vps2

vps2

Hostinger VPS. Public `187.52.126.150`, Tailscale `100.64.0.16`, Debian 13, 8 GB RAM. SSH: `ssh vps2` (key `~/.ssh/cbcore`, key-only, port 22 open to the internet on purpose so access survives a Tailscale outage).

As of 2026-11-05 vps2 replaces `vps` (`203.57.114.42` / `100.64.0.2`). The old box is being retired; anything still only on it is listed at the bottom.

What runs here

Service	Path / port	Notes
Caddy (public edge)	`:80`, `:443`	`roles/caddy/files/vps2/Caddyfile`, ~33 site blocks. Proxies to cbcore `100.64.0.3` and cbfarm `100.64.0.4` over the tailnet.
headscale + headplane	`127.0.0.1:8080`, `127.0.0.1:3000`	Docker, `/home/conor/Docker/headscale`. State copied from vps 2026-11-05; nodes kept their keys, no re-registration.
marketdata	`/var/www/marketdata`	PHP 8.4-FPM + MariaDB 11.8, DB `market-data` (42 tables). Moved from cbfarm 2026-11-05.
marketdata pipeline	`/home/conor/cronjobs/market-data`	`uv run data_getter.py`, cron `0 5 * * 2-6`. Chromium 1161 + GNAF in `~/.cache`.
strata app + demo	`/home/conor/strata-project`, PM2 on `127.0.0.1:3009` / `:3011`	Moved from cbfarm 2026-11-05. Node 24.16.0 via nvm.
Orca IDE	`0.0.0.0:6768`, `127.0.0.1:43353`	User `orcaide` (uid 1001), linger on. Reachable on the tailnet only.
cli-proxy-api	`100.64.0.16:8317`	Docker container.

Firewall (ufw, active)

`deny incoming`, `allow outgoing`. Allowed: `22/tcp` from anywhere, `80`, `443`, mail ingress `25,465,587,993,4190`, everything `in on tailscale0`. Managed by `roles/firewall` + `host_vars/vps2.yml`.

ufw is the host firewall, and it is what blocks things — not Hostinger. Hostinger's own docs confirm port 25 is not filtered. A test listener on `0.0.0.0:4190` was unreachable purely because of the ufw default deny.

Gotchas

- `ufw.service` reports `inactive (dead)` while the ruleset is loaded and enforced. `sudo ufw status verbose` is the truth, not `systemctl is-active`.
- Reverse DNS is set in the Hostinger panel: VPS → Settings → IP address tab → Set PTR record. Do this before any outbound mail: HELO/PTR mismatch is what sends mail to spam.
- `cron` is **not** installed on a stock Debian 13 image (`apt-get install cron`). This cron build does **not** support `CRON_TZ`, and the box runs `Etc/UTC` while cbfarm ran `Australia/Sydney`, so a copied `0 5 * * 2-6` fires at 16:00 local. Fix the timezone (`sudo timedatectl set-timezone Australia/Sydney`) rather than offsetting the schedule, or it drifts again at the DST change.
- `web/` and `marketing/` are separate npm projects (no `workspaces` field), so `npm install` at the repo root does not install them. Without `npm --prefix web install` the frontend build watcher dies every 30 s with `Cannot find module .../web/node_modules/vite/bin/vite.js`.
- System node is 22.x; the strata repo pins `24.16.0` in `.nvrc`/nvm. PM2 must be started from the nvm path or `node` resolves to the wrong binary.
- `rsync -a` from a source host **overwrites ownership**. After copying `/var/www/marketdata`, the tree was `conor:conor 0750` and PHP (`www-data`, group `caddy`) could not read it. Always re-run `chown -R conor:caddy /var/www/<site>` after a copy.

Prepared but not yet live (2026-11-05)

- **Mail ingress**: `roles/haproxy/files/vps2/haproxy.cfg` (bind `187.52.126.150`, backends `100.64.0.3:10025/10465/10587/10993/14190`, `send-proxy-v2`).
- **Outbound relay**: `roles/postfix_relay` — `inet_interfaces = 100.64.0.16`, `mynetworks = 127.0.0.0/8, 100.64.0.3/32`, plus a boot-order drop-in so postfix waits for the tailnet address instead of dying.

- mailcow on cbcore still relays through the **old** VPS (`[100.64.0.2]:25`).

Still only on vps

Mail ingress (HAProxy) and the outbound relay, plus the DNS records still pointing at `203.57.114.42`. See [[domains]] and [[ops-journal]].

Revision #7
Created 6 November 2026 12:14:32 by bot
Updated 6 November 2026 13:15:54 by bot