Docker : larguez les amarres !

Martin Souchal 2021 (APC - FACe - ComputeOps)

ComputeOps

- Le projet ComputeOps a pour objectif d'étudier les avantages des conteneurs pour les applications de type HPC. Lancé en 2018, le projet est financé par le master project DecaLog de l'IN2P3 dans le cadre du programme de R&D transverse.
- Participants IN2P3 : APC, LAL, LPNHE, LLR, IPHC
- Partenaires extérieurs :
  - Groupe de travail Aristote sur la virtualisation légère.
  - Ecole Centrale de Nantes
  - IAS
  - INRAE
  - Intel
  - Sylabs

Plan

20 min pour arrêter Docker

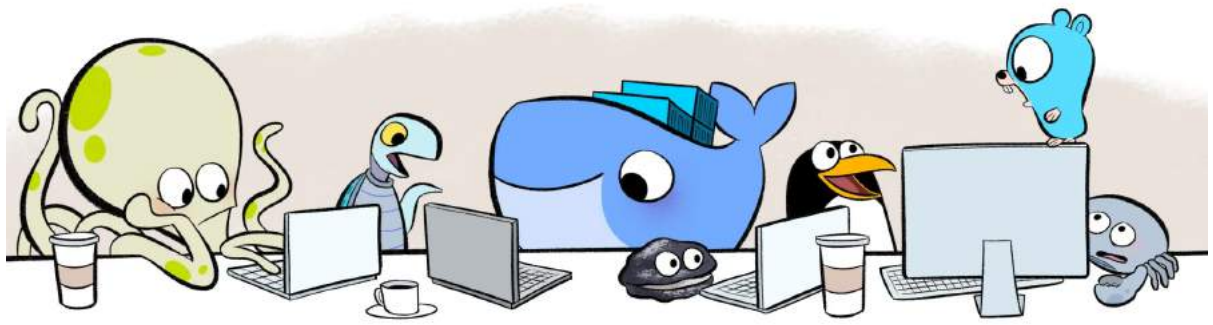
- Docker, c'est quoi ?
- Les alternatives
- Conclusion

Docker c'est quoi ?

Un peu d'histoire...

Docker est avant tout une société

- Issue d'un projet la société française dotCloud
- LXC/LXD en 2008
- Docker en 2013, début du DevOps
- Kubernetes en 2014 chez Google, Nomad chez HashiCorp. Création de la CNCF
- 2015 : Docker top 15 GitHub, création de l'Open Container Initiative (OCI) et naissance de runc

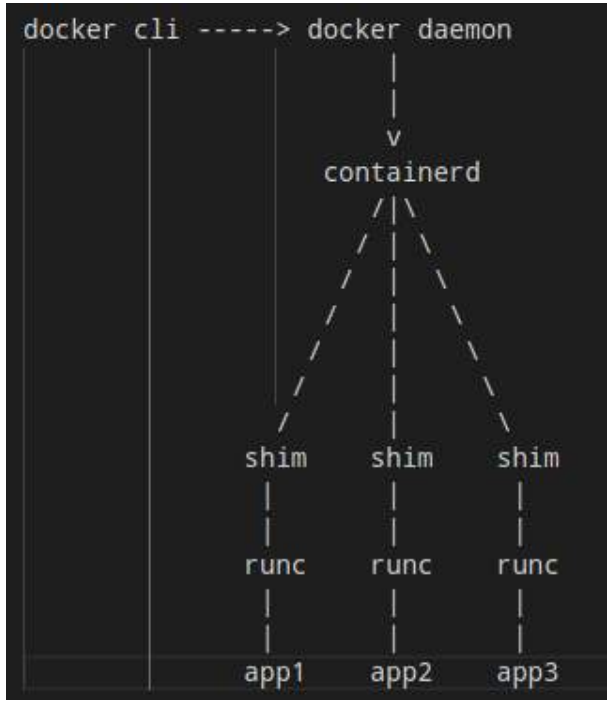


Docker c'est quoi ?

Un peu d'histoire...

concrètement ?

- Un "moteur" : en fait une API et un environnement bâti autour de LXC/LXD et du noyau linux
- Docker fait tout : construire des images, gérer une registry locale, partager des images sur le DockerHub, créer des volumes et des réseaux et démarrer des conteneurs.
- Depuis la création de OCI, Docker n'est qu'une interface vers des runtimes ouvertes (runc, containerd, etc...)



Docker c'est quoi ?

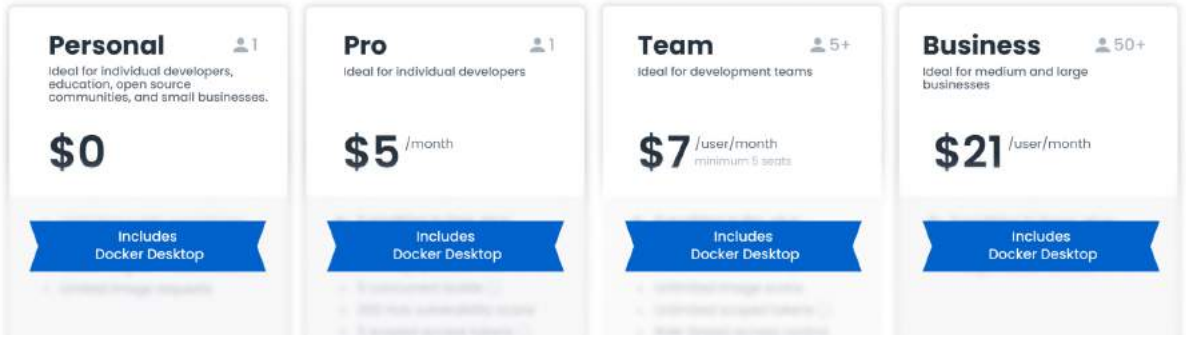
Un peu d'histoire...

concrètement ?

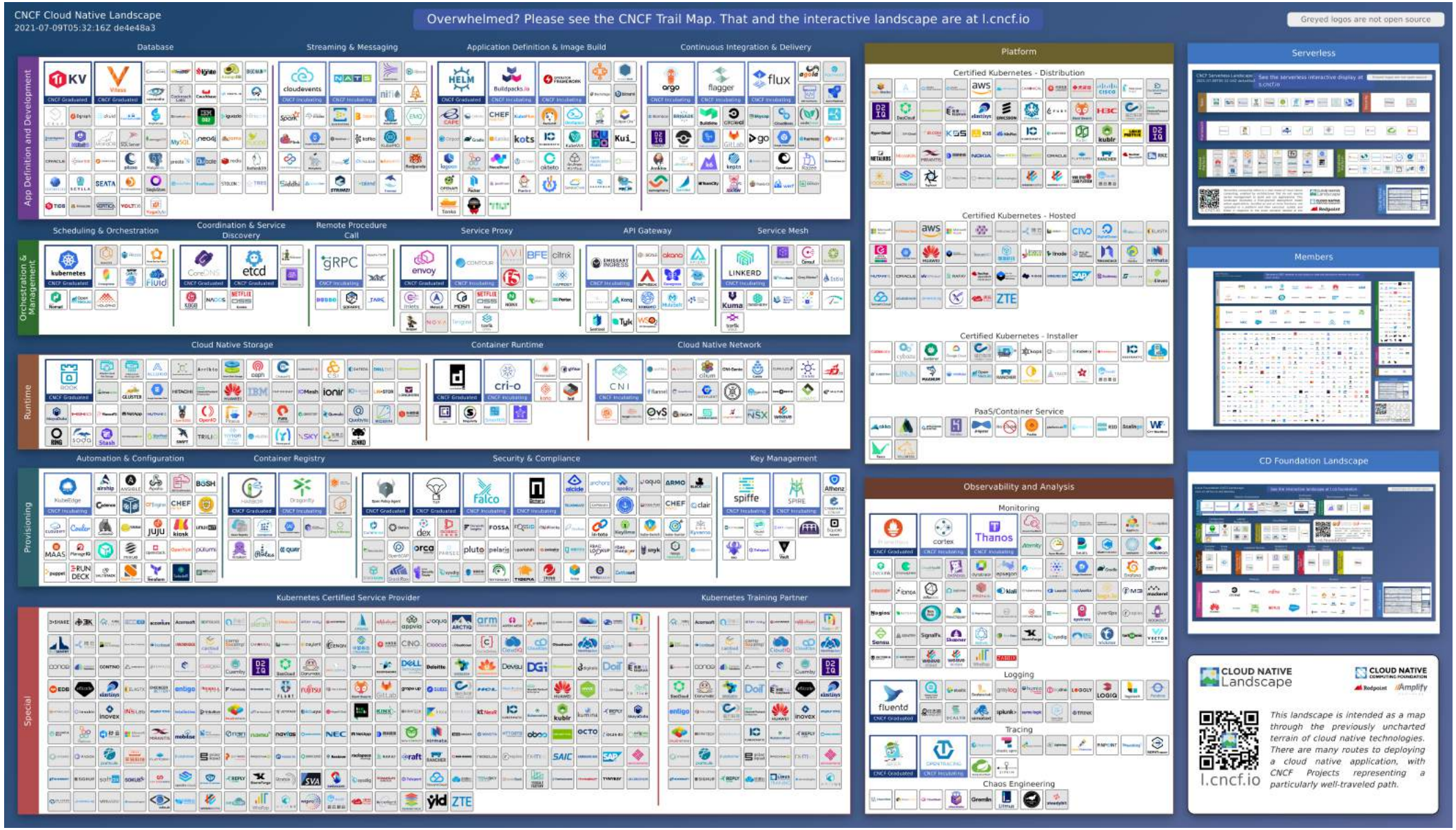
Aujourd'hui ?

Une entreprise qui vends :

- Docker Desktop (GUI MacO$ / M$)
- Du stockage (DockerHub, cloud...)
- Des services autour des conteneurs (sécurité, ressources pour entreprises, support...)



Alternatives


CNCF Cloud Native Landscape
2021-07-09T05:32:16Z de4e48a3
Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io
Greyed logos are not open source
App Definition and Development
Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Runtime
Cloud Native Storage
Container Runtime
Cloud Native Network
Provisioning
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Special
Kubernetes Certified Service Provider
Kubernetes Training Partner
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
Logging
Tracing
Chaos Engineering
Serverless
Members
CD Foundation Landscape
CLOUD NATIVE Landscape
CLOUD NATIVE COMPUTING FOUNDATION
Redpoint
Amplify
l.cncf.io
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

Alternatives

Open Container initiative (OCI)

Le processus de démarrage des conteneurs, ainsi que le format de l'image sur le disque, sont définis et régis par des normes.

- Gouvernance ouverte chapeautée par la Linux Foundation pour répondre à la volonté d'avoir un écosystème hétérogène dans K8S.
- Standard pour les runtimes (CRI) et les images de conteneurs (pas les manifestes !)
- Ligne de commande unifiée

```
docker run example.com/org/app:v1.0.0
alias docker=podman
alias docker=singularity
...
```

Alternatives

Open Container initiative (OCI)

Manifeste

- Plusieurs formats de manifestes : Dockerfile, Singularity...
- Un manifeste est transformé en image via un mécanisme de build (intégré ou non)
- Un conteneur peut être construit "from scratch" ou a partir d'une autre image
- La base d'une image est un OS Linux (Alpine Linux, Busybox, Ubuntu, CentOs...)
- Pas de standards pour les manifestes

```
docker build -f Dockerfile  -t Container .
```

```
singularity build Container.sif Singularity.def
```

```
buildah bud -f Dockerfile -t Container .
```

Alternatives

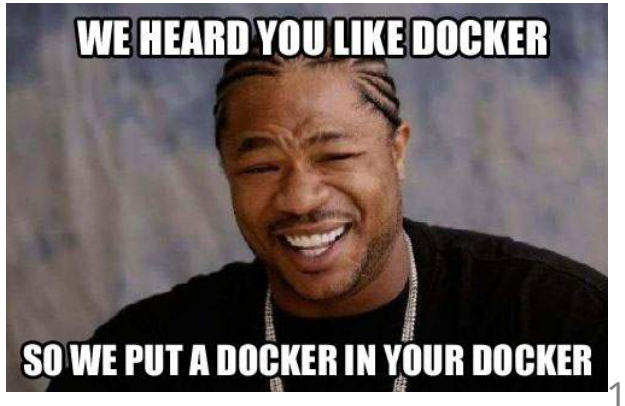
Open Container initiative (OCI)

Manifeste

CI/CD

```
docker-build:
image: quay.io/containers/buildah:latest
stage: build
script:
  - echo "$CI_REGISTRY_PASSWORD" | buildah login -u "$CI_REGISTRY_USER" --password-stdi
  - buildah bud -f tp/Dockerfile -t "$CI_REGISTRY_IMAGE:$CI_COMMIT_REF_SLUG" tp/
  - buildah push "$CI_REGISTRY_IMAGE:$CI_COMMIT_REF_SLUG"
```

```
docker-build:
image: docker:latest
stage: build
services:
  - docker:dind
before_script:
  - docker login -u "$CI_REGISTRY_USER" -p "$CI_REGISTRY_PASSWORD" $CI_REGISTRY
script:
  - docker build --pull -t "$CI_REGISTRY_IMAGE:$CI_COMMIT_REF_SLUG"
  - docker push "$CI_REGISTRY_IMAGE:$CI_COMMIT_REF_SLUG"
```



Alternatives

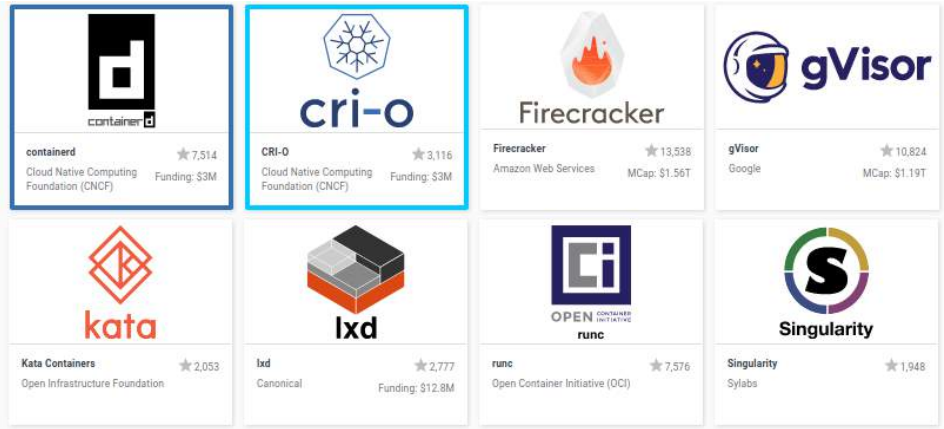
Open Container initiative (OCI)

Manifeste

CI/CD

Runtimes

- Runtimes bas niveau (proche du kernel) : runc (docker), LXC/LXD, crun, conmon (RedHat), nvidia-docker (Nvidia), youki (Rust)
- Runtimes haut niveau (réseau, etc...) : containerd (Docker), CR-IO (Kubernetes), enroot (Nvidia), SmartOs (Samsung), Singularity CRI
- Outils : Docker, Singularity, Podman (RedHat)
- MicroVms : KataContainer (INTEL), Firecracker (AWS), gVisor (google)
- Image builder : buildah, img, orca-build...



Toutes ces solutions sont interopérables grâce à OCI. Avec des performances qui varient selon le niveau d'isolation.

Alternatives

Open Container initiative (OCI)

Manifeste

CI/CD

Runtimes

Registres publics

- Images vérifiées
  - NVIDIA NGC - images orientées GPU
  - Docker Hub - images officielles
- Libres
  - Docker Hub
  - Singularity Hub
  - Sylabs cloud - images signées
  - Quay.io (scan de sécurité)

Alternatives

Open Container initiative (OCI)

Manifeste

CI/CD

Runtimes

Registres publics

Registres privés

- Gitlab (Registre Docker)
- Harbor (Registre Docker)
- Singularity Hub (Registre Singularity)
- Azure, AWS, etc... (OCI)
- Pour stocker des images OCI dans des registres docker : ORAS

```
singularity push --docker-username user --docker-password passwd container.sif oras://g
```

Alternatives

Open Container initiative (OCI)

Manifeste

CI/CD

Runtimes

Registres publics

Registres privés

Orchestration

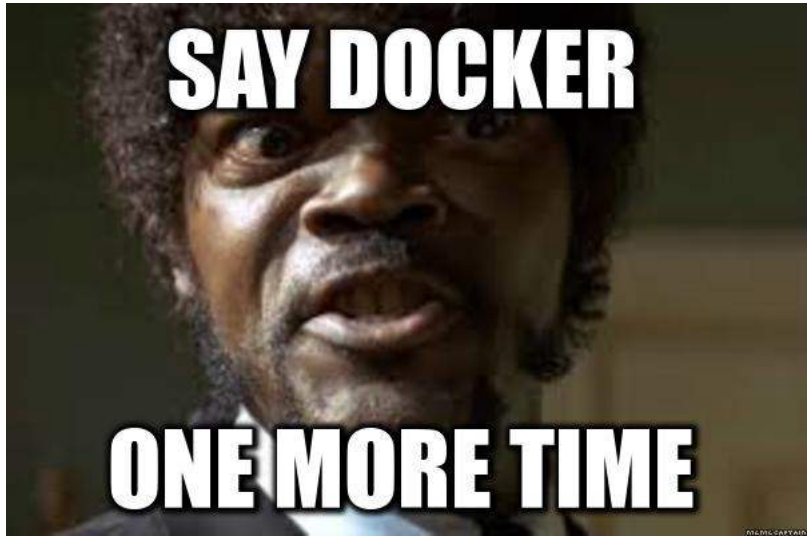
- Docker compose : podman-compose (en développement), nerdctl

✅ Même ligne de commande que DC
✅ Supporte les fichiers Docker Compose (nerdctl compose up)
✅ Supporte le mode rootless
✅ Supporte le lazy-pulling (Stargz)
✅ Supporte les images chiffrées (ocicrypt)

- Kubernetes :

Changelog 1.20 "Docker support in the kubelet is now deprecated and will be removed in a future release." (08/12/2020)

Conclusion



- Utiliser docker desktop en 2021 n'a aucun intérêt (sauf sur maco$?)
- Toutes les fonctionnalités de Docker existent ailleurs, et souvent en mieux
- Sauf pour les applications qui n'exploitent que l'API Docker (Portainer, VScode, traefik...)

Questions

Retrouvez nous sur

- Rocket Chat : #computeops
- Citadel CNRS