Monitoring The Industrial Internet Of Things

A Guide To Application Performance Monitoring In Splunk

Chris Winkler

Performance Engineering Team Lead, EnerNOC

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> .conf2016

Agenda

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

ENERNOC

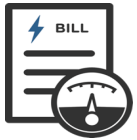
EnerNOC's Energy Intelligence Software

- 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

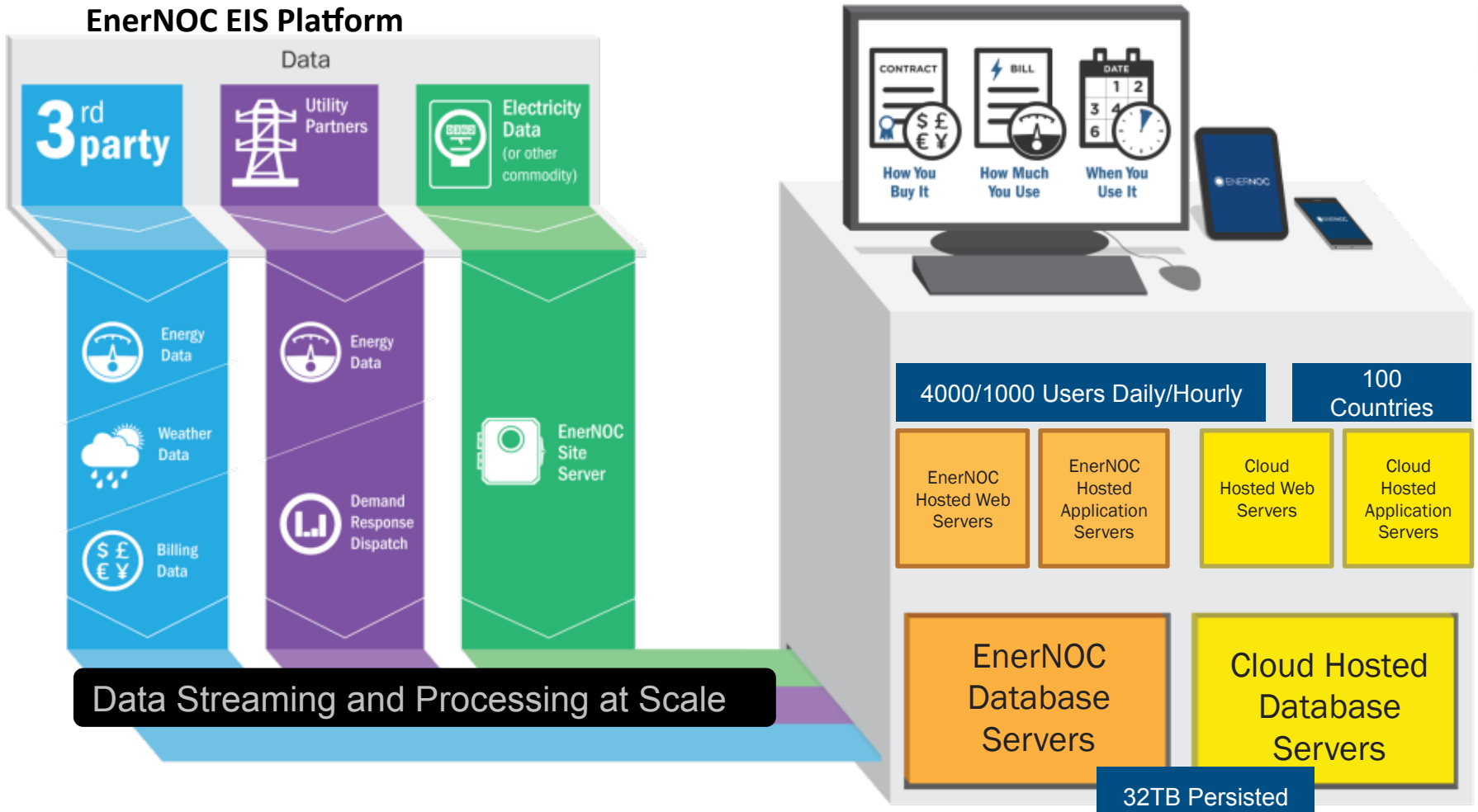
When you use it

Demand Response

Demand Management

ENERNOC

EnerNOC EIS Platform



splunk> .conf2016

About Chris

- Performance Engineering Team Lead @ EnerNOC since 2011

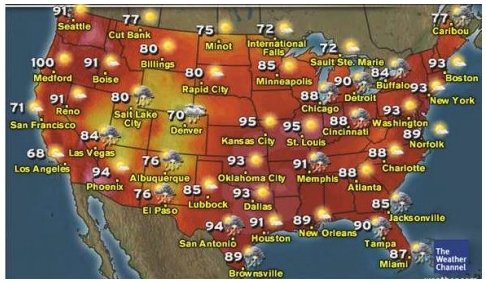
- #1 Goal – Improve customers' experience while ensuring reliable and scalable applications are delivered into production

- 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

splunk> .conf2016

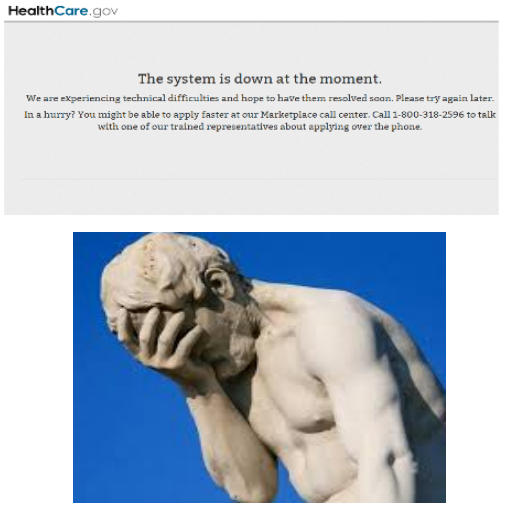
Team Mission: Ensure Platform Scalability & Stability

"Bet your Business" platform



+

=



Questions We Want Answers To:

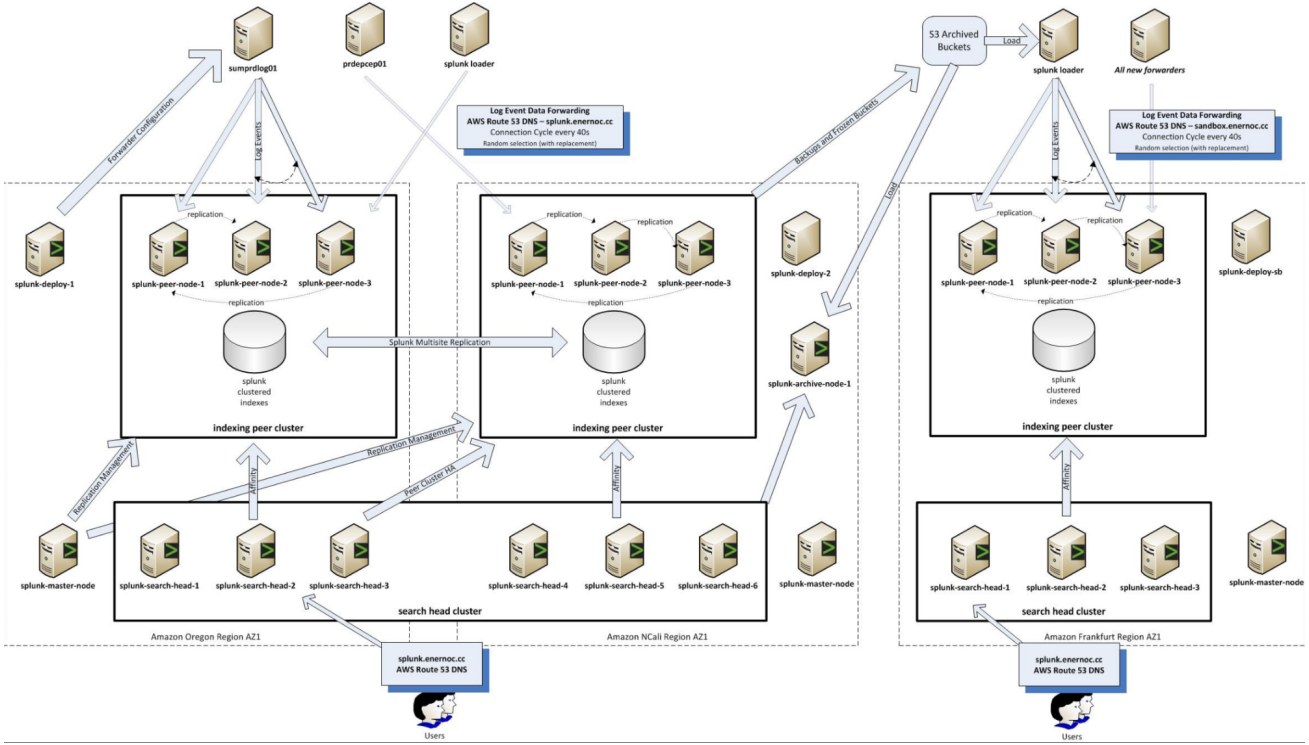
Q: How fast can we reduce energy consumption across all of the buildings in a region?
Q: How quickly can we send Demand Response notifications?
Q: How quickly are we processing device readings into our platform
Q: Who is using our platform?
Q: How many people logged into each of our applications today?
Q: What did they do after logging in?
Q: How was their experience?

Answer before Splunk:

Where Did We Start With Splunk?

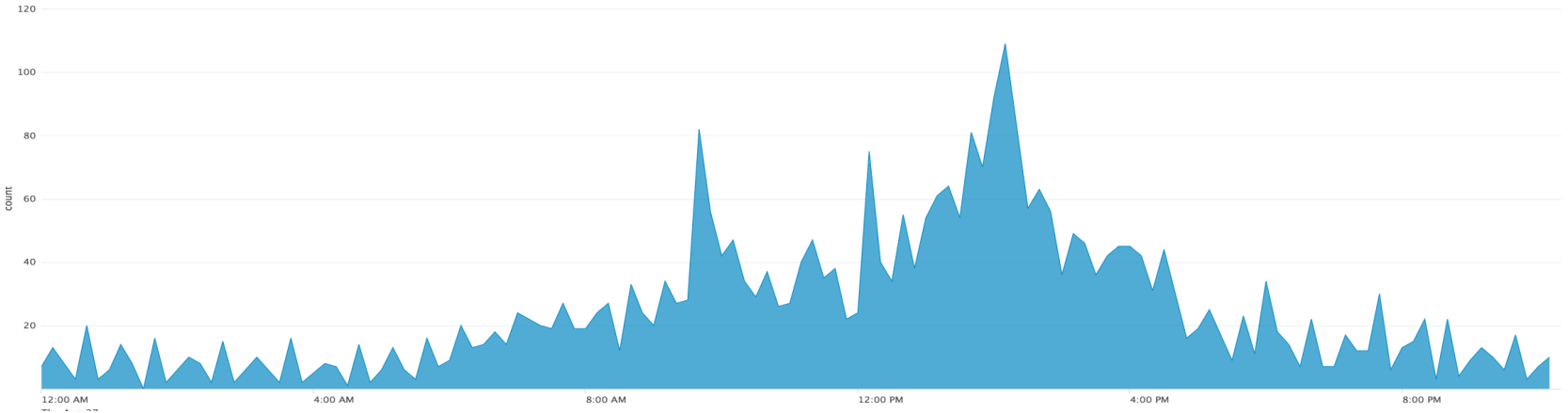
- 2012 Splunk POC
  - Web logs forwarded into Splunk for analysis
- 2013 Splunk On-site training

Where Are We Now?



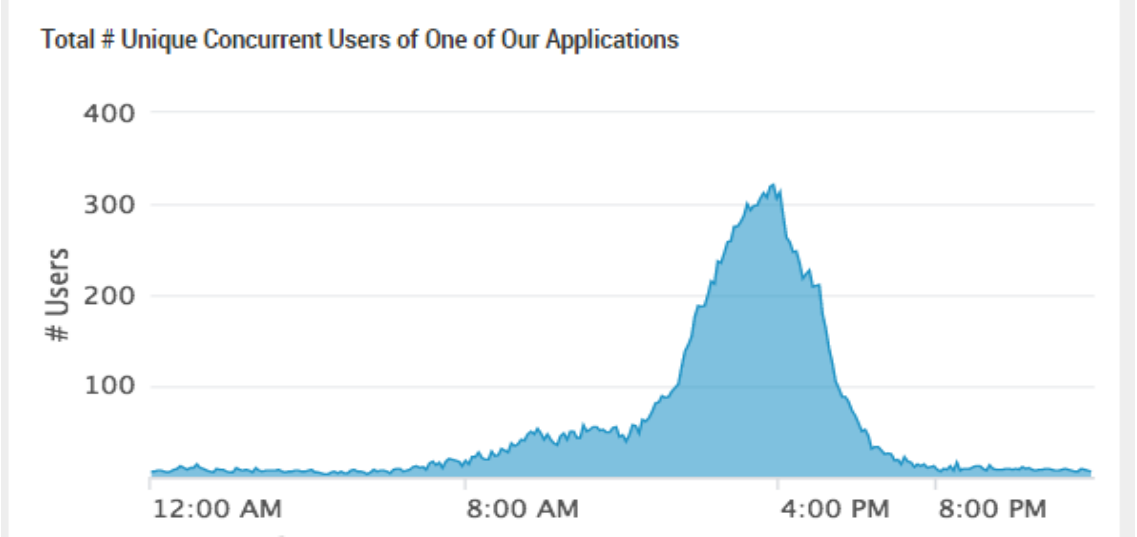
My Splunk Epiphany

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

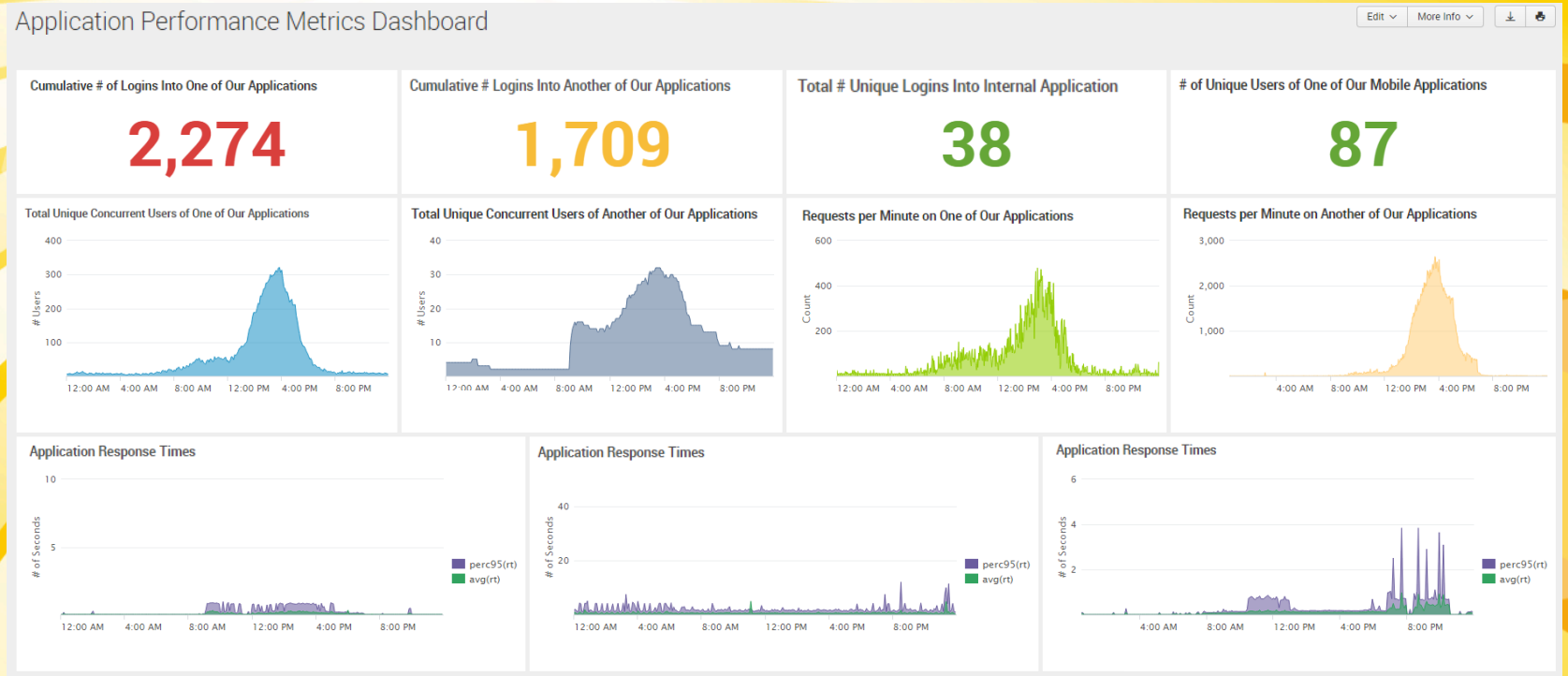


Which Led To:

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



Which Led To:


Application Performance Metrics Dashboard
Edit
More Info
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
Users
12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Total Unique Concurrent Users of Another of Our Applications
Users
4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Requests per Minute on One of Our Applications
Count
12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Requests per Minute on Another of Our Applications
Count
4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Application Response Times
# of Seconds
perc95(rt)
avg(rt)
12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Application Response Times
# of Seconds
perc95(rt)
avg(rt)
12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Application Response Times
# of Seconds
perc95(rt)
avg(rt)
4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM

Secret Sauce: Instrumentation

- UserId
- Method
- Elapsed time


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

Epiphany #2

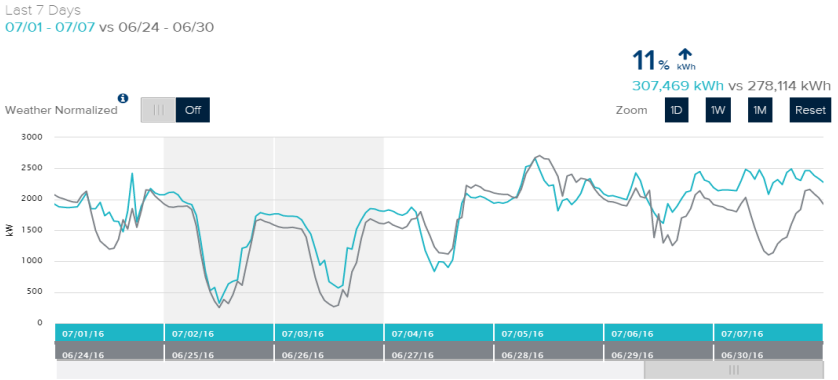
Use Splunk to monitor critical business processes: interval data collection

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

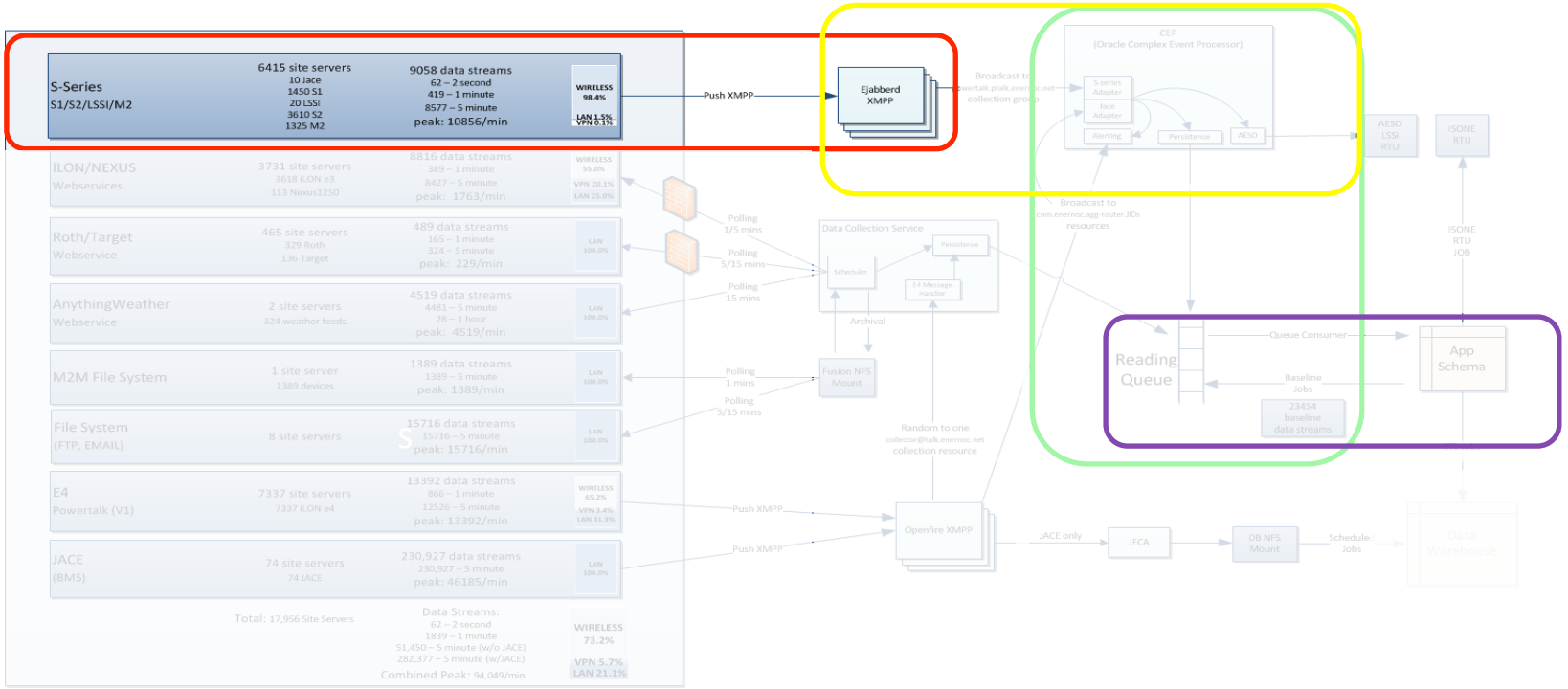
- Are we meeting our data collection SLA and can we proactively alert on data latency problems?
- How long does it take for readings to be processed and available to our front end applications?
- Does our data collection process scale?
- What are the interval collection counts, by device type, over time?

Data Collection: From Device To Disk

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

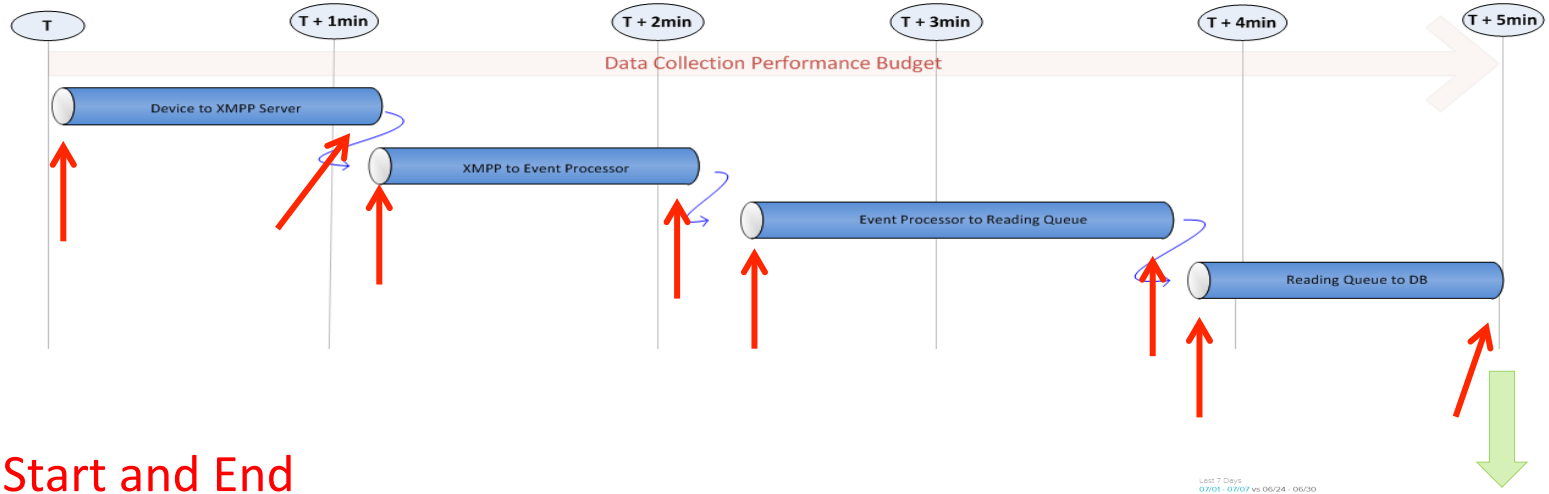


Data Collection Architecture



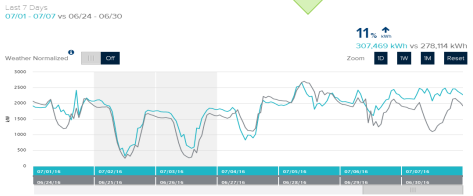
Performance Budget and Instrumentation Requirements

Interval Timestamp



KPI's: Start and End timestamps of each component

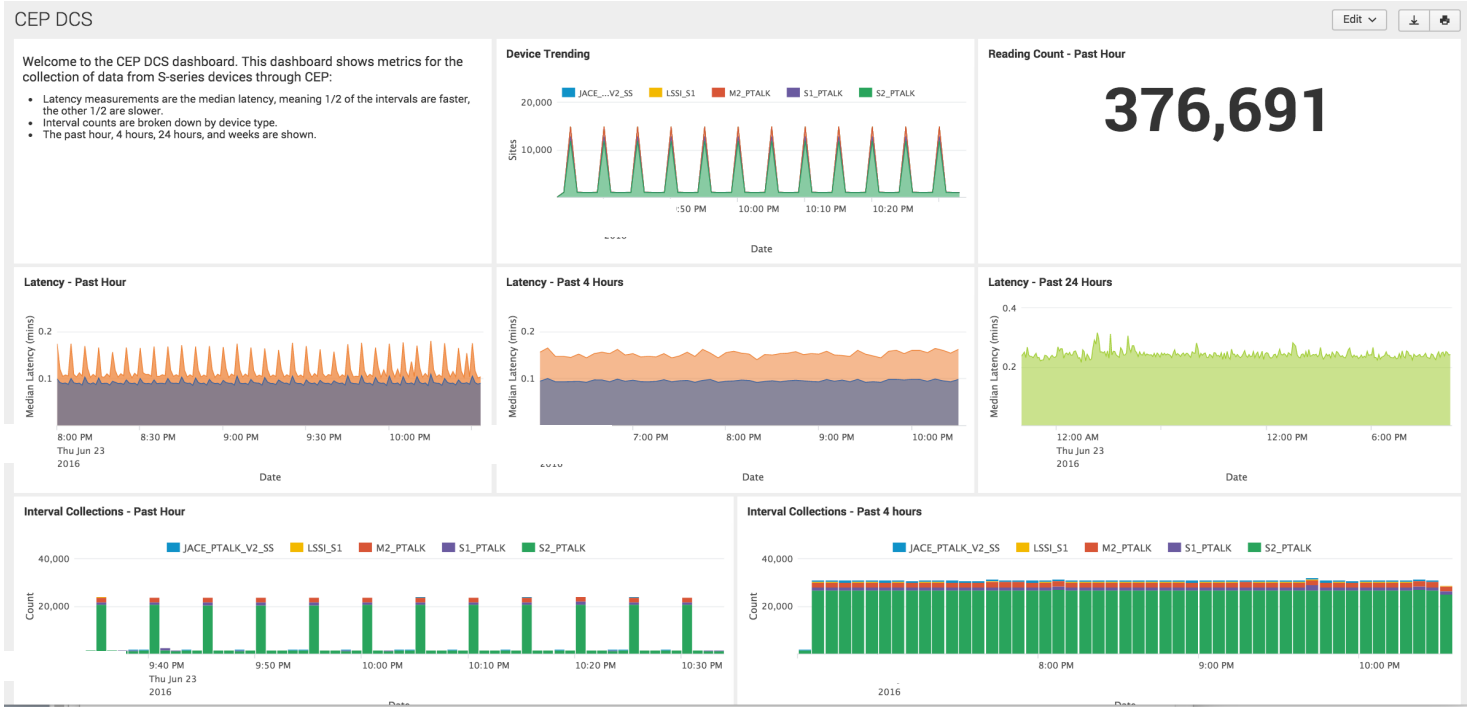
Interval available to front end apps



Secret Sauce: Instrument the Incoming Data

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

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

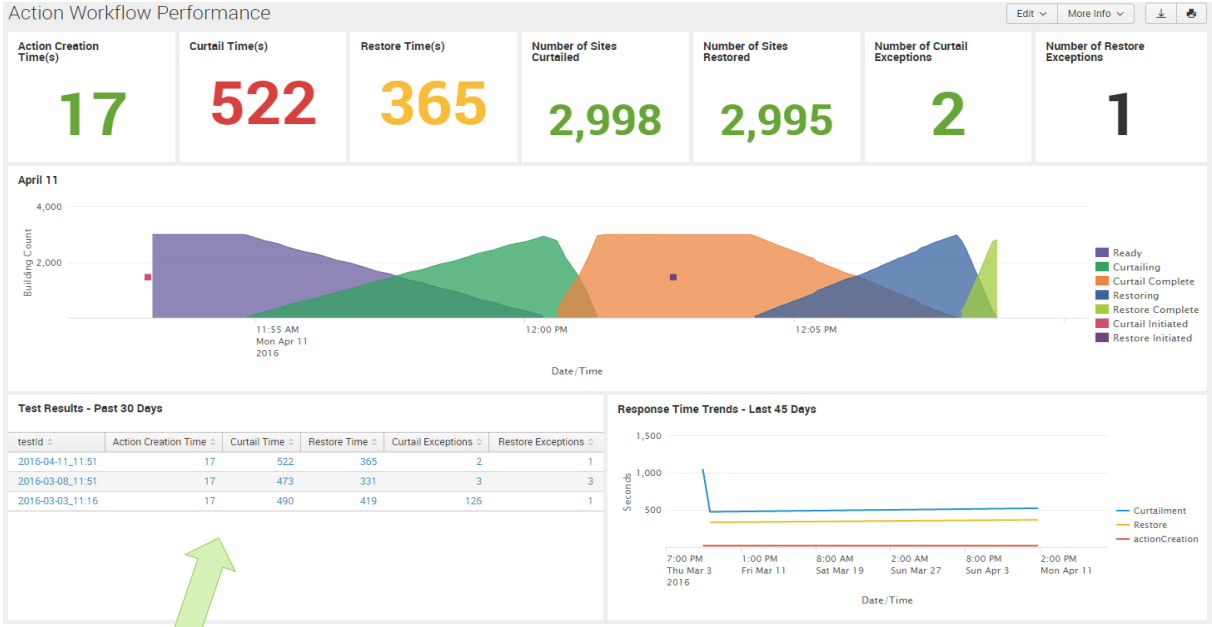
- Monitoring enhanced to capture device workflow states


```
<sample t="768" ts="1465180883859" lb="Polling AUWF 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:

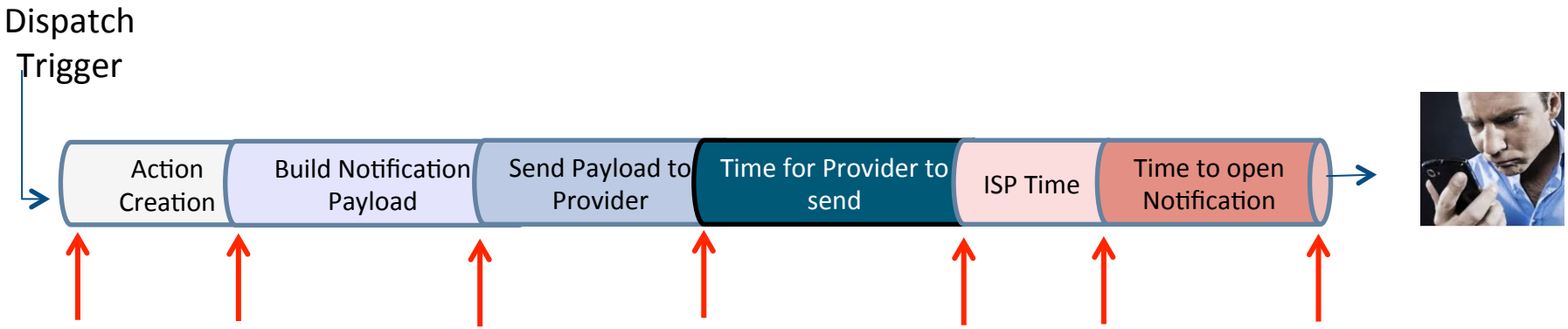
Use Splunk to monitor Notification Platform Performance

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?

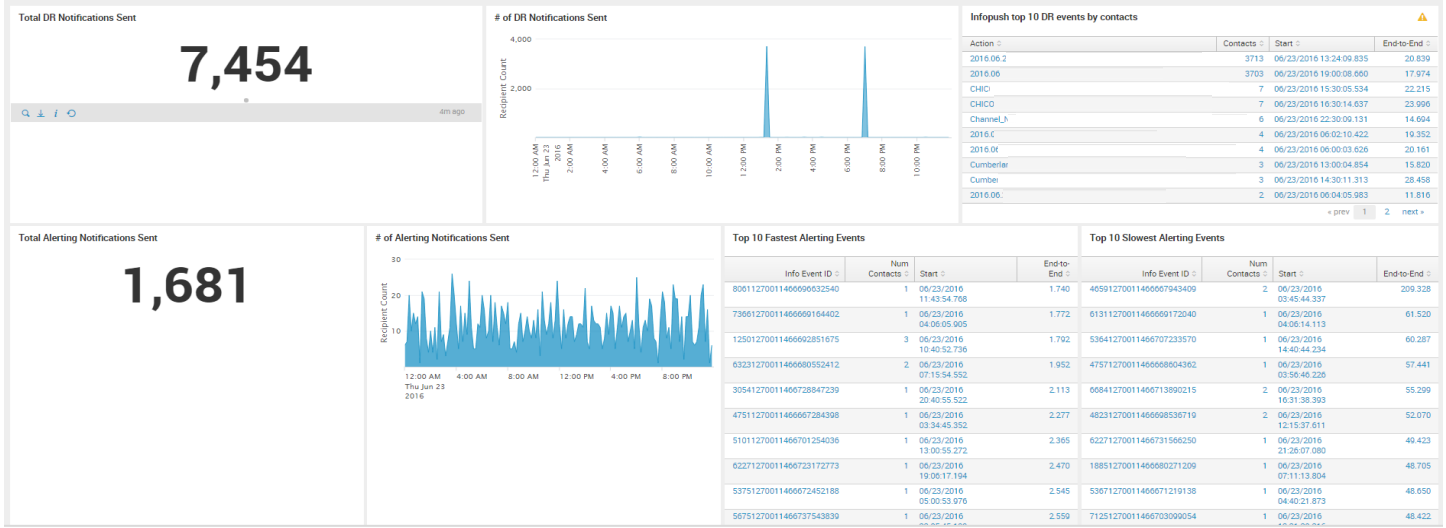
Notification Instrumentation Requirements

First Step: breakdown architecture and identify KPI's



- 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



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

+

splunk>

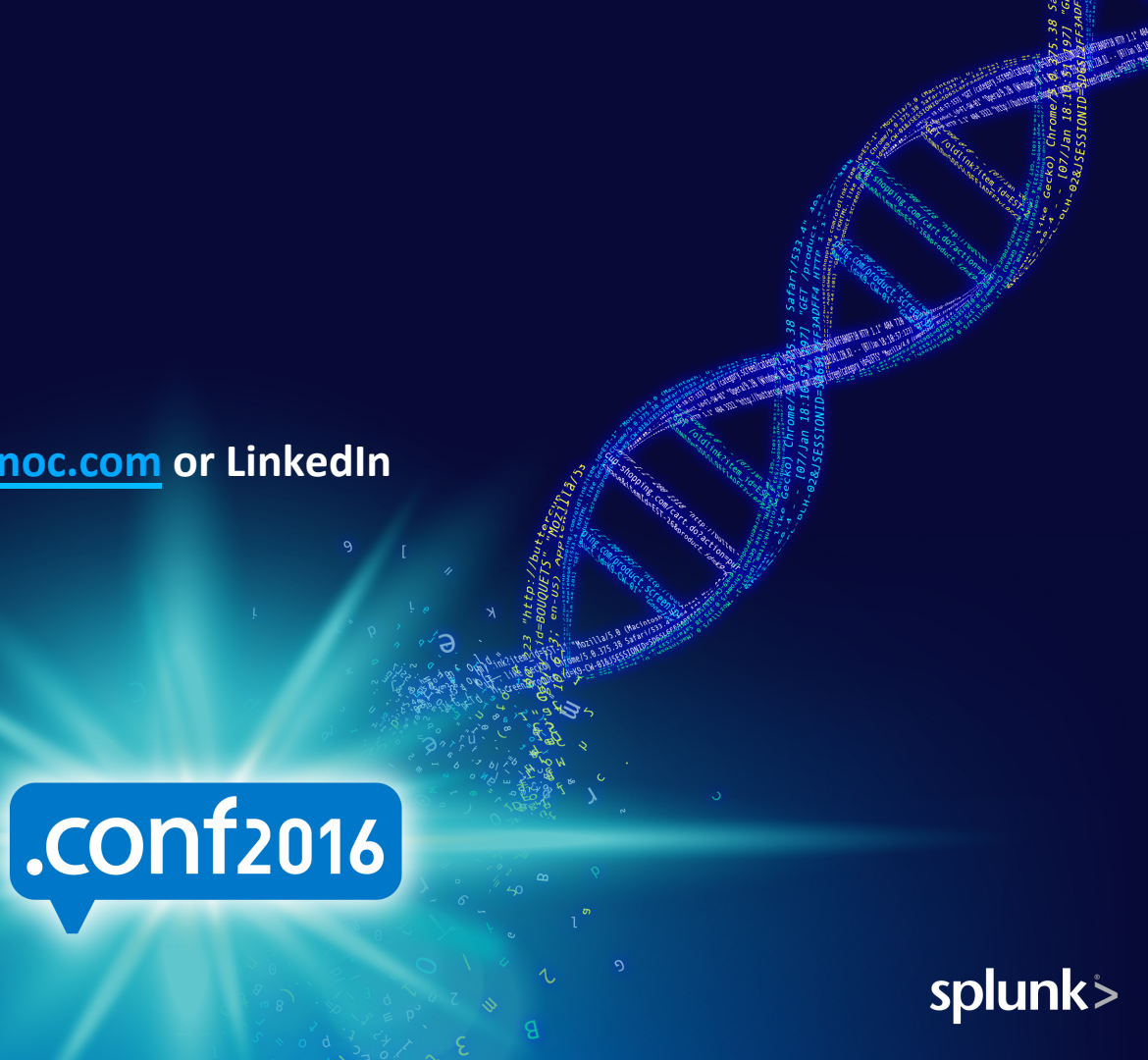
=

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 or LinkedIn**



.conf2016

splunk>