

Exceptional service in the national interest



Implementing Log Analytics for Operational Intelligence

Randolph Abeyta

Solutions Architect SE

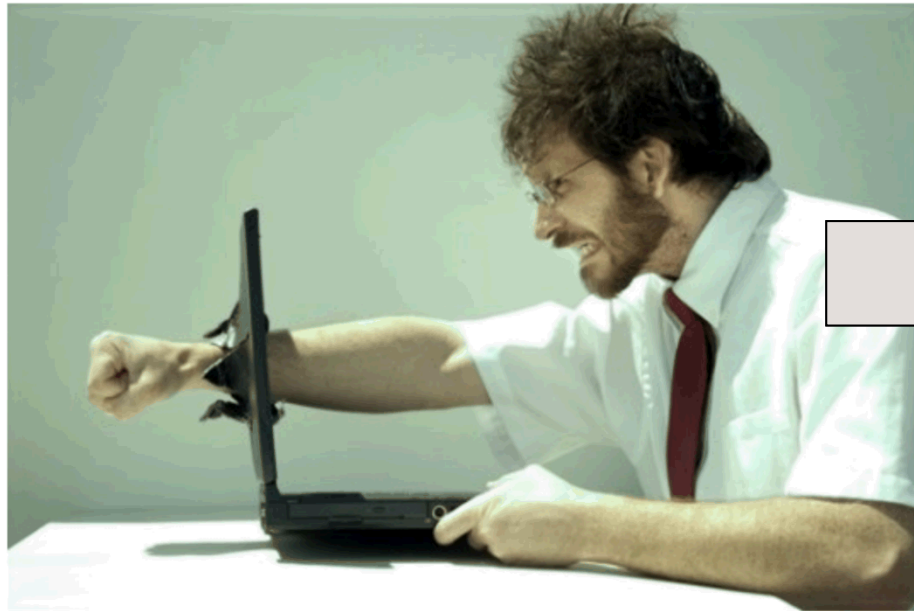


Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

ME



You've been here before, an end user experiences a problem...

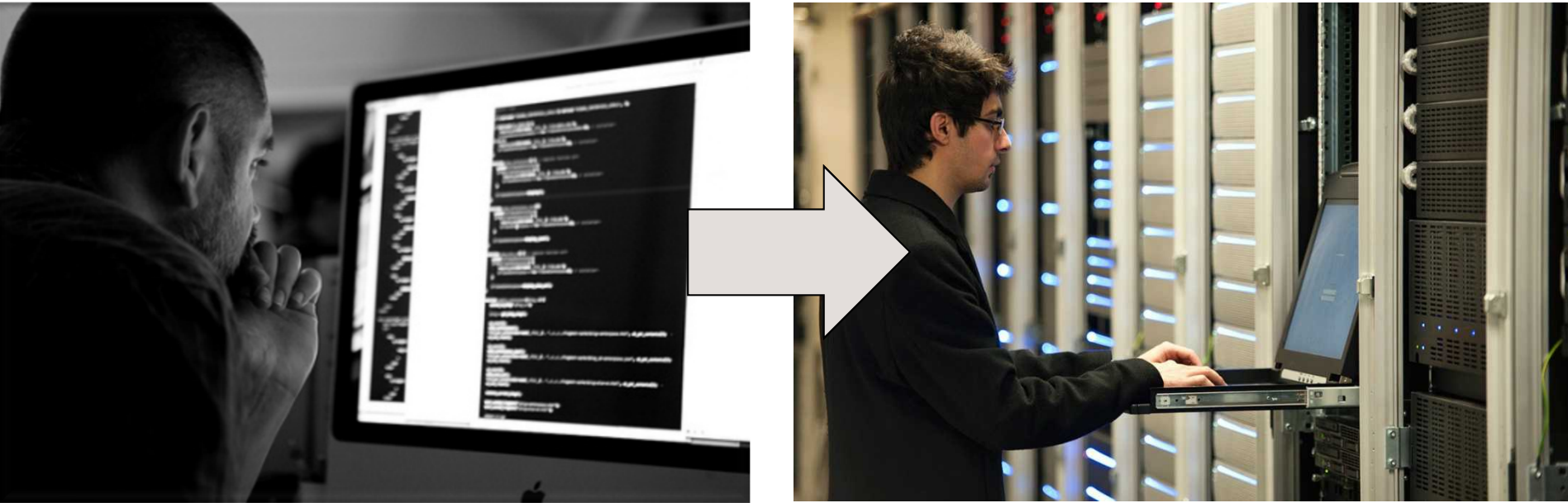


“The web site is down!”



“Ok, checking code...”

Developer can't find an issue with the code...



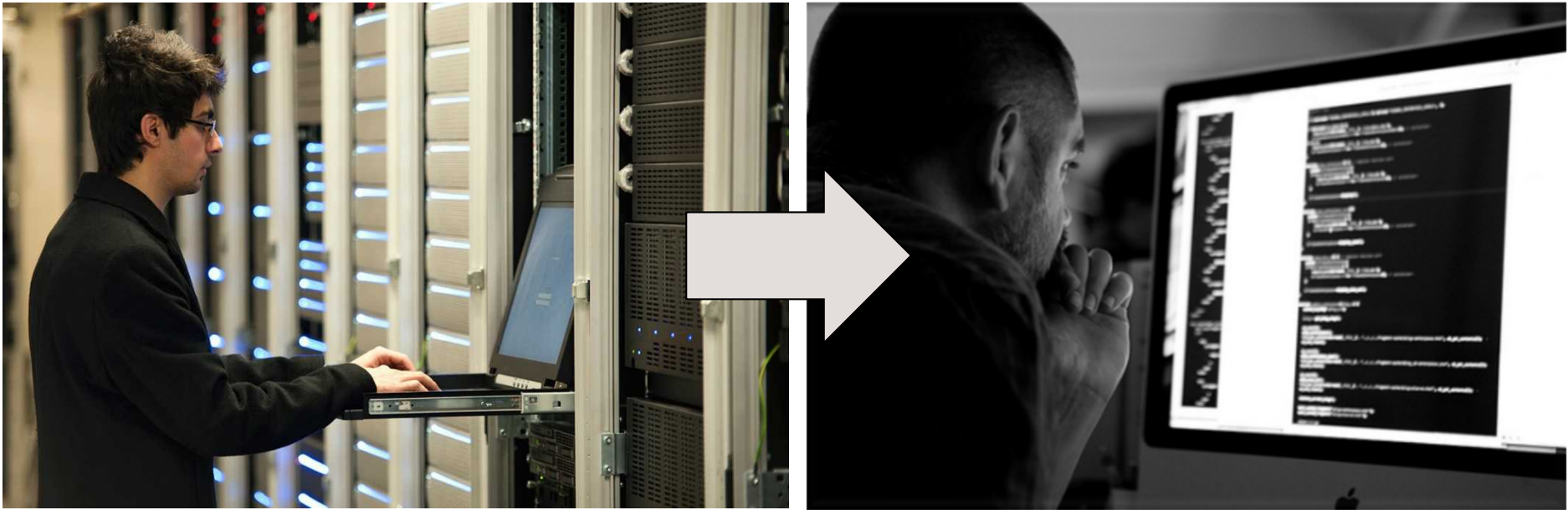
“Sys admin, something is wrong, can you check the logs??”

“Sure thing.”


```
134.253.182.64 - user [06/Apr/2016:13:29:34 -0600] "GET  
/USER_App/reset.html HTTP/1.1" 404 583  
"https://companyapp.com/USER_App/reset.html" "Mozilla/5.0  
(Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"  
rt=75624
```

“Found it!”

Simple solution for an overcomplicated problem.



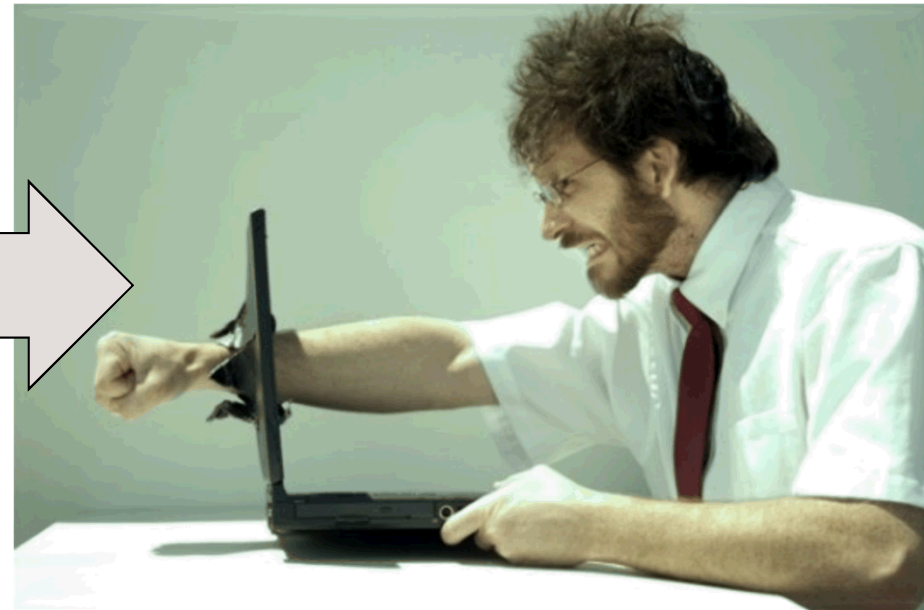
“User typed in old URL.”

“Ahhh...”

Until next time...



“Make sure to use new URL.”



“Ok, still hate the experience.”

What is the problem?

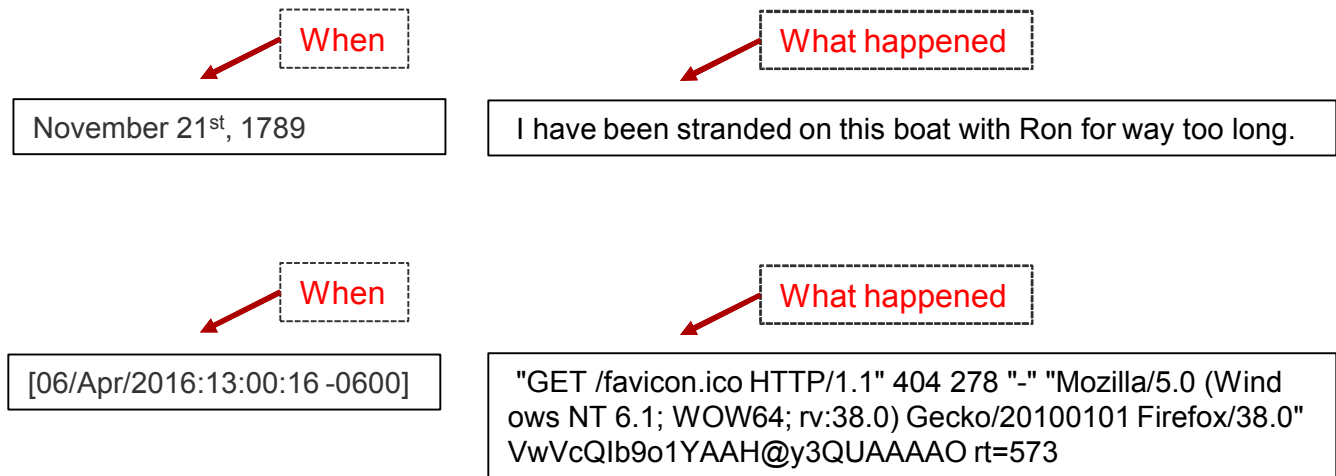
- In this scenario
 - Time Consumed
 - No Metrics
 - No Long Term Solution

—_ (ツ) _ / —

- [illegible]

Logs

- A record of an event.
- Contains a timestamp and relative information.
- Used to understand the activity of the system and to diagnose problems.



How do we obtain Operational Intelligence?

- Understand the value of your data.
- Aggregate, Investigate, and Report.
- Analyze for predictive rather than purely descriptive purposes.

Understand the value of your data

- What is the system trying to accomplish?
- What data do you already rely on?
- What value can you bring to the organization and the customer?

Aggregate, Investigate, and Report

- Aggregate

- Install a data aggregation tool.
 - Splunk ²
 - The Elastic Stack (ELK) ³
 - Elasticsearch
 - Logstash
 - Kibana
 - Loggly ⁴

- Investigate

- Search data efficiently, drilling down and up across data to quickly find the needle in the haystack.

- Report

- Build reports, graphs and charts to create insights into current trends, advanced visualizations, and view the frequency of conditions.

Demo

- Splunk
 - Come on, I am CERTIFIED.
- Using server and client side logging
 - Splunk Forwarder and HTTP Event Collector
 - Custom jQuery Plugin
 - Log4php
- Use Visualizations for Insight

DEMO (cont.)

FizzBuzz Checker

Type in a Number, "Fizz", "Buzz", or "FizzBuzz".

Instructions:
If you type in a number, multiples of 3 display "Fizz", multiples of 5 display "Buzz", and multiples of both display "FizzBuzz".
If you type "Fizz", "Buzz", or "FizzBuzz", it will display numbers up to 100 that fit the description. (ex. "Fizz" == 3, 6, 9, etc.)

Input	Output
Required Submit Clear Output	



Sandia National Laboratories: Enterprise Architectures and Strategies

DEMO (cont.)

```
function start(response) {

    //get the timestamp right before the function guts execute
    startApp = new Date().getTime();

    //initiate logger
    $.ec_logger();
    //log users input
    $.ec_logger.info("user:" + userid + " Response:" + response);

    //check if input is string or numeric
    if ($.isNumeric(response)) {
        $.ec_logger.info(response + " submission is numeric.");
        number(response);
    } else {
        $.ec_logger.info(response + " submission is a string.");
        if (response.toLowerCase() == "fizz") {
            fizz(response);
        } else if (response.toLowerCase() == "buzz") {
            buzz(response);
        } else if (response.toLowerCase() == "fizzbuzz") {
            fizzbuzz(response);
        } else if (response.toLowerCase() == "buttz") {
            buttz(response);
        } else {
            //if input doesn't meet input criteria, log error
            $.ec_logger.error("Response" + response + " is not numeric, or
                meet the String requirements.");

            $('#output').append('<div class="usa-alert usa-alert-error"
                role="alert">' +
                '<div class="usa-alert-body">' +
                '<h3 class="usa-alert-heading">Error Status</h3>' +
                '<p class="usa-alert-text">Your input <span style="text-
                    decoration: underline">' + response + '</span>' +
                ' is not valid!</p>' +
                '</div></div>');
            endFunction();
        }
    }
}
```

```
function fizz(a) {

    //get the timestamp right before the function guts execute
    var start = new Date().getTime();

    //main code being run
    $('#output').append(
        '<div class="usa-alert usa-alert-success" role="alert">' +
        '<div class="usa-alert-body">' +
        '<h3 class="usa-alert-heading">' + a + '</h3>' +
        '<p class="usa-alert-text" id="output_' + counter + '"></p>' +
        '</div></div>');

    for (var i = 1; i <= 100; i++) {
        if (i % 3 == 0) {
            $('#output_' + counter).append(i + "<br>");
        }
    }

    //get end of code timestamp
    var end = new Date().getTime();

    //create execution time of function
    var time = end - start;

    //log the execution time
    $.ec_logger.info('user:' + userid + ' et=' + time);

    counter++;
    endFunction();
}
```

DEMO (cont.)

Instructions:
If you type in a number, multiples of 3 display "Fizz", multiples of 5 display "Buzz", and multiples of both display "FizzBuzz".
If you type "Fizz", "Buzz", or "FizzBuzz", it will display numbers up to 100 that fit the description. (ex. "Fizz" == 3, 6, 9, etc.)

Input

Required

Submit

Clear Output

Output

✓ fizz

3
6
9
12
15
18
21
24
27
30
33
36
39
42
45
48
51
54
57
60
63
66
69
72
75
78
81
84
87
90
93
96
99

 Sandia National Laboratories: Enterprise Architectures and Strategies

Input

Required

Submit

Clear Output

Output

✓ 82
Neither Fizz, Buzz, or FizzBuzz!

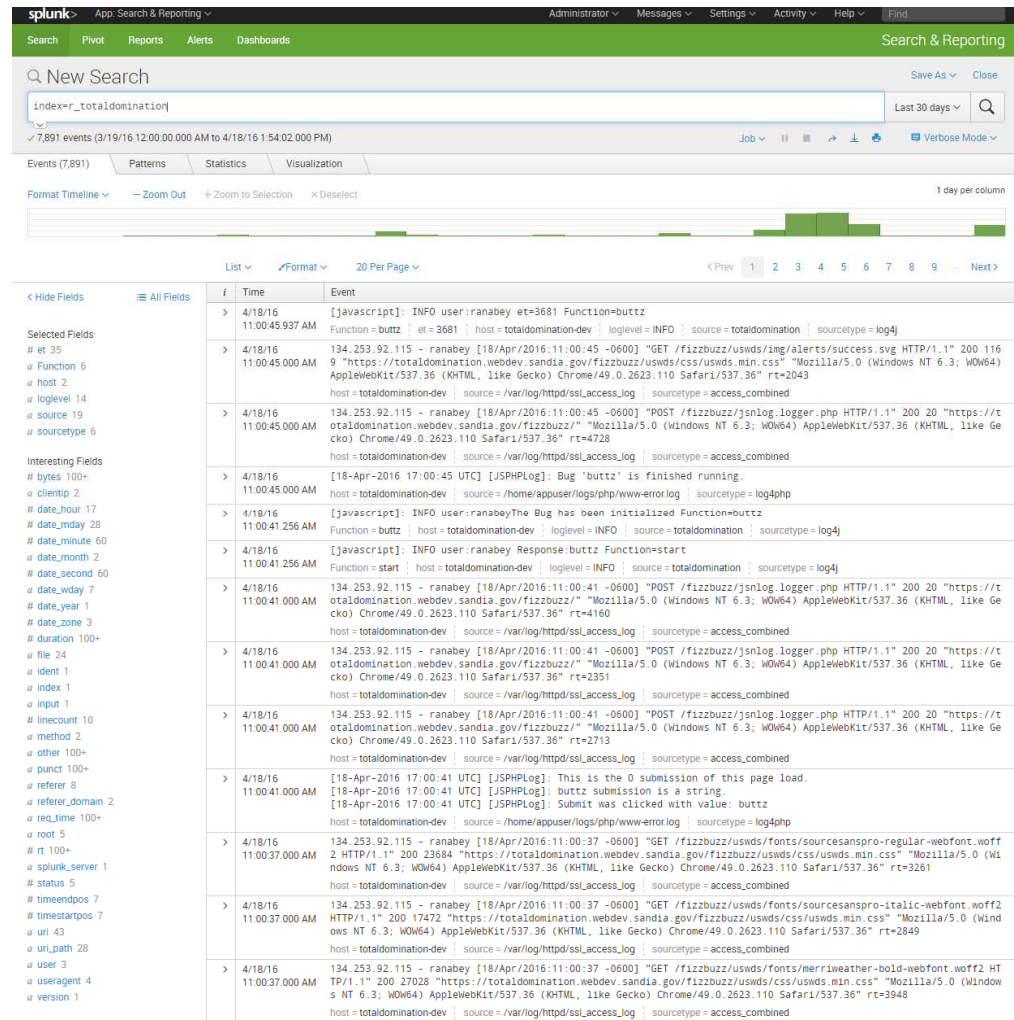
✓ 854693765
Buzz

✓ fizzbuzz
15
30
45
60
75
90

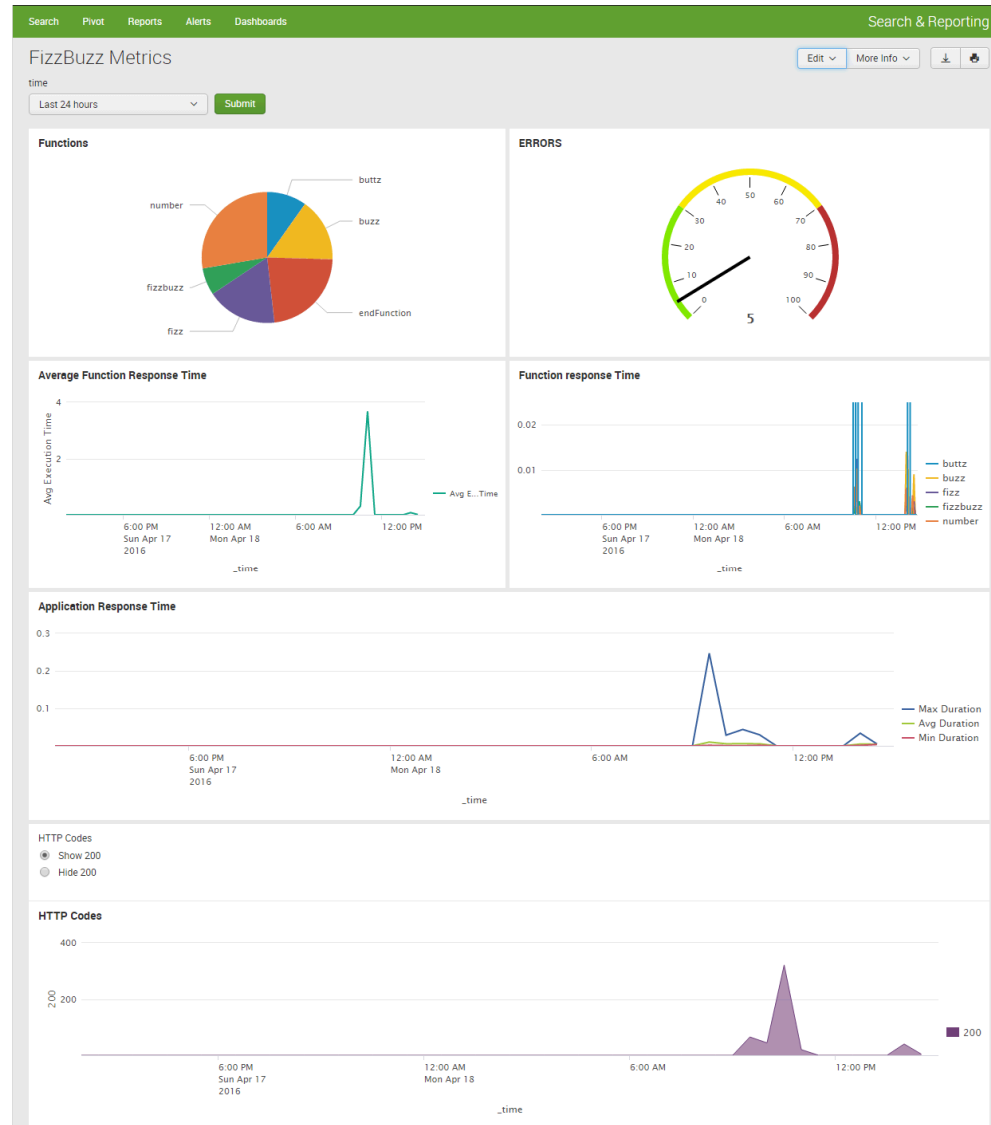
✓ buzz
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100

 Sandia National Laboratories: Enterprise Architectures and Strategies

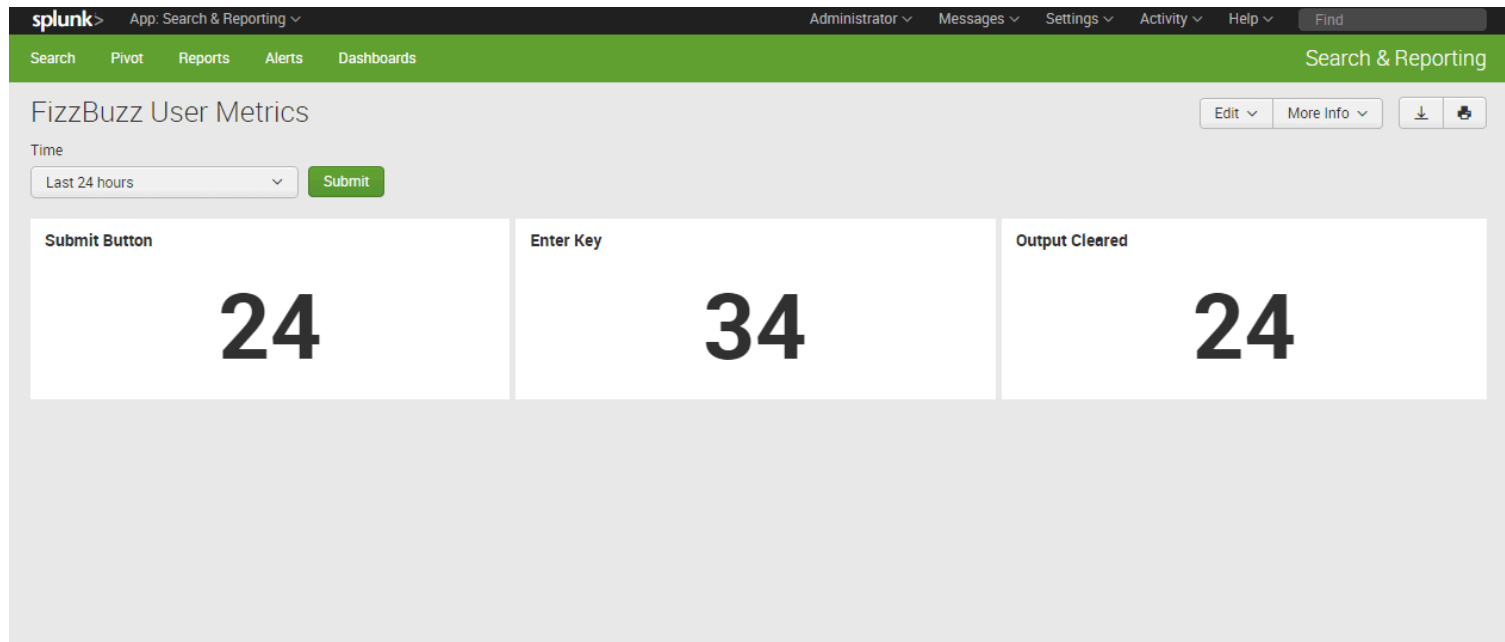
DEMO (cont.)



DEMO (cont.)

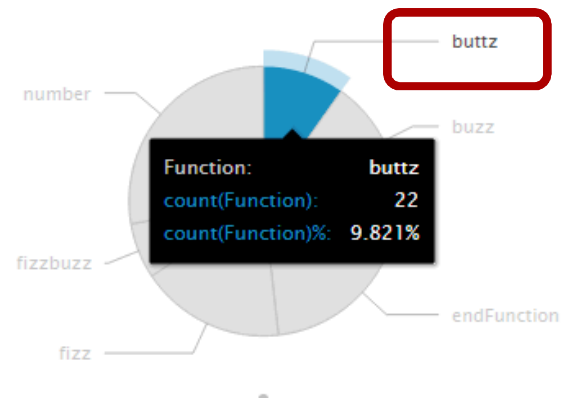


DEMO (cont.)

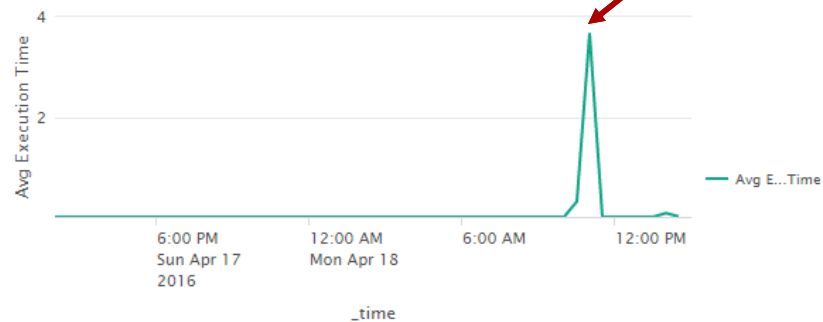


DEMO (cont.)

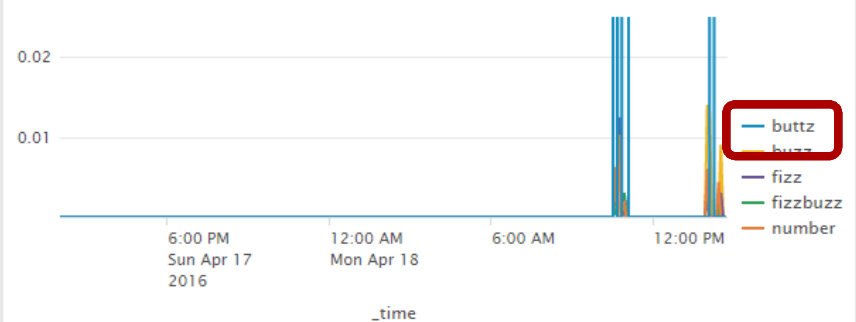
Functions



Average Function Response Time



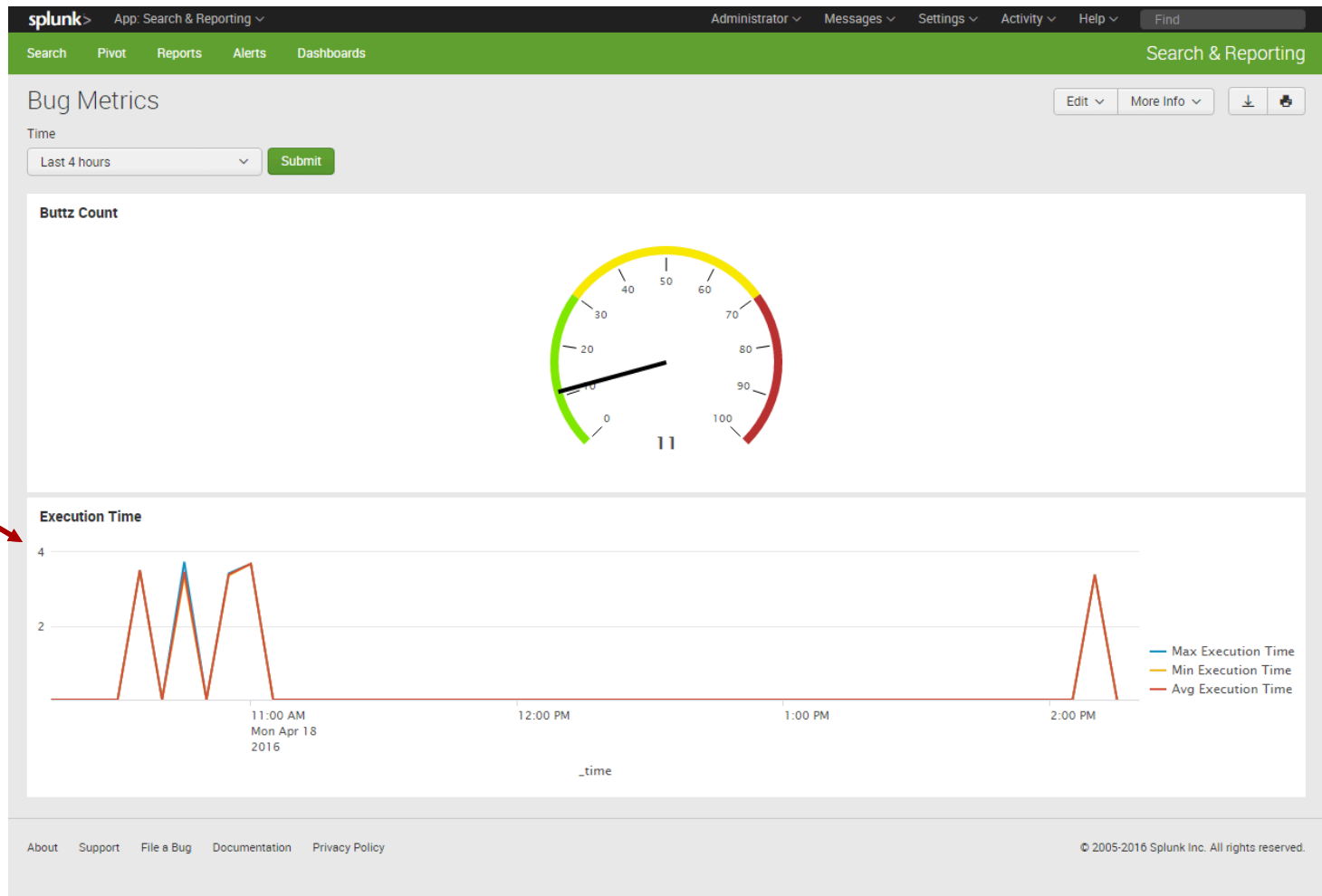
Function response Time



DEMO (cont.)

[illegible]

DEMO (cont.)



DEMO (cont.)

```
function fizz(a) {
```

```
...
```

```
  for (var i = 1; i <= 100; i++) {  
    if (i % 3 == 0) {  
      $('#output_' + counter).append(i + "<br>");  
    }  
  }
```

```
...
```

```
  endFunction();  
}
```

```
function buttz(a) {
```

```
...
```

```
  for (var i = 1; i < 1000000; i++) {  
    if (i % 3 == 0 && i % 5 == 0) {  
      $('#output_' + counter).append("!buttz!<br>");  
    }  
  }
```

```
...
```

```
  endFunction();  
}
```

DEMO (cont.)

Instructions:

If you type in a number, multiples of 3 display "Fizz", multiples of 5 display "Buzz", and multiples of both display "FizzBuzz".

If you type "Fizz", "Buzz", or "FizzBuzz", it will display numbers up to 100 that fit the description. (ex. "Fizz" == 3, 6, 9, etc.)

Input

Required

Submit

Clear Output

Output

✓ 45
FizzBuzz

✓ 34
Neither Fizz, Buzz, or FizzBuzz!

✓ 87
Fizz

! **Error Status**
Your input buttz is not valid!



Sandia National Laboratories: Enterprise Architectures and Strategies

DEMO (cont.)

FizzBuzz Metrics

time

Last 60 minutes

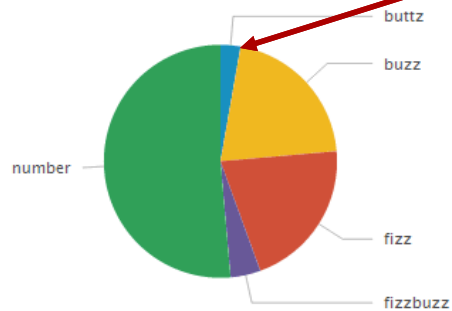
Submit

Edit

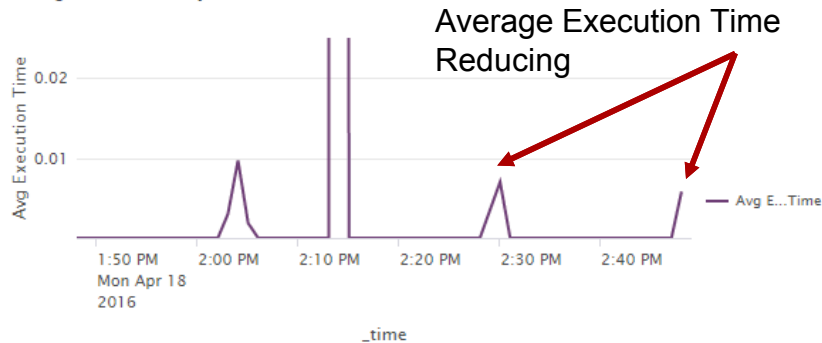
More Info



Functions

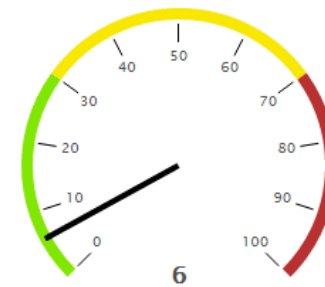


Average Function Response Time



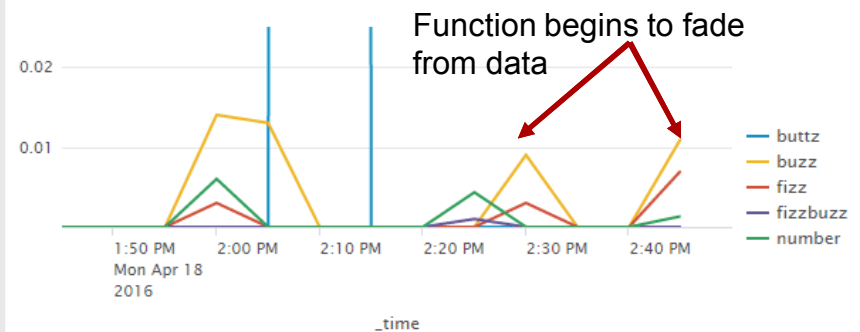
Captured as Error

ERRORS



Function response Time

9m ago



Questions



End Notes

- 1 <http://www.theclarogroup.com/hidden-gems-creating-value-from-unstructured-data/>
- 2 <http://www.splunk.com/>
- 3 <https://www.elastic.co/webinars/introduction-elk-stack>
- 4 <https://www.loggly.com/>