

Infrastructure PaaS

Université de Lorraine

Frédéric Nass, Pierre Maffeis
Juin 2024



Contexte universitaire

- Université de Lorraine : 60 000 étudiants, 7100 personnels, 60 laboratoires
- Direction du Numérique (~200 pers) :
 - 4 sous-directions
 - Infrastructures et Services (~40 pers.)
 - Système d'Information Études et Développement (~40 pers.)
 - Services aux Usagers (~90 pers.)
 - Usages du Numérique (~30 pers.)



Contexte projet

- Projet PaaS initié à l'Infra en Avril 2021
 - Besoins : 500+ sites web, applications métiers, besoins pédagogiques
 - Consultation ESR : 11 réponses, 5 adopté ou en cours d'adoption de K8s
 - Moyens :
 - GT composé de 7 ingénieurs (infras, devs, proximité) élargi ensuite à 13 membres
 - Prestation « Jumpstart » assurée par un SRE (Guilhem Lettron)
 - Formation de 40 collègues de la DN à Kubernetes et au DevOps (Wescale)



Choix d'infrastructure

- Swarm rapidement écarté
- Étude comparative de Rancher / RKE2 vs OpenShift
- Choix de Rancher / RKE2
 - Rancher : déploie et maintient différentes versions de K8s sur des clouds **privés** et **publics**
 - RKE2 : la version communautaire et la version sous support utilisent le même code. Mêmes fonctionnalités, stabilité et sécurité.
 - RKE2 : plus ouvert sur le choix des briques CNCF (y compris supportées).
 - Étude financière en faveur de Rancher pour un support en production.



Déploiement



Packer

• **Packer** : pour construire les images des nœuds K8s



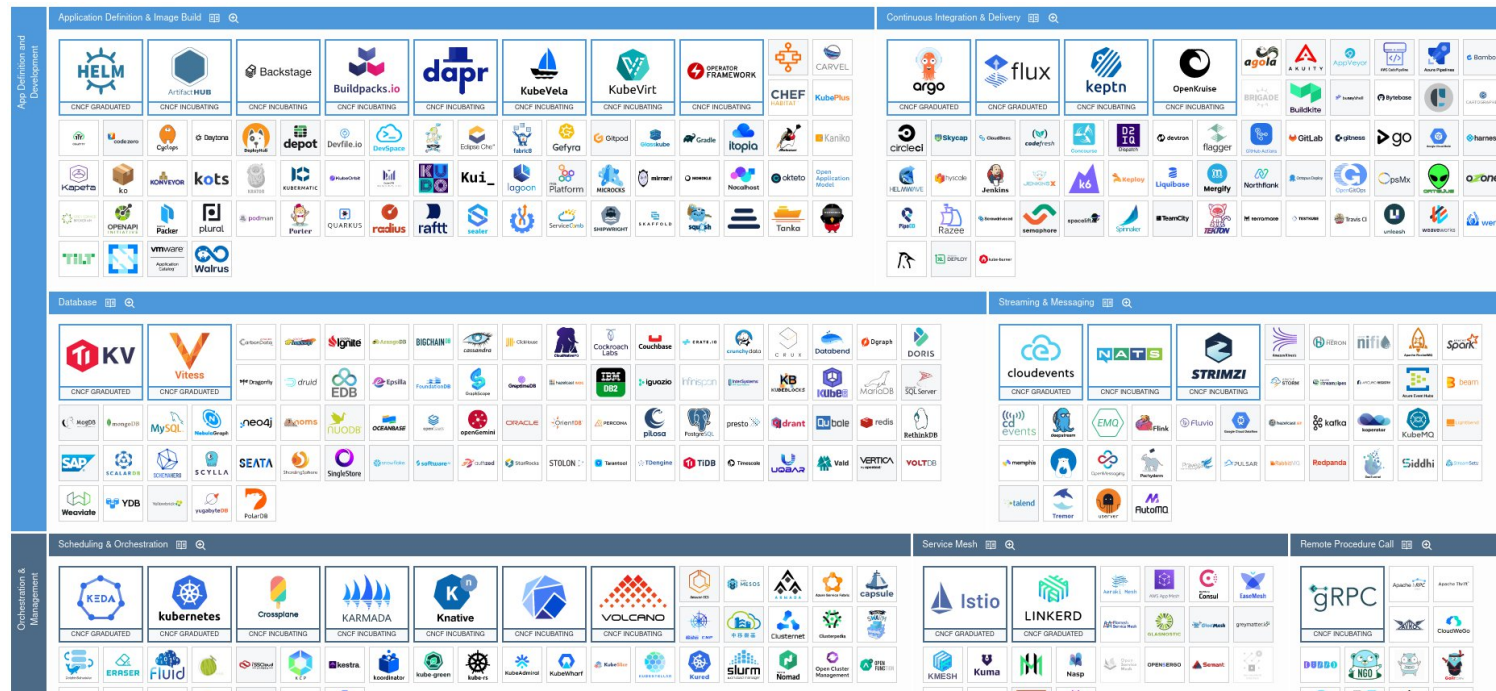
RANCHER
BY SUSE

• **Rancher** : pour déployer et maintenir les clusters K8s dans notre infrastructure de virtualisation VMware vSphere



Configuration (post-déploiement)

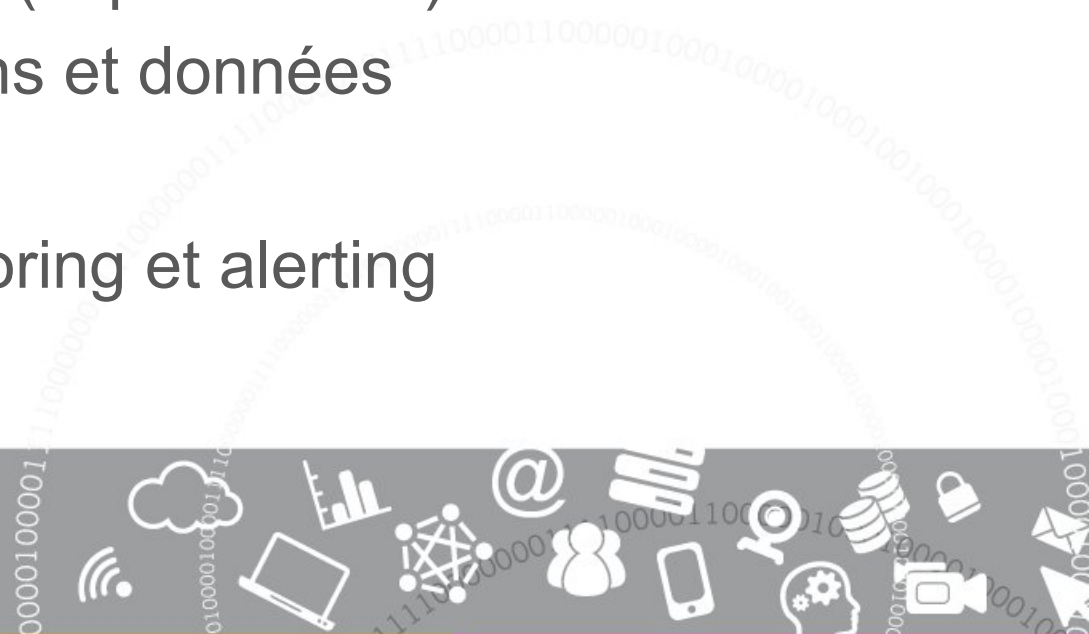
- Un cluster RKE2 est « nu » une fois déployé
- CNCF, on prend quoi ? (réseau, stockage, sauvegarde, déploiement, certificats...)



Éléments indispensables retenus



- **ArgoCD** : déploiement d'applications
- **Vault** : coffre fort de mots de passes
- **MetaLB** : annonce BGP des IPs de type LoadBalancer
- **Traefik** : proxy d'accès aux services
- **Cert-manager** : génération de certificats HTTPs
- **Ceph-CSI** : stockage persistant (cephfs et rbd)
- **Velero** : sauvegarde applications et données
- **Calico** : gestion du réseau
- **Prometheus / Grafana** : monitoring et alerting



Éléments facultatifs retenus / développés



- **External-dns** : génération d'enregistrements DNS à la volée (pédagogie)



- **UL-logs** : exposition des logs Traefik et conteneurs



Éléments de sécurité retenus



- **Neuvector** : audit, remédiation, isolation des conteneurs en cours d'exécution



- **CrowdSec** : prévention des attaques par bannissement d'IPs



- **Network-policies** : gestion d'ACLs réseau in-cluster



Éléments communs à l'infrastructure



- **Gitlab** : forge source de vérité



HARBOR

- **Harbor** : entrepôt d'images de conteneurs



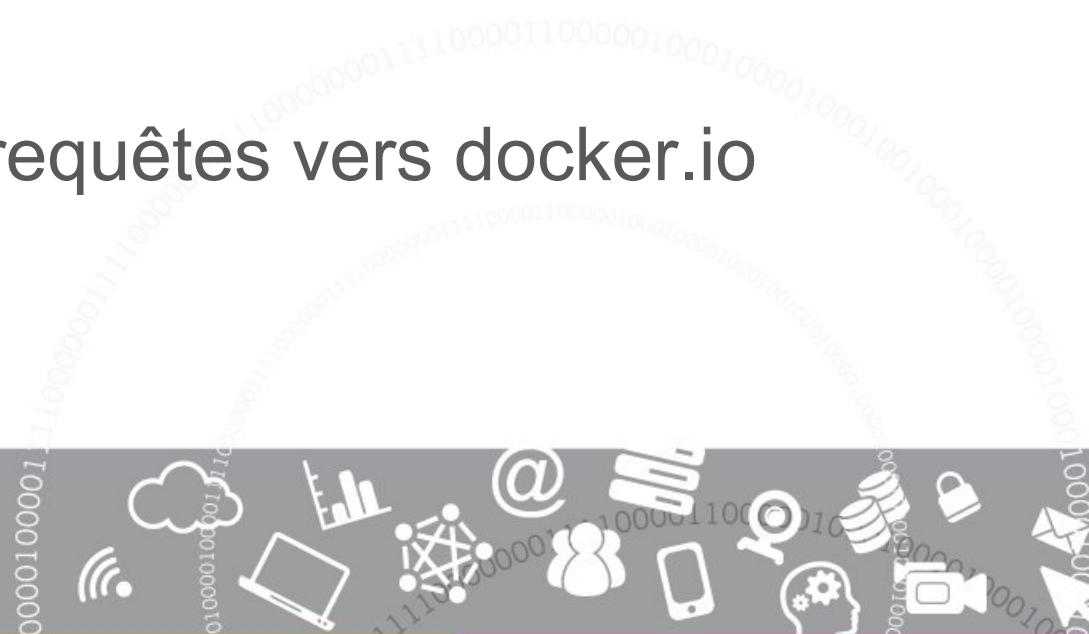
aqua
trivy

- **Trivy** : scanner de vulnérabilités des images de conteneurs

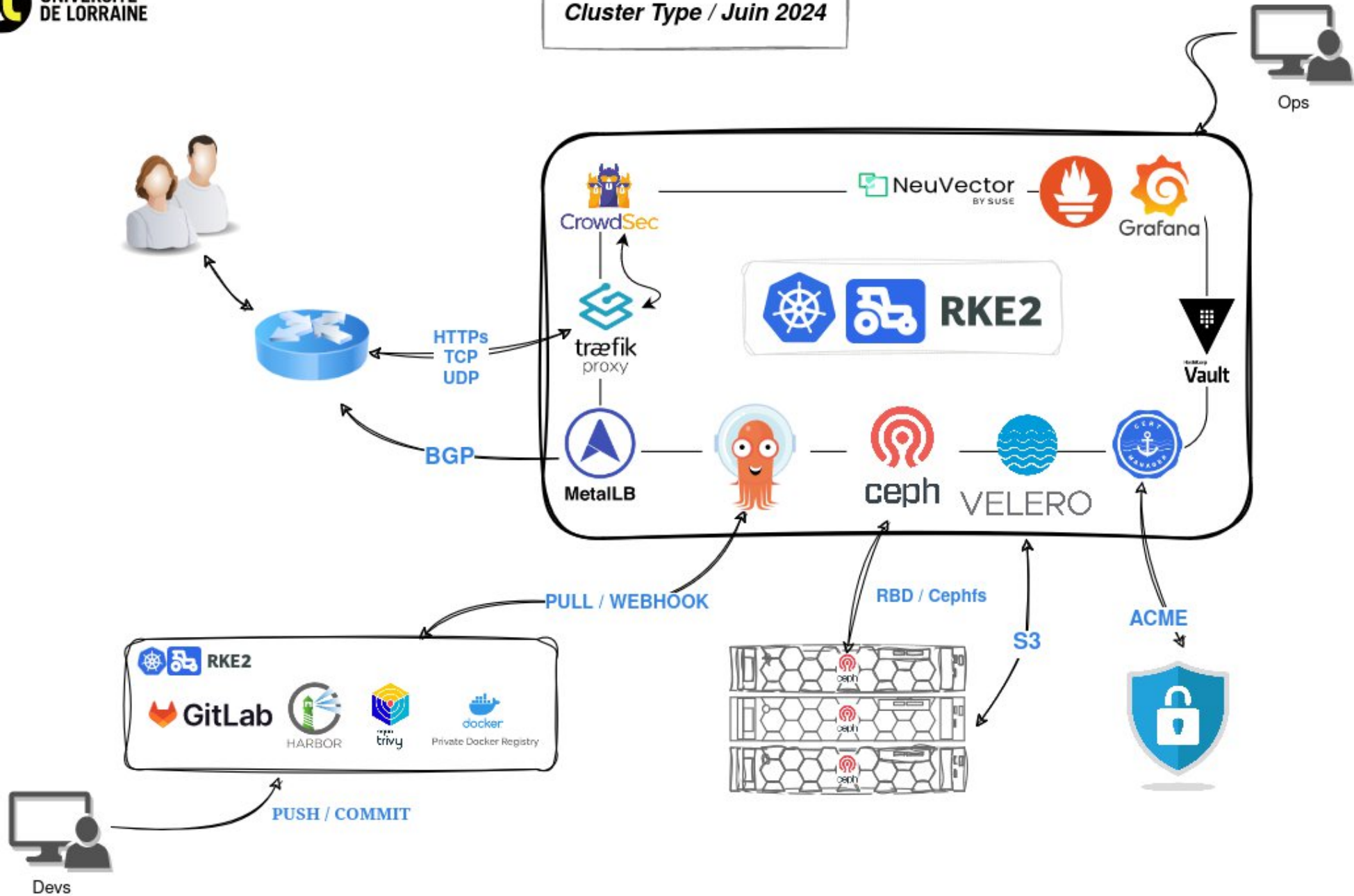


Private Docker Registry

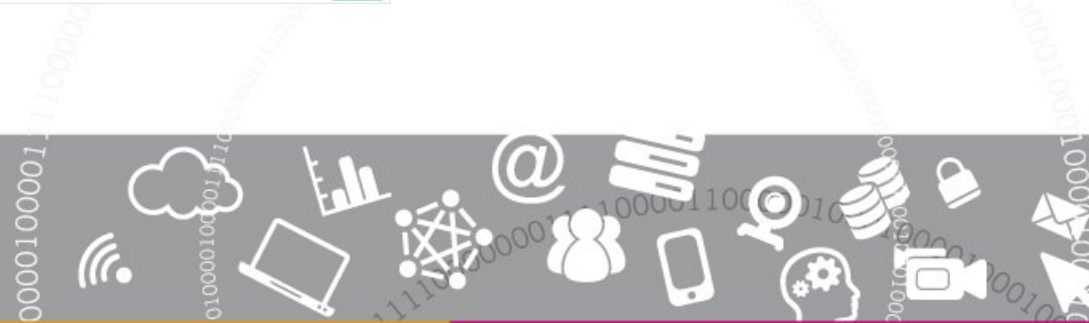
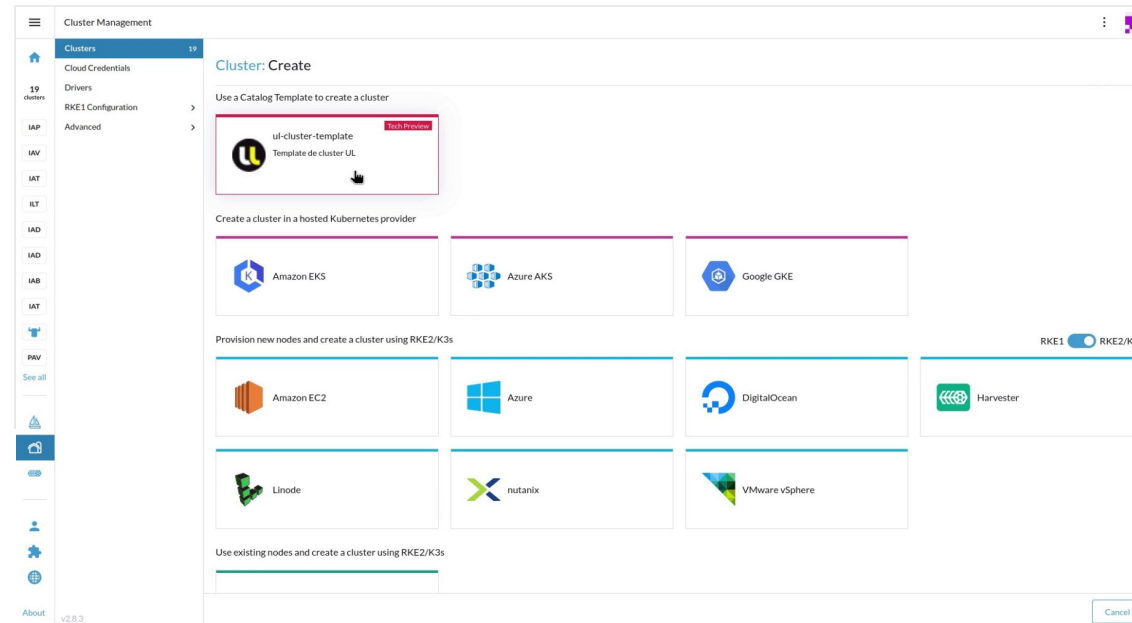
- **Docker-registry** : limiter les requêtes vers docker.io



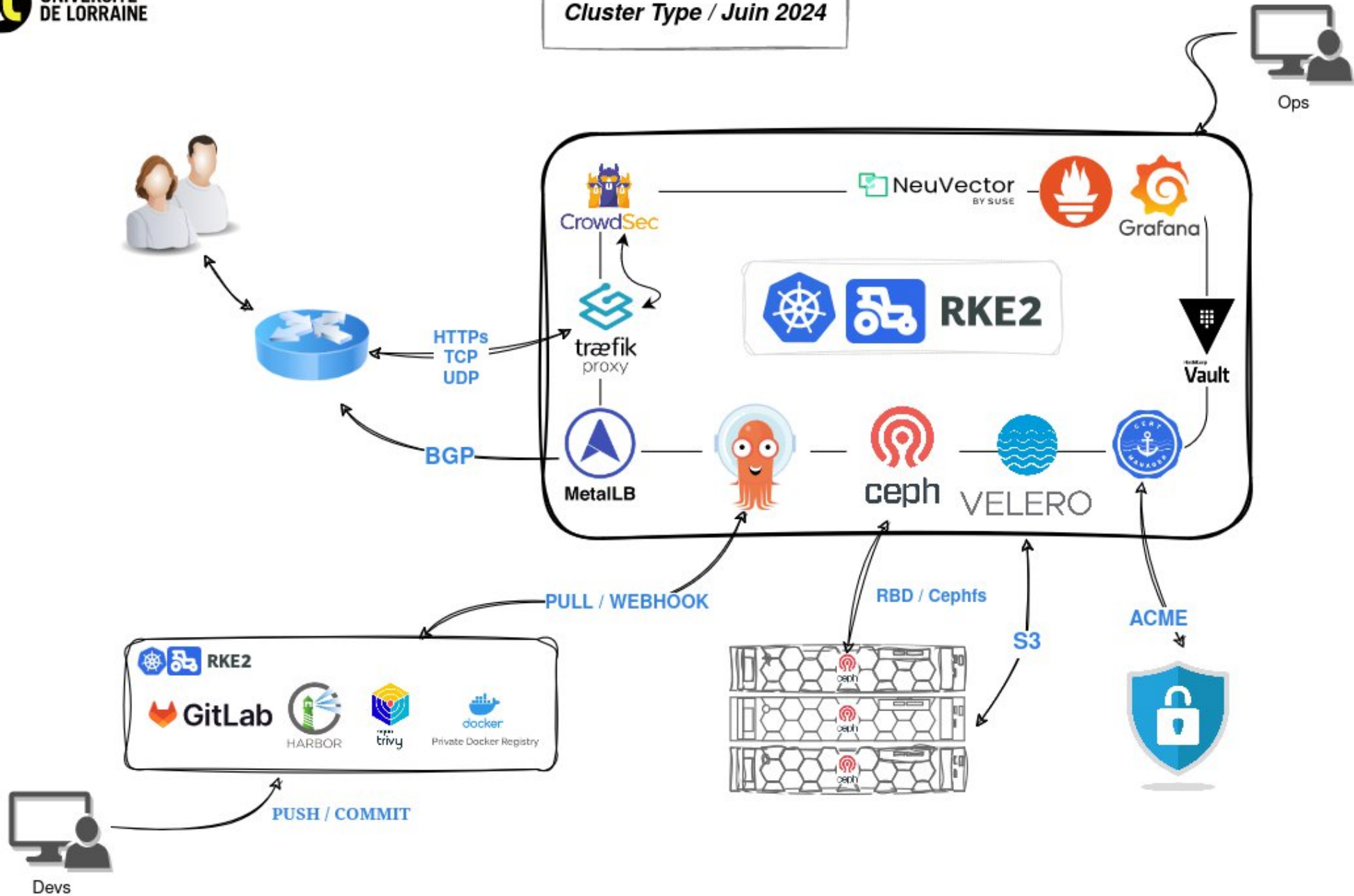
Cluster Type / Juin 2024



Déploiement d'un cluster Rancher RKE2



Cluster Type / Juin 2024

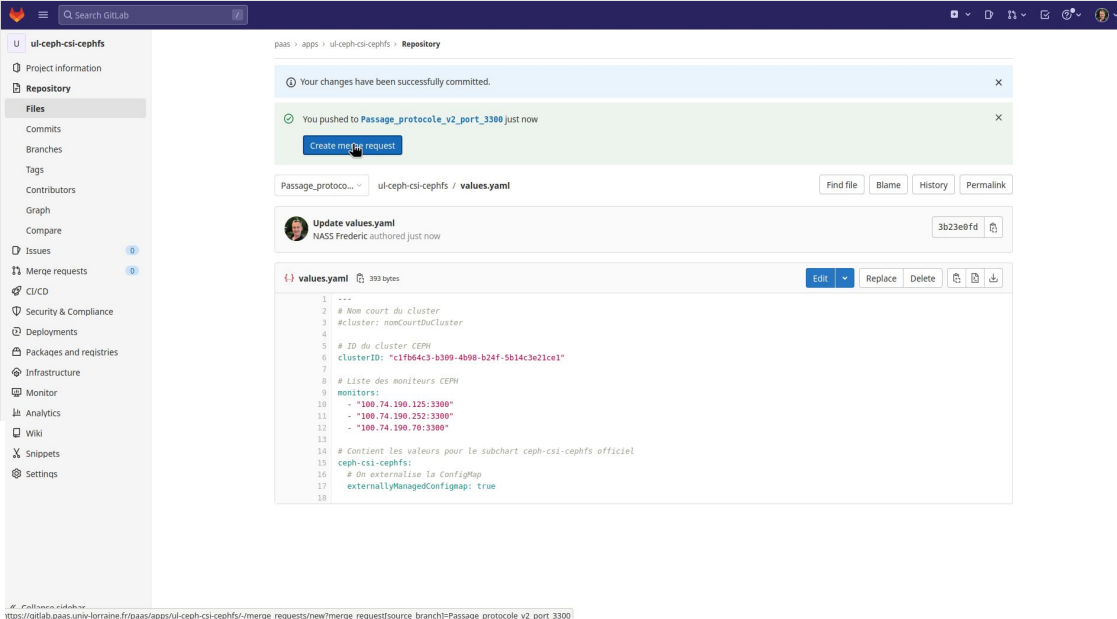


Configuration GitOps

- Nos clusters sont déployés par Rancher
- Nos clusters sont configurés par un ArgoCD central dédié à l'infrastructure PaaS qui déploie et configure leurs composants additionnels (22 possibles, 8 obligatoires)
- Chaque composant additionnel est décrit sous forme d'une application Helm sur un Gitlab dédié à l'infrastructure PaaS
- Les clusters héritent tous d'un même modèle de configuration qui peut être surchargé par cluster (composant supplémentaire ou autre version d'un composant)



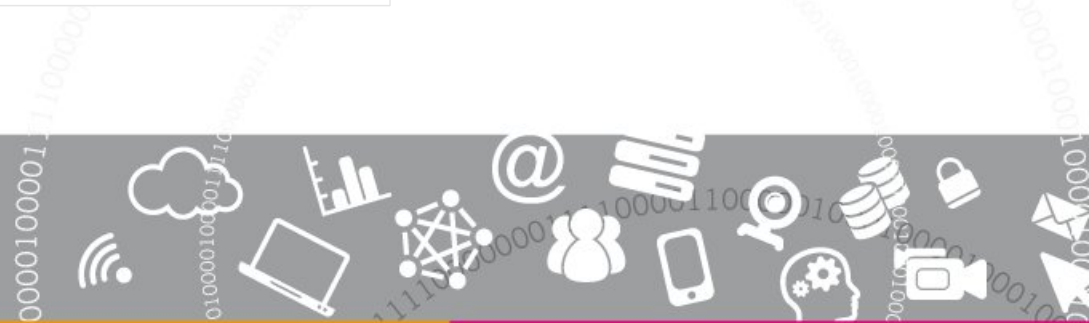
Gitops, test de version sur un cluster



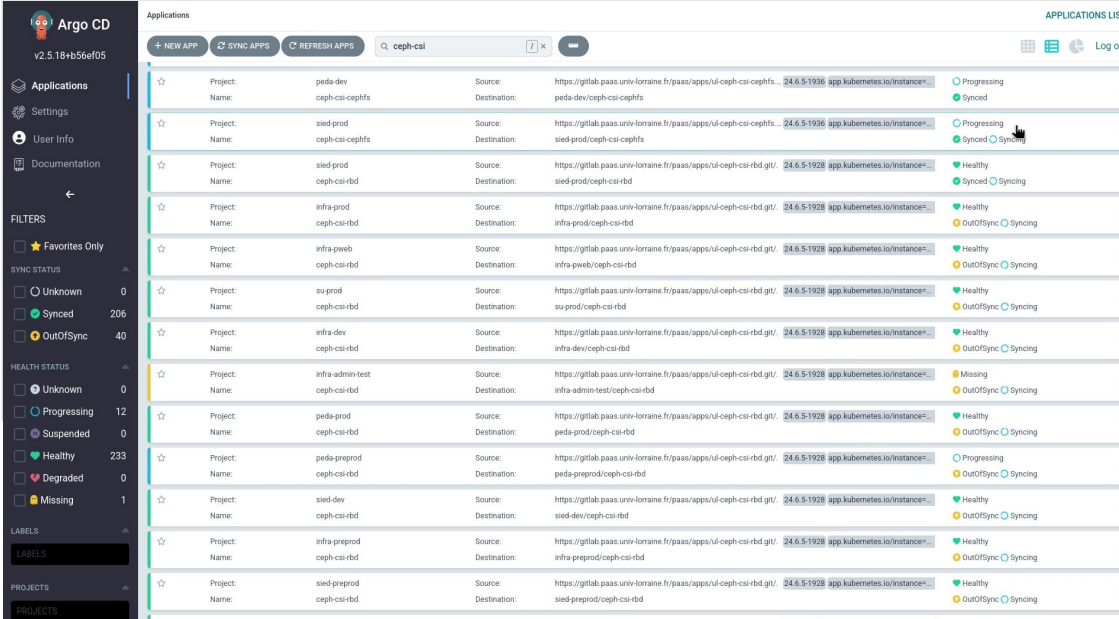
The screenshot displays the GitLab web interface for a repository named 'ul-ceph-csi-cephfs'. The main content area shows a commit titled 'Update values.yaml' by 'NASS Frederic' with commit hash '3b23e9fd'. Below the commit information, the content of the 'values.yaml' file is shown, which is a configuration file for a Ceph CSI driver. The file includes comments in French and configuration parameters for the cluster and monitors.

```
1 ---
2 # Nom court du cluster
3 #cluster: nonCourDuCluster
4
5 # ID du cluster CEPH
6 clusterID: "c1f664c3-b309-4090-b24f-5b14-3e11ce1"
7
8 # Liste des moniteurs CEPH
9 monitors:
10   - "100.74.190.125:3300"
11   - "100.74.190.252:3300"
12   - "100.74.190.70:3300"
13
14 # Contient les valeurs pour le subchart ceph-csi-cephfs officiel
15 ceph-csi-cephfs:
16   # On externalise la ConfigMap
17   externallyManagedConfigmap: true
18
```

At the bottom of the screenshot, a URL is visible: [https://gitlab.paas.univ-lorraine.fr/paas/apps/ul-ceph-csi-cephfs/-/merge_requests/new/merge_request\[source_branch\]=Passage_protocolle_v2_port_3300](https://gitlab.paas.univ-lorraine.fr/paas/apps/ul-ceph-csi-cephfs/-/merge_requests/new/merge_request[source_branch]=Passage_protocolle_v2_port_3300)



Gitops, montée de version sur tous les clusters



The screenshot displays the Argo CD web interface. On the left is a sidebar with navigation options: Applications, Settings, User Info, and Documentation. Below this are filter sections for SYNC STATUS (Unknown, Synced, OutOfSync) and HEALTH STATUS (Unknown, Progressing, Suspended, Healthy, Degraded, Missing). The main area shows a table of application instances for the 'ceph-csi' project. The table columns include Project Name, Source, Destination, and Sync/Health status. A QR code is visible on the left side of the interface.

Project Name	Source	Destination	Sync Status	Health Status
peda-dev-ceph-csi-cephfs	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-cephfs... 24.6.5-1936	app.kubernetes.io/instance-... peda-dev/ceph-csi-cephfs	Progressing Synced	Healthy
sied-prod-ceph-csi-cephfs	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-cephfs... 24.6.5-1936	app.kubernetes.io/instance-... sied-prod/ceph-csi-cephfs	Progressing Synced	Healthy
sied-prod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... sied-prod/ceph-csi-rbd	Progressing Synced	Healthy
infra-prod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... infra-prod/ceph-csi-rbd	Healthy OutOfSync	Healthy
infra-pweb-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... infra-pweb/ceph-csi-rbd	Healthy OutOfSync	Healthy
su-prod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... su-prod/ceph-csi-rbd	Healthy OutOfSync	Healthy
infra-dev-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... infra-dev/ceph-csi-rbd	Healthy OutOfSync	Healthy
infra-admin-test-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... infra-admin-test/ceph-csi-rbd	Missing OutOfSync	Missing
peda-prod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... peda-prod/ceph-csi-rbd	Healthy OutOfSync	Healthy
peda-preprod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... peda-preprod/ceph-csi-rbd	Progressing OutOfSync	Progressing
sied-dev-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... sied-dev/ceph-csi-rbd	Healthy OutOfSync	Healthy
infra-preprod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... infra-preprod/ceph-csi-rbd	Healthy OutOfSync	Healthy
sied-preprod-ceph-csi-rbd	https://gitlab.paas.univ-lorraine.fr/paas/apps/ui-ceph-csi-rbd.git/... 24.6.5-1928	app.kubernetes.io/instance-... sied-preprod/ceph-csi-rbd	Healthy OutOfSync	Healthy



Notre infrastructure

- 2 infrastructures Rancher 2.8.3 (test et production)
- Infrastructure Rancher de production :
 - 1 cluster K8s autonome hébergeant Rancher
 - 1 cluster K8s d'administration de l'infrastructure (ArgoCD Central + Gitlab PaaS + Vault + Docker Registry)
 - 17 clusters K8s :
 - 5 clusters K8s INFRA (dev, preprod, prod, ext, pweb) + 2 clusters (développement et intégration)
 - 4 clusters SIED (dev, preprod, prod, ext)
 - 3 clusters PEDDA (dev, preprod, prod)
 - 3 clusters SU (dev, preprod, prod)
- Un cluster : 3 Masters et 4 Workers, minimum 16 vCPU et 16Go RAM



Exploitation

- Opérée par 7 personnes de l'INFRA (2-3 ETP)
- Tâches courantes :
 - Montées de versions des clusters RKE2 et de Rancher (2 à 3 par an).
On opère prudemment : clusters dev et pré-prod puis clusters de production
 - Montées de versions des composants additionnels.
Le suivi est opéré par abonnement aux flux RSS Github. Chaque membre de l'équipe suit, propose et opère les mises à jour des composants qu'il gère.
 - Montées de version des images des nœuds Kubernetes : Ex. passage de CentOS 7 à Rocky 9



Évolutions envisagées

- Création, évolution et suppression des clusters en Gitops via ArgoCD
- Distribution Linux plus légère. Garden Linux ?
- Déverrouillage automatique des Vaults déployés dans les clusters
- Neuvector et CrowdSec sur tous les clusters exposés publiquement
- Observabilité et interconnexion de services in and out K8s. Traefik Mesh ? Istio / Envoy ? Cilium eBPF ?
- Usage des VolumeSnapshots CSI avec Velero. Charge sur Ceph ? Dégradation des performances des PV ?
- Partage de ressources au sein d'un même cluster



Bilan

- Quelles applications en production ?

- [Application mobile](#) de l'université
- [Application ULEP](#) (Pléiades Relation)
- [Application Numériscore](#)
- [Kapps'UL](#) (pédagogique)
- Gestionnaire de réunions BBB [Greenlight](#)
- Sites internet divers (500+ pweb)
- ESUP-Pod ([Offre SaaS ESUP](#))
- etc.

- Est-ce que le jeu en vaut la chandelle ? Absolument !

- Quels bénéfices ?

- Une nouvelle plateforme d'hébergement de sites Internet plus performante et plus évolutive
- Un développement et une mise à disposition des applications facilités
- Une solution numérique moderne pour soutenir la pédagogie
- La capacité d'instancier rapidement des applications pour des établissements extérieurs



Questions ?

Contactez l'équipe d'exploitation : paas-contact@univ-lorraine.fr

