



KUBERMATIC

Container Days '23 - Hamburg

Why Securing Kubelet API is Critical for K8S Security?

```
?    former coreinformers.PodInformer().Inform("pods", jm.EnqueueController)
?    cord.NewBroadcaster()
?    Logging(klog.Infof)
?    tRecordingToSink(&v1core.EventRecorder)
?
?    l && kubeClient.CoreV1().RESTClient().Post().Resource("events").Body(event).Do()
?    gisterMetricAndTrackRateLimit()
?
?    controller: controller.NewController(
?        kubeClient,
?        : controller.RealPodController{
?            client: kubeClient,
?            recorder: eventBroadcaster.NewRecorder("events"),
?            workqueue: NewNamedRateLimiter("events"),
?            actions: controller.NewControllerActions{
?                addFunc: func(obj interface{}) {
?                    jm.enqueueController(obj, true)
?                },
?                updateFunc: jm.updateJob,
?                deleteFunc: func(obj interface{}) {
?                    jm.enqueueController(obj, true)
?                },
?            },
?        }
?    )
?}
```



koray@kubermatic.com



@korayoksay



linkedin.com/in/korayoksay/

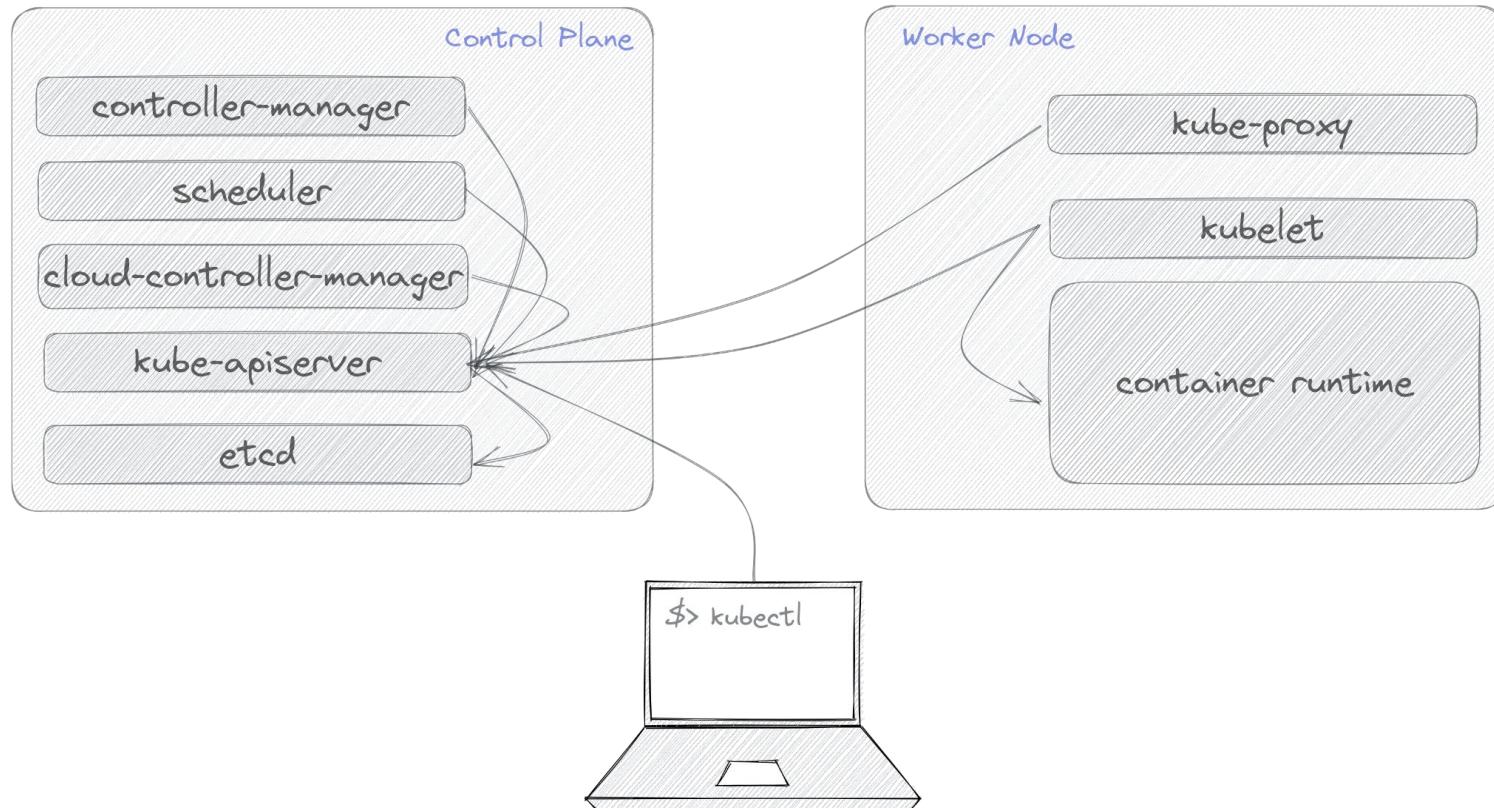


koksay

| 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.*

I Kubernetes Architecture



I 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 forwarding to containers (kubectl port-forward)

kubernetes port:10250 - S x +

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...



vulnerabilities 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**

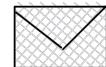
Code Blame 1146 lines (1031 loc) · 40.3 KB

```
460     // InstallDebuggingHandlers registers the HTTP request patterns that serve logs or run commands/containers
461     func (s *Server) InstallDebuggingHandlers() {
462         klog.InfoS("Adding debug handlers to kubelet server")
463
464         s.addMetricsBucketMatcher("run")
465         ws := new(restful.WebService)
466         ws.
467             Path("/run")
468         ws.Route(ws.POST("/{podNamespace}/{podID}/{containerName}").
469                 To(s.getRun).
470                 Operation("getRun"))
471         ws.Route(ws.POST("/{podNamespace}/{podID}/{uid}/{containerName}").
472                 To(s.getRun).
473                 Operation("getRun"))
474         s.restfulCont.Add(ws)
475
476         s.addMetricsBucketMatcher("exec")
477         ws = new(restful.WebService)
478         ws.
479             Path("/exec")
480         ws.Route(ws.GET("/{podNamespace}/{podID}/{containerName}").
481                 To(s.getExec).
482                 Operation("getExec"))
483         ws.Route(ws.POST("/{podNamespace}/{podID}/{containerName}").
484                 To(s.getExec).
485                 Operation("getExec"))
486         ws.Route(ws.GET("//{podNamespace}/{podID}/{uid}/{containerName}").
487                 To(s.getExec).
488                 Operation("getExec"))
489         ws.Route(ws.POST("//{podNamespace}/{podID}/{uid}/{containerName}").
490                 To(s.getExec).
491                 Operation("getExec"))
492         s.restfulCont.Add(ws)
493
```

>
DEMO

| QUESTIONS?

I THANK YOU!



koray@kubernetes.com



@korayoksay



linkedin.com/in/korayoksay/



koksay