KUBERMATIC

Koray Oksay

Why Securing Kubelet API is Critical for K8S Security?

Cloud_Native Rejekts [EU'23]
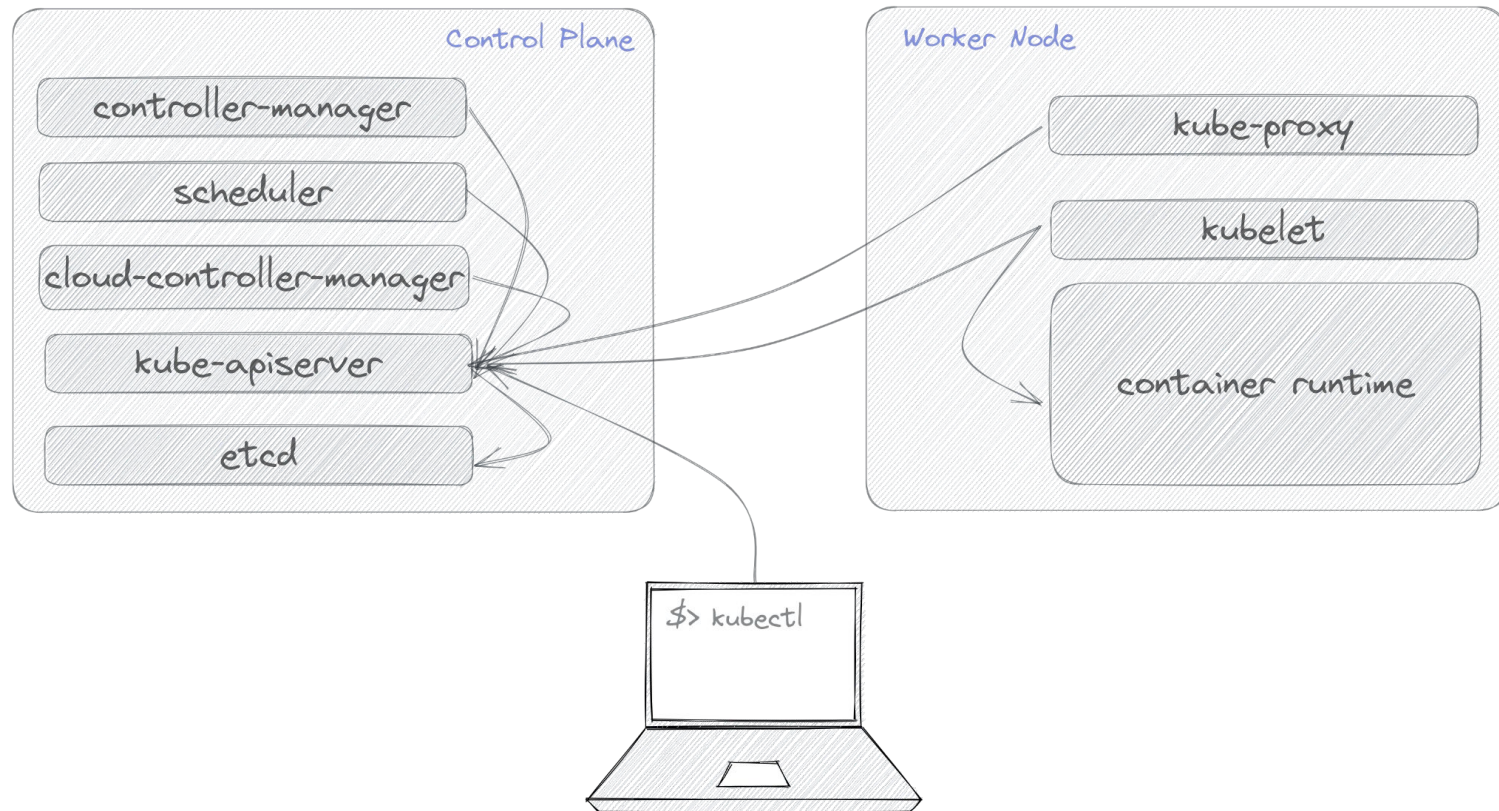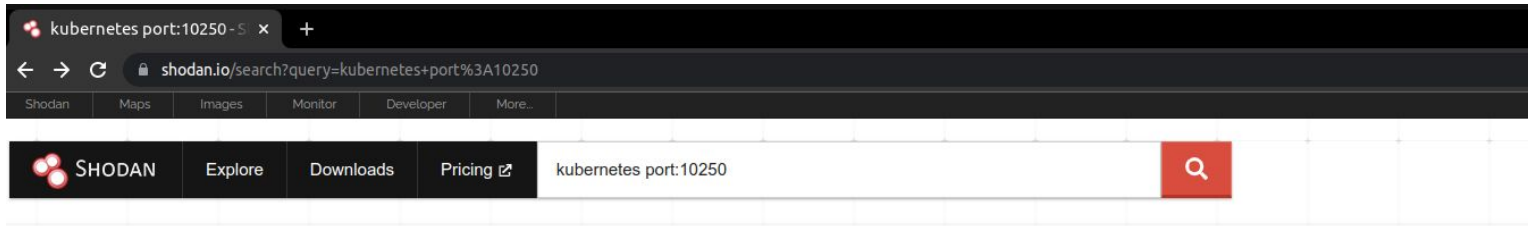
Who am I?

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

Koray Oksay
Kubernetes Consultant

✉ koray@kubermatic.com

🐦 @korayoksay

koksay

Kubernetes Architecture Recap

Kubelet

- By default runs on port **10250**

- <= Getting the PodSpecs From the kubeapi-server

- => Fetching logs for pods

- => Attaching (usually through `kubectl`) to running pods

- => Providing `kubectl port-forward`

SHODAN   Explore   Downloads   Pricing ⟋ | kubernetes port:10250 | 🔍 |

TOTAL RESULTS

164

TOP COUNTRIES

📊 View Report   🗺 View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using **InternetDB**

61.109.216.232 ⟋
Sejong Telecom
🇰🇷 Korea, Republic of, Seoul

`devops`

China	133
United States	6
Japan	5
Germany	4
Korea, Republic of	3

More...

TOP ORGANIZATIONS

CHINANET HUNAN PROVINCE NETWORK	79
China Mobile Communications Corporation	25
Aliyun Computing Co., LTD	8
CHINANET Hunan province network	6
Amazon Technologies Inc.	4

More...

🔒 **SSL Certificate**

Issued By:
|- Common Name:
  host-172-16-2-210-ca@1679539544

Issued To:
|- Common Name:
  host-172-16-2-210@1679539545

Supported SSL Versions:
TLSv1.2

```
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...

34.239.165.141 ⟋
ec2-34-239-165-141.compute-1.am
azonaws.com
Amazon Technologies Inc.
🇺🇸 United States, Ashburn

`cloud` `devops` `self-signed`

🔒 **SSL Certificate**

Issued By:
|- Common Name:
  **ip-172-20-210-
  221.ec2.internal@1530610450**

Issued To:
|- Common Name:
  **ip-172-20-210-
  221.ec2.internal@1530610450**

Supported SSL Versions:
TLSv1.2

```
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?

- Kubelet API is not documented
- [Code](#) can be checked

```
~
) grep "Path(" server.go
        root := getURLRootPath(path)
                Path("/pods").
                ws.Path("/checkpoint").Produces(restful.MIME_JSON)
                Path("/run")
                Path("/exec")
                Path("/attach")
                Path("/portForward")
                Path("/containerLogs")
                Path("/runningpods/").
                ws.Path(logsPath)
        ws := new(restful.WebService).Path(pprofBasePath)
func getURLRootPath(path string) string {
```
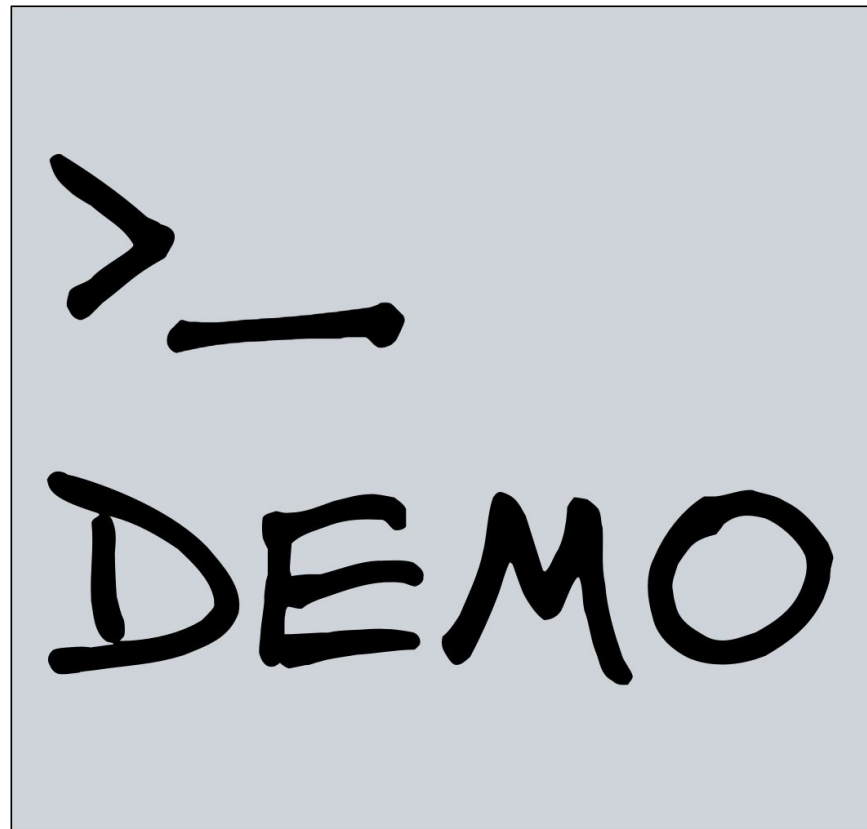
Thank you!

✉ koray@kubermatic.com

🐦 @korayoksay

○ koksay

KUBERMATIC