

CLOUD PRIVÉ MULTI-ORGANISATIONS · RUST

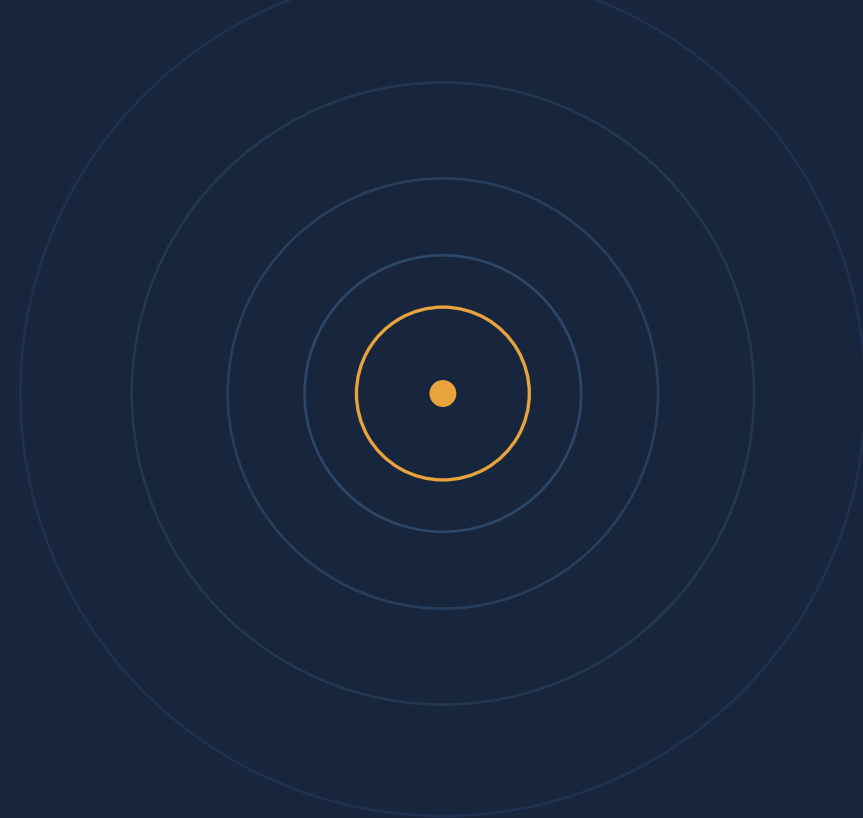
CIRROSTRATUS

Le meilleur de chaque nuage, dans le vôtre.

v0.136 · 101 services réels · ~340 000 lignes de Rust

Revue complète du projet — 16 volets · octobre 2026

Sources : [README.md](#) · [CHANGELOG.md](#) · [docs/](#) · [git log](#) — dépôt [project344-cirrostratus](#) (Gitea LAN)



Chaque cloud excelle quelque part — et déçoit ailleurs

	CE QUI EST REPRIS	L'ANTI-PATTERN ÉCARTÉ
AWS	IAM, policies, simulateur de refus	console labyrinthique
GCP ♦ Azure	hiérarchie org → projets · scopes RBAC propres	facturation illisible
EC2 ♦ Scaleway	compute simple et lisible	verrouillage propriétaire
OVH ♦ Scaleway	transparence tarifaire, prix affichés €/h	coûts cachés en fin de mois

Cirrostratus prend le meilleur de chacun — sans les anti-patterns — dans une plateforme auto-hébergeable que vous maîtrisez de bout en bout.

Un cloud public entier — réel, mesuré, chez vous

101

services réels, zéro simulé

chacun exposé en API REST, CLI, TUI, WebUI et MCP — événements sur le bus, audit chaîné

5

surfaces d'accès

REST, CLI, TUI, WebUI, MCP — toutes parlent au même noyau, sans logique dupliquée

100 %

composants permissifs

~50 briques MIT / Apache / BSD dans la BOM, zéro copyleft, vérifiées cargo-deny

« Aucune donnée inventée : ce qui n'est pas mesuré est affiché comme tel. »

~340 000 lignes de Rust en 36 jours

~340 000

lignes de Rust — monorepo de 167 fichiers ; la seule crate métier (cirro) en compte 318 000 sur 130 modules

837

commits du 29/08 au 11/10/2026 — 36 jours actifs, 30 branches de travail

2 396

tests verts à la v0.136 — 2 237 lib + 159 e2e · clippy -D warnings : 0 avertissement

0

CVE connue au binaire — 503 crates auditées (cargo-audit · osv-scanner · cargo-deny, 06/10/2026)

20

tags v0.91.0 → v1.6.0 — version courante 0.136.0

Un monorepo Cargo, cinq crates



État : SQLite en développement — FerroDB / PostgreSQL en production · 14 tables typées (docs/MODELE-DONNEES.md)

Cinq façons d'atteindre le même cloud

UN NOYAU

store · événements · audit
chaîné

API REST

802 chemins · 1 059 opérations

/v1/* — OpenAPI 3.1 embarquée, Swagger UI hors-ligne

CLI cirro

même store que la REST

106 commandes — scripts, automatisation, CI

TUI cirro-tui

6 onglets

console terminal ratatui

WebUI

responsive 1280 et 470 px

~35 produits · 48 vues — thème Nuit & Halo

MCP

183 outils

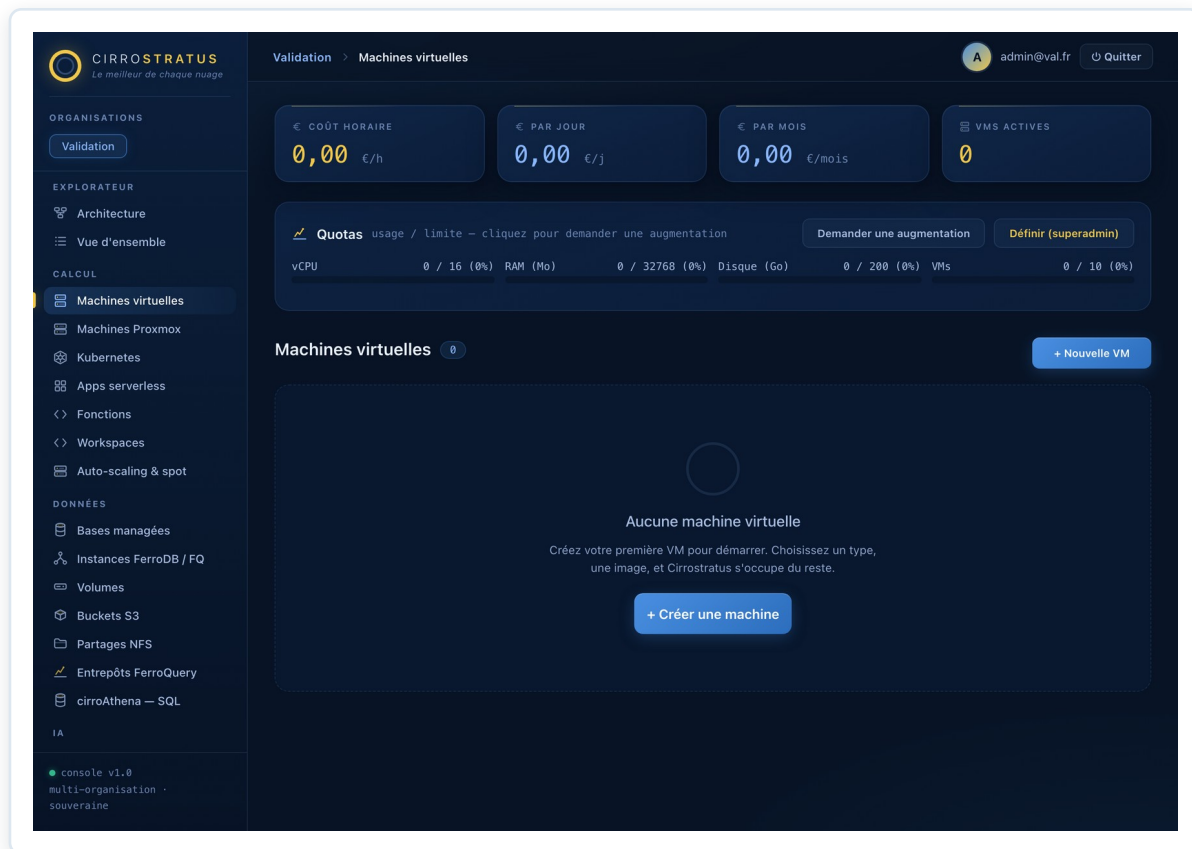
JSON-RPC / stdio — pour les agents IA

Chaque surface appelle les mêmes handlers que l'API REST — pas de logique dupliquée.

101 services réels, par famille

Famille	Réalisé avec (composants réels)	Équivalent public
Compute	VMs Proxmox VE + QEMU/KVM (driver QMP) · spot −70 % · auto-scaling · fonctions Knative	EC2 · Spot · ASG · Lambda
Conteneurs	k3s managés · CSI Longhorn · Traefik · Kyverno + scans CVE à l'admission	EKS
Données	FerroDB (pgwire, Raft) · FerroQuery · buckets SeaweedFS · cirroAthena SQL ad hoc	RDS · BigQuery · S3 · Athena
Messagerie	ferroq MQTT / HTTP / gRPC · cirroTopics fan-out HMAC · cirroRegles · cirroFlux · cirroWorkflows	SQS · SNS · EventBridge · Step Functions
IA	endpoints LLM (llama.cpp, RTX 3090) · créneaux GPU exclusifs · cirroModeles · cirroAgents	Bedrock · SageMaker
Réseau	VNets + NACL · pare-feu L3/L7 · cirroDNS · cirroLB · cirroVPN WireGuard · IPv6	VPC · Route 53 · ELB
Sécurité & gouvernance	IAM 3 rôles + MFA TOTP · cirroCA X.509 · quotas · showback €/h · budgets & alertes	IAM · ACM · Cost Explorer

La console, capturée en recette réelle



cirroMachines — VMs, quotas, zones, coûts €/h (2560×1800)



/swagger — OpenAPI 3.1 embarquée, hors-ligne

Ce que prouvent les captures

- thème Nuit & Halo — responsive vérifié 1280 et 470 px
- compteurs et coûts réels — rien de simulé
- 136 dossiers de recettes dans docs/preuves/

Quand rien n'existe en permissif, la brique s'écrit

Les briques absentes de l'écosystème permissif s'écrivent en Rust — dans le dépôt ou en projets sœurs :

FerroDB	SGBD transactionnel maison — protocole pgwire + Raft, quorum 2/3 multi-site (v0.3)
----------------	--

FerroQuery	moteur analytique maison — l'équivalent BigQuery du cloud (v1.19)
-------------------	---

ferroq	messagerie MQTT / STOMP / HTTP / gRPC — files et topics gérés
---------------	---

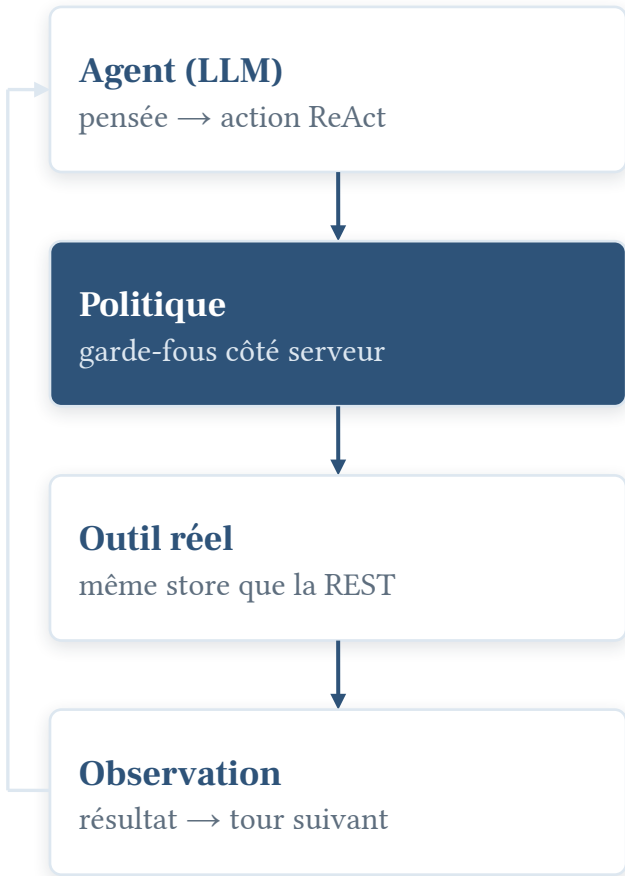
cirroCA	autorité de certification X.509 maison — secrets chiffrés AES-GCM
----------------	---

ferroIdp	fournisseur d'identité complet (clone Keycloak) — 15 883 lignes · 118 tests
-----------------	---

ferroIndex	moteur de recherche (clone Elasticsearch) — 5 562 lignes · 91 tests
-------------------	---

Côté IA, la pile se complète : ferroKB · ferromemo · ferroDeepResearch.

cirroAgents — des agents ReAct sur des outils réels



107	outils réels — 91 lectures + 16 actions, alloués par agent ; l'agent ne voit que ses outils
Garde-fous	lecture_seule · max_etapes · cout_max_euros · outils_interdits — vérifiés AVANT chaque exécution d'outil
Mémoire	200 notes persistées ; les 12 dernières sont injectées dans le prompt système à chaque run
Évals	critères mécaniques (contient · exact · regex · outil_utilise) — score reproductible, aucun juge LLM

Équivalent Bedrock Agents / AgentCore · scaffold en une requête · timeline de run complète (pensée / observation / erreur)

Programmer le cloud, sans dépendance

34 ♦ 3

Provider Terraform / OpenTofu

écrit en Go (terraform-plugin-framework v1.15) —
resources et data sources natives

[terraform/RESOURCES.md](#)

36 ♦ 36

SDK Python & TypeScript

zéro dépendance externe — tests miroir dans les deux
langages

[sdks/python](#) · [sdks/typescript](#)

25

exemples déployables

shop, ML, vision, paiement... — validés de bout en bout

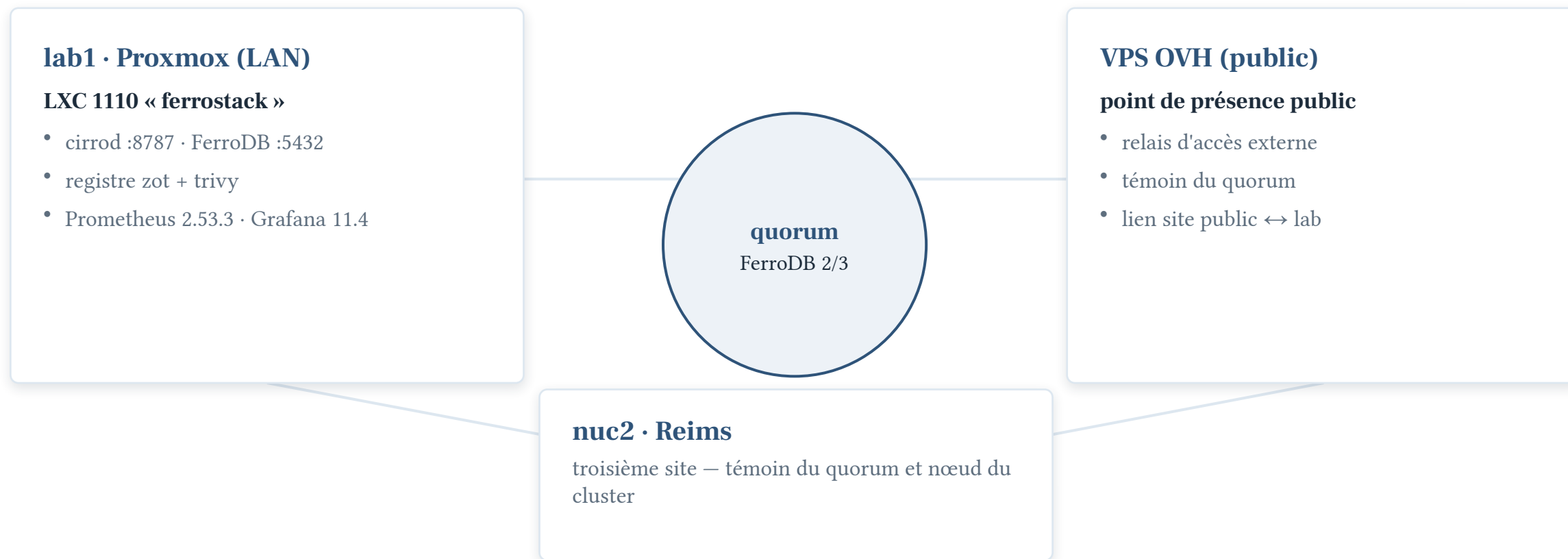
307 ressources validées (tofu validate)

```
$ cirro vm new acme front-web --type cs-small --image debian-12 --spot
```

```
$ cirro athena acme exec "SELECT count(*) FROM vms"
```

```
$ tofu plan # 307 ressources validées sur les 25 exemples
```

Trois sites, un quorum, un k3s tri-site



Cluster k3s tri-site interconnecté headscale / Tailscale · SLO + error budgets (docs/SLO.md) · perf mesurée (PERF.md)

Du chiffrement au changement audité

Socle sécurité

- audit chaîné SHA-256 — chaque mutation est scellée
- secrets chiffrés AES-GCM · MFA TOTP · Argon2id
- JWT signés · cirroCA — PKI X.509 maison
- cirroPolitiques — 7 contraintes SCP, refus 403 réels
- cirroInspecteur — scans SSH (Inspector)
- cirroInsights — détections H5 / H6 (GuardDuty)
- break-glass scellé · protection VM or / argent / bronze
- webhooks signés HMAC avec rejeu

Qualité

O

CVE connue au binaire — 503 crates auditées : cargo-audit · osv-scanner · cargo-deny (06/10/2026)

- clippy -D warnings : 0 avertissement
- 136 dossiers de preuves de recette (docs/preuves/)
- 29 études comparatives (etudes/)
- cahier des charges : ~200 exigences tracées
- CHANGELOG tenu version par version — 298 Ko

Cinq flux parallèles, un worktree chacun



Chaque tranche : 5 flux isolés dans des worktrees git dédiés, fusionnés dans main en fin de tranche.

355

actions planifiées — plan « 89 services » documenté

98,3 %

livrées à ce jour : 346 actions sur 351 (tranche t21)

30

branches de travail · CI sur Gitea act_runner et GitHub

Documentation d'exécution : docs/tranches-execution-2026-10.md — le plan et son avancement sont écrits, pas implicites.

36 jours du premier commit à la v0.136



Livré

- lots 0 → 6 : 100 % livrés (docs/ROADMAP.md)
- V2 partielle : serverless Knative, workspaces, SVID SPIFFE

Reste à faire

- réplication stretch FerroDB multi-site
- réparer la base de contrôle FerroDB (post-incident Raft du 11/10)
- pile d'observabilité encore colocalisée dans les clusters monitorés
- plan d'actions : 332/355 (94 %) — collisions DNS inter-orgs, fonctions en échec rollout

Le meilleur de chaque nuage, dans le vôtre.

1

Complet et réel

101 services mesurés, zéro simulé — prouvés par 136 dossiers de recette

2

Souverain

100 % composants permissifs, auto-hébergé sur trois sites, audit chaîné

3

Sain pour la suite

2 396 tests verts, 0 CVE, roadmap et dettes écrites noir sur blanc