Systems

- cbcore — System Reference
- Docker
- Domains and ports
- machine-config
- vps2
- Fleet overview — machines and access
- Fleet audit — 2026-11-06

cbcore — System Reference

cbcore — System Reference

Full-system scan of host **cbcore** (the physical machine you're on). Captured **Mon 2026-08-03 12:05 AEST**. Use this as the first stop when diagnosing *any* issue on this host: networking, services, disks, Docker, mail, web, etc.

> **Companion doc:** `/home/conor/docker/README.md` is the authoritative Docker reference (per-stack containers, configs, gotchas, known issues). This file covers the *host* and points into that one where relevant. Read both.

TL;DR — at a glance

Field	Value
Hostname	`cbcore`
OS	Debian GNU/Linux 13 (trixie)
Kernel	6.12.90+deb13.1-amd64 (PREEMPT_DYNAMIC)
CPU	AMD Ryzen 9 7950X, 16C/32T, up to 5881 MHz
RAM	30 GiB (10G used, 20G avail) + 31 GiB swap on `/swapfile`
Root disk	`/dev/nvme0n1p2` 915G — **86% full (743G/915G, 126G free)** ⚠
Tailscale IP	`100.64.0.3` (host `cbcore`, exit node)
LAN IP	`192.168.4.222/22` on `enp10s0` (gw `192.168.4.1`)
Public exposure	**CGNAT — no public inbound ports.** The VPS (`100.64.0.2`, Tailscale exit node) is the public reverse proxy for all sites. Caddy here is the *origin*.
Reverse proxy (origin)	**Caddy** (`caddy.service`, `/etc/caddy/Caddyfile`) on :80/:443 — reaches public via VPS over Tailscale

Field	Value
Mail server	**mailcow** (Docker, `mail.seabee.me`) — recovered 2026-08-03 after network-disconnect fix (see Past issue)
Containers	35 total (26 running, 9 stopped/exited)
Timezone	`Australia/Sydney` (AEST, +1000), NTP active
Locale	`en_AU.UTF-8`
Load avg	0.65 / 0.46 / 0.38 (healthy)
Failed systemd units	**0**

Past issue (FIXED 2026-08-03 12:16): mailcow containers disconnected from their network

Resolved. Documented here so the root cause is known if it recurs.

- **Symptom:** `https://mail.seabee.me/admin/` returned 502 (VPS Caddy → `100.64.0.3:8005` not listening). Postfix & dovecot also down. Whole mail path dead from the public internet.
- **Root cause:** `mailcowdockerized-nginx-mailcow-1` and `mailcowdockerized-postfix-mailcow-1` had become **disconnected from the `mailcowdockerized_mailcow-network` bridge** (`docker inspect ... .NetworkSettings.Networks` was **empty**). With no network attachment:
  - Their `/etc/resolv.conf` pointed at `172.29.1.254` (unbound) but they had no route to it.
  - Docker's embedded DNS (`127.0.0.11`) refused connections (it only works on user-defined networks).
  - nginx looped on `Waiting for PHP...` (`ping: bad address 'php-fpm-mailcow'`); postfix looped on `Waiting for DNS...`.
  - No ports were published → `100.64.0.3:{25,465,587,143,993,4190,8005,8443}` all silent.
  - dovecot had exited (137) in the same episode.
- **Why `docker compose restart` wouldn't have worked:** restart keeps the existing (broken) container object with its empty network set. You must `rm -f` + `up -d` to recreate the container and reattach the network.
- **Fix that was applied:**

```
cd /home/conor/docker/mailcow
docker compose stop nginx-mailcow dovecot-mailcow postfix-mailcow
docker compose rm -f   nginx-mailcow dovecot-mailcow postfix-mailcow
docker rm -f 91321de73b87_mailcowdockerized-dovecot-mailcow-1 2>/dev/null  # stale duplicate
docker compose up -d  nginx-mailcow dovecot-mailcow postfix-mailcow
```

- **Verification:** `ss -tlnp | grep '100.64.0.3' | grep -E ':(25|465|587|993|4190|8005|8443)'` (all 8 listening), `curl -skI https://mail.seabee.me/admin/` → `HTTP/2 200`, `ssh vps 'echo QUIT | nc 203.57.114.42 25'` → `220 mail.seabee.me ESMTP Postcow`.
- **How to spot it next time:** if any mailcow container logs `Waiting for DNS...` / `Waiting for PHP...` / `ping: bad address`, run `docker inspect <name> --format '{{range $k,$v := .NetworkSettings.Networks}}{{$k}} {{end}}'` — empty output means it's disconnected. Recreate it; don't just restart.

Other notes

1. **Root disk 86% full** — monitor; clear logs/cache (`journalctl --vacuum-size=500M`, `docker system prune`) before it hits 100%.
2. `systemd-sslh-generator` **segfaults at boot** (seen in `journalctl -p err`) — harmless generator crash, not user-affecting; file bug upstream if it recurs.
3. `tailscale status` **warns:** "Subnet routing is enabled, but IP forwarding is disabled." If subnet routing is intended, enable `net.ipv4.ip_forward=1` in `/etc/sysctl.d/`.
4. `fail2ban` **and** `ufw` **are enabled as services but status couldn't be read** (sudo needs password in non-interactive shell). Verify manually: `sudo ufw status verbose; sudo fail2ban-client status`. (Same on the VPS.)

Hardware & disks

Block devices

Device	Size	Type	Mount	Notes
`nvme0n1p2`	930 G	NVMe	`/` (ext4)	**OS/root — 86% used**
`nvme0n1p1`	512 M	NVMe	`/boot/efi` (vfat)	EFI
`nvme0n1p3`	977 M	NVMe	(unmounted)	likely recovery/swap-ish
`sda`	9.1 T	HDD	`/mnt/drives/10tb_new`	53% used
`sdc1`	9.1 T	HDD	`/mnt/drives/10tb`	64% used — holds `web_servers/`
`sdb1`	9.1 T	HDD	`/mnt/drives/10c`	44% used — holds `online_videos/`
`sdd1`	3.6 T	HDD	`/mnt/drives/4tb`	51% used
`sde1`	1.9 T	SSD	`/mnt/drives/2tb-ssd`	<1% used (noatime)

- **No mdraid / LVM** (`/proc/mdstat` empty, no vgs/lvs).
- `/swapfile` provides 31 GiB swap (mounted via fstab).
- **fstab** mounts everything by UUID except `/swapfile`. Drives use plain `defaults` (only `2tb-ssd` has `noatime`).
- **SMART couldn't be read** (`smartctl` needs sudo); `smartmontools.service` is running. To check: `sudo smartctl -H /dev/sdX`.

UPS (Network UPS Tools)

- **CyberPower Value2200E** via `usbhid-ups` driver.
- Services: `nut-driver@cyberpower`, `nut-server`, `nut-monitor` (all running).
- Battery: 100%, runtime ~6000s, voltage 26.0V.
- Check status: `upsc cyberpower`. `nut-monitor` will trigger shutdown on low battery.

RGB

- `openrgb-black.service` / `openrgb-off.service` set all RGB to black/off at boot (MS-7D75 motherboard).

Networking

Interfaces

Iface	State	IP	Notes
`enp10s0`	UP	`192.168.4.222/22` + IPv6 (`2401:d002:1805:3800::...`, `fd3b:3257:a88b:1::...`)	Primary LAN
`wlp11s0`	DOWN	—	WiFi off
`tailscale0`	UP	`100.64.0.3/32`	Tailscale, exit node
`docker0`	UP	`172.17.0.1/16`	Default Docker bridge
`br-mailcow`	UP	`172.29.1.1/24`	mailcow network
`br-0225b1b4c4b3`	UP	`172.28.0.1/16`	archivetube_default
`br-8c11a6c3172c`	UP	`172.25.0.1/16`	comfytax_default
`br-a46e8c30ed6b`	UP	`172.22.0.1/16`	forgejo_forgejo
`br-bee2a21d4878`	UP	`172.21.0.1/16`	headscale_default

Iface	State	IP	Notes
`br-b270b9179076`	UP	`172.19.0.1/16`	nextcloud_default
`br-1743ee00f070`	UP	`172.30.0.1/16`	rss-hub_default
`br-1b9242b0d6a7`	UP	`172.23.0.1/16`	tradingjournal_default
`vethN@if2` (×many)	UP	link-local only	container veth pairs

Routes

- Default: `192.168.4.1` via `enp10s0`.
- Direct subnets for each Docker bridge + `192.168.4.0/22`.
- Tailscale traffic handled by `tailscale0` (MagicDNS domain `ts.seabee.me`).

DNS (systemd-resolved)

- Stub listener at `127.0.0.53` and `127.0.0.54:53`.
- Per-link: `enp10s0` → `1.1.1.1` / `1.0.0.1`; `tailscale0` → `100.100.100.100` (MagicDNS, domain `ts.seabee.me ~.`); global fallback `192.168.4.1`, `9.9.9.9`.
- LLMNR enabled on LAN; mDNS off; DNSSEC off.
- `/etc/resolv.conf` is the systemd-resolved stub symlink — **don't edit directly**.

Tailscale fleet

IP	Node	User	OS	State
100.64.0.3	**cbcore** (self)	conor	linux	idle; exit node
100.64.0.2	**vps**	conor	linux	**public reverse proxy (CGNAT bypass); exit node; relay syd**
100.64.0.4	cbfarm	conor	linux	active; exit node; direct
100.64.0.5	rpi3	conor	linux	idle; exit node
100.64.0.6	cbdesktop	conor	linux	—
100.64.0.7	jamies-mac-studio	conor	macOS	—
100.64.0.8	bbb	conor	linux	offline 14d
100.64.0.9	jamievps	jamie	linux	active; exit node
100.64.0.10	localhost	conor	iOS	offline 13d
100.64.0.1	conors-mbp	conor	macOS	offline 1d

IP	Node	User	OS	State
100.64.0.11	jamievps	jamie	linux	(dup name)
100.64.0.12	jamie-desktop	jamie	windows	—

Exit nodes available: cbcore, vps, cbfarm, rpi3, jamievps.

Public exposure: CGNAT + VPS reverse proxy ⚠ important

- This host sits behind **CGNAT** — it has **no directly-reachable public IP** and **no port forwarding** can be configured on the ISP router. Public inbound traffic does **not** reach cbcore directly.
- The **VPS** (Tailscale `100.64.0.2`, node `vps`, a BinaryLane VM in Sydney — public IP `203.57.114.42`, exit node) is the **public-facing reverse proxy** for all services. Public DNS for the seabee.me / conorbriggs.com.au subdomains resolves to the **VPS's public IP**; the VPS terminates TLS (Caddy) for web and forwards TCP (HAProxy) for mail, then both traverse the Tailscale tunnel to cbcore.
- **Traffic flow:**
  - Web/HTTPS: `internet → VPS:443 (Caddy, TLS) → 100.64.0.3:<port> (cbcore origin) → service`
  - Mail: `internet → VPS:25/587/465/993/4190 (HAProxy, raw TCP) → 100.64.0.3:<same port> (mailcow) → container`
- **Diagnostic implication:** if a public site is down, the failure could be on the **VPS** (Caddy/HAProxy/cert/uplink) OR on **cbcore** (origin). Check both:
  1. From the VPS: `curl -sI https://<domain>`, `tailscale ping cbcore` (or `ssh cbcore`), `systemctl status caddy haproxy`.
  2. From cbcore: confirm the backing service is up locally and listening on the Tailscale IP (see playbook below).
  3. Confirm the Tailscale path is healthy: `tailscale status` (both ends active).
- **mailcow** (`mail.seabee.me`) reaches the public via the VPS HAProxy — see the full VPS section below for the port map. **Currently the cbcore side is not listening on those mail ports** (see live issue #1).
- **SSH to cbcore from outside:** only via Tailscale (`ssh conor@cbcore` / `100.64.0.3`), never via public IP. Public-key auth only (see SSH config above). SSH to the VPS itself is on `203.57.114.42:22` (password auth **disabled**, pubkey only, BinaryLane sshd drop-in at `/etc/ssh/sshd_config.d/10-binarylane.conf`).

VPS (public edge) — `vps.seabee.me` / `203.57.114.42`

The VPS is the public-facing edge for everything. This section is a full scan captured **Mon 2026-08-03 12:11 AEST** over SSH (`ssh vps`, Tailscale `100.64.0.2`). **SSH to it to debug the public edge:** `ssh vps`.

At a glance

Field	Value
Hostname	`vps`
Provider	BinaryLane (Sydney) — KVM VM (`std-min`)
OS	Debian GNU/Linux 13 (trixie)
Kernel	6.12.94+deb13-amd64
CPU	1 vCPU (Common KVM Processor v5, Intel)
RAM	**967 MiB total, 814 MiB used, 152 MiB avail — tight** ⚠ no swap
Disk	`/dev/vda1` 20G — 38% used (7G/20G, 12G free)
Public IP	`203.57.114.42/24` on `eth0` (gw `203.57.114.1`)
Tailscale IP	`100.64.0.2` (exit node)
Uptime	30 days
Failed units	0
Packages	562 installed

Networking

- `eth0` — `203.57.114.42/24` (public), DNS `43.229.61.2` / `43.229.62.2` / `8.8.8.8`, search domain `seabee.me`.
- `tailscale0` — `100.64.0.2/32` + `fd7a:115c:a1e0::2`.
- `docker0` — DOWN (172.17.0.1/16, linkdown).
- `br-8b77d98edbcd` — `172.18.0.1/16` (headscale network).
- Tailscale listens UDP `:41641` (direct, not relayed) — direct path to cbcore `125.253.46.252:1194`.

Listening ports (public edge)

Port	Listener	Binds to	Forwards to
22	sshd	`0.0.0.0` + `[::]`	(local, pubkey only)

Port	Listener	Binds to	Forwards to
25	HAProxy `smtp_in`	`203.57.114.42`	`100.64.0.3:25` (cbcore mailcow)
465	HAProxy `smtps_in`	`203.57.114.42`	`100.64.0.3:465`
587	HAProxy `submission_in`	`203.57.114.42`	`100.64.0.3:587`
993	HAProxy `imaps_in`	`203.57.114.42`	`100.64.0.3:993`
4190	HAProxy `sieve_in`	`203.57.114.42`	`100.64.0.3:4190`
80, 443	Caddy	`*` (all)	per-domain (see Caddyfile below)
5355	systemd-resolved LLMNR	`0.0.0.0`	(local)
127.0.0.1:3000	headplane (Docker)	localhost	(headscale admin UI)
127.0.0.1:8080	headscale (Docker)	localhost	(headscale API)
127.0.0.1:9090	headscale (Docker)	localhost	(headscale metrics)
127.0.0.1:2019	Caddy admin API	localhost	(local)
127.0.0.1:61209	glances	localhost	(local)
100.64.0.2:25	postfix	Tailscale	(local MTA, see below)
100.64.0.2:46590	(random)	Tailscale	outbound mail relay ephemeral

Caddy (public reverse proxy) — `/etc/caddy/Caddyfile`

ACME email `letsencrypt@conorbriggs.com.au`. Uses two snippets:

- `(cbcore_proxy)` → `reverse_proxy 100.64.0.3:{args[0]}` (the standard "forward to cbcore over Tailscale" pattern, sets `X-Real-IP` + `X-Forwarded-Proto https`).
- `(cbfarm_proxy)` → `reverse_proxy http://100.64.0.4:81` (unused below).

Domain	Action	Target
`vps.seabee.me`	file_server	`/var/www/vps`
`seabee.me`	file_server	`/var/www/seabee`
`headscale.seabee.me`	split	`/admin*` → `127.0.0.1:3000` (headplane), else `127.0.0.1:8080` (headscale)
`archive.seabee.me`	`import cbcore_proxy 8000`	`100.64.0.3:8000` (cbcore Caddy static)
`comfytax.com.au`	`import cbcore_proxy 7331`	`100.64.0.3:7331` (comfytax container)
`files.seabee.me`	`import cbcore_proxy 8001`	`100.64.0.3:8001`

Domain	Action	Target
`phpma.seabee.me`	`import cbcore_proxy 8002`	`100.64.0.3:8002`
`videos.seabee.me`	`import cbcore_proxy 8075`	`100.64.0.3:8075` (archivetube)
`media.seabee.me`	`import cbcore_proxy 8096`	`100.64.0.3:8096` (jellyfin/plex on cbcore)
`home.seabee.me`	`import cbcore_proxy 8003`	`100.64.0.3:8003`
`rss.seabee.me`	`import cbcore_proxy 8004`	`100.64.0.3:8004` (fusion)
`git.seabee.me`	`import cbcore_proxy 3000`	`100.64.0.3:3000` (forgejo)
`git.farm.seabee.me`	reverse_proxy	`http://100.64.0.4:81` (cbfarm, **not** cbcore)
`mail.seabee.me`	reverse_proxy	`100.64.0.3:8005` (mailcow nginx HTTP) with `Host` + `X-Forwarded-Proto`
`autodiscover.seabee.me`, `autoconfig.seabee.me`	reverse_proxy	`https://100.64.0.3:8443` (mailcow nginx HTTPS, `tls_insecure_skip_verify`)

Note: `mail.seabee.me` on the VPS proxies to `100.64.0.3:8005` (mailcow's own HTTP), NOT via the `cbcore_proxy` snippet. The mailcow HTTPS UI (`:8443`) is only reached via the autodiscover/autoconfig blocks. Currently `100.64.0.3:8005` and `:8443` are **not actually listening** on cbcore (mailcow nginx has no published ports — see live issue #1).

HAProxy (mail TCP passthrough) — `/etc/haproxy/haproxy.cfg`

The VPS does NOT run mailcow. It is a dumb TCP forwarder only — mailcow lives on cbcore (`/home/conor/docker/mailcow`); the VPS just relays the public mail ports to cbcore's Tailscale IP. Mode `tcp`, plain passthrough (no TLS termination on the VPS — mailcow on cbcore does its own TLS). All frontends bind the VPS public IP `203.57.114.42`; backends point at `100.64.0.3` (cbcore) over Tailscale:

Frontend (port)	Backend target	Comment
`smtp_in` (25)	`100.64.0.3:25`	inbound SMTP
`submission_in` (587)	`100.64.0.3:587`	submission (MSA)
`smtps_in` (465)	`100.64.0.3:465`	SMTPS
`imaps_in` (993)	`100.64.0.3:993`	IMAPS
`sieve_in` (4190)	`100.64.0.3:4190`	ManageSieve

The config has a comment: "*add `ssl` to the server lines once the home side is ready*" — i.e. currently no TLS between HAProxy and cbcore (relies on the Tailscale transport being encrypted). Backups: `haproxy.cfg.bak`, `haproxy.cfg.bak.2026-08-01`. **Right now all five backends point at dead**

targets (cbcore mailcow ports not listening — live issue #1), so inbound internet mail is failing at the VPS.

Headscale (on the VPS, Docker)

- Path: `/home/conor/docker/headscale/` (compose `docker-compose.yml`)
- Two containers (both up 4 weeks):
  - `headscale` — `headscale/headscale:0.29.0`, `127.0.0.1:8080->8080`, `127.0.0.1:9090->9090`, healthy
  - `headplane` — `ghcr.io/tale/headplane:0.7.0`, `127.0.0.1:3000->3000`, healthy (admin UI)
- Network: `headscale_headscale-net` (`172.18.0.0/16`)
- Configs: `./headscale/config` (mounted to `/etc/headscale`), `./headscale/lib` (state), `./headplane/config/config.yaml`, `./headplane/lib`
- **Note:** there is ALSO a headscale stack on **cbcore** (`/home/conor/docker/headscale`, headscale 0.28, ports 8107/8109). The VPS one (0.29) is the one exposed publicly via `headscale.seabee.me`. Confirm which is the authoritative control plane before changing either.
- Restart: `ssh vps 'cd /home/conor/docker/headscale && docker compose up -d'`

Postfix (local MTA on the VPS)

- `postfix.service` running, master.cf has `smtp inet n - y - - smtpd` on port 25.
- `postconf -n` returned empty (config mostly defaults). The VPS postfix listens on both `203.57.114.42:25` (public — but HAProxy already owns `203.57.114.42:25`, so there's a **port-25 bind conflict risk**; in practice HAProxy binds first and postfix falls back to `100.64.0.2:25` only — verify with `ss -tlnp | grep :25` on the VPS).
- Likely used as an **outbound relay** for the VPS itself (system mail, fail2ban, unattended-upgrades). Not the primary mail path.

Systemd services (enabled)

caddy, haproxy, docker, containerd, tailscaled, fail2ban, ufw, postfix, glances, ssh, sshd-keygen, apparmor, lm-sensors, systemd-networkd (+wait-online), systemd-resolved, systemd-timesyncd, unattended-upgrades, cloud-init (×4), getty@, grub-common, e2scrub_reap, systemd-pstore, systemd-network-generator.

Timers

apt-daily(+upgrade), dpkg-db-backup, man-db, e2scrub_all, fstrim, **mpanel-memory-graph** (every 5 min — likely a memory graphing helper for a control panel; check `/etc/systemd/system/mpanel-memory-graph.*`).

Users / SSH

- Only one user: `conor` (uid 1000, `/home/conor`, bash).
- sshd: `PermitRootLogin no`, `PasswordAuthentication no`, pubkey only, `ClientAliveInterval 120`. Drop-in: `/etc/ssh/sshd_config.d/10-binarylane.conf`.
- No root crontab, no `/etc/cron.d` entries except `e2scrub_all`.

Web roots

- `/var/www/seabee` — `seabee.me` static site
- `/var/www/vps` — `vps.seabee.me` static site

Security

- `ufw` enabled (status unreadable without sudo — `ssh vps 'sudo ufw status verbose'`).
- `fail2ban` enabled (status unreadable — `ssh vps 'sudo fail2ban-client status'`).
- `unattended-upgrades` enabled (auto security updates).
- No certbot — Caddy handles ACME for all its domains. `/etc/letsencrypt/live/` is empty.

VPS gotchas

- **RAM is tight (152 MiB free, no swap).** If Caddy + HAProxy + Docker headscale + postfix + fail2ban all spike, the OOM killer may fire. Consider adding swap or upsizing the VM. `mpanel-memory-graph.timer` suggests this is already being watched.
- **Port 25 dual-bind:** both HAProxy and postfix are configured for `203.57.114.42:25`. HAProxy should win; postfix ends up on `100.64.0.2:25`. If you ever restart postfix and it fails to bind, that's why.
- **Mail backend currently dead:** every HAProxy mail backend points at `100.64.0.3:<port>` which is not listening on cbcore right now (live issue #1). Fix the cbcore side, not the VPS.
- **Two headscale instances** (VPS 0.29 + cbcore 0.28). Know which one clients join before changing either.
- Backups of `haproxy.cfg` exist (`.bak`, `.bak.2026-08-01`) — the current cfg is the one in use; the `.bak.2026-08-01` is a wider/older variant (diff shows whitespace + extra sections removed).

Networking (cbcore) — listening ports

Listening TCP ports (notable)

Port	Listener	Note
22	sshd	`PermitRootLogin no`, pubkey only
80, 443	Caddy	Reverse proxy for most public sites
111	rpcbind	NFS portmap
139, 445	smbd/nmbd	Samba (SMB)
222	xrdp	(also forgejo git-ssh maps 222→22)
137, 138 (UDP)	nmbd	NetBIOS
2049	nfsd	NFS server
42729, 46141, 46999	(high)	NFS/bluetooth/random
5355	systemd-resolved	LLMNR (TCP+UDP)
8384, 22000	syncthing (conor user)	GUI + sync protocol
21027 (UDP)	syncthing	discovery
3000	forgejo	Caddy proxies `git.conorbriggs.com.au` →3000
3303	(docker host)	—
32400	plexmediaserver	Plex (all interfaces)
32410-32414 (UDP)	plex	Plex discovery/streaming
3389	xrdp	RDP
5201	iperf3?	—
60785, 32600	plex	local
7331	comfytax-app	Caddy block commented; direct
7654	redis (mailcow)	127.0.0.1 only
8000-8003	Caddy (Tailscale-bound)	archive/files/home/phpma static+PHP
8004	rss-hub (fusion)	conflicts with vbox stack
8075	archivetube	—
8090	tradingjournal	127.0.0.1 only, Caddy fronts

Port	Listener	Note
8096	(Tailscale)	—
8100	portmgr	systemd service `/usr/local/bin/portmgr`
8101	nextcloud-app	Caddy fronts `cloud.conorbriggs.com.au`
8102	collabora	Caddy fronts `collabra.conorbriggs.com.au`
8107, 8109	headscale / headscale-ui	Caddy fronts `headscale.conorbriggs.com.au`
8388	shadowsocks-libev	127.0.0.1 only (chacha20-ietf-poly1305 + v2ray-plugin)
9090	(all)	—
9443	portainer	HTTPS UI
10000	webmin	HTTPS (UDP+TCP)
11434	ollama	127.0.0.1 only
13306	mariadb (mailcow)	127.0.0.1 only
3493	nut (UPS)	127.0.0.1
3260	(iSCSI)	open-iscsi enabled
5432	postgresql 15-main	127.0.0.1 (host DB) + `[::1]`
61209	glances	127.0.0.1 server

Firewall

- `ufw.service` **enabled** but status unreadable without sudo. Verify with `sudo ufw status verbose` .
- `fail2ban.service` enabled (active running) — jails unknown without sudo: `sudo fail2ban-client status` .

Systemd services

Enabled & running (64 active, 0 failed)

Web/Proxy/DB: caddy, php8.4-fpm, mariadb (11.8.6), postgresql@15-main **Mail-adjacent (Docker):** (mailcow is in Docker, not host systemd) **Containers/Runtimes:** docker, containerd, podman (+ podman-auto-update, podman-restart) **File sharing:** smbd, nmbd, winbind, samba-ad-

dc, nfs-server, nfs-blkmap, nfs-idmapd, nfs-mountd, nfsdcld, rpcbind, rpc-statd, fsidd **Remote access:** ssh, xrdp, xrdp-sesman **VPN/network:** tailscaled, NetworkManager, NetworkManager-dispatcher, NetworkManager-wait-online, netavark-dhcp-proxy, netavark-firewalld-reload, wpa_supplicant, shadowsocks-libev **Security:** fail2ban, ufw, apparmor, watchdog **Monitoring/ops:** glances, iperf3, portmgr, smartmontools, sysstat, lm-sensors, power-profiles-daemon, udisks2, upower, accounts-daemon, drkonqi-coredump-processor@, systemd-pstore **Virtualization:** libvirtd, libvirt-guests, virtlockd, virtlogd, open-iscsi **Media:** jellyfin, plexmediaserver **AI:** ollama **UPS:** nut-driver@cyberpower, nut-monitor, nut-server, nut-driver-enumerator **Misc:** avahi-daemon, bluetooth, blueman-mechanism, ModemManager, lightdm (display mgr), switcheroo-control, syslog-ng, systemd-resolved, systemd-timesyncd, cron, anacron, grub-common, e2scrub_reap, autofs, getty@tty1, fwupd, polkit, rtkit-daemon, webmin, lvm2-monitor, blk-availability, keyboard-setup, console-setup, nvmefc-boot-connections, nvmf-autoconnect, sshd-keygen

Enabled but NOT running (idle/one-shot)

certbot.timer-driven, openrgb-black/off (one-shot at boot)

Timers (enabled)

phpsessionclean, sysstat-collect/rotate/summary, anacron, apt-daily(+upgrade), certbot, dpkg-db-backup, e2scrub_all, fstrim, fwupd-refresh, logrotate, lynis, mailcow-cert-pull, man-db, mdcheck_*, mdmonitor-oneshot, podman-auto-update

> **Note:** `mailcow-cert-pull.timer` exists on the **host** — a host-side timer pulls certs for mailcow. Check it if mail TLS breaks: `systemctl status mailcow-cert-pull.timer`.

User-level services (conor, uid 1000)

- **syncthing.service** (running, PID 11779) — GUI :8384, sync :22000, discovery :21027 UDP
- pipewire, pipewire-pulse, wireplumber, filter-chain, mpris-proxy, dbus

---

Databases & runtimes (host-installed)

Runtime	Version	Port	Note
MariaDB	11.8.6	host `:5432`? no — host MariaDB listens 127.0.0.1:5432? **Actually**: host `mariadb.service` (system) — but the listening `127.0.0.1:5432` is **PostgreSQL**; MariaDB host port unclear from scan. Container MariaDB (mailcow) → 127.0.0.1:13306.	
PostgreSQL	15 (cluster `15-main`)	127.0.0.1:5432 + `[::1]:5432`	Host PG
PHP-FPM	8.4.21	`/run/php/php-fpm.sock`	Caddy `php_fastcgi` uses this unix socket
Redis	(mailcow container)	127.0.0.1:7654	mailcow only
Ollama	—	127.0.0.1:11434	Local LLM server

> **3316 packages installed** total. Key infra packages: caddy 2.11.4, docker-ce 29.6.0, podman, libvirt 11.3, nfs-kernel-server 2.8.3, nut 2.8.1, samba, fail2ban 1.1.0, tailscale, openrgb, jellyfin 10.11.11, plexmediaserver, glances 4.3.1.

Web servers (static/PHP sites)

Web roots live on the big disk: **`/mnt/drives/10tb/10tb/web_servers/`**

Site dir	Served at	Caddy block	Engine
`home`	`:8003` (Tailscale)	`:8003` bind 100.64.0.3	PHP
`seabee-archive`	`:8000` (Tailscale)	`:8000` bind 100.64.0.3	file_server browse
`conorbriggs-files`	`:8001` (Tailscale)	`:8001` bind 100.64.0.3	file_server browse
`phpma`	`:8002` (Tailscale)	`:8002` bind 100.64.0.3	PHP (phpMyAdmin)
`mx`	`mx.home.conorbriggs.com.au`	public	file_server
`cal/baikal/html`	`cal.conorbriggs.com.au`	public	PHP (Baïkal calendar)
`marketdata`	`marketdata.seabee.me` (redir from .com.au)	public	PHP, SPA fallback, PDF redirects, caches versioned assets
`pdb/bookstack/public`	`pdb.seabee.me` (redir from .com.au)	public	PHP (BookStack/Laravel)

Site dir	Served at	Caddy block	Engine
`test`	`test.conorbriggs.com.au`	public	PHP
`timesheet`	`timesheet.conorbriggs.com.au`	public	PHP
`todo`	`todo.conorbriggs.com.au`	public	PHP
`tradingjournal`	`tradingjournal.seabee.me` (redir from .com.au)	**Docker** 127.0.0.1:8090	Caddy reverse_proxy
(cloud)	`cloud.conorbriggs.com.au`	**Docker** 127.0.0.1:8101	nextcloud
(collabora)	`collabra.conorbriggs.com.au` (typo'd domain)	**Docker** 127.0.0.1:8102	Collabora
(headscale)	`headscale.conorbriggs.com.au`	**Docker** localhost:8107	headscale

Other dirs in `web_servers/` without an active Caddy block: `cloud` (Nextcloud data, served via Docker), `db`, `default`, `myip`, `seabee`, `smtps-archive`, `videos` (block commented out — `videos.conorbriggs.com.au` disabled).

Caddy

- Config: `/etc/caddy/Caddyfile` (single file, no `conf.d/` imports)
- ACME email: `letsencrypt@conorbriggs.com.au`
- Tailscale-bound blocks (`:8000`–`:8003`) use `bind 100.64.0.3`
- **Known boot-race bug (verified Aug 2026):** Caddy fails at boot because `100.64.0.3` isn't up yet. Fix drop-in documented in `/home/conor/Docker/README.md` § Caddy. **Symptom: no sites resolve after reboot → check `ss -tlnp | grep -E ':80 |:443 '`; if silent, `sudo systemctl start caddy`.**
- Reload: `sudo systemctl reload caddy`; validate: `sudo caddy validate --config /etc/caddy/Caddyfile`
- Logs per-site under `/var/log/caddy/*.log`

Domains owned (from AGENTS.md)

- `conorbriggs.com.au` — primary
- `comfytax.com.au`
- `seabee.me` — subdomains: archive, files, git.farm, headscale, home, mail, marketdata, media, pdb, phpma, rss, temp, tradingjournal, videos, vps

---

Docker (summary — full detail in `/home/conor/Docker/README.md`)

- Docker Engine **29.6.0** + containerd v2.2.5 + compose plugin 5.1.4. Also `podman` installed.
- **35 containers** (26 up, 9 stopped). 11 networks, ~90 volumes.
- Compose stacks under `/home/conor/Docker/<stack>/`: **mailcow, nextcloud, forgejo, headscale, comfytax, archivetube, rss-hub, tradingjournal** (note: tradingjournal compose is at `/mnt/drives/10tb/10tb/web_servers/tradingjournal`), **cosmos-server** (not running), **vpn-box** (stopped).
- Standalone: **portainer** (`:9443`, full docker socket — privileged-equivalent).

Running stacks

Stack	Key containers	Host ports
mailcow (~18)	nginx, postfix, dovecot⚠, sogo, rspamd, clamd, mysql, redis, memcached, unbound, acme, watchdog, ofelia, php-fpm, netfilter, dockerapi, olefy, postfix-tlspol	127.0.0.1:13306, 127.0.0.1:7654
nextcloud	app, cron, db(mariadb 11.4), redis, collabora	127.0.0.1:8101, 127.0.0.1:8102
forgejo	forgejo(16.0.1), db(postgres 16)	3000, 222
headscale	headscale(0.28), headscale-ui	8107, 8109
comfytax	app, postgres(17-alpine)	7331
archivetube	app, postgres(16-alpine)	8075
rss-hub	fusion(1.1.1)	8004
tradingjournal	app, mariadb(11)	127.0.0.1:8090
portainer	portainer-ce	9443

Stopped/inactive (don't accidentally restart)

- `stalwart` (v0.16) — mail ports conflict with mailcow; keep stopped.
- `cosmos-server` — wants `100.64.0.3:8443`, same as mailcow nginx; **port conflict**.
- `taxhacker-main-app-1` + `taxhacker-main-postgres-1` — exited ~2 months.
- `vpn-http-proxy` (squid), `vpn-qbittorrent`, `nordvpn`, `vpn-proxy` — stopped 2–4 months.
- `onlyoffice-docs` — exited 5 months; Collabora is active.
- `91321de73b87_...dovecot-mailcow-1` — **stale duplicate, remove**.

Quick Docker commands

```
docker ps -a --format "table {{.Names}}\t{{.Image}}\t{{.Status}}\t{{.Ports}}"
docker inspect <name> --format '{{index .Config.Labels "com.docker.compose.project.working_dir"}}'
docker logs -f <name>
cd /home/conor/Docker/<stack> && docker compose rm -fs <svc> && docker compose up -d <svc>
```

Mail (mailcow) — recovered 2026-08-03 (see Past issue above)

- **Path:** `/home/conor/Docker/mailcow` (compose + `mailcow.conf`)
- **Hostname:** `mail.seabee.me` (ADDITIONAL_SERVER_NAMES same)
- **Intended binds (from `mailcow.conf`):** `HTTP_BIND=100.64.0.3`, `HTTPS_BIND=100.64.0.3`, mail ports `SMTP_PORT=100.64.0.3:25`, `SMTPS_PORT=100.64.0.3:465`, `SUBMISSION_PORT=100.64.0.3:587`, `IMAP_PORT=100.64.0.3:143`, `IMAPS_PORT=100.64.0.3:993`, `SIEVE_PORT=100.64.0.3:4190`.
- `SKIP_LETS_ENCRYPT=y` — certs handled externally; host `mailcow-cert-pull.timer` + `mailcow-cert-expiry-check.sh` cron at 06:30.
- Internal DNS: `unbound-mailcow` (172.22.x.254).
- Webmail: **SOGo** (via mailcow nginx).
- DB: `mariadb:10.11` on `127.0.0.1:13306`; cache: `redis:7.4.6-alpine` on `127.0.0.1:7654`.
- **Public path:** VPS HAProxy `203.57.114.42:{25,587,465,993,4190}` → `100.64.0.3:{...}` (see VPS § HAProxy). VPS Caddy `mail.seabee.me` → `100.64.0.3:8005`; `autodiscover/autoconfig.seabee.me` → `https://100.64.0.3:8443`.

2026-08-03 outage (FIXED) — see "Past issue" in the TL;DR for the full root-cause + fix

Containers that were disconnected from `mailcowdockerized_mailcow-network`: `dovecot-mailcow-1` (Exited 137), `postfix-mailcow-1` (Waiting for DNS, no ports), `nginx-mailcow-1` (Waiting for PHP, no ports). Recreating all three (plus removing stale duplicate `91321de73b87_...`) restored the full mail path. The stale-duplicate symptom from `/home/conor/Docker/README.md` § "Known issue: dovecot crash-loop" was a manifestation of the same network-disconnect problem.

Scheduled jobs (cron + timers)

conor's crontab (`crontab -u conor -l`)

Schedule	Job
`0 5 * * 2-6`	`~/sync/Stuff/Programming/Python/asx_dashboard/run.sh` (market data, Tue–Sat)
`0 4 * * *`	`/home/conor/backup/calendar-db-backup.sh` → `calendar-backup.log`
`30 6 * * *`	`/usr/local/bin/mailcow-cert-expiry-check.sh`
(commented)	jamie crypto update, db backup

/etc/cron.d

`anacron`, `certbot`, `e2scrub_all`, `php` (session clean), `roundcube-core`, `sysstat`

/etc/cron.{daily,weekly,monthly}

`apt-compat`, `dpkg`, `logrotate`, `man-db`, `sysstat`, `brave-browser` (daily); `man-db` (weekly)

systemd timers (key)

`certbot.timer` (daily ~06:16), `apt-daily(-upgrade).timer`, `mailcow-cert-pull.timer` (00:43), `fstrim.timer` (weekly), `e2scrub_all.timer` (Sun), `lynis.timer`, `dpkg-db-backup.timer` (00:00), `podman-auto-update.timer`

Users & groups

Users (uid ≥ 1000)

User	UID	Shell	Home
conor	1000	/bin/bash	/home/conor
ciara	1002	/bin/bash	/home/ciara

User	UID	Shell	Home
guest	1003	/bin/sh	/home/guest
dad	1004	/bin/sh	/home/dad
libvirt-qemu	64055	nologin	/var/lib/libvirt

Groups of note

- `docker:x:991:conor` — conor is in docker group (passwordless docker)
- `nextcloudshare:1001`, `webdata:1003`, `dad:1005`
- No custom sudoers.d entries (only the default README)

SSH

- Port 22, `PermitRootLogin no`, pubkey auth, `KbdInteractiveAuthentication no`, `UsePAM yes`, X11 forwarding on.
- Config dir: `/etc/ssh/sshd_config.d/*.conf` (includes).

Other services & notes

- **NFS:** server enabled, `/etc/exports` has **no active exports** (all commented examples). nfs-kernel-server running but idle.
- **Samba:** `smbd` / `nmbd` / `winbind` / `samba-ad-dc` all running. `testparm` needs sudo to dump config — check `/etc/samba/smb.conf` for shares.
- **Shadowsocks:** `shadowsocks-libev.service` running, 127.0.0.1:8388, `chacha20-ietf-poly1305` + v2ray-plugin (server mode).
- **xrdp:** RDP on :3389 (xrdp + xrdp-sesman).
- **Webmin:** HTTPS on :10000.
- **Plex:** `plexmediaserver.service` on :32400 (all interfaces) + discovery UDP 32410-32414.
- **Jellyfin:** `jellyfin.service` (10.11.11) — port not clearly exposed on host (likely internal/Docker-less; check `jellyfin` config).
- **Ollama:** 127.0.0.1:11434, runs as `ollama` user. PATH in unit includes a crypto venv + nvm node — odd but works.
- **libvirt/QEMU:** enabled; no active VMs seen in scan, but `libvirtd` up.
- **Glances:** web/CLI monitor on 127.0.0.1 (server mode).
- **iperf3:** server running as `iperf3` user.
- **autofs:** enabled (on-demand mounts).
- **OpenRGB:** sets RGB black at boot.

Diagnostic playbook (start here)

"No website works" / sites down

Remember: public traffic goes `internet → VPS Caddy/HAProxy → Tailscale → cbcore (origin) → service`. Isolate the hop:

1. **Is it the VPS edge?** From outside, `curl -sI https://<domain>`. From the VPS: `ssh vps 'systemctl status caddy haproxy; tailscale ping cbcore'`. If the VPS can't reach cbcore, the Tailscale tunnel is the problem, not your services. Check `ssh vps 'sudo journalctl -u caddy -n 50 --no-pager'` for VPS Caddy errors.
2. **Is it cbcore's Caddy (origin)?** `ss -tlnp | grep -E ':80 |:443 '` — if silent, **Caddy is down**. Most likely the Tailscale boot-race: `sudo systemctl start caddy` (see `/home/conor/Docker/README.md` § Caddy known issue).
3. If cbcore Caddy up but one site 502/504 → check the backing container/service: `docker ps | grep <stack>`. Confirm the container is listening on the port the VPS Caddy forwards to (e.g. `100.64.0.3:7331` for comfytax).
4. `sudo journalctl -u caddy -n 50 --no-pager` (cbcore) for bind/proxy errors.
5. DNS check: `resolvectl status`; for a domain: `curl -sI https://<domain>` (do it from the VPS too — public DNS must resolve to `203.57.114.42`).

Mail not delivering / can't log in to webmail

Public path is `internet → VPS HAProxy (203.57.114.42:{25,587,465,993,4190}) → 100.64.0.3:{…} → mailcow`. Check both ends.

1. **From cbcore:** `docker ps | grep mailcow` — look for any `Exited` or `Created`. Then check published ports: `docker inspect mailcowdockerized-postfix-mailcow-1 --format '{{json .NetworkSettings.Ports}}'` — if `{}`, postfix isn't actually reachable (current state — see live issue #1).
2. **Confirm cbcore listens on Tailscale IP:** `ss -tlnp | grep '100.64.0.3' | grep -E ':(25|465|587|993|4190|8005|8443)'`. Empty = mail path broken on the origin.
3. **Logs:** `cd /home/conor/Docker/mailcow && docker compose logs --tail=80 dovecot-mailcow postfix-mailcow unbound-mailcow nginx-mailcow watchdog-mailcow` — look for `Waiting for DNS...` (the current root cause).
4. **From the VPS:** `ssh vps 'ss -tlnp | grep -E ":25|:587|:465|:993|:4190"'` (HAProxy frontends up?), `ssh vps 'nc -w2 100.64.0.3 25'` (backend reachable?). If HAProxy is up but `nc` to cbcore fails, the problem is cbcore, not the VPS.

5. Apply the live-issue-#1 fix (restart unbound, recreate dovecot+postfix+nginx, remove stale duplicate).
6. Certs: `systemctl status mailcow-cert-pull.timer; /usr/local/bin/mailcow-cert-expiry-check.sh`.
7. Watchdog is your friend: `docker logs mailcowdockerized-watchdog-mailcow-1 --tail 30` — it prints per-service health levels.

Disk space

1. `df -h` — root at 86% is the concern.
2. Free: `docker system prune -a --volumes` (careful), `sudo journalctl --vacuum-size=500M`, clear `/tmp`, check `/var/log/caddy/*.log` sizes.
3. Big drives: `du -sh /mnt/drives/*/* 2>/dev/null | sort -h | tail`.

"Container won't start" / weird state

1. `cd /home/conor/Docker/<stack> && docker compose ps` + `docker compose logs --tail=100 <svc>`.
2. Hash-prefixed duplicate container? → `docker rm -f <hash>_<name>`.
3. Network broken? → `docker compose rm -fs <svc> && docker compose up -d <svc>` (recreate, don't just restart).

Can't reach a service on Tailscale IP `100.64.0.3`

1. `ip -4 addr show tailscale0` — confirm `100.64.0.3` present.
2. `tailscale status` — check for "IP forwarding disabled" warning if subnet routing.
3. Service bound to `100.64.0.3` must start **after** tailscaled. Caddy drop-in (see Docker README) addresses this.

Network/ports

1. `ss -tlnp` / `ss -ulnp` for listeners.
2. `sudo ufw status verbose` — firewall rules.
3. `sudo fail2ban-client status` — are you banned?
4. Tailscale ACL/exit node: `tailscale status`.

General "is X healthy?"

```
systemctl --failed                       # any failed units
journalctl -p err --since "-24h" --no-pager  # recent errors
docker ps -a --filter "status=exited"        # dead containers
df -h                                    # disk
free -h                                  # mem
sensors 2>/dev/null                      # temps (lm-sensors)
upsc cyberpower                          # UPS
```

Key file locations

On cbcore (this host)

What	Where
Docker stacks	`/home/conor/Docker/<stack>/` (tradingjournal on `/mnt/drives/10tb/...`)
Docker reference (READ FIRST)	`/home/conor/Docker/README.md`
Caddy config (origin)	`/etc/caddy/Caddyfile`
Caddy logs	`/var/log/caddy/<site>-caddy.log`
Mailcow env	`/home/conor/Docker/mailcow/mailcow.conf`
Web roots (static/PHP)	`/mnt/drives/10tb/10tb/web_servers/<site>/`
PHP-FPM socket	`/run/php/php-fpm.sock`
SSH config	`/etc/ssh/sshd_config` + `/etc/ssh/sshd_config.d/`
Samba config	`/etc/samba/smb.conf`
NFS exports	`/etc/exports` (currently empty)
fstab	`/etc/fstab` (UUID-based)
conor crontab	`crontab -u conor -l`
Tailscale state	`/var/lib/tailscale/`
Backups	`/home/conor/backup/` (calendar-db-backup.sh)
AGENTS.md (opencode)	`/home/conor/.config/opencode/AGENTS.md`

On the VPS (`ssh vps`, `203.57.114.42` / `100.64.0.2`)

What	Where
Caddy config (public edge)	`/etc/caddy/Caddyfile`
HAProxy config (mail TCP)	`/etc/haproxy/haproxy.cfg` (backups `.bak`, `.bak.2026-08-01`)
Headscale stack	`/home/conor/Docker/headscale/docker-compose.yml` (+ `headscale/`, `headplane/` subdirs)
Web roots	`/var/www/seabee` (seabee.me), `/var/www/vps` (vps.seabee.me)
SSH drop-in	`/etc/ssh/sshd_config.d/10-binarylane.conf`
Postfix	`/etc/postfix/{master,main}.cf` (local relay only)
Tailscale	`tailscaled.service` (exit node, direct UDP :41641)

---

*Generated 2026-08-03 by opencode full-system scan of **cbcore** + SSH scan of the **VPS** (`203.57.114.42`). Re-run the scan after major changes (new containers, new sites, disk additions). Update `/home/conor/Docker/README.md` for Docker-specific changes on cbcore; update the VPS § above when the VPS Caddy/HAProxy/headscale config changes.*

Docker

Docker

The authoritative reference is **`/home/conor/Docker/README.md`** — read it before exploring stack directories. This note only points at it and records the conventions.

- Compose stacks: `/home/conor/Docker/<stack>/`
- Host reverse proxy: systemd `caddy.service`, `/etc/caddy/Caddyfile`
- Containers currently include: mailcow (~18), nextcloud + collabora, forgejo, twenty CRM, tradingjournal, comfytax, rss-hub, feishin, strata-poc, qbittorrent + nordvpn, helios rollout.

```
docker ps --format '{{.Names}}\t{{.Image}}\t{{.Status}}'
docker compose -f /home/conor/Docker/<stack>/docker-compose.yml ps
```

Gotchas worth remembering: mailcow serves itself (Caddy does not proxy it), and `mynetworks` must never trust the bridge gateway `172.29.1.1` (see the 2026-08-16 open-relay entry in [[ops-journal]]).

Domains and ports

Domains and ports

Public DNS/TLS terminates on **vps2** (`187.52.126.150` / `100.64.0.16`) as of 2026-11-05, which proxies over Tailscale to **cbcore** (`100.64.0.3`) and **cbfarm** (`100.64.0.4`). It replaced the old **vps** (`203.57.114.42` / `100.64.0.2`); see [[vps2]]. Caddy on cbcore is the origin and binds each site to the Tailscale IP only. Host config: `/etc/caddy/Caddyfile`.

Sites served locally on vps2 (no proxy hop): `headscale.seabee.me` → `:8080` / `/admin` → `:3000`, `marketdata.seabee.me` → `/var/www/marketdata/public` (PHP), `strata360.com.au` → `/var/www/strata360`, `app.strata360.com.au` → `127.0.0.1:3009`, `demo.strata360.com.au` → `127.0.0.1:3011`, `vps.seabee.me` and `seabee.me` → `/var/www/{vps,seabee}`. Mail ports (25/465/587/993/4190) are HAProxy on vps2 → cbcore, still to be cut over.

Local Caddy sites (cbcore)

Port	Site	Root / upstream
8000	archive	`/mnt/drives/10tb/10tb/web_servers/seabee-archive`
8001	files	`/mnt/drives/10tb/10tb/web_servers/conorbriggs-files`
8002	phpma	`/mnt/drives/10tb/10tb/web_servers/phpma`
8003	home	`/mnt/drives/10tb/10tb/web_servers/home`
8006	cal (Baikal CalDAV/CardDAV)	`.../cal/baikal/html`
8007	marketdata	`/mnt/drives/10tb/10tb/web_servers/marketdata`
8008	**pdb (BookStack)**	`.../pdb/bookstack/public`
8009	tradingjournal	Docker `127.0.0.1:8090`
8011	test	`/mnt/drives/10tb/10tb/web_servers/test`

Domains

`conorbriggs.com.au`

- `cloud.conorbriggs.com.au` — Nextcloud + Collabora
- `git.conorbriggs.com.au` — Forgejo
- `headscale.conorbriggs.com.au` — Headscale + web UI
- `comfytax.com.au` — comfytax Next.js app

`seabee.me`

- `mail.seabee.me` — mailcow (serves itself on `100.64.0.3:8005` / `:8443`)
- `pdb.seabee.me` — BookStack ("SeaBee's Personal DB")
- `tradingjournal.seabee.me` — trading journal (redirect from `.conorbriggs.com.au`)
- Other subdomains: archive, files, git.farm, headscale, home, marketdata, media, phpma, rss, temp, videos, vps

Network

- Tailscale: cbcore `100.64.0.3`, VPS `100.64.0.2`.
- CGNAT — **no public inbound ports** at home. VPS is the only public ingress.
- LAN: `192.168.4.222/22` on `enp10s0`, gateway `192.168.4.1`.

Verify before editing: `grep -n "################" /etc/caddy/Caddyfile` and `docker ps --format '{{.Names}}\t{{.Ports}}'`.

machine-config

machine-config

Ansible repo that configures cbcore and the VPS. Clone: `https://git.seabee.me/conor/machine-config.git` → `/home/conor/Documents/machine-config`.

- `inventory/hosts.yml`, `host_vars/cbcore.yml`, `host_vars/vps2.yml`
- `roles/` — haproxy, mail, caddy helpers, etc.
- `run.yml` — main playbook; `playbooks/facts.yml` for host facts
- `docs/` — long-form notes (e.g. `vps2-helios.md`)
- `setup-guide.md`, `commands.md` — how the host was built, common commands

Rule: configuration changes belong in a role and get committed here, not made by hand on the box. Anything done by hand should be back-ported or recorded in [[ops-journal]].

```
cd /home/conor/Documents/machine-config
ansible-playbook run.yml --check --diff   # dry run first
```

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]].

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.

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.