KODEKLOUD

www.kodekloud.com

cks.kodekloud.com

Disclaimer

THE INFORMATION FOUND ON THE WEBSITE, E-LEARNING PLATFORM AND WITHIN THE ONLINE COURSES ARE FOR INFORMATIONAL PURPOSES ONLY. KODEKLOUD WILL NOT BE HELD RESPONSIBLE FOR ANY DAMAGES THAT MAY BE INCURRED BY YOU AS A RESULT OF YOUR USE OF SUCH INFORMATION. ALL INFORMATION AND CONTENT ON THE WEBSITE, E-LEARNING PLATFORM AND ONLINE COURSE IS COPYRIGHTED, AND MAY NOT BE REPUBLISHED, COPIED, SOLD OR POSTED ANYWHERE ONLINE OR IN PRINT. KODEKLOUD RESERVES THE RIGHT TO TAKE THE NECESSARY LEGAL ACTION TO PREVENT YOU FROM (RE)-PUBLISHING, COPYING, SELLING, POSTING OR PRINTING ANY COPYRIGHTED INFORMATION AND CONTENT AVAILABLE ON THE WEBSITE, E-LEARNING PLATFORM AND ONLINE COURSE.

For the full terms & conditions visit terms.kodekloud.com

For questions write to support@kodekloud.com

Notice

- This presentation is to refer to course contents only.
- Some of the slides are meant to be animated. So may not be displayed correctly.
- Do not copy and paste command, code or YAML files from this file as it may not be in the right format and may contain hidden characters
- For code refer to the solutions in the lab or the Git repository associated with this course or official Kubernetes documentation pages.
- Some of the code in this deck maybe hidden for brevity

https://github.com/kodekloudhub/certified-kubernetes-security-specialist-cks-course

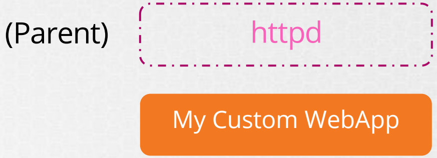
Minimize Base Image Footprint

Base vs Parent Image

Dockerfile – My Custom Webapp

Parent

```
FROM httpd

COPY index.html htdocs/index.html
```



Base vs Parent Image

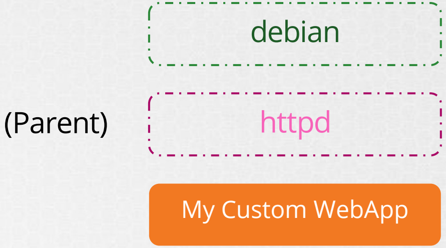
Dockerfile - httpd

```
FROM debian:buster-slim

ENV HTTPD_PREFIX /usr/local/apache2
ENV PATH $HTTPD_PREFIX/bin:$PATH
WORKDIR $HTTPD_PREFIX
<content trimmed>
```

Parent

Dockerfile – My Custom Webapp

```
FROM httpd

COPY index.html htdocs/index.html
```



Base vs Parent Image

Base

Dockerfile - debian:buster-slim

```
FROM scratch
ADD rootfs.tar.xz /
CMD ["bash"]
```

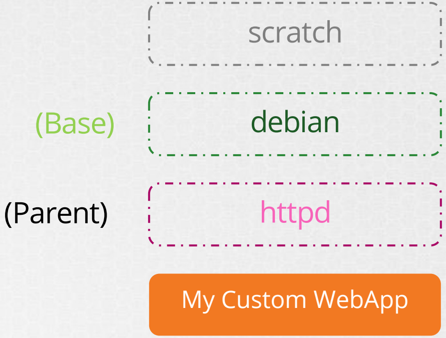
Dockerfile - httpd

```
FROM debian:buster-slim

ENV HTTPD_PREFIX /usr/local/apache2
ENV PATH $HTTPD_PREFIX/bin:$PATH
WORKDIR $HTTPD_PREFIX
<content trimmed>
```

Parent

Dockerfile – My Custom Webapp

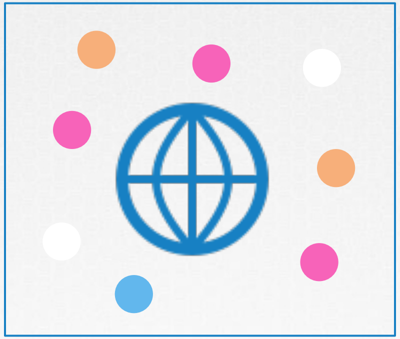
```
FROM httpd

COPY index.html htdocs/index.html
```



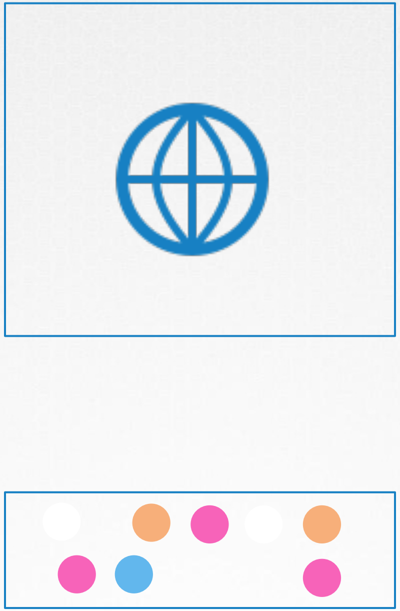
Modular

Modular

Persist State



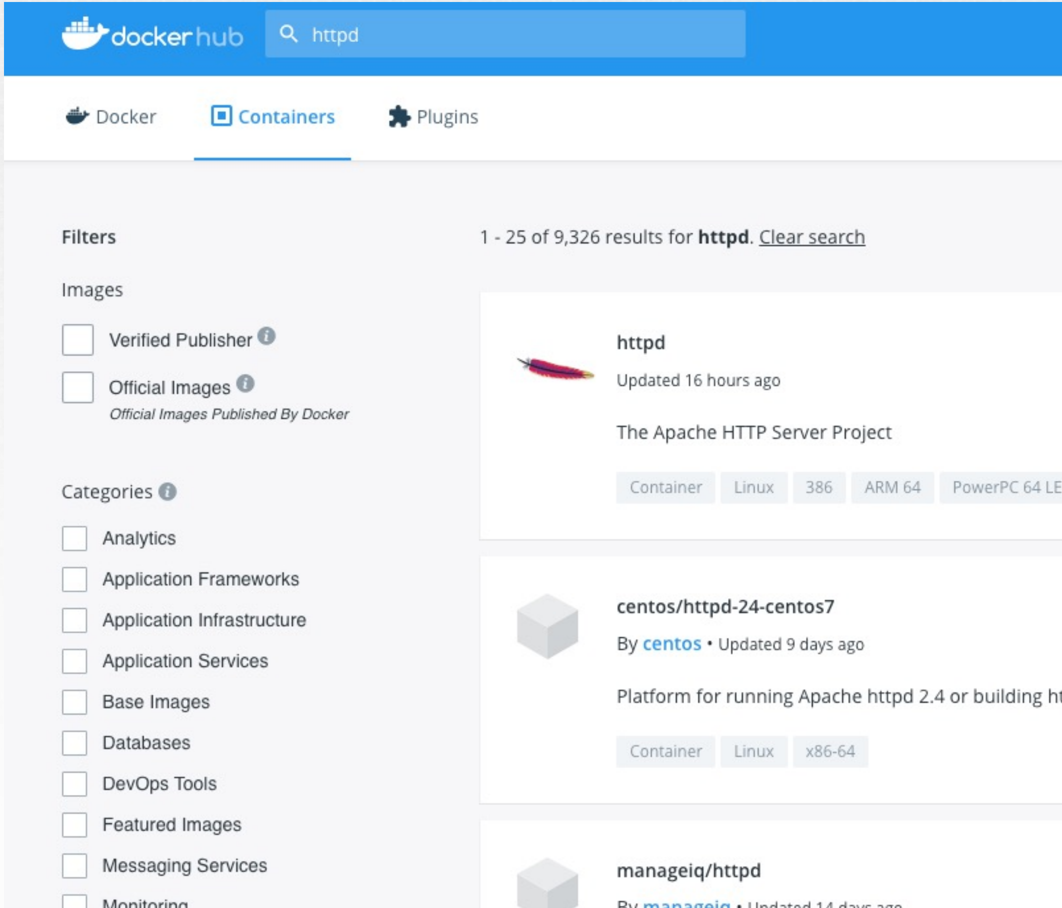
Persist State



Choosing a base image

Dockerfile – My Custom Webapp

```
FROM ??????

COPY index.html htdocs/index.html
```



Filters

Images

□ Verified Publisher

□ Official Images
Official Images Published By Docker

Categories

□ Analytics
□ Application Frameworks
□ Application Infrastructure
□ Application Services
□ Base Images
□ Databases
□ DevOps Tools
□ Featured Images
□ Messaging Services
□ Monitoring

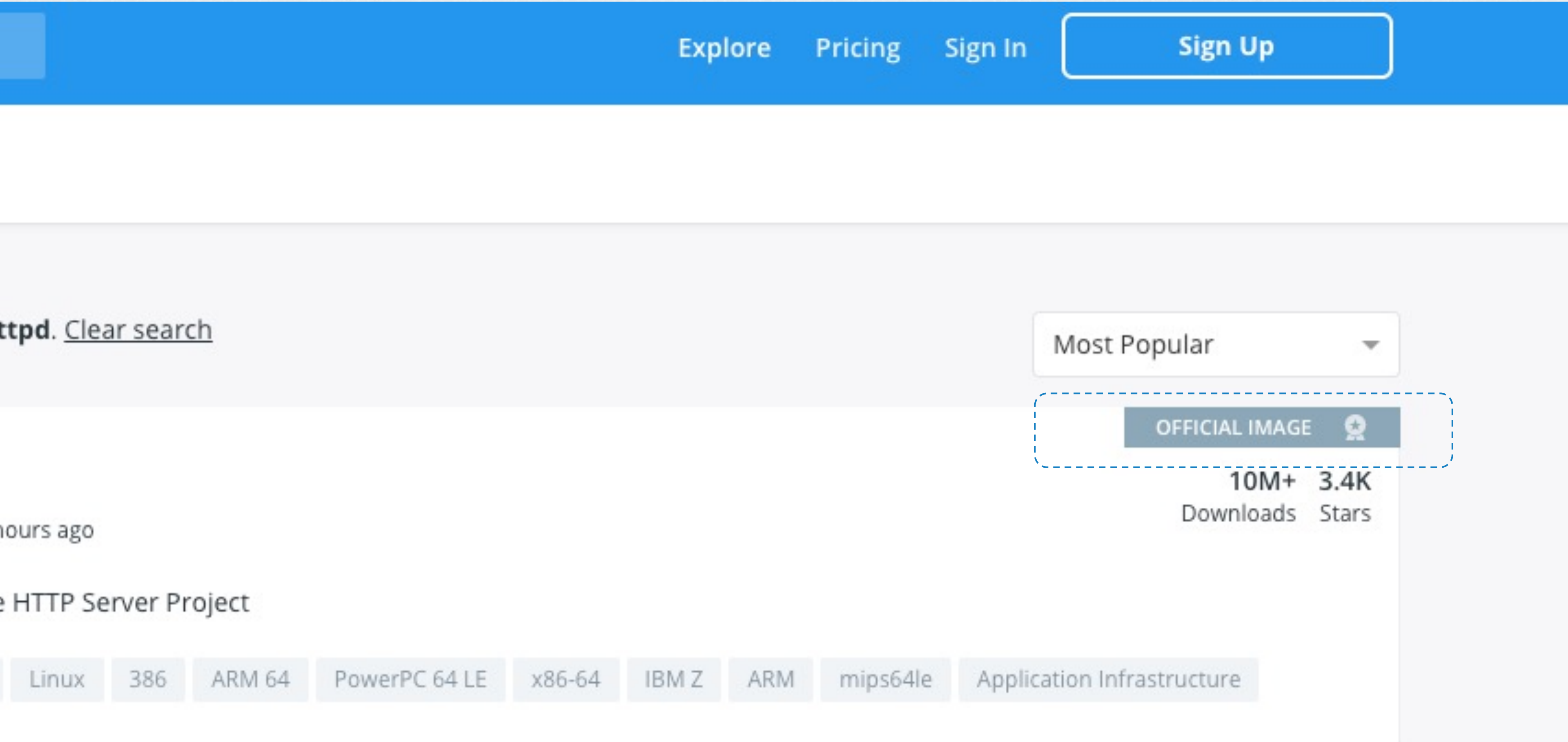
1 - 25 of 9,326 results for **httpd**. Clear search

httpd
Updated 16 hours ago
The Apache HTTP Server Project
Container | Linux | 386 | ARM 64 | PowerPC 64 LE

centos/httpd-24-centos7
By centos • Updated 9 days ago
Platform for running Apache httpd 2.4 or building ht
Container | Linux | x86-64

manageiq/httpd
By manageiq • Updated 14 days ago

Authenticity



ttpd. Clear search

10M+ Downloads

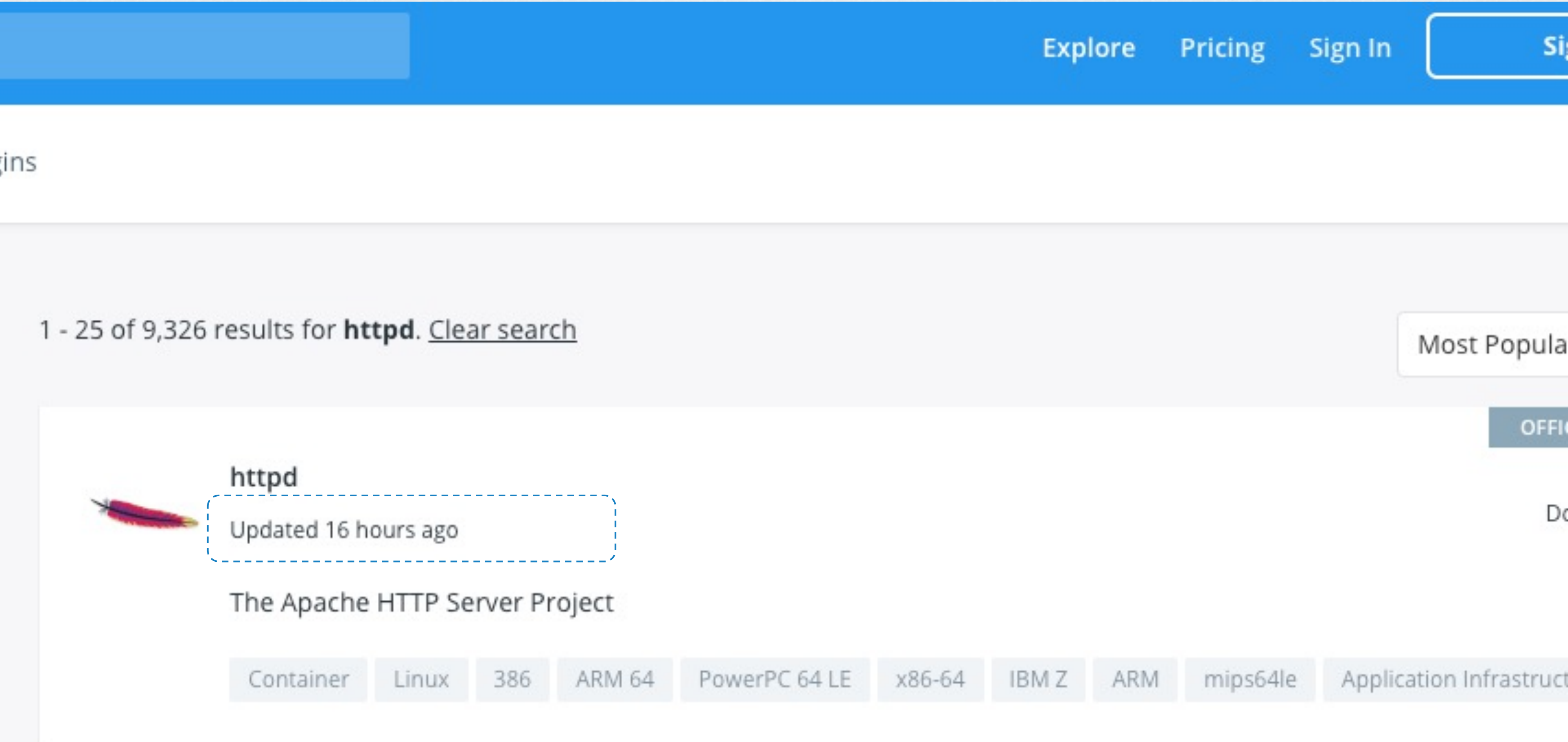
3.4K Stars

ours ago

e HTTP Server Project

Linux | 386 | ARM 64 | PowerPC 64 LE | x86-64 | IBM Z | ARM | mips64le | Application Infrastructure

Up-to-date



1 - 25 of 9,326 results for **httpd**. Clear search

httpd

Updated 16 hours ago

The Apache HTTP Server Project

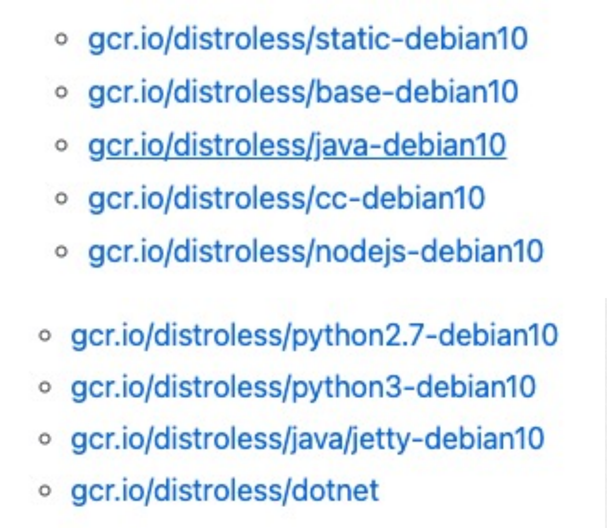
Slim/Minimal Images

1. Create slim/minimal images
2. Find an official minimal image that exists
3. Only install necessary packages
    - Remove Shells/Package Managers/Tools
4. Maintain different images for different environments:
    - Development – debug tools
    - Production - lean
5. Use multi-stage builds to create lean production ready images.

Distroless Docker Images

Contains:
- Application
- Runtime Dependencies

Does not contain:
- Package Managers
- Shells
- Network Tools
- Text editors
- Other unwanted programs

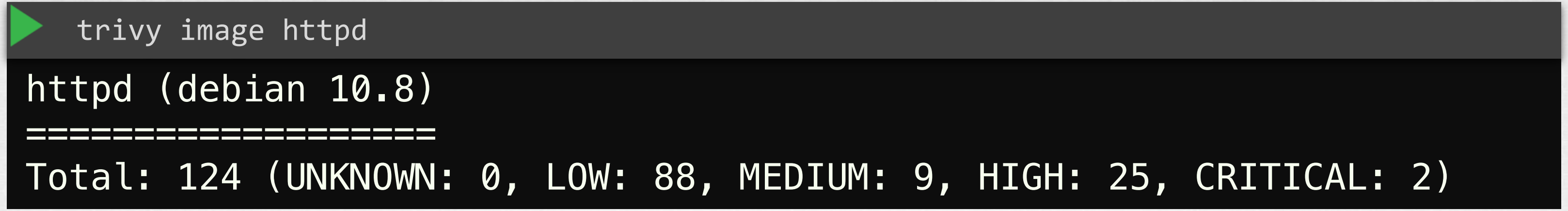


- gcr.io/distroless/static-debian10
- gcr.io/distroless/base-debian10
- gcr.io/distroless/java-debian10
- gcr.io/distroless/cc-debian10
- gcr.io/distroless/nodejs-debian10

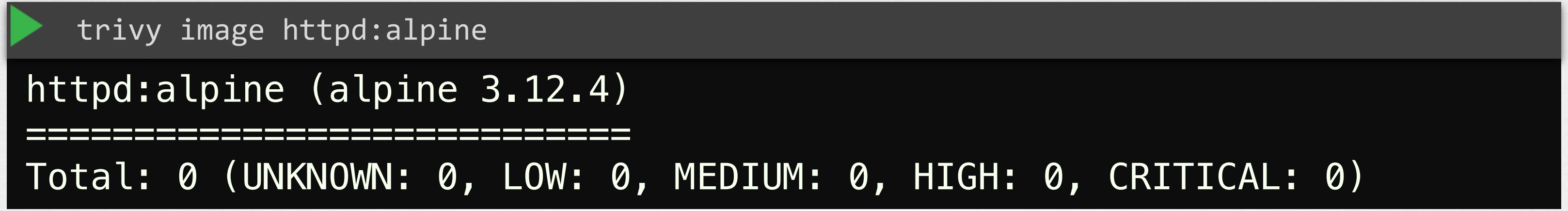
- gcr.io/distroless/python2.7-debian10
- gcr.io/distroless/python3-debian10
- gcr.io/distroless/java/jetty-debian10
- gcr.io/distroless/dotnet

https://github.com/GoogleContainerTools/distroless

Vulnerability Scanning



```
▶ trivy image httpd
httpd (debian 10.8)
===================
Total: 124 (UNKNOWN: 0, LOW: 88, MEDIUM: 9, HIGH: 25, CRITICAL: 2)
```



```
▶ trivy image httpd:alpine
httpd:alpine (alpine 3.12.4)
============================
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)
```

Hands-on Labs

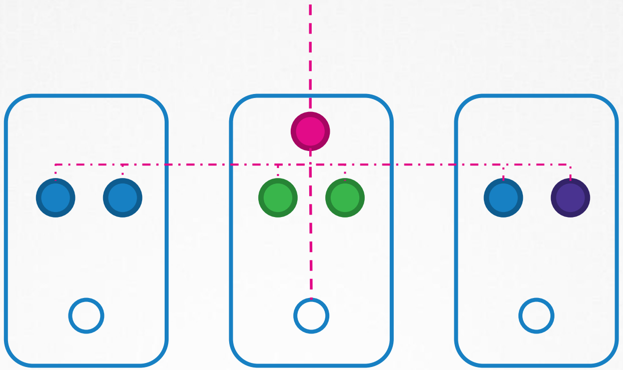
cks.kodekloud.com

KODEKLOUD

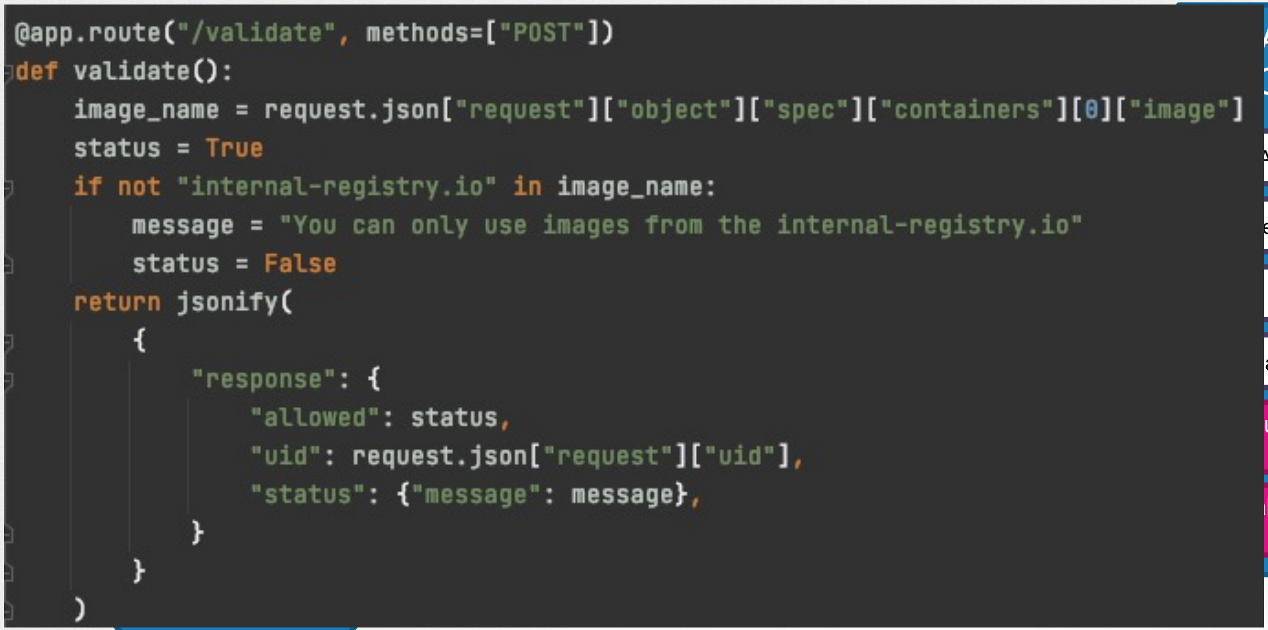
www.kodekloud.com

Whitelist Allowed Registries

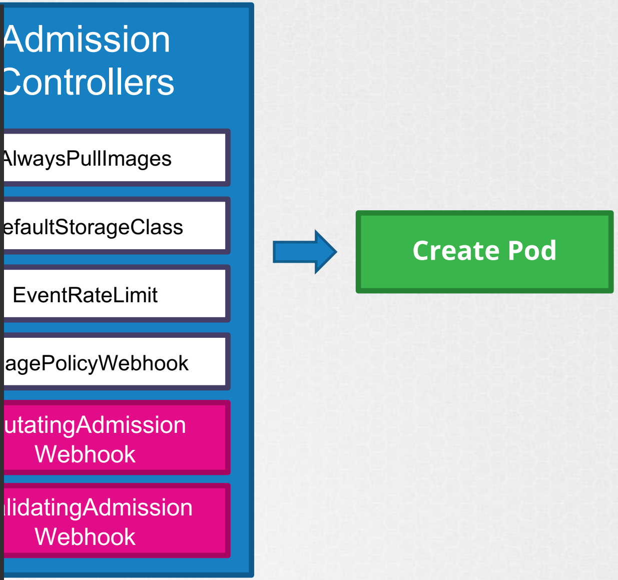
```yaml
apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
spec:

  containers:
   - name: sample-app
     image: some-registry.io/a-very-vulnerable-image
```



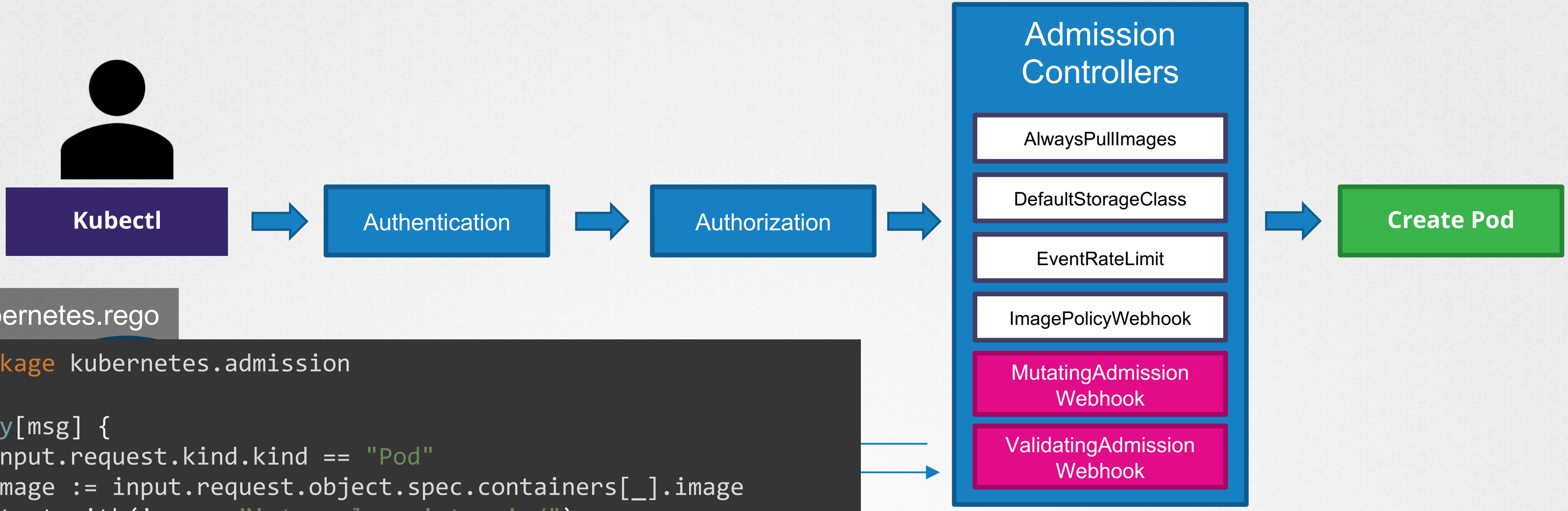
Admission Controllers



```
@app.route("/validate", methods=["POST"])
def validate():
    image_name = request.json["request"]["object"]["spec"]["containers"][0]["image"]
    status = True
    if not "internal-registry.io" in image_name:
        message = "You can only use images from the internal-registry.io"
        status = False
    return jsonify(
        {
            "response": {
                "allowed": status,
                "uid": request.json["request"]["uid"],
                "status": {"message": message},
            }
        }
    )
```



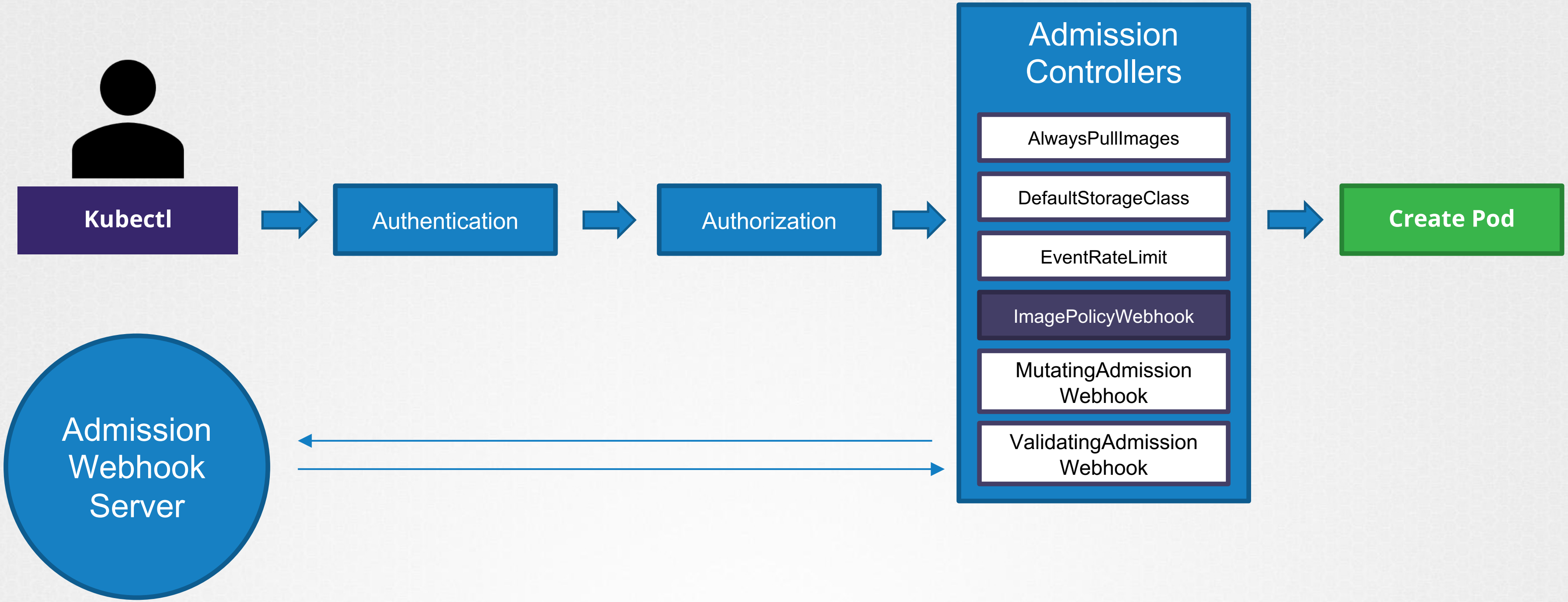
Admission Controllers



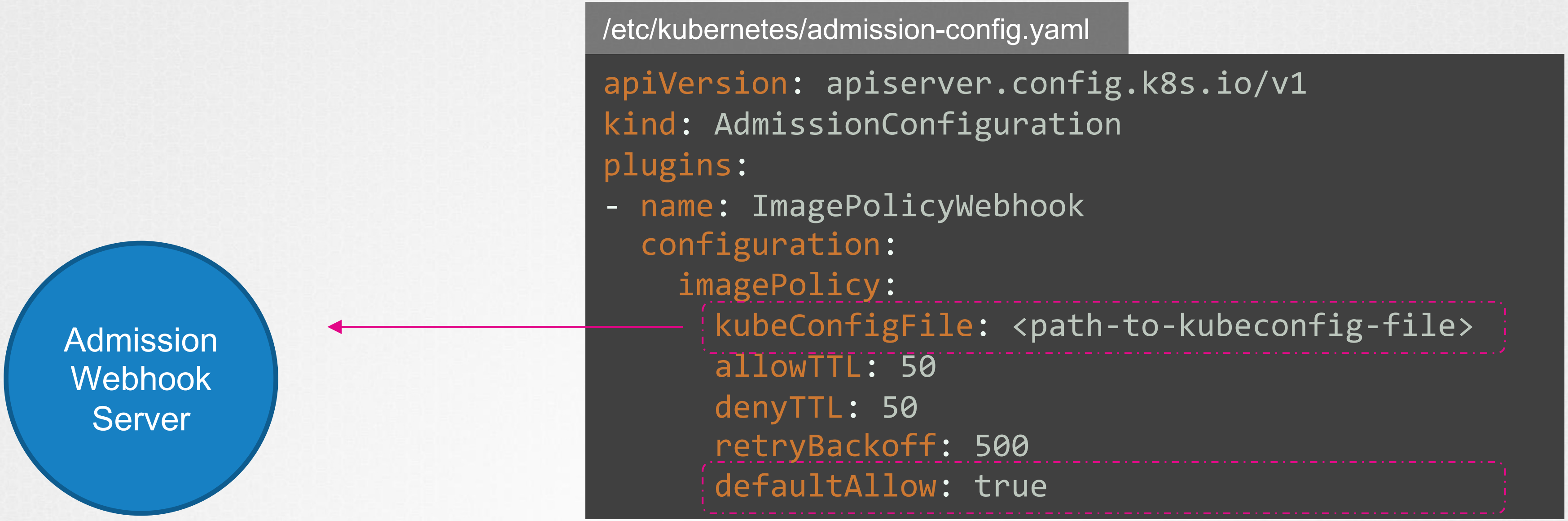
kubernetes.rego

```
package kubernetes.admission

deny[msg] {
  input.request.kind.kind == "Pod"
  image := input.request.object.spec.containers[_].image
  startswith(image, ”internal-registry.io/")
  msg := sprintf("image not from trusted registry")
}
```

Admission Controllers



Admission Configuration



/etc/kubernetes/admission-config.yaml

```yaml
apiVersion: apiserver.config.k8s.io/v1
kind: AdmissionConfiguration
plugins:
- name: ImagePolicyWebhook
  configuration:
    imagePolicy:
      kubeConfigFile: <path-to-kubeconfig-file>
      allowTTL: 50
      denyTTL: 50
      retryBackoff: 500
      defaultAllow: true
```

Admission Configuration

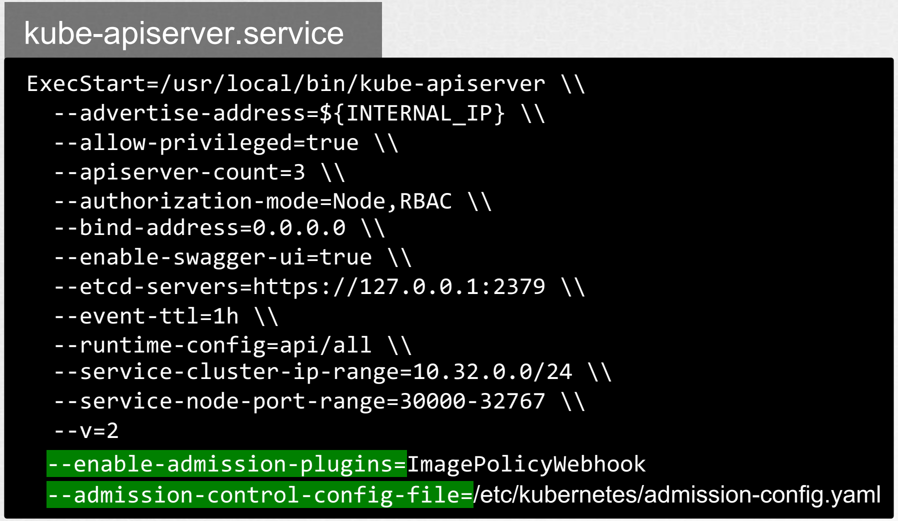
<path-to-kubeconfig-file>

```
clusters:
- name: name-of-remote-imagepolicy-service
  cluster:
    certificate-authority: /path/to/ca.pem
    server: https://images.example.com/policy

users:
- name: name-of-api-server
  user:
    client-certificate: /path/to/cert.pem
    client-key: /path/to/key.pem
```

/etc/kubernetes/admission-config.yaml

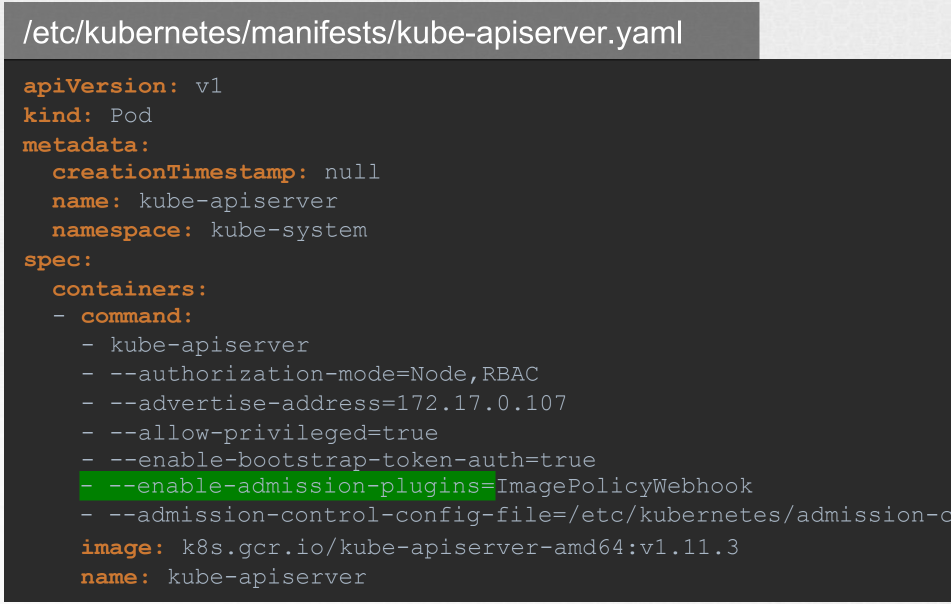
```
apiVersion: apiserver.config.k8s.io/v1
kind: AdmissionConfiguration
plugins:
- name: ImagePolicyWebhook
  configuration:
    imagePolicy:
      kubeConfigFile: <path-to-kubeconfig-
      allowTTL: 50
      denyTTL: 50
      retryBackoff: 500
      defaultAllow: true
```

Enable Admission Controllers



kube-apiserver.service

```
ExecStart=/usr/local/bin/kube-apiserver \\
  --advertise-address=${INTERNAL_IP} \\
  --allow-privileged=true \\
  --apiserver-count=3 \\
  --authorization-mode=Node,RBAC \\
  --bind-address=0.0.0.0 \\
  --enable-swagger-ui=true \\
  --etcd-servers=https://127.0.0.1:2379 \\
  --event-ttl=1h \\
  --runtime-config=api/all \\
  --service-cluster-ip-range=10.32.0.0/24 \\
  --service-node-port-range=30000-32767 \\
  --v=2
  --enable-admission-plugins=ImagePolicyWebhook
  --admission-control-config-file=/etc/kubernetes/admission-config.yaml
```



/etc/kubernetes/manifests/kube-apiserver.yaml

```
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: null
  name: kube-apiserver
  namespace: kube-system
spec:
  containers:
  - command:
    - kube-apiserver
    - --authorization-mode=Node,RBAC
    - --advertise-address=172.17.0.107
    - --allow-privileged=true
    - --enable-bootstrap-token-auth=true
    - --enable-admission-plugins=ImagePolicyWebhook
    - --admission-control-config-file=/etc/kubernetes/admission-c
    image: k8s.gcr.io/kube-apiserver-amd64:v1.11.3
    name: kube-apiserver
```

References

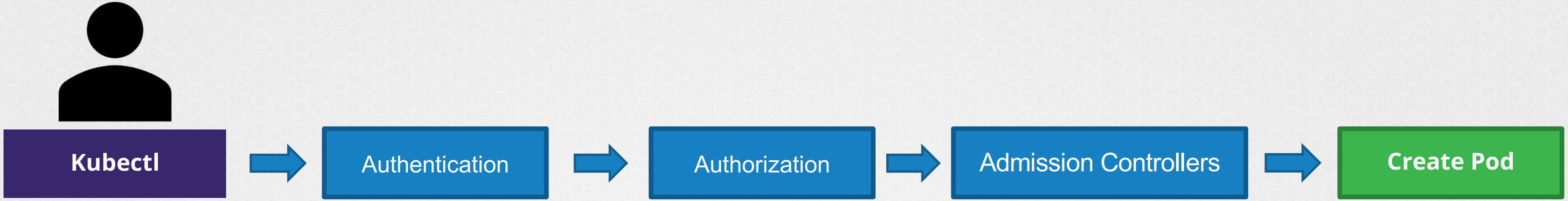
https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/#imagepolicywebhook

Hands-on Labs

cks.kodekloud.com

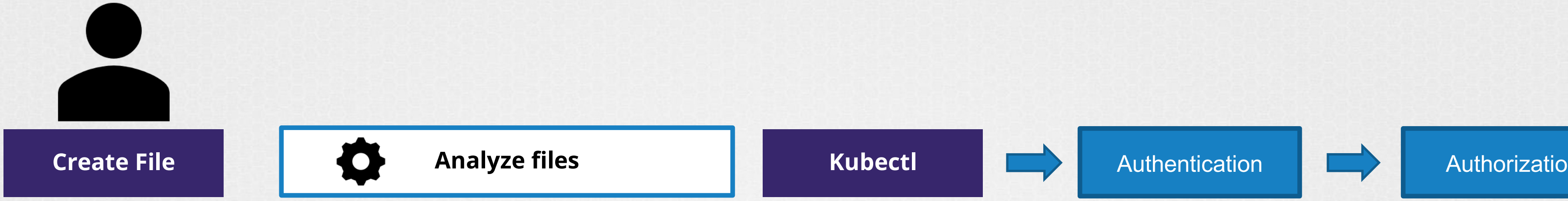
www.kodekloud.com

Use static analysis of user workloads



```yaml
apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
spec:
  containers:
   - name: ubuntu
     image: ubuntu
     command: ["sleep", "3600"]
     securityContext:
       privileged: True
       runAsUser: 0
       capabilities:
          add: ["CAP_SYS_BOOT"]
   volumes:
   - name: data-volume
     hostPath:
        path: /data
        type: Directory
```

Static Analysis of User Workloads



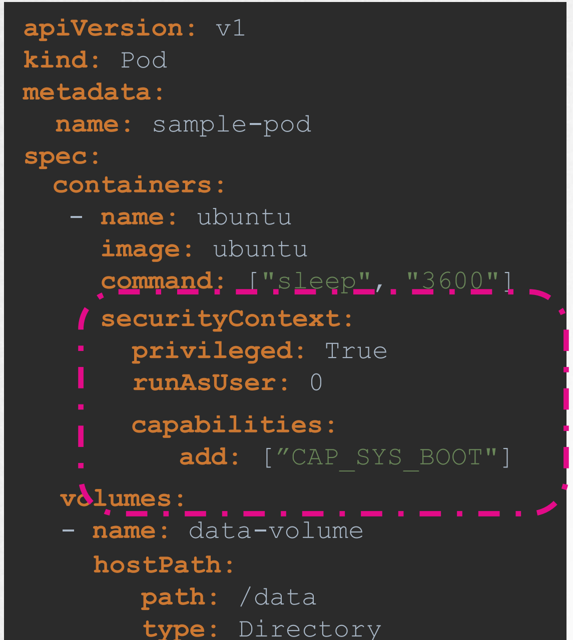
Create File

Analyze files

Kubectl

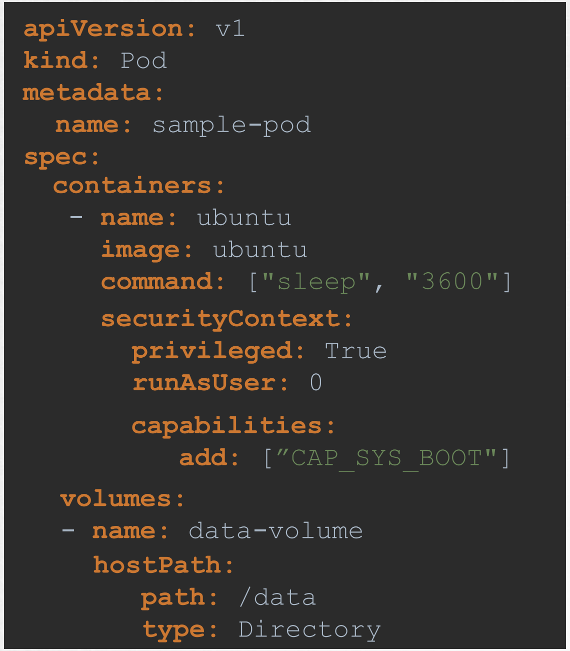
Authentication

Authorizatio



```
apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
spec:
  containers:
   - name: ubuntu
     image: ubuntu
     command: ["sleep", "3600"]
     securityContext:
       privileged: True
       runAsUser: 0
       capabilities:
          add: [”CAP_SYS_BOOT"]
  volumes:
  - name: data-volume
    hostPath:
       path: /data
       type: Directory
```

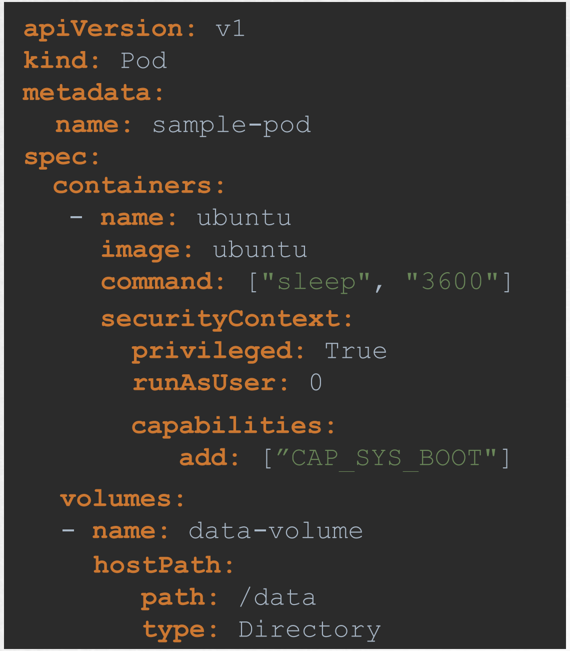
kubesec



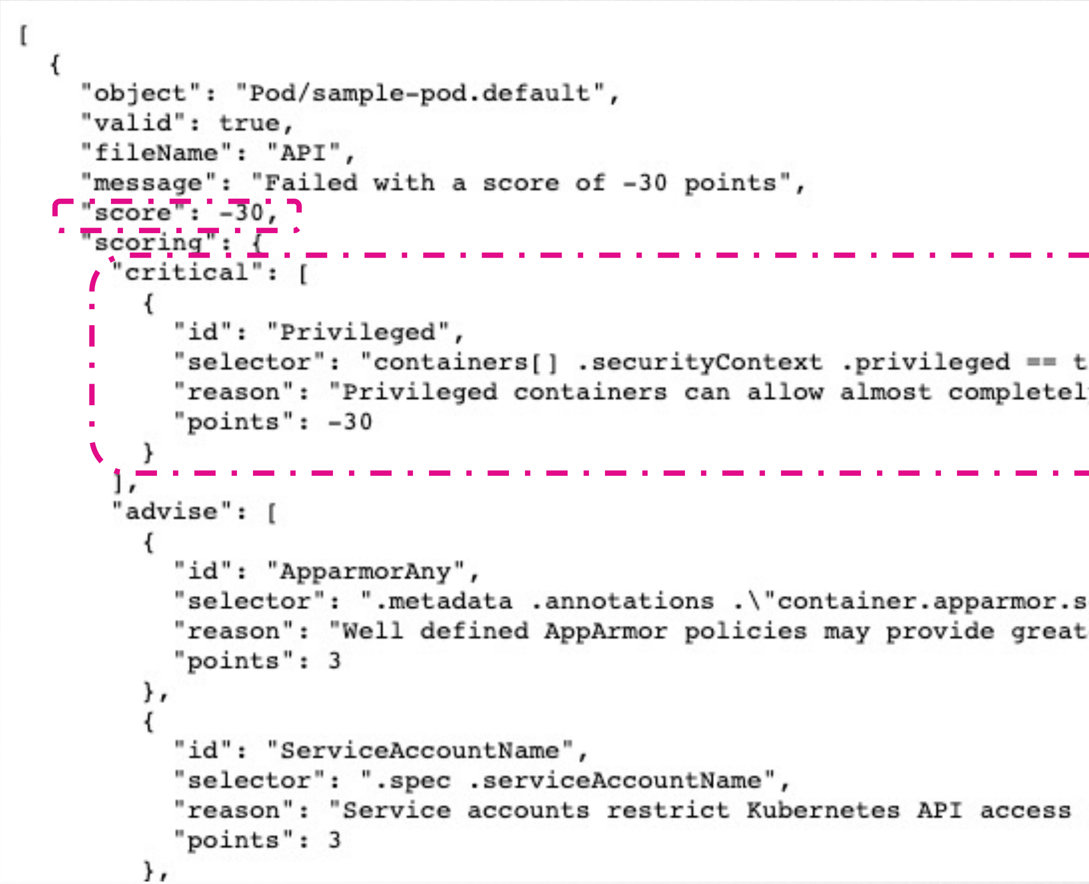
```
apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
spec:
  containers:
   - name: ubuntu
     image: ubuntu
     command: ["sleep", "3600"]
     securityContext:
       privileged: True
       runAsUser: 0
       capabilities:
          add: [”CAP_SYS_BOOT"]
  volumes:
  - name: data-volume
    hostPath:
       path: /data
       type: Directory
```

https://kubesec.io/

kubesec



```yaml
apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
spec:
  containers:
   - name: ubuntu
     image: ubuntu
     command: ["sleep", "3600"]
     securityContext:
       privileged: True
       runAsUser: 0
       capabilities:
          add: ["CAP_SYS_BOOT"]
  volumes:
  - name: data-volume
    hostPath:
       path: /data
       type: Directory
```



```
[
  {
    "object": "Pod/sample-pod.default",
    "valid": true,
    "fileName": "API",
    "message": "Failed with a score of -30 points",
    "score": -30,
    "scoring": {
      "critical": [
        {
          "id": "Privileged",
          "selector": "containers[] .securityContext .privileged == t
          "reason": "Privileged containers can allow almost completel
          "points": -30
        }
      ],
      "advise": [
        {
          "id": "ApparmorAny",
          "selector": ".metadata .annotations .\"container.apparmor.s
          "reason": "Well defined AppArmor policies may provide great
          "points": 3
        },
        {
          "id": "ServiceAccountName",
          "selector": ".spec .serviceAccountName",
          "reason": "Service accounts restrict Kubernetes API access
          "points": 3
        },
```

kubesec

```
kubesec scan pod.yaml
```

```
curl -sSX POST --data-binary @”pod.yaml" https://v2.kubesec.io/scan
```

```
kubesec http 8080 &
```

Hands-on Labs

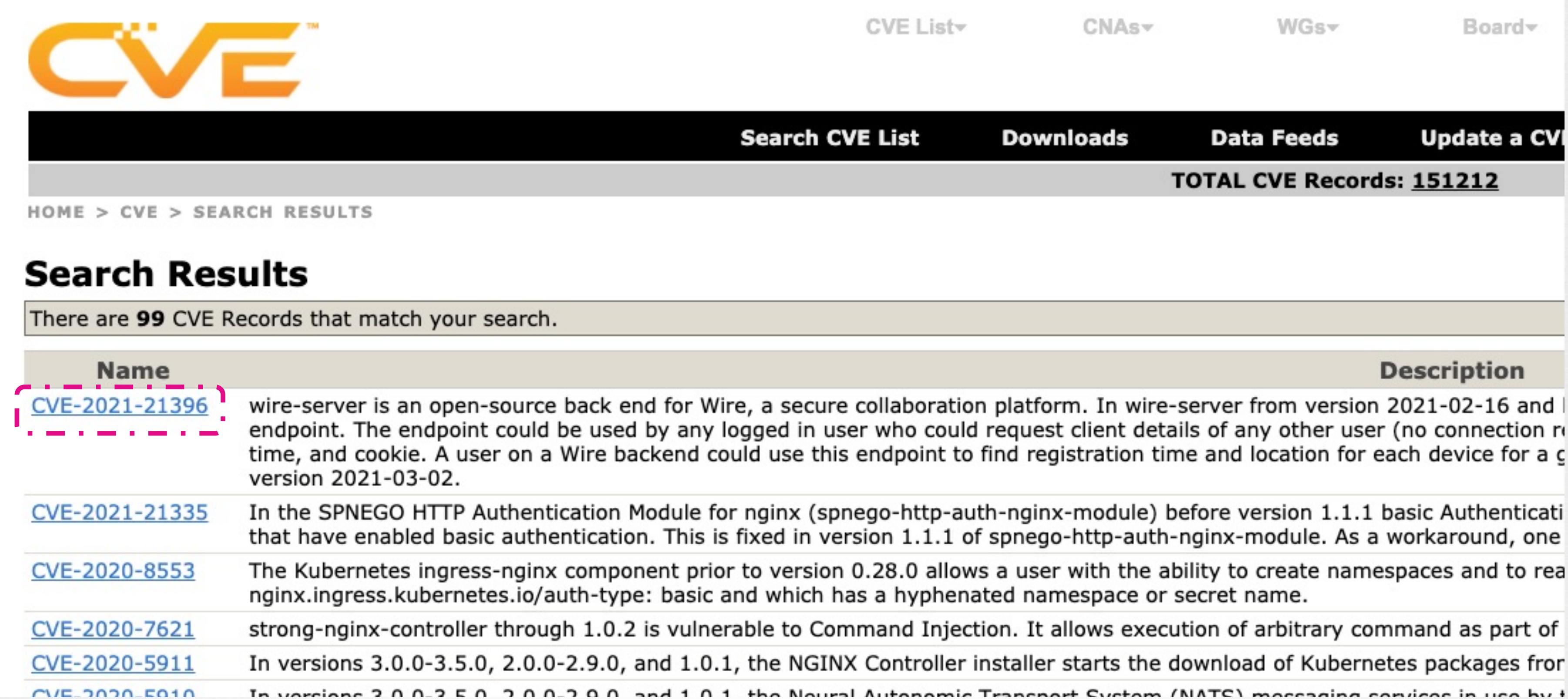
cks.kodekloud.com

KODEKLOUD

www.kodekloud.com

Scan Images for Known Vulnerabilities

Common Vulnerabilities and Exposures (CVE)



TOTAL CVE Records: 151212

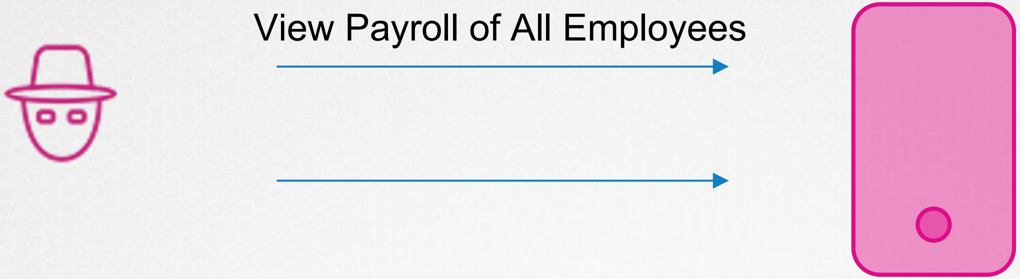
Search Results

There are **99** CVE Records that match your search.

Name	Description
CVE-2021-21396	wire-server is an open-source back end for Wire, a secure collaboration platform. In wire-server from version 2021-02-16 and l endpoint. The endpoint could be used by any logged in user who could request client details of any other user (no connection re time, and cookie. A user on a Wire backend could use this endpoint to find registration time and location for each device for a g version 2021-03-02.
CVE-2021-21335	In the SPNEGO HTTP Authentication Module for nginx (spnego-http-auth-nginx-module) before version 1.1.1 basic Authenticati that have enabled basic authentication. This is fixed in version 1.1.1 of spnego-http-auth-nginx-module. As a workaround, one
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 rea nginx.ingress.kubernetes.io/auth-type: basic and which has a hyphenated namespace or secret name.
CVE-2020-7621	strong-nginx-controller through 1.0.2 is vulnerable to Command Injection. It allows execution of arbitrary command as part of
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 fror
CVE-2020-5910	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the Neural Autonomic Transport System (NATS) messaging services in use by t

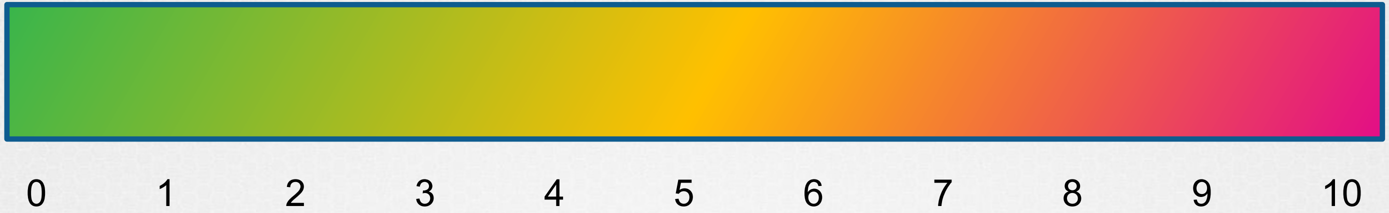
https://cve.mitre.org/

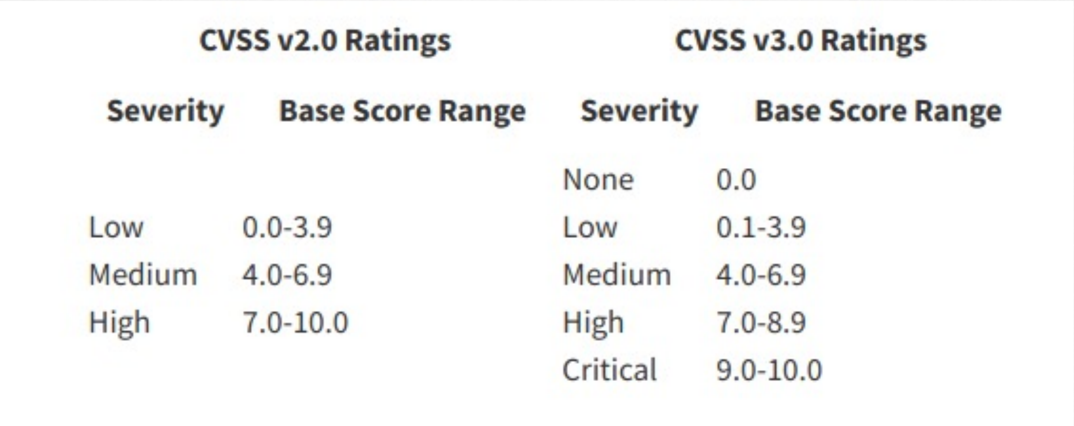
Common Vulnerabilities and Exposures (CVE)



View Payroll of All Employees

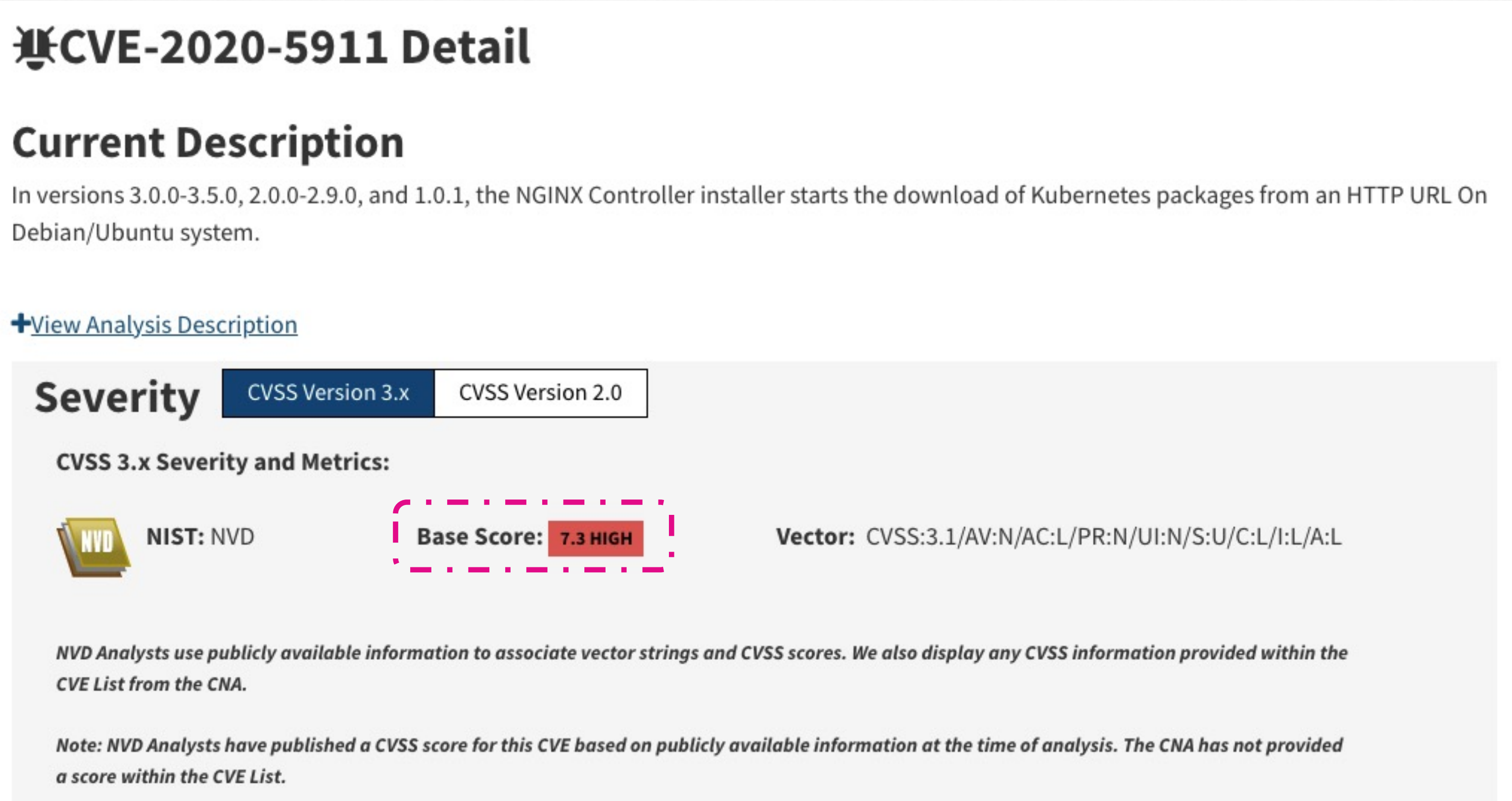
CVE Severity Scores





CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

CVE Severity Scores



CVE-2020-5911 Detail

Current Description

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.

+View Analysis Description

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD

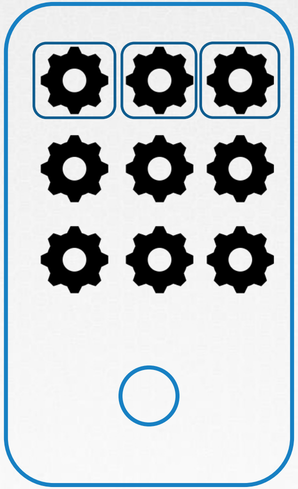
Base Score: 7.3 HIGH

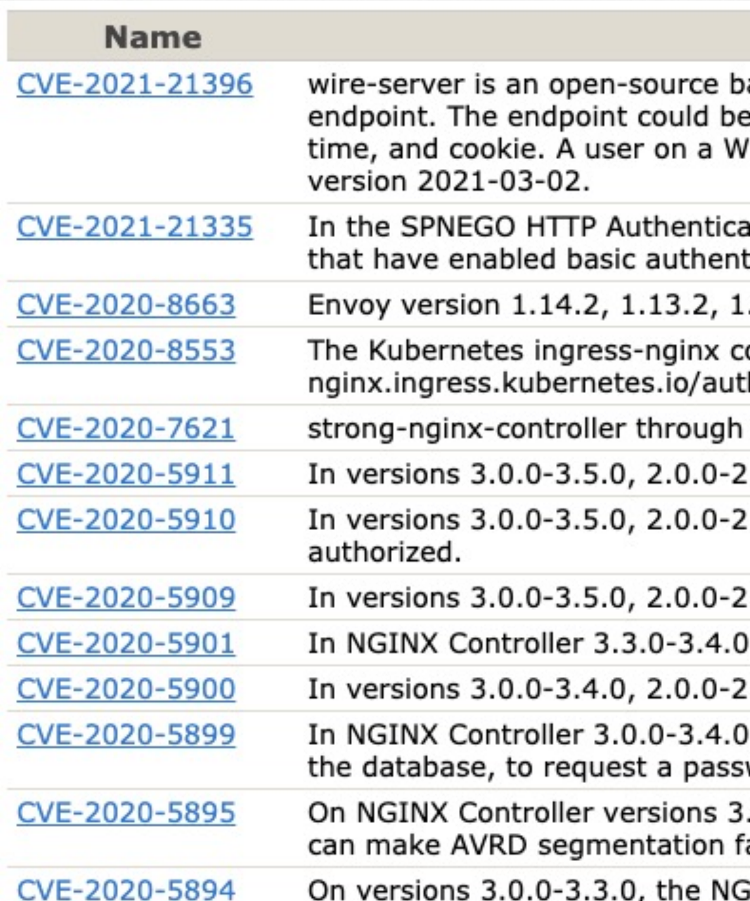
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

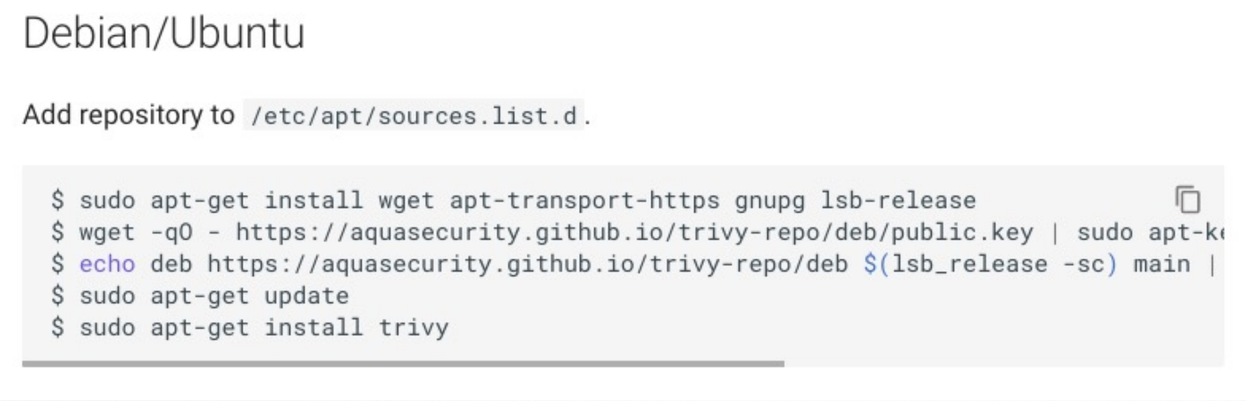
CVE Scanner





Name	
CVE-2021-21396	wire-server is an open-source ba endpoint. The endpoint could be time, and cookie. A user on a W version 2021-03-02.
CVE-2021-21335	In the SPNEGO HTTP Authentica that have enabled basic authent
CVE-2020-8663	Envoy version 1.14.2, 1.13.2, 1.
CVE-2020-8553	The Kubernetes ingress-nginx co nginx.ingress.kubernetes.io/autl
CVE-2020-7621	strong-nginx-controller through
CVE-2020-5911	In versions 3.0.0-3.5.0, 2.0.0-2
CVE-2020-5910	In versions 3.0.0-3.5.0, 2.0.0-2 authorized.
CVE-2020-5909	In versions 3.0.0-3.5.0, 2.0.0-2
CVE-2020-5901	In NGINX Controller 3.3.0-3.4.0
CVE-2020-5900	In versions 3.0.0-3.4.0, 2.0.0-2
CVE-2020-5899	In NGINX Controller 3.0.0-3.4.0 the database, to request a passw
CVE-2020-5895	On NGINX Controller versions 3. can make AVRD segmentation fa
CVE-2020-5894	On versions 3.0.0-3.3.0, the NG

Trivy



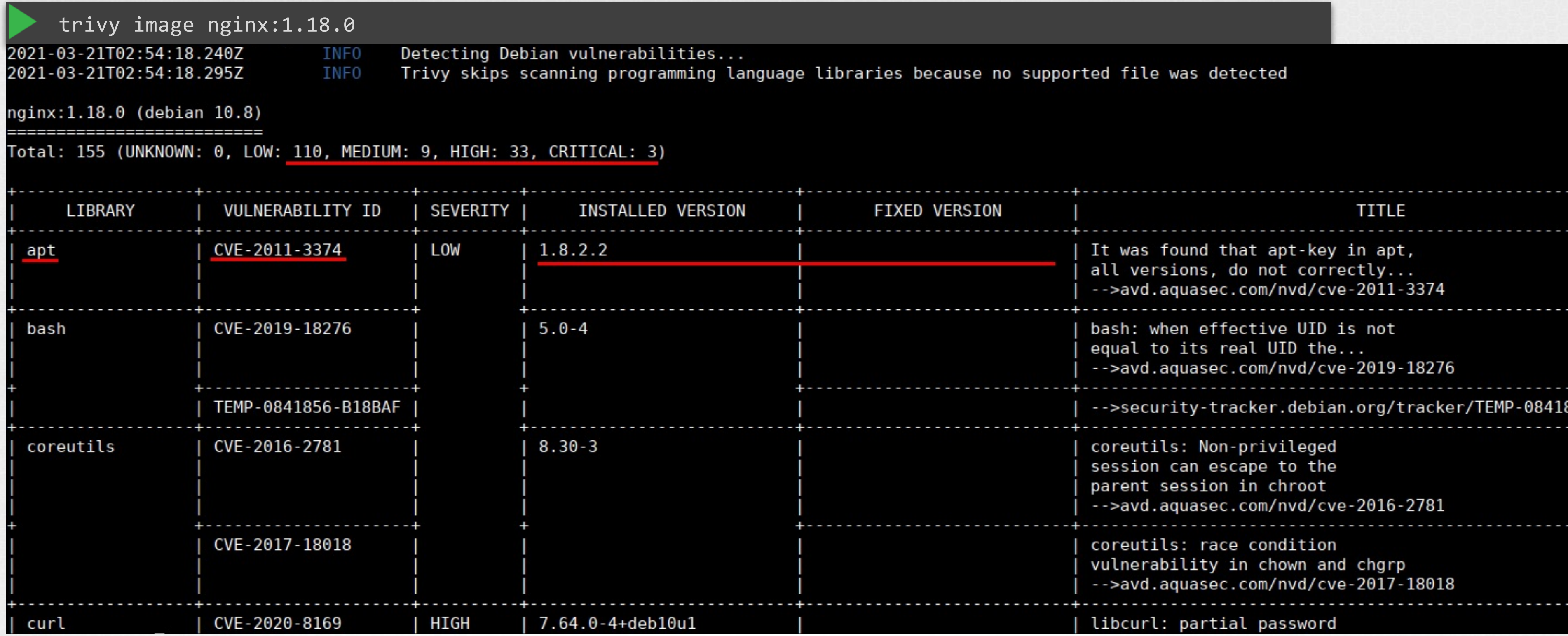
Debian/Ubuntu

Add repository to `/etc/apt/sources.list.d`.

```
$ sudo apt-get install wget apt-transport-https gnupg lsb-release
$ wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-ke
$ echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main |
$ sudo apt-get update
$ sudo apt-get install trivy
```

https://aquasecurity.github.io/trivy/latest/installation/

Trivy



```
▶ trivy image nginx:1.18.0
```

```
2021-03-21T02:54:18.240Z        INFO    Detecting Debian vulnerabilities...
2021-03-21T02:54:18.295Z        INFO    Trivy skips scanning programming language libraries because no supported file was detected

nginx:1.18.0 (debian 10.8)
==========================
Total: 155 (UNKNOWN: 0, LOW: 110, MEDIUM: 9, HIGH: 33, CRITICAL: 3)

+------------------+---------------------+----------+--------------------------+--------------------------+------------------------------------------------------
|     LIBRARY      |  VULNERABILITY ID   | SEVERITY |    INSTALLED VERSION     |      FIXED VERSION       |                          TITLE
+------------------+---------------------+----------+--------------------------+--------------------------+------------------------------------------------------
| apt              | CVE-2011-3374       | LOW      | 1.8.2.2                  |                          | It was found that apt-key in apt,
|                  |                     |          |                          |                          | all versions, do not correctly...
|                  |                     |          |                          |                          | -->avd.aquasec.com/nvd/cve-2011-3374
+------------------+---------------------+          +--------------------------+--------------------------+------------------------------------------------------
| bash             | CVE-2019-18276      |          | 5.0-4                    |                          | bash: when effective UID is not
|                  |                     |          |                          |                          | equal to its real UID the...
|                  |                     |          |                          |                          | -->avd.aquasec.com/nvd/cve-2019-18276
+                  +---------------------+          +                          +--------------------------+------------------------------------------------------
|                  | TEMP-0841856-B18BAF |          |                          |                          | -->security-tracker.debian.org/tracker/TEMP-08418
+------------------+---------------------+          +--------------------------+--------------------------+------------------------------------------------------
| coreutils        | CVE-2016-2781       |          | 8.30-3                   |                          | coreutils: Non-privileged
|                  |                     |          |                          |                          | session can escape to the
|                  |                     |          |                          |                          | parent session in chroot
|                  |                     |          |                          |                          | -->avd.aquasec.com/nvd/cve-2016-2781
+                  +---------------------+          +                          +--------------------------+------------------------------------------------------
|                  | CVE-2017-18018      |          |                          |                          | coreutils: race condition
|                  |                     |          |                          |                          | vulnerability in chown and chgrp
|                  |                     |          |                          |                          | -->avd.aquasec.com/nvd/cve-2017-18018
+------------------+---------------------+----------+--------------------------+--------------------------+------------------------------------------------------
| curl             | CVE-2020-8169       | HIGH     | 7.64.0-4+deb10u1         |                          | libcurl: partial password
```

Trivy

```
trivy image --severity CRITICAL nginx:1.18.0
```

```
trivy image --severity CRITICAL,HIGH nginx:1.18.0
```

```
trivy image --ignore-unfixed nginx:1.18.0
```

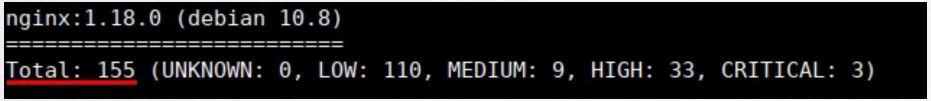
```
docker save nginx:1.18.0 > nginx.tar
```

```
trivy image --input archive.tar
```

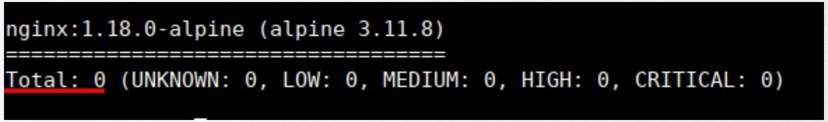
Trivy

nginx:1.18.0

nginx:1.18.0-alpine



```
nginx:1.18.0 (debian 10.8)
==========================
Total: 155 (UNKNOWN: 0, LOW: 110, MEDIUM: 9, HIGH: 33, CRITICAL: 3)
```



```
nginx:1.18.0-alpine (alpine 3.11.8)
===================================
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)
```

Best Practices

- Continuously rescan images
- Kubernetes Admission Controllers to scan images
- Have your own repository with pre-scanned images ready to go
- Integrate scanning into your CI/CD pipeline

Hands-on Labs

cks.kodekloud.com

KODEKLOUD

www.kodekloud.com