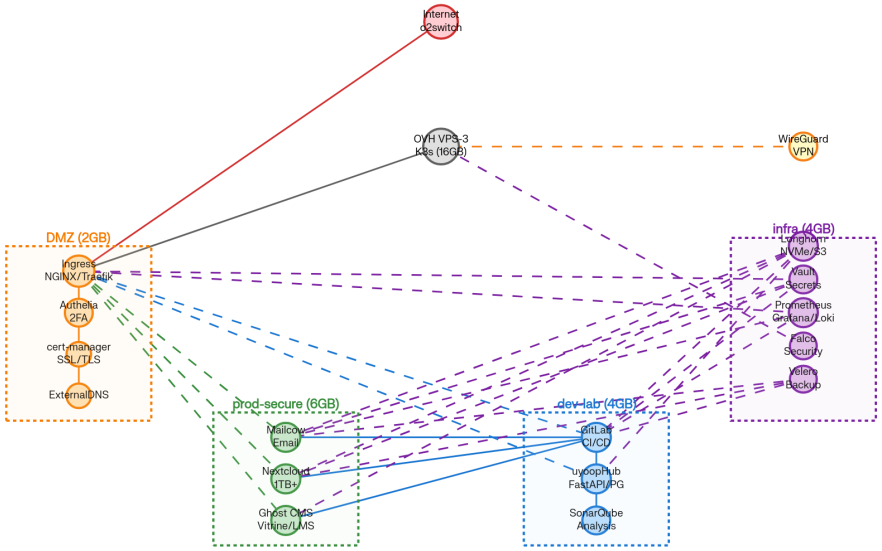
Dossier Projet UYOOP

DOSSIER PROJET : INFRASTRUCTURE SOUVERAINE UYOOP



Logo Uyoop

"Une stratégie à votre image."

Architecture DevSecOps à l'image de vos exigences.

PROJET DE TITRE RNCP 36061 (Niveau 6)
Administrateur Systèmes DevOps

Auteur : Christopher JENKINS
Date : Février 2026
Version : 3.0 (Validée V1 - FinOps & IaC Ready)

SOMMAIRE EXÉCUTIF

Ce dossier présente la refonte complète de l'infrastructure numérique **uyoop**.
Du statut de consommateur de services SaaS dispersés, nous passons à celui d'architecte d'une plateforme souveraine, sécurisée et pilotée par le code (**Infrastructure as Code**).

Ce projet, mené en parallèle des missions de stage, sert de terrain d'application réel aux compétences visées par le titre **Administrateur Systèmes DevOps** : 1. **Concevoir** une architecture sécurisée (Zero-Trust). 2. **Mettre en œuvre** une chaîne CI/CD complète (GitLab). 3. **Superviser et Maintenir** en condition opérationnelle. 4. **Intégrer** les nouveaux paradigmes (IA & FinOps).

PLAN DU DOSSIER

00. CADRE & INSTRUCTIONS

1. Contexte du Projet

La migration **uyoopVPS** n'est pas une simple opération technique. C'est un projet structurant réalisé durant la période de stage (Fév-Mai 2026). Il démontre la capacité du candidat à gérer un projet d'infrastructure complet ("Side Project" professionnel) tout en assurant ses missions quotidiennes en entreprise.

2. Environnement Technique

- **Poste de Travail** : Debian 13 (Labo Perso) & Environnement Enterprise.
- **Cloud Provider** : OVHcloud (France).
- **Philosophie** : "Zero-Trust", "Infrastructure as Code", "Souveraineté des Données".

01. ARCHITECTURE TECHNIQUE

> **Cible** : Infrastructure Souveraine, DevSecOps, support Titre RNCP (Juin 2026). **Statut** : Validé V1 (Février 2026)

1. Vision Technique & Slogan

uyoop : “Une stratégie à votre image”

En DevSecOps, “votre image” n’est pas seulement graphique, c’est votre empreinte numérique (Docker Images, System Images). Notre stratégie est de rendre cette image **souveraine, sécurisée et immuable**. Nous passons d’une consommation passive de services (SaaS) à une **Infrastructure as Code (IaC)** où chaque configuration reflète exactement les besoins métier, sans compromis sur la sécurité.

2. Infrastructure Physique (Topologie Distribuée)

Pour garantir la sécurité (isolation) et la performance (IA), l’architecture repose sur deux nœuds interconnectés (Cluster Hybride).

Node A : “CORE-PROD” (Opérationnel Février)

- **Infrastructure** : OVH **VPS-3** (8 vCores / 24 Go RAM / 200 Go NVMe).
- **Rôle** : Hébergement des services critiques “Business”.
- **Charge** : Stable, haute disponibilité requise.
- **Services** : Mailcow (Mail), Nextcloud (Data), GitLab (Code), Authelia (Secu).

Node B : “AI-LAB” (Extension Phase 2 - Avril)

- **Infrastructure** : OVH **VPS-2** (4 vCores / 8-12 Go RAM).
- **Rôle** : R&D, Intelligence Artificielle, Analyse de Code.
- **Charge** : Variable (Burstable), traitements lourds.
- **Services** : LLM Local ou Gateway API, SonarQube (Quality Gate), Perplexica (Search).

> **Liaison** : Tunnel WireGuard privé (Mesh) pour sécuriser les flux inter-nœuds sans exposition publique.

3. La “Golden Stack” Technologique

A. Orchestration & Système (Infrastructure as Code)

Toute l’infrastructure est définie par le code (GitOps). * **OS** : Debian 12 (Bookworm) durci. * **Provisioning** : **Ansible** (Configuration Management) pour l’initialisation des nœuds et la sécurité. * **Orchestrateur** : **K3s** (Lightweight Kubernetes). * *Architecture* : Multi-node capable (Server + Agent). * **Ingress** : **Traefik** Cloud Native Router. * **Certificats** : **Cert-Manager** (ACME Let’s Encrypt). * **Maintenance** : **Renovate Bot** (Mises à jour automatiques des dépendances).

B. Matrice des Services Applicatifs

Service	Rôle	Namespace K8s	Stockage
Mailcow	Serveur Mail Complet (Postfix/ Dovecot)	`prod-mail`	NVMe
Nextcloud	Hub Collaboratif (Fichiers, Cal, Contacts)	`prod-cloud`	Mixte (Cache NVMe / Data S3)
GitLab CE	Forge Logicielle & CI/CD	`devops-factory`	NVMe (Repo) + S3 (Artifacts)
Ghost	CMS Vitrine & LMS	`prod-web`	NVMe
Authelia	Fournisseur d’Identité (SSO, OIDC, 2FA)	`security`	Redis (Session)

C. Sécurité “Defense-In-Depth”

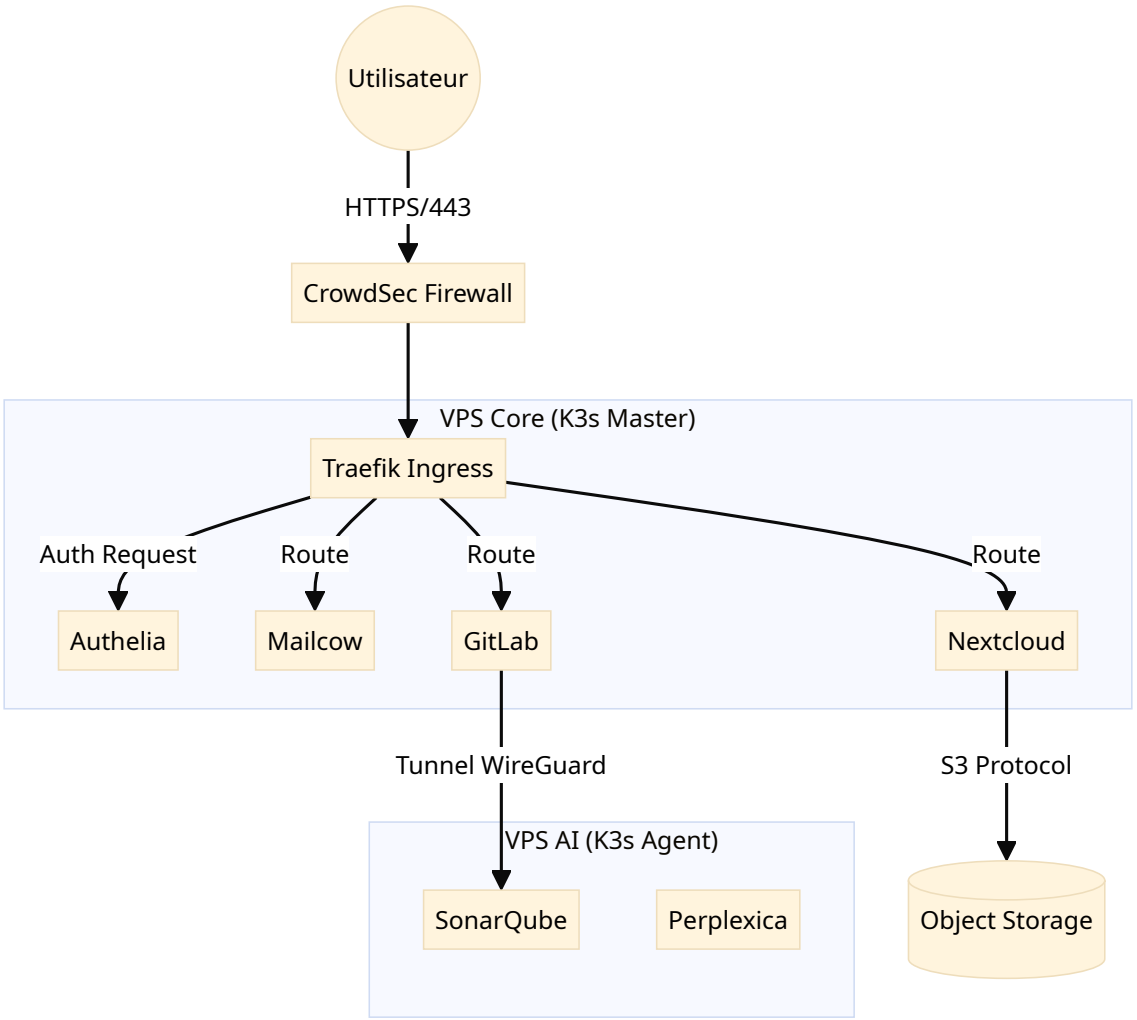
1. **Périmètre Collaboratif** : **CrowdSec** (remplace Fail2Ban) pour une détection d’intrusions basée sur la réputation IP communautaire.
2. **Identité Zero-Trust** : Portail unique (SSO Authelia) pour toutes les WebUIs. Pas d’accès direct sauf exception documentée.
3. **Application** : Scans de vulnérabilités (Trivy) et analyse statique (SonarQube) intégrés aux pipelines CI/CD.
4. **Réseau** : `NetworkPolicies` Kubernetes interdisant le trafic `dev` -> `prod`.

4. Stratégie de Données (Stockage Hybride & Immuable)

Pour optimiser les coûts et la performance des disques NVMe limités :

- **Tier 1 (Performance)** : Base de données, Code source, Emails récents (< 90 jours).
  - *Support* : NVMe Local (VPS).
- **Tier 2 (Capacité)** : Drive personnel, Archives mails, Artifacts CI/CD.
  - *Support* : **Object Storage S3** (Scalable à l'infini).
- **Stratégie Backup** : Règle du **3-2-1** renforcée.
  - Snapshots locaux (Longhorn/LVM).
  - Backup S3 chiffré (Restic/Velero) avec **Object Lock** (Immuabilité Ransomware).
  - Copie froide (Disque dur local Admin).
  - **Test DRP** : Exercice biannuel de restauration complète.

5. Flux Réseaux Critiques



02. PLANNING DE MIGRATION

> **Statut** : Validé V1 (Février 2026) **Stratégie** : “Continuité d’abord, Code ensuite”. **Contexte de Travail** : Projet mené en parallèle du stage. Charge de travail adaptée.

🔥 PHASE 1 : “OPÉRATION SOCLE” (Immédiat - 22 Février)

Objectif Critique : Continuité de service Mail/Data avant expiration contrats. **Plan B (Secours)** : Si retard technique au 20/02, activation d’un mois de **Proton Unlimited** (12.99€) pour sécuriser les données sans pression.

Semaine 06 (Infrastructure as Code Init)

- [ ] **Repo** : `git init` et structure du dépôt (Dossiers `ansible`, `k8s-manifests`, `docs`).
- [ ] **Souscription** : Commande VPS Core-Prod (OVH) et domaines.
- [ ] **Provisioning** : Création des rôles **Ansible** de base (`common`, `security`, `docker`).
  - *Sécurité* : Installation auto de **CrowdSec** + SSH Hardening.

Semaine 07 (Services Vitaux)

- [ ] **Cluster** : Déploiement K3s via Ansible (Rôle `k3s-ansible`).
- [ ] **Mail** : Déploiement Mailcow (Stack Docker).
  - *Test* : Validation Score SpamCheck (SPF/DKIM/DMARC).
- [ ] **Data** : Déploiement Nextcloud.
  - *Migration* : Upload manuel des 24 Go critiques.
- [ ] **Bascule** : Changement DNS MX `cjenti.com` (Target : 21/02).

🛠️ PHASE 2 : “L’USINE LOGICIELLE” (Mars - Avril)

Objectif Titre : Industrialisation et Sécurité (DevSecOps).

Mars : Identité & Web

- [ ] **Migration Web** : Transfert domaines O2Switch -> OVH.
- [ ] **SSO** : Déploiement **Authelia** (LDAP Mailcow backend).
- [ ] **CMS** : Ghost Blog paramétré avec accès SSO.
- [ ] **Maintenance** : Activation de **Renovate Bot** pour suivi des mises à jour.

Avril : IA & Qualité (Extension “AI-Lab”)

- [ ] **Infra** : Provisioning VPS-2 (Ansible Playbook réutilisé).
- [ ] **Réseau** : Configuration Tunnel WireGuard Mesh entre les nœuds.
- [ ] **CI/CD** : GitLab installé et runners configurés sur Node B.
- [ ] **Qualité** : SonarQube avec Quality Gate stricte.

🚀 PHASE 3 : “CONSOLIDATION & RÉSILIENCE” (Mai - Juin)

Objectif Certification : Preuves de robustesse et Documentation finale.

Mai : Big Data & FinOps

- [ ] **Storage** : Activation S3 Object Storage et règles de cycle de vie.
- [ ] **Archivage** : Migration OneDrive -> S3 (Rclone).
- [ ] **Observabilité** : Dashboard Grafana “FinOps” (Coûts OVH API).

Juin : Soutenance & DRP

- [ ] **Crash Test (DRP)** : “Journée du Chaos”.
  - *Scénario* : Suppression volontaire du namespace `prod` et restauration depuis Backup S3.
  - *Preuve* : Vidéo du rétablissement pour la soutenance.
- [ ] **Livrable** : Repo Git nettoyé et public (ou accès Jury).

Calendrier des Risques & Mitigations

Échéance	Risque Identifié	Impact	Plan de Mitigation
21 Février	Migration Mail inachevée	Perte de mails entrants	Activation **Proton Mensuel ($12.99)** (Buffer).

Échéance	Risque Identifié	Impact	Plan de Mitigation
15 Mars	Transerts Domaines bloqués	Coupure Web	Vérification codes EPP à J-30.
Mai	Crash Disque VPS	Perte Données	Backups S3 quotidiens + Test de restauration (DRP).
Soutenance	Panne “Effet Démo”	Échec Présentation	Environnement de secours ou Vidéo enregistrée.

03. ANALYSE FINOPS

> **Statut** : Validé V1 (Février 2026) **Approche** : Rationalisation des coûts par la maîtrise technologique. Passage d'un modèle OPEX SaaS (pay-per-user) à un modèle IaaS (pay-per-resource).

1. Situation Initiale (2025 - Legacy)

Coûts dispersés, dépendance forte aux éditeurs, aucun contrôle sur la localisation précise des données.

Fournisseur	Services Fournis	Coût Annuel HT	Mensuel TTC (Est.)
Proton	Mail, VPN, Drive (Suisse)	119.88 €	~12.00 €
Microsoft	Office 365, Exchange (US/EU)	66.24 €	~6.62 €
O2Switch	Hébergement mutualisé (France)	84.00 €	~8.40 €
Registrars	Portfolio Noms de domaine	125.00 €	~12.50 €
TOTAL		**395.12 € HT**	**~39.52 € TTC**

2. Infrastructure Cible (2026 - Souveraine)

Basée sur OVHcloud (Roubaix/Gravelines), facturation prévisible et évolutive.

Coûts Fixes (Infrastructure)

Ressource	Rôle	Coût Mensuel TTC	Note
VPS-3	Nœud Core (Prod)	14.28 €	Base 2026 stable
Domaines	Identité Numérique	~10.00 €	Centralisés OVH
TOTAL IaaS		**~24.28 €**	Socle de base

Coûts Variables & Options (Flexibilité)

Ressource	Type	Coût	Stratégie
VPS-2 (IA)	R&D	~7.20 € / mois	*Optimisation* : Facturation horaire (Cloud) possible durant tests.
S3 Buffer	Backup	~3.00 € / mois	Stockage froid chiffré.
Risque Proton	Assurance	12.99 € / mois	**Plan B** : Abonnement mensuel si migration retardée (Budget “Sérénité”).

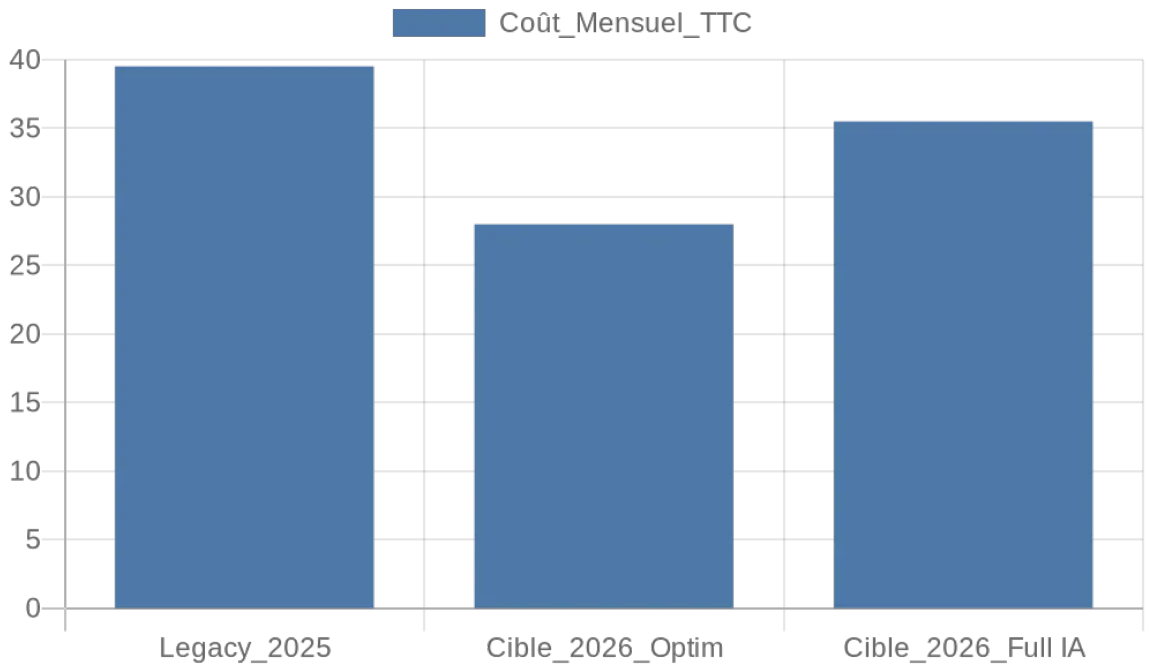
3. Synthèse ROI & Valeur Ajoutée

Gains Financiers

- **Total Cible Optimisé** : ~28 € / mois (hors IA intensive).
- **Total Cible “Full Package”** : ~35 € / mois (avec VPS IA permanent).
- **Économie nette** : ~10-30% selon usage, mais à périmètre fonctionnel **largement supérieur** (Puissance de calcul dédiée).

Valeur Métier (Intangible)

Cette transition génère une valeur inestimable pour le profil professionnel : 1. **Souveraineté** : Données 100% hébergées en France, code auditable. 2. **Compétence** : Preuve technique d’un savoir-faire “Architecte Cloud” et culture FinOps. 3. **Innovation** : Capacité à intégrer des LLM privés sans surcoût de licence (ex: Copilot à 19$/mois économisé).



(Graphique généré automatiquement pour illustration FinOps)

04. PERSPECTIVES I.A.

> **Vision** : Transformer une infrastructure d'hébergement classique en une plateforme intelligente d'assistance aux opérations.

1. Pourquoi l'IA dans ce projet ?

Dans une démarche **"Stratégie à votre image"**, l'IA ne doit pas être une boîte noire externe (ChatGPT/Copilot SaaS) qui ingère nos données sensibles. Elle doit être un composant interne de l'infrastructure (`ai-node`), capable de comprendre le contexte métier (Documentation, Code propriétaire) sans fuite de données.

2. Cas d'Usage Implémentés (Phase 2)

A. Moteur de Recherche Documentaire (RAG)

Problème : La documentation technique est dispersée (Markdown GitLab, Docs Nextcloud, Notes). **Solution** : **Perplexica** (ou équivalent Open Source). * **Fonctionnement** : Indexation vectorielle des dépôts GitLab et des documents Nextcloud. * **Usage** : Interface "Chat" permettant de poser des questions en langage naturel : *"Quelle est la procédure de rotation des clés SSH ?"* ou *"Résume l'architecture réseau du namespace prod"*. * **Souveraineté** : L'index reste local. Aucune donnée ne part chez OpenAI.

B. Analyse Statique Augmentée (SAST)

Problème : Détecter les vulnérabilités dans le code avant déploiement. **Solution** : **SonarQube** + **Plugins IA**. * **Pipeline** : À chaque `git push` sur GitLab, le code est analysé. * **Apport IA** : Détection de patterns complexes, suggestions de refactoring et explication des failles de sécurité aux développeurs juniors.

3. Architecture Logique du Nœud IA

Le VPS-2 est configuré comme un "Worker" spécialisé.

Couche	Technologie	Rôle
Interface	UI Web / API	Point d'entrée pour l'utilisateur et les webhooks

Couche	Technologie	Rôle
Cerveau	**Ollama**	Exécution des modèles (LLM) optimisés (ex: Mistral-7B, Llama3)
Mémoire	**Qdrant**	Base de données vectorielle pour le contexte (RAG)
Calcul	CPU (AVX2)	Inférence sur CPU (Pas de GPU, modèles quantifiés Q4_K_M)

4. Futur : Vers l'Auto-Remédiation ?

À terme (Post-Stage), l'objectif est de coupler le monitoring (AlertManager) à l'IA pour proposer des diagnostics automatiques en cas d'incident : * *Alerte* : "Disk Usage High on /var/lib/docker". * *IA* : "Analyse : Logs conteneur Mailcow anormalement volumineux. Suggestion : `docker system prune` ou rotation logs."

05. RÉFÉRENTIEL DE COMPÉTENCES

> **Titre visé** : Administrateur Systèmes DevOps (RNCP 36061). **Objectif** : Ce chapitre démontre la couverture des blocs de compétences du titre par les réalisations concrètes du projet uyoopVPS.

Bloc 1 : Automatiser le déploiement d'une infrastructure (RNCP36061BC01)

Compétence Référentiel	Réalisation Concrète Projet uyoop	Livrable Dossier
Automatiser la création de serveurs	Provisioning des VPS (Core & AI) via scripts de bootstrap (Cloud-init / Bash). Configuration initiale automatisée.	Scripts de setup (`setup.sh`), configuration SSH/ User.
Automatiser le déploiement	Utilisation de l'approche **GitOps** (ArgoCD) ou **Helm Charts** pour déployer K3s, Mailcow, Nextcloud. L'état désiré est défini dans le code.	Dépôt Git d'Infrastructure, Manifests Kubernetes.
Sécuriser l'infrastructure	Architecture **Zero-Trust**. Mise en place de **Authelia** (2FA), **Vault** (Secrets), **NetworkPolicies** (Isolation Namespaces), et durcissement OS (Firewall UFW, Fail2Ban).	Chap. 01 (Architecture), config Firewall, Politiques K8s.
Mettre en prod. dans le cloud	Gestion de l'exposition Internet via **Traefik** (Ingress Controller), gestion DNS (OVH/	URL accessibles (`mail.uyoop.fr`, etc), Dashboards Traefik.

Compétence Référentiel	Réalisation Concrète Projet uyoop	Livrable Dossier
	Cloudflare) et certificats TLS auto (Cert-Manager).	

Bloc 2 : Déployer en continu une application (RNCP36061BC02)

Compétence Référentiel	Réalisation Concrète Projet uyoop	Livrable Dossier
Préparer environn. de test	Création d'un namespace dédié `dev-lab` ou utilisation du VPS-2 (AI-Lab) pour valider les mises à jour avant la prod.	Configuration Namespaces K8s, Scénarios de test.
Gérer le stockage des données	Implémentation d'une stratégie de stockage hybride : **PV/PVC Kubernetes** (Longhorn/LocalPath) sur NVMe + **Object Storage S3** pour les archives.	Chap. 01 (Stratégie Données), Config StorageClasses.
Gérer des containers	Conteneurisation de tous les services (Mailcow, Nextcloud, Apps uyoop). Gestion des images Docker et Registre privé.	`docker-compose.yml`, Pods K8s, Dockerfiles.
Automatiser la mise en prod	Mise en place de pipelines **GitLab CI/CD** : Build, Scan de sécurité (Trivy/Sonar), Déploiement auto sur Cluster K3s.	Fichiers `.gitlab-ci.yml`, Rapport de scan SonarQube.

Bloc 3 : Superviser les services déployés

(RNCP36061BC03)

Compétence Référentiel	Réalisation Concrète Projet uyoop	Livrable Dossier
Définir statistiques services	Identification des indicateurs clés (KPI) : Disponibilité Web, Espace Disque (Alerte NVMe), Charge CPU (notamment sur Node IA).	Liste des métriques surveillées, SLA définis.
Exploiter solution supervision	Déploiement de la stack d'observabilité : **Prometheus** (Collecte), **Grafana** (Visualisation), **AlertManager** (Notifications Discord/ Mail).	Screenshots Dashboards Grafana, Exemples d'alertes.
Echanger en anglais	La totalité de la documentation technique du code (Commentaires, Commits Git) et la veille technologique sont réalisées en anglais international.	Commits Git, README techniques des repos.

Synthèse de la Couverture

Le projet uyoopVPS couvre **100% des compétences techniques** du titre. Il dépasse le cadre standard par l'intégration d'une dimension **DevSecOps** (Sécurité avancée) et **AIOps** (Intégration Intelligence Artificielle), apportant une valeur ajoutée distinctive présentée au Jury.

Fin du Dossier Technique - uyoop 2026