Java on Kubernetes

What I wish I knew first

Alberto C. Ríos

@Albertoimpl

Abel Salgado

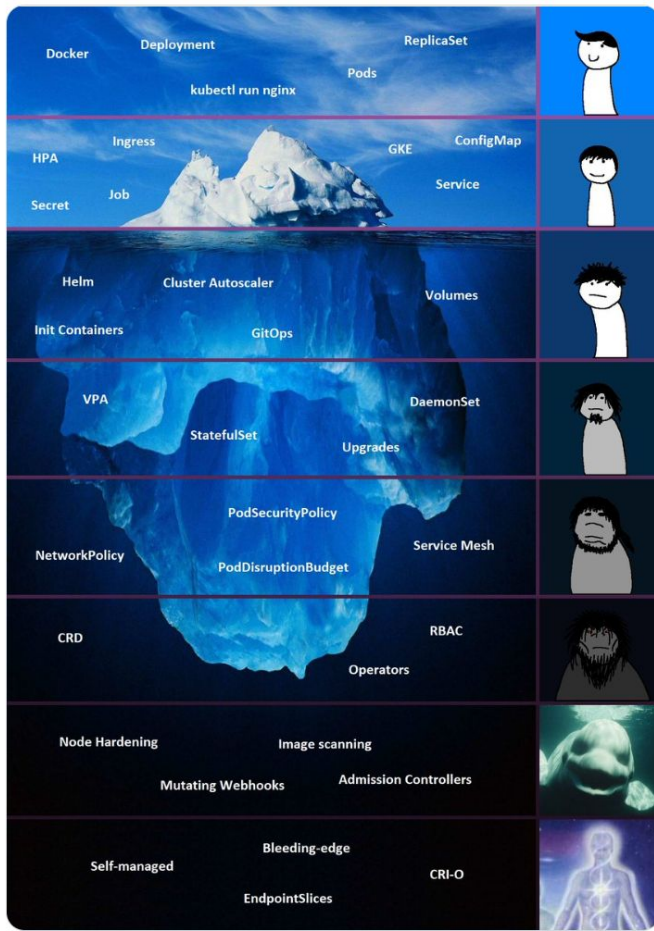@abelsromero

VMware

Why this talk

Why are we here?

An opinionated view of what we would have liked to know when we began our K8s journey

👷‍♀️Choosing your development cluster

🧰 Making your life easier

🛡️Security best practices

🚀 Time to deploy

💡 Final tips

Choosing your development cluster

Choosing your development cluster

Microk8s https://microk8s.io

Minikube https://minikube.sigs.k8s.io

KinD https://kind.sigs.k8s.io

K3s https://k3s.io with k3d https://k3d.io

Choosing your development cluster

Microk8s https://microk8s.io

- Neat addons system
- Manually configure cluster nodes

Minikube https://minikube.sigs.k8s.io

- Feels very real
- Not light at all

Choosing your development cluster

KinD https://kind.sigs.k8s.io

- You get a cluster in seconds
- Not a real distribution
- Need to tune it if you want to use some more specific features

```
%time kind create cluster

Creating cluster "kind" ...
 ✓ Ensuring node image (kindest/node:v1.21.1) 🖼
 ✓ Preparing nodes 📦
 ✓ Writing configuration 📜
 ✓ Starting control-plane 🕹️
 ✓ Installing CNI 🔌
 ✓ Installing StorageClass 💾
Set kubectl context to "kind-kind"
You can now use your cluster with:

kubectl cluster-info --context kind-kind

Have a nice day! 👋
kind create cluster  6.41s user 3.34s system 25% cpu 38.091 total
```

Choosing your development cluster

```
execute(
"kind","create","cluster",
"--name",testName,
"--kubeconfig",kubeConfigPath,
"--config",kindConfigPath);
```

https://kind.sigs.k8s.io/docs/user/quick-start/#creating-a-cluster

Choosing your development cluster

k3s https://k3s.io with k3d https://k3d.io

- Real distribution and lightweight

```
%time k3d cluster create mycluster2
INFO[0000] Prep: Network
INFO[0000] Created network 'k3d-mycluster2'
INFO[0000] Created image volume k3d-mycluster2-images
INFO[0000] Starting new tools node...
INFO[0000] Starting Node 'k3d-mycluster2-tools'
INFO[0001] Creating node 'k3d-mycluster2-server-0'
INFO[0001] Creating LoadBalancer 'k3d-mycluster2-serverlb'
INFO[0001] Using the k3d-tools node to gather environment information
INFO[0001] Starting new tools node...
INFO[0001] Starting Node 'k3d-mycluster2-tools'
INFO[0003] Starting cluster 'mycluster2'
INFO[0003] Starting servers...
INFO[0003] Starting Node 'k3d-mycluster2-server-0'
INFO[0008] All agents already running.
INFO[0008] Starting helpers...
INFO[0008] Starting Node 'k3d-mycluster2-serverlb'
INFO[0014] Injecting records for hostAliases (incl. host.k3d.internal) and for 3 network members into CoreDNS configmap...
INFO[0017] Cluster 'mycluster2' created successfully!
INFO[0017] You can now use it like this:
kubectl cluster-info
k3d cluster create mycluster2  0.12s user 0.10s system 1% cpu 17.104 total
```

Choosing your development cluster

```java
K3sContainer k3s =
new K3sContainer(DockerImageName.parse("rancher/k3s:v1.21.3-k3s1"));

String kubeConfigYaml = k3s.getKubeConfigYaml();

ApiClient client = Config.fromConfig(new StringReader(kubeConfigYaml));
CoreV1Api api = new CoreV1Api(client);

// interact with the running K3s server, e.g.:
V1NodeList nodes = api.listNode(...);
```
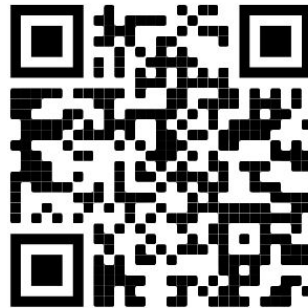
https://www.testcontainers.org/modules/k3s/

Choosing your development cluster

Microk8s https://microk8s.io

Minikube https://minikube.sigs.k8s.io

KinD https://kind.sigs.k8s.io

K3s https://k3s.io with k3d https://k3d.io

Making your life easier

Demo time: https://github.com/abelsromero/devnexus22

Let's see…

- Skaffold - https://skaffold.dev
- Cloud Code - https://plugins.jetbrains.com/plugin/8079-cloud-code
- K9s - https://k9scli.io
- Octant - https://octant.dev
- kubectx & kubens - https://github.com/ahmetb/kubectx

Security best practices

Security best practices

Problems can come from:

- ● Operating System
- ● JRE
- ● Dependencies

Security best practices

Problems can come from:

- Operating System
- JRE
- Dependencies

Two factors that can cause us to be vulnerable:

- We add a vulnerable dependency
- A new vulnerability gets discovered

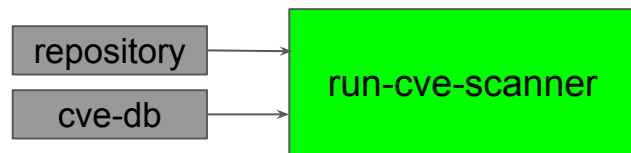# Security best practices
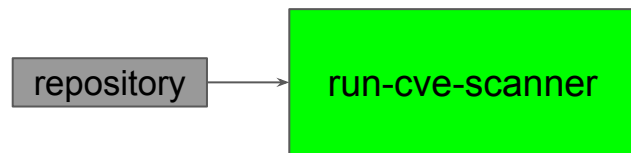
We run a CVE scanner tool on:

- Every commit

repository → run-cve-scanner

Security best practices
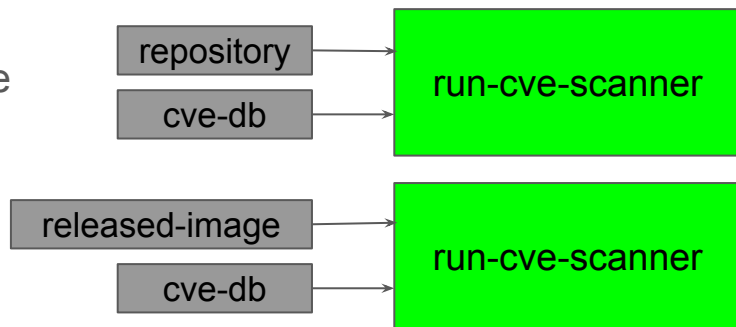
We run a CVE scanner tool on:

- Every commit
- Every update to the vulnerabilities database
  - Current code

```
repository ──→  run-cve-scanner
cve-db     ──→
```

Security best practices

We run a CVE scanner tool on:

- Every commit
- Every update to the vulnerabilities database
    - Current code
    - Released code

| repository | → | run-cve-scanner |
| cve-db | → | |

| released-image | → | run-cve-scanner |
| cve-db | → | |

Security best practices

Use paketo buildpacks https://paketo.io

With Spring boot:

```
./gradlew bootBuildImage --imageName=albertoimpl/spring-dependency-demo-app
```

Alternatively:

```
pack build albertoimpl/spring-dependency-demo-app
```

Security best practices

```
%pack inspect-image albertoimpl/spring-dependency-demo-app --bom | jq .
```

```
{
    {
     "name": "jre",
     "metadata": {
       "layer": "jre",
       "name": "BellSoft Liberica JRE",
       "sha256": "e02991fe14c22fa1326ad670829af12214f5f4af8b69e272f4757262e0ae8cc3",
       "uri": "https://github.com/bell-sw/Liberica/releases/download/11.0.14.1+1/bellsoft-jre11.0.14.1+1-linux-amd64.tar.gz",
       "version": "11.0.14"
     },
     {
     "name": "dependencies",
     "metadata": {
       "dependencies": [
         {
           "name": "jackson-databind",
           "sha256": "56cfbdc9e1736b5c56b43757f6cf546ee6d49393c79383c4e495c4f7047cb506",
           "version": "2.13.1"
         },
         {
           "name": "log4j-api",
           "sha256": "ab9cadc80e234580e3f3c8c18644314fccd4b3cd3f7085d4e934866cb561b95d",
           "version": "2.17.0"
         }
       ]
     }
   }
}
```

Security best practices

```
%trivy image --severity "HIGH,CRITICAL" --exit-code 1
'albertoimpl/spring-dependency-demo-app'
2022-04-04T14:09:09.062+0200    INFO    Need to update DB
2022-04-04T14:09:09.062+0200    INFO    Downloading DB...
2022-04-04T14:10:41.221+0200    INFO    Detected OS: ubuntu
2022-04-04T14:10:41.221+0200    INFO    Detecting Ubuntu vulnerabilities...
2022-04-04T14:10:41.230+0200    INFO    Number of language-specific files: 5
2022-04-04T14:10:41.230+0200    INFO    Detecting gobinary vulnerabilities...
2022-04-04T14:10:41.234+0200    INFO    Detecting jar vulnerabilities...

albertoimpl/spring-dependency-demo-app (ubuntu 18.04)
=====================================================
Total: 0 (HIGH: 0, CRITICAL: 0)

Java (jar)
==========
Total: 4 (HIGH: 2, CRITICAL: 2)
```

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
com.fasterxml.jackson.core:jackson-databind	**CVE-2020-36518**	**HIGH**	**2.13.1**	**2.12.6.1, 2.13.2.1**	jackson-databind: denial of service via a large depth of nested objects -->avd.aquasec.com/nvd/cve-2020-36518
org.springframework.boot:spring-boot	CVE-2022-22965		2.6.2	2.5.12, 2.6.6	spring-framework: RCE via Data Binding on JDK 9+ -->avd.aquasec.com/nvd/cve-2022-22965
org.springframework:spring-beans		CRITICAL	5.3.14	5.3.18, 5.2.20	
org.springframework:spring-webflux					

Security best practices

You want to be patching all the time.
So you get CVE fixes automatically.

Bonus point, you are as close as you can to the latest stable version in case of breaking changes.

We recommend dependabot for that.

https://docs.github.com/en/code-security/dependabot/dependabot-security-updates/configuring-dependabot-security-updates

Security best practices

Automate all the things!

- Use buildpacks to avoid problems with OS and JRE
- Update often with dependabot
- Use a CVE scanner

Time to deploy
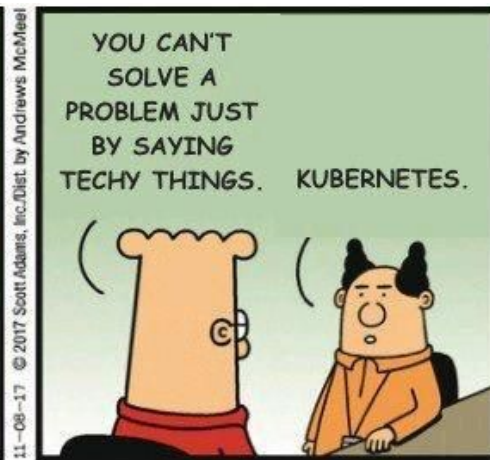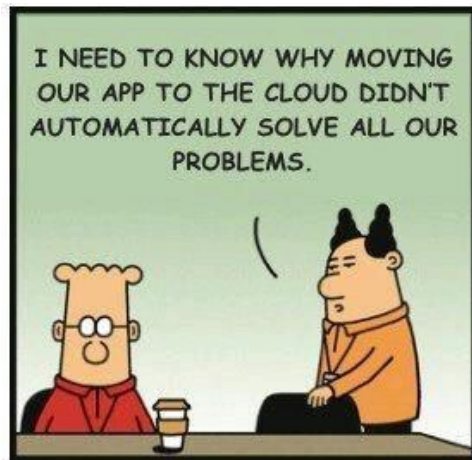
Lots of moving pieces means…

Time to deploy

MOAR tools to handle complexity!!

	Kustomize.io	HELM	CARVEL
Templating	✅	✅	✅ (ytt)
Building	❌	❌	✅ (kbld)
Packaging & distribution	❌	🤔❓	✅ (imgpkg)
Versioning	❌	✅	✅
Dependencies	❌	✅	✅
Config, deployment & upgrading	❌	✅	✅ (kapp cli, kapp-controller)

Final tips

- Everything is Asynchronous & Declarative
- `alias k="kubectl"`
- Take your time at each step
- Don't let the details drag you, let the abstractions do their job
- Play with local clusters, you can simulate a small cluster in a modern PC. Just beware of limitations like metrics or networking.

Some resources

- Take care of books, because they can get outdated quite quickly

    - https://www.oreilly.com/library/view/kubernetes-up-and/9781491935668/
    - https://www.oreilly.com/library/view/programming-kubernetes/9781492047094/
    - https://sysdig.com/blog/kubernetes-1-23-whats-new/
    - https://kubernetes.io/blog/2021/12/07/kubernetes-1-23-release-announcement/

- Other talks

    - Inner Loop Development with Spring Boot on Kubernetes

      https://www.youtube.com/watch?v=akSskYvcmFo

- Compilation of Java and Kubernetes resources

    - https://github.com/Albertoimpl/k8s-for-the-busy

Thanks!

Alberto C. Ríos

@Albertoimpl

Abel Salgado

@abelsromero

VMware