Fleet overview — machines and access

Fleet overview — machines and access

Everything Conor runs, what it is for, and how to reach it. Audited read-only on 2026-11-06. Per-host detail and open issues: **Fleet audit — 2026-11-06**.

host	role	public	tailnet	ssh from cbcore
cbcore	home server, Docker host, mail, Forgejo, wiki	125.253.17.92 (dynamic residential)	100.64.0.3	local
vps2	public edge: DNS, TLS, Caddy, headscale	187.52.126.150	100.64.0.16	`vps2-conor`
cbfarm	marketdata pipeline, Docker, KVM farm	65.181.15.26	100.64.0.4	`cbfarm`
jamievps	Jamie's production (Helios), not Conor's to break	31.97.188.242	100.64.0.17	`jamievps-conor`
vps (old)	still the public mail edge, being retired	203.57.114.42	100.64.0.2	`conor@100.64.0.2`

cbcore — Debian 13, Ryzen 9 7950X (32 threads), 31 GB RAM, 915 GB root

The always-on box. Public entry is only through vps2's Caddy over the tailnet; almost every service binds `100.64.0.3:<port>` rather than `0.0.0.0`. Runs ~40 containers: mailcow (18), Forgejo + Postgres, Nextcloud + Collabora, Twenty CRM, ComfyTax, tradingjournal, rss-hub, Feishin, qBittorrent behind NordVPN, Plex, Ollama, netdata. Host Caddy serves the tailnet-bound site ports (:8000–:8102). **Root filesystem is 89% full (101 GB free)** — the only real capacity timer in the fleet. `conor` is in `sudo` and `docker`.

vps2 — Debian 13, 2 vCPU EPYC 9355P, 7.9 GB RAM, 99 GB disk (60 GB free)

The public edge since 2026-11-05. Caddy terminates TLS for all ~33 hostnames and proxies back over the tailnet. Also runs headscale + headplane (tailnet control plane, 12 nodes), cli-proxy-api on `100.64.0.16:8317`, marketdata PHP on :8001, and strata under PM2 on :3009/:3011. Sites live in `/home/deploy/sites/<site>/ {releases,current,shared}`, deployed by `deploy-sites.timer` every 60 s from Forgejo. Only 2 vCPU — CPU-heavy work does not belong here.

cbfarm — Debian 13, Ryzen 5 3600 (12 threads), 16 GB RAM, 922 GB disk (800 GB free)

Bulk storage and compute. Source of the marketdata pipeline (cron `0 5 * * 2-6`, `~/cronjobs/market-data`) and of the strata repo. Docker runs Forgejo, Twenty CRM and a MariaDB; host Caddy serves PHP sites on :8000–:8003 and :8007. KVM is present and nested virt is enabled, so it can host VMs. 800 GB free — the place to put anything big.

jamievps — Debian 13, 8 vCPU EPYC 9354P, 32 GB RAM, 394 GB

disk (313 GB free)

Jamie's box, Conor has an account but **no sudo**. Runs the Helios stack (api :8770, terminal :8030, coverage :8766, playground, gli-webhook), Caddy, MariaDB on `127.0.0.1:3306`, plus Helios timers including an auto-deployer. No Docker installed. `/home/jamie` is `0700` and holds production — Conor's user cannot read it and must not be given docker group membership, which would be root-equivalent.

vps (old) — Debian 13, 1 vCPU, 967 MB RAM, 20 GB disk

Former edge. Everything except mail has moved to vps2, so it now only does Postfix/Dovecot/HAProxy on the public mail ports (25, 465, 587, 993, 4190) and holds the `caddy-cert-stage`, `mailcow-ban-sync` and `mpanel-memory-graph` timers. Retire it once mail has cut over to vps2. RAM is tight (967 MB).

Conventions that bite

- `vps.seabee.me` no longer means the old vps — DNS points at vps2, so the `vps` ssh alias fails the host-key check. Use `conor@100.64.0.2`.
- Service ports on these hosts are usually bound to the tailnet IP. Reachable from anywhere on the tailnet, invisible from the internet; `ss -tln` alone does not show whether that is intended, so check the bind address.
- Sudo needs a password everywhere; automated work has to either ask Conor or use a pre-installed narrow `sudoers.d` rule.
- Timezones are `Australia/Sydney` on all five, but cron on vps2 has no `CRON_TZ` support in Debian 13, so the host clock is what sets the schedule.

Revision #3
Created 6 November 2026 12:36:49 by bot
Updated 6 November 2026 13:15:52 by bot