

## # VPS Apps – Updated Overview

### ## Current Apps (what's running where)

#### #### FreePaper (Flask/Gunicorn)

- **Domain**: daneshmehr.org → Nginx → Gunicorn on 127.0.0.1:8000
- **Certs**: Let's Encrypt on the box
- **Notes**: Runs as root (⚠️), no systemd unit for Gunicorn, UFW inactive

---

#### #### Kerit (Node/PM2)

- **Domains**: kerit.com.ru, www.kerit.com.ru → Nginx → 127.0.0.1:3001
- **Extra Listener**: webhook on 127.0.0.1:3002 (PM2) for auto deploys
- **DB**: PostgreSQL `kerit\_db` / role `kerit\_user` (creds in `.env`)
- **Process**: Runs as non-root user `kerit`, PM2 cluster mode
- **TLS**: Certbot-managed
- **Notes**: UFW inactive

---

#### #### SmartCover (Node/PM2)

- **Domain**: smartcover.kerit.com.ru → Nginx → localhost:3004
- **TLS**: Behind Cloudflare (SSL offloaded)
- **DB**: `smartcover\_db` / `smartcover\_user` (with Gemini API key in `.env`)
- **Process**: PM2 single instance
- **Extra Settings**: `app.set('trust proxy', 1)`, `cookie sameSite:'lax'`
- **Notes**: Cloudflare proxy considerations

---

#### #### TrustLine (Node/PM2)

- **Domain**: trustline.chat → Nginx → 127.0.0.1:3003
- **DB**: None (in-memory store)
- **Process**: Runs as `trustline` user, PM2 cluster (1 instance)
- **TLS**: Certbot-managed

---

#### #### TopTeachers (Node/PM2)

- **Domain**: topteachers.online → Nginx → 127.0.0.1:3005
- **Process**: Runs as `topteachers` user, PM2 single instance
- **DB**: PostgreSQL `topteachers\_db` / role `topteachers\_user`
- **Provision**: Script creates user, DB, PM2 config, Nginx site, Certbot certs

---

### ### PartnerSystems (Node/React/PM2) \*New\*

- **Domain**: partnersystems.online, www.partnersystems.online → Nginx → 127.0.0.1:3006
- **Process**: Runs as dedicated `partnersystems` user, PM2 cluster mode (1 instance)
- **DB**: PostgreSQL `partnersystems\_db` / role `partnersystems\_user`
- **Env file**:
  - `PORT=3006`
- - `DATABASE\_URL=postgresql://partnersystems\_user:<password>@localhost:5432/partnersystems\_db`
  - `SESSION\_SECRET=<secret>`
- **Logs**: Stored in `/home/partnersystems/logs/` (`partnersystems.log`, `partnersystems-error.log`, `partnersystems-out.log`)
- **TLS**: Let's Encrypt via Certbot (Nginx integration)
- **Security**: Dedicated non-root user, isolated home directory, `.env` chmod 600
- **Nginx Config**: Redirects 80→443, proxies to 127.0.0.1:3006, with security headers & gzip
- **Special Notes**:
  - Ensure Cloudflare proxy (if enabled) is gray-cloud during cert issuance, then switch to "Full (strict)"
  - Uses strict Content Security Policy, gzip caching, and static assets caching (1 year immutable)

---

### ## Conflict-Prevention Checklist for New Apps

#### 1. **Reverse Proxy & Domains**

- Ensure unique `server\_name` in `/etc/nginx/sites-available/`.
- Always redirect HTTP→HTTPS.

#### 2. **App Ports**

- Currently in use: 8000, 3001, 3002, 3003, 3004, 3005, 3006.
- Pick a new unused port for future apps (e.g., 3007+).

#### 3. **Users & Processes**

- Each app runs as a dedicated non-root user with PM2/systemd.
- Keep logs per-app, avoid mixing users.

#### 4. **PostgreSQL**

- Each app has its own DB and user (`kerit\_db`, `smartcover\_db`, `topteachers\_db`, `partnersystems\_db`).
- Only localhost access.

## 5. **\*\*Security\*\***

- Let's Encrypt certs handled via Certbot, or Cloudflare offload where noted.
- UFW still inactive (consider enabling with `OpenSSH` and `Nginx Full` rules).

## 6. **\*\*Deployment Notes\*\***

- Kerit has webhook auto-deploy.
- PartnerSystems uses build pipeline (`npm run build` + `db:push`).
- Always run migrations per-app, not globally.

---