

.conf2015

Splunk: Uniting Ops and Dev (before DevOps was cool)

Grace Sumner

Sr. Production Operations
Engineer, EnerNOC

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.

Agenda

- EnerNOC
- Splunk and EnerNOC
 - Dev and Ops and Dev ...
- Splunk raises all ships (my story)
- Our pain is your gain (lessons learned)
- Q&A

The Power of **splunk**>

**COLLECT DATA
FROM ANYWHERE**

**SEARCH
AND ANALYZE
EVERYTHING**

**GAIN REAL-TIME
OPERATIONAL
INTELLIGENCE**

ENERNOC

.conf2015

4

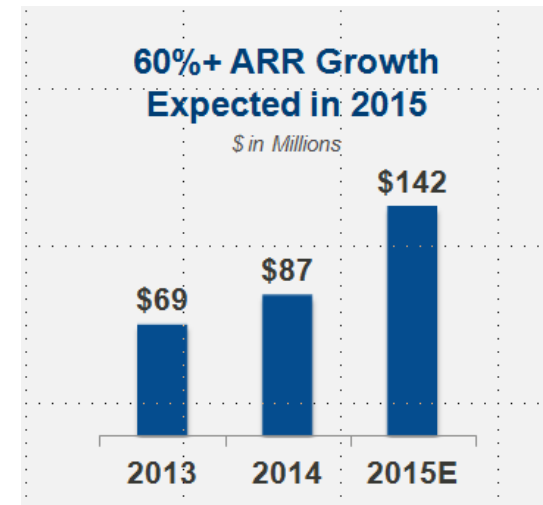
splunk>

About Grace

- ...Actually, lets do that later.

EnerNOC at a Glance

- A leading provider of SaaS-based Energy Intelligence Software (EIS) and related solutions
- Market leader in demand response (DR)
- Global company (over 1,300 employees in countries across North America, APAC, Europe) with HQ in Boston, MA



ENOC
NASDAQ
LISTED

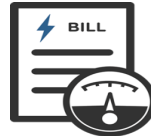
EnerNOC's Energy Intelligence Software

For enterprises: platform and solutions focus on the 3 drivers of energy expense



How you buy it

Budgets and Procurement
Utility Bill Management (UBM)



How much you use

Visibility and Reporting
Facility Optimization
Project Tracking



When you use it

Demand Response
Demand Management



.conf2015

2015

splunk>

Increase Use of Enterprise Energy Intelligence Software

EnerNOC Is Transforming Energy Management Across Industries



Over **6,000** companies globally rely on EnerNOC to drive energy savings



More than **70,000** sites and devices stream data into EnerNOC's energy intelligence software platform

Demonstrated expertise trusted by the largest companies in the world:

SEARS

ExxonMobil

CSU The California State University



Blommer
CHOCOLATE



American Red Cross



Leggett & Platt
INCORPORATED



pepsi



Kimberly-Clark

Morgan Stanley

CATERPILLAR®

CBRE

Coca-Cola

BASF

The Chemical Company

.conf2015

Utility and Grid Operator Partnerships

EnerNOC has Extensive Expertise Working With Utilities and Grid Operators Globally

Our utility partners include:

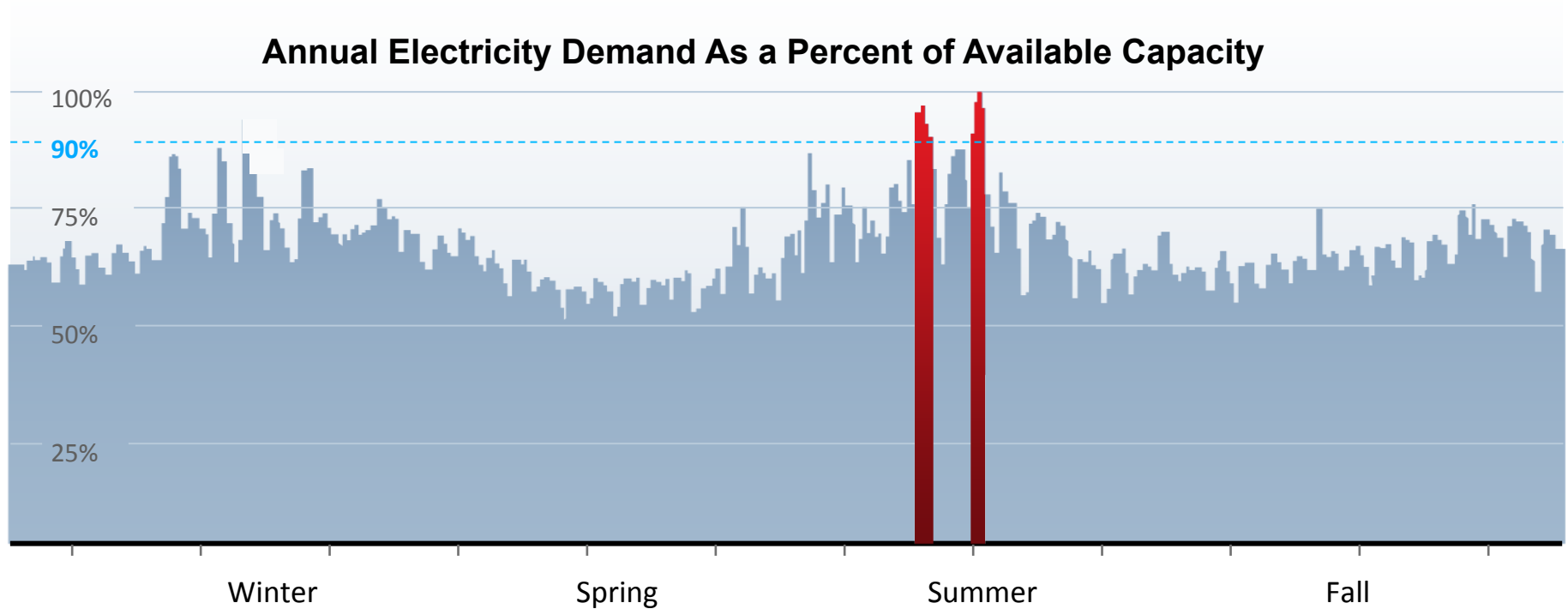


We also operate in wholesale markets:



The Case for Demand Response

Balancing supply and demand on the electricity grid is difficult and expensive. End users that provide a balancing resource are compensated for the service.



Ops vs Ops



Ops vs Ops



ENERNOC

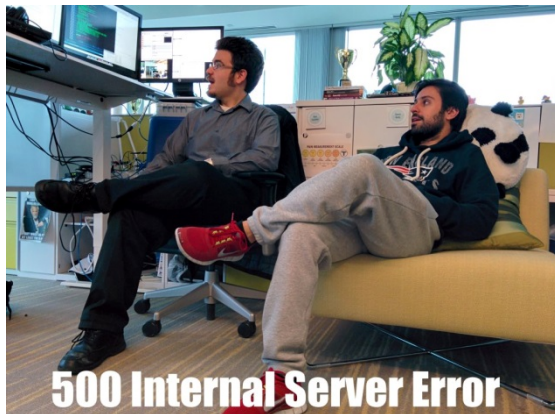
.conf2015

2015

12

splunk>

Usually when we talk about Dev Ops:

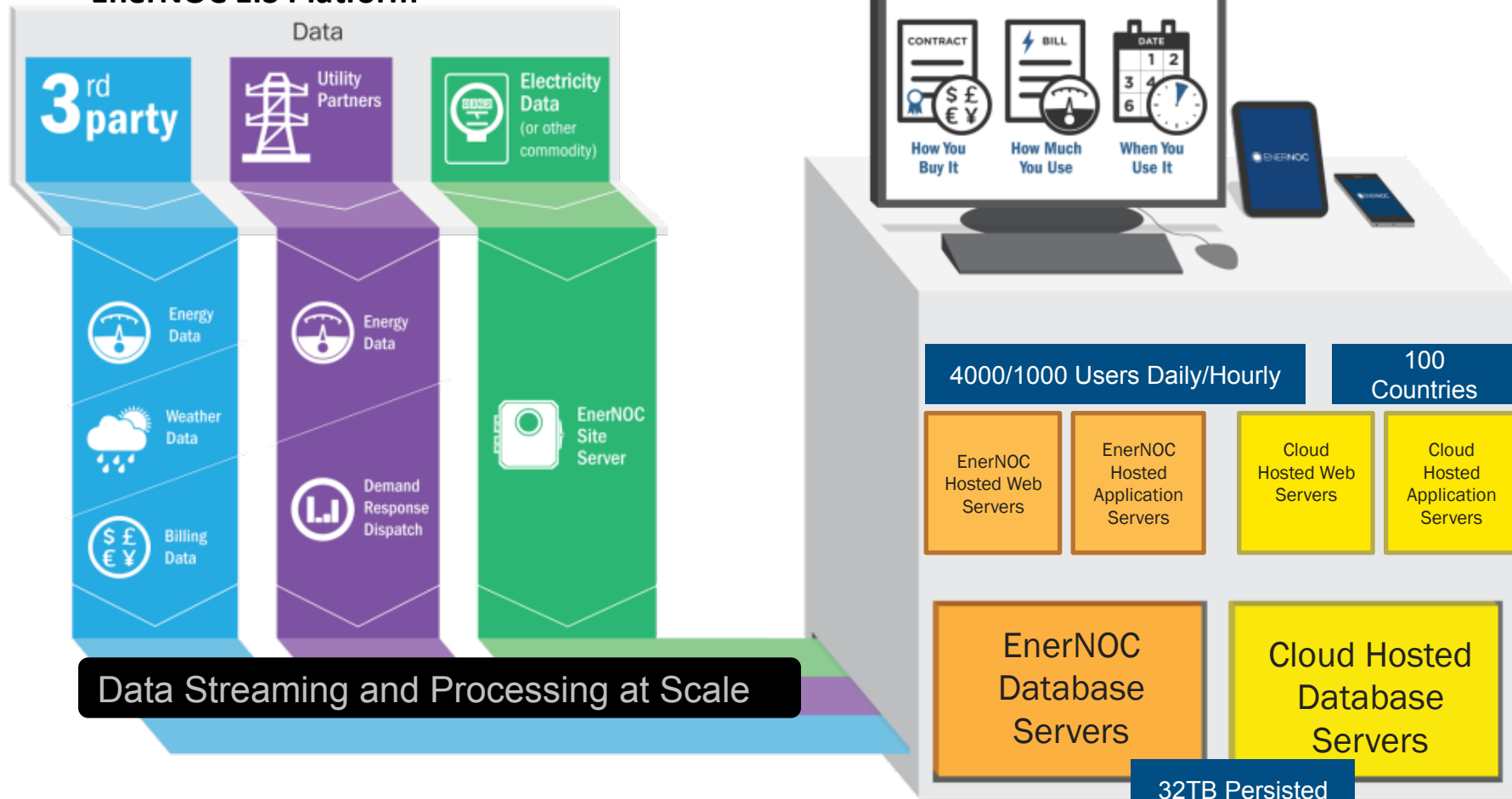


ENERNOC

EnerNOC ♥ Data

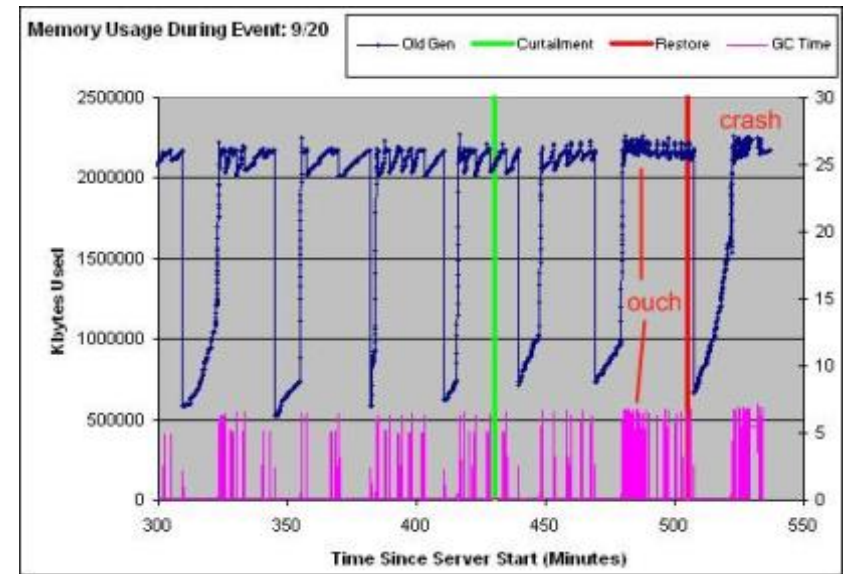
- As an **energy company**, we like to measure things:
 - Staff of HVAC experts with decades of experience to guide what to measure (air flow, temperature inside and out)
 - Add metrics based on customer needs
- As a **technology company**, we really like to measure things:
 - Performance engineers, architects and developers with years of experience to guide what to measure
 - Add metrics based on what Ops needs

EnerNOC EIS Platform



Before Splunk in Eng

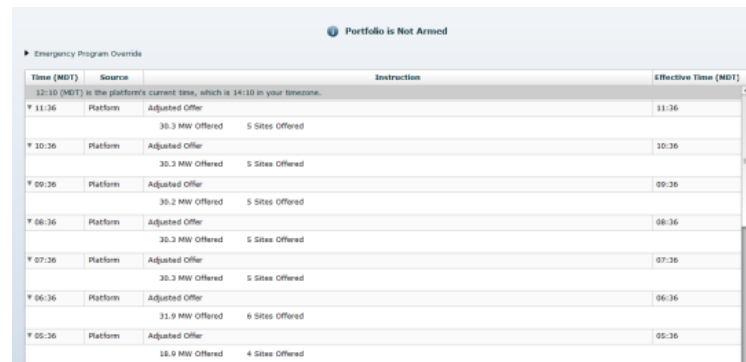
- Cron jobs
- Perl scripts to process log files, insert data
- “Huge” mysql databases
- Manually send emails with slick Excel charts and PowerPoint
- New metrics could take weeks
- Files being copied all over
- Ran out of disk one day...



Before Splunk in Ops

Tight regulations

- 2 second data
- 2ms response requirements
- 24x7x365 participation

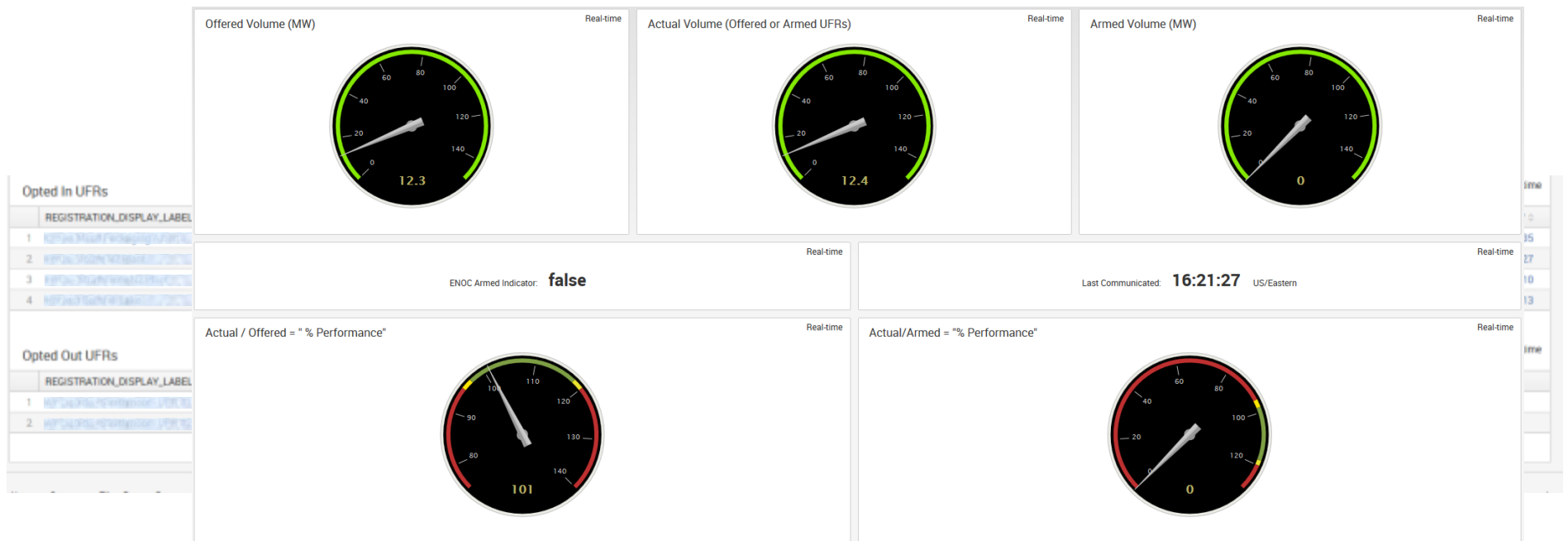


Time (MDT)	Source	Instruction	Effective Time (MDT)
12:10 (MDT) is the platform's current time, which is 14:10 in your timezone.			
11:36	Platform	Adjusted Offer	11:36
		30.3 MW Offered 5 Sites Offered	
10:36	Platform	Adjusted Offer	10:36
		30.3 MW Offered 5 Sites Offered	
09:36	Platform	Adjusted Offer	09:36
		30.2 MW Offered 5 Sites Offered	
08:36	Platform	Adjusted Offer	08:36
		30.3 MW Offered 5 Sites Offered	
07:36	Platform	Adjusted Offer	07:36
		30.3 MW Offered 5 Sites Offered	
06:36	Platform	Adjusted Offer	06:36
		31.9 MW Offered 6 Sites Offered	
05:36	Platform	Adjusted Offer	05:36
		18.9 MW Offered 4 Sites Offered	

Ops tools provide

- High level aggregates
- Hourly updates

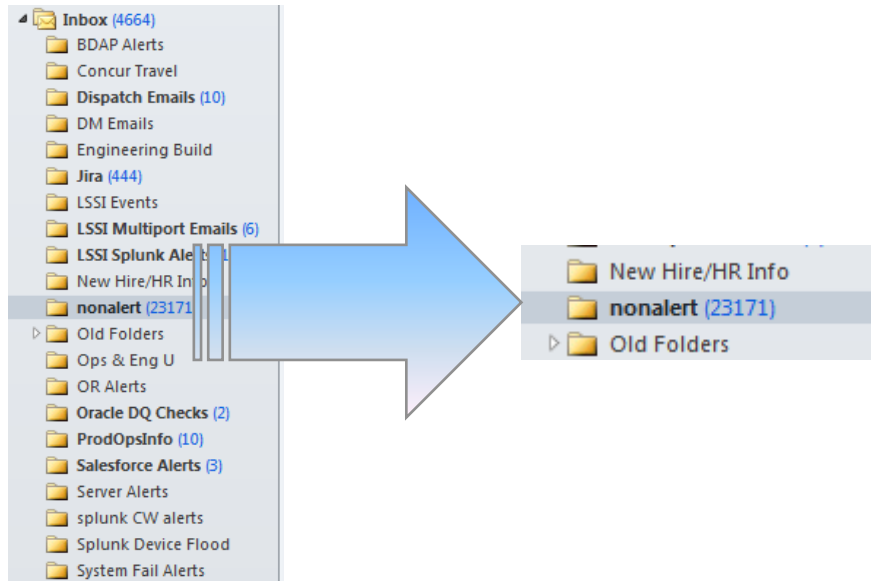
Ops after Splunk



Alerting 101

What makes a good alert?

Actionable
Instructive
Timely
Manageable



Exact manner of problems is not always known in advance...

Create better Outlook rules?

Alerts

Alerts set a condition that triggers an action, such as sending an email to people. Click the name to view the alert.

Alerts

Alerts set a condition that triggers an action, such as sending an email to people. Click the name to view the alert. Open the alert in Search to refine the parameters.

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

320 Alerts

i	Title ^
>	AAA Test alert
>	ACTION UNIT FAILURE
>	ACTION UNIT FAILURE
>	AESO OR Actual Volume
>	AESO OR Screenscrap
>	AESO OR Screenscrap
>	AESO OR Screenscrap
>	AESO Send Messages
>	AESOEEventManagerBe
>	Alert - syslog errors la
>	Atlas 404 errors are gr
>	BDAP Low Ack Counts
>	BDAP Storm Supervise
>	BDAP_Alert_Oracle_Er
>	BDAP_alert_IDSQS_Er
>	BOS STG Arm Status C
>	Bonita Connection Err
>	Bonita Error - Check A
>	Bonita License Expirat
>	Bonita Transactional I
>	Boss man S2 not send
>	Boston Staging Staten
>	Boston Staging - Shun
>	Boston Staging Perme
>	Boston Staging canno
>	CDS Nightly - preprod
>	CEP Device Flood

320 Alerts

i	Title ^
>	Infopush PRD Invalid Country Code
>	Infopush PRD MAPS SQL Exception
>	Infopush PRD NonExistentQueue
>	Infopush PRD Promotion Process Alert
>	Infopush PRD Queue Deleted Recently
>	Infopush PRD SQL Exception
>	Infopush PRD SQL Exception - Invalid DB Username
>	Infopush PRD SQL Exception - Pool Error Timeout
>	Infopush PRD SQL Exception - PoolableConnectionFactory
>	Infopush PRD Unreachable Node
>	Infopush PreProd - Dist Pong
>	Infopush PreProd - Hips Pong
>	Infopush PreProd - Maps Pong
>	Infopush PreProd - Notification Error
>	Infopush PreProd - Subsc Pong
>	Infopush Prod - Dist Pong
>	Infopush Prod - Hips Pong
>	Infopush Prod - Maps Pong
>	Infopush Prod - Notification Error
>	Infopush Prod - Subsc Pong
>	JBoss - 3 or More SF sync errors in the last hour
>	JBoss - Multicast MPING Connection Error
>	JBoss - Shunning Alert
>	JBoss - java.lang.OutOfMemoryError - Heap Space
>	Jim or Grace login
>	Korea Notification Query Error
>	LSSI Arm Status Change

320 Alerts

i	Title ^
>	PRD: PJMPolling Stopped User:ENOAPS_engine
>	PRD: PJMPolling Stopped User:ENOBGE_engine
>	PRD: PJMPolling Stopped User:ENODPL_engine
>	PRD: PJMPolling Stopped User:ENOPEP_engine
>	PRD: PJMeLRSTranslator - Duplicates Received
>	PRD: PJMeLRSTranslator - Error Publishing to RabbitMQ
>	PRD: PJMeLRSTranslator - Error writing to DB on CURTAIL
>	PRD: PJMeLRSTranslator Error - Action Already Updated
>	PRD: PJMeLRSTranslator Error's
>	PRD: ZooKeeper Backup Not Running
>	PRD: ZooKeeper cluster down
>	PRD: ZooKeeper host is down
>	Platform cannot connect to database
>	Potentially Troubling AWS Activity
>	Processes_Exceeds_by_Host
>	Prod Energy Profiling Response Times
>	Prod Home Page Response Times
>	Prod Login Response Times
>	Prod Portfolio View Response Times
>	Prod Portfolio View Response Times B
>	<u>QA1 Error authenticating to bonitasoft service</u>
>	QA1 Null parameters in org.ow2.bonita.facade.uuid.AbstractUUID
>	QA1 PermGen Space Full
>	QA1 Platform RabbitMQ Connection Failure
>	QA1 Statement / Result Set Leak
>	QA1 cannot connect to database

All Yours This App's filter

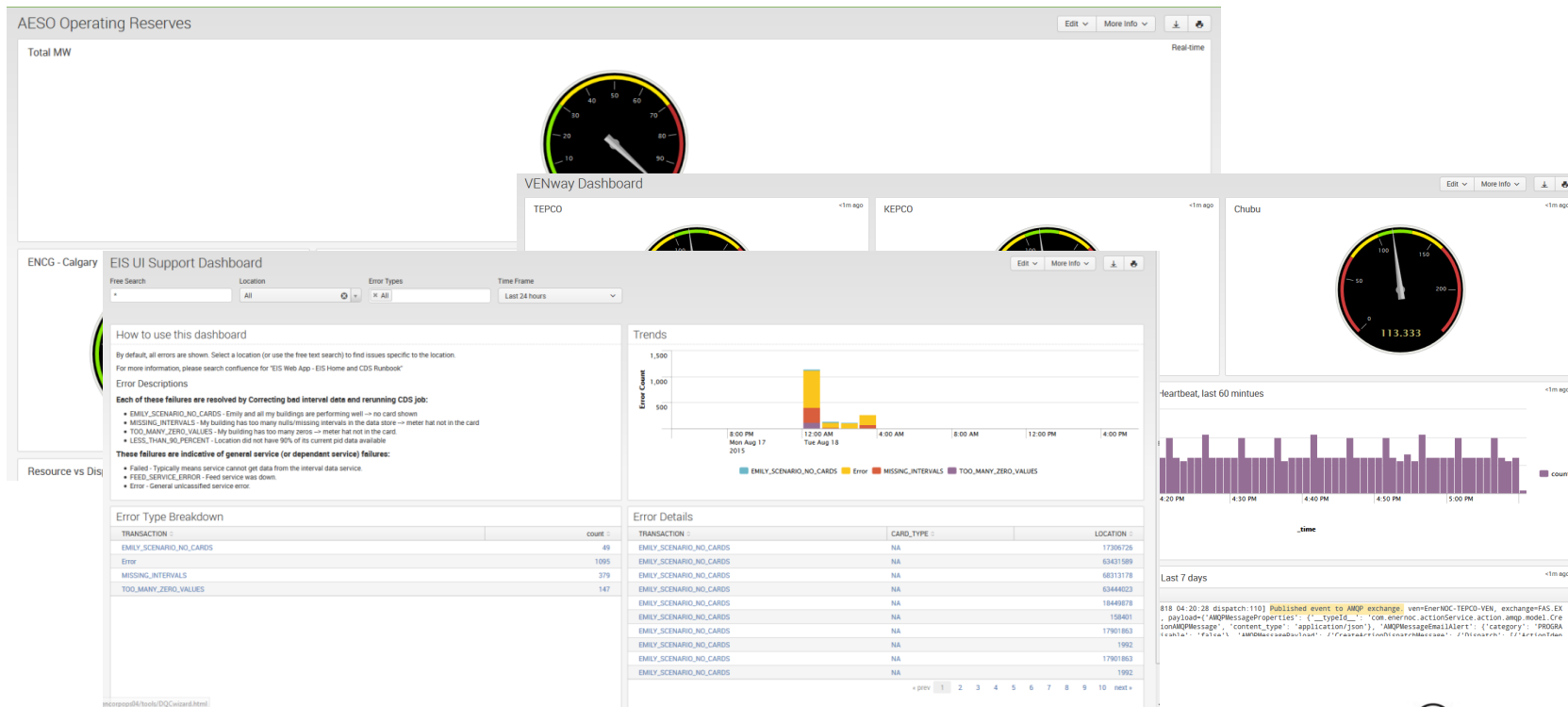


.conf2015

2015

splunk>

Dashboards & Alerts



Splunk moves back from Ops to Dev

- Development takes off in many directions
 - Many microservices
 - Cloud platforms being developed in AWS
 - Servers are cattle, not pets
- Need to start setting standards → Splunk is the standard

Splunk in Dev

- What does it mean Splunk is the standard?
- Logging format – timestamps, key value pairs, unique IDs
- Learn to log – not alert
 - Give info about what an error means, let the stakeholder decide if its critical

```

> 8/7/15 [E 150808 03:59:36 oadm_client:184] Error polling vmy, vendor=NOCD-Chu-ven
11:59:36.000 PM
Traceback (most recent call last):
  File "/opt/vmware/vmware/oadm_client.py", line 181, in _oadr_poll
    self._oadr_client_send_poll()
  File "/usr/lib/python2.7/requests/lib/python2.7/site-packages/oadr2/_init_.py", line 176, in send_poll
    Show all 23 lines

host > 10-10-10-10-89.ec2.internal source > /usr/lib/vmware/vmlog source > vmy
> 8/7/15 [E 150808 03:59:36 oadm_client:184] Error polling vmy, vendor=NOCD-KEPCO-ven
11:59:36.000 PM
Traceback (most recent call last):
  File "/opt/vmware/vmware/oadm_client.py", line 181, in _oadr_poll
    self._oadr_client_send_poll()
  File "/usr/lib/python2.7/requests/lib/python2.7/site-packages/oadr2/_init_.py", line 176, in send_poll
    Show all 23 lines

host > 10-10-10-10-89.ec2.internal source > /usr/lib/vmware/vmlog source > vmy
> 8/7/15 [E 150808 03:59:36 oadm_client:184] Error polling vmy, vendor=NOCD-TPCO-ven
11:59:36.000 PM
Traceback (most recent call last):
  File "/opt/vmware/vmware/oadm_client.py", line 181, in _oadr_poll
    self._oadr_client_send_poll()
  File "/usr/lib/python2.7/requests/lib/python2.7/site-packages/oadr2/_init_.py", line 176, in send_poll
    Show all 23 lines

host > 10-10-10-10-89.ec2.internal source > /usr/lib/vmware/vmlog source > vmy
> 8/7/15 [E 150808 03:59:36 oadm_client:184] Error polling vmy, vendor=NOCD-Chu-ven
11:59:36.000 PM
Traceback (most recent call last):
  File "/opt/vmware/vmware/oadm_client.py", line 181, in _oadr_poll
    self._oadr_client_send_poll()
  File "/usr/lib/python2.7/requests/lib/python2.7/site-packages/oadr2/_init_.py", line 176, in send_poll
    Show all 23 lines

host > 10-10-10-10-89.ec2.internal source > /usr/lib/vmware/vmlog source > vmy
> 8/7/15 [E 150808 03:59:36 oadm_client:184] Error polling vmy, vendor=NOCD-KEPCO-ven
11:59:36.000 PM
Traceback (most recent call last):
  File "/opt/vmware/vmware/oadm_client.py", line 181, in _oadr_poll
    self._oadr_client_send_poll()
  File "/usr/lib/python2.7/requests/lib/python2.7/site-packages/oadr2/_init_.py", line 176, in send_poll
    Show all 23 lines

host > 10-10-10-10-89.ec2.internal source > /usr/lib/vmware/vmlog source > vmy
> 8/7/15 [E 150808 03:59:36 oadm_client:184] Error polling vmy, vendor=NOCD-TPCO-ven
11:59:36.000 PM
Traceback (most recent call last):
  File "/opt/vmware/vmware/oadm_client.py", line 181, in _oadr_poll
    self._oadr_client_send_poll()
  File "/usr/lib/python2.7/requests/lib/python2.7/site-packages/oadr2/_init_.py", line 176, in send_poll
    Show all 23 lines

```

[illegible]

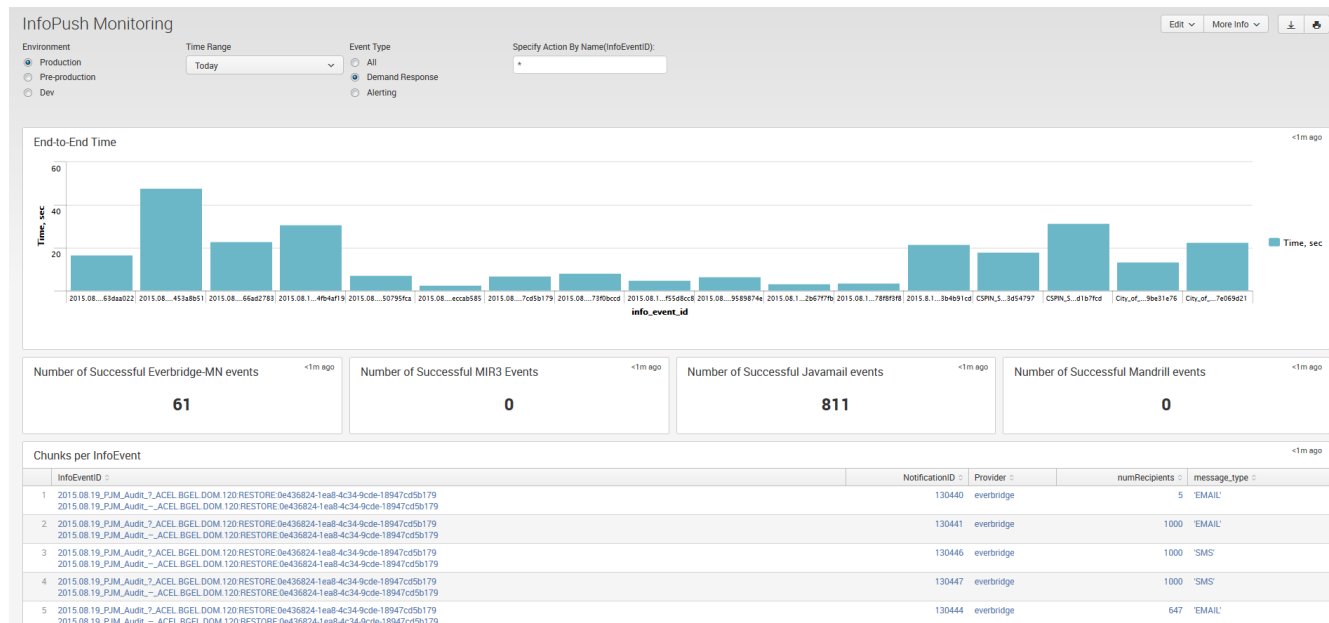
- > VTN Initial Alert
- > VEN - VTN Alert



Multiple Environment Alerting

- Saw an error in dev, couldn't reproduce but could be critical – use alerting to catch it in production

Multiple Environment Monitoring



event_monitoring_stats

[User interface](#) » [Views](#) » event_monitoring_stats

View type:

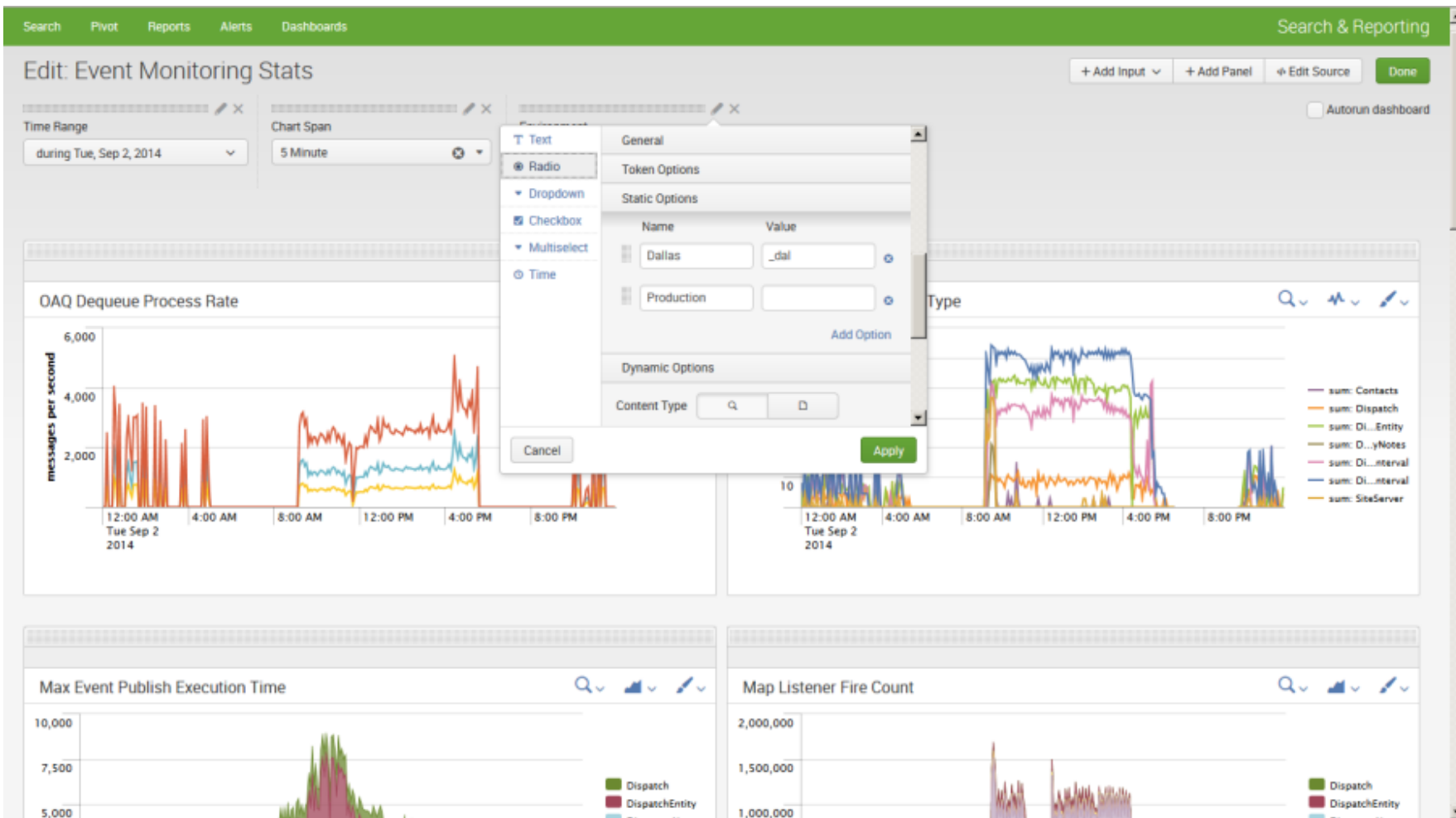
XML

View *

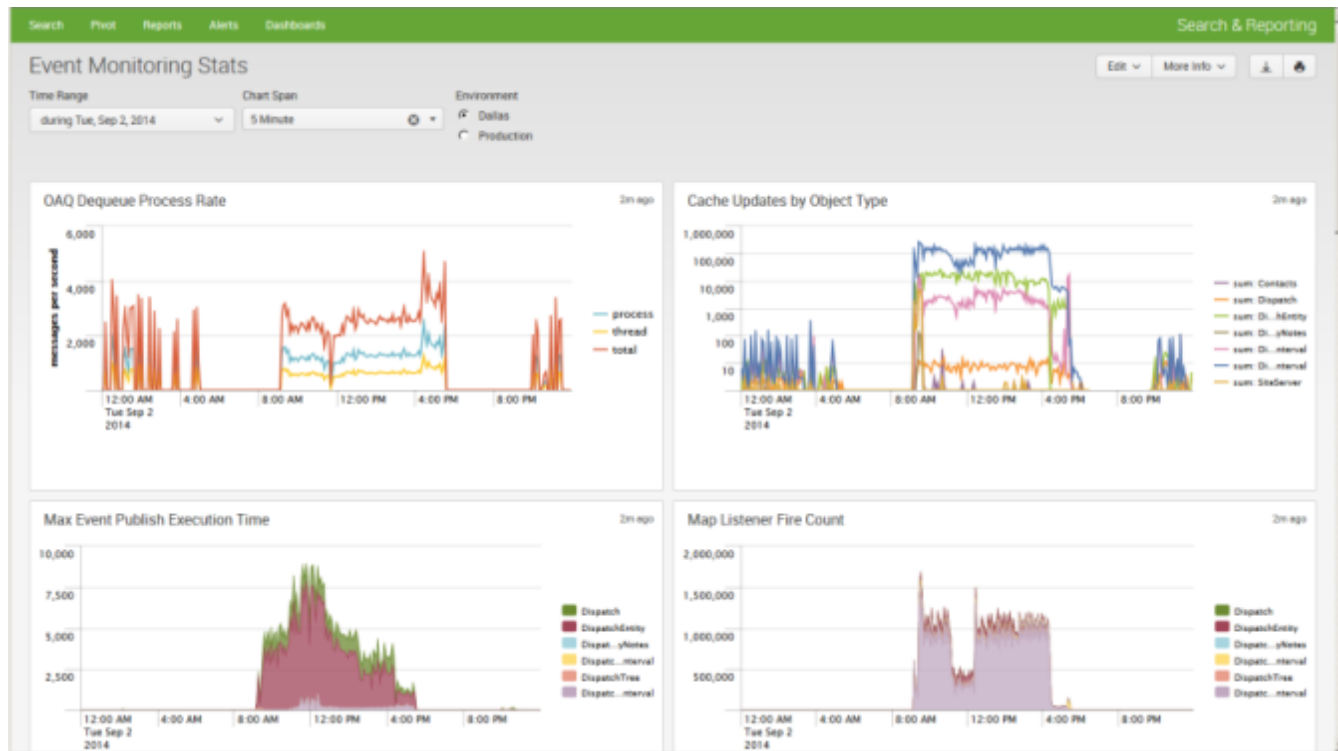
Enter and edit view configuration.

Plain Text

```
<default>5m</default>
</input>
<input type="radio" token="idx" searchWhenChanged="true">
  <label>Environment</label>
  <choice value="_dal">Dallas</choice>
  <choice value="">Production</choice>
  <default>_dal</default>
</input>
</fieldset>
<row>
  <panel>
    <chart>
      <title>OAQ Dequeue Process Rate</title>
      <searchString>index=dus$idx$ StatsManager dequeuedMessages>5 | timechart span="$SPAN$" avg(messagesPerSecond) AS p
      <earliestTime>$field1.earliest$</earliestTime>
      <latestTime>$field1.latest$</latestTime>
      <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
      <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
      <option name="charting.axisTitleX.visibility">collapsed</option>
      <option name="charting.axisTitleY.visibility">visible</option>
      <option name="charting.axisTitleY2.visibility">visible</option>
      <option name="charting.axisX.scale">linear</option>
      <option name="charting.axisY.scale">linear</option>
```



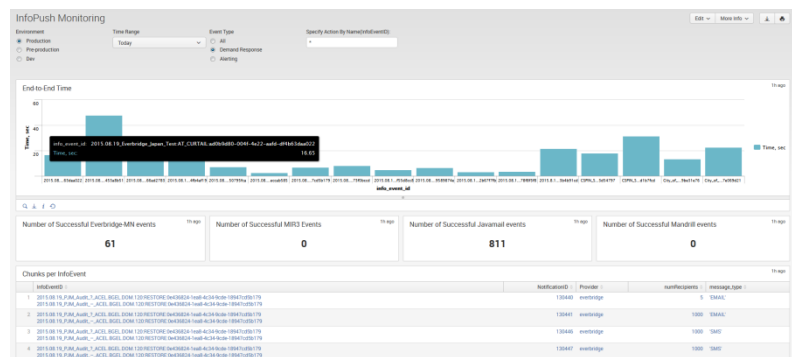
Performance Metrics from Day 1



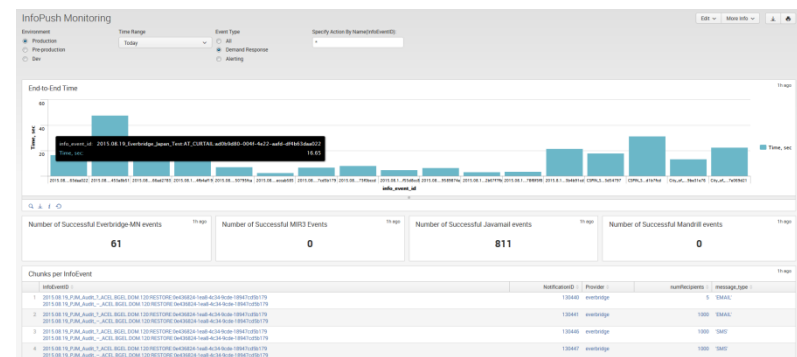


<http://www.bostonglobe.com/business/technology/2015/03/08/enernoc-faces-important-transition/TtJ7ejXmauZUKaHvtsZoxL/story.html>

Eng sees:



Ops sees:



.conf2015

2015

2015

splunk>

A little more about me...



ENERNOC

.conf2015

2015

splunk>

My story

- Started in operations, using Splunk as a way to see what was really happening
- Building alerts, giving access we never had before
- Became interested in the administration, helped design and build out new highly available cluster
- Got Splunk 6 admin certification last year

Splunk raises all ships

Why is Splunk particularly well suited to raising all ships in technical literacy?

- 1) Accessible – easy query language
- 2) Real – this is the data, it's not translated
- 3) Powerful – once you dig in, it has almost endless possibilities

Tips and Tricks

- Importance of a Splunk knowledge manager – someone who can translate business needs
- Find the pieces of data your team wants to see
- Logging is cheap. Outages are not.
- Pay attention to alert management
- Realtime searches – be careful of usage

Tips and Tricks

- How many indexes?
- RTFM - Read the documentation
 - Ask questions, come to .conf
- Search head cluster stories
 - Moving from a standalone search head has some quirks
- Think about administration as you go

Summary

- Know the data, love the data, share the data
- Involve Ops by finding out what they need
 - Dashboards give insights to opaque technologies
 - Good alerts will make data accessible and actionable
- Set some standards
 - Learn to log, let Ops alert
 - Splunk across environments
- Use Splunk to raise all ships

Next Steps

- Get in touch – gsumner@enernoc.com, splunk-admins@enernoc.com, or LinkedIn
- Boston Splunk Users Group



.conf2015

THANK YOU

splunk>