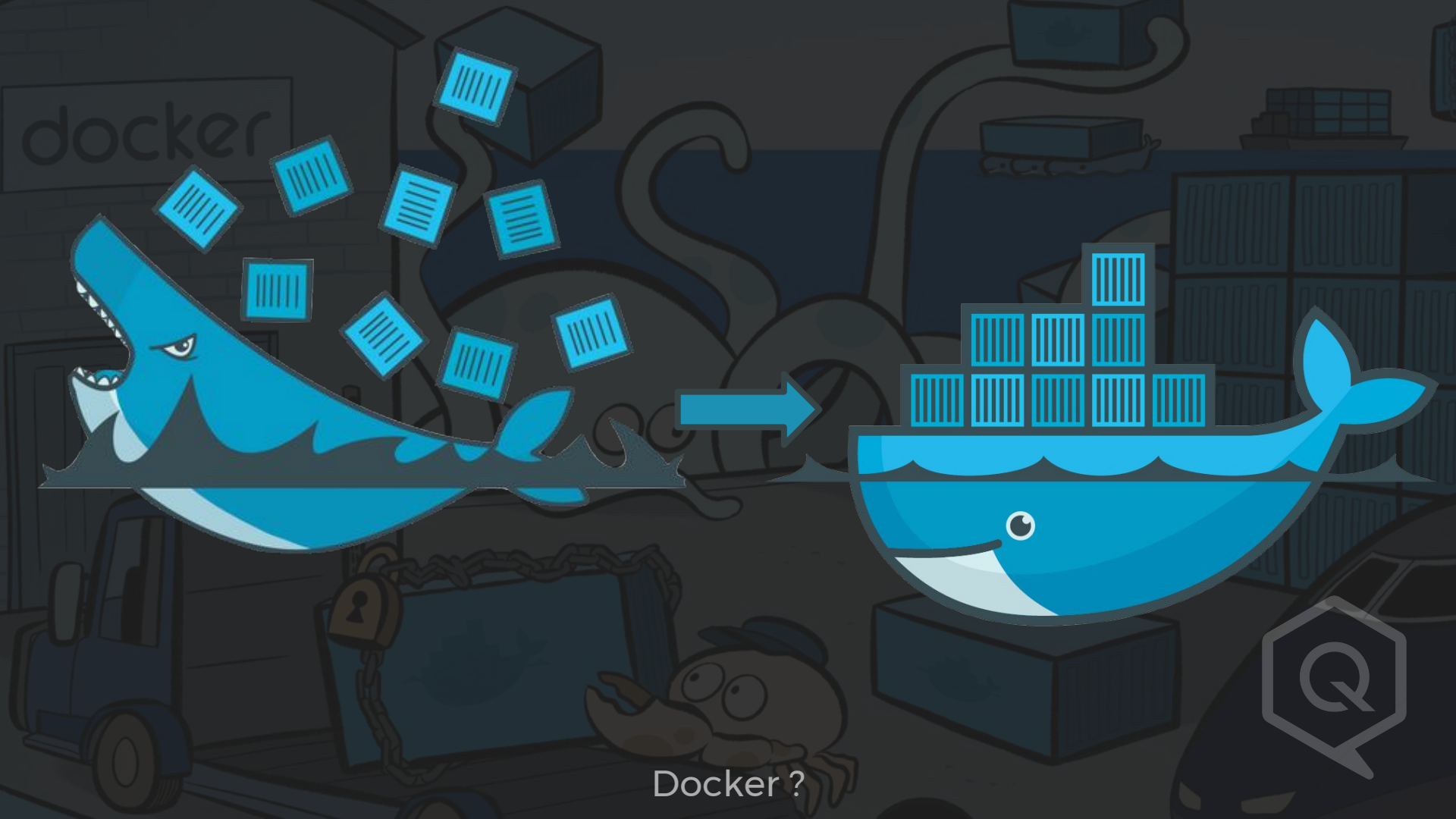


docker

Q TechNote #3
Docker hands-on



docker

Docker ?





docker

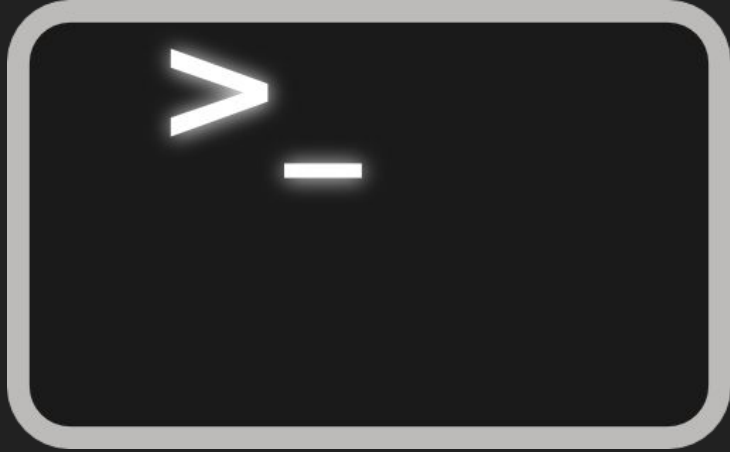
Démos

Docker, c'est quoi ?



Client Docker

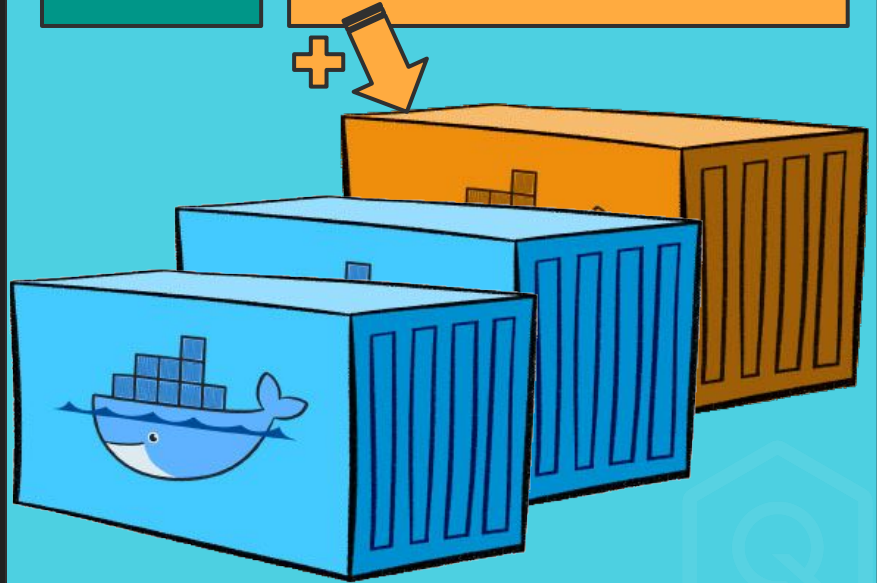
ligne de commande, ...



Docker engine/containerd

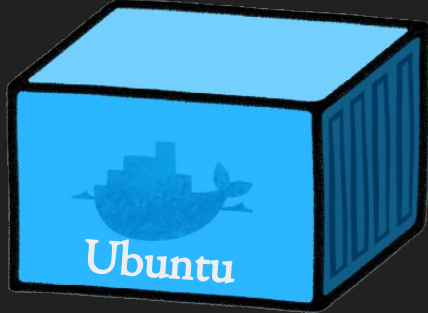
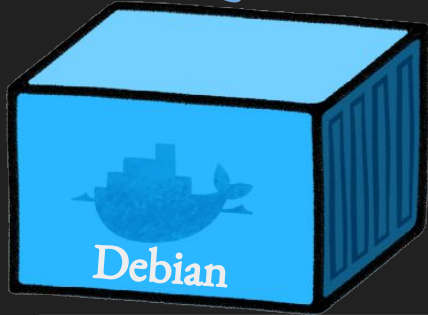
API

libcontainer/runc

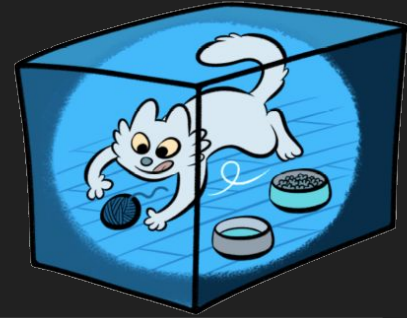
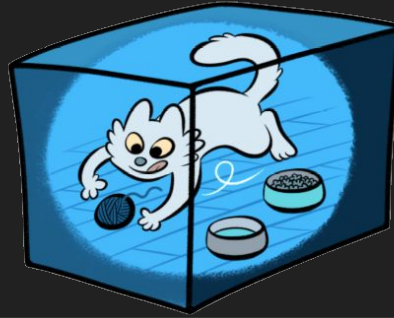
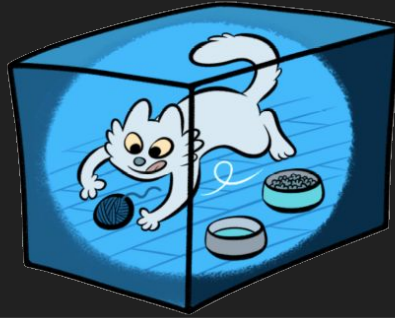


Les différents composants de Docker

Images



Conteneurs



Images vs. containers

```
$ docker run hello-world
```



Dissection du sucre sur l'URL de l'image

```
$ docker run hello-world
```

==

```
$ docker run registry-1.docker.io/library/hello-world
```



Dissection du sucre sur l'URL de l'image

```
$ docker run hello-world
```

==

```
$ docker run registry-1.docker.io/library/hello-world
```

[https://registry-1.docker.io/v2/\\$REPO/manifests/latest](https://registry-1.docker.io/v2/$REPO/manifests/latest)



Dissection du sucre sur l'URL de l'image


```
$ docker run hello-world
```

==

```
$ docker run registry-1.docker.io/library/hello-world
```

[https://registry-1.docker.io/v2/\\$REPO/manifests/latest](https://registry-1.docker.io/v2/$REPO/manifests/latest)

```
$ docker run registry.qarnot.net/qrad-v3
```



docker

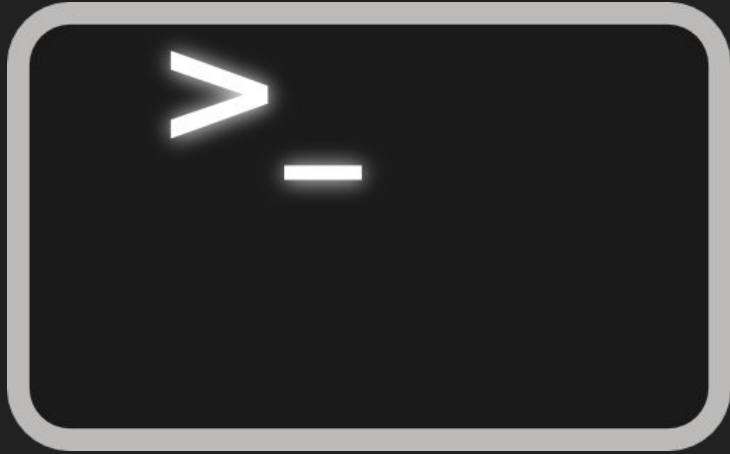
Démos

Un manifest ?



Client Docker

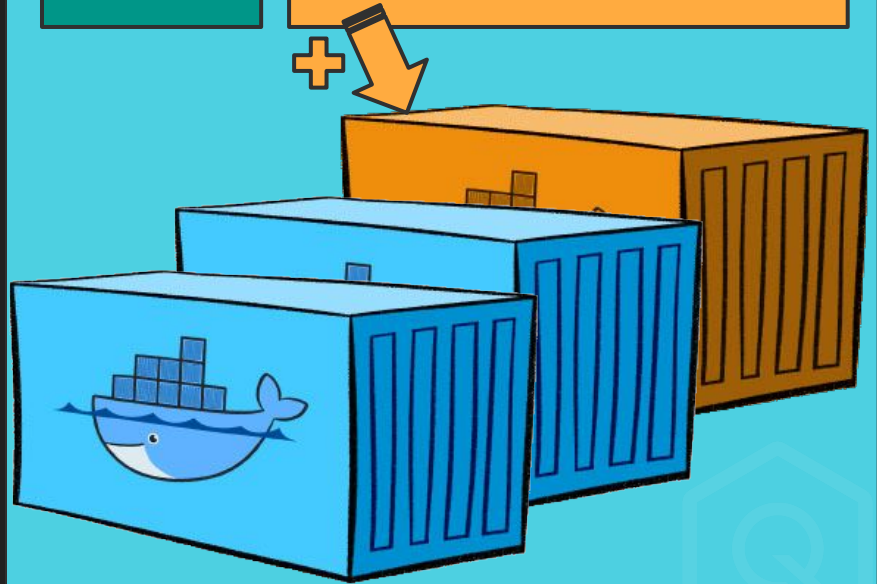
ligne de commande, ...



Docker engine/containerd

API

libcontainer/runc



Les différents composants de Docker



docker

Démos

Construire un conteneur



```
host% docker run -it ubuntu /bin/bash
```

```
myubuntu$ apt-get update
```

```
myubuntu$ apt-get install nano
```

```
myubuntu$
```

```
host% docker commit myubuntu nanobuntu
```

```
...
```

```
host% docker run -it nanobuntu
```



```
FROM scratch
```

```
LABEL maintainer nemunaire@nemunai.re
```

```
COPY hello /hello
```

```
CMD /hello
```



```
FROM scratch
LABEL maintainer nemunaire@nemunai.re
LABEL com.qarnot.profile="batch"

COPY hello /hello

CMD /hello
```



```
FROM scratch
```

```
LABEL maintainer nemunaire@nemunai.re
```

```
LABEL com.qarnot.profile="batch"
```

```
COPY hello /hello
```

```
CMD ["/hello"]
```




```
FROM debian:latest
LABEL maintainer nemunaire@nemunai.re

RUN apt-get update && apt-get install -y \
    nginx-light \
    && apt-get clean && rm -rf /var/lib/apt/lists/*

COPY index.html /var/www/html/index.html
CMD ["nginx", "-g", "daemon off;"]
```



```
FROM golang:1.9-alpine
```

```
COPY hello.go /go/src/hello/hello.go
```

```
RUN go build /go/src/hello/hello.go
```

```
FROM scratch
```

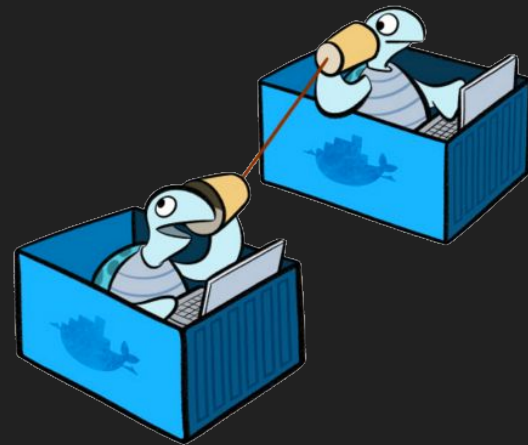
```
LABEL maintainer nemunaire@nemunai.re
```

```
COPY --from=0 /go/hello /hello
```

```
CMD ["/hello"]
```

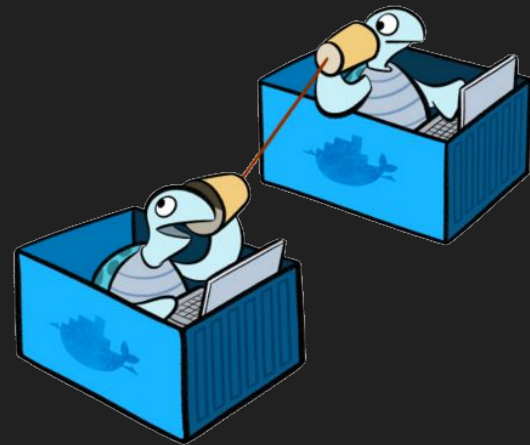


- Réduire les privilèges



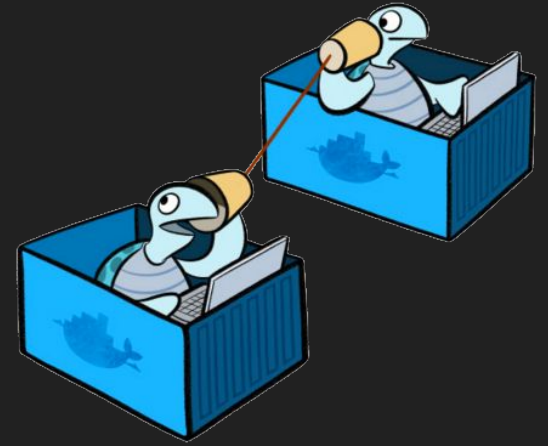
Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`



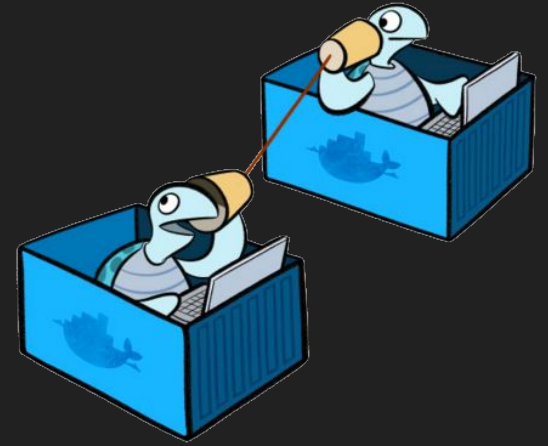
Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards



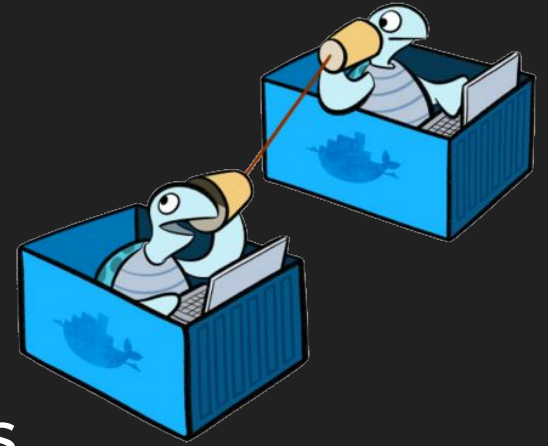
Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards
- Ne rien installer de superflus



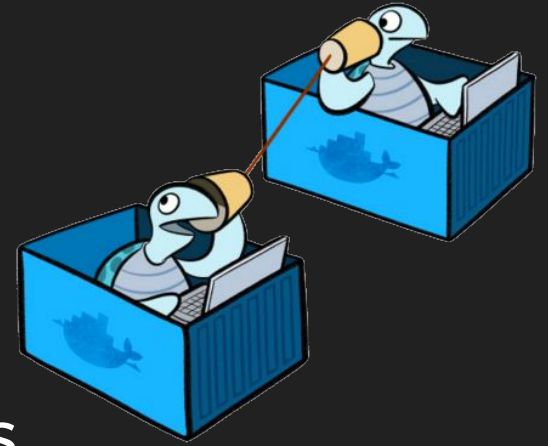
Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards
- Ne rien installer de superflus
- Minimiser le nombre de couches



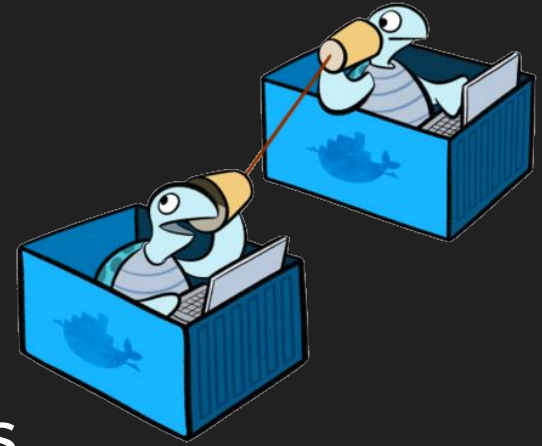
Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards
- Ne rien installer de superflus
- Minimiser le nombre de couches
- Trier les commandes multilignes



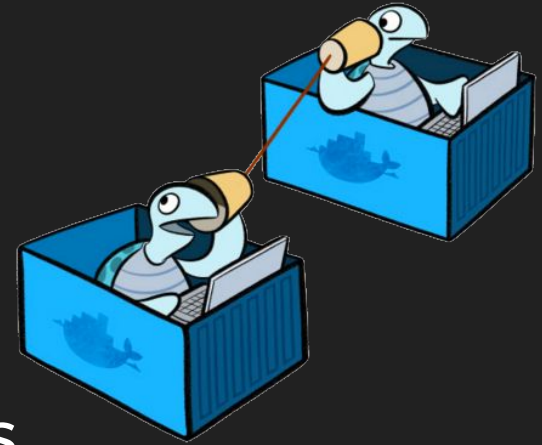
Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards
- Ne rien installer de superflus
- Minimiser le nombre de couches
- Trier les commandes multilignes
- Faire des conteneurs éphémères

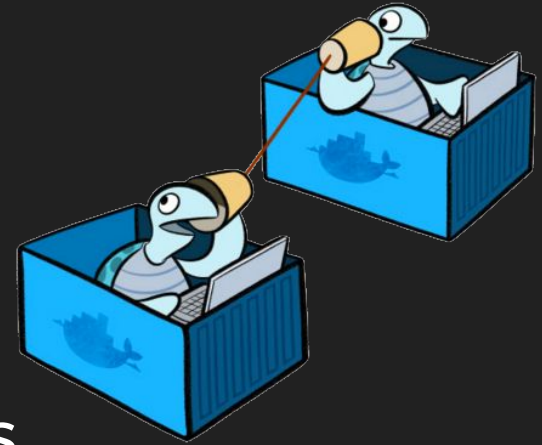


Quelques bonnes pratiques

- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards
- Ne rien installer de superflus
- Minimiser le nombre de couches
- Trier les commandes multilignes
- Faire des conteneurs éphémères
- Exécuter un seul processus par conteneur



- Réduire les privilèges
- Utiliser `.dockerignore`
- Exposer les ports standards
- Ne rien installer de superflus
- Minimiser le nombre de couches
- Trier les commandes multilignes
- Faire des conteneurs éphémères
- Exécuter un seul processus par conteneur
- Profiter du système de cache d'instruction



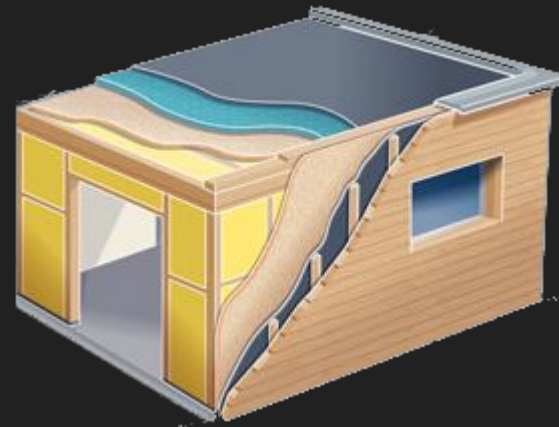
Quelques bonnes pratiques

docker

Démos

Volumes et liaisons

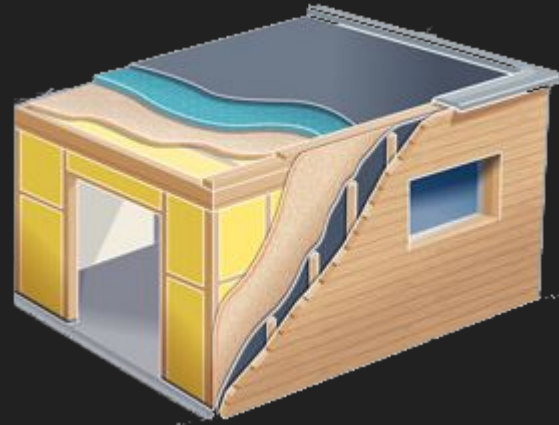




Comment bien isoler ?

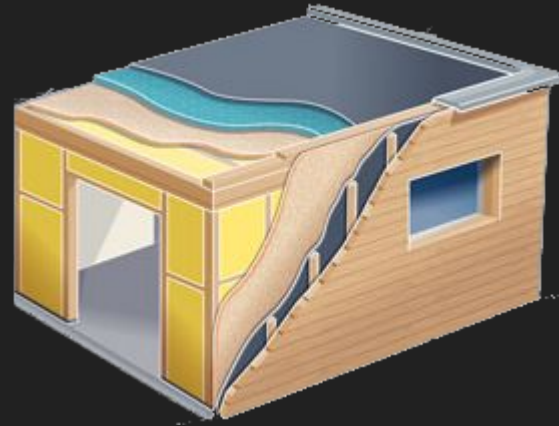


- Namespaces



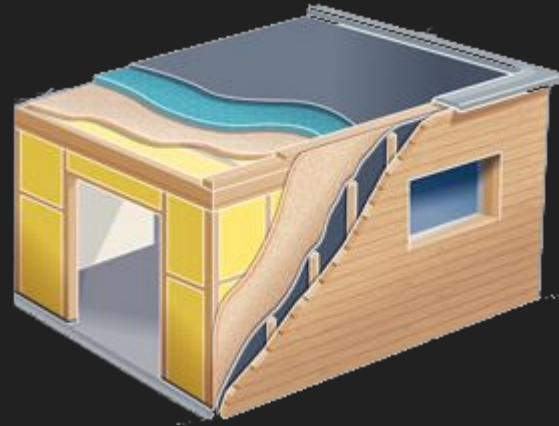
Comment bien isoler ?

- Namespaces
- Cgroups



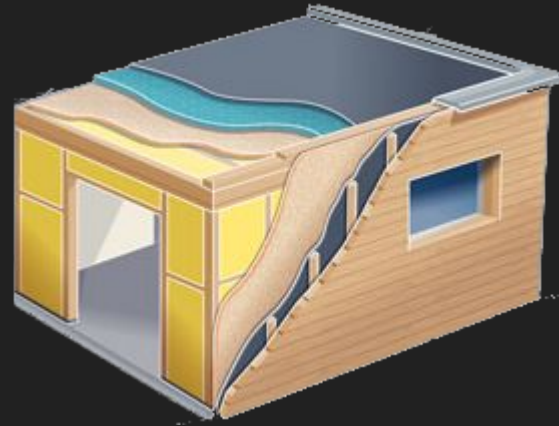
Comment bien isoler ?

- Namespaces
- Cgroups
- Capabilities



Comment bien isoler ?

- Namespaces
- Cgroups
- Capabilities
- seccomp



Comment bien isoler ?

docker

Questions ?

