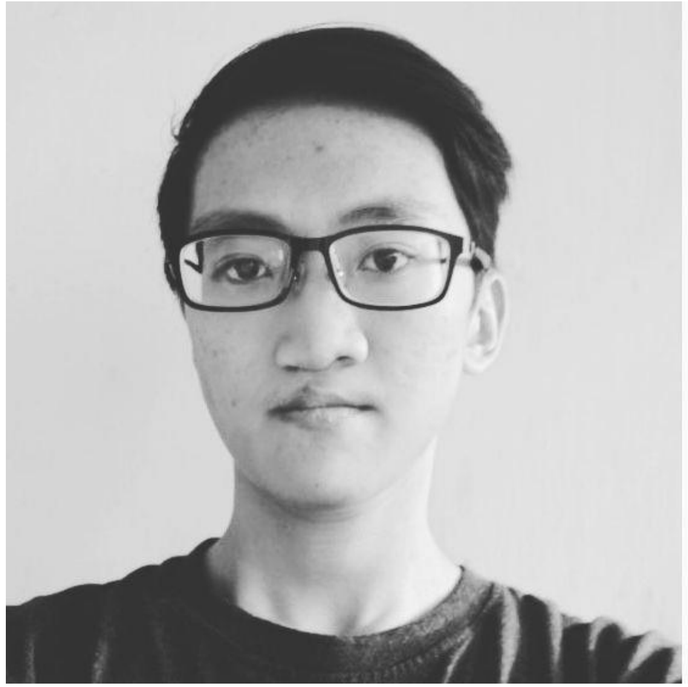
Securing Kubernetes (k8s) with Kubernetes Goat

Muhammad Yuga Nugraha @ Practical DevSecOps



About Me

- DevSecOps Engineer at Practical DevSecOps.
- Student at AMIKOM University of Yogyakarta.
- Interest in Information Security, Cloud Native, Container, and Automation.
- Community: Docker Indonesia, Kubernetes & Cloud Native Indonesia, DevOps Indonesia, DevSecOps Indonesia.
- Telegram: @jerukitumanis
- LinkedIn: myugan

DISCLAIMER

- Educational purposes only.
- Information found in this presentation is based on publicly available resources

Agenda

- Kubernetes Introduction
- Kubernetes Goat
- Attack Surfaces
- Defending your Kubernetes Cluster
- Question & Answer

CLOUD NATIVE COMPUTING FOUNDATION About Projects Certification People Community Newsroom JOIN NOW

Certified Kubernetes Security Specialist (CKS) Coming in November

0

By **cncf** July 15, 2020 in **Blog**

CNCF Staff Post

This autumn The Linux Foundation and CNCF are excited to add a new Certified Kubernetes Security Specialist (CKS) to the growing list of Kubernetes certification programs. CKS will join the popular and highly respected Certified Kubernetes Administrator (CKA) and Certified Kubernetes Application Developer (CKAD) programs. This new certification is for those who have passed the CKA exam and want third party validation for their working knowledge of container security.

Start your preparations now!

In order to take the CKS exam, you must hold a current CKA certification to demonstrate you possess sufficient Kubernetes expertise. If you want to make sure you are ready for the CKS and have not already achieved the CKA, we encourage you to start today! We provide a wealth of resources to help you prepare for CKA.

The details

CKS is similar in format to CKA and will consist of a performance-based certification exam – testing competence across best practices for securing container-based applications and Kubernetes platforms during build, deployment, and runtime.

The new certification is designed to enable cloud native professionals to demonstrate security skills to current and potential employers. The exam will test domains and competencies including:

- Cluster Setup
- Cluster Hardening
- System Hardening
- Minimize Microservice Vulnerabilities

START HACKING | LOG IN

hackerone

SOLUTIONS PRODUCTS WHY HACKERONE COMPANY RESOURCES CONTACT US

Kubernetes

https://kubernetes.io/ · @kubernetesio

Submit report

Bug Bounty Program
Launched on Jan 2020

Managed by HackerOne
Bounty splitting enabled

Reports resolved	Assets in scope	Average bounty
14	82	$250-$500

Policy Hacktivity Thanks Updates (0)

Policy

We're incredibly grateful for security researchers and users that report vulnerabilities to the Kubernetes Open Source Community. All reports are thoroughly investigated by a set of community volunteers.

Response Targets

Cloud Native Computing Foundation will make a best effort to meet the following response targets for hackers participating in our program:

- Time to first response (from report submitted) - 1 business day
- Time to triage (from report submitted) - 10 business days
- Time to bounty (from triage) - 10 business days

We'll try to keep you informed about our progress throughout the process.

Disclosure Policy

- A public disclosure date is negotiated by the Kubernetes Product Security Committee and the bug submitter. We prefer to fully disclose the bug as soon as possible once user mitigation is available. It is reasonable to delay disclosure when the bug or the fix is not yet fully understood, the solution is not well-tested, or for vendor coordination. The timeframe for disclosure is very dependent on the context of the bug and varies from immediate for publicly known issues to months

Response Efficiency

5 hrs
Average time to first response

about 1 day
Average time to triage

11 days
Average time to bounty

2 months
Average time to resolution

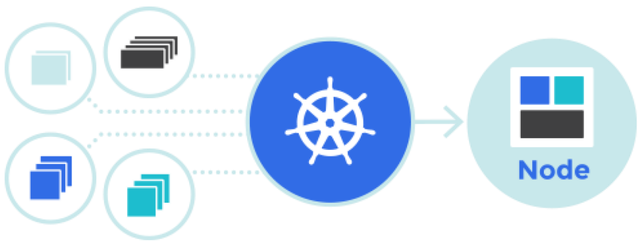
100% of reports
Meet response standards
Based on last 90 days

1

Kubernetes Introduction

Overview basic of Kubernetes components.

What is Kubernetes

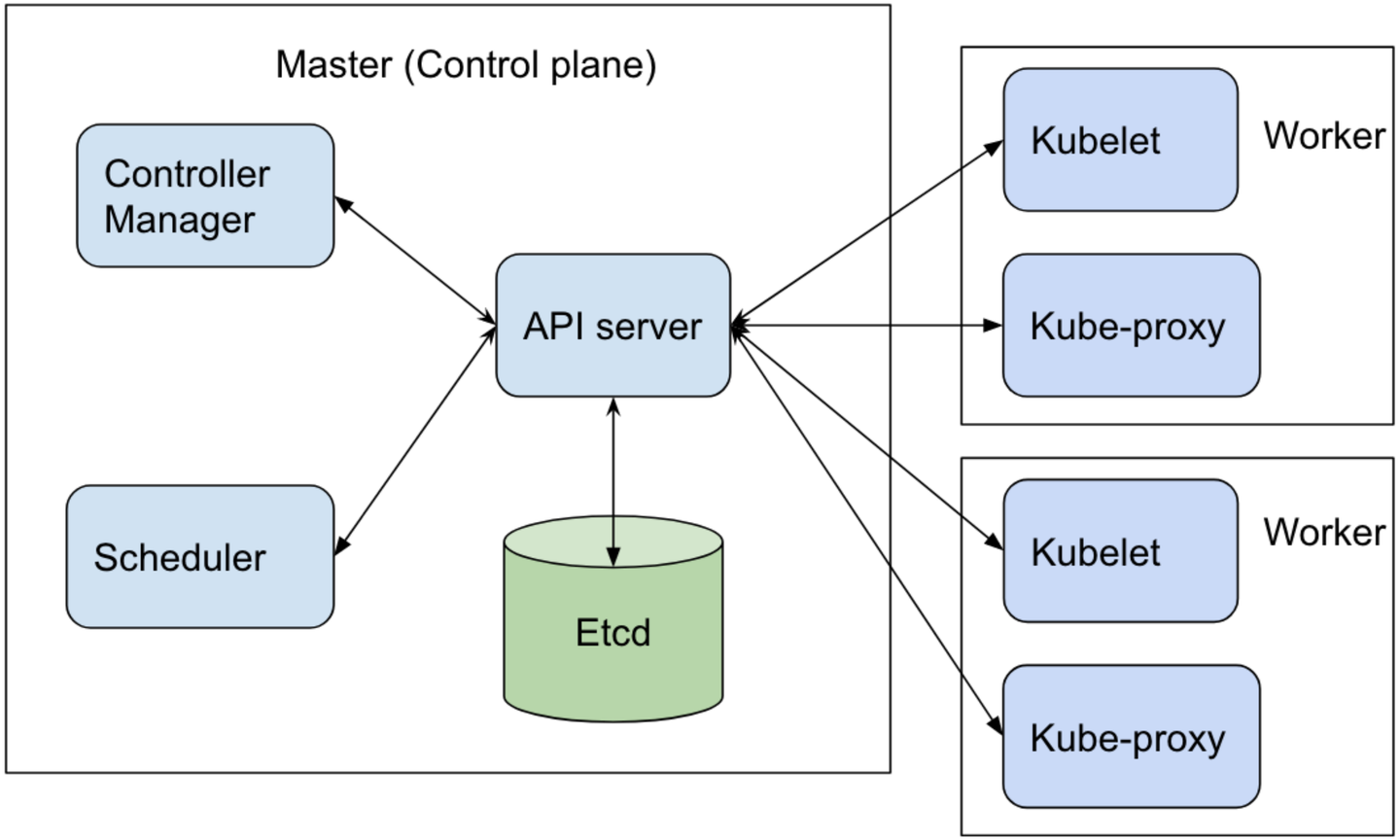


"Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available."

Source: https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/

What are the components in Kubernetes

1. Kubernetes API Server (main component)
2. ETCD
3. Controller Manager
4. Scheduler
5. Kubelet
6. Kube Proxy



Kubernetes API

“The Kubernetes API lets you query and manipulate the state of objects in Kubernetes. The core of Kubernetes' control plane is the API server and the HTTP API that it exposes. Users, the different parts of your cluster, and external components all communicate with one another through the API server.”

Source: https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/

Accessing Kubernetes API using kubectl proxy

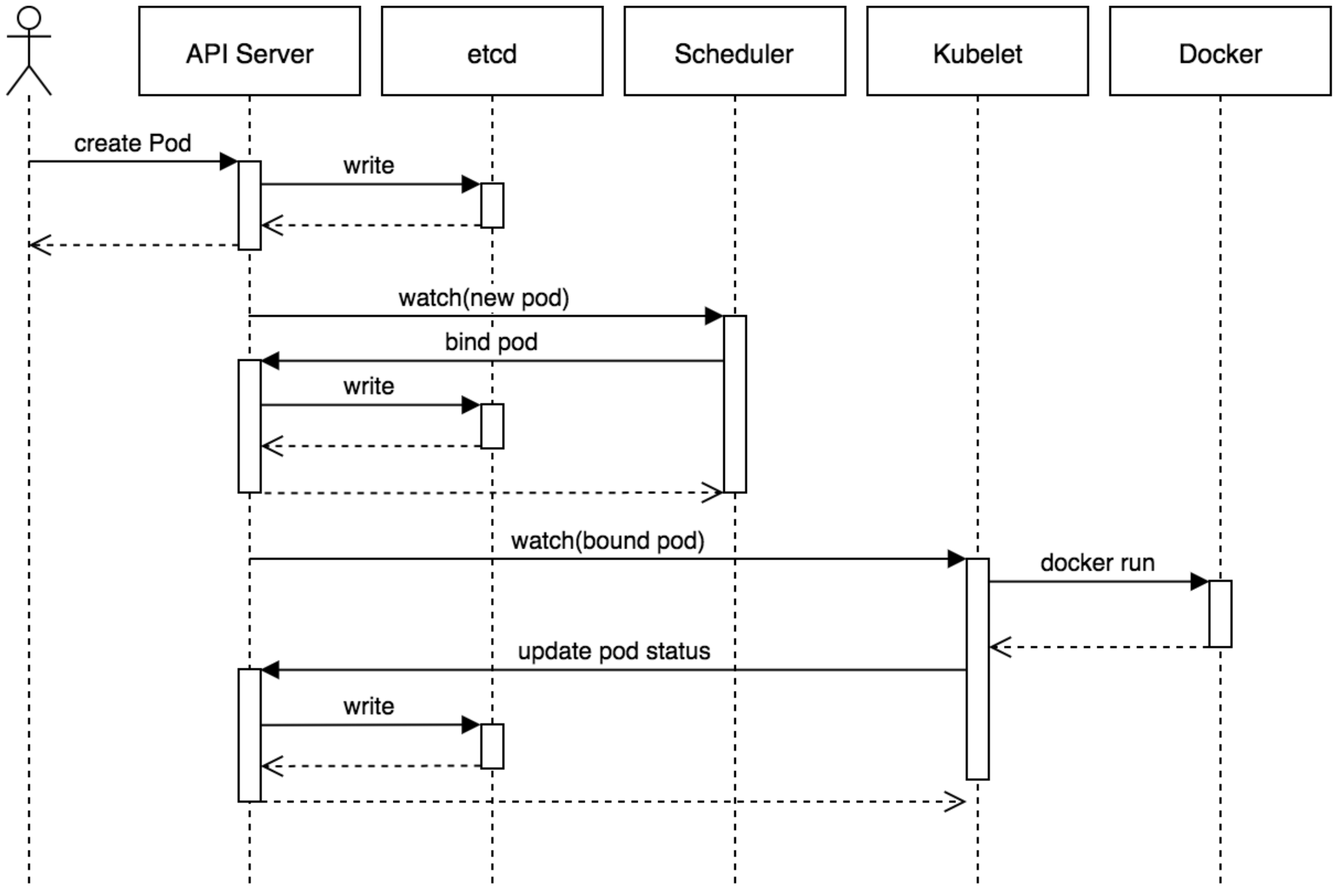
```
ubuntu@stealth:~$ kubectl proxy --port=8080 &
[1] 2116
ubuntu@stealth:~$ Starting to serve on 127.0.0.1:8080

ubuntu@stealth:~$ curl http://localhost:8080/api/
{
  "kind": "APIVersions",
  "versions": [
    "v1"
  ],
  "serverAddressByClientCIDRs": [
    {
      "clientCIDR": "0.0.0.0/0",
      "serverAddress": "[redacted]:443"
    }
  ]
}ubuntu@stealth:~$
```

```
{
  "paths": [
    "/api",
    "/api/v1",
    "/apis",
    "/apis/",
    "/apis/admissionregistration.k8s.io",
    "/apis/admissionregistration.k8s.io/v1",
    "/apis/admissionregistration.k8s.io/v1beta1",
    "/apis/apiextensions.k8s.io",
    "/apis/apiextensions.k8s.io/v1",
    "/apis/apiextensions.k8s.io/v1beta1",
    "/apis/apiregistration.k8s.io",
    "/apis/apiregistration.k8s.io/v1",
    "/apis/apiregistration.k8s.io/v1beta1",
    "/apis/apps",
    "/apis/apps/v1",
    "/apis/authentication.k8s.io",
    "/apis/authentication.k8s.io/v1",
    "/apis/authentication.k8s.io/v1beta1",
    "/apis/authorization.k8s.io",
    "/apis/authorization.k8s.io/v1",
    "/apis/authorization.k8s.io/v1beta1",
    "/apis/autoscaling",
    "/apis/autoscaling/v1",
    "/apis/autoscaling/v2beta1",
    "/apis/autoscaling/v2beta2",
    "/apis/batch",
    "/apis/batch/v1",
    "/apis/batch/v1beta1",
    "/apis/certificates.k8s.io",
    "/apis/certificates.k8s.io/v1beta1",
    "/apis/cilium.io",
```

ETCD – Data store

“is a consistent and highly-available key value store used as Kubernetes' backing store for all cluster data”



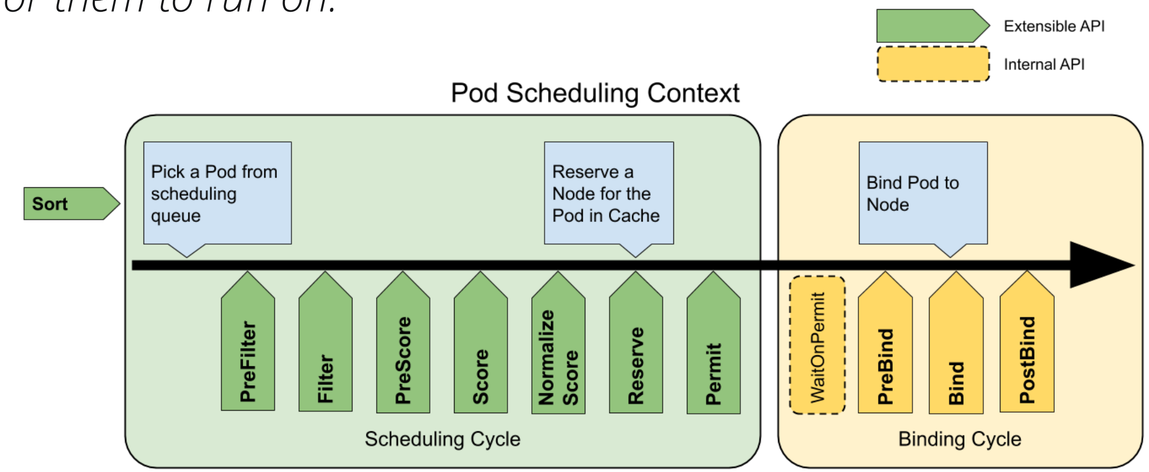
Source: blog.heptio.com

Controller Manager

“The Kubernetes API lets you query and manipulate the state of objects in Kubernetes. The core of Kubernetes' control plane is the API server and the HTTP API that it exposes. Users, the different parts of your cluster, and external components all communicate with one another through the API server.”

Scheduler

"Control plane component that watches for newly created Pods with no assigned node, and selects a node for them to run on."



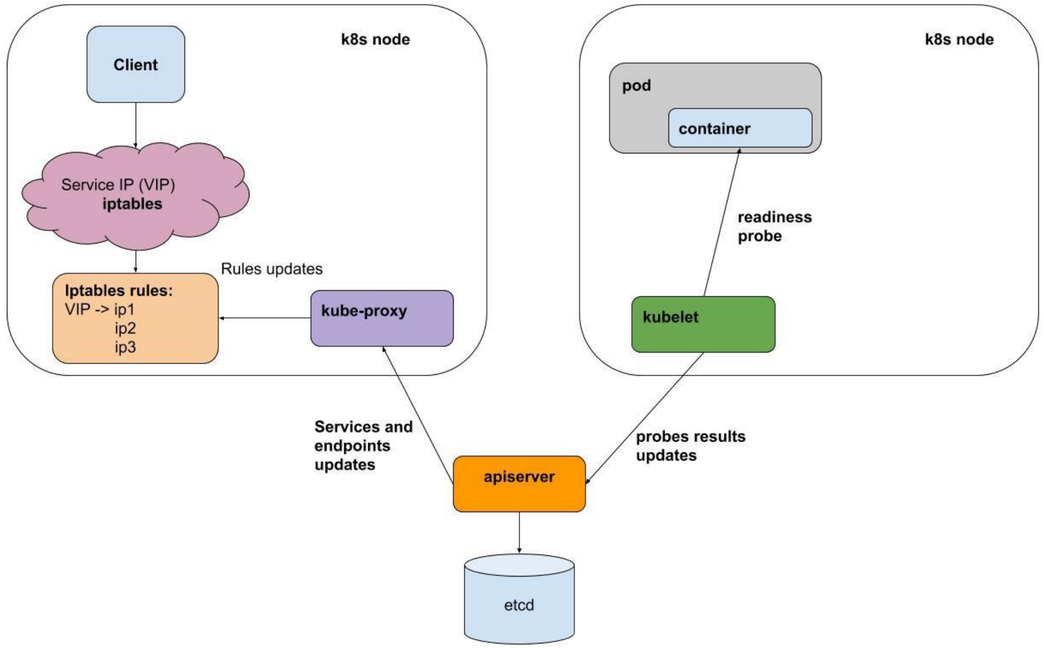
Source: https://kubernetes.io/docs/concepts/scheduling-eviction/kube-scheduler/

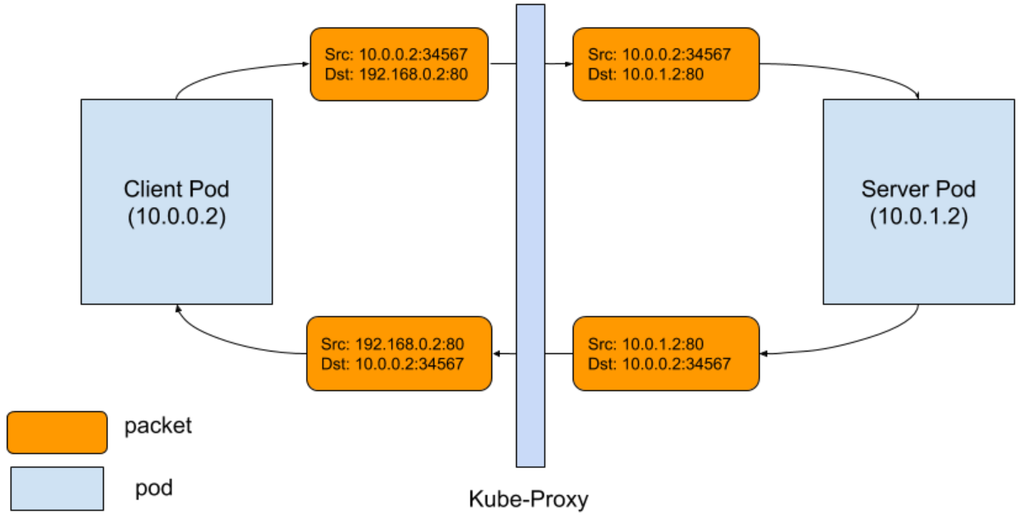
Kubelet

“The kubelet is the primary "node agent" that runs on each node. It can register the node with the api server using one of: the hostname; a flag to override the hostname; or specific logic for a cloud provider.”

Source: http://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/

Kube Proxy





"A network proxy that runs on each node in your cluster, implementing part of the Kubernetes Service concept

2

Kubernetes Goat

Covering some scenarios from Kubernetes goat with demo

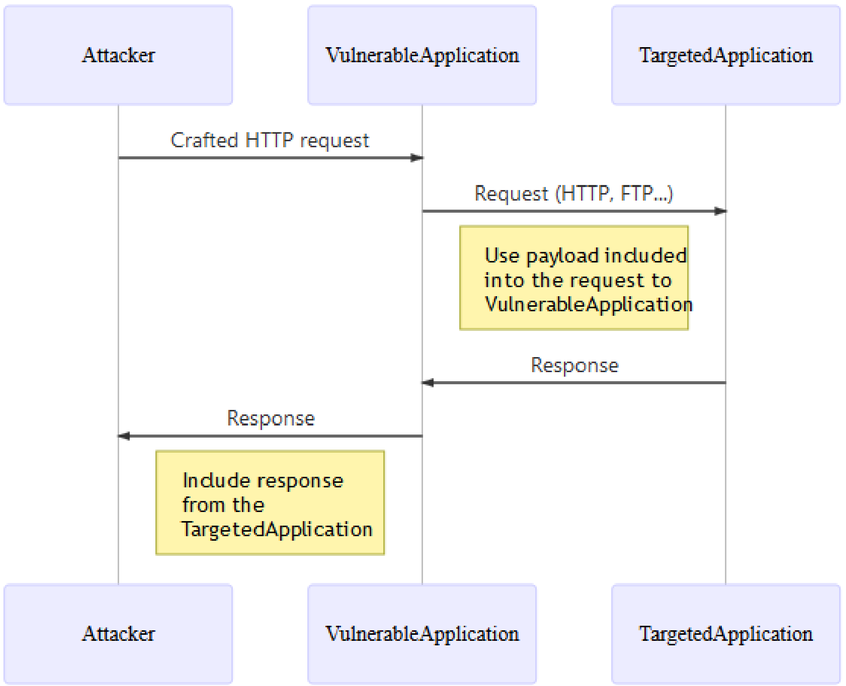
KUBERNETES GOAT

The Kubernetes Goat designed to be intentionally vulnerable cluster environment to learn and practice Kubernetes security with some scenarios such as:

1. Server Side Request Forgery
2. Container Escape
3. Attacking Private Registry
4. etc.

```
ubuntu@stealth:~/kubernetes-goat$ bash setup-kubernetes-goat.sh
kubectl setup looks good.
helm2 setup looks good.
setting up helm2 rbac account and initialise tiller
serviceaccount/tiller created
clusterrolebinding.rbac.authorization.k8s.io/tiller created
setup-kubernetes-goat.sh: line 29: helm2: command not found
waiting for helm2 tiller service to be active.
deploying helm chart metadata-db scenario
setup-kubernetes-goat.sh: line 37: helm2: command not found
deploying the vulnerable scenarios manifests
job.batch/batch-check-job created
deployment.apps/build-code-deployment created
service/build-code-service created
namespace/secure-middleware created
service/cache-store-service created
deployment.apps/cache-store-deployment created
deployment.apps/health-check-deployment created
service/health-check-service created
deployment.apps/hunger-check-deployment created
service/hunger-check-service created
deployment.apps/internal-proxy-deployment created
service/internal-proxy-api-service created
service/internal-proxy-info-app-service created
deployment.apps/kubernetes-goat-home-deployment created
service/kubernetes-goat-home-service created
deployment.apps/poor-registry-deployment created
service/poor-registry-service created
secret/goatvault created
deployment.apps/system-monitor-deployment created
service/system-monitor-service created
Successfully deployed Kubernetes Goat. Have fun learning Kubernetes Security!
Ensure pods are in running status before running access-kubernetes-goat.sh script
Now run the bash access-kubernetes-goat.sh to access the Kubernetes Goat environment.
```

Estimate: 10 Minutes



Server Side Request Forgery

Vulnerability that allows to make a requests (like proxy) into internal system" (Remote Code Execution of the Cloud) and often used to:

1. Exploit vulnerable application.
2. Extract credentials.
3. Pivot to organization account.

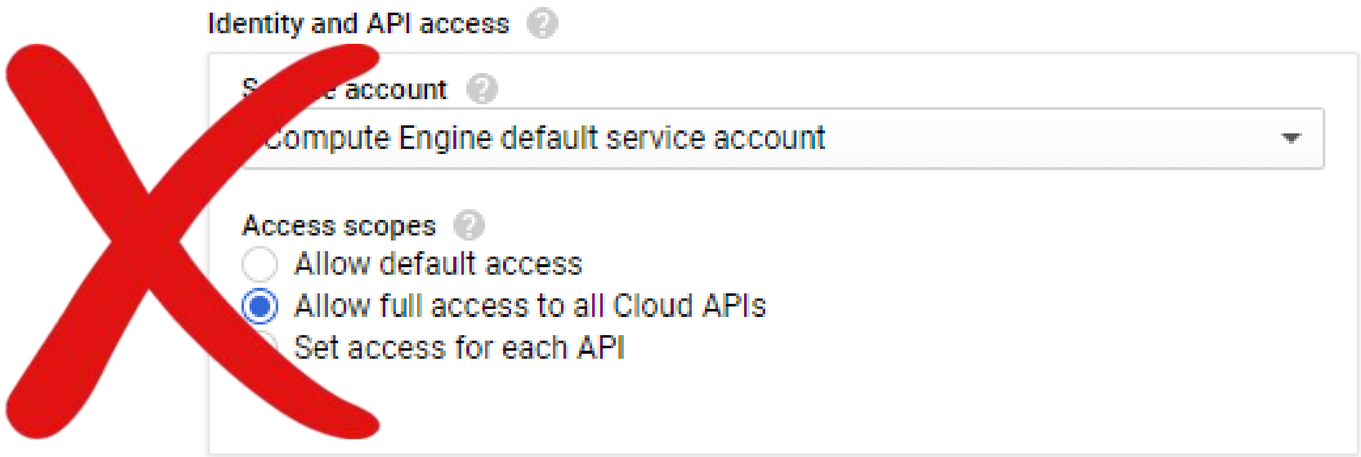
Cloud Metadata

"Small pieces of information that can be attached to files and other objects in a computing"

GCP Metadata

```
root@ubuntu-78fdc464b5-fqgql:/# curl -v -H 'Metadata-Flavor: Google' http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token
*   Trying 169.254.169.254:80...
* TCP_NODELAY set
* Connected to metadata.google.internal (169.254.169.254) port 80 (#0)
> GET /computeMetadata/v1/instance/service-accounts/default/token HTTP/1.1
> Host: metadata.google.internal
> User-Agent: curl/7.68.0
> Accept: */*
> Metadata-Flavor: Google
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Metadata-Flavor: Google
< Content-Type: application/json
< Date: Thu, 13 Aug 2020 05:44:16 GMT
< Server: Metadata Server for VM
< Content-Length: 253
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
<
* Connection #0 to host metadata.google.internal left intact
{"access_token":"ya29.c.KokB1weRr-YHX_5Yt4vMpy94dk2nFbM0_XNbGa2EIzB5W4jfNoWetRQzT4bONHFchd_Dt248n-D3mxeFlldbcTEvDSzv42dZI5y51shKnJszdspkRNCHFTwwS2mqleRGEwd5cTMGdH7IarD
"Bearer"}root@ubuntu-78fdc464b5-fqgql:/#
```

Instance can call Cloud API



Digital Ocean Metadata

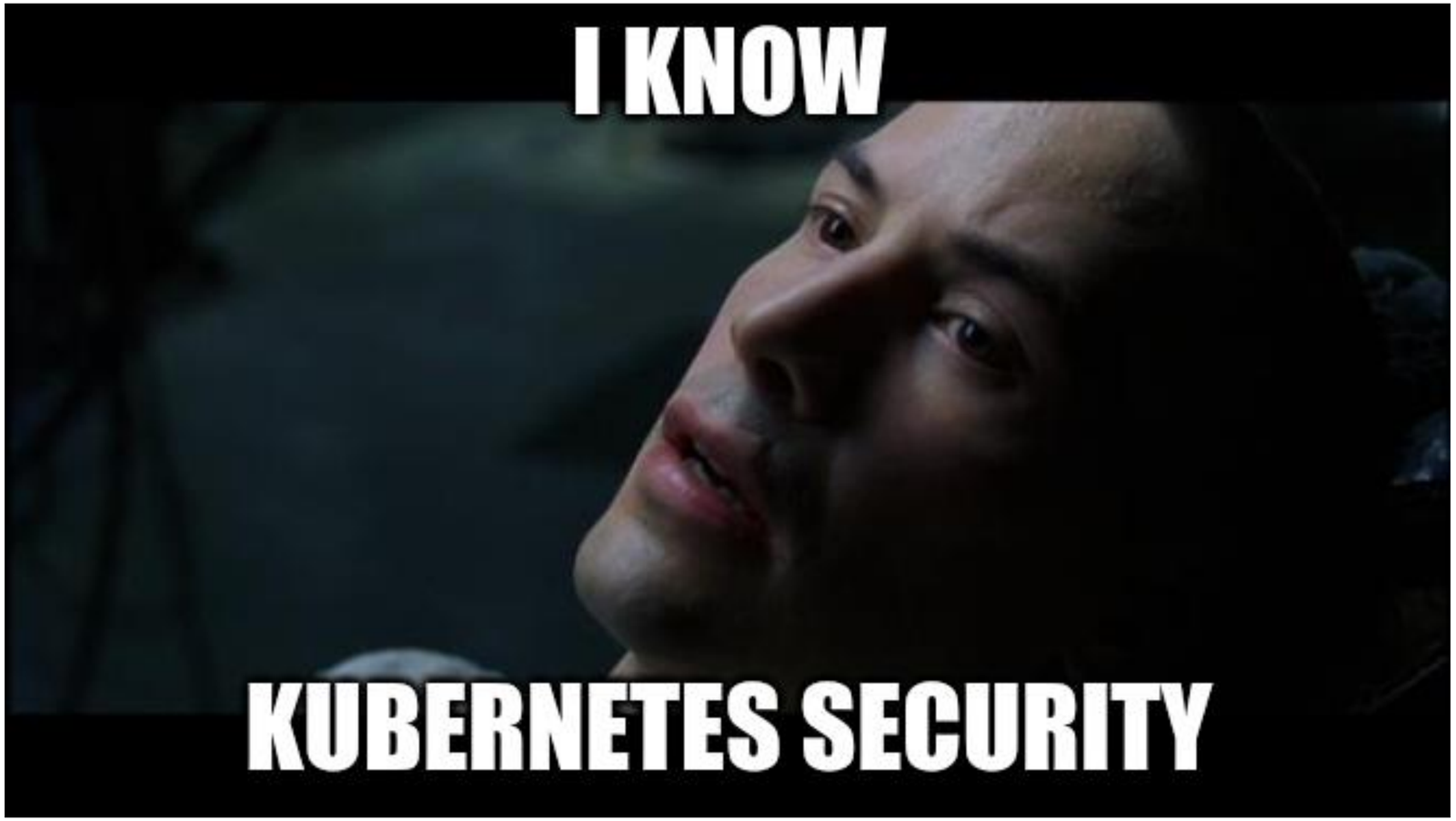
```
root@nginx-deployment-6b474476c4-r68vt:/# curl -qs http://169.254.169.254/metadata/v1/user-data
#cloud-config
k8saas_role: kubelet
k8saas_master_domain_name: "7e9[illegible]ef3106d.internal.k8s.ondigitalocean.com"
k8saas_bootstrap_token: "03r7[illegible]rb829"
k8saas_proxy_token: "2f[illegible]"
k8saas_ca_cert: "-----BEGIN CERTIFICATE-----[illegible]UEChMMRGln[illegible]
ggEKAo[illegible]aiQvtI0cq[illegible]
[illegible]AQn/AgEA[illegible]
6Kf4kGAh[illegible]3bdtE[illegible]
k8saas_overlay_subnet: "10.244.0.0/16"
k8saas_cluster_uuid: "7e9b84e1-fde4-49fa-8957-922ddef3106d"
k8saas_dns_service_ip: "10.245.0.10"
k8saas_node_labels: "doks.digitalocean.com/node-id=d6baac14-e4d8-42b1-b9a3-de3589b85ae8,doks.digitalocean.com/[illegible]

root@nginx-deployment-6b474476c4-r68vt:/#
```

3

Attack Surfaces

How your Kubernetes cluster can compromise by attacker.



ATT&CK™

Adversarial Tactics, Techniques
& Common Knowledge

Knowledge base of adversary tactics and techniques based on real-world observations.

Threat Matrix for Kubernetes

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed Dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

Source: https://microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

André Baptista (0xacb)

1802	-	6.02	93rd	21.85	93rd
Reputation	Rank	Signal	Percentile	Impact	Percentile

468 #341876 **SSRF in Exchange leads to ROOT access in all instances**

Share:

State	Resolved (Closed)	Severity	Medium (6.9)
Disclosed	May 24, 2018 4:09am +0700	Participants	
Reported To	Shopify	Visibility	Disclosed (Full)
Asset	https://exchangemarketplace.com/ (Domain)		
Weakness	Server-Side Request Forgery (SSRF)		
Bounty	$25,000		

Vulnerable Kubelet on the internet

SHODAN port:"10250" product:"kubernetes"

Explore | Downloads | Reports | Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

856

TOP COUNTRIES

China	341
United States	193
India	60
Japan	59
France	34

TOP ORGANIZATIONS

Amazon.com	267
China Unicom Liaoning	92
Tencent cloud computing	49
SoftLayer Technologies	31
China Telecom	22

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

[redacted]
ec2-1[redacted]compute-1.amazonaws.com
Amazon.com
Added on 2020-08-11 05:42:44 GMT
United States, Ashburn

cloud | devops

SSL Certificate
Issued By:
|- Common Name: ip-10-0-2-111-ca@1595350172
Issued To:
|- Common Name: ip-10-0-2-111@1595350173

Supported SSL Versions
TLSv1.2

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 11 Aug 2020 05:42:44 GMT
Content-Length: 19
```

[redacted]
ec2-[redacted]cn-north-1.compute.amazonaws.com.cn
Beijing Guanghuan Xinwang Digital
Added on 2020-08-11 02:50:14 GMT
China, Beijing

cloud | devops | self-signed

SSL Certificate
Issued By:
|- Common Name: aws-k8s-applet01@1595583716
Issued To:
|- Common Name: aws-k8s-applet01@1595583716

Supported SSL Versions
TLSv1.2

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 11 Aug 2020 02:50:14 GMT
Content-Length: 19
```

[redacted]
ec2-[redacted]ap-east-1.compute.amazonaws.com
Amazon.com
Added on 2020-08-11 05:06:59 GMT
Hong Kong

cloud | devops

SSL Certificate
Issued By:
|- Common Name: ip-172-31-41-195-ca@1558534600
Issued To:
|- Common Name: ip-172-31-41-195@1558534601

Supported SSL Versions
TLSv1.2

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 11 Aug 2020 05:06:59 GMT
Content-Length: 19
```

Pods Information Disclosure

https://[redacted]10250/pods

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON


```
kind:                                  "PodList"
apiVersion:                            "v1"
metadata:                              {}
items:
  0:
    metadata:
      name:                            "frontend-ubuntu"
      namespace:                       "[redacted]"
      selfLink:                        "/api/v1/namespaces/[redacted]/pods/frontend-ubuntu"
      uid:                             "2c65c663d56ced02c887aee81e6eba2e"
      creationTimestamp:               null
      annotations:
        kubernetes.io/config.hash:     "2c65c663d56ced02c887aee81e6eba2e"
        kubernetes.io/config.seen:     "2020-04-22T17:53:09.815344764Z"
        kubernetes.io/config.source:   "http"
    spec:
      containers:
        0:
          name:                        "[redacted]"
          image:                       "registry.[redacted]"
          ports:
            0:
              hostPort:                80
              containerPort:           80
              protocol:                "TCP"
```

ars TECHNICA

BIZ & IT | TECH | SCIENCE | POLICY | CARS | GAMING & CULTURE | STORE | FORUMS | SUBSCRIBE | SIGN IN

BEWARE —

Backdoored images downloaded 5 million times finally removed from Docker Hub

17 images posted by a single account over 10 months may have generated $90,000.

DAN GOODIN - 6/14/2018, 10:10 AM

Oren neu dag / Wikimedia

Enlarge

imperva

Products | Solutions | Support | Partners | Customers | Resources | Research Labs | About Us

Home > Blog > Hundreds of Vulnerable Docker Hosts Exploited by Cryptocurrency Miners

Research Labs: Application Security, Data Security

Hundreds of Vulnerable Docker Hosts Exploited by Cryptocurrency Miners

Vitaly Simonovich, Ori Nakar
Mar 4, 2019 • 4 mins read

Docker is a technology that allows you to perform operating system level virtualization. An incredible number of companies and production hosts are running Docker to develop, deploy and run applications inside containers.

“Sometimes, node in cluster expose their Docker API without authentication also private registry that can be reach by other users to exfiltrate images or push backdoored images”

Search Results

There are **79** CVE entries that match your search.

Name	Description
CVE-2020-8559	The Kubernetes kube-apiserver in versions v1.6-v1.15, and versions prior to v1.16.13, v1.17.9 and v1.18.6 are vulnerable to an unvalidated redirect on proxied upgrade requests that could allow an attacker to escalate privileges from a node compromise to a full cluster compromise.
CVE-2020-8558	The Kubelet and kube-proxy components in versions 1.1.0-1.16.10, 1.17.0-1.17.6, and 1.18.0-1.18.3 were found to contain a security issue which allows adjacent hosts to reach TCP and UDP services bound to 127.0.0.1 running on the node or in the node's network namespace. Such a service is generally thought to be reachable only by other processes on the same host, but due to this defeect, could be reachable by other hosts on the same LAN as the node, or by containers running on the same node as the service.
CVE-2020-8557	The Kubernetes kubelet component in versions 1.1-1.16.12, 1.17.0-1.17.8 and 1.18.0-1.18.5 do not account for disk usage by a pod which writes to its own /etc/hosts file. The /etc/hosts file mounted in a pod by kubelet is not included by the kubelet eviction manager when calculating ephemeral storage usage by a pod. If a pod writes a large amount of data to the /etc/hosts file, it could fill the storage space of the node and cause the node to fail.
CVE-2020-8555	The Kubernetes kube-controller-manager in versions v1.0-1.14, versions prior to v1.15.12, v1.16.9, v1.17.5, and version v1.18.0 are vulnerable to a Server Side Request Forgery (SSRF) that allows certain authorized users to leak up to 500 bytes of arbitrary information from unprotected endpoints within the master's host network (such as link-local or loopback services).
CVE-2020-8553	The Kubernetes ingress-nginx component prior to version 0.28.0 allows a user with the ability to create namespaces and to read and create ingress objects to overwrite the password file of another ingress which uses nginx.ingress.kubernetes.io/auth-type: basic and which has a hyphenated namespace or secret name.
CVE-2020-8552	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.
CVE-2020-7922	X.509 certificates generated by the MongoDB Enterprise Kubernetes Operator may allow an attacker with access to the Kubernetes cluster improper access to MongoDB instances. Customers who do not use X.509 authentication, and those who do not use the Operator to generate their X.509 certificates are unaffected.
CVE-2020-7010	Elastic Cloud on Kubernetes (ECK) versions prior to 1.1.0 generate passwords using a weak random number generator. If an attacker is able to determine when the current Elastic Stack cluster was deployed they may be able to more easily brute force the Elasticsearch credentials generated by ECK.
CVE-2020-5911	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the NGINX Controller installer starts the download of Kubernetes packages from an HTTP URL On Debian/Ubuntu system.
CVE-2020-4062	In Conjur OSS Helm Chart before 2.0.0, a recently identified critical vulnerability resulted in the installation of the Conjur Postgres database with an open port. This allows an attacker to gain full read & write access to the Conjur Postgres database, including escalating the attacker's privileges to assume full control. A malicious actor who knows the IP address and port number of the Postgres database and has access into the Kubernetes cluster where Conjur runs can gain full read & write access to the Postgres database. This enables the attacker to write a policy that allows full access to retrieve any secret. This Helm chart is a method to install Conjur OSS into a Kubernetes environment. Hence, the systems impacted are only Conjur OSS systems that were deployed using this chart. Other deployments including Docker and the CyberArk Dynamic Access Provider (DAP) are not affected. To remediate this vulnerability, clone the latest Helm Chart and follow the upgrade instructions. If you are not able to fully remediate this vulnerability immediately, you can mitigate some of the risk by making sure Conjur OSS is deployed on an isolated Kubernetes cluster or namespace. The term "isolated" refers to: - No other workloads besides Conjur OSS and its backend database are running in that Kubernetes cluster/namespace. - Kubernetes and helm access to the cluster/namespace is limited to security administrators via Role-Based Access Control (RBAC).
CVE-2020-2211	Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin 1.3 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.
CVE-2020-2121	Jenkins Google Kubernetes Engine Plugin 0.8.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.
CVE-2020-1753	A security flaw was found in Ansible Engine, all Ansible 2.7.x versions prior to 2.7.17, all Ansible 2.8.x versions prior to 2.8.11 and all Ansible 2.9.x versions prior to 2.9.7, when managing kubernetes using the k8s module. Sensitive parameters such as passwords and tokens are passed to kubectl from the command line, not using an environment variable or an input configuration file. This will disclose passwords and tokens from process list and no_log directive from debug module would not have any effect making these secrets being disclosed on stdout and log files.
CVE-2020-15127	In Contour (Ingress controller for Kubernetes) before version 1.7.0, a bad actor can shut down all instances of Envoy, essentially killing the entire ingress data plane. GET requests to /shutdown on port 8090 of the Envoy pod initiate Envoy's shutdown procedure. The shutdown procedure includes flipping the readiness endpoint to false, which removes Envoy from the routing pool. When running Envoy (For example on the host network, pod spec hostNetwork=true), the shutdown manager's endpoint is accessible to anyone on the network that can reach the Kubernetes node that's running Envoy. There is no authentication in place that prevents a rogue actor on the network from shutting down Envoy via the shutdown manager endpoint. Successful exploitation of this issue will lead to bad actors shutting down all instances of Envoy, essentially killing the entire ingress data plane. This is fixed in version 1.7.0.

4

Defending your Kubernetes Cluster

We will discover some tools to reduce attack surfaces and impact on your cluster when compromise or not.

“ Why need to defending our cluster?

- Preventing from attacker to compromise the cluster.
- Source code and API key leaks.
- Crypto miner malware.
- Deleting a cluster.
- Data breach.
- Etc.

Kube Hunter

- Open Source project from Aqua Security
- Written in Python language.
- Hunt for security weaknesses in Kubernetes clusters.
- Vulnerability Assessment for Kubernetes.
- Support with Docker deployment and Pod in cluster as job.

```
ubuntu@stealth:~/kube-hunter$ python3 kube_hunter
Choose one of the options below:
1. Remote scanning      (scans one or more specific IPs or DNS names)
2. Interface scanning   (scans subnets on all local network interfaces)
3. IP range scanning    (scans a given IP range)
Your choice: 1
Remotes (separated by a ','): 7e9b84e1-fde4-49fa-8957-922ddef3106d.k8s.ondigitalocean.com
2020-08-11 10:46:26,962 INFO kube_hunter.modules.report.collector Started hunting
2020-08-11 10:46:26,963 INFO kube_hunter.modules.report.collector Discovering Open Kubernetes Services
2020-08-11 10:46:35,408 INFO kube_hunter.modules.report.collector Found open service "API Server" at 7e9b84e1-fde4-49fa-8957-922ddef3106d.k8s.ondigitalocean.com:443
2020-08-11 10:46:35,639 INFO kube_hunter.modules.report.collector Found vulnerability "K8s Version Disclosure" in 7e9b84e1-fde4-49fa-8957-922ddef3106d.k8s.ondigitalocean.com:443

Nodes
+-------------+----------------------+
| TYPE        | LOCATION             |
+-------------+----------------------+
| Node/Master | 7e9b84e1-fde4-49fa-8 |
|             | 957-922ddef3106d.k8s |
|             | .ondigitalocean.com  |
+-------------+----------------------+

Detected Services
+------------+----------------------+----------------------+
| SERVICE    | LOCATION             | DESCRIPTION          |
+------------+----------------------+----------------------+
| API Server | 7e9b84e1-fde4-49fa-8 | The API server is in |
|            | 957-922ddef3106d.k8s | charge of all        |
|            | .ondigitalocean.com: | operations on the    |
|            | 443                  | cluster.             |
+------------+----------------------+----------------------+

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 |
+--------+----------------------+----------------------+----------------------+----------------------+----------+
| KHV002 | 7e9b84e1-fde4-49fa-8 | Information          | K8s Version          | The kubernetes       | v1.18.6  |
|        | 957-922ddef3106d.k8s | Disclosure           | Disclosure           | version could be     |          |
|        | .ondigitalocean.com: |                      |                      | obtained from the    |          |
|        | 443                  |                      |                      | /version endpoint    |          |
+--------+----------------------+----------------------+----------------------+----------------------+----------+
```

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	[illegible]:443	Unauthenticated Access	Unauthenticated access to API	The API Server port is accessible. Depending on your RBAC settings this could expose access to or control of your cluster.	b'{"kind":"APIVersions","versions":["v1" ...
KHV036	[illegible]:10250	Remote Code Execution	Anonymous Authentication	The kubelet is misconfigured, potentially allowing secure access to all requests on the kubelet, without the need to authenticate	
KHV002	[illegible]:443	Information Disclosure	K8s Version Disclosure	The kubernetes version could be obtained from the /version endpoint	v1.14.9-eks-f459c0
KHV002	[illegible]:443	Information Disclosure	K8s Version Disclosure	The kubernetes version could be obtained from the /version endpoint	v1.16.8-eks-e16311

CIS Benchmark?

- Security configuration guide.
- Best current practices for secure configuration.
- Can automated by tools like InSpec.
- A lot of hardening checklist to used at container level, system operation or software.

Overview of CIS Benchmarks and CIS-CAT Demo

Register for the Webinar
Tues. August 18 at 10:00 AM EDT
Tues. September 1 at 1:30 PM EDT

CIS Benchmarks FAQ

Access all Benchmarks

Operating Systems | Server Software | Cloud Providers | Mobile Devices | Network Devices | Desktop Software | Multi Function Print Devices

Currently showing ALL Technologies. Use the buttons above to filter the list.

Operating Systems Linux	**Aliyun Linux** Expand to see related content	Download CIS Benchmark Build Kit also available
Operating Systems Linux	**Amazon Linux** Expand to see related content	Download CIS Benchmark CIS Hardened Image and Build Kit also available
Cloud Providers	**Amazon Web Services** Expand to see related content	Download CIS Benchmark
Server Software Database Server	**Apache Cassandra** Expand to see related content	Download CIS Benchmark
Server Software Web Server	**Apache HTTP Server** Expand to see related content	Download CIS Benchmark
Server Software Web Server	**Apache Tomcat** Expand to see related content	Download CIS Benchmark

Feedback

Waiting for www.google.co.id...

kube-bench

Kube Bench

- Open Source project from Aqua Security
- Written in Golang.
- Automate compliance for your Kubernetes Cluster based on CIS Kubernetes Benchmark best practices

```
ubuntu@stealth:~/kube-bench$ kubectl apply -f job.yaml
job.batch/kube-bench created
ubuntu@stealth:~/kube-bench$ kubectl get pods
NAME                READY   STATUS              RESTARTS   AGE
kube-bench-bw47t    0/1     ContainerCreating   0          8s
ubuntu@stealth:~/kube-bench$ kubectl logs kube-bench-bw47t
[INFO] 4 Worker Node Security Configuration
[INFO] 4.1 Worker Node Configuration Files
[PASS] 4.1.1 Ensure that the kubelet service file permissions are set to 644 or more restrictive (Scored)
[PASS] 4.1.2 Ensure that the kubelet service file ownership is set to root:root (Scored)
[FAIL] 4.1.3 Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive (Scored)
[FAIL] 4.1.4 Ensure that the proxy kubeconfig file ownership is set to root:root (Scored)
[PASS] 4.1.5 Ensure that the kubelet.conf file permissions are set to 644 or more restrictive (Scored)
[PASS] 4.1.6 Ensure that the kubelet.conf file ownership is set to root:root (Scored)
[FAIL] 4.1.7 Ensure that the certificate authorities file permissions are set to 644 or more restrictive (Scored)
[FAIL] 4.1.8 Ensure that the client certificate authorities file ownership is set to root:root (Scored)
[PASS] 4.1.9 Ensure that the kubelet configuration file has permissions set to 644 or more restrictive (Scored)
[PASS] 4.1.10 Ensure that the kubelet configuration file ownership is set to root:root (Scored)
[INFO] 4.2 Kubelet
[FAIL] 4.2.1 Ensure that the --anonymous-auth argument is set to false (Scored)
[FAIL] 4.2.2 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[FAIL] 4.2.3 Ensure that the --client-ca-file argument is set as appropriate (Scored)
[FAIL] 4.2.4 Ensure that the --read-only-port argument is set to 0 (Scored)
[PASS] 4.2.5 Ensure that the --streaming-connection-idle-timeout argument is not set to 0 (Scored)
[FAIL] 4.2.6 Ensure that the --protect-kernel-defaults argument is set to true (Scored)
[PASS] 4.2.7 Ensure that the --make-iptables-util-chains argument is set to true (Scored)
[PASS] 4.2.8 Ensure that the --hostname-override argument is not set (Not Scored)
[WARN] 4.2.9 Ensure that the --event-qps argument is set to 0 or a level which ensures appropriate event capture (Not Scored)
[FAIL] 4.2.10 Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (Scored)
[PASS] 4.2.11 Ensure that the --rotate-certificates argument is not set to false (Scored)
[FAIL] 4.2.12 Ensure that the RotateKubeletServerCertificate argument is set to true (Scored)
[WARN] 4.2.13 Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers (Not Scored)
```

“

https://github.com/ramitsurana/awesome-kubernetes

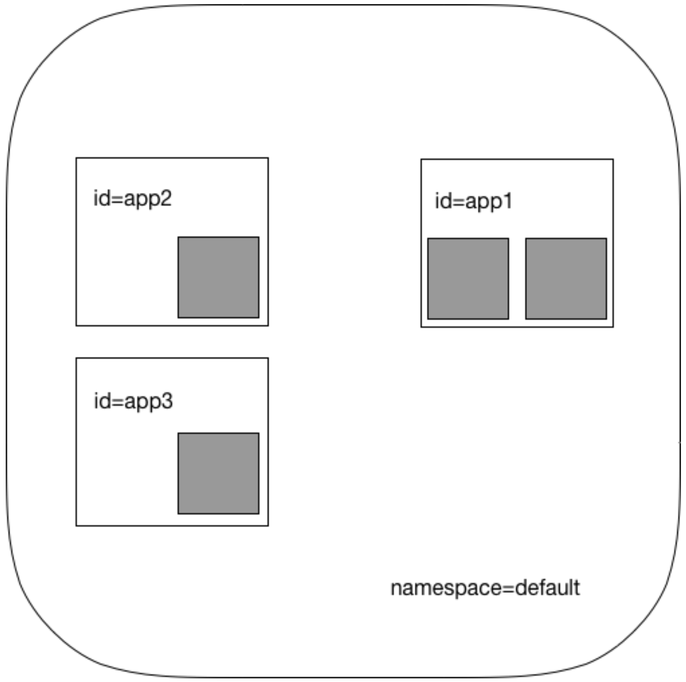
Calico

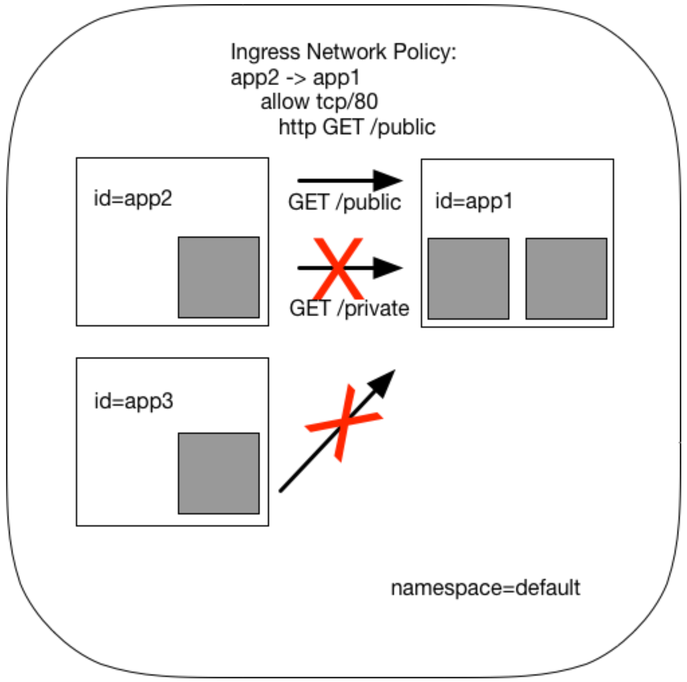
- Open Source project from Project Calico.
- Written in Golang.
- Scalable, simpler and flexible network policy.
- Uses L2 by default and possible to use L3.
- Project: https://github.com/projectcalico/calico

Cilium

- Open Source project from Project Calico.
- Written in Golang.
- Use BPF as packet filter at the kernel level.
- Flexible and effective rules to applied.
- Support L3, L4 and L7.
- Project: https://github.com/cilium/cilium

Cilium at Application Layer (L7)





Security Best Practices

- Update Kubernetes component with patched version that affect by CVE.
- Do a compliance using CIS benchmark.
- Using Role Based Access Control (RBAC).
- Separate CI/CD or Private registry from production cluster.
- Run container with low privileged user not as root.
- Limiting the pod resources to prevent from DoS.
- Protecting cluster metadata.
- Pod Security Policy.
- Network Policy.
- Logging & Monitoring.
- Etc.

Q & A