Splunk ITSI as a Foundation for ITOA

Measuring End-to-End User Experience

Patrick Combs | Data Center Services & Analytics
Scott Hamrick | IT Director – Operations Analytics

Date | 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, 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.
Biography

Patrick Combs
TCS, Data Center Service & Analytics Leader
▶ 16 yrs combined experience at PwC
  • Web Development
  • Database Reporting
  • Platform Services
  • Data Analytics
  • Soccer coach and avid cyclist

Scott Hamrick
PwC, IT Director – Operations Analytics
▶ 20 yrs combined experience with GE/PwC
  • Networking (CCNP)
  • InfoSec (CISSP)
  • Data Analytics
  • Softball professional, MST3K backer
PricewaterhouseCoopers

Our purpose is to build trust in society and solve important problems

▶ Globally - 223,468 people in 743 locations in 157 countries
▶ 46k partners and staff in the US
▶ Provide industry-focused assurance, advisory and tax services for over 90% of the companies in the Fortune Global 500 list
PwC IT Environment

Diverse IT Infrastructure

Data Center Services Responsibilities
• Support Multiple Lines of Service
• 100s of applications
• 24x7 support for production applications
• Distributed workforce
• Dedicated support teams by technology
• Numerous “Mission Critical” application environments
Legacy Challenges

Troubleshooting Outages
• Issues reported by users or by Up/Down device monitoring
• Large audience Conference calls
• Siloed investigation of possible cause
• Lack of data availability lead to slow progress.

Problem Management
• Lengthy investigations relying on Vendors or manual analysis
• Root Cause frequently incomplete
• Repetitive outages from similar causes
My Top 5 Least Favorite…

My least favorite comments to hear on a troubleshooting call are…

1. Can we get the Vendor on the call??
2. I am not familiar with this technology but…
3. My application is working but it is slow…
4. Can someone “check” the Network??
5. Has anyone made any changes??
IT Operations Analytics Mission

“Sunlight is said to be the best of disinfectants”

Justice Louis D. Brandeis
Holistic approach to data analytics
• Become “The” source of information
• Aggregate all relevant data
• Organize complex data sources
• Offer guided navigation
• Provide targeted data detail

Critical Success Factors
• Quantify / Track User Experience
• Eliminate unplanned downtime
• Reduce MTTR for Incidents
• Improve IT capacity management
• Remove Manual Reporting

Measure and improve end-to-end user experience
IT Operation Analytics

Variable levels of specificity based on organizational role

- Executive
- Domain Leads
- Team Leads
- Administrators

- System Health
- Strategic Planning
- Tactical Execution
- Troubleshooting

uberAgent

End User Experience

ITOA

Splunk ITSI
IT Operation Analytics
End-to-End visibility for user experience

- Infrastructure
- Applications
- Core Services
- Incident Mgmt
- Service Mgmt

Platform
Network
Storage

Custom Business Applications

AD/DNS
ED
IdAM
Siteminder

Major/Minor Incidents Interactions

Change Problem Release Knowledge
IT Operations Analytics
Leveraging Splunk ITSI backbone to organize info in custom application
Overview of IT Health based on real-time status

Aggregates KPIs across dimensions

Allows custom navigation
  - Drop-down menus
  - Drill-down links
ITOA Application
Custom service health dashboard of critical KPIs

- Metrics determined by service SMEs
- Dashboard nested in dropdown menu
- Consistent look and feel based on branding standards
- Filtered by host
- Minimalized time picker
ITOA Application – Health Score
Service health overview for Domain Leaders

- KPIs listed by segment
  - Infrastructure
  - Application
  - Service Management
- Trendline metrics included for context
- Asset/Service navigation
- Punchout links to native ITSI functionality
ITOA Application – Splunk ITSI
Splunk ITSI Glass Table view for Team Leaders

- Launch Splunk ITSI in new tab
  - KPIs listed by service
    - Real-time value
    - Trend metrics included
  - Infrastructure KPIs listed per server
  - Drilldown links to deep dive
  - ITOA application active in previous tab
ITOA Application – Splunk ITSI
Deep-dive troubleshooting view for Administrators

- Native Splunk ITSI functionality
- Correlate KPIs in context with each other
- Viewable by entity
- Service dependencies available as defined
  - Authentication tier
  - Web/Database tier
Integrating Splunk ITSI with ITOA app

Technical walkthrough
Splunk ITSI and ITOA Overview

- Key components required by ITOA app
  - Splunk ITSI Service / KPI Definitions
  - Splunk ITSI Entity and Base Searches
  - ITOA Lookups
  - ITOA Weighted Average Macro
  - ITOA Framework to present results
### ITOA Application – Splunk ITSI

#### Entity Definitions

- **Assign entities to the service**
  - Either literally list the entities or define rules
  - Confirm all entities present
  - Plan for future changes

---

**Figure:**

- **Siteminder**
  - **Service description**
  - **Entities**
    - **KPI**
    - **Service Dependencies**
  - **Entity Rules** allow for the optional, dynamic filtering of KPIs and can help in root cause analysis. A service need not define any Entity Rules and is not limited to only the entities matching Entity Rules.

<table>
<thead>
<tr>
<th>Title</th>
<th>Alias</th>
<th>Info</th>
</tr>
</thead>
</table>
| MATLKSAMPSFP001 | MATLKSAMPSFP001 | 6.1.7601 operating_system_host, Microsoft Windows Server 2008
host, WinHostMon
| MATLKSAMPSFP002 | MATLKSAMPSFP002 | 6.1.7601 operating_system_host, Microsoft Windows Server 2008
host, WinHostMon
| MATLKSAMPSFP003 | MATLKSAMPSFP003 | operating_system_host, WinHostMon, 6.1.7601, Microsoft Windows
Server 2008 R2 Enterprise
Utilize KPI base search for standard OS metrics

- Custom KPIs generate app specific health scores.
- Both combine for overall health
- Results written to the summary index
Utilize Splunk ITSI Service Health to assign weights

Overall Service Health based on KPI and assigned weighting

Weighting process is iterative
Applies the ITOA app framework around Splunk ITSI Data

Provides the glue between Splunk ITSI and ITOA App

Group KPIs into different levels

Detailed descriptions providers for users
Utilize Splunk ITSI weighted average calculation to produce health scores

Pass time, search term, and service grouping details to calculate health at any level

Maintain separation from development environment
Call the `wavg_all` macro

- Pass necessary variables
  - Time
  - Service Group
  - By clause
Closing The User Experience Gap

Desktop monitoring
Desktop User Experience
Augment ITOA with 3rd party add-on uberAgent data
Desktop User Experience

- Utilizes Splunk Index/SH servers
- Integrated with Universal Forwarder
- Deployed to 68k+ laptops in multiple countries
- Established real-time monitoring and analysis of PC health
- Data correlated with Splunk ITSI to close the end user experience gap
Desktop User Experience
Boot & logon dashboard – uberAgent (custom)

- Tracking boot metrics
  - Startup/Shutdown
  - Standby/Resume
- Filter by
  - Host
  - IP address
  - Hardware model
- Histogram of days since last boot for troubleshooting
### Desktop User Experience

#### Storage Monitoring – uberAgent (custom)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total devices</td>
<td>62,918</td>
</tr>
<tr>
<td>Total hardware models</td>
<td>66</td>
</tr>
<tr>
<td>Total free space (%)</td>
<td>56.7%</td>
</tr>
<tr>
<td>Total free space (GB)</td>
<td>229.5 GB</td>
</tr>
</tbody>
</table>

- **Tracking disk capacity**
  - Total GB remaining
  - % of capacity
- **Disk usage grouped by**
  - Hardware Model
  - Host
- **Mounted volumes sorted per user by Free Space (% or GB)**

---

[Image of Splunk user interface showing disk capacity metrics]
Desktop User Experience
Single Machine Detail – uberAgent (default)

Drill down to single machine detail
- Avg CPU/RAM
- Avg disk available
- Network volume and latency
- Session detail
- Startup/shutdown duration
- Application & process detail
Key Takeaways

Summary
Key Learnings
If we had it to do all over…

▶ Establishing analytics as a service
  • Commitment from leadership
  • Addressing technical concerns
    • CPU utilization
    • Network firewall access
    • Network bandwidth
  • Building analytic ambassadors

▶ Defining innovation opportunities
  • Multiple demos required per team
  • 10-50-80% method

▶ Managing environment complexity
  • Cloud-based vs on-prem
  • Heavy Forwarders & syslog
  • Managing Universal Forwarders
  • Developing add-ons

▶ Overcoming data onboarding issues
  • VMWare
  • Cisco Wireless (SNMP vs Syslog)
  • Storage
  • Websphere
Thank You

Don't forget to rate this session in the .conf2017 mobile app
Want to Learn More About Splunk ITSI at .conf2017?

- **Ready, Set, Go! Learn From Others** - The First 30 Day Experiences of ITSI Customers: Tuesday, September 26th, 2017 12:05 PM-12:50 PM Room Salon C
- **Splunk ITSI Overview**: Tuesday, September 26th, 2017 1:10 PM-1:55 PM Room 147AB
- **PWC: End-to-End Customer Experience**: Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room 143ABC
- **RSI: Operational Intelligence**: How to go From Engineering to Operationalizing IT Service Intelligence Where the Rubber Meets the Road: Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room147AB
- **Cardinal Health: Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring Using Splunk ITSI**: Tuesday, September 26th, 2017 3:30 PM-4:15 PM Room143ABC
- **ITSI in the Wild - Why Micron Chose ITSI and Lessons Learned From Real World Experiences**: Tuesday, September 26th, 2017 4:35 PM-5:20 PM Room Salon C
- **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT**: Wednesday, September 27th, 2017 11:00 AM-11:45 AM Ballroom C
- **Triggering Alerting (xMatters) and Automated Recovery Actions from ITSI**: Wednesday, September 27th, 2017 1:10 PM-1:55 PM Room Salon C
- **Leidos - Our Journey to ITSI**: Wednesday, September 27th, 2017 2:15 PM-3:00 PM Room147AB
- **How Rabobank's Monitoring Team Got a Seat at the Business Table by Securing Sustainability on Competitive Business Services Built on Splunk’s ITSI**: Wednesday, September 27th, 2017 2:15-3:00pm Room 147AB
- **Here Comes the Renaissance: Digital Transformation of the IT Management Approach**: Wednesday, September 27th, 2017 3:30 PM-4:15 PM Room Salon C
- **The ITSI 'Top 20' KPI's**: Thursday, September 28th, 2017 10:30 AM-11:15 AM Room Salon C
- **Automation of Event Correlation and Clustering with Machine Learning Algorithms – An ITSI Tool**: Thursday, September 28th, 2017 11:35 AM-12:20 PM Room Salon C
- **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT**: Thursday, September 28th, 2017 11:35 AM - 12:20 PM in Ballroom B
- **IT Service Intelligence for When Your Service Spans Your Mainframe and Distributed ITSI**: Thursday, September 28th, 2017 1:20 PM-2:05 PM Room Salon C