

# Monitoring The Industrial Internet Of Things

## A Guide To Application Performance Monitoring In Splunk

Chris Winkler

Performance Engineering Team Lead, EnerNOC

.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.

# Agenda

- EnerNOC Intro
- Performance Engineering Intro
- Splunk and EnerNOC
- Epiphanies
- Q&A

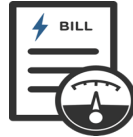
# EnerNOC's Energy Intelligence Software

- 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**



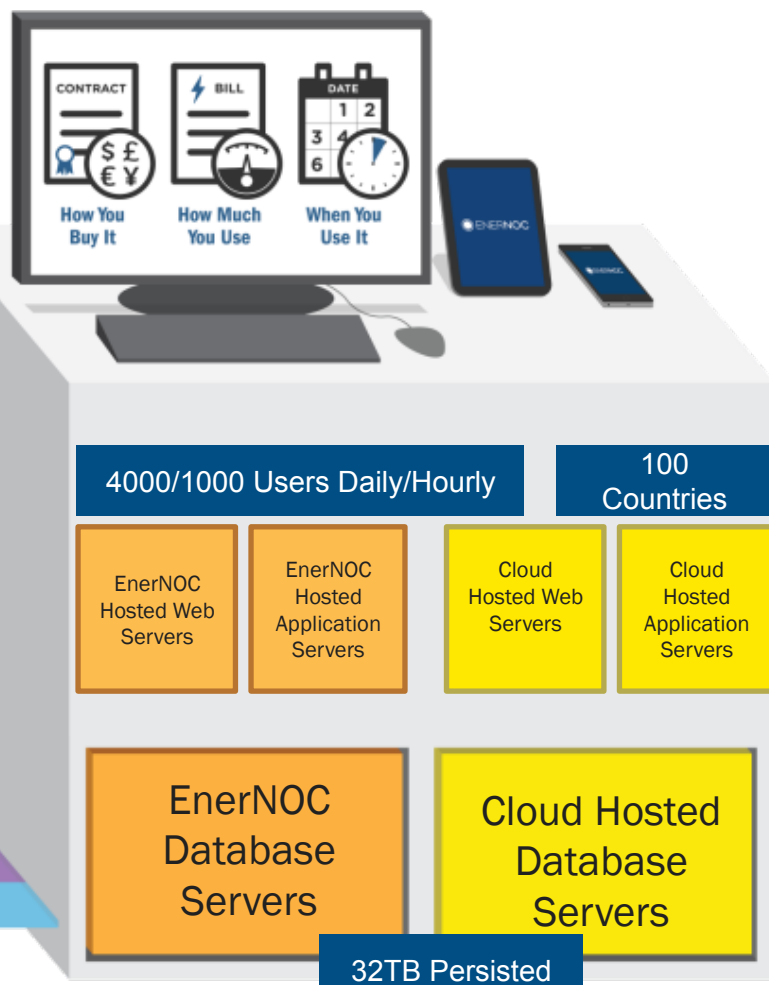
# EnerNOC EIS Platform

Data

3<sup>rd</sup> party



Data Streaming and Processing at Scale



# About Chris

- Performance Engineering Team Lead @ EnerNOC since 2011
- #1 Goal – Improve customers' experience while ensuring reliable and scalable applications are delivered into production
- Started using Splunk to parse data from web logs in March 2012
  - Self proclaimed winner of the “Best Splunk Index” award at EnerNOC ,  
3 years in a row
- Fostering a culture of performance at EnerNOC

# Team Mission: Ensure Platform Scalability & Stability

“Bet your Business” platform



+



=

HealthCare.gov

The system is down at the moment.

We are experiencing technical difficulties and hope to have them resolved soon. Please try again later.

In a hurry? You might be able to apply faster at our Marketplace call center. Call 1-800-318-2596 to talk with one of our trained representatives about applying over the phone.



# Questions We Want Answers To:

Q: How fast can we reduce energy consumption across all of the buildings in a region?

Q: How quickly can we send Demand Response notifications?

Q: How quickly are we processing device readings into our platform

Q: Who is using our platform?

Q: How many people logged into each of our applications today?

Q: What did they do after logging in?

Q: How was their experience?

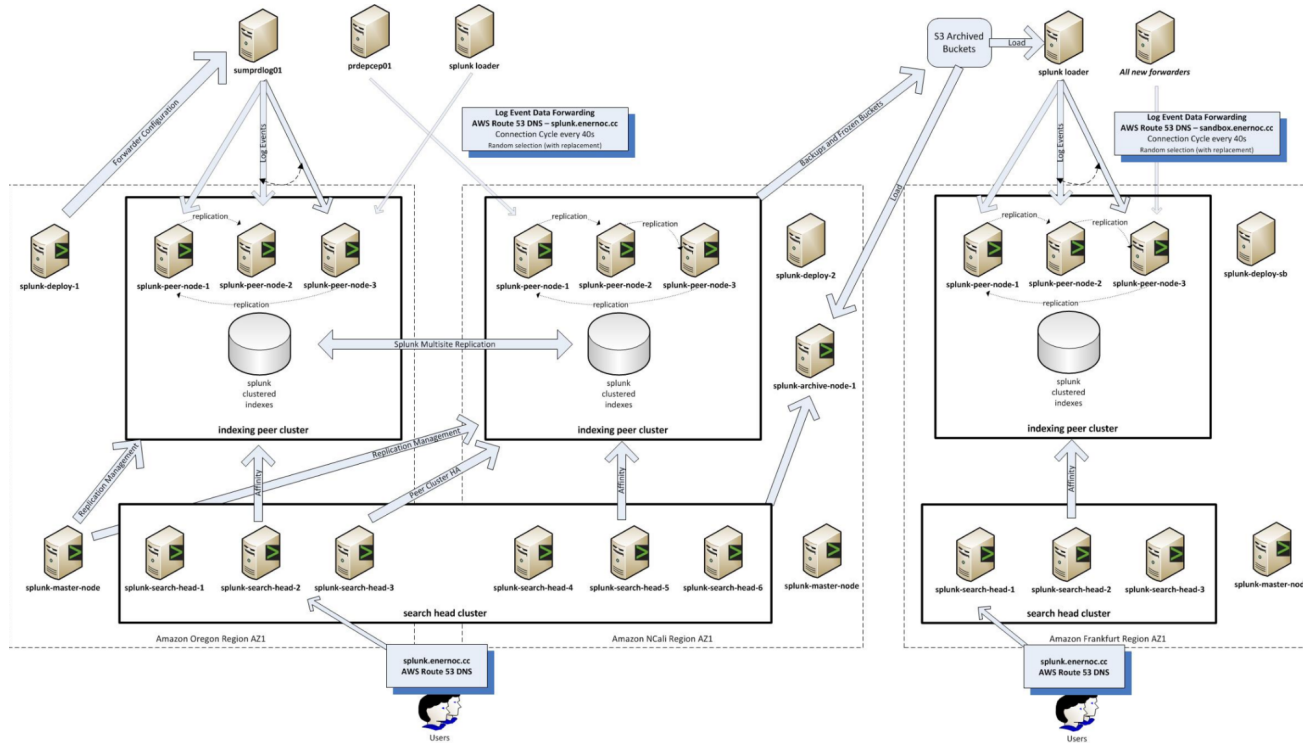
Answer before Splunk:



# Where Did We Start With Splunk?

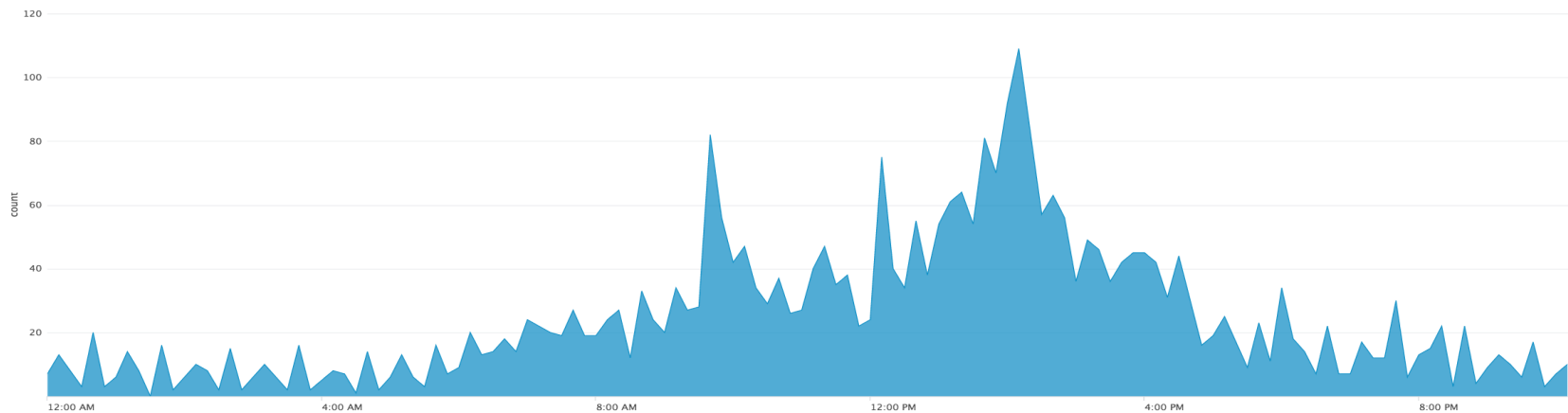
- 2012 Splunk POC
  - Web logs forwarded into Splunk for analysis
- 2013 Splunk On-site training

# Where Are We Now?



# My Splunk Epiphany

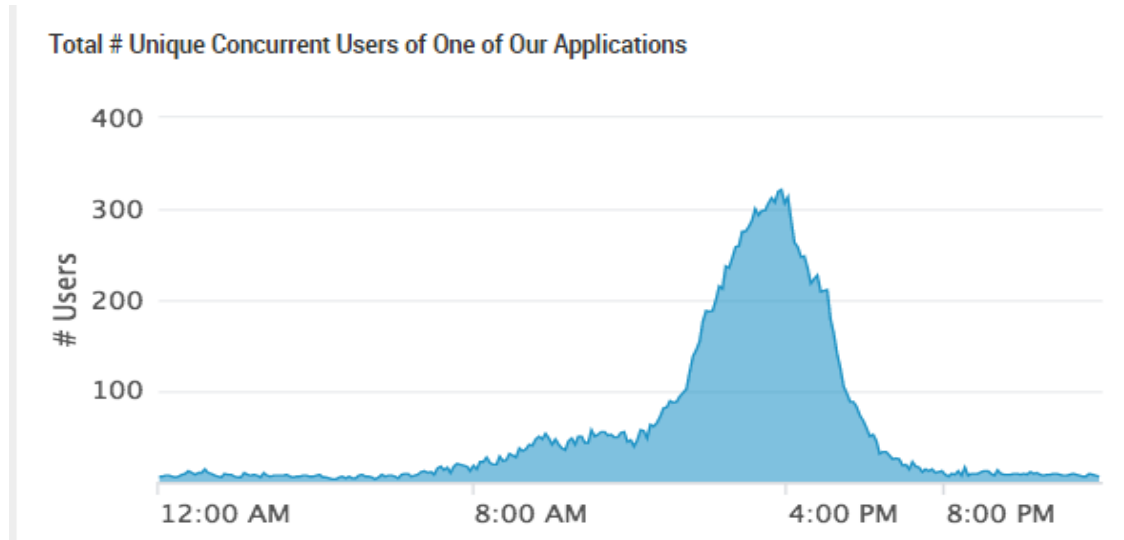
- `index=server "logged in" | timechart span=10m count`





# Which Led To:

- `index=web | timechart span=2m dc(userName)`



# Which Led To:

## Application Performance Metrics Dashboard

Edit More Info Download Print

Cumulative # of Logins Into One of Our Applications

2,274

Cumulative # Logins Into Another of Our Applications

1,709

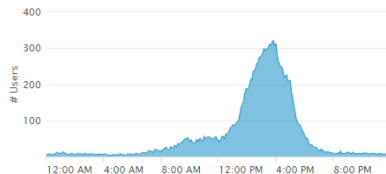
Total # Unique Logins Into Internal Application

38

# of Unique Users of One of Our Mobile Applications

87

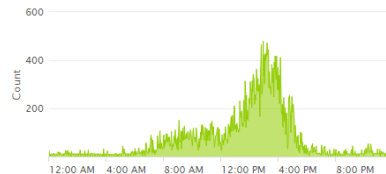
Total Unique Concurrent Users of One of Our Applications



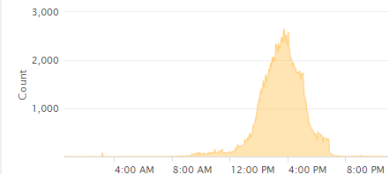
Total Unique Concurrent Users of Another of Our Applications



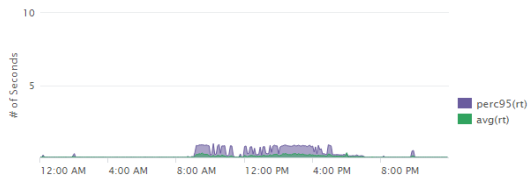
Requests per Minute on One of Our Applications



Requests per Minute on Another of Our Applications



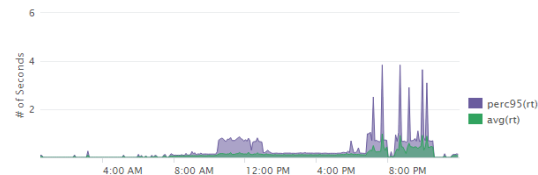
Application Response Times



Application Response Times



Application Response Times



# Secret Sauce: Instrumentation

- UserId
- Method
- Elapsed time



```
INFO [EernocAbstractBlazeAdapter] ajp-10.1.15.191-8009-4 ServiceCall service=data-services method=GetIntervalData user=demo_cwinkler elapsedTime=14
sourcetype = jboss
INFO [EernocAbstractBlazeAdapter] ajp-10.1.15.191-8009-4 ServiceCall service=data-services method=GetDayTypeDataPerHour user=demo_cwinkler elapsedTime=298
sourcetype = jboss
INFO [EernocAbstractBlazeAdapter] ajp-10.1.15.191-8009-4 ServiceCall service=data-services method=GetChildNodes user=demo_cwinkler elapsedTime=381
sourcetype = jboss
```

# Epiphany #2



Use Splunk to monitor critical business processes: interval data collection

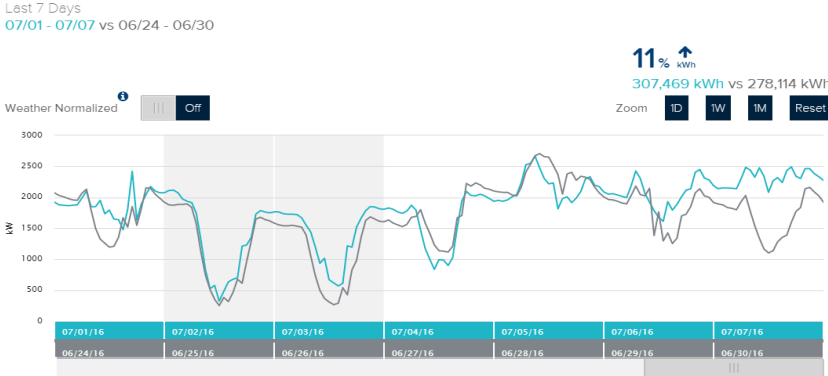
## Challenge:

Our meter data needs to be fresh, accurate, and available to our customers.

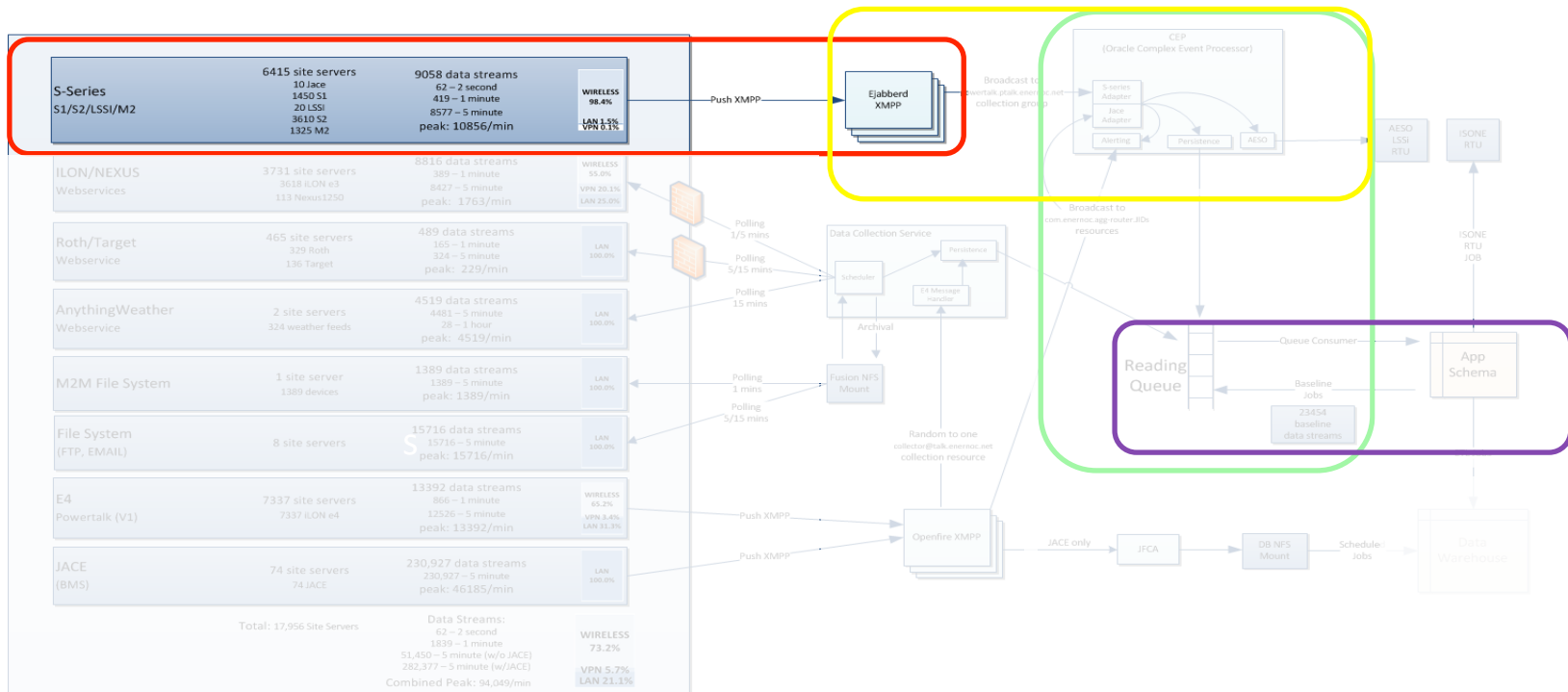
- Are we meeting our data collection SLA and can we proactively alert on data latency problems?
- How long does it take for readings to be processed and available to our front end applications?
- Does our data collection process scale?
- What are the interval collection counts, by device type, over time?

# Data Collection: From Device To Disk

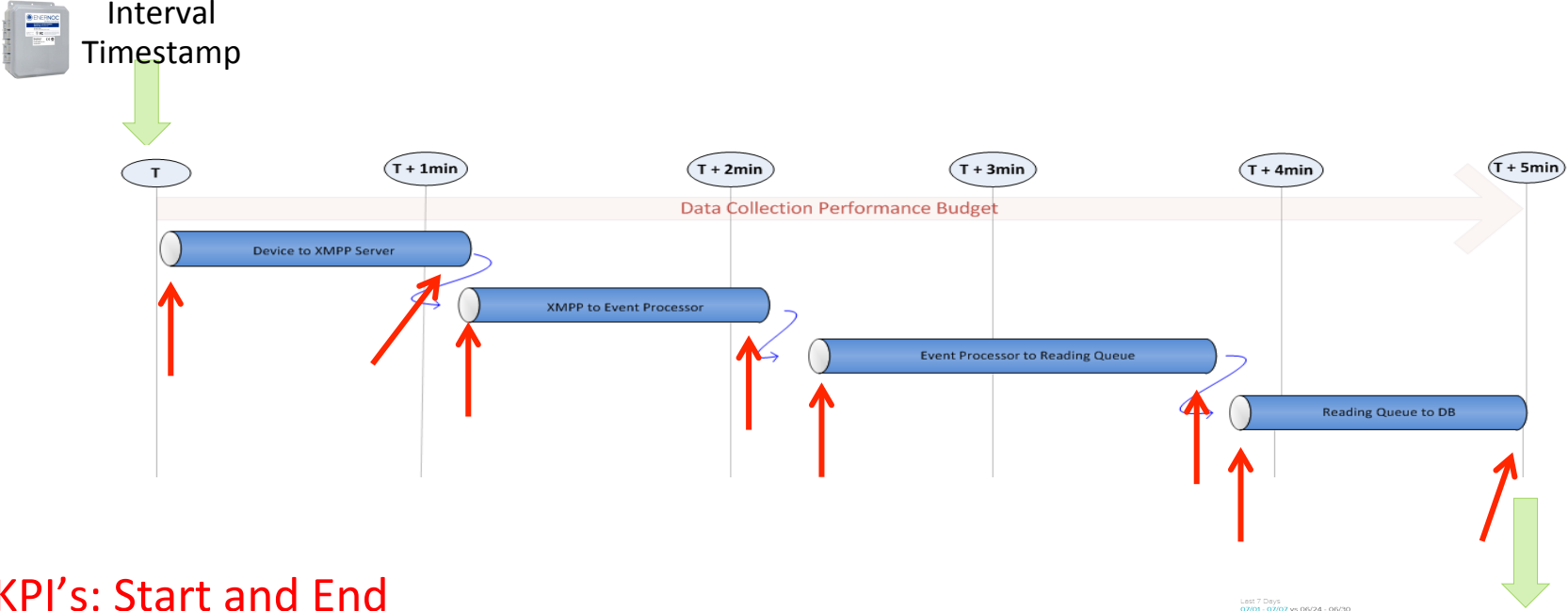
Device Data Needs To Be Available To Our Front End Apps Quickly



# Data Collection Architecture

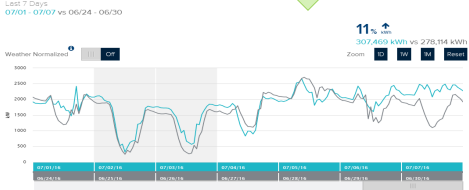


# Performance Budget and Instrumentation Requirements



KPI's: Start and End timestamps of each component

Interval available to front end apps





# Secret Sauce: Instrument the Incoming Data

- Data stream ID
- Device type
- Reading value
- Source timestamp
- Processed timestamp

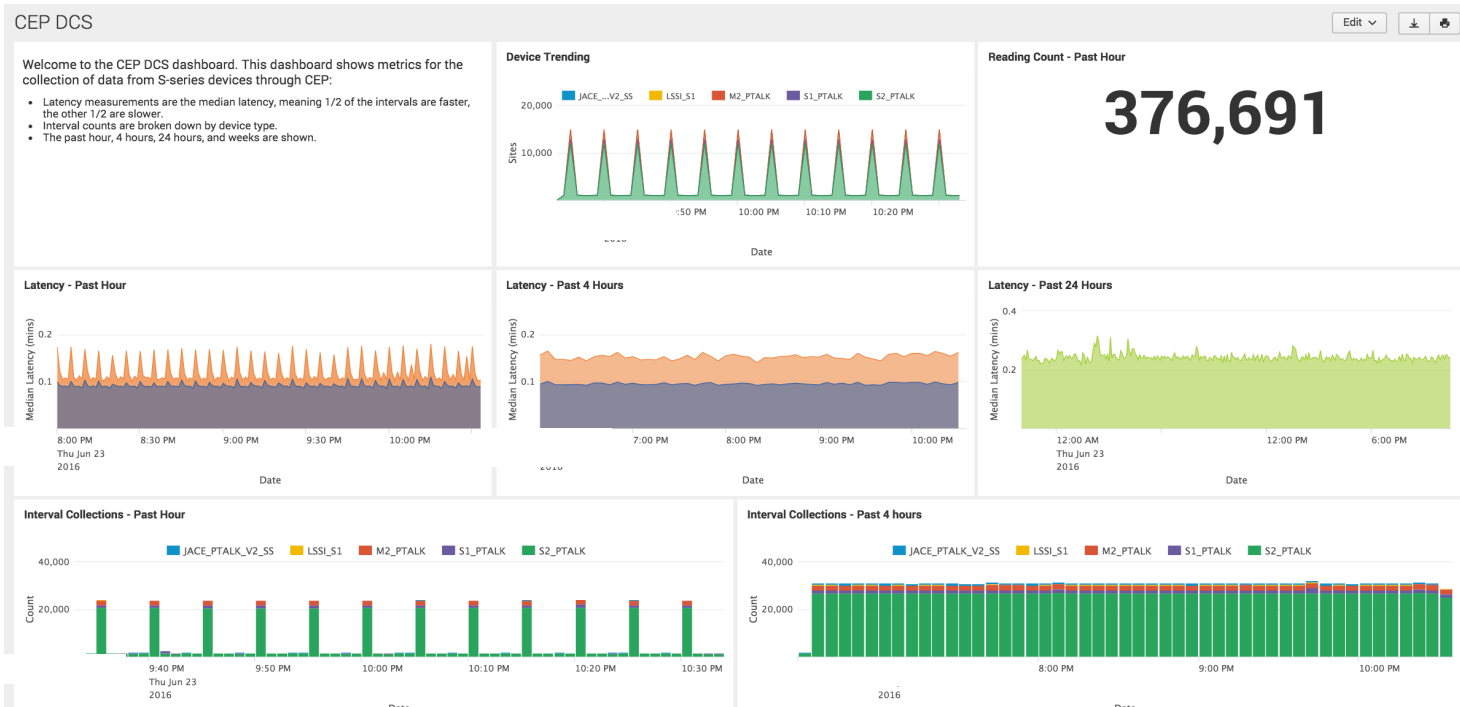


```
> 7/8/16 10:55:54.000 AM #####-Jul 8, 2016 2:55:54 PM UTC< <Warning> <com.enernoc.cep.message.SaveReadingBean> <> <myServer> <[ACTIVE] ExecuteThread: '13' for queue: 'weblogic.kernel.Default (self-tuning)'> <> <> <1467989754437> <BEA-000000> <IntervalReadingEvent: [sender=001ec0a26be9@ptalk.enernoc.net/s1, recipient=oracep-1@ptalk.enernoc.net, messageId=null, systemType=S1-CEP, deviceId=001ec0a26be9, dstreamName=001ec0a26be9@ptalk.enernoc.net/s1/00000000/pulse_1, definedDstreamName=001ec0a26be9@ptalk.enernoc.net/s2/000000/pulse_1, commodity=ELECTRICITY, measure=USAGE, measurementType=ACTUAL, readingTime=2016-07-08 14:55:02, readingValue=4126436.0, unitOfMeasure=KWH, cumulativeInd=1, errorFlag=0, siteServerType=S2_PTALK, dataStreamMemberId=17930089, siteServerMemberId=157766647, convertedUOM=KW, channelId=1, convertedChannelId=268, saveReading=true, messageBody=null]>
host = prdepcep01.enernoc.net | source = /opt/oracle2/middleware/user_projects/domains/enernoc_domain/server01/server.log

> 7/8/16 10:55:54.000 AM #####-Jul 8, 2016 2:55:54 PM UTC< <Warning> <com.enernoc.cep.message.SaveReadingBean> <> <myServer> <[ACTIVE] ExecuteThread: '13' for queue: 'weblogic.kernel.Default (self-tuning)'> <> <> <1467989754436> <BEA-000000> <IntervalReadingEvent: [sender=0004a32ef1c3@ptalk.enernoc.net/s1, recipient=oracep-1@ptalk.enernoc.net, messageId=null, systemType=S1-CEP, deviceId=0004a32ef1c3, dstreamName=0004a32ef1c3@ptalk.enernoc.net/s1/00000000/pulse_2, definedDstreamName=0004a32ef1c3@ptalk.enernoc.net/s1/000000/pulse 2, commodity=ELECTRICITY, measure=USAGE, measurementType=ACTUAL, readingTime=2016-07-08 14:55:02, readingValue=2.5726942E7, unitOfMeasure=KWH, cumulativeInd=1, errorFlag=0, siteServerType=S1_PTALK, dataStreamMemberId=17636566, siteServerMemberId=17636560, convertedUOM=KW, channelId=1, convertedChannelId=268, saveReading=true, messageBody=null]>
host = prdepcep01.enernoc.net | source = /opt/oracle2/middleware/user_projects/domains/enernoc_domain/server01/server.log

> 7/8/16 10:55:54.000 AM #####-Jul 8, 2016 2:55:54 PM UTC< <Warning> <com.enernoc.cep.message.SaveReadingBean> <> <myServer> <[ACTIVE] ExecuteThread: '13' for queue: 'weblogic.kernel.Default (self-tuning)'> <> <> <1467989754435> <BEA-000000> <IntervalReadingEvent: [sender=0004a32ef1c3@ptalk.enernoc.net/s1, recipient=oracep-1@ptalk.enernoc.net, messageId=null, systemType=S1-CEP, deviceId=0004a32ef1c3, dstreamName=0004a32ef1c3@ptalk.enernoc.net/s1/00000000/pulse_1, definedDstreamName=0004a32ef1c3@ptalk.enernoc.net/s1/000000/pulse 1, commodity=ELECTRICITY, measure=USAGE, measurementType=ACTUAL, readingTime=2016-07-08 14:55:01, readingValue=2.7614969E7, unitOfMeasure=KWH, cumulativeInd=1, errorFlag=0, siteServerType=S1_PTALK, dataStreamMemberId=17636563, siteServerMemberId=17636560, convertedUOM=KW, channelId=1, convertedChannelId=268, saveReading=true, messageBody=null]>
host = prdepcep01.enernoc.net | source = /opt/oracle2/middleware/user_projects/domains/enernoc_domain/server01/server.log
```

# Data Collection Dashboard



# Epiphany #3



Use Splunk to monitor our platform during Demand Response events

## Challenge:

When EnerNOC is dispatched by a grid operator, we have to reduce energy consumption across a region...FAST!!!

- How quickly have our devices responded to our control commands?
- How many devices can be curtailed within SLA? Does our platform scale?
- How does today's performance compare to the past?

# Secret Sauce: Monitor Device Workflow States

- Monitoring enhanced to capture device workflow states



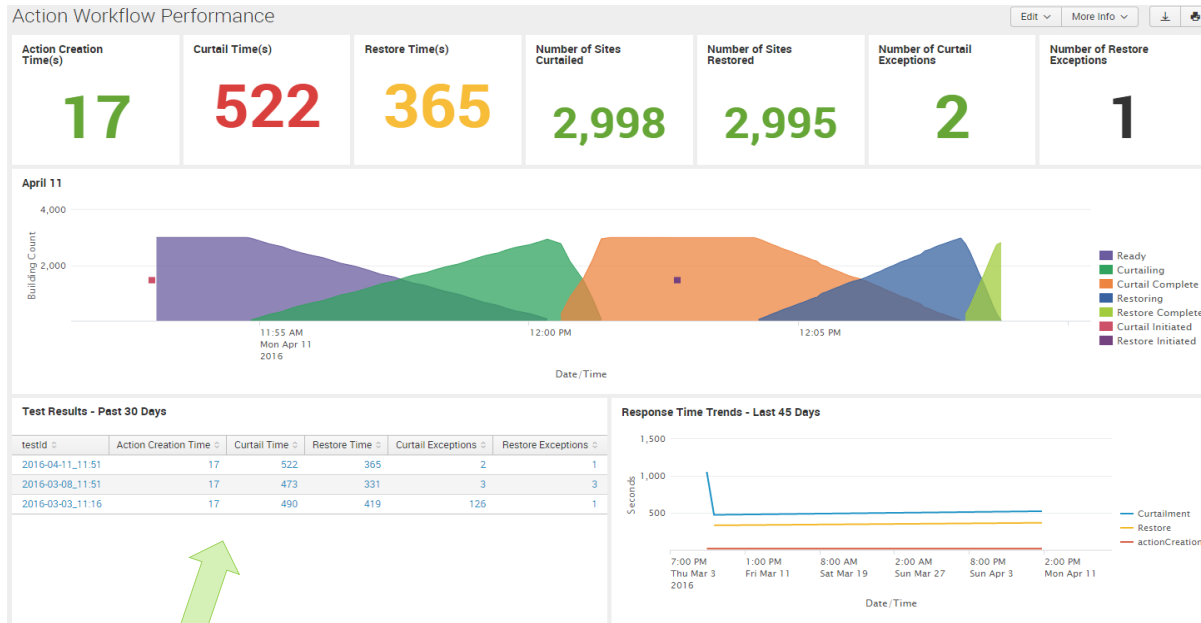
```
<sample t="768" ts="1465180883859" lb="Polling AUF table for AU states, 2016-06-05_22:33" rm="OK" ng="1" na="1">  
  <responseData class="java.lang.String">COUNT(*)      AUSM_STATE  
2827    CURTAILING  
171    CURTAIL_COMPLETE  
2      CURTAIL_EXCEPTION_DETECTED  
</responseData>  
</sample>
```

# Monitoring Device States During Demand Response Event

KPI's highlighted in the top row



Count of meters as they progress through all phases of the event



Performance comparison to recent events

**Key Takeaway:**  
Log KPI's to track performance in Splunk

# Epiphany #4:

Use Splunk to monitor Notification Platform Performance



## Challenge:

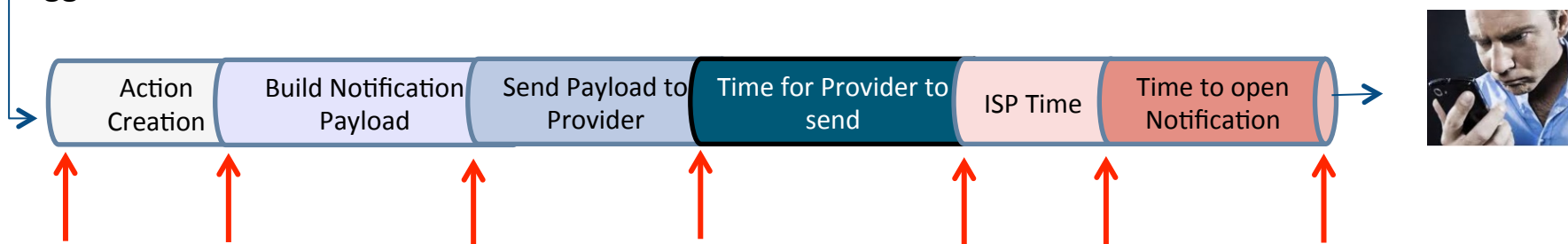
When EnerNOC is dispatched by a grid operator, we have to notify our customers.....FAST!!!

- How long did it take to send out the notifications?
- How many notifications were sent?
- Does our notification process scale? How many can we send within our SLA?

# Notification Instrumentation Requirements

First Step: breakdown architecture and identify KPI's

Dispatch  
Trigger



- Start and end timestamps of each component
- Unique identifier for each notification event (allows us to find the needle in the haystack)



# Notification Performance Dashboard

Total DR Notifications Sent

## 7,454

4m ago

# of DR Notifications Sent

Infopush top 10 DR events by contacts

Action	Contacts	Start	End-to-End
2016.06.2	3713	06/23/2016 13:24:00.835	20.839
2016.00	3703	06/23/2016 19:00:08.660	17.974
CHIC	7	06/23/2016 15:30:05.534	22.215
CHICD	7	06/23/2016 16:30:14.637	23.990
ChannelLj	6	06/23/2016 22:30:00.131	14.604
2016.C	4	06/23/2016 06:10:42.19352	
2016.Or	4	06/23/2016 06:00:03.626	20.161
Cumberfar	3	06/23/2016 13:00:04.854	15.820
Cumber	3	06/23/2016 14:30:11.313	28.458
2016.00.	2	06/23/2016 06:04:05.983	11.816

Total Alerting Notifications Sent

## 1,681

# of Alerting Notifications Sent

Top 10 Fastest Alerting Events

Info Event ID	Num Contacts	Start	End-to-End
8061127001146699632540	1	06/23/2016 11:43:54.768	1.740
73661270011466669164402	1	06/23/2016 04:05:05.905	1.772
12501270011466662851675	3	06/23/2016 10:40:52.736	1.792
63231270011466680552412	2	06/23/2016 07:15:54.552	1.952
30541270011466728847239	1	06/23/2016 20:40:55.522	2.113
47511270011466667284398	1	06/23/2016 03:34:45.352	2.277
51011270011466701254036	1	06/23/2016 13:00:55.272	2.365
62271270011466723172773	1	06/23/2016 19:06:17.194	2.470
53751270011466672452188	1	06/23/2016 05:00:53.976	2.545
56751270011466737543830	2	06/23/2016 08:05:05.444	2.590

Top 10 Slowest Alerting Events

Info Event ID	Num Contacts	Start	End-to-End
40591270011466067943409	2	06/23/2016 03:45:44.337	209.328
61311270011466669172040	1	06/23/2016 04:06:14.113	61.520
53641270011466707233570	1	06/23/2016 14:40:44.234	60.287
4757127001146666804362	1	06/23/2016 03:56:46.226	57.441
06641270011466713890215	2	06/23/2016 16:31:38.393	55.299
48231270011466698536710	2	06/23/2016 12:15:37.611	52.070
62271270011466731566250	1	06/23/2016 21:26:07.080	49.423
1885127001146668021209	1	06/23/2016 07:11:13.804	48.705
53671270011466671219138	1	06/23/2016 04:40:21.873	48.650
7125127001146670309054	1	06/23/2016 15:04:05.444	48.422

**Key Takeaway:**  
Instrument your code and log KPI's to track performance in Splunk

# Key Takeaways

- Use Splunk to visualize performance of your IOT infrastructure
- Breakdown the anatomy of your application & identify the KPI's
- Instrument your application to capture the KPI's
- Create Performance Dashboards for critical business processes



+



=



# Business Benefit

- Promoting a culture of performance:
  - Increased visibility in performance metrics = increased incentive to make apps faster
- Performance monitoring against SLA's in development and production
- In depth understanding of our limitations/capabilities
- Alerting of performance issues to minimize custom impact

# THANK YOU

- Get in touch: [cwinkler@enernoc.com](mailto:cwinkler@enernoc.com) or LinkedIn

.conf2016