

ThinkServer TS140 Handbook

QCS Server (qcserver.com) — Authoritative Reference

Draft 1 — July 2026

1. Overview

The TS140 is Lenovo ThinkServer hardware, repurposed as a consolidated application host for Quality Car Stereo's business systems. It underwent a major hardware and software overhaul in **December 2025**, moving from a traditional single-disk office server into a tiered-storage, containerized platform. ChatGPT was involved in planning and executing that overhaul; this handbook consolidates and verifies that work, with ongoing support transitioning to Claude.

Administration is primarily via user `lee` (sudo), with a custom **QCS Server Menu** used for day-to-day monitoring and manual backup operations.

2. Hardware & Storage

Physical devices

Device	Model	Size	Type	Role
<code>sda</code>	WDC WDS500G2B0A	G	SATA SSD	OS root, <code>/home</code> , <code>/tmp</code> , swap
<code>sdd</code>	Samsung 870 EVO	G	SATA SSD	<code>/var</code> only
<code>1</code>	Sabrent SB-1342-512	G	NVMe	<code>/srv/fastapps</code> (apps, DB, Docker)
<code>sdb</code>	WDC WD20EZBX	1.8T	HDD	<code>/media/Cloud</code> (Nextcloud data)
<code>sdc</code>	WDC WD20EZBX	1.8T	HDD	<code>/media/iCloudBackup</code> (1.3T) + <code>/media/SystemBackups</code> (563G)

Logical volumes (**think-vg**)

- `root` (23G, on `sda`) — 32% used
- `home` (429.9G, on `sda`) — **only 5.2G actually used** (~1.2%), heavily over-provisioned
- `tmp`, `swap_1` — on `sda`
- `fastapps` (416.9G, on `nvme0n1`) — 66G used / 323G free (17% used)
- `nvme_cache` + `nvme_cache_meta` (55G + 4G, on `nvme0n1`) — **unattached, idle**, leftover from an

abandoned dm-cache plan; superseded by placing apps directly on NVMe

- `var` (9.31G) — historical/retired LVM volume, do-not-mount; `/var` now lives on the dedicated Samsung SSD instead

Storage design principle

Fast solid-state storage (NVMe + SSD) is reserved for the OS, Docker runtime, databases, and all active application code. Mechanical disks are reserved for user-facing bulk data (Nextcloud), backups, and archives. This principle holds true in practice, confirmed by live inspection — see Section 5.

3. Operating System & Software Stack

- **OS:** Debian 12 (Bookworm), kept close to stock; business applications live outside the OS under `/srv/fastapps`
- **Web:** Apache (HTTPS, virtual hosts, reverse proxy where needed)
- **Language runtime:** PHP 8.2
- **Database:** MariaDB 10.11 — data directory bind-mounted from `/srv/fastapps/mysql` into `/var/lib/mysql`, physically on NVMe
- **Cache/session store:** Redis (small footprint, ~4MB, no evictions)
- **Mail:** Postfix + Dovecot (see Section 6)
- **Security:** Fail2Ban + UFW (see Section 8)

Filesystem symlink

`/var/www` is a **symlink** to `/srv/fastapps/www` (confirmed via `ls -ld`, created Dec 12, 2025). This means every vhost's application code physically resides on the NVMe tier, regardless of which path is used to reach it.

4. Caching Strategy (Dec 2025 design, confirmed still accurate)

Layered model, each layer with exactly one responsibility:

```
Browser -> Apache -> PHP OPcache -> Redis -> MariaDB -> Disk
```

- **OPcache** — compiled PHP bytecode, ~2,400 scripts cached, 1.5M+ hits, 128MB allocation
- **Redis** — sessions and transient state only; business data intentionally excluded
- **MariaDB** — authoritative data only, never used as a cache
- **Linux page cache** — left untuned, works naturally since app tree is on SSD/NVMe
- **Storage placement** — the strategy's answer to storage-tier performance was placing

`/srv/fastapps` directly on NVMe, not block-level (dm-cache) caching

Note: The idle `nvme_cache/nvme_cache_meta` LVs (Section 2) fall outside this documented strategy and were most likely an early exploratory step, abandoned once direct NVMe placement was chosen instead.

5. Hosted Applications

Web vhosts (`/srv/fastapps/www`, reached via `/var/www` symlink)

Vhost	Purpose	Status
<code>que_qualitycarstereo_com</code>	Live vTiger CRM (v8.4.0)	Production
<code>cloud_qualitycarstereo_com</code>	Nextcloud (v32.0.1.2)	Production
<code>oldque_qualitycarstereo_com</code>	Prior vTiger version	Retained pending backup validation of <code>que</code> ; slated for removal
<code>stage_qualitycarstereo_com</code>	Staging copy	Retained pending backup validation; slated for removal
<code>crm_qualitycarstereo_com</code>	Unconfirmed — likely a retired install	Purpose to be confirmed before removal
<code>forum_myorigins_net</code> , <code>myorigins_net</code> , <code>fourwindsfoods_com</code> , <code>wiki_qualitycarstereo_com</code> , <code>think_qualitycarstereo_com</code> , <code>tf_qualitycarstereo_com</code> , <code>forms_qualitycarstereo_com</code> , <code>socialmgr_qcsserver_com</code>	Other business web properties	Production

vTiger CRM detail

- Version 8.4.0, patch build `202507009`
- **Two known CVEs remain open** (both require authenticated access) — not yet patched or upgraded
- **CRM is fully WAN-reachable** (UFW allows 80/443 from Anywhere) — this raises real-world risk since the authentication bar is "any valid login from anywhere," not LAN-only
- Inbound mail-to-CRM pipeline (see Section 6) is production-stable

Nextcloud detail

- App code: `/srv/fastapps/www/cloud_qualitycarstereo_com/nextcloud` (NVMe)
- User data (`datadirectory`): `/media/Cloud` (spinning disk, 1.8T, 242G used / 1.5T free)

- Expected to be the largest-growing storage consumer going forward

Docker services (root: `/srv/fastapps/docker`, confirmed via `docker info`)

Stack	Created	Notes
DomainMod	2025-11-02	Data lives outside fastapps — see below
Postiz	2026-01-01	Postgres via bind mount, on NVMe
Graylog	2026-01-16	MongoDB component currently stopped — see Section 7
Formbricks	2026-01-23	Not previously documented; Postgres + Redis, named volumes on NVMe
Portainer	—	Management UI for all stacks; data volume on NVMe

DomainMod exception: both its app code (`/opt/domainmod/app`) and database (`/opt/domainmod/db`, 255M) are bind-mounted to the **root filesystem**, not `/srv/fastapps`. Small footprint, no capacity concern, but it breaks the "apps live outside the OS" design principle and needs explicit confirmation it's covered by backups. **Migration to the fastapps convention is an open task.**

6. Mail Architecture

```
Outbound: Application -> Postfix -> SMTP2GO -> Internet
Inbound:  Internet -> Postfix -> Maildir -> Dovecot -> vTiger MailScanner -> vTiger
```

- Fully validated, production-stable pipeline
- Confirmed workflow: external reply -> mailbox -> scan -> CRM record attachment (Lead/Contact linkage)
- The historical "Scanning Failed" error is fully resolved
- MailScanner runs via `vtigercron.sh` on a 5-minute cadence under `www-data`

7. Known Operational Issues

- **Graylog MongoDB (`graylog-mongodb-1`) has been stopped since 2026-04-10** — confirmed via logs to be a clean, deliberate shutdown (exit code 0), not a crash. Graylog itself has been running in a degraded/unhealthy state since. Left stopped intentionally for now; a proper, careful restart is an open task rather than an emergency fix.
 - **`graylog-datanode-1`** showed a very recent restart at time of inspection — worth confirming during the Graylog fix whether this is a one-off or a recurring pattern.
-

8. Security & Network Access

Firewall (UFW)

- Active, default-deny incoming
- Explicit allows: 22 (SSH), 10000 (Webmin), 80/tcp, 443, 3388, 25 (SMTP) — both IPv4 and IPv6

Fail2Ban

Five active jails: `apache-auth`, `apache-badbots`, `apache-noscript`, `nextcloud`, `sshd`

Access model — tunnel-only administration

All internal management interfaces are reached exclusively via **SSH tunnel from WAN**, never exposed directly:

- Cockpit, Graylog, DomainMod, phpMyAdmin, router admin, Webmin, Portainer

This explains several apparent inconsistencies resolved during review:

- **sshd listens only on port 22.** Port 3388 (allowed in UFW) has no listener on the host — WAN access via 3388 is understood to be a router-level NAT/port-forward to 22, not a second host-side service.
- **Webmin (port 10000)** is bound to `127.0.0.1` only. It's reachable at `https://127.0.0.1:10000` only after establishing a tunnel/shell session — the UFW rule permitting 10000 inbound is not exploitable externally since nothing listens on any public-facing interface.
- The exact client-side tunnel configuration (e.g., saved PuTTY session details) is not currently documented and should be captured at some point for continuity.

Discourse

Fully decommissioned — no containers, images, or volumes remain.

9. Backups

Current state: manual, not automated. This was a deliberate choice, so each backup's success or failure can be observed directly rather than trusting unattended automation. Operated via the QCS Server Menu and associated helper scripts.

Known gaps to validate:

- Coverage for the Docker services (Formbricks, Graylog, Portainer, Postiz, DomainMod) is unconfirmed — the backup routine may predate their existence
- DomainMod's off-convention location (`/opt/domainmod`, root filesystem) needs explicit confirmation of coverage

- Purpose and contents of `/srv/backups` (a separate top-level directory from `fastapps`, owned by `lee`) not yet reviewed
 - **No documented restore test has been performed** — this remains the single largest unvalidated risk in the environment
-

10. Open Tasks (prioritized)

Higher priority (real-world exposure):

1. **vTiger CVE remediation/mitigation** — WAN-facing CRM with two known open CVEs; decide between upgrade path and interim mitigations (2FA if supported, credential audit, Fail2Ban verification on `apache-auth`)

Routine housekeeping (no active exposure):

2. Reclaim idle `nvme_cache/nvme_cache_meta` LVs (~59G on NVMe)
 3. Review/right-size `/home` (429.9G allocated, 5.2G used)
 4. Perform and document a controlled restore test
 5. Properly restart `graylog-mongodb-1` (currently safely stopped)
 6. Migrate DomainMod (app + db) from `/opt/domainmod` into the `/srv/fastapps` convention
 7. Validate and build out backup coverage — Docker stacks, DomainMod, and confirm `/srv/backups` purpose
 8. Remove retired vTiger installs (`oldque_qualitycarstereo_com`, `stage_qualitycarstereo_com`, and confirm/retire `crm_qualitycarstereo_com`) — tied to task 7, only after live site backup is validated
 9. Clean up orphaned UFW rules (3388, 10000) once router-side forwarding is confirmed — cosmetic, not a security fix
 10. Maintain a cron-job inventory; confirm logrotate coverage for custom app/backup logs
 11. Review and remove obsolete/transitional user accounts
 12. Document the client-side SSH tunnel configuration for continuity
-

11. Document Notes

This handbook consolidates and reconciles four source documents (original architecture brief, storage layout assessment, caching strategy, and a second filesystem/hardware baseline) against live, hands-on verification performed July 2026. Every claim in Sections 2–8 has been cross-checked against actual command output on the box; discrepancies between the original documentation and live findings have been resolved in favor of live evidence, with both noted where relevant.

Draft 1 — subject to revision as open tasks are completed and further details (e.g., DomainMod migration outcome, backup validation results) become available.