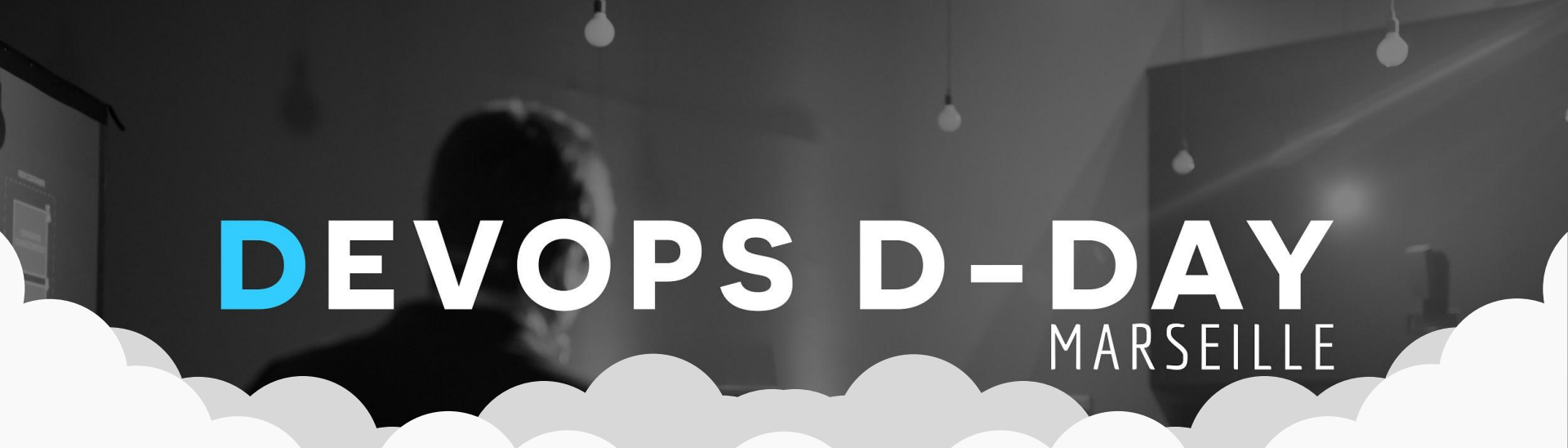


REX : Migration d'une application legacy dans un cluster K8S

J. Masson, N. Tournier (Treeptik, Linkbynet)

2018

Toto IT

Organisation et Présentation

1 SI central

10 M

Clients

100 K

Employés

39

Agences

Toto IT

Aspects techniques

Parc

Multi-datacenter

Techno

Hétéroclites
Dev
&
Ops

Récent

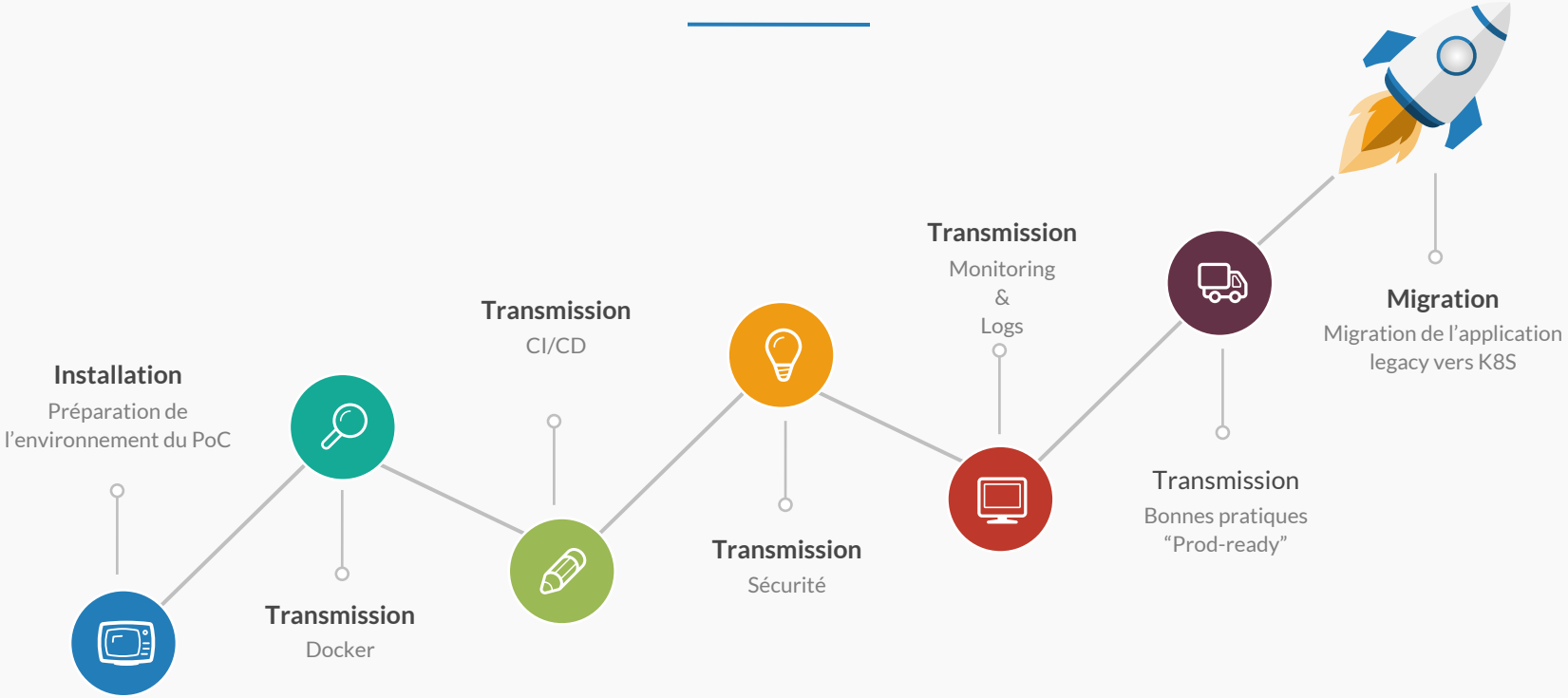
Depuis quelques mois

Toto IT &
Treeptik

Toto IT

TREEPTiK.
A LINKBYNET COMPANY

Contexte


Installation
Préparation de l'environnement du PoC
Transmission
Docker
Transmission
CI/CD
Transmission
Sécurité
Transmission
Monitoring & Logs
Transmission
Bonnes pratiques "Prod-ready"
Migration
Migration de l'application legacy vers K8S

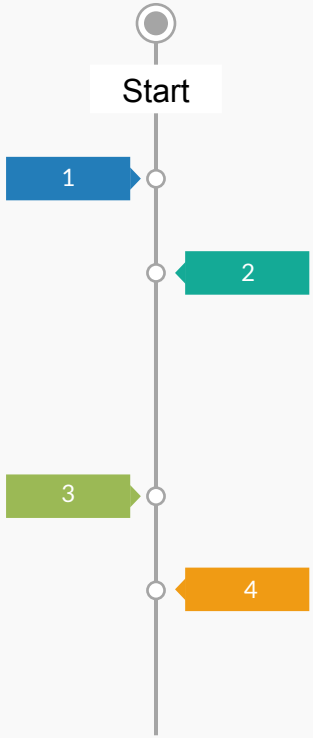
Timeline

Images & registry

- Socle images Docker
- Choix de la Registry
- Exemple : Migration d'une application

Monitoring & Logging

- Infrastructure centralisée
- Infrastructure décentralisée



CI / CD

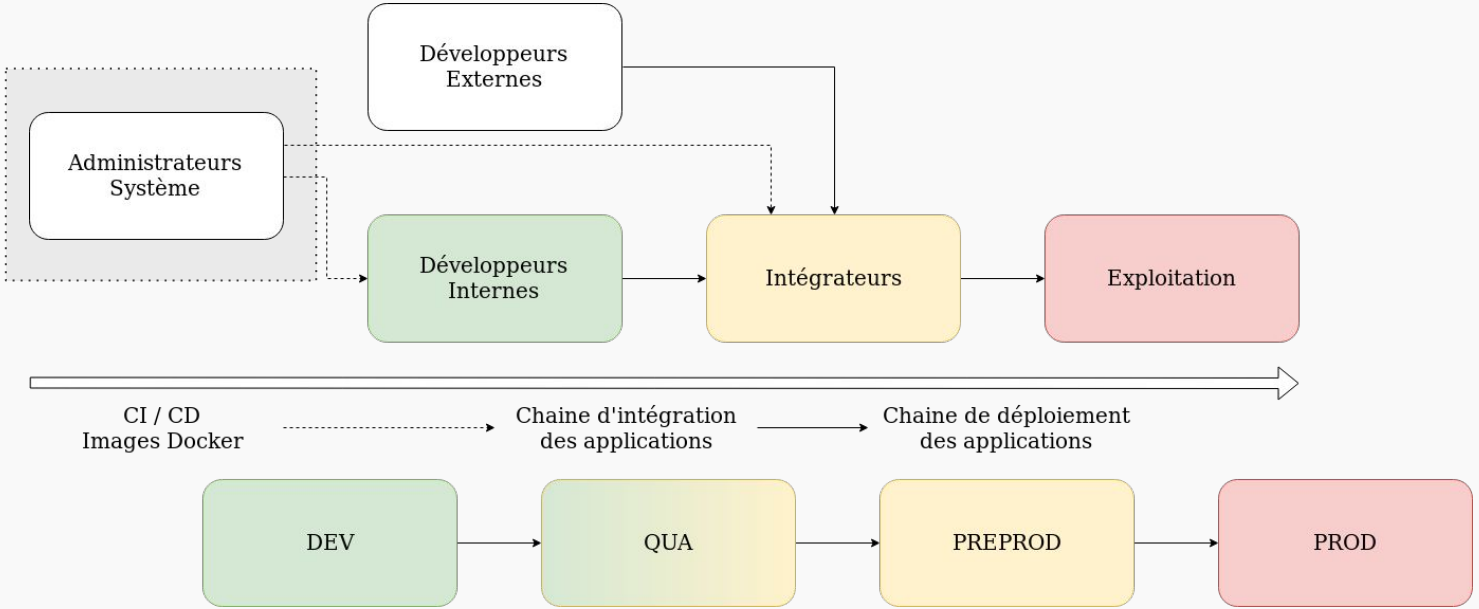
- Environnement développeurs
- Namespace & Environnement
- Déploiement dans K8S

Sécurité

- Objets Kubernetes
- CI / CD
- Infrastructure

L’accompagnement Image & Registry

Socle d'images Docker



Socle d'images Docker

Méthodologie

Conception des images de base

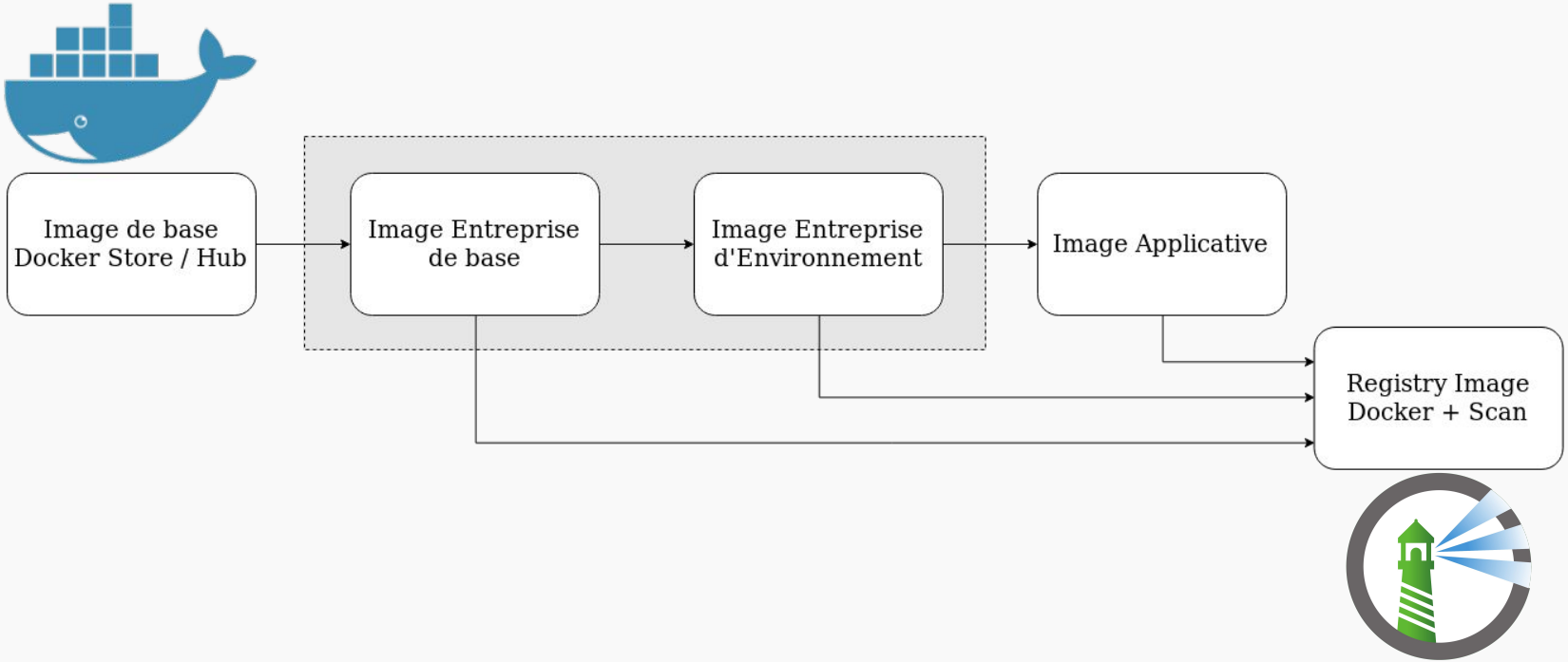
1. Image OS de confiance
2. Construction de l'environnement
   => Analogie à la mise en place d'une VM
3. Mise à disposition pour les images app.

vs. Distroless
github.com/GoogleContainerTools/distroless

Docker Store / Hub
store.docker.com / hub.docker.com

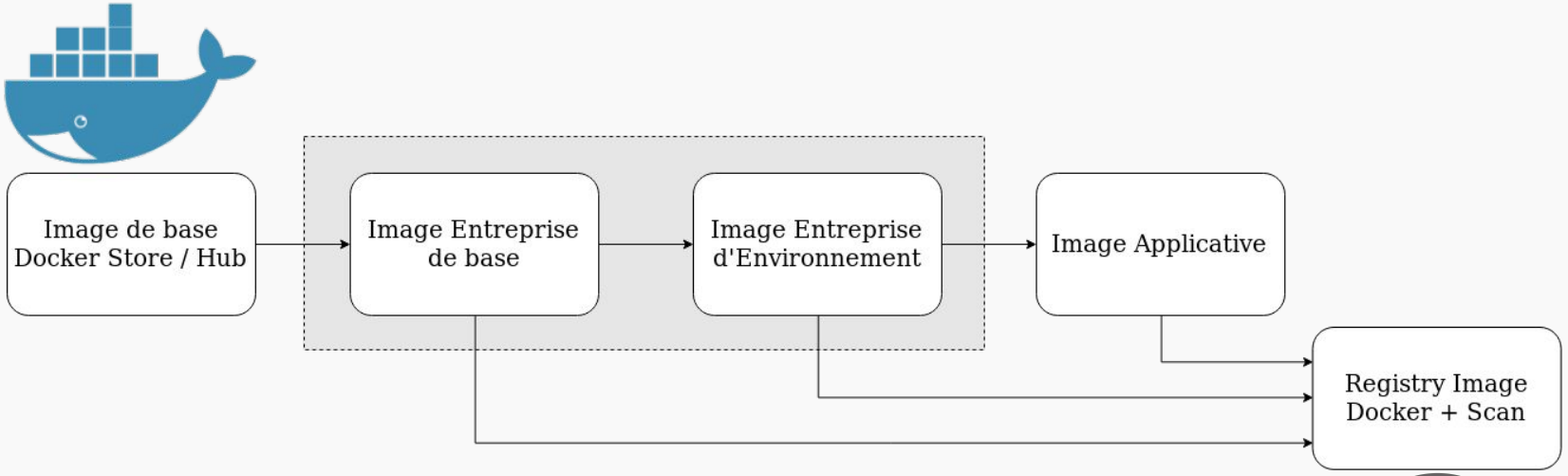
Socle d'images Docker

Méthodologie & Repository



Socle d'images Docker

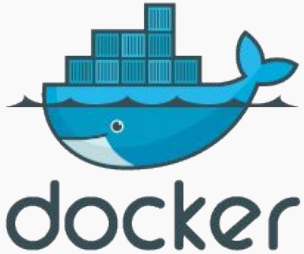
Méthodologie & Repository

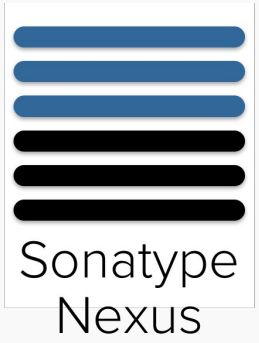


ANSIBLE

HashiCorp
Packer

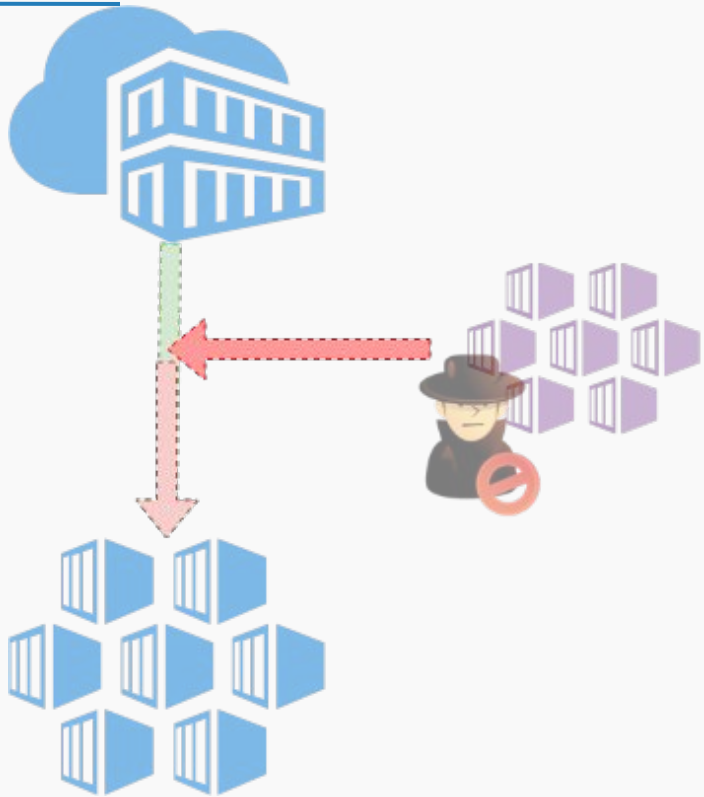
Choix de la registry





vs

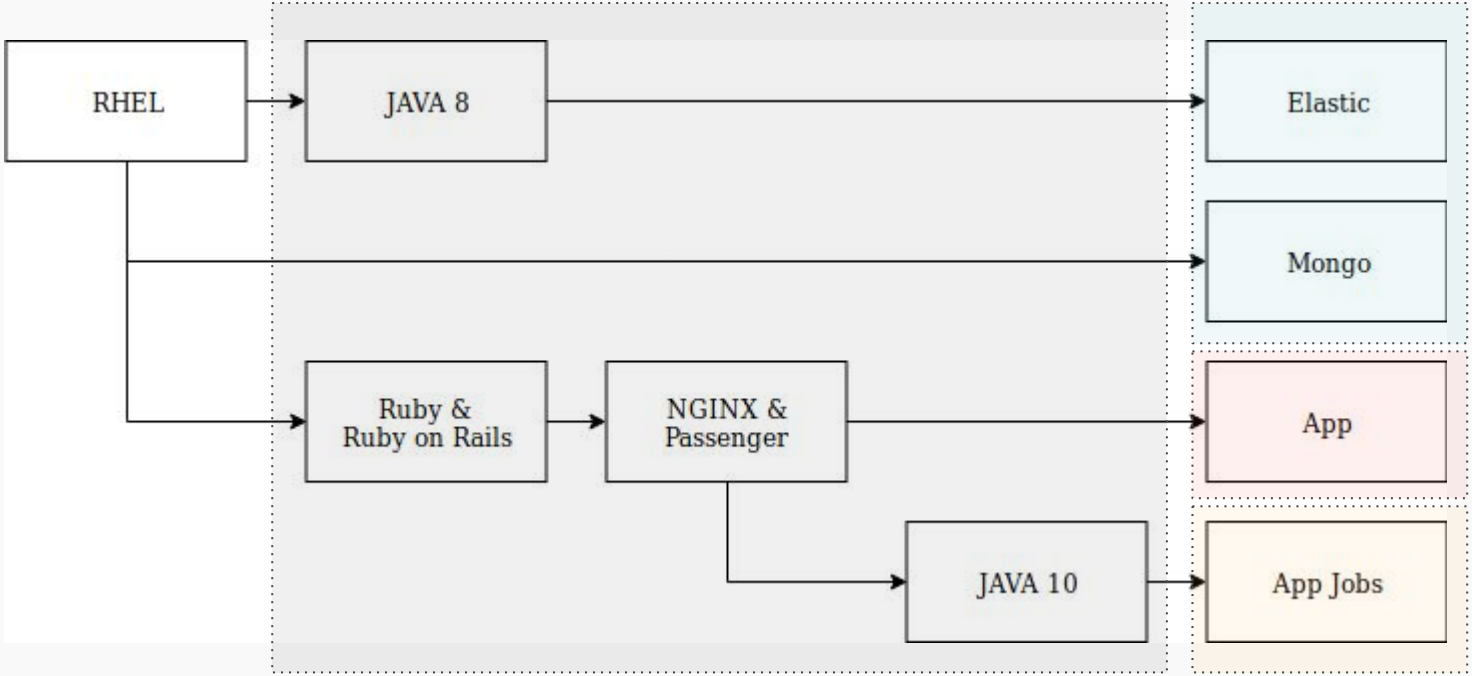
Notary & Helm provenance



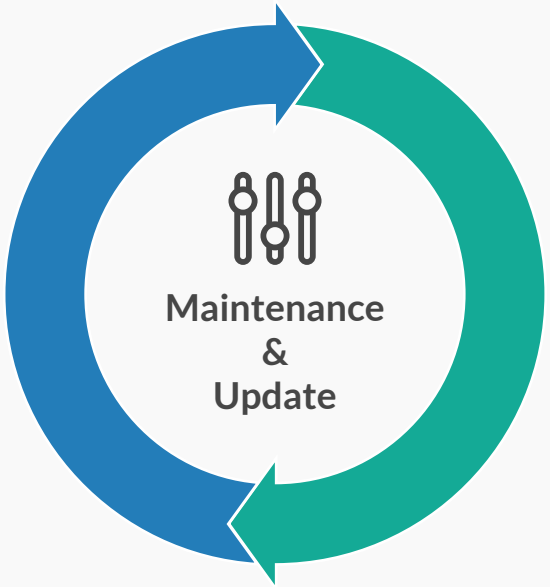
L’accompagnement
Choix de l’application

Socle d'image Docker

Exemple sur l'application legacy

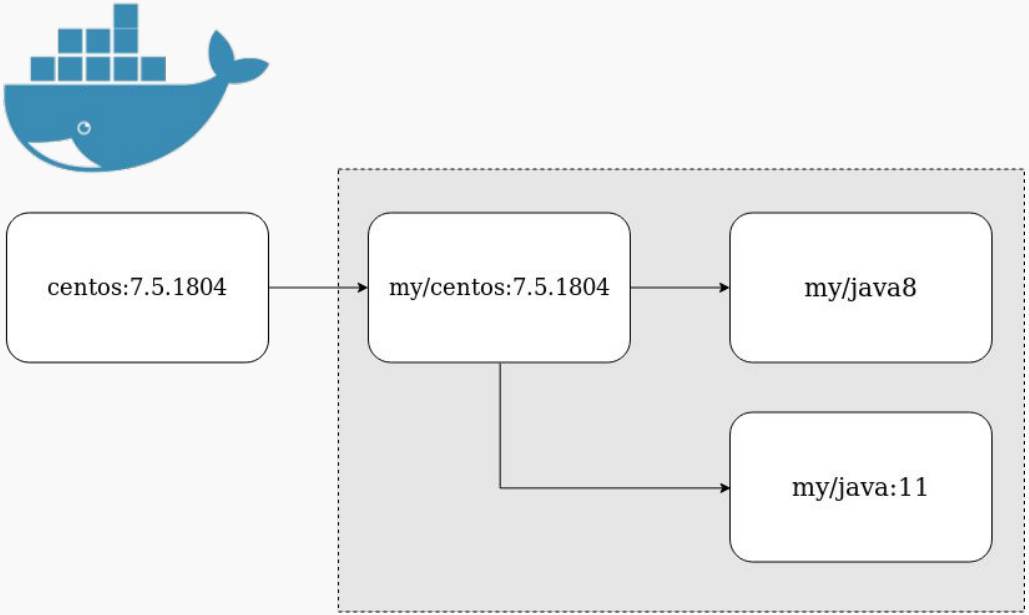


Étapes techniques



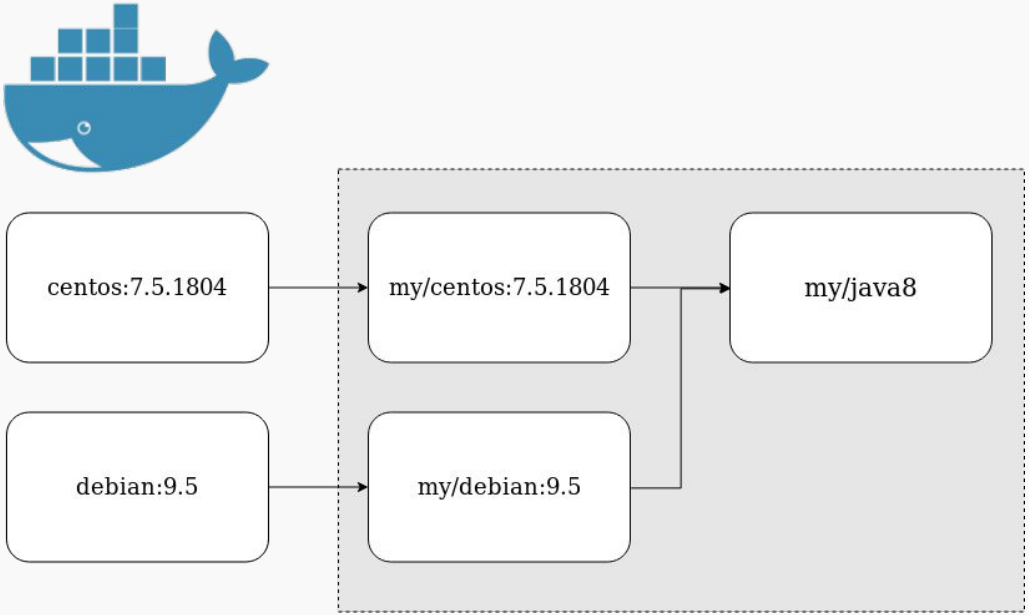
Socle d'image Docker

Simplification du problème (2/2)



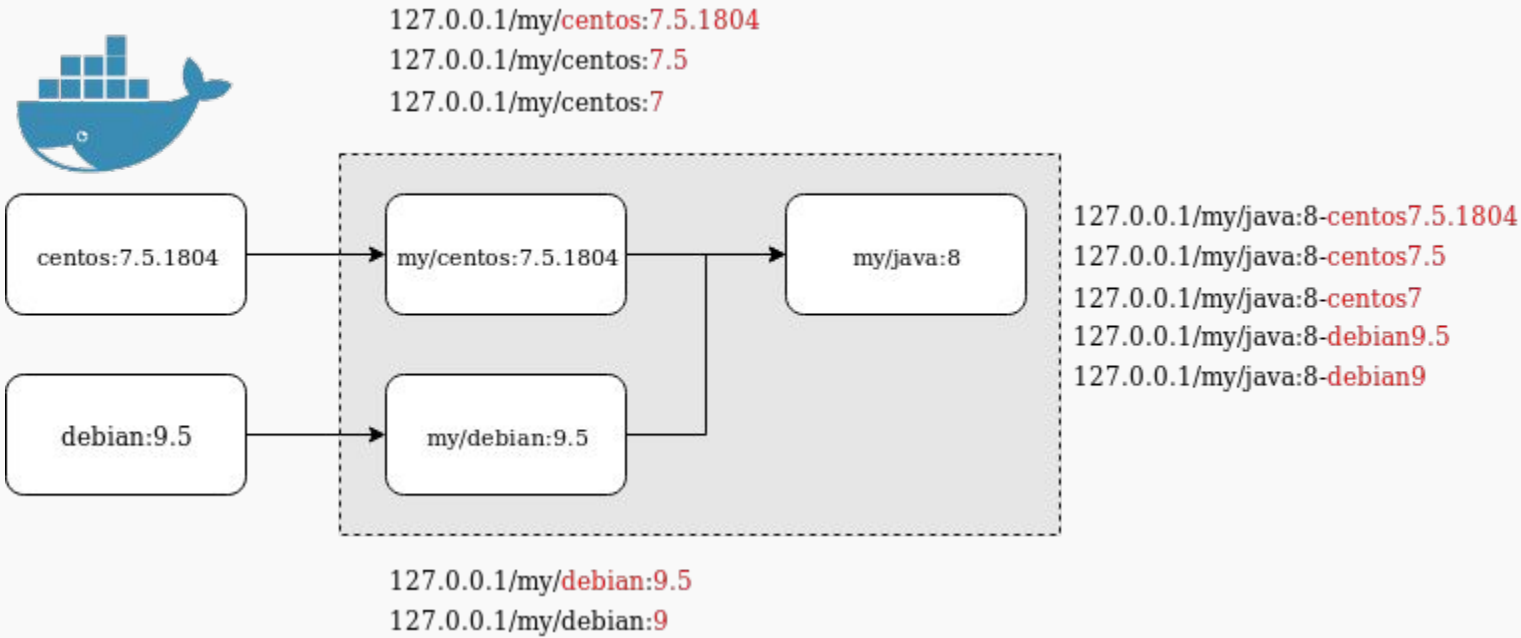
Socle d'image Docker

Simplification du problème (2/2)



Socle d'image Docker

Convention de nommage



Socle d'image Docker

Automatisation et Jenkinsfile

Pré-requis :

- Jenkins & Docker
- Plugins suggérés à l'installation
- + Parameterized Trigger Plugin
- Harbor

Jenkinsfile :

github.com/n1c0l4stournier

```
/**
 * Struture d'un pipeline Jenkins pour l'automatisation du build d'un socle Docker
 */
pipeline {

    agent any

    parameters {

        /**
         * Liste des paramètres en provenance de l'image sur laquelle on repose
         * Elle doit être en lien avec le précédent job
         */

    }

    environment {

        /**
         * Variables correspondant à l'image que nous construisons
         */

    }
```

```
stage ('Triggers') {
    steps {
        script {

            def buildParameters = [

                /**
                 * Liste des variables à transmettre au job suivant
                 */
            ]

            /**
             * Liste des jobs à déclancher
             * Les jobs suivants devront prendre en paramètre cette liste
             * ex : build job: 'app/master', parameters: buildParameters
             */

        }
    }
}
```

Socle d'image Docker

Automatisation et Jenkinsfile

Conclusion :

- Mise en place d'une CI/CD pour les Ops. Adm. Sys.
- Analogie avec la mise en place de VM
- Automatisation des mises à jour
- Ensemble d'images entreprise à la disposition des Dev.

Perspectives :

- Avant de passer au conteneur, automatiser les opérations manuelles actuelles
- Terraform + Ansible
- Mutualiser ce changement avec Packer

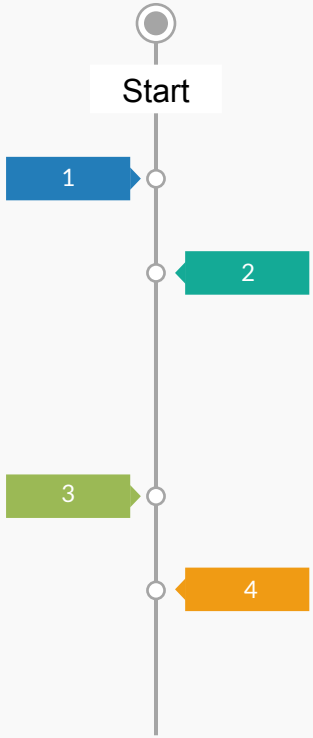
Timeline

Images & registry

- Socle images Docker
- Choix de la Registry
- Exemple : Migration d'une application

Monitoring & Logging

- Infrastructure centralisée
- Infrastructure décentralisée



CI / CD

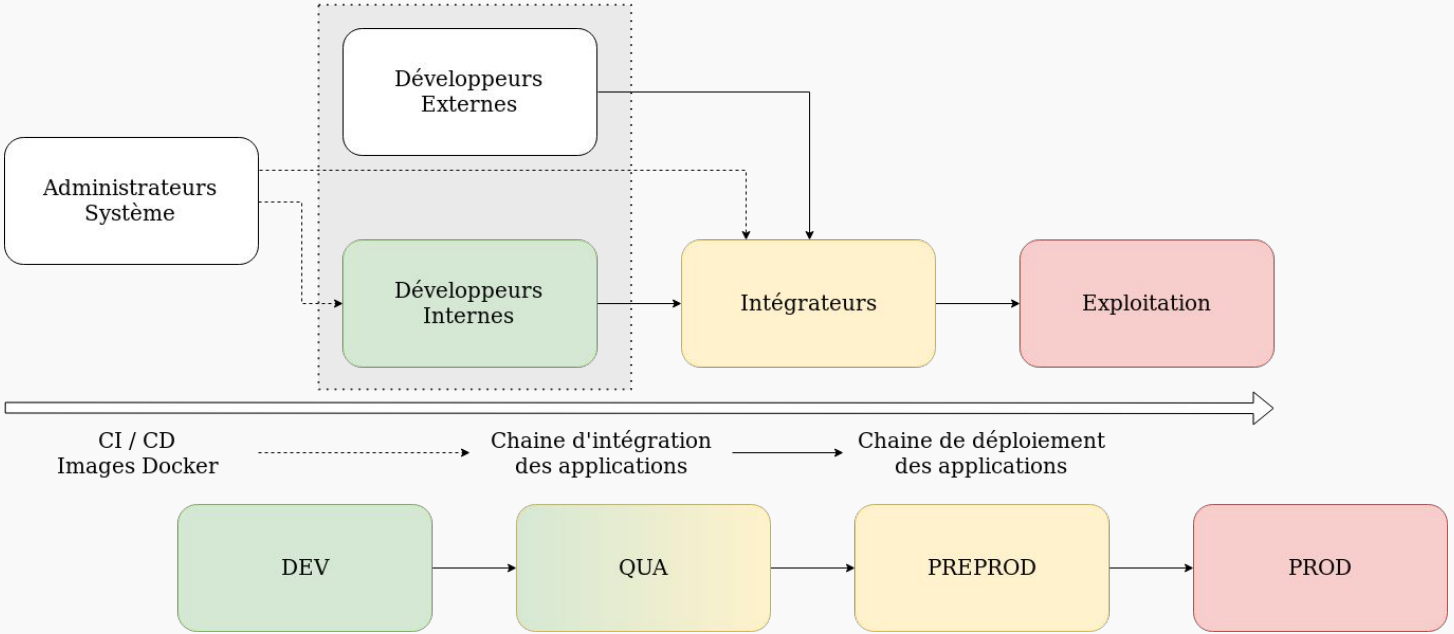
- Environnement développeurs
- Namespace & Environnement
- Déploiement dans K8S

Sécurité

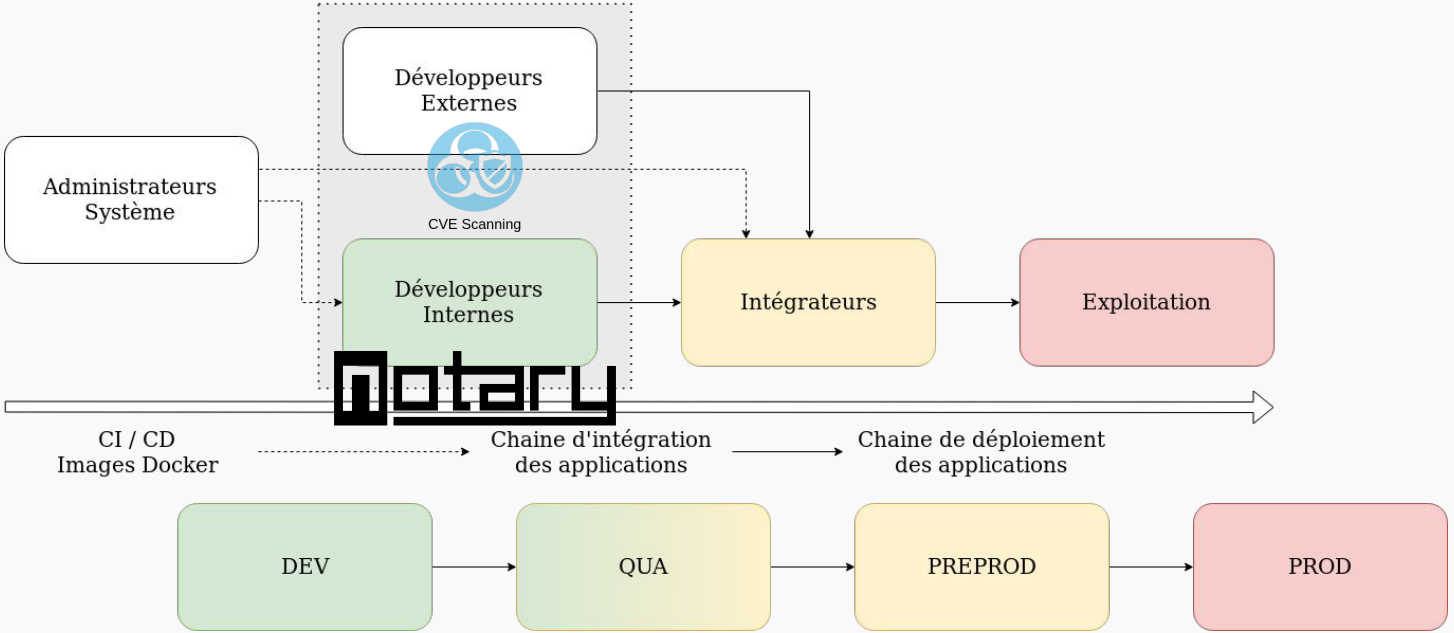
- Objets Kubernetes
- CI / CD
- Infrastructure

L’accompagnement CI/CD

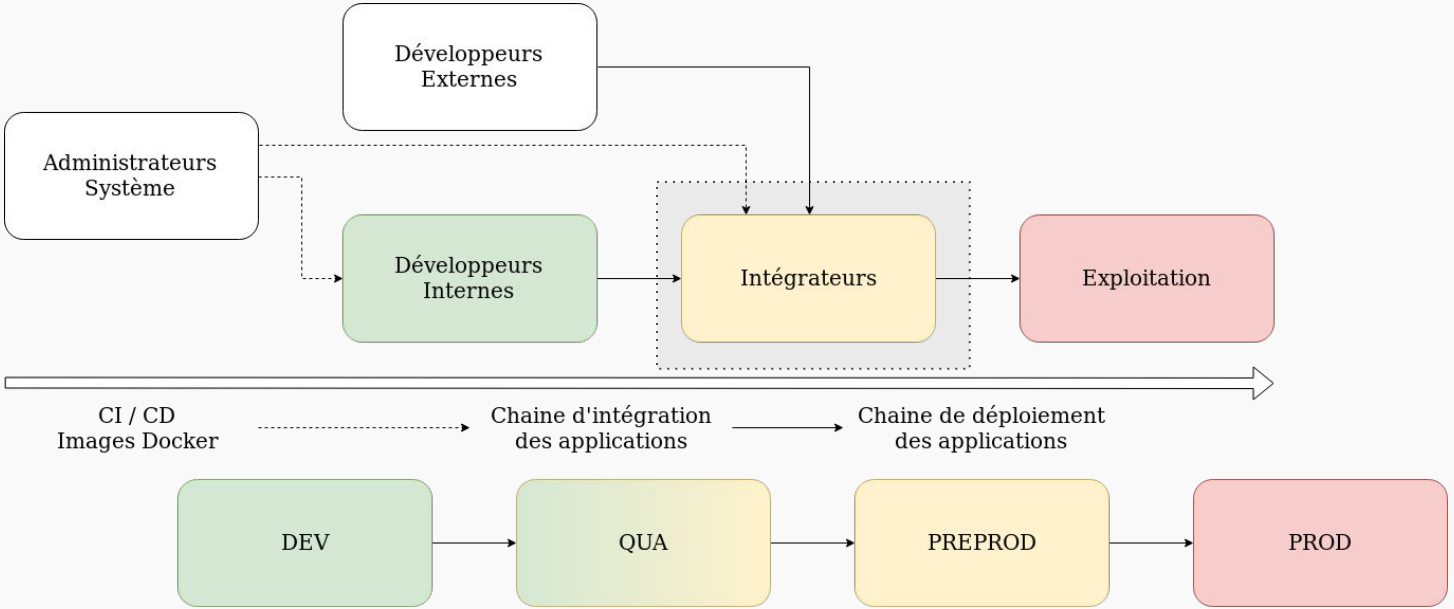
Déploiement K8S



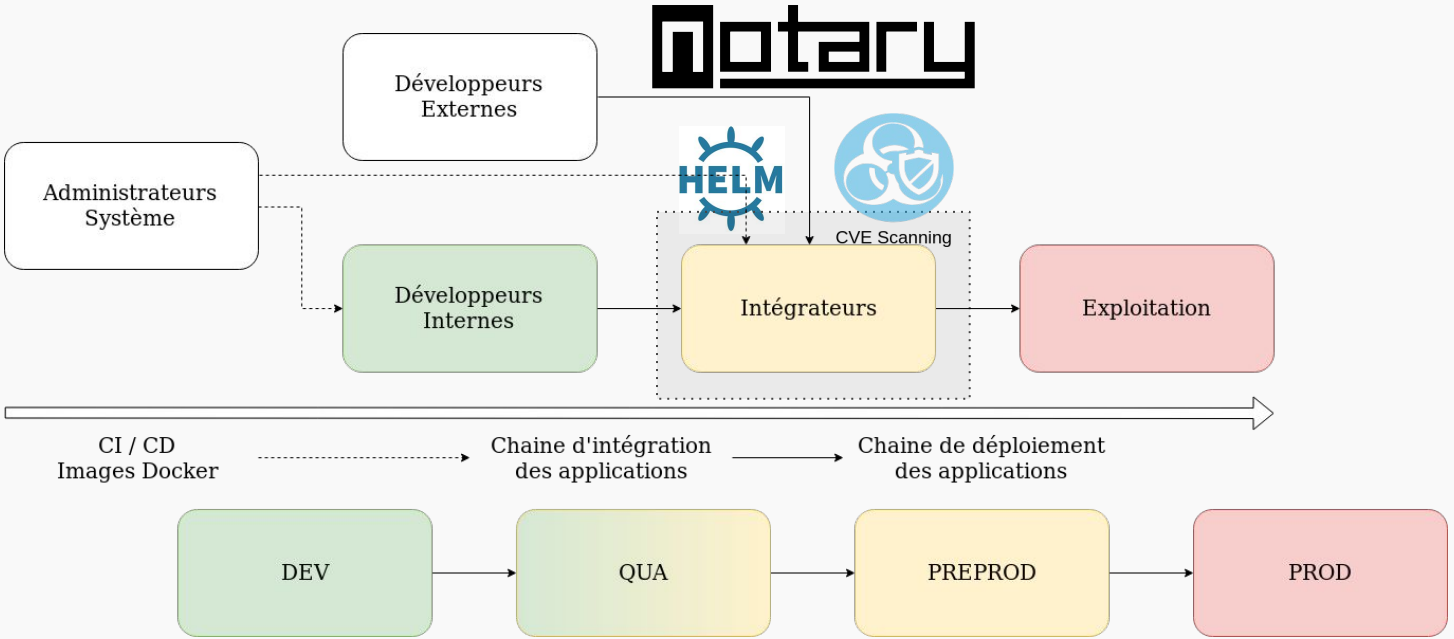
Déploiement K8S



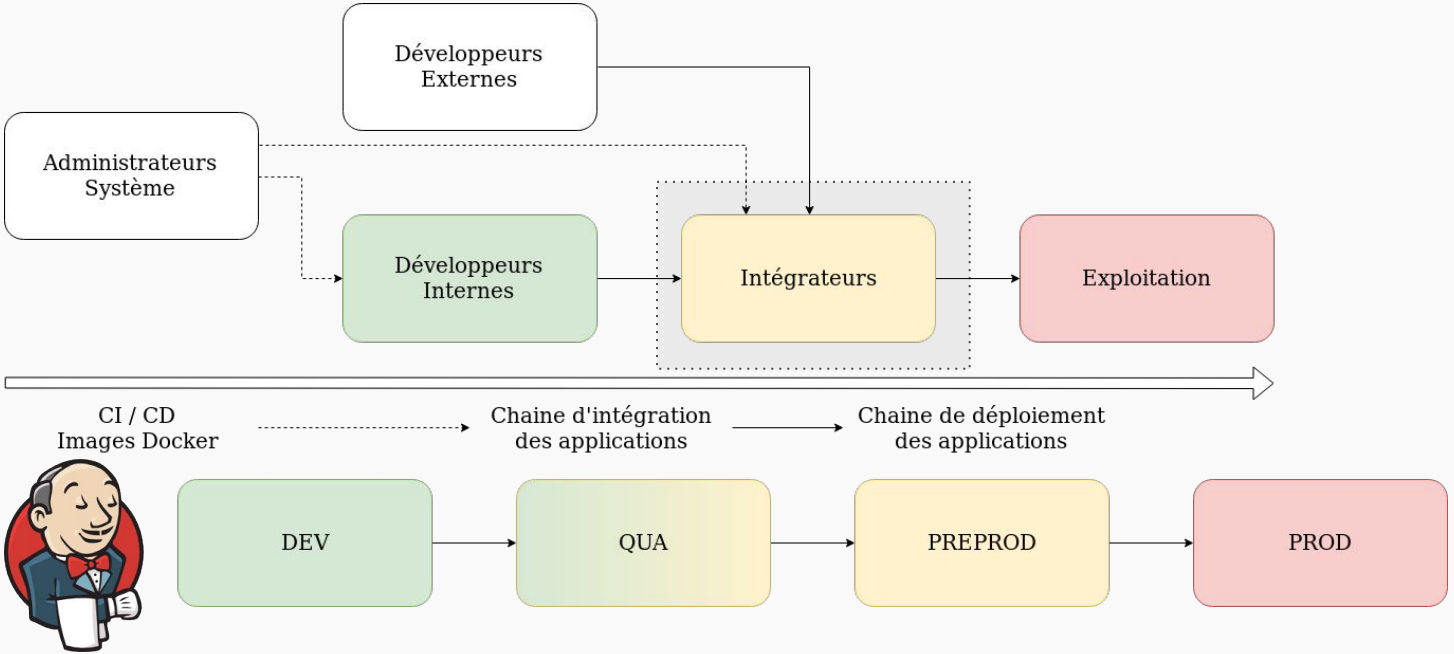
Déploiement K8S



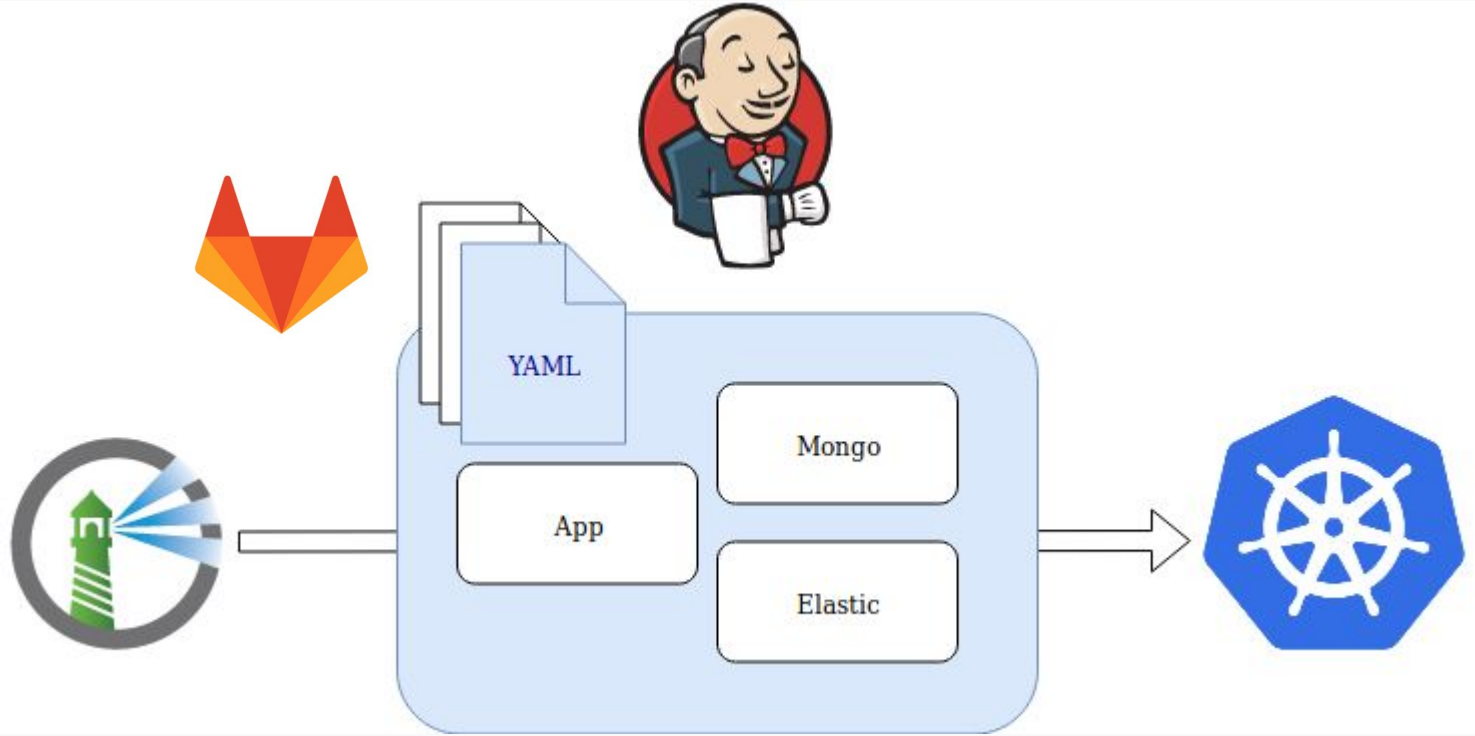
Déploiement K8S



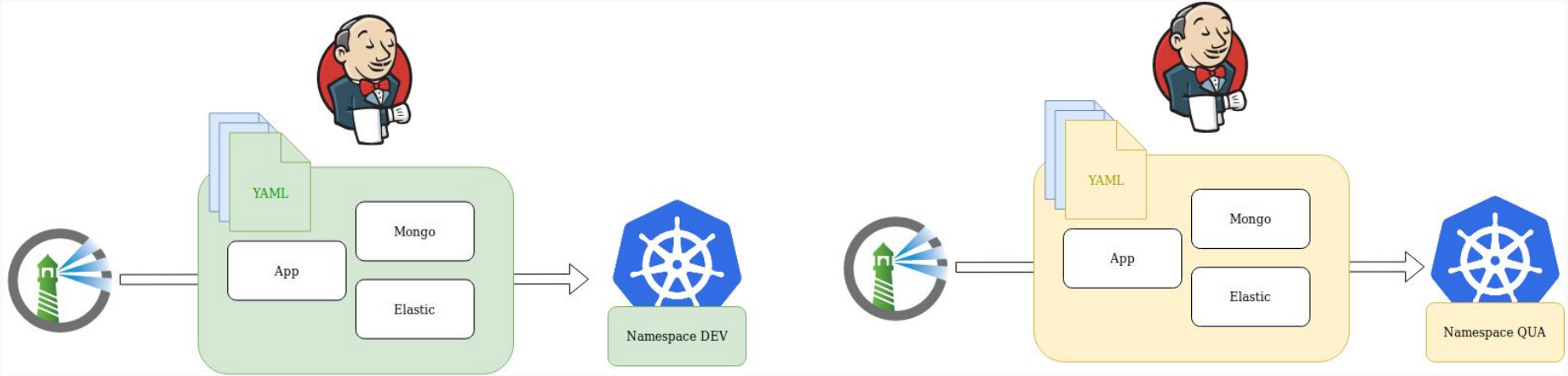
Déploiement K8S



Déploiement K8S



Déploiement K8S



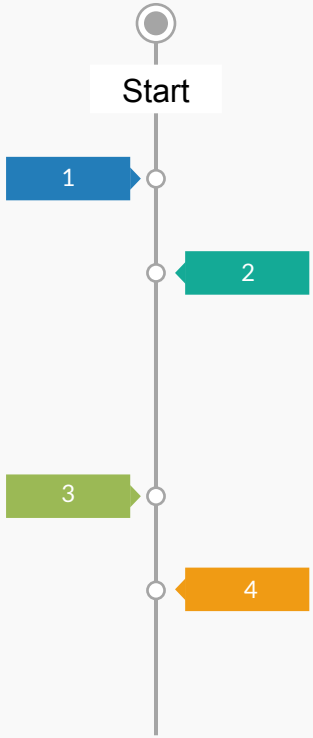
Timeline

Images & registry

- Socle images Docker
- Choix de la Registry
- Exemple : Migration d'une application

Monitoring & Logging

- Infrastructure centralisée
- Infrastructure décentralisée



CI / CD

- Environnement développeurs
- Namespace & Environnement
- Déploiement dans K8S

Sécurité

- Objets Kubernetes
- CI / CD
- Infrastructure

L’accompagnement Monitoring - Logging

Monitoring & Logging

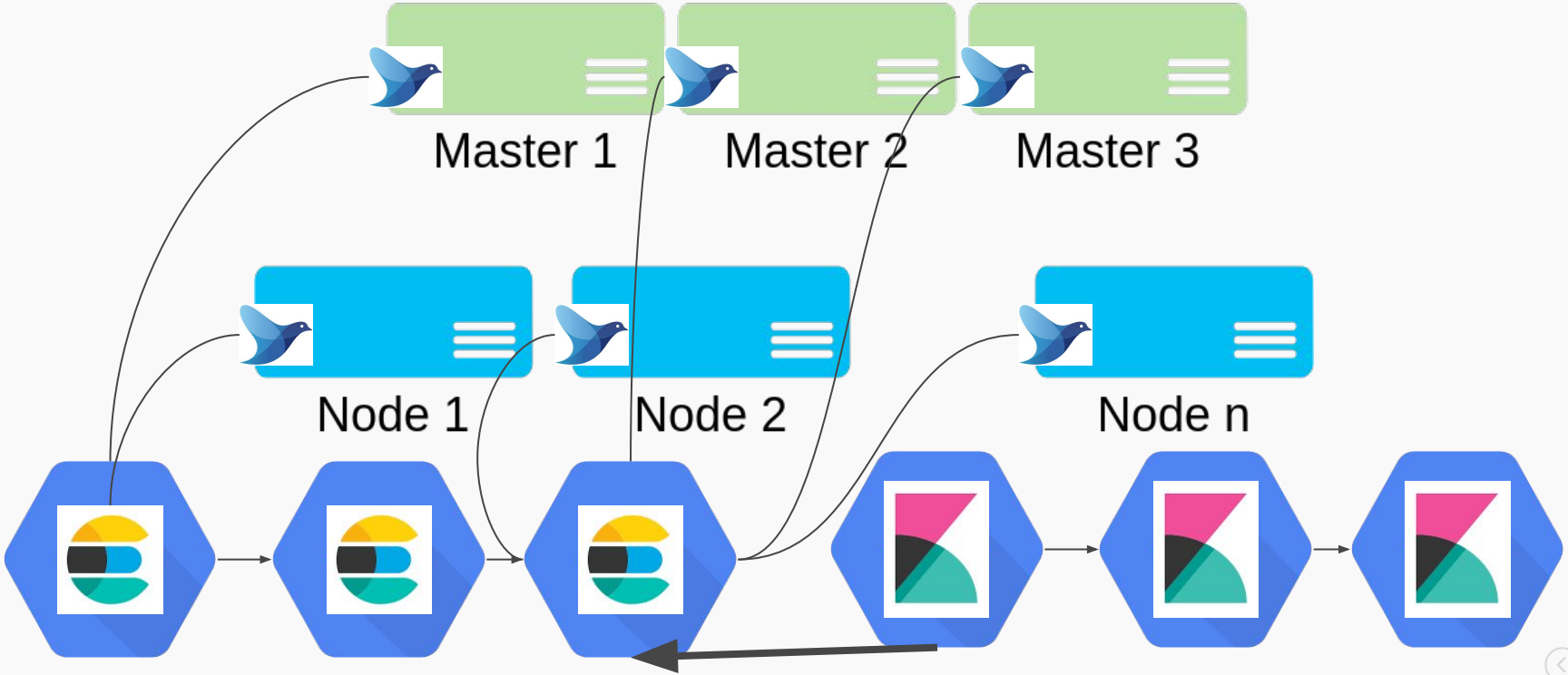
La centralisation et le découplage

Les objets Kubernetes :

- Hôte
- Cluster
- Pods
- Service Kubelet, ...

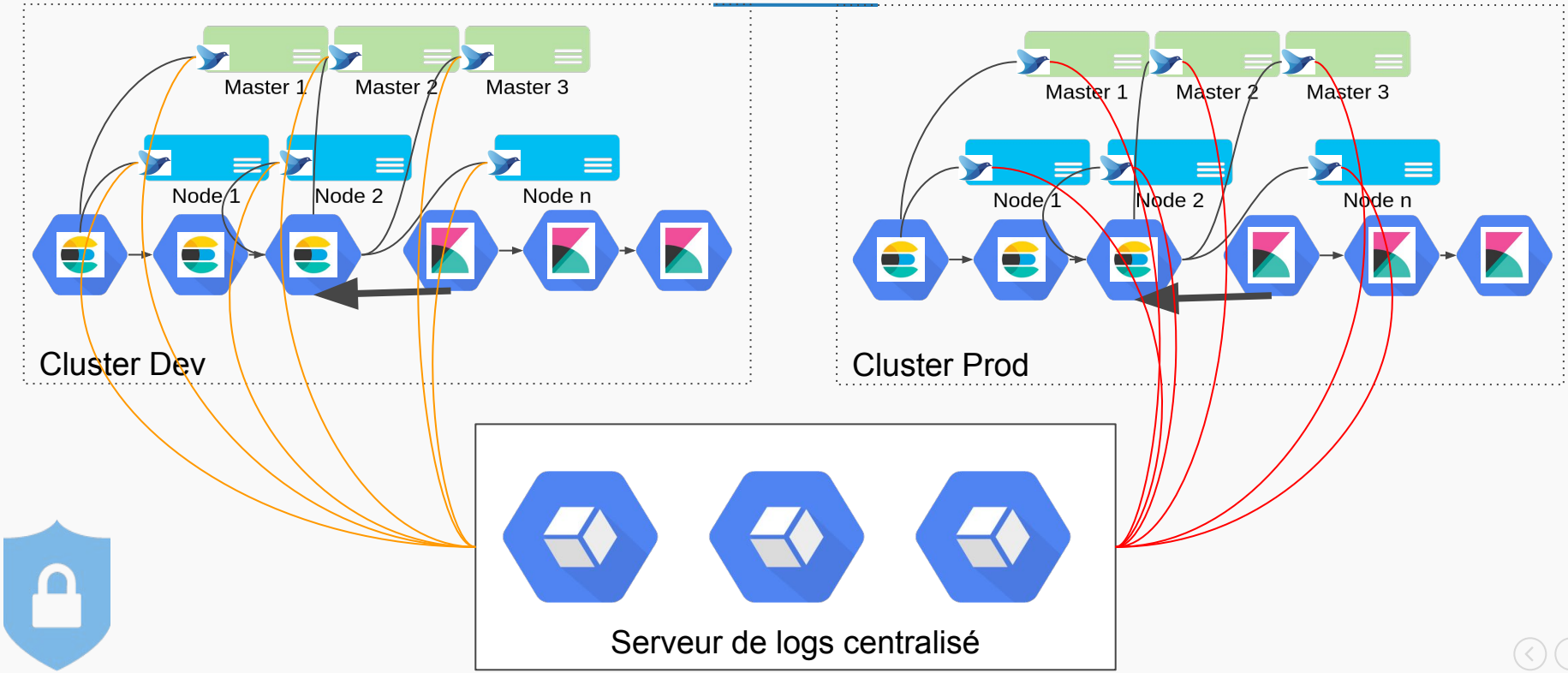
Monitoring & Logging

La centralisation et le découplage



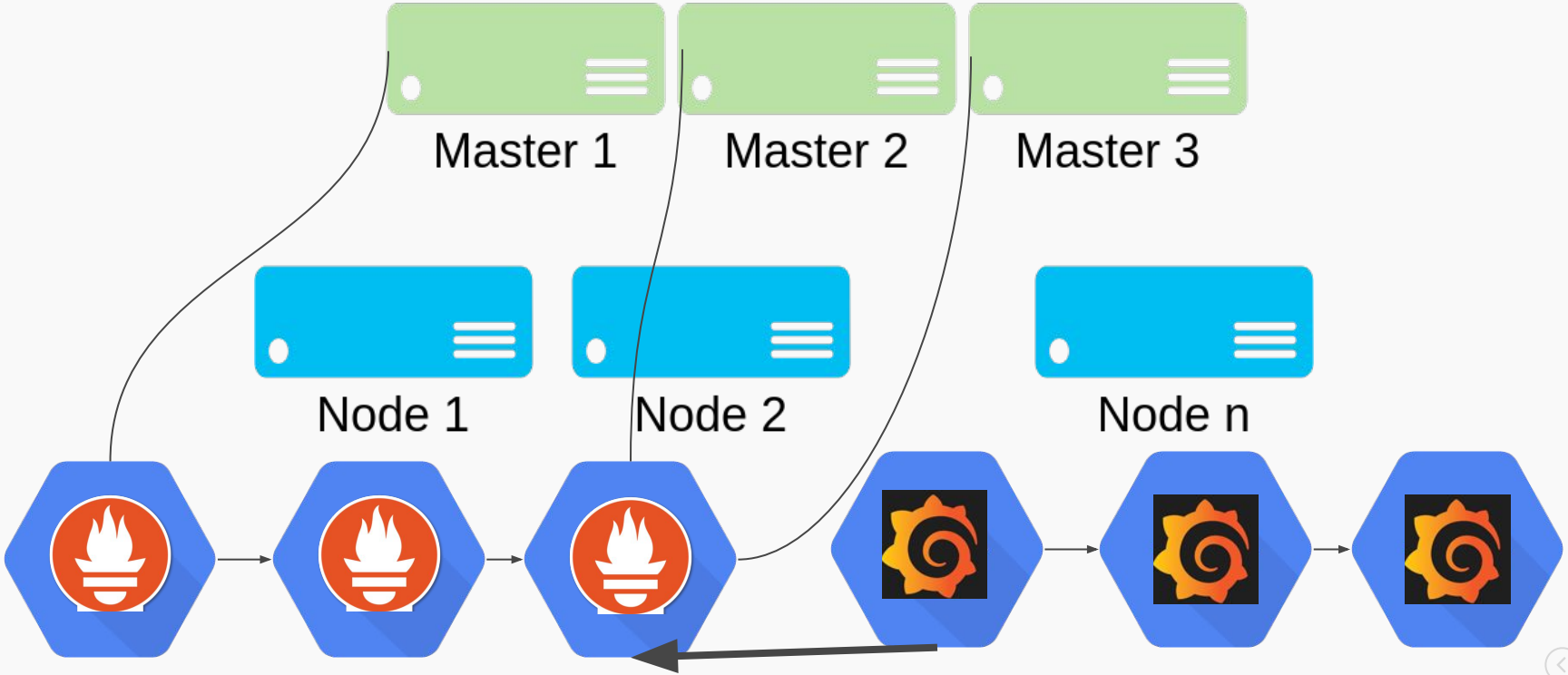
Monitoring & Logging

La centralisation et le découplage



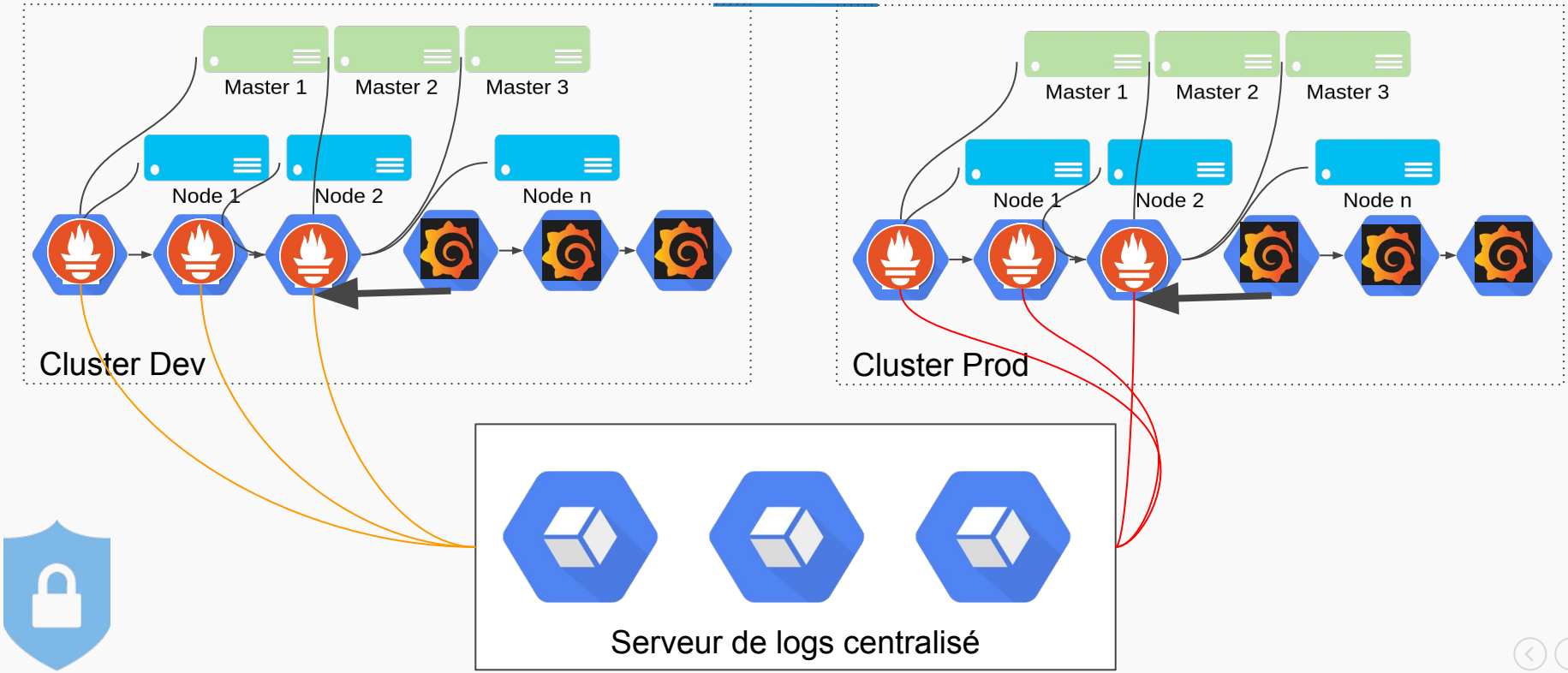
Monitoring & Logging

Le monitoring et l'interconnexion aux outils entreprises



Monitoring & Logging

La centralisation et le découplage



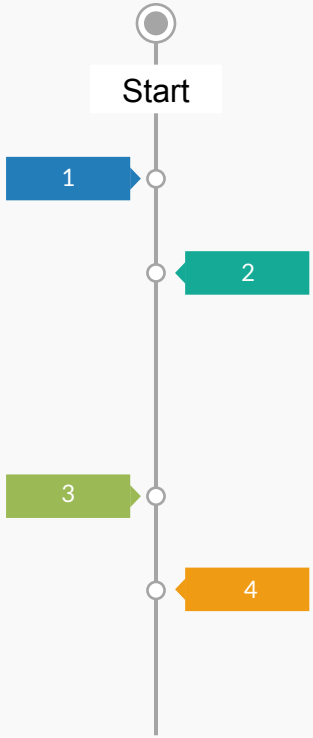
Timeline

Images & registry

- Socle images Docker
- Choix de la Registry
- Exemple : Migration d'une application

Monitoring & Logging

- Infrastructure centralisée
- Infrastructure décentralisée



CI / CD

- Environnement développeurs
- Namespace & Environnement
- Déploiement dans K8S

Sécurité

- Objets Kubernetes
- CI / CD
- Infrastructure

L’accompagnement Sécurité

Sécurité

Autour des images Docker

- Fréquence de mise à jour
- Capitalisation des déploiements
- Signature d'image Docker

ANSIBLE

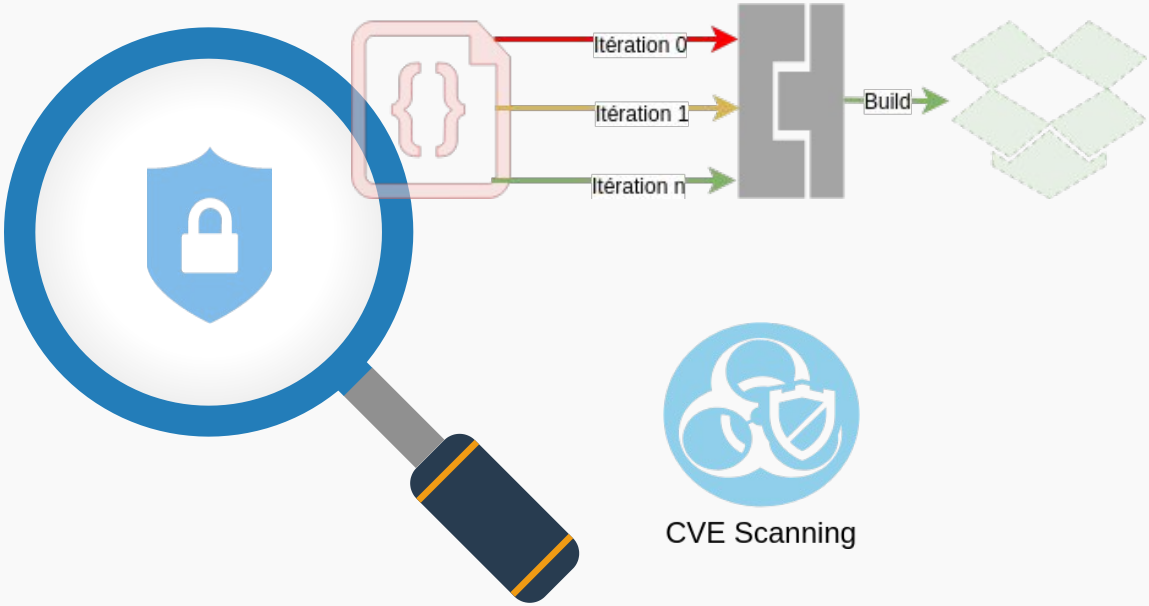
HashiCorp Packer

notary

Sécurité

Autour de la CI / CD

- Scan CVE
- TDD
- TDI



Sécurité

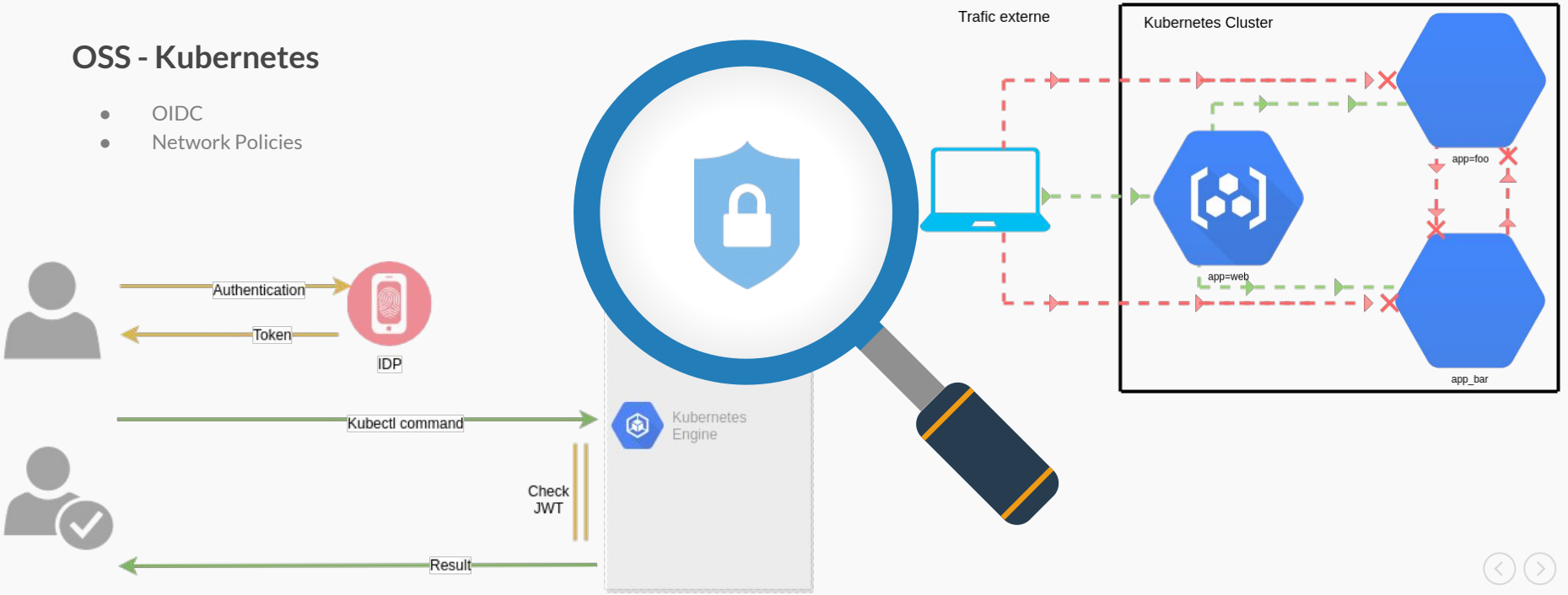
L’infrastructure

- Savoir
- Centraliser
- Simplifier

Sécurité

OSS - Kubernetes

- OIDC
- Network Policies



Sécurité

OSS - Kubernetes

- Signature d'image et utilisation de hash
- Helm Provenance

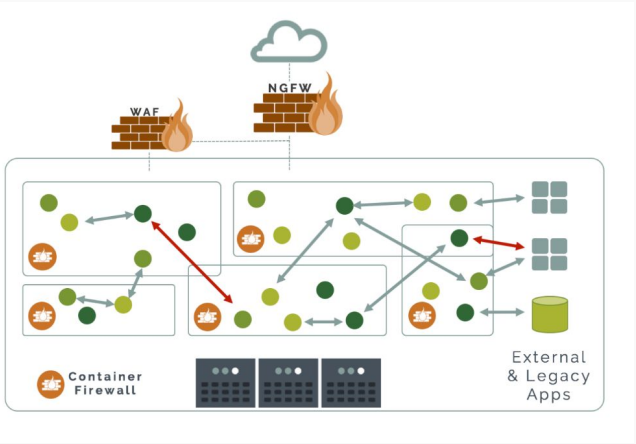
notary

HELM

Sécurité

Licence - Kubernetes

- Firewall inter-container
- Scan temps réel Hôte & Container
- Registry & Container Scan



NeuVector

Bilan

Thanks for Watching

Treeptik, Linkbynet : J. Masson, N. Tournier

Contact us:

www.treeptik.fr

j.masson@treeptik.fr

n.tournier@treeptik.fr

@sphinxgaiaone

@n1c0l4stournier

Sphinxgaia

n1c0l4stournier