What's New for Splunk Enterprise and Cloud

Mark Groves

Sr. Director Product Management

Safe Harbor Statement

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 Enterprise & Cloud 6.3

Breakthrough Performance & Scale

- 2X Search & Indexing Speed
- 20-50% Increased Capacity
- 20%+ Reduced TCO

Doubles performance and lowers TCO

Advanced Analysis & Visualization

- Anomaly Detection
- Geospatial Mapping
- Single-Value Display

Simplifies analysis of large datasets

High Volume Event Collection

- HTTP Event Collector
- Developer API & SDKs
- 3rd Party Integrations

Supports DevOps and IoT data analysis at scale

Enterprise-Scale Platform

- Expanded Management
- Custom Alert Actions
- Data Integrity Control

Delivers Enterprise platform requirements

Meeting the needs of the most demanding organizations

Splunk Enterprise & Cloud 6.3

Breakthrough Performance & Scale

- 2X Search & Indexing Speed
- 20-50% Increased Capacity
- 20%+ Reduced TCO

Doubles performance and lowers TCO

Advanced Analysis & Visualization

- Anomaly Detection
- Geospatial Mapping
- Single-Value Display

Simplifies analysis of large datasets

High Volume Event Collection

- HTTP Event Collector
- Developer API & SDKs
- 3rd Party Integrations

Supports DevOps and IoT data analysis at scale

Enterprise-Scale Platform

- Expanded Management
- Custom Alert Actions
- Data Integrity Control

Delivers Enterprise platform requirements

Meeting the needs of the most demanding organizations

Breakthrough Performance, Scale, TCO

Vertical scaling maximizes use of CPU power

Search Performance
2X Execution Speed

Indexing Speed
2-4X Data Rate

Intelligent Scheduling
25%+ Capacity Gain

Total System Capacity
20-50% Increase

Improve speed of searches & reports

Onboard & analyze larger datasets

Optimize resource utilization

Reduce TCO by 20% or more

Comparisons are to Splunk Enterprise 6.2.
Customer performance and TCO will vary according to workload, configuration and available processing capacity.

So What Does Breakthrough Mean?

Release 6.3
vs.
Release 6.2

- Critical reports can be available in **¼ the time**
- It takes **20% less** indexing HW to expand or deploy Splunk
- New data is ready for analysis in **½ the time**

Release 6.3
vs.
Release 6.0

- Splunk expansion costs have dropped **over 50%** since 2013
- A new customer can deploy Splunk **using 1/3 the HW** vs. 2013
- Splunk deployment is now **½ the cost** vs. 2013

Vertical Scaling: Search & Reporting

- Multiple CPU cores can be used to execute more searches *faster*
- Common "batch-style" searches & reports can execute 2x as fast (or faster!)
- Search performance can be optimized without additional systems

Search Performance

2x Execution Speed

At least double the execution speed of most common activities

Vertical Scaling: Data Indexing

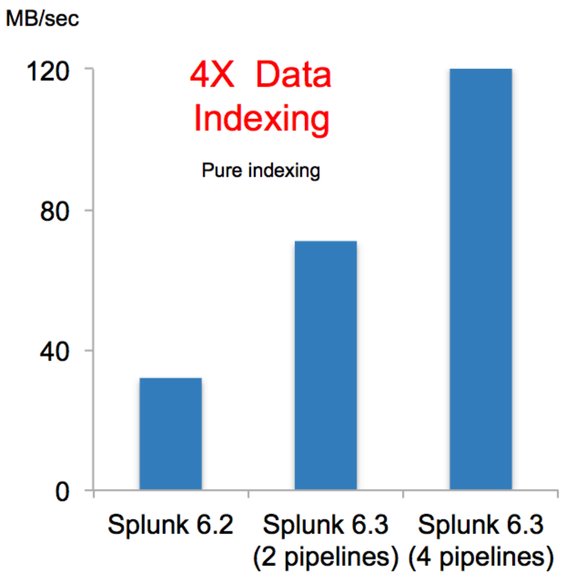
- Additional CPU cores can be used to:
  - Increase data onboarding capacity
  - Increase burst data ingestion speed by 2x or more
- The new architecture guideline is raised from 250 to 300GB/day per indexer (commodity hardware)

Onboarding Speed

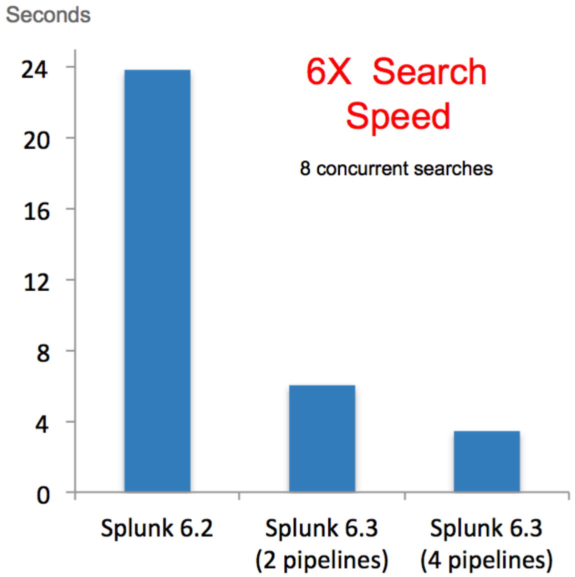
2-4x Data Rate

Increased Data Throughput With Fewer Indexers

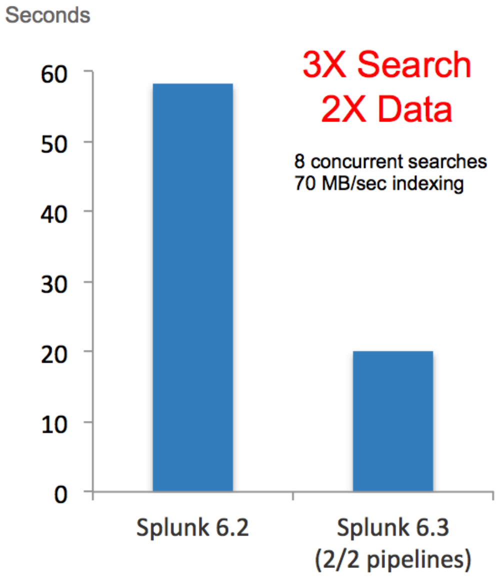
Splunk – Cisco UCS Benchmark Preview


4X Data Indexing

Pure indexing


6X Search Speed

8 concurrent searches


3X Search 2X Data

8 concurrent searches
70 MB/sec indexing

Vertical Scaling: Forwarders

- With 6.2: Using more than 4 cores requires multi-instance installation and management
- With 6.3: Use additional CPU cores (4 packs) with single instance simplicity
  - E.g. a 16 core system can now process 4X the data

Forwarder Efficiency

Simplify Forwarder Management

Deep Dive Session

Harnessing Performance and Scalability in the Next Version of Splunk

Sourav Pal & Abhinav Nekkanti

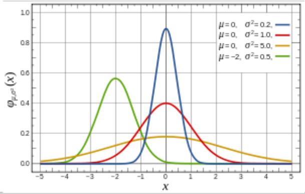
9/22 4:15PM-5:00PM

Intelligent Job Scheduling

- Simplified and more effective scheduling
- Admin can use “finish by” criteria for daily jobs
- Splunk automatically profiles workloads and controls scheduling
- Optimizes resource utilization; Reduces skipped searches
- Helps ensure timely execution of time-critical searches

Job Scheduling

Smooths workloads over time



Can Increase Capacity by 25% or More

Deep Dive Session

Making The Most Of The New Splunk Scheduler

Paul Lucas

9/23 4:15PM – 5:00PM

Splunk Enterprise & Cloud 6.3

Breakthrough Performance & Scale

- 2X Search & Indexing Speed
- 20-50% Increased Capacity
- 20%+ Reduced TCO

Doubles performance and lowers TCO

Advanced Analysis & Visualization

- Anomaly Detection
- Geospatial Mapping
- Single-Value Display

Simplifies analysis of large datasets

High Volume Event Collection

- HTTP Event Collector
- Developer API & SDKs
- 3rd Party Integrations

Supports DevOps and IoT data analysis at scale

Enterprise-Scale Platform

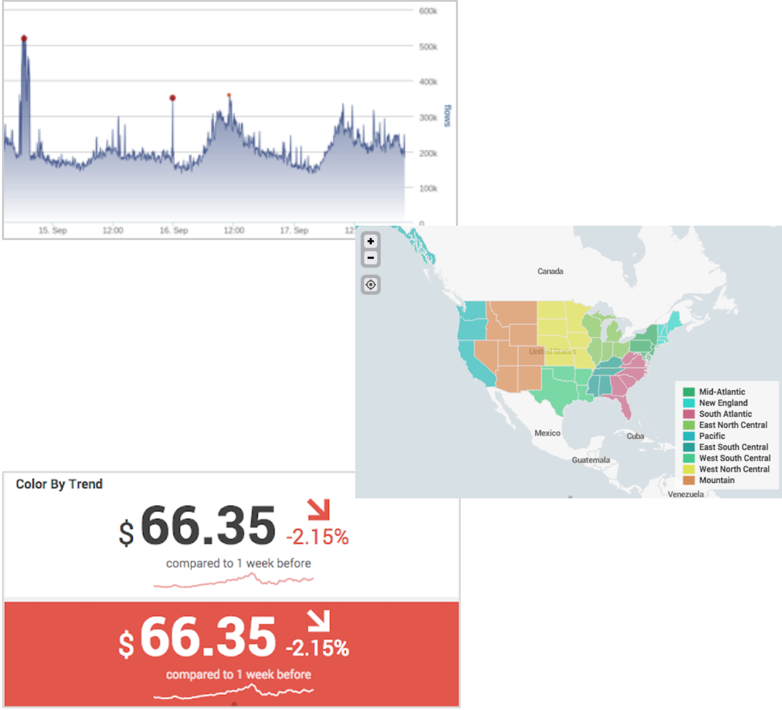
- Expanded Management
- Custom Alert Actions
- Data Integrity Control

Delivers Enterprise platform requirements

Meeting the needs of the most demanding organizations

Analysis & Visualization

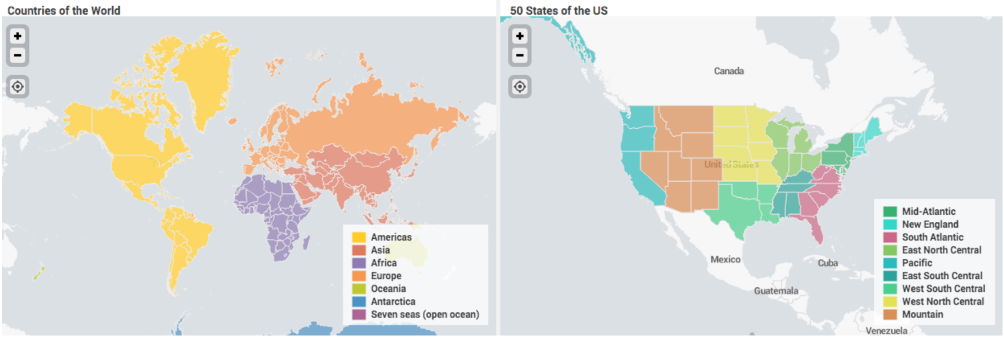
- Anomaly Detection
  - *Incorporates Z-Score, IQR & histogram methodologies in a single command*
- Geospatial Visualization
  - *Visualizes metric variance across a customizable geographic area*
- Single Value Display
  - *At-a-glance, single-value indicators with useful context*



Geospatial Visualization

Visualizes metric variance across a customizable geographic area

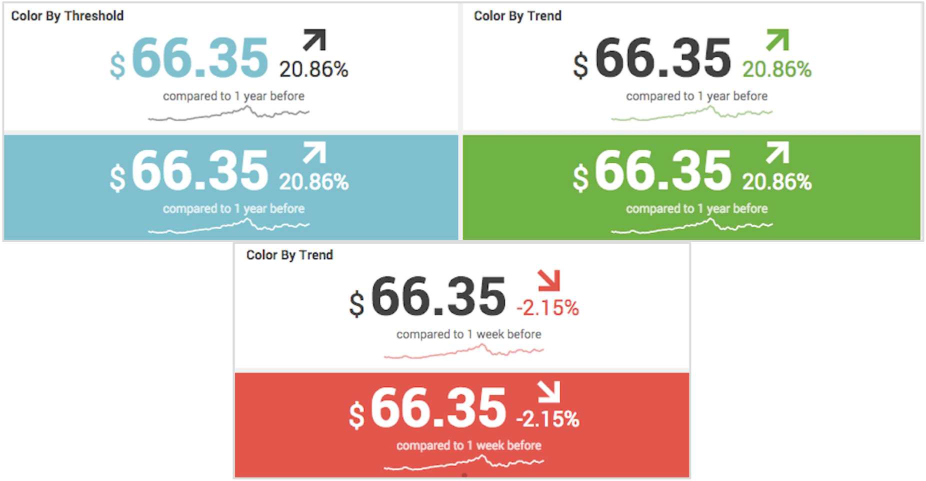
- Choropleth maps help users to easily spot spatial patterns
- Color scales can be configured per use case
- Users can upload their own geographical polygon definitions



Single Value Display

At-a-glance, single-value indicators with useful context

- Large type and prominent colors make values or changes visible, even from a distance
- Sparkline shows trends in the recent history
- Delta indicator shows changes since a previous time


Color By Threshold
$66.35 20.86%
compared to 1 year before
$66.35 20.86%
compared to 1 year before
Color By Trend
$66.35 20.86%
compared to 1 year before
$66.35 20.86%
compared to 1 year before
Color By Trend
$66.35 -2.15%
compared to 1 week before
$66.35 -2.15%
compared to 1 week before

Deep Dive Session

Paint By Number: The New Geo Visualization in Splunk

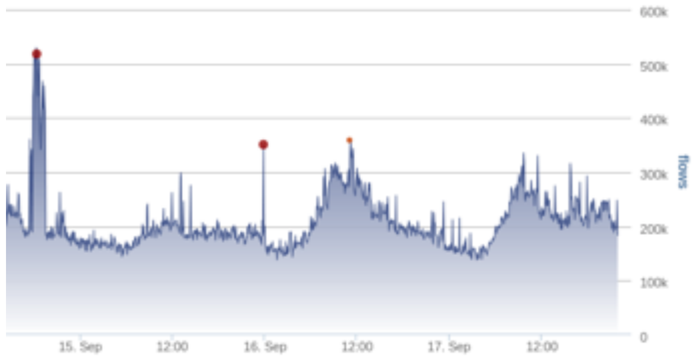
Michael Porath & Geoffrey Hendrey

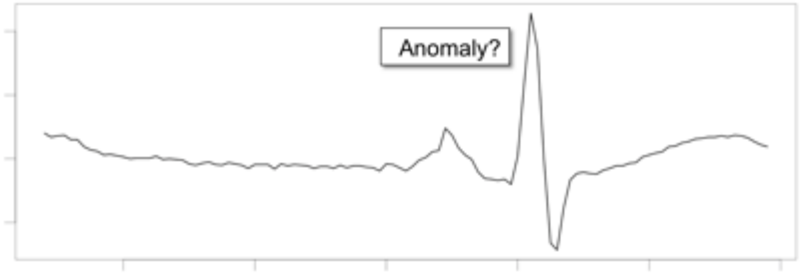
9/23 11:15AM-12:00PM

Anomaly Detection

New SPL command provides histogram-based anomaly detection

- Net new histogram-based approach offers a more accurate detection method
- Single command offers 3 options: zscore, IQR & histogram
- Replaces existing Outlier and AnomalousValue commands





Deep Dive Session

Machine Learning and Analytics in Splunk

Adam Oliner & Jacob Leverich

9/22 1:00PM-1:45PM

Splunk Enterprise & Cloud 6.3

Breakthrough Performance & Scale

- 2X Search & Indexing Speed
- 20-50% Increased Capacity
- 20%+ Reduced TCO

Doubles performance and lowers TCO

Advanced Analysis & Visualization

- Anomaly Detection
- Geospatial Mapping
- Single-Value Display

Simplifies analysis of large datasets

High Volume Event Collection

- HTTP Event Collector
- Developer API & SDKs
- 3rd Party Integrations

Supports DevOps and IoT data analysis at scale

Enterprise-Scale Platform

- Expanded Management
- Custom Alert Actions
- Data Integrity Control

Delivers Enterprise platform requirements

Meeting the needs of the most demanding organizations

HTTP Event Collector

Supports DevOps and IoT data analysis needs at scale

1. Standard API and logging libraries send events directly to Splunk
2. Libraries integrated into popular platforms and services

DevOps & Developers

AWS Lambda

docker

IoT Devices & Applications

octoblu

xively™ by LogMeIn

Scales to Millions of Events/Second

Deep Dive Sessions

Liberate your application logging!

Glenn Block & Jian Lee

9/22 5:15PM-6:00PM

HTTP Event Collector, a New Way for Developers to Send Events to Splunk - Glenn Block

9/23 10:00AM – 10:45AM

Splunk Enterprise & Cloud 6.3

Breakthrough Performance & Scale

- 2X Search & Indexing Speed
- 20-50% Increased Capacity
- 20%+ Reduced TCO

Doubles performance and lowers TCO

Advanced Analysis & Visualization

- Anomaly Detection
- Geospatial Mapping
- Single-Value Display

Simplifies analysis of large datasets

High Volume Event Collection

- HTTP Event Collector
- Developer API & SDKs
- 3rd Party Integrations

Supports DevOps and IoT data analysis at scale

Enterprise-Scale Platform

- Expanded Management
- Custom Alert Actions
- Data Integrity Control

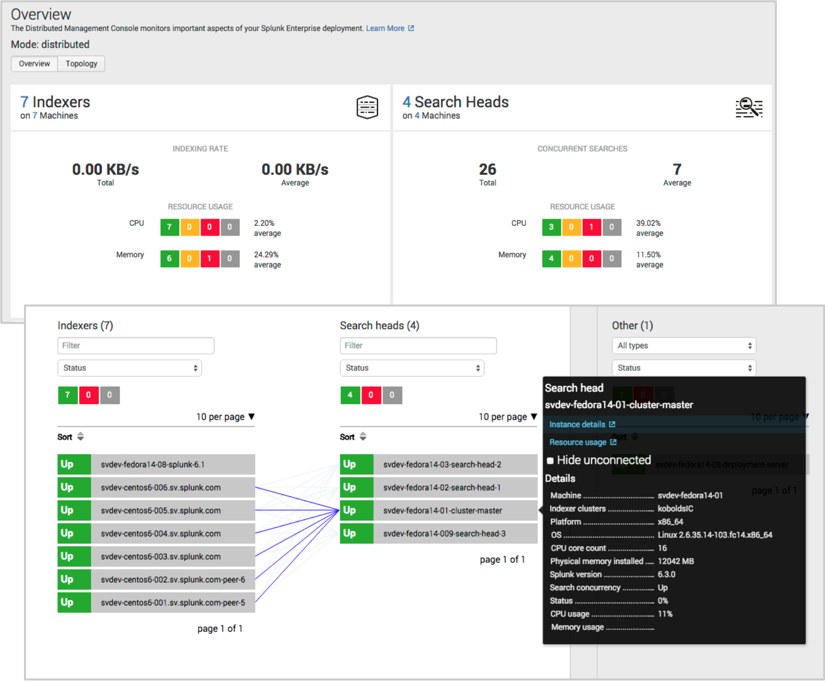
Delivers Enterprise platform requirements

Meeting the needs of the most demanding organizations

Distributed Management Console - II

New topology views, status, and alerting for Splunk deployments

- Visualizes Search Head/Indexer matrix with KPI and performance overlays
- Search Head clustering replication and scheduler views
- Forwarder views with status and performance data
- Index and metadata storage utilization
- System health alerting



Overview

The Distributed Management Console monitors important aspects of your Splunk Enterprise deployment. Learn More

Mode: distributed

7 Indexers on 7 Machines

INDEXING RATE

0.00 KB/s Total | 0.00 KB/s Average

RESOURCE USAGE

CPU	7	0	0	0	2.20% average
Memory	6	0	1	0	24.29% average

4 Search Heads on 4 Machines

CONCURRENT SEARCHES

26 Total | 7 Average

RESOURCE USAGE

CPU	3	0	1	0	39.02% average
Memory	4	0	0	0	11.50% average

Indexers (7)

Up	svdev-fedora14-08-splunk-6.1
Up	svdev-centos6-006.sv.splunk.com
Up	svdev-centos6-005.sv.splunk.com
Up	svdev-centos6-004.sv.splunk.com
Up	svdev-centos6-003.sv.splunk.com
Up	svdev-centos6-002.sv.splunk.com-peer-6
Up	svdev-centos6-001.sv.splunk.com-peer-5

page 1 of 1

Search heads (4)

Up	svdev-fedora14-03-search-head-2
Up	svdev-fedora14-02-search-head-1
Up	svdev-fedora14-01-cluster-master
Up	svdev-fedora14-009-search-head-3

page 1 of 1

Other (1)

Search head

svdev-fedora14-01-cluster-master

■ Hide unconnected

Details

```
Machine ................................ svdev-fedora14-01
Indexer clusters ..................... koboldsIC
Platform ................................ x86_64
OS ........................................ Linux 2.6.35.14-103.fc14.x86_64
CPU core count ...................... 16
Physical memory installed ..... 12042 MB
Splunk version ........................ 6.3.0
Search concurrency ............... Up
Status .................................... 0%
CPU usage .............................. 11%
Memory usage .......................
```

Deep Dive Session

Splunk Distributed Management Console: New Views for the DMC in the next version of Splunk

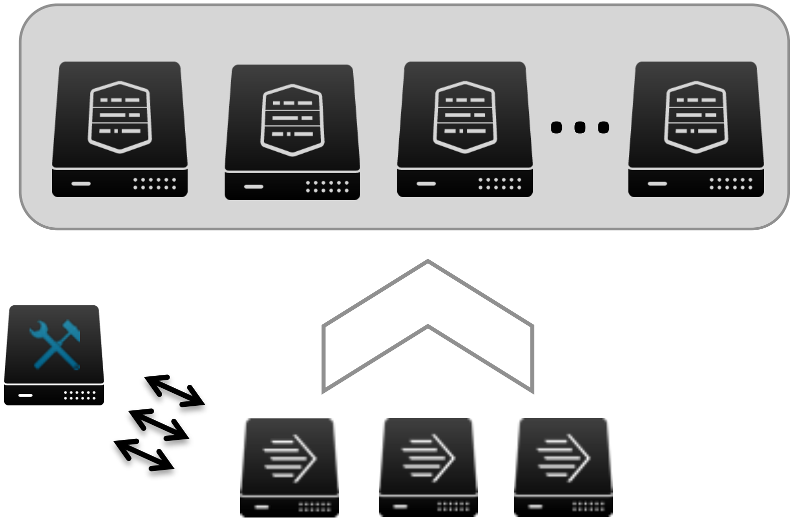
Octavio Di Sciullo & Patrick Ogdin

9/22 5:15PM-6:00PM

Indexer Auto-Discovery

Simplifies Forwarders management in a dynamic environment

- Cluster master maintains dynamic Indexer list accessed by Forwarders
- Indexers can be added/removed without affecting Forwarder configuration or operation



Data Integrity Control

Helps Ensure data fidelity; Meets GPG13 compliance requirements

- Hash signatures of selected index data are saved at regular intervals
- Intervals can be validated by the admin
- Meets security and compliance requirements by verifying that data has not been tampered with
- Hashes can be exported to further ensure security

Deep Dive Session

Clustered Index Integrity Check

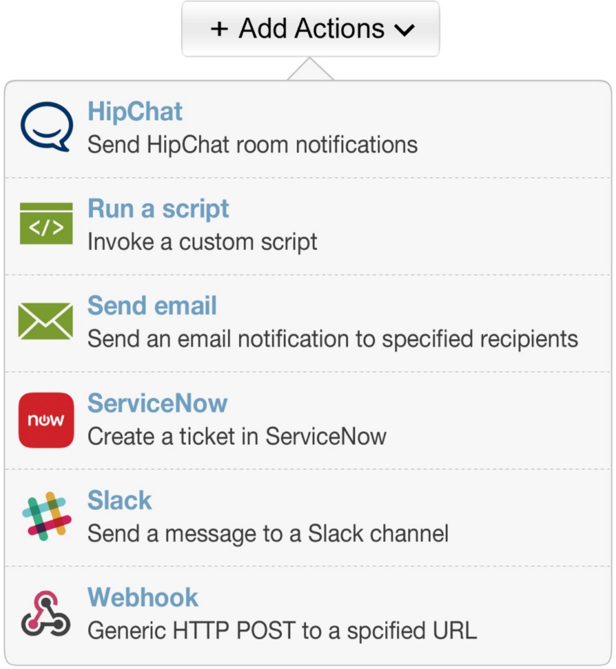
Dhruva Bhagi

9/22 1:00PM – 1:20PM

Custom Alert Actions

Use Splunk Alerts to trigger & automate workflows

- Allows packaged integration with third-party applications
- Simple admin/user configuration
- Developers can build, package, and publish alert actions within an app
- Growing list of integrations available



HipChat
Send HipChat room notifications

Run a script
Invoke a custom script

Send email
Send an email notification to specified recipients

ServiceNow
Create a ticket in ServiceNow

Slack
Send a message to a Slack channel

Webhook
Generic HTTP POST to a spcified URL

Alert Action Examples

- Notification Services
  - Send message to IM clients (HipChat, Slack)
  - Send SMS
- Incident Remediation / Ticketing
  - Automate the creation of tickets (ServiceNow, Jira)
- IT Monitoring
  - Send incident/alert into monitoring tools (xMatters, BigPanda)
- Security
  - Take action or send events to firewalls, devices, management consoles
- Internet-of-Things
  - Trigger device-level actions (change lights, sounds an alarm, send action to device)
- Custom Action
  - Trigger any organization-specific action (restart application, integrate with homegrown service, and more)

Eco-system Partners

(x) matters®

servicenow

octoblu

Now a part of Citrix

bigpanda

twilio™

Deep Dive Session

Creating and Using Custom Alert Actions

Nicholas Filippi & Siegfried Puchbauer

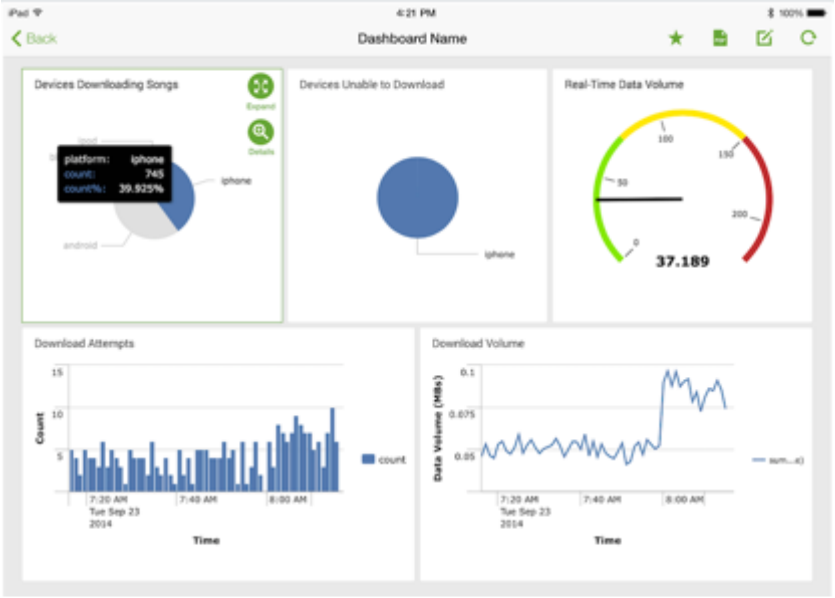
9/23 12:15-1:00PM

Splunk Mobile Access

Splunk dashboards, alerts and more for iOS and Android devices

- Monitor dashboards, KPIs, reports
- Receive real-time business and operational alerts
- Annotate and share data
- Supports MDM and single sign-on
- No longer requires separate Mobile Access Server

Formally called "Splunk Mobile App"



Release 6.3 – Value Across Products

Splunk Enterprise
All 6.3 features & performance

Splunk Cloud
Most features, scalability

Hunk
Visualization & analysis of large datasets

Splunk Light
Visualization, HTTP events, data integrity

	Enterprise	Cloud	Hunk	Light
Performance & Scale	Yes	Scale	Search only	No
HTTP Events	Yes	Yes	No	Yes
Data Visualization	Yes	Yes	Yes	Yes
Alert Action Integration	Yes	Yes	Yes	No
Data Integrity Check	Yes	Yes	No	Yes
Distributed Mgt Console	Yes	No	Yes	No
Other Management	Yes	Yes	Partial	Partial

Splunk Enterprise & Cloud 6.3

Breakthrough Performance & Scale

- 2X Search & Indexing Speed
- 20-50% Increased Capacity
- 20%+ Reduced TCO

Doubles performance and lowers TCO

Advanced Analysis & Visualization

- Anomaly Detection
- Geospatial Mapping
- Single-Value Display

Simplifies analysis of large datasets

High Volume Event Collection

- HTTP Event Collector
- Developer API & SDKs
- 3rd Party Integrations

Supports DevOps and IoT data analysis at scale

Enterprise-Scale Platform

- Expanded Management
- Custom Alert Actions
- Data Integrity Control

Delivers Enterprise platform requirements

Meeting the needs of the most demanding organizations

.conf2015

Q&A

splunk>

.conf2015

THANK YOU

splunk>