Action Packed Session!

Live Demos

Audience Challenges

Learn More “Pop Outs”
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.
Splunk Enterprise Releases

6.3  
Sep 2015

6.4  
Apr 2016

6.5  
Sep 2016

6.6  
Sep 2017

7.0  
Sep 2017

MLTK
1.0

MLTK
2.0

MLTK
2.1

MLTK
2.2

MLTK
2.3

MLTK
2.4

MLTK
3.0

MLTK
1.0

MLTK
2.0

MLTK
2.1

MLTK
2.2

MLTK
2.3

MLTK
2.4

MLTK
3.0
Monitoring & Investigation

Performance, Scale & Manageability

Machine Learning & Intelligence

Increased productivity for a wider range of users

Faster, more scalable and easier to manage than ever before

More powerful and extensible machine learning capabilities

Solve problems faster

Grow more easily

Do less work
Monitoring & Investigation

*Increased productivity for a wider range of users*

Performance, Scale & Manageability

*Faster, more scalable and easier to manage than ever before*

Machine Learning & Intelligence

*More powerful and extensible machine learning capabilities*
Metrics and Events
New, high-speed metrics engine that integrates seamlessly with events!

**Metrics**
- Set of numbers describing a particular process or activity measured over an interval of time - i.e., *time series data*
- Virtually unlimited number of use cases

![Graph showing time series data](image)

**Common metrics sources:**
- System metrics (CPU, memory, disk), Sensor data (temperature, …)
- Infrastructure metrics (AWS CloudWatch), Web Tracking (Google Analytics)
- Application agents (Application Performance Monitoring, error tracking)

**Events**
- Traditional Splunk - typically text, binary, un/structured data that describe a set of discrete events that happen over time
- Virtually unlimited number of use cases

**Common event sources:**
- System and server logs (syslog, journald), APIs (Twitter, Wunderground)
- Firewall data (Palo Alto Networks, etc)
- Application, platform and other logs (log4j, log4net, Apache, MySQL, AWS)

![Sample Log](image)
New Metrics Features in the Platform

Ingest and Query metrics natively with new, high speed metrics engine

**Metric Store**
New metrics engine and index to ingest and store metrics *natively* at scale

**mstats**
Query metrics data from metrics indexes (similar to tstats)

**Metrics Catalog**
REST APIs and mcatalog to query lists of ingested metrics and dimensions
Splunk Metrics – Index Creation

New Metrics Index Data Type
Splunk Metrics – Data Ingestion

Supports StatsD, CollectD, and CSV files natively

Supports other Metrics Clients via manual configuration

```conf
# props.conf.example
[graphite_plaintext]
TIME_PREFIX = \$(\{d(0,10)\})$
TIME_FORMAT = %s
NO_BINARY_CHECK = true
SHOULD_LINEMERGE = false
pulldown_type = 1
TRANSFORMS=graphite-host = graphite_host
TRANSFORMS=graphite-metricname = graphite_metric_name
TRANSFORMS=graphite-metricvalue = graphite_metric_value
category = Metrics
```
What is the CPU impact of plugging in my phone and playing a video?

Metrics
- Ingest CPU metrics data from my laptop (using CollectD into HTTP Event Collector)
- Take a video of all you (everyone wave)!
- Plug in my phone, Play the video
- Watch what happens to my CPU

Events
- Monitor system.log for events that signal I plugged in my phone
- Look for events with “connected apple”
- Run the query
- Save the query to use later

Combine Metrics and Event data using new Event Annotation
Splunk Metrics
Taking the *meh* out of metrics

- New, high speed metrics engine and index
- Get all the benefits of the Splunk platform:
  - Visualizations and alerting
  - Easy Data ingestion
  - Clustering, Scaling
  - Leverage open source for existing sourcetypes (*statsd, collectd*)
- 20x and beyond performance improvement for monitoring and alerting use cases with metrics data
- Integrates beautifully with traditional Splunk events

…and we’re just getting started…lots more to come!
Splunk Event Annotation

Surfaces more insights from your data

► Doesn’t just correlate logs and metrics in a single view
► Adds context to any time chart (e.g., line, column, area)
► Under the covers, it’s just an embedded search that enables you to pull markers and labels from many different sources
  • (e.g., log data, lookup files, or external sources)
Chart Enhancements & Report Actions
Chart Enhancements
Perfect for metric and multi-series monitoring use cases

- Change Line Width
- View and Compare Values in a Chart Legend
- Change Line Styles (dashes, dots etc)
Report Actions

Ability to set any action when scheduling a report

- Use any action that is installed and enabled in your alert actions framework
Trellis Layout
Trellis Layout

Go from one chart to multiple charts with a single click of a button!

▶ Perfect for comparing information across dimensions
▶ Super easy to use via new icon directly in the UI
▶ Super efficient at runtime as it executes the base search only once
▶ Uses results from chart, stats, and timechart commands
▶ Works in Search, Reports, Dashboards
But what if I want to see multiple charts and compare across website actions?

And I don’t want to manually create new queries and charts….

Simple example of how Trellis can help!
Traveling on Time with Trellis

- Airlines with the most cancelled flights (vs previous week)
- Airlines with the most delays (vs previous week)
- Leveraging simple Single Value visualization
Trellis Contest Winner

Matt Zerfas, SONIFI Solutions

- Shows Wi-Fi Signal Strength across 40 floors of a hotel
- Uses Trellis with a customer choropleth map
- Measures wi-fi signal strength in dBm (decibel milliwatts)
Dashboard, Search, and Datasets

User Productivity Improvements
New Dashboard Drilldown Editor

Build custom interactivity in your dashboards without the need to learn XML

- Link to search
- Link to dashboard
- Link to report
- Link to custom URL
- Manage tokens

Using a simple gui-based drilldown editor
New Dashboard Search Editor

*Improved search editing experience on dashboards*

- Added Search Assistance to Dashboard Search Editor
  - Syntax Highlighting
  - Keyboard Shortcuts
  - Compact Search Assistant
Search Productivity Enhancements

Continuing to implement the most asked for Search IDE productivity features

Line Numbers, Auto-formatting, and Dark Mode

Macro Expansions and Keyboard Shortcuts
Table Datasets

Turn raw, unstructured events into structured tables without writing SPL

- Launched last year with Enterprise 6.5
- Available from Datasets Listings page
- Lots of new capabilities in 6.6…
Table Datasets

Turn raw, unstructured events into structured tables without writing SPL
Amazon Kinesis Firehose
Amazon Kinesis Firehose Support (Private Beta)

Push data from Kinesis Firehose into Splunk

Key Benefits

▶ Fully managed and **highly available service** for getting data into Splunk
▶ **Well integrated** with various data sources
▶ **Bypass** the need for setting up and managing **heavy weight forwarder**
▶ Ability to **transform raw data prior** to sending it to Splunk
▶ **Easy to use** with no programming requirement
Monitoring & Investigation

Increased productivity for a wider range of users

Performance, Scale & Manageability

Faster, more scalable and easier to manage than ever before

Machine Learning & Intelligence

More powerful and extensible machine learning capabilities
Improved Search Performance & Scale
Splunk Metrics Performance
Monitoring and Alerting use cases with metrics improved 20X+

Racing Data (4MM+ Events)
- Chart average speed over 12 hours
- Top panel is Standard Splunk Event Index
- Bottom panel is new Metrics Index
- Watch how quickly the Metrics index (bottom) finishes

Play Video ➔
Buttercup Games

If we raise prices 15%, how many of the Strategy products could we sell for over $20?

Can you make this search more efficient?

...search result out of 232,630 events

<table>
<thead>
<tr>
<th>product_name</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dream Crusher</td>
<td>5609</td>
</tr>
<tr>
<td>Final Sequel</td>
<td>4887</td>
</tr>
<tr>
<td>Mediocre Kingdoms</td>
<td>5922</td>
</tr>
</tbody>
</table>
SPL Optimizer

You Actually Don’t Need to Know!
Under the covers, Splunk optimizes the search for you

Without OPTIMIZER
Scanned 232,630 events in 11.949 seconds

With OPTIMIZER
Scanned 28,329 events in 2.184 seconds

buttercupgames | eval new_price=price*1.15 | where new_price>20 AND categoryId="STRATEGY" | stats count by product_name

predicate splitting

categoryId="STRATEGY" buttercupgames | eval new_price=price*1.15 | where new_price>20 | stats count by product_name
Search Performance Optimizations

Predicate Splitting
Splits predicates and execute early
(Splits ANDs not Ors)

search 500 | eval x=a*b | where x=100 AND y="Test"

search 500 y="Test" | eval x=a*b | where x=100

limits.conf:
[search_optimization::predicate_split]
enabled = true

Projection Elimination
Removes commands that produce unneeded new fields

search 500 | eval x=a*b | lookup cust id OUTPUT name | stats count by host

search 500 | stats count by host

limits.conf:
[search_optimization::projection_elimination]
enabled = true
cmds_black_list = <Commands List>

Automatically applies optimizations to optimize query execution speed
Faster Data Model Acceleration (DMA)
Big Improvements in Search Performance and Resource Usage

- Applicable to both platform and premium solutions
  - Acceleration searches run up to 3x faster*.
  - Data Model summarization lag is up to 1/3 less*.
  - Less Resources used (CPU, MEM, IO)
  - Improved Responsiveness - acceleration data available more quickly for *tstats* querying
  - Enterprise Security models get a big boost in speed

* From 6.5 → 7.0 (based on test lab data)
Enhanced Indexer Clustering Scalability

- 6.5
  - 1.5 Million Unique Buckets
  - 4.5 Million Total Buckets

- 6.6
  - 5+ Million Unique Buckets
  - 15+ Million Total Buckets

Delivers seamless scalability to 100s of Petabytes
Improved Manageability

Improved Resiliency and Developer Productivity
Cluster Resiliency
Improved resiliency to hardware and networking failures

**Indexer Clustering**

If an Indexer goes offline, search is not disrupted

Indexer recovery time is much faster

In a multi-site cluster, Forwarders can automatically failover to a secondary site

**Search Head Clustering**

Smarter knowledge object (config) replication across search heads

Intelligent captain selection based on configuration awareness

Improved replication speed across search heads and indexers for apps, lookup tables, etc
Cluster Management
Improved manageability as you grow and scale

Indexer Clustering

Manual Indexer Detention - Selectively control the flow of data into an Indexer

- Deploy new apps (with reloadable configs) without cluster restart
- Rollback to previous configuration if any operational issues encountered

Search Head Clustering

New User Interface

Transfer Search Head Captain

Begin Rolling Restart
Knowledge Object Management

Automatically detect orphaned Knowledge Objects when an employee leaves your company

Manually Re-assign to a different user

Settings → All Configurations
Data Ingestion Management

New Regex Profiling views for Admins to monitor incoming data

- Found in the Monitoring Console under “Indexing → Indexing Performance”
- Find CPU time spent on Regex Extraction
- Split-by source, sourcetype, index and host
Data Ingestion Management

New Data Quality views for Admins to check the accuracy of incoming data

- Found in the Monitoring Console under Indexing → Inputs
- Surfaces index-time warnings and errors (splunkd.log)
- Find Timestamp, Linebreaking, and Aggregation issues with incoming data
Cloud App Management – Certified Apps
Install and Update Splunk certified apps with the click of a button

Automatically install most Splunk Certified Apps (without filing a Splunk Support ticket)

Also installs not just the App but also its dependencies

New App Management control page centralizes Download, Update, and Uninstall
Cloud Application Management – Private Apps

Quickly install and uninstall *private apps*

- New self-service Upload App interface for the cloud
  - No support ticket needed!
- Automatically runs AppInspect and generates a detailed AppInspect vetting report
- If approved, Install/Update private apps with a single click

*7.0 deployment dates in the cloud will vary across customers (planned initial delivery starting later this year)*
Get your apps built and deployed faster than ever!
Monitoring & Investigation

Increased productivity for a wider range of users

Performance, Scale & Manageability

Faster, more scalable and easier to manage than ever before

Machine Learning & Intelligence

More powerful and extensible machine learning capabilities
Machine Learning Overview

Learning by Example

Start

Use Case / Problem
(hard for human to figure out)

Input Data
(examples)

Machine

Model

prediction

(vs truth)

Evaluate

Intelligence
(hard for human to figure out)

adjust / iterate

Use Case / Problem

Network Optimization
Detect & Prevent Equipment Failure

NTT docomo

Security / Fraud Prevention

Telco

Prevent Cell Tower Failure
Optimize Repair Operations

Zillow

Prioritize Website Issues
and Predict Root Cause

Entertainment Company

Predict Gaming Outages
Fraud Prevention

Concanan

Machine Learning Consulting Services

Scianta Analytics

Analytics App built on ML Toolkit
Machine Learning Process

1. **Use Case / Problem** (hard for human to figure out)
2. **Collect Data**
   - Lots of different tools and environments
3. **Model**
4. **Explore / Visualize**
5. **Deploy / Use**
6. **Clean / Transform**
7. **Evaluate**

**CORE PLATFORM**
- SEARCH + Smarter Splunk

**PACKAGED PREMIUM SOLUTIONS**

**MACHINE LEARNING TOOLKIT**

**Platform for Operational Intelligence**

© 2017 SPLUNK INC.
Machine Learning Toolkit
Send me an email alert when Server Power consumption is way outside of predicted values

- **Collect Data**
  - Input `server_pow.csv`

- **Explore / Visualize**
  - Checkout the data

- **Clean / Transform**
  - Normalize the data (apply pre-processing step)

- **Model**
  - Predict power consumption
  - Detect numeric outliers

- **Evaluate**

- **Deploy / Use**
  - Setup thresholds, alerts, and actions
Machine Learning Toolkit – What’s New

Enhanced Detect Numeric Outliers assistant

Segment outlier detection by field

New visualizations, including data distribution histogram

Expanded pre-processing capabilities

Predict Numeric Fields

Predict Categorical Fields

Cluster Numeric Events

ML-SPL API

Makes it easier to import open source and proprietary algorithms

© 2017 SPLUNK INC.
Machine Learning Toolkit – What’s New

Model Management (MLTK 3.0)

Assign permissions to models to control access

Spark Support (private beta open now)

▶ Use your existing Spark cluster with MLTK
  • Distributed fit on massive datasets
  • Apply MLlib models for supported algos
▶ Go to Splunk Innovation Labs (NDA only)
▶ Contact mlprogram@splunk.com
  • What is your use case (e.g., predicting server downtime)?
  • How are you using Spark today?

Leverage your Spark Infrastructure
Monitoring & Investigation

- Increased productivity for a wider range of users
- Chart Enhancements
- Report Actions
- Trellis Layout
- Dashboard Drilldown editor
- Dashboard Search Bar
- Search Productivity Enhancements
- Table Datasets Explorer
- AWS Kinesis Firehose Support (Private Beta)

Performance, Scale & Manageability

- Faster, more scalable and easier to manage than ever before
- New High Speed Metrics Engine
- Improved SPL Optimizer
- Faster Data Model Acceleration
- Improved Indexer Scalability (5M buckets)
- Improved SHC/IC Resiliency and Management
- Orphaned knowledge object detection
- New Data Ingestion Management views
- Cloud Self-Service App Installation (private apps too)
- New App Packaging Toolkit

Machine Learning & Intelligence

- Fully Integrated across portfolio
- Enhanced Detection machine learning capabilities
- Expanded pre-processing capabilities
- Extended ML-SPL-API
- Additional Algorithms
- Model Management (3.0)
- Spark Support (Private Beta)

….plus lots more we didn’t get a chance to cover
Splunk Enterprise 7.0 Available Now

Plus check out the Overview Apps for What’s New

Splunk 6.6 Overview App

Splunk 7.0 Overview App
Visit Splunk Labs

Room: 301-303
Tues 10:30am – 2:30pm, 4:30pm – 6:30pm
Wed 10:30am – 3:00pm
Thank You

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