Righting a Sinking Ship

Troubleshooting systems with available data

Laura Santamaria
Developer Advocate

@nimbinatus
#righttheship

https://www.flickr.com/photos/nzdefenceforce/6386334175/

http://www.defensie.nl/media/In_vuur_en_vlam_tcm46-102834.jpg

Now What?

Naked Gun courtesy of Giphy: https://gph.is/2kvXCEp

Step 1: Don’t Panic

90% Perseverance and Patience; 10% Luck

Maybe some knowledge sprinkled on

Step 2: Get Data

If you’re lucky

Logs!

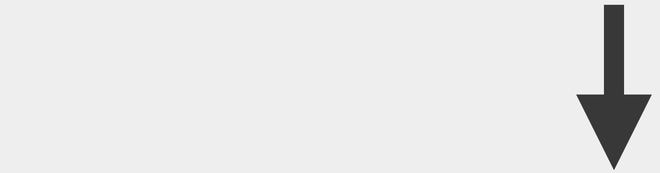
Alerts

Monitoring and historical data

Commands

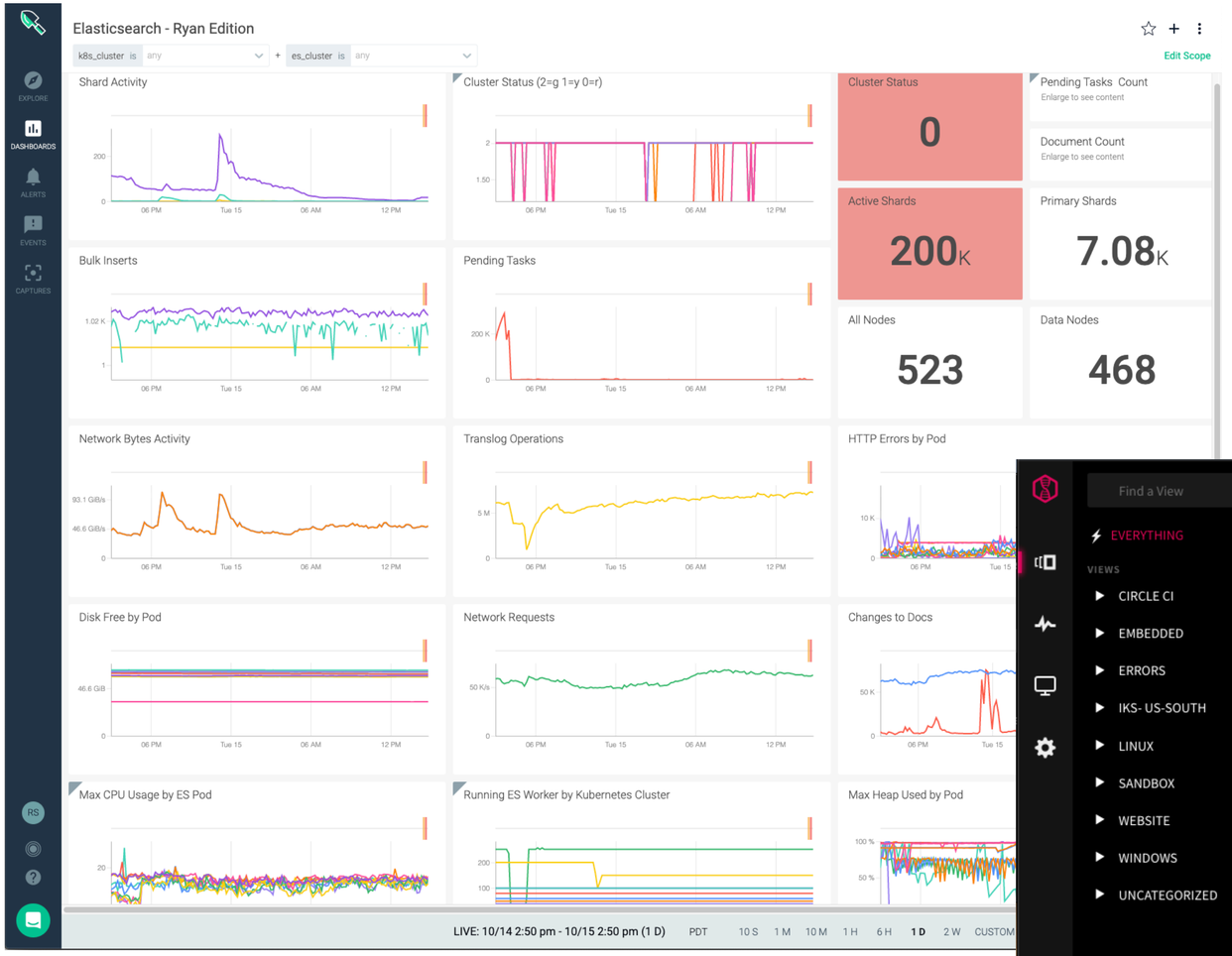
Depends on system

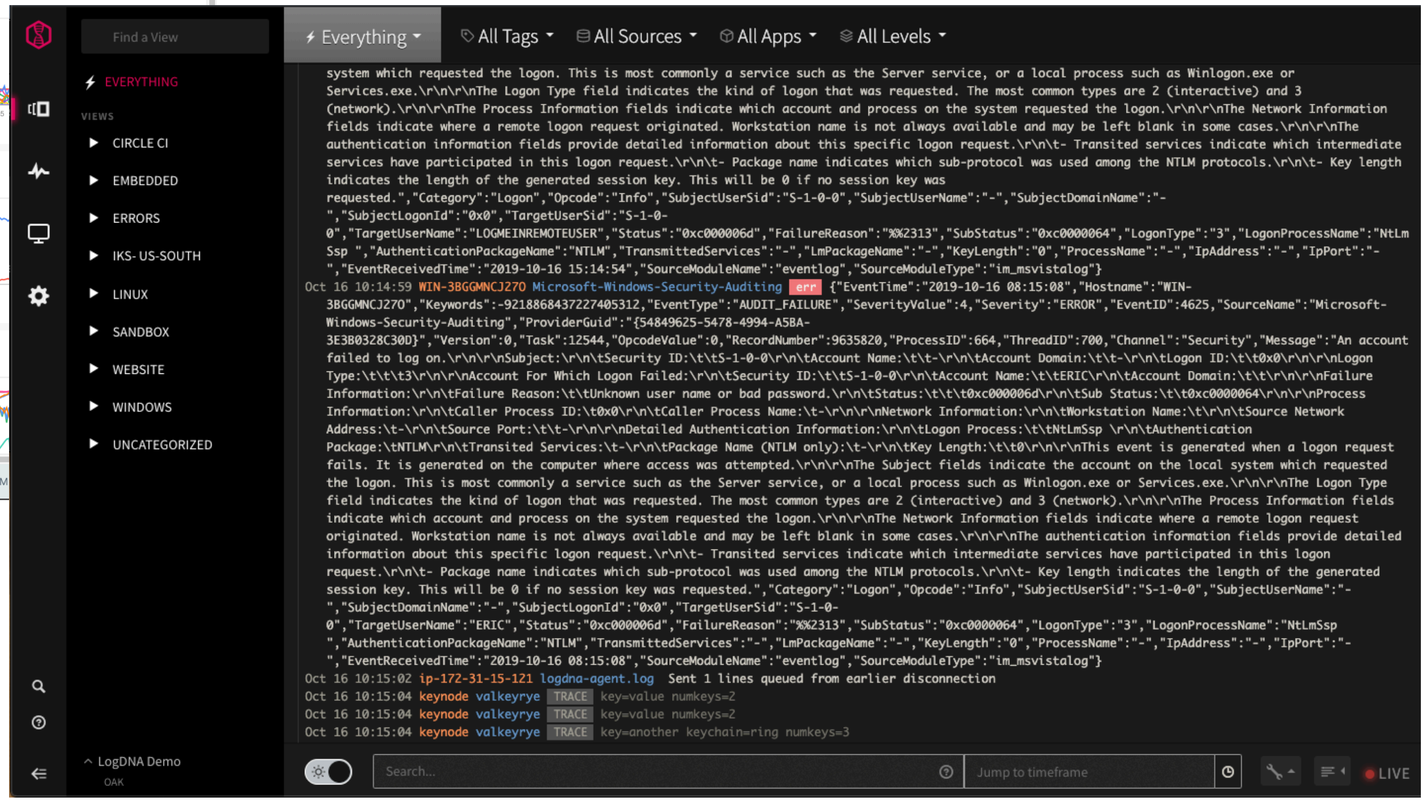
```
$ journalctl -xe

$ docker logs <container>

$ kubectl logs <object>

$ minikube logs

$ oc logs -f <object>
```



```
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.74267760
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.74271610
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.74276936
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.74330549
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.79389898
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.97063899
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.97093528
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.97098198
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.97101145
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.97103973
```

logdna


Elasticsearch - Ryan Edition
k8s_cluster is any
es_cluster is any
Edit Scope
EXPLORE
DASHBOARDS
ALERTS
EVENTS
CAPTURES
Shard Activity
Cluster Status (2=g 1=y 0=r)
Cluster Status
0
Pending Tasks Count
Enlarge to see content
Document Count
Enlarge to see content
Active Shards
200K
Primary Shards
7.08K
Bulk Inserts
Pending Tasks
All Nodes
523
Data Nodes
468
Network Bytes Activity
Translog Operations
HTTP Errors by Pod
Disk Free by Pod
Network Requests
Changes to Docs
Max CPU Usage by ES Pod
Running ES Worker by Kubernetes Cluster
Max Heap Used by Pod
LIVE: 10/14 2:50 pm - 10/15 2:50 pm (1 D)
PDT
10 S
1 M
10 M
1 H
6 H
1 D
2 W
CUSTOM


Find a View
EVERYTHING
VIEWS
CIRCLE CI
EMBEDDED
ERRORS
IKS- US-SOUTH
LINUX
SANDBOX
WEBSITE
WINDOWS
UNCATEGORIZED
LogDNA Demo
OAK
Everything
All Tags
All Sources
All Apps
All Levels
Search...
Jump to timeframe
LIVE

If you’re not lucky

Hit and observe

Test envs

Brute force

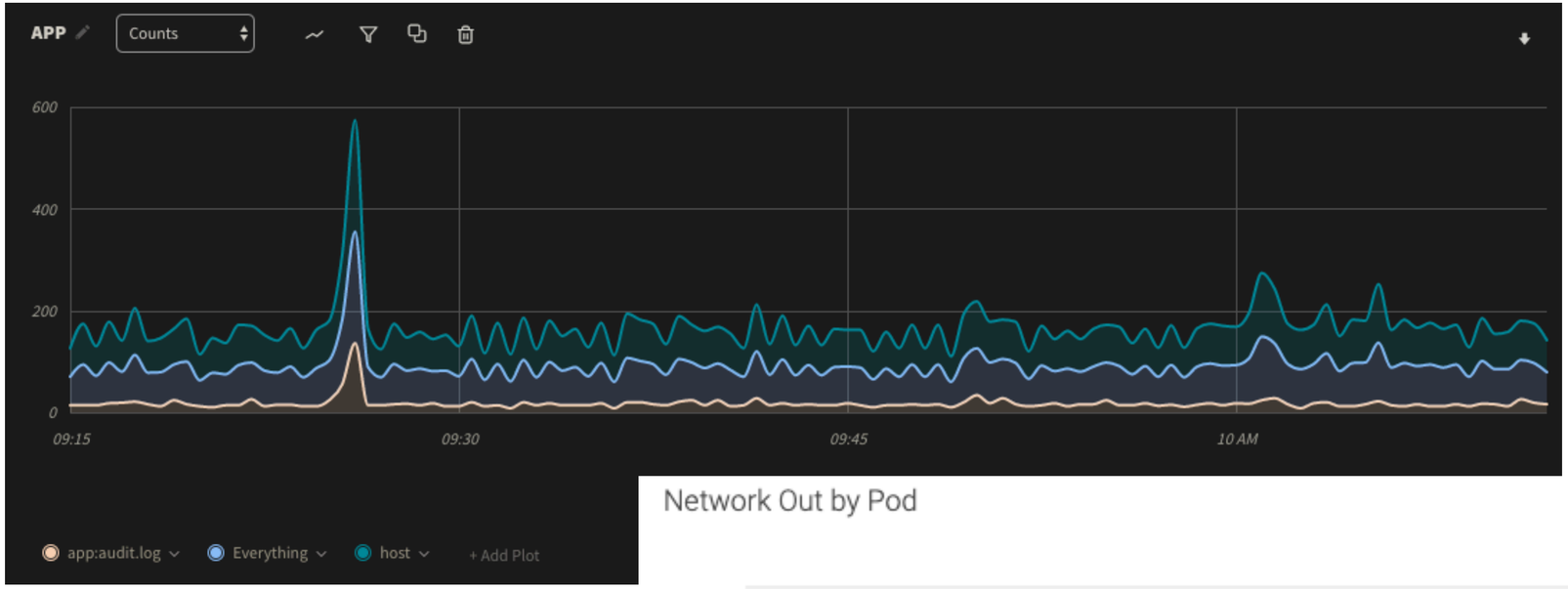
Step 3: Analyze

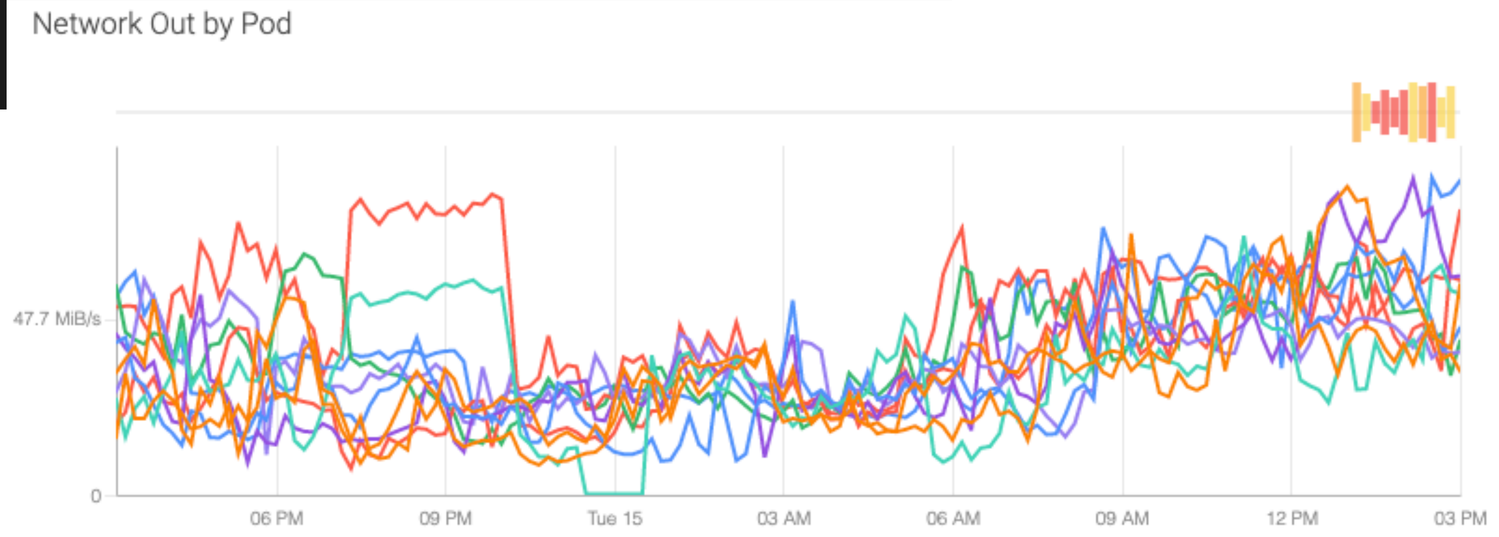
Evaluation tools

History

(Generated) Analytics

Your brain


APP
Counts
600
400
200
0
09:15
09:30
09:45
10 AM
app:audit.log
Everything
host
+ Add Plot


Network Out by Pod
47.7 MiB/s
0
06 PM
09 PM
Tue 15
03 AM
06 AM
09 AM
12 PM
03 PM

Step 4: Act

Wait!

Try it!

Run command

Observe

Step 5 (optional): Fail

Common Reasons

The rabbit hole

Multiple causes

Red herrings

You can still fix it!

Step 6: Repeat as Necessary

Common Container Issues

Code

Releases

Incompatibility

Dependencies

Configurations

Errors

Missing data

Networking

DNS

Routing

Virtual ethernet

External

Physical network

OS Updates

Physical changes

http://www.photolib.noaa.gov/coastline/line0534.htm

Thank you!

@nimbinatus || @logdna

#righttheship

https://nimbinatus.com