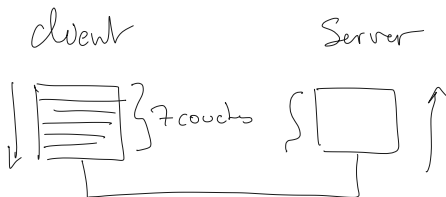
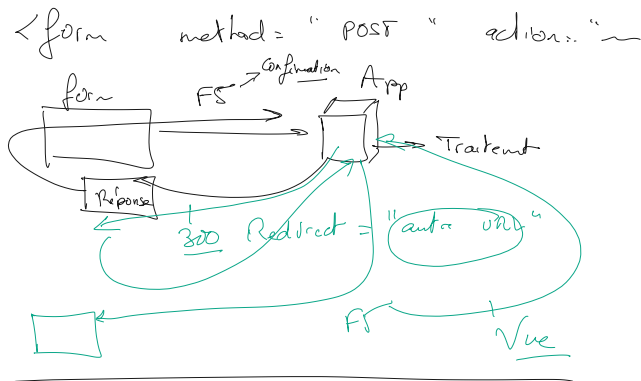


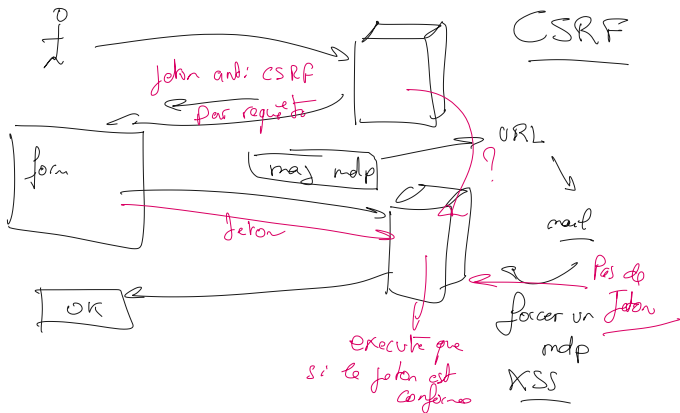
Bonjour Tout le Monde

Repost de données



OWASP CheatSheets :

[Introduction - OWASP Cheat Sheet Series](#)



Server httpd → user httpd

Contexte:

user / process

/etc/

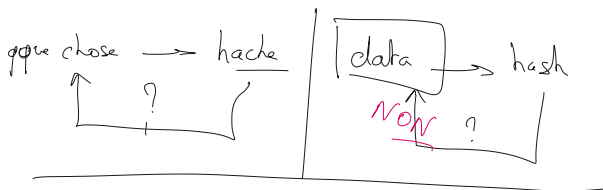
R → pour tout le monde

apache → lire /etc

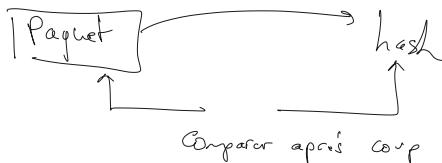
initialisation /etc faille → lecture /etc
apache → lecture OK /var /bo

Server les pays → interdite (etc) Contexte

Hash (Hachage)

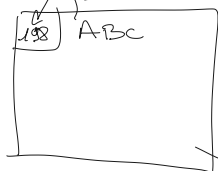


hash $\rightarrow$ empreinte



CRC Control Redundancy Check.

Exemple de contrôle ex:



A = 65

B = 66

C = 67

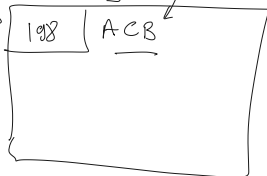
no match pos
 $\rightarrow$ ERROR CRC

erreur

contrôle
lecture

198/AB~~C~~ $\rightarrow$ erreur de lecture

198/ACB $\rightarrow$ collision



algos évitent les collisions.

md5 $\rightarrow$ Très bon $\rightarrow$ risque de collision

Très faible

sha(0) $\rightarrow$ Trop de collision

$>$ milliards de milliards

sha1 $\rightarrow$ Pos nég

$\rightarrow$ Possible

sha2/56 $\rightarrow$ extrêmement faible

$\rightarrow$ md5




hacker

patcher

$\rightarrow$ y mettre un code
compromis

$\rightarrow$ ayant le md5

$\rightarrow$ Combien de temps cela
Prendra?

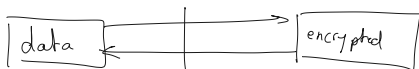
Cryptage

fonc de cryptage

- faible

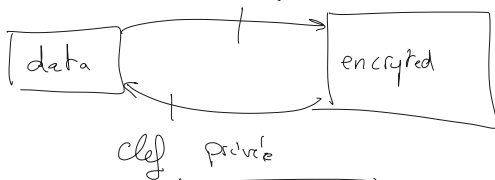
- + fortes, + complexes -

Cryptage Symétrique



mot de passe est
identique

Asymétrique clef publique



Publique $\rightarrow$ librement distribuable

Privée $\rightarrow$ ne doit pas être compromise (récupérée, ...)

clef Privée $\xrightarrow{\text{dérivation}}$ clef publique

Mot de passe : chaîne mémorisable $\rightarrow$ Copie/collé $\rightarrow$ OK

Secret : chaîne alphanum non mémorisable $\rightarrow$ Copie/collé $\rightarrow$ OK

Clef $\rightarrow$ 512 bits : flux binaire $\rightarrow$ représentation en base 64

Leton d'Auth. = secret $\rightarrow$ Copie/collé $\rightarrow$ OK

défini

64 octets = 0..255 caractères non imprimables

Imprimable : a-z A-Z 0-9 * / : = 64

csr : format pkcs10

pem, key, cert, crt : base64 dont multipart, pub et priv keys

\$-----BEGIN CERTIFICATE-----

\$-----BEGIN CERTIFICATE REQUEST-----

\$-----BEGIN PRIVATE KEY-----

\$-----BEGIN ENCRYPTED PRIVATE KEY-----

\$ key : format pem, uniquement la clef privée

\$ cert, cer, crt : Windows

pkcs12, p12, pfx : PKCS#12 (binaire)

der : flux binaire du certificat.

p7b, keystore : inclut le chemin de certification.

crl : liste de révocation.

def $\rightarrow$ fichier — cer
 — .pem
 p12, pfx etc ...

Certificat X.509 $\rightarrow$ flux aux normes ISO
 fichier

Users

$\swarrow$ a l'etablissement par user

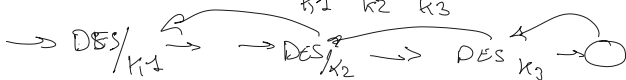
id	login	pwd	sel
1	t@t.com		x
2	user2		y

mdp + "sel"
 hash

3DES $\rightarrow$ DES 3 clefs

1 clef $\rightarrow$ 2?

bonjour
 k1 k2 k3



Suite au 10/11 : [TinyCert](#)

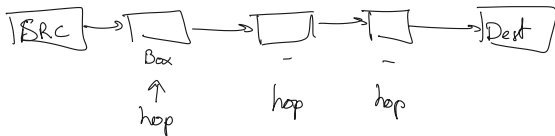
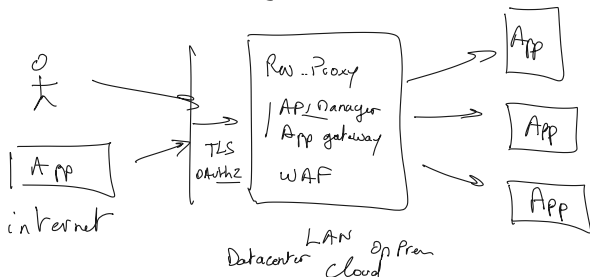
Reverse proxy :

Nginx (SRV Web, reverse proxy)

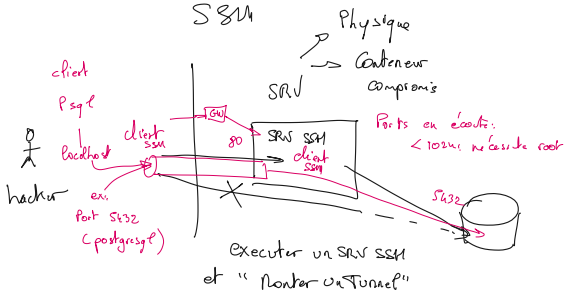
Kong

Traefik

→ Facturation
→ gouvernance



SSH



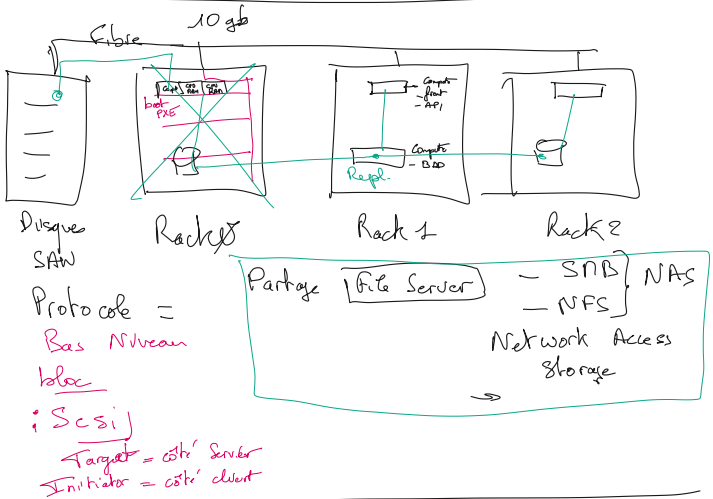
Différence Cloud / Hébergement Hosting

Hébergement = uniquement des machines / VN
IaaS -

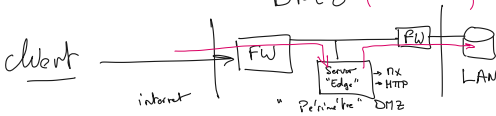
Cloud = PaaS, IaaS, SaaS, VM, -...

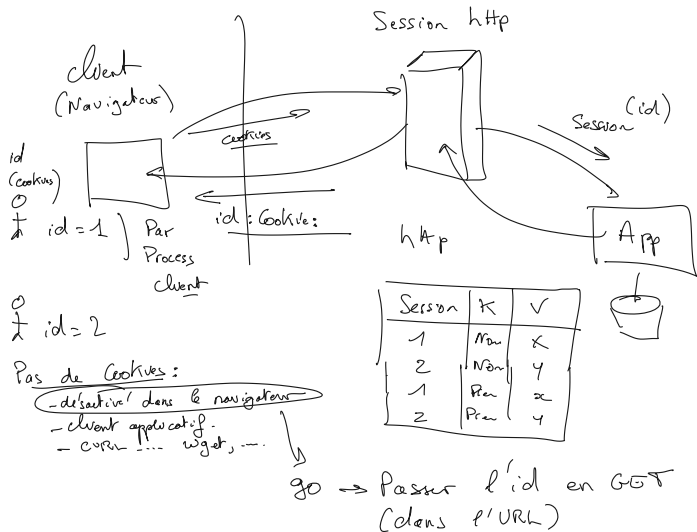
privé = OpenStack (opensource)

VM, stockage, bdd, réseau (SDN),



DMZ (obsolekte)





Docker CE → Container Runtime
(Moteur Docker local)

Concurrents: CRIO, Containd, podman(CR1)
LXD

Dev → Docker → [image] → Podman CRIO → K8s
ISO

Docker CE → gratuit

Docker Hub →
 - fonctionnalités
 -) gratuite
 -
 -
 -
 -
 -
) Premium

~~Docker Machine~~ → Virtual
Hypervisor
→ cloud AWS, Azure

↓
(Vagrant, Terraform + Ansible)

~~Desktop~~ → Windows → Ctr | Windows
→ Mac | Linux

↳ WSL2 → Docker CE natif

DOCKERCE

Locale par Noeud

↳ pas Enterprise Compliant

Pas de High Avail

→ OK pour du Dev

Ent. Compliant
avec HA.

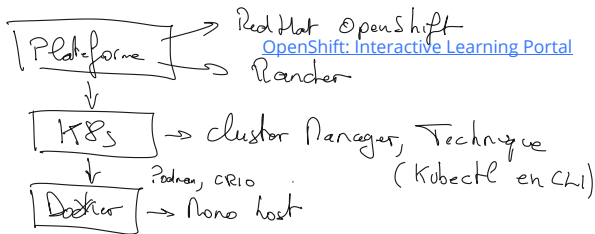
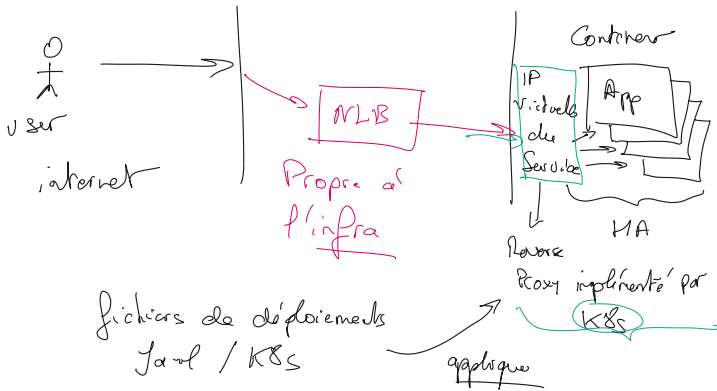
- Docker Swarm → cluster
La limite fonctionnellement
(gratuit)

- Docker EE → puissant
fonction
log, gouvernance
→ CHER
→ QUE DOCKER

⇒ Kubernetes (K8s)

→ Produit Opensource Dev Google à la base

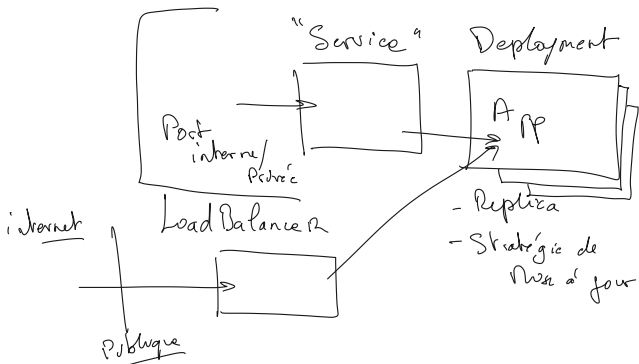
→ GRATUIT, Reconnu, Puissant, Technique



K8s → Cluster Impl → Compose

Dev → pas besoin d'un cluster Enterprise
 ↳ "Bac à sable" → Tests -

Minikube → Déploiement de K8s pour le
 Test / Dev



-
- Sécurité - Docker n'écoute pas en IP par défaut
 - Si IP → pas d'auth par défaut
- Ajouter la prise en charge TLS
- faire une auth. par certificats
-

K8s → cluster sécurisé par défaut

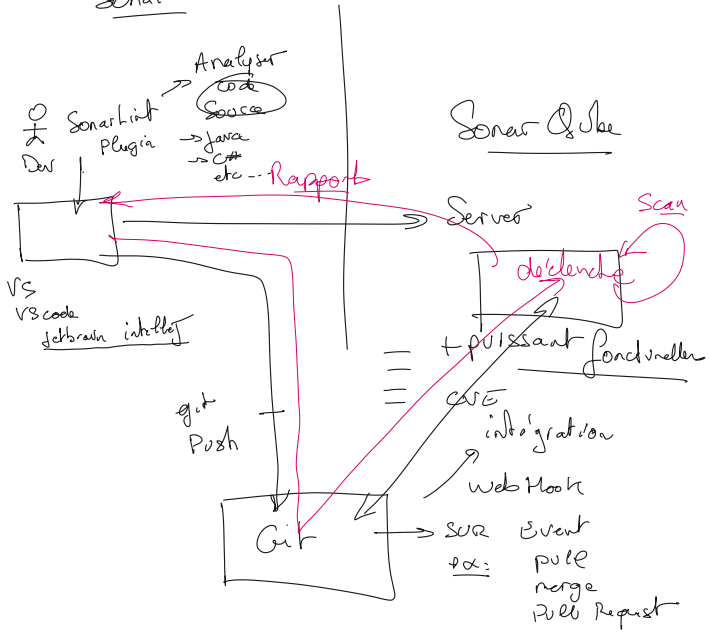
Souvent les images sont en USER Root
 (directive USER dans le Dockerfile)

RECOMMANDÉ

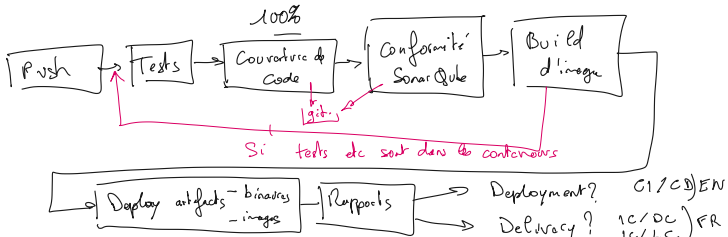
K8s → Conteneurs Root sont acceptés

OpenShift → " " sont interdits

Sonar

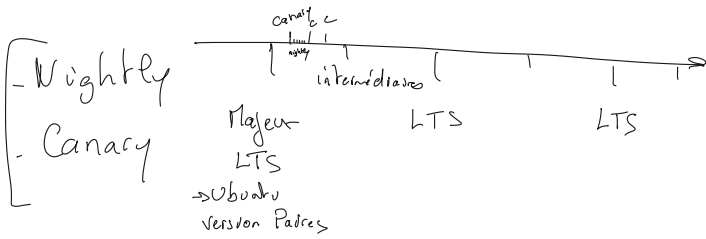


CI / CD Pipeline



Livraison = Mettre à Disposition

Deployment = Mettre en Prod



Conteneurs

REPO : TAG

ex: helloworld

ex latest

20

20-beta

v1

2021-11-10

K8s

App LTS

↑
Route LTS

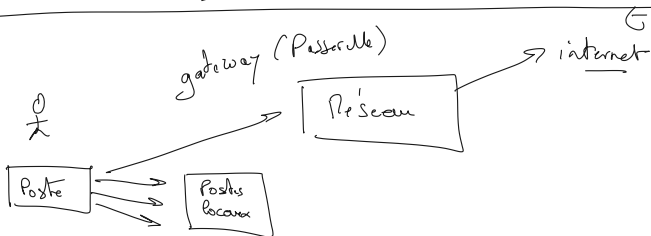
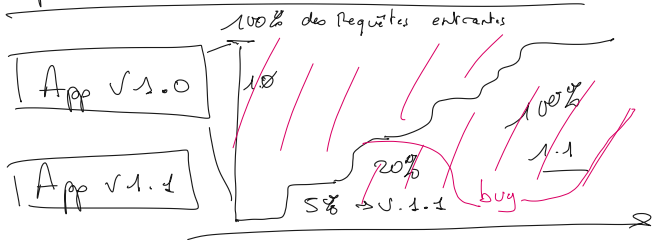
IMAGE

Remontez

App Canary Release

↑
Route Canary

Déploiement Progressif



- Lan d'entreprise (Compromis)

- Maison

- AP Public

AP Hacker "Mac Do"

