



Journée ESUP Déploiement d'Applications

Nancy, 12 & 13 Juin 2024



&





Infrastructures de PC-Scol et usage de Kubernetes

- + PC-Scol
- + Pégase
- + L'infrastructure de PC-Scol
- + Génération 1
- + Génération 2
- + Stack NG



PC-Scol: Projet Commun de la Scolarité

- + Débuté en 2017
- + AMUE & Association Cocktail
- + Co-construction avec les établissements
- + Solution logicielle Pégase pour 120+ établissements



PÉGASE

Produit des Établissements pour la Gestion,
l'Accompagnement et le Service aux Études

- Remplace Apogée/Rof et Scholarix/SVE
- Application métier :
 - Construction de l'offre de formation
 - De l'inscription à la diplomation des apprenants, via le choix et le contrôle du cursus
 - Intégrations dans les SI établissement et partenaires ESR

DIRECTION

DIRECTEUR DE PROJET (DP) & DIRECTEUR OPÉRATIONNEL (DO)
DIRECTEUR TECHNIQUE (DT)

GOVERNANCE

INSTANCES DE PILOTAGE
CODIR
COPIL
COSUIS

ÉTABLISSEMENTS EXPERTS

MÉTIER ET TECHNIQUE
UNIVERSITÉ,
ÉCOLE,
TUTELLE, NCU, ...

INSTITUTIONS TIÈRES

PARCOURSUP,
CNOUS,ESUP, ...

PRODUCTION LOGICIELLE

EQUIPE DE TOULOUSE

1 PRODUCT OWNER 1 SCRUM / DEV
5 DÉVELOPPEURS +3 (+1) 1 TESTEUR

EQUIPE DE STRASBOURG

1 PRODUCT OWNER 1 SCRUM / DEV
5 DÉVELOPPEURS+1 (+1) 1 TESTEUR

EQUIPE DE NANTES

1 PRODUCT OWNER 1 SCRUM / DEV
4 DÉVELOPPEURS (+1) 1 Testeur

EQUIPE DE MARSEILLE

1 PRODUCT OWNER 1 SCRUM / DEV
5 DÉVELOPPEURS+1 1 TESTEUR

EQUIPE DE QUALIFICATION

3 TESTEURS AUTOMATISEURS

ARCHI TECHNIQUE, URBANISTES, DBA / RDD

1 RESPONSABLE ARCHI TECHNIQUES 1 ARCHI TECHNIQUE
1 Archi DBA / RDD, 1 Dev RDD, 1 Urbaniste, 1 urbaniste de données
1 EXPERTS TECHNIQUES (+1)

COORDINATION

PRODUCT MANAGER
RTE & PILOTE OPÉRATIONNEL
RESP SÉCURITÉ NUM & QUALITÉ

2 EXPERTS MÉTIER

AMOA

Recueil Spécifications
déploiements Accompagnement
formations

*Pôle spécification : 4 CF
*Pôle relations aux
établissements : 4 CF dont
1 coordination du pôle, 1
CF déploiement
X FORMATEURS EXTERNES

OPS

1 RESPONSABLE OPS
2 DEVOPS (+1)

**EXPLOITATION
HÉBERGEMENT, SUPPORT,
CO-ADMINISTRATION**

MULTI-LOCALISATIONS

2 DEVOPS +2 (+1)
4 SUPPORTS FONCTIONNELS

SOUTIEN

GESTION ADMINISTRATIVE
CONTRÔLE DE GESTION
COMMUNICATION
ERGONOME (PRESTATION)

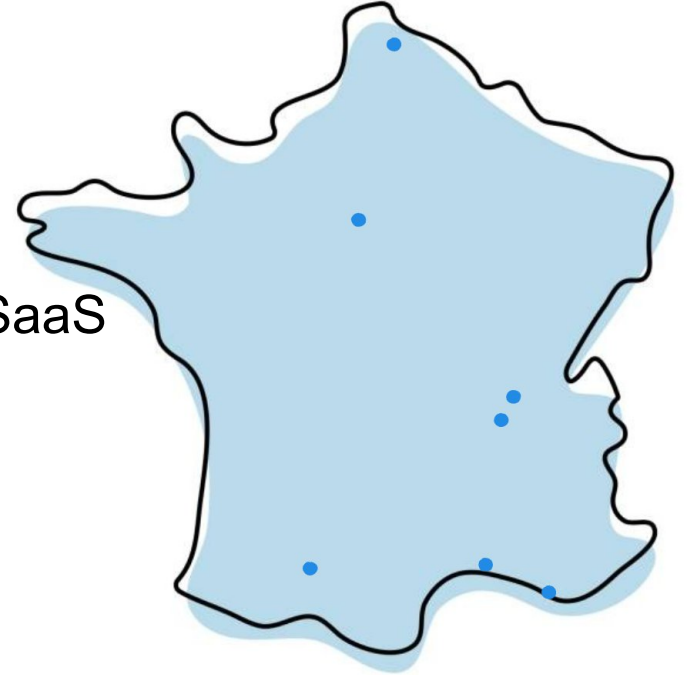
SUPPORT

SERVICES JURIDIQUE
SERVICES FINANCIER.
GESTIONNAIRES RH
RELATIONS ETABLIS.
INTERV. TECHNIQUES



L'équipe Ops

- + Outils & Services PC-Scol
- + Usine logicielle
- + Infrastructures de construction
- + Infrastructures de production SaaS
- + Pégase
- + MCO & Supervision





Pégase sous le capot

- + DDD & Architecture hexagonale
- + Application distribuée
- + API first, OpenAPIv3
- + Front, Back, Storage, MOM

- + Pégase v24
 - + 12 applications frontend (Angular)
 - + 15 services backend (Spring Boot)
 - + 9 connecteurs (Spring Boot)
 - + 1 MOM (Kafka)
 - + 15 composants & outils transverses
 - + 24 bases de données (Postgres, MongoDB)



Pégase sortie d'usine

- + Artefacts versionnés pour chaque composant :
 - + Spécifications d'API
 - + Composants applicatifs front, back
 - + Une ou plusieurs images de conteneur
 - + Un chart Helm

- + Pégase : un chart Helm "umbrella"
 - + Avec tous les composants (fronts, backs, Pg, Mg, Kafka, etc)
 - + 57 sous-charts (requirements)



PÉGASE

Cycle de vie et versions

- Une release majeure tous les 3 mois
- Releases mineures possibles
- Hotfix et bugfix relativement nombreux

158 versions différentes depuis la v1.0.0 (2020)



Infrastructures - 2018-2020, les débuts

- + DNUM Unistra
 - + IaaS OpenNebula
- + Kubernetes RKE
- + Quelques addons :
 - + Ingress Nginx Controller
 - + KubeDB
 - + Strimzi
 - + Cert-manager
 - + NFS Provisionner
 - + ...



Infrastructures - 2019, un premier bilan

- + RKE
- + Kubernetes et le modèle déclaratif
- + Majorité des addons validés
- Intégrations OpenNebula absentes
 - Pas de stockage mode bloc
 - Pas de fonctionnalités réseau

La DNUM Unistra devient hébergeur officiel de l'offre SaaS Pégase (eu-sxb-1)



Infrastructures - 2020-2024, l'hébergement SaaS

- + IaaS OpenStack
- + Stockage Ceph
 - + Mode bloc Cinder
 - + Mode objet (S3) via Object Gateway

- + Utilisation intensive de Terraform
 - + modules, sous-modules
 - + projets, sous-projets

- + Déploiement des instances via jobs Jenkins



Infrastructures - 2024, quelques chiffres

Usage	Clusters	Workers	Pégases	Pods	Postgres	Volumes
Construction	4	92	50	4 338	836	1 154
Production	9	527	415	26 164	5 498	8 216

1 Worker = 8vCPUs / 32Go RAM



Infrastructures - 2023, le bilan

- + Un IaaS pilotable et performant
 - + Terraform
 - + Intégration Kubernetes
 - + Load balancing
 - + Volumes
 - + Maturité de Kubernetes et son éco-système
- Deuxième hébergeur :
Université Clermont Auvergne (fr-cfe-uca)
- Modèle Terraform complexe
 - Rancher/RKE
 - Cluster polyvalent
 - Montées de version complexes
 - Surconsommation de ressources
 - Addons :
 - Obsolescence
 - Changement de licence
 - Croissance de Pégase
 - De plus en plus de secrets



Infrastructures - Stack NG, les principes

+ **Sécurité**

- + Distribution : Siderolabs Talos
- + Coffre fort : Hashicorp Vault
- + Diversification des clusters

+ **Performances & Économies**

- + Création de services : DBaaS, KaaS
- + Recentrage des releases Pégase sur ses composants applicatifs

+ **Accélérer**

- + Minimum de Terraform
- + Code d'infrastructure global (hébergeurs/régions, projets/usage, AZ)
- + Déploiement Pégase auto-portant et jetable
- + Déploiement continu ArgoCD

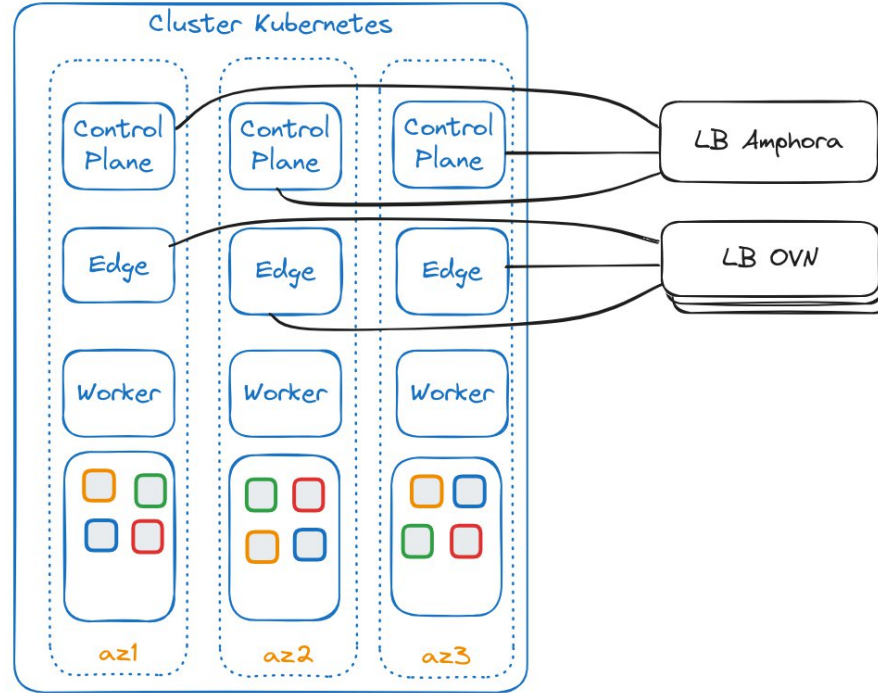


Infrastructures - Stack NG, Talos

- + OS minimal sécurisé
 - + Pas de shell ni d'accès SSH
 - + Root FS en lecture seule
 - + Expose une API dédiée à l'administration
- + Kubernetes Vanilla minimal
- + Releases alignées sur Kubernetes
- + Montées de version facilitées
 - + OS et Kubernetes

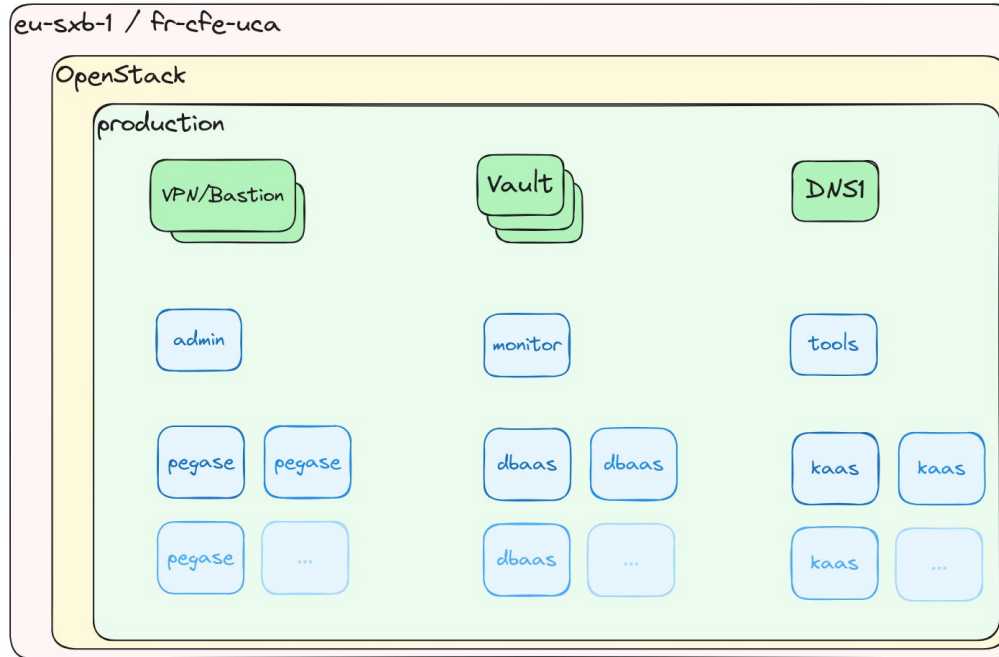
- + Évalué depuis v1.3 (Janvier 2023)
 - + Techniquement : RaS
 - + Développeurs réactifs et accessibles
 - + Communauté en croissance







Infrastructures - Stack NG, big picture





Infrastructures - Stack NG, ArgoCD

- + Outil de déploiement automatisé GitOps
- + Sécurité auditée
- + Full GitOps
- + Prise en charge de Helm, Kustomize
- + Extensible par plugins
 - + ArgoCD Vault Plugin
- + ApplicationSet
- + Dashboard pour les Ops et les Devs
- + Forte communauté

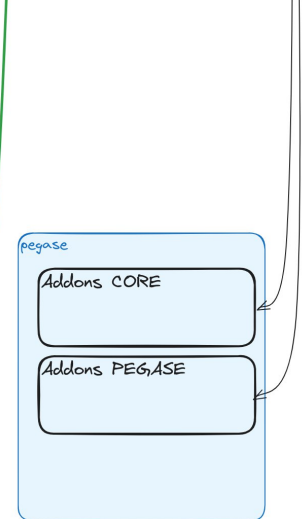
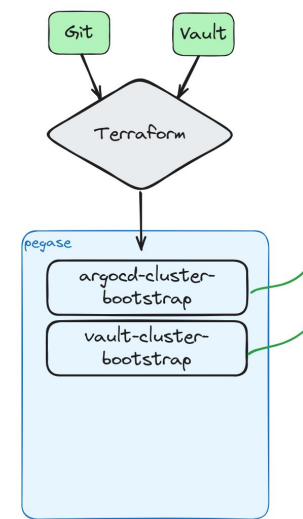
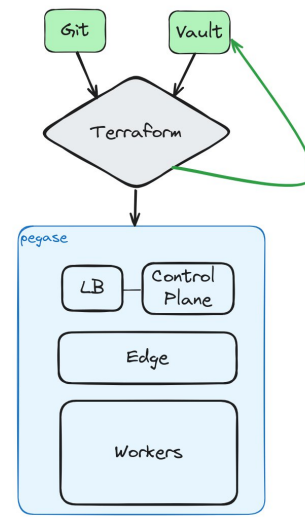
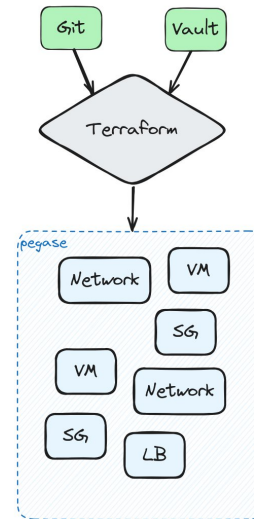
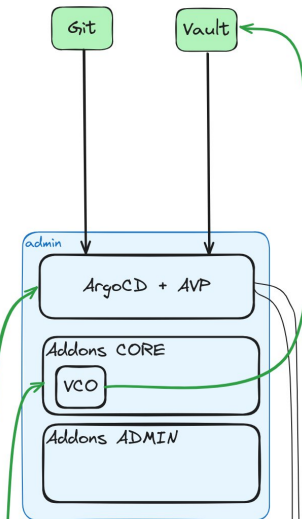
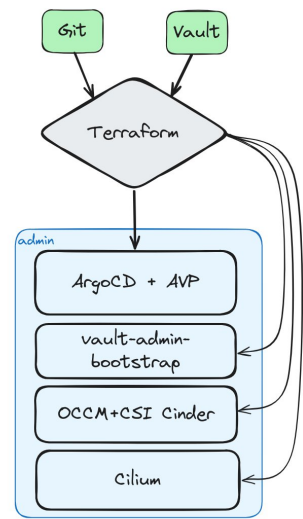
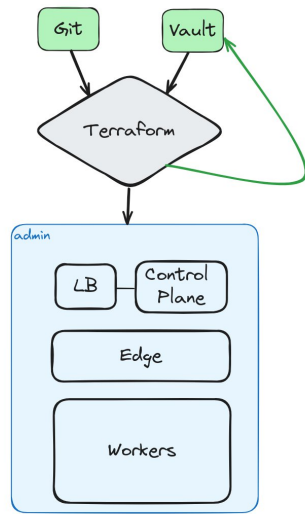
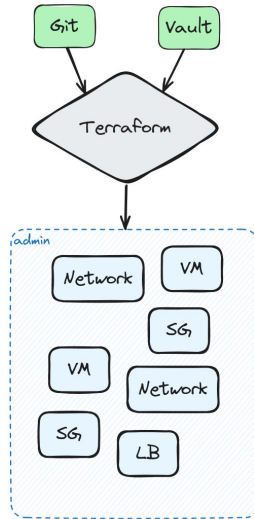




Infrastructures - Stack NG, ArgoCD à PC-Scol

- + ArgoCD sur un cluster admin unique, dédié
- + Clusters enregistrés dans ArgoCD avec labels
- + Clusters Addons
 - + Regroupés dans des app-of-apps par type de cluster
 - + ApplicationSet sur cluster generator et cluster labels
 - + Dépôt Git unique commun aux différentes régions et usages
 - eu-sxb-1
 - fr-cfe-uca
 - sandbox
 - construction
 - production
- + Instances Pégase (WIP)
 - + App-of-apps par type d'instance
 - + ApplicationSet sur Git/JSON generator : Inventaire des instances
 - + Application multi-source : charts Pégase + Values spécifiques







Infrastructures - Stack NG, Vault

- + Coffre fort devenu standard de l'industrie
- + Réputé pour sa sécurité et sa qualité
- + Auditable
- + Support de multiples
 - + Authentication methods
 - + Secret Engines
- + Multiples intégrations
 - + Terraform
 - + ArgoCD
 - + Kubernetes
 - + Spring Boot
 - + Pégase
 - + Teller





Infrastructures - Stack NG, Vault à PC-Scol

- + Un cluster à 3 noeuds sur chaque région
- + Recopie toutes les 30min

Doit être l'unique stockage des secrets :

- + Intégralité des secrets d'infrastructures
- + Secrets des instances Pégase
- + Secrets des bases de données

En gardant une segmentation et gestion des droits fortes, à l'échelle !





Infrastructures - Stack NG, Vault à PC-Scol

Vault Config Operator

Gestion déclarative des ressources Vault :

- Roles
- Policies
- Authentication Engine
- Secret Engine
- ...





Infrastructures - Stack NG, Vault à PC-Scol

Ressources déployées avec les clusters :

- + Password Policies
 - + Postgres
 - + MongoDB
- + Rôles par type de composants
- + Politiques génériques avec modèles de chemins d'ACL
- + Kubernetes Authentication Engine par cluster



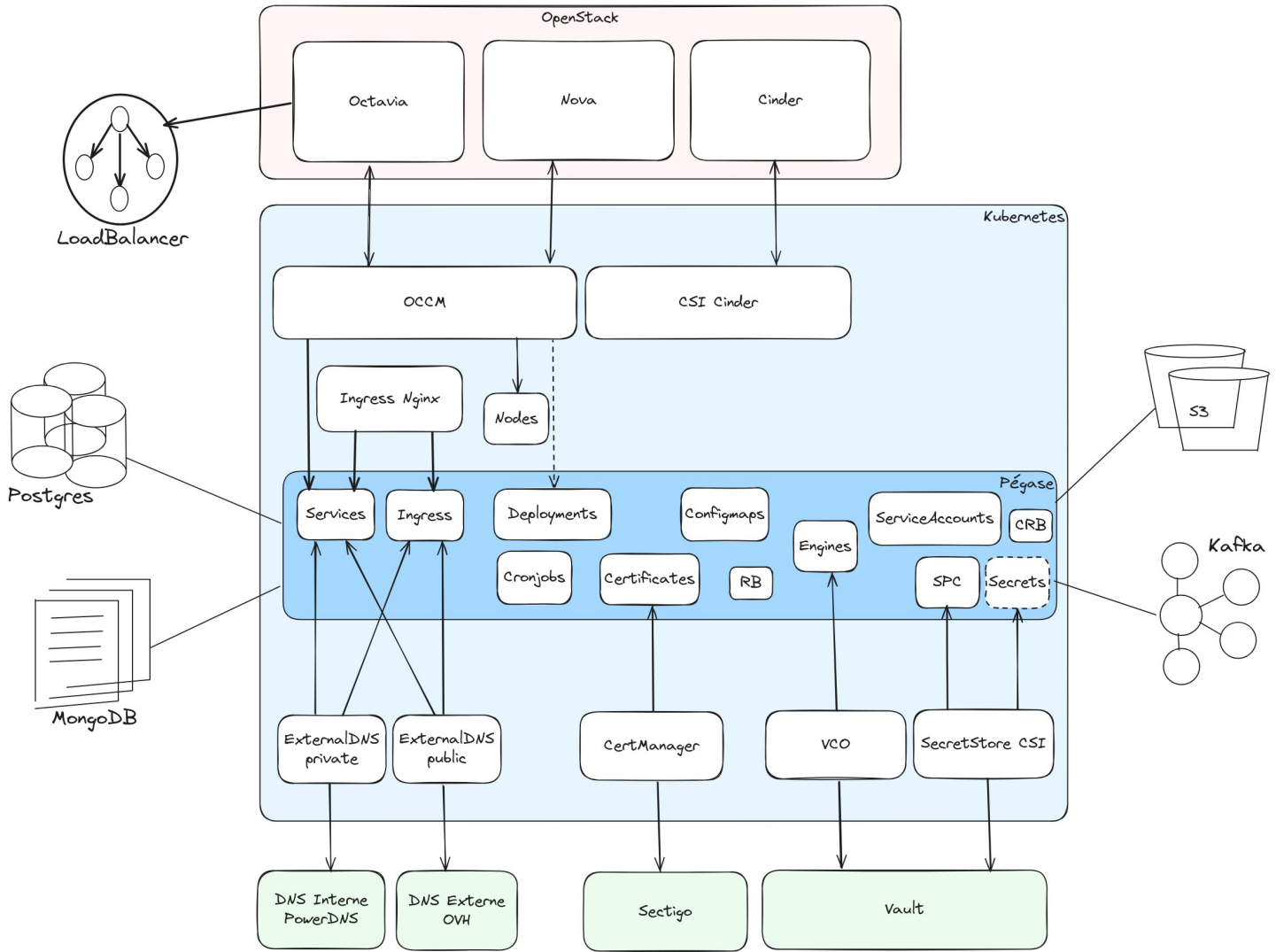


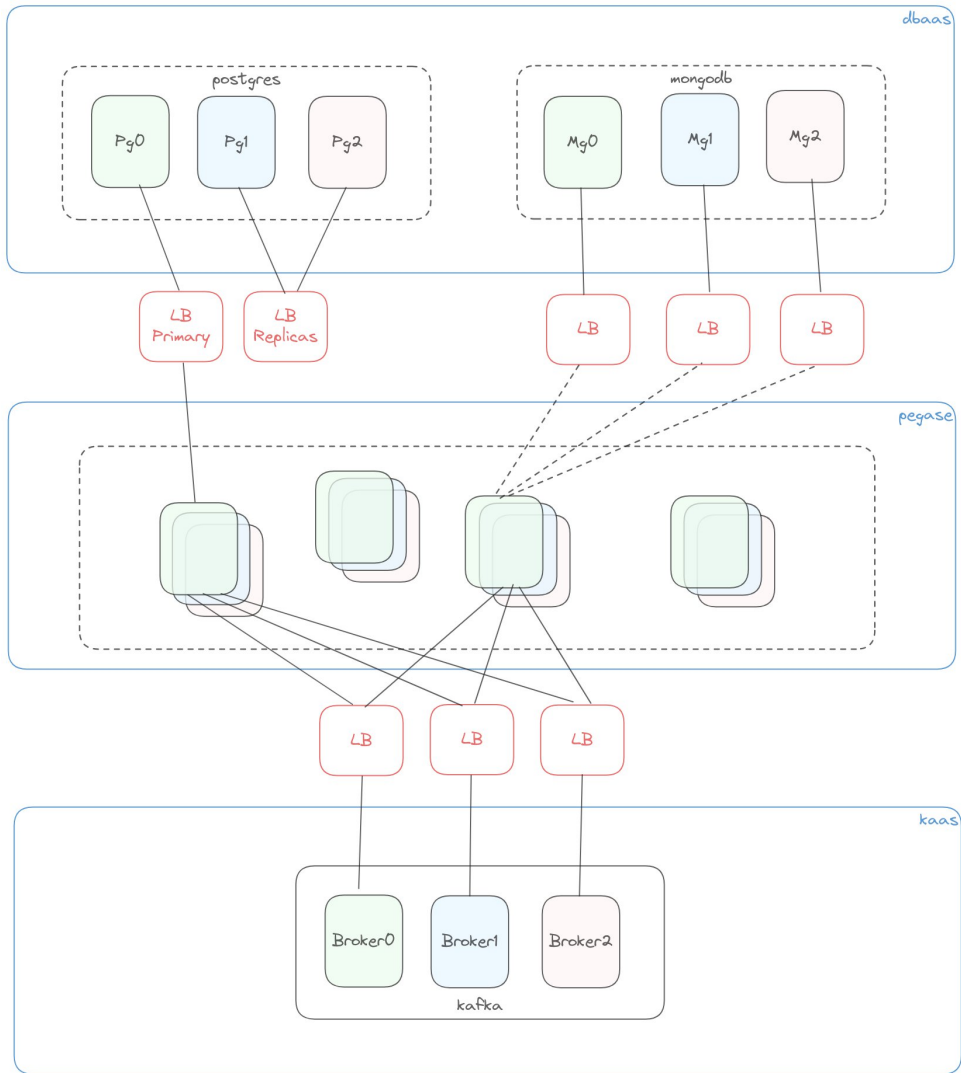
Infrastructures - Stack NG, Vault à PC-Scol

Ressources déployées avec Pégase :

- + Secret Engines dédiés à chaque instance Pégase
 - + KV Engine
 - + Database Engine
 - + 2 connexions : Postgres & MongoDB
 - + DatabaseStaticRole : owner, rw
 - + Database(Dynamic)Role : ro
- + Chaque composant s'identifie avec un serviceAccount unique et un rôle générique









Infrastructures - Stack NG, dans le futur

- + Migration de toutes les instances Pégase établissements
- + Définir un workflow de développement avec ArgoCD
- + Kafka NG
- + Sécurité
- + PRA/PCA entre nos 2 régions
- + Plus performant & économe en ressources



Merci
de votre attention !



&





Infrastructures - Stack NG, addons CORE

Addons	Rôle
Cilium	Container Network Interface
OpenStack Cloud Controller Manager	Intégration Nova (Compute) Octavia (LB)
CSI Cinder	Intégration Cinder (Volume)
Metrics Server	Métriques des noeuds et pods
Kube Prometheus Stack	Moissonnage et stockage des métriques
Promtail	Shipper de logs
Secret Store CSI	Driver pour présenter des secrets (Vault) sous forme de volume CSI
Vault CSI Driver	Driver Vault pour Secret Store CSI
Cert Manager	Gestion de certificats (connecté à Sectigo)
Ingress Nginx	Gestion des ingress (ingressClass=private)
External DNS	Gestion des enregistrements DNS privés



Infrastructures - Stack NG, addons ADMIN, MONITOR

Addons	Rôle
ArgoCD	Déploiement GitOps
Vault Config Operator	Gestion de ressources Vault

Addons	Rôle
Kube Prometheus Stack	Moissonnage et stockage des métriques, Grafana
Thanos	Gestion consolidée des métriques
Loki	Gestion consolidées des logs



Infrastructures - Stack NG, addons PEGASE

Addons	Rôle
Vault Config Operator	Gestion des ressources Vault livrées par Pégase
Reloader	Contrôleur pour le redémarrage automatique de pods
Ingress Nginx	Gestion des ingress (ingresClass=public)
External DNS	Gestion des enregistrements DNS publiques



Infrastructures - Stack NG, addons DBAAS, KAAS

Addons	Rôle
Zalando Postgres Operator	Gestion des clusters Postgres

Addons	Rôle
Strimzi Kafka Operator	Gestion des clusters Kafka