Fleet audit — 2026-11-06

Fleet audit — 2026-11-06

Read-only pass over every reachable host (`~/.hermes/scripts/host-audit.sh`, run as each host's `conor`). Facts as found that night; nothing was changed.

cbcore (100.64.0.3)

- Debian 13 trixie, kernel 6.12.113, up 8 days, load 1.06.
- Ryzen 9 7950X, 32 threads, 31 188 MB RAM (12 048 used, 19 139 available).
- Root 915 GB, 767 GB used, 101 GB free, **89%**. `/home/conor` alone is 212 GB.
- Docker 29.8.1, 40 containers running. Forgejo 16.0.6, Nextcloud 33, Twenty v2.45.0, ComfyTax, tradingjournal, rss-hub fusion 1.1.1, Feishin 1.15, Plex, Ollama, netdata, Collabora, mailcow (watchdog 2.11, postfix 3.10.12, dovecot 2.3.21.1, rspamd 4.2.1, nginx 1.30.6, mysql 10.11, sogo 5.12.12).
- Node 24.16.0, npm 11.13.0, PHP 8.4.27, Caddy 2.11.4, MariaDB 11.8.6, PostgreSQL 17.11, Python 3.13.5, uv 0.11.18, git 2.47.3, pm2 7.0.4.
- Users with shells: conor (1000, sudo + docker), ciara (1002), guest (1003), dad (1004). `adm` includes conor, www-data, netdata.
- Cron (conor): calendar DB backup 04:00, `docker builder prune -af` weekly, TLS cert check 05:20, container health 05:40, vpn-box watchdog every 5 min.
- **Anomaly:** `certbot.service` failed. Caddy owns TLS here, so it is almost certainly a leftover from an older setup — worth masking rather than debugging.
- **Risk:** disk at 89% is the fleet's tightest margin.

vps2 (100.64.0.16)

- Debian 13, kernel 6.12.113, up 5 days, load 0.04. EPYC 9355P, **2 vCPU**, 7 945 MB RAM (1 899 used), 99 GB disk (35 used, 60 free).
- Docker 29.9.2: `headscale` 0.29.6, `headplane` 0.8.2, `cli-proxy-api` v8.0.50 (listening `100.64.0.16:8317`).

- Node 22.23.4 system-wide, but strata runs on nvm 24.16.0 as `conor`; PHP 8.4.27, Caddy 2.11.7, MariaDB 11.8.6.
- Users: conor (1000, sudo + docker), orcaide (1001). Service accounts include `caddy` (999) and `deploy` (995); groups `caddy:www-data` and `web:caddy,www-data`.
- Listening publicly: 22, 80, 443. Everything else is loopback or tailnet: 6768 (Orca), 8317 (cli-proxy).
- Cron (conor): market-data pipeline 05:00 Tue–Sat.
- Timers include `deploy-sites` (60 s), `exim4-base`.
- **Anomaly:** `helios-playground-v4.service` failed — unit *not found*, a stale leftover from the 4–5 Nov rebuild. Safe to remove.
- **Anomaly:** system `exim4` is still active; it must go before the Postfix relay role can bind port 25 for the mail cutover.

cbfarm (100.64.0.4)

- Debian 13, kernel 6.12.113, up 1 day, load 0.09. Ryzen 5 3600, 12 threads, 15 922 MB RAM (4 123 used), 922 GB disk (76 used, **800 free**).
- Docker 29.9.2: `forgejo` 16.0.6 + `forgejo_db`, `twenty-*` (server, worker, db, redis) — all up 27 h. Note Forgejo and Twenty also exist on cbcore; one of the two is the live instance and the other is a leftover — confirm before either is touched.
- Host Caddy 2.11.7 listening :80, :81, :8000, :8001, :8002, :8003, :8007. Also 222, 3389 (xrdp), 22000 (syncthing), 8384, 6768.
- PHP 8.4.27, MariaDB 11.8.6, Python 3.13.5, git 2.47.3. No Node in PATH for the audit user.
- Users: conor only, in `sudo` + `docker`. Cron: market-data pipeline.
- **Anomaly:** `NetworkManager-wait-online.service` failed — cosmetic on a wired box, but it slows boot ordering.

jamievps (100.64.0.17)

- Debian 13, kernel 6.12.115, up 1 day, load 1.32. EPYC 9354P, 8 vCPU, 32 100 MB RAM (14 839 used), 394 GB disk (66 used, 313 free).
- **No Docker.** Node 22.23.4, MariaDB 11.8.6, Caddy (installed, `--version` unsupported flag), Python 3.13.5.
- Listening: 22/80/443 public; on tailnet 3306 (MariaDB), 5180, 8096, 8770.
- Users: conor (1000, no sudo), jamie (1001, sudo + adm). Service account `helios` (999), `caddy` (994).
- Timers: `helios-bitformance-live` (5 min), `helios-daily-refresh` 03:00, `helios-stream-freshness` weekly, `helios-hf-strategy-backtest` monthly (2026-12-05), plus the every-few-minutes deployer.
- No failed units.

vps — old edge (100.64.0.2)

- Debian 13, kernel 6.12.113, up 6 days, load 0.20. **1 vCPU, 967 MB RAM**, 20 GB disk (7.8 used, 11 free).
- Public ports: 25, 80, 443, 465, 587, 993, 4190 — it still owns the mail edge. Tailnet: 100.64.0.2:25 (relay for cbcore), plus its two tailscaled ports.
- Timers: `caddy-cert-stage`, `mailcow-ban-sync` (every min), `mpanel-memory-graph`, the apt/dpkg set.
- **Anomaly:** `systemd-sysctl.service` failed.
- **Trap:** `ssh vps` now resolves to vps2 through DNS, so the host key check fails. Address it as `100.64.0.2` until the alias is fixed.

Cross-cutting

- Every host is Debian 13 with `conor` as the administrative account except jamievps (no sudo) and vps2's `deploy`/`orcaide` service accounts.
- `conor` is in `docker` on cbcore, cbfarm and vps2 — equivalent to root on those boxes, which is why jamievps deliberately does not have Docker.
- TLS is Caddy everywhere; the old certbot on cbcore and the cert-staging timer on vps are legacy from before the edge moved.
- Only 101 GB free on cbcore against 800 GB on cbfarm and 313 GB on jamievps — bulk data belongs off cbcore.

Revision #3
Created 6 November 2026 12:36:50 by bot
Updated 6 November 2026 13:15:47 by bot