

Sécurité des conteneurs

Meetup du 8 février 2024



Bertrand Thomas - Architecte Solution @ SUSE

Objectifs

- 🚫 Présentation exhaustive
- 🚫 Discours vendeur
- 🚫 Solution propriétaire / coûteuse
- ✓ Conseils pratiques
- ✓ Actions rapides
- ✓ Outils (réellement) open-source



Wolfgang Staudt

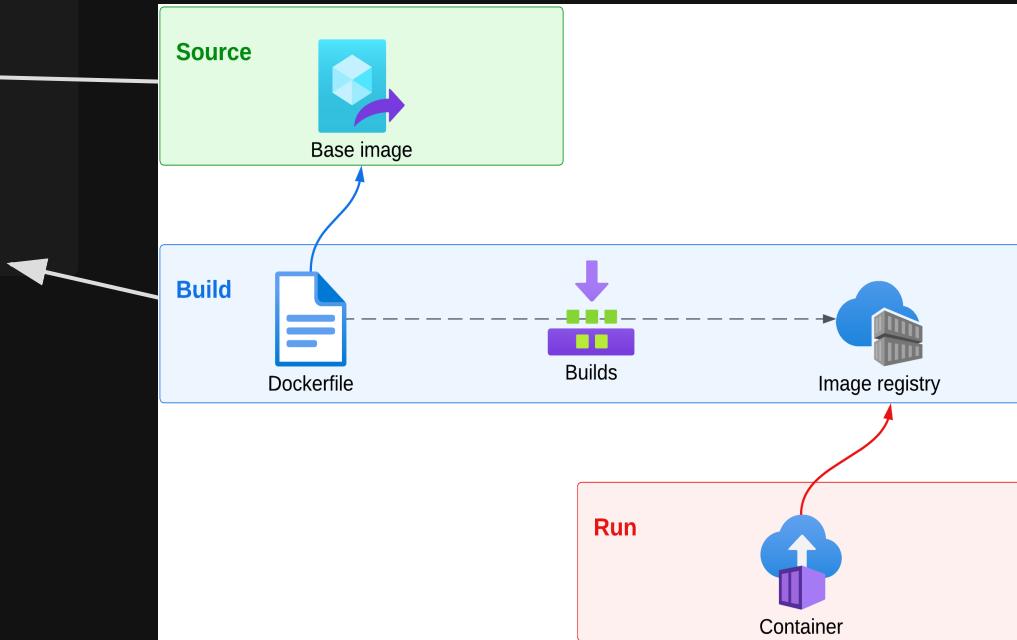
Partie I - Cycle de vie d'un container



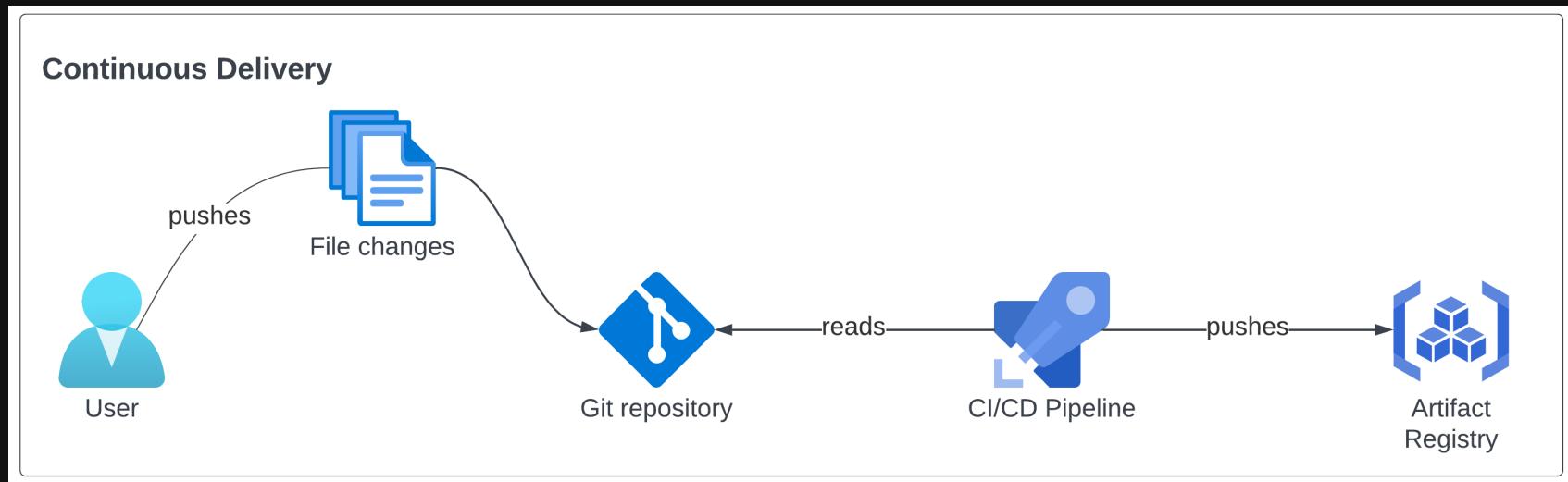
Construction d'une image

- Exemple (Docker getting started)

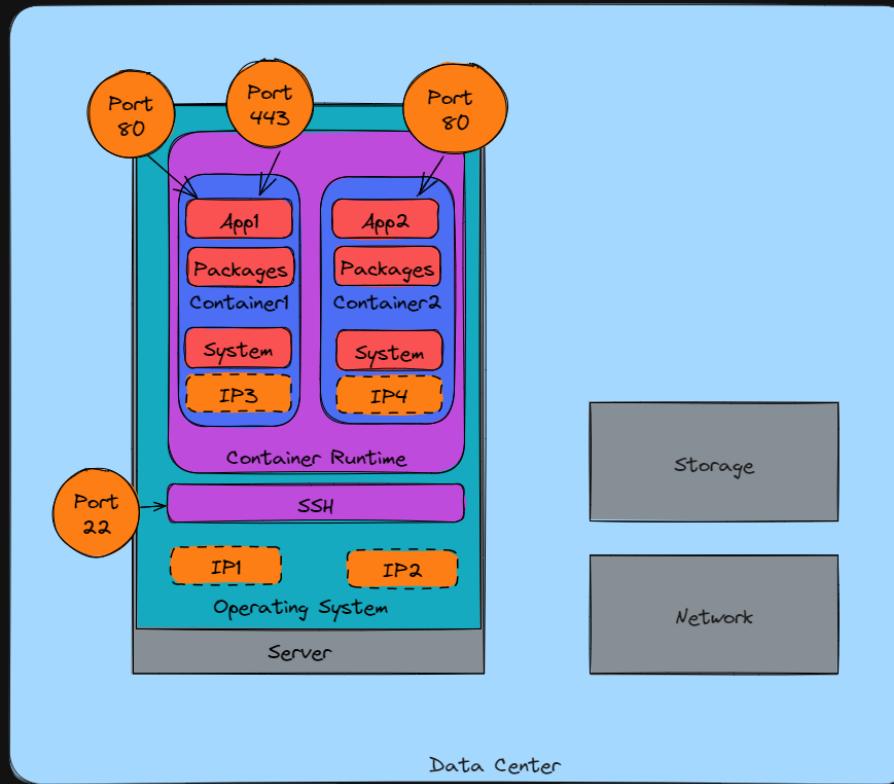
```
# Dockerfile
FROM node:18-alpine
WORKDIR /app
COPY . .
RUN yarn install --production
CMD ["node", "src/index.js"]
EXPOSE 3000
```



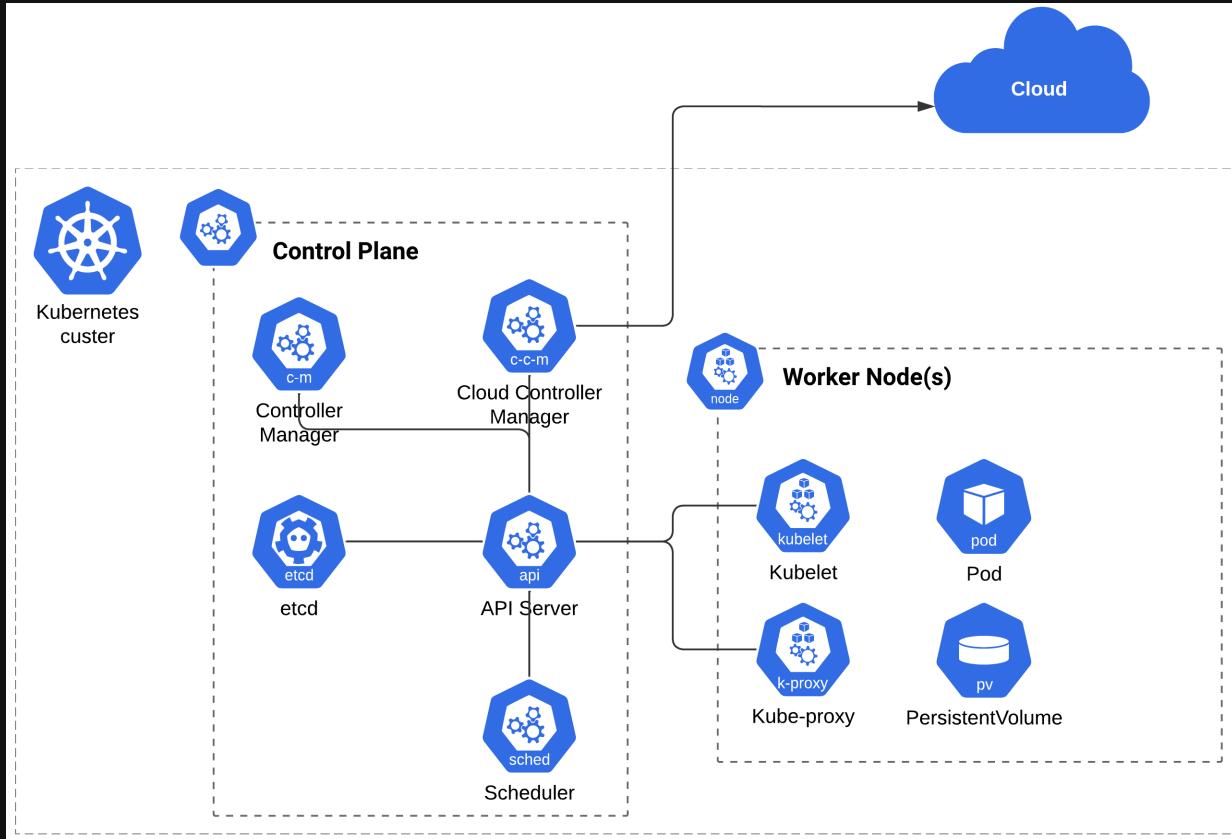
Chaîne d'approvisionnement



Conteneur et centre de données



Orchestration de conteneurs



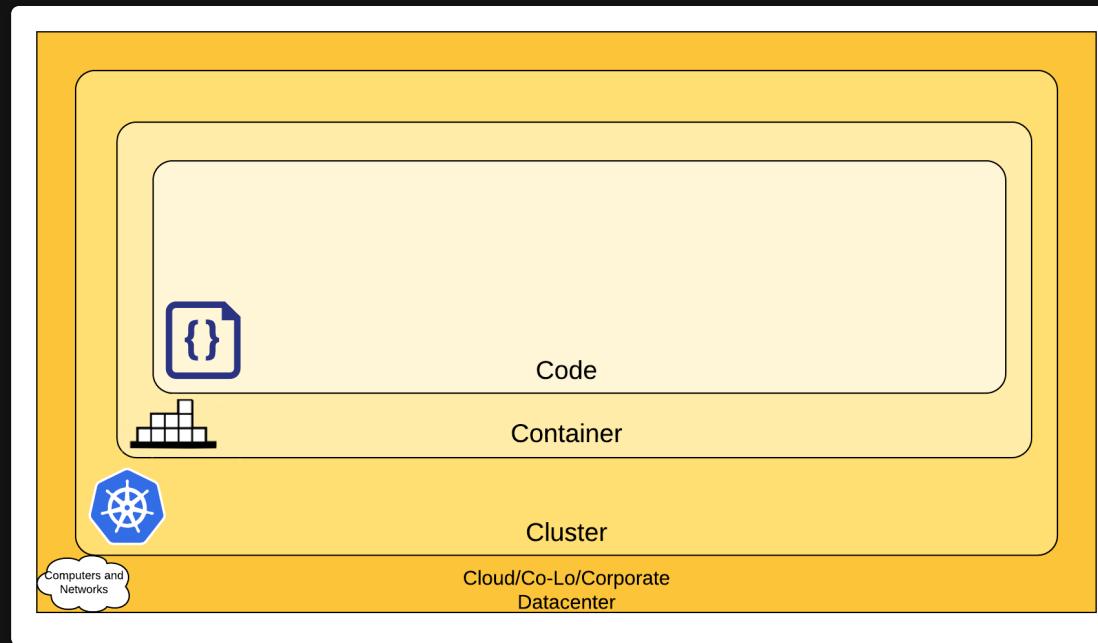
Atelier - Surfaces d'attaque



Partie II - Stratégie de sécurisation



Les 4 C de la sécurité Cloud native



Source: kubernetes.io/docs/concepts/security/overview

Cluster Kubernetes

- Recommendation de configuration
 - CIS Benchmark (Center for Internet Security)
 - kube-bench
- Communication sécurisée
 - Ingress with TLS (Kubernetes)
- Contrôle d'accès
 - Role Based Access Control (Kubernetes)
- Restrictions réseau
 - Network Policies (Kubernetes)
- Analyse comportementale
 - ⚡ Security & Compliance (CNCF Landscape)
 - Cilium
 - Falco
 - NeuVector
 - Tetragon
- Dépannage
 - Audit (Kubernetes)

Exécution du conteneur

- Admission & policies
 - Kubewarden
 - OPA Gatekeeper (Open Policy Agent)
 - Pod Security Admission (Kubernetes)
- Bacs à sable
 - gVisor
 - Kata Containers
 - Runtime Class (Kubernetes)
- Durcissement des systèmes
 - AppArmor
 - seccomp
- Immutabilité
 - Security Context (Kubernetes)

Image du conteneur

- Images de base
 - Alpine Linux
 - Bitnami Containers Library
 - SUSE BCI [1]
- Catalogue d'applications
 - Bitnami Application Catalog
 - Docker Hub
 - SUSE Application Collection
- Définition de l'image (pipelines CI/CD)
 - Dockerfile best practices
 - MegaLinter
 - Sonar
- Analyse d'image (pipelines CI/CD [2] + registres)
 - Clair
 - NeuVector
 - Trivy

[1] Base Container Images

[2] Continuous Integration/Continuous Delivery

Trop d'informations ?



Conception de la solution

- Principes
 - Least privilege
 - Zero Trust
- Conformités
 - GDPR [1]
 - HIPAA [2]
- Fonctionnalités
 - Analyse du traffic Nord-Sud et Est-Ouest
 - Détection des CVE [3]
 - Gestion des menaces connues (OWASP [4])
 - Impact faible sur les ressources
 - Pare-feu applicatif internet (WAF)
 - Prévention contre les pertes de donnée (DLP)
 - Protection contre les dérives (Drift)

[1] General Data Protection Regulation

[2] Health Insurance Portability and Accountability Act

[3] Common Vulnerabilities and Exposures (cve.org)

[4] Open Worldwide Application Security Project (owasp.org)

Points d'attention

- Analyse des images
 - Statique vs en cours d'exécution
 - Ponctuelle (CI/CD) vs régulière
- Différence dans le comportement
 - Détection (après-coup) vs protection (empêchement)
- Choix stratégiques
 - Open-source vs propriétaire
 - Liberté vs "lock-in"
- Pratiques DevOps
 - Cycles courts (agilité, CI/CD)
 - Shift-Left
 - DevSecOps != personne/équipe
 - Outils accessibles à tous
 - Automatisation (security-as-code)

Partie III - Démonstrations



Images de base .NET

- Analyse des images officielles de Microsoft et SUSE

```
alias trivy="docker run -it --rm  
-v trivy-cache:/root/.cache/ -v /var/run/docker.sock:/var/run/docker.sock:ro -v $HOME/.kube/config:/root/.kube/config \  
aquasec/trivy:latest"
```

```
trivy image mcr.microsoft.com/dotnet/aspnet:8.0 | grep Total
```

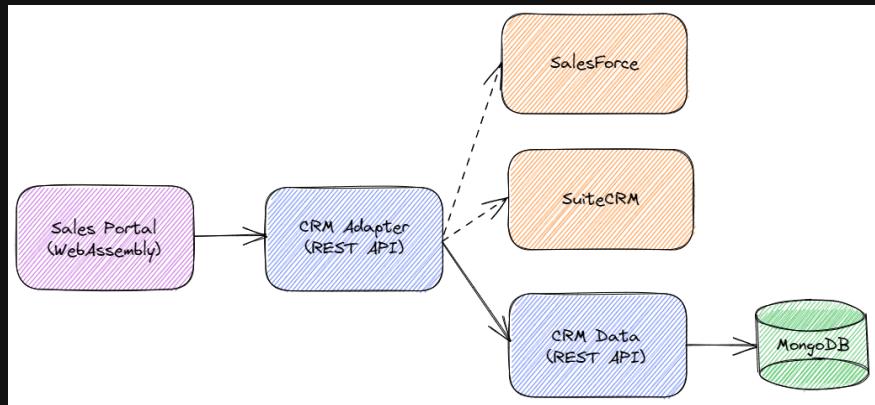
```
# Total: 86 (UNKNOWN: 0, LOW: 60, MEDIUM: 22, HIGH: 3, CRITICAL: 1)
```

```
trivy image registry.suse.com/bci/dotnet-aspnet:8.0 | grep Total
```

```
# Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)
```

Architecture microservice

- Infrastructure Cloud (**Azure**)
- Clusters Kubernetes (**AKS**)
- Chaîne d'assemblage (**GitHub**)
- Front avec Web SPA (**Angular**)
- Back avec API REST (**.NET**)
- Base de données NoSQL (**MongoDB**)



Source: devpro/sales-portal

Check-list

- Image validation in CI
- RBAC
- Registry scanning
- CIS Benchmark
- Zero-trust

Liens

- [Evènement meetup](#)
- [Helm charts utilisés \(approche GitOps\)](#)
- [Guide d'étude pour la certification CKS](#)

Merci

- ★ A mon employeur, **SUSE** , pour le temps alloué à préparer cette présentation et les ressources infrastructure pour la démo.
- ★ A **Matthieu Robin** et les organisateurs du meetup pour la confiance accordée.
- ★ A **Cédric Berriguiot** pour son état d'esprit, son aide et sa bonne humeur.
- ★ A mon corsair préféré, **Nuno do Carmo**, pour la relecture, la bienveillance et les conseils.