

How To Keep Your Boss, And Their Bosses Happy (And Still Sleep At Night!) With IT Service Intelligence And Splunk

Jon LeBaugh

ITOA Architect, Splunk

.conf2016

splunk >

Disclaimer

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 the 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 IT Service Intelligence

Data-driven service monitoring and analytics



Dynamic
Service Models



At-a-Glance
Problem Analysis



Early Warning
on Deviations



Simplified Incident
Workflows

SPLUNK IT SERVICE INTELLIGENCE

splunk> Platform for Machine Data

Time-Series Index

Schema-on-Read

Data Model

Common
Information Model

Today's Talk

- War Stories.
- Management Personas & Responsibilities.
- Specific Benefits of ITSI.
- Sleep.

Personas – “Jason”



- Middle Manager.
- Responsible for day to day operations.
- Not overly technical, but sometimes thinks he is.
- “Block and Tackle” guy.
- Always coming up with new ideas.
- Moves on to new things... Quickly.



Personas - “E.B.”



- Director, Development
- Responsible for Technical Direction and ‘Care and Feeding’ of a real time, highly distributed, high availability business service
- Needs accurate data quickly to prioritize development and troubleshoot real time incidents
- Known to make really bad jokes and/or “sing” on long incident calls



Personas - “Tom”



- Vice President – Information Technology
- Worked his way up through the technical ranks – and it shows
- Responsible to the business for meeting SLA’s and guaranteeing availability
- Loves a good dashboard
- Very involved
- Pretty sure he hasn’t slept more than 2 hours a night in a decade



Personas - “Jon”



- Senior Analyst
- Stunningly handsome
- Jack of many trades, master of none
- Responsible for keeping the lights on
 - Usually the first call for escalated incidents
- Is a big fan of sleep
- Generally awesome
- This is what happens when they let me make a slide about myself

A story about a database...

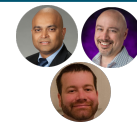
- “Breaks often.”
- Disjointed tools – specific to teams
- Slow time to value
- Multiple workflows for the same end goal
- Confusion
- Hyper sensitivity
- Post event reports are time consuming and monotonous

Current Challenges

Service Aware Monitoring



Performance data and alerts lack business context



Troubleshooting



*Answering not just the **what** but the **why***



Visibility



Putting all the data at everyone's disposal



Analytics



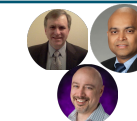
Answering questions your vendors did not anticipate



Problem Detection



Being alerted before your help desk calls



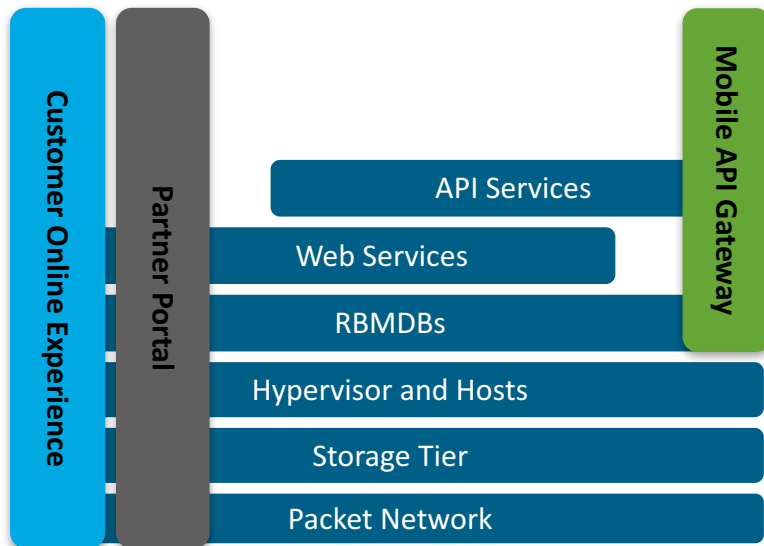
Why Splunk IT Service Intelligence

Service Aware approach maximizes Splunk value

Integrated solution based on customer successes

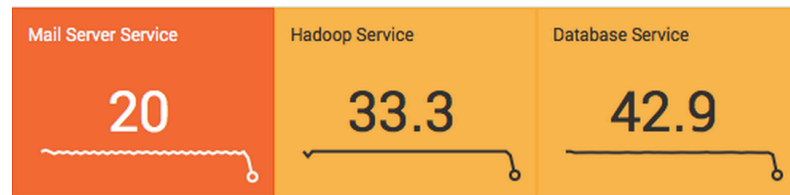
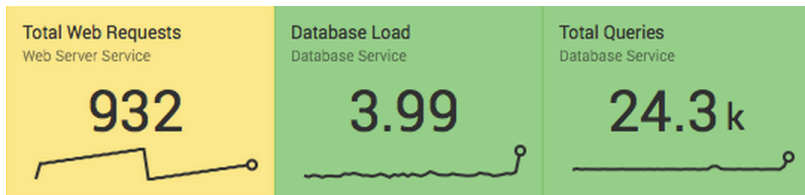
Instant, IT-focused value built on Splunk platform

Services



In ITSI a **Service** is a logical group of technology components that a user deems need to be monitored together. KPIs and Health scores constitute the means by which Services are monitored. Services can be IT Services/Tiers like the Storage Tier or they can be more abstract concepts like a Partner Portal, which encompass several tiers.

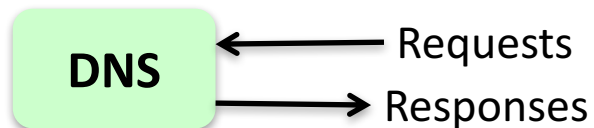
KPIs and Health scores



A **Key Performance Indicator (KPI)** is a Splunk saved search created within the ITSI UI that helps monitor a specific field like CPU, Memory, Number of Errors and so on. KPIs are contained within Services.

A **Health score** is a score from 0-100 (0 being critical and 100 being normal) that helps determine the health of a Service. It is calculated based on all KPIs importance and its status (e.g. green, orange, red), once every minute.

What is a KPI?



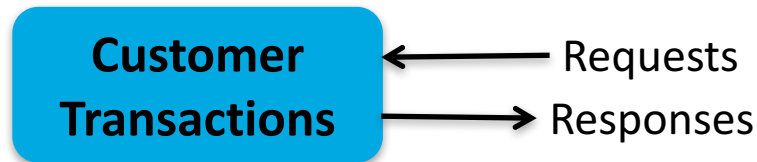
KPI: Number of requests

KPI: Error rate

KPI: Average response time

KPI: Servicer CPU load

KPI: Server network I/F errors



KPI: Number of transactions

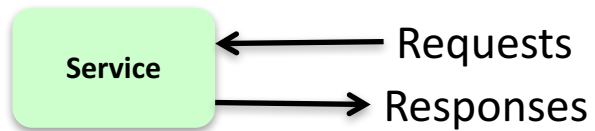
KPI: Error rate

KPI: Average response time

KPI: Count of Incident Tickets

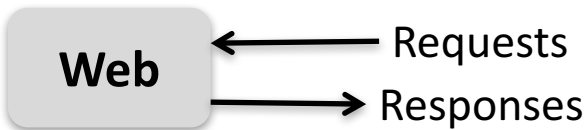
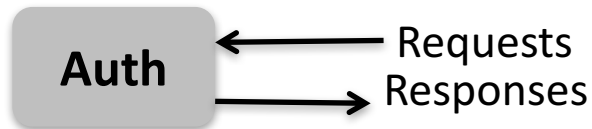
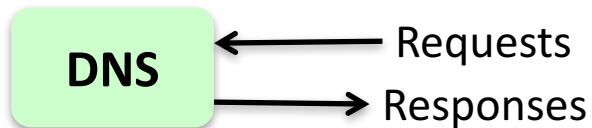
KPI: Synthetic Transx Health

What is a Service?



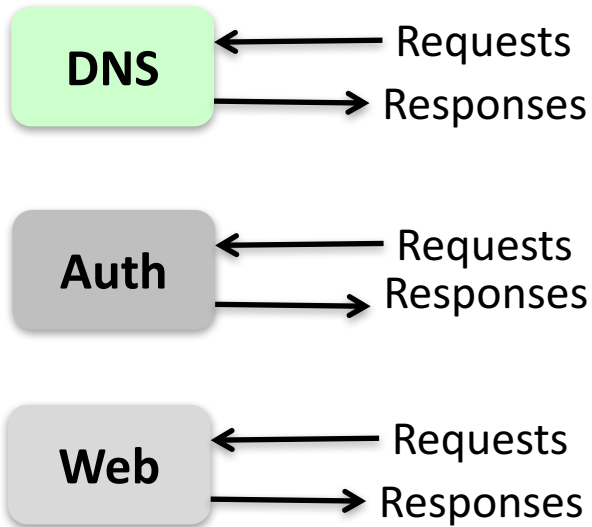
What is a Service?

Technical Services

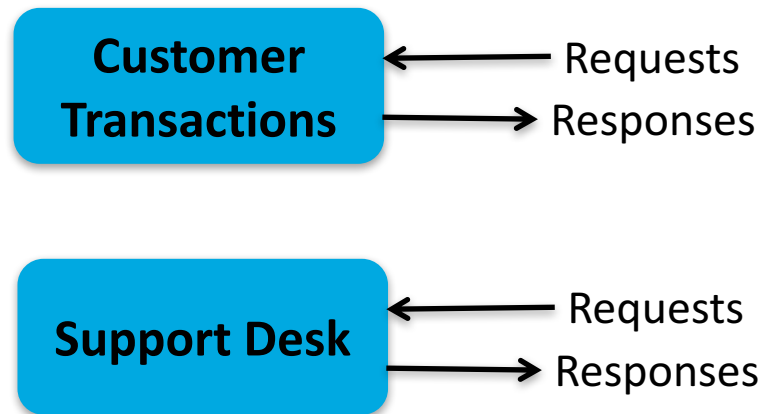


What is a Service?

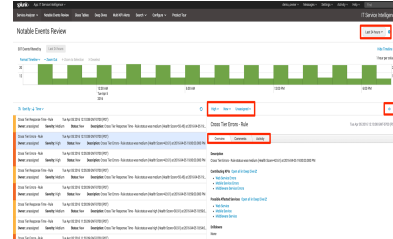
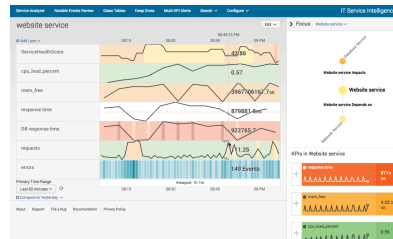
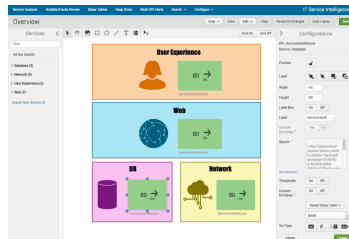
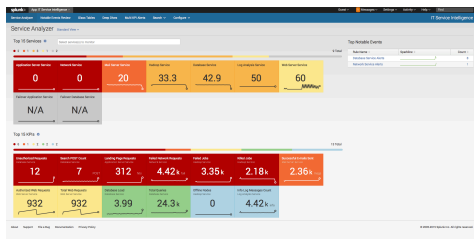
Technical Services



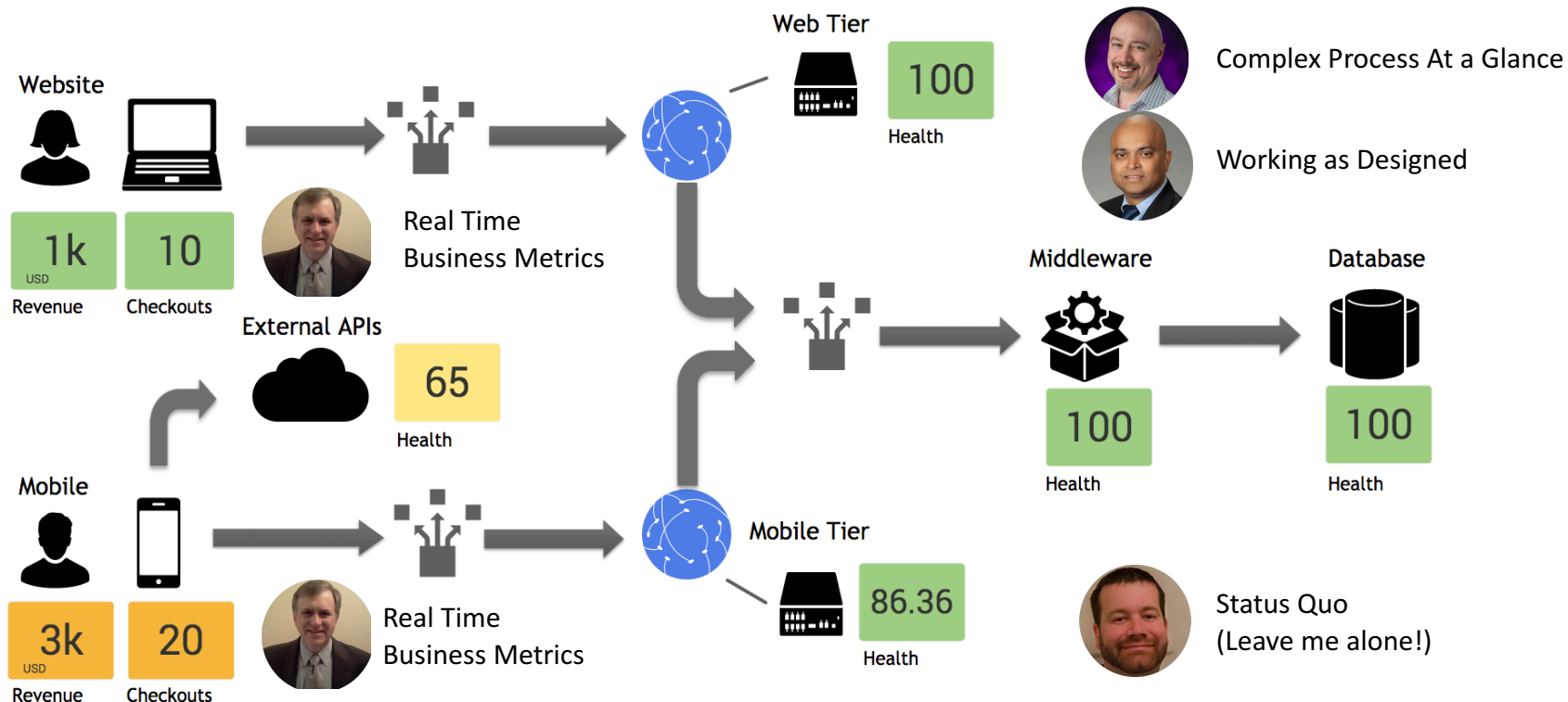
Business Services



Service Analyzer, Glass Tables, Deep Dives, Multi KPI Alerts



- Service Analyzer** – Auto generated filterable and tiled view of Service Healthscores and KPIs
- Glass Tables** – Customizable free form drawing dashboards to view Healthscores and KPIs of choice with visual tools to create context
- Deep Dives** – Swim lane analysis dashboard to show all those indicators over time for investigations
- Multi KPI Alerts** – Visual tool to create correlation searches based on KPIs



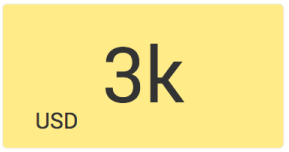
All values are per minute



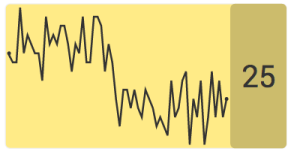
Store Status



Health score



Revenue per minute



Checkouts per minute
(Last 1 hour)



Create Any Dashboard Easily



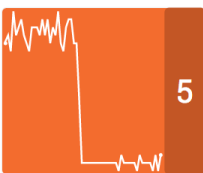
Simple & Effective - perfect for the CxO



Website Component



Revenue per minute



Checkouts per minute
(Last 1 hour)

Mobile Component



Revenue per minute



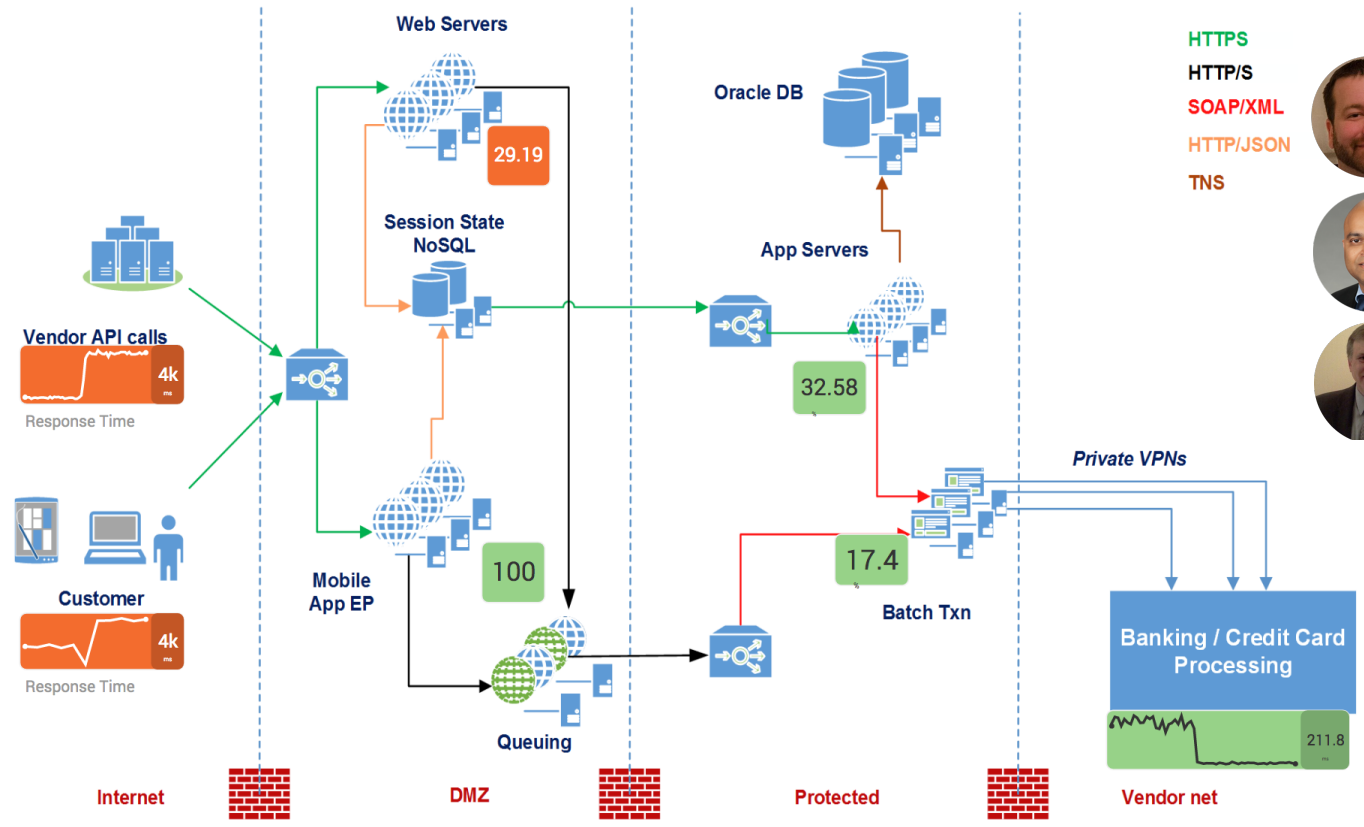
Checkouts per minute
(Last 1 hour)



Zero time spent gathering additional data, or building dashboards.

On Line Transaction Service

Now Edit



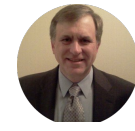
- HTTPS
- HTTP/S
- SOAP/XML
- HTTP/JSON
- TNS



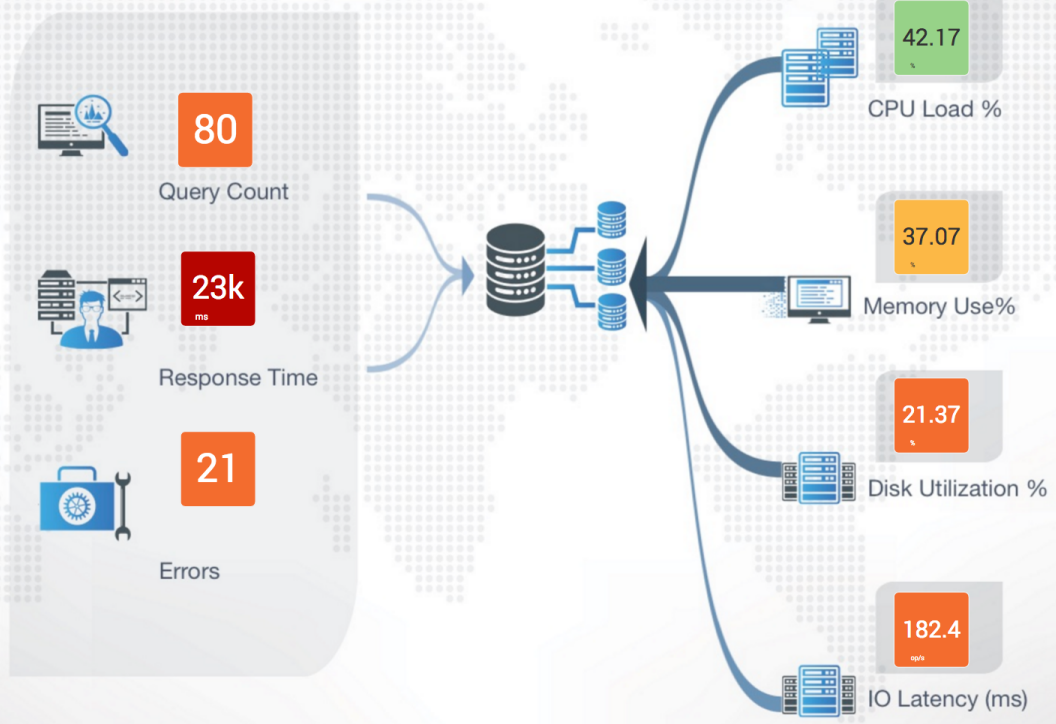
Technical at a glance
- Even at 3 AM.



Change verification
- Real time.

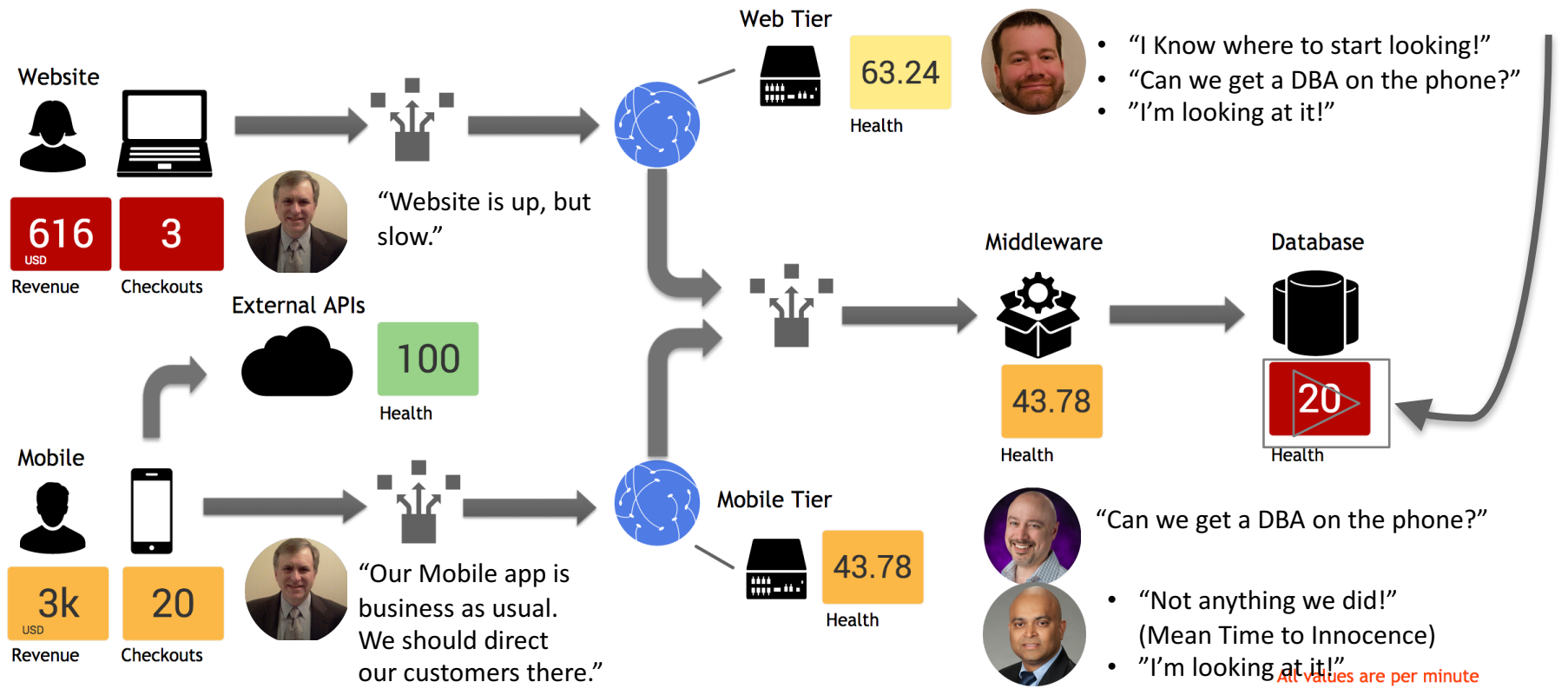


Hates sleep
for some reason.



As detailed as I want to get!

End to End Health

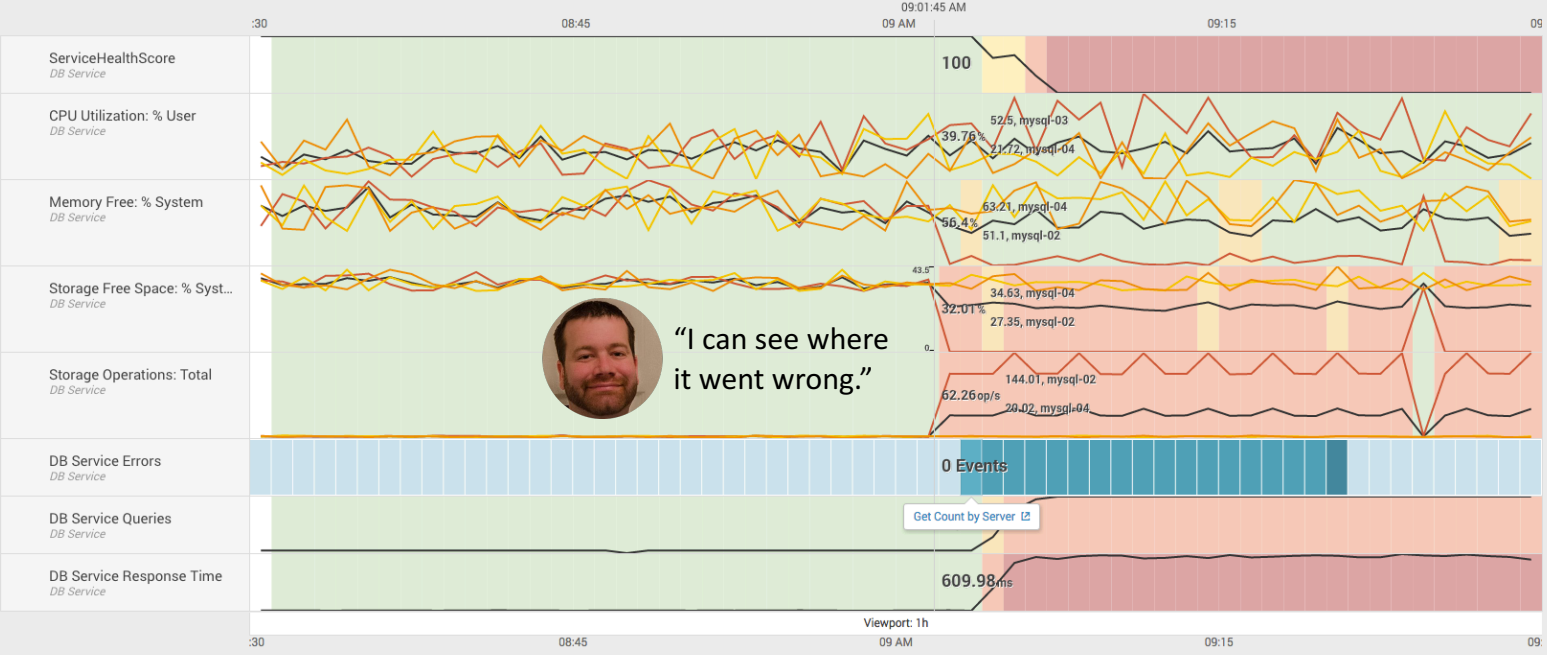


DB Deep Dive

Date time range Save as... Save

Bulk Actions

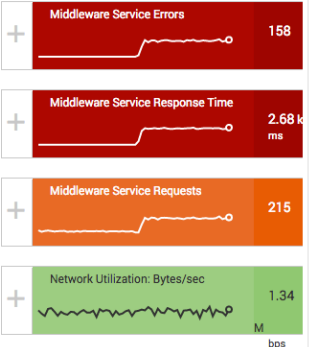
+ Add Lane Compare to ...



Focus: Middleware Service



KPIs in Middleware Service

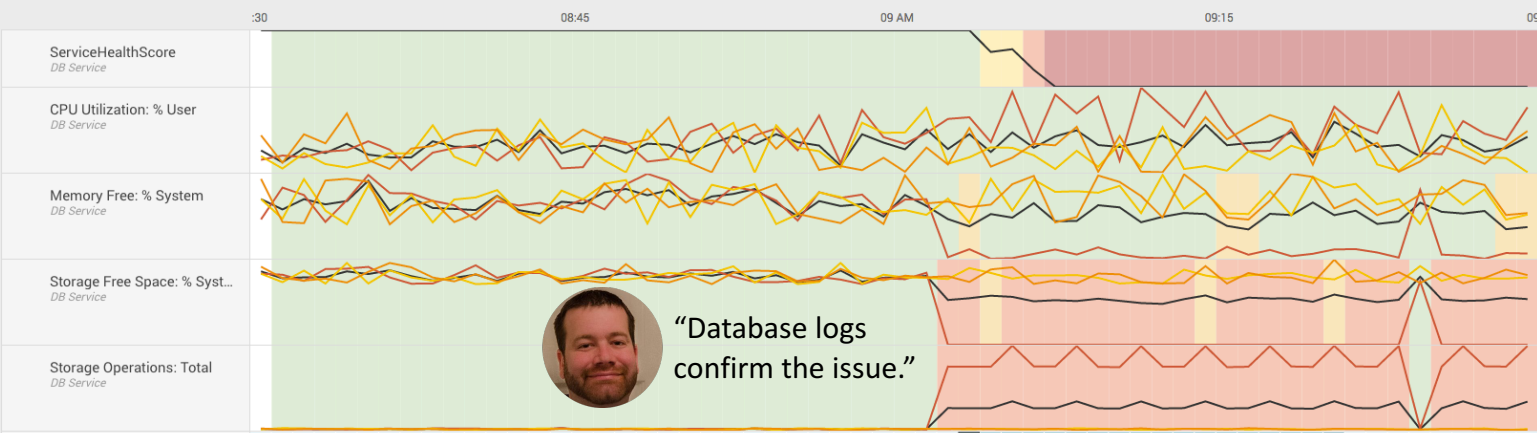



DB Deep Dive

Date time range Save as... Save

Bulk Actions


+ Add Lane Compare to ...

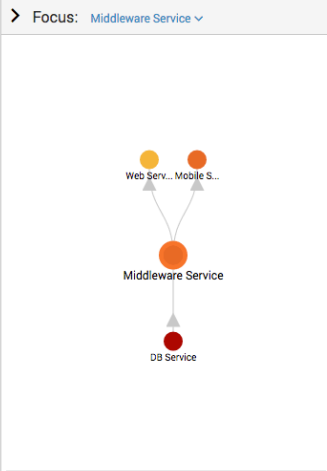


 "Database logs confirm the issue."

5 Events View in Search Hide Events

	Time	Event
1	7/22/16 2:03:53.797 PM	22-Jul-2016 14:03:53:79713 [CRITICAL] Could not write to file '/mysqllog/binlog/localhost_3306-bin' for logging (error 28) host = mysql-02 ; source = /usr/local/mysql/logs/mysqld.log ; sourcetype = mysqld
2	7/22/16 2:03:53.541 PM	22-Jul-2016 14:03:53:54131 [CRITICAL] /opt/mysql/bin/mysqld: Disk is full writing '/mysqllog/binlog/localhost_3306-bin.000020' (Errcode: 28). Waiting for someone to free space... Retry in 60 secs host = mysql-02 ; source = /usr/local/mysql/logs/mysqld.log ; sourcetype = mysqld
3	7/22/16 2:03:53.365 PM	22-Jul-2016 14:03:53:365627 [CRITICAL] /opt/mysql/bin/mysqld: Disk is full writing '/mysqllog/binlog/localhost_3306-bin.000020' (Errcode: 28). Waiting for someone to free space... Retry in 60 secs host = mysql-02 ; source = /usr/local/mysql/logs/mysqld.log ; sourcetype = mysqld
4	7/22/16 2:03:53.232 PM	22-Jul-2016 14:03:53:232665 [CRITICAL] Error writing file '/mysqllog/binlog/localhost_3306-bin' (error 28) host = mysql-02 ; source = /usr/local/mysql/logs/mysqld.log ; sourcetype = mysqld
5	7/22/16 2:03:53.039 PM	22-Jul-2016 14:03:53:039410 [CRITICAL] Error writing file '/mysqllog/slow_log/localhost_3306_slow_queries.log' (errno: 1) host = mysql-02 ; source = /usr/local/mysql/logs/mysqld.log ; sourcetype = mysqld

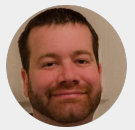
 "I will let the business know we have root cause."



KPIs in Middleware Service

- Middleware Service Errors: 158
- Middleware Service Response Time: 2.68 ms
- Middleware Service Requests: 215
- Network Utilization: Bytes/sec: 1.34 bps

OS Host Details



"This server is in trouble!"

Total Storage Used (%)
0.2 TB / 0.4 TB



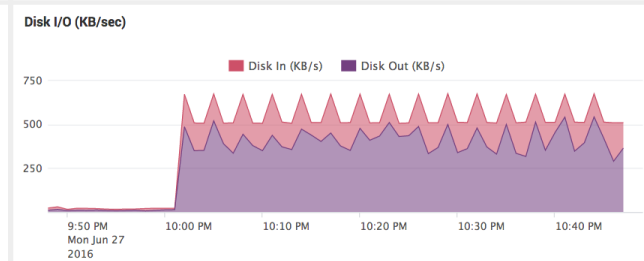
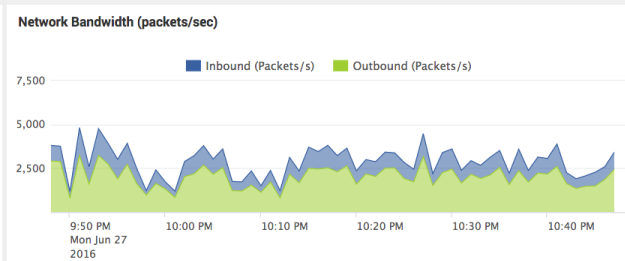
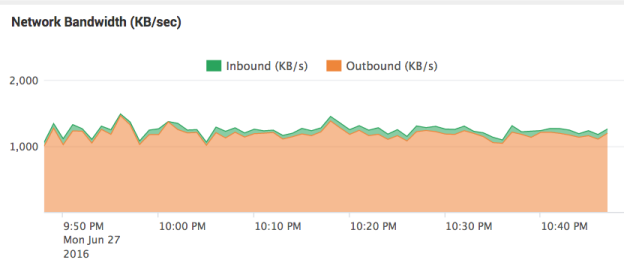
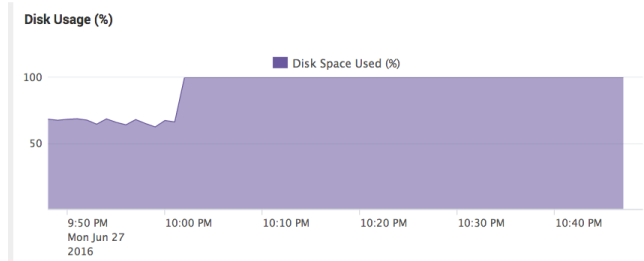
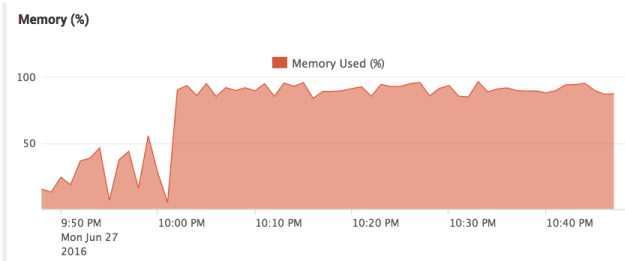
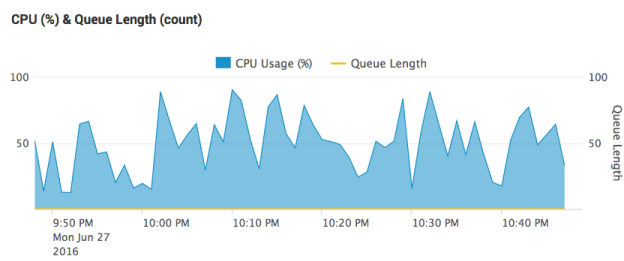
Host Events (count)
1,014 events



CPU Usage (%)
Range: 3.0 - 68.1%, Average: 33.5%

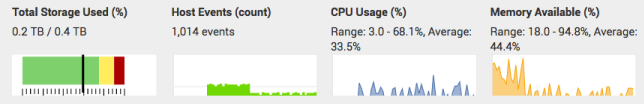


Memory Available (%)
Range: 18.0 - 94.8%, Average: 44.4%



OS Host Details

Edit More Info Last 1 hour



Overview CPU Memory Storage Splunk_Events

Filesystems

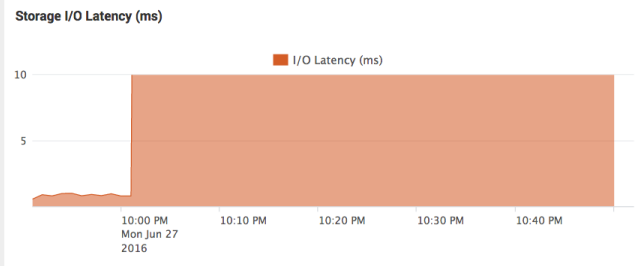
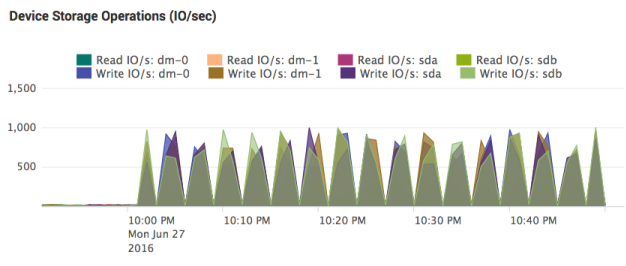
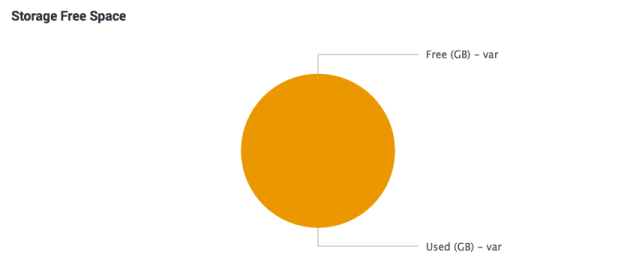


"Right here."

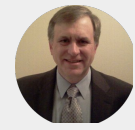
Device	% Free	Size	Used
/	44.80	931G	526643
etc	41.10	931G	561664
home	35.80	931G	612250
var	0.00	931G	953344

Device IO Statistics

Device	Read Ops/s	Total Ops/s	Write Ops/s
dm-0	2.50	9.90	7.37
dm-1	17.70	31.40	13.74
sda	19.11	31.54	12.43
sdb	6.08	7.76	1.68



"Good Job!"

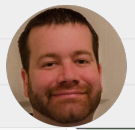


"Get this man a raise!"

DB Deep Dive

Last 60 minutes Save as... Save

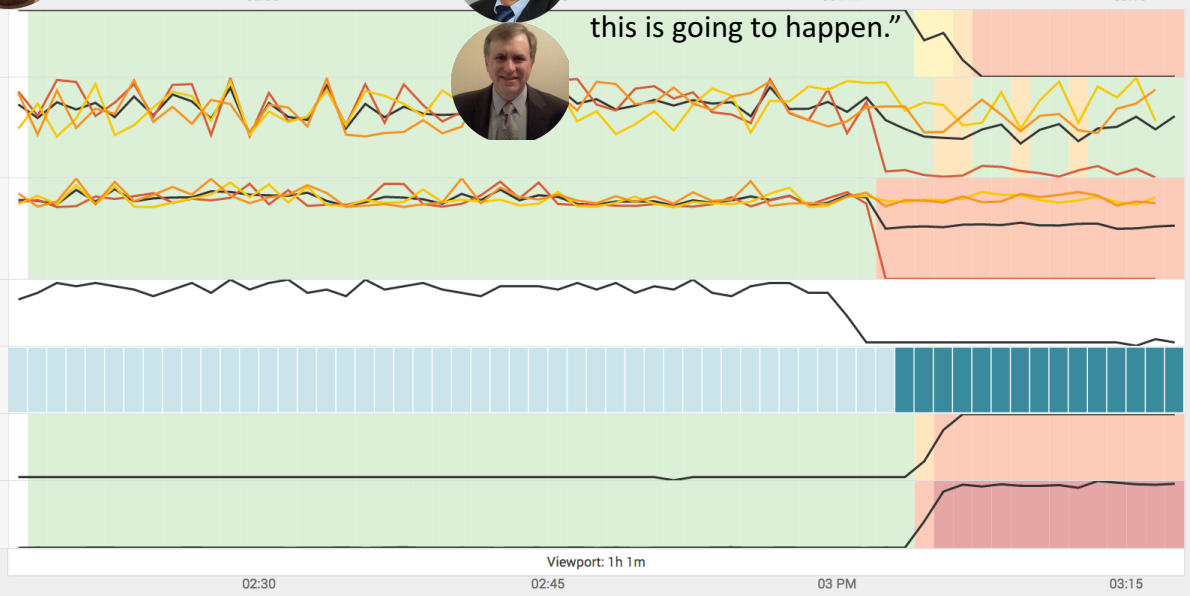
- Bulk Actions
 - Create Multi KPI Alert
 - Show State Thresholds
 - Show Level Thresholds
 - Hide Thresholds
 - Show Entity Overlays
 - Hide Entity Overlays
 - Delete



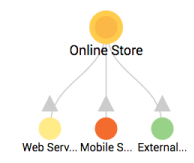
"On it!"



"We need to know when this is going to happen."



Focus: Online Store



KPIs in Online Store

- Online Store Successful Web Store Cher 4
- Online Store Web Store Revenue 492
- Online Store Successful Mobile Checko 16

Multi KPI Alerts

Create Correlation Search based upon selected KPIs

Composite score Status over time Last 60 minutes

1. Services

Select services that contain KPIs for your alert. Include service dependencies?

- Deselect All**
- DB Service
 - Depends on
 - Impacts
 - External APIs
 - Middleware Service
 - Mobile Service
 - Online Store
 - Depends on
 - Impacts
 - Propulsion
 - Shields
 - Sick Bay
 - USS Enterprise (NCC-170...)
 - Web Service

2. KPIs in Selected Services

+Add Selected *View Selected in Deep Dive filter 10 Per Page

« prev 1 2 next »

i	<input type="checkbox"/>	Add	KPI	Service	Percentage Status Breakdown	Latest Status
>	<input type="checkbox"/>	+ Add	CPU Utilization: % User	DB Service		Normal
>	<input type="checkbox"/>	+ Add	DB Service Errors	DB Service		High
>	<input type="checkbox"/>	+ Add	DB Service Queries	DB Service		High
>	<input type="checkbox"/>	+ Add	DB Service Response Time	DB Service		Critical
>	<input type="checkbox"/>	+ Add	Memory Free: % System	DB Service		Critical
>	<input type="checkbox"/>	+ Add	Storage Free Space: % System	DB Service		Critical
>	<input type="checkbox"/>	+ Add	Storage Operations: Total	DB Service		High
>	<input type="checkbox"/>	+ Add	Online Store Mobile Revenue	Online Store		Medium

3. Selected KPIs

The associated correlation search runs when severity-level thresholds exceed trigger conditions

Composite Score: 20 ■ Critical
Range: Critical 0-20, High 20-40, Medium 40-60, Low 60-80, Normal 80-100

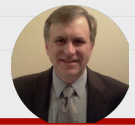
-Remove Selected *View Selected in Deep Dive filter 10 Per Page

i	<input type="checkbox"/>	Remove	KPI	Service	Latest Status	Importance
>	<input checked="" type="checkbox"/>	- Remove	Storage Free Space: % System	DB Service	Critical	<input type="range" value="10"/>
>	<input checked="" type="checkbox"/>	- Remove	DB Service Response Time	DB Service	Critical	<input type="range" value="10"/>
>	<input checked="" type="checkbox"/>	- Remove	Online Store Successful Web Store Checkouts	Online Store	Critical	<input type="range" value="5"/>

Service Analyzer

1 hour window Save as... Save Large Tiles

Filter Services Select service(s) to monitor



“There is a lot of red here... this can’t be good.”

Top 50 Services

3 2 3 2

10 Total

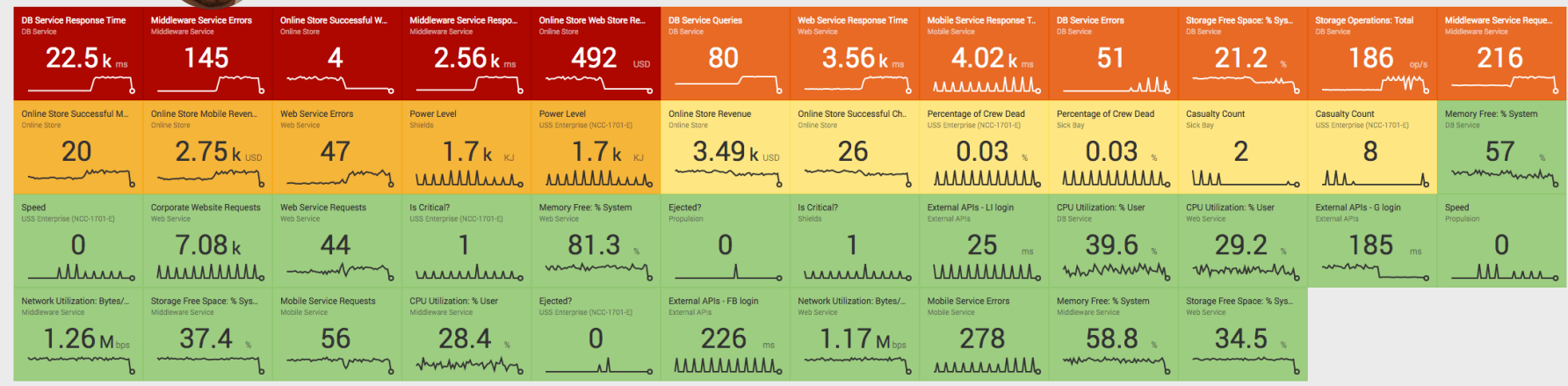


Top 50 KPIs

6 7 5 6 23

46 Total

“We should start here.”



Service Analyzer

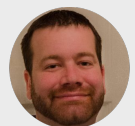
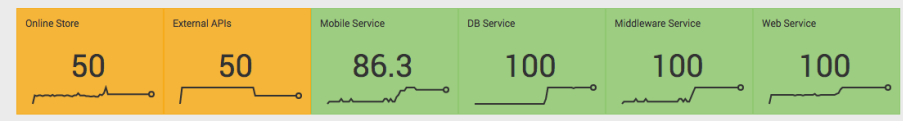
1 hour window Save as... Save Large Tiles

Filter Services x Middleware Service x Web Service x Mobile Service x External APIs x DB Service x Online Store

Top 50 Services

2 4

6 Total



“Status Quo.”
(Leave me alone.)

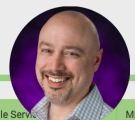
Top 50 KPIs

1 2 1 1 1 29

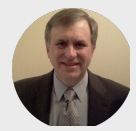
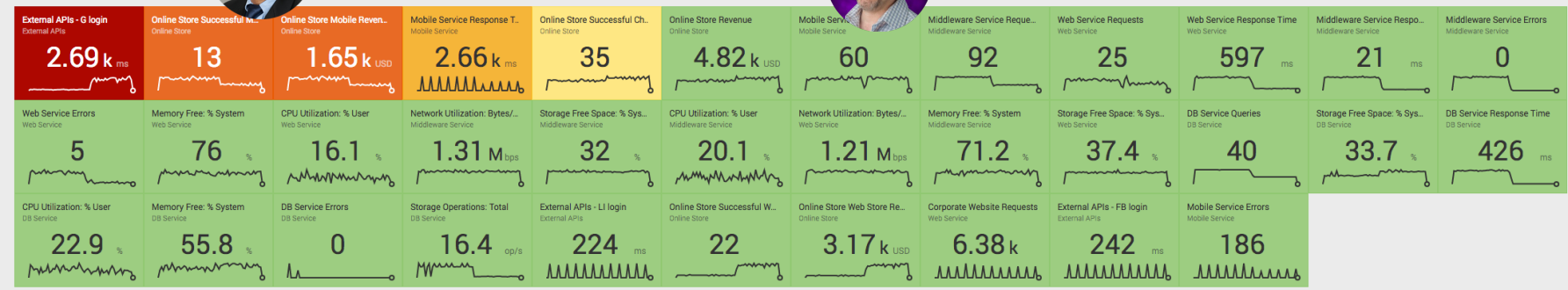
34 Total



“We should focus our development here.”



“Look, A Squirrel!”



“I need to have a conversation
with our vendor.”

Takeaways

- Avoid Dad jokes
- Find trouble
- Chase squirrels
- Sleep at night!

What Now?

Related breakout sessions and activities...

- Live demo at booth XYZ
- Sandbox
- Sign up for Glass Table Exercise

THANK YOU

.conf2016

