

System Change log

- 2026-10-21 Wednesday

- **Minecraft Web Control Plane (`mc.drheck.dev`) Mobile Browser Detection & Slidable Low-Density UI (`u1`):**

- Added server-side mobile detection (`IsMobileRequest` / `ServeIndexHTML` in `internal/mcmanager/mobile.go` inspecting `?view=mobile|desktop`, `Sec-CH-UA-Mobile: ?1`, and mobile `User-Agent` headers with `Vary: User-Agent, Sec-CH-UA-Mobile`) plus synchronous client-side viewport/storage detection and one-tap **Mobile** $\longleftrightarrow$ **Desktop** mode switching in `mc-manager` (`v1.2`).
- Built a dedicated mobile shell (`#mobile-shell`) organized into four hardware-accelerated horizontal `scroll-snap` views (**World**, **Console**, **Players**, and **Settings**) with `100dvh` safe-area layout, `16px` zoom-safe form inputs, compact WebSocket log formatting, UUID-free player access lists, and thumb navigation tabs while preserving 100% of the desktop studio interface.
- Added Go unit tests (`mobile_test.go`) and full JSDOM desktop + iPhone Safari mobile end-to-end tests (`e2e/run_dom_e2e.js`), verified all Go + DOM E2E tests pass, deployed `/usr/local/bin/mc-manager`, restarted `mc-manager.service`, and updated [Minecraft Worlds](#).

- **System Package Maintenance (`u1`):**

- Upgraded host packages via `pacman -Syu` (`gperftools` `2.19-1`, `luajit` `2.1.1792527110+95f931c-1`, `mise` `2026.10.17-1`, and `python-fastapi` `0.156.6-1`).

- 2026-10-20 Tuesday

- **Forgejo Two-Factor Authentication (`git.drheck.dev`) Cipher Migration Fix (`u1`):**

- Resolved `HTTP 500 Internal Server Error` on `POST /user/two_factor` (`UserSignIn: chacha20poly1305: message authentication failed`) caused by legacy Gitea `AES-CFB` (`md5(SECRET_KEY)`) + double-Base64 ciphertext remaining in `two_factor.secret` after the Gitea $\rightarrow$ Forgejo `16.0.6` migration.
- Decrypted the existing 64-character Base32 TOTP seed without requiring authenticator re-enrollment, re-sealed `two_factor.secret` using Forgejo `16.0.6` 's `modules/keying` `HKDF-SHA256` (`totp` subkey) + `XChaCha20-Poly1305` AEAD with `ColumnAndID("secret", id)` big-endian associated data, verified all 27 `forgejo doctor check --all` checks (`OK`), and refreshed PAR2 backups.

- **Docker Package Removal, Root NVMe Reclamation & ZFS `data/podman` Dataset Migration (`u1`):**

- Uninstalled `docker` (`1:29.9.1-1`), `docker-compose` (`5.6.0-1`), and `containerd` (`2.4.2-1`) via `pacman -Rns` and purged `/var/lib/docker`, `/var/lib/containerd`, and `/etc/docker` (`43 GB` freed on `/`).
- Provisioned dedicated ZFS dataset `data/podman` (`compression=lz4`, `xattr=sa`, `acltype=posix`, `dnodesize=auto`, `atime=off`, `mountpoint=/home/docker-data/.local/share/containers`) and migrated Podman's `67 GB` image/layer store

from the root NVMe onto the 160 TB ZFS pool via two-pass `rsync -aHAX`.

- Cleaned `39 GB` of obsolete package tarballs from `/var/cache/pacman/pkg` (`paccache -rk2` + `paccache -ruk0`) and enabled weekly `paccache.timer`.

- **System Package & Plex Media Server Upgrade (u1):**

- Upgraded host packages via `paru -Syu` / `pacman -Syu` (`postgresql 18.6-4`, `polkit 128-1`, `poppler 26.10.0-1`, `python-fastapi 0.156.2-1`, `python-starlette 1.9.0-1`, `python-pyarrow 26.0.0-1`, `python-pycryptodome 4.1.0-1`, and `shellcheck 0.11.0-159`) and upgraded `plex-media-server` (`1.43.4.10903-1` $\rightarrow$ `1.43.5.11029-1`).

- 2026-10-19 Monday

- **Complete 30-Service / 40-Container Rootless Podman Cutover & Docker Decommissioning (u1):**

- Decommissioned `docker.service`, `docker.socket`, and `containerd.service` completely (`inactive` / disabled), removed all 10 leftover Docker kernel bridges (`docker0` + `br-*`), archived legacy artifacts into `/data/backups/legacy_docker_archive/`, and replaced `docker-prune.timer` with rootless `/etc/systemd/system/podman-prune.{service,timer}` (`User=docker-data`).
- Migrated all remaining 19 services (29 containers) alongside the initial 11 standalone services—totaling **all 30 containerized services (41 containers)**—to rootless Podman Quadlets (`docker-data`, `UID 1100`, subordinate range `docker-data:624288:65536`, `Pull=never` offline boot resilience, `/home/docker-data/.config/containers/systemd/*.{container,network}`).
- Migrated shared Valkey to native host `valkey.service` bound strictly to `127.0.0.1:6379` with per-service ACL users (`authentic`, `immich`, `nextcloud`, `vikunja`, `degoog`), `default` disabled, and dangerous admin commands disabled; locked host `postgresql.service` strictly to `127.0.0.1:5432` and upgraded the legacy MD5 role password to `SCRAM-SHA-256`.
- Configured host HAProxy Layer-4 TCP passthrough (`/etc/haproxy/conf.d/ldap.cfg`) relaying ports `389/636` to rootless `authentic-ldap` (`:3389/6636`) and removed `/etc/nginx/certs:/certs:ro` from all Authentik containers so zero host TLS/mTLS keys (`pikvm_client.key`, `studio_secret.conf`) are mounted inside containers.
- Remediated security & operational findings uncovered during migration:
 - Enabled `YOURLS_PRIVATE=true`, rotated weak `yourls` credentials (`admin_pass_9213` / `yourls_db_pass_9213`), and gated `https://drheck.dev/yourls-api.php` behind Authentik ForwardAuth while keeping short-link `301` redirects public.
 - Removed `/home/luke:/host_home:ro` mount from `subocr`, restricted Collabora WOPI wildcard `https://.*` strictly to `ccloud.drheck.dev`, set `DISABLE_SIGN_UP=true` and `0770` permissions on `wipstudio`, and archived the deleted upstream `minio/minio` image at `/data/docker/wipstudio/minio_image_backup.tar.xz`.
 - Fixed silent data-loss gaps in `/home/luke/git/backups/ul/scripts/`: pointed `backup/nextcloud` + `restore/nextcloud` at live `nextcloud_db` (instead of stale `nextcloud`) + `config.php`; migrated `penpot` Postgres & assets out of `/var/lib/docker/volumes` onto ZFS `/data/docker/penpot/{postgres_data,assets}` and added `assets` to

- backup/penpot; added `pg_dumpall -U funkwhale` to `backup/funkwhale`;
 - added `authentik-*.container` to `backup/authentik`; and expanded `backup/systemd` to archive `/etc/containers`, `/etc/haproxy`, `/etc/nftables.conf`, and `/home/docker-data/.config/containers/systemd`.
- Fixed HTTP 500 ForwardAuth errors on secondary hostname aliases (`music.drheck.dev` $\rightarrow$ `navidrome.drheck.dev`, `scontroll.drheck.dev` $\rightarrow$ `scontrol.drheck.dev`) and OIDC callback host mismatches (`vault.drheck.dev` $\rightarrow$ `pw.drheck.dev`, `bookstack.drheck.dev` $\rightarrow$ `wiki.drheck.dev`) with dedicated TLS 301 redirects across `/etc/nginx/sites-available/`.
- Pruned a stale `aardvark-dns` entry in `/run/user/1100/containers/networks/aardvark-dns/penpot_net` (10.89.13.2 ahead of 10.89.13.5) that caused `penpot-backend` Lettuce Redis timeouts, fixed root-owned cache generation in `/home/luke/bin/read-bookstack-page` (`-u abc -e HOME=/config`), and updated `/usr/local/bin/{update-authentik-cert.sh,mc-blue-map-provision,degoog-update}`, `/data/minecraft/ipctl`, `/etc/nftables.conf`, and all 43 PAR2-verified service backups.
- Backup Architecture Decoupling (ul):**
 - Refactored `/home/luke/git/backups/ul/scripts/run_all_backups` so default invocations execute fast local snapshots and `par2` verification only (`--all` runs the full local + cloud + ISO pipeline).
 - Extracted standalone `/home/luke/git/backups/ul/scripts/stage_cloud_archive`, `/home/luke/git/backups/ul/scripts/upload_cloud_archive`, and `/home/luke/git/backups/ul/scripts/stage_iso_archive` scripts and updated [Backup Process](#).
- amux Synchronous Command Waiting (ul):**
 - Implemented native event-driven command completion waiting in `amux` (`/home/luke/git/amux`, installed at `/usr/local/bin/tmux-custom`) via `read-pane -w` (`-S <token>`, `-e <var>`, `-E <file>`, `-O <offset>`, `-t <timeout>`), eliminating polling loops.
 - Added `atx-exec` helper to `/home/luke/.agent_profile` and updated [amux - Agent modified tmux](#) and [SSH & Agent Command Tracking Guide](#).
- Gitea $\rightarrow$ Forgejo Migration (ul):**
 - Migrated [git.drheck.dev](#) from Gitea (28.1.0-1) to Forgejo (16.0.6-1), renaming ZFS dataset `data/gitea` to `data/forgejo` (`/data/forgejo`), PostgreSQL database/role to `forgejo`, configuration to `/etc/forgejo/app.ini`, and working state to `/var/lib/forgejo` (`User=git`).
 - Added `/etc/tmpfiles.d/forgejo.conf` (`git:git` override) to prevent `pacman 30-systemd-tmpfiles.hook` from resetting `/var/lib/forgejo` and `/etc/forgejo/app.ini` ownership to `forgejo:forgejo` during package upgrades.
 - Updated Nginx (`/etc/nginx/sites-available/forgejo`), Authentik OIDC provider/application (`Forgejo / forgejo`), `pass` entries (`forgejo/*`), `repo_tools` (`forgejo-create`, `forgejo-delete`, `forgejo-Visibility`, `gpush`), and backup/restore scripts (`/home/luke/git/backups/ul/scripts/{backup,restore}/forgejo`).

- **Kasm Decommissioning & Rootless Podman Quadlet Migration (u1):**
 - Decommissioned `kasm` (`kasm.drheck.dev`, `/data/docker/kasm`, PostgreSQL `kasm_db`, ULA IPv6 `:ca53`, Authentik OIDC app, Nginx config, Unbound DNS, and `/data/kasm_profiles`) and removed obsolete `/data/docker/sunshine` container stack.
 - Configured rootless Podman (`6.1.4-1`) with `passt` user-mode networking, subordinate UID/GID ranges (`docker-data:100000:65536`), ZFS-backed graphroot (`/data/podman/docker-data/storage`), and systemd user lingering (`loginctl enable-linger docker-data`).
 - Migrated 11 standalone single-container services (`audiomass`, `bentopdf`, `excalidraw`, `tlldraw`, `wick`, `webrcade`, `drawpile`, `navidrome`, `vaultwarden`, `sopro`, `demucs`) from rootful Docker Compose to rootless Podman systemd Quadlets (`/home/docker-data/.config/containers/systemd/*.container`).
 - Updated `/home/luke/bin/status_all`, backup/restore scripts, [Service List](#), [Service Update Process](#), and authored [podman](#).
- 2026-10-18 Sunday
 - **Fleet-Wide Git Repository Check-In, Licensing & PAR2 Backup Parity Sweep (u1, danknasty, metropolis):**
 - Audited all custom services, scripts, router configs, and local repositories across `u1`, `danknasty`, and `metropolis`, GPG-signing all commits and syncing to [git.drheck.dev](#).
 - Created and pushed new repositories `luke/amux` (inheriting upstream `tmux`'s ISC license across `COPYING`, `LICENSE`, `cmd-read-pane.c`, and `cmd-write-pane.c`), `luke/cam`, `luke/craft-web`, `luke/grill-sync` (integrating the `grill.drheck.dev` web backend under `server/`), and `luke/xmms2` (BSD 3-Clause).
 - Committed and pushed pending live changes across `luke/router_config` (`e0d4883` on `danknasty`: camera DHCP leases, `update_dns.py` + 11 unit tests, `dns_danger_sync.py`, `verify_dns.sh`, `ipv6_heartbeat.sh`, `pf.conf`), `luke/configs` (`755fcda`: `nftables.conf`, BookStack CLI helpers, `audit-log`, `opencode_list`, WireGuard client helpers, SSH CA scripts, CrowdSec utilities, and Gamescope/Sunshine helpers), `luke/nginx` (`2a093a8`: synced 30 active site definitions while excluding TLS/mTLS secrets via `.gitignore`), `luke/scontrol` (`f3d83e9`: serialized RF outlet commands via file lock and version-agnostic Ardour process check), `luke/ldap_deploy` (`daf4d5c`), `luke/library_works` (`6bd4e50`), `luke/ssl-update` (`bcad606`), `luke/smart_stats` (`784c339`), `luke/repo_tools`, and `luke/pass` (`fe9fc81`).
 - Initialized local GPG-signed Git repositories in `/home/luke/git/` for `mc_manager` (`78b9117`), `subocr` (`10971bd`), `demucs` (`e60cc3f`), `webshell` (`bcb10a6`), `sopro` (`8a766d4`), `gpg_paper_backup` (`5e795cc`), `battery_serials` (`18b89f8`), `network` (`f5c732c`), `ansview` (`4211cf2`), `flac_opus` (`4b88fa3`), and `lukegemini` (`6455c16`).
 - Added and `shellcheck`-verified 10% `par2` backup and restore scripts (`2a2629f` in `/home/luke/git/backups`) for `amux`, `anchor`, `cam`, `degoog`, `subocr`, `valkey`, and `vikunja`, and updated `immich` and `mc_manager`.
 - **Shared `valkey` Dynamic IP Allocation & `vikunja` / `immich` Recovery (u1):**
 - Resolved a static/dynamic IPAM collision on `infra_net` (`172.28.0.10` held by `authentik-worker` preventing `valkey` startup) by removing `ipv4_address:`

172.28.0.10 from /data/docker/infra/docker-compose.yml, updating /data/docker/vikunja/config.yml to resolve valkey:6379 by container name, and restoring valkey, vikunja, and immich_server to healthy operation.

- 2026-10-17 Saturday

- **Fiber Demarc & Physical Plant Documentation** (wiki.drheck.dev):

- Created the [Network](#) wiki book and authored [Network Details](#) documenting the Comcast ISP demarc (Modem → CAT6 → Media Converter → Singlemode BiDi Optic) and Corning ALTOS outdoor armored direct-burial singlemode LC-UPC fiber assemblies (100 ft through 370 ft, 2-strand and 12-strand runs).

- 2026-10-16 Friday

- **DrHeck Camera Hub AI Event Timeline, Two-Way Talk, Optical Auto-Zoom, Night Lighting & Static DHCP** (ul, danknasty):

- Added static DHCP reservations (host cam1 ec:71:db:f1:25:5a → 10.0.0.122 and host cam2 ec:71:db:6d:84:ce → 10.0.0.123) in /etc/dhcpd.conf and ~/git/router_config/dhcpd.conf on danknasty, validated with doas dhcpd -n, and restarted dhcpd.
 - Deployed YOLOv8n (yolov8n.onnx CPU inference) and continuous Baichuan hardware alarm capture (event_monitor_loop) on [cam.drheck.dev](#), storing clean unannotated JPEG snapshots (/data/docker/cam/data/events/<event_id>.jpg) and rendering a **Detection Event Timeline & Metadata Log** with America/New_York (EDT/EST) timestamps, AI trigger badges (people, vehicle, dog_cat, motion, manual), motion percentages, per-object class labels and confidence scores in text, and per-class AI/motion sensitivity sliders (cmd_id = 342/343, 46/47).
 - Implemented two-way audio talk (POST /api/cameras/{ip}/talk) over RTSP ONVIF Backchannel (track3 PCMU/8000 on port 554) supporting browser microphone **Push-to-Talk** (MediaRecorder → FFmpeg mulaw) and **Speak Text** (espeak-ng TTS).
 - Added smart night lighting and deterrent controls (spotlight schedule/AI trigger modes cmd_id = 289/290, IR night-vision toggle cmd_id = 208/209, stealth status LED toggle, day/night ISP modes, **Auto-Siren on Detection** defaulted off via cmd_id = 439/440, and 3D microphone noise reduction), one-click **Privacy Sleep Mode** (cmd_id = 574/575) + hardware privacy masks (cmd_id = 52/53), interactive **3D Click-to-Zoom** (cmd_id = 445) + autofocus lock (cmd_id = 224/225) + optional **Auto-Zoom on Moving Objects**, and time.google.com:123 NTP synchronization (cmd_id = 38/39), updating [ip cameras](#).

- 2026-10-15 Thursday

- **DrHeck IP Camera Hub Deployment** (cam.drheck.dev), **Hardware ISP Controls & Google TV App** (ul, danknasty):

- Provisioned [cam.drheck.dev](#) (/data/docker/cam, dedicated ULA IPv6 [fd77:7777:5010:0:1337:f1ac:d00d:ca30]:8000 on eth77, /etc/nginx/sites-available/cam with proxy_buffering off, split Unbound/deSEC DNS on danknasty, and 10% par2 backup/restore scripts) for the two PoE **Reolink**

RLC-811A (P430) 4K cameras (10.0.0.122 and 10.0.0.123).

- Created the `camera_access` group in Authentik (`luke`, `ikura`, `haruka`), bound it to the `Cameras` (`cam`) ProxyProvider/Application, passed `X-Authentik-Groups` (`$authentik_groups`) in `/etc/nginx/sites-available/cam`, and enforced group authorization across all routes.
- Built native binary **Baichuan** (`9000/tcp`) discovery/control and **RTSP** (`554/tcp`) streaming pipelines supporting multi-client low-latency video (`yuvj420p` full-range normalization + instant `<150 ms` initial `cmd_id = 182` snapshot yield), 6 WAN/LAN bandwidth presets (`2 Mbps` HD down to `14 kbps` stateless snapshot polling), `5X` motorized optical zoom (`0..28`) and focus (`0..238`), zero-CPU hardware ISP `180°` upside-down mount flip/mirror (`cmd_id = 25`), disabled burned-in Reolink logo watermarks (`<enWatermark>0</enWatermark>`, `cmd_id = 45`), enabled `16 kHz` AAC microphone audio streaming (`/api/cameras/{ip}/audio.mp3`), built and signed the sideloadable Google TV APK (`dev.drheck.cam` wrapping `https://cam.drheck.dev/tv`), and authored [ip cameras](#).

- **Native Rust Winamp Client Wayland Fix** (`xmms2`) (`u1`, `luket7`):

- Fixed `minifb` Wayland `NoKeymap` panic, Wayland proxy teardown ordering, and in-place window resizing (`97f788a` in `/home/luke/git/xmms2`).

- 2026-10-14 Wednesday

- **Demucs Audio Stem Separation AMD ROCm GPU Migration** (`demucs.drheck.dev`) (`u1`):

- Migrated `demucs` (`/data/docker/demucs`) from CPU-only PyTorch (`2.13.0+cpu`, hardcoded `--device cpu`) to **ROCm 7.2** (`torch==2.11.0+rocm7.2`, `torchaudio==2.11.0+rocm7.2`) with `/dev/dri` + `/dev/kfd` GPU passthrough (`video/render` groups) on the **AMD Radeon AI PRO R9700** (`gfx1201`), persistent `/data/docker/demucs/cache/{huggingface,miopen}` volumes, and `/api/status` telemetry—reducing separation of a `3m 42s` FLAC track from ~30 minutes on CPU to **9 seconds** (`25.25x` real-time).

- **LDAP + SSSD Client Enrollment Fix, `locallogin` Group, GDM Pre-Provisioning & Funkwhale CSRF Fix** (`u1`, `client fleet`):

- Resolved fresh client SSSD bind and enumeration failures (`Invalid credentials (49)` from `ldapservice` password drift plus `enumerate = false` and Authentik `modifyTimestamp=>` filter incompatibility), isolated `funkwhale` onto `funkwhale-ldap-sa` with `search_full_directory`, and exposed `authentik-ldap` on LAN IPv4 (`10.0.0.3`, `10.0.0.100`) alongside ULA IPv6.
- Created dedicated Authentik LDAP group `locallogin` (`cn=locallogin,ou=groups,dc=ldap,dc=goauthentik,dc=io` containing `luke`, `haruka`, and `ikura`) decoupled from `studio`, updated `/home/luke/git/ldap_deploy/ldap_deploy.py` (with unit tests in `tests/ldap_deploy_test.py`) and `/usr/local/bin/gdm-ldap-user-session.sh` to configure `enumerate = true`, `ldap_entry_usn = entryUSN`, `locallogin` search filtering, and `/var/lib/AccountsService/users/` GDM tile pre-provisioning, and expanded [LDAP + SSSD Client Enrollment Guide](#) with an offline troubleshooting runbook.

- Persisted Funkwhale's Django CSRF/session overrides (`common.py` and `views.py`) as read-only volume mounts in `/data/docker/funkwhale/docker-compose.yml` to prevent container recreations from resetting login CSRF handling (`403 Permission denied`).
 - **Craft Web Font Serving & Native Rust Winamp 2/3/5 Client (u1, luket7):**
 - Added dynamic host system font and `craft-fonts` serving across all web apps on craft.drheck.dev (`7011b0b` in `/home/luke/git/craft-web`).
 - Built a native Rust Winamp `2.x` (`.wsz`) and Winamp `3/5` (`.wal` + MAKI bytecode VM) audio player client with file dialogs, context menus, and playlist editor (`99d707b`, `4682388` in `/home/luke/git/xmms2`).
- 2026-10-12 Monday
 - **Craft WebAssembly Creative Suite Portal & Per-User Server Storage (craft.drheck.dev) (u1, danknasty):**
 - Built and deployed `craft-web` (`/home/luke/git/craft-web`, `craft-web.service` on `[fd77:7777:5010::1337:flac:d00d:c4af]:8090`, `/etc/nginx/sites-available/craft`, Authentik ForwardAuth identity middleware, split Unbound/deSEC DNS, and `craft` `10%` `par2` backup/restore scripts) serving WASM builds of `effectcraft`, `filmcraft`, `lightcraft`, and companion apps at craft.drheck.dev.
 - Implemented isolated per-user server filesystem and preferences storage (`/data/craft/data`), REST file storage + HTTP byte-range streaming endpoints, an injected browser native-FS modal bridge (`rfd` `save/open` + `?open=` canvas auto-open), and a non-agentic WASM build/deploy pipeline throttled via `nice` `19`, `ionice idle`, and a `25%` CPU core cap.
 - **Templated Per-World BlueMap Services & Weekly Degoo Extension Updater (u1):**
 - Deployed templated `bluemap@.service` (`bluemap@desertworld.service`), `/usr/local/bin/mc-bluemap-run`, `/usr/local/bin/mc-bluemap-provision`, and `/etc/nginx/sites-available/desertworld`, and added BlueMap units/helpers to `backup/mc_manager` (`fb7294d`).
 - Deployed `degoog-update.{service,timer}` (`/usr/local/bin/degoog-update`) to refresh Degoo search engine extensions weekly on Sundays.
- 2026-10-10 Saturday
 - **Minecraft Server Control Plane, Live Console, Seed Studio & Text/Icon Studio (u1, danknasty):**
 - Built and deployed `mc-manager` (`/usr/local/bin/mc-manager`, `mc-manager.service`), `mc-runner` (`/usr/local/bin/mc-runner`, `minecraft@<slug>.service` PTY wrapper with `/run/mc-manager/<slug>.sock`), and `mc-seed-render` (`/usr/local/bin/mc-seed-render`, native `cubiomes` biome & structure map generator) at mc.drheck.dev behind Nginx and Authentik ForwardAuth.
 - Added **Minecraft Text, MOTD, Color Gradient & 8-Bit Pixel Icon Studio** to both the **+ New World** wizard and existing server **Configuration** panel (Unicode font styles, Java-safe symbols, `$` RGB gradient interpolator, live server-list preview, and 64×64 8-bit pixel badge/icon generator).
 - Updated `/etc/haproxy/minecraft.lua` and HAProxy backend rules so all Multiplayer Server List pings (`state == 1`) query `mc-manager` (`BuildLiveStatusJSON`), overlaying live `motd` (`server.properties`) and `favicon` (

`server-icon.png`) onto running server status responses without requiring a server restart.

- Updated `/data/minecraft/ipctl` to authenticate programmatically to `danknasty` using short-lived (5-minute) SSH user certificates issued by `step-ca` (`webshell-svc` provisioner) and trusted via `/etc/ssh/config.d/10-drheck-certs.conf` on `danknasty`.
- Externalized all dynamic `ipctl` state out of code-reviewed base configs into `/etc/systemd/network/20-wired.network.d/minecraft.conf`, `/etc/haproxy/conf.d/minecraft_backends.cfg`, `/etc/haproxy/minecraft_hosts.map`, and `/var/unbound/etc/unbound.minecraft.conf` (included from `unbound.conf` and parsed recursively by `update_dns.py`, `dns_danger_sync.py`, and `verify_dns.sh`), with tracked mirrors in `/data/minecraft/.network/`.
- Provisioned `desertworld.drheck.dev` (`fd77:7777:5010::1337:3c:d00d:2/64`) and updated [Minecraft Worlds](#) and [Service List](#).
- Deployed weekly `mc-datapack-update.{service,timer}` (`mc-manager -update-binaries -update-datapacks`) and created 10% `par2` backup/restore scripts for `mc_manager` (`a860eb1`).

◦ **Host Service Health Audit, Systemd Boot Cycle Fix & Offline LAN Resilience** (`u1`):

- Resolved a 4-way systemd ordering cycle caused by `After=network-online.target` `docker.service` in `/etc/systemd/system/ollama-docker-proxy.socket` (`Before=sockets.target`), enabled `containerd.service`, and added `Requires=containerd.service` to `/etc/systemd/system/docker.service.d/override.conf`.
- Fixed `/usr/local/bin/crowdsec-update-ipv6-whitelist` (`s02-enrich/00-lan-whitelist.yaml` path + `10.77.0.0/24` and `fd77:7777:5010:7700::/64`), exported `DISPLAY` and `WAYLAND_DISPLAY` into `systemd --user` inside `launch-gamescope-esde.sh` and `launch-gamescope-steam.sh` for `xdg-desktop-portal-gtk.service`, added `RestartSec=5s` + `StartLimitIntervalSec=0` to `nginx.service.d/override.conf` so Nginx survives power-recovery races ahead of `danknasty`, and removed `reflector.service` from `multi-user.target.wants` so `u1` boots cleanly with full local LAN functionality when WAN is offline.

◦ **Vikunja Task Manager Deployment** (`vikunja.drheck.dev`) (`u1`, `danknasty`):

- Deployed Vikunja (`/data/docker/vikunja`, ULA IPv6 `[fd77:7777:5010:0:1337:f1ac:d00d:71c0]:3456` on `eth77`) behind `/etc/nginx/sites-available/vikunja` with Authentik OIDC single sign-on, PostgreSQL + Valkey state storage, and split local/public DNS records on `danknasty`.

• 2026-10-04 Sunday

◦ **Degoog Private Metasearch Engine Deployment** (`search.drheck.dev`, `s.drheck.dev`) (`u1`, `danknasty`):

- Deployed `degoog` (`ghcr.io/degoog-org/degoog`, `/data/docker/degoog`, ULA IPv6 `[fd77:7777:5010:0:1337:f1ac:d00d:de90]:4444` on `eth77`, backed by Valkey) behind `/etc/nginx/sites-available/search.drheck.dev` and Authentik SSO, with local Unbound and public deSEC DNS records for `search.drheck.dev` and short alias `s.drheck.dev`.

- 2026-10-03 Saturday
 - **SubOCR Japanese Video Subtitle OCR & Study Platform Deployment (`subocr.drheck.dev`) (`u1` , `danknasty`):**
 - Built and deployed **SubOCR** (`/data/docker/subocr` , `/home/luke/bin/subocr` , ULA IPv6 `[fd77:7777:5010:0:1337:f1ac:d00d:0c70]:8000` on `eth77`) behind `/etc/nginx/sites-available/subocr` , Authentik ForwardAuth, and split Unbound/deSEC DNS at subocr.drheck.dev , documented on [subocr service](#).
 - Implemented a two-stage **AMD Radeon AI PRO R9700 (`gfx1201`)** ROCm 7.2 GPU pipeline combining **PP-OCRv5** (`onnxruntime-rocm` `MIGraphXExecutionProvider`) burned-in *telop* detection/recognition with **Qwen2.5-32B** (`ollama-rocm` via `ollama-docker-proxy.socket`), UniDic morphological tokenization, an offline **JMdict + JLPT N5-N1** SQLite dictionary (`218,856` entries), interactive furigana/study-note pages (`vocab_pages.py`), and automatic sidecar subtitle exports to `/data/language/Japanese/Video` .
- 2026-09-28 Monday
 - **`amux` Native Output Extraction (`read-pane`) & FireBoard Grill Hardware Switch Refinement (`u1`):**
 - Implemented `read-pane` (`readp` in `cmd-read-pane.c`) in `amux` (`/home/luke/git/tmux`) to capture unwrapped per-pane PTY byte streams and `OSC 133` command output blocks with structured `sd_journal_send` audit logging.
 - Updated the Seeed XIAO ESP32-C3 BLE-to-Wi-Fi bridge firmware (`/home/luke/git/grill-sync` , commits `1886b89` , `60b0150` , `6c4e13f`) to use the 4-wire `IRLB8721PBF` MOSFET hardware power switch exclusively, disable floating ADC deep-sleep cutoffs, set hostname `fireboardctl` , and send periodic HTTP heartbeats to `grill.drheck.dev` .
- 2026-09-27 Sunday
 - **`amux` (Agent-Modified tmux) & Persistent Session Infrastructure (`u1`):**
 - Created custom tmux fork (`amux`) built from `/home/luke/git/tmux` and installed at `/usr/local/bin/tmux-custom` .
 - Implemented native `write-pane` (`writep`) command supporting `-b <base64>` and `-f <file>` with `-e` (auto-enter) to inject scripts directly into PTY buffers with zero quote escaping or keystroke lag.
 - Built structured audit logging directly into `cmd-write-pane.c` using `sd_journal_send` (`SYSLLOG_IDENTIFIER=amux` , `AMUX_PANE_ID` , `AMUX_WINDOW_NAME` , `AMUX_ARCHIVE_PATH`).
 - Configured automatic pre-execution script archival to persistent storage in `/data/amux/scripts/` (`YYYY-MM-DD_HHMM.SS_<window_name>.sh`).
 - Configured dedicated `atx` agent session in `/home/luke/bin/tmux_control` on socket `/tmp/tmux-1000/tmux_luke_atx` , styled with orange status bar (`#ff8800`), `C-b` prefix, and persistent agent environment in `~/.agent_profile` .
 - Added backup and restore scripts for `amux` (`/home/luke/git/backups/u1/scripts/backup/amux` and `/restore/amux`).
 - Documented architecture and audit procedures on [amux - Agent modified tmux](#) and [SSH & Agent Command Tracking Guide](#).
 - **Minecraft Datapack Enhancements (`poke lovers`) (`u1`):**

- Installed 5 verified Minecraft 26.3 datapacks in `/data/minecraft/pokelovers/world/datapacks/`:
 - `fast_leaf_decay` (rapid leaf decay upon log breakage)
 - `graves` (death chest/grave saving inventory and XP)
 - `invisframes` (invisible item frames via shears while sneaking)
 - `player-drops-head` (player head drops on death)
 - `shulker-drops-two-shells` (guaranteed 2 shulker shells)
- Broadcasted in-game countdown notices to online players prior to executing live `/reload`.
- **BlueMap 3D Web Map & Authentik SSO Integration (`pokelovers`) (`uL`):**
 - Deployed BlueMap 5.28 standalone CLI renderer running as `bluemap-pokelovers.service` in watch mode (`-w -u`), serving live world updates and Server-Sent Events (SSE) on port 8100.
 - Configured NGINX reverse proxy on port 443 with wildcard SSL (`*.drheck.dev`) in `/etc/nginx/sites-available/pokelovers`.
 - Gated `https://pokelovers.drheck.dev` behind Authentik ForwardAuth proxy provider and application on embedded outpost, protecting map coordinates and player builds behind authentication.
- 2026-09-26 Saturday
 - **Zero-Config Minecraft HAProxy SNI Stream Routing (`uL` , `danknasty`):**
 - Decommissioned application-level proxy (Velocity) to preserve native vanilla Diffie-Hellman encryption and Microsoft `online-mode=true` authentication.
 - Deployed HAProxy 3.4.5 on dual-stack endpoints (`10.0.0.113:25565` and `[fd77:7777:5010::1337:f1ac:d00d:3c]:25565`).
 - Implemented `/etc/haproxy/minecraft.lua` using non-draining buffer peeking (`txn.req.dup()`) to inspect the raw unencrypted Minecraft handshake packet (`0x00`), dynamically extracting the SNI virtual host (`pokelovers.drheck.dev`).
 - Routed traffic via `/etc/haproxy/minecraft_hosts.map` directly to dedicated internal ULA addresses on standard port 25565 (`[fd77:7777:5010::1337:3c:d00d:1]:25565`).
 - Implemented native fallback responder (`mc_offline`) returning custom protocol packets when backends are stopped:
 - Multiplayer Server List MOTD: `"[Server] is currently offline. Ping Luke"`
 - Multiplayer Join Screen: Immediate disconnect with red bold error: `"[Server] is currently offline. Ping Luke"`
 - **Network & DNS Automation (`ipctl`) (`uL` , `danknasty`):**
 - Developed `/data/minecraft/ipctl` (symlinked in `/home/luke/bin/ipctl`).
 - Automates ULA IPv6 allocation (`fd77:7777:5010::1337:3c:d00d:<hex>/64`) on `eth77` with `systemd-networkd` reload.
 - Automates HAProxy backend and map configuration reload.
 - Integrated SSH agent validation checking for key `ultra-arikui` (`SHA256:7Xr0vCxfpPhbKE3hN9fE2IC9y4x3Kj+kYmXwzgJY3s`).
 - Implemented 7-step automated DNS provisioning over SSH to `danknasty`: updates `~/git/router_config/unbound.conf`, validates via `unbound-checkconf`, deploys to `/var/unbound/etc/`, restarts `unbound`, verifies local resolution, and triggers `dns_danger_sync.py --force` to push public A and AAAA records to deSEC.io.

- Created dedicated backup and restore scripts in `/home/luke/git/backups/ul/scripts/backup/minecraft_router` and `/restore/minecraft_router`.
- Documented entire architecture and quickstart HOWTO on HeckWiki page 136 ([Minecraft Worlds](#)).
- **Firewall Configuration for Minecraft Port 25565 (danknasty):**
 - Configured `mc_ipv4` (`10.0.0.113`), `mc_gu` (`$gu_prefix:1337:f1ac:d00d:3c`), and `mc_ula` (`$ula_prefix:1337:f1ac:d00d:3c`) in `~/git/router_config/pf.conf`.
 - Added inbound port 25565 forwarding rules for IPv4 NAT and IPv6 ULA redirection.
 - Validated with `pfctl -nf`, deployed to `/etc/pf.conf`, loaded into the kernel, and verified reachability externally from `rng`.
- 2026-09-21 Monday
 - **Native Sunshine & Gamescope Migration on ul:**
 - Decommissioned legacy `steam-headless` container; migrated to bare-metal Gamescope DRM compositor + Sunshine host on AMD Radeon AI PRO R9700 (`1002:7551`, Navi 48).
 - Injected AOC 1080p EDID on `DP-1` via `mkinitcpio` & `systemd-boot` loader options.
 - Configured Steam library paths directly to 151TB ZFS pool (`/data/games/steam/steamapps`).
 - Resolved PS5 DualSense controller disconnection: disabled Steam proprietary HIDAPI polling (`SDL_JOYSTICK_HIDAPI_PS5=0`, `SDL_JOYSTICK_HIDAPI=0`) to prevent `hid_read` failure timeout on virtual `uhid` devices.
 - Added `-e` (`--steam`) integration flag to Gamescope launch script to ensure proper Wayland focus relaying to Steam, enabling Steam Input in-game instead of dropping to Desktop mouse layout.
 - Documented complete architecture, launch scripts, and controller gotchas on HeckWiki page 130 ([Sunshine Remote Setup](#)).
- 2026-09-21 Monday
 - **Steam Storage Migration to 151TB ZFS Pool (`/data/games/steam`) (`ul`):**
 - Discovered root NVMe filesystem at 85% utilization (71GB free).
 - Consolidated all Steam games, runtimes, manifests, and shader caches from temporary docker volumes to `/data/games/steam/steamapps/` on the 151TB ZFS pool.
 - Replaced `~/local/share/Steam/steamapps` and `~/steam/steam/steamapps` with permanent atomic symlinks pointing to `/data/games/steam/steamapps/`.
 - Cleaned `libraryfolders.vdf` ensuring 100% of game downloads route directly to `/data/games/steam/` with zero bytes hitting the root SSD.
 - **TTY1 Getty Deactivation & Display Console Fix (`ul`):**
 - Disabled `getty@tty1.service` (`systemctl disable --now getty@tty1.service`) to prevent Linux console login prompts from broadcasting over KMS on `DP-1`.
- 2026-09-20 Sunday
 - **PS5 DualSense Controller Hardware Support & uhid Activation (`ul`):**
 - Identified PlayStation 5 DualSense controller emulation failure in Sunshine due to missing `/dev/uhid` (User HID) device node.

- Loaded `uhid` kernel module and made persistent across reboots in `/etc/modules-load.d/uhid.conf`.
- Configured udev rule in `/etc/udev/rules.d/85-sunshine-uinput.rules` granting `input` group permissions to both `/dev/uinput` and `/dev/uhid` (`MODE="0660", GROUP="input"`).
- **Native Gamescope + Headless DRM Stack Migration (u1):**
 - Decommissioned legacy `steam_headless` Docker container to eliminate Xorg CPU dummy-driver bottleneck (`xf86-video-dummy`) and software rasterization (15 FPS).
 - Installed native Arch Linux gaming stack: `gamescope`, `steam`, `vulkan-radeon`, `lib32-vulkan-radeon`, `pipewire-pulse`, `wireplumber`, `seatd`, `socat`, and `sunshine-bin` (AUR).
 - Granted real-time scheduling capabilities to Gamescope (`setcap cap_sys_nice=eip /usr/bin/gamescope`) and rootless DRM frame capture to Sunshine (`setcap cap_sys_admin,cap_sys_nice=eip /usr/bin/sunshine`).
 - Configured `seatd` daemon with group `video` override in `/etc/systemd/system/seatd.service.d/group.conf` to allow Gamescope DRM session management without an active logind seat.
 - Configured Gamescope launcher script `/home/luke/bin/launch-gamescope-steam.sh` driving connector `DP-1` via `--backend drm` with RADV Vulkan acceleration on the AMD Radeon AI PRO R9700.
- **Headless Virtual Display via Boot-Time EDID Injection (u1):**
 - Resolved `*ERROR* No EDID found on connector: DP-1` kernel spam on headless AMD GPU.
 - Sourced verified 1080p 144Hz CEA-861 DisplayPort EDID (`aoc_1080p.bin`) in `/usr/lib/firmware/edid/`.
 - Packaged EDID into early initramfs via `FILES=(/usr/lib/firmware/edid/aoc_1080p.bin)` in `/etc/mkinitcpio.conf` and regenerated boot image via `mkinitcpio -P`.
 - Configured bootloader kernel parameters in `/boot/loader/entries/arch.conf`: `drm.edid_firmware=DP-1:edid/aoc_1080p.bin video=DP-1:1920x1080@60e`.
 - Pinned Sunshine KMS capture explicitly to `adapter_name = /dev/dri/card1` and `output_name = DP-1`, preventing BMC graphics capture (`VGA-1`).
- **Dual-Stack IPv4/IPv6 socat Bridge (u1):**
 - Bound native Sunshine directly to dedicated IPv6 ULA address `[fd77:7777:5010:0:1337:f1ac:d00d:4799]`.
 - Deployed `/usr/local/bin/sunshine-ipv4-bridge.sh` and systemd unit `/etc/systemd/system/sunshine-ipv4-bridge.service` listening on `10.0.0.112` and forwarding all GameStream TCP and UDP ports bidirectionally to IPv6 to prevent asymmetric routing drops on dual-stack LANs.
- **Client Authentication & Stale Certificate Remediation (u1):**
 - Diagnosed `Warning: SSL Verification error :: Client certificate identity is not enabled` (LizardByte issue #5696) caused by duplicate client certificates with conflicting UUIDs in `sunshine_state.json`.
 - Cleared stale device records in `sunshine_state.json` allowing clean one-time client pairing across desktop and TV clients.
- **NetworkManager D-Bus Mock for Steam (u1):**

- Diagnosed Steam Gamepad UI offline status (`An internet connection is required to load this content` / slashed Wi-Fi icon) caused by absence of NetworkManager on `systemd-networkd` host.
 - Implemented lightweight Python D-Bus daemon `/usr/local/bin/fake-networkmanager.py` and service `/etc/systemd/system/fake-networkmanager.service` reporting `NM_STATE_CONNECTED_GLOBAL` (70) and `NM_CONNECTIVITY_FULL` (4) to satisfy Steam network checks.
- **Documentation:**
 - Authored and published comprehensive architecture and setup runbook on HeckWiki: [sunshine remote setup](#) (Page 130).
- 2026-09-19 Saturday
 - **Sunshine Network Tuning & Steam Container Bootstrap (`u1`):**
 - Diagnosed container web assets and API communication issues on `josh5/steam-headless`.
 - Configured Sunshine CORS origins (`csrf_allowed_origins = https://sunshine.drheck.dev`) and dual-stack network settings in `sunshine.conf`.
 - Bootstrapped Steam runtime inside container and configured Steam Big Picture startup commands.
 - Authored and published initial HeckWiki guide: [Steam Streaming](#) (Page 129).
 - Updated LDAP group enrollment documentation (`ldap-sssd-client-enrollment-guide`, Page 25) with corrected repository clone instructions.
- 2026-09-18 Friday
 - **Immich Machine Learning AMD ROCm Migration (`u1`):**
 - Migrated `immich_machine_learning` from NVIDIA CUDA to native AMD ROCm: pulled `ghcr.io/immich-app/immich-machine-learning:v3.1.0-rocm`.
 - Updated `/data/docker/immich/.env` (`IMMICH_MACHINE_LEARNING_GPU_TYPE=rocm`).
 - Recreated Immich stack and verified PyTorch ROCm device detection (`torch.cuda.is_available() = True` on AMD Radeon AI PRO R9700 `gfx1201`).
 - Verified VA-API hardware video acceleration on `/dev/dri/renderD128` inside `immich_server`.
 - **Sunshine & Steam-Headless Initial Deployment (`u1` & `danknasty`):**
 - Provisioned dedicated internal IPv4 (`10.0.0.112`) and IPv6 ULA (`fd77:7777:5010:0:1337:f1ac:d00d:4799`).
 - Updated `unbound.conf` in `~/git/router_config` on `danknasty` with `sunshine.drheck.dev` A and AAAA records; deployed via `./sync_unbound`.
 - Synced public DNS records via `dns_danger_sync.py` on deSEC.io.
 - Configured `/etc/nginx/sites-available/sunshine` with Authentik ForwardAuth and deployed reverse proxy.
 - Provisioned `sunshine` application and ProxyProvider in Authentik embedded outpost.
 - Deployed `josh5/steam-headless` container in `/data/docker/sunshine/docker-compose.yml`.
- 2026-09-17 Thursday
 - **Tmux & SSH Auth Environment Maintenance (`u1`):**
 - Re-initialized Tmux Plugin Manager (`tpm`) and checked plugin compatibility (`check_tmux_version.sh`).

- Maintained persistent SSH agent socket symlinks.
- 2026-09-15 Tuesday
 - **System Package Maintenance & Initramfs Rebuild (ul):**
 - Upgraded system packages via `paru -Syu`.
 - Rebuilt `initramfs-linux-lts.img` via ALPM hooks.
 - Verified systemd service health.
- 2026-09-12 Saturday
 - **System Package Maintenance & LTS Kernel Update (ul):**
 - Upgraded system packages via `paru -Syu` / `pacman -Syu`.
 - Kernel update to `6.18.52-1-lts` and regenerated `initramfs-linux-lts.img`.
 - Re-verified NVIDIA kernel module conf test compilation checks for `580.178.04`.
 - Media library maintenance: sorted and updated Adventure Time subtitle filenames.
- 2026-09-08 Tuesday - 2026-09-11 Friday
 - **System Maintenance & Driver Toolchain Compilation (ul):**
 - Executed routine system maintenance and package updates across `ul`.
 - Kernel module conf test compilation and pacman keyring verification.
- 2026-09-05 Saturday
 - **OpenBSD Router Reinstallation & CrowdSec Perimeter Restoration (danknasty):**
 - Reinstalled and configured `crowdsec-firewall-bouncer` connecting to `ul`'s LAPI over IPv6 ULA (`http://[fd77:7777:5010:0:1337:flac:d00d:c70d]:8080/`).
 - Restored OpenBSD PF firewall tables (`<crowdsec-blacklists>`, `<crowdsec-blacklists>`, `<bruteforce>`) with rate limiting (`max-src-conn-rate 3/30`), loading ~23,880 blacklisted attacker IPs directly into kernel tables.
 - Verified remote syslog forwarding of `auth,authpriv.info` over IPv6 UDP to `ul`'s CrowdSec syslog parser.
 - **Router Network Mapping & Dynamic IPv6 DNS Cron Jobs (danknasty):**
 - Aligned network interface roles after hardware reinstallation (`em0` WAN, `em1` LAN with delegated `/64` prefix).
 - Updated interface configurations across `/etc/hostname.em0`, `/etc/hostname.em1`, `/etc/dhcp6leased.conf`, `/etc/rad.conf`, and `/etc/dhcpd.conf`.
 - Deployed dynamic deSEC.io IPv6 DNS updater (`/etc/update_dns.py`) and keepalive monitor (`/etc/ipv6_keepalive.sh`).
 - Restored root crontab on `danknasty` to run `/etc/update_dns.py` every minute and `/etc/ipv6_keepalive.sh` every 5 minutes.
 - Triggered manual sync: verified all 43 domain AAAA records updated on deSEC and verified public IPv6 reachability via `rng` to `https://auth.drheck.dev/`.
 - **Router Disaster Recovery & Reinstall Survival Automation (danknasty):**
 - Created single-command idempotent provisioning script `~/git/router_config/bootstrap.sh` (`doas ./bootstrap.sh`): installs package dependencies, copies system configs, sets file permissions and ownership, restores root crontab, applies `sysctl`, and starts all services.
 - Created zero-touch OpenBSD post-install hook `~/git/router_config/install.site` to automatically pull repository and execute `bootstrap.sh` inside `chroot /mnt` at OS installation completion.

- Added `/etc/sysctl.conf` (`net.inet.ip.forwarding=1`, `net.inet6.ip6.forwarding=1`) to repo with automated activation via `sysctl -f`.
- Added package manifests to repo: `pkglist` (generated via `pkg_info -mz` for native OpenBSD `pkg_add -I -l` restoration) and `packages.txt` (human-readable catalog with descriptions).
- Added `/etc/dhcpd.conf` (DHCPv4 server) and `/var/unbound/etc/unbound.conf` (DNS resolver) deployment and service management into `bootstrap.sh`.
- Backed up all router configuration templates into `~/git/router_config` (`boot.conf`, `ttys`, `doas.conf`, `crontab.root`, `dhcp6leased.conf`, `rad.conf`, `pf.conf`, `syslog.conf`, `rc.conf.local`, `mygate`, `crowdsec-firewall-bouncer.yaml`).
- **Nextcloud Landing Page & occ Runbook Guide ([u1](#))**:
 - Configured post-authentication redirect on `cloud.drheck.dev` to default directly to `/apps/files/files` (`occ config:system:set defaultapp files`, `occ config:app:set core defaultpage /apps/files/files`).
 - Authored and published comprehensive [Nextcloud occ Guide](#) on HeckWiki documenting command-line administration, alias setups, user management, and maintenance mode operations.
- 2026-09-04 Friday
 - **Danknasty Router Hardware & Platform Diagnostics ([danknasty](#))**:
 - Identified router hardware platform: Broachlink NOAH4C V10 (Intel Atom E3845 quad-core @ 1.91GHz, 4GB RAM, 4x Intel I210 Gigabit Ethernet ports `em0`-`em3`).
 - Enabled RJ45 serial console access on `com0` at 115200 baud via `/etc/boot.conf` (`stty com0 115200`, `set tty com0`) and `/etc/ttys` (`tty00 std.115200 vt220 on secure`).
 - Diagnosed periodic SSH responsiveness latency: traced kernel system CPU lockups and interrupt activity using `vmstat -i`, `sensorsd`, and `bsd.re-config`.
 - **Split-Horizon Unbound Authoritative LAN Resolution ([danknasty](#))**:
 - Analyzed Unbound configuration on `danknasty` acting as authoritative LAN resolver (`local-zone` / `local-data` with `aa` flag set in LAN responses).
 - Evaluated DNS high-availability options: Git-based Unbound configuration replication vs authoritative secondary migration to NSD.
- 2026-09-03 Thursday
 - **SSH CA Documentation Modularization (HeckWiki)**:
 - Cleanly partitioned SSH Certificate Authority documentation into two focused reference runbooks under the `LDAP+PAM+SSH CA` book:
 1. [SSH CA setup](#) (Page 26): Core architecture, Ed25519 CA keys, Vaultwarden storage, signing principles, and Certificate Revocation Lists (CRL).
 2. [SSH Client and Host Onboarding Guide](#) (Page 112): Step-by-step out-of-band bootstrap and verification workflows for onboarding new clients and servers without circular SSH dependencies.
- 2026-09-02 Wednesday
 - **OpenBSD Router IPv6 Dynamic DNS Rewrite (`update_dns.py`) ([danknasty](#))**:
 - Diagnosed HTTP 400 bulk update failures on deSEC.io caused by regex string parsing errors and duplicate records in `unbound.conf`.

- Replaced legacy bash/awk script (`update_dns.sh`) with robust Python 3 implementation (`update_dns.py`) using Python's native `ipaddress` library and typed dictionary deduplication.
- Added unit test suite `test_update_dns.py` with 9 unit tests verifying zone record parsing, address synthesis, and deduplication.
- Removed duplicate `libresprite.drheck.dev` entry and cleaned up interleaved records in `unbound.conf`.
- Deployed `/etc/update_dns.py` (0755 root:wheel), removed `/etc/update_dns.sh`, and signed/committed all changes to `~/git/router_config`.
- **CrowdSec Log Synchronization & False-Positive Ban Remediation (`u1` & `danknasty`):**
 - Investigated repetitive `/var/log/authlog` session spam on `danknasty`.
 - Identified redundant SSH polling in `crowdsec-sync-authlog` on `u1` running via `crowdsec-export-bans.timer` every 60s.
 - Disabled unnecessary SSH scraping, relying on native real-time UDP IPv6 syslog forwarding (`auth,authpriv.info`) from `danknasty` to CrowdSec on `u1`.
 - Resolved false-positive ban on VPS `rng` (`66.186.37.205`) in `<crowdsec-blacklists>` PF table caused by unprivileged TCP connect scans.
- **SSH CA Inventory Tracking & Streamlined Key Signing (`u1`):**
 - Implemented key archival and inventory management in `/usr/local/bin/sign-host-key` and `/usr/local/bin/sign-user-key` archiving signed public keys in `/etc/ssh/ca_inventory/{hosts,users}` with mandatory labeling for revocation tracking.
 - Built revocation utility `/usr/local/bin/revoke-ssh-key`.
 - Documented out-of-band onboarding workflow on HeckWiki.
- 2026-08-31 Monday
 - **System Package Maintenance & Toolchain Updates (`u1`):**
 - Executed system upgrades via `paru` / `pacman`.
 - Updated Haskell libraries (`haskell-uuid-types`, `haskell-vector`, `haskell-witherable`), `shellcheck`, and system info documentation.
 - Updated Opencode CLI, `csvtools`, and `nethack-git`.
- 2026-08-30 Sunday
 - **Demucs Stem Separation Deployment (`https://demucs.drheck.dev/`):**
 - Added `demucs.drheck.dev` DNS records to `unbound.conf` on `danknasty` (`~/git/router_config`).
 - Built and deployed container running Demucs v4 web service (`app.py`, HTML5 Multi-Track Mixer) on dedicated ULA IPv6 (`fd77:7777:5010:0:1337:flac:d00d:de3:8000`).
 - Supports `htdemucs_ft` (Fine-tuned 4-Stem), `htdemucs` (4-Stem), `htdemucs_6s` (6-Stem with Piano & Guitar), and `mdx_extra`.
 - Features synchronized multi-track audio playback with per-stem Solo, Mute, Volume faders, and ZIP export.
 - Provisioned Authentik ForwardAuth `demucs` ProxyProvider and Application in Authentik Embedded Outpost.
 - Configured `/etc/nginx/sites-available/demucs` reverse proxy with 512MB max body size and 600s read timeout.
 - Added firewall isolation reject rule in `/etc/nftables.conf`.

- Created `demucs` backup and restore scripts with `par2` parity in `~/git/backups`.
- 2026-08-29 Saturday
 - **Sopro V2 TTS Deployment** (`https://sopro.drheck.dev/`):
 - Enhanced web interface and backend API to expose configurable acoustic solver `Steps` (1-64 steps).
 - Added `sopro.drheck.dev` DNS records to `unbound.conf` on `danknasty` (`~/git/router_config`).
 - Built and deployed container running `soprotts serve --device cpu --host 0.0.0.0 --port 7860 --no-open` on dedicated ULA IPv6 (`fd77:7777:5010:0:1337:f1ac:d00d:509:7860`).
 - Provisioned Authentik ForwardAuth `sopro` ProxyProvider and Application in Authentik Embedded Outpost.
 - Configured `/etc/nginx/sites-available/sopro` reverse proxy with WebSocket support and pushed to `~/git/nginx`.
 - Added firewall isolation reject rule in `/etc/nftables.conf` and pushed to `~/git/configs`.
 - Created `sopro` backup and restore scripts with `par2` parity in `~/git/backups`.
 - **BentoPDF Deployment** (`https://bentopdf.drheck.dev/`):
 - Added `bentopdf.drheck.dev` DNS records to `unbound.conf` on `danknasty` (`~/git/router_config`).
 - Deployed `ghcr.io/alam00000/bentopdf:latest` container on dedicated ULA IPv6 (`fd77:7777:5010:0:1337:f1ac:d00d:bdf:8080`).
 - Provisioned Authentik ForwardAuth `bentopdf` ProxyProvider & Application in Authentik Embedded Outpost.
 - Configured `/etc/nginx/sites-available/bentopdf` reverse proxy and pushed to `~/git/nginx`.
 - Added firewall isolation reject rule in `/etc/nftables.conf` and pushed to `~/git/configs`.
 - Created `bentopdf` backup and restore scripts with `par2` parity in `~/git/backups`.
 - **SSL Certificate Automation & SSSD TLS:**
 - Fixed expired LDAP `CertificateKeyPair` inside Authentik database via `ak shell` and restarted `authentik-ldap`.
 - Deployed `/usr/local/bin/update-authentik-cert.sh` automated renewal hook in `acme.sh` configuration with `/etc/sudoers.d/acme_ssl` NOPASSWD grant.
 - **Docker .env & Secret File Hardening:**
 - Stripped POSIX extended ACLs (`setfacl -b`) across all `.env` files and SSH keys in `/data/docker/`.
 - Restricted permissions to `0640 root:docker-data` and parent directories to `0750`.
 - **Universal Admin Account Transition:**
 - Transferred administrative roles to `akadmin` / `admin` across Authentik, Gitea, Immich, Anchor, BookStack, Nextcloud, Kavita, Navidrome, and RomM.
 - Demoted `luke` to standard user on web applications while preserving `wheel` (sudo) access on host OS.
 - **PostgreSQL Authentication Hardening:**

- Removed obsolete `0.0.0.0/0` and `::/0` wildcard rules for non-existent `infisical` role from `/data/postgres/data/pg_hba.conf`.
- **nftables Egress Isolation (chain output):**
 - Added reject rules (`meta skuid != { 0, 33, 1101 } reject`) in `chain output` for all 26 active ULA IPv6 backend services to prevent unprivileged local processes on `ul` from bypassing Authentik ForwardAuth.
 - Tracked `/etc/nftables.conf` in `~/git/configs/nftables.conf`.
- **Nginx Hash Table Performance Tuning:**
 - Added `variables_hash_max_size 2048;` and `variables_hash_bucket_size 128;` to `/etc/nginx/nginx.conf` and pushed to `~/git/nginx`.
- **Authentik 2026.8.0 Outpost & OIDC Remediation:**
 - Populated missing `authentication_flow` (`default-authentication-flow`) and `invalidation_flow` (`default-invalidation-flow`) UUIDs across all 19 `ProxyProvider` database records, fixing Rust Embedded Outpost deserialization crash and restoring ForwardAuth across all services.
 - Updated OpenID `email` ScopeMapping expression to enforce `email_verified = True` for Better-Auth (WIPStudio) / SSO client logins.
- **Cockpit Removal:**
 - Uninstalled `cockpit` and `cockpit-docker` packages; purged `/etc/motd.d/cockpit`, `/etc/issue.d/cockpit.issue`, and `/run/cockpit`.
- **Arch .pacnew Merge & Maintenance:**
 - Adopted updated upstream makepkg drop-ins and TPM2 FAPI JSON profiles.
 - Tuned `/etc/pacman.conf` with `DownloadUser = alpm` and `ParallelDownloads = 5`.
 - Cleaned all lingering `.pacnew` files in `/etc/`.
- **BM095 Display Mirroring (~/git/audio_config):**
 - Installed `wl-mirror` on `bmo95` and configured Sway (`common/sway/config`) to mirror DisplayPort `DP-3` to HDMI `HDMI-A-1` (TV) via zero-copy DMA-BUF.
 - Consumed Sway configuration into `~/git/audio_config` and committed changes.
- **Studio Control (scontrol) UI & Toggle Controls:**
 - Added `POST /api/power/{device}/{action}` supporting individual Sub-GHz RF outlet toggling (`pa`, `sub`, `rack`, `computer`, `tv`, `newer`, `mrc`, `all`) and `POST /api/atx/{action}` for PiKVM motherboard ATX button clicks.
 - Added **Individual Power Controls** view with dedicated toggle buttons and view-switcher button to `scontrol.drheck.dev`.
 - Checked in and pushed to `https://git.drheck.dev/luke/scontrol.git`.
- **Kavita Arch Linux / AUR Upgrade & Database Migrations (ul):**
 - Checked SQLite database integrity on `/opt/kavita/config/kavita.db` (`PRAGMA integrity_check`).
 - Created safety database backup at `/opt/kavita/config/kavita.db.pre_0.9.1_upgrade`.
 - Restarted `kavita.service` following `paru` upgrade to Kavita `v0.9.1.0`.
 - Executed automatic backup (`/opt/kavita/config/temp/migration/0.9.0.2`) and applied database migrations (`MetadataSettingFieldRenummer`, `ManualMigrateOriginalNameBackfill`, `ManualMigrateNormalizedOriginalNameBackfill`, `ManualMigrateLastReadDates`, `ManualMigrationExternalSeriesMetadataIds`, `ManualMigrationCorrectAuditStatus`).

- Verified service initialization and HTTP 200 on `http://[fd77:7777:5010:0:1337:flac:d00d:7ead]:5000/`.
- **Full Docker Fleet Update & Service Migrations (u1):**
 - **Authentik:** Created PostgreSQL database backup at `/tmp/authentik_pre_upgrade.dump`. Upgraded `server`, `worker`, and `ldap` to `2026.8.0`. Applied blueprint and Django migrations across all applications. Verified `email_verified: True` in `ak shell` scope mapping and tested `https://auth.drheck.dev/`.
 - **Infra (Valkey):** Upgraded shared Redis/cache container to `valkey/valkey:8.1-alpine` (v8.1.9). Verified active session reconnection for Authentik, Immich, and Nextcloud.
 - **Immich:** Upgraded `immich-server` and `immich-machine-learning` to latest `v3.1.0` builds with GPU acceleration. Verified `https://photos.drheck.dev/`.
 - **Kasm Workspaces:** Upgraded manager container to `lscr.io/linuxserver/kasm:latest` (Kasm 1.19.0). Initialized internal services and verified `https://kasm.drheck.dev/`.
 - **BookStack:** Upgraded `bookstack` (v26.05.4) and internal `mariadb:latest`. Verified Laravel migrations and `https://wiki.drheck.dev/`.
 - **Penpot:** Upgraded `frontend`, `backend`, `exporter` (v2.17.2), `postgres:15.19`, and `redis:7`. Verified `https://penpot.drheck.dev/`.
 - **Anchor:** Upgraded image tag to `ghcr.io/zhfahim/anchor:0.16.0`. Executed database schema migrations and verified `https://keep.drheck.dev/`.
 - **Vaultwarden:** Upgraded to `vaultwarden/server:latest` (v1.37.2). Verified `https://pw.drheck.dev/`.
 - **Navidrome:** Upgraded to `deluan/navidrome:latest` (v0.63.2). Verified web and Subsonic API endpoints on `https://navidrome.drheck.dev/` and `https://music.drheck.dev/`.
 - **WebShell / Step-CA:** Upgraded `smallstep/step-ca:latest` (v0.30.2). Verified HTTPS on port 9000.
 - **WIPStudio / MinIO:** Upgraded storage backend to `minio/minio:latest`.
 - **YOURLS:** Upgraded `yourls:latest` (1.10.5) and internal `mariadb:10.11`.
 - **Drawpile:** Upgraded server to `drawpile/drawpile-srv:2` (2.3.0). Verified TCP/WebSocket listeners on ports 27750-27752.
 - **Stateless Web Services:** Upgraded `wick` (`nginx:alpine`), `webrcade` (`webrcade:latest`), `excalidraw` (`excalidraw:latest`), and `tldraw` (`ratneo/tldraw:latest`).
 - **Offsite Cloud Backups:** Executed full service backups and synced to Google Drive and Proton Drive via rclone (`2026-08-29_112824`).
- 2026-08-28 Friday
 - **Funkwhale Audio Streaming & Range Request Fix (u1):**
 - Diagnosed audio playback failures and stream disconnects on Funkwhale API endpoints (`/api/v1/listen/.../?upload=...` and transcoded audio streams).
 - Resolved Nginx reverse proxy byte-range streaming failure (`206 Partial Content`) by updating `/data/docker/funkwhale/funkwhale_nginx.template` and volume mounting custom `/data/docker/funkwhale/mime.types` inside the container.

- Recreated container and verified byte-range audio playback via `curl -i -r 0-65535` returning HTTP `206 Partial Content`.
 - Updated Funkwhale backup and restore scripts (`/home/luke/git/backups/u1/scripts/backup/funkwhale` and `restore/funkwhale`) to include `mime.types` and `funkwhale_nginx.template` in backup tarballs (verified with `shellcheck`).
- 2026-08-27 Thursday
 - System Package Maintenance & Kernel Audit (`u1`):**
 - Executed system package upgrades via `paru -Syu` / `pacman -Syu`.
 - Updated mirrorlist and restarted `reflector.service`.
 - Verified kernel image and module consistency using `kernel-check` against `/boot/vmlinuz-linux-lts`.
- 2026-08-26 Wednesday
 - Studio Control Gateway & ATX Power Automation (`u1` & `pikvm-studio`):**
 - Integrated ATX motherboard power button controls (`kvmd-cli atx`) into `studio-power` CLI and synchronized executable between `u1` and `pikvm-studio`.
 - Resolved container DNS and IPv6 resolution for `bmo95.drheck.dev` inside `scontrol` Docker container on `infra_net` bridge.
 - Updated and redeployed `app.py` in `/data/docker/scontrol` and committed changes to `/home/luke/git/scontrol`.
- 2026-08-24 Monday
 - Studio PiKVM Hardware & Perimeter Ingress Security (`u1` & `pikvm-studio`):**
 - Configured dual-hostname architecture: `studio-kvm-ssh.drheck.dev` (direct hardware & SSH) and `studio-kvm-web.drheck.dev` (Authentik-gated Web UI).
 - Implemented kernel-level outbound firewall isolation in `/etc/nftables.conf` (`chain output`) on `u1` blocking non-root, non-nginx (`http`, UID 33) users from connecting to PiKVM ports 80/443.
 - Configured Pre-Shared Proxy Secret Header (`X-Proxy-Secret`) in `/etc/nginx/certs/studio_secret.conf` (mode `0600`, owned by `http:http`).
 - Configured Mutual TLS (mTLS) with internal CA and client certificate authentication (`/etc/nginx/certs/pikvm_ca.crt`, `pikvm_client.crt`, `pikvm_client.key`).
 - Updated Authentik `ProxyProvider` and `Application` (`Studio PiKVM`) with implicit consent (`default-provider-authorization-implicit-consent`) and group `studio` access restriction.
 - Set `kvmd.auth.enabled: false` in `/etc/kvmd/override.yaml` (committed in `/home/luke/git/pikvm_studio`).
 - Updated [Studio PiKVM & Studio Control Gateway](#) documentation.
 - Studio Control Gateway Deployment (`scontrol.drheck.dev`) (`u1`):**
 - Developed and deployed asynchronous FastAPI orchestration service (`scontrol`) in `/data/docker/scontrol` binding to dedicated ULA IPv6 address `[fd77:7777:5010:0:1337:f1ac:d00d:5c01]:8000`.
 - Implemented tactile mobile-optimized dark UI with dynamic state buttons, live monospace console, and status indicators.
 - Generated dedicated service ed25519 key (`/data/docker/scontrol/id_scontrol`) registered in `luke@studio-kvm-ssh.drheck.dev:~/.ssh/authorized_keys`.

- Integrated real-time Server-Sent Events (SSE) streaming pipeline (`/api/stream/on` and `/api/stream/off`):
 1. RF Power Outlets: switches all 7 studio devices via `studio-power all on` over SSH.
 2. ATX Motherboard: queries PiKVM `/api/atx` and pulses motherboard power button if off.
 3. Studio PC Boot: probes DNS hostname `bmo95.drheck.dev` with a 100-second boot timeout.
 4. Soundcards & Audio: audits ALSA/JACK multi-channel recording interfaces.
- Created Nginx ForwardAuth reverse proxy configuration `/etc/nginx/sites-available/scontrol` (symlinked to `/etc/nginx/sites-enabled/scontrol`) with SSE buffering bypass.
- Configured Authentik `ProxyProvider` and `Application` (`Studio Control`) bound to Authentik Group `studio`.
- Created Git repository at `/home/luke/git/scontrol` tracking `build.sh` (verified with `shellcheck`), `Dockerfile`, `entrypoint.sh`, `app.py`, `docker-compose.yml`, `templates/index.html`, and `README.md`.
- Created, tested, and verified backup/restore scripts (`scontrol_backup` and `scontrol_restore` in `/home/luke/git/backups/ul/scripts/`) with `par2` 10% redundancy.
- **Studio PC (`bmo95`) Boot & Audio Stack Audit:**
 - Resolved `libkmod: ERROR: conf_files_filter_out: Cannot stat directory entry: /etc/modprobe.d/no_intel_sound.conf` by replacing early-boot symlink with a direct regular file (`blacklist snd_hda_intel`).
 - Verified 4x Echo AudioFire 12 FireWire interfaces (`hw:AudioFire12,0` .. `hw:AudioFire12,3,0`), Emagic Uinitor8 USB MIDI interface, `jackd`, `zita-a2j` / `zita-j2a` bridges, and autostarting `ardour.service` DAW instance.
- **SSH Command Tracking Enhancement (`ul`):**
 - Upgraded `/usr/local/bin/audit-log` helper script to automatically decode hexadecimal kernel byte strings into plaintext and sort rotated log files (`audit.log.*`) in chronological order.
 - Updated [SSH Command Tracking Guide](#) documentation.
- 2026-08-22 Saturday
 - **Sub-GHz RF Studio Power Automation (`pikvm-studio`):**
 - Integrated Great Scott Gadgets YARD Stick One (`1d50:605b`, CC1111) on `pikvm-studio` to switch 433.92 MHz RF wireless power relays.
 - Reverse-engineered 33-bit Princeton / Fosmon PWM baseband protocol ($\$T_e = 291.27 \mu\text{s}$, 3433.22 baud).
 - Identified and resolved critical CC1111 24.0 MHz reference crystal mismatch (recalculated `FREQ = 0x121473` from 26.0 MHz default `0x10B071`, resolving a 33 MHz carrier transmission error).
 - Resolved double sync gap bug and configured 30-frame contiguous burst streaming (630 bytes, 1.468 s) to satisfy superheterodyne receiver AGC settling.
 - Installed `/usr/local/bin/studio-power` CLI tool managing all 7 studio devices and whole-studio batch switching.

- Built standalone C direct transceiver utilities (`yard_tx.c`, `flipper_replay.c`, `cc1111_rfc4105.h`) with `libusb-1.0`.
- Created, configured, and pushed Gitea repository at [studio_yardstick](#).
- [Documentation](#)
- **PiKVM GPG / Pass Pinentry TUI Fix (`pikvm-studio`):**
 - Resolved `gpg: public key decryption failed: Screen or window too small` when executing `gpush pass` in subshell pipes.
 - Configured `/home/luke/.gnupg/gpg-agent.conf` with `pinentry-program /usr/bin/pinentry-tty` and `allow-loopback-pinentry`.
 - Configured `export GPG_TTY="$(tty)"` and `gpg-connect-agent updatestartuptty /bye` in `~/.bashrc` on `pikvm-studio`.
- **48-Channel FireWire Synchronous Audio Stack (`bmo95`):**
 - Consolidated 4x Echo AudioFire12 interfaces into a sample-accurate 48-channel synchronous recording engine on Linux 6.13 PREEMPT_RT kernel.
 - Established hardware color mapping (`Red` Master `fc79`, `Blue` Slave 1 `9815`, `Green` Slave 2 `8525`, `Yellow` Slave 3 `94e8`) with 75Ω BNC Word Clock daisy-chain wiring.
 - Configured master `jackd` bound to `Red` with synchronous `zita-a2j` / `zita-j2a` duplex ALSA bridges (locked at $\rho = 1.000000000000$).
 - Conducted 10-minute continuous 1 kHz stress test proving absolute phase synchronization (0.000 ms / 0 samples drift across 28.8M samples).
 - Deployed systemd user services (`jack.service`, `zita-*`, `{blue,green,yellow}.service`) and canonical port alias mapping (`Red_01..12`, `Blue_01..12`, `Green_01..12`, `Yellow_01..12`).
 - [Documentation](#)
- **Studio Hardware Documentation ([Setup Detail](#)) (`u1`):**
 - Published comprehensive hardware register maps, wiring diagrams, and automation runbooks for the recording studio, audio stack, and RF power systems under the new [Setup Detail](#) book.
- **BookStack KaTeX TeX Math & Typography Integration (`u1`):**
 - Globally enabled **KaTeX 0.16.11** client-side LaTeX math rendering across BookStack via `app-custom-head`.
 - Implemented a CSP `strict-dynamic` compliant nonced JavaScript loader to dynamically load KaTeX assets without violating browser security policies.
 - Published the [Meta: Wiki Capabilities, TeX Math & Typography Reference](#) guide documenting TeX math syntax, Japanese Furigana (`<ruby>`), callout alert banners, and collapsible accordions.
 - Updated the [Agent Guide: Updating BookStack Wiki Pages](#) with typography standards, CLI helper workflows, and operational gotchas.
 - Verified automated backup and restore scripts (`/home/luke/git/backups/u1/scripts/{backup,restore}/bookstack`) properly archive and restore database settings and media with `par2` parity.
- 2026-08-20 Thursday
 - `pikvm-studio` (PiKVM V4 Plus) Configuration & Dotfile Management:

- 1080p60 Video Pass-Through & Capture Optimization:
 - Imported and applied the `v4plus.no-1920x1200` EDID preset via `kvmd-edidconf` to lock capture to uncropped 1920x1080 @ 60Hz.
 - Enabled `gpu_freq=700` in `/boot/config.txt` for H.264 60fps hardware encoding boost.
 - Configured `h264_boost: true` and `desired_fps: 60` in `/etc/kvmd/override.yaml`.
- Chezmoi Configuration Repository Setup:
 - Installed and configured `chezmoi` on `pikvm-studio` (`~/.config/chezmoi/chezmoi.yaml`) with `sourceDir: ~/git/pikvm_studio` and `destDir: /`.
 - Established clean 2-stage signed Git history: baseline vanilla OS configuration followed by 1080p60 optimizations.
 - Connected and pushed repository to Gitea (`https://git.drheck.dev/luke/pikvm_studio.git`) via `gpush`.
- SSH Auth Socket & GPG Agent Fixes:
 - Resolved SSH key retention issue in `/home/luke/bin/auth_socket.sh` by prioritizing existing live agent sockets and testing responsiveness with `ssh-add -l` rather than relying on obsolete PID suffix parsing.
 - Cleaned up stale lockfiles in `~/.gnupg/` on `pikvm-studio` and configured `pinentry-program /usr/bin/pinentry-curses` in `~/.gnupg/gpg-agent.conf`.
 - Successfully committed and pushed updated password store entry (`gitea/token/pikvm_studio`) via `gpush pass`.
- HeckWiki Documentation & Host Maintenance:
 - Authored and verified HeckWiki documentation pages for [pikvm-studio](#) and [automation](#).
 - Verified LTS kernel update (`kernel-check`), performed planned system reboot on `ul`, and verified all running systemd services and Docker containers via `status_all`.
- 2026-08-19 Wednesday
 - VPS rng Assessment & Infrastructure Monitoring Plan:
 - Inspected VPS `rng` (`rng.drheck.dev`) hardware resources, memory, disk, network, and listening services.
 - Authored and published the [Infrastructure Monitoring & Alerting Plan](#) on HeckWiki detailing metrics, alerting strategy, and agent deployment.
 - PiKVM Network Configuration:
 - Verified dual-stack IPv4/IPv6 reachability and latency response (`fping`) for `pikvm-studio`.
 - Added host entry and identity mapping in `~/.ssh/config` for direct SSH connectivity.
 - System Package & Media Maintenance:
 - Upgraded host packages via `paru -Syu` including Java runtime environment updates.
 - Built and installed latest `nethack-git` (5.0.0 release) from AUR.
 - Restarted `plexmediaserver` and monitored service journal logs.
- 2026-08-18 Tuesday

- ul NVIDIA Driver Upgrade & Container CDI Fix:
 - Diagnosed Immich Outage: Immich server (`immich_server`) and machine learning (`immich_machine_learning`) exited (127) after host NVIDIA driver upgrade (`580.173.02` → `580.178.04`). The OCI runtime failed mounting `/usr/lib/libEGL_nvidia.so.580.173.02` due to obsolete paths in `/etc/cdi/nvidia.yaml`.
 - Regenerated CDI Spec & Restored Services: Ran `nvidia-ctl cdi generate --output=/etc/cdi/nvidia.yaml` to update the CDI specification for `580.178.04`, restarted the Immich container stack, and verified healthy container status and restored upstream proxying via Nginx (`photos.drheck.dev`).
 - Automated via Pacman Hook: Created `/etc/pacman.d/hooks/nvidia-cdi.hook` with a `PostTransaction` trigger on `nvidia*` and `*nvidia*` packages to automatically regenerate `/etc/cdi/nvidia.yaml` on future `paru`/`pacman` driver updates.
- Opencode Wiki Skill & Knowledge Integration:
 - Embedded HeckWiki / BookStack management rules and helper workflows into global Opencode instructions (`~/.config/opencode/INSTRUCTIONS.md`).
 - Created dedicated skill `~/.config/opencode/skill/update-wiki/SKILL.md` for seamless automated wiki editing and querying.
- Funkwhale Album Track Ordering Fix:
 - Diagnosed track numbering and sort discrepancy in Funkwhale where album and artist views displayed tracks out of sequence.
 - Directly updated track `position` attributes and calibrated `creation_date` timestamps in the Funkwhale database via Django management shell (`/app/api/manage.py shell`) for Album 10 so both default chronological sorting and album sequence sorting correctly align.
- 2026-08-17 Monday
 - bmo95 Arch Linux Boot & dmesg Diagnostics & Resolution:
 - Resolved FireWire Audio Crash Loop & Massive dmesg Spam:
 - Diagnosed >50,000 repeating kernel errors (`snd_fireworks fw1.0: oPCR0: plug is already in use`) and FireWire CMP stack trace warnings (`sound/firewire/cmp.c:300 / cmp.c:193`).
 - Fixed missing ALSA period count in `zita-j2a.service` and `zita-a2j.service` by adding `-n 3` (required by `snd_fireworks` driver) and fixed client naming (`-j Up` / `-j Up_In`).
 - Cleaned up `set-port-aliases.sh` to remove conflicting `pkill -9` invocations and background spawns that were killing services mid-handshake and wedging the FireWire CMP isochronous plug state.
 - Fixed hardware clock synchronization sequence: moved clock configuration into `firewire-ready.service` (`wait-for-firewire.sh`) using dynamic GUID-to-node matching (`0x00148602c583fc79` → Internal Master, `0x001486a296a59815` → Word Clock Slave) with a 2-second bus settling delay before starting JACK.
 - Verified full 24-channel capture/playback routing stably running in JACK with zero kernel errors on boot.
 - Udev Rules & System Tuning:

- Fixed udev substitution syntax in `50-firewire-irq.rules` (piping `pgrep` into `xargs` to avoid invalid `$( )` substitution error in `udev`).
 - Fixed quote syntax and `power/control` attribute assignment in `50-usb-midi.rules` for low-latency Emagic Unit8 USB MIDI operation.
 - Configured `WIRELESS_REGDOM="US"` in `/etc/conf.d/wireless-regdom`.
 - Wireless Regulatory Database: Installed `wireless-regdb` package to resolve Direct firmware load for regulatory.db failed with error -2.
 - PCIe Correctable AER Timeouts: Added `pci=noaer` to `GRUB_CMDLINE_LINUX_DEFAULT` in `/home/luke/git/audio_config/common/grub` and regenerated GRUB config to eliminate spurious correctable error logging from the ASMedia USB 3.1 controller.
 - ASUS ACPI SuperIO Hardware Monitor Conflict: Added `acpi_enforce_resources=lax` to GRUB kernel parameters to resolve ACPI OpRegion conflict on ASUS PRIME Z270-A motherboard.
- 2026-08-16 Sunday
 - bmo95 Audio Workstation Infrastructure & Low-Latency Tuning:
 - Multi-Profile Audio Config Repo: Established `/home/luke/git/audio_config` git repository tracking audio profiles (`jack-alsa`, `pipewire`), metadata mappings (`filedata.json`), and custom management scripts (`apply-profile`, `consume`).
 - Sound Card & Clock Synchronization: Configured dual Echo AudioFire12 interfaces with forced internal clock on primary card (Node 1 / Bottom card) and Word Clock sync on secondary card (Node 2 / Top card).
 - ALSA + JACK2 Engine Setup: Configured JACK2 server via ALSA backend (48kHz / 512 period / 3 buffer) for low-latency audio processing.
 - Systemd User Service Modularization: Modularized JACK audio services into individual systemd user units (`jack.service`, `firewire-ready.service`, `zita-j2a.service`, `zita-a2j.service`, `a2jmidid.service`, `jack-aliases.service`, `patchage.service`, `ardour.service`).
 - Custom Port Aliases & Metadata: Scripted automatic routing and pretty-name metadata (`Down_01`..`Down_12` and `Up_01`..`Up_12`) for hardware inputs and outputs.
 - Realtime System & Kernel Tuning: Configured GRUB kernel parameter `threadirqs`, udev rules for FireWire IRQ thread scheduling (`50-firewire-irq.rules`), HPET/RTC audio timers, `sysctl` swappiness, and PAM realtime privileges.
 - Software & Documentation: Enabled Ardour 9 integration (`use-jack-pretty-names`) and added comprehensive architecture and routing documentation (`README.md`).
 - System SSH Audit Logging Setup on bmo95:
 - Installed `audit` package, enabled `auditd`, and configured `/etc/audit/rules.d/execve.rules` with strict `audit >= 1000` human session command tracking.
 - Deployed `/usr/local/bin/audit-log` execution tracking script.
- 2026-08-12 Wednesday
 - BookStack Wiki & Nginx Reverse Proxy SSO Integration:
 - Reverse Proxy Routing: Configured Nginx `/login` redirect behavior.

- Unauthenticated Homepage Auto-Redirect: Implemented DOMContentLoaded JavaScript trigger in BookStack's `app-custom-head` setting.
- Ensured unauthenticated visitors accessing `https://wiki.drheck.dev/` are automatically forwarded to Authentik (`/login`), while keeping deep links (e.g. `/books/...`) publicly viewable.
- this is for convenience, not security. I just don't want to click in "login" if I visit [wiki/](https://wiki.drheck.dev/)
- 2026-08-10 Monday
 - Opencode CLI Agent Configuration & Setup:
 - Configured Opencode settings (`opencode.json` / `opencode.jsonc`) and system instructions.
 - Added instruction mandate to comment bash tool command batches.
 - Deployed global Opencode skills under `~/.config/opencode/skill/`.
 - SSH Audit Logging & Command Tracking:
 - Configured Linux `auditd` rules on `ul` for `audit >= 1000` system call executions.
 - Configured OpenBSD process accounting (`acct`) and verbose SSH payload auditing on `danknasty`.
 - Implemented unified `audit-log` CLI helper scripts across both machines.
 - Documented SSH command tracking guide and created `daily-change-list` skill.
- 2026-08-09 Sunday
 - [documenting services](#)
 - in this process saw that kavita permissions were messed up, fixed
 - saw that moebius is like halfway removed but don't know why, leading to the realization that I need to track commands.
 - [SSH Command Tracking](#)
 - now I remember why it was removed, because it sucks. The "web service" is just a viewer for multiple drawers connecting with thier own clients.
 - some updates to the crowdsec blocks. realized it has crowd sourced blocking rules, not sure about implementing them though.
- 2026-08-08 Saturday
 - setting up navidrome, and other audio related software.
 - put albums up on funkwhale
 - power outage caused IPv6 netblock to change, the IPv6 update scripts still suck. Tried to make them better
 - had AI write a script to pull down missing artwork for Jellyfin
 - noticed collation version mismatch when poking around in postgresql.
 - created a short-link service
 - `drheck.dev/$short_link`
 - editable at `drheck.dev/admin`

1. Check Which Databases Have Collation Version Mismatches

```
sudo -u postgres bash -c 'for db in $(psql -At -c "SELECT datname FROM pg_database WHERE datistemplate = false;"); do
    echo "=== DATABASE: $db ==="
```

```
psql -d "$db" -c "SELECT 1;" 2>&1
done'
```

2. Run amcheck to Detect Corrupted B-Tree Indexes

```
sudo -u postgres bash -c '
for db in spacebar immich nextcloud_db anchor authentik postgres gitea nextcloud; do
  echo "=== AMCHECK: $db ==="
  psql -d "$db" -c "
    CREATE EXTENSION IF NOT EXISTS amcheck;
    SELECT c.relname, bt_index_check(c.oid, true)
    FROM pg_index i
    JOIN pg_class c ON c.oid = i.indexrelid
    JOIN pg_namespace n ON n.oid = c.relnamespace
    WHERE c.relkind = 'i' AND i.indisready AND
i.indisvalid AND n.nspname = 'public';" 2>&1
done'
```

3. Reindex Databases and Refresh Collation Versions

```
sudo -u postgres bash -c '
for db in spacebar immich nextcloud_db anchor authentik postgres gitea nextcloud; do
  echo "=== REINDEXING & REFRESHING: $db ==="
  psql -d "$db" -c "REINDEX DATABASE \\\\\"$db\\\\\\";"
  psql -d "$db" -c "ALTER DATABASE \\\\\"$db\\\\\\" REFRESH COLLATION VERSION;"
done'
```

4. Verify All Warnings Are Cleared

```
sudo -u postgres bash -c '
for db in $(psql -At -c "SELECT datname FROM pg_database WHERE datistemplate =
false;"); do
  echo "=== VERIFY: $db ==="
  psql -d "$db" -c "SELECT 1;" 2>&1
done'
```

- 2026-08-05 Wednesday
 - updates to crowdsec
 - parsing more SSH errors
 - generated a table of banned IPs but it's not very interesting. Live world view would be cooler
- 2026-08-04 Tuesday
 - docker updates
 - anchor: 0.13.0 → 0.14.0
 - authentik: 2026.5.5 → 2026.5.6

- bookstack: Updated to latest image
- immich: v3.0.3 → v3.1.0
- infra (valkey): Updated to latest image build
- kasm: Updated to latest image
- nextcloud: 34.0.1-apache → 34.0.2-apache
- penpot: Frontend, backend, exporter, postgres, and redis updated
- romm: Updated to latest image (5.1.0)
- vaultwarden: Updated to latest image
- webrcade: Updated to latest image
- wick: Updated to latest image
- installed crowdsec
 - review of publicly accesible service logs (eg: wiki) shows no bot traffic (yet)!
 - review of nginx logs straight from the public IPs shows bot traffic looking for common vulnerabilities, exploits, and staged malware.
 - [documentation](#)
- 2026-08-03 Monday
 - pull all new docker images and prepare for update
 - in preparation for more users, ensure unencrypted backups aren't world readable
 - gdrive backup credentials failed again
 - finally cleaned up google cloud project, renamed properly and created two separate subprojects, google sso, and rclone for ul
 - redid the certs for rclone, tested good
 - ran a backup to repare for docker update and all the online backups had no files except the instructions!
 - setting all the backups to root rendered the rclone script useless.
 - Trying all backup files owned by my user with a plan
 - create a dedicated backup user
 - create a new gpg key for backups
 - backup gpg key
 - move rclone credentials to backup user
 - chown all backups to 700 backup user
 - Profit!
- 2026-08-02 Sunday
 - Removed old unused "web shells" like the old ttyd, whatever else. Also warpgate.
 - Made webshell awesome. Picked a single font, created a service to show ANSI art on login
 - made big improvements to ansview
 - first render is completely in memory, remove all jumps and relative and exact positions. This allows the final product to be rendered correctly when not placed at the first screen column.
 - due to this success, added an auto wide mode, if artwork can fit on the screen multiple times horizontally, do it
 - also truncate the artwork if viewing on a smaller screen rather than an awful wrap. This is great for the phone shell.
- 2026-08-01 Saturday

- Created webshell, and spent a lot time trying to make it customizable per user. This was a failure.
- 2026-07-31 Friday
 - Set up moebius in KASM, generated a [KASM setup guide](#).
- 2026-07-30 Thursday
 - giving up on warpgate for now, trying ttyd again with step-ca to tie it into OIDC. I really want an authentik OIDC enabled direct web -> shell.
- 2026-07-28 Tuesday
 - got warpgate to stop crashing but I'm not sure how I can use it for a web based terminal.. we'll see
- 2026-07-26 Sunday
 - accidentally blocked the git users with the new firewall rules, allowed it to access the gitea service and we are able to upload again
 - started to set up [warpgate](#) as it looks like it can provide a shell that can login with OIDC
- 2026-07-25 Saturday
 - replaced gemini-cli with opencode, it's way better
 - went through each docker service moving off of the default 1000 UID
 - removed broken web "shells"
 - Made a process to generate short lived ssh certs for web users to get a shell without typing a password but it felt really insecure and I think you could impersonate other users, so I killed it.
- 2026-07-23 Thursday
 - Set nginx to cache large uploads on the ZFS array as / was filling up with video uploaded from immich
 - Set permanent redirects on short names in the browser for convenience, eg: `http://photos -> https://photos.drheck.dev/`
- 2026-07-22 Wednesday
 - Configured rclone for Google drive and Proton drive. [Added](#) this to the backup scripts. Now we have automated on-line backups.
 - created rclone client config in Google's [cloud console](#)
- 2026-07-21 Tuesday
 - transmission would timeout quickly since exposed behind authentik. After some research I modified the nginx config to start forwarding `$host`, `$remote_addr`, `$proxy_add_x_forwarded_for`, and `$scheme`.
- 2026-07-20 Monday
 - IPv6 netblock was wrong again. This time an IPv6 netblock change was detected then the network went out. This caused the API call to desec.io to fail. We were writing the new IPv6 netblock unconditionally though so no more updates were going to happen. Script is updated [1](#) [2](#)
 - also added logging to the desec.io call in change 2 ^
- 2026-07-19 Sunday
 - Tested LDAP users
 - could log in but did not have the ability to choose the window environment
 - [LDAP](#) guide updated to fix this problem

- 2026-07-17 Friday
 - [LDAP](#) guide updated to add `systemd` to `shadow` for NSS. This was breaking the graphical boot environment on Mitsuki's laptop.
 - [write-up](#)
- 2026-07-16 Thursday
 - [router updates](#)
 - Remote IPv6 was not updated in public DNS. The router update script was failing to execute in cron
 - shebang was `/usr/local/bin/bash` but
 - cron executed `/bin/ksh $script...` (just openbsd things!)
 - fixed
 - also router IPv6 [update script updated](#) to use persistent storage for IPv6 address as a reboot would remove the older address
 - bad firewall rule forwarded all IPv6 traffic arriving on 22 to ul
 - fixed
- 2026-07-13 Monday
 - created [ldap enable](#) doc and test on desktop
 - works!
 - completed SSH [cert setup](#) for desktop
 - works!
 - drafted a process to [auto generate ssh keys and sign them with authentic](#)
- 2026-07-12 Sunday
 - created "admin" specific firefox profile on desktop
 - cleared all old disparate passwords for the old individual service passwords
 - fixed www server for mitsuki
 - checked in [kanji service](#) in [gitea](#)
 - added bounding boxes
 - changed the stroke order color to be more legible and not run into the background
- 2026-07-11 Saturday
 - created this server change log
 - added "backup_all" script to run each service backup
 - finally [checked in](#) backup/restore scripts
 - separated backup output into current and all previous to simplify disk backup
 - modified nginx config for immich, upload cap 30GB -> 100GB

Revision #43

Created 2026-07-14 04:04:22 UTC by admin

Updated 2026-10-21 14:28:33 UTC by luKe