



# A Monitoring Tool for Kubernetes Cluster Security

Vincent Ruijter  
@\_evict

Valentine Mairret  
@vm00z

# \$ who

## Vincent Ruijter

- KPN CERT
- Openbook
- hacker-in-residence
- Null Amsterdam moderator
- knows how to quit vim

## Valentine Mairret

- KPN REDteam
- defender gone attacker
- WICCA organiser
- uses nano

# \$ 1s outline

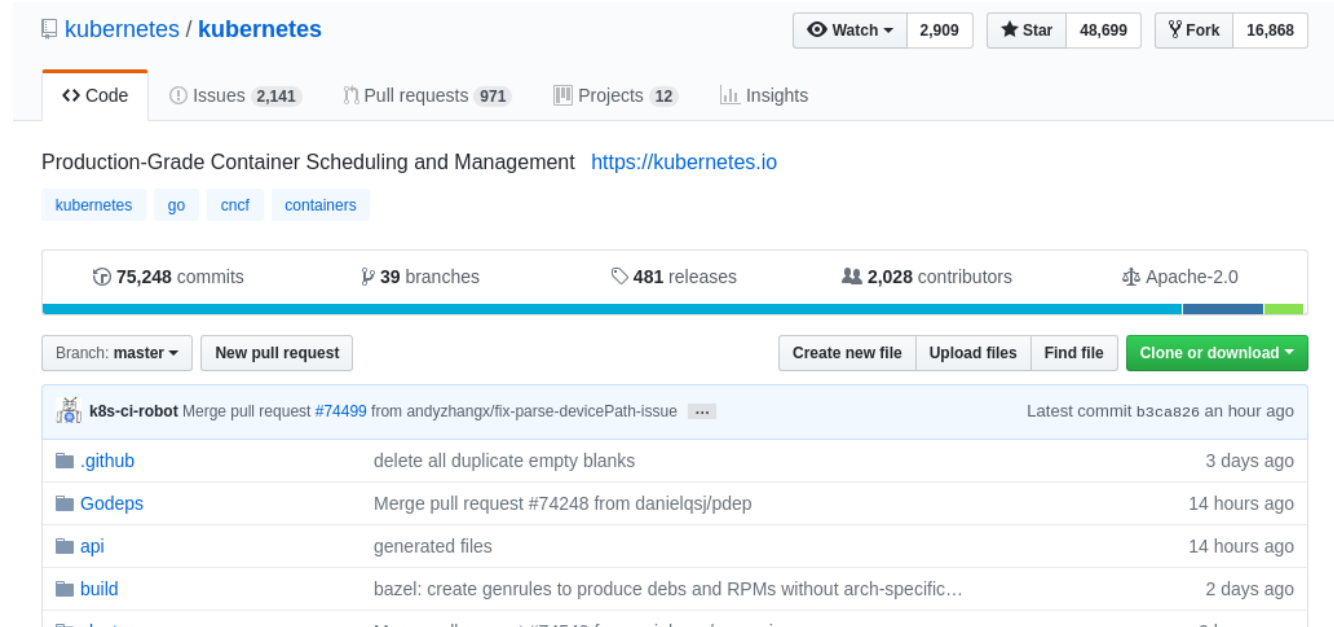
- introduction
- attacking kubernetes
- logging architecture
  - fluentd + elasticsearch + kibana
- attack traces in the logs
- alert system
- k8s security dashboard
- demo time!



# what is kubernetes?

# \$ man k8s

- open source container orchestration
- written in go
- usually runs with docker
- made by Google
- now part of the Cloud Native Computing Foundation



The screenshot shows the GitHub repository for Kubernetes. At the top, it says 'kubernetes / kubernetes' with a 'Watch' button (2,909), a 'Star' button (48,699), and a 'Fork' button (16,868). Below this are tabs for 'Code', 'Issues' (2,141), 'Pull requests' (971), 'Projects' (12), and 'Insights'. The main heading is 'Production-Grade Container Scheduling and Management' with a link to 'https://kubernetes.io'. Below this are tags for 'kubernetes', 'go', 'cncf', and 'containers'. A statistics bar shows '75,248 commits', '39 branches', '481 releases', '2,028 contributors', and 'Apache-2.0' license. Below the statistics bar are buttons for 'Branch: master', 'New pull request', 'Create new file', 'Upload files', 'Find file', and 'Clone or download'. The main content area shows a list of recent commits, including a merge pull request from 'andyzhangx/fix-parse-devicePath-issue' and several other commits related to .github, Godeps, api, and build.



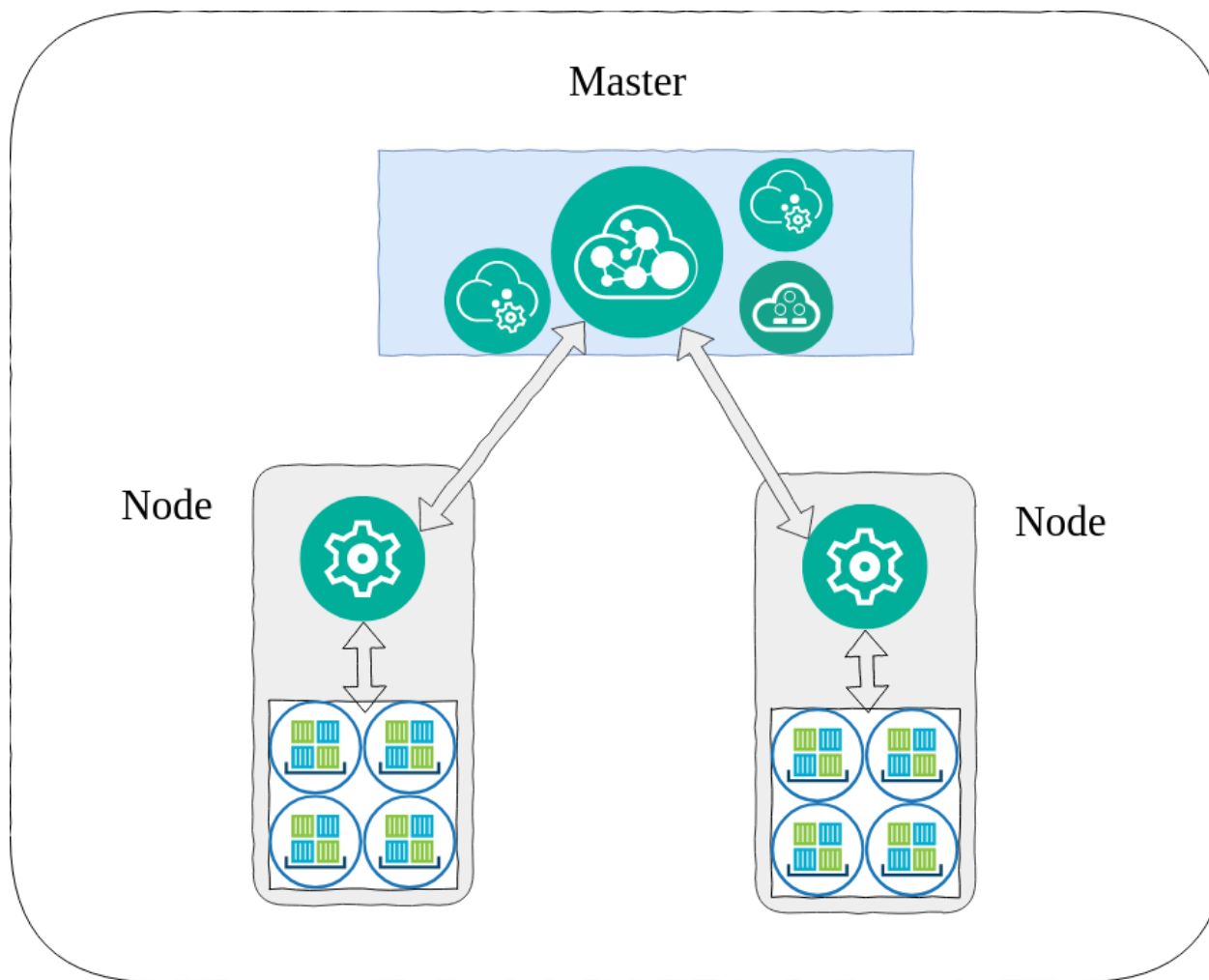
# \$ man k8s

- insecure deployments on the internet
- since v1.9 RBAC (Role Based Authentication) enabled by default
- since v1.7 Dashboard no longer cluster admin
- `>= v1.7 && etcd >= v3`, secret encryption

```
I1129 03:22:24.147056 "heapster.go:72] /heapster --source=kubernetes:https://kubernetes.default --sink=influxdb:http://monitoring-influxdb.kube-system.svc:8086"
I1129 03:22:24.147142 "heapster.go:73] Heapster version v1.4.3
I1129 03:22:24.147637 "configs.go:61] Using Kubernetes client with master "https://kubernetes.default" and version v1
I1129 03:22:24.147661 "configs.go:62] Using kubelet port 10255
E1129 03:22:54.149023 "kubelet.go:334] Failed to load nodes: Get https://kubernetes.default/api/v1/nodes: dial tcp: i/o timeout
E1129 03:22:59.158123 "influxdb.go:264] issues while creating an InfluxDB sink: failed to ping InfluxDB server at "monitoring-influxdb.kube-system.svc:8086" - Get http://monitoring-influxdb.kube-system.svc:8086/ping: dial tcp 172.16.0.167:8086: getsockopt: connection refused, will retry on use
I1129 03:22:59.158903 "influxdb.go:278] created influxdb sink with options: host=monitoring-influxdb.kube-system.svc:8086 user=root db=k8s
```

# \$ cat k8s-terms.txt

term	definition
node	a worker machine in kubernetes
secrets	all authentication tokens, credentials, ssh keys, etc
namespace	abstraction to support multiple virtual clusters on the same physical cluster
pod	set of running containers on a cluster
container	executable image that contains software and all of its dependencies
kubelet	agent that runs on nodes and makes sure that containers are running in a pod
kubect1	command line tool for communicating with a Kubernetes API server
daemonset	ensures a copy of a pod is running across a set of nodes in a cluster







why are we here?

# \$ cat why.txt

- to present a monitoring tool!
- configure a logging architecture for k8s to store audit logs
- perform analysis on these logs to detect and label events
- create a security dashboard for k8s

# \$ cat why.txt

- no explicit resources on how to audit k8s
- no tools online to label activity
- no security dashboard 😎



# attacking kubernetes

# \$ cat attacking-k8s.md

- creating pods with privileged mode
- creating pods with a hostpath
- abusing privileged pods (e.g. dashboard)
- stealing / abusing tokens
- default tiller deployment exploitation
- many more...



# \$ cat privileged.yml

- commonly allowed
- set a security context
- allow privileged -> true

```
apiVersion: v1
kind: Pod
metadata:
  name: host-escape
spec:
  containers:
  - image: nginx:1.7.9
    name: nginx
    securityContext:
      privileged: true
```

# \$ cat host-mount.yml

- append following lines to container spec
- mounts host root in /root
- if running as root, node compromised
- attach to daemon set to instantly own all nodes

```
apiVersion: v1
kind: Pod
metadata:
  name: host-escape
spec:
  containers:
  [...SNIP...]
  volumeMounts:
    - mountPath: /root
      name: hostroot
  volumes:
    - name: hostroot
      hostPath:
        path: /
```



# logging architecture

# \$ cat log-architecture.txt

- append lines to  
/etc/kubernetes/manifests/  
kube-apiserver.yaml
- create audit log policy  
(example in git)
- writes logs to  
/var/log/kubernetes
- quite verbose!

```
spec:
  containers:
  - command:
    - kube-apiserver
    - --authorization-mode=Node,RBAC
    - --advertise-address=10.0.2.15
    - --audit-policy-
file=/etc/kubernetes/policies/adv-
audit.yml
    - --audit-log-
path=/var/log/kubernetes/kube-apiserver-
audit.log
    - --audit-log-format=json
    - --allow-privileged=true
```

# \$ ./get-k8s-audit.sh

- quite verbose logging
- logs request object / response objects
- contains for instance entire pod configuration (yaml -> json)
- as stated: very verbose

```
{
  "kind": "Event",
  "apiVersion": "audit.k8s.io/v1beta1",
  "metadata": {
    "creationTimestamp": "2019-02-
13T13:18:34Z"
  }, [...SNIP...]
  "spec": {
    "volumes": [
      {
        "name": "100tz",
        "hostPath": {
          "path": "/",
          "type": ""
        }
      }
    ]
  }
}
```



# \$ cat how-to-log.txt

- fluentd
  - easy to use, can run in cluster
  - daemonset
  - initcontainer to install and compile ruby gems
    - No need for compilers and headers in the actual container
- elasticsearch
  - good with variate datasets
  - kibana

# \$ cat how-to-log.txt

- elasticsearch problems
  - static mapping, k8s objects vary
  - when working with multiple nodes -> duplicate requests

pushing to elasticsearch, random issues with kube-apiserver audit logs #452



billiaz opened this issue on Jul 29, 2018 · 18 comments



billiaz commented on Jul 29, 2018 • edited ▾



## Problem

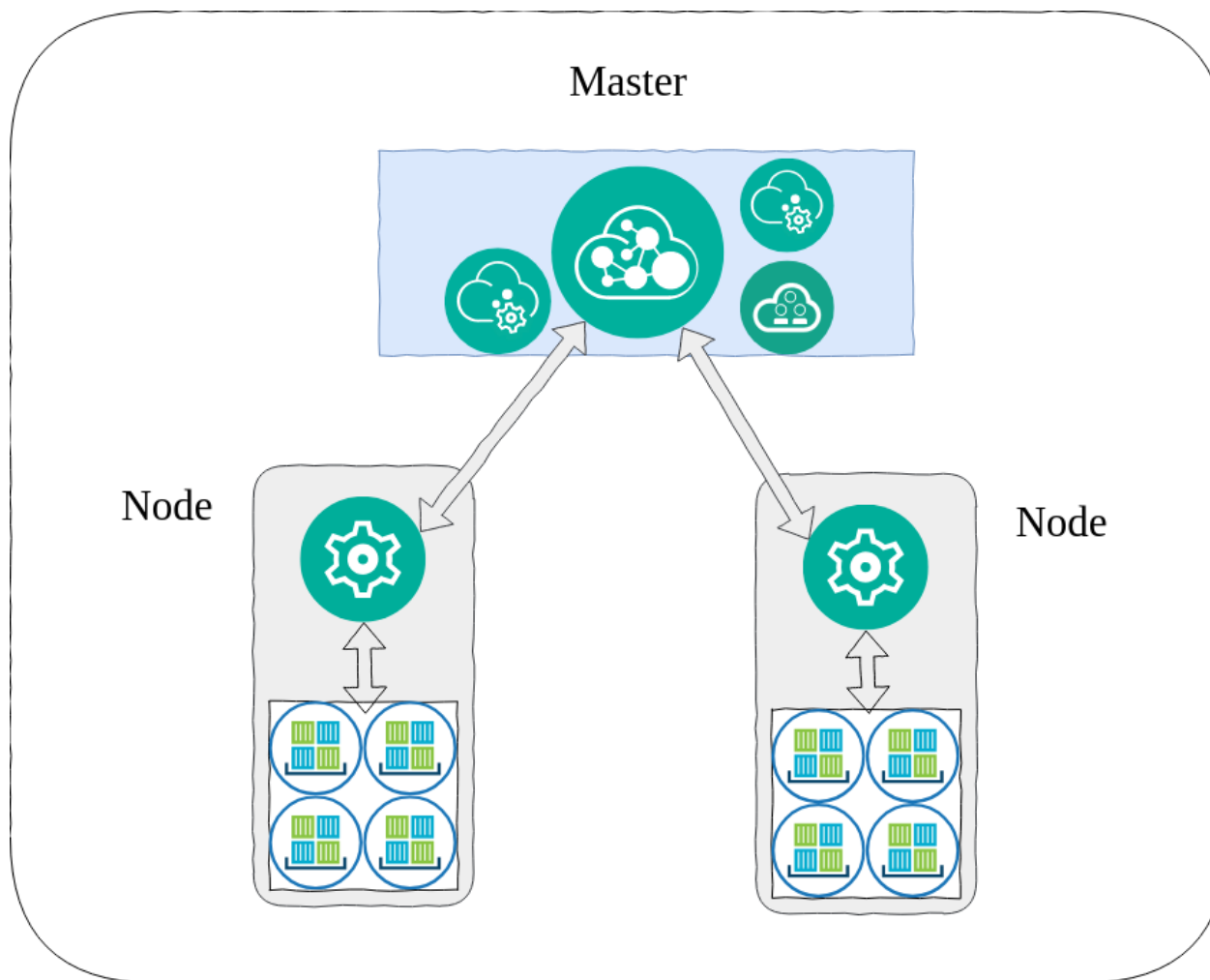
My Fluent D throws random exception when parsing auditlog of kube-apiserver  
example:

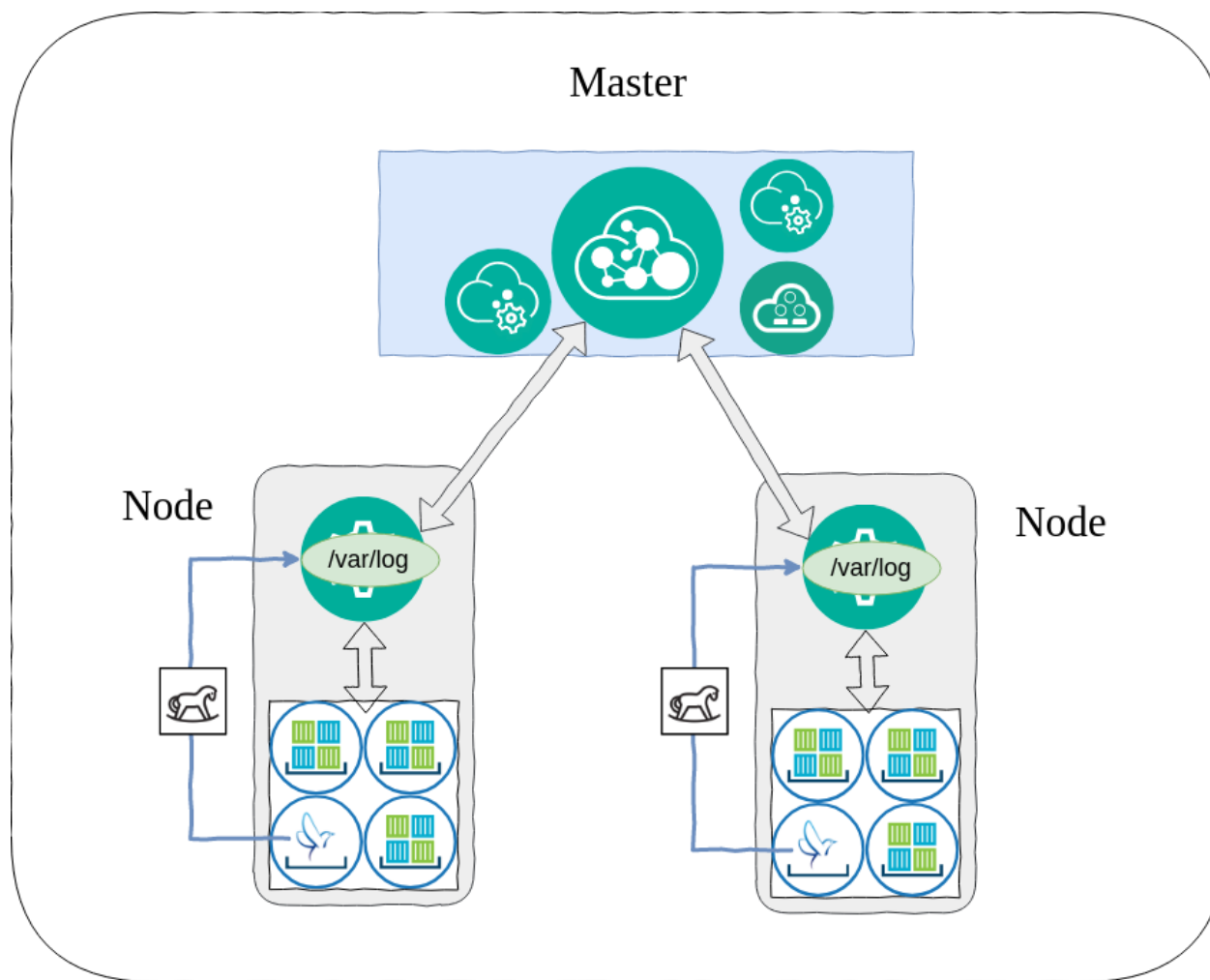
Assignee

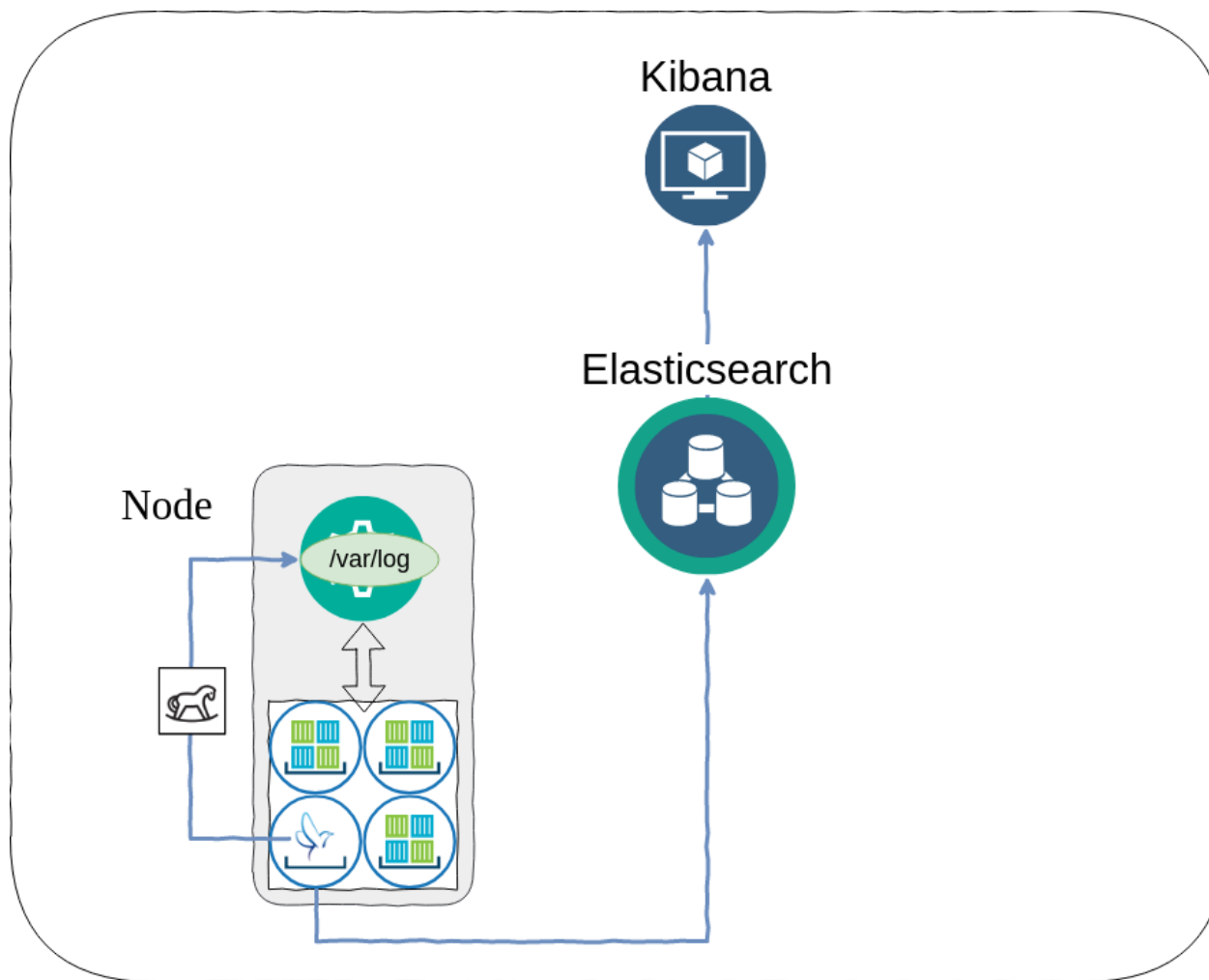
No one assigned

Labels

help









February 24th 2019, 23:17:55	system:serviceaccount:kube-logging:fluentd	/api/v1/watch/namespaces?resourceVersion=170579	http.rb/0.9.8	watch
February 24th 2019, 23:17:55.000	system:serviceaccount:kube-logging:fluentd	/api/v1/watch/pods?resourceVersion=170579	http.rb/0.9.8	watch
February 24th 2019, 21:39:43.000	kubernetes-admin	/api/v1/namespaces/default/pods	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	create
February 24th 2019, 21:39:42.000	kubernetes-admin	/openapi/v2?timeout=32s	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	get
February 24th 2019, 21:39:20.000	kubernetes-admin	/api/v1/namespaces/default/pods/host-escape	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	delete



# attack traces

## \$ api usage \*

- activity on cluster
- user-agent, verb and username

All Requests

1-50 of 227 < >

Time ▾	user.username	requestURI	userAgent	verb
▶ February 26th 2019, 13:42:34.000	system:serviceaccount:default:exec-only	/openapi/v2?timeout=32s	kubectl/v1.12.0 (linux/amd64) kube-rnetes/0ed3388	get
▶ February 26th 2019, 13:42:34.000	system:serviceaccount:default:exec-only	/api/v1/namespaces/default/pods/host-escape	kubectl/v1.12.0 (linux/amd64) kube-rnetes/0ed3388	get
▶ February 26th 2019, 13:42:34.000	system:serviceaccount:default:exec-only	/api/v1/namespaces/default/pods	kubectl/v1.12.0 (linux/amd64) kube-rnetes/0ed3388	create
▶ February 26th 2019, 13:42:30.000	system:serviceaccount:default:exec-only	/api/v1/namespaces/default/pods?limit=500	kubectl/v1.12.0 (linux/amd64) kube-rnetes/0ed3388	list



## \$ kubectl get secrets

- access to secret resources
- enumeration, dumping etc.

user.username	requestURI	userAgent	verb
kubernetes-admin	/api/v1/secrets?limit=500	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	list
kubernetes-admin	/api/v1/secrets?limit=500	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	list
kubernetes-admin	/api/v1/namespaces/default/secrets?limit=500	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	list
kubernetes-admin	/api/v1/namespaces/default/secrets?limit=500	kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388	list

## \$ kubectl exec

- exec activity on cluster
- commands that were executed and requestURI
- cannot see executed interactive commands

kubernetes-admin	/api/v1/namespaces/kube-system/pods/etcd-kubernetes/exec?command=%2Fbin%2Fls&command=%2F&container=etcd&container=etcd&stdin=true&stdout=true&tty=true
kubernetes-admin	/api/v1/namespaces/kube-system/pods/etcd-kubernetes/exec?command=%2Fbin%2Fls&command=%2F&container=etcd&container=etcd&stdin=true&stdout=true&tty=true





```
$ ./spawn-privileged.sh
```

- allowed privileged pod creations
- good indication for compromise attempts

Privileged allowed

Time ▼	annotations.authorization.k8s.io/decision	objectRef.name	user.username
▶ February 26th 2019, 13:42:34.000	allow	host-escape	system:serviceaccount:default:exec-only
▶ February 24th 2019, 17:09:43.000	allow	host-escape	kubernetes-admin



# alert system



# k8scop

a helper for k8s security monitoring



# \$ man k8scop

- makes the analysis of k8s audit logs easier
- classifies logs into labelled events using regular expressions
- provides more clarity about events



# \$ ./k8scop

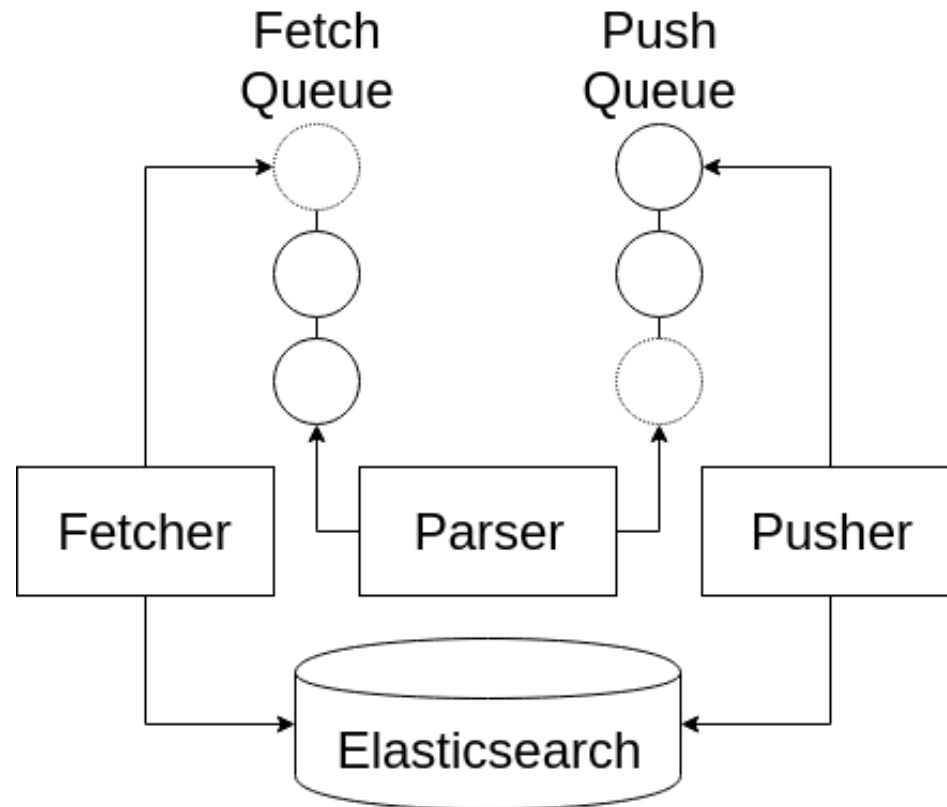
- performs static analysis on a date range
- can perform streaming analysis in (almost) real time
- python elasticsearch client
- multi-threaded for extra speed

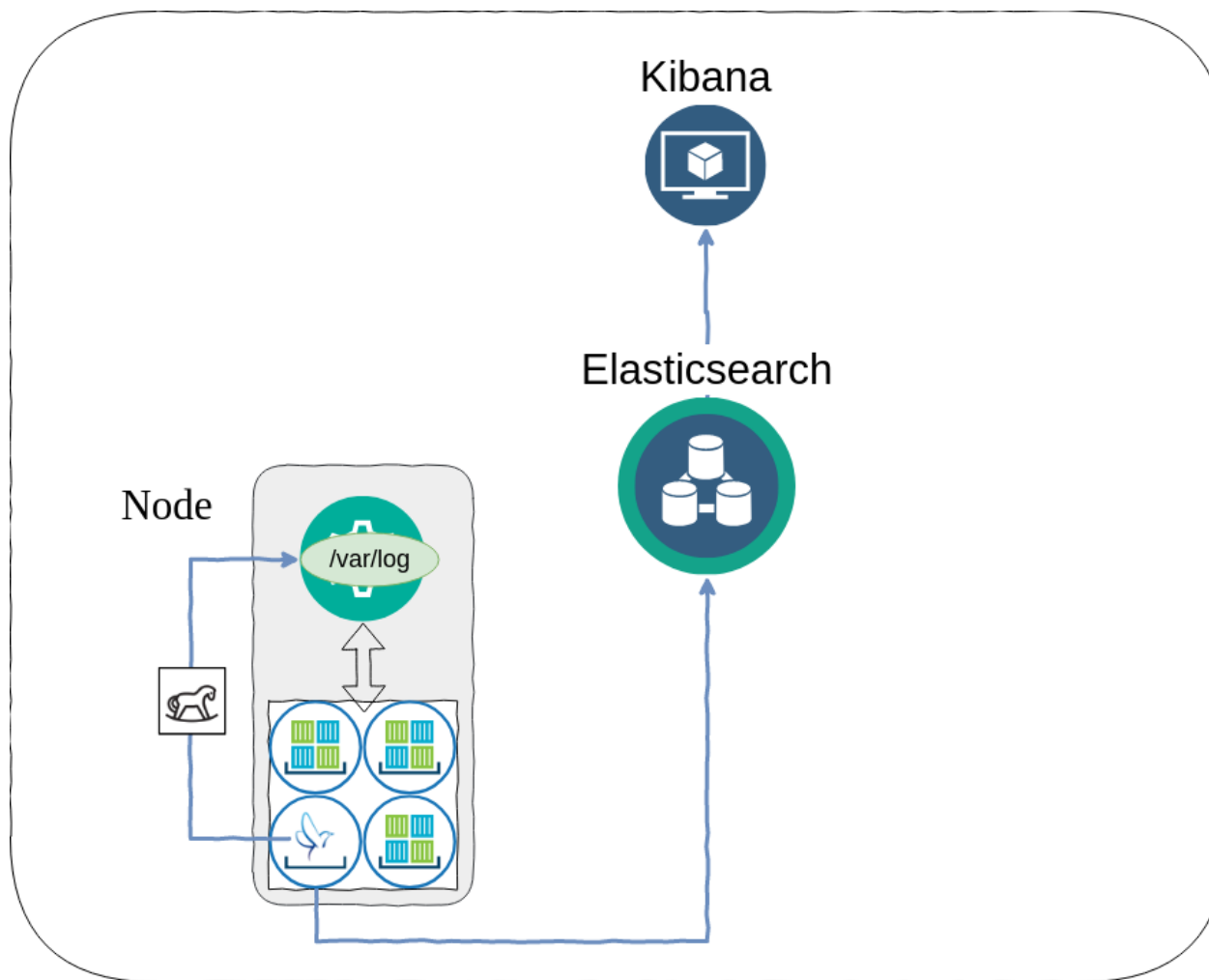


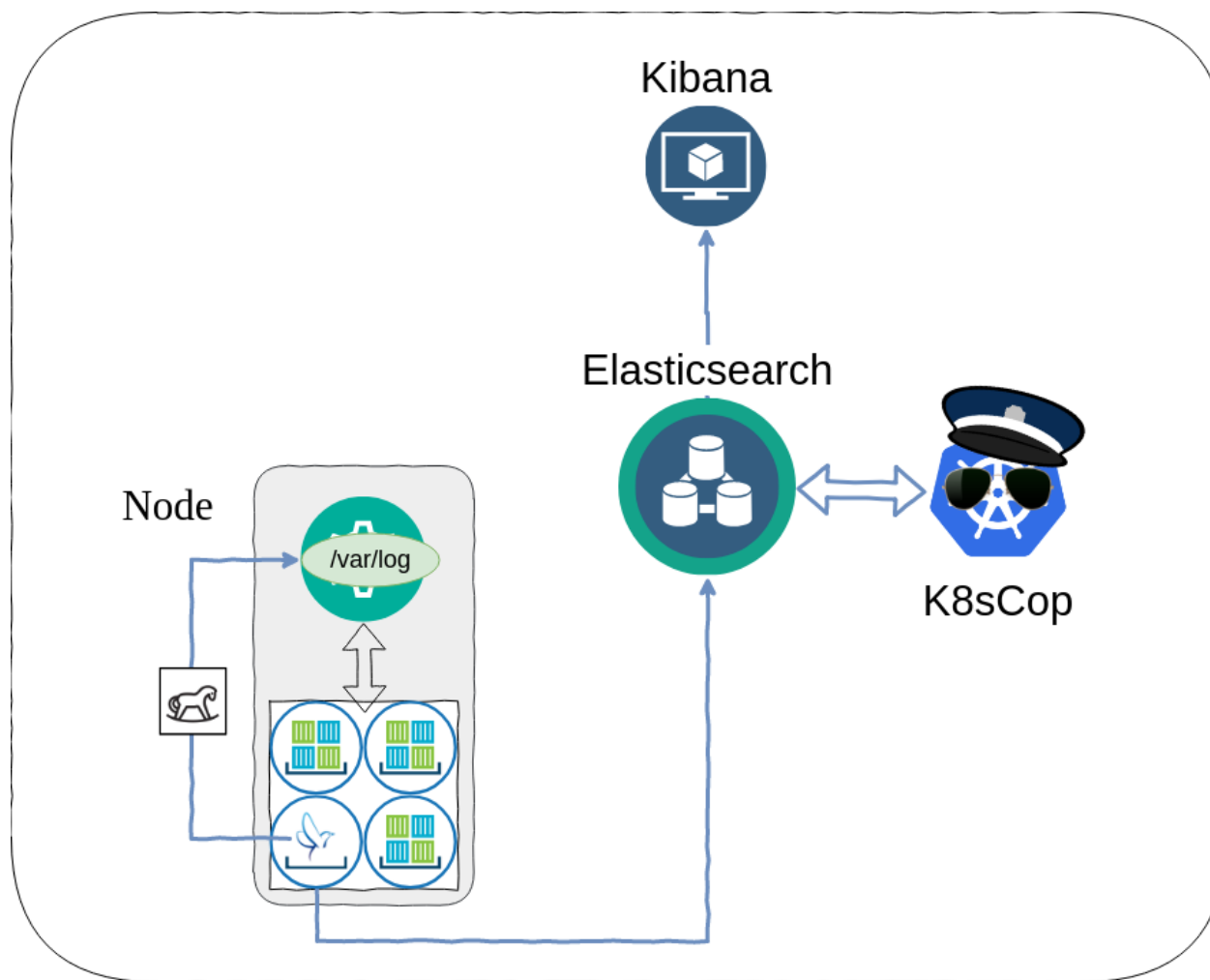


# \$ ./k8scop

- fetches logs from elasticsearch
- parses logs with a set of regular expressions
- pushes *alerts* back to elasticsearch







# \$ ./k8scop

▶ February 24th 2019, 21:39:14.000	Pod enumeration in all name spaces	kubernetes-admin	N/A	N/A
▶ February 24th 2019, 21:39:07.000	Attempt to get all secrets from default	kubernetes-admin	default	N/A
▶ February 24th 2019, 21:23:55.000	Information request on kube-scheduler-kubernetes in kube-system	kubernetes-admin	kube-system	kube-scheduler-kubernetes
▶ February 24th 2019, 21:23:55.000	Command execution detected	kubernetes-admin	kube-system	kube-scheduler-kubernetes

# \$ which limitations

- classification is a 1-to-1 mapping
- cannot (yet) correlate multiple events
- new rules need to be coded

these limitations are potential for future work!





# \$ which future-work

- create an interface for adding new rules
- correlate multiple events to detect more complex attack traces
- integrate triggers
- connect the alert system to k8s itself?





# kubernetes security dashboard



demo time!



# conclusion



# \$ ./conclude

- kubernetes is cool for hacks
- k8s security dashboard
  - fluentd + elasticsearch + k8scop + kibana
- visibility over k8s cluster activity
- future work
  - since k8s 1.13
    - new logging methods
  - k8scop can be improved and extended



# Thank you!

Vincent Ruijter  
@\_evict

Valentine Mairet  
@vm00z

<https://github.com/k8scop/k8s-security-dashboard>