SERVERE & VPS

Ghid Administrare Servere VPS

Linux, nginx, SSL, PM2, MySQL, firewall și Docker — manual practic pentru antreprenori români cu server propriu

~38 pagini · 28 min citire · PDF A4

Ai cumpărat un VPS pentru site, aplicație Node.js sau magazin online și te confrunți cu SSH, nginx, certificate SSL expirate sau servicii care cad noaptea? Acest ghid traduce administrarea serverelor în pași clari, fără presupuneri de experiență sysadmin. Este orientat spre proprietari de afaceri mici și medii din România care vor control și costuri predictibile, dar au nevoie de proceduri sigure pentru producție.

Cuprins

1 VPS vs shared hosting — când merită upgrade-ul

Un VPS (Virtual Private Server) îți oferă resurse garantate, root access și libertatea de a rula orice stack software. Shared hosting e mai simplu, dar limitează PHP, interzice unele porturi și pune zeci de site-uri pe același IP. Treci la VPS când ai nevoie de Node.js, Redis, cron jobs complexe sau când shared-ul devine lent la trafic crescut.

- Shared: 5–15€/lună, zero administrare, limitat la PHP/MySQL, ideal sub 10.000 vizite/lună
- VPS entry (Hetzner, DigitalOcean, Contabo): 5–20€/lună, 2GB RAM, administrare de tine sau partener
- VPS managed: 40–100€/lună, providerul se ocupă de OS updates și securitate de bază
- Semnale de upgrade: timeout-uri frecvente, CPU throttling, interzicere Redis/Node de host
- VPS în EU (Frankfurt, Helsinki, București): GDPR compliant, latenta mică pentru RO
- Calculează TCO: VPS ieftin + 2h/lună admin vs managed — uneori managed e mai ieftin total

2 Bazele Linux pentru administratori începători

Majoritatea VPS-urilor rulează Ubuntu LTS sau Debian. Nu trebuie să devii expert Linux, dar 15 comenzi esențiale îți permit să navighezi, editezi fișiere, verifici log-uri și repornești servicii fără panică.

1. Conectează-te prin SSH din terminal (Windows: PowerShell sau PuTTY).
2. Rulează sudo apt update && sudo apt upgrade -y — prima acțiune pe VPS nou.
3. Creează user non-root cu sudo: adduser deploy && usermod -aG sudo deploy.
4. Dezactivează login root prin parolă în /etc/ssh/sshd_config.

- ssh user@IP — conectare securizată; folosește chei SSH, nu parolă
- cd, ls, pwd — navigare directoare; ls -la arată permisiuni și fișiere ascunse
- nano /etc/nginx/sites-available/site.conf — editor simplu pentru configurări
- systemctl status nginx / restart nginx — verifică și repornește servicii
- journalctl -u nginx -f — log-uri live ale unui serviciu systemd
- df -h și free -m — spațiu disk și memorie RAM disponibilă

3 Securitate SSH — prima linie de apărare

Portul 22 este scanat continuu de botnet-uri. Un VPS cu root + parolă slabă e compromis în medie sub 24 de ore. Securizarea SSH este primul pas obligatoriu imediat după crearea serverului.

1. Pe PC local: ssh-keygen -t ed25519 -C "email@firma.ro".
2. Copiază cheia publică: ssh-copy-id -p 22 deploy@IP_SERVER.
3. Testează login cu cheie ÎNAINTE de a dezactiva parola.
4. Instalează fail2ban: sudo apt install fail2ban -y && sudo systemctl enable fail2ban.

- Dezactivează autentificarea cu parolă: PasswordAuthentication no în sshd_config
- Folosește chei SSH ed25519 — mai sigure și rapide decât RSA 4096
- Schimbă portul SSH de la 22 la un port > 1024 (ex. 2222) — reduce zgomotul botnet
- Fail2ban: blochează IP-uri după 3–5 încercări eșuate de login
- Permite doar useri specifici: AllowUsers deploy în sshd_config
- Dezactivează login root direct: PermitRootLogin no

4 Configurare nginx — site rapid și sigur

nginx servește site-ul tău static, face reverse proxy către Node.js și termină SSL. O configurare corectă include gzip, cache headers, limitare upload și protecție împotriva fișierelor sensibile.

1. sudo apt install nginx -y && sudo systemctl enable nginx.
2. Creează fișier site în sites-available, activează cu ln -s.
3. Testează config: sudo nginx -t — OBLIGATORIU înainte de reload.
4. sudo systemctl reload nginx — aplică fără downtime.

- Structură: /etc/nginx/sites-available/domeniu.ro + symlink în sites-enabled/
- server_name domeniu.ro www.domeniu.ro; redirect www → non-www sau invers, consistent
- root /var/www/domeniu.ro/public; index index.html index.php;
- location / { try_files $uri $uri/ /index.php?$args; } pentru WordPress
- client_max_body_size 64M; — permite upload imagini mari
- gzip on; gzip_types text/css application/javascript image/svg+xml;

5 SSL și Let's Encrypt — HTTPS gratuit

Certificatul SSL nu e opțional: Google penalizează site-urile HTTP, browserele afișează „Not Secure”, iar formularele de contact pierd încredere. Let's Encrypt oferă certificate gratuite, reînnoite automat cu Certbot.

1. Asigură-te că DNS A record pointează la IP-ul VPS (propagare 1–24h).
2. Instalează certbot: sudo apt install certbot python3-certbot-nginx.
3. Rulează certbot --nginx și alege redirect HTTP→HTTPS.
4. Verifică pe ssllabs.com/ssltest — țintă rating A sau A+.

- Certbot + plugin nginx: sudo certbot --nginx -d domeniu.ro -d www.domeniu.ro
- Reînnoire automată: certbot renew rulează via cron/systemd timer — verifică cu certbot renew --dry-run
- Certificat expiră la 90 zile — reînnoirea automată trebuie testată lunar
- HSTS header opțional după 30 zile HTTPS stabil: add_header Strict-Transport-Security "max-age=31536000";
- Mixed content (imagini HTTP pe site HTTPS) strică lacătul verde — corectează URL-uri
- Wildcard SSL (*.domeniu.ro) necesită DNS challenge — util pentru subdomenii multiple

6 PM2 și aplicații Node.js în producție

Node.js pe VPS nu rulează direct în terminal — ai nevoie de un process manager care repornește aplicația la crash, la reboot server și gestionează log-urile. PM2 este standardul pentru aplicații Next.js, Express și API-uri.

1. Clone repo în /var/www/app && npm ci --production=false.
2. npm run build && pm2 start npm --name app -- start.
3. Configurează nginx reverse proxy către portul 3000.
4. pm2 startup systemd && pm2 save.

- Instalare globală: npm install -g pm2
- Start app: pm2 start npm --name "site" -- start (Next.js) sau pm2 start server.js
- pm2 startup + pm2 save — supraviețuire la reboot server
- pm2 logs site — log-uri live; pm2 monit — CPU/RAM per proces
- Zero-downtime deploy: pm2 reload site după git pull + npm run build
- Variabile mediu în ecosystem.config.js — nu hardcoda secrete în cod

7 MySQL / MariaDB — bază de date pe VPS

WordPress, WooCommerce și multe aplicații PHP folosesc MySQL sau MariaDB. Pe VPS, baza de date rulează local — performanță bună, dar tu ești responsabil de backup și securitate.

1. sudo mysql -e "CREATE DATABASE site_db CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;"
2. Creează user: CREATE USER 'site'@'localhost' IDENTIFIED BY 'parola_puternica';
3. GRANT ALL ON site_db.* TO 'site'@'localhost'; FLUSH PRIVILEGES;
4. Testează conexiunea din wp-config.php sau .env.

- Instalare: sudo apt install mariadb-server -y && sudo mysql_secure_installation
- Creează user dedicat per aplicație — nu folosi root pentru WordPress
- Bind doar localhost: bind-address = 127.0.0.1 în /etc/mysql/mariadb.conf.d/50-server.cnf
- Backup zilnic: mysqldump -u user -p baza > backup.sql — automatizează cu cron
- Monitorizare: verifică slow query log pentru query-uri > 2 secunde
- InnoDB buffer pool: setează la 50–70% din RAM disponibilă pe server dedicat DB

8 Backup-uri server — fișiere, DB, configurații

Pe VPS, nu există buton „restore” la provider (cu excepția snapshot-urilor plătite). Backup-ul tău trebuie să acopere cod, uploads, baza de date și fișierele de configurare nginx/SSL.

1. Instalează restic: configurare repo B2/S3, parolă puternică stocată în password manager.
2. Cron: 0 3 * * * /root/backup.sh >> /var/log/backup.log 2>&1.
3. Verifică dimensiunea backup-ului săptămânal — creșteri bruște pot indica probleme.

- Snapshot VPS (Hetzner/DO): săptămânal, retenție 4 snapshot-uri — rollback rapid
- Backup off-site zilnic: rclone către Backblaze B2, AWS S3 sau Google Drive
- Include: /var/www/, /etc/nginx/, /etc/letsencrypt/, dump MySQL
- Script cron unificat: backup.sh la 03:00, log + notificare email/Telegram la eșec
- Criptează backup-urile cu date clienți: gpg sau restic cu parolă
- Test restore trimestrial pe VPS de test — nu aștepta disaster real

9 Monitorizare uptime și resurse

Site-ul poate cădea la 3 dimineața fără să știi — Google pierde indexare, clienții comandă de la concurență. Monitorizarea proactivă costă 0–10€/lună și îți trimite alertă înainte ca clienții să sune.

- UptimeRobot gratuit: monitor HTTP la 5 min, alertă email/SMS/Telegram
- Healthchecks.io pentru cron jobs — verifică că backup-ul chiar rulează
- Netdata sau htop: CPU, RAM, disk I/O în timp real pe server
- Alerte disk > 80% — log-urile și backup-urile umplu SSD-ul rapid
- Log rotation: logrotate configurat pentru nginx, PM2, aplicație
- Status page public (opțional): status.domeniu.ro pentru transparență clienți B2B

10 Firewall UFW — porturi deschise minim

În mod implicit, un VPS expune toate porturile. UFW (Uncomplicated Firewall) blochează tot traficul neautorizat, permițând doar SSH, HTTP, HTTPS și porturile strict necesare.

1. Configurează regulile UFW ÎNAINTE de a activa firewall-ul.
2. Păstrează consola web provider deschisă ca backup.
3. sudo ufw enable — confirmă.
4. Testează SSH și site-ul imediat după activare.

- sudo ufw default deny incoming && sudo ufw default allow outgoing
- sudo ufw allow 2222/tcp (SSH pe port custom) — ÎNAINTE de ufw enable!
- sudo ufw allow 'Nginx Full' — deschide 80 și 443
- Nu expune MySQL (3306) sau Redis (6379) public — doar localhost
- sudo ufw enable && sudo ufw status verbose — verifică regulile active
- Fail2ban + UFW: dublă protecție împotriva brute force

11 Docker — introducere pentru deploy simplificat

Docker containerizează aplicația cu toate dependențele — același mediu pe laptop, staging și producție. Nu e obligatoriu pentru un singur site WordPress, dar simplifică deploy-ul aplicațiilor Node.js, microservicii și stack-uri complexe.

- Instalare: curl -fsSL https://get.docker.com | sh && sudo usermod -aG docker deploy
- Docker Compose: definește app + nginx + db în docker-compose.yml
- Imagini oficiale: node:20-alpine, nginx:alpine, mariadb:11 — mai mici, mai sigure
- Volume persistente pentru date DB și uploads — nu pierde date la recreare container
- docker compose up -d — start în background; docker compose logs -f — debug
- Actualizări: docker compose pull && docker compose up -d — zero-downtime cu health checks

12 Troubleshooting — probleme frecvente și soluții

Când site-ul cade, ordinea diagnosticului contează: verifică dacă serverul răspunde, apoi nginx, apoi aplicația, apoi baza de date. Panica și restart-ul aleatoriu agravează uneori problema.

1. 1. Ping IP server — răspunde?
2. 2. curl -I https://domeniu.ro — ce status code?
3. 3. sudo nginx -t && sudo systemctl status nginx.
4. 4. pm2 status / systemctl status php8.2-fpm.
5. 5. sudo tail -50 /var/log/nginx/error.log.
6. 6. Dacă totul eșuează: restore din ultimul snapshot/backup.

- 502 Bad Gateway: aplicația Node/PHP nu rulează — pm2 status sau systemctl status php8.2-fpm
- 504 Gateway Timeout: query DB lent sau app blocată — verifică slow log MySQL
- Certificat expirat: sudo certbot renew --force-renewal && nginx reload
- Disk full: df -h, șterge log-uri vechi, curăță /tmp, mută backup-uri off-site
- Site lent brusc: htop — proces zombie? atac DDoS? plugin WP nou?
- Nu te poți conecta SSH: consolă web provider, verifică UFW și fail2ban

Întrebări frecvente

Cât RAM am nevoie pe VPS pentru WordPress + WooCommerce?

Minimum 2GB RAM pentru magazin mic (< 100 produse, < 5.000 vizite/lună). Recomandat 4GB pentru trafic mediu sau cu Redis object cache. Sub 2GB, MySQL și PHP-FPM intră în swap și site-ul devine imposibil de navigat.

Pot administra VPS-ul singur sau e obligatoriu un sysadmin?

Poți gestiona un VPS simplu (1 site WordPress sau 1 app Node) după acest ghid, cu 2–4 ore setup inițial și 1–2 ore/lună mentenanță. Pentru producție critică (magazin cu venituri mari, date sensibile), recomandăm fie managed VPS, fie contract mentenanță cu specialist — costul downtime-ului depășește rapid economia DIY.

Ce provider VPS recomandați pentru România?

Hetzner (Frankfurt/Nuremberg) — cel mai bun raport preț/performanță în EU. DigitalOcean pentru documentație excelentă și marketplace apps. Contabo pentru buget mic (atenție la CPU shared). Alege locație EU pentru GDPR și latenta sub 30ms din București.

Implementare completă

Site + SEO + Google Ads + Mentenanță
Audit gratuit · Demo site gratuit · Răspuns în 24h

valcode.dev/contact

+40 750 205 515 · contact@valcode.dev