



The Splunk IT Service Intelligence (ITSI) 'Top' 20 KPIs

Bill Babilon | Global ITOA Solution Architect

William von Alt II | Staff Sales Engineer - HHS, Splunk, Inc

Sept 28, 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, 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.

Outline

- ▶ What is a KPI?
- ▶ What makes a ‘good’ KPI?
- ▶ Where to Find ‘good’ KPIs?
- ▶ Pre-built KPI’s in ITSI
 - Modules
 - 3rd Party
- ▶ Field experience on the evolution of KPI’s
- ▶ Interesting KPI’s from the ITOA Practice

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 468 125.17.14.189 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.action=remove&itemId=EST-18" "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 468 125.17.14.189 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.action=remove&itemId=EST-18" "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K0-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0" "137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 468 125.17.14.189 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.screen?category_id=SURPRISE&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 187 "GET /category.action=remove&itemId=EST-18" "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100801 Firefox/53.0"

What is a KPI?

Key Performance Indicator

Let's Look At How Others Define KPI

“A performance indicator or key performance indicator (**KPI**) is a type of [performance measurement](#)”

– *Wikipedia*

“**Performance measurement**^[1] is the process of collecting, analyzing and/or reporting information regarding the performance of an individual, group, organization, system or component..”

– *Wikipedia*

“A key performance indicator (**KPI**) is a high-level measure of system output, traffic or other usage, simplified for gathering and review on a weekly, monthly or quarterly basis.”

– *Gartner*

Splunk ITSI KPI

“A [KPI](#) (Key Performance Indicator) is a **recurring saved search** that returns the **value of an IT performance metric**, such as CPU load percentage, memory used percentage, response time, and so on.”

– *Splunk*

For The Next 35 Minutes, Let's Use This:

“A KPI (Key Performance Indicator) is a ***recurring saved search*** that returns the ***value of an IT performance metric***, such as CPU load percentage, memory used percentage, response time, and ... ***any any valid business metric like revenue, orders/minute, Helpdesk tickets, pending change requests, etc***”

What Is A 'Good' KPI ...

... and what is a 'bad' KPI

What Makes A ‘Good’ KPI?

... and a not so good KPI

- ▶ It is insightful
 - Metric – a value
 - KPI – a value with meaning (think: thresholds)

- ▶ Intuitive/Easy to Understand

- ▶ Is relevant to the user’s role/job function
 - Executives want less detail, more aggregation
 - Admin’s want more detail

What Makes A 'Good' KPI?

... and a not so good KPI

▶ Bad KPIs:

- Data is sporadic
- Alerts only when something is bad: CPU Status Critical
- Counter data: 1234gb, 1239gb, 1299 gb

▶ Somewhat OK KPIs:

- Count-based data: 38 login fails last 15 minutes (is that OK or not?)

▶ Good KPIs:

- Provide data regularly, whether systems are good or critical: cpu=45%
- Self normalizing data: login success=90%
- Data with deltas not counters: 1.2 KB/min, 2.1 KB/min, 1.1 KB/min

Where To Find 'Good' KPIs

ITSI Modules, Ask and Service Decomposition

Where To Find 'Good' KPIs – ITS Modules

<http://docs.splunk.com/Documentation/ITSI/2.6.1/IModules/AboutITSIModules>

- ▶ ITSI v2.6 ships with nine (9) modules each with prebuilt KPI's
 - Application Servers – 17 KPI's
 - Cloud Services – 7 KPI's
 - Database Systems – 7 KPI's
 - End Use Experience – 8 KPI's
 - Load Balancers – 7 KPI's
 - Operating Systems – 12 KPI's
 - Storage Arrays – 10 KPI's
 - Virtualization – 10 KPI's
 - Web Servers - 8 KPI's
- ▶ 86+ available today!

Pre-Built KPIs – Application Server Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/ApplicationServerModuleKPIsandthresholds>

KPI Name	Splunk Add-on for Tomcat	Splunk Add-on for Websphere	Visualization Panel - Tomcat	Visualization Panel - WebSphere
4xx Errors Count	X	X	X	X
5xx Errors Count	X	X	X	X
Active Threads Count	X	X	X	X
Available Threads Count %	X	X	X	X
Average Transaction Response Time	X	X	X	X
Active Sessions Count	X	X	X	X
CPU Utilization %	X	X	X	X
Garbage Collection Time	X	X	X	X
Garbage Collections Count	X		X	
Hung Threads Count	X	X	X	X
Memory Heap Free %	X	X	X	X
Memory Heap Size	X	X	X	X
Memory Heap Used	X	X	X	X
Memory Pool Size	X		X	
Memory Used	X		X	
PermGen Usage	X		X	
Request Count	X	X	X	X

Pre-Built KPIs – Application Server Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/ApplicationServerModuleKPIsandthresholds>

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
4xx Errors Count	Total transaction errors for the analyzed time window	Count	Normal: 0-5, Medium: 5-50, High: >50
5xx Errors Count	Total transaction errors for the analyzed time window	Count	Normal: 0, Medium: 1-25, High: >25
Active Threads Count	Total count of active threads.	Count	No predefined threshold values
Available Thread Count %	Amount of threads that are currently available.	Percentage	Normal: >20, Medium: 5-20, High: <5
Average Transaction Response Time	Average response time (ms) for successful transactions	ms	2-hour blocks every day (adaptive/quantile), adaptive thresholding enabled
Active Sessions Count	Currently active sessions on the application server.	Count	2-hour blocks every day (adaptive/quantile), adaptive thresholding enabled
CPU Utilization %	Amount of CPU utilized by the application server process instance	Percentage	Normal: <70, Medium: 70-90, High: >90
Garbage Collection Time (ms)	Processing time of garbage collection.	ms	No predefined threshold values
Garbage Collections Count	Total count of collected unused heap memory.	Count	No predefined threshold values
Hung Threads Count	Total count of hung threads.	Count	No predefined threshold values
Memory Heap Free %	Amount of Memory Heap available.	Percentage	Normal: <70, Medium: 70-90, High: >90
Memory Heap Size (MB)	Total size of Memory Heap.	MB	No predefined threshold values
Memory Heap Used (MB)	Amount of Memory Heap currently used by all applications.	MB	No predefined threshold values
Memory Pool Size	Total size of allocated memory blocks.	MB	No predefined threshold values
Memory Used (MB)	Count of total memory in use.	MB	No predefined threshold values
Perm Gen Usage (MB)	Total PermGen space currently in use.	MB	No predefined threshold values
Request count	Total number of requests over the analyzed time window.	Count	2-hour blocks every day (adaptive/quantile), adaptive thresholding enabled

ITS Modules – A Word Of Caution On Performance

The difference between 'easy' and 'efficient'

▶ Easy

- Data Model base KPI's are VERY easy to create
- Data Model based KPI's are NOT very efficient/performance

▶ Efficient

- Base Searches are the recommended implementation for KPIs
- You can't change a base search, it must be cloned

▶ Consider the following – How could this search be made more efficient?

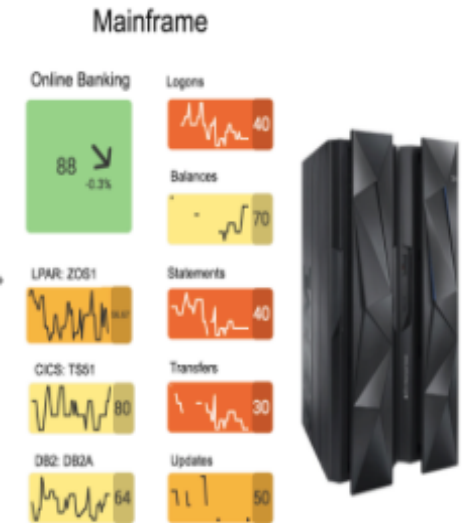
- *(index=* tag=oshost tag=performance tag=cpu)*



Where To Find 'Good' KPIs – 3rd Party Modules

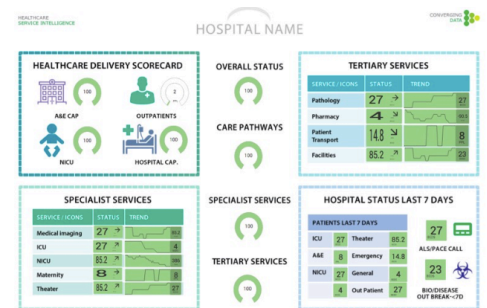
► Syncsort Ironstream Module for Splunk IT Service Intelligence

- <https://splunkbase.splunk.com/app/3329/>
- Capture real-time information from:
 - Mainframe (CPC)
 - z/OS® LPARs
 - CICS® systems
 - DB2® systems



► Converging Data Patient Flow Module for Splunk IT Service Intelligence

- <https://splunkbase.splunk.com/app/3325/>
- Captures HL7 data related to patient care pathways



Where To Find ‘Good’ KPIs – Ask

- ▶ Ask the customer/user
 - Existing Dashboards
 - Daily/weekly/Monthly Status Reports

- ▶ Bad: “I am here to create KPIs for your system. What do you want?”

- ▶ Good: “Think about the last time your had an outage, what did you look at in order to resolve the issue?”

- ▶ Different KPI’s for different user roles
 - Executives want less
 - Admin’s want more



Where To Find 'Good' KPIs – Service Decomposition

SERVICE DECOMPOSITION

What is the service to be monitored?

What are the components of the service?

What are the metrics/what do you care about?

What are the KPIs for service?

Identify data sources for each KPI

Onboard missing data into Splunk.

Show value!

Real-time Service Insights

Multi KPI Alerts

Create Glass Tables

Create Deep Dives

Create KPIs, tune thresholds

Create Services, Dependencies

Ready for ITSI



Observations on the Evolution of KPIs

“I’d Rather See Three (3) Or Four (4) Meaningful, Business Level KPIs Than 15 Or 20 Noisy, Technical KPIs.”

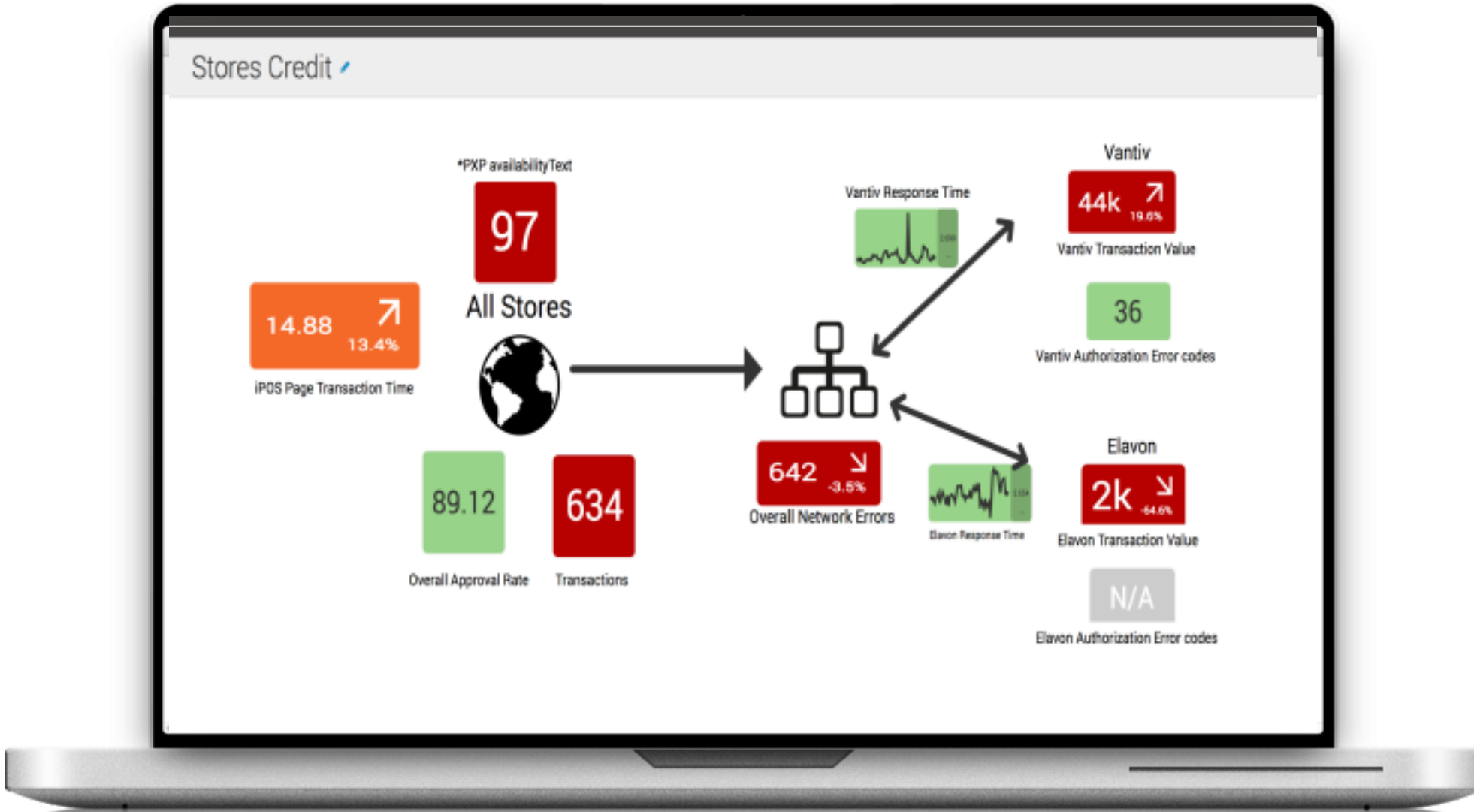
VP of Enterprise Service Monitoring, National Telecommunications Company

Observations On The Evolution Of KPIs

It often start technical but shouldn't end technical

- ▶ Like most activities in ITSI, creating KPIs is iterative
- ▶ Yes, you many start with the technical ones that are pre-built...
- ▶ ... But, But, **BUT DO NOT STOP WITH JUST TECHNICAL KPIs**
 - We see this happening far too often
- ▶ Remember the user
 - Admins want more technical detail
 - Executive want more business relevant KPIs

Major Retailer



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttcup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttcup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttcup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttcup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01"
10.0.0.1:5V1: .NET CLR 1.1.4322" 468 125.17 14 "http://buttcup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttcup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01"
10.0.0.1:5V1: .NET CLR 1.1.4322" 468 125.17 14 "http://buttcup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttcup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CB-01"

Some Interesting KPIs And Some Glass Tables For Context

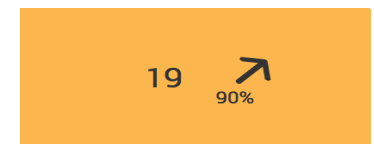
CIO Scorecard



Enterprise Service Status



Major Incidents



Major Changes

Service Health: 100

Volume: 5.8 k

Revenue: 2k USD

Incidents: 0

Changes: 0

Service Health: 100

Volume: 5.8 k

Revenue: 2k USD

Incidents: 0

Changes: 0

Service Health: 48.36

Volume: 206

Revenue: 492.8 USD

Incidents: 3

Changes: 18

Service Health: 60

Volume: 5.8 k

Ontime Delivery: 63.24

Incidents: 0

Changes: 0

Service Health: 90

Volume: 207

Revenue: 2k USD

Incidents: 0

Changes: 0

Service Health: 100

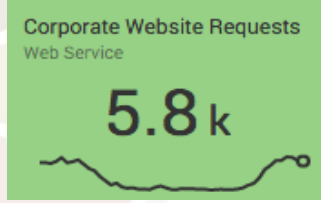
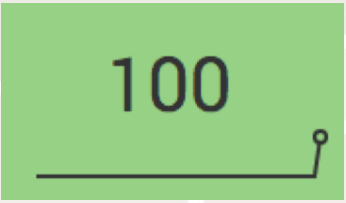
Throughput: 5.8 k

Container Util: 63.24

Incidents: 0

Changes: 0

Money Transfer Services

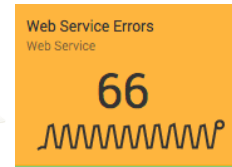


Service Health

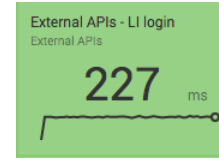
Corporate



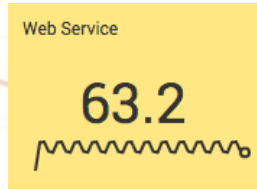
Internal Transfer Service



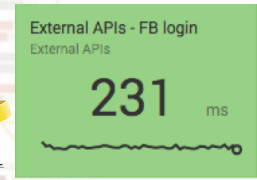
External Wire Service



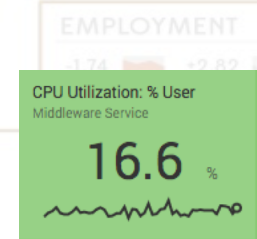
Online Transactions Services



Fed Exchange Service

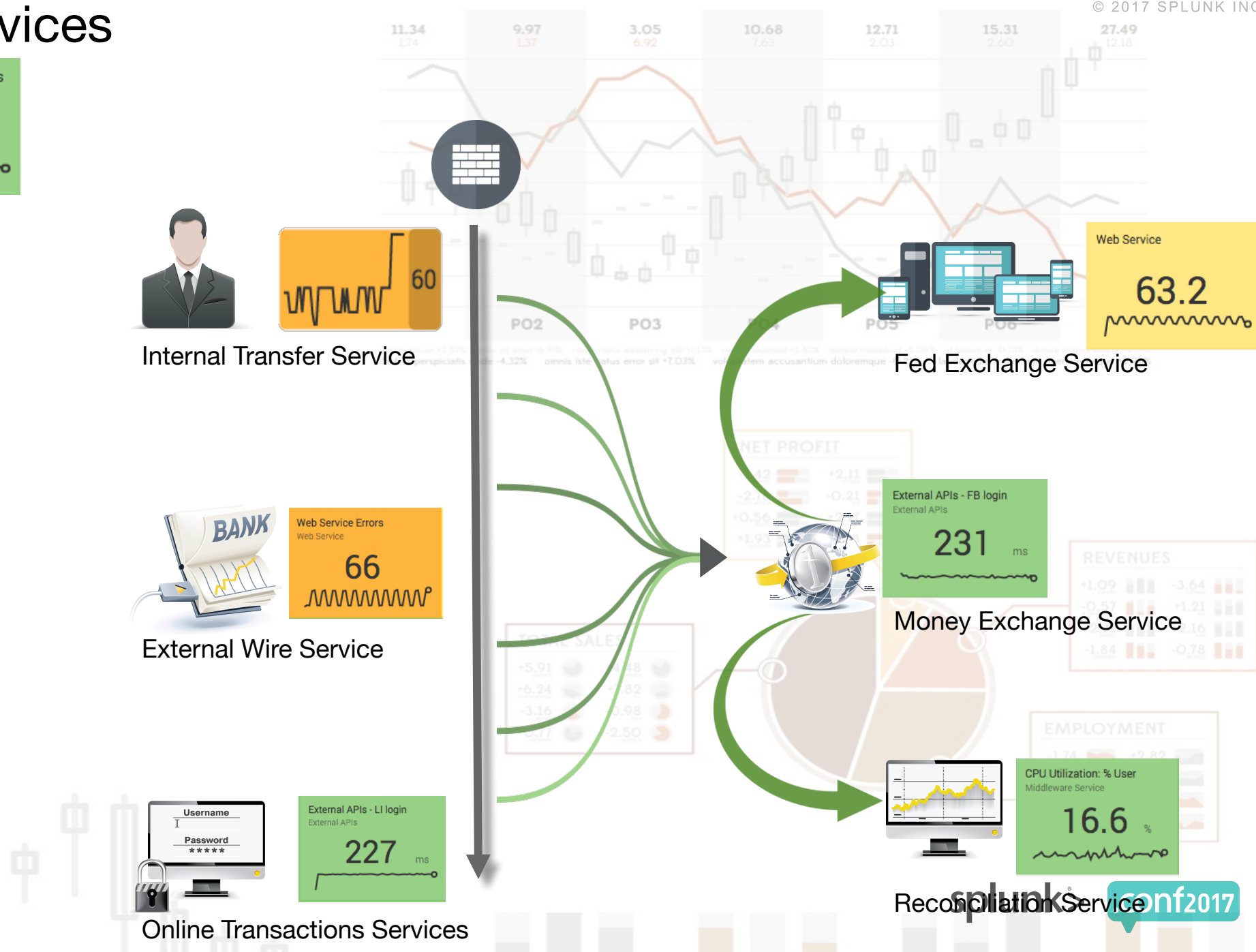


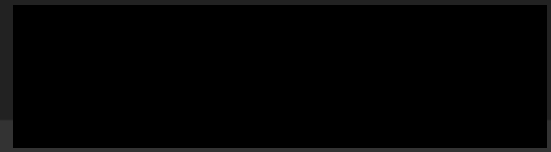
Money Exchange Service




Reconciliation Service

Core Splunk Searches	
Transaction History	●
System Investigation	●
Heat Map Analysis	●






 Click Through Rate: 90

 Bounce Rate: 20

 Click Through Cost: .23

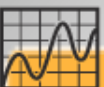
 Time On Site: 82 s


 Conversion Rate: 100

 Return On Investment: 375




100 ms
Response Time


60
Outbound Queue Size


866ms/s
Send Rate

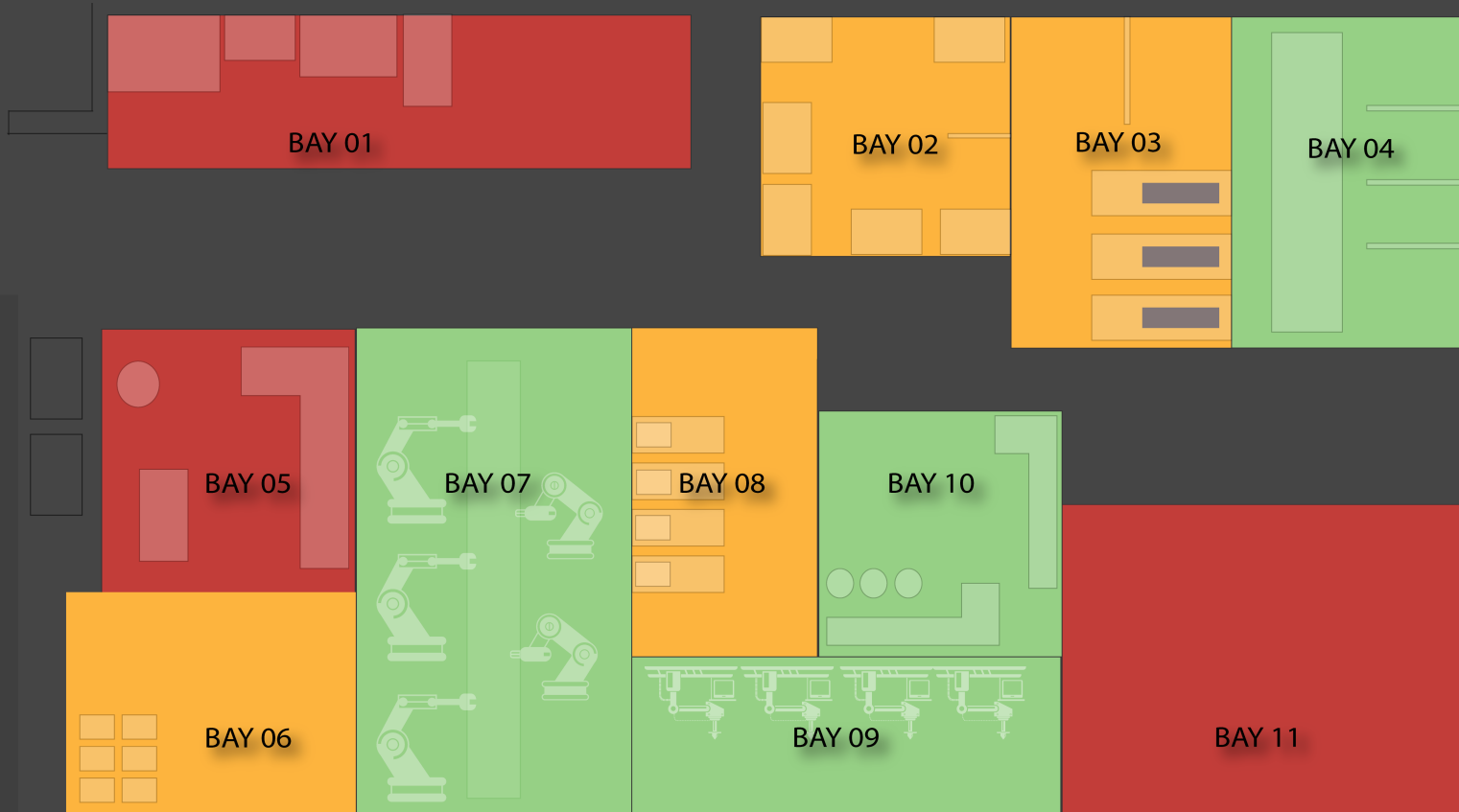

100
Campaign Health

XXX +: ●

YYY APP: ●

ZZZ : ●

Operational Status Production Line



Service Levels

System	Status
Network	■
Database	■
CNC Milling	■
Automation	■
JIT Ordering	■
Mobile	■
Power / Cooling	■

splunk >

12 ↑
1.2%

Production Delay

42

Changeover Time (m)

91

Fill Rate %

1.7

Customer Rejects

92

Operations Uptime





**Making machine data
accessible, usable and
valuable to everyone.**

Key Takeaways

What makes a good
KPI

1. Remember the user and what they care about
2. There is way more to service monitoring than technical KPIs
3. It is iterative
4. Less is more when it come to executives

Thank You

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

splunk> .conf2017

Want to Learn More About ITSI at .conf2017?

Tuesday
September
26th, 2017

- ▶ **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 147 AB
- ▶ **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

Wednesday
September
27th, 2017

- ▶ **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, 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

Thursday
September
28th, 2017

- ▶ **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 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

Q&A

Bill Babilon | Global ITOA Solution Architect

William von Alt II | Staff Sales Engineer - HHS, Splunk, Inc

Pre-built KPIs in ITSI Modules

Pre-Built KPIs – Application Server Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/ApplicationServerModuleKPIsandthresholds>

KPI Name	Splunk Add-on for Tomcat	Splunk Add-on for Websphere	Visualization Panel - Tomcat	Visualization Panel - WebSphere
4xx Errors Count	X	X	X	X
5xx Errors Count	X	X	X	X
Active Threads Count	X	X	X	X
Available Threads Count %	X	X	X	X
Average Transaction Response Time	X	X	X	X
Active Sessions Count	X	X	X	X
CPU Utilization %	X	X	X	X
Garbage Collection Time	X	X	X	X
Garbage Collections Count	X		X	
Hung Threads Count	X	X	X	X
Memory Heap Free %	X	X	X	X
Memory Heap Size	X	X	X	X
Memory Heap Used	X	X	X	X
Memory Pool Size	X		X	
Memory Used	X		X	
PermGen Usage	X		X	
Request Count	X	X	X	X

Pre-Built KPIs – Application Server Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/ApplicationServerModuleKPIsandthresholds>

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
4xx Errors Count	Total transaction errors for the analyzed time window	Count	Normal: 0-5, Medium: 5-50, High: >50
5xx Errors Count	Total transaction errors for the analyzed time window	Count	Normal: 0, Medium: 1-25, High: >25
Active Threads Count	Total count of active threads.	Count	No predefined threshold values
Available Thread Count %	Amount of threads that are currently available.	Percentage	Normal: >20, Medium: 5-20, High: <5
Average Transaction Response Time	Average response time (ms) for successful transactions	ms	2-hour blocks every day (adaptive/quantile), adaptive thresholding enabled
Active Sessions Count	Currently active sessions on the application server.	Count	2-hour blocks every day (adaptive/quantile), adaptive thresholding enabled
CPU Utilization %	Amount of CPU utilized by the application server process instance	Percentage	Normal: <70, Medium: 70-90, High: >90
Garbage Collection Time (ms)	Processing time of garbage collection.	ms	No predefined threshold values
Garbage Collections Count	Total count of collected unused heap memory.	Count	No predefined threshold values
Hung Threads Count	Total count of hung threads.	Count	No predefined threshold values
Memory Heap Free %	Amount of Memory Heap available.	Percentage	Normal: <70, Medium: 70-90, High: >90
Memory Heap Size (MB)	Total size of Memory Heap.	MB	No predefined threshold values
Memory Heap Used (MB)	Amount of Memory Heap currently used by all applications.	MB	No predefined threshold values
Memory Pool Size	Total size of allocated memory blocks.	MB	No predefined threshold values
Memory Used (MB)	Count of total memory in use.	MB	No predefined threshold values
Perm Gen Usage (MB)	Total PermGen space currently in use.	MB	No predefined threshold values
Request count	Total number of requests over the analyzed time window.	Count	2-hour blocks every day (adaptive/quantile), adaptive thresholding enabled

Pre-Built KPIs – DataBase Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/IModules/DatabaseModuleKPIsandthresholds>

Database Module KPI Availability

The table below displays KPI availability based on the add-on that is used to collect data, and will display in its corresponding ITSI KPI swim lane.

KPI Name	Microsoft SQL Server Add-on	Oracle Add-on
Database Active Connection	X	X
Database Connection Pool Used%	X	X
Database Deadlock Rate	X	X
Database Query Response Time	X	X
Database Storage Read IOPS	X	X
Database Storage Write IOPS	X	X
Database Transaction Rate	X	X

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
Database Active Connection	The number of connections currently active per database instance.	Count/Numeral	Adaptive Thresholding Enabled
Database Connection Pool Used%	The percentage of the connection pool being used per database instance.	Percentage	Adaptive Thresholding Enabled
Database Deadlock Rate	The number of deadlocks per second per database instance.	Deadlocks per second	Adaptive Thresholding Enabled
Database Query Response Time	The average amount of time it takes for a query request to return a response per database instance.	Milliseconds	Adaptive Thresholding Enabled
Database Server Storage Read IOPS	The number of reads per second to storage per database instance.	Reads per second	Adaptive Thresholding Enabled
Database Server Storage Write IOPS	The number of writes per second to storage per database instance.	Writes per second	Adaptive Thresholding Enabled
Database Transaction Rate	The number of transactions per second per database instance.	Transactions per second	Adaptive Thresholding Enabled

Pre-Built KPIs – End Use Experience Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/EndUserExperienceMonitoringModuleKPIsandthresholds>

End User Experience Module KPI Availability

KPI Name	Android OS availability	iOS availability
Crash Count	x	x
Crash Rate	x	x
HTTP Error Rate	x	x
Network Error Rate	x	x
Network Latency	x	x
Page Load Time		x
Sessions Count	x	x
Unique Users Count	x	x

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
Crash Count	Average count of all unhandled crashes.	Count	Static: Normal: 0, High: > 50
Crash Rate	Average rate for unhandled crashes.	%	Static: Normal: > 0, Medium: > 25, High: > 75
HTTP Error Rate	Average rate for HTTP errors.	Count	Static: Normal: > 0, Medium: > 25, High: > 75
Network Error Rate	Average rate for network errors.	%	Static: Normal: > 0, Medium: > 25, High: > 75
Network Latency	Average latency for network requests.	ms	Static: Low: > 50, Normal: > 150, High: > 300
Page Load Time	Average time taken for pages to load.	ms	Static: Low: > 50, Normal: > 150, High: > 300
Sessions Count	Count of total number of sessions opened.	Count	Static: Low: > 10, Normal: > 50, High: > 100
Unique Users Count	Distinct count of unique users.	Count	Static: Low: > 5, Normal: > 50, High: > 100

Pre-Built KPIs – Load Balancer Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/IModules/LoadBalancerModuleKPIsandthresholds>

Load Balancer Module KPI Availability

KPI Name	Splunk Add-on for F5 Big-IP	Splunk Add-on for Citrix Netscaler
5XX Responses from Server	x	x
Availability	x	x
Client Connections	x	x
Client Throughput	x	x
Concurrent Sessions	x	x
CPU Utilization % By System	x	x
Failover	x	x
Memory Used % By System	x	x
Round Trip Time	x	x
Server Connections	x	x
Server Throughput	x	x
SSL Transactions per Second	x	x
System Storage Used % By System	x	x

Pre-Built KPIs – Load Balancer Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/IModules/LoadBalancerModuleKPIsandthresholds>

End User Experience Module KPI Availability

KPI Name	Android OS availability	iOS availability
Crash Count	x	x
Crash Rate	x	x
HTTP Error Rate	x	x
Network Error Rate	x	x
Network Latency	x	x
Page Load Time		x
Sessions Count	x	x
Unique Users Count	x	x

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
Crash Count	Average count of all unhandled crashes.	Count	Static: Normal: 0, High: > 50
Crash Rate	Average rate for unhandled crashes.	%	Static: Normal: > 0, Medium: > 25, High: > 75
HTTP Error Rate	Average rate for HTTP errors.	Count	Static: Normal: > 0, Medium: > 25, High: > 75
Network Error Rate	Average rate for network errors.	%	Static: Normal: > 0, Medium: > 25, High: > 75
Network Latency	Average latency for network requests.	ms	Static: Low: > 50, Normal: > 150, High: > 300
Page Load Time	Average time taken for pages to load.	ms	Static: Low: > 50, Normal: > 150, High: > 300
Sessions Count	Count of total number of sessions opened.	Count	Static: Low: > 10, Normal: > 50, High: > 100
Unique Users Count	Distinct count of unique users.	Count	Static: Low: > 5, Normal: > 50, High: > 100

Pre-Built KPIs – Operating System Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/OSModuleKPIsandthresholds>

Operating System Module KPI Availability

KPI Name	Splunk Add-on for Microsoft Windows	Splunk Add-on for Unix and Linux
CPU Utilization: %	X	X
CPU Utilization: Interrupts/second	X	X
CPU Utilization: System Threads	X	X
Memory Available: MB	X	X
Memory Free: %	X	X
Memory Operations: Paging	X	X
Memory Used: MB System	X	X
Network Utilization: Total packets/second (in/out)	X	X
Processor Queue Length: System	X	X
Storage Free Space: %	X	X
Storage Operations: Latency	X	X
Storage Operations: Total	X	X

Pre-Built KPIs – Operating System Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/OSModuleKPIsandthresholds>

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
CPU Utilization: %	Total average across all available CPU cores.	%	Normal: < 70, Medium: 70-90, High: > 90
CPU Utilization: Interrupts/second	Measures the number of CPU interrupts per second.	count	Adaptive thresholding - 2 hour window every day
CPU Utilization: System Threads	Measures the total number of threads (running and waiting) in the system.	count	Adaptive thresholding - 2 hour window every day
Memory Available: MB	Measures of the amount of memory available in the system.	count	Aggregate Thresholds
Memory Free: %	Detects memory overutilization across the system using free memory.	%	Normal: >40, Medium: 10-40, High: 0-10
Memory Operations: Paging	Measures the number of paging operations per second.	count	Aggregate Thresholds
Memory Used: MB System	Measures the amount of memory used in the system.	count	Aggregate Thresholds
Network Utilization: Total packets/second (in/out)	Measures the total packets transferred over all network interfaces.	count	Aggregate Thresholds
Processor Queue Length: System	Detects excessive processor load averages.	count	Normal: 0-1, Medium: 2-5, High: >5
Storage Free Space: %	Detects storage overutilization across the system using free storage space.	count	Normal: 25, Medium: 10, High: 0
Storage Operations: Latency	Measures the latency of all I/O operations to disk.	count	Adaptive thresholding - 3 hour window every day.
Storage Operations: Total	Measures the total number of storage operations per second.	count	Aggregate Thresholds

Pre-Built KPIs – Storage Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/StorageModuleKPIsandthresholds>

Storage Module KPI Availability

KPI Name	Splunk Add-on for NetApp ONTAP 7-mode	Splunk Add-on for NetApp ONTAP Cluster mode	Splunk Add-on for EMCVNX Block mode	Splunk Add-on for EMCVNX File mode
Storage Array CPU Utilization	x	x	x	x
Storage Array Highest Latency	x	x		
Storage Array IOPS	x	x	x	x
Storage Array Network Received Throughput	x	x		x
Storage Array Network Transmitted Throughput	x	x		x
Storage Array Read Latency	x	x		
Storage Array Read Throughput	x	x	x	x
Storage Array Storage Used	x	x	x	x
Storage Array Write Latency	x	x		
Storage Array Write Throughput	x	x	x	x
Storage Pool IOPS		x		
Storage Pool Storage Used	x	x	x	x
Volume Highest Latency	x	x		
Volume IOPS	x	x		x
Volume Read Latency	x	x		
Volume Read Throughput	x	x		x
Volume Write Latency	x	x		
Volume Write Throughput	x	x		x
LUN Highest Latency	x	x		
LUN IOPS	x	x	x	
LUN Read Latency	x	x		
LUN Read Throughput	x	x	x	

Pre-Built KPIs – Storage Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/StorageModuleKPIsandthresholds>

KPI and Threshold Reference Table

Storage Array Monitoring

KPI Name	KPI Description	Unit of measurement type	Threshold Values
Storage Array CPU Utilization	Percentage of the storage device CPU currently used	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical
Storage Array Highest Latency	Maximum time required for a storage system to process a single storage transaction (read and write)	ms	info
Storage Array IOPS	Count of the number of I/O operations per second	count	Adaptive – 7 days
Storage Array Network Received Throughput	The payload size of network received throughput	MBps	Adaptive – 7 days
Storage Array Network Transmitted Throughput	The payload size of network transmitted throughput	MBps	Adaptive – 7 days
Storage Array Read Latency	Read latency is the time required for a storage system to process a single read operation	ms	Low < 10 < Medium < 15 < High
Storage Array Read Throughput	The payload size of storage read operations	MBps	Adaptive – 7 days
Storage Array Storage Used	The percentage of storage capacity used	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical
Storage Array Write Latency	Write latency is the time required for a storage system to process a single write operation	ms	Low < 10 < Medium < 15 < High
Storage Array Write Throughput	The payload size of storage write operations	MBps	Adaptive – 7 days

Storage Pool Monitoring

KPI Name	KPI Description	Unit of measurement type	Threshold Values
Storage Pool IOPS	Count of the number of I/O operations per second	count	Adaptive – 7 days
Storage Pool Storage Used	The percentage of storage capacity used	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical

Pre-Built KPIs – Storage Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/StorageModuleKPIsandthresholds>

Volume Monitoring

KPI Name	KPI Description	Unit of measurement type	Threshold Values
Volume Highest Latency	Maximum time required for a storage volume to process a single storage transaction (read and write)	ms	Info
Volume IOPS	Count of the number of I/O operations per second	count	Adaptive – 7 days
Volume Read Latency	The time required for a storage volume to process a single read operation	ms	Low < 10 < Medium < 15 < High
Volume Read Throughput	The payload size of storage read operations	Adaptive – 7 days	MBps
Volume Write Latency	Write latency is the time required for a storage volume to process a single write operation	ms	Low < 10 < Medium < 15 < High
Volume Write Throughput	The payload size of storage write operations	MBps	Adaptive – 7 days

LUN Monitoring

KPI Name	KPI Description	Unit of measurement type	Threshold Values
LUN Highest Latency	The maximum time required for a LUN to process a single storage transaction (read and write)	ms	Info
LUN IOPS	Count of the number of I/O operations per second	count	Adaptive – 7 days
LUN Read Latency	The time required for a storage LUN to process a single read operation	ms	Low < 10 < Medium < 15 < High
LUN Read Throughput	The payload size of storage read operations	MBps	Adaptive – 7 days
LUN Write Latency	The time required for a storage LUN to process a single write operation	ms	Low < 10 < Medium < 15 < High
LUN Write Throughput	The payload size of storage write operations	MBps	Adaptive – 7 days

Disk Monitoring

KPI Name	KPI Description	Unit of measurement type	Threshold Values
Disk Highest Latency	The maximum time required for a storage disk to process a single storage transaction (read and write)	ms	Info
Disk IOPS	Count of the number of I/O operations per second	count	Adaptive – 7 days
Disk Read Blocks Throughput	The number of disk blocks read per second	count	Adaptive – 7 days
Disk Read Latency	Read latency is the time required for a storage disk to process a single read operation	ms	Low < 10 < Medium < 15 < High
Disk Read Throughput	The payload size of storage read operations	MBps	Adaptive – 7 days
Disk Write Blocks Throughput	The number of disk blocks written per second	count	Adaptive – 7 days
Disk Write Latency	The time required for a storage disk to process a single write operation	ms	Low < 10 < Medium < 15 < High
Disk Write Throughput	The payload size of storage write operations	MBps	Adaptive – 7 days

Pre-Built KPIs – Virtualization Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/VirtualizationModuleKPIsandthresholds>

Virtualization Module KPI availability

KPI Name	Splunk Add-on for VMware	Splunk Add-on for Microsoft Hyper-V
Hypervisor CPU Allocation	X	X
Hypervisor CPU Demand	X	
Hypervisor CPU Utilization	X	X
Hypervisor Memory Pages	X	X
Hypervisor Memory Provisioning	X	X
Hypervisor Memory Used	X	X
Hypervisor Network Utilization	X	X
Hypervisor Storage Highest Latency	X	X
Hypervisor Storage Read Latency	X	X
Hypervisor Storage Write Latency	X	X
Virtual Machine CPU Demand	X	
Virtual Machine CPU Utilization	X	X
Virtual Machine Memory Provisioning	X	X
Virtual Machine Memory Reserved	X	X
Virtual Machine Memory Used	X	
Virtual Machine Network Utilization	X	
Virtual Machine Storage Highest Latency	X	X
Virtual Machine Storage Read Latency	X	X
Virtual Machine Storage Used	X	X
Virtual Machine Storage Write Latency	X	X
Datastore Highest Latency	X	X
Datastore Read Latency	X	X
Datastore Storage Used	X	X
Datastore Write Latency	X	X

Pre-Built KPIs – Virtualization Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/VirtualizationModuleKPIsandthresholds>

KPI and Threshold Reference Table

Hypervisor Monitoring

KPI Name	Description	Unit Type	Threshold Values
Hypervisor CPU Allocation	The percentage of CPU resources allocated to all the VMs for the host.	%	Static: Low: < 30, Normal: < 50, Medium: < 75, High: < 90, Critical: > 90
Hypervisor CPU Demand	The amount of CPU resources a host would use if there were no CPU contention or CPU limit.	MHz	Adaptive - 7 days
Hypervisor CPU Utilization	Actively used CPU of the host, as a percentage of the total available CPU. Active CPU is approximately equal to the ratio of the used CPU to the available CPU.	%	Static: Low: < 30, Normal: < 50, Medium: < 75, High: < 90, Critical: > 90
Hypervisor Memory Pages	Pages/sec is the rate at which pages are read from or written to disk, to resolve hard page faults. This is a measure of memory pressure because it tracks hard faults. Hard faults are page faults that require disk access.	Count	Adaptive - 7 days
Hypervisor Memory Provisioning	The sum of all vmmemct(memory ballooning) values for all powered-on virtual machines, plus management server (e.g. vSphere) on the host. If the balloon target value is greater than the balloon value, the VMkernel inflates the balloon, causing more virtual machine memory to be reclaimed. If the balloon target value is less than the balloon value, the VMkernel deflates the balloon, which allows the virtual machine to consume additional memory if needed.	%	Adaptive - 7 days
Hypervisor Memory Used	Average memory usage as a percent of total memory.	%	Static: Low: < 30, Normal: < 50, Medium: < 75, High: < 90, Critical: > 90
Hypervisor Network Utilization	Network utilization (combined transmit- and receive-rates) across the host's physical adapter. Sum of data transmitted and received across all physical NIC instances connected to the host.	KBps	Adaptive - 7 days
Hypervisor Storage Highest Latency	Highest latency value across all disks used by the host. Latency measures the time taken to process an SCSI command issued by the guest OS to the virtual machine. The kernel latency is the time the VMkernel takes to process an IO request. The device latency is the time it takes the hardware to handle the request.	ms	Info: Low < 10 < Medium < 15 < High
Hypervisor Storage Read Latency	Average amount of time taken during the collection interval to process an SCSI read command issued from the Guest OS to the virtual machine. The sum of kernelReadLatency and deviceReadLatency.	ms	Static: Low < 10 < Medium < 15 < High
Hypervisor Storage Write Latency	Average amount of time taken during the collection interval to process an SCSI write command issued by the Guest OS to the virtual machine. The sum of kernelWriteLatency and deviceWriteLatency.	ms	Static: Low < 10 < Medium < 15 < High

Pre-Built KPIs – Virtualization Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/VirtualizationModuleKPIsandthresholds>

Virtual Machine Monitoring

KPI Name	Description	Unit Type	Threshold Values
Virtual Machine CPU Demand	The amount of CPU resources a virtual machine would use if there were no CPU contention or CPU limit.	MHz	Adaptive - 7 days
Virtual Machine CPU Utilization	Average CPU Usage in percent	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical
Virtual Machine Memory Provisioning	Amount of guest physical memory that is currently reclaimed from the virtual machine through ballooning. This is the amount of guest physical memory that has been allocated and pinned by the balloon driver.	MB	Adaptive - 7 days
Virtual Machine Memory Reserved	Amount of memory reserved by userworlds. ESX/ESXi provides a memory compression cache to improve virtual machine performance when you use memory overcommitment. Memory compression is enabled by default. When a host's memory becomes overcommitted, ESX/ESXi compresses virtual pages and stores them in memory.	MB	Adaptive - 7 days
Virtual Machine Memory Used	Average memory usage as a percent of total memory.	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical
Virtual Machine Network Utilization	Network utilization (combined transmit- and receive-rates) across the VM's virtual network adapter. Sum of data transmitted and received across all NIC instances connected to the VM.	KBps	Adaptive - 7 days
Virtual Machine Storage Highest Latency	Highest latency value across all disks used by the host. Latency measures the time taken to process an SCSI command issued by the guest OS to the virtual machine. The kernel latency is the time VMkernel takes to process an IO request. The device latency is the time it takes the hardware to handle the request.	ms	Info: Low < 10 < Medium < 15 < High
Virtual Machine Storage Read Latency	Average amount of time taken during the collection interval to process an SCSI read command issued from the Guest OS to the virtual machine. The sum of kernelReadLatency and deviceReadLatency.	ms	Low < 10 < Medium < 15 < High
Virtual Machine Storage Used	Amount of space actually used by the virtual machine. May be less than the amount provisioned at any given time, depending on whether the virtual machine is powered-off, whether snapshots have been created or not, and other such factors.	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical
Virtual Machine Storage Write Latency	Average amount of time taken during the collection interval to process an SCSI write command issued by the Guest OS to the virtual machine. The sum of kernelWriteLatency and deviceWriteLatency.	ms	Low < 10 < Medium < 15 < High

Datastore Monitoring

KPI Name	Description	Unit Type	Threshold Values
Datastore Highest Latency	Highest latency value across all disks used by the host. Latency measures the time taken to process an SCSI command issued by the guest OS to datastore.	ms	Info: Low < 10 < Medium < 15 < High
Datastore Read Latency	Average amount of time for a read operation from the datastore. Total latency = kernel latency + device latency.	ms	Static: Low < 10 < Medium < 15 < High
Datastore Storage Used	Amount of space actually used by the datastore.	%	Low < 30 < Normal < 50 < Medium < 75 < High < 90 < Critical
Datastore Write Latency	Average amount of time for a write operation from the datastore. Total latency = kernel latency + device latency.	ms	Static: Low < 10 < Medium < 15 < High

Pre-Built KPIs – Web Server Module

<http://docs.splunk.com/Documentation/ITSI/2.6.1/Modules/WebServerModuleKPIsandthresholds>

Web Server Module KPI Availability

The table below displays KPI availability based on use of the supported Web Server Module technologies.

If there is data in the ITSI swim lanes, the corresponding KPI field is checked (X), otherwise, it is empty.

KPI Name	Splunk Add-on for Apache Web Server	Splunk Add-on for Microsoft IIS
4xx Errors	X	X
5xx Errors	X	X
Availability	X	X
Bytes In	X	X
Bytes Out	X	X
Hits Per Minute	X	X
Percent Error Codes	X	X
Response Times	X	X

Web Server Module KPIs

KPIs to collect various web server transaction and performance metrics

KPI Name	Description	Unit Type	Threshold Values
4XX Errors	The count of 4xx response statuses	Count	Adaptive: 7 Days
5XX Errors	The count of 5xx response statuses	Count	Adaptive: 7 Days
Bytes In	Sum of bytes from requests to the server (search is run every 5 minutes)	kB	Adaptive: 7 Days
Bytes Out	Sum of bytes sent out from the server (search is run every 5 minutes)	kB	Adaptive: 7 Days
Hits Per Minute	Number of requests handled per minute by the web server	RPS (requests per second)	Adaptive: 7 Days
Percent Error Codes	The percentage of total responses that resulted in a 4xx or 5xx error code	Percentage	High: 10 Medium: 5-10 Normal: 0-5
Response Times	The average response time for all requests	ms	Adaptive: 7 Days
WebServer Availability	Percent of successful transactions out of total transactions	Binary	None