Elasticsearch In Netflix

Danny Yuan, Jae Bae

Welcome

Hashtag: #ES_in_Netflix

@Elasticsearch - Elasticsearch

@stonse - Sudhir Tonse

@g9yuayon - Danny Yuan

@metacret - Jae Bae

NETFLIX

Who Are We?

Who Are We?

Software engineers in Netflix's Platform Engineering team, working on large scale data infrastructure

NETFLIX®

Who Are We?

Software engineers in Netflix's Platform Engineering team, working on large scale data infrastructure

Building and operating Netflix's cloud real-time query service

NETFLIX®

Why Are We Here?

Why Are We Here?

How We Use Elasticsearch

Why Are We Here?

How We Use Elasticsearch

Why Elasticsearch

Why Are We Here?

How We Use Elasticsearch

Why Elasticsearch

How We Run Elasticsearch

Why Are We Here?

How We Use Elasticsearch

Why Elasticsearch

How We Run Elasticsearch

To Seek Your Feedback

How We Use Elasticsearch

Querying Log Events

Tracking Service Deployments

Querying Log Events

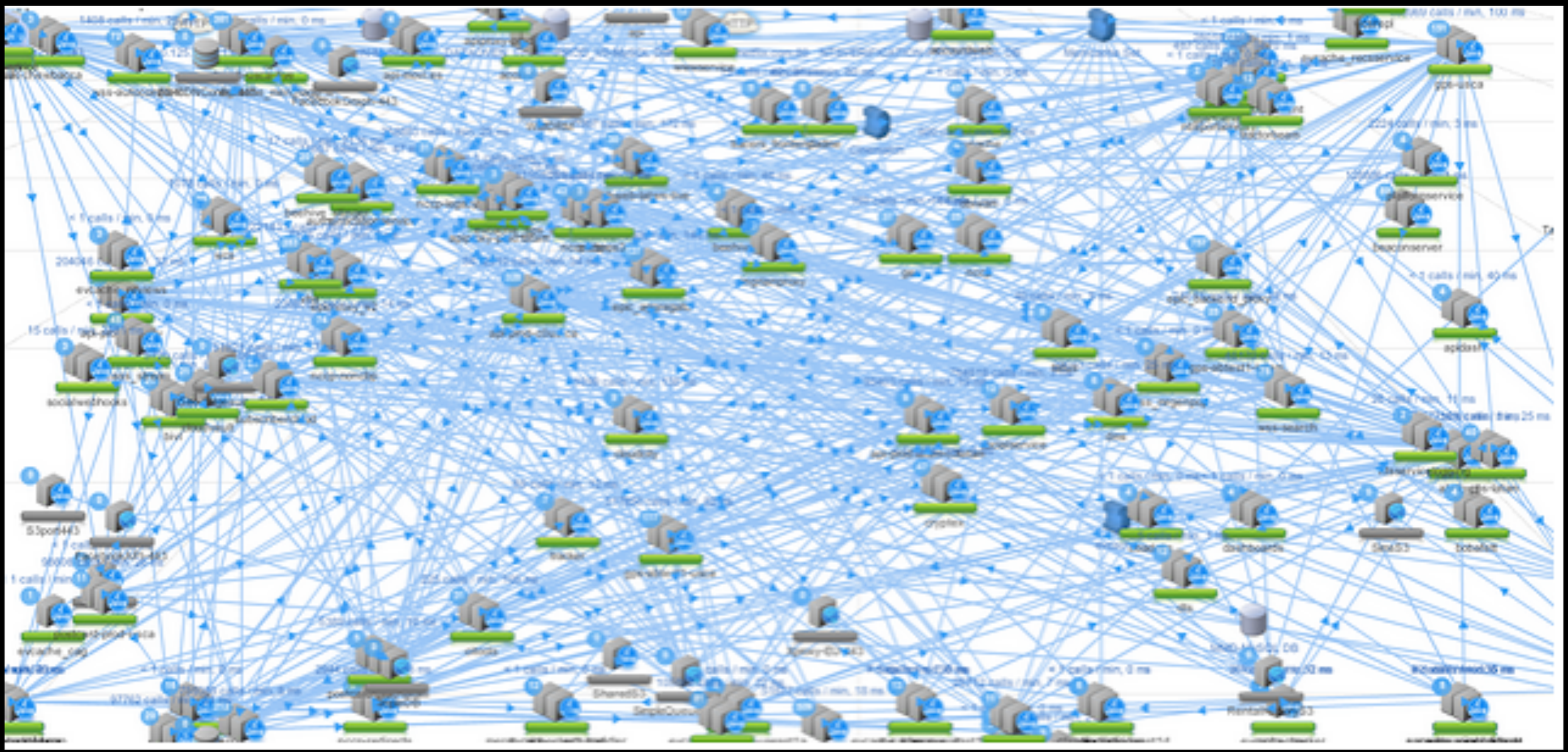
A Little Historical Perspective

Netflix is a log generating company that also happens to stream movies

- Adrian Cockroft

photo credit: http://www.flickr.com/photos/decade_null/142235888/sizes/o/in/photostream/

NETFLIX®



NETFLIX®

Operational

Insights

Business

Analysis Debugging

Trend

NETFLIX®

A Humble Beginning

A Humble Beginning

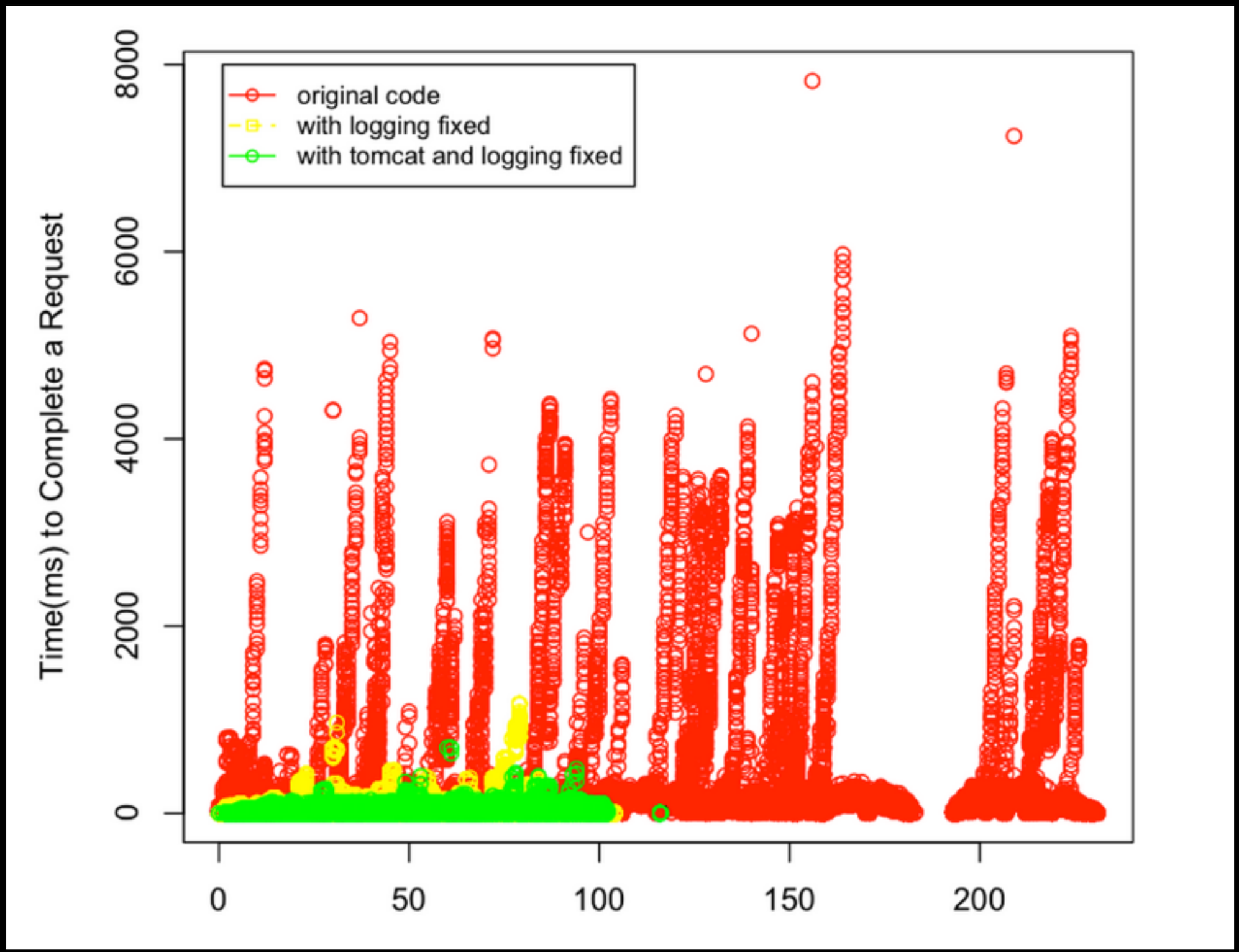
```
awk '{print $3, $10}' access.log | sort | uniq -c | sort -nr
```

A Humble Beginning

```
plot_all <- function(files, colors){
  file <- head(files, 1)
  color <- head(colors, 1)
  data <- load_data(file)
  plot(data, type="p", col=color, xlab="Elapse        ds)", ylab="Ti

max_latency = max(data$V2)
```

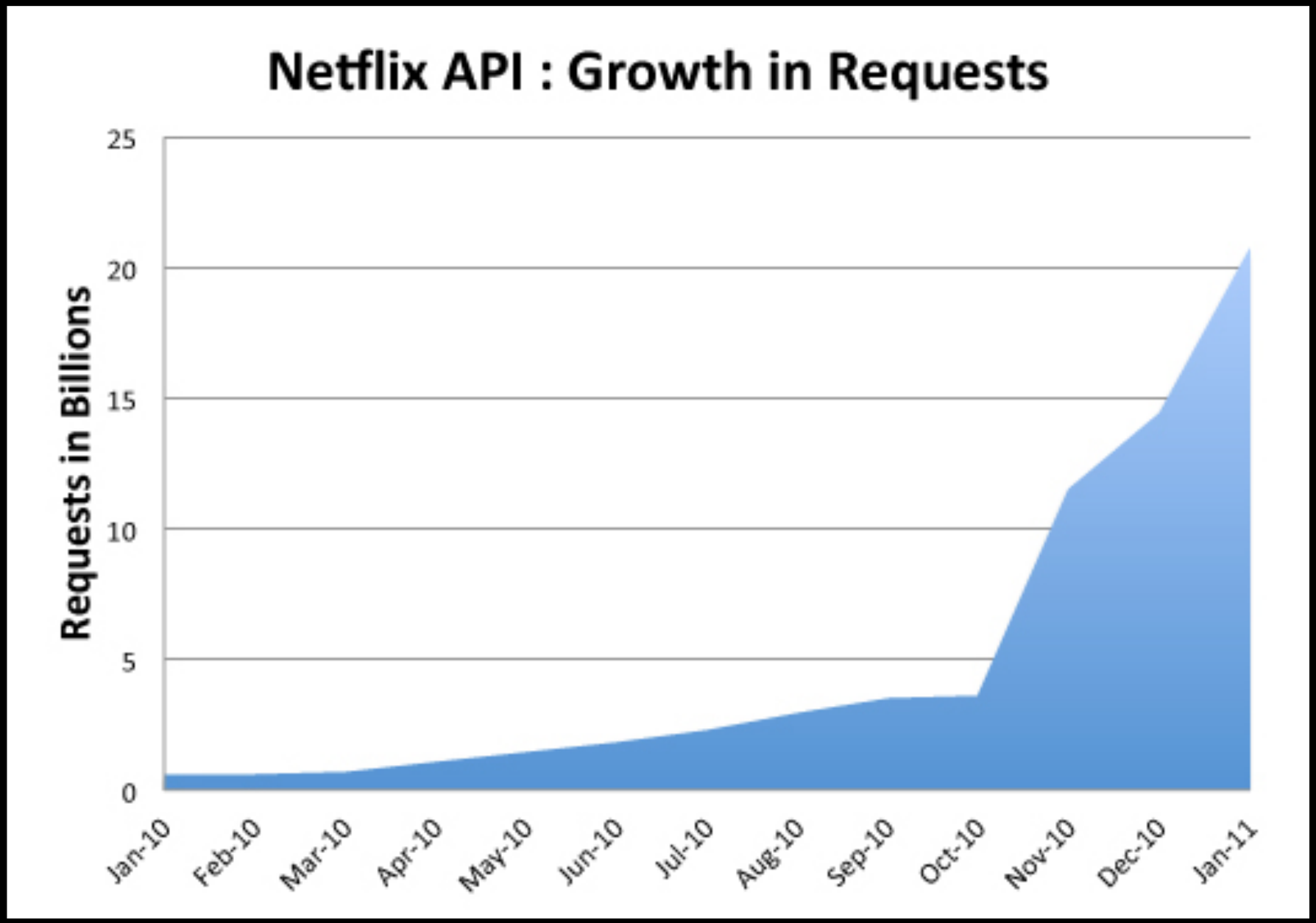
NETFLIX


original code
with logging fixed
with tomcat and logging fixed
Time(ms) to Complete a Request
0
2000
4000
6000
8000
0
50
100
150
200

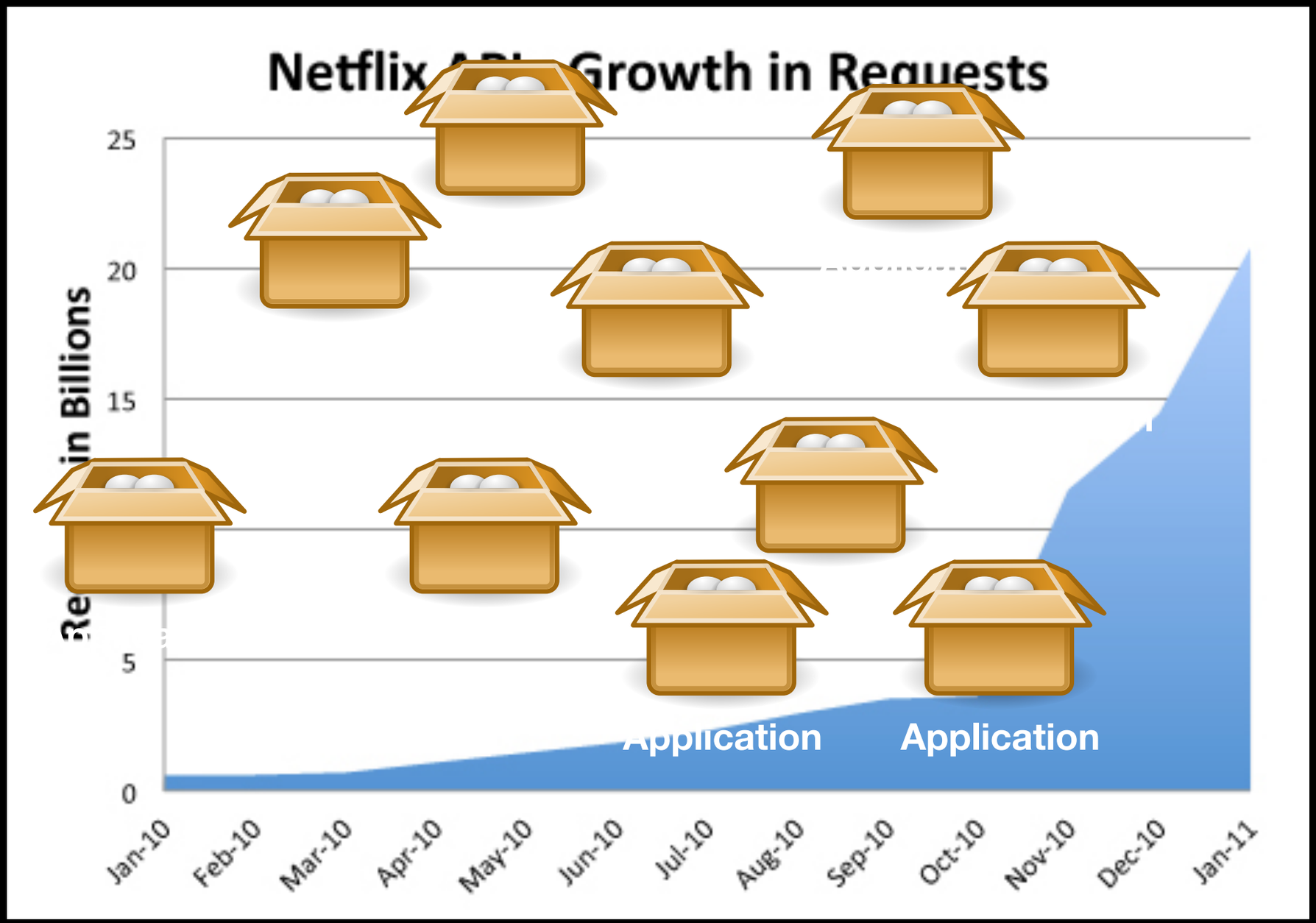
NETFLIX

Things Changed


NETFLIX®


Netflix API : Growth in Requests
Requests in Billions
25
20
15
10
5
0
Jan-10
Feb-10
Mar-10
Apr-10
May-10
Jun-10
Jul-10
Aug-10
Sep-10
Oct-10
Nov-10
Dec-10
Jan-11

NETFLIX®


Netflix API - Growth in Requests
Billions in
25
20
15
5
0
Jan-10
Feb-10
Mar-10
Apr-10
May-10
Jun-10
Jul-10
Aug-10
Sep-10
Oct-10
Nov-10
Dec-10
Jan-11
Application
Application

NETFLIX®

70,000,000,000

NETFLIX®

1,500,000

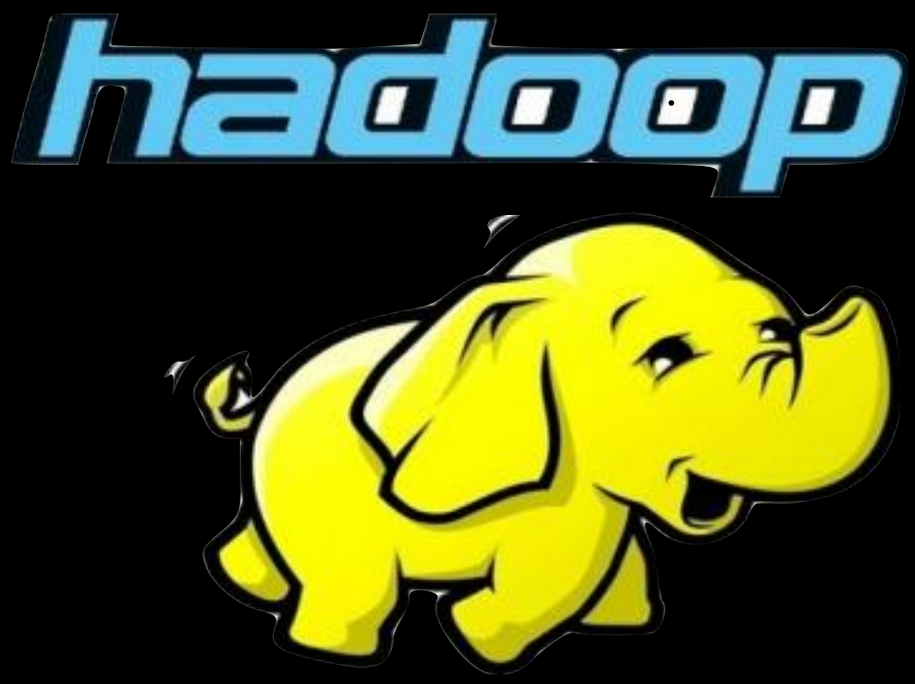
NETFLIX®

Making Sense of Billions of Events

luckey_sun | Flickr via Creative Commons

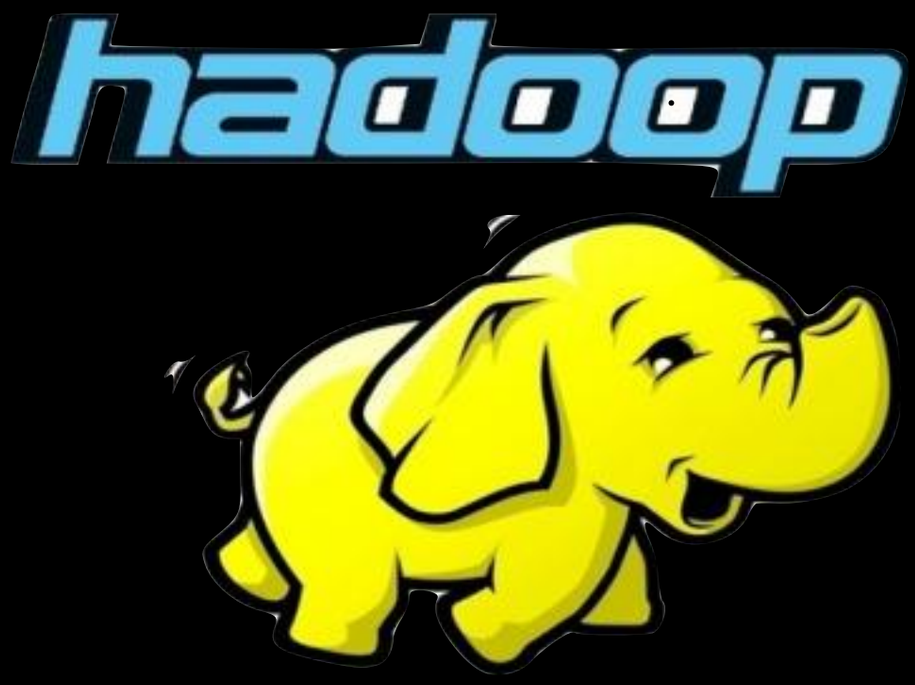
So We Evolved

So We Evolved



NETFLIX®

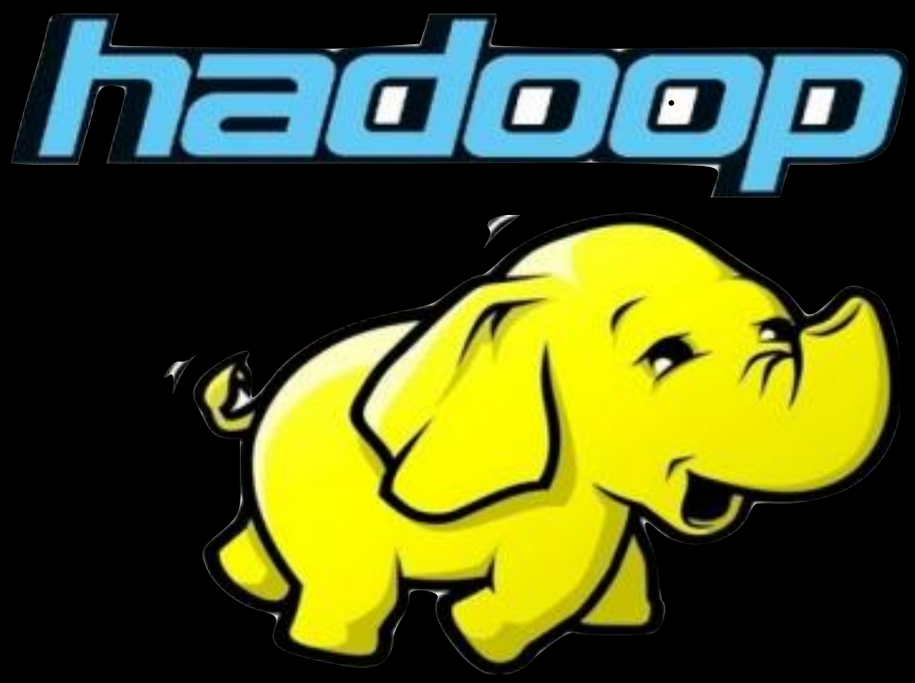
So We Evolved



hgrep -C 10 -k 5,2,3 'users.*[1-9]{3}' *catalina.out s3//bucket

NETFLIX

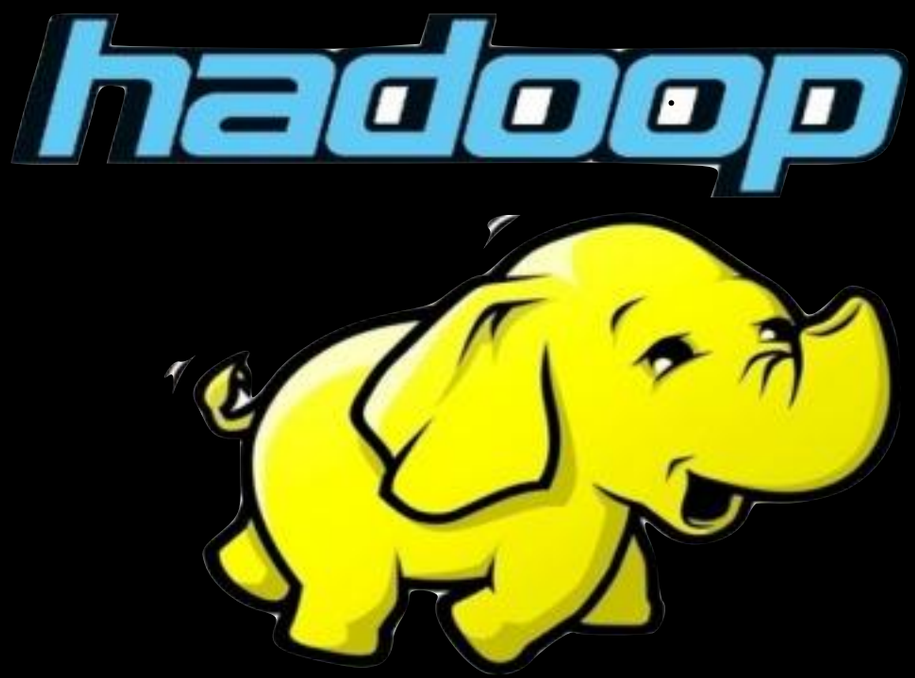
So We Evolved



hgrep -C 10 -k 5,2,3 'users.*[1-9]{3}' *catalina.out s3//bucket

NETFLIX

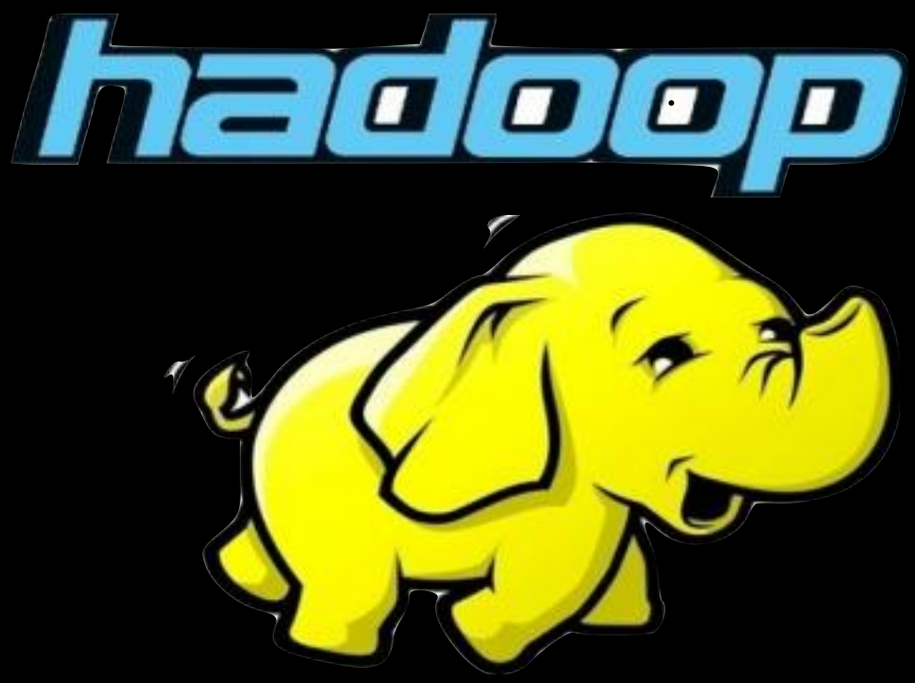
So We Evolved



hgrep -C 10 -k 5,2,3 'users.*[1-9]{3}' *catalina.out s3//bucket

NETFLIX

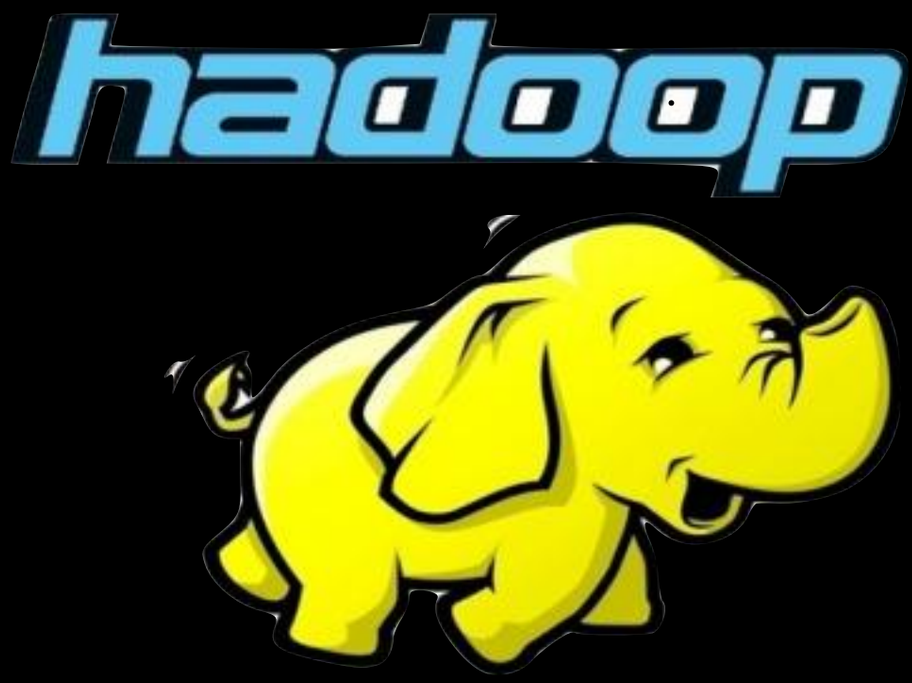
So We Evolved



hgrep -C 10 -k 5,2,3 'users.*[1-9]{3}' *catalina.out s3//bucket

NETFLIX

So We Evolved



hgrep -C 10 -k 5,2,3 'users.*[1-9]{3}' *catalina.out s3//bucket

select * from log_events where dateint=20140101

NETFLIX

Field Name	Field Value
Client	“API”
Server	“Cryptex”
StatusCode	200
ResponseTime	73

Server Farm

Log data

Server Farm

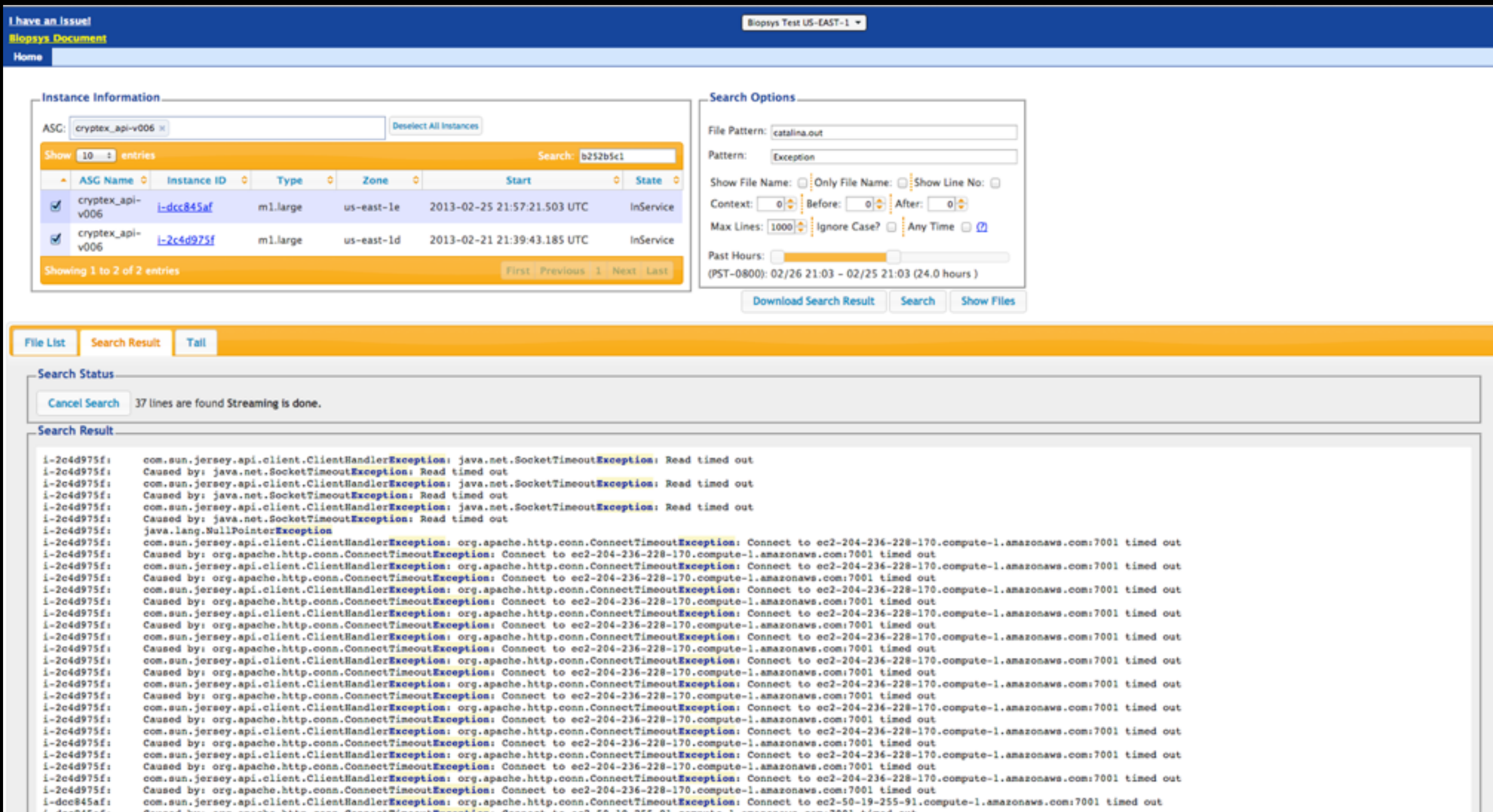
Log data

Log Collectors

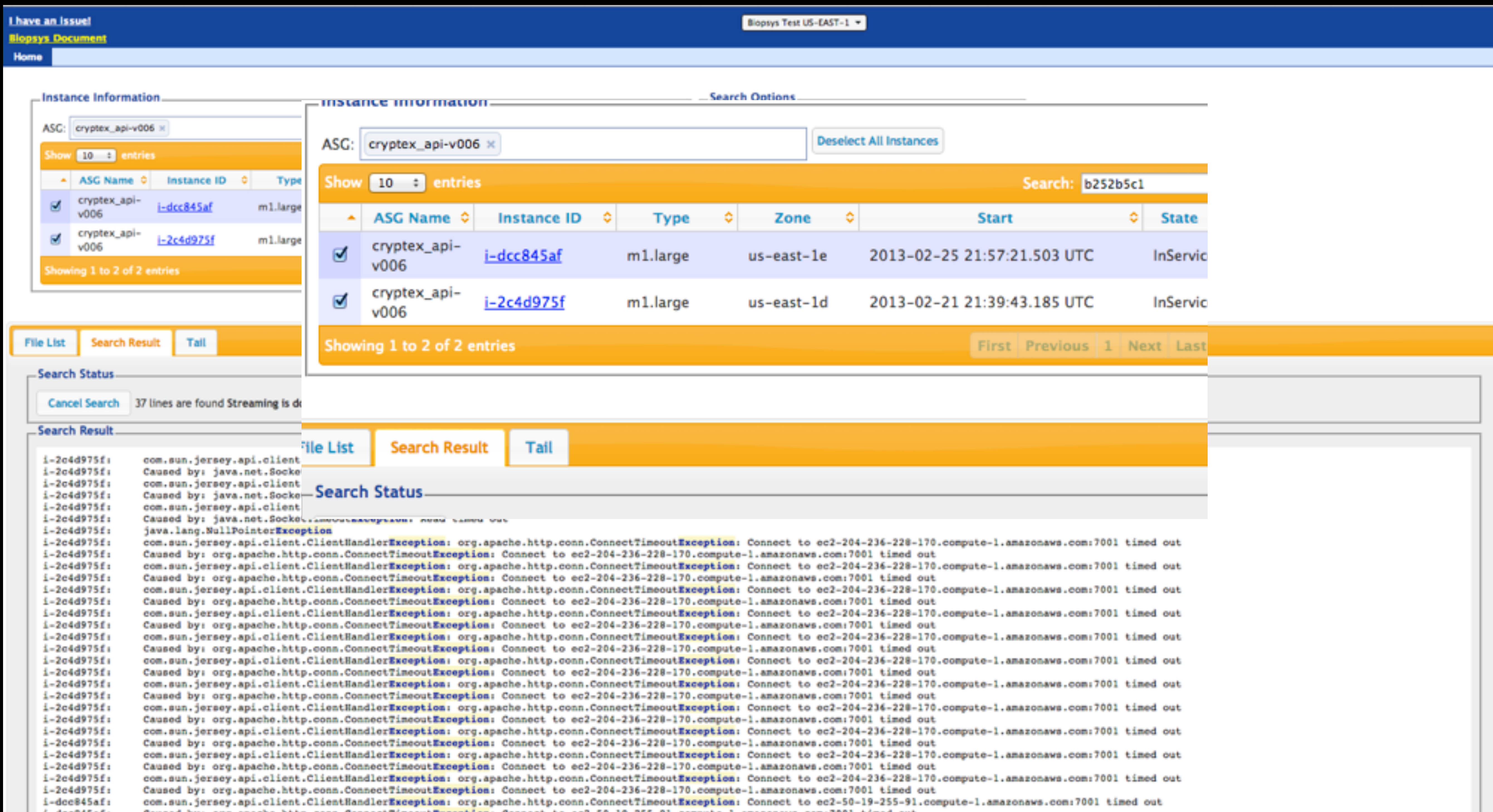
Server Farm

Log data

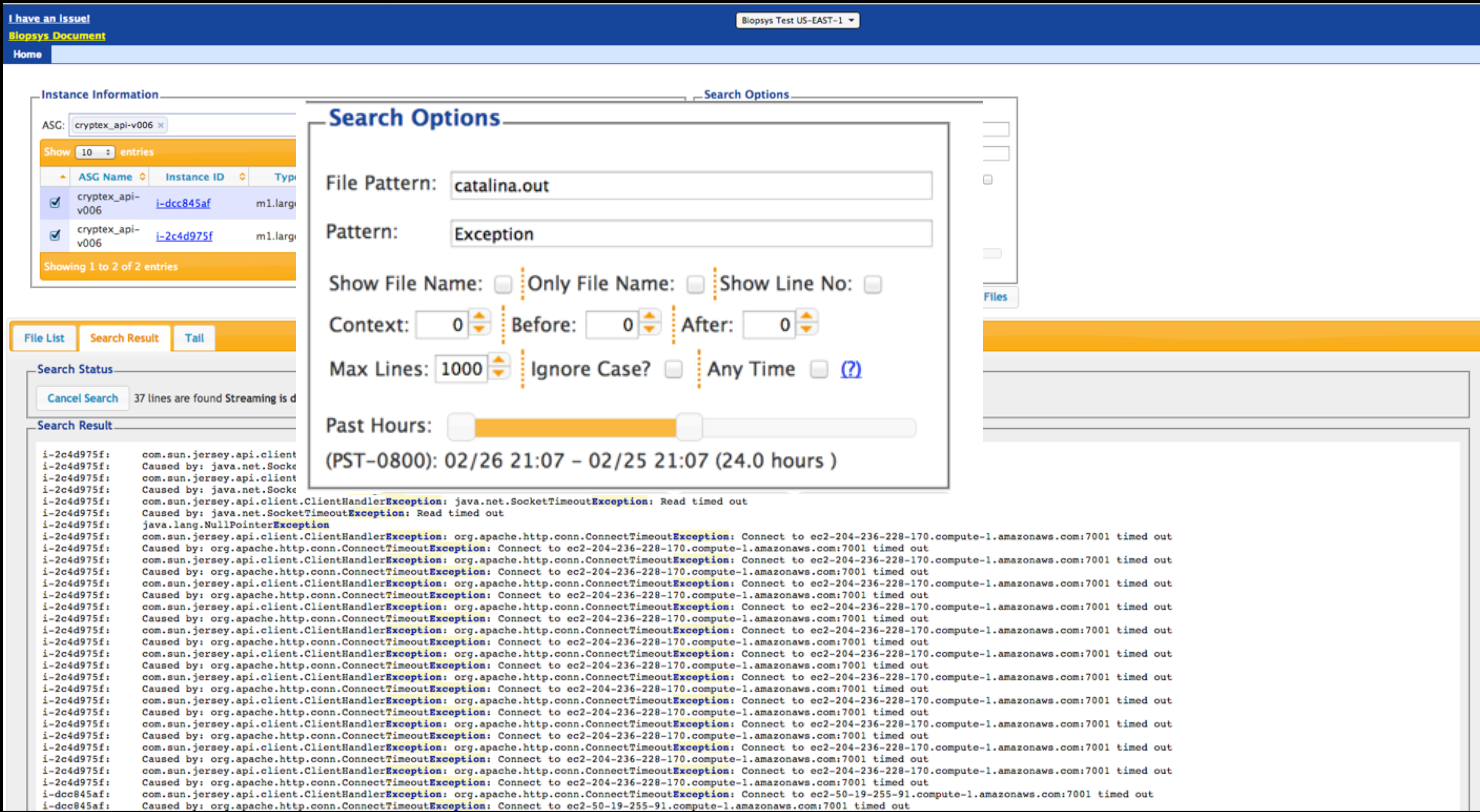
NETFLIX



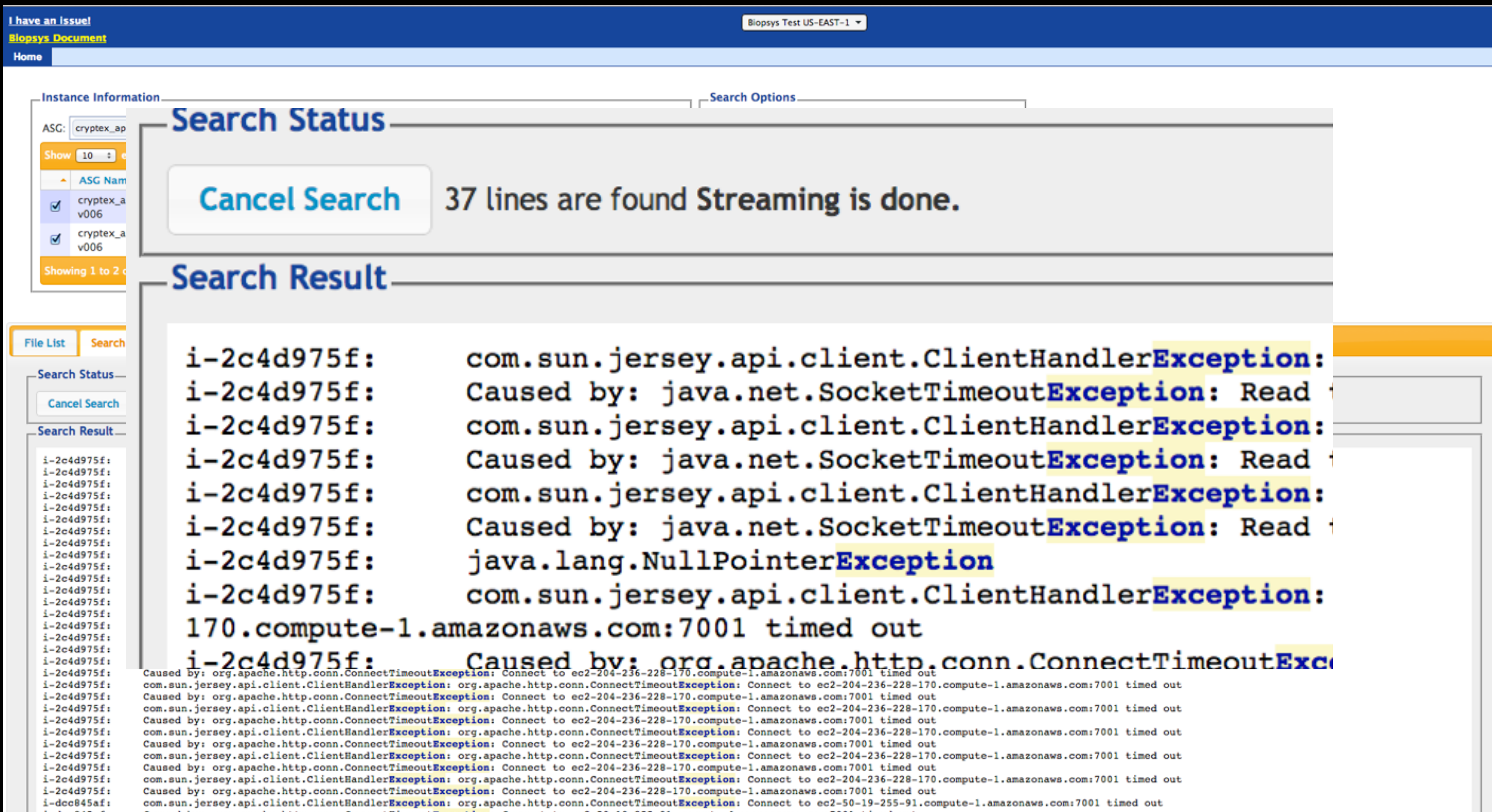
I have an issue!
Biopsys Document
Biopsys Test US-EAST-1
Home
Instance Information
ASG: cryptex_api-v006
Deselect All Instances
Show 10 entries
Search: b252b5c1
ASG Name | Instance ID | Type | Zone | Start | State
cryptex_api-v006 | i-dcc845af | m1.large | us-east-1e | 2013-02-25 21:57:21.503 UTC | InService
cryptex_api-v006 | i-2c4d975f | m1.large | us-east-1d | 2013-02-21 21:39:43.185 UTC | InService
Showing 1 to 2 of 2 entries
First Previous 1 Next Last
Search Options
File Pattern: catalina.out
Pattern: Exception
Show File Name: Only File Name: Show Line No:
Context: 0 Before: 0 After: 0
Max Lines: 1000 Ignore Case? Any Time (?)
Past Hours:
(PST-0800): 02/26 21:03 - 02/25 21:03 (24.0 hours)
Download Search Result
Search
Show Files
File List
Search Result
Tail
Search Status
Cancel Search
37 lines are found Streaming is done.
Search Result
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: java.lang.NullPointerException
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-dcc845af: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out
i-dcc845af: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out


I have an issue!
Biopsys Document
Biopsys Test US-EAST-1
Home
Instance Information
Search Options
ASG: cryptex_api-v006
Deselect All Instances
Show 10 entries
Search: b252b5c1
ASG Name
Instance ID
Type
Zone
Start
State
cryptex_api-v006
i-dcc845af
m1.large
us-east-1e
2013-02-25 21:57:21.503 UTC
InServic
cryptex_api-v006
i-2c4d975f
m1.large
us-east-1d
2013-02-21 21:39:43.185 UTC
InServic
Showing 1 to 2 of 2 entries
First Previous 1 Next Last
File List
Search Result
Tail
Search Status
Cancel Search
37 lines are found Streaming is d
Search Result
i-2c4d975f: java.lang.NullPointerException
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-dcc845af: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out
i-dcc845af: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out

NETFLIX



I have an issue!
Biopsys Document
Biopsys Test US-EAST-1
Home
Instance Information
ASG: cryptex_api-v006
Show 10 entries
ASG Name
Instance ID
Typ
cryptex_api-v006 i-dcc845af m1.larg
cryptex_api-v006 i-2c4d975f m1.larg
Showing 1 to 2 of 2 entries
Search Options
Search Options
File Pattern: catalina.out
Pattern: Exception
Show File Name:
Only File Name:
Show Line No:
Context: 0
Before: 0
After: 0
Max Lines: 1000
Ignore Case?
Any Time
(?)
Past Hours:
(PST-0800): 02/26 21:07 - 02/25 21:07 (24.0 hours)
Files
File List
Search Result
Tail
Search Status
Cancel Search
37 lines are found Streaming is d
Search Result
i-2c4d975f: com.sun.jersey.api.client
i-2c4d975f: Caused by: java.net.Sock
i-2c4d975f: com.sun.jersey.api.client
i-2c4d975f: Caused by: java.net.Sock
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read timed out
i-2c4d975f: java.lang.NullPointerException
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-dcc845af: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out
i-dcc845af: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out


I have an Issue!
Biopsys Document
Biopsys Test US-EAST-1
Home
Instance Information
Search Options
ASG: cryptex_ap
Show 10
ASG Nam
cryptex_a v006
cryptex_a v006
Showing 1 to 2
File List
Search
Search Status
Cancel Search
37 lines are found Streaming is done.
Search Result
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException:
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException:
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException:
i-2c4d975f: Caused by: java.net.SocketTimeoutException: Read
i-2c4d975f: java.lang.NullPointerException
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException:
170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutExc
com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-dcc845af: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out
i-dcc845af: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out

NETFLIX

I have an issue!

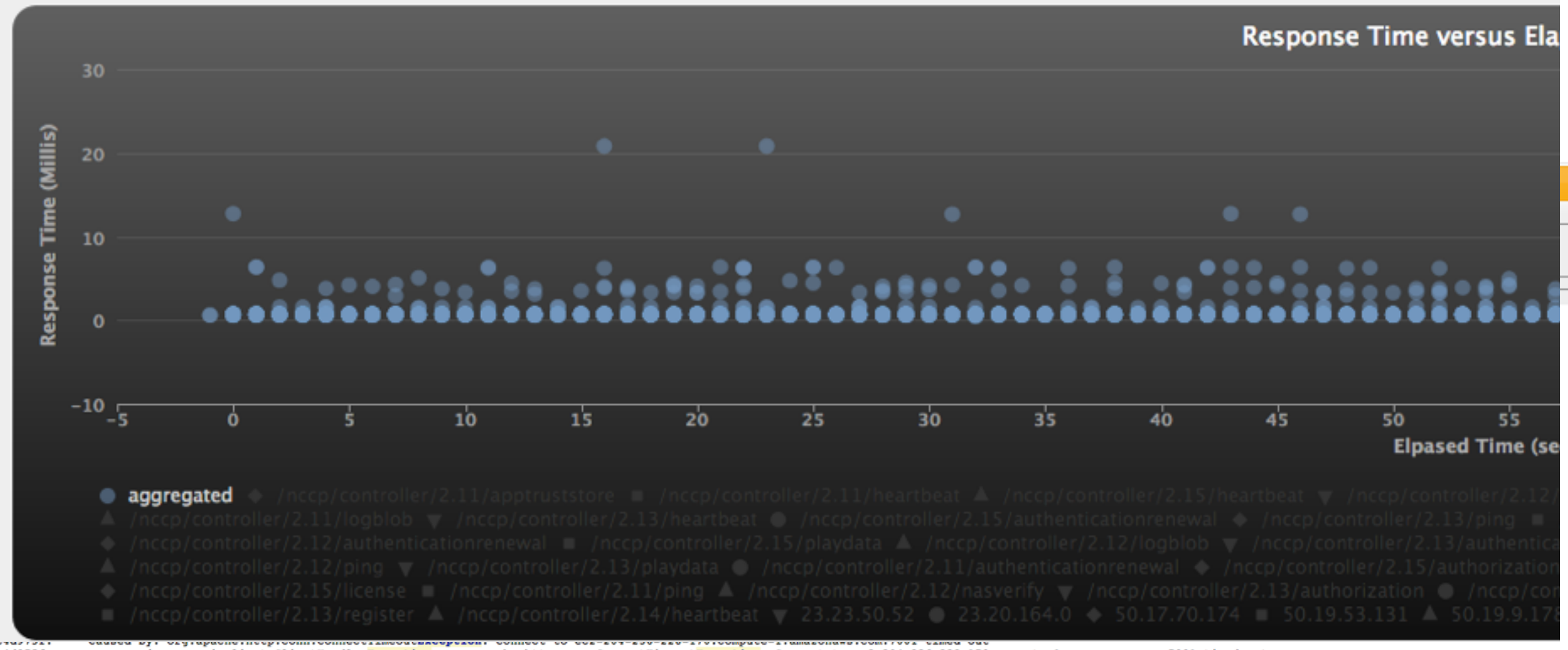
Biopsys Test US-EAST-1

Home

Tail Controls

Lock Scroll: ☐ | Cancel Tail | Select Log Type: NCCP Apache Log | Tail View | Aggregate: ☑ | Clear Results

Access Graph



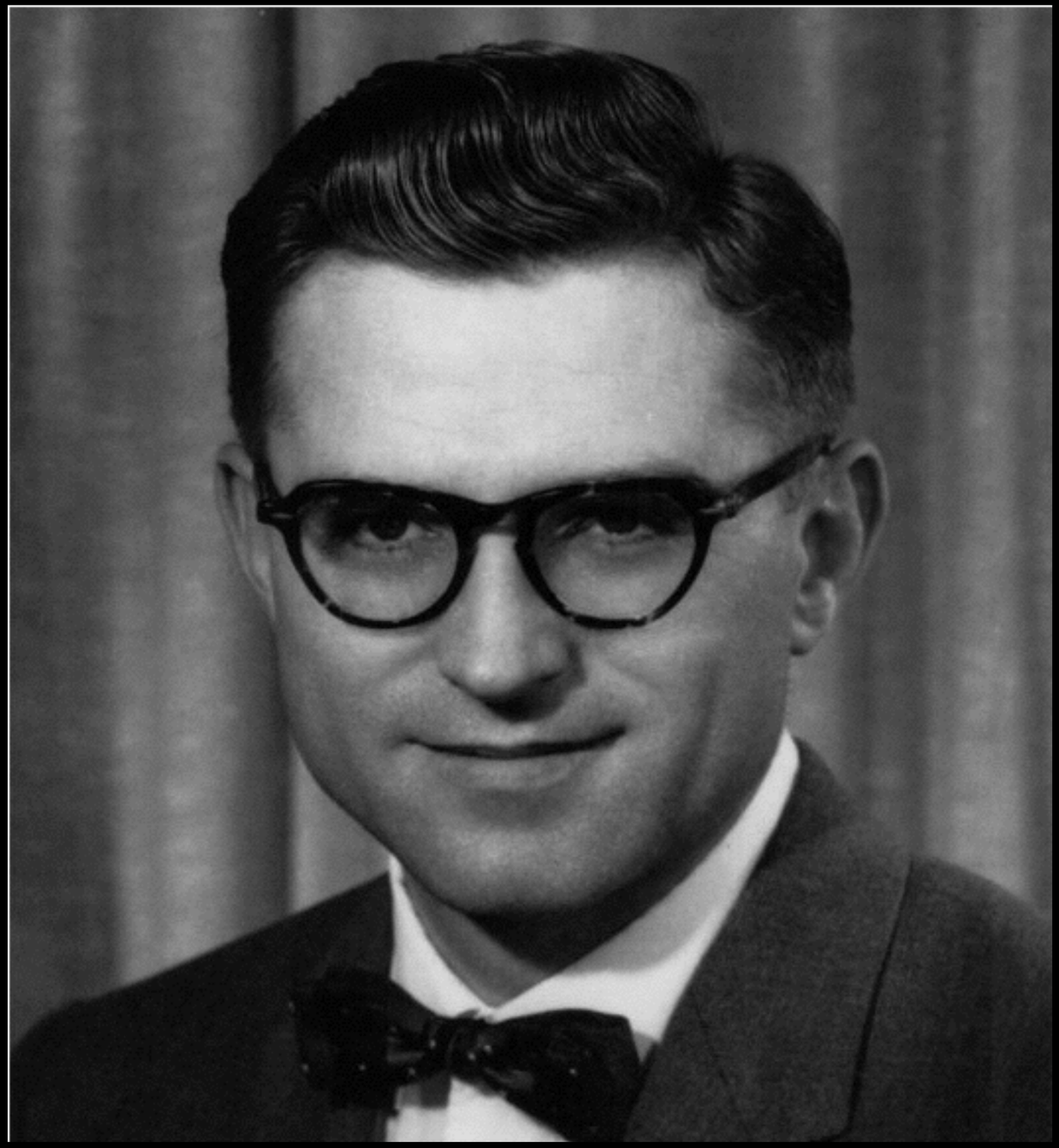

```
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-2c4d975f: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-204-236-228-170.compute-1.amazonaws.com:7001 timed out
i-dcc845af: com.sun.jersey.api.client.ClientHandlerException: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out
i-dcc845af: Caused by: org.apache.http.conn.ConnectTimeoutException: Connect to ec2-50-19-255-91.compute-1.amazonaws.com:7001 timed out
```

NETFLIX®

What Could Go Wrong?

"BRUTE FORCE"

NETFLIX®



You thought parallelization would save the day?
Think again

NETFLIX®

$$T(N) = \frac{N}{1 - (1 - B)N)}$$

NETFLIX®

What Is Missing?

Interactive Exploration

NETFLIX®

Functional Requirements

Arbitrary Boolean Queries

Aggregated Query
- Top N Query
- Trend
- Distribution

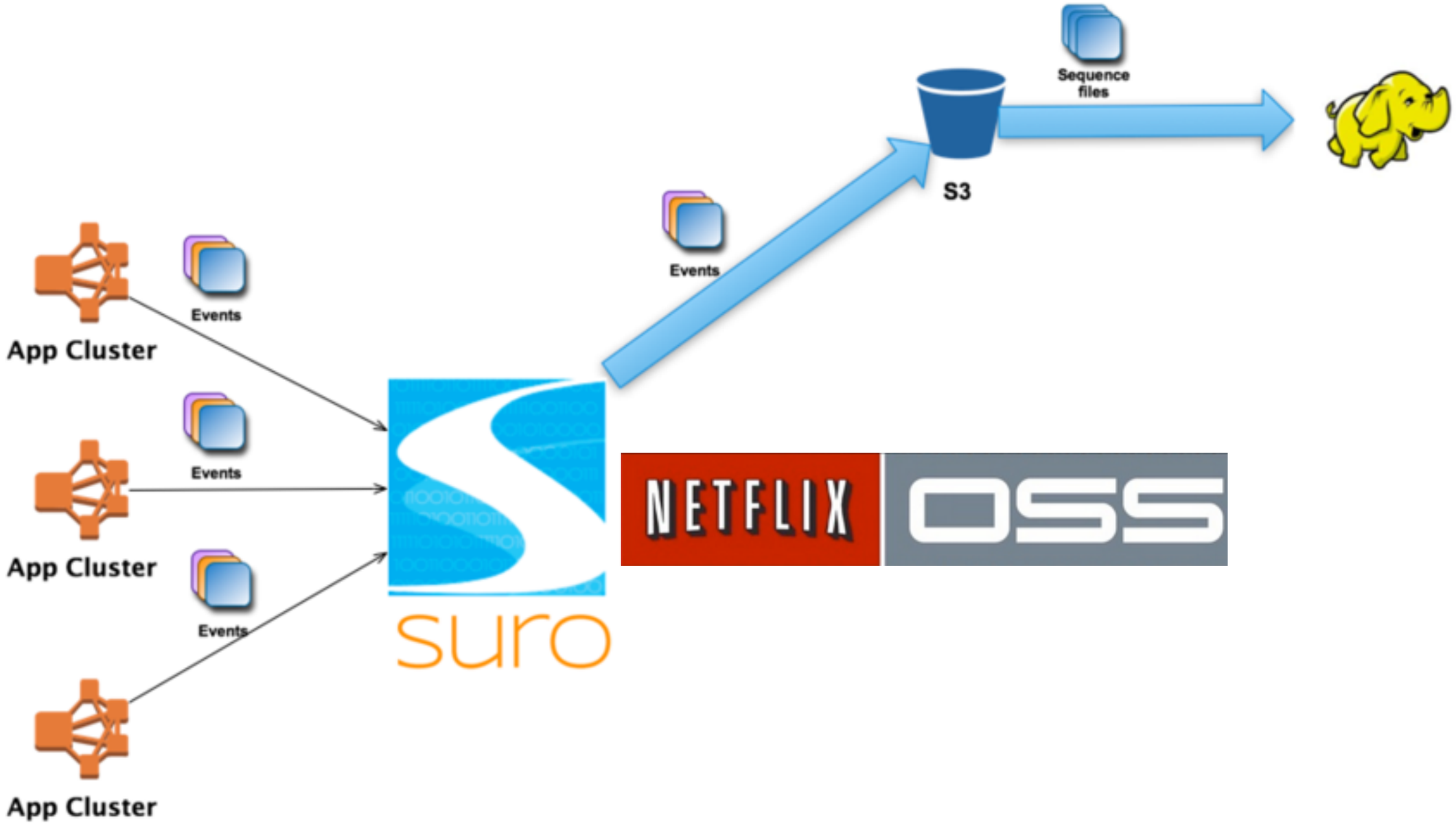
Non-Functional Requirements

- Interactive (response within seconds)

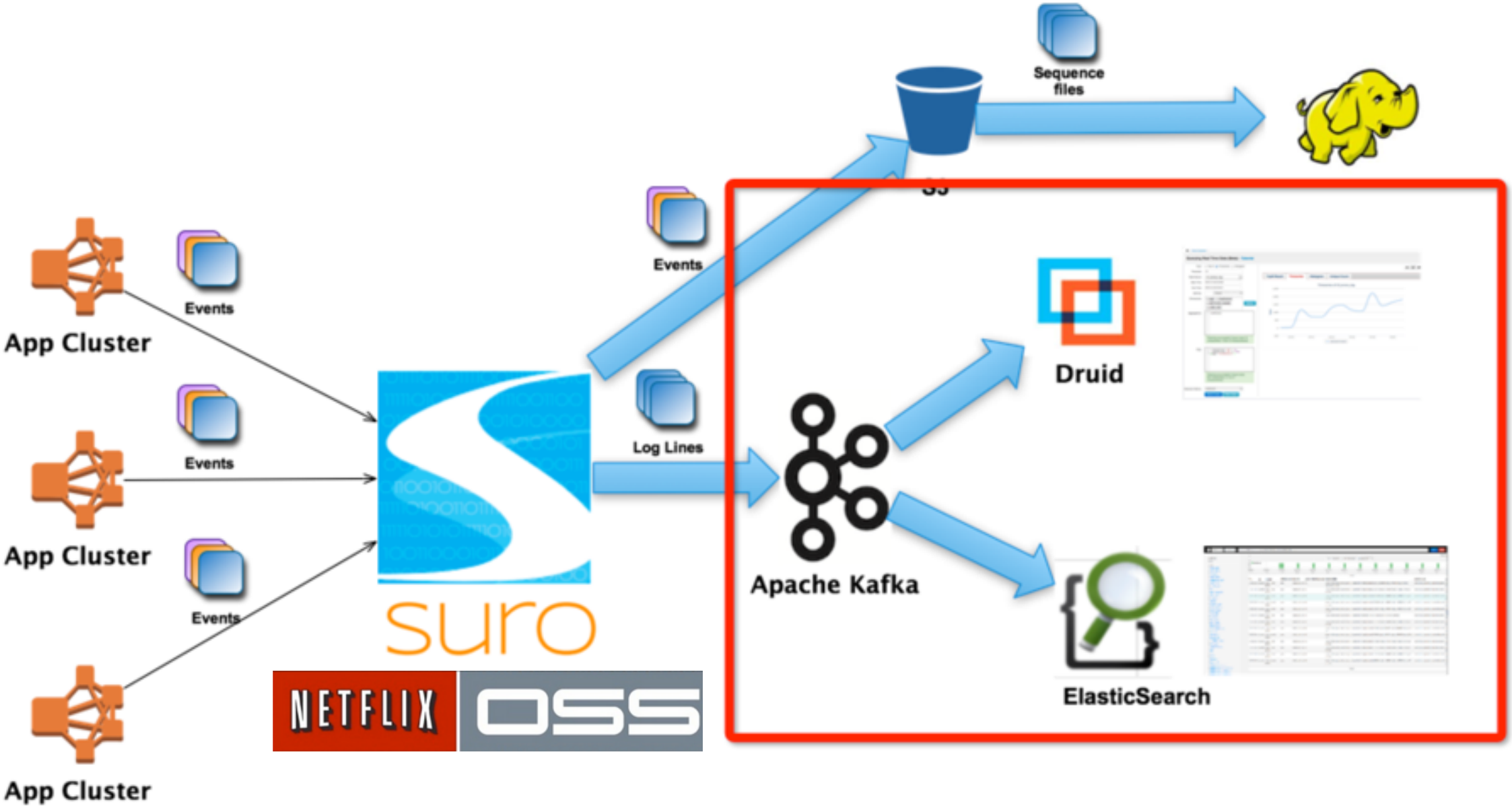
- Quickly locates the right log events

- Minimal programming effort

It’s All about Extracting Small Data Out of Big Data


Sequence files
S3
Events
Events
App Cluster
Events
App Cluster
Events
App Cluster
suro

NETFLIX OSS


Sequence files
Events
Events
Druid
App Cluster
Events
Log Lines
Apache Kafka
App Cluster
Events
suro
ElasticSearch
NETFLIX
OSS
App Cluster


NETFLIX®

Now Back to the Use Case

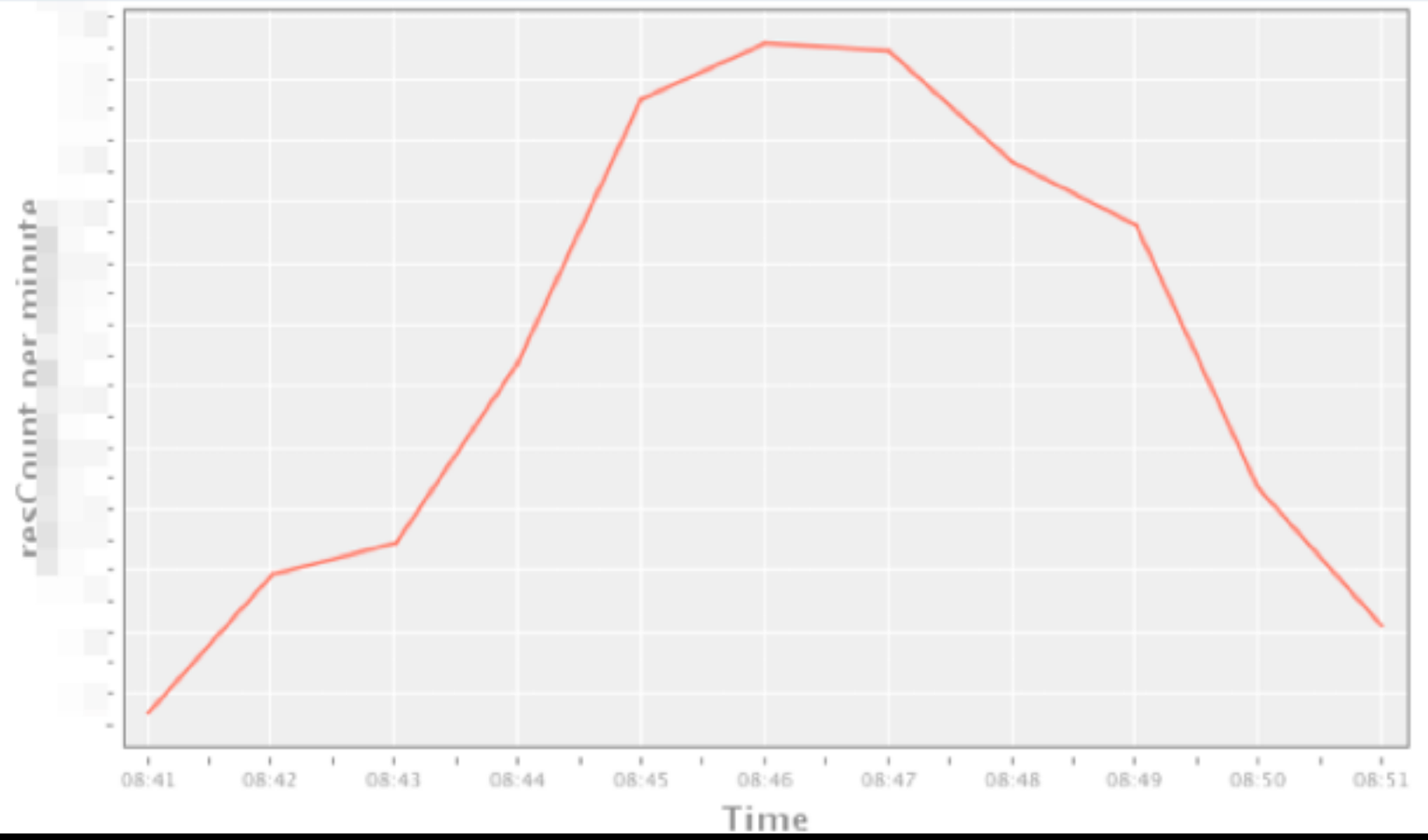
Intelligent Alerts

Investigate the Errors	**Start with finding potential outliers among cluster instances:** Top 10 Errors grouped by Application, Logging Class, Host Name, and Line Number Log Summary Doc **You should also check out dominant errors:** 1. Find dominant errors by removing "hostname" from Dimensions box, and click on the button "Submit Query" below. You' 2. Click on any text in the error table cell (they are links), and you'll see error details

Details of Error Surge

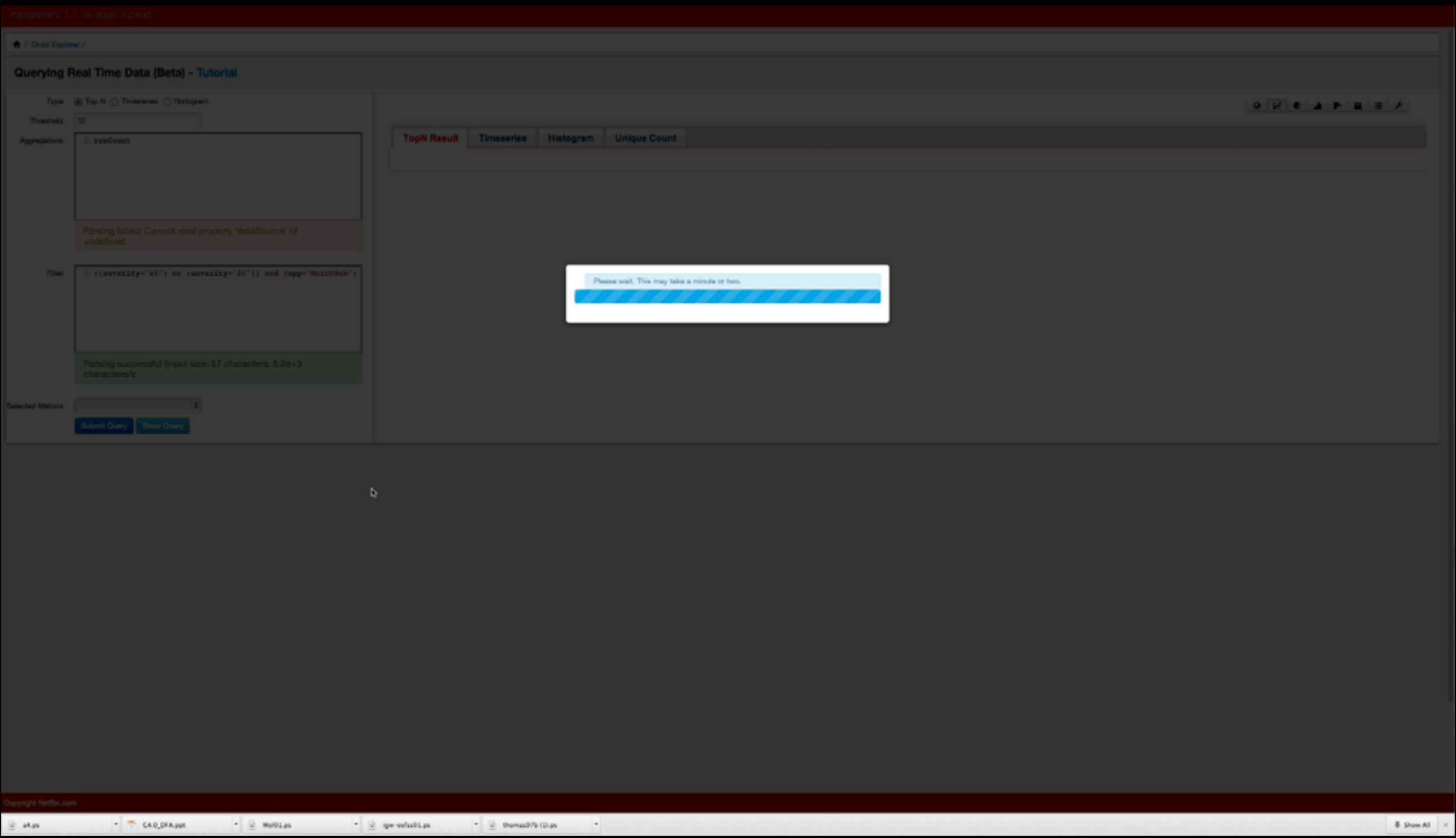
Contacts	Contacts
About Automated Log Summary Alerts	Log Summary Documentation About Automated Alerts
NAC	RECS_PRECOMPUTE
Trend Explorer	Error Trend that Caused This Alert (RTExplorer's Documentation)

Trigger Graph



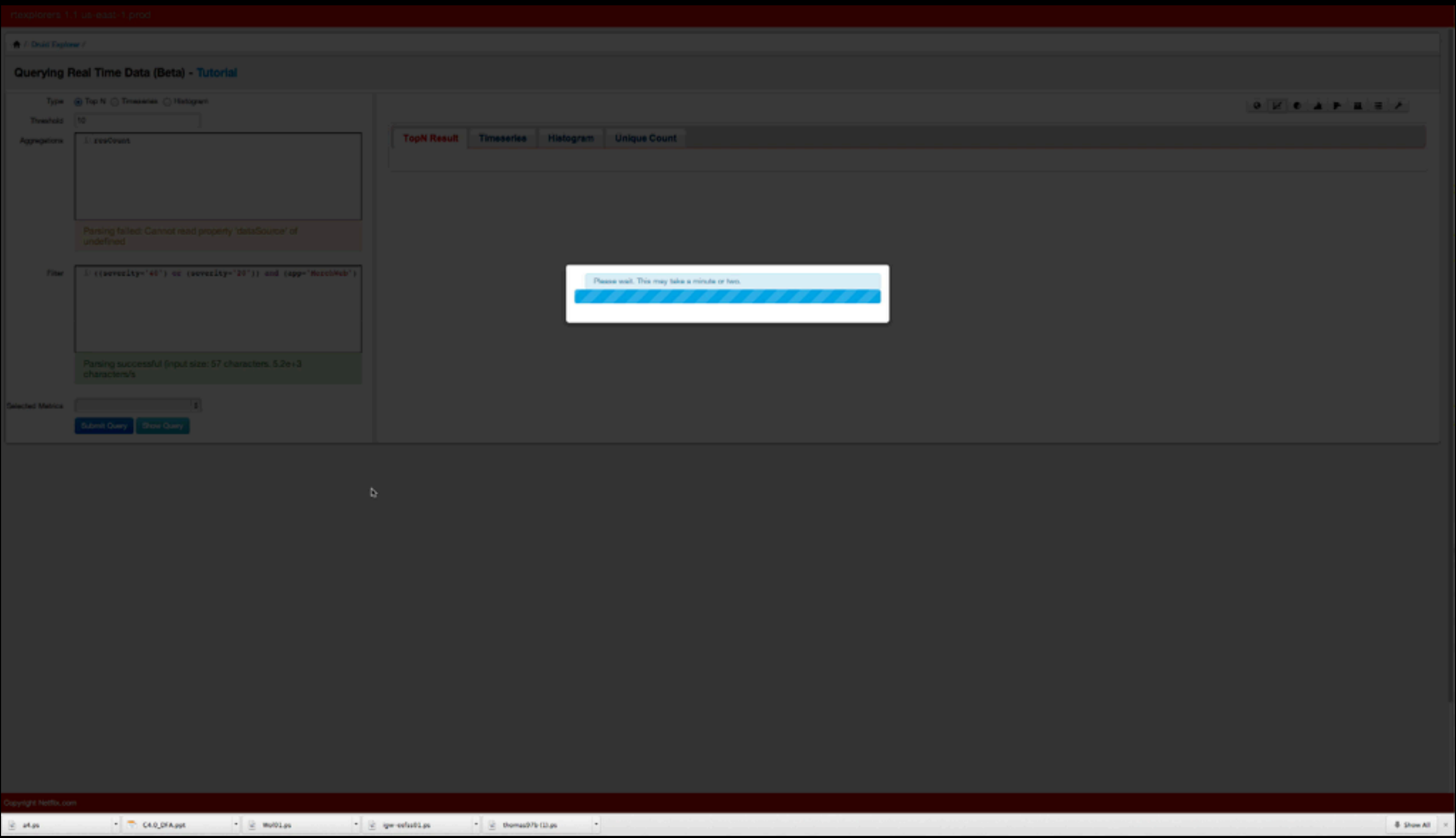
NETFLIX®

Guided Debugging in the Right Context



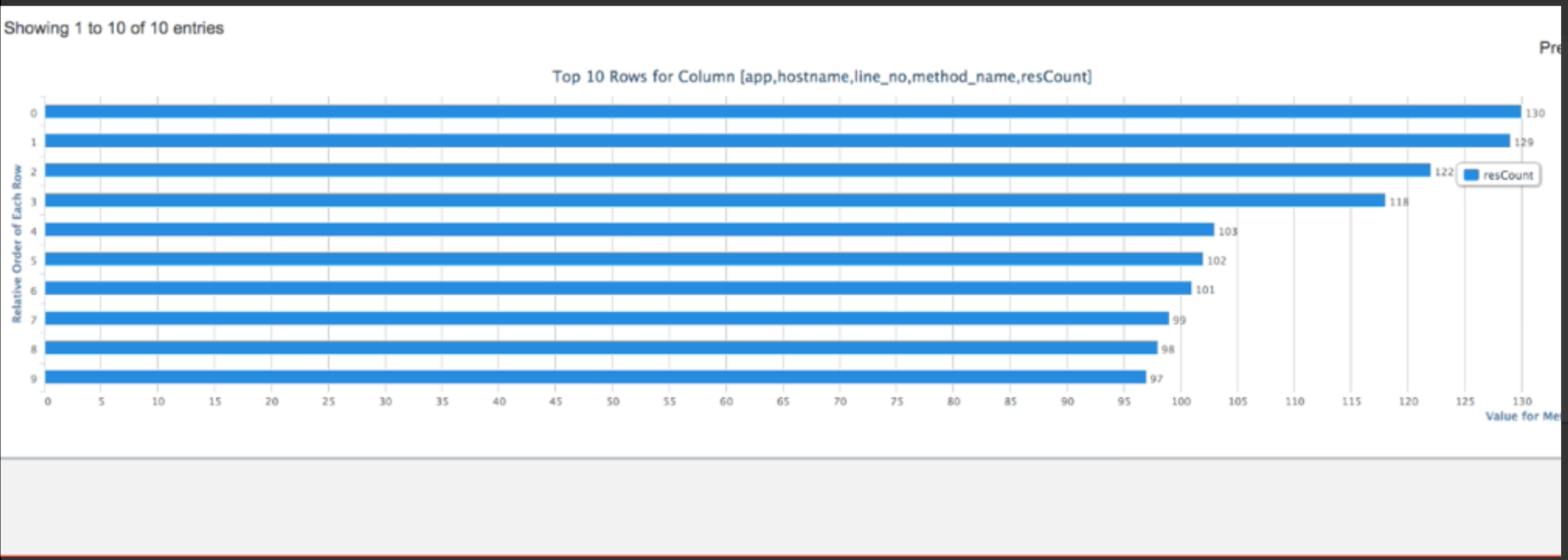
NETFLIX®

Guided Debugging in the Right Context



NETFLIX®

Guided Debugging in the Right Context



Guided Debugging in the Right Context

rtexplorers 1.1 us-east-1.prod

/ Druid Explorer /

Querying Real Time Data (Beta) - Tutorial

Type: (•) Top N ( ) Timeseries ( ) Histogram

Threshold: 10

Data Source: nf_errors_log

Start Time: 2013-09-04 12:59

End Time: 2013-09-04 13:11

Shift By: Day(s)

Dimensions: × app × hostname × METHOD_NAME × LINE_NO — Metrics

Aggregations:
```
1 resCount
```
Parsing successful (input size: 8 characters. 2.7e+3 characters/s)

Filter:
```
1 ((severity='40') or (severity='20')) and (app='MerchWeb')
```
Parsing successful (input size: 57 characters. 2.8e+4 characters/s

Selected Metrics: resCount

Submit Query | Show Query

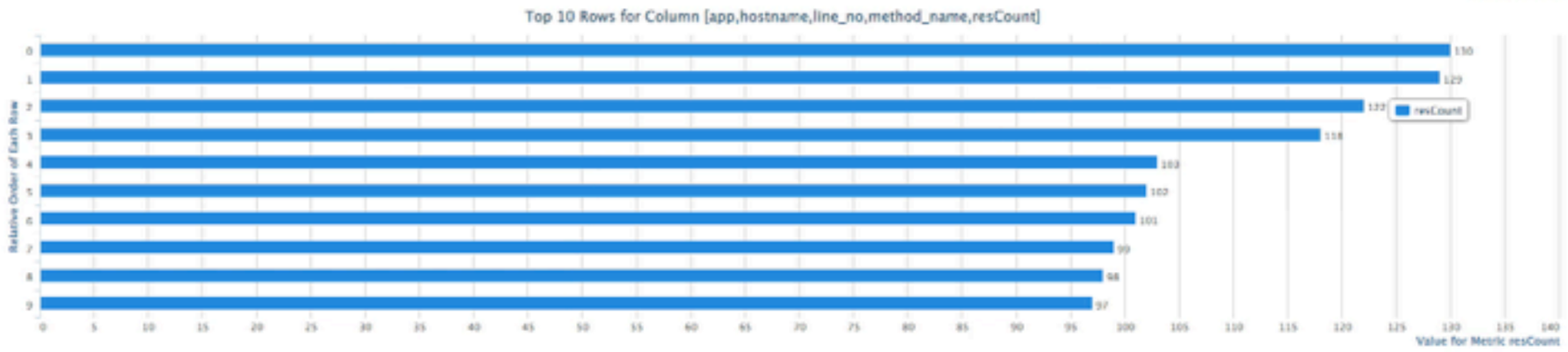
TopN Result | Timeseries | Histogram | Unique Count

Show 10 entries

app	hostname	line_no	method_name	resCount	Time
MerchWeb	merchweb-usca-live-i-801523ee	317	executeWithResponse	130	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-961523f8	317	executeWithResponse	129	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-801523ee	164	getProfiles	122	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-961523f8	164	getProfiles	118	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-1ae7137d	291	getNavigationItemsFromMap	103	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-9c1523f2	317	executeWithResponse	102	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-8a1523e4	291	getNavigationItemsFromMap	101	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-801523ee	291	getNavigationItemsFromMap	99	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-8a1523e4	317	executeWithResponse	98	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-9c1523f2	164	getProfiles	97	2013-09-04T19:59:00/2013-09-04T20:12:00

Showing 1 to 10 of 10 entries

Previous Next



NETFLIX

Guided Debugging in the Right Context

rtexplorers 1.1 us-east-1.prod

/ Druid Explorer /

Querying Real Time Data (Beta) - Tutorial

Type: (•) Top N ( ) Timeseries ( ) Histogram

Threshold: 10

Data Source: nf_errors_log

Start Time: 2013-09-04 12:59

End Time: 2013-09-04 13:11

Shift By: Day(s)

Dimensions: × app × hostname × METHOD_NAME × LINE_NO — Metrics

Aggregations:
```
1 resCount
```
Parsing successful (input size: 8 characters. 2.7e+3 characters/s)

Filter:
```
1 ((severity='40') or (severity='20')) and (app='MerchWeb')
```
Parsing successful (input size: 57 characters. 2.8e+4 characters/s

Selected Metrics: resCount

Submit Query | Show Query

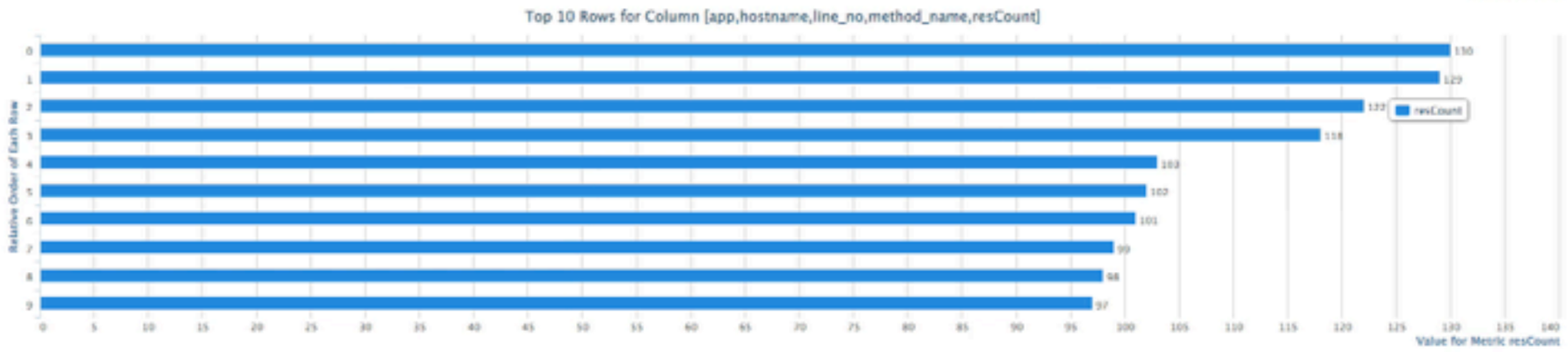
TopN Result | Timeseries | Histogram | Unique Count

Show 10 entries

app	hostname	line_no	method_name	resCount	Time
MerchWeb	merchweb-usca-live-i-801523ee	317	executeWithResponse	130	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-961523f8	317	executeWithResponse	129	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-801523ee	164	getProfiles	122	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-961523f8	164	getProfiles	118	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-1ae7137d	291	getNavigationItemsFromMap	103	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-9c1523f2	317	executeWithResponse	102	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-8a1523e4	291	getNavigationItemsFromMap	101	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-801523ee	291	getNavigationItemsFromMap	99	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-8a1523e4	317	executeWithResponse	98	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	merchweb-usca-live-i-9c1523f2	164	getProfiles	97	2013-09-04T19:59:00/2013-09-04T20:12:00

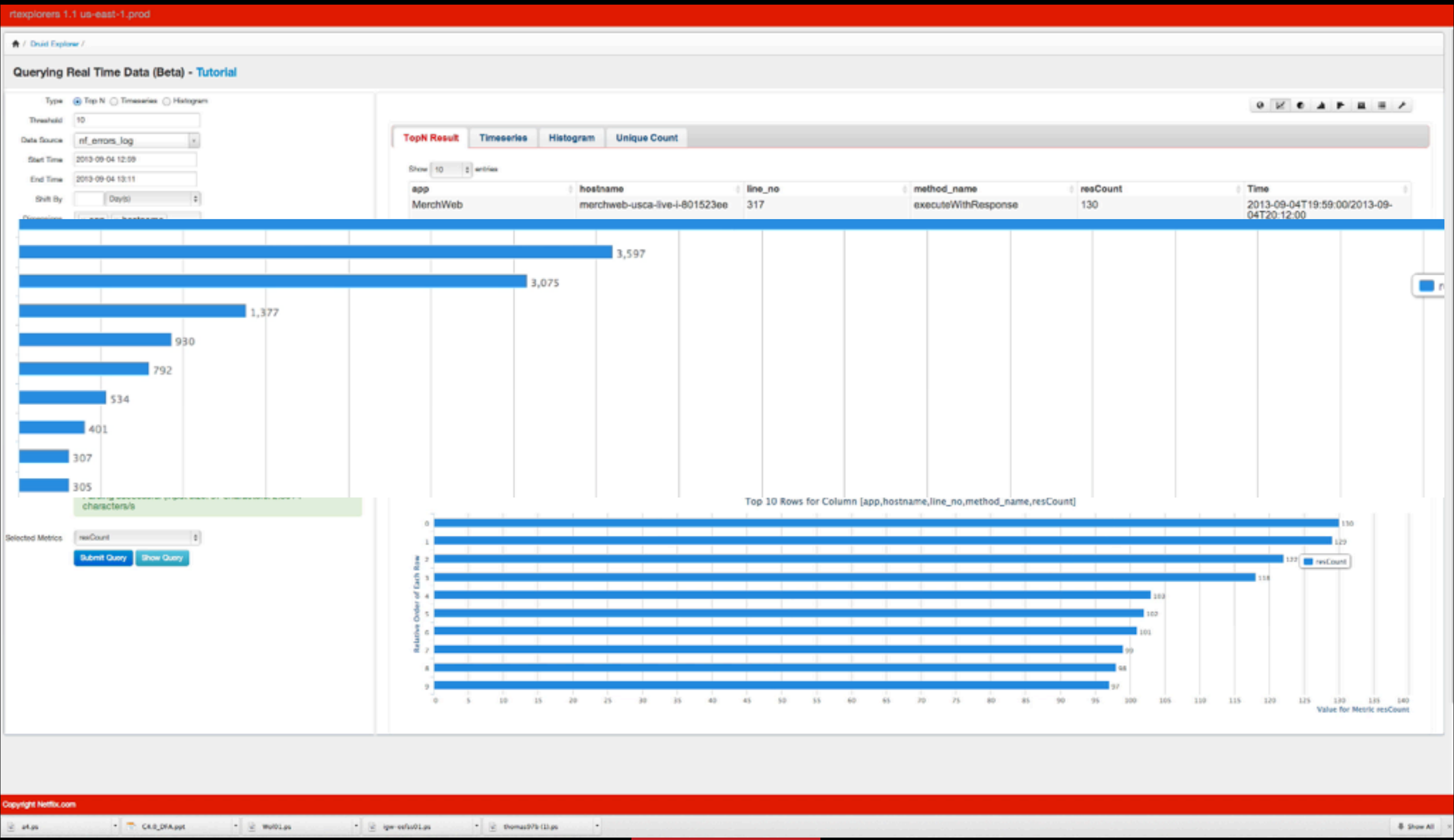
Showing 1 to 10 of 10 entries

Previous Next



NETFLIX

Guided Debugging in the Right Context



NETFLIX®

Guided Debugging in the Right Context

rtexplorers 1.1 us-east-1.prod

/ Druid Explorer /

Querying Real Time Data (Beta) - Tutorial

Type: (•) Top N ( ) Timeseries ( ) Histogram

Threshold: 10

Data Source: nf_errors_log

Start Time: 2013-09-04 12:59

End Time: 2013-09-04 13:11

Shift By: Day(s)

Dimensions: × app × METHOD_NAME × LINE_NO — Metrics

Aggregations:
```
1 resCount
```
Parsing successful (input size: 8 characters. 2.7e+3 characters/s)

Filter:
```
1 ((severity='40') or (severity='20')) and (app='MerchWeb')
```
Parsing successful (input size: 57 characters. 2.8e+4 characters/s

Selected Metrics: resCount

Submit Query | Show Query

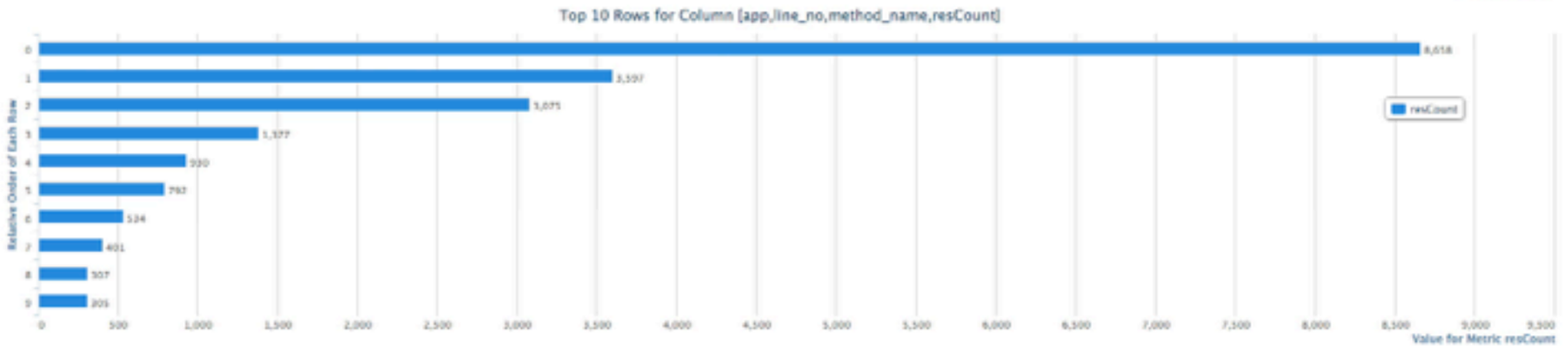
TopN Result | Timeseries | Histogram | Unique Count

Show 10 entries

app	line_no	method_name	resCount	Time
MerchWeb	291	getNavigationItemsFromMap	8658	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	317	executeWithResponse	3597	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	164	getProfiles	3075	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	79	log	1377	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	488	setIdentityGracePeriod	930	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	284	_getVideoSimilars	792	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	339	run	534	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	631	run	401	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	71	run	307	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	63	getVideoHistoryItems	305	2013-09-04T19:59:00/2013-09-04T20:12:00

Showing 1 to 10 of 10 entries

Previous Next



NETFLIX®

Guided Debugging in the Right Context

rtexplorers 1.1 us-east-1.prod

/ Druid Explorer /

Querying Real Time Data (Beta) - Tutorial

Type: (•) Top N ( ) Timeseries ( ) Histogram

Threshold: 10

Data Source: nf_errors_log

Start Time: 2013-09-04 12:59

End Time: 2013-09-04 13:11

Shift By: Day(s)

Dimensions: × app × METHOD_NAME × LINE_NO — Metrics

Aggregations:
```
1 resCount
```
Parsing successful (input size: 8 characters. 2.7e+3 characters/s)

Filter:
```
1 ((severity='40') or (severity='20')) and (app='MerchWeb')
```
Parsing successful (input size: 57 characters. 2.8e+4 characters/s

Selected Metrics: resCount

Submit Query | Show Query

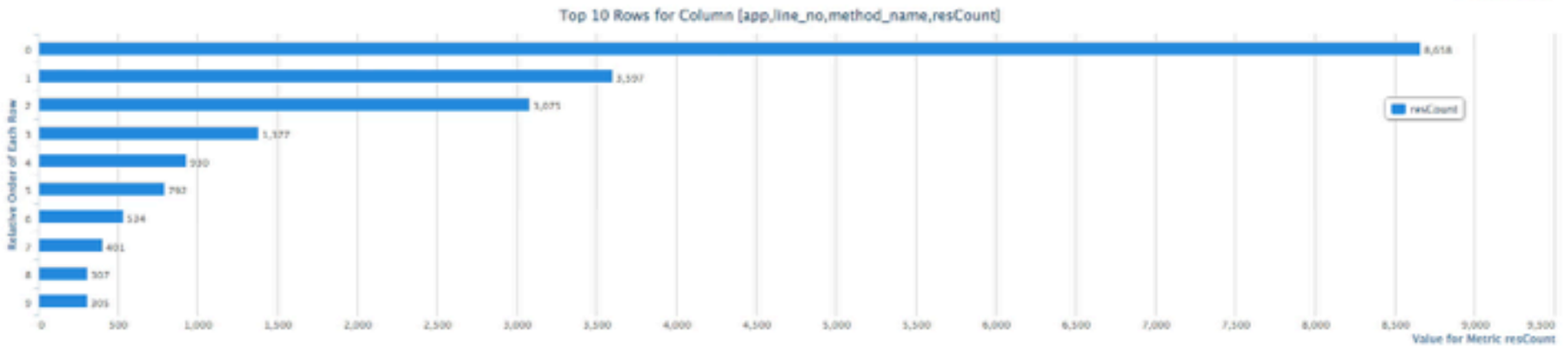
TopN Result | Timeseries | Histogram | Unique Count

Show 10 entries

app	line_no	method_name	resCount	Time
MerchWeb	291	getNavigationItemsFromMap	8658	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	317	executeWithResponse	3597	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	164	getProfiles	3075	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	79	log	1377	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	488	setIdentityGracePeriod	930	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	284	_getVideoSimilars	792	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	339	run	534	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	631	run	401	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	71	run	307	2013-09-04T19:59:00/2013-09-04T20:12:00
MerchWeb	63	getVideoHistoryItems	305	2013-09-04T19:59:00/2013-09-04T20:12:00

Showing 1 to 10 of 10 entries

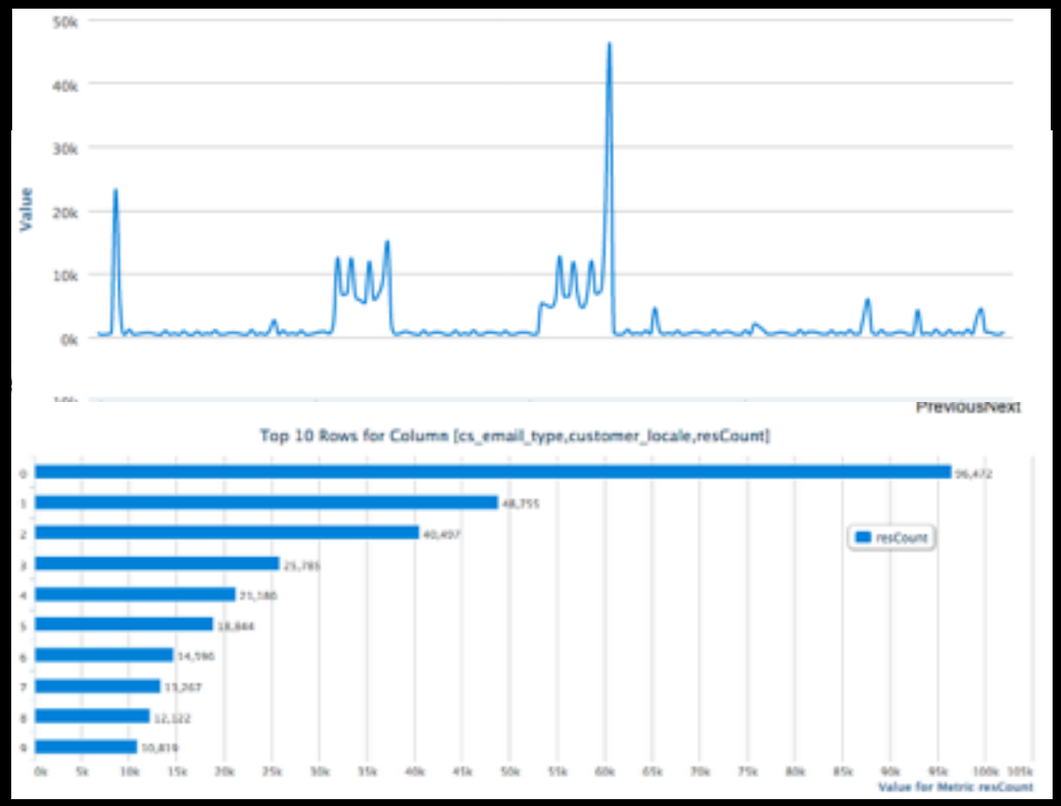
Previous Next

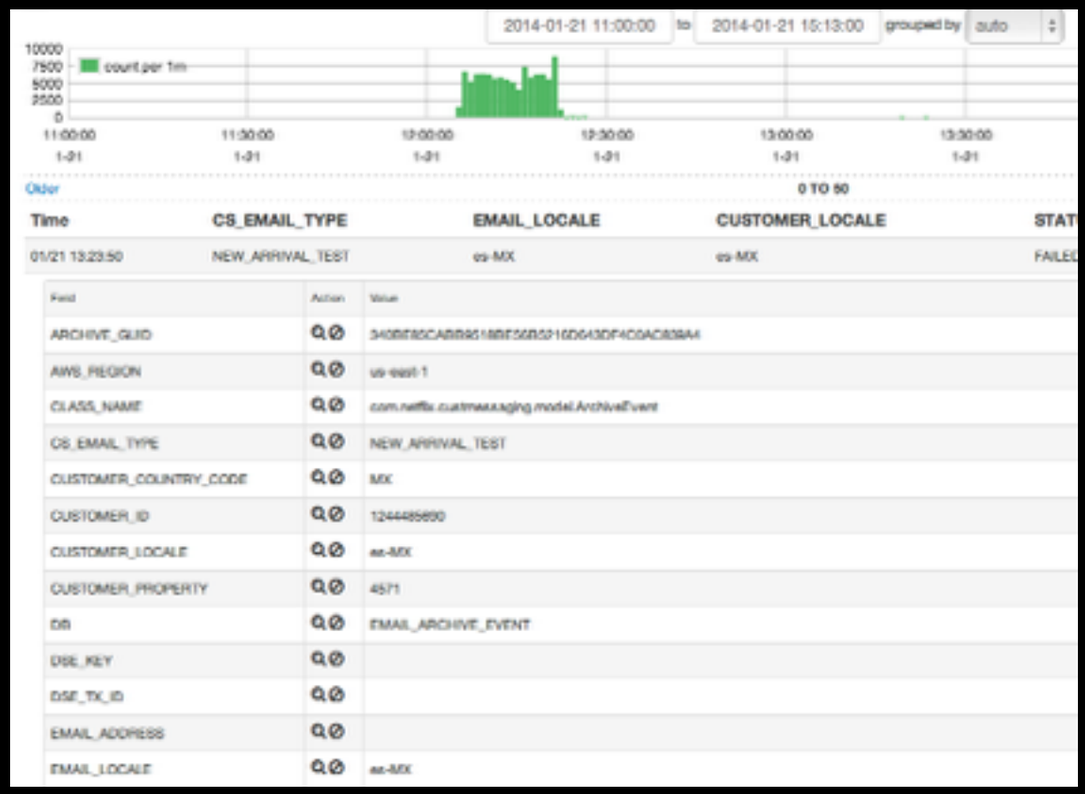


NETFLIX®

A Useful Pattern

Aggregated Query -> Individual Query





NETFLIX®

Examples

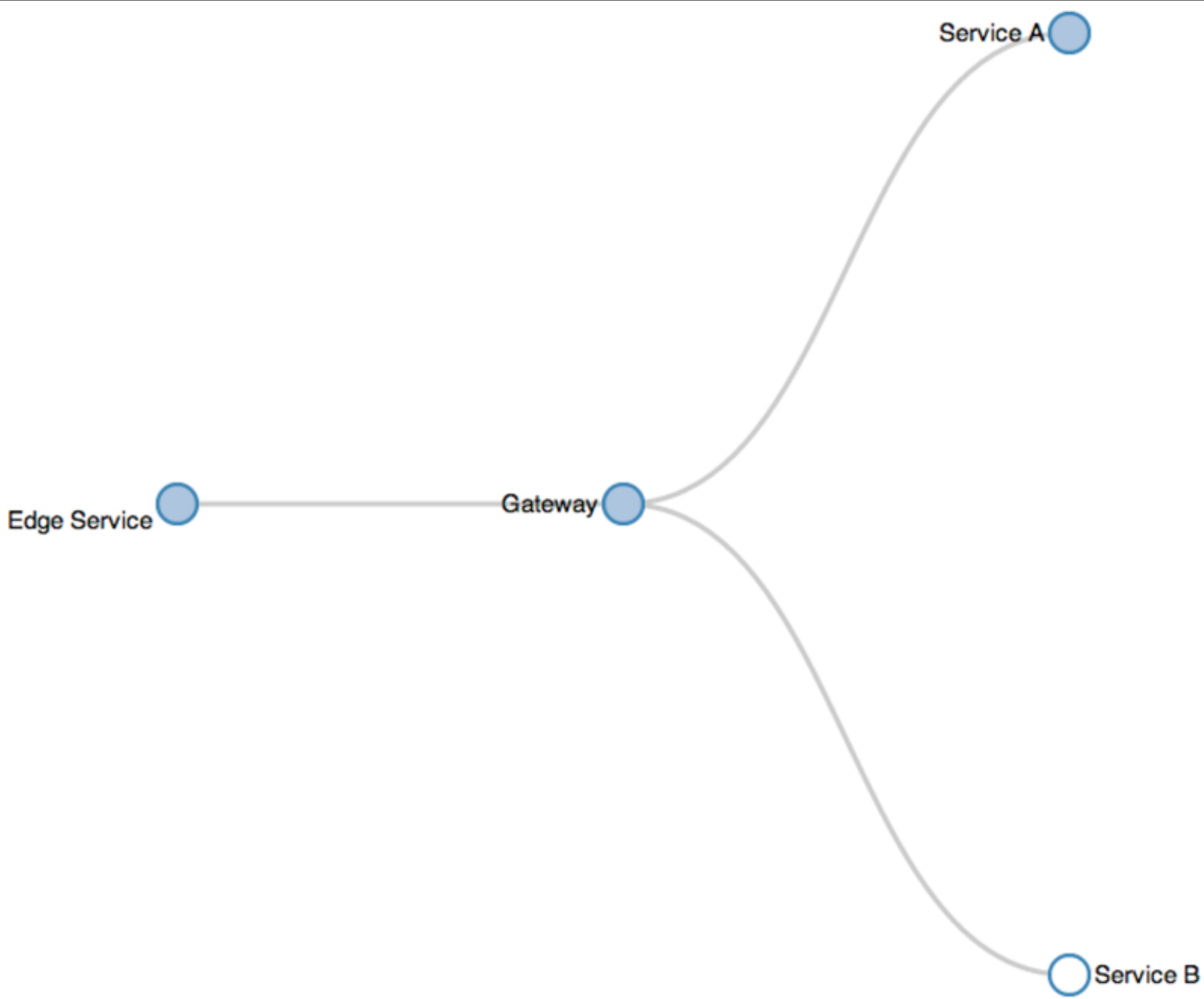
- S3 diagnostics

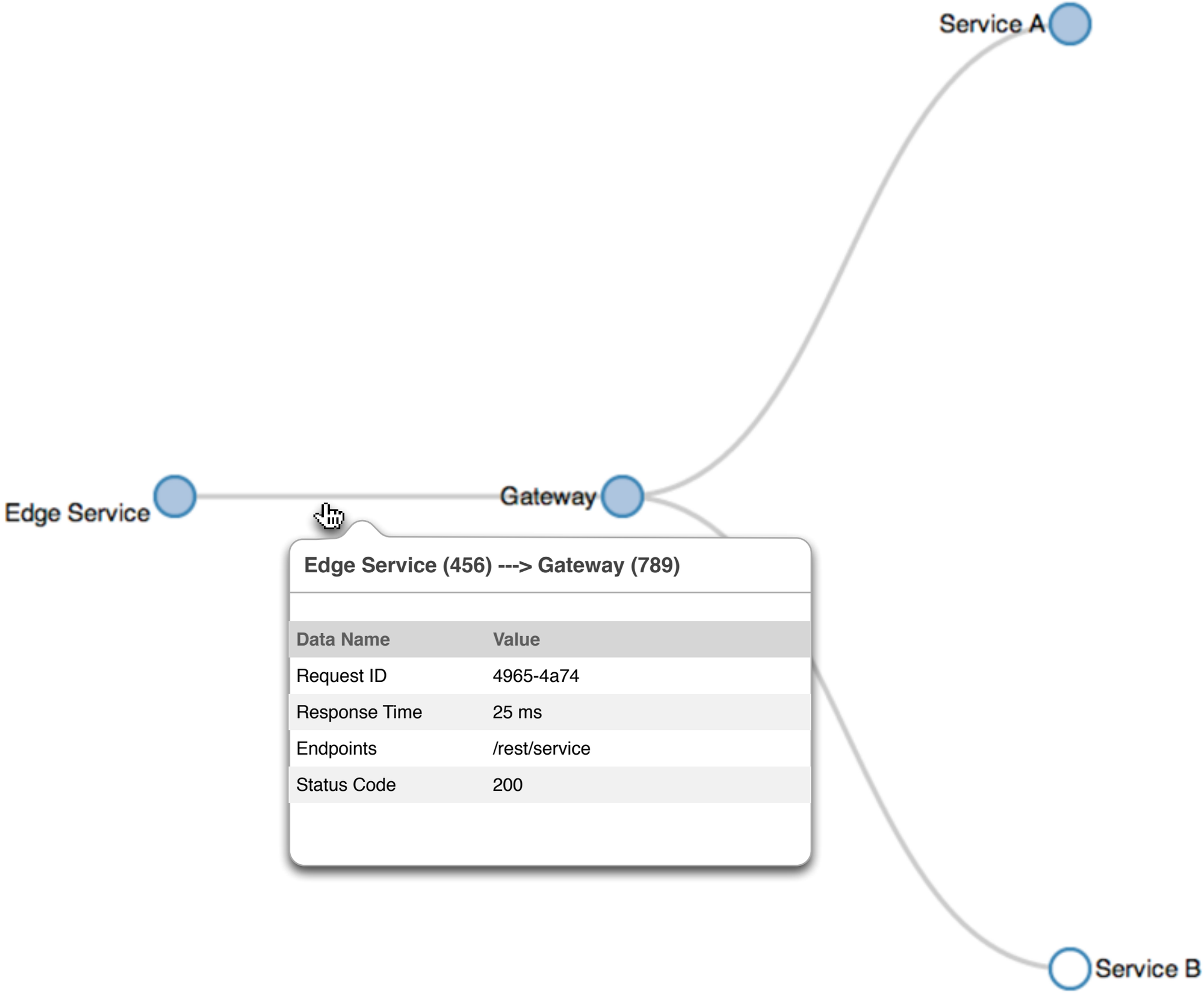
- Tracking email campaigns

- Request traces

Status:200

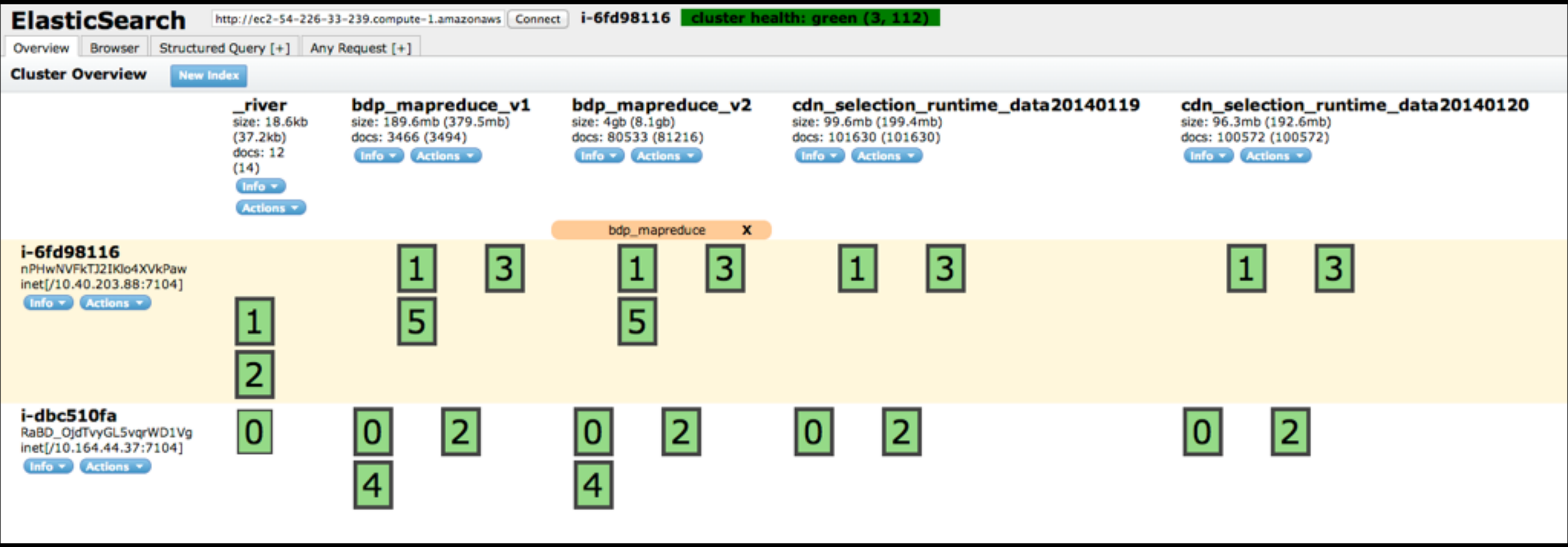
RequestId	Parent Id	Node Id	Service Name	Status
4965-4a74	0	123	Edge Service	200
4965-4a74	123	456	Gateway	200
4965-4a74	456	789	Service A	200
4965-4a74e	456	abc	Service B	200


Service A
Edge Service
Gateway
Service B


Service A
Edge Service
Gateway
Edge Service (456) ---> Gateway (789)
Data Name
Value
Request ID
4965-4a74
Response Time
25 ms
Endpoints
/rest/service
Status Code
200
Service B

Why Elasticsearch?

Automatic Sharding and Replication



NETFLIX®


NETFLIX®

Flexible Schema

Flexible Schema

- Schemaless

Flexible Schema

- Schemaless
- Reasonable defaults


NETFLIX®

Nice Extension Model

Nice Extension Model

- Customizable REST Actions

Nice Extension Model

- Customizable REST Actions
- Site Plugins

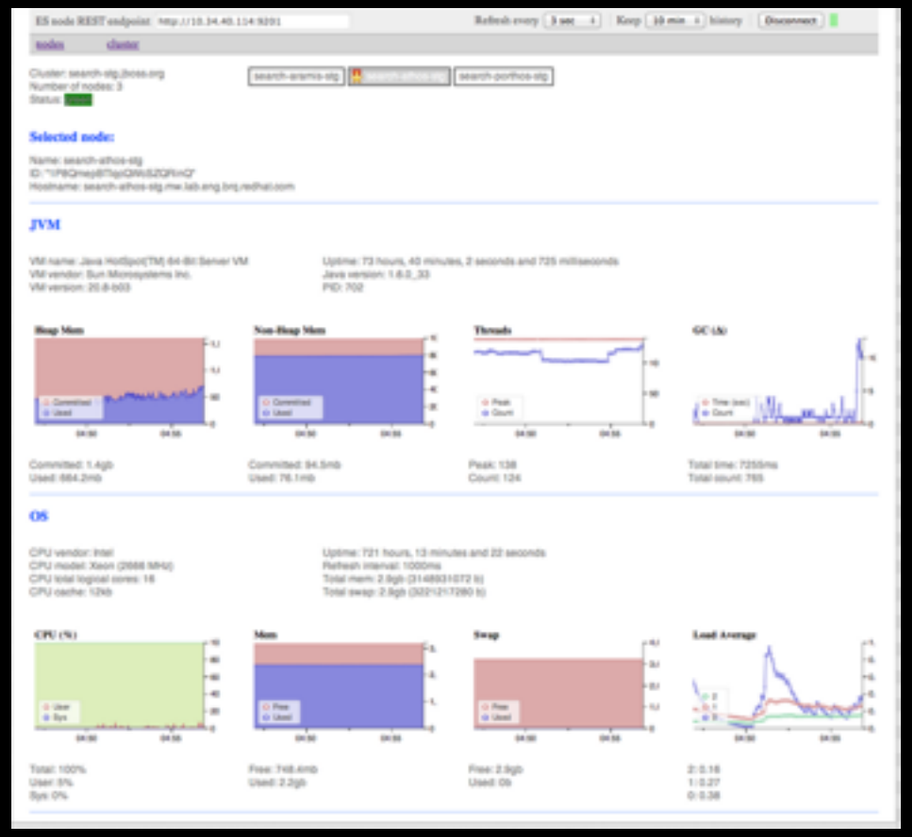
Nice Extension Model

- Customizable REST Actions
- Site Plugins
- River Plugins

Nice Extension Model

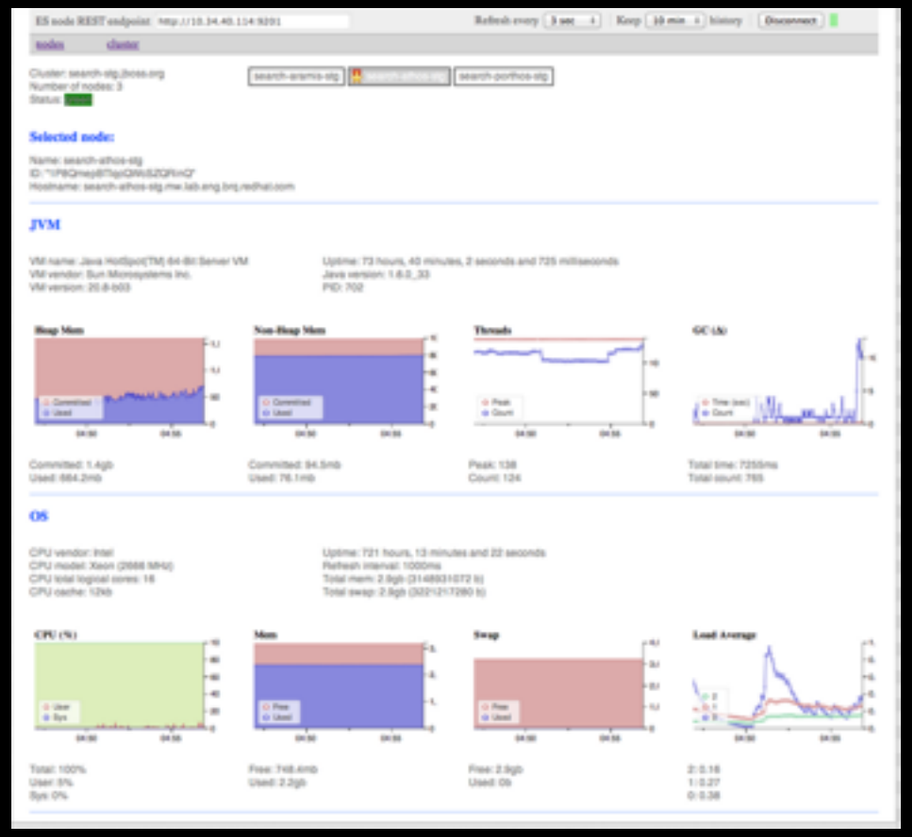
- Customizable REST Actions
- Site Plugins
- River Plugins
- Discovery Module


Logstash Search
Query Alias
Images
Search
php
png OR gif
css
Zoom Out
Chart
Terms
Term
Count
Action
id 1856
br 1567
pk 1437
ng 1207
bd 1172
ru 1078
jp 959
mx 678
Missing field 9818
Other values 20582
time must
field : @timestamp
from : "2013-07-24T21:13:04.743Z"
to : "2013-07-26T21:13:04.743Z"
terms must not
field : country
value : cn
Toggle
value : us


ES node REST endpoint:
nodes
cluster
Selected node:
JVM
OS
CPU (%)
Mem
Swap
Load Average

NETFLIX®

Ecosystem - Plugins, Kibana



NETFLIX®

Tracking Service Deployments

NETFLIX OSS

{ edda }

NETFLIX®

NETFLIX®

Built by Netflix Monitoring Eng Team

NETFLIX®

Built by Netflix Monitoring Eng Team

Tracks History and Changes to Service Deployments

NETFLIX®

Built by Netflix Monitoring Eng Team

Tracks History and Changes to Service Deployments

Keeps Many Revisions

NETFLIX®

Built by Netflix Monitoring Eng Team

Tracks History and Changes to Service Deployments

Keeps Many Revisions

Tracks Dozens of Document Types

NETFLIX®

- Collection APIs
  - /aws
    - /aws/addresses
    - /aws/alarms
    - /aws/autoScalingGroups
    - /aws/buckets
    - /aws/databases
    - /aws/iamGroups
    - /aws/iamRoles
    - /aws/iamUsers
    - /aws/iamVirtualMFADevices
    - /aws/images
    - /aws/instances
    - /aws/launchConfigurations
    - /aws/loadBalancers
    - /aws/reservedInstances
    - /aws/scalingPolicies
    - /aws/securityGroups
    - /aws/snapshots
    - /aws/tags
    - /aws/volumes
  - /group
    - /group/autoScalingGroups
  - /view
    - /view/instances
    - /view/loadBalancerInstances
    - /view/simpleQueues

NETFLIX®

- Collection APIs
  - /aws
    - /aws/addresses
    - /aws/alarms
    - /aws/autoScalingGroups
    - /aws/buckets
    - /aws/databases
    - /aws/iamGroups
    - /aws/iamRoles
    - /aws/iamUsers
    - /aws/iamVirtualMFADevices
    - /aws/images
    - /aws/instances
    - /aws/launchConfigurations
    - /aws/loadBalancers
    - /aws/reservedInstances
    - /aws/scalingPolicies
    - /aws/securityGroups
    - /aws/snapshots
    - /aws/tags
    - /aws/volumes
  - /group
    - /group/autoScalingGroups
  - /view
    - /view/instances
    - /view/loadBalancerInstances
    - /view/simpleQueues

- General
  - Select Matrix Arguments
  - Modifier Matrix Arguments
    - _all
    - _at=<ms timestamp>
    - _callback=<name>
    - _diff[=<context>]
    - _expand
    - _limit=<num>
    - _live
    - _meta
    - _pp
    - _since=<ms timestamp>
    - _until=<ms timestamp>
    - _updated
  - Field Selectors

NETFLIX

Why Elasticsearch?


NETFLIX®

Schemas may change at any time

Schemas may change at any time

Go schemaless


NETFLIX®

Users may search for any combination of fields

NETFLIX®

Users may search for any combination of fields

This is what search engine is designed for


NETFLIX®

Users often needs only a few fields

Users often needs only a few fields

Projection via “fields” query


NETFLIX®

Need range queries on date and revisions

Need range queries on date and revisions

Natively supported by Elasticsearch

Need range queries on date and revisions

Natively supported by Elasticsearch

Route by document ID

Running ES in Netflix

Operational Challenges

Operational Challenges

Back pressure when indexing

Operational Challenges

Back pressure when indexing

Diverse configurations and data

Operational Challenges

Back pressure when indexing

Diverse configurations and data

Dynamic flow of log events

Operational Challenges

Back pressure when indexing

Diverse configurations and data

Dynamic flow of log events

Needs extensive monitoring and alerting

Operational Challenges

Back pressure when indexing

Diverse configurations and data

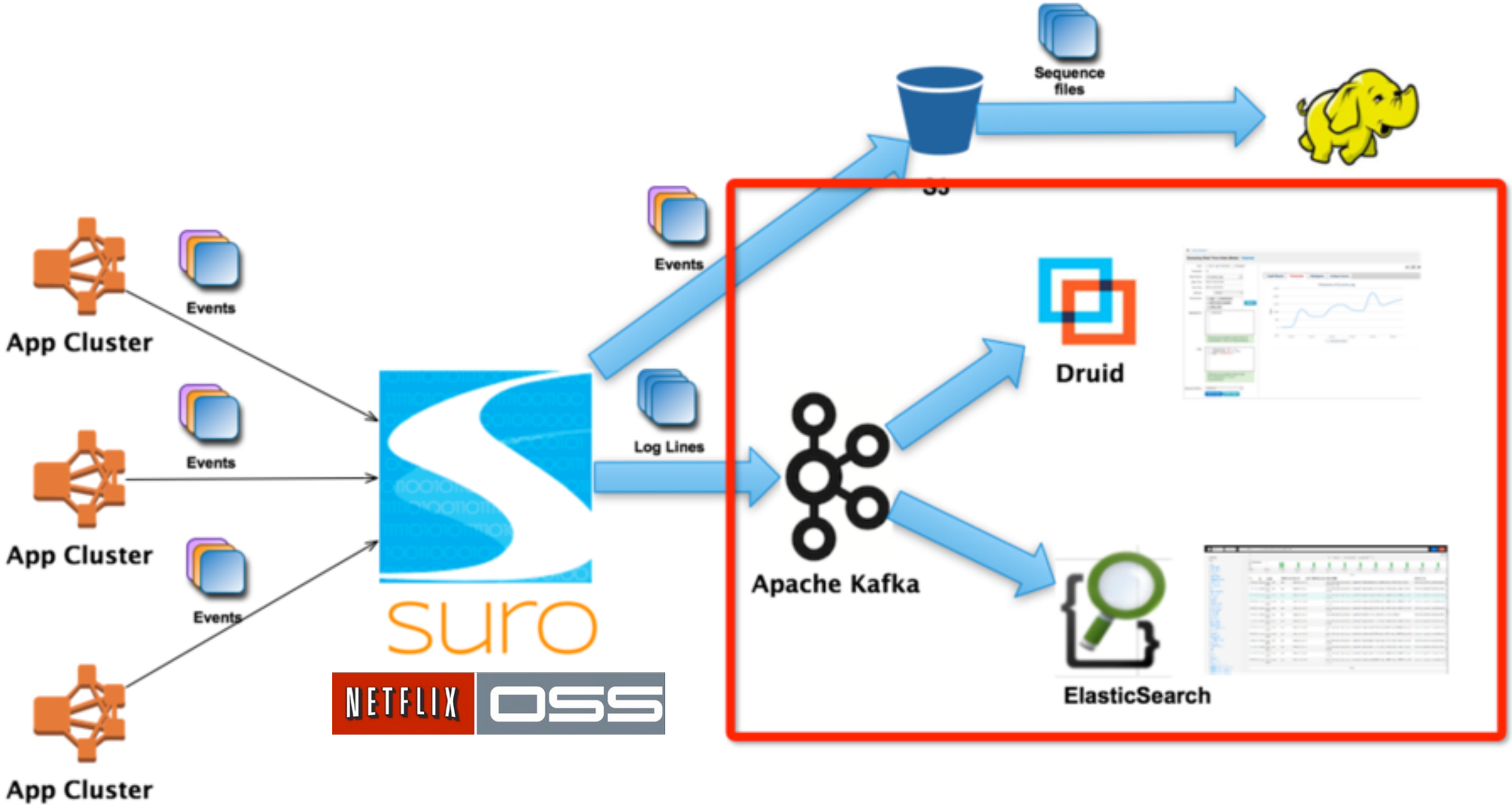
Dynamic flow of log events

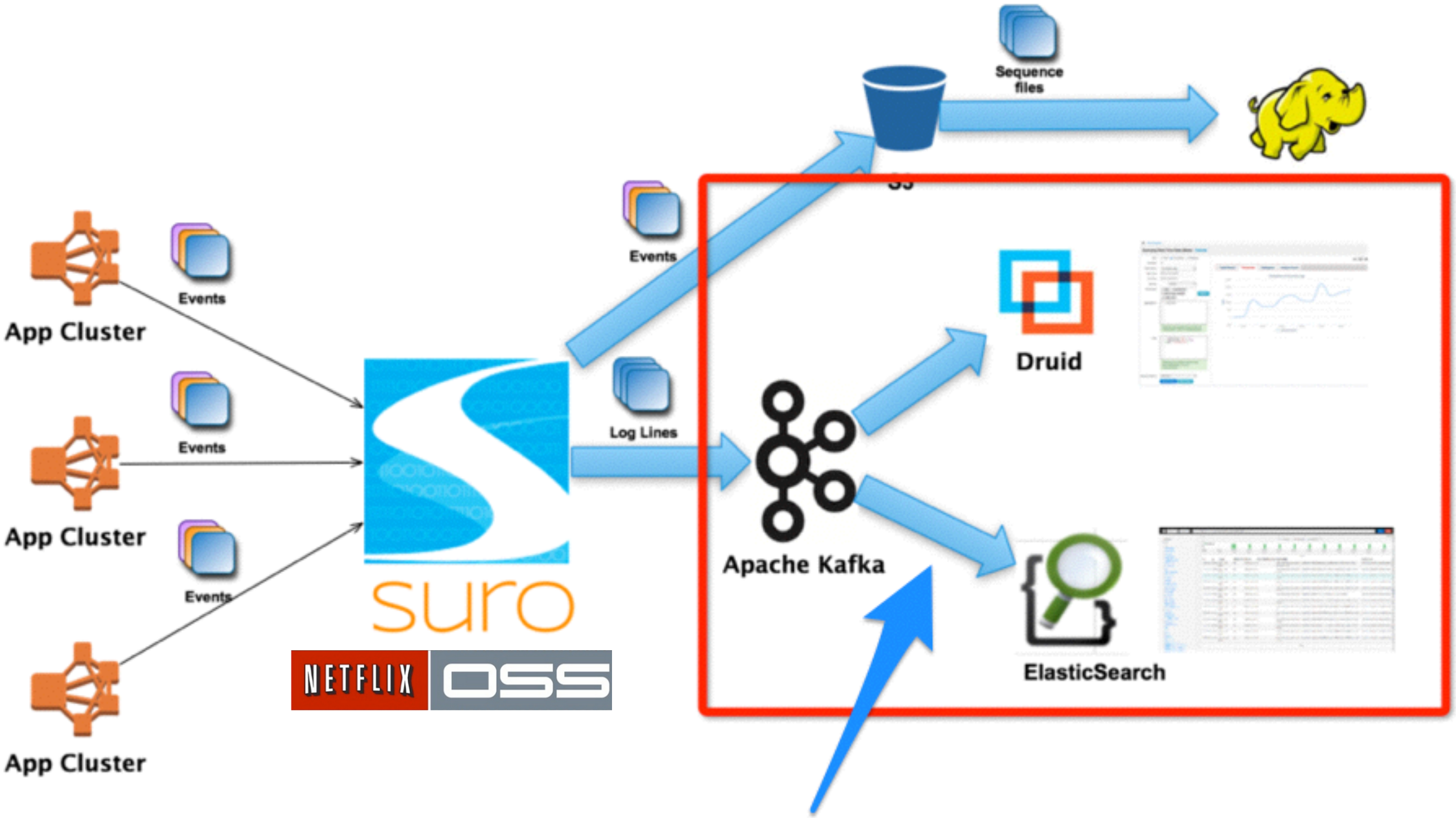
Needs extensive monitoring and alerting

Tolerating outage at different scales

Favor Pulling Over Pushing

NETFLIX®

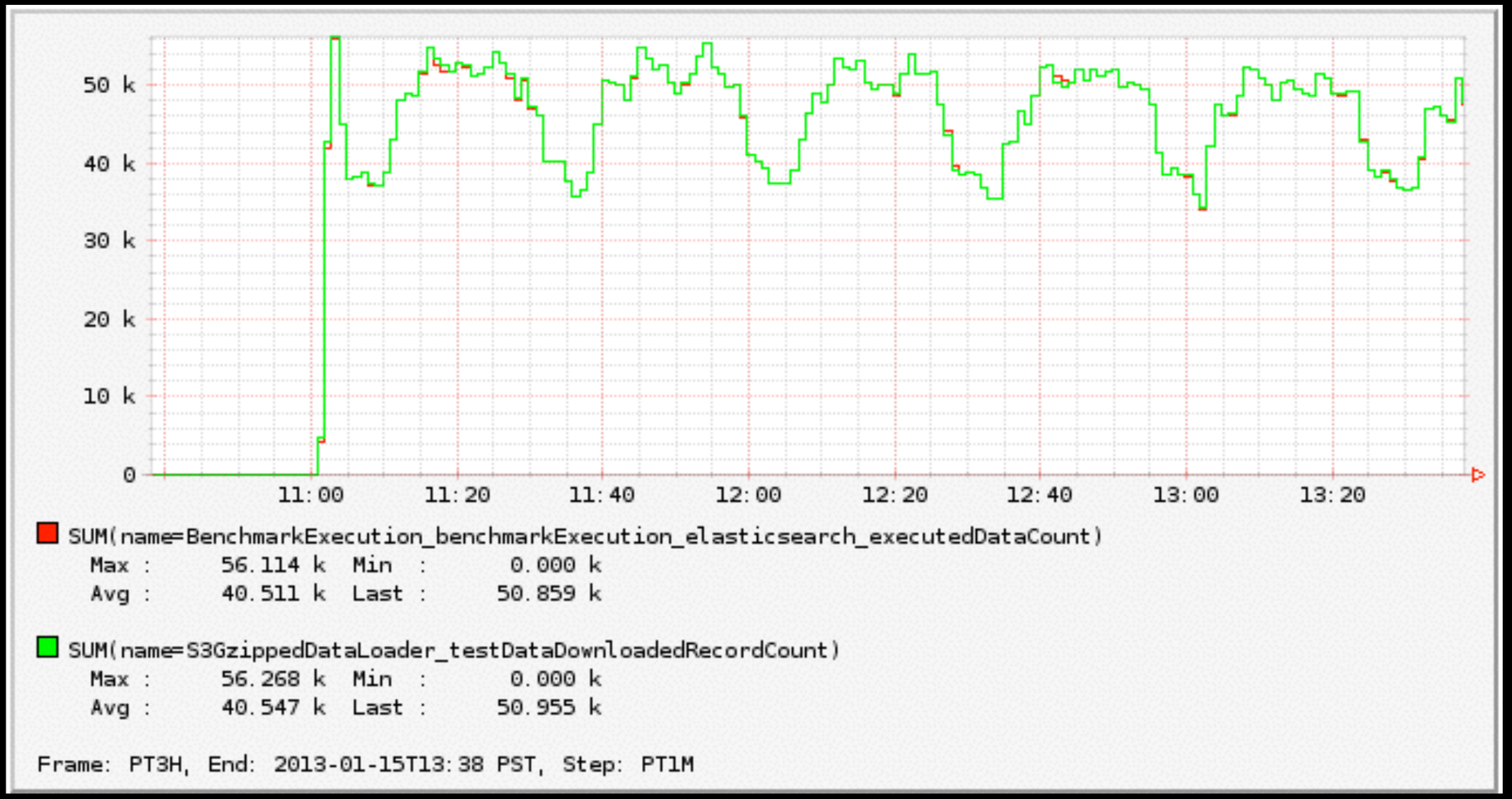

Sequence files
Events
Events
App Cluster
Events
Log Lines
Druid
Events
App Cluster
suro
Apache Kafka
Events
NETFLIX OSS
ElasticSearch
App Cluster



Elasticsearch Kafka River

NETFLIX®

Choose Config with Data


50 k
40 k
30 k
20 k
10 k
0
11:00
11:20
11:40
12:00
12:20
12:40
13:00
13:20
SUM(name=BenchmarkExecution_benchmarkExecution_elasticsearch_executedDataCount)
Max : 56.114 k Min : 0.000 k
Avg : 40.511 k Last : 50.859 k
SUM(name=S3GzippedDataLoader_testDataDownloadedRecordCount)
Max : 56.268 k Min : 0.000 k
Avg : 40.547 k Last : 50.955 k
Frame: PT3H, End: 2013-01-15T13:38 PST, Step: PT1M

NETFLIX®

Integrating ES

NETFLIX OSS

NETFLIX®

AMI for Deployment by Asgard

NETFLIX OSS

ASGARD prod us-east-1

Home | App | AMI | Cluster | ELB | EC2 | SDB | SNS | SQS | RDS | Task

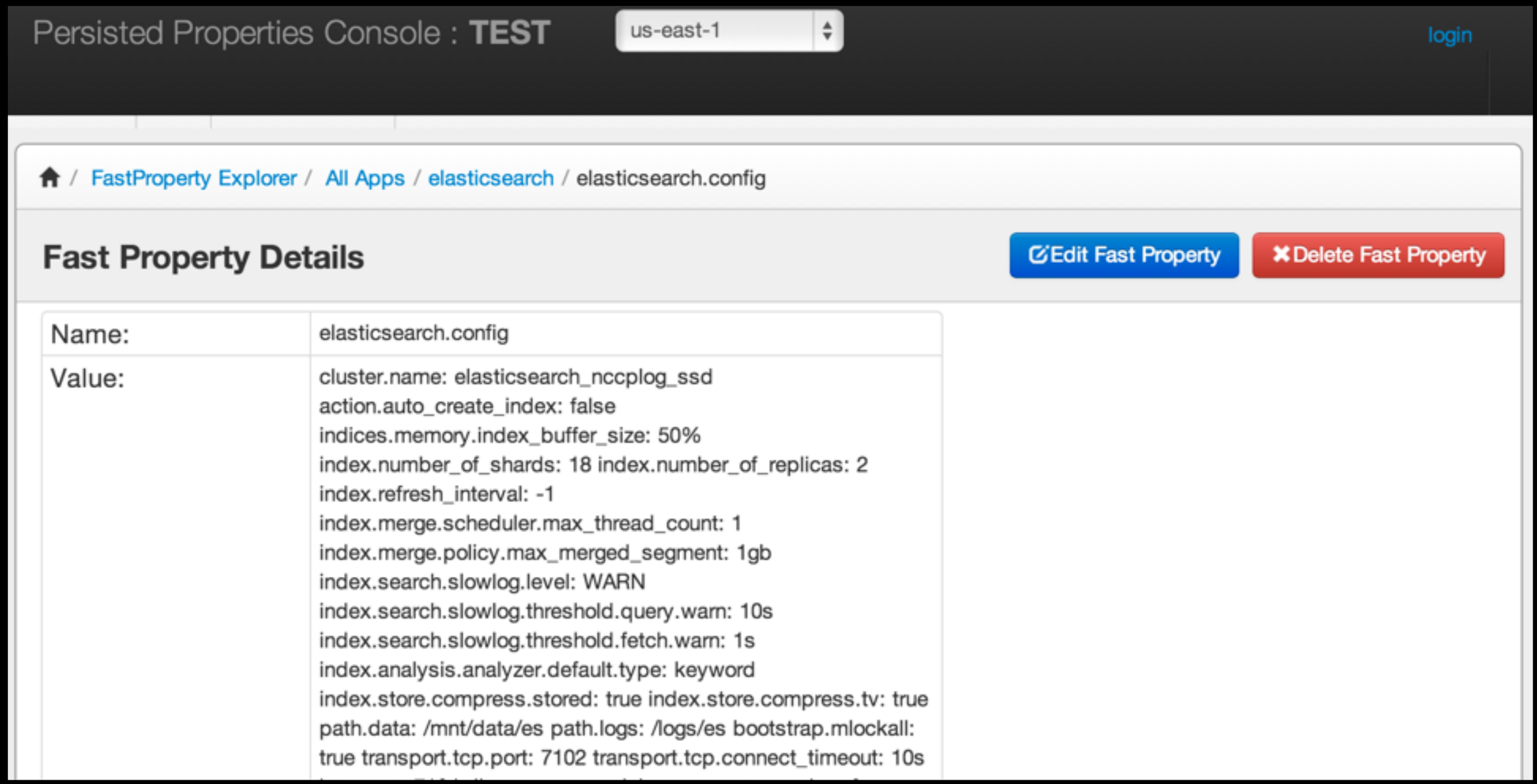
Images in us-east-1 (Virginia)

ID	Name	Description	State	Owner	Creator	Creation Time ▲	Last Used	Package Version
ami-2de3d344	nfelasticsearch-0.90.10-h9.e4350d2-x86_64-201401142121-centos-pv-ebs	name=nfelasticsearch, arch=x86_64, ancestor_name=centosbase-x86_64-201308302051-ebs, ancestor_id=ami-4d185424, ancestor_version=nflx-base-1.2.1-1942837.h806	available	test	jbae	2014-01-14 21:28:05 UTC	2014-01-21 12:01:20 PST	nfelasticsearch-0.90.10-h9.e4350d2/WE-APP-ElasticSearch-Kafka_0_7/9
ami-0720116e	nfelasticsearch-0.90.10-h4.e632b09-x86_64-201401110827-centos-pv-ebs	name=nfelasticsearch, arch=x86_64, ancestor_name=centosbase-x86_64-201308302051-ebs, ancestor_id=ami-4d185424, ancestor_version=nflx-base-1.2.1-1942837.h806	available	test	gmuthusamy	2014-01-11 08:33:32 UTC	2014-01-21 12:01:20 PST	nfelasticsearch-0.90.10-h4.e632b09/WE-APP-ElasticSearch-V0_90_10/4
ami-0330066a	nfelasticsearch-0.90.2-h3.34288b6-x86_64-201401081823-centos-pv-ebs	name=nfelasticsearch, arch=x86_64, ancestor_name=centosbase-x86_64-201308302051-ebs, ancestor_id=ami-4d185424, ancestor_version=nflx-base-1.2.1-1942837.h806	available	test	jbae	2014-01-08 18:27:17 UTC	2014-01-21 12:01:20 PST	nfelasticsearch-0.90.2-h3.34288b6/WE-APP-ElasticSearch-Cass/3
ami-31e3d458	nfelasticsearch-0.90.2-h2.ccbad33-x86_64-201401070019-centos-pv-ebs	name=nfelasticsearch, arch=x86_64, ancestor_name=centosbase-x86_64-201308302051-ebs, ancestor_id=ami-4d185424, ancestor_version=nflx-base-1.2.1-1942837.h806	available	test	jbae	2014-01-07 00:23:09 UTC	2014-01-16 00:01:22 PST	nfelasticsearch-0.90.2-h2.ccbad33/WE-APP-ElasticSearch-Cass/2

NETFLIX®

Archaius for Configuration

NETFLIX OSS



NETFLIX®

Eureka for Server Discovery

NETFLIX OSS

Instances

Total Instances: 3 | Run All Health Checks | Terminate Instances

Load Balancing: | Deregister Instances from ELBs | Register Instances with group's ELBs

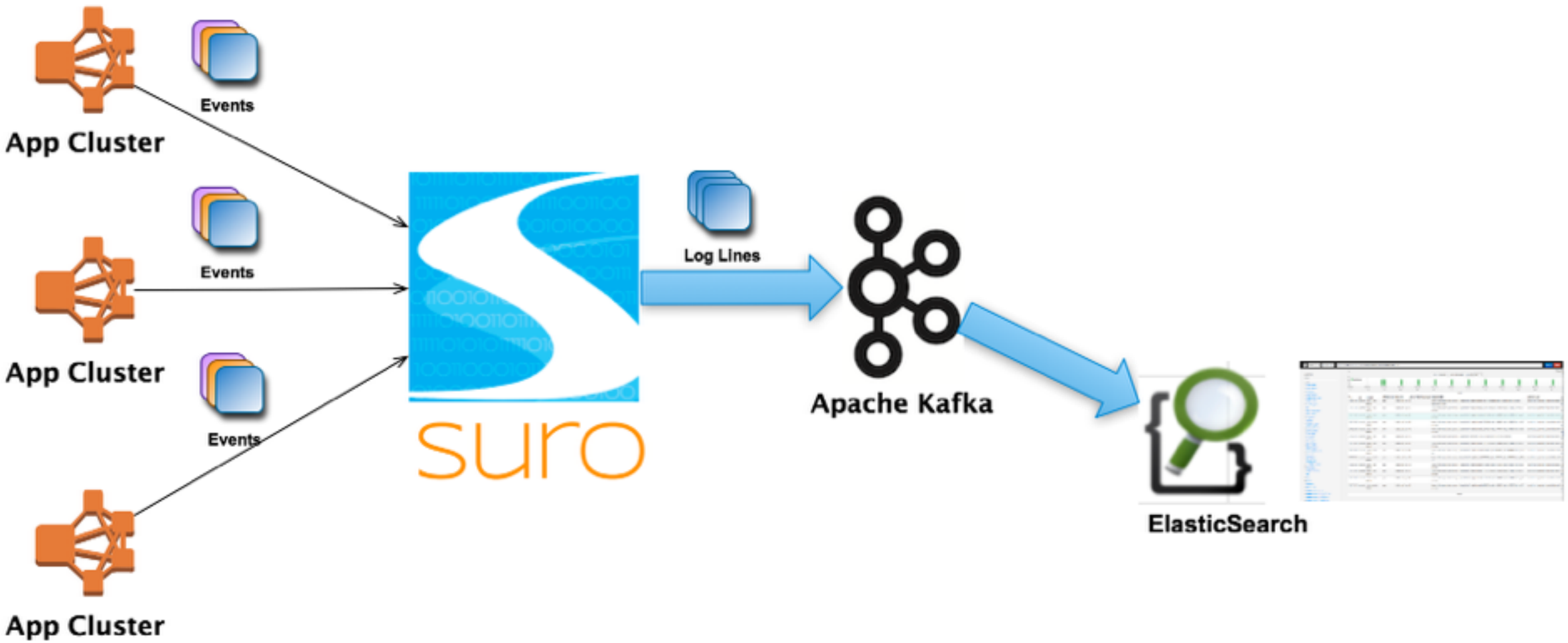
Eureka: | Deactivate in Eureka | Activate in Eureka

Instance	Zone	State	Launch Time	Package	Ver	Commit	Build	ELBs	Eureka	Health
i-e2174a9e	us-east-1c	InService	2013-12-19 13:04:59 PST	nfelasticsearch	0.90.2	40863c2	8		UP	
i-dad344a5	us-east-1e	InService	2013-12-19 13:45:38 PST	nfelasticsearch	0.90.2	40863c2	8		UP	
i-c77d0fbf	us-east-1d	InService	2013-12-19 13:47:39 PST	nfelasticsearch	0.90.2	40863c2	8		UP	

NETFLIX®

Suro for Data Delivery

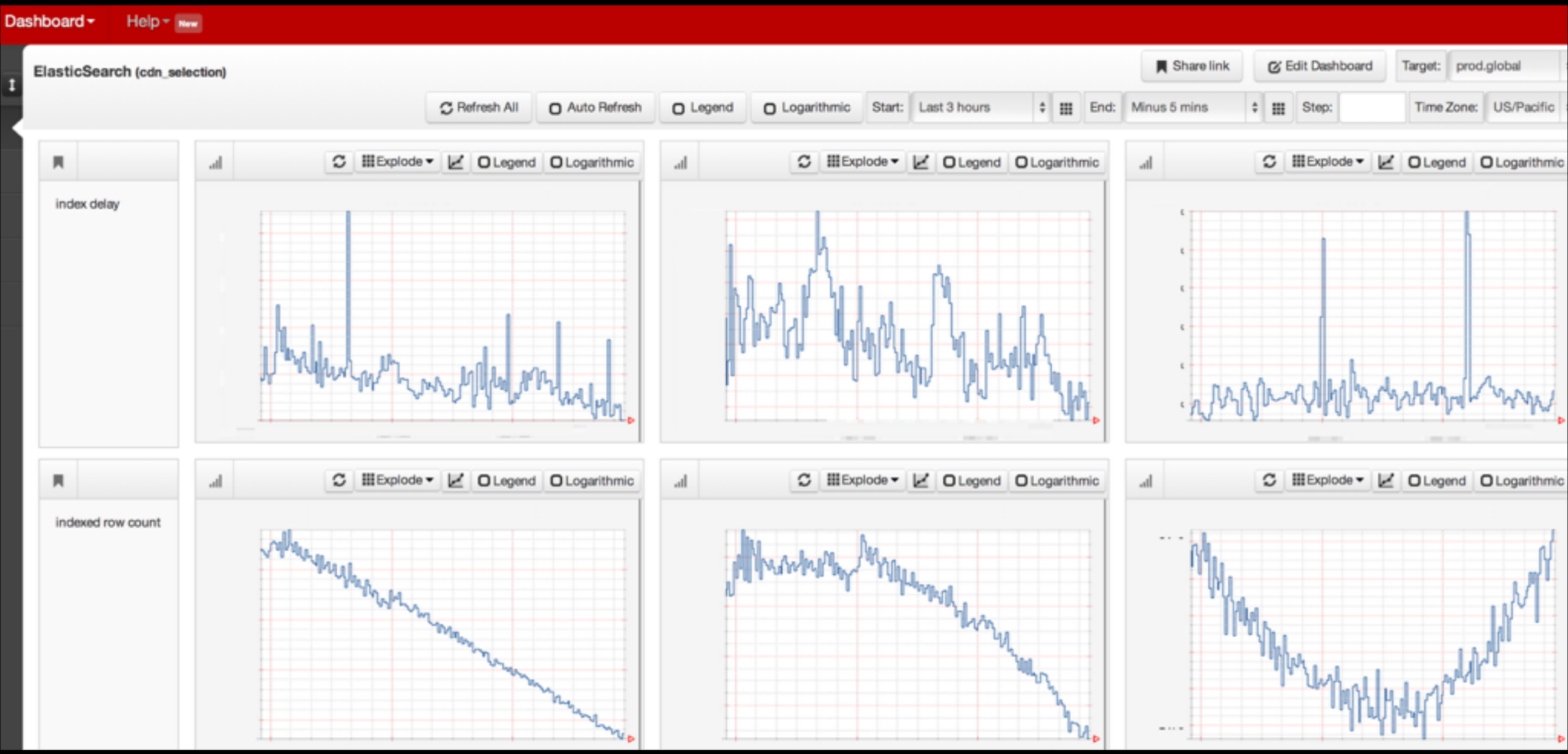
NETFLIX OSS



NETFLIX®

Servo for Monitoring Metrics

NETFLIX OSS



NETFLIX®

Zone-aware Replication

Multi-region Deployment

Multi-region Deployment

Discovery over Cassandra

Region-aware replication

Favor Index Rolling Over TTL

Favor Index Rolling Over TTL

A dedicated service manages index rolling

Uses index template and routing

Worth Trying G1

Worth Trying G1

Not recommended by ES team, but

Worth Trying G1

Not recommended by ES team, but

Has fewer and shorter GC pauses

Worth Trying G1

Not recommended by ES team, but

Has fewer and shorter GC pauses

Occasional SIGSEGV, but it’s okay

Simple Majority for Master Election

Simple Majority for Master Election

Split-brain problem

Simple Majority for Master Election

Split-brain problem

discovery.zen.minimum_master_nodes

Simple Majority for Master Election

Split-brain problem

discovery.zen.minimum_master_nodes

Dynamically updated

Future Work

Future Work

Automatic incremental backup and restore

Future Work

Automatic incremental backup and restore

Auto scaling

Future Work

Automatic incremental backup and restore

Auto scaling

Fully automated deployment

Future Work

Automatic incremental backup and restore

Auto scaling

Fully automated deployment

Support more use cases

We’re Hiring

Thank You!