

# 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](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>
```

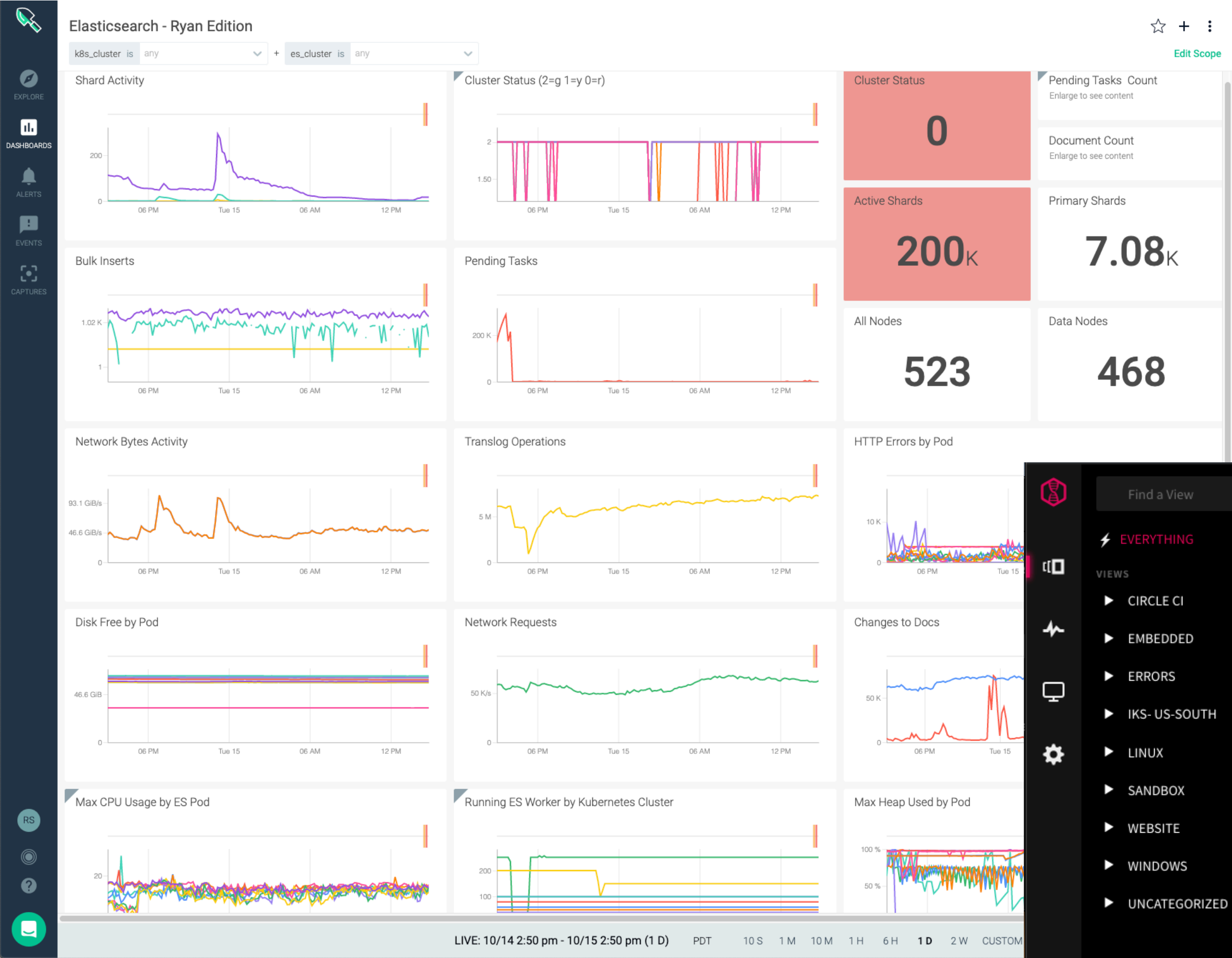
```
$ minikube logs
```

```
$ oc logs -f <object>
```



```
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.742677603Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.742716103Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.742769363Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.743305497Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.793898988Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.970638998Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.970935288Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.970981988Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.971011458Z" level=info msg="Docker daemon"
Oct 14 15:32:11 minikube dockerd[2347]: time="2019-10-14T15:32:11.971039738Z" level=info msg="Docker daemon"
```





Find a View

EVERYTHING

VIEWS

CIRCLE CI

EMBEDDED

ERRORS

IKS- US-SOUTH

LINUX

SANDBOX

WEBSITE

WINDOWS

UNCATEGORIZED

Everything

All Tags

All Sources

All Apps

All Levels

system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).\r\n\r\n\r\nThe Process Information fields indicate which account and process on the system requested the logon.\r\n\r\n\r\nThe Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\r\n\r\n- Transited services indicate which intermediate services have participated in this logon request.\r\n\r\n\r\n- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\r\n\r\n- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.", "Category": "Logon", "Opcode": "Info", "SubjectUserSid": "S-1-0-0", "SubjectUserName": "-", "SubjectDomainName": "-", "SubjectLogonId": "0x0", "TargetUserSid": "S-1-0-0", "TargetUserName": "LOGMEINREMOTEUSER", "Status": "0xc000006d", "FailureReason": "%2313", "SubStatus": "0xc0000064", "LogonType": "3", "LogonProcessName": "NtLmSsp", "AuthenticationPackageName": "NTLM", "TransmittedServices": "-", "LmPackageName": "-", "KeyLength": "0", "ProcessName": "-", "IpAddress": "-", "IpPort": "-", "EventReceivedTime": "2019-10-16 15:14:54", "SourceModuleName": "eventlog", "SourceModuleType": "im\_msvistalog"}  
Oct 16 10:14:59 WIN-3BGGMNCJ270 Microsoft-Windows-Security-Auditing errr {"EventTime": "2019-10-16 08:15:08", "Hostname": "WIN-3BGGMNCJ270", "Keywords": "-9218868437227405312", "EventType": "AUDIT\_FAILURE", "SeverityValue": 4, "Severity": "ERROR", "EventID": 4625, "SourceName": "Microsoft-Windows-Security-Auditing", "ProviderGuid": "{54849625-5478-4994-A58A-3E3B0328C30D}", "Version": 0, "Task": 12544, "OpcodeValue": 0, "RecordNumber": 9635820, "ProcessID": 664, "ThreadID": 700, "Channel": "Security", "Message": "An account failed to log on.\r\n\r\n\r\nSubject:\r\n\r\n\r\nSecurity ID:\t\tS-1-0-0\r\n\r\n\r\nAccount Name:\t\t-\r\n\r\n\r\nAccount Domain:\t\t-\r\n\r\n\r\nLogon ID:\t\t0x0\r\n\r\n\r\nLogon Type:\t\t3\r\n\r\n\r\nAccount For Which Logon Failed:\r\n\r\n\r\nSecurity ID:\t\tS-1-0-0\r\n\r\n\r\nAccount Name:\t\tERIC\r\n\r\n\r\nAccount Domain:\t\t\r\n\r\n\r\nFailure Information:\r\n\r\n\r\nFailure Reason:\t\tUnknown user name or bad password.\r\n\r\n\r\nStatus:\t\t0xc000006d\r\n\r\n\r\nSub Status:\t\t0xc0000064\r\n\r\n\r\nProcess Information:\r\n\r\n\r\nCaller Process ID:\t0x0\r\n\r\n\r\nCaller Process Name:\t-\r\n\r\n\r\nNetwork Information:\r\n\r\n\r\nWorkstation Name:\t\r\n\r\n\r\nSource Network Address:\t-\r\n\r\n\r\nSource Port:\t\t-\r\n\r\n\r\nDetailed Authentication Information:\r\n\r\n\r\nLogon Process:\t\tNtLmSsp\r\n\r\n\r\nAuthentication Package:\tNTLM\r\n\r\n\r\nTransited Services:\t-\r\n\r\n\r\nPackage Name (NTLM only):\t-\r\n\r\n\r\nKey Length:\t\t0\r\n\r\n\r\nThis event is generated when a logon request fails. It is generated on the computer where access was attempted.\r\n\r\n\r\n\r\nThe Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\n\r\n\r\nThe Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).\r\n\r\n\r\n\r\nThe Process Information fields indicate which account and process on the system requested the logon.\r\n\r\n\r\n\r\nThe Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\n\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\r\n\r\n\r\n- Transited services indicate which intermediate services have participated in this logon request.\r\n\r\n\r\n\r\n- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\r\n\r\n\r\n- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.", "Category": "Logon", "Opcode": "Info", "SubjectUserSid": "S-1-0-0", "SubjectUserName": "-", "SubjectDomainName": "-", "SubjectLogonId": "0x0", "TargetUserSid": "S-1-0-0", "TargetUserName": "ERIC", "Status": "0xc000006d", "FailureReason": "%2313", "SubStatus": "0xc0000064", "LogonType": "3", "LogonProcessName": "NtLmSsp", "AuthenticationPackageName": "NTLM", "TransmittedServices": "-", "LmPackageName": "-", "KeyLength": "0", "ProcessName": "-", "IpAddress": "-", "IpPort": "-", "EventReceivedTime": "2019-10-16 08:15:08", "SourceModuleName": "eventlog", "SourceModuleType": "im\_msvistalog"}  
Oct 16 10:15:02 ip-172-31-15-121 logdna-agent.log Sent 1 lines queued from earlier disconnection  
Oct 16 10:15:04 keynode valkeyrye TRACE key=value numkeys=2  
Oct 16 10:15:04 keynode valkeyrye TRACE key=value numkeys=2  
Oct 16 10:15:04 keynode valkeyrye TRACE key=another keychain=ring numkeys=3

LogDNA Demo

OAK

Search...

Jump to timeframe

LIVE

# If you're not lucky

Hit and observe

Test envs

Brute force



# Step 3: Analyze

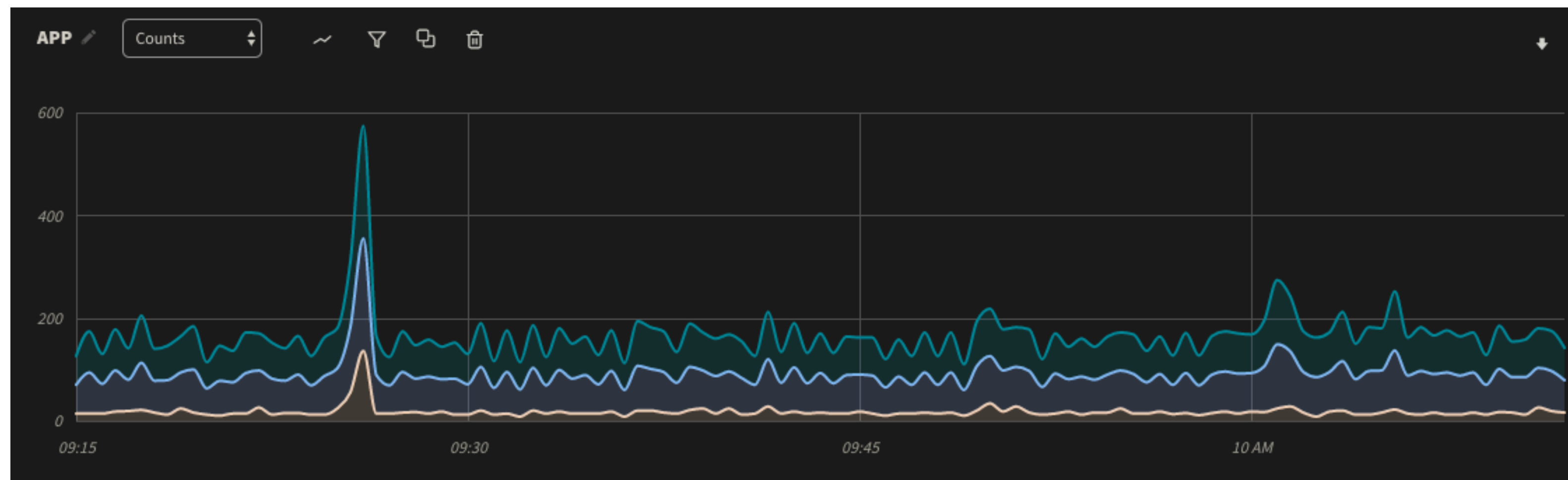
# Evaluation tools

History

(Generated) Analytics

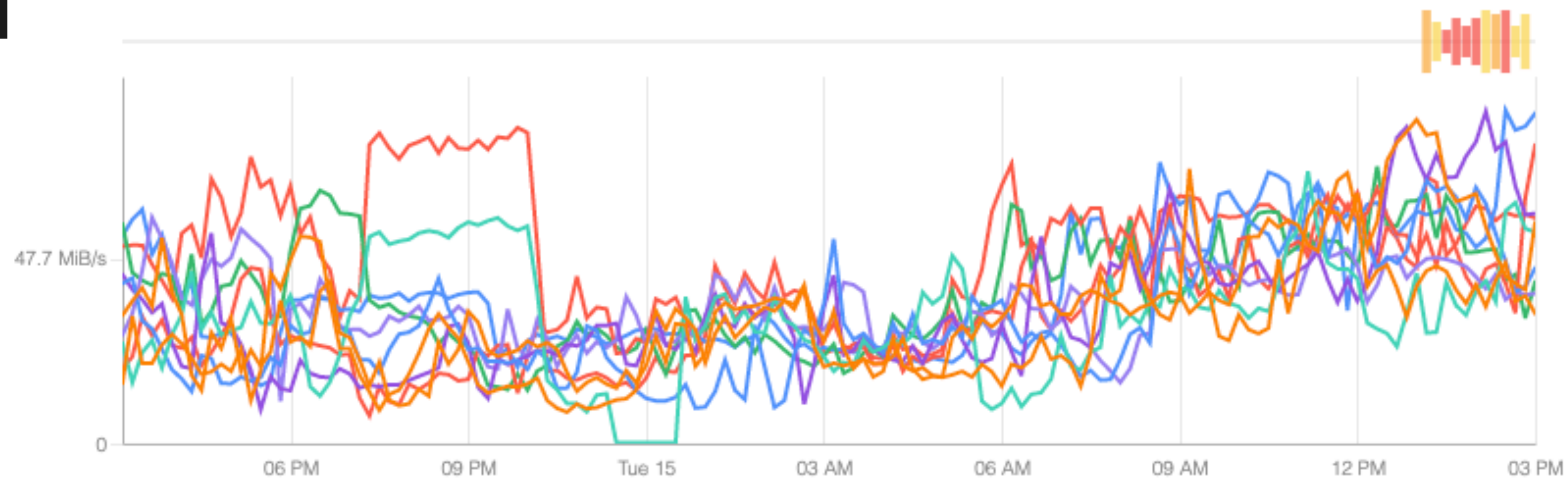
Your brain





● app:audit.log ▾ ● Everything ▾ ● host ▾ + Add Plot

Network Out by Pod



# 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>

@nimbinatus | #righttheship