KUBERMATIC

Container Days '23 - Hamburg

Why Securing Kubelet API is Critical for K8S Security?

koray@kubermatic.com

@korayoksay

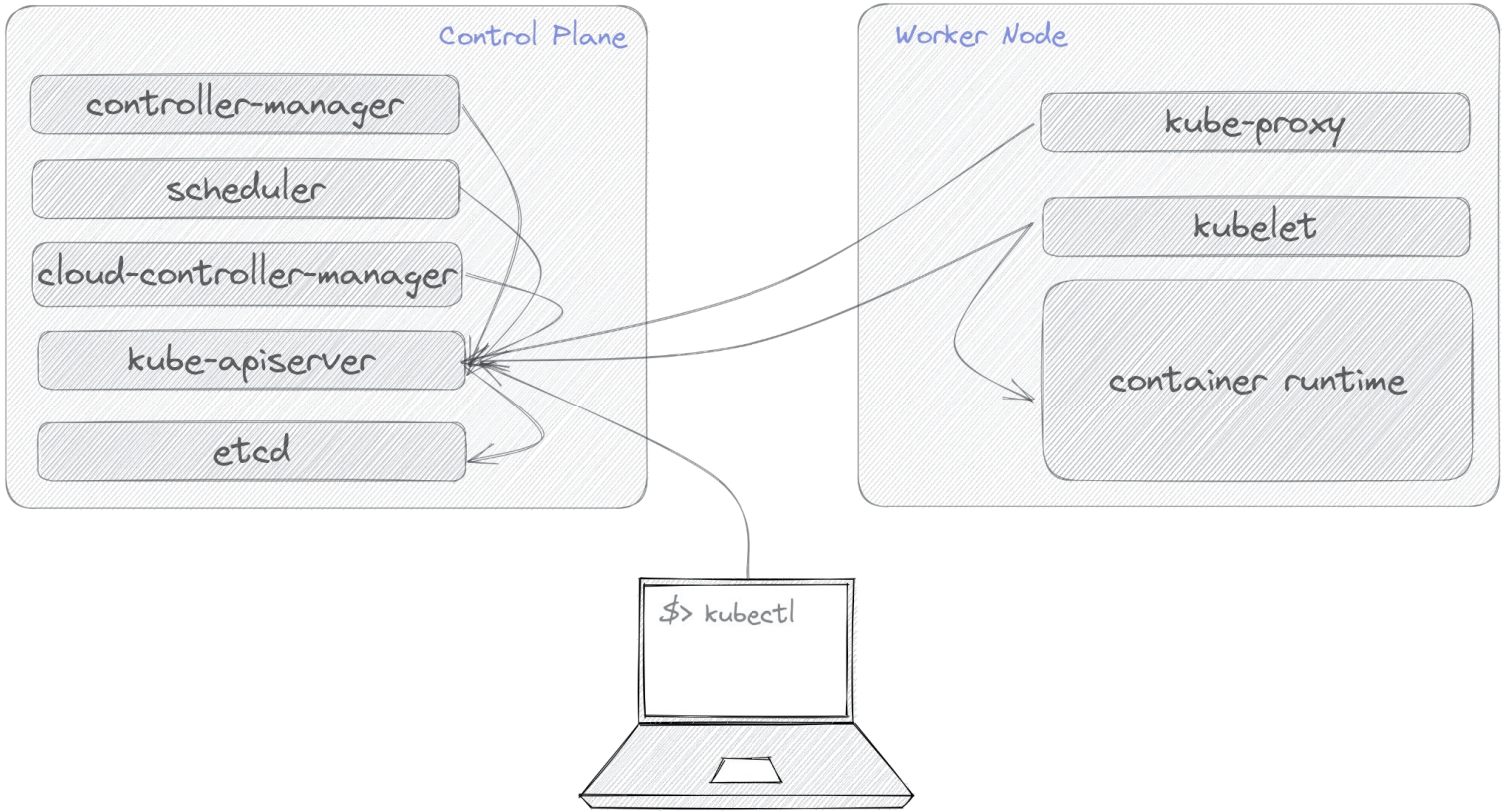
linkedin.com/in/korayoksay/

koksay

Who am I?

- Kubernetes Consultant & Instructor
- Working remotely from Istanbul
- Interested in Linux, Kubernetes, and cloud technologies
- CKA | CKAD | CKS | RHCE
- Linux Foundation Instructor for CK.*

Kubernetes Architecture



Kubelet

- By default: Port 10250
- Gets the PodSpec from the kube-apiserver
- Fetching the logs from containers (kubectl logs)
- Attaching to containers (kubectl exec)
- Port forwarging to containers (kubectl port-forward)

kubernetes port:10250 - S

shodan.io/search?query=kubernetes+port%3A10250

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads

TOTAL RESULTS

164

TOP COUNTRIES

China

United States

Japan

Germany

Korea, Republic of

More...

TOP ORGANIZATIONS

CHINANET HUNAN PROVINCE NETWORK

China Mobile Communications Corporation

Aliyun Computing Co., LTD

CHINANET Hunan province network

Amazon Technologies Inc.

More...

ulnerabilities using InternetDB

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Sun, 16 Apr 2023 05:23:03 GMT
Content-Length: 19

Kubernetes:
  Node #1:
    Name: kube-apiserver-host-172-16-2-210
    Container #1:
      Name: kube-apiserver
      Image: k8s.gcr.io/kube...
```

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Sun, 16 Apr 2023 02:46:50 GMT
Content-Length: 19

Kubernetes:
  Node #1:
    Name: kube-proxy-ip-172-20-210-221.ec2.internal
    Container #1:
      Name: kube-proxy
      Image: gcr.io/goo...
```

API Documentation?

- API is not documented!
- The code can be checked

kubernetes / pkg / kubelet / server / server.go

Code | Blame | 1146 lines (1031 loc) · 40.3 KB

```go
// InstallDebuggingHandlers registers the HTTP request patterns that serve logs or run commands/containers
func (s *Server) InstallDebuggingHandlers() {
	klog.InfoS("Adding debug handlers to kubelet server")

	s.addMetricsBucketMatcher("run")
	ws := new(restful.WebService)
	ws.
		Path("/run")
	ws.Route(ws.POST("/{podNamespace}/{podID}/{containerName}").
		To(s.getRun).
		Operation("getRun"))
	ws.Route(ws.POST("/{podNamespace}/{podID}/{uid}/{containerName}").
		To(s.getRun).
		Operation("getRun"))
	s.restfulCont.Add(ws)

	s.addMetricsBucketMatcher("exec")
	ws = new(restful.WebService)
	ws.
		Path("/exec")
	ws.Route(ws.GET("/{podNamespace}/{podID}/{containerName}").
		To(s.getExec).
		Operation("getExec"))
	ws.Route(ws.POST("/{podNamespace}/{podID}/{containerName}").
		To(s.getExec).
		Operation("getExec"))
	ws.Route(ws.GET("/{podNamespace}/{podID}/{uid}/{containerName}").
		To(s.getExec).
		Operation("getExec"))
	ws.Route(ws.POST("/{podNamespace}/{podID}/{uid}/{containerName}").
		To(s.getExec).
		Operation("getExec"))
	s.restfulCont.Add(ws)

```

KUBERMATIC

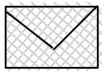
DEMO

KUBERMATIC

QUESTIONS?

KUBERMATIC

THANK YOU!



koray@kubermatic.com

@korayoksay

linkedin.com/in/korayoksay/

koksay