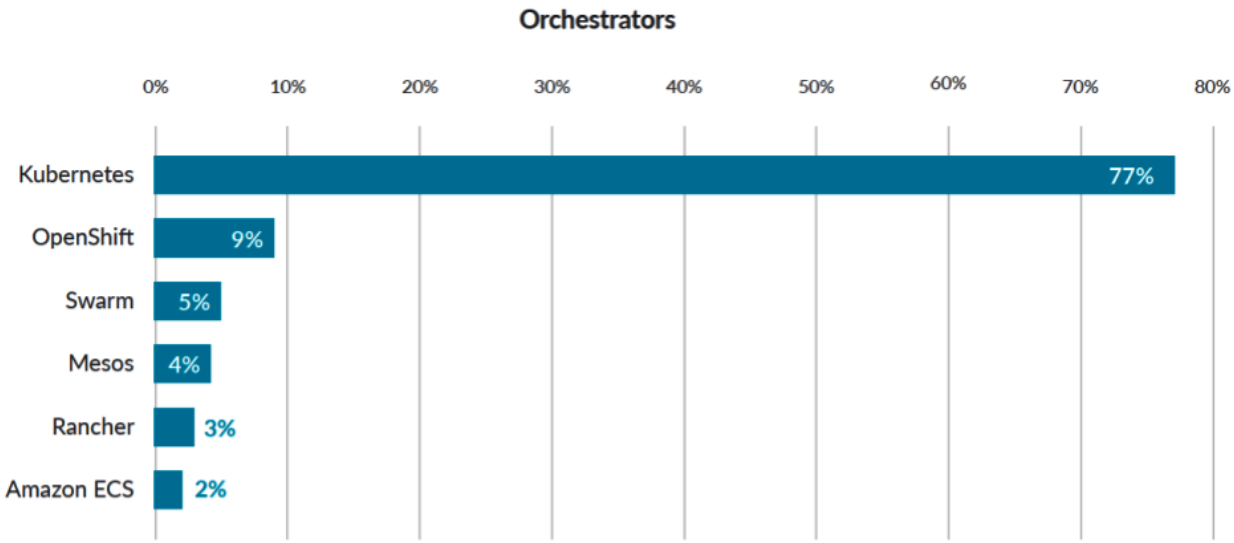
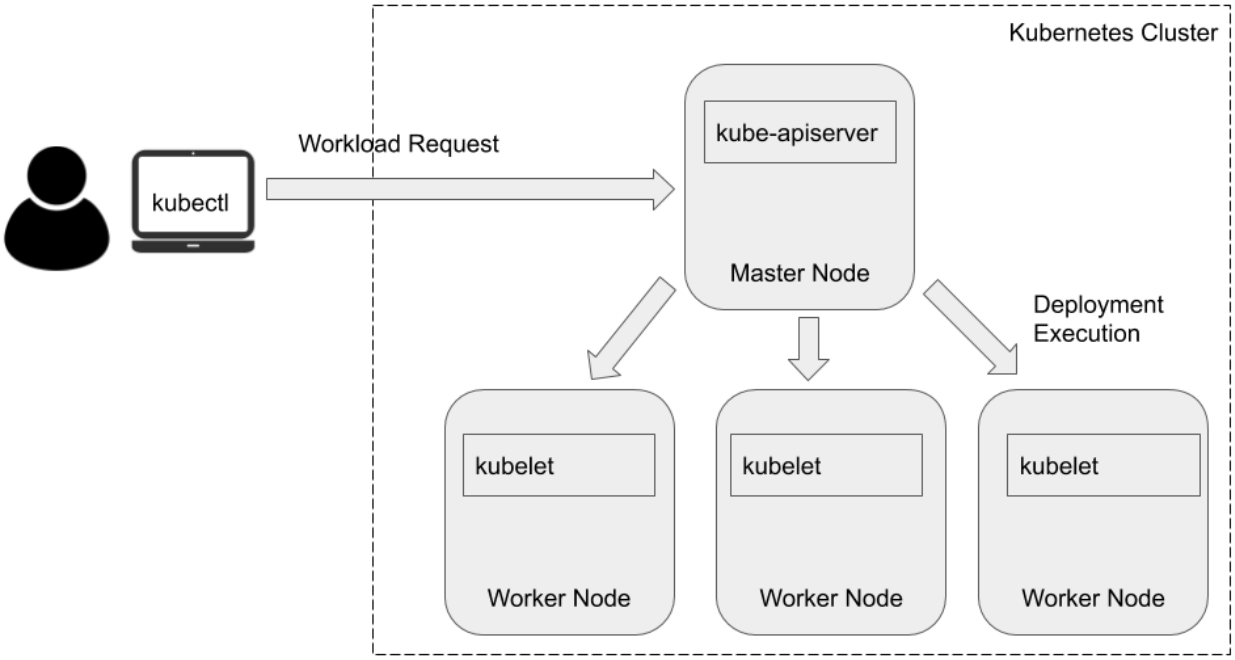
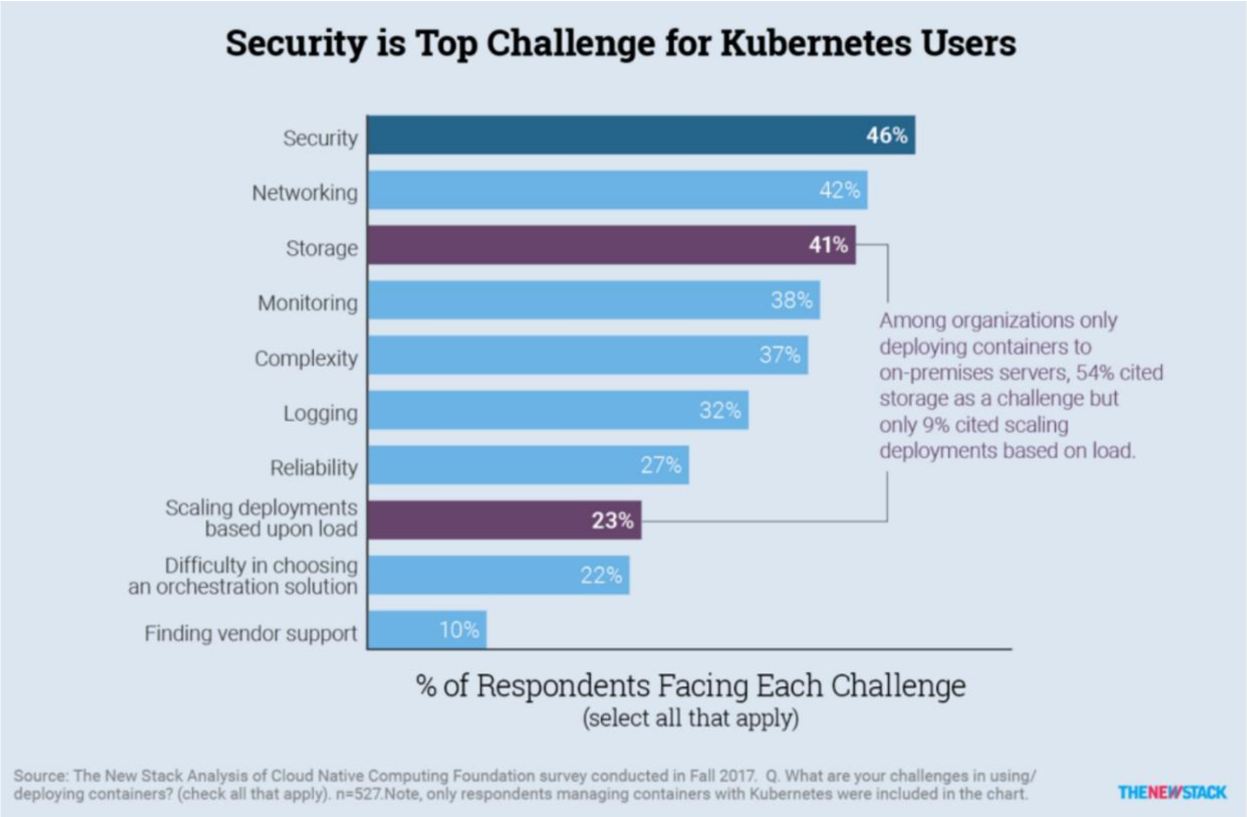
Chapter 1: Kubernetes Architecture





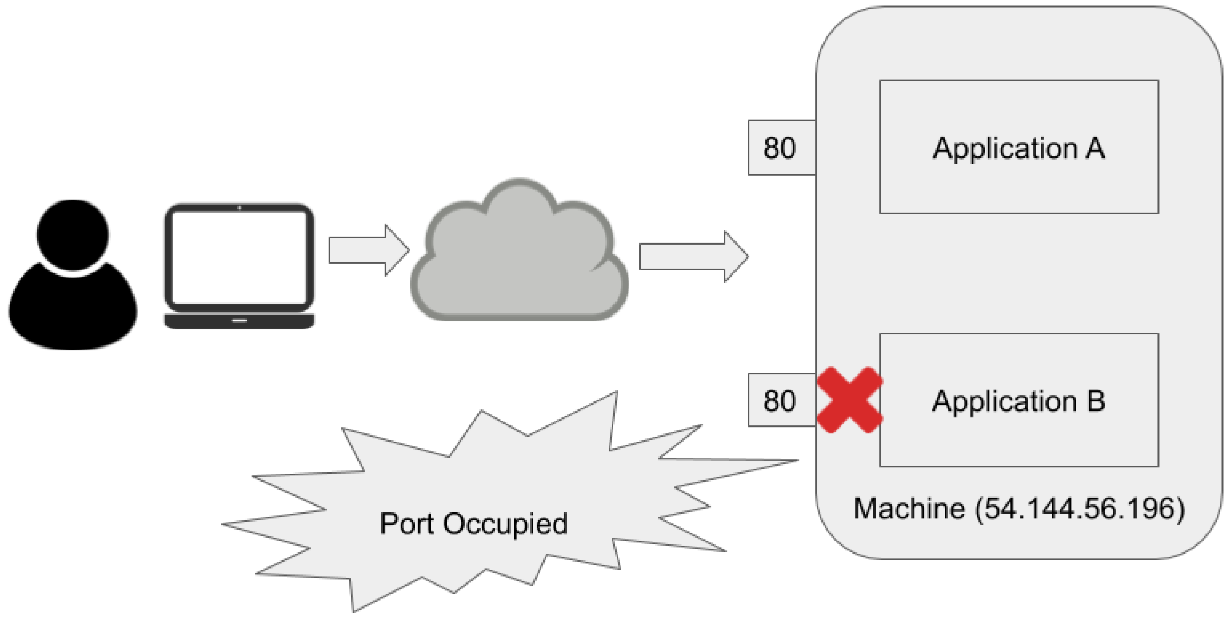


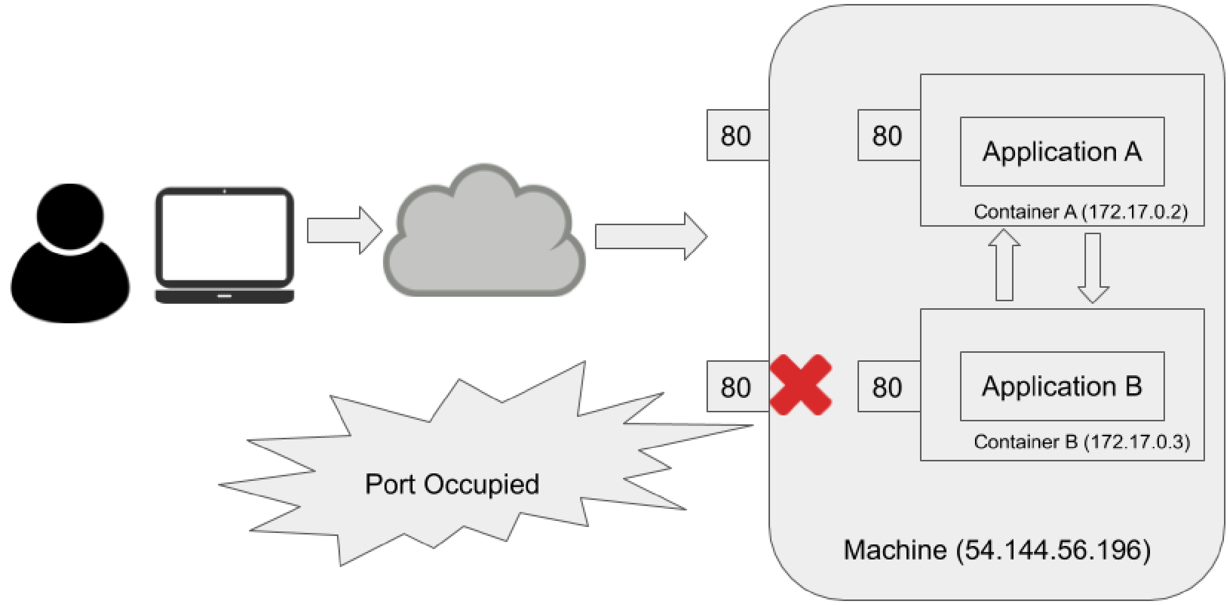
Security is Top Challenge for Kubernetes Users

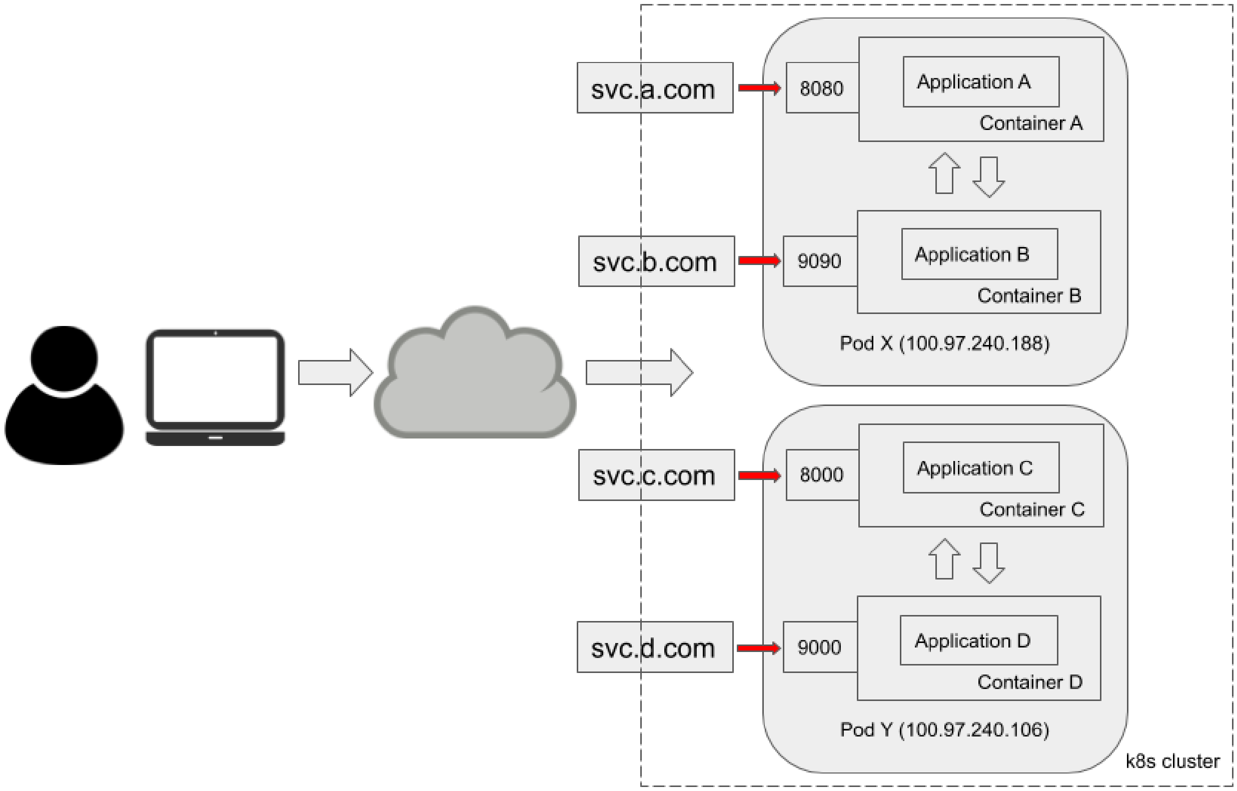
Among organizations only deploying containers to on-premises servers, 54% cited storage as a challenge but only 9% cited scaling deployments based on load.

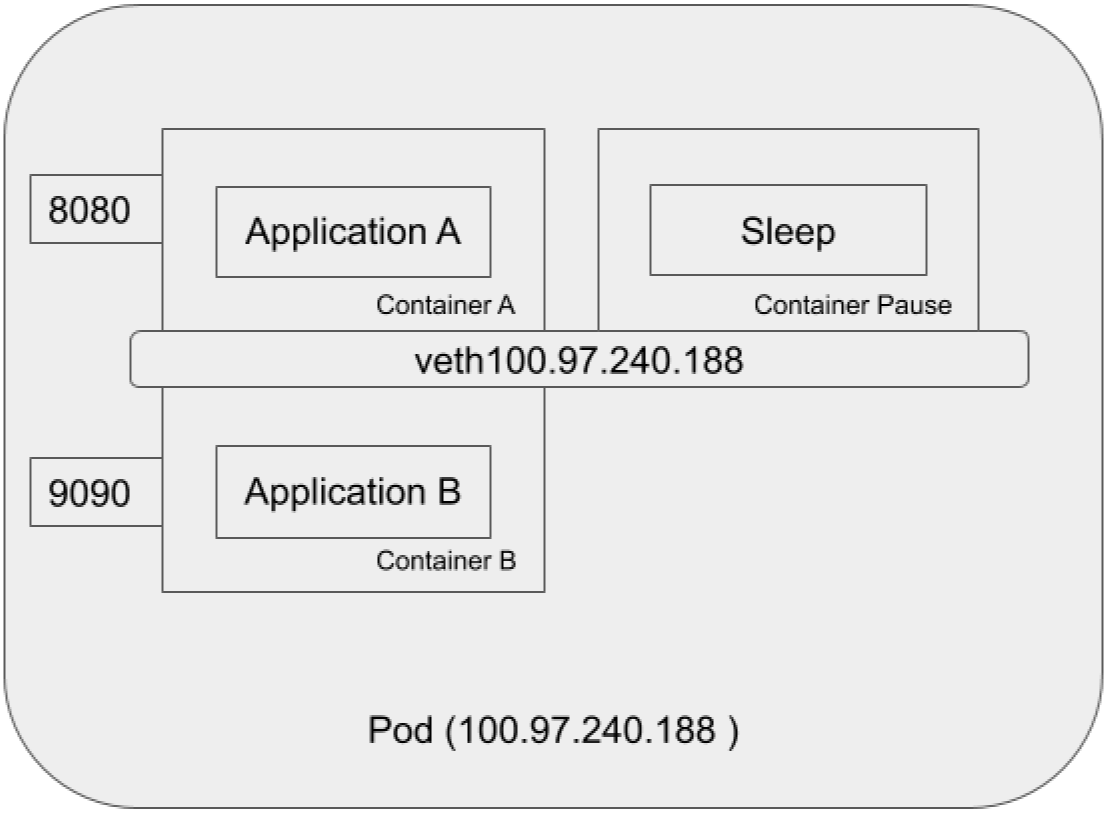
Source: The New Stack Analysis of Cloud Native Computing Foundation survey conducted in Fall 2017. Q. What are your challenges in using/deploying containers? (check all that apply). n=527.Note, only respondents managing containers with Kubernetes were included in the chart.

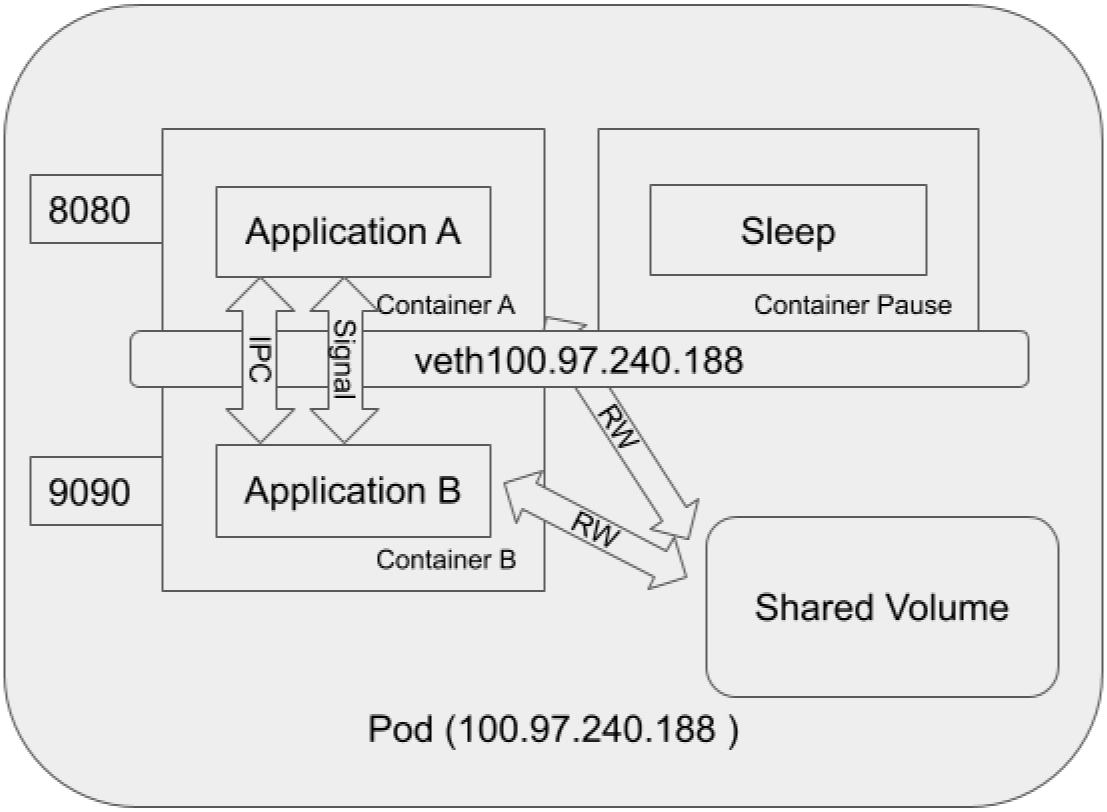
Chapter 2: Kubernetes Networking

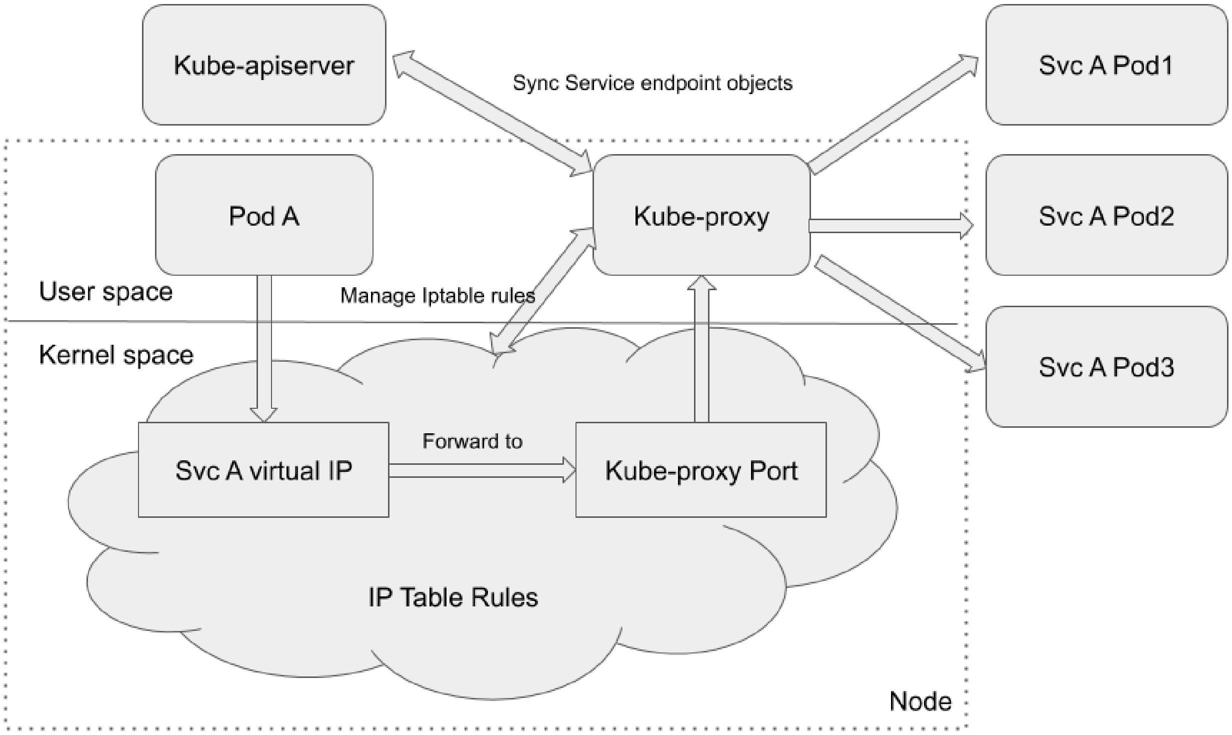


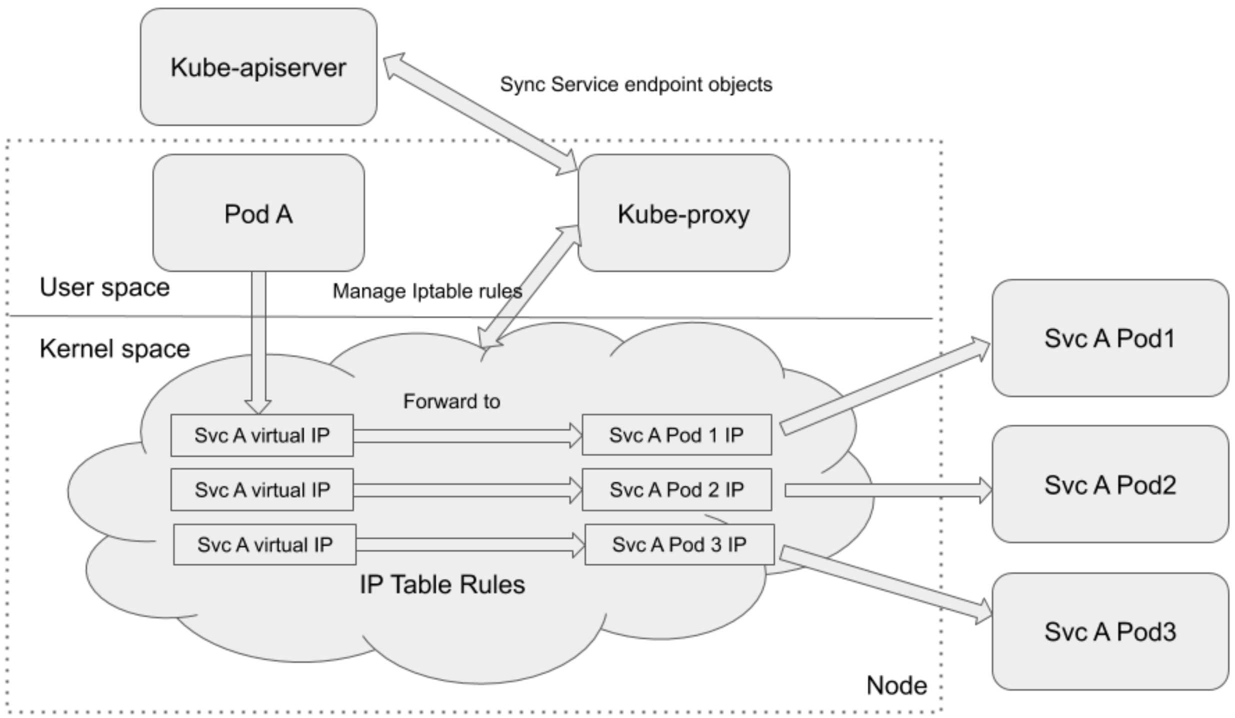


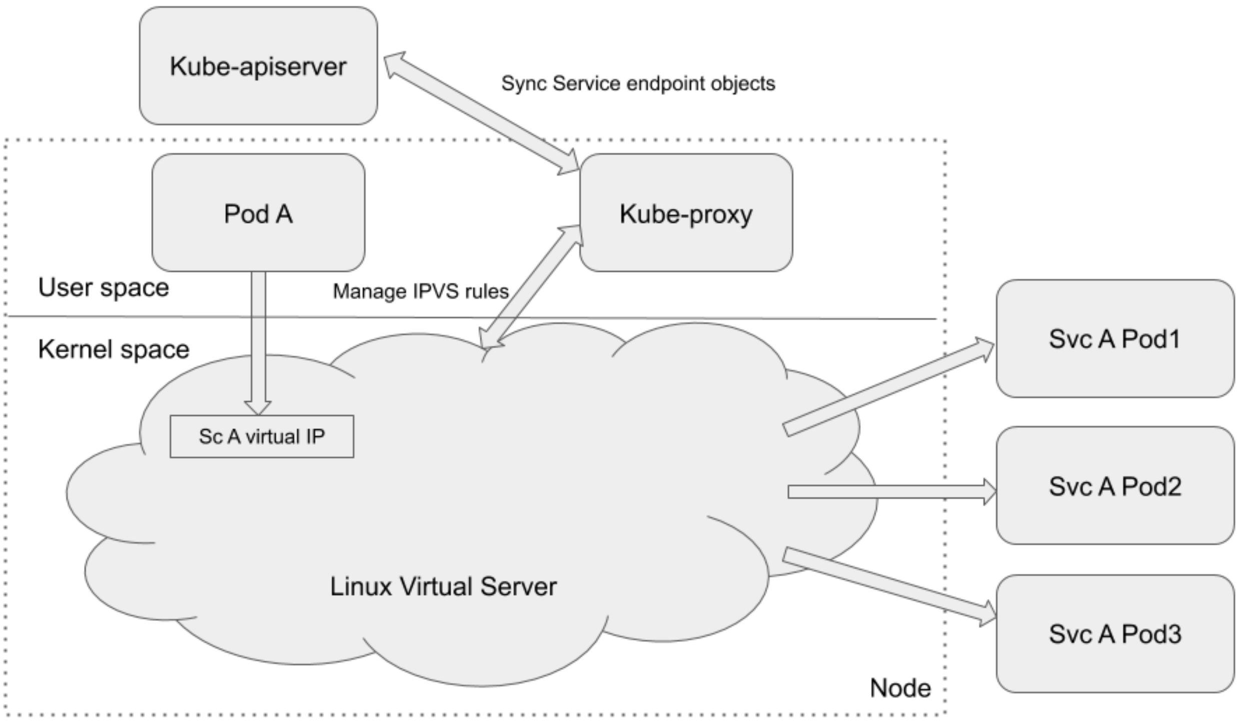

svc.a.com
svc.b.com
svc.c.com
svc.d.com
8080
Application A
Container A
9090
Application B
Container B
Pod X (100.97.240.188)
8000
Application C
Container C
9000
Application D
Container D
Pod Y (100.97.240.106)
k8s cluster


8080
Application A
Container A
Sleep
Container Pause
veth100.97.240.188
9090
Application B
Container B
Pod (100.97.240.188)


8080
Application A
Container A
Sleep
Container Pause
IPC
Signal
veth100.97.240.188
RW
9090
Application B
RW
Container B
Shared Volume
Pod (100.97.240.188)

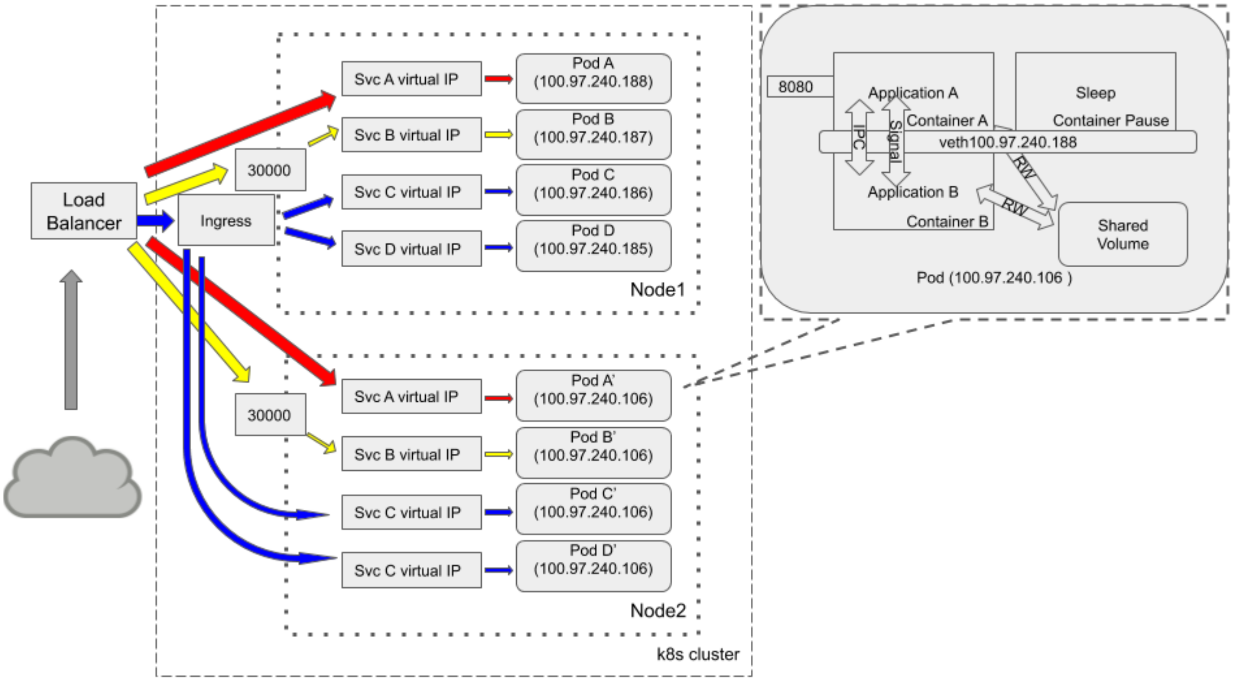

Kube-apiserver
Sync Service endpoint objects
Svc A Pod1
Pod A
Kube-proxy
Svc A Pod2
User space
Manage Iptable rules
Kernel space
Svc A Pod3
Svc A virtual IP
Forward to
Kube-proxy Port
IP Table Rules
Node


Kube-apiserver
Sync Service endpoint objects
Pod A
Kube-proxy
User space
Manage Iptable rules
Kernel space
Forward to
Svc A virtual IP
Svc A Pod 1 IP
Svc A virtual IP
Svc A Pod 2 IP
Svc A virtual IP
Svc A Pod 3 IP
IP Table Rules
Node
Svc A Pod1
Svc A Pod2
Svc A Pod3

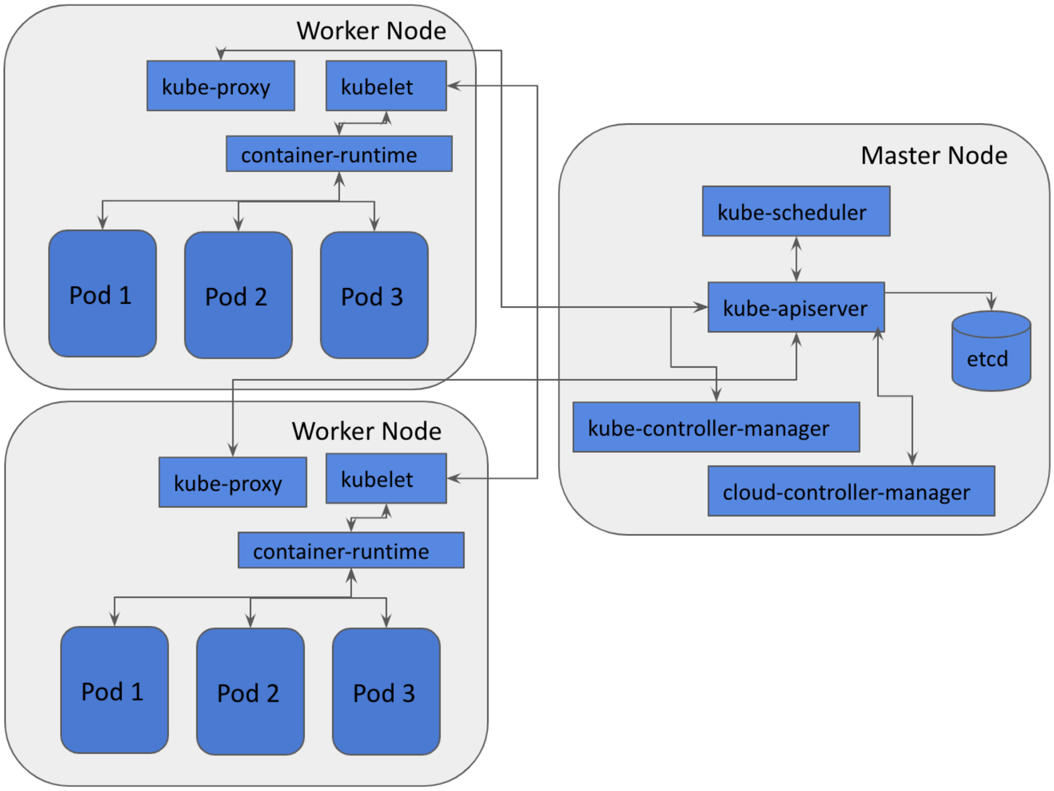

Kube-apiserver
Sync Service endpoint objects
Pod A
Kube-proxy
User space
Manage IPVS rules
Kernel space
Sc A virtual IP
Linux Virtual Server
Node
Svc A Pod1
Svc A Pod2
Svc A Pod3

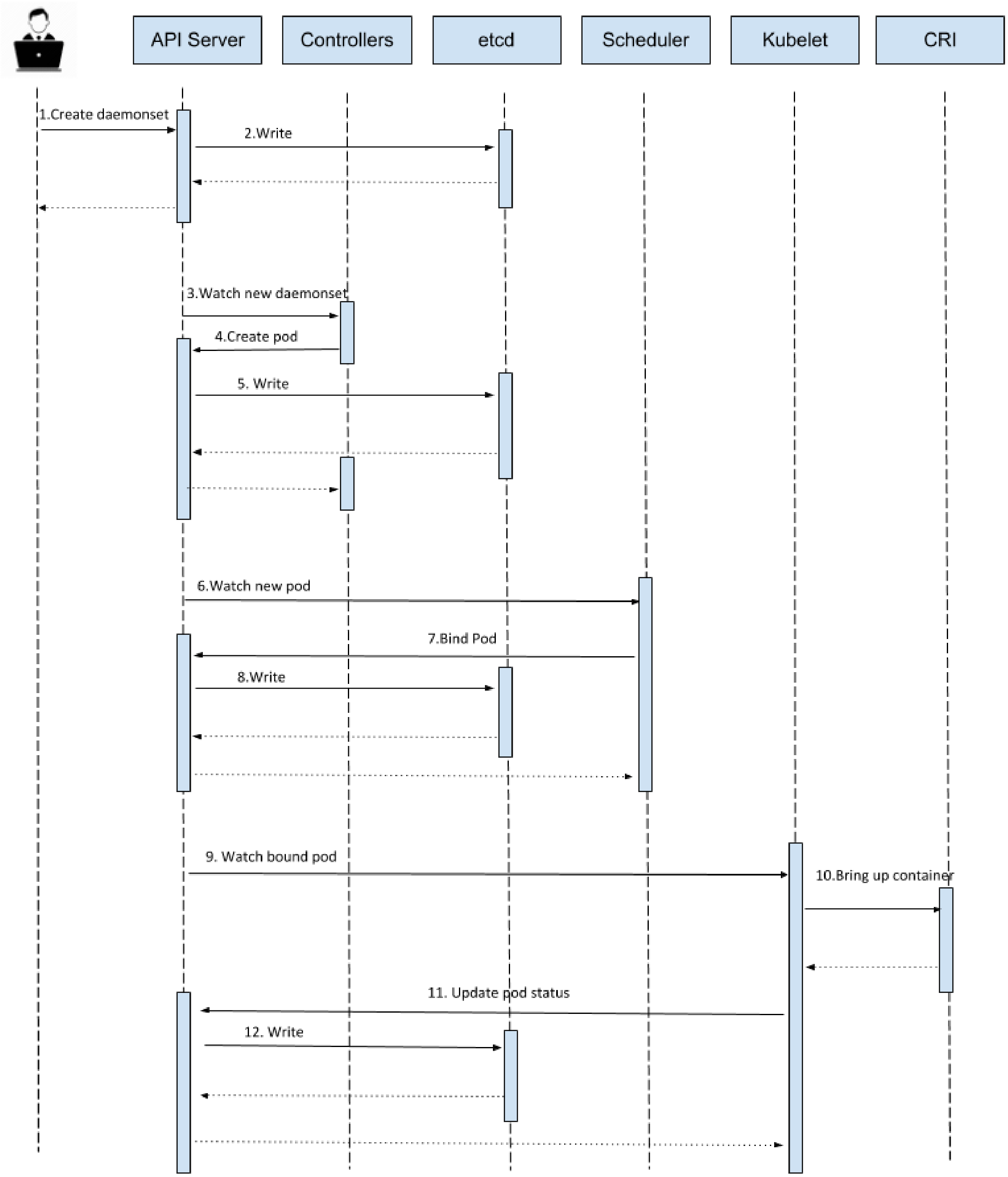
CNI	Encryption	Network Policies
Calico	😐 No	😁 **Ingress + Egress**
Canal	😐 No	😁 **Ingress + Egress**
Cilium	😁 **Yes**	😁 **Ingress + Egress**
Flannel	😐 No	😠 No
Kube-router	😐 No	😐 Ingress only
WeaveNet	😁 **Yes**	😁 **Ingress + Egress**

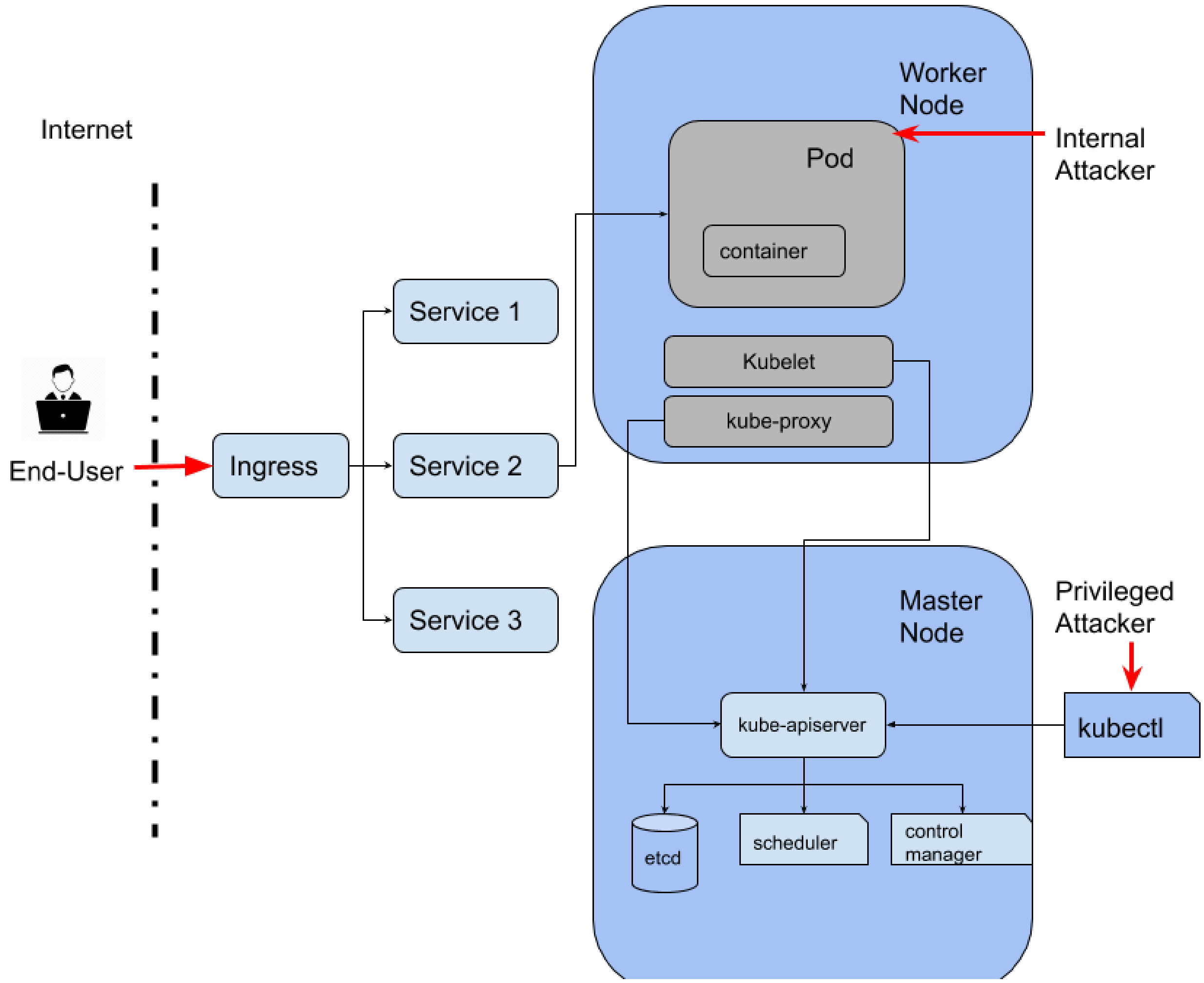
- Blue = Fair

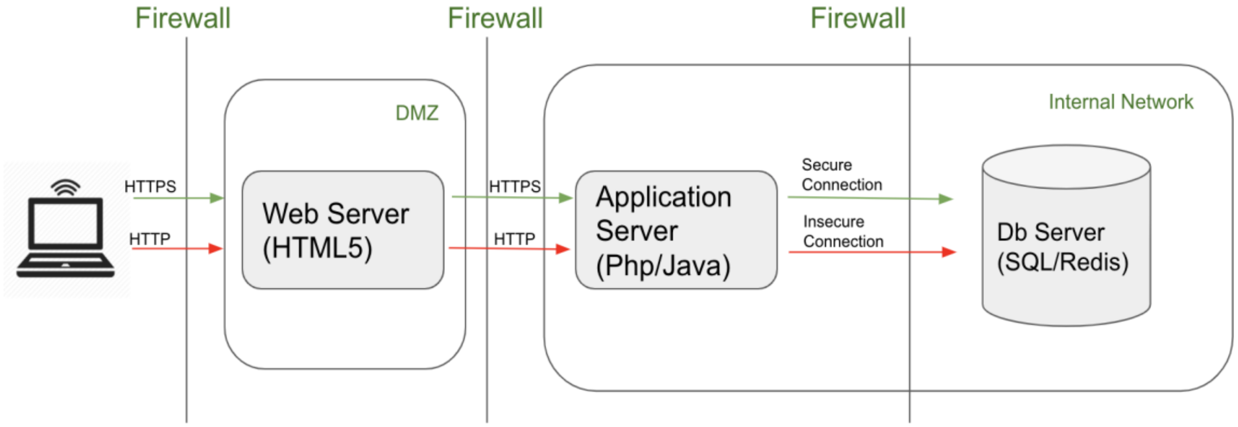


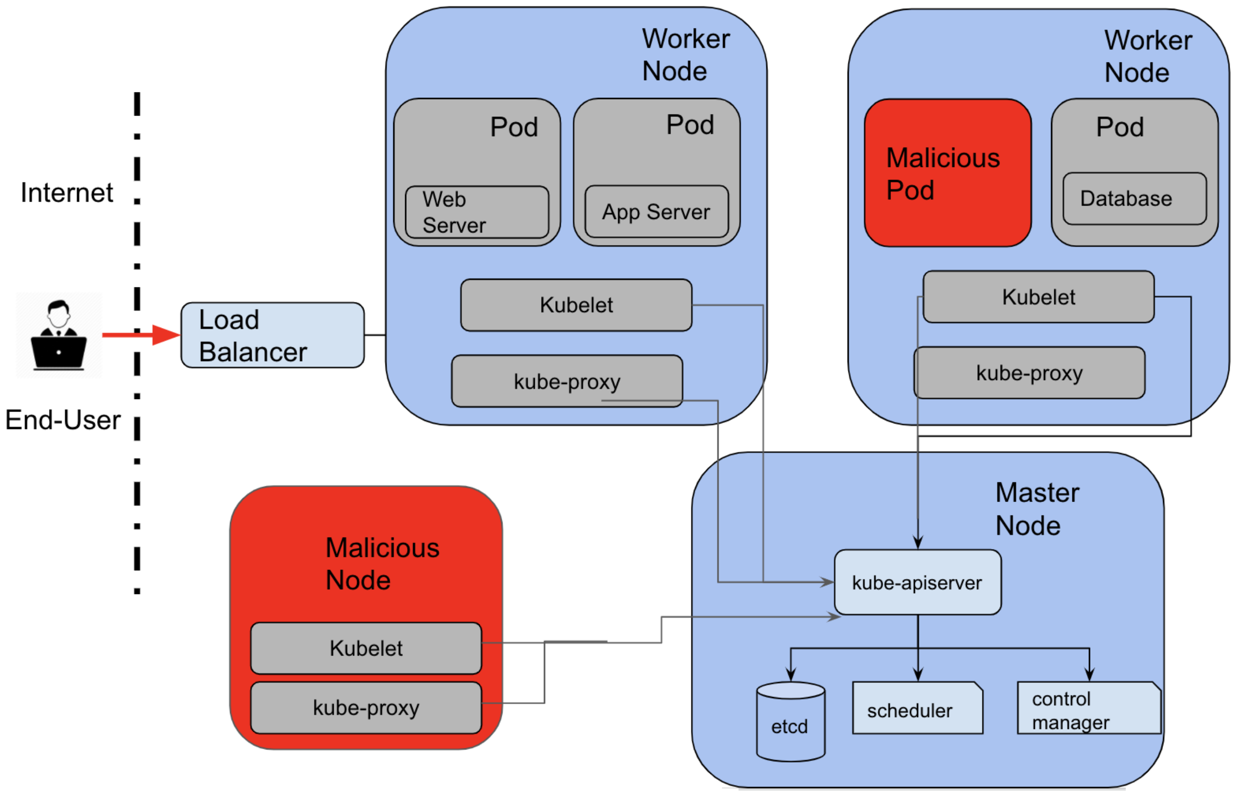
Chapter 3: Threat Modeling



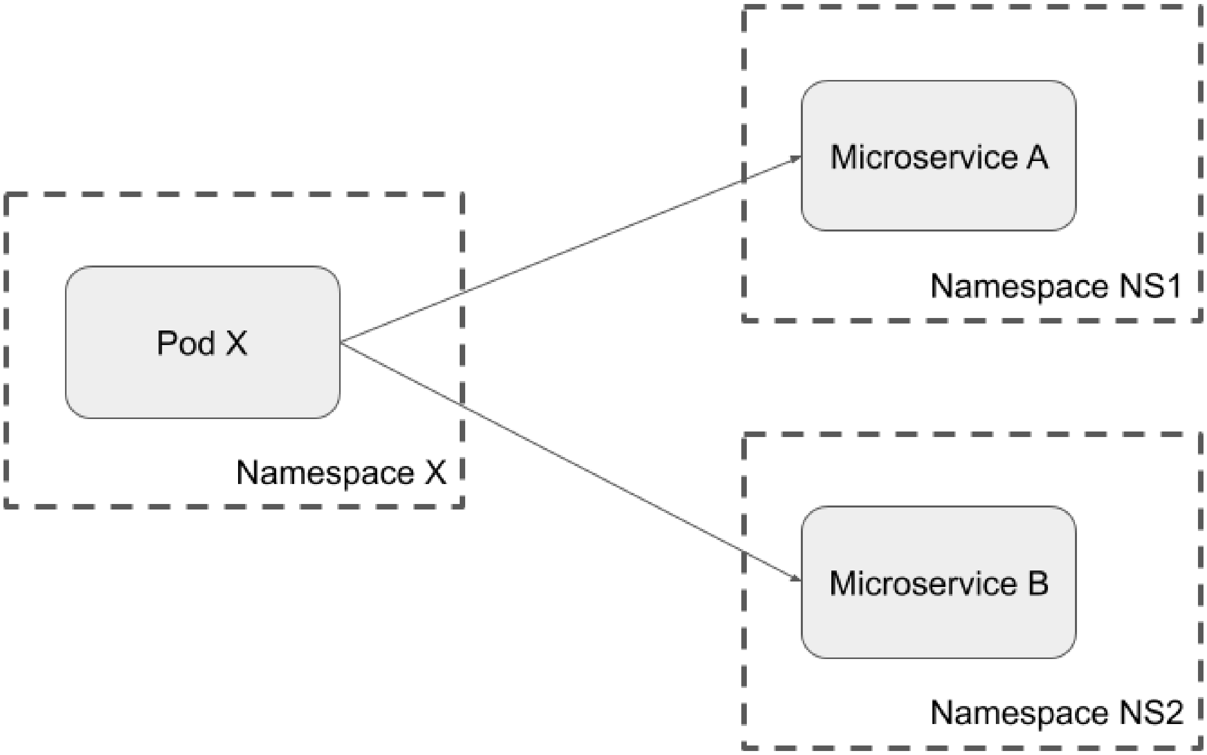

API Server
Controllers
etcd
Scheduler
Kubelet
CRI
1.Create daemonset
2.Write
3.Watch new daemonset
4.Create pod
5. Write
6.Watch new pod
7.Bind Pod
8.Write
9. Watch bound pod
10.Bring up container
11. Update pod status
12. Write

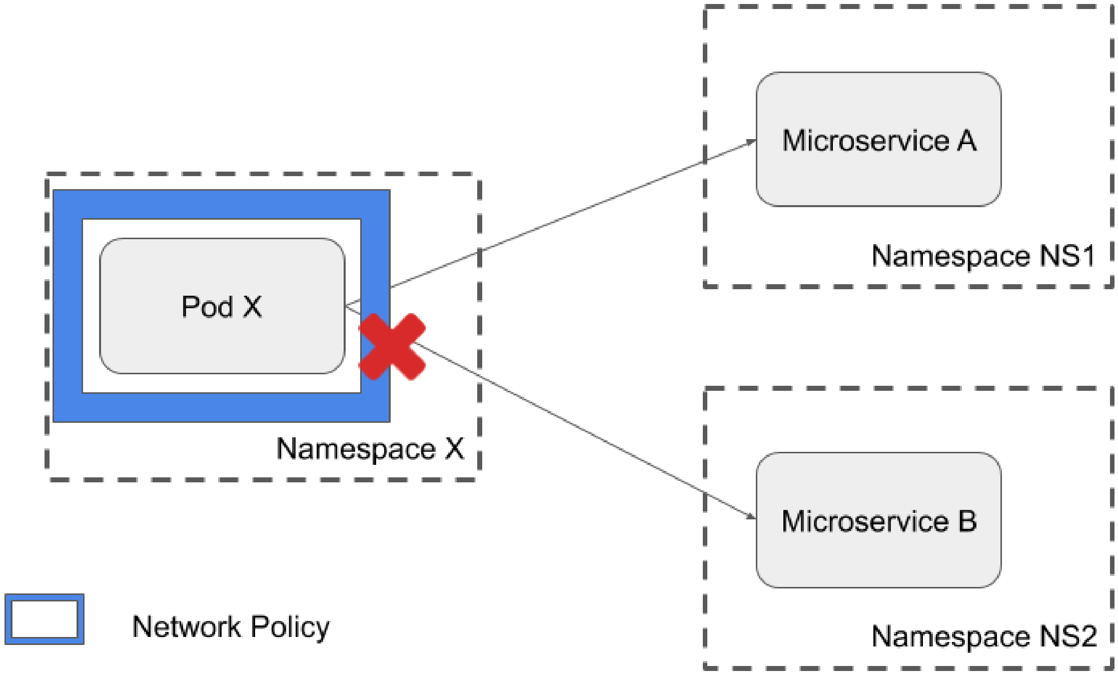

Internet
End-User
Ingress
Service 1
Service 2
Service 3
Worker Node
Pod
container
Kubelet
kube-proxy
Internal Attacker
Master Node
Privileged Attacker
kubectl
kube-apiserver
etcd
scheduler
control manager


Firewall
Firewall
Firewall
DMZ
Internal Network
HTTPS
HTTP
Web Server (HTML5)
HTTPS
HTTP
Application Server (Php/Java)
Secure Connection
Insecure Connection
Db Server (SQL/Redis)

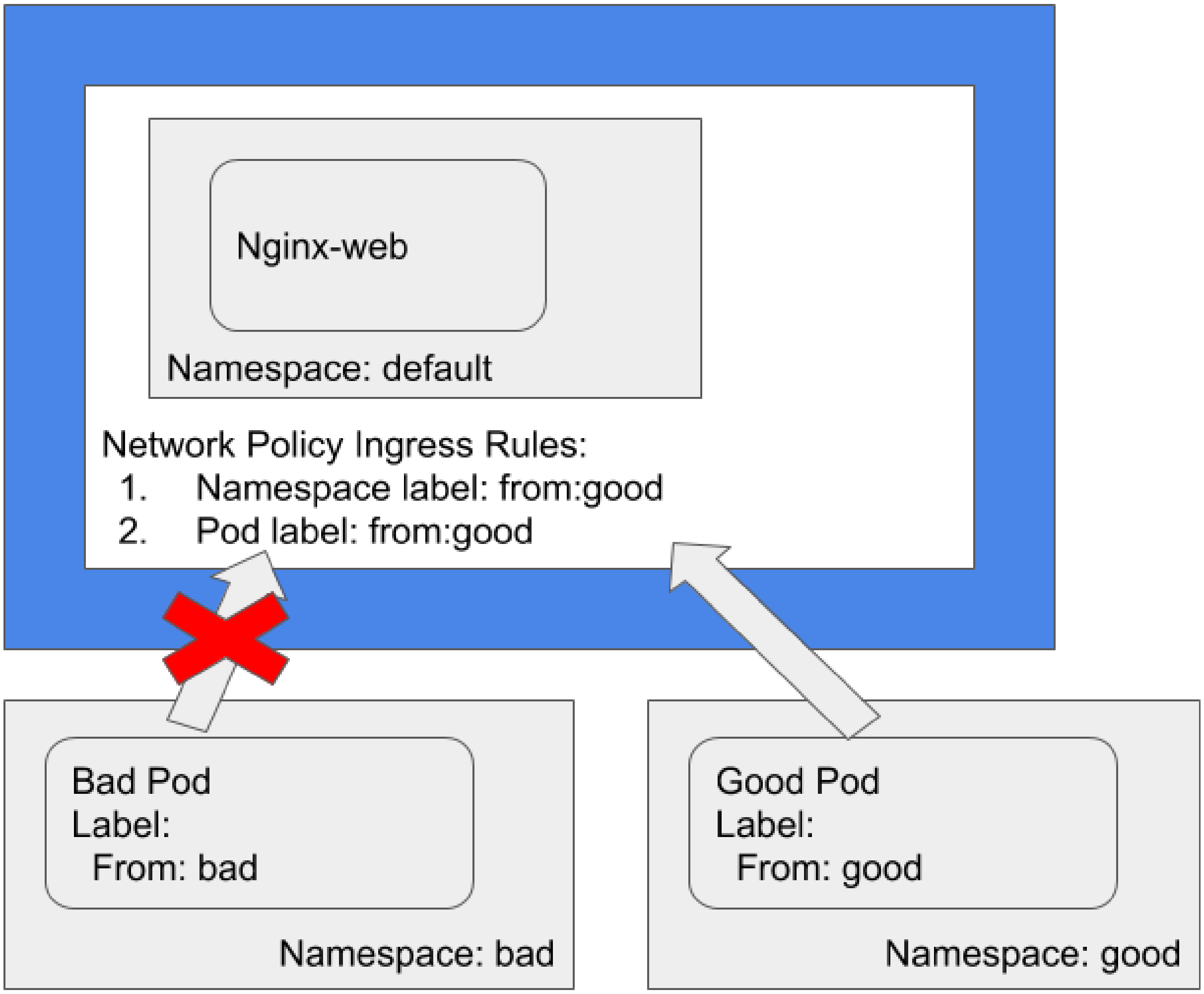

Internet
End-User
Load Balancer
Worker Node
Pod
Web Server
Pod
App Server
Kubelet
kube-proxy
Worker Node
Malicious Pod
Pod
Database
Kubelet
kube-proxy
Malicious Node
Kubelet
kube-proxy
Master Node
kube-apiserver
etcd
scheduler
control manager

Chapter 4: Applying the Principle of Least Privilege in Kubernetes

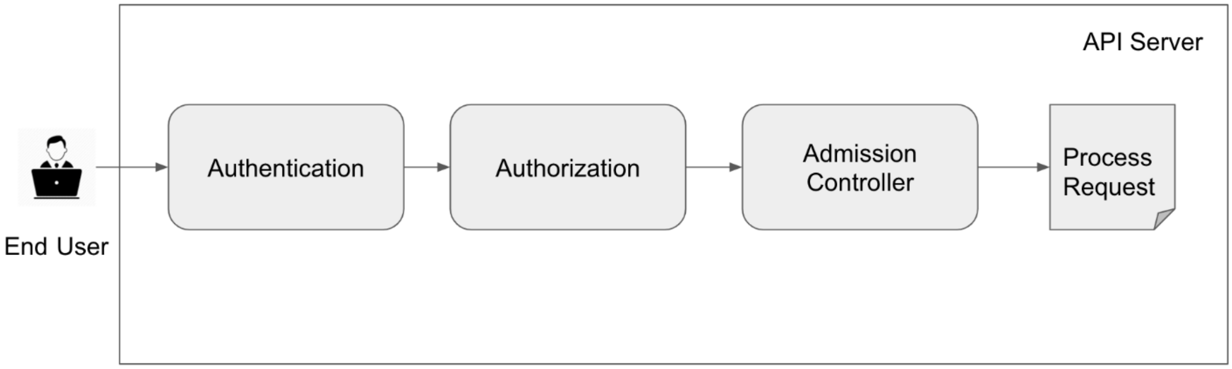


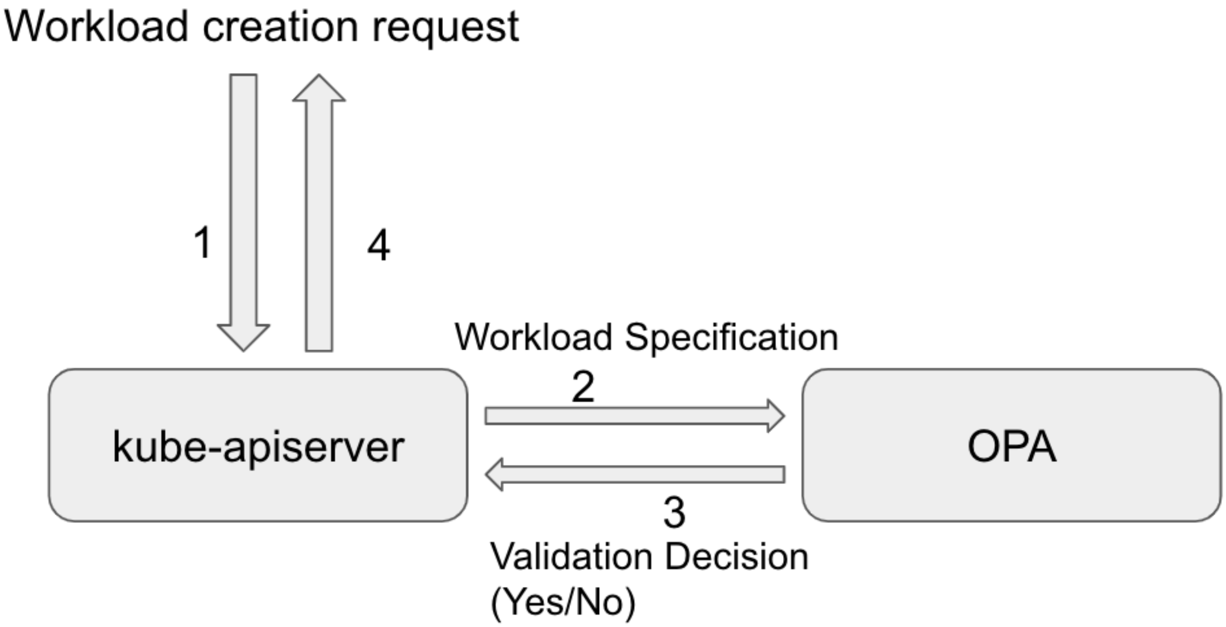


Chapter 5: Configuring Kubernetes Security Boundaries

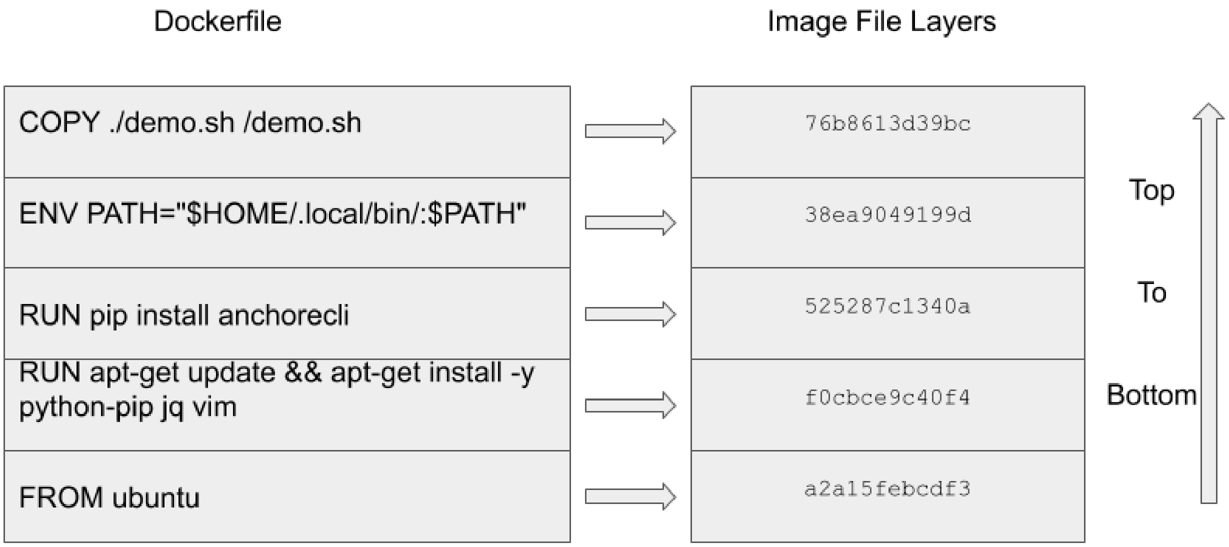


Chapter 7: Authentication, Authorization, and Admission Control

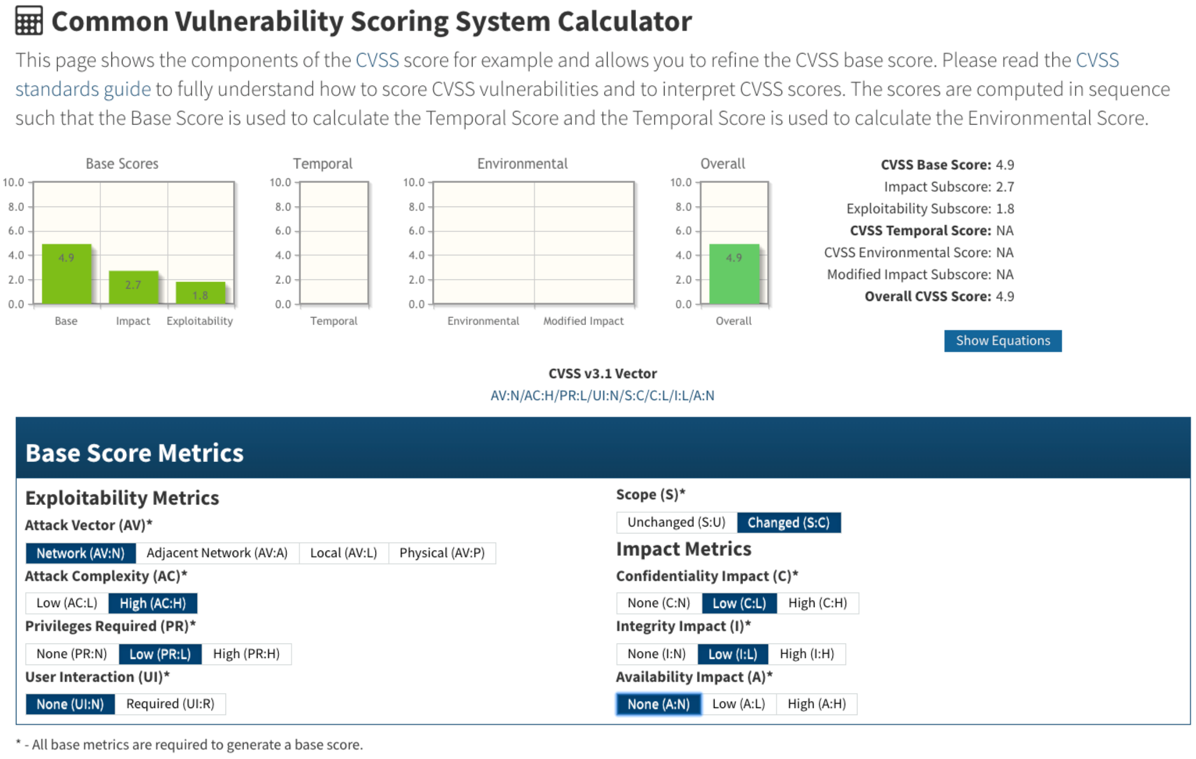




Chapter 9: Image Scanning in DevOps Pipelines



```
COPY ./demo.sh /demo.sh
ENV PATH="$HOME/.local/bin/:$PATH"
RUN pip install anchorecli
RUN apt-get update && apt-get install -y
python-pip jq vim
FROM ubuntu
```



Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 4.9
Impact Subscore: 2.7
Exploitability Subscore: 1.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 4.9

CVSS v3.1 Vector
AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) [✓ High (AC:H)]

Privileges Required (PR)*
None (PR:N) [✓ Low (PR:L)] High (PR:H)

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
Unchanged (S:U) [✓ Changed (S:C)]

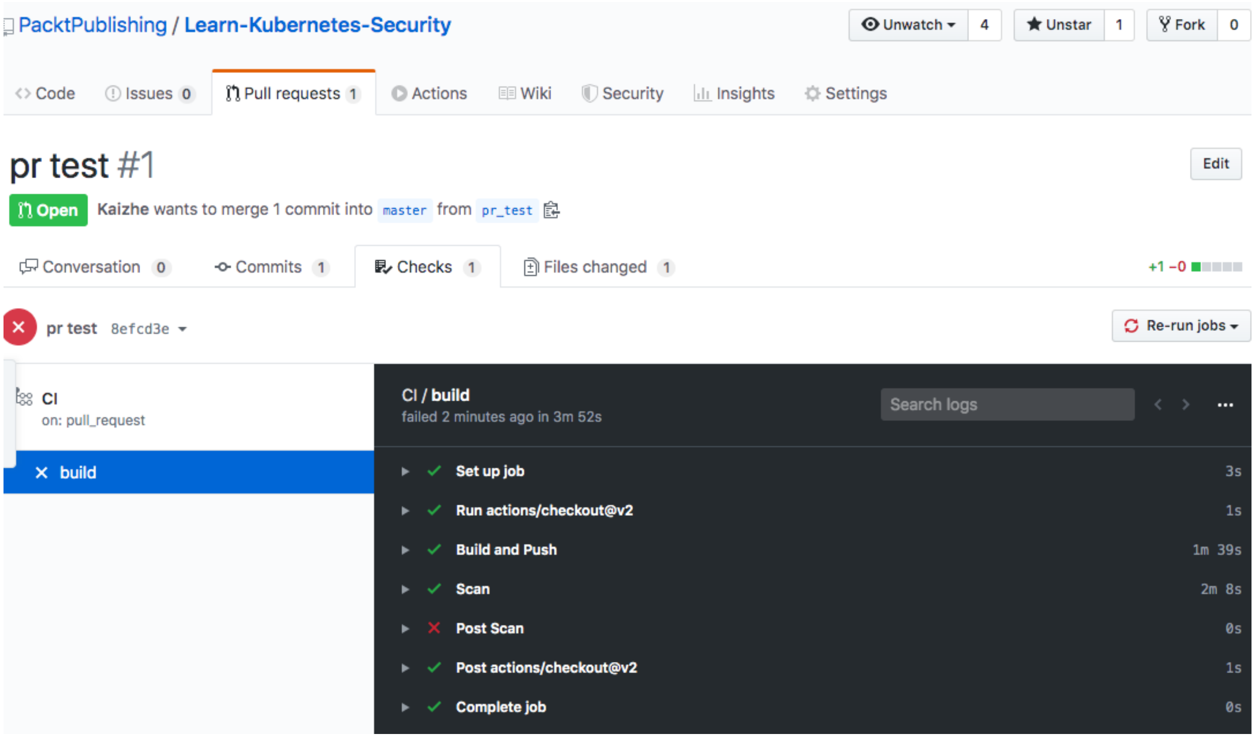
Impact Metrics

Confidentiality Impact (C)*
None (C:N) [✓ Low (C:L)] High (C:H)

Integrity Impact (I)*
None (I:N) [✓ Low (I:L)] High (I:H)

Availability Impact (A)*
[✓ None (A:N)] Low (A:L) High (A:H)

* - All base metrics are required to generate a base score.



pr test #1

Open Kaizhe wants to merge 1 commit into `master` from `pr_test`

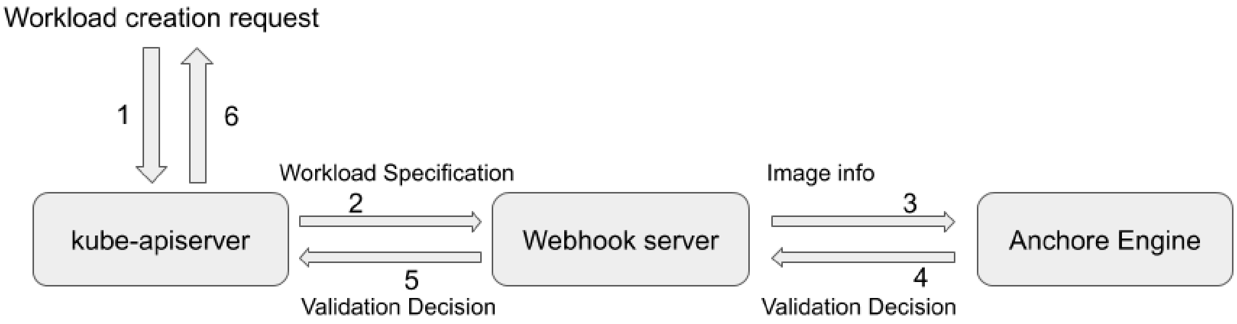
pr test 8efcd3e

CI
on: pull_request

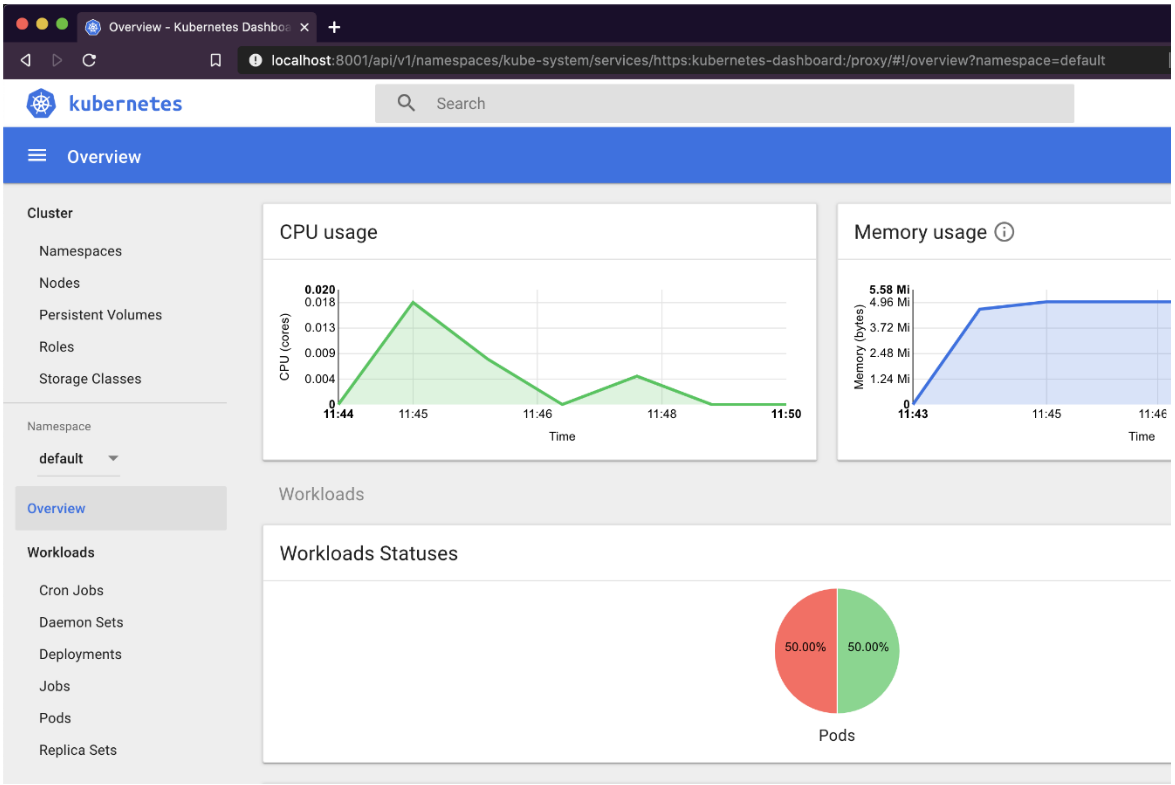
build

CI / build
failed 2 minutes ago in 3m 52s

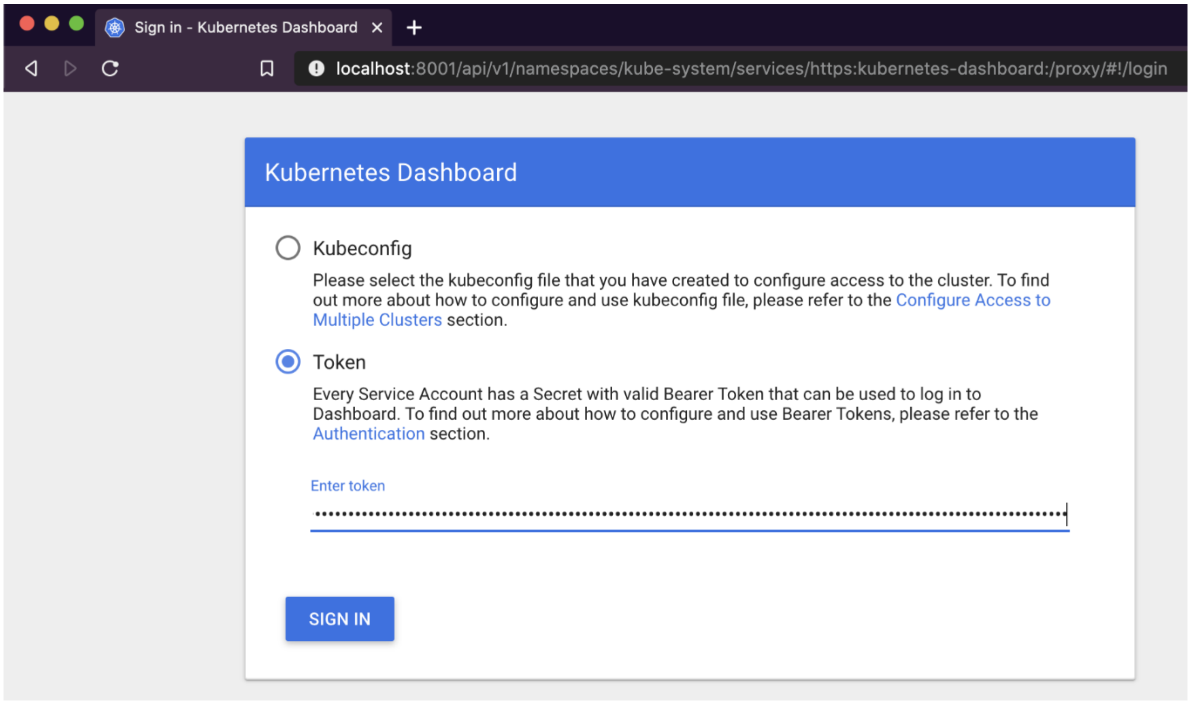
```
▸ ✓ Set up job                      3s
▸ ✓ Run actions/checkout@v2         1s
▸ ✓ Build and Push              1m 39s
▸ ✓ Scan                         2m 8s
▸ ✗ Post Scan                       0s
▸ ✓ Post actions/checkout@v2        1s
▸ ✓ Complete job                    0s
```



Chapter 10: Real-Time Monitoring and Resource Management of a Kubernetes Cluster



localhost:8001/api/v1/namespaces/kube-system/services/https:kubernetes-dashboard:/proxy/#!/overview?namespace=default



localhost:8001/api/v1/namespaces/kube-system/services/https:kubernetes-dashboard:/proxy/#!/login

Kubernetes Dashboard

○ Kubeconfig

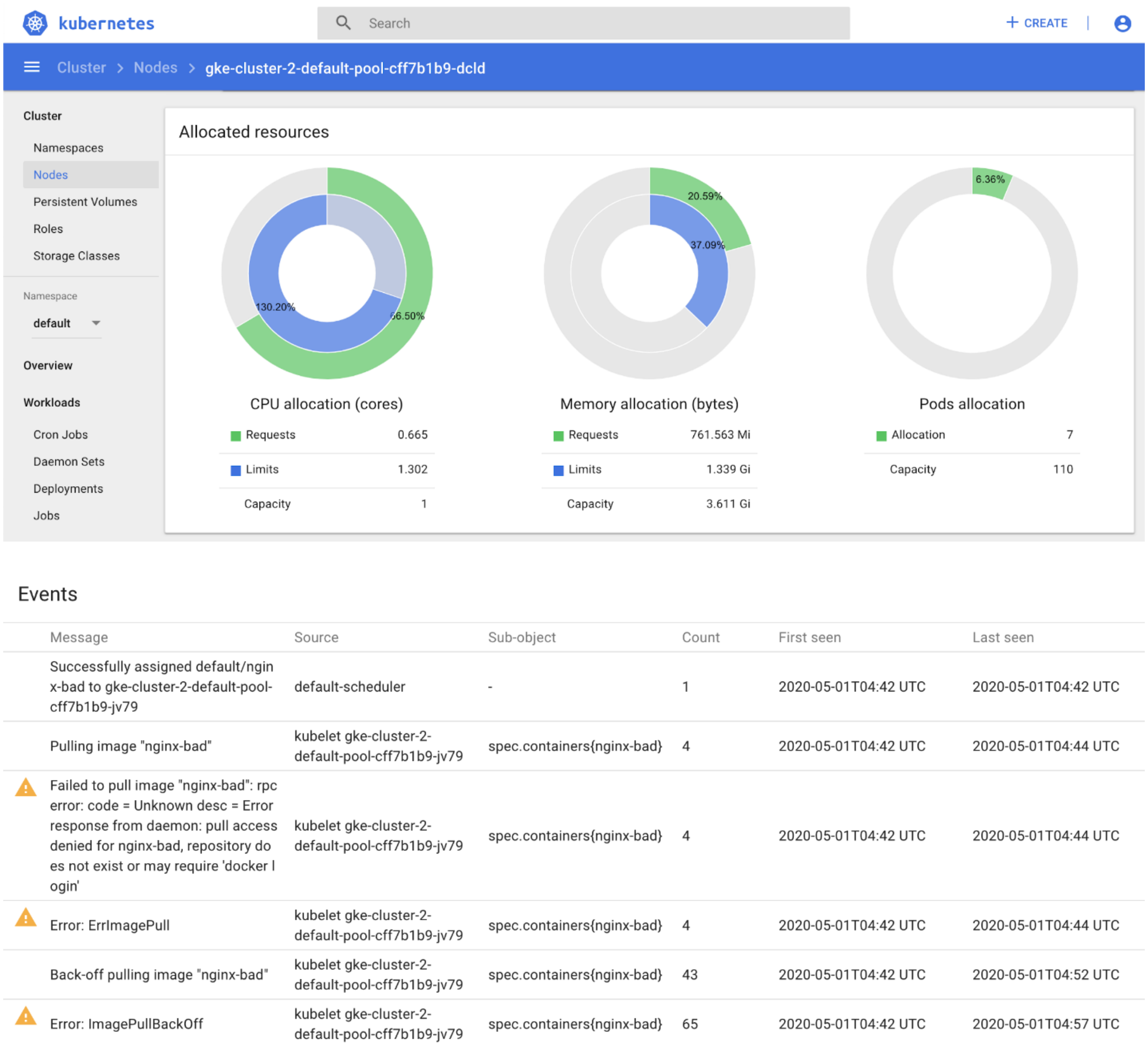
Please select the kubeconfig file that you have created to configure access to the cluster. To find out more about how to configure and use kubeconfig file, please refer to the Configure Access to Multiple Clusters section.

● Token

Every Service Account has a Secret with valid Bearer Token that can be used to log in to Dashboard. To find out more about how to configure and use Bearer Tokens, please refer to the Authentication section.

Enter token

••



Allocated resources

CPU allocation (cores)

🟩 Requests	0.665
🟦 Limits	1.302
Capacity	1

Memory allocation (bytes)

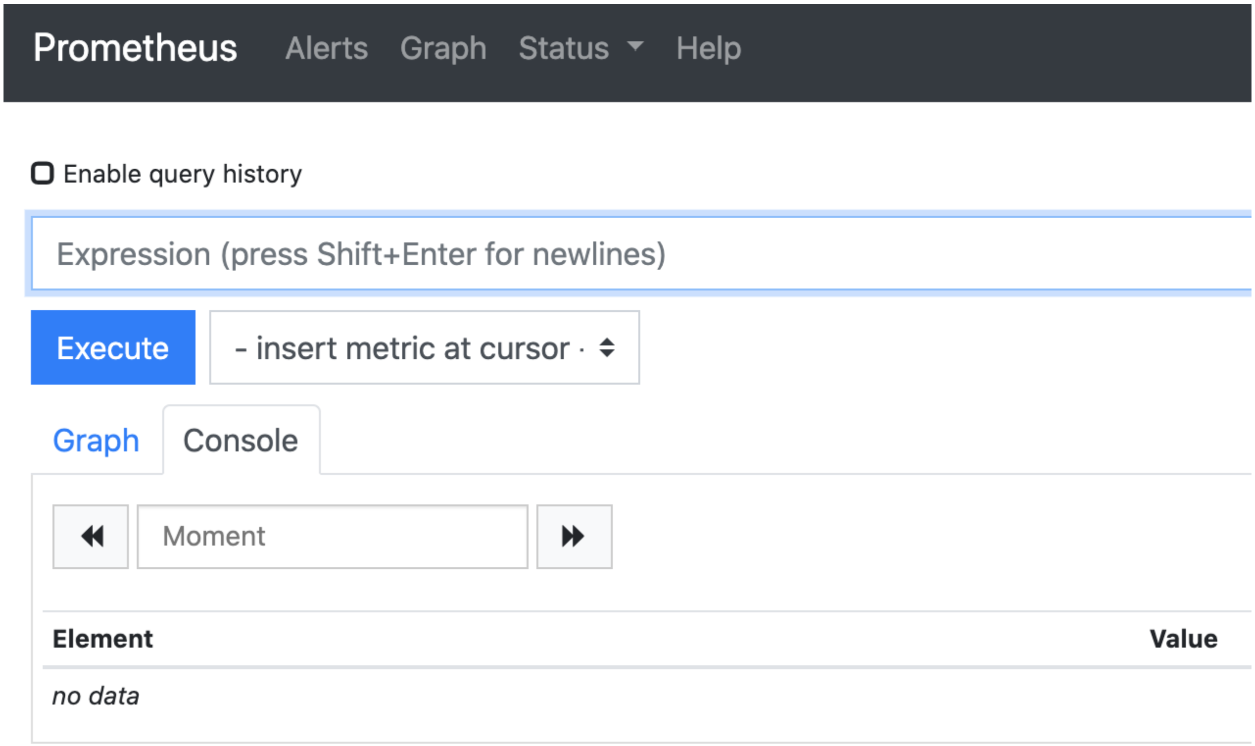
🟩 Requests	761.563 Mi
🟦 Limits	1.339 Gi
Capacity	3.611 Gi

Pods allocation

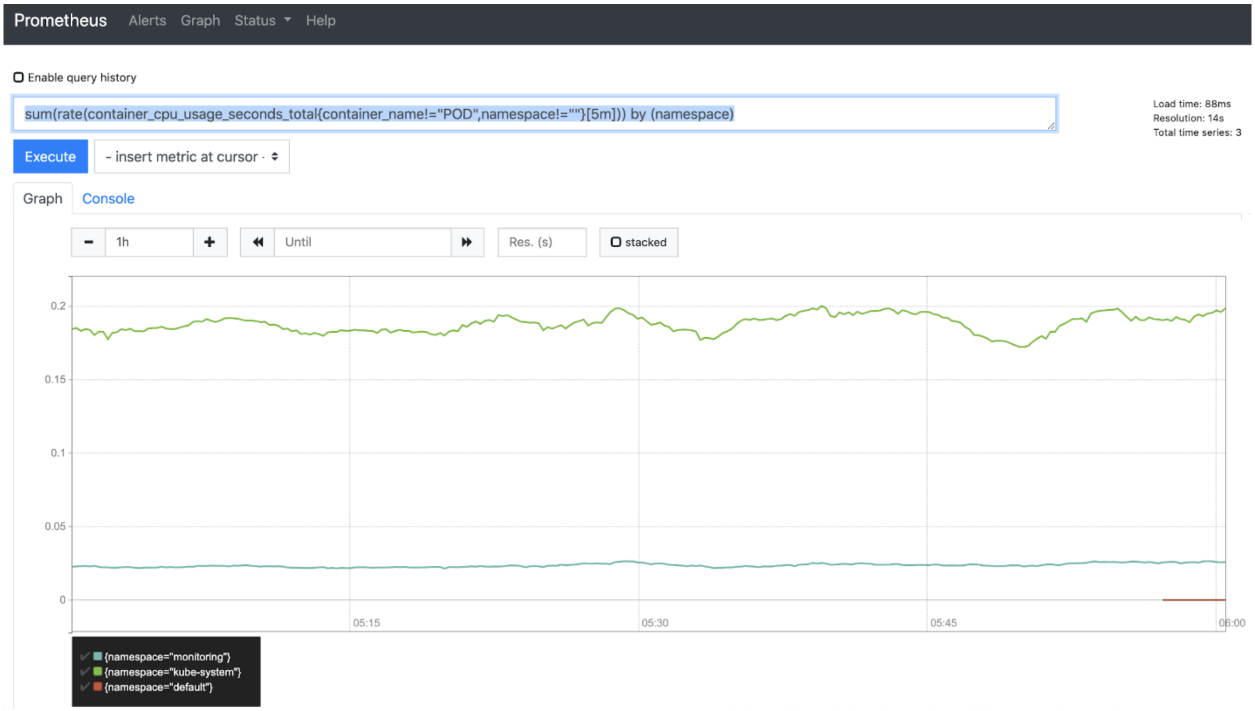
🟩 Allocation	7
Capacity	110

Events

	Message	Source	Sub-object	Count	First seen	Last seen
	Successfully assigned default/nginx-bad to gke-cluster-2-default-pool-cff7b1b9-jv79	default-scheduler	-	1	2020-05-01T04:42 UTC	2020-05-01T04:42 UTC
	Pulling image "nginx-bad"	kubelet gke-cluster-2-default-pool-cff7b1b9-jv79	spec.containers{nginx-bad}	4	2020-05-01T04:42 UTC	2020-05-01T04:44 UTC
⚠	Failed to pull image "nginx-bad": rpc error: code = Unknown desc = Error response from daemon: pull access denied for nginx-bad, repository does not exist or may require 'docker login'	kubelet gke-cluster-2-default-pool-cff7b1b9-jv79	spec.containers{nginx-bad}	4	2020-05-01T04:42 UTC	2020-05-01T04:44 UTC
⚠	Error: ErrImagePull	kubelet gke-cluster-2-default-pool-cff7b1b9-jv79	spec.containers{nginx-bad}	4	2020-05-01T04:42 UTC	2020-05-01T04:44 UTC
	Back-off pulling image "nginx-bad"	kubelet gke-cluster-2-default-pool-cff7b1b9-jv79	spec.containers{nginx-bad}	43	2020-05-01T04:42 UTC	2020-05-01T04:52 UTC
⚠	Error: ImagePullBackOff	kubelet gke-cluster-2-default-pool-cff7b1b9-jv79	spec.containers{nginx-bad}	65	2020-05-01T04:42 UTC	2020-05-01T04:57 UTC

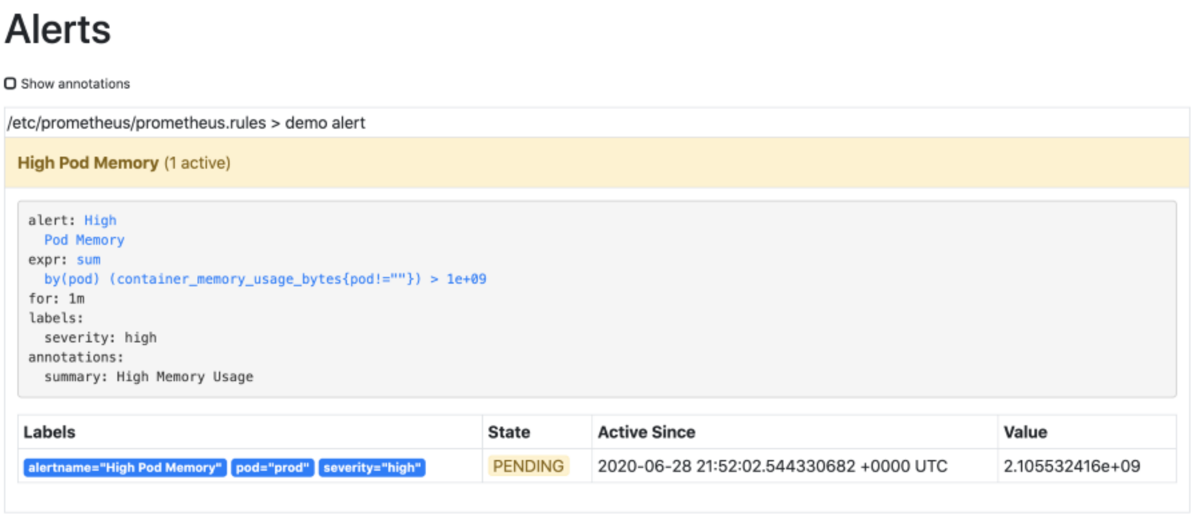


Element	Value
no data	



```
sum(rate(container_cpu_usage_seconds_total{container_name!="POD",namespace!=""}[5m])) by (namespace)
```

Load time: 88ms
Resolution: 14s
Total time series: 3



Alerts

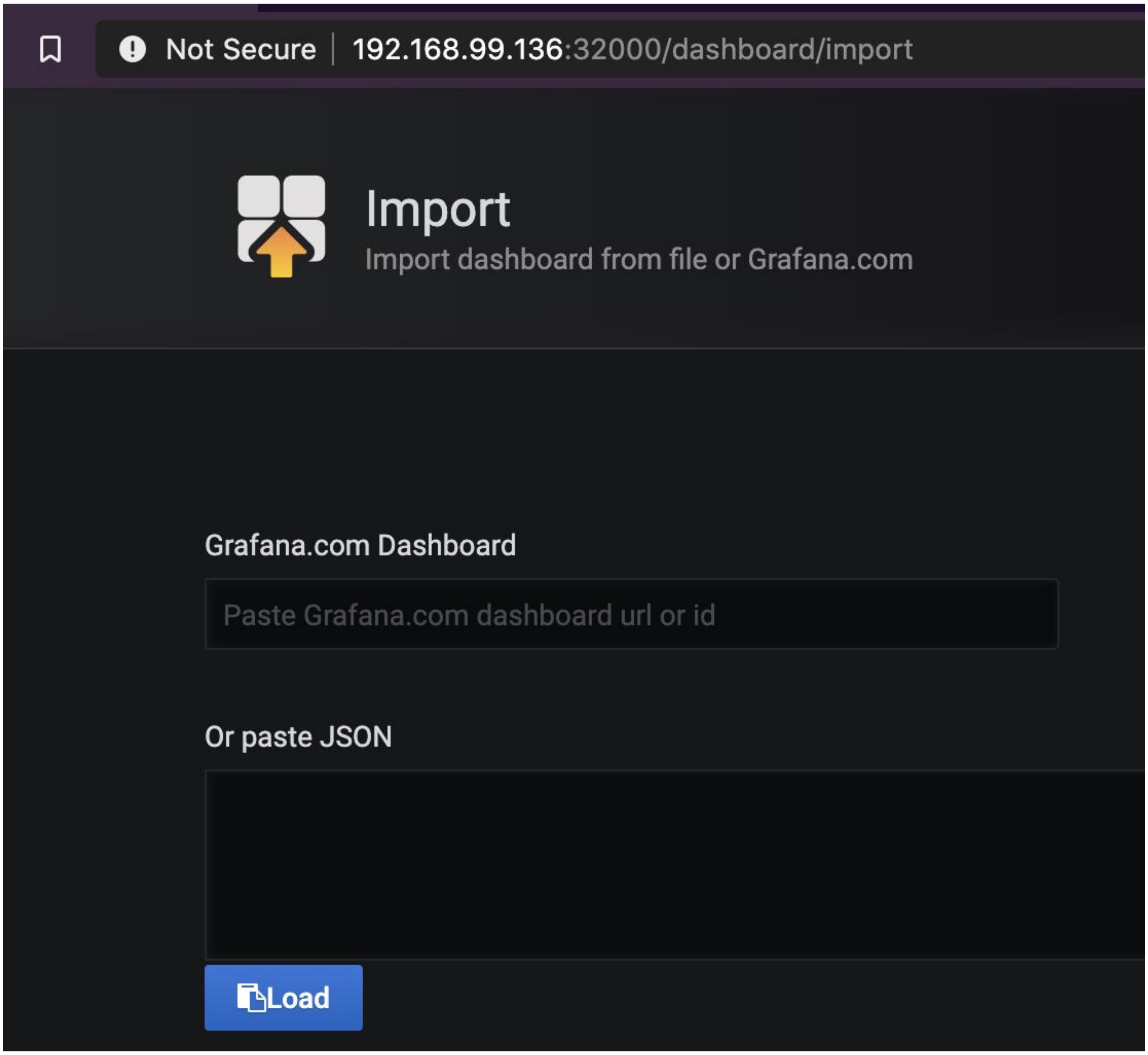
□ Show annotations

/etc/prometheus/prometheus.rules > demo alert

High Pod Memory (1 active)

```
alert: High
  Pod Memory
expr: sum
  by(pod) (container_memory_usage_bytes{pod!=""}) > 1e+09
for: 1m
labels:
  severity: high
annotations:
  summary: High Memory Usage
```

Labels	State	Active Since	Value
alertname="High Pod Memory" pod="prod" severity="high"	PENDING	2020-06-28 21:52:02.544330682 +0000 UTC	2.105532416e+09



Not Secure
192.168.99.136:32000/dashboard/import

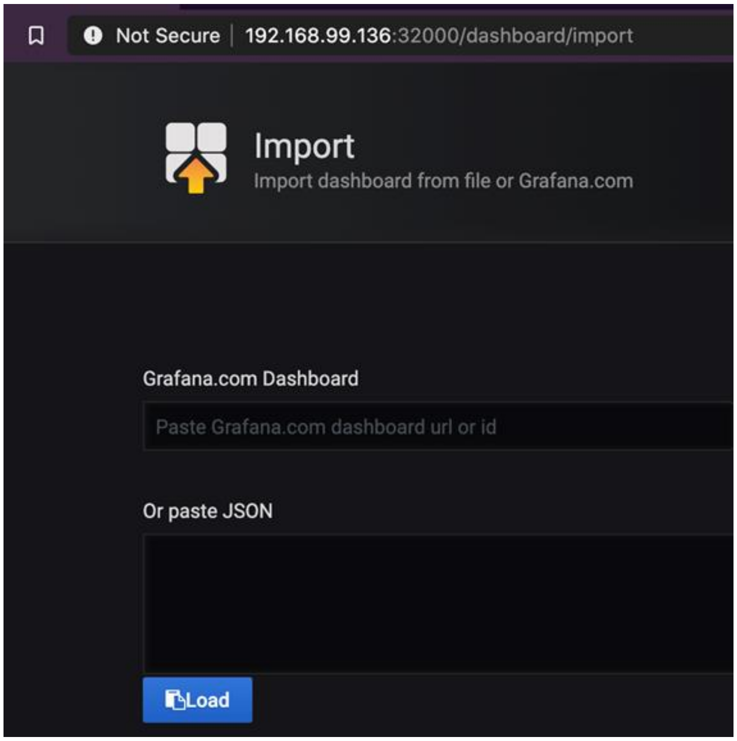
Import

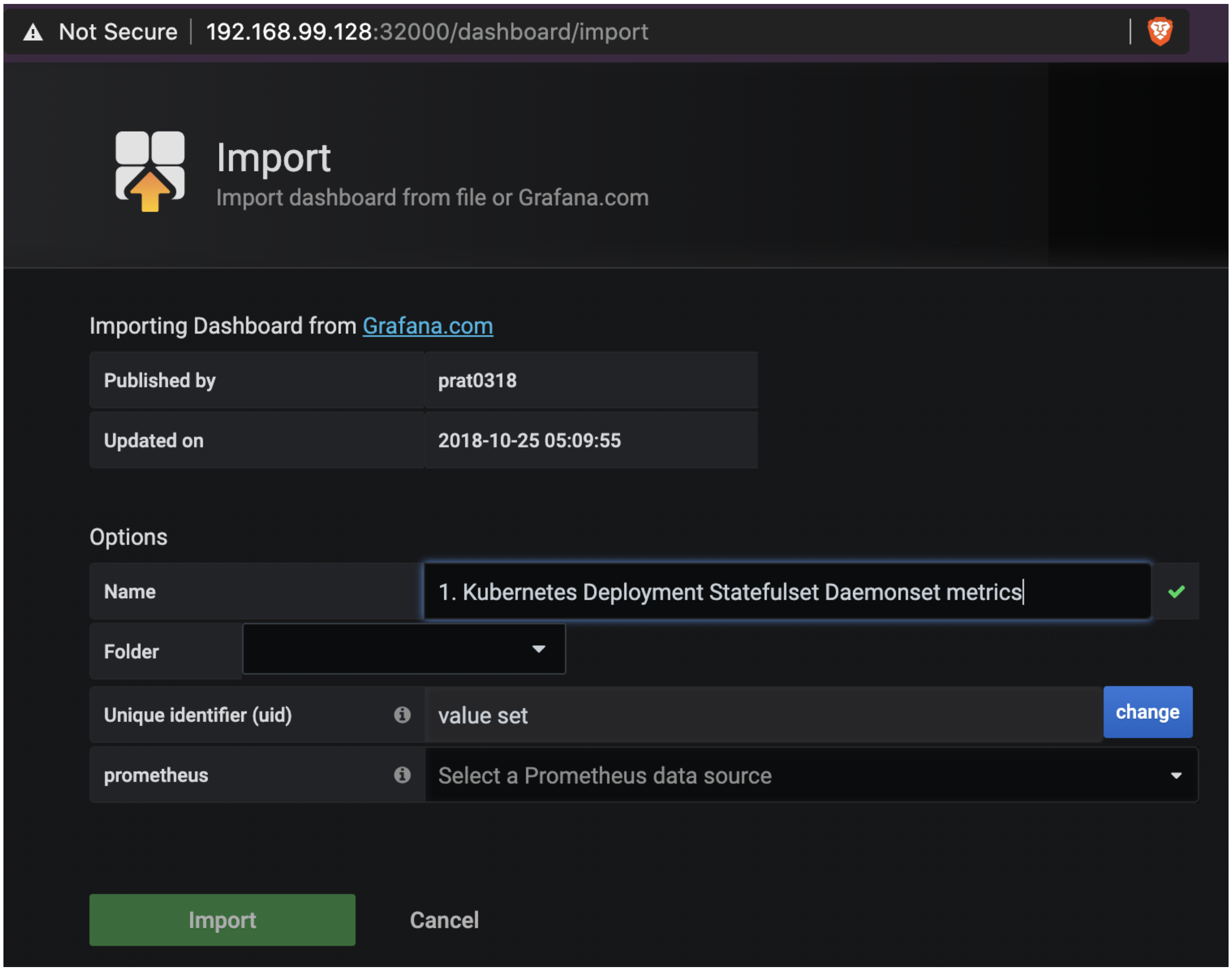
Import dashboard from file or Grafana.com

Grafana.com Dashboard

Paste Grafana.com dashboard url or id

Or paste JSON


Not Secure
192.168.99.136:32000/dashboard/import
Import
Import dashboard from file or Grafana.com
Grafana.com Dashboard
Paste Grafana.com dashboard url or id
Or paste JSON
Load



Not Secure | 192.168.99.128:32000/dashboard/import

Import

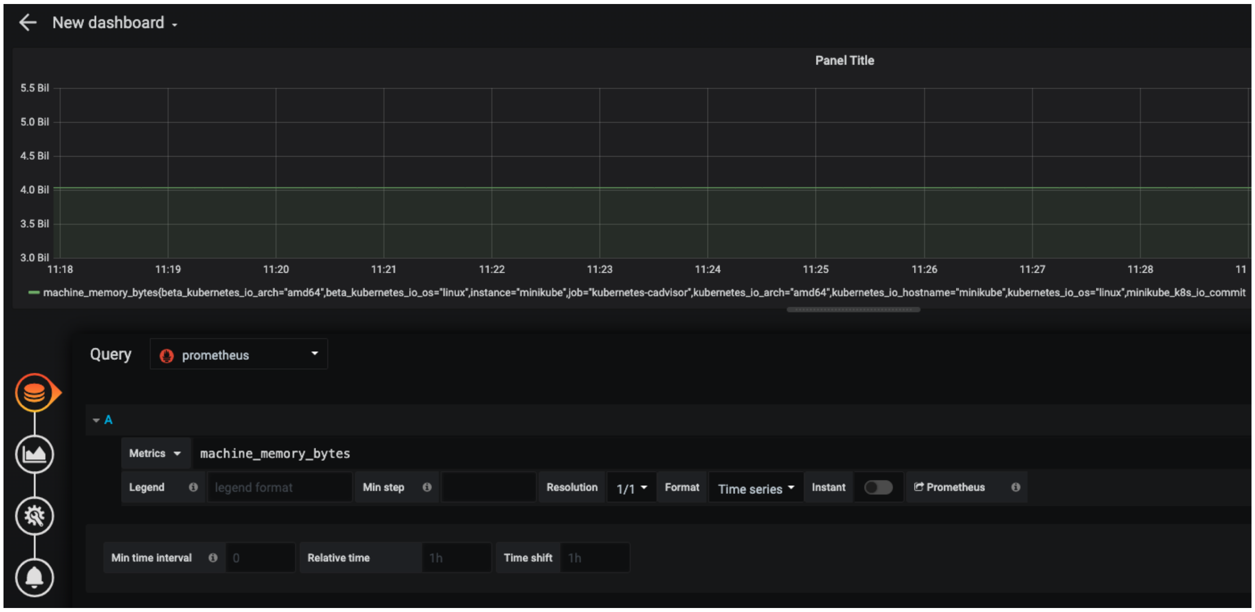
Import dashboard from file or Grafana.com

Importing Dashboard from Grafana.com

Published by	prat0318
Updated on	2018-10-25 05:09:55

Options

Name	1. Kubernetes Deployment Statefulset Daemonset metrics
Folder	
Unique identifier (uid)	value set
prometheus	Select a Prometheus data source



New dashboard

machine_memory_bytes{beta_kubernetes_io_arch="amd64",beta_kubernetes_io_os="linux",instance="minikube",job="kubernetes-cadvisor",kubernetes_io_arch="amd64",kubernetes_io_hostname="minikube",kubernetes_io_os="linux",minikube_k8s_io_commit

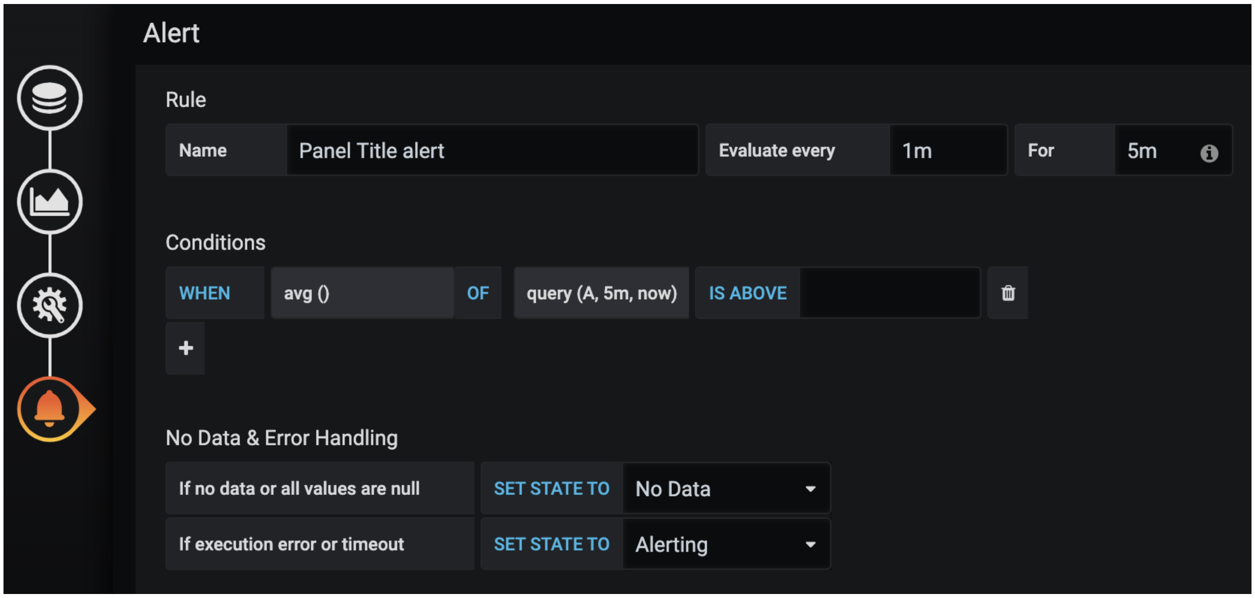
Query: prometheus

A

Metrics: machine_memory_bytes

Legend: legend format | Min step | Resolution: 1/1 | Format: Time series | Instant | Prometheus

Min time interval: 0 | Relative time: 1h | Time shift: 1h



Alert

Rule

Name: Panel Title alert | Evaluate every: 1m | For: 5m

Conditions

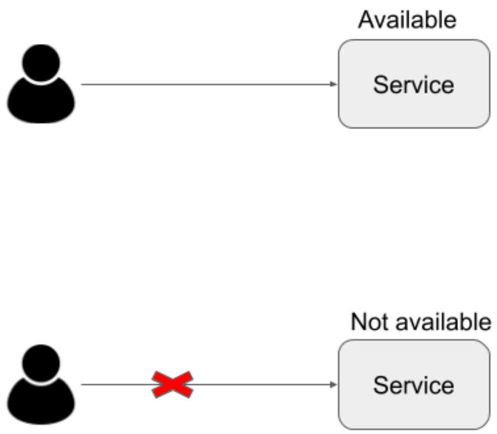
WHEN avg () OF query (A, 5m, now) IS ABOVE

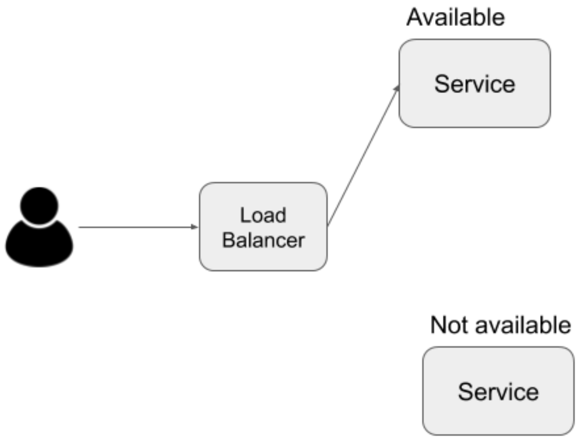
No Data & Error Handling

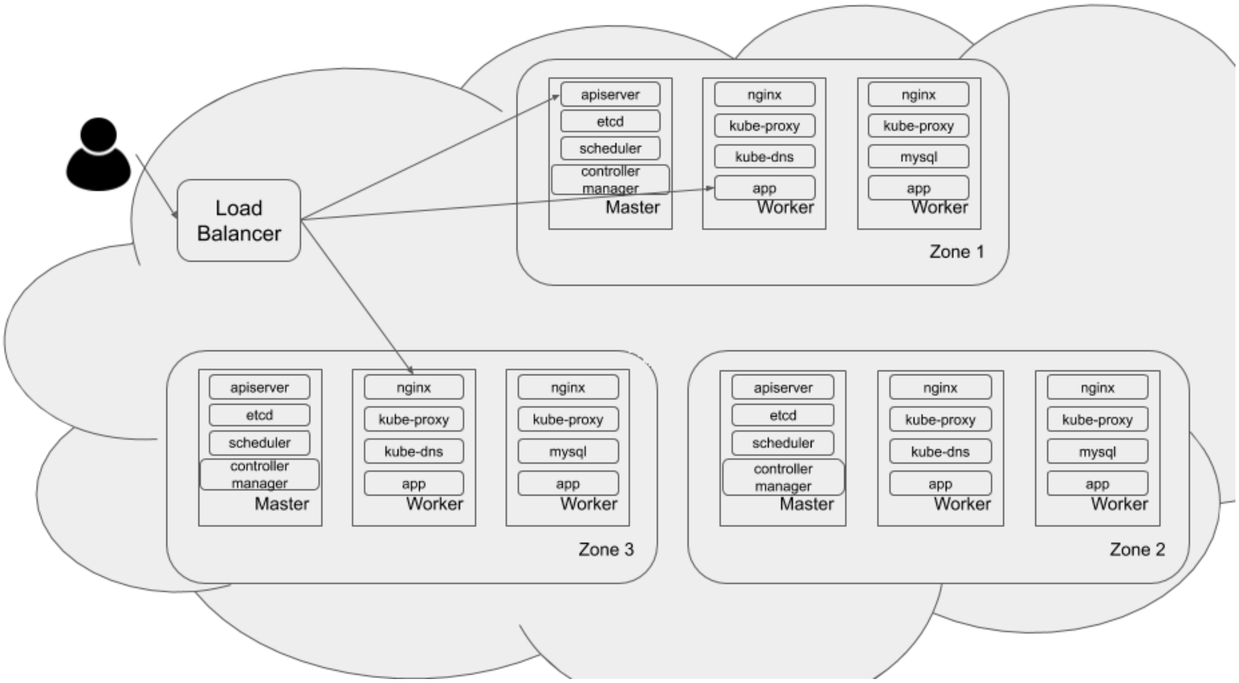
If no data or all values are null SET STATE TO No Data

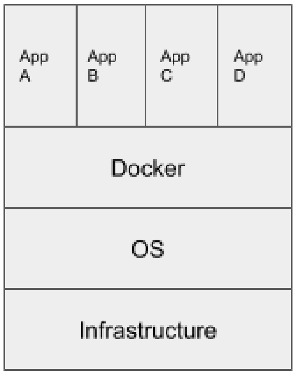
If execution error or timeout SET STATE TO Alerting

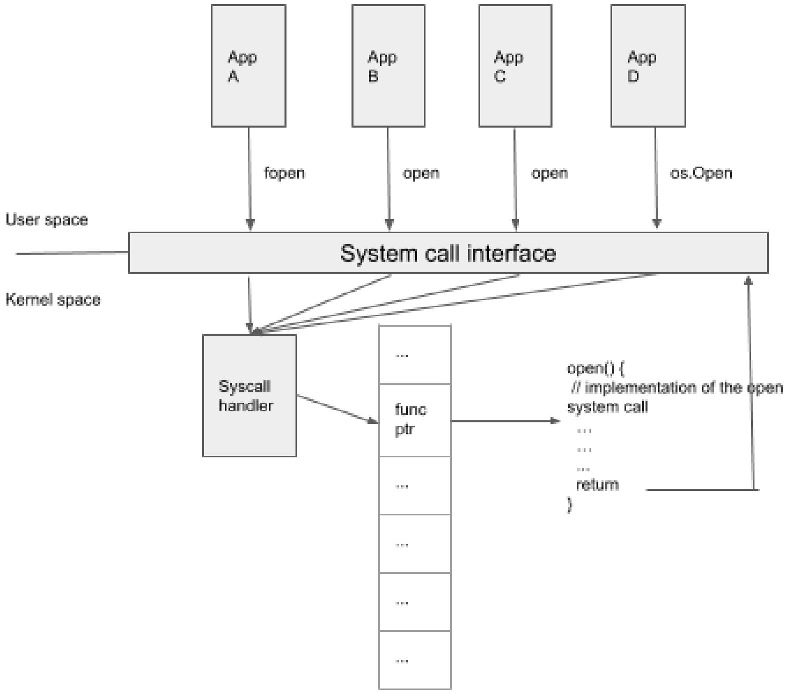
Chapter 11: Defense in Depth



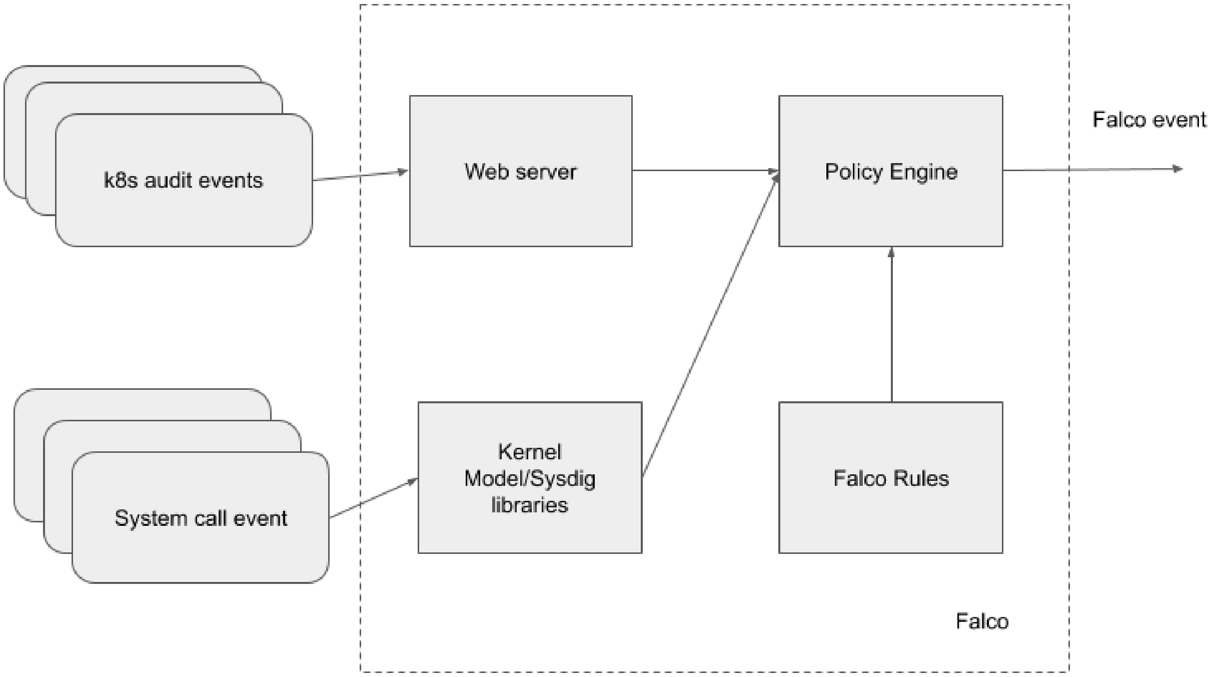


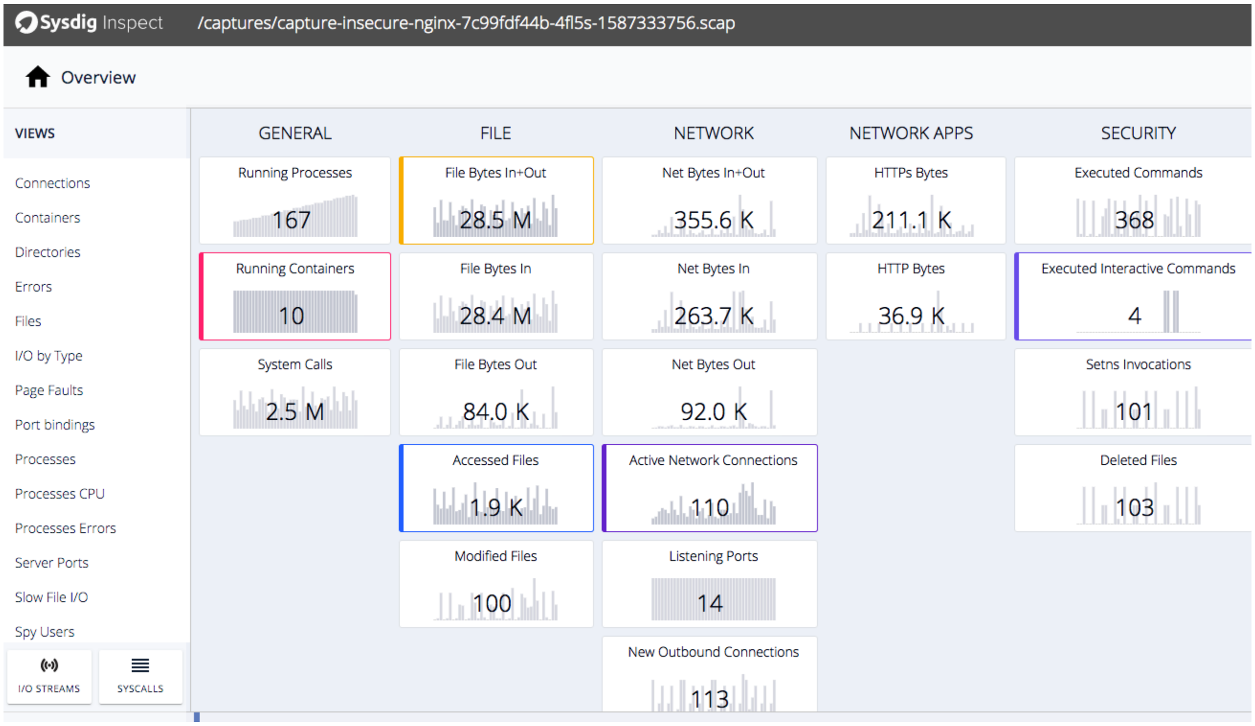






```
open() {
 // implementation of the open
system call
  ...
  ...
  ...
  return
}
```





/captures/capture-insecure-nginx-7c99fdf44b-4fl5s-1587333756.scap

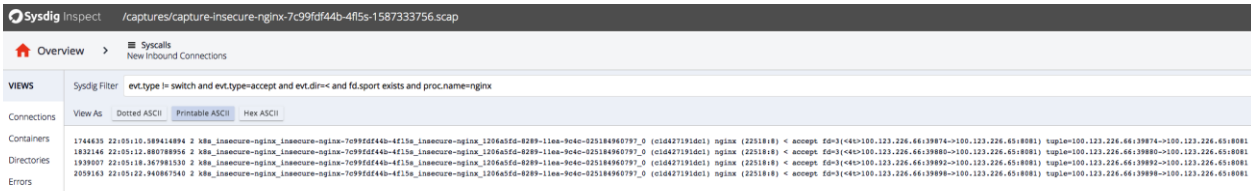
GENERAL
Running Processes 167
Running Containers 10
System Calls 2.5 M

FILE
File Bytes In+Out 28.5 M
File Bytes In 28.4 M
File Bytes Out 84.0 K
Accessed Files 1.9 K
Modified Files 100

NETWORK
Net Bytes In+Out 355.6 K
Net Bytes In 263.7 K
Net Bytes Out 92.0 K
Active Network Connections 110
Listening Ports 14
New Outbound Connections 113

NETWORK APPS
HTTPs Bytes 211.1 K
HTTP Bytes 36.9 K

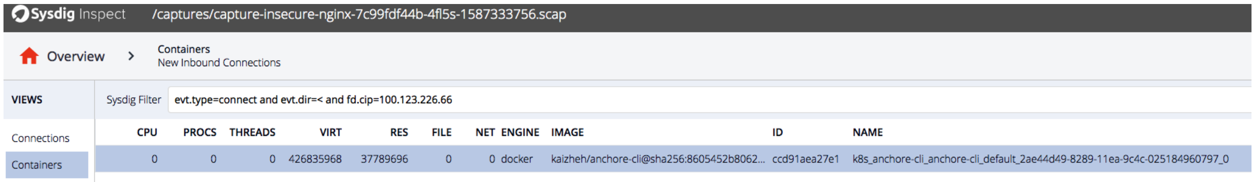
SECURITY
Executed Commands 368
Executed Interactive Commands 4
Setns Invocations 101
Deleted Files 103



/captures/capture-insecure-nginx-7c99fdf44b-4fl5s-1587333756.scap

Sysdig Filter: evt.type != switch and evt.type=accept and evt.dir=< and fd.sport exists and proc.name=nginx

```
1744635 22:05:10.589414894 2 k8s_insecure-nginx_insecure-nginx-7c99fdf44b-4fl5s_insecure-nginx_1206a5fd-8289-11ea-9c4c-025184960797_0 (c1d427191dc1) nginx (22518:8) < accept fd=3(<4t>100.123.226.66:39874->100.123.226.65:8081) tuple=100.123.226.66:39874->100.123.226.65:8081
1832146 22:05:12.880788956 2 k8s_insecure-nginx_insecure-nginx-7c99fdf44b-4fl5s_insecure-nginx_1206a5fd-8289-11ea-9c4c-025184960797_0 (c1d427191dc1) nginx (22518:8) < accept fd=3(<4t>100.123.226.66:39880->100.123.226.65:8081) tuple=100.123.226.66:39880->100.123.226.65:8081
1939007 22:05:18.367981530 2 k8s_insecure-nginx_insecure-nginx-7c99fdf44b-4fl5s_insecure-nginx_1206a5fd-8289-11ea-9c4c-025184960797_0 (c1d427191dc1) nginx (22518:8) < accept fd=3(<4t>100.123.226.66:39892->100.123.226.65:8081) tuple=100.123.226.66:39892->100.123.226.65:8081
2059163 22:05:22.940867540 2 k8s_insecure-nginx_insecure-nginx-7c99fdf44b-4fl5s_insecure-nginx_1206a5fd-8289-11ea-9c4c-025184960797_0 (c1d427191dc1) nginx (22518:8) < accept fd=3(<4t>100.123.226.66:39898->100.123.226.65:8081) tuple=100.123.226.66:39898->100.123.226.65:8081
```

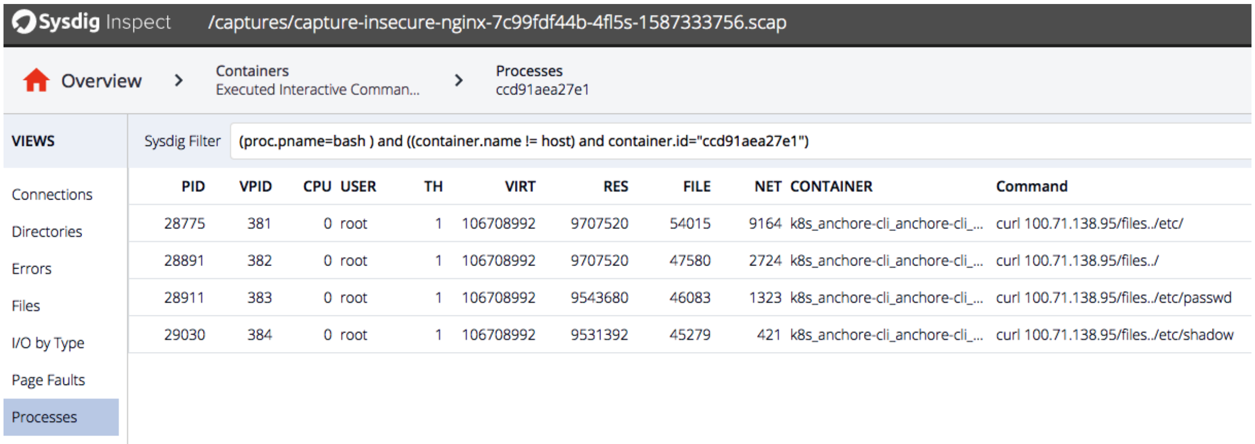


/captures/capture-insecure-nginx-7c99fdf44b-4fl5s-1587333756.scap

Overview > Containers
New Inbound Connections

Sysdig Filter: evt.type=connect and evt.dir=< and fd.cip=100.123.226.66

CPU	PROCS	THREADS	VIRT	RES	FILE	NET	ENGINE	IMAGE	ID	NAME
0	0	0	426835968	37789696	0	0	docker	kaizheh/anchore-cli@sha256:8605452b8062...	ccd91aea27e1	k8s_anchore-cli_anchore-cli_default_2ae44d49-8289-11ea-9c4c-025184960797_0



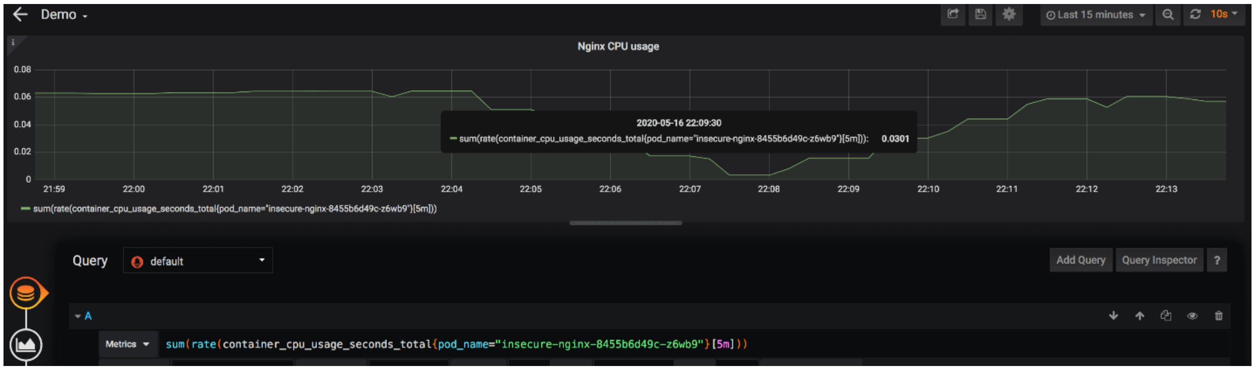
/captures/capture-insecure-nginx-7c99fdf44b-4fl5s-1587333756.scap

Overview > Containers
Executed Interactive Comman... > Processes
ccd91aea27e1

Sysdig Filter: (proc.pname=bash) and ((container.name != host) and container.id="ccd91aea27e1")

PID	VPID	CPU	USER	TH	VIRT	RES	FILE	NET	CONTAINER	Command
28775	381	0	root	1	106708992	9707520	54015	9164	k8s_anchore-cli_anchore-cli_...	curl 100.71.138.95/files../etc/
28891	382	0	root	1	106708992	9707520	47580	2724	k8s_anchore-cli_anchore-cli_...	curl 100.71.138.95/files../
28911	383	0	root	1	106708992	9543680	46083	1323	k8s_anchore-cli_anchore-cli_...	curl 100.71.138.95/files../etc/passwd
29030	384	0	root	1	106708992	9531392	45279	421	k8s_anchore-cli_anchore-cli_...	curl 100.71.138.95/files../etc/shadow

Chapter 12: Analyzing and Detecting Crypto-Mining Attacks

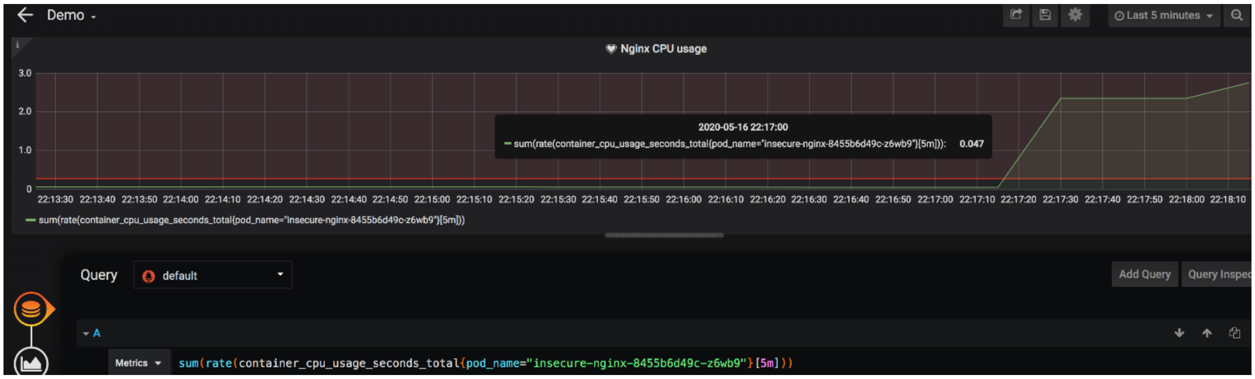


2020-05-16 22:09:30

sum(rate(container_cpu_usage_seconds_total{pod_name="insecure-nginx-8455b6d49c-z6wb9"}[5m])): 0.0301

sum(rate(container_cpu_usage_seconds_total{pod_name="insecure-nginx-8455b6d49c-z6wb9"}[5m]))

```
sum(rate(container_cpu_usage_seconds_total{pod_name="insecure-nginx-8455b6d49c-z6wb9"}[5m]))
```



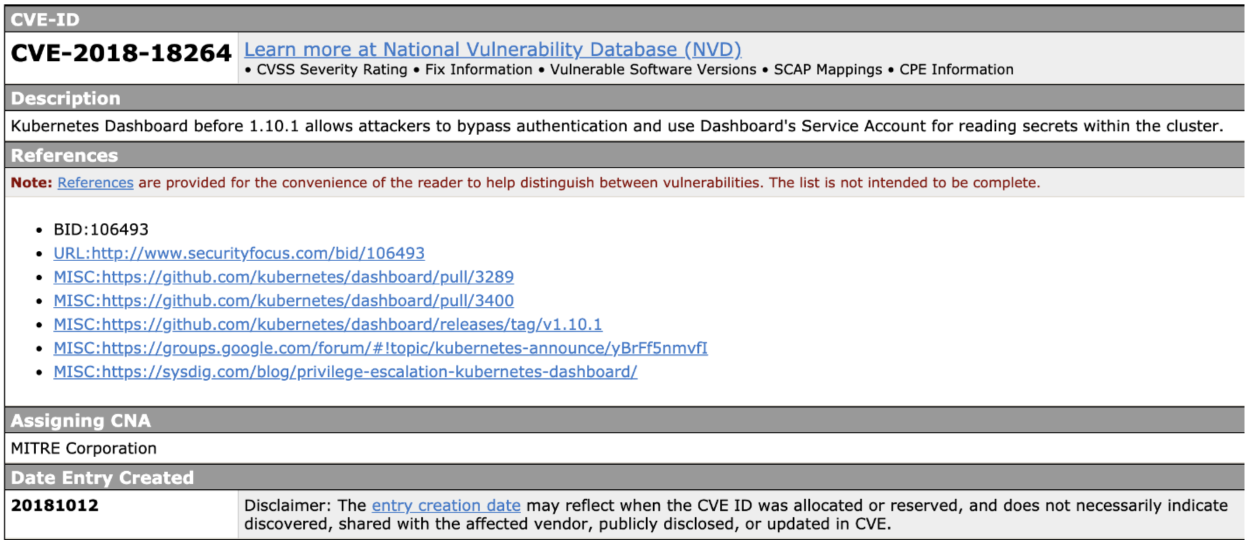
2020-05-16 22:17:00

sum(rate(container_cpu_usage_seconds_total{pod_name="insecure-nginx-8455b6d49c-z6wb9"}[5m])): 0.047

sum(rate(container_cpu_usage_seconds_total{pod_name="insecure-nginx-8455b6d49c-z6wb9"}[5m]))

```
sum(rate(container_cpu_usage_seconds_total{pod_name="insecure-nginx-8455b6d49c-z6wb9"}[5m]))
```

Chapter 13: Learning from Kubernetes CVEs



CVE-ID

CVE-2018-18264 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Kubernetes Dashboard before 1.10.1 allows attackers to bypass authentication and use Dashboard's Service Account for reading secrets within the cluster.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

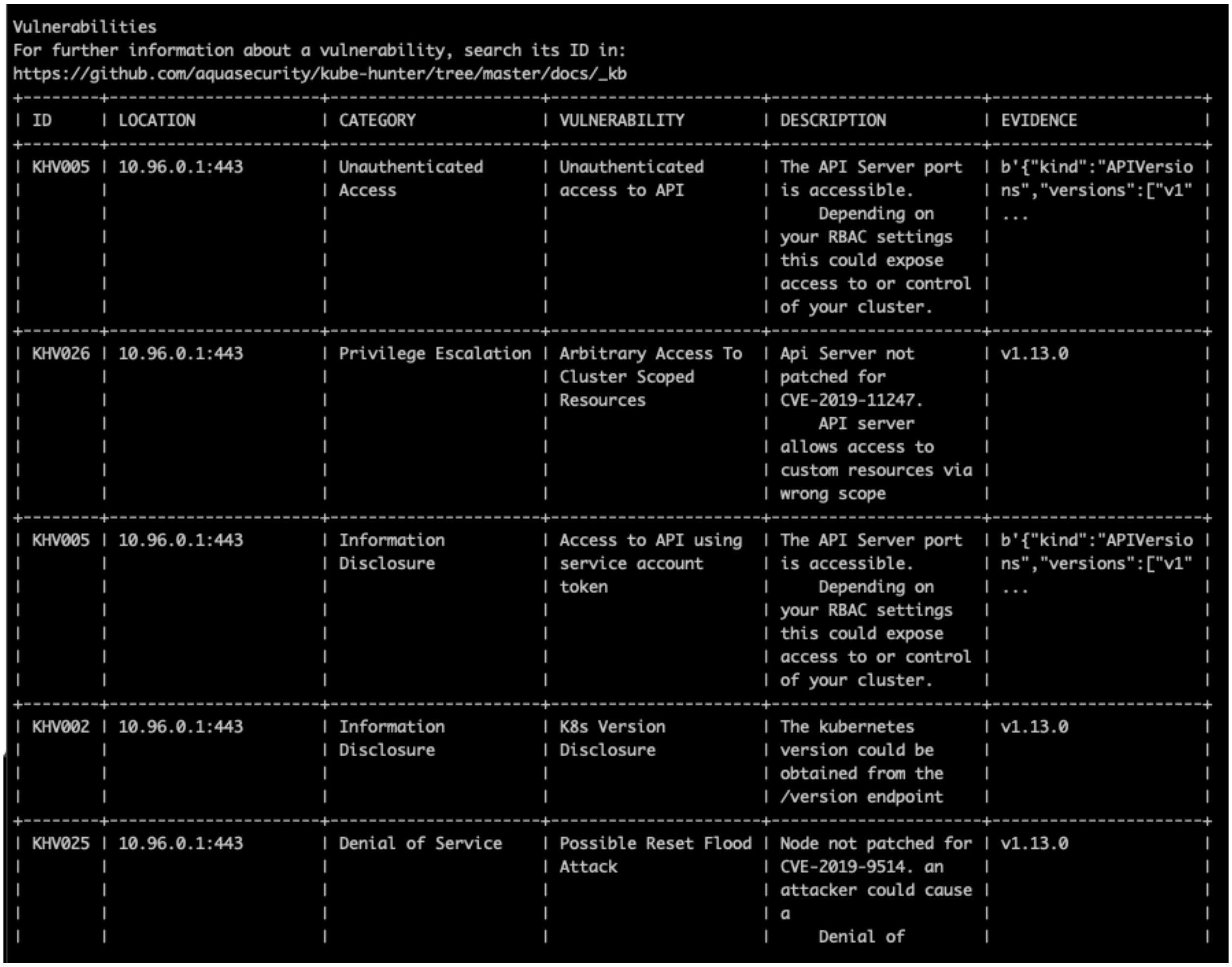
- BID:106493
- URL:http://www.securityfocus.com/bid/106493
- MISC:https://github.com/kubernetes/dashboard/pull/3289
- MISC:https://github.com/kubernetes/dashboard/pull/3400
- MISC:https://github.com/kubernetes/dashboard/releases/tag/v1.10.1
- MISC:https://groups.google.com/forum/#!topic/kubernetes-announce/yBrFf5nmvfI
- MISC:https://sysdig.com/blog/privilege-escalation-kubernetes-dashboard/

Assigning CNA

MITRE Corporation

Date Entry Created

20181012 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.



```
Vulnerabilities
For further information about a vulnerability, search its ID in:
https://github.com/aquasecurity/kube-hunter/tree/master/docs/_kb
+--------+----------------------+----------------------+----------------------+----------------------+----------------------+
| ID     | LOCATION             | CATEGORY             | VULNERABILITY        | DESCRIPTION          | EVIDENCE             |
+--------+----------------------+----------------------+----------------------+----------------------+----------------------+
| KHV005 | 10.96.0.1:443        | Unauthenticated      | Unauthenticated      | The API Server port  | b'{"kind":"APIVersio |
|        |                      | Access               | access to API        | is accessible.       | ns","versions":["v1" |
|        |                      |                      |                      |     Depending on     | ...                  |
|        |                      |                      |                      | your RBAC settings   |                      |
|        |                      |                      |                      | this could expose    |                      |
|        |                      |                      |                      | access to or control |                      |
|        |                      |                      |                      | of your cluster.     |                      |
+--------+----------------------+----------------------+----------------------+----------------------+----------------------+
| KHV026 | 10.96.0.1:443        | Privilege Escalation | Arbitrary Access To  | Api Server not       | v1.13.0              |
|        |                      |                      | Cluster Scoped       | patched for          |                      |
|        |                      |                      | Resources            | CVE-2019-11247.      |                      |
|        |                      |                      |                      |     API server       |                      |
|        |                      |                      |                      | allows access to     |                      |
|        |                      |                      |                      | custom resources via |                      |
|        |                      |                      |                      | wrong scope          |                      |
+--------+----------------------+----------------------+----------------------+----------------------+----------------------+
| KHV005 | 10.96.0.1:443        | Information          | Access to API using  | The API Server port  | b'{"kind":"APIVersio |
|        |                      | Disclosure           | service account      | is accessible.       | ns","versions":["v1" |
|        |                      |                      | token                |     Depending on     | ...                  |
|        |                      |                      |                      | your RBAC settings   |                      |
|        |                      |                      |                      | this could expose    |                      |
|        |                      |                      |                      | access to or control |                      |
|        |                      |                      |                      | of your cluster.     |                      |
+--------+----------------------+----------------------+----------------------+----------------------+----------------------+
| KHV002 | 10.96.0.1:443        | Information          | K8s Version          | The kubernetes       | v1.13.0              |
|        |                      | Disclosure           | Disclosure           | version could be     |                      |
|        |                      |                      |                      | obtained from the    |                      |
|        |                      |                      |                      | /version endpoint    |                      |
+--------+----------------------+----------------------+----------------------+----------------------+----------------------+
| KHV025 | 10.96.0.1:443        | Denial of Service    | Possible Reset Flood | Node not patched for | v1.13.0              |
|        |                      |                      | Attack               | CVE-2019-9514. an    |                      |
|        |                      |                      |                      | attacker could cause |                      |
|        |                      |                      |                      | a                    |                      |
|        |                      |                      |                      |     Denial of        |                      |
```