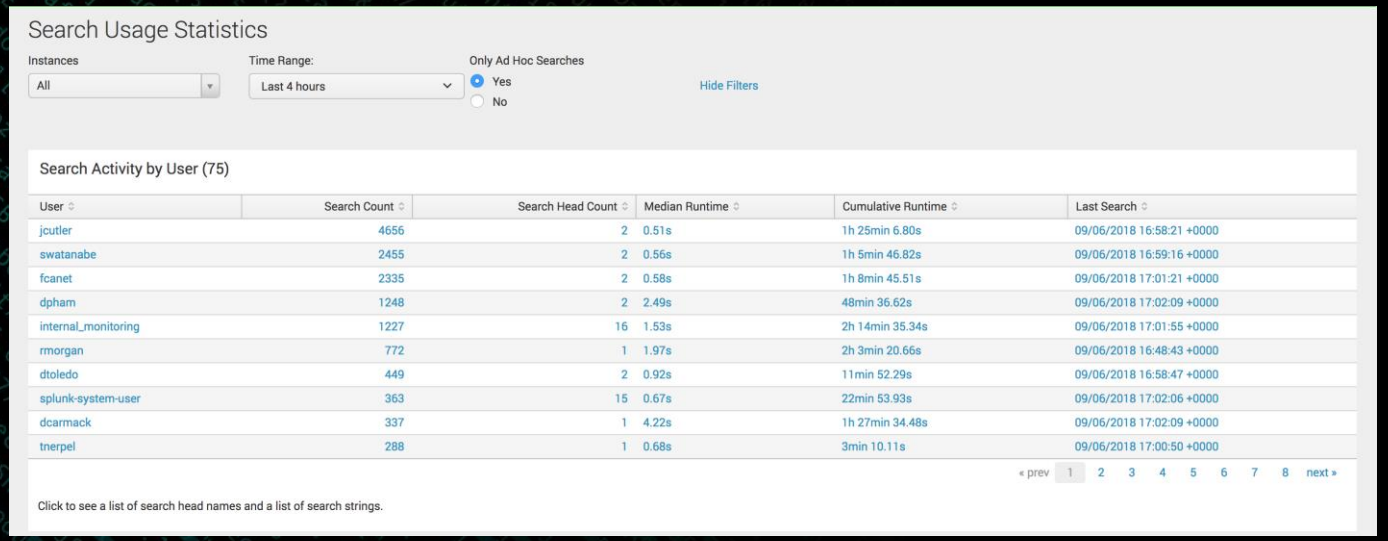
« prev 1 2 3 4 5 6 7 8 9 10 next »

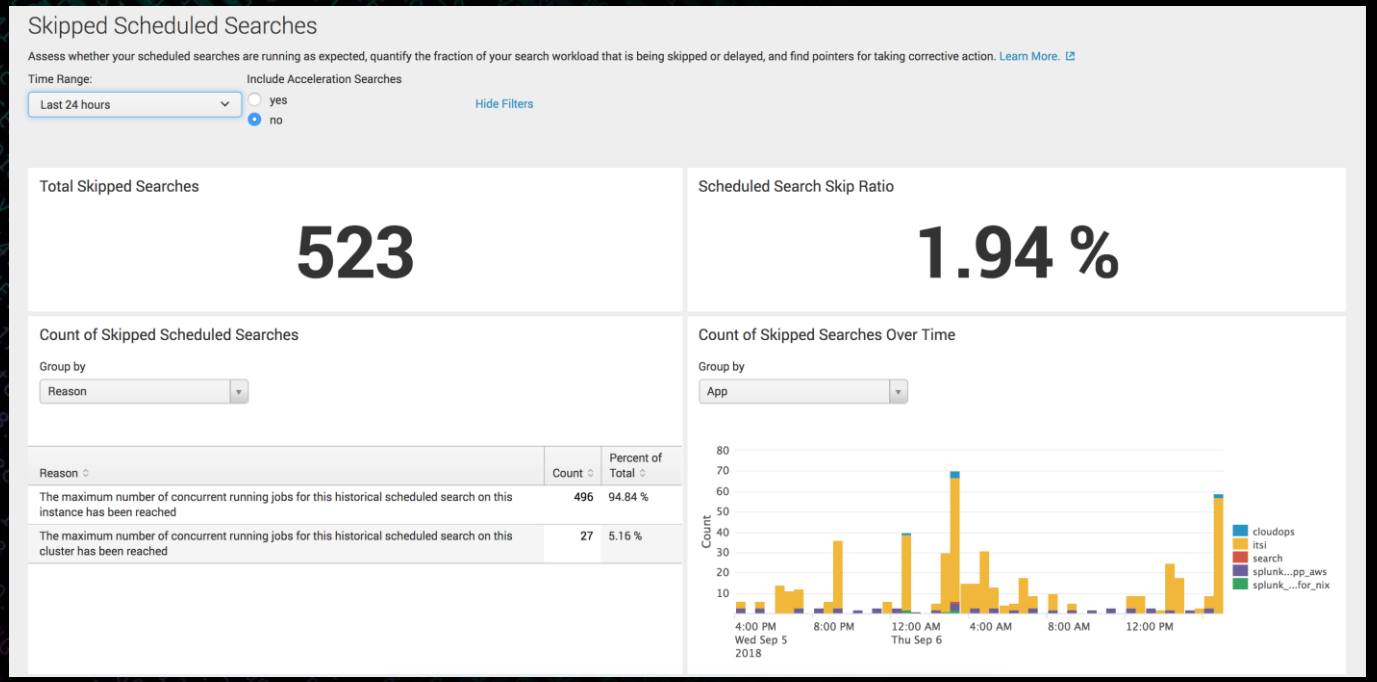
- **Index Usage (GB):** The amount of raw data stored for the index in GB
- **Total Event Count:** The total number of events currently stored for the index.
- **Total Bucket Count:** The total number of buckets currently stored for the index.

splunk> .conf18

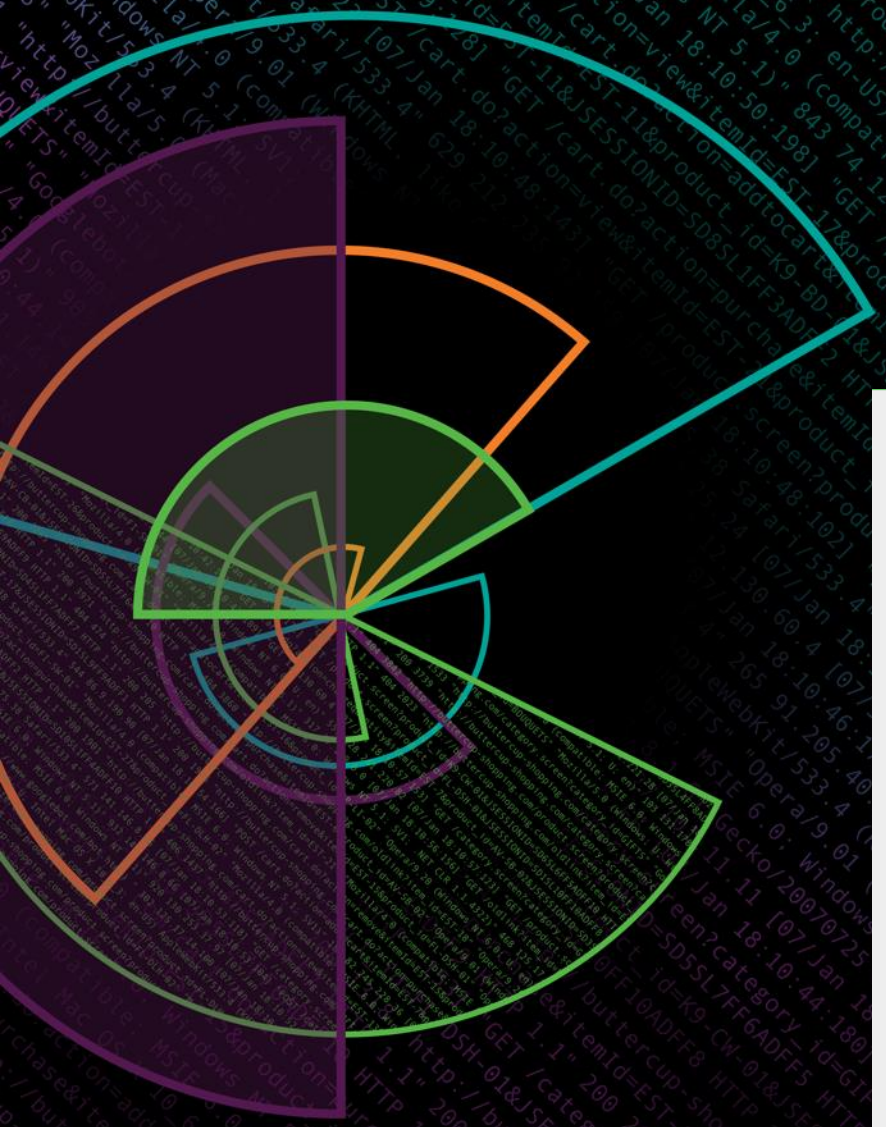
Understanding Search Performance

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



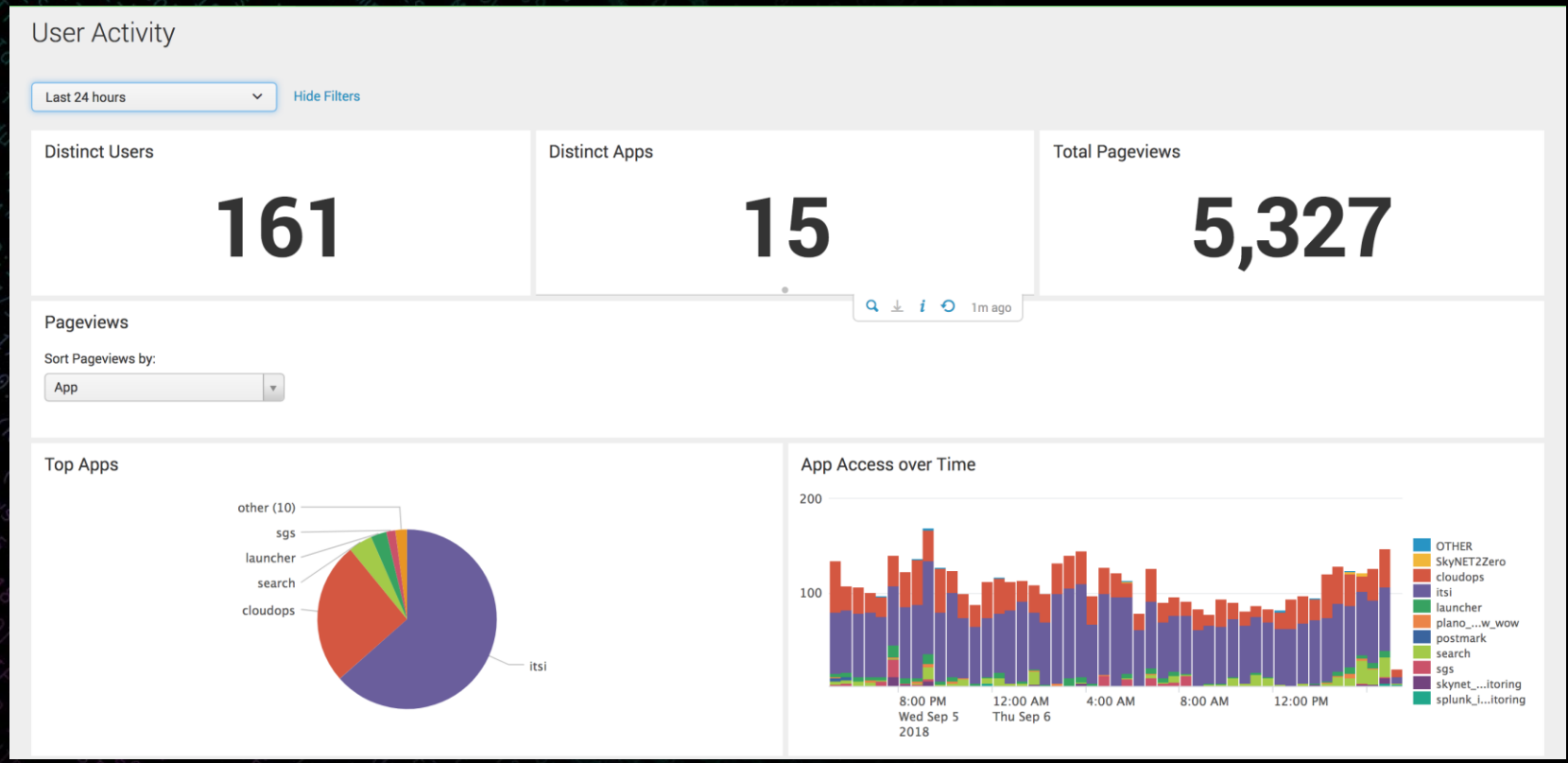


splunk> .conf18

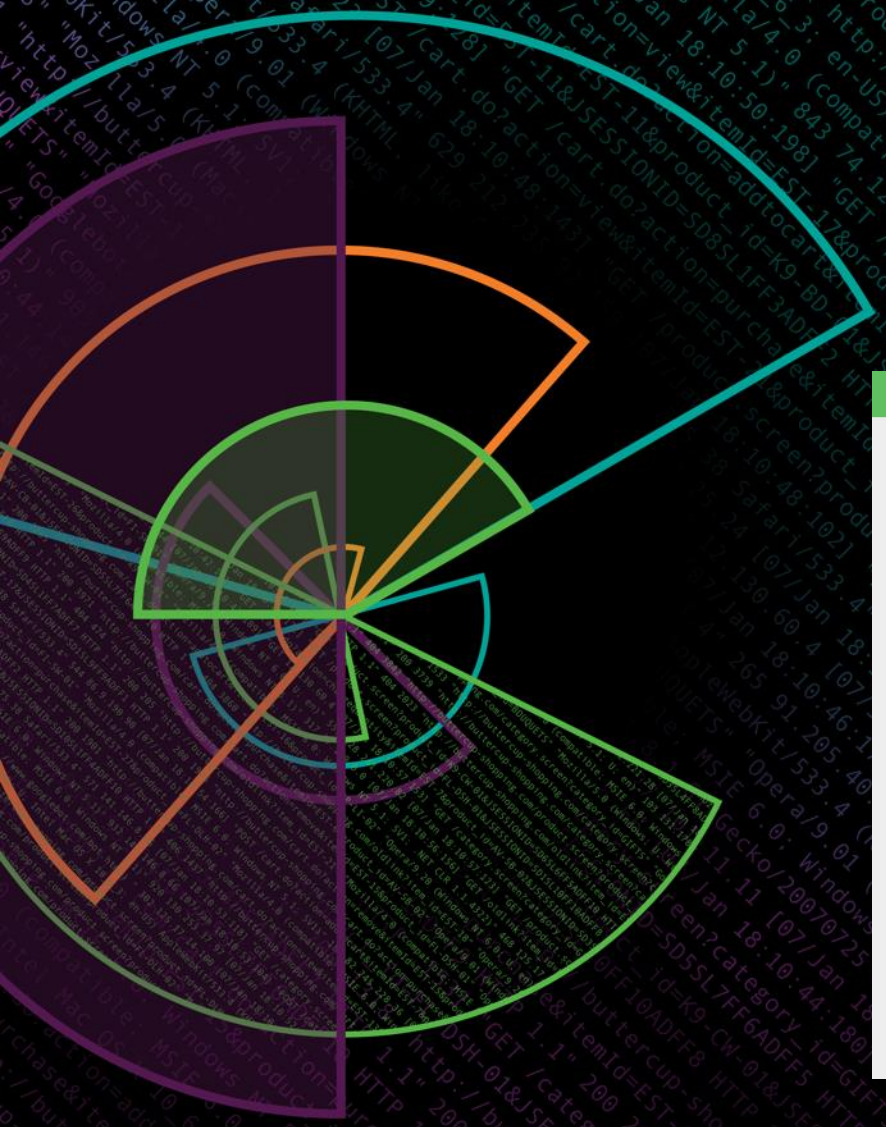


Usage Review

How are your users gaining value from Splunk Cloud?



splunk> .conf18



Troublesome Data

Do your configs match your logs?

Overview | Indexing | Search | User Activity | License Usage | Forwarders | Settings | Cloud Monitoring Console

Data Quality

This dashboard helps you assess the quality of your incoming data by revealing issues that occur when the data is being indexed. These issues appear as warnings and errors in your splunkd.log.

Time Range: Last 4 hours

Include Splunk Sourcetypes: (•) No ( ) Yes

Hide Filters

Event Processing Issues by Source Type

Sourcetype	Total Issues	Source Count	Line Breaking Issues	Timestamp Parsing Issues	Aggregation Issues
splunk_python	44957	1	0	44957	0
splunkd	26076	18	25251	825	0
netstat	19958	1	25	91	19842
ps	10377	1	1	5660	4716
syslog	8219	5	4	8215	0
top	6071	1	0	205	5866
linux_secure	5266	2	0	5266	0
suricata	4062	9	0	4062	0
package	1956	1	0	80	1876
linux_messages_syslog	1932	8	1	1931	0

« prev 1 2 3 4 5 6 next »

Clicking a source type shows issues by source, helping you locate the origin of this data. [Show more info]

splunk> .conf18

Skynet

Skynet has not yet attained sentience.

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]

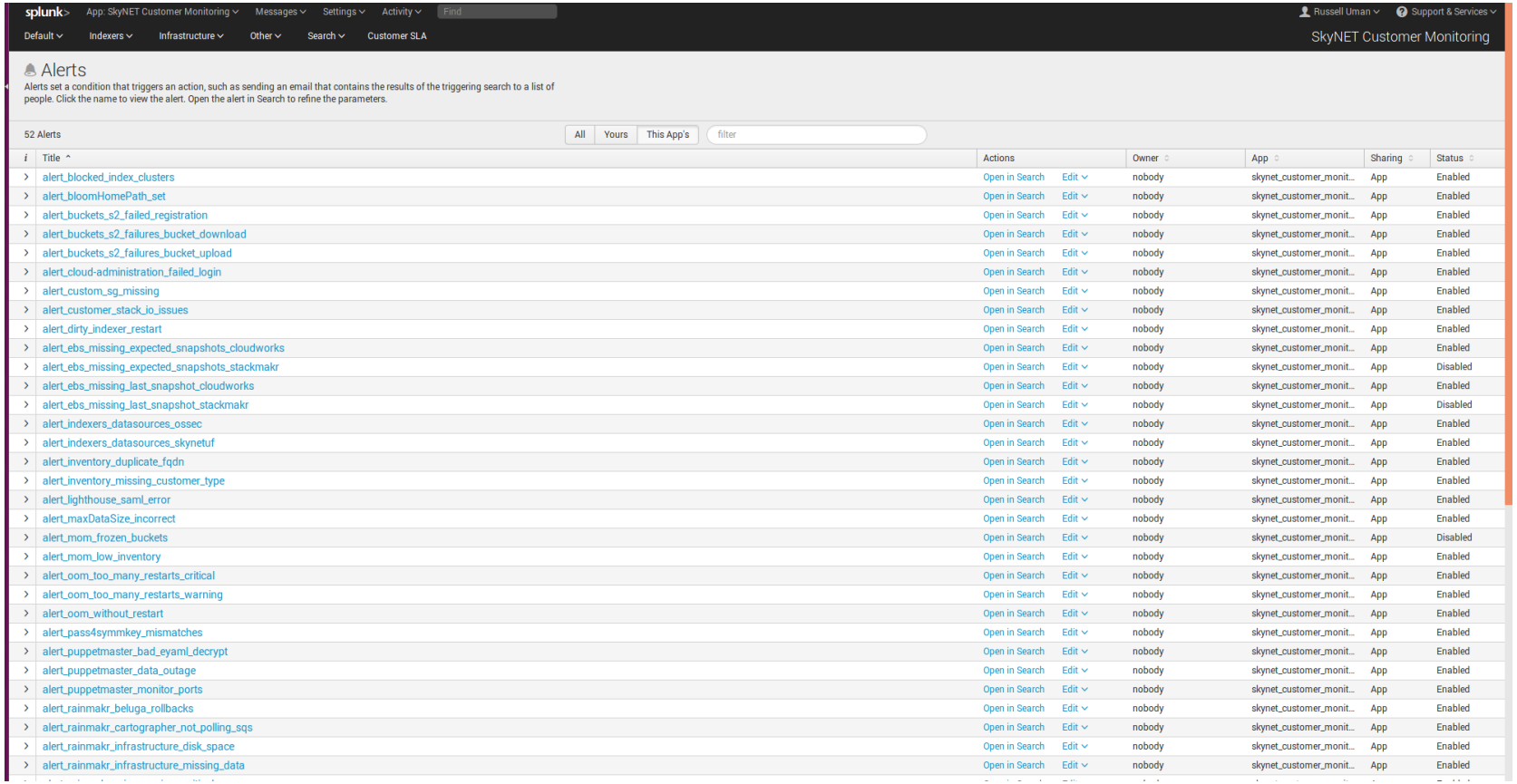
```
index=aws_description source=*:ec2_instances
| fillnull value="null" alertable aws_account_shortname bucket_location customer_type tags.Role
  tags.Stack vpc_id tags.CloudworksEnv
| stats count by alertable account_id aws_account_shortname aws_account_name bucket_location id
  instance_type ip_address 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_shortname 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
```

splunk> .conf18

Monitoring/Ops Process

- Cloud Monitoring team writes alerts.
- SRE team writes runbooks, and develops dashboards for troubleshooting.
- NOC receives alerts (via ITSI), runs runbook, uses dashboards, escalates to SRE if necessary.

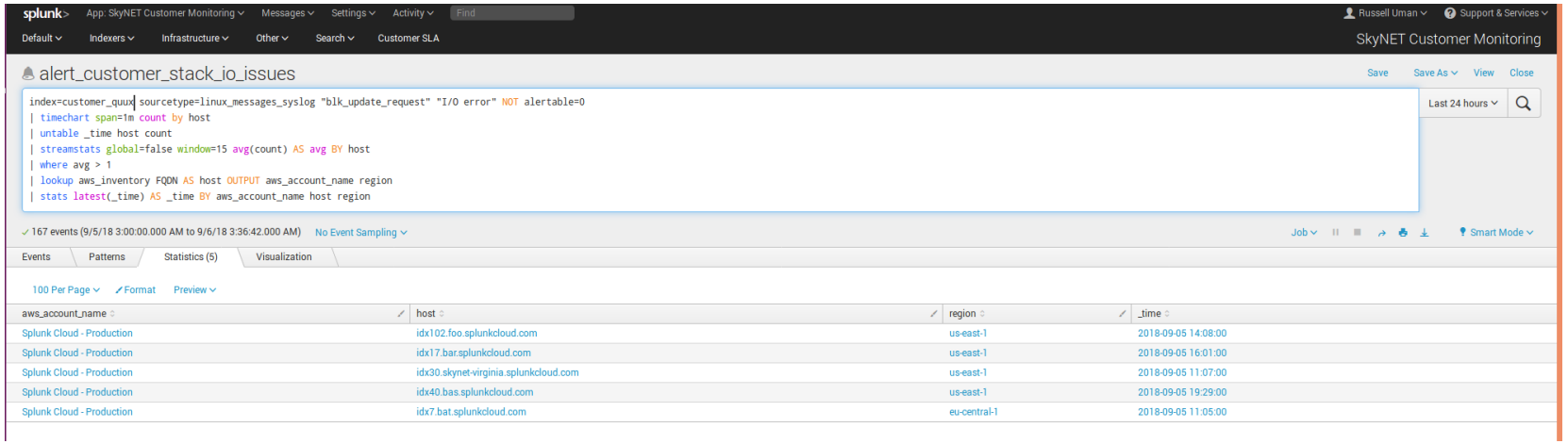
Cloud Monitoring Alerts



splunk> .conf18

Cloud Monitoring Alerts

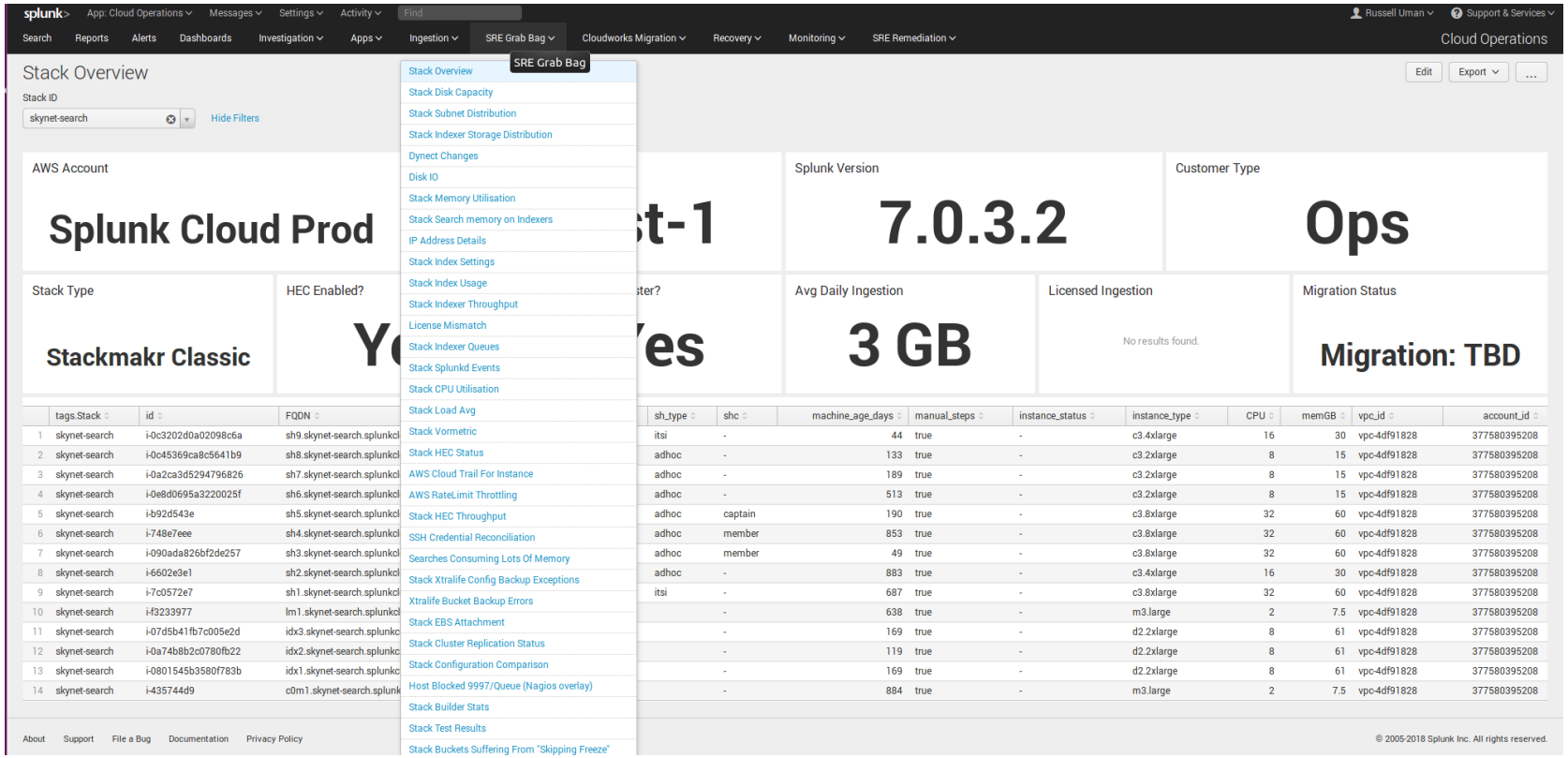
IO issues



splunk> .conf18

Cloud Ops Dashboards

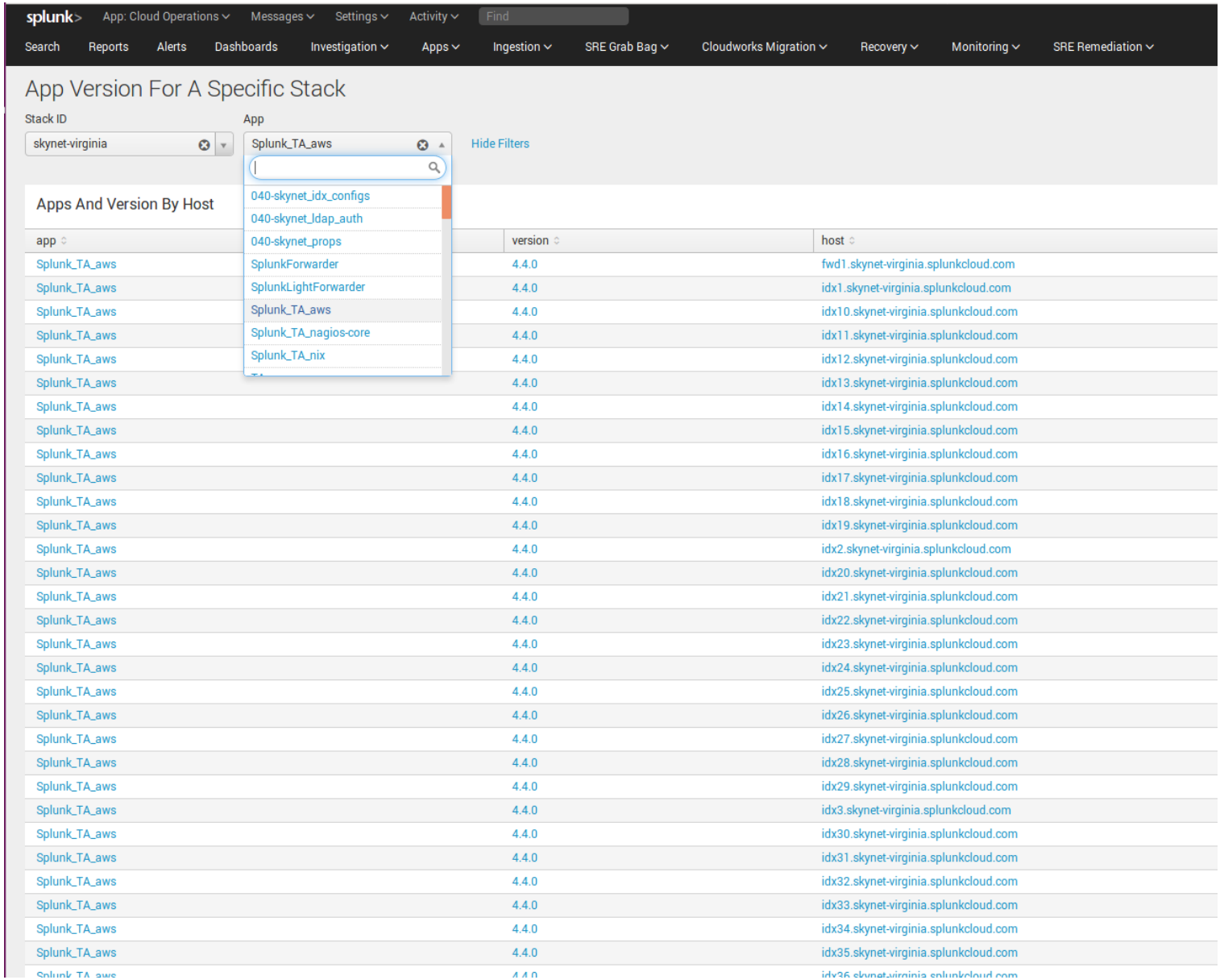
Stack Overview



splunk> .conf18

Cloud Ops Dashboards

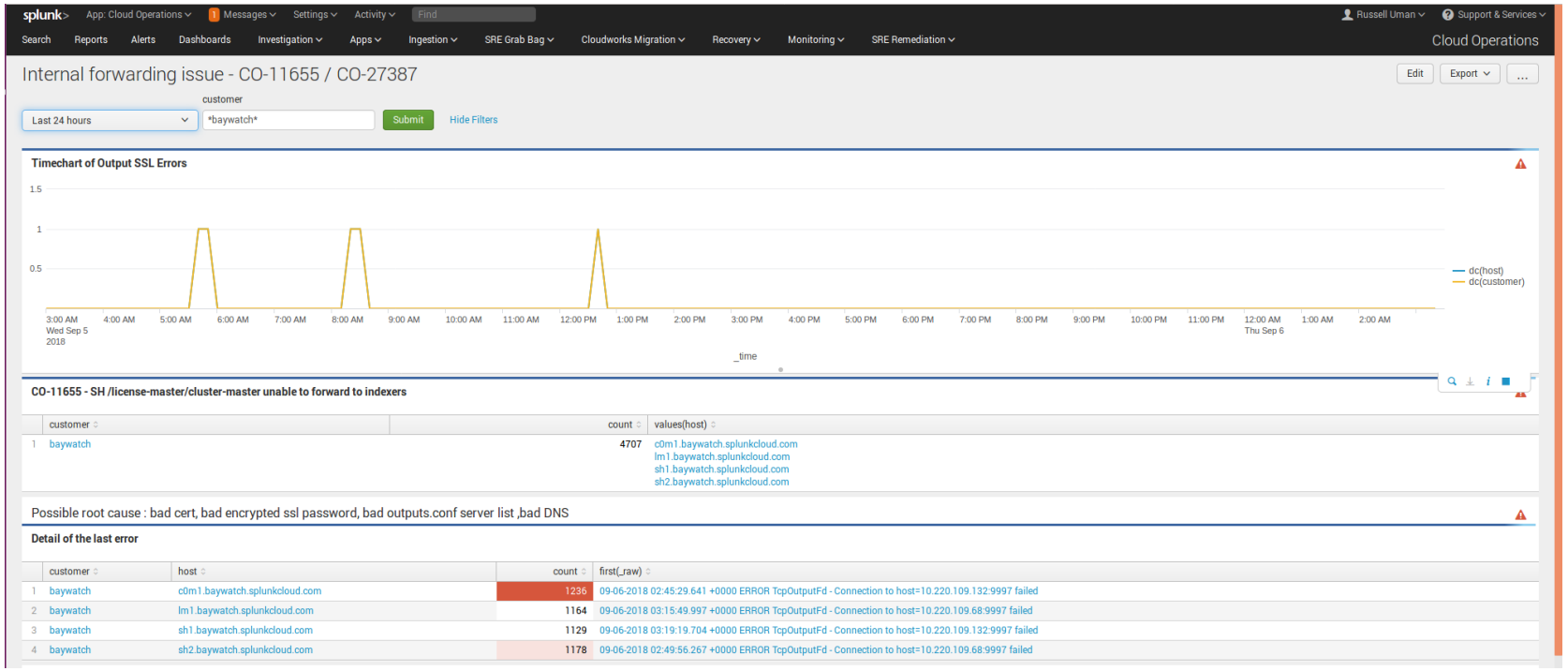
App Versions



splunk> .conf18

Cloud Ops Dashboards

Specific Incidents



splunk> .conf18

ITSI

Don’t call it “ITSI”.

Notable Events

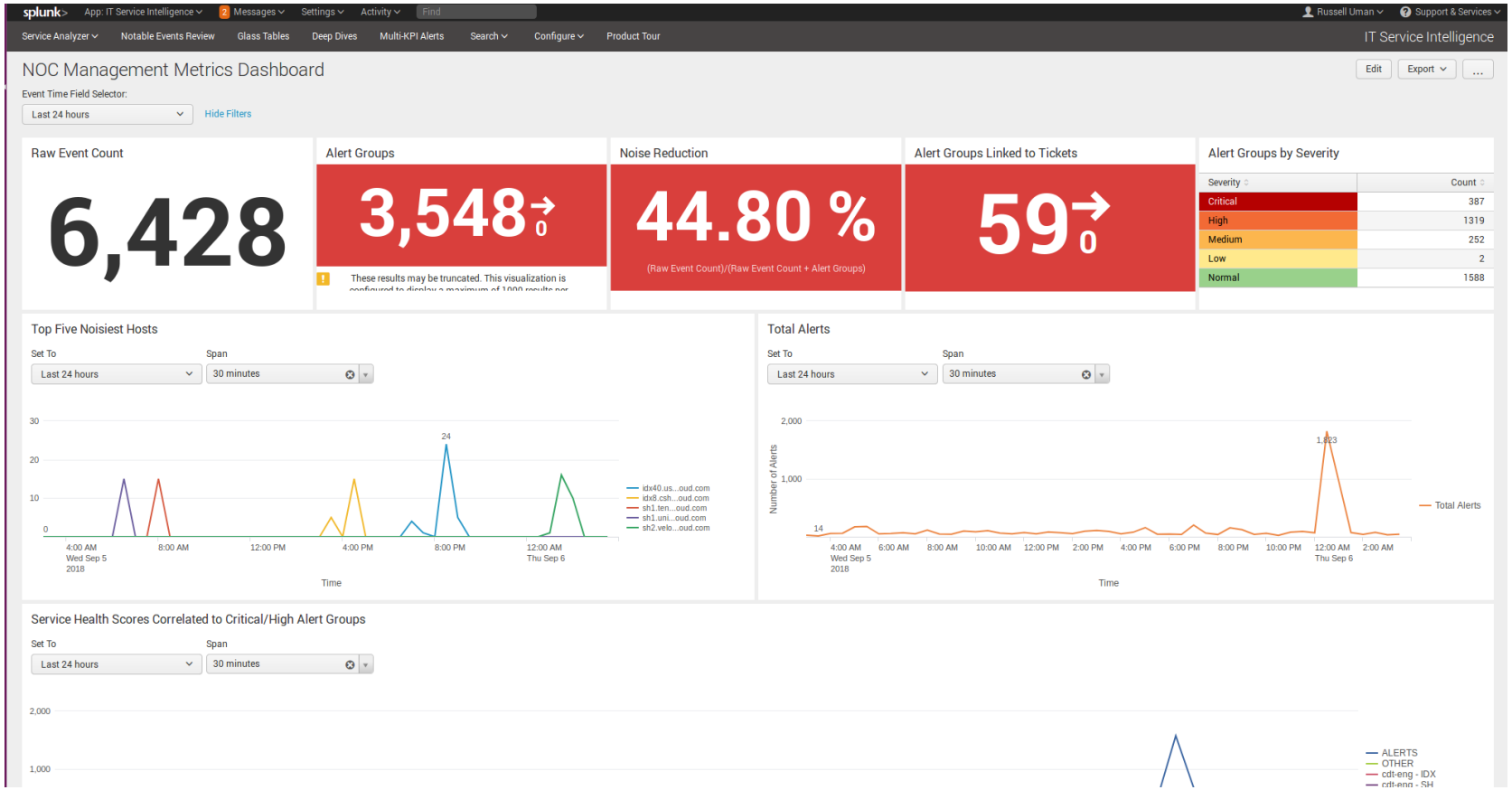
- ITSI creates Notable Events from the Skynet alert stream.
- Notable Events are enriched with data from related JIRA tickets and SFDC cases.
- Notable Events are grouped by customer, with severity determined by the collection of grouped alerts.
- This allows NOC to work holistically on the most critical customers first instead of having to whack every mole separately.

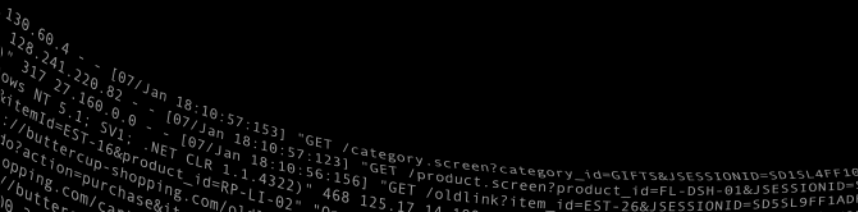
ITSI

NOC Criticals

ITSI

NOC Management Metrics





splunk> .conf18

Virga

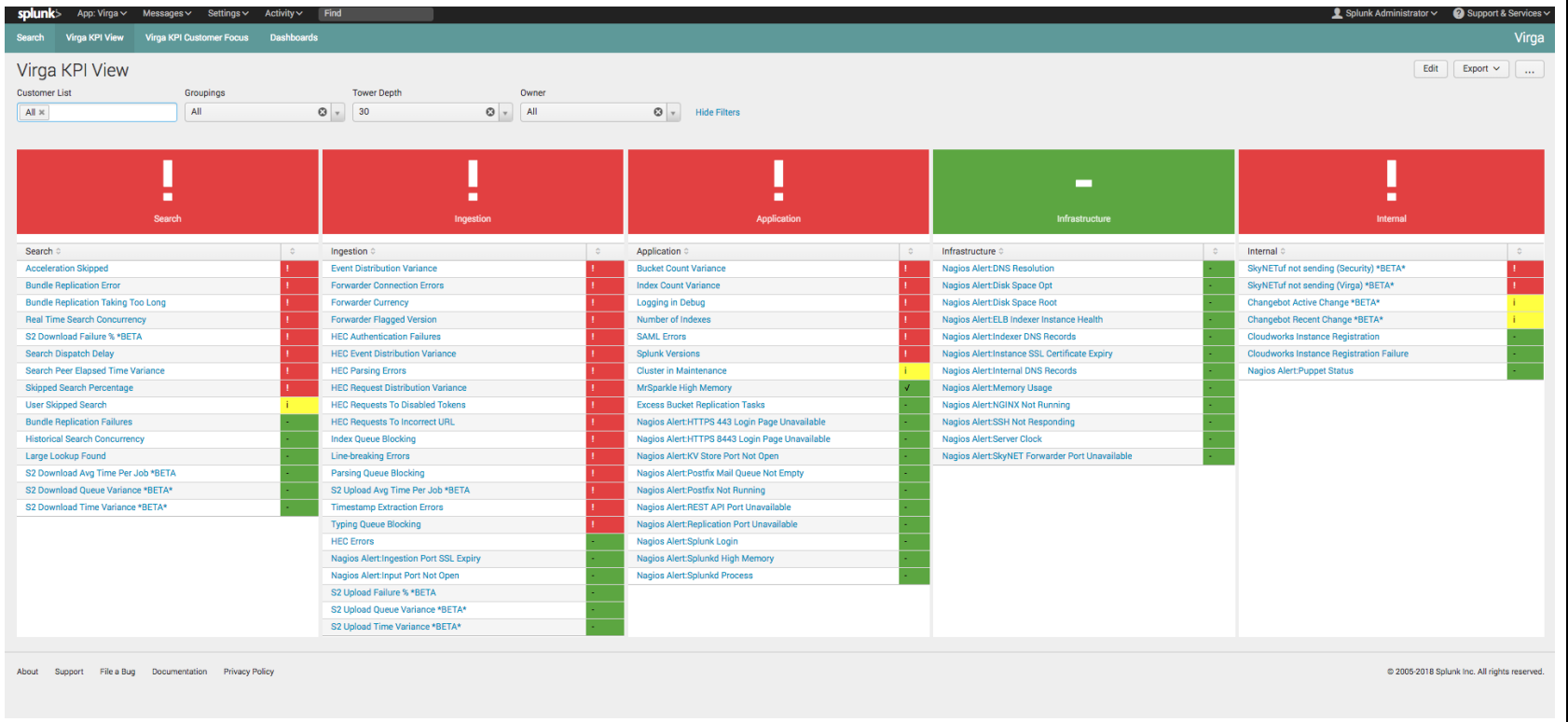
If rain evaporates before it hits a tree that fell in the forest...wait, now I'm confused.

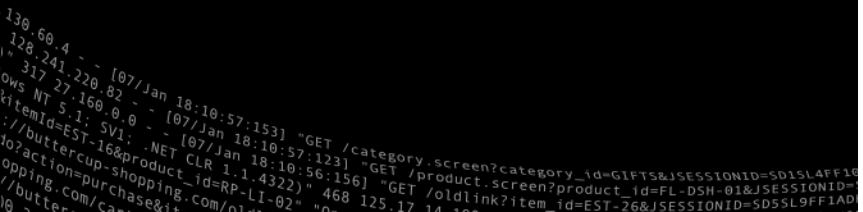
KPIs for Support

- 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





splunk> .conf18

VIRGA

KPI Deep Dive

splunk> .conf18

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

splunk> .conf18

Q&A

splunk> .conf18

Thank You

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