SciLifeLab

PROTEGER LAS CARGAS DE TRABAJO DE KUBERNETES: DEL CÓDIGO AL CLÚSTER

XOPS CONFERENCE 2024

ÁLVARO REVUELTA

SciLifeLab

ABOUT ME

Alvaro Revuelta.

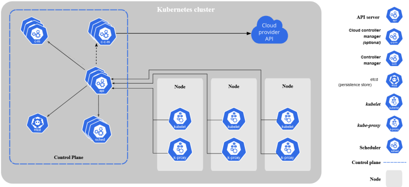
- Systems Developer
- Laboratory for Life Sciences - SciLifeLab

PRESENTATION STRUCTURE

1. Introduction
2. Inner Loop
3. Outer Loop
4. Other Security challenges
5. Other tools for security
6. Final

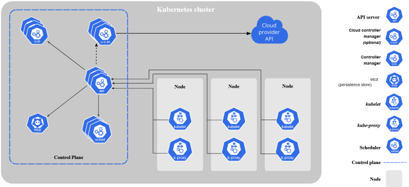
INTRODUCTION - ASSUMPTIONS

- Talk will cover both, developer and platform. But focus a bit more in security from a developer perspective.
- Assumes knowledge about containers and DevOps principles. Some knowledge about Kubernetes is also useful.



INTRODUCTION - WHY KUBERNETES

- Container management manually is difficult, leading to the rise of orchestration platforms like Kubernetes.
- It is a highly flexible tool, thus, it doesn’t make any assumptions and the engineers have to be aware of all the possible vulnerabilities.

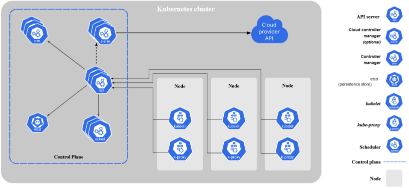


SciLifeLab

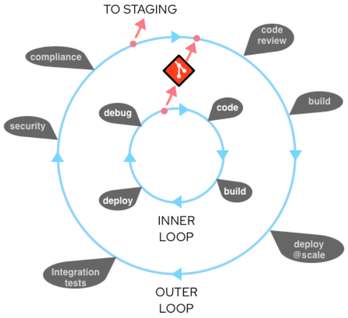
INTRODUCTION - WHY KUBERNETES

Perception on security issues in Kubernetes are underestimated.

- **53 %** of Organizations using Kubernetes experienced security issues; **55%** delayed deployments
  redhat.com/rhdc/managed-files/cl-state-of-kubernetes-security-report-2022-ebook-f31209-202205-en.pdf.
- ***63%*** of public code templates had improper configurations; ***96%*** of cloud applications had known vulnerabilities,
  unit42.paloaltonetworks.com/cloud-threat-report-2h-2021.



INTRODUCTION - INNER OUTER DEVELOPMENT LOOP



-

SOURCE: REDHAT

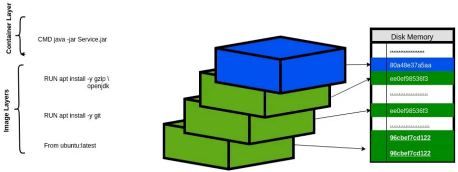
INNER LOOP

1. Write Code.
2. Build (containerize the application).
3. Debug Locally.

- This is where the Developer spends most of their time.

INNER LOOP: KEY CONSIDERATIONS

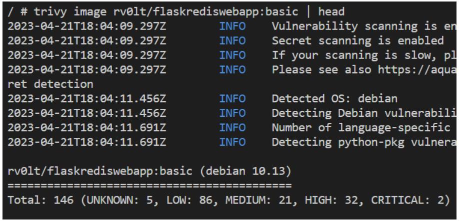
- Use a secure base image.
- Scan code dependencies for vulnerabilities (e.g., Trivy, Snyk).
- Optimize the application builds by doing good use of concepts such as the cache of layers.
- Increase productivity with Editor/IDE integration: VSCode Remote Containers



(**Source**: UnionFS : A File System of a Container)

INNER LOOP: SCAN IMAGE

trivy image imagetag:version



```
/ # trivy image rv0lt/flaskrediswebapp:basic | head
2023-04-21T18:04:09.297Z        INFO    Vulnerability scanning is en
2023-04-21T18:04:09.297Z        INFO    Secret scanning is enabled
2023-04-21T18:04:09.297Z        INFO    If your scanning is slow, pl
2023-04-21T18:04:09.297Z        INFO    Please see also https://aqua
ret detection
2023-04-21T18:04:11.456Z        INFO    Detected OS: debian
2023-04-21T18:04:11.456Z        INFO    Detecting Debian vulnerabili
2023-04-21T18:04:11.691Z        INFO    Number of language-specific
2023-04-21T18:04:11.691Z        INFO    Detecting python-pkg vulnera

rv0lt/flaskrediswebapp:basic (debian 10.13)
===========================================
Total: 146 (UNKNOWN: 5, LOW: 86, MEDIUM: 21, HIGH: 32, CRITICAL: 2)
```

(github.com/aquasecurity/trivy)

INNER LOOP: OPTIMIZE IMAGES

Minimizing the Number of Layers:

- Combine multiple RUN commands into one (e.g., chaining commands using &&).
- Removing unnecessary files during the build process (e.g., apt-get clean).
- Avoid using COPY to add files that won't be needed during runtime.

Using Smaller Base Images:

- Alpine Linux vs. Ubuntu: Trade-offs between size and functionality.
- Multi-stage builds: Using one image for building the application and another for the final image (stripped of development tools).

Caching Layers Efficiently:

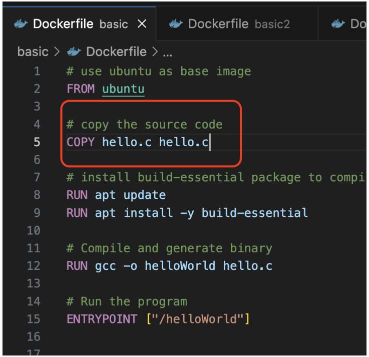
- Take advantage of layer caching by ordering Dockerfile instructions logically.
- Place less frequently changed commands earlier in the Dockerfile to maximize caching.

Removing Unnecessary Packages and Files:

- Remove temporary files, build dependencies, or logs to reduce image size.
- Clean up the file system after installations (e.g., rm -rf /var/lib/apt/lists/*).

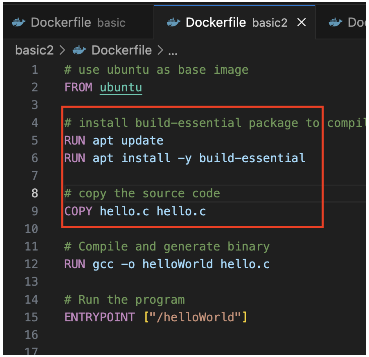
INNER LOOP: OPTIMIZE IMAGES

Subsequent building times: +60s



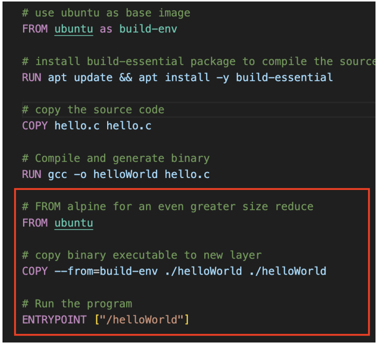
```
# use ubuntu as base image
FROM ubuntu

# copy the source code
COPY hello.c hello.c

# install build-essential package to compi
RUN apt update
RUN apt install -y build-essential

# Compile and generate binary
RUN gcc -o helloWorld hello.c

# Run the program
ENTRYPOINT ["/helloWorld"]
```

Subsequent building times: 1s



```
# use ubuntu as base image
FROM ubuntu

# install build-essential package to compil
RUN apt update
RUN apt install -y build-essential

# copy the source code
COPY hello.c hello.c

# Compile and generate binary
RUN gcc -o helloWorld hello.c

# Run the program
ENTRYPOINT ["/helloWorld"]
```

INNER LOOP: OPTIMIZE IMAGES



```
# use ubuntu as base image
FROM ubuntu as build-env

# install build-essential package to compile the source
RUN apt update && apt install -y build-essential

# copy the source code
COPY hello.c hello.c

# Compile and generate binary
RUN gcc -o helloWorld hello.c

# FROM alpine for an even greater size reduce
FROM ubuntu

# copy binary executable to new layer
COPY --from=build-env ./helloWorld ./helloWorld

# Run the program
ENTRYPOINT ["/helloWorld"]
```

WEIGHT IN MB REDUCED BY 4X TIMES

OUTER LOOP

1. Code Review
2. Automated testing
3. Production build
4. Compliance, and security checks,
5. Deployment to target environments.

- The platform engineer sets up the automation processes.

OUTER LOOP: CI - CD

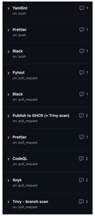
Continuous Integration:
Build-Test-Merge.

Continuous Delivery:
Someone decides when to push to prod.

Continuous Deployment:
Automatically deploy to prod.

OUTER LOOP: SECURITY IN CI/CD

- Scan code and images during builds.
- Block deployments for high-severity vulnerabilities.



Yamllint
on: push
1

Prettier
on: push
1

Black
on: push
1

Pytest
on: pull_request
1

Black
on: pull_request
1

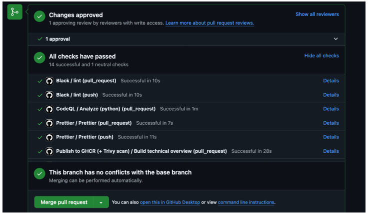
Publish to GHCR (+ Trivy scan)
on: pull_request
2

Prettier
on: pull_request
1

CodeQL
on: pull_request
2

Snyk
on: pull_request
2

Trivy - branch scan
on: pull_request
2



Changes approved
1 approving review by reviewers with write access. Learn more about pull request reviews.

Show all reviewers

✓ 1 approval

All checks have passed
14 successful and 1 neutral checks

Hide all checks

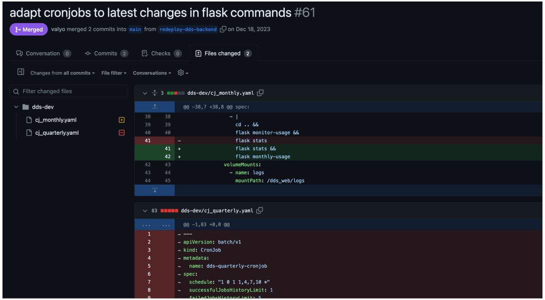
✓ Black / lint (pull_request) Successful in 10s Details
✓ Black / lint (push) Successful in 10s Details
✓ CodeQL / Analyze (python) (pull_request) Successful in 1m Details
✓ Prettier / Prettier (pull_request) Successful in 7s Details
✓ Prettier / Prettier (push) Successful in 11s Details
✓ Publish to GHCR (+ Trivy scan) / Build technical overview (pull_request) Successful in 28s Details

This branch has no conflicts with the base branch
Merging can be performed automatically.

Merge pull request

You can also open this in GitHub Desktop or view command line instructions.

OUTER LOOP - GITOPS AND CD



adapt cronjobs to latest changes in flask commands #61

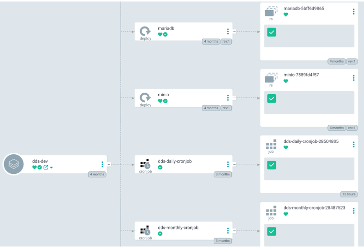
Merged valyo merged 2 commits into `main` from `redeploy-dds-backend` on Dec 18, 2023

3 dds-dev/cj_monthly.yaml

```
@@ -38,7 +38,8 @@ spec:
                  - |
                    cd .. &&
                    flask monitor-usage &&
-                   flask stats
+                   flask stats &&
+                   flask monthly-usage
                volumeMounts:
                  - name: logs
                    mountPath: /dds_web/logs
```

83 dds-dev/cj_quarterly.yaml

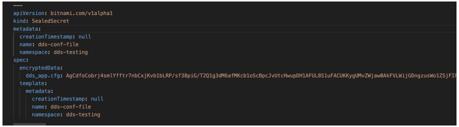
```
@@ -1,83 +0,0 @@
- ---
- apiVersion: batch/v1
- kind: CronJob
- metadata:
-   name: dds-quarterly-cronjob
- spec:
-   schedule: "1 0 1 1,4,7,10 *"
-   successfulJobsHistoryLimit: 1
-   failedJobsHistoryLimit: 5
```



ArgoCD

OUTER LOOP - SEALEDSECRETS

- The Kubernetes object Secrets, is not encrypted, it is encoded (base64)
- If we want to store our secrets in a repository, we can use sealed secrets.
- github.com/bitnami-labs/sealed-secrets
- *kubeseal -f secret.yaml -w sealsecret.yaml*



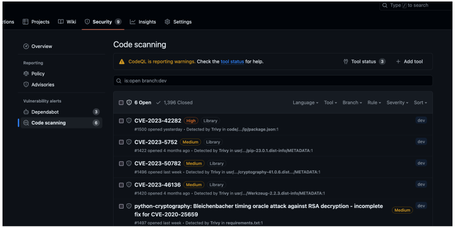
```yaml
---
apiVersion: bitnami.com/v1alpha1
kind: SealedSecret
metadata:
  creationTimestamp: null
  name: dds-conf-file
  namespace: dds-testing
spec:
  encryptedData:
    dds_app.cfg: AgCdfoCobrj4smlYfftr7nbCxjKvb1bLRP/sf38piG/T2Q1g3dM6afMKcb1oScBpcJvUtcHwupDH1AFUL8S1uFACUKKygUMvZWjaw0AkFVLWijGDngzusWo1ZSjFIF
  template:
    metadata:
      creationTimestamp: null
      name: dds-conf-file
      namespace: dds-testing
```

OUTER LOOP: CONTINUOUS VULNERABILITY MANAGEMENT

Why Continuous Scanning Matters

- The evolving threat landscape.
- New Vulnerabilities pop up quite often, CVE database

Integrate tools like Trivy into CI/CD pipelines to schedule scans of image repositories.



Code scanning

CodeQL is reporting warnings. Check the tool status for help.

is:open branch:dev

□ 6 Open ✓ 1,396 Closed

□ CVE-2023-42282 High Library dev
#1500 opened yesterday • Detected by Trivy in code/.../ip/package.json:1

□ CVE-2023-5752 Medium Library dev
#1422 opened 4 months ago • Detected by Trivy in usr/.../pip-23.0.1.dist-info/METADATA:1

□ CVE-2023-50782 Medium Library dev
#1496 opened last week • Detected by Trivy in usr/.../cryptography-41.0.6.dist.../METADATA:1

□ CVE-2023-46136 Medium Library dev
#1420 opened 4 months ago • Detected by Trivy in usr/.../Werkzeug-2.2.3.dist-info/METADATA:1

□ python-cryptography: Bleichenbacher timing oracle attack against RSA decryption - incomplete fix for CVE-2020-25659 Medium dev
#1497 opened last week • Detected by Trivy in requirements.txt:1

OTHER SECURITY CHALLENGES IN K8S

Default permissions

- By default, containers run as a root user.
- Malicious agents can exploit root access.
- We need to define security contexts to run as a non-privileged user and apply restrictions.

Communication between pods

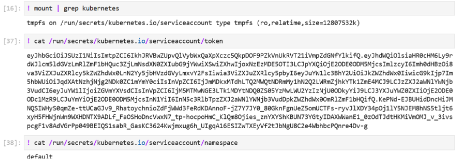
- By default, all resources can communicate with each other.
- We need to ensure resource separation to provide better security in case of breach.
- The solution is to limit traffic flow for better control.

SciLifeLab

OTHER SECURITY CHALLENGES IN K8S

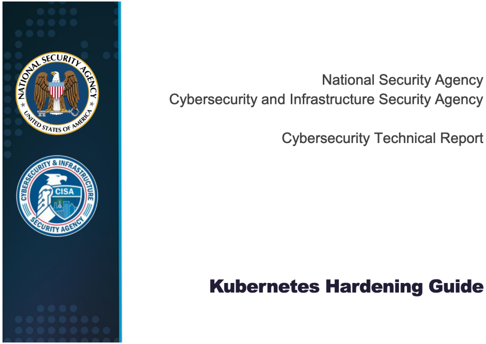
Service account tokens

- Containers are automatically created with a Token used to authenticate with the API.
- This means that, by default, containers can interact with the cluster and deploy resources.
- We need to disable mounting tokens if not needed (most cases).



```
[16]: ! mount | grep kubernetes

tmpfs on /run/secrets/kubernetes.io/serviceaccount type tmpfs (ro,relatime,size=12807532k)

[37]: ! cat /run/secrets/kubernetes.io/serviceaccount/token

eyJhbGciOiJSUzI1NiIsImtpZCI6IkhJRVBwZUpvQlVybWxQaXpXczc5QkpDOF9PZkVnUkRVT21iVmpZdGNfYlkifQ.eyJhdWQiOlsiaHR0cHM6Ly9r
dWJlcm5ldGVzLmRlZmF1bHQuc3ZjLmNsdXN0ZXIubG9jYWwiXSwiZXhwIjoxNzEzMDE5OTI3LCJpYXQiOjE2ODE0ODM5MjcsImlzcyI6Imh0dHBzOi8
va3ViZXJuZXRlcy5kZWZhdWx0LnN2Yy5jbHVzdGVyLmxvY2FsIiwia3ViZXJuZXRlcy5pbyI6eyJuYW1lc3BhY2UiOiJkZWZhdWx0IiwicG9kIjp7Im
5hbWUiOiJqdXAtNzhjNjg2NDk0ZC1mYmY0ciIsInVpZCI6IjJmMDkxMTdhLTQ2MWQtNDRmMy1hN2Q2LWRmZjhkYTk1ZmE4MCJ9LCJzZXJ2aWNlYWNjb
3VudCI6eyJuYW1lIjoiZGVmYXVsdCIsInVpZCI6IjM5MTMwNGE3LTk1MDYtNDQ0ZS05YzMwLWU2YzIzNjU0ODkyYiJ9LCJ3YXJuYWZ0ZXIiOjE2ODE0
ODc1MzR9LCJuYmYiOjE2ODE0ODM5MjcsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWNjb3VudDpkZWZhdWx0OmRlZmF1bHQifQ.KePNd-EJBUHidDncHiJM
NQSIWHyS0qmZe-ttUCaGJv9_RhatoychnioZdFjWWd3FeRdKDAnnoF-jZ7Y7JY0_80GknFgnUeZ5omUCTFs-ryvJlXDY34pOj1lY5NJEM8hNS5tljt6
xyH5FHWjnWn9WXHDNTX9ADLf_FaOSHoDncVwxN7_tp-hocpoHmC_KlQm8Ojies_znYXYShKBUN73YGtyIDAXWWanE1_0zOdTJdtHKMiVmOMJ_v_3ivs
pcgF1v8AdVGrPp049BEIQS1sabR_GasKC3624Kwjmxug6h_UIgqA16ESIZwTXEyVf2tJbNgU8C2e4WbhbcPQnre4Dv-g

[38]: ! cat /run/secrets/kubernetes.io/serviceaccount/namespace

default
```

VERY INTERESTING LECTURE



National Security Agency
Cybersecurity and Infrastructure Security Agency

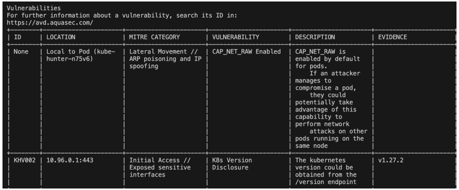
Cybersecurity Technical Report

Kubernetes Hardening Guide

KUBERNETS HARDENING GUIDE

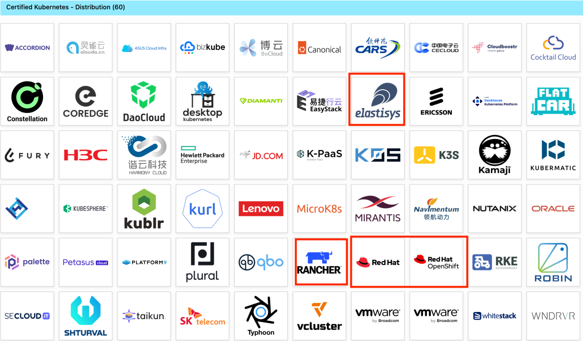
OTHER TOOLS FOR SECURITY

- Kube-hunter: Cluster Misconfiguration Detection; Pen-testing.
  - Same makers as Trivy
  - github.com/aquasecurity/kube-hunter
- Kubescape: similar than kube-hunter.
  - github.com/kubescape
- Kube-linter: Same as Trivy, but to find misconfiguration in k8s yaml files.
- Falco: Runtime Security.



```
Vulnerabilities
For further information about a vulnerability, search its ID in:
https://avd.aquasec.com/
+---------+-----------------------+-----------------------+-----------------------+-----------------------+-----------------------+
| ID      | LOCATION              | MITRE CATEGORY        | VULNERABILITY         | DESCRIPTION           | EVIDENCE              |
+---------+-----------------------+-----------------------+-----------------------+-----------------------+-----------------------+
| None    | Local to Pod (kube-   | Lateral Movement //   | CAP_NET_RAW Enabled   | CAP_NET_RAW is        |                       |
|         | hunter-n75v6)         | ARP poisoning and IP  |                       | enabled by default    |                       |
|         |                       | spoofing              |                       | for pods.             |                       |
|         |                       |                       |                       |     If an attacker    |                       |
|         |                       |                       |                       | manages to            |                       |
|         |                       |                       |                       | compromise a pod,     |                       |
|         |                       |                       |                       |     they could        |                       |
|         |                       |                       |                       | potentially take      |                       |
|         |                       |                       |                       | advantage of this     |                       |
|         |                       |                       |                       | capability to         |                       |
|         |                       |                       |                       | perform network       |                       |
|         |                       |                       |                       |     attacks on other  |                       |
|         |                       |                       |                       | pods running on the   |                       |
|         |                       |                       |                       | same node             |                       |
+---------+-----------------------+-----------------------+-----------------------+-----------------------+-----------------------+
| KHV002  | 10.96.0.1:443         | Initial Access //     | K8s Version           | The kubernetes        | v1.27.2               |
|         |                       | Exposed sensitive     | Disclosure            | version could be      |                       |
|         |                       | interfaces            |                       | obtained from the     |                       |
|         |                       |                       |                       | /version endpoint     |                       |
```

CNCF LANDSCAPE



Certified Kubernetes - Distribution (60)

OFFICIAL COMPLIANT KUBERNETES CNCF.IO

FINAL

CONTACT:
LINKEDIN - ALVARO REVUELTA MARTINEZ
ALVARO.REVUELTA@SCILIFELAB.UU.SE

FINAL

Q & A