splunk> .conf2017

Agency Chargeback models to enable Enterprise Splunk deployments

Using Data to Finance Shared Services

Adilson Jardim | AVP, Public Sector Sales Engineering
Mike Wilson | Principal Sales Engineer, Public Sector

Sep 2017 | Washington, DC

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.

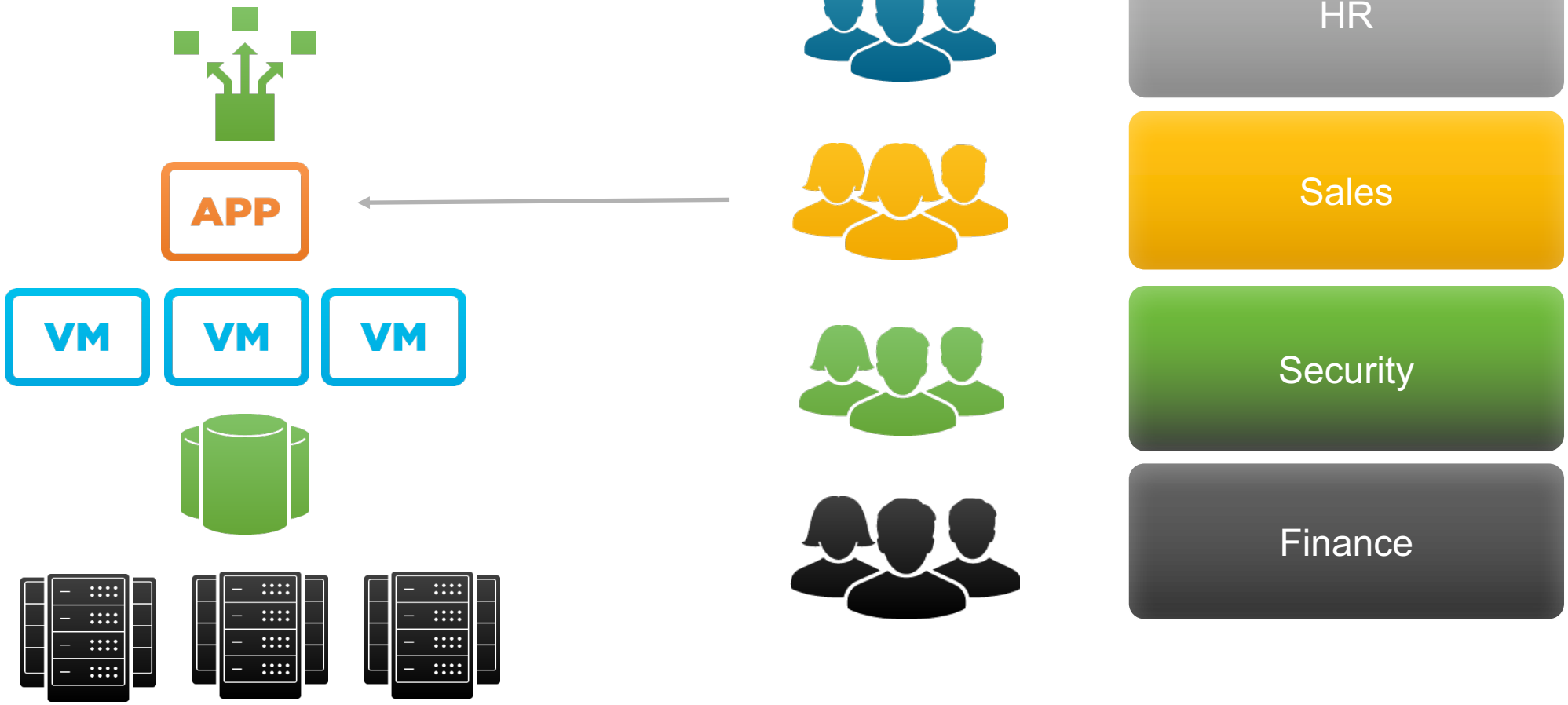
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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> .conf2017

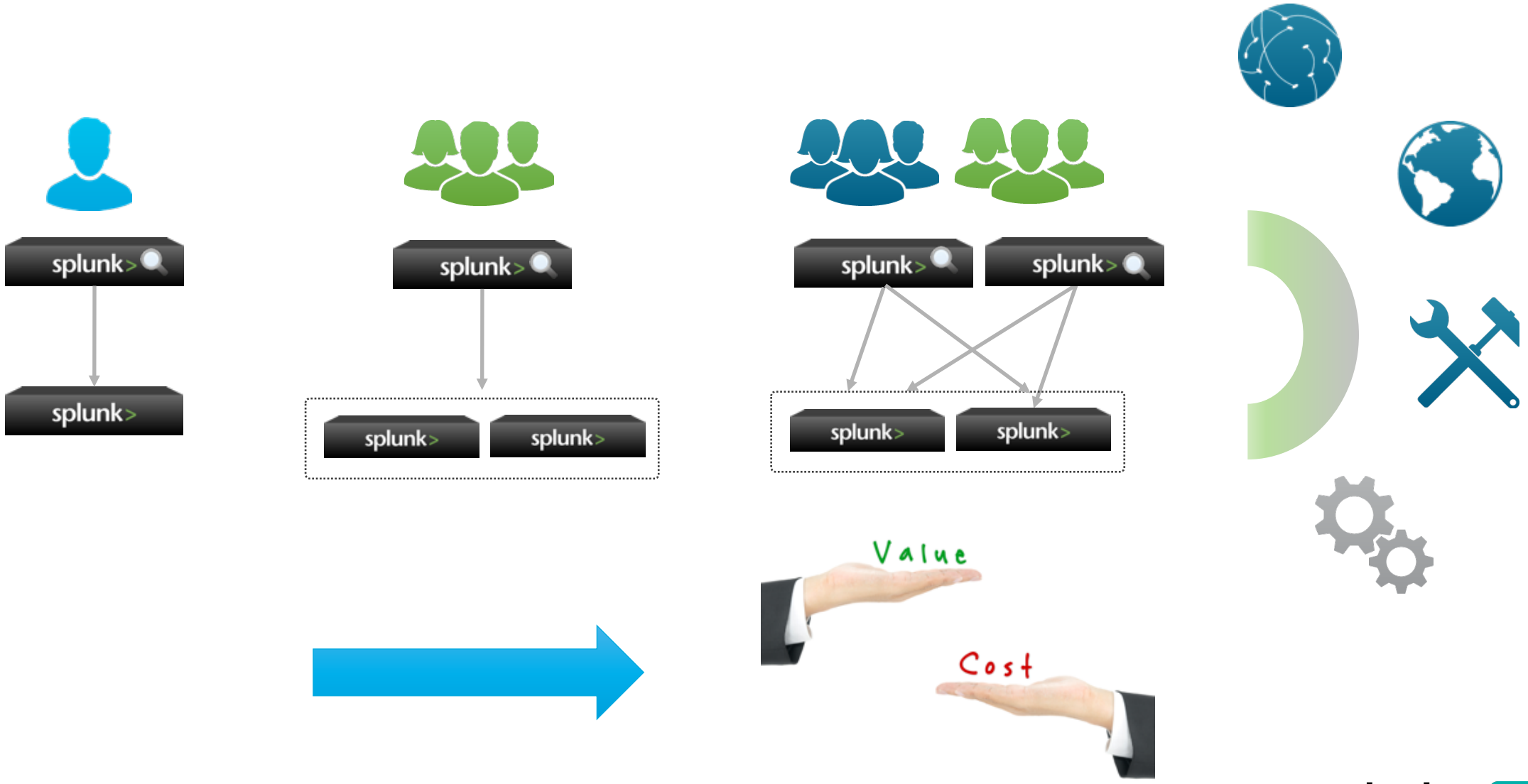
A Framework for quantifying IT service costs

splunk> .conf2017

Who bears the cost of providing a service?



Splunk is a service too!



It’s not just chargeback…

Framework for applying a "total cost" to running any service (license + compute + storage + ...)

Do you need the help?

5 votes | 1 answer | 927 views

How do you handle chargebacks to business units within your organization?

licensing | chargeback | billing | business

commented Jan 21, '16 by jplumsdaine22 2.6k

0 votes | 0 answers | 252 views

Has anyone created a Splunk Chargeback Model that includes number of and performance heavy searches, not just data indexed and support costs?

search | indexing | model | chargeback

edited Jan 8, '15 by shaun dubie 66

0 answers

1 vote | 2 answers | 502 views

How to Create Chargeback Reports in Splunk.

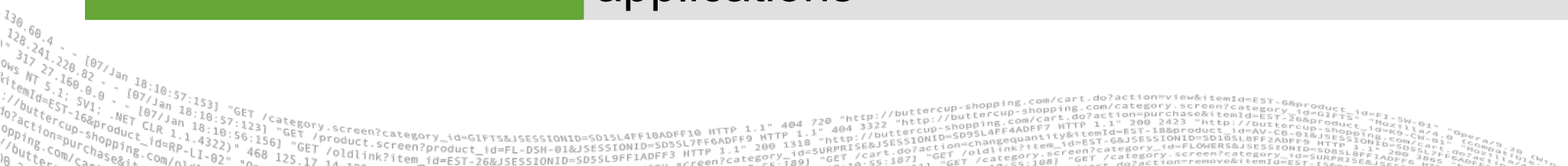
Splunk License Usage | splunk | report | chargeback

edited May 15, '14 by rohit31dec91 31

splunk> .conf2017

But first - Vocabulary

Term	Definition
Showback	Providing metrics and data regarding resource utilization (without charging)
Chargeback	Implementing formal accounting practices to cross-charge departments for resource or application utilization
Multi-tenant	Architecture supporting multiple different customers on one implementation
Resources	In this context, all elements of a system, including: CPU, memory, storage, virtual environments/machines, applications



Defining Cost Basis

Type	Definition
Fixed	Service type with fixed costing, e.g. # of users
Allocation Based	• Variable costs per environment like # of Search Heads, Indexers, Apps, etc. • VM Based – small, medium, large VM costing
Utilization Based	Variable costs – CPU, Memory, Storage, I/O

What we will address

Business	Metrics	On-Premise	Application Services	Charging
Requirements for chargeback Structuring a team	Finding: I/O, CPU, Search Costs, Storage *What else you can use*	Architecture & topology discussion	Cloud as a Service AWS Metrics	Considerations for charging / showback

splunk> .conf2017

Defining Splunk as a Service

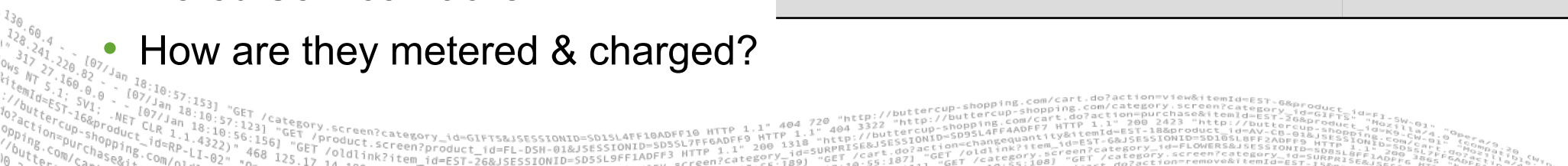
splunk> .conf2017

A Splunk Center of Excellence

Center of Excellence

- Define Consumer Organizations
- Define your services:
  - Design & Development
  - Analytics, Dashboards, APIs, alerts
  - Tiered Service Packs
  - How are they metered & charged?

Engineering	Operations
Requirements Lead	Admin
Knowledge Admin	Systems/Storage Admin
Developer	Knowledge Admin
Analyst	
Analytics Lead	



splunk> .conf2017

Let’s dive into the meaty stuff

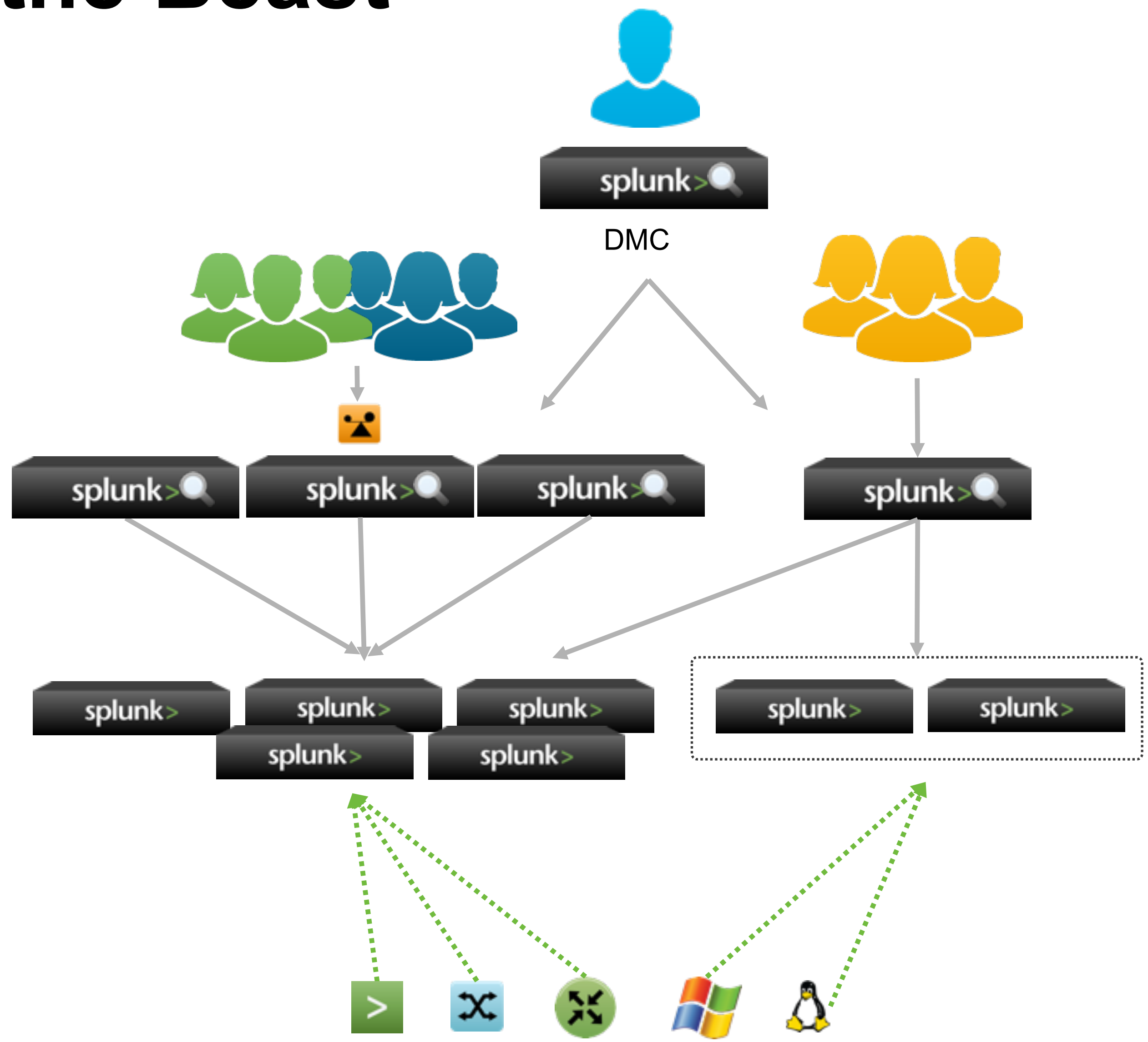
Splunk Internals Overview

Component	Purpose
Search Head	In a distributed search environment, a Splunk Enterprise instance that handles search management functions, directing search requests to a set of search peers and then merging the results back to the user.
Indexer	A Splunk Enterprise instance that indexes data, transforming raw data into events and placing the results into an index. It also searches the indexed data in response to search requests.
Forwarder	A Splunk Enterprise instance that forwards data to another Splunk Enterprise instance, such as an indexer or another forwarder, or to a third-party system.
Application	An application that runs on Splunk Enterprise and typically addresses several use cases. An app contains one or more views. An app can include various Splunk Enterprise knowledge objects such as reports, lookups, scripted inputs, and modular inputs.
Index	When you add data, the indexer processes it and stores it in an index. By default, data you feed to an indexer is stored in the main index, but you can create and specify other indexes for different data inputs.

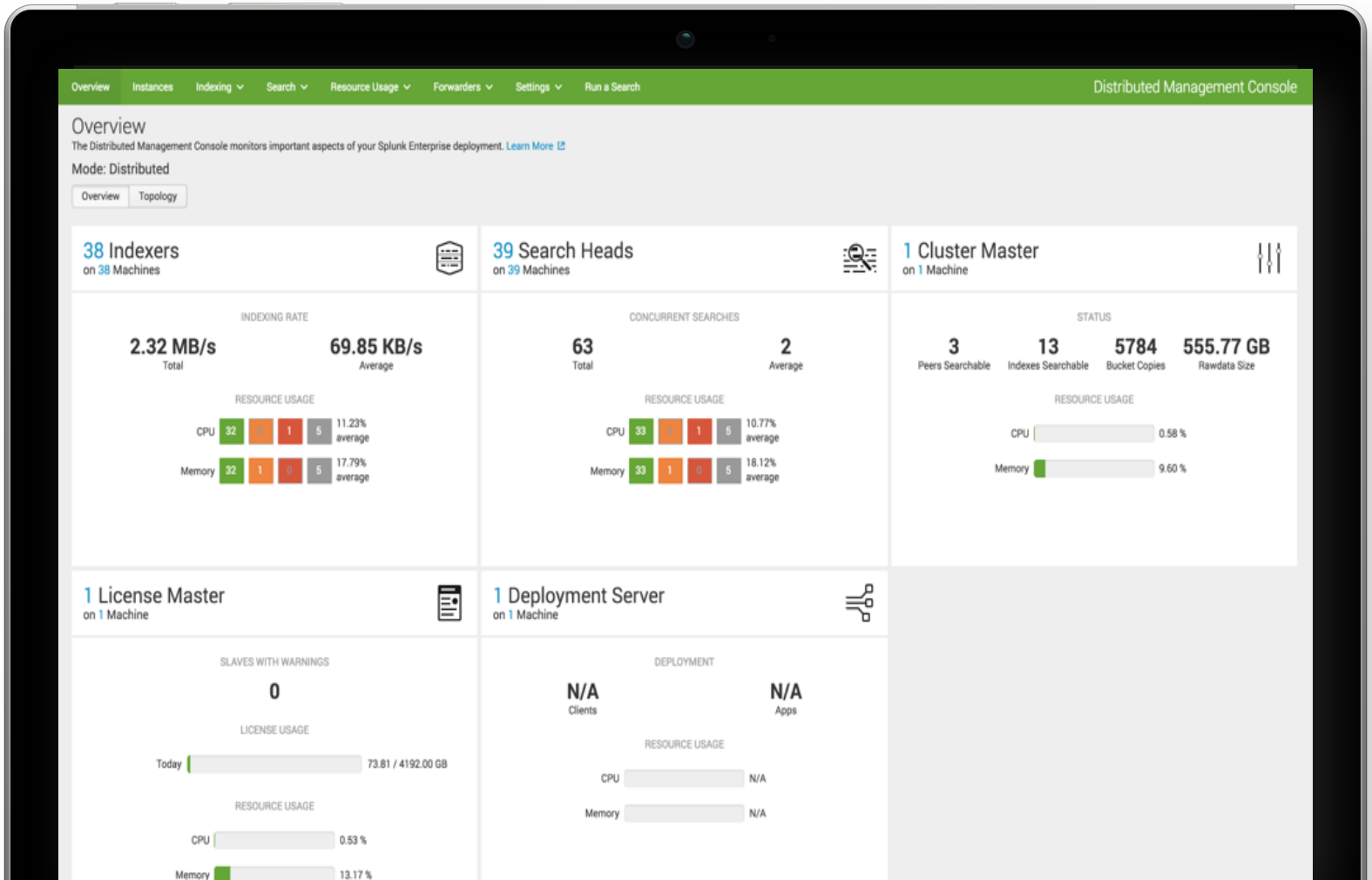
splunk> .conf2017

Taming the Beast

- Internal Splunk metrics will assist in understanding resource usage across the infrastructure
- You can choose when to charge and how to report against customer usage
- Splunk architecture is flexible, but considering how to chargeback may help to define index layouts or naming conventions



On-Premise: Monitoring Console



The data necessary for chargebacks is available via Splunk Core and easily attained through the Splunk Monitoring Console (aka Distributed Management Console).

splunk> .conf2017

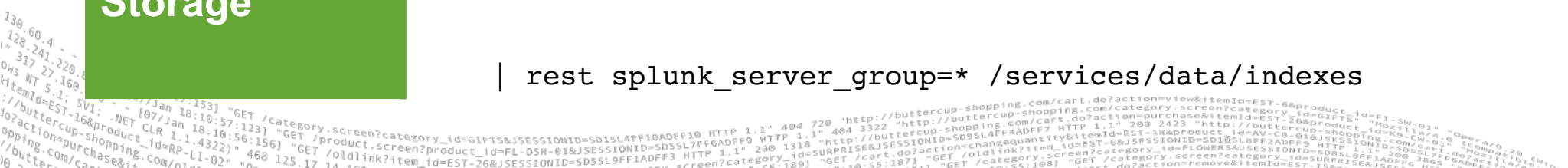
Splunk Internals Overview

Component	Relevant Search

Search	Search statistics can be used to calculate cumulative runtime per user or for groups of users
	
	`index=_audit sourcetype=audittrail`
	OR
	`` `dmc_audit_get_searches_for_groups(*)` ``

License	License Usage statistics can be split by license pool, host, source, sourcetype, or index
	
	`index=_internal source=*license_usage.log type=Usage`
	OR
	`` `dmc_licensing_base_usage(*,"")` ``

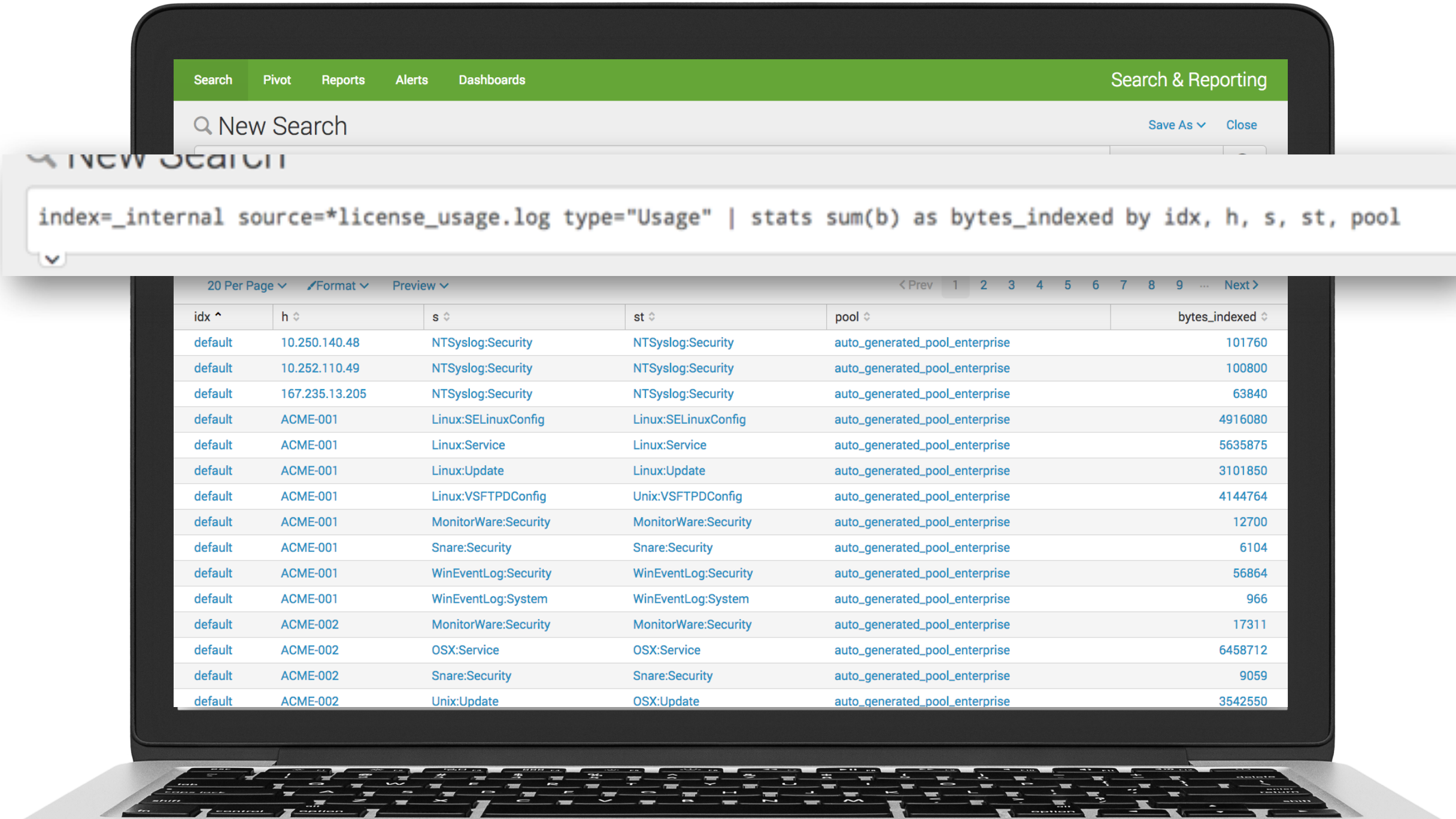
Storage	Disk utilization may vary versus indexing rate. Index sizes can be captured via REST calls. `| rest splunk_server_group=* /services/data/indexes`



splunk> .conf2017

License Utilization

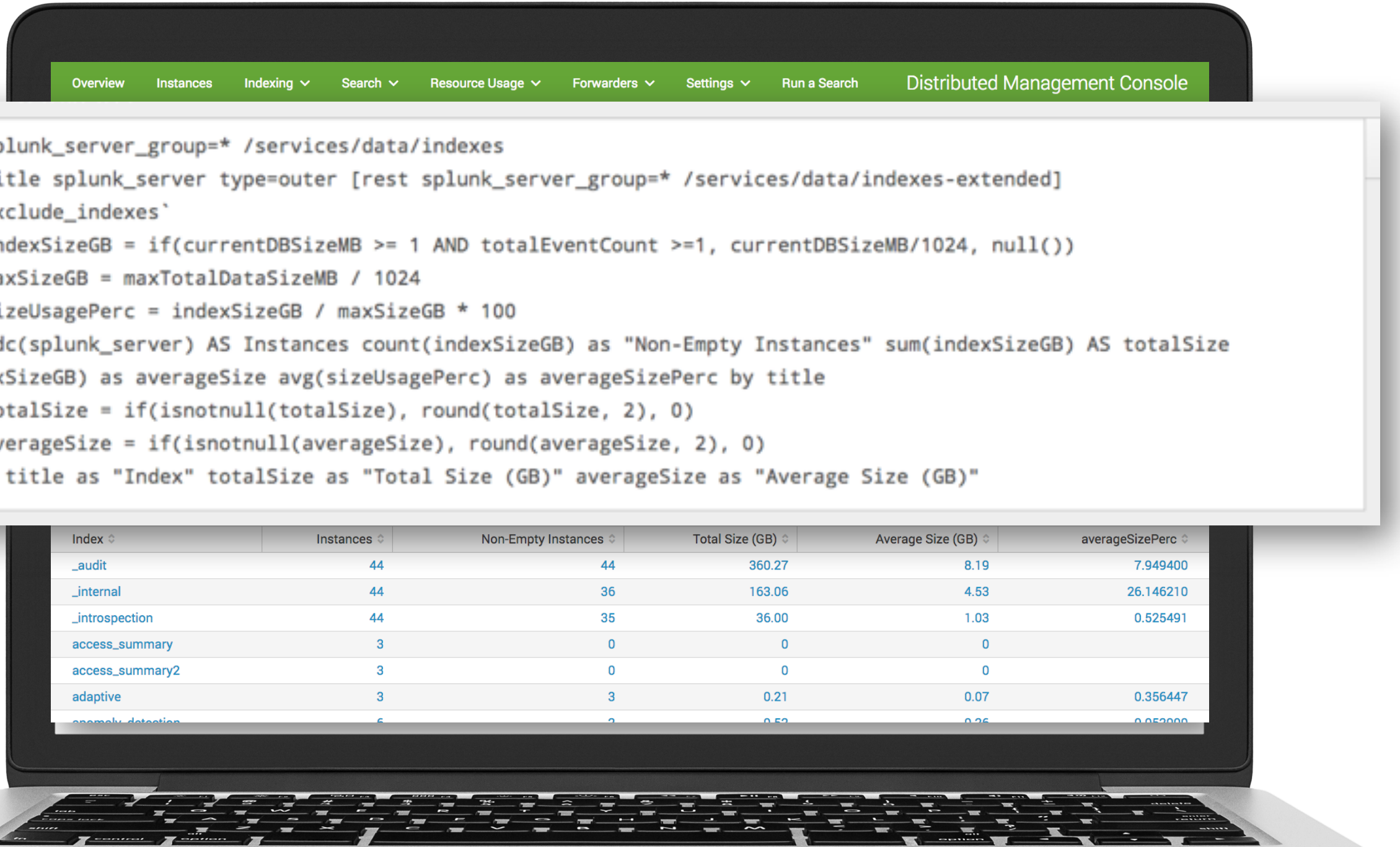
- Monitoring the indexing rate within the infrastructure
- Direct recoupment of Splunk license fees
- Useful when infrastructure growth can be attirbuted primarily to data ingest
- Flexible and granular ability to split license cost against:
  - Types of data
  - Hosts
  - Specific data sources
  - Assigned indexers
  - Some combination of those factors



idx	h	s	st	pool	bytes_indexed
default	10.250.140.48	NTSyslog:Security	NTSyslog:Security	auto_generated_pool_enterprise	101760
default	10.252.110.49	NTSyslog:Security	NTSyslog:Security	auto_generated_pool_enterprise	100800
default	167.235.13.205	NTSyslog:Security	NTSyslog:Security	auto_generated_pool_enterprise	63840
default	ACME-001	Linux:SELinuxConfig	Linux:SELinuxConfig	auto_generated_pool_enterprise	4916080
default	ACME-001	Linux:Service	Linux:Service	auto_generated_pool_enterprise	5635875
default	ACME-001	Linux:Update	Linux:Update	auto_generated_pool_enterprise	3101850
default	ACME-001	Linux:VSFTPDConfig	Unix:VSFTPDConfig	auto_generated_pool_enterprise	4144764
default	ACME-001	MonitorWare:Security	MonitorWare:Security	auto_generated_pool_enterprise	12700
default	ACME-001	Snare:Security	Snare:Security	auto_generated_pool_enterprise	6104
default	ACME-001	WinEventLog:Security	WinEventLog:Security	auto_generated_pool_enterprise	56864
default	ACME-001	WinEventLog:System	WinEventLog:System	auto_generated_pool_enterprise	966
default	ACME-002	MonitorWare:Security	MonitorWare:Security	auto_generated_pool_enterprise	17311
default	ACME-002	OSX:Service	OSX:Service	auto_generated_pool_enterprise	6458712
default	ACME-002	Snare:Security	Snare:Security	auto_generated_pool_enterprise	9059
default	ACME-002	Unix:Update	OSX:Update	auto_generated_pool_enterprise	3542550

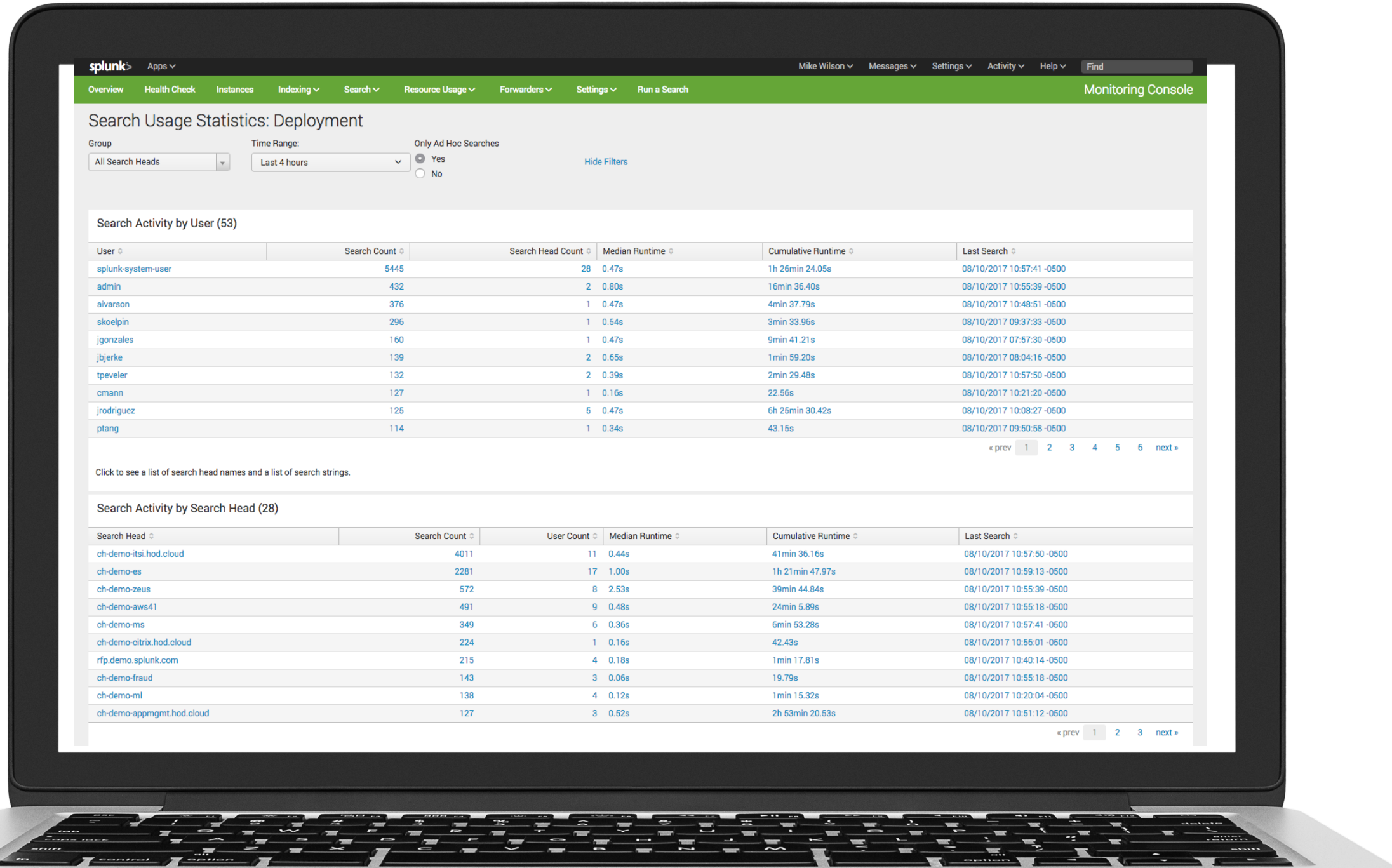
Storage Utilization

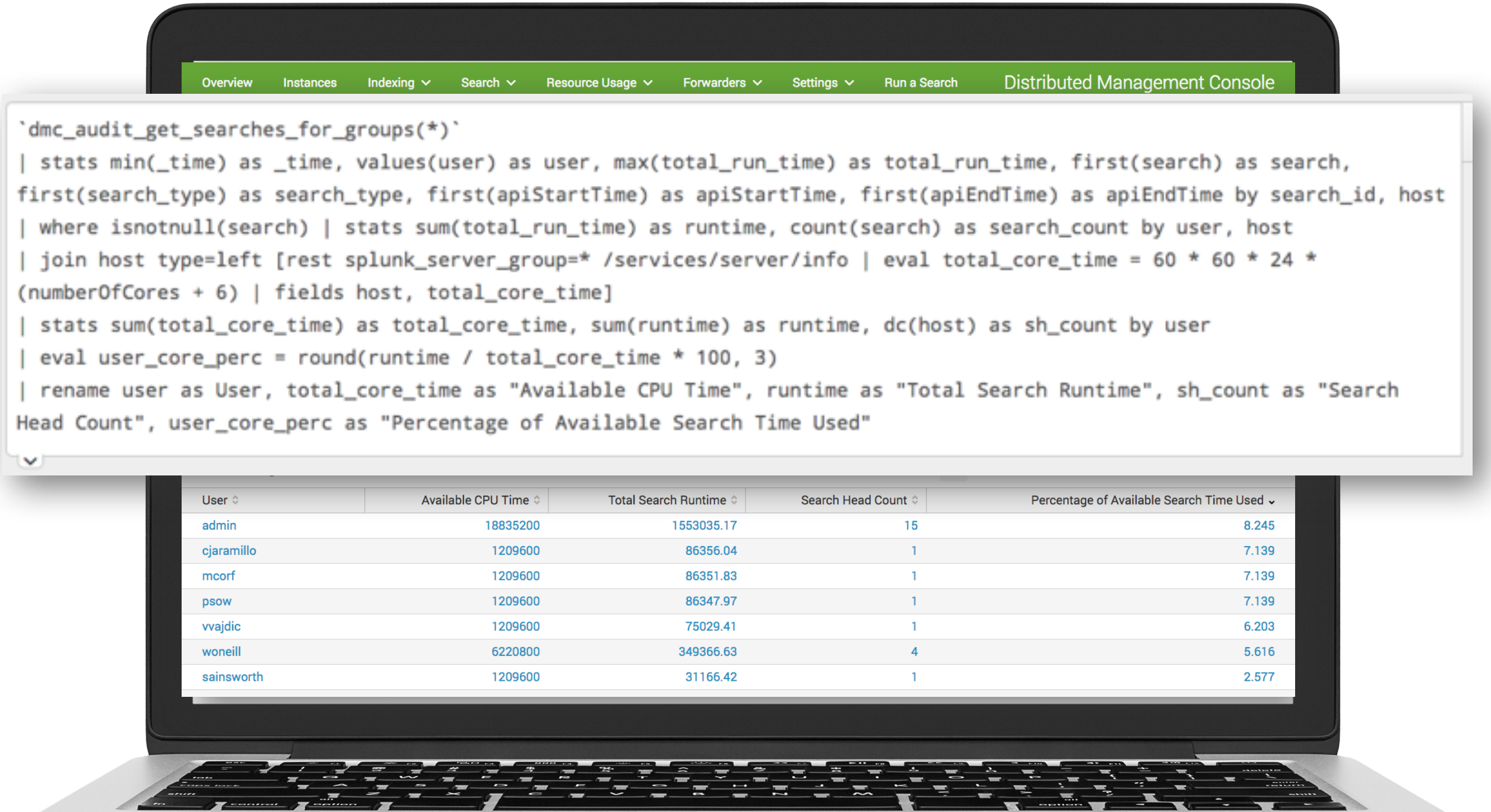
- Monitoring individual or aggregate index sizes and/or capacity
- Provides understanding of impact on storage cost
- Useful when indexes can be mapped to specific customers
- Account for usage outside of just ingest:
  - Accelerated data models
  - Summary indexing
  - Data retention needs
  - Replicated buckets



Search Utilization

- Monitoring searches against available capacity
- Recoupment of Splunk infrastructure costs
- Works well for customers with low indexing rates, but high search volume
- Provides a depiction of system resource utilization within the environment
- Cost can be associated with the number of searches or of search runtime as a flat fee or as a percentage of total or relative capacity
- Cost can be increased for peak hour workloads and discounted in off-peak hours in order to discourage or incentivize users to schedule within specific time windows
- May target users, apps, or search name





Grouping to Cost Centers

- Utilizing lookups allows you to group units of usage together and assign costs:
  - Map users, data sources, indexes, and other units to chargeable organizations and usage allocations
  - Associate a dollar value with search, license, or storage usage

- Example: associate index with group and license volume

Edit Lookup File

Import from CSV file: Choose File No file chosen

customers.csv

Right-click the table cells for more editing options

Revision: Current version

	group	idx	max_lic_GB	percent_ownership
2	Unix	os	3	50
3	Development Team	os	3	30
4	Marketing	icloud	2.25	100
5	Marketing	stocks	2.25	100

Customer-wide Services

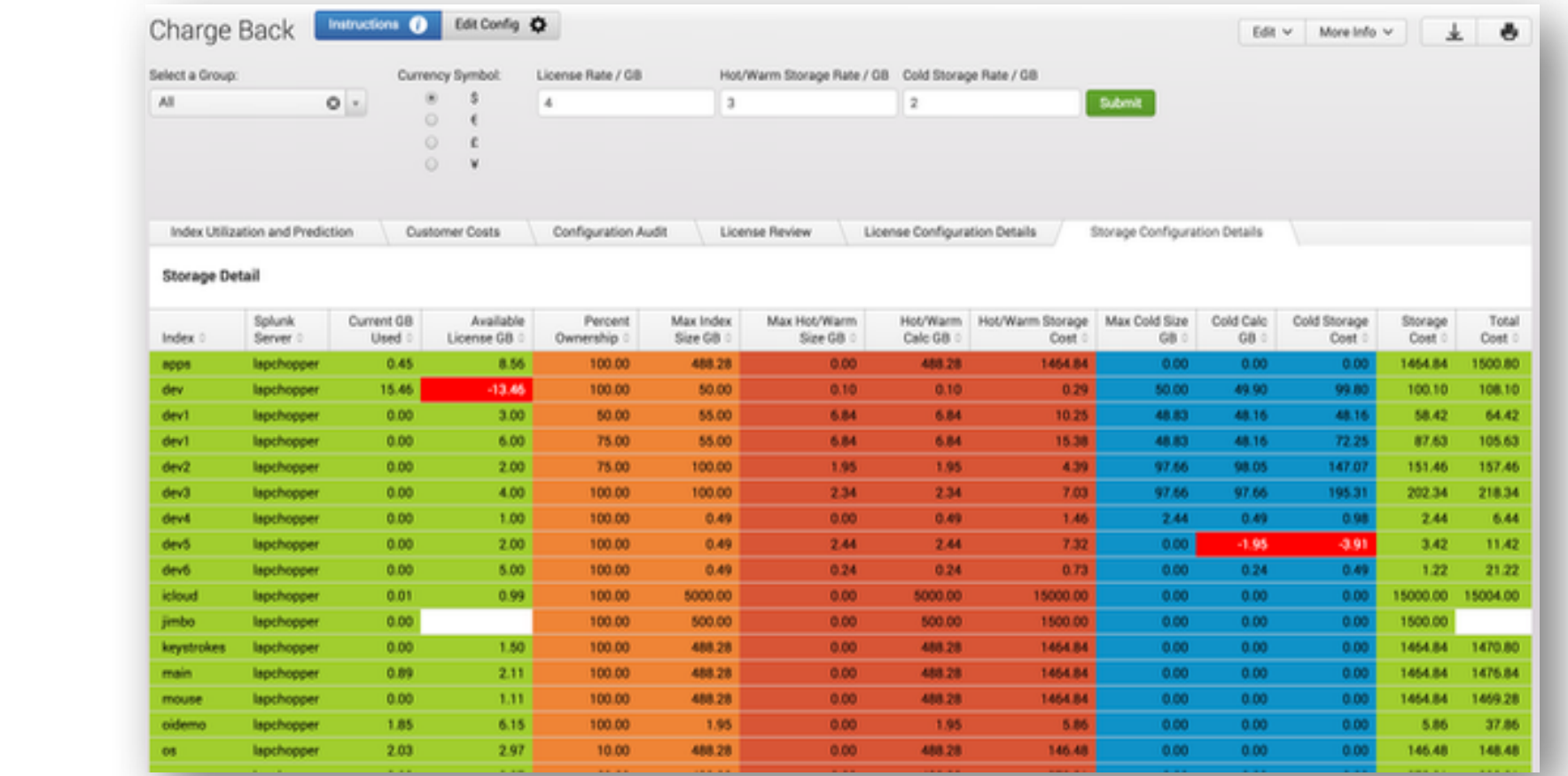
- Some usage will be in the best interest of the entire customer base
  - Summary indexing
  - Lookup generation
  - Knowledge object creation (e.g. macros)
  - Custom integrations

- Consider whether you'd want to charge for these or not
  - Will you increase cost units across the board to account for this?
  - Is this a beneficial service which actually helps to save resources (e.g. increases search speeds, alleviates support burden, etc)?

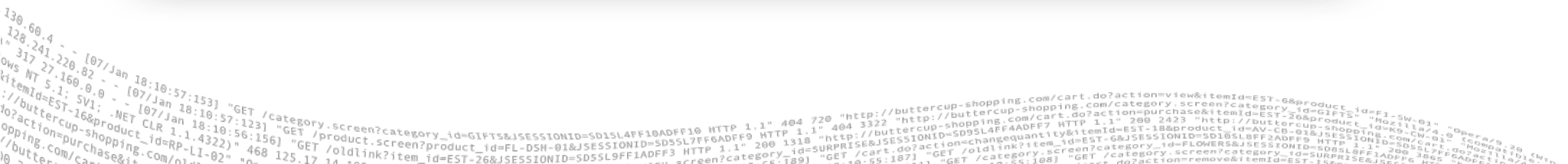
Best Practices

- Summary indexing should be used in order to capture metrics, this enables:
  - Access to a wider internal audience via RBAC
  - Long term reporting without the need to extend internal log retention
  - The ability to save data and calculate growth for storage metrics gathered via REST
- Use data enrichment (e.g. lookups) to group to cost centers
- Ensure that the DMC, License Master, and Search Heads are forwarding data back to the indexing tier
- Chargebacks should not discourage use. Value derived could be used as showback/credits
- Use all three methods together

On-Premise: Chargeback App



Index	Splunk Server	Current GB Used	Available License GB	Percent Ownership	Max Index Size GB	Max Hot/Warm Size GB	Hot/Warm Calc GB	Hot/Warm Storage Cost	Max Cold Size GB	Cold Calc GB	Cold Storage Cost	Storage Cost	Total Cost
apps	lapchopper	0.45	8.56	100.00	488.28	0.00	488.28	1464.84	0.00	0.00	0.00	1464.84	1500.80
dev	lapchopper	15.46	-13.46	100.00	50.00	0.10	0.10	0.29	50.00	49.90	99.80	100.10	108.10
dev1	lapchopper	0.00	3.00	50.00	55.00	6.84	6.84	10.25	48.83	48.16	48.16	58.42	64.42
dev1	lapchopper	0.00	6.00	75.00	55.00	6.84	6.84	15.38	48.83	48.16	72.25	87.63	105.63
dev2	lapchopper	0.00	2.00	75.00	100.00	1.95	1.95	4.39	97.66	98.05	147.07	151.46	157.46
dev3	lapchopper	0.00	4.00	100.00	100.00	2.34	2.34	7.03	97.66	97.66	195.31	202.34	218.34
dev4	lapchopper	0.00	1.00	100.00	0.49	0.00	0.49	1.46	2.44	0.49	0.98	2.44	6.44
dev5	lapchopper	0.00	2.00	100.00	0.49	2.44	2.44	7.32	0.00	-1.95	-3.91	3.42	11.42
dev6	lapchopper	0.00	5.00	100.00	0.49	0.24	0.24	0.73	0.00	0.24	0.49	1.22	21.22
icloud	lapchopper	0.01	0.99	100.00	5000.00	0.00	5000.00	15000.00	0.00	0.00	0.00	15000.00	15004.00
jimbo	lapchopper	0.00		100.00	500.00	0.00	500.00	1500.00	0.00	0.00	0.00	1500.00	
keystrokes	lapchopper	0.00	1.50	100.00	488.28	0.00	488.28	1464.84	0.00	0.00	0.00	1464.84	1470.80
main	lapchopper	0.89	2.11	100.00	488.28	0.00	488.28	1464.84	0.00	0.00	0.00	1464.84	1475.84
mouse	lapchopper	0.00	1.11	100.00	488.28	0.00	488.28	1464.84	0.00	0.00	0.00	1464.84	1469.28
oidemo	lapchopper	1.85	6.15	100.00	1.95	0.00	1.95	5.86	0.00	0.00	0.00	5.86	37.86
os	lapchopper	2.03	2.97	10.00	488.28	0.00	488.28	146.48	0.00	0.00	0.00	146.48	148.48



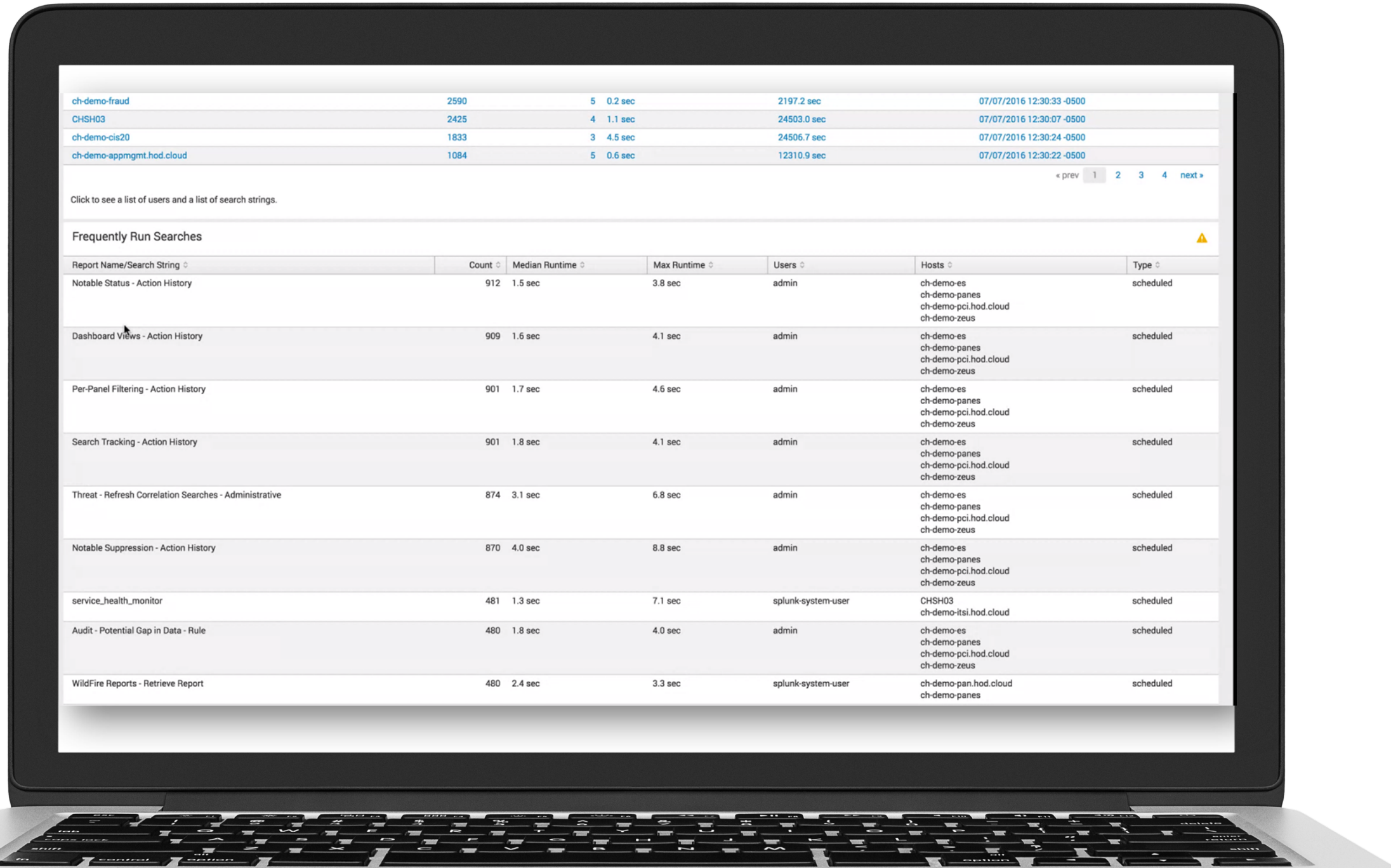
By Jim Donn

The Chargeback App
Wednesday, September 28, 2016 | 11:00 AM-11:45 AM

splunk> .conf2017

Chargebacks for Other Services

- Identify where cost is incurred
  - E.g. licenses, hardware, services
- Identify measurable metrics which relate directly to the utilization and cost of the system
  - E.g. CPU cores, users, count of queries, servers, etc
- Capture metrics within Splunk
- Use data enrichment to associate responsible groups with cost centers
- Profit! (save money)



ch-demo-fraud	2590	5	0.2 sec	2197.2 sec	07/07/2016 12:30:33 -0500
CHSH03	2425	4	1.1 sec	24503.0 sec	07/07/2016 12:30:07 -0500
ch-demo-cis20	1833	3	4.5 sec	24506.7 sec	07/07/2016 12:30:24 -0500
ch-demo-appmgmt.hod.cloud	1084	5	0.6 sec	12310.9 sec	07/07/2016 12:30:22 -0500

« prev 1 2 3 4 next »

Click to see a list of users and a list of search strings.

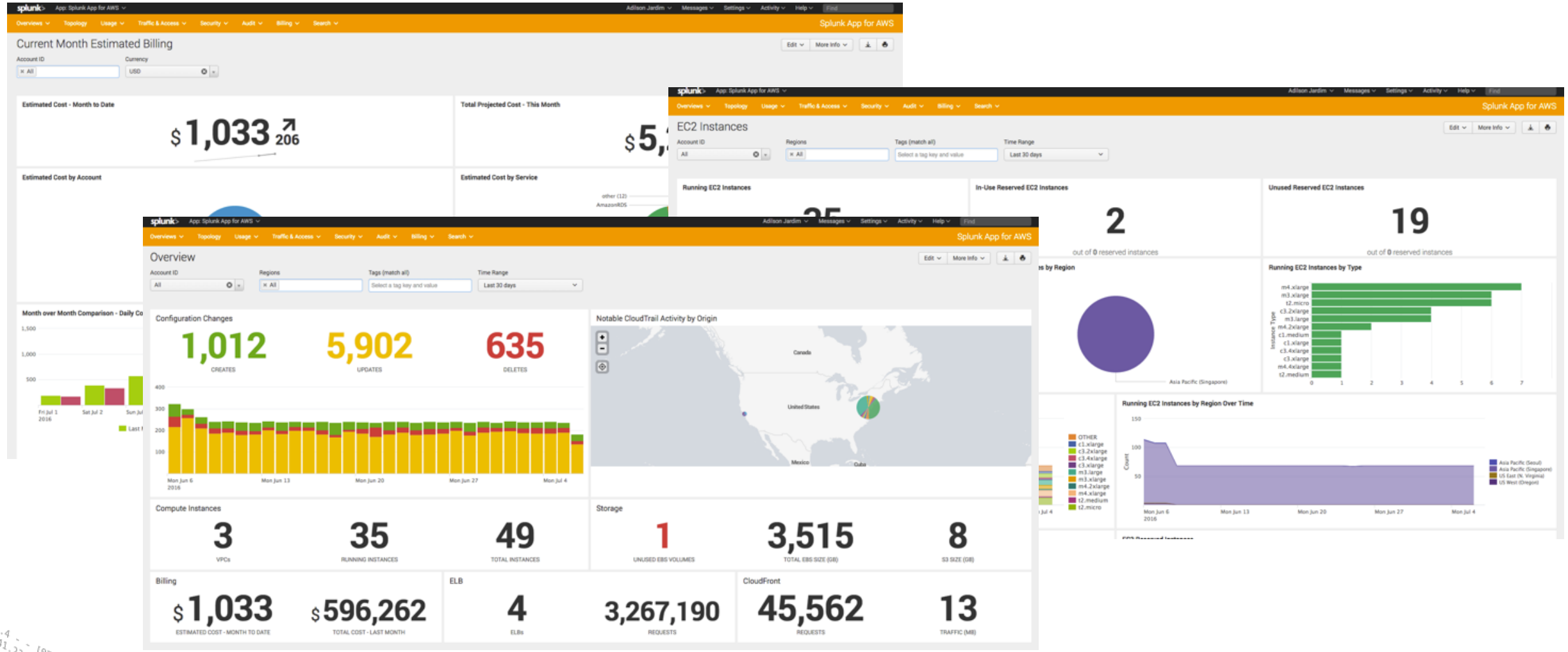
Frequently Run Searches

Report Name/Search String	Count	Median Runtime	Max Runtime	Users	Hosts	Type
Notable Status - Action History	912	1.5 sec	3.8 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
Dashboard Views - Action History	909	1.6 sec	4.1 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
Per-Panel Filtering - Action History	901	1.7 sec	4.6 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
Search Tracking - Action History	901	1.8 sec	4.1 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
Threat - Refresh Correlation Searches - Administrative	874	3.1 sec	6.8 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
Notable Suppression - Action History	870	4.0 sec	8.8 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
service_health_monitor	481	1.3 sec	7.1 sec	splunk-system-user	CHSH03 ch-demo-itsi.hod.cloud	scheduled
Audit - Potential Gap in Data - Rule	480	1.8 sec	4.0 sec	admin	ch-demo-es ch-demo-panes ch-demo-pci.hod.cloud ch-demo-zeus	scheduled
WildFire Reports - Retrieve Report	480	2.4 sec	3.3 sec	splunk-system-user	ch-demo-pan.hod.cloud ch-demo-panes	scheduled

Measuring Cloud Services Splunk App for AWS

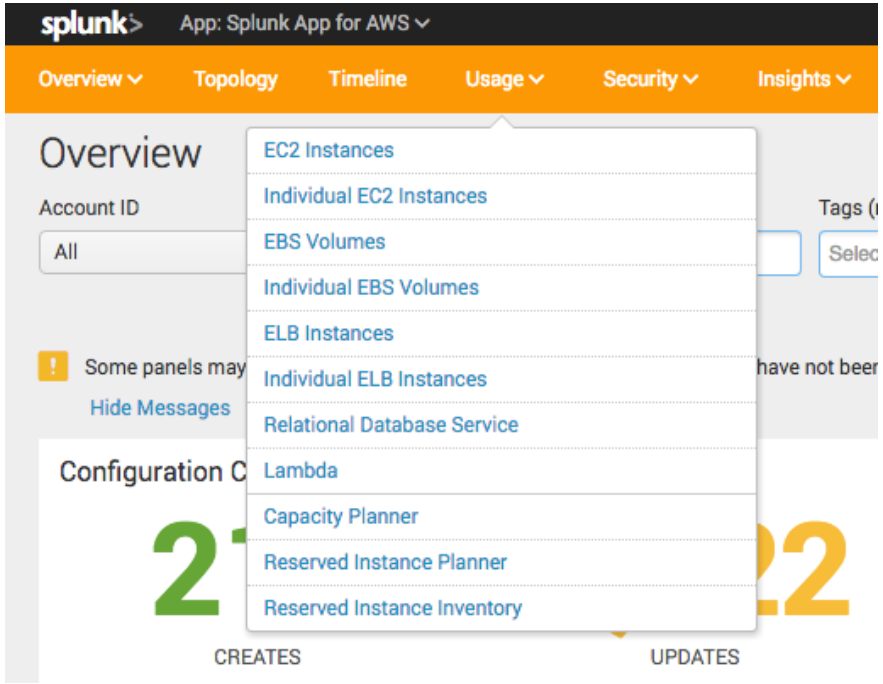
splunk> .conf2017

Cloud: AWS App

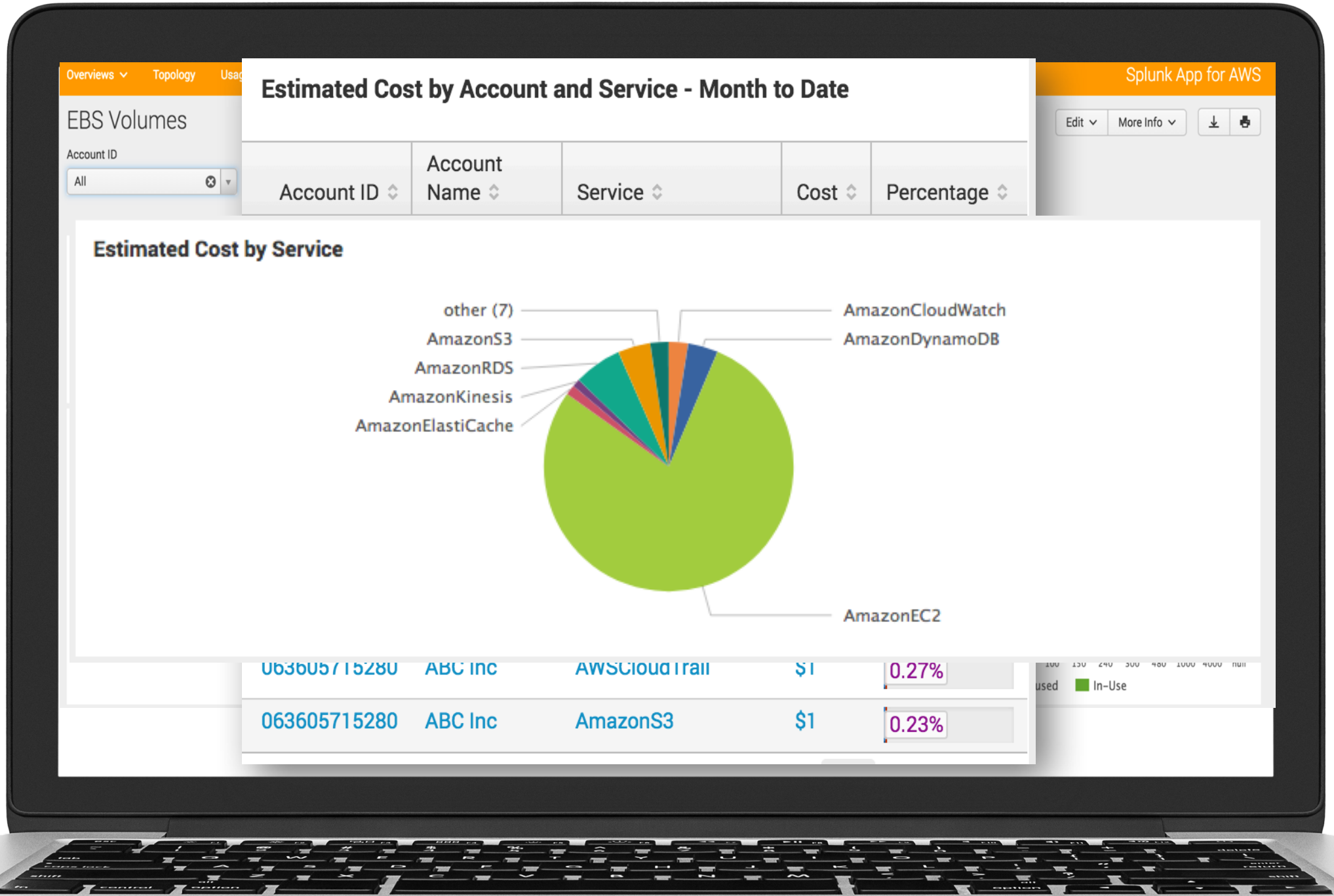


splunk> .conf2017

Quantifying Usage



Metered Component	Function
EC2	Compute & Application
EBS	Storage
ELB	Load Balancing
Capacity Planner	Intended growth / chargeback modeling
Database Service	Storage / Data management



Charging for service

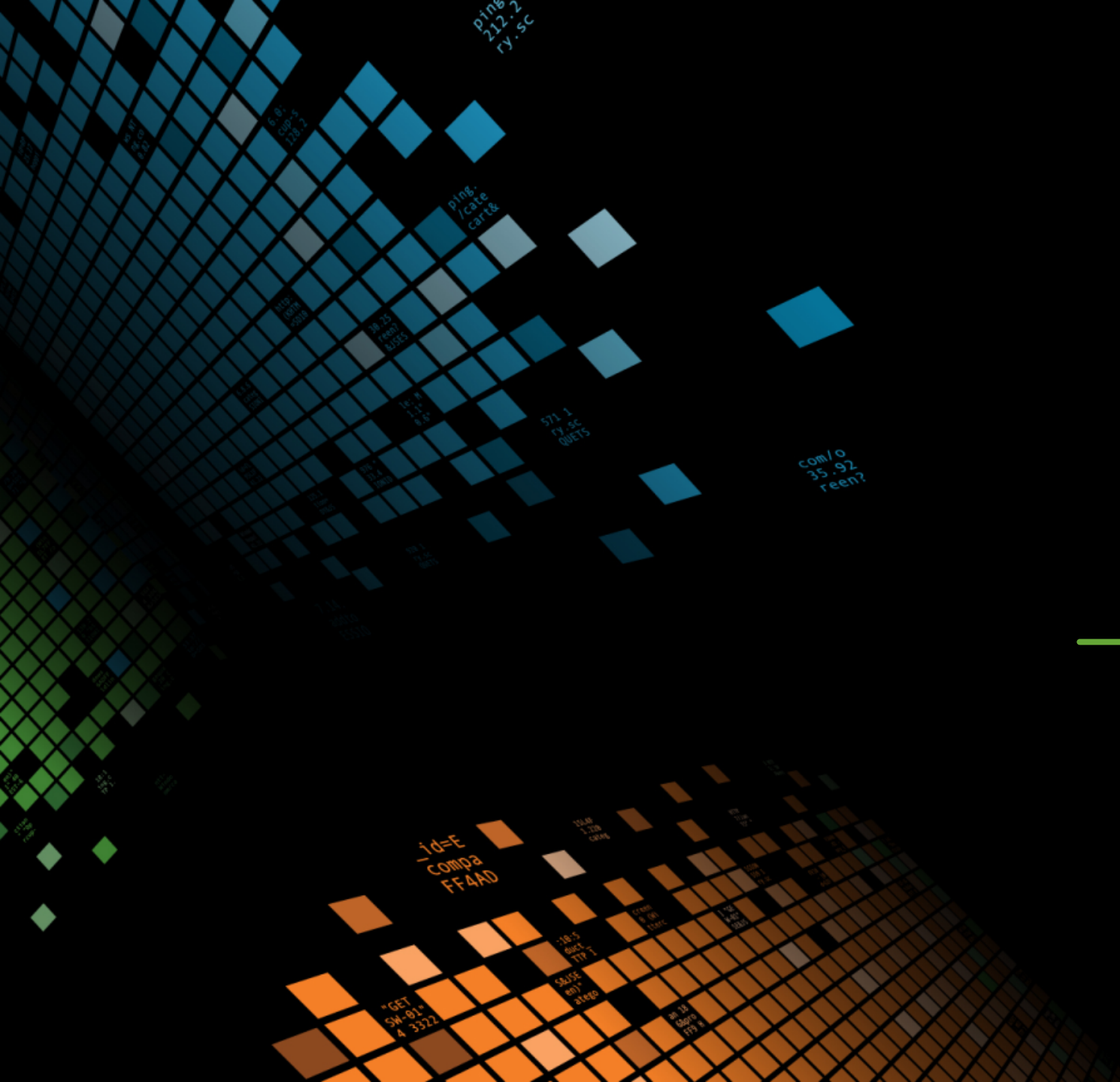
splunk> .conf2017

Quantifying Usage

Estimated Cost by Account and Service - Month to Date

Account ID	Account Name	Service	Cost	Percentage
063605715280	ABC Inc	AmazonEC2	$504	93.56%
063605715280	ABC Inc	AWSDirectoryService	$7	1.22%
063605715280	ABC Inc	AmazonCloudFront	$6	1.14%
063605715280	ABC Inc	AWSDataTransfer	$6	1.07%
063605715280	ABC Inc	AmazonRDS	$5	1.02%
063605715280	ABC Inc	AmazonSimpleDB	$4	0.68%
063605715280	ABC Inc	AmazonElastiCache	$2	0.30%
063605715280	ABC Inc	AmazonKinesis	$2	0.28%
063605715280	ABC Inc	AWSCloudTrail	$1	0.27%
063605715280	ABC Inc	AmazonS3	$1	0.23%

Service	Type	Metrics	Cost Basis
Dashboard	Fixed	# of users	Actual cost + service fee
Storage	Variable	Disk storage by hot/cold buckets	$/GB + service fee



Searches

splunk> .conf2017

Search Appendix

- Search statistics from DMC

```
`dmc_audit_get_searches_for_groups(*)`
  | stats min(_time) as _time, values(user) as user, max(total_run_time) as
total_run_time, first(search) as search, first(search_type) as search_type,
first(apiStartTime) as apiStartTime, first(apiEndTime) as apiEndTime by search_id, host
  | where isnotnull(search)
  | stats sum(total_run_time) as runtime, count(search) as search_count by user, host
  | join host type=left [rest splunk_server_group=* /services/server/info | eval
total_core_time = 60 * 60 * 24 * (numberOfCores + 6) | fields host, total_core_time]
  | stats sum(total_core_time) as total_core_time, sum(runtime) as runtime, dc(host) as
sh_count by user
  | eval user_core_perc = round(runtime / total_core_time * 100, 3)
  | rename user as User, total_core_time as "Available CPU Time", runtime as "Total
Search Runtime", sh_count as "Search Head Count", user_core_perc as "Percentage of
Available Search Time Used"
```

Search Appendix

- License usage statistics from core

```
index=_internal source=*license_usage.log type="Usage"
  | stats sum(b) as bytes_indexed by idx, h, s, st, pool
```

- License usage statistics from DMC

```
`dmc_licensing_base_usage(*, "")`
```

splunk> .conf2017

Search Appendix

- Storage statistics from DMC

```
| rest splunk_server_group=* /services/data/indexes
  | join title splunk_server type=outer [rest splunk_server_group=*
/services/data/indexes-extended]
  | `dmc_exclude_indexes`
  | eval indexSizeGB = if(currentDBSizeMB >= 1 AND totalEventCount >=1,
currentDBSizeMB/1024, null())
  | eval maxSizeGB = maxTotalDataSizeMB / 1024
  | eval sizeUsagePerc = indexSizeGB / maxSizeGB * 100
  | stats dc(splunk_server) AS Instances count(indexSizeGB) as "Non-Empty Instances"
sum(indexSizeGB) AS totalSize avg(indexSizeGB) as averageSize avg(sizeUsagePerc) as
averageSizePerc by title
  | eval totalSize = if(isnotnull(totalSize), round(totalSize, 2), 0)
  | eval averageSize = if(isnotnull(averageSize), round(averageSize, 2), 0)
  | rename title as "Index" totalSize as "Total Size (GB)" averageSize as "Average Size
(GB)"
```

splunk> .conf2017

What Now?

The Chargeback App

Wednesday, September 28, 2016 | 11:00 AM-11:45 AM

GOOD FOR ALL SKILL LEVELS | **Products:** Splunk Enterprise | **Role:** Operations Manager, Administrator, Splunk Technical Champion, Business Manager | **Track:** Splunk Foundations | **Session Focus:** Managing Splunk | **Other Topics:** Best Practices, Big Data Architecture

Speakers
James Donn, Senior Sales Engineer, Splunk Inc.

Splunking AWS for End-to-end Visibility

Wednesday, September 28, 2016 | 12:05 PM-12:50 PM

BEGINNER | **Industries:** Energy & Utilities, Technology | **Products:** Splunk Cloud, Splunk Enterprise | **Role:** Operations Manager, Security Analyst | **Track:** Splunk for Operational Intelligence | **Session Focus:** Cloud Strategies | **Other Topics:** Amazon Web Services, Customer Success Story

Speakers
Randall Young, Principal Product Manager, Splunk Inc.
Qianjie Zhong, Director, Software Engineering, Splunk Inc.

splunk> .conf2017

CLOSING REMARKS & CALL TO ACTION

splunk> .conf2017

splunk> .conf2017

Public Sector & Education Industry Day at .conf2017

Wednesday, September 27th, 2017

11:00am-7:00pm | Room 202A

400+
Attendees

5
Sessions

15
Customer Speakers

10+
Birds of Feather Sessions

splunk> .conf2017

Public Sector Birds of a Feather

Meal Room (Lower Level Hall B)

Wednesday, September 27th

1:15pm-2:00pm

Compliance
Security
IT Modernization
Situational Awareness
Mission Analytics

Institutional Intelligence
Learning Analytics
Supply Chain
Smart Communities
Cloud

splunk> .conf2017

Public Sector Reception

Walter E. Washington Convention Center
South Pre-Function Space on Level 3

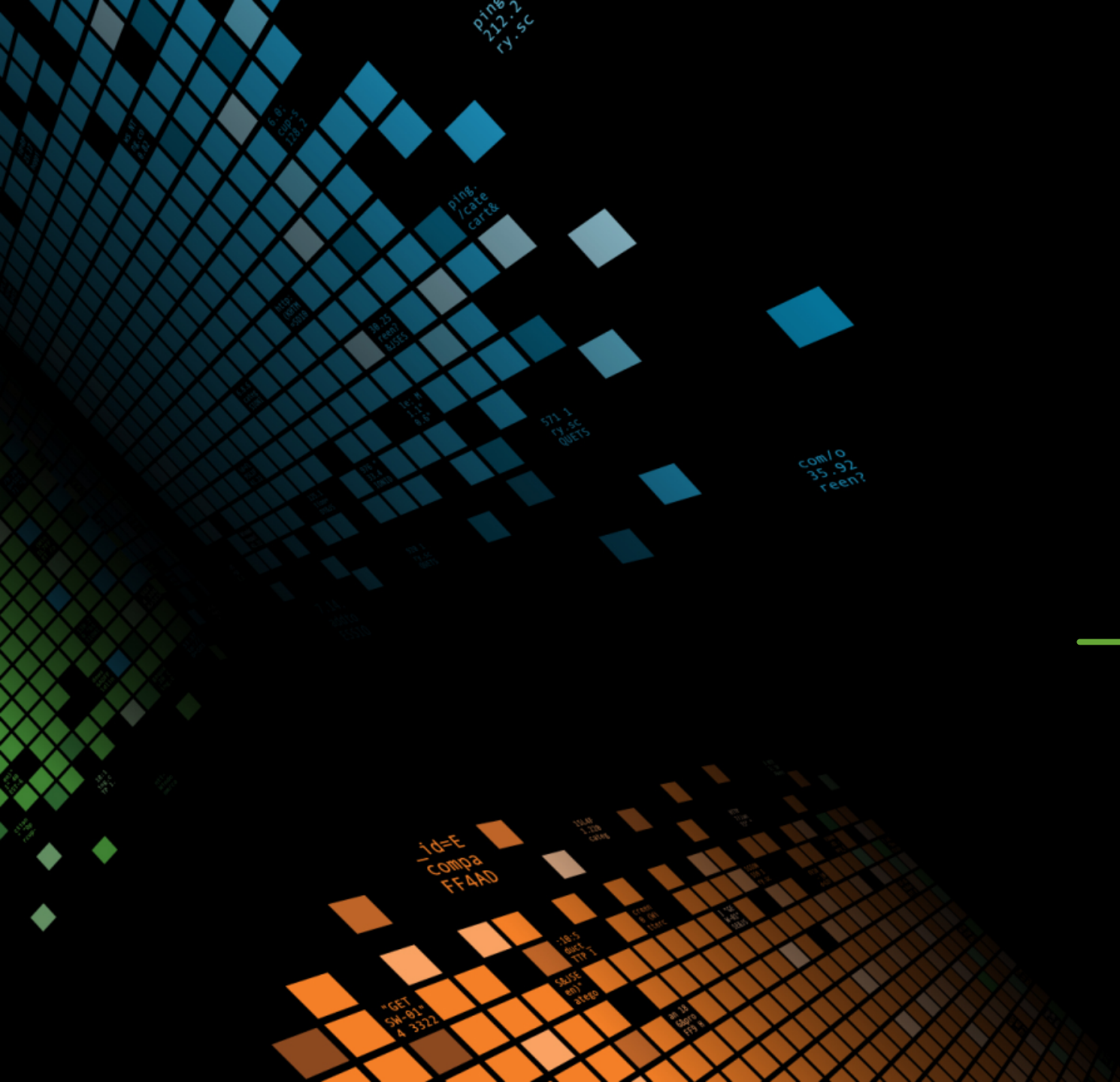
5:30pm-7:00pm

Join Splunk and your peers for hors d'oeuvres and drinks.
Unwind, discuss hot topics and share your stories!

**.conf badge required for entry*

Thank You

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



THANK YOU!

splunk> .conf2017