

.conf18

splunk>

# Getting the Most Out of Splunk Infrastructure Monitoring

Domnick Eger - Global DevOps Practitioner  
Nick Tankersley - Principal Product Manager

October 2018

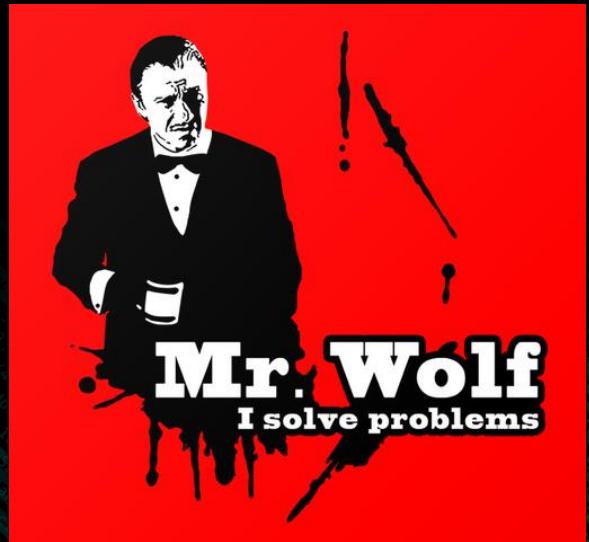


# Our Speakers



**Nick Tankersley**

**Principal Product Manager**

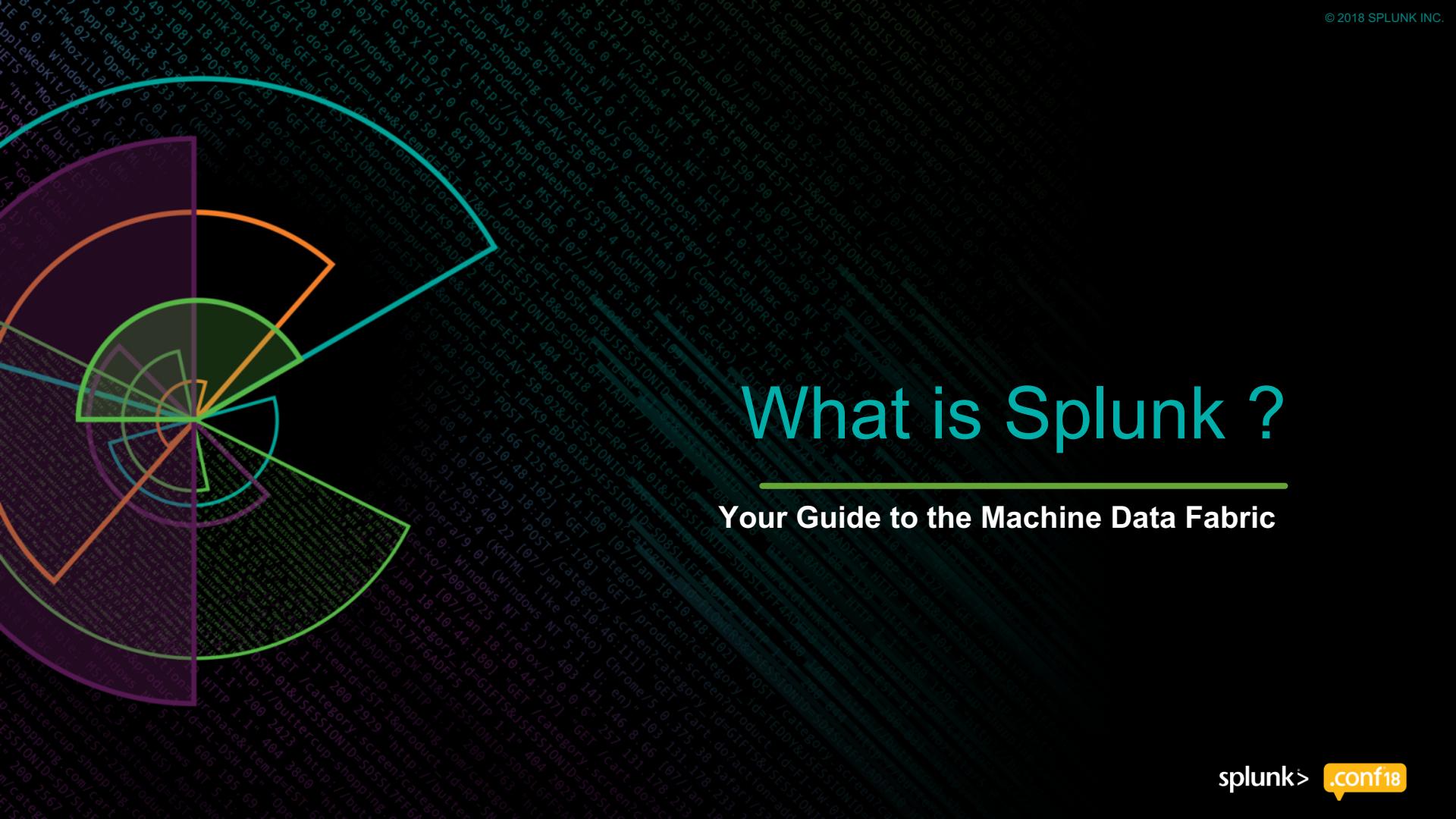


**Domnick Eger**

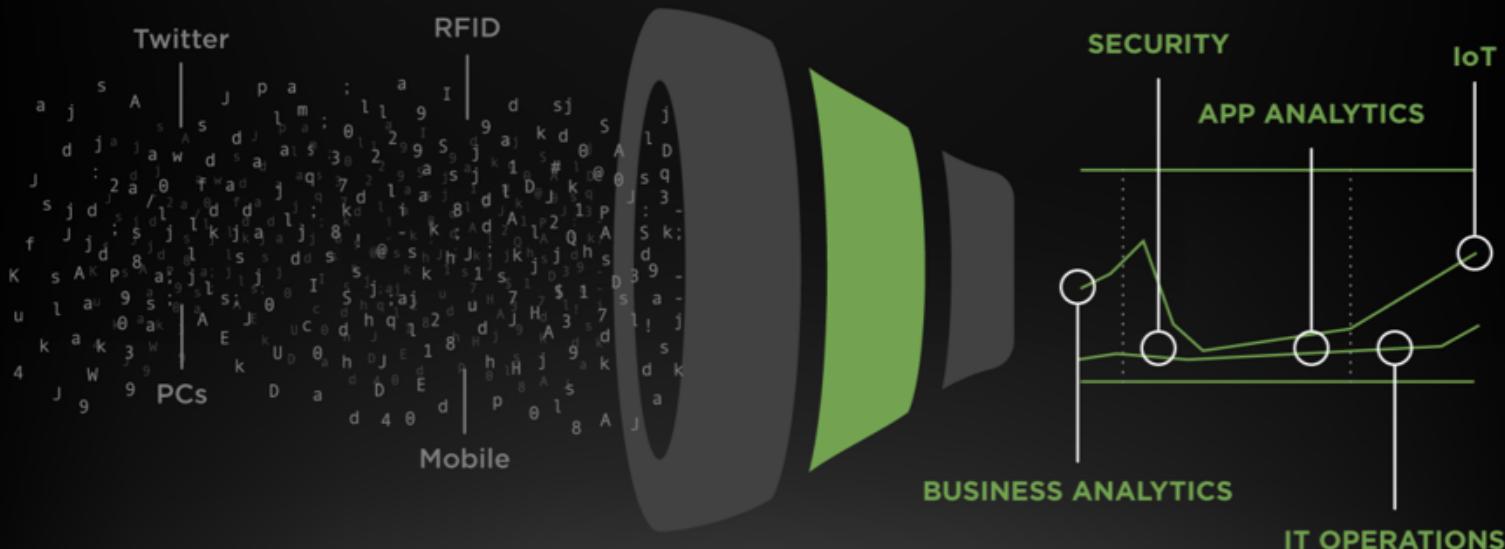
**Global DevOps Practitioner**

# What is Splunk ?

Your Guide to the Machine Data Fabric



**Splunk turns machine data into answers.**



## Why Splunk ?



## FAST TIME-TO-VALUE

#### ONE PLATFORM. MANY USE CASES

## VISIBILITY ACROSS STACK–NO SILOS

**ASK ANY QUESTION OF DATA**

**ANY DATA. ANY SOURCE.**



# Splunk solutions

# Splunk Premium Solutions



Splunk IT Service  
Intelligence™



# Splunk Enterprise Security™



## Splunk User Behavior Analytics™

## 1,000+ Apps and Add-Ons



splunk>enterprise

splunk>cloud

**splunk> Platform for Operational Intelligence**

# Infrastructure Monitoring Challenges

# Infrastructure monitoring isn't new, but constantly changing demands require a new approach

# Monitoring and Troubleshooting In Silos

“ Why am I monitoring with one tool and troubleshooting with another? ”

## Nonstop increase in complexity makes finding and fixing problems harder

“ Applications keep getting more complex and I’m required to monitor more than ever and find problems faster! ”

## Spending too much time administering monitoring software

“ We don’t have enough people and budget to buy and maintain complex monitoring tools. ”

# Splunk App for Infrastructure

Seamless metrics and logs / Easy to deploy and use / Inexpensive



- ▶ Collects, correlates, and analyzes metrics and logs to monitor on-premises and AWS server infrastructure
  - ▶ Designed and optimized for infrastructure monitoring – from configuration to infrastructure problem investigation
  - ▶ Out of the box integrations for Linux OS, Mac OSX, Windows Servers and over 100 integrations with collectd and Windows Perfmon

# Install to Insights in Minutes

## Built for easy development and configuration

Single interface for configuring metric and log collection  
Easy method for pushing monitoring software to hosts

The screenshot shows the Splunk Insights for Infrastructure interface. On the left, there's a navigation bar with 'splunk > Insights for Infrastructure' and tabs for 'Investigate', 'Configure', and 'Alerts'. Below the navigation is a section titled 'Configure Integrations' for 'Unix' and 'AWS'. Step 1, 'Specify configuration options', includes fields for 'Data to be collected' (5 Metrics + 5 Log sources), 'Dimensions' (with a 'Filter dimensions' link), and 'Monitoring machine' (set to 'ec2-18-144-72-53.us-west-1.compute.amazonaws.com'). Step 2, 'Copy and paste the following into the command line of your entity', contains a shell script for setting up the agent. Step 3, 'Once the script finishes running, verify your data connection.', has a note about auto-refresh. On the right, a 'Customize Data Collection' panel is open, showing '7 Metrics Selected' (CPU, df, disk, interface, load, memory, swap) and '5 Log Sources Selected' (var/log/syslog, var/log/demon.log, var/log/rauth.log, var/log/apache/access.log, var/log/apache/error.log). There are 'Select All' and 'Deselect All' buttons at the top of each list. A 'Metric Options' section has a checked checkbox for '(cpu) Collect data for each cpu'. At the bottom right of the panel are 'Cancel' and 'Save' buttons.

“From start to finish, we analyzed metrics from both AWS and Unix servers within 30 minutes of downloading the Splunk Insights for Infrastructure deployment package.”

--Lance O'Connor, Senior Principal Engineer, TiVo

# Seamless Monitoring and Troubleshooting

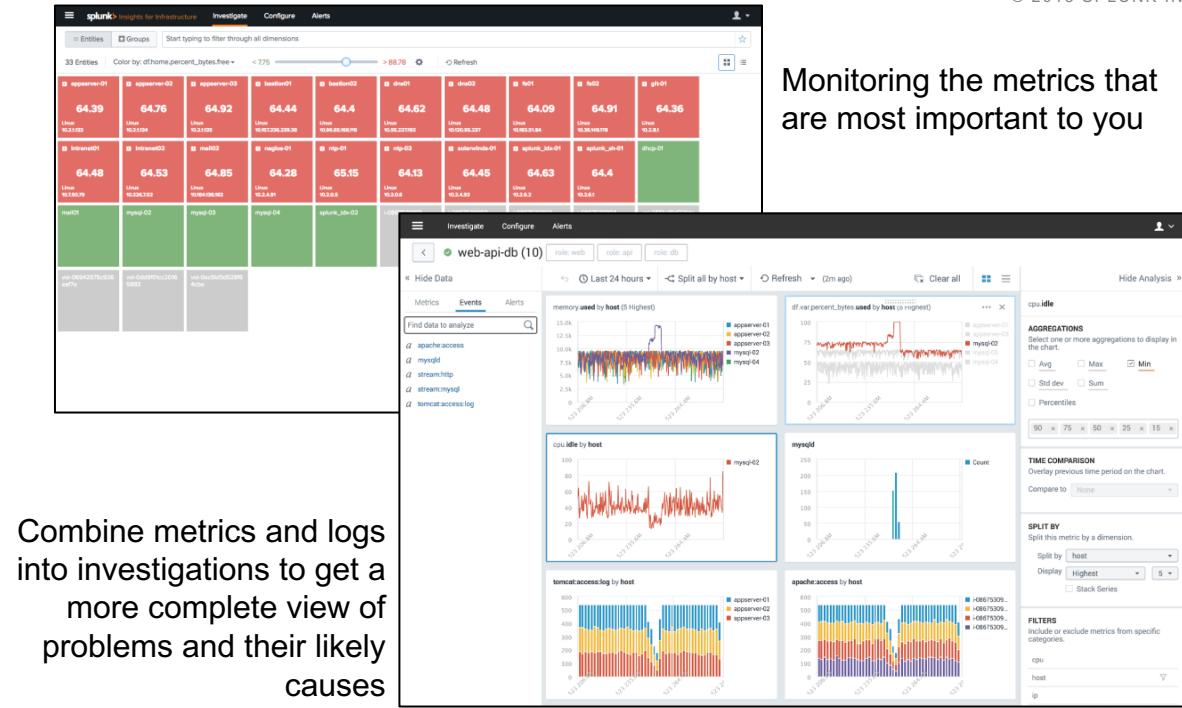
Collect and analyze logs and metrics together

Combine metrics and logs into investigations to get a more complete view of problems and their likely causes

“Splunk Insights for Infrastructure cleverly combines metrics and logging for a more complete view of infrastructure performance. We can see unusual behavior such as a CPU spike and correlate it with logs to troubleshoot problems much more quickly.”

*– Daryl Robbins, Senior Cloud Architect at Entrust Datacard*

splunk> .conf18



Monitoring the metrics that are most important to you

# Time for a Demo

# splunk® essentials

## for Infrastructure Troubleshooting and Monitoring



<https://splunkbase.splunk.com/app/4091/>



splunk® enterprise App: Splunk Essentials for Infrastructure Troubleshooting and Monitoring

Introduction Infrastructure Troubleshooting and Monitoring Content Advanced Documentation

Administrator Messages Settings Activity Help Export

Splunk Essentials for Infrastructure Troubleshooting and Monitoring

Assistant: Simple Search

Summary

Use collectd to ingest your Web server's health metrics. Apache provides many metrics via the mod\_status extension and those can be easily ingested into Splunk using collectd.

Learn how to use this page View Demo Data

**Use Case**  
Infrastructure Troubleshooting

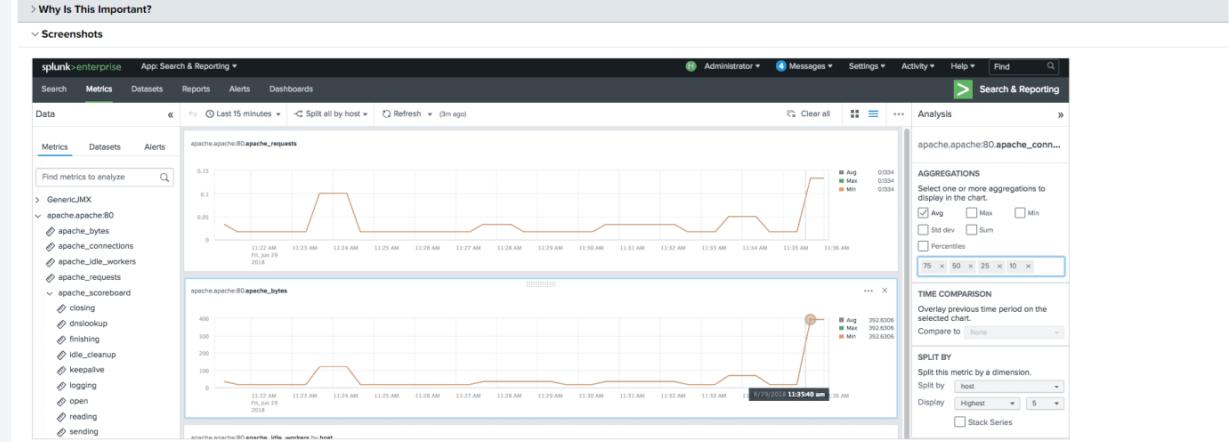
**Capabilities**  
Monitor Apache Web Servers with collectd

**Description**  
The Splunk App for Infrastructure provides a 1-line installation of collectd for your Linux servers. Once installed you can add any of the many collectd plug-ins to monitor components of your IT infrastructure including Apache Web servers.

**SPL Difficulty**  
Easy

**Stage 2**  
Data Sources

Application Metrics Application Usage Data





# Download Splunk App for Infrastructure!

**Come See us  
on the Demo Floor!**

The screenshot shows the Splunkbase marketplace interface. On the left, there's a sidebar with a search bar, account navigation, and support links. The main area displays the "Splunk App for Infrastructure" page. It features a green icon with a lightbulb, a title, a 5-star rating (4 reviews), and a "Splunk Built" badge. Below this is a preview window showing a heatmap-style visualization of log data across various hosts. At the bottom of the page are administrator tools like Manage App, View App, and View Analytics.

---

The screenshot shows the Splunk app dashboard for "apps-demo05". It includes an overview section with metrics: Number of Events (286), CPU Usage (86%), Network I/O (28,181 bytes/sec), Memory (0 read bytes), and Disk (81 read bytes). There are also sections for Disk Usage (a bar chart) and CPU Utilization by State (a line chart). On the right, there are sections for System Information (OS: kernel\_version=3.16.0-4-vmwgfx, IP Address: n/a, Version: 8 (jew)), Dimensions (dimensions=host=hostnames-dev05), and a "See all" link.

The screenshot displays three separate Splunk dashboards for the application 'apps-demo05'. Each dashboard includes navigation tabs for Overview and Analysis.

- Left Dashboard:** Shows two line charts for CPU usage over time (Last 1 hour). The top chart is for 'cpu\_usage' and the bottom for 'cpu\_load'. It also includes a sidebar for 'Metrics' and 'Events' analysis.
- Middle Dashboard:** Shows a histogram for 'Network Octets In/Out' over time (Last 1 hour). The histogram has two main peaks, one at approximately 180 and another at approximately 240. It includes an 'Analysis' section for 'cpu\_system' with aggregation options like Avg, Max, Min, Sum, and Percentiles.
- Right Dashboard:** Shows a histogram for 'Network Octets In/Out' over time (Last 30 days). It includes an 'Analysis' section for 'NagiosExtractions' with a dimension 'Count' and a table view of extracted data.

The overall interface features a dark theme with light-colored cards for each dashboard. The 'Analysis' sections include dropdown menus and checkboxes for selecting specific metrics or dimensions.

splunk> .conf18

# Q&A



# Thank You

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

.conf18  
splunk>