

Container Architecture

Container Architecture

The Flora Family homelab relies on a standardized Docker deployment pattern to ensure security, portability, and ease of management.

☐☐ Directory Layout

To maintain a clean separation between configuration and state, Terra uses two primary directories:

- **/srv/[service-name]/**: Contains `docker-compose.yaml` and `.env` files.
 - *Ownership*: `root:root` (Modified only via `sudo`).
 - *Permissions*: folders `755`, configs `644`, `.env` `600`.
- **/main/appdata/[service-name]/**: Contains persistent application data.
 - *Ownership*: Mapped to the specific service account (UID/GID).
 - *Permissions*: `755` (folders) / `644` (files) generally.

☐☐ Deployment Standards

☐☐ Non-Root Execution

Every service is configured to run as a non-privileged user, with the specific exceptions of **Watchtower** and **Beszel Agent** (which require root/host socket access to monitor system health and container status).

Non-root execution is achieved through one of three methods:

1. **Standard `user:` flag**: For images that support it (e.g., `user: "51100:61100"`).
2. **Environment Variables**: Many linuxserver.io images use `PUID`/`PGID` variables.
3. **Custom Dockerfile Builds**: Used for "scratch" images or minimalist images (like OpenWebUI and SearXNG) to manually inject the desired UID/GID and install local CA

certificates.

☐☐ Shared Infrastructure

Common backend services are standardized to simplify inter-container networking and permissions:

- **Postgres:** Standardized on GID `70` across all instances (Immich, n8n, etc.).
- **Redis/Valkey:** Standardized on GID `970` for caching and session management.
- **Shared Identities:** The `node-user` (UID 1000) is shared between several JS-based apps (n8n, Uptime Kuma) where common file access is required.

☐☐ Lifecycle Management

- **Updates:** Managed by **Watchtower**, configured to run every Sunday at 04:00 AM.
- **Image Tagging:**
 - *Pinned:* Databases and critical infrastructure (e.g., `postgres:18`) to prevent breaking updates.
 - *Floating:* Application layers (e.g., `sonarr:latest`) to receive automated security patches.

Revision #2

Created 2026-02-09 16:06:44 UTC by Chris

Updated 2026-02-09 16:10:40 UTC by Chris