Quentin Lapointe

Site Reliability / DevSecOps Engineer — Kubernetes, GitOps & Internal Platforms (PaaS)

Profile Photo

Summary

SRE / DevSecOps engineer with 8+ years of experience designing, securing and operating Kubernetes platforms at scale. Sole operator of a production fleet of 200+ websites on 60 servers and 50 parallel QA environments; platform engineer for a 250-employee zero-trust infrastructure (Vault, SSO for 3,000+ users, ISO27001). €1,600/month (≈19k€/year) infrastructure cost reduction through cloud-native migrations/decommissions, monitor of availability and TLS expiry of 30 services, dependency update and CVE checks across 20+ repositories. Deep expertise in Kubernetes, Docker and developer-facing PaaS tooling in Go and Python.

Contact

quentin@lapw.at

Education

- **Engineering Degree** / **Master in Computer science engineer curriculum** / **Artificial intelligence Master**, *ENSIMAG*
- **Two-year university degree in Computer science**, *IUT de Vélizy-Villacoublay*

Skills

Kubernetes & Containers: Kubernetes (OVH MKS, k3s, Talos Linux), FluxCD / GitOps / OCI artifacts, Helm & chart authoring, Cilium (eBPF CNI, NetworkPolicies), Docker & image pipelines (ghcr.io), MetalLB, Traefik, Nginx Ingress, Gateway API, Longhorn / OpenEBS / CSI storage, OpenFaaS serverless

Security & DevSecOps: HashiCorp Vault (HA Raft, PKI, SSH CA, AppRole, OIDC), OAuth2 / SSO / OIDC (OneLogin, OAuth2-Proxy), Kyverno policy-as-code, External Secrets Operator, SOPS + age, cert-manager / Let's Encrypt, ISO27001 compliance & audit logs (Graylog), Renovate OSV/CVE automation, Zero-trust architecture, Tailscale

CI/CD & Automation: GitHub Actions, GitLab CI, Renovate (automerge, dependency dashboard), flux bootstrap / cluster reconciliation, Terraform, Ansible, Staged cluster & control-plane upgrades

PaaS & Developer Tooling: Internal developer platforms (self-service deploy, app templates), CLIs & automation in Go and Python, Helm chart library for product teams, Secrets-as-a-service for developers, Runbooks, wikis and platform documentation

Observability: Prometheus (custom exporters & queries), Grafana dashboards & KPIs, Alertmanager, Gatus blackbox monitoring (30+ services), Graylog / Fluent-Bit log pipeline, InfluxDB / Flux

Cloud & Infrastructure: AWS (Lambda, API Gateway, IAM, SES, Chalice), Google Cloud, OVH, Scaleway, Hetzner, vSphere, S3 / Object Storage, CEPH

Languages: Go (Golang), Python, Bash / Shell, YAML, TypeScript / Node.js (fullstack background), Java

Professional Experience

Site Reliability / DevSecOps Engineer Jan 2024 - Jan 2026

Scality

Enterprise object-storage software publisher (RING, ARTESCA). Owned the company-wide internal platform: Kubernetes (OVH), HashiCorp Vault HA, SSO/OAuth for 300+ internal users and up to 3,000 employees + customers — in support of the ISO27001 certification achieved during this period.

- Designed and operated the internal Kubernetes platform on OVH Managed Kubernetes: 5 core IT services (Vault, Netbox, OAuth2-Proxy-protected apps, monitoring) fully declared in Git, reconciled by FluxCD every 1–10 minutes — zero manual kubectl changes in production.
- Built a High-Availability HashiCorp Vault platform (2 logical instances): 5 replicas spread across 5 different server racks, Raft integrated storage (atomic snapshots, 2-minute disk commit), daily encrypted snapshots to GCS with 1-year object lock, and audit logs streamed through Fluent-Bit to Graylog, archived 12 months.
- Implemented a zero-trust identity architecture: all Vault access via OIDC / OneLogin SSO covering 250 internal employees within a 3,000-user SSO population; every key signing and certificate issuance gated by policy checks; AppRole machine identities with 1-minute token TTLs; least-privilege access profiles (employee / intern / contractor / guest) modeled from BambooHR & Salesforce.
- Vault as PKI & SSH Certificate Authority: short-lived signed SSH certificates for engineers connecting to customer servers through the VPN bastion — replaced long-lived authorized_keys with one-time keys verified client-side by a trusted CA.
- Led the vSphere → Kubernetes and block-storage → S3 migrations: moved Vault and Netbox off 20 legacy VMs (10 dev + 10 prod), migrated 20 TB from CEPH volumes to Object Storage at 8€/TB/month instead of 20–26€/TB — saving €1,600/month (~€19,200/year) while decommissioning entire VM fleets.
- Automated dependency and CVE management with Renovate across 20+ application repositories and all infrastructure manifests: automerge on non-major bumps, OSV vulnerability alerts and dependency dashboards; cleared services (Vault, Netbox) running several major versions behind — closing a backlog of known CVEs before the ISO27001 audit.
- Eliminated certificate-expiry outages: cert-manager + Let's Encrypt issuing and renewing 10 TLS certificates (including *.it.scality.com wildcard via OVH DNS), with Gatus blackbox health-probing of ~30 internal services and automatic alerting — 100% reduction of certificate expiry / failed-renewal incidents since deployment.
- Zero-downtime Kubernetes upgrades using a temporary 3-node 'upgrade' node pool (billed hourly): drain/cordon of the low-resource pool, rolling update, scale-to-zero — company tooling stays available through every version bump, with a documented runbook for Vault unsealing during control-plane rollouts.
- Security data visualization for ISO27001: Grafana dashboards fed by custom Prometheus queries (fleet-wide device compliance per employee, InfluxDB/Flux queries on package-download logs) as auditor-facing evidence of endpoint security posture for the 250-employee fleet.
- CI/CD for internal services: GitHub Actions + Docker pipelines (docker/build-push-action → ghcr.io, timestamped tags) and OAuth2-Proxy in front of every exposed endpoint (replacing Basic-Auth), including force-logout session revocation.
- Technologies: Kubernetes (OVH), FluxCD, HashiCorp Vault, OIDC/OneLogin, OAuth2-Proxy, Renovate, GitHub Actions, Docker, Terraform, Grafana, Prometheus, Graylog, Gatus, InfluxDB, CEPH, S3, vSphere
- Day-to-day work entirely in English: runbooks, wikis, design docs and meetings with an international team.

Platform Engineer — GitOps Kubernetes Platform (Talos Linux) Jan 2023 - Present

Personal Projects — Home-Lab

Self-hosted, security-first home lab running my public services — a full PaaS where any application ships as a single HelmRelease commit. Bare-metal nodes run immutable Talos Linux (declarative config, API-only access, no SSH)

- 7 self-hosted applications (Postgres, Redis, Radicale CalDAV/CardDAV, Vaultwarden, blogs, web apps) deployed as namespaces + HelmReleases from a shared app-template repository — each with rclone backups to Scaleway Object Storage.
- FluxCD installed via the flux-operator with OCIRepository sources: charts and kustomize artifacts pulled as OCI images from ghcr.io, 1-minute reconciliation, prune enabled, 100% of cluster state declared in Git — including SOPS + age encrypted secrets decrypted only in-cluster.
- Policy-as-code with Kyverno: GeneratingPolicies automatically create a default-deny CiliumNetworkPolicy in every new namespace (zero-trust network isolation with explicit allows only for ingress, monitoring and Tailscale) and auto-generate Traefik IP-filter policies on every HTTPRoute.
- Secrets pipeline: HashiCorp Vault + External Secrets Operator with ClusterSecretStore and AppRole tokens of 1-minute TTL, read-only Vault policy — no secret ever committed in clear.
- Fully automated control-plane upgrades: Renovate manages Kubernetes manifests, Flux HelmReleases and OCI tags (automerge non-major, approval gated per critical component); a CRD-based upgrade operator (TalosUpgrade / KubernetesUpgrade) orchestrates staged rollouts — currently running Talos v1.14.4 and Kubernetes v1.37.
- Networking & observability: Cilium eBPF CNI, MetalLB, Tailscale operator, Traefik behind Gateway API, cert-manager wildcard certificates (Let's Encrypt + Cloudflare DNS), kube-prometheus-stack, Gatus blackbox probing, Forecastle service catalog.
- Technologies: Talos Linux, k3s, Kubernetes, FluxCD, Cilium, Kyverno, Vault, External Secrets, SOPS/age, Renovate, Tailscale, MetalLB, Traefik, cert-manager, Prometheus, Grafana, Docker, GitHub Actions, Go

Site reliability / DevOps Engineer Jan 2021 - Jan 2024

Cap Collectif

French responsible-digital agency. Sole DevOps/SRE for a team of 8 developers (3 frontend, 4 backend): single-handedly operated the whole production infrastructure — 200+ client websites across 60 servers (OVH, Scaleway) — plus a Kubernetes cluster hosting 50 parallel QA environments.

- Ran 200+ production websites on 60 servers alone: provisioning, hardening, ingress routing, TLS, per-client isolation — effectively an internal PaaS for 8 developers and the agency's client base.
- Operated a Kubernetes cluster hosting 50 concurrent QA/staging instances alongside production: per-project namespaces, templated Helm Releases, developers shipping through pull requests instead of asking ops.
- Adopted GitOps early with FluxCD: applications described as Helm Releases and Kustomizations in Git, drift automatically reconciled; wrote the agency's Helm chart library (Deployment, Service, Ingress, Certificate, PVC templates) so a new project was a one-file commit away from production.
- Designed storage and backup strategy for stateful workloads: Longhorn (Rancher) replicated block storage with scheduled snapshots, OpenEBS LocalPV for performance-sensitive cases, off-cluster backups to Scaleway S3 Object Storage — with tested restore procedures, not just backups.
- Built the observability stack from scratch: Prometheus metrics across clusters and exporters, Grafana dashboards for system and business KPIs, alerting on SLO-relevant signals.
- Delivered a serverless data pipeline on OpenFaaS: functions ingesting Cloudflare log streams to power a new backoffice feature letting agency clients analyze traffic on their sites — scale-to-zero for batch-friendly workloads, ingress and auth handled by the platform.
- Automated developer toil with internal Python CLIs used daily by the 4 backend developers: one-command access to instances, server operations, deploy helpers and credential fetching — cutting recurring ops requests to the platform team.
- Automated certificate lifecycle for 200+ domains with cert-manager + Let's Encrypt (wildcard DNS-01, automatic renewal): zero manual TLS operations during the tenure.
- Infrastructure as code: Terraform for cloud resources, IAM and Object Storage buckets; Ansible for server provisioning, hardening and routine operations.
- Technologies: Kubernetes, FluxCD, Helm, OpenFaaS, Longhorn, OpenEBS, OVH, Scaleway, Terraform, Ansible, Prometheus, Grafana, Python, cert-manager

Project development – Fullstack Jan 2019 - Jan 2020

Vauban

Dashboard 2.0 development (Node.js / Vue.js / Typescript) – AWS Lambda – AWS SES – Python – Pandas – Scipy – Jupyter

- Designed the cloud architecture and built a fullstack dashboard 2.0 from scratch (Node.js / Vue.js / TypeScript); chose the tech stack and recruited and led a 3-developer team.
- Full CI/CD on GitLab-CI with 4 environments (dev, nightly, staging, production) deployed to Heroku on merge; serverless backend on AWS API Gateway + Lambda with IAM-based auth and Chalice automation.
- Productized legal operations: automatic generation of legal documents and e-signature flows for offshore vehicles from declarative YAML + Markdown templates; crypto trade-aggregation analytics in Python (Pandas, SciPy).
- Technologies: Node.js, Vue.js, TypeScript, AWS (Lambda, API Gateway, SES, IAM), Chalice, GitLab CI, Heroku, Python, HashiCorp Vault, Cloudflare

Operational Research Engineer (Startup) Apr 2018 - Dec 2018

ShopRunBack

Startup – NLP – Golang – AWS Lambda – Grafana

- Backend services in Go (Golang): name-based product classification (NLP) over retail catalogs and constrained shortest-path computation for shopping-route optimization.
- Serverless deployment: Go binaries packaged as AWS Lambdas via Docker-based builds, Grafana monitoring of invocations.
- Technologies: Go, AWS Lambda, Docker, Grafana

Computer vision for precision agriculture May 2017 - Aug 2017

RGX-Systems

Startup – AI – OpenCV

- Image classification of crops using AI / OpenCV pipelines in a precision-agriculture startup.

Big Data POC – Neo4j Jun 2016 - Jul 2016

Cabestan

Big Data – Python

- E-marketing POC on Neo4j: linked CRM and web navigation data across several clients; contact-list generation via least-cost path computation over a price matrix.

Big Data POC – Neo4j Apr 2015 - Jul 2015

Médiamétrie

Big Data – Java

- Relational-to-graph transposition (Neo4j) to detect inconsistencies in audience measurement databases; modeling, ingestion and rectification proposals in Java.

iOS Application Developer Jul 2014 - Jul 2014

Arismore

Mobile Dev – Objective-C

- Development of TogafMore (Objective-C).