

h08-utilities

- [00-chapter-intro.md](#)
- [01-guacamole.md](#)
- [02-filebrowser.md](#)
- [03-kiwix.md](#)
- [04-drawio.md](#)
- [05-it-tools.md](#)
- [06-pairdrop.md](#)
- [07-convertx.md](#)
- [08-minuspod.md](#)
- [09-docker-proxy.md](#)

00-chapter-intro.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page:
Chapter Introduction tags:
[utilities, tools, remote-access, file-
management]

Overview

This chapter covers general-purpose utility services — remote access, file management, offline content, productivity tooling, and infrastructure support containers.

Services in This Chapter

Service	Container(s)	Purpose
Guacamole	guacamole , guacd , guacamole_db	Clientless remote desktop gateway
FileBrowser	filebrowser	Web-based file manager
Kiwix	kiwix	Offline Wikipedia and ZIM content
Draw.io	drawio	Self-hosted diagram editor
IT Tools	it-tools	Developer and IT utility collection
PairDrop	pairdrop	LAN file sharing (AirDrop-like)
ConvertX	convertx	File format converter
MinusPod	minuspod	AI-powered podcast manager and transcriber

Service	Container(s)	Purpose
Docker Proxy	<code>dockerproxy</code>	Read-only Docker socket proxy

Last Updated: 2026-06-17

01-guacamole.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page: Apache
Guacamole tags: [guacamole,
remote-desktop, rdp, vnc, ssh,
authentik, postgres]

Overview

Apache Guacamole is a clientless remote desktop gateway. It provides browser-based access to RDP, VNC, SSH, and Telnet sessions with no client software required. Authentication is via Authentik OpenID Connect (native Guacamole extension — not Traefik ForwardAuth). The stack is three containers: the web application, the `guacd` native protocol daemon, and PostgreSQL 15 for connection and user data.

Access

Type	URL	Auth
External	<code>https://guac.jeeves5454.ddns.net</code>	Authentik OIDC + GeoBlock + CrowdSec
Internal	<code>https://guac.home.local</code>	Authentik OIDC (Step-CA TLS)

Guacamole uses its built-in `openid` extension with `EXTENSION_PRIORITY=openid` to handle the Authentik OIDC flow directly. Traefik does not apply `authentik-auth@docker` ForwardAuth.

Containers

Container	Image	Role
guacamole	guacamole/guacamole:latest	Web application (Tomcat/Java)
guacd	guacamole/guacd:latest	Native protocol daemon (RDP/VNC/SSH)
guacamole_db	postgres:15-alpine	PostgreSQL database

guacamole (application)

Runtime: Apache Tomcat / Java. WEBAPP_CONTEXT=R00T serves the app at / rather than /guacamole.

Key environment variables:

Variable	Value / Notes
GUACD_HOSTNAME	guacd
POSTGRESQL_HOSTNAME	postgres (internal alias for guacamole_db)
POSTGRESQL_DATABASE	guacamole_db
POSTGRESQL_USER	guacamole_user
POSTGRESQL_PASSWORD	REDACTED
WEBAPP_CONTEXT	R00T
EXTENSION_PRIORITY	openid
OPENID_ISSUER	https://auth.jeevesconsults.ca/application/o/guacamole/
OPENID_CLIENT_ID	A1l7KFyrugknbc8jtFjPxm520XkcNVjGMfTFtJMt
OPENID_CLIENT_SECRET	REDACTED
OPENID_REDIRECT_URI	https://guac.jeeves5454.ddns.net/
OPENID_AUTHORIZATION_ENDPOINT	https://auth.jeevesconsults.ca/application/o/authorize/
OPENID_JWKS_ENDPOINT	https://auth.jeevesconsults.ca/application/o/guacamole/jwks/
OPENID_SCOPE	openid email profile
OPENID_USERNAME_CLAIM_TYPE	preferred_username

No bind mounts — app state is stored in PostgreSQL.

guacd

The native protocol daemon that handles the actual RDP, VNC, SSH, and Telnet protocol sessions. Guacamole app proxies all protocol traffic through guacd.

Bind mounts:

Host Path	Container Path	Purpose
/home/jeeves/docker/guacamole/drive	/drive	Virtual drive for file transfer
/home/jeeves/docker/guacamole/record	/record	Session recordings

guacamole_db (PostgreSQL 15)

Image: postgres:15-alpine

Variable	Value
POSTGRES_DB	guacamole_db
POSTGRES_USER	guacamole_user
POSTGRES_PASSWORD	REDACTED
PGDATA	/var/lib/postgresql/data/guacamole

Bind mounts:

Host Path	Container Path	Purpose
/home/jeeves/docker/guacamole/db-data	/var/lib/postgresql/data	Database files
/home/jeeves/docker/guacamole/init	/docker-entrypoint-initdb.d	Init SQL scripts

Traefik Labels

```
traefik.http.routers.guacamole-external.rule: Host(`guac.jeeves5454.ddns.net`)
traefik.http.routers.guacamole-external.entrypoints: websecure
traefik.http.routers.guacamole-external.tls.certresolver: letsencrypt
traefik.http.routers.guacamole-external.middlewares: plex-geoblock@file,crowdsec-bouncer@file
traefik.http.routers.guacamole-external.service: guac-svc

traefik.http.routers.guacamole-internal.rule: Host(`guac.home.local`)
traefik.http.routers.guacamole-internal.entrypoints: websecure
traefik.http.routers.guacamole-internal.tls.certresolver: step-ca
```

```
traefik.http.routers.guacamole-internal.service: guac-svc
```

```
traefik.http.services.guac-svc.loadbalancer.server.port: 8080
```

```
traefik.docker.network: traefik-net
```

Notes / Gotchas

- `EXTENSION_PRIORITY=openid` means Guacamole's OpenID extension takes precedence over any local user database. If Authentik is down, Guacamole login is unavailable — there is no local admin fallback while OpenID is primary.
- `OPENID_REDIRECT_URI` must exactly match the redirect URI registered in Authentik. It points to the **external** domain (`guac.jeeves5454.ddns.net`) even when accessing internally — Authentik sends the browser there after authentication.
- `WEBAPP_CONTEXT=ROOT` removes the `/guacamole` path prefix. The app responds directly at `/`. Without this, Traefik would need to strip the prefix or all URLs would be `/guacamole/...`.
- Session recordings are stored in the `record` bind mount. Manage disk usage if many long sessions are recorded.
- The `init` bind mount contains the SQL schema initialisation scripts for the database. These run once on first start. Do not remove them if the container has not yet initialised.

Last Updated: 2026-06-17

02-filebrowser.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page:
FileBrowser tags: [filebrowser,
files, storage, authentik]

Overview

FileBrowser is a web-based file manager that provides browsing, uploading, downloading, and editing of files across multiple mounted host paths. The external route is protected by Authentik ForwardAuth. The internal route requires no additional middleware. Several significant host directories are exposed.

Access

Type	URL	Auth
External	<code>https://files.jeeves5454.ddns.net</code>	Authentik ForwardAuth + GeoBlock + CrowdSec
Internal	<code>https://files.home.local</code>	FileBrowser own auth (Step-CA TLS)

Configuration

Image: `filebrowser/filebrowser:latest`

Traefik Labels

```
traefik.http.routers.filebrowser-external.rule: Host(`files.jeeves5454.ddns.net`)
traefik.http.routers.filebrowser-external.entrypoints: websecure
traefik.http.routers.filebrowser-external.tls.certresolver: letsencrypt
traefik.http.routers.filebrowser-external.middlewares: authentik-auth@docker,plex-geoblock@file,crowdsec-bouncer@file
traefik.http.routers.filebrowser-external.service: filebrowser-svc

traefik.http.routers.filebrowser-internal.rule: Host(`files.home.local`)
traefik.http.routers.filebrowser-internal.entrypoints: websecure
traefik.http.routers.filebrowser-internal.tls.certresolver: step-ca
traefik.http.routers.filebrowser-internal.service: filebrowser-svc

traefik.http.services.filebrowser-svc.loadbalancer.server.port: 80
```

Volumes / Bind Mounts

Host Path	Container Path	Purpose
/home/jeeves/docker/filebrowser/config	/config	FileBrowser config file
/home/jeeves/docker/filebrowser/database	/database	FileBrowser database (SQLite)
/home/jeeves	/srv/home	Jeeves home directory
/media/jeeves/1TB_Vol2/downloads	/srv/downloads	Download staging area (Ceph OSD)
/mnt	/srv/mnt	NFS mounts (Multimedia, Photos, data)

“ FileBrowser provides access to the full home directory, download staging area, and all NFS mounts. Treat external access with appropriate caution.

Notes / Gotchas

- Authentik ForwardAuth is applied on the external route — external access requires a valid Authentik session before FileBrowser's own login is shown. FileBrowser still maintains its

own user database internally.

- `/mnt` is exposed as `/srv/mnt` — this includes all NFS shares from UnRAID (`/mnt/Multimedia`, `/mnt/Photos`, `/mnt/data`). Changes made via FileBrowser are live on the NFS shares.
 - The SQLite database in `/database` stores FileBrowser users, permissions, and settings. Back it up alongside `/config`.
 - `PUID=1000 / GID=1000` — FileBrowser runs as the `jeeves` user, so file operations respect the same ownership as files on disk.
-

Last Updated: 2026-06-17

03-kiwix.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page: Kiwix
tags: [kiwix, offline, wikipedia, zim,
authentik]

Overview

Kiwix serves offline ZIM-format content — primarily Wikipedia snapshots and other reference material — accessible without an internet connection. ZIM files are stored on the Ceph OSD volume. The external route is gated behind Authentik ForwardAuth. The internal route has no additional auth middleware.

Access

Type	URL	Auth
External	<code>https://kiwix.jeeves5454.ddns.net</code>	Authentik ForwardAuth + GeoBlock + CrowdSec
Internal	<code>https://kiwix.home.local</code>	No additional auth (Step-CA TLS)

Configuration

Image: `ghcr.io/kiwix/kiwix-serve:latest`

Traefik Labels

```
traefik.http.routers.kiwix-external.rule: Host(`kiwix.jeeves5454.ddns.net`)
traefik.http.routers.kiwix-external.entrypoints: websecure
traefik.http.routers.kiwix-external.tls.certresolver: letsencrypt
traefik.http.routers.kiwix-external.middlewares: plex-geoblock@file,crowdsec-bouncer@file,authentik-auth@docker
traefik.http.routers.kiwix-external.service: kiwix-svc

traefik.http.routers.kiwix-internal.rule: Host(`kiwix.home.local`)
traefik.http.routers.kiwix-internal.entrypoints: websecure
traefik.http.routers.kiwix-internal.tls.certresolver: step-ca
traefik.http.routers.kiwix-internal.service: kiwix-svc

traefik.http.services.kiwix-svc.loadbalancer.server.port: 8080
```

Volumes / Bind Mounts

Host Path	Container Path	Purpose
/media/jeeves/1TB_Vol1/Kiwix_Images	/data	ZIM content files

ZIM files are stored on the second Ceph OSD volume (`nvme2n1`, `/media/jeeves/1TB_Vol1`). `kiwix-serve` auto-discovers all `.zim` files in `/data` on startup and presents them in the library UI.

Notes / Gotchas

- ZIM files can be very large (Wikipedia full English is ~100GB). Ensure adequate space on the Ceph volume before downloading new content.
- New ZIM files can be added by placing them in `/media/jeeves/1TB_Vol1/Kiwix_Images`. A container restart is required for `kiwix-serve` to discover them.
- Kiwix has no built-in authentication — the internal route is unprotected on the LAN. The external route relies entirely on Authentik ForwardAuth.
- ZIM files can be downloaded from `library.kiwix.org` and transferred to the Ceph volume via FileBrowser or SCP.

04-drawio.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page: Draw.io
tags: [drawio, diagrams,
productivity]

Overview

Draw.io (now diagrams.net) is a self-hosted diagramming application for creating network diagrams, flowcharts, architecture diagrams, and more. This instance is stateless — diagrams are saved locally by the browser or to connected storage (Google Drive, OneDrive, etc.), not on the server. External-only access with GeoBlock and CrowdSec.

Access

Type	URL	Auth
External	<code>https://drawio.jeeves5454.ddns.net</code>	GeoBlock + CrowdSec (no auth)

No authentication middleware — Draw.io is accessible to anyone who bypasses GeoBlock. The app itself has no user accounts.

Configuration

Image: `jgraph/drawio:latest`

Runtime: Java 11 / Apache Tomcat

Key Environment Variables

Variable	Value / Notes
<code>DRAWIO_BASE_URL</code>	<code>https://drawio.jeeves5454.ddns.net</code>
<code>PUBLIC_DNS</code>	<code>drawio.jeeves5454.ddns.net</code>
<code>DRAWIO_GOOGLE_CLIENT_ID</code>	<code>jeeves5454@gmail.com</code> (Google integration)
<code>LETS_ENCRYPT_ENABLED</code>	<code>false</code> (TLS handled by Traefik)

Traefik Labels

```
traefik.http.routers.drawio.rule: Host(`drawio.jeeves5454.ddns.net`)
traefik.http.routers.drawio.entrypoints: websecure
traefik.http.routers.drawio.tls.certresolver: letsencrypt
traefik.http.routers.drawio.middlewares: plex-geoblock@file,crowdsec-bouncer@file,drawio-headers
traefik.http.middlewares.drawio-headers.headers.customrequestheaders.X-Forwarded-Proto: https
traefik.http.services.drawio.loadbalancer.server.port: 8080
```

Volumes / Bind Mounts

None — Draw.io is completely stateless. All diagram data is stored client-side (browser localStorage or connected cloud storage).

Notes / Gotchas

- `LETS_ENCRYPT_ENABLED=false` is correct — Traefik handles TLS termination. The Draw.io container itself serves plain HTTP on port 8080.
- The `X-Forwarded-Proto: https` header is required so Draw.io generates correct HTTPS URLs for embedded resources and exports.
- Diagrams are not stored on the server. To preserve diagrams, save them to a local file (`.drawio` / `.xml`) or configure a cloud storage backend in the Draw.io UI.
- `DRAWIO_GOOGLE_CLIENT_ID` enables the Google Drive integration in the file picker. Users must authorise their own Google account in the app.

05-it-tools.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page: IT Tools
tags: [it-tools, developer-tools,
utilities]

Overview

IT Tools is a collection of handy online developer and IT utilities — including JWT decoders, UUID generators, hash generators, cron expression parsers, base64 encoders, regex testers, and many more. It is a static React app served by NGINX. Internal-only access. No configuration, no authentication, no persistent state.

Access

Type	URL	Auth
Internal	<code>https://ittools.home.local</code>	None (LAN only)

Configuration

Image: `corentinth/it-tools:latest`

Runtime: NGINX 1.26 (static SPA)

Traefik Labels

```
traefik.http.routers.ittools.rule: Host(`ittools.home.local`)  
traefik.http.routers.ittools.entrypoints: websecure  
traefik.http.routers.ittools.tls.certresolver: step-ca  
traefik.http.services.ittools.loadbalancer.server.port: 80
```

Volumes / Bind Mounts

None — fully stateless static application.

Notes / Gotchas

- No data leaves the browser — all tools run client-side in JavaScript. Safe to use for sensitive values (passwords, tokens, keys) that should not be sent to external services.
- The tool list expands with each release of the `corentinh/it-tools` image. Pull the latest tag to get new tools.

Last Updated: 2026-06-17

06-pairdrop.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page:
PairDrop tags: [pairdrop, file-
sharing, webrtc, lan]

Overview

PairDrop is a local network file sharing app inspired by Apple AirDrop. It uses WebRTC for peer-to-peer file transfers between devices on the same LAN session. No accounts, no file storage on the server — files transfer directly between browsers. Internal-only access.

Access

Type	URL	Auth
Internal	<code>https://pairdrop.home.local</code>	None (LAN only)

Configuration

Image: `lscr.io/linuxserver/pairdrop:latest`

Environment Variables

Variable	Value	Purpose
----------	-------	---------

TZ	America/Toronto	Timezone
PUID	1000	User ID
PGID	1000	Group ID
WS_FALLBACK	false	WebSocket fallback (disabled)
RATE_LIMIT	false	Rate limiting (disabled for LAN)
RTC_CONFIG	false	External STUN/TURN (not needed on LAN)
DEBUG_MODE	false	Debug logging

Traefik Labels

```
traefik.http.routers.pairedrop.rule: Host(`pairedrop.home.local`)
traefik.http.routers.pairedrop.entrypoints: websecure
traefik.http.routers.pairedrop.tls.certresolver: step-ca
traefik.http.services.pairedrop.loadbalancer.server.port: 3000
```

Volumes / Bind Mounts

None — fully stateless. Files are transferred peer-to-peer and never stored on the server.

Notes / Gotchas

- PairDrop discovers peers in the same "room" — by default, all users behind the same NAT/gateway appear to each other. On a home LAN this means all devices on the network can see each other.
- `RTC_CONFIG=false` is correct for LAN use — no external STUN/TURN server is needed when all peers are on the same network.
- For Tailscale peers to use PairDrop, they would need a TURN server since Tailscale creates separate subnets. Current config is LAN-only.

07-convertx.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page:
ConvertX tags: [convertx, file-
conversion, utilities]

Overview

ConvertX is a self-hosted file format conversion tool. It supports converting between video, audio, image, document, and other file formats using a web interface. Internal-only access. Account registration is enabled, allowing any LAN user to create an account.

Access

Type	URL	Auth
Internal	<code>https://convertx.home.local</code>	ConvertX own auth (Step-CA TLS)

Configuration

Image: `ghcr.io/c4illin/convertx`

Environment Variables

Variable	Value	Purpose
----------	-------	---------

HTTP_ALLOWED	true	Allows HTTP connections (Traefik terminates TLS)
ACCOUNT_REGISTRATION	true	Any LAN user can self-register
QTWEBENGINE_CHROMIUM_FLAGS	--no-sandbox	Required for headless Chromium in container

Traefik Labels

```
traefik.http.routers.convertx.rule: Host(`convertx.home.local`)
traefik.http.routers.convertx.entrypoints: websecure
traefik.http.routers.convertx.tls.certresolver: step-ca
traefik.http.services.convertx.loadbalancer.server.port: 3000
```

Volumes / Bind Mounts

Host Path	Container Path	Purpose
/data/compose/43/data	/app/data	App data and SQLite

“ The data directory is a Portainer-managed compose path (/data/compose/<stack-id>/data) — this stack is managed entirely via Portainer with no local compose file. The path is determined by the Portainer stack ID (43).

Notes / Gotchas

- ACCOUNT_REGISTRATION=true allows any user on the LAN to self-register. Disable this if access should be restricted to a single admin account.
- Converted files are stored temporarily in the app data directory and deleted after download. Do not use this path for long-term storage.
- no-sandbox is a Chromium security flag required when running in a container (no user namespace isolation). This is standard for containerised headless browser setups.
- ConvertX uses FFmpeg, ImageMagick, and other converters internally — available formats depend on the image build.

08-minuspod.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page:

MinusPod tags: [minuspod,
podcasts, transcription, whisper,
ai, cuda]

Overview

MinusPod is an AI-powered podcast manager and transcriber. It manages podcast feeds, downloads episodes, and transcribes audio using a local Whisper model. Summaries and notes are generated via an LLM (Qwen3:14b) through the Ollama API. The container runs with NVIDIA GPU access (RTX 5080) for accelerated Whisper inference. Internal-only access. Episode data is retained for 180 days.

Access

Type	URL	Auth
Internal	<code>https://minuspod.home.local</code>	MinusPod own auth (Step-CA TLS)

No external route — LAN access only.

Configuration

Image: `ttlequals0/minuspod:2.1.9`
Runtime: CUDA 12.9 / NVIDIA runtime (RTX 5080)

Key Environment Variables

Variable	Value / Notes
<code>BASE_URL</code>	<code>https://minuspod.home.local</code>
<code>WHISPER_BACKEND</code>	<code>local</code>
<code>WHISPER_DEVICE</code>	<code>cuda</code>
<code>WHISPER_MODEL</code>	<code>medium</code>
<code>LLM_PROVIDER</code>	<code>ollama</code>
<code>OPENAI_BASE_URL</code>	<code>https://ollama.home.local/v1</code>
<code>OPENAI_MODEL</code>	<code>qwen3:14b</code>
<code>OPENAI_API_KEY</code>	REDACTED
<code>RETENTION_PERIOD</code>	<code>4320</code> hours (180 days)
<code>MINUSPOD_TRUSTED_PROXY_COUNT</code>	<code>1</code>
<code>NVIDIA_VISIBLE_DEVICES</code>	<code>all</code>
<code>NVIDIA_DRIVER_CAPABILITIES</code>	<code>compute,utility</code>

Traefik Labels

```
traefik.http.routers.minuspod.rule: Host(`minuspod.home.local`)
traefik.http.routers.minuspod.entrypoints: websecure
traefik.http.routers.minuspod.tls.certresolver: step-ca
traefik.http.services.minuspod.loadbalancer.server.port: 8000
```

Volumes / Bind Mounts

Host Path	Container Path	Purpose
<code>/home/jeeves/dockers/minuspod/data</code>	<code>/app/data</code>	Episode database and downloads

“ Note: The data directory is under `/home/jeeves/dockers/` (not `docker/`) — this is the actual bind mount path as confirmed by `docker inspect`.

AI Integration

MinusPod uses two AI components:

Component	Model	Transport	Purpose
Whisper	medium	Local CUDA inference (RTX 5080)	Audio transcription
Qwen3:14b	qwen3:14b	Ollama API at ollama.home.local/v1	Summaries and notes

`OPENAI_BASE_URL` points to the internal Ollama instance (which exposes an OpenAI-compatible API). The `OPENAI_MODEL` is `qwen3:14b` — this model must be present in Ollama. Verify with `docker exec ollama ollama list`.

Notes / Gotchas

- The Whisper `medium` model on CUDA provides a good balance of speed and accuracy. Upgrade to `large-v3` if accuracy is more important than speed (uses more VRAM). The RTX 5080 has 16GB GDDR7 — ample for either.
- `RETENTION_PERIOD=4320` hours = 180 days. Episodes older than this are automatically removed. Adjust if long-term episode storage is needed.
- `MINUSPOD_TRUSTED_PROXY_COUNT=1` tells MinusPod to trust one level of proxy headers (Traefik) for correct IP and protocol detection.
- The bind mount path is `/home/jeeves/dockers/minuspod/data` (note: `dockers`, not `docker`). This is different from the convention used by most other stacks.
- Ensure `qwen3:14b` is loaded in Ollama before enabling LLM summaries:

```
docker exec ollama ollama pull qwen3:14b
```

09-docker-proxy.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page: Docker
Socket Proxy tags: [dockerproxy,
security, docker, infrastructure]

Overview

The Docker Socket Proxy (`dockerproxy`) provides a read-only, filtered proxy to the Docker daemon socket. It exposes a limited subset of the Docker API over TCP, allowing containers like Homepage to query running container data without requiring direct access to `/var/run/docker.sock`. No Traefik route — internal use only.

Configuration

Image: `tecnativa/docker-socket-proxy`

Environment Variables (API Permission Flags)

Variable	Value	Permission granted
<code>CONTAINERS</code>	<code>1</code>	Read container list and inspect data
<code>EVENTS</code>	<code>1</code>	Subscribe to Docker events stream
<code>POST</code>	<code>0</code>	Disabled — no write operations

Variable	Value	Permission granted
ALLOW_START	0	Cannot start containers
ALLOW_STOP	0	Cannot stop containers
ALLOW_RESTARTS	0	Cannot restart containers
AUTH	0	No auth endpoint access
BUILD	0	No build operations
COMMIT	0	No commit operations
CONFIGS	0	No config access
DISTRIBUTION	0	No distribution endpoint access

All write operations are disabled. The proxy grants read-only container metadata access only.

Volumes / Bind Mounts

Host Path	Container Path	Purpose
/var/run/docker.sock	/var/run/docker.sock	Docker socket (read-only proxy source)

Consumer

The primary consumer is **Homepage** (`homepage.home.local`), which connects to `dockerproxy:2375` to discover running containers and display live service status widgets. This avoids mounting the Docker socket directly into Homepage.

Notes / Gotchas

- The proxy listens on TCP port 2375 (standard Docker API port) inside the Docker network — it is not exposed on any host port or Traefik route.
 - Allowing only `CONTAINERS=1` and `EVENTS=1` means Homepage can list containers and receive real-time status events, but cannot perform any management actions.
 - If Homepage shows containers as offline or fails to discover services, verify `dockerproxy` is running and on the same Docker network as Homepage.
 - The `tecnativa/docker-socket-proxy` image is the community standard for this pattern. It is based on HAProxy 3.x and routes allowed API paths only.
-

Last Updated: 2026-06-17