



How I build a LAMP VPS

Every decision below has a reason next to it. Server one is built this way by hand; from server two onward it comes out of an Ansible playbook, so every server is identical.

01 ACCESS & BASE

SSH keys only, root login off

Password auth is how VPSes get owned. fail2ban on top.

Default-deny firewall

80, 443 and SSH open. Nothing else, including the DB port.

Unattended security updates

Security patches apply themselves; feature upgrades never do.

Separate deploy user, sudo logged

So an audit can answer “who changed what, when”.

02 WEB & TLS

TLS 1.2+ only, modern ciphers

Server tokens off. Security headers set at the vhost.

Let's Encrypt with renewal tested

Installed is not the same as renewing. I force one renewal.

PHP-FPM pool sized to actual RAM

Defaults will happily swap the box to death under load.

03 PHP

php.ini tuned to the app, not a template

memory_limit, upload and post sizes, execution time.

OPcache sized to the codebase

Undersized OPcache silently thrashes and nobody notices.

Only the extensions the app needs

Smaller surface, faster startup, fewer CVEs to chase.

04 MARIADB

Bound to localhost by default

Remote access over an SSH tunnel, never open to the world.

innodb_buffer_pool sized to the box

The single tuning knob that matters most on a LAMP VPS.

Slow query log on from day one

You cannot fix “the site feels slow” without it.

One least-privilege user per app

No shared root credentials between client projects.

05 BACKUPS

Nightly database, weekly full, offsite

A backup on the same VPS is not a backup.

Restore tested before handover

An untested backup is a guess. I restore one and show you.

Retention agreed in writing

So “how far back can we go?” has an answer before it is asked.

06 MONITORING & HANDOVER

Disk, memory and service checks

Alerting before the client notices, not after they call you.

Log rotation configured

Full disks from unrotated logs are a top-three outage cause.

One-page runbook per server

What is where, how to restart it, where backups live.

FROM SERVER TWO ONWARD

The standard above becomes a playbook. Server two takes about twenty minutes, and every server after it is identical — which is what makes them supportable two years later.

```
roles/ base-hardening/ webserver/ php-fpm/ mariadb/ backups/ monitoring/  
host_vars/ client-a.yml client-b.yml # only the differences live here
```