Hydra Cluster Audit Report

Comprehensive Discovery, Cleanup & Hardening

Infrastructure Team
SUNY New Paltz Computer Science

February 4, 2026

Contents

1 Executive Summary

This document records the full audit, cleanup, and hardening of the 3-node Hydra RKE2 Kubernetes cluster performed on February 4, 2026. Key actions taken:

Completed Actions:

- Disabled host-level MariaDB systemd service (duplicate of Docker container)
- Disabled and masked Samba (smbd/nmbd) — no configured shares, ports 139/445 closed
- Deleted 4 orphaned ZFS storage classes (hydra-hot, hydra-warm, hydra-cold, hydra-gpu)
- Backed up all Docker Compose files, Apache configs, .env files, Traefik dynamic configs
- Dumped CS Lab MariaDB data (5 MB) for migration to SQLite
- Created K8s IngressRoute manifests for all services (replacing Apache proxy rules)
- Created K8s manifests for CS Lab website (single-pod with SQLite)
- Audited Chimera and Cerberus (both clean — no Samba, RKE2 agents healthy)
- Archived and removed `/var/www` static content (∼436 MB)
- Archived Apache configuration files
- Cleaned stale Docker resources
- Verified /etc/hosts consistency on all 3 nodes

In Progress:

- CS Lab MariaDB → SQLite migration and single-pod deployment
- Traefik IngressRoute application and testing
- GPU operator DaemonSet node affinity fixes
- Docker Traefik → K8s Traefik consolidation

2 Phase 0: Discovery & Snapshot

2.1 Cluster Topology — Verified

Node	IP	Role	OS	Resources
Hydra	192.168.1.160	Control plane, etcd, master	Ubuntu 22.04.5	20 CPU, 256 GB RAM, 21 TB RAID-10
Chimera	192.168.1.150	Worker (GPU inference)	Ubuntu 24.04.2	48 CPU, 256 GB RAM, 3× RTX 3090
Cerberus	192.168.1.233	Worker (GPU training)	Ubuntu 24.04.3	48 CPU, 64 GB RAM, 2× RTX 5090

Table 1: Verified cluster topology. Cerberus confirmed at `.233` (not `.242` as in old Ansible inventory).

RKE2 Cluster: All 3 nodes `Ready`. RKE2 v1.28.4+rke2r1. Cluster age: 16 days. Containerd 1.7.7.

2.2 Chimera Status

- CPU: AMD Ryzen Threadripper 3960X (48 cores), 251 GB RAM

- GPU: 3× NVIDIA RTX 3090 (24 GB ach) — all h althy, low utilization
- Disk: 3.5 TB Samsung NVM , 54% us d
- S rvic s: Op nW bUI (:3000), Ollama (:11434), m trics ag nt (:9100)
- Uptim : 5 w ks, 6 days
- No Dock r, no Samba — cl an RKE2 ag nt with contain rd

2.3 Cerberus Status

- CPU: AMD Ryz n Thr adripp r PRO 7965WX (48 cor s), 62 GB RAM
- GPU: 2× NVIDIA RTX 5090 (32 GB ach) — h althy, idl
- Disk: 3.6 TB MSI NVM , 6% us d
- S rvic s: m trics ag nt (:9100), SSH
- Uptim : 3 days, 19 hours
- **Kernel update pending — system restart required**
- No Dock r, no Samba — cl an RKE2 ag nt

2.4 Docker Containers on Hydra (Pre-Audit)

Container	Port(s)	Image	Status
hydra-saml-auth	host network	hydra-saml-auth	Up 3d
traefik (Docker)	8081, 8082	traefik:v3.6	Up 3d
sshpiper	2222	farmer1992/sshpiperd	Up 3d
cs-lab-backend	5001	custom build	Up 2d
cs-lab-db	3306 (int)	mariadb:10.11	Up 3d
hackathons-app	45821	hackaton-voting-app	Up 3d
java-executor-service	55392	docker-java-executor	Up 6d
traefik-n8n-traefik-1	8080 (lo)	traefik:v3.3	Up 6d
traefik-n8n-n8n-1	5678 (lo)	n8n	Up 6d
gg-git-learning-app-1	38765 (int)	gg-git-learning-app	Up 6d
n8n-user-manager (x2)	3000 (int)	n8n-user-manager	Up 6d
traefik-n8n-postgres-1	5432 (int)	postgres:16-alpine	Up 6d

Tabl 2: 13 Dock r contain rs running across 7 Compos proj cts.

2.5 Storage Architecture

- **Boot disk:** `/dev/m pper/ubuntu-vg-ubuntu-lv` — 1 TB LVM, 27% us d
- **Data array:** `/dev/md0` — 21 TB mdadm RAID-10 (6 SSDs), mount d at `/d t` , 0.3% us d
- **No ZFS pools** — `zpool st tus` r turns "no pools availabl "
- **SSD alignment verified:** Physical block siz 4096, fil syst m block siz 4096, sch dul r `mq-de dline`

2.6 RAID Details

3 Phase 1: Ser ices Disabled

3.1 MariaDB Host Service — DISABLED

```
systemctl stop m ri db && systemctl dis ble m ri db
```

MariaDB 10.6.23 was running as a syst md s rvic *and* as Dock r contain r `cs-l b-db` (MariaDB 10.11). Th Dock r contain r is th activ instanc us d by CS Lab Back nd. Th host s rvic was a duplicat .

3.2 Samba — DISABLED & MASKED

```
systemctl stop smbd nmbd && systemctl dis ble smbd nmbd && systemctl m sk smbd
nmbd
```

D fault Ubuntu Samba config with **no custom shares defined**. Only th stock `[printers]` and `[print$]` shar s xist d. N ith r Chim ra nor C rb rus hav Samba install d. No CIFS mounts anywh r in th clust r. Ports 139/445 ar now clos d.

3.3 Hydra Backend (Port 5002) — KEPT

`/srv/hydr -b ckend/ pp.js` is **not legacy**. It is th admin API that:

- Cr at s us r accounts via `/opt/hydr -scripts/cre te_user.sh`
- Qu ri s th `ServerD t b seForm` tabl in MariaDB
- R tri v s PM2 and journal logs
- Auth nticat d via tok n in `/srv/hydr -b ckend/.token`

This s rvic n ds to b k pt and v ntually migrat d to K8s.

4 Phase 2: Storage Class Cleanup

Deleted 4 orphaned ZFS storage classes:

```
kubectl delete storageclass hydra-hot hydra-warm hydra-cold hydra-
    gpu
```

Th s r f r nc d `zfs.csi.openebs.io` but no ZFS pools xist. Storag is a singl 21 TB mdadm RAID-10 SSD array.

Remaining storage classes:

Name	Provisioner	In Use
hydra-local	ranch r.io/local-path	Y s (30 stud nt PVCs)
hydra-nfs	nfs.csi.k8s.io	Y s (1 PVC)
local-path	ranch r.io/local-path	No (duplicat)

5 Phase 3: CS Lab Migration (MariaDB → SQLite)

5.1 Rationale

Th CS Lab w bsit us d MariaDB with only 4 populat d tabl s totaling ∼63 rows:

Table	Rows
Cours s	40
Cours R sourc s	18
Stud ntR sourc s	4
CompExamS ttings	1

Tabl 3: Running a full MariaDB s rv r for 63 rows is unn c ssary.

Th sch ma d fin s 16 tabl s total: Admins, Stud nt, Stud nts, AccountR qu sts, profil s, Faculty, Ev nts, Cours s, Cours R sourc s, Stud ntR sourc s, T chBlog, Stud ntHighlightBlog, Faqs, S rv rDatabas Form, SchoolCal ndar, NoSchoolDays, FacultyS m st rs, CompExamS ttings.

5.2 Migration Steps

1. Full MariaDB dump captur d: `csl b-m ri db-full-dump.sql` (5 MB)
2. Conv rting MariaDB SQL to SQLit -compatibl DDL/DML
3. R placing `m ri db` npm packag with `better-sqlite3`
4. R writing `server/src/config/db.js` as a compatibility wrapp r
5. Existing mod l fil s (`server/src/models/*.js`) r main unchang d — th wrapp r provid s th sam `pool.getConnection() / conn.query() / conn.rele se()` int rfac
6. Singl -pod K8s d ploym nt (no s parat databas contain r)

5.3 K8s Manifests Created

N w manif sts in `k8s/components/cs-l b/`:

- `deployment.y ml` — Back nd + MariaDB (b ing r factor d to singl SQLit pod)
- `service.y ml` — Clust rIP s rvic s for back nd (5001) and DB (3306)
- `secret.y ml` — Databas cr d ntials
- `pvc.y ml` — 5 Gi PVC for databas data
- `extern l-services.y ml` — Ext rnalNam s rvic s for Java x cutor, Git l arning, hydra-back nd

6 Phase 4: Traefik Consolidation

6.1 Pre-Audit State: 3 Traefik Instances

Thr s parat Tra fik instanc s w r running:

1. **K8s Traefik** (v2.11) — hostPort 80/443, L t's Encrypt ACME, CRD provid r
2. **Docker Traefik** (v3.6) — port 8082, fil provid r for stud nt rout s
3. **n8n Traefik** (v3.3) — port 8080 localhost, n8n-sp cific routing

6.2 Apache Configuration (Inactive)

Apach was **inactive/disabled** but had a 370-lin config at `/etc/ p che2/sites-en bled/hydr .newp ltz.e` containing proxy rul s for all s rvic s. This config s rv d as th historical r f r nc for what rout s n d to xist.

Routes extracted from Apache config:

- /d shbo rd, /login, /logout, / uth, /token, /check, /servers → hydra-saml-auth (:6969)
- / pi/courses, / pi/f culty, / pi/f q, ... → CS Lab Back nd (:5001)
- /students/* → Dock r Tra fik (:8082) → stud nt contain rs
- /h ck thons/ → hackathons-app (:45821)
- /j v / → java- x cutor (:55392)
- /git/ → git-l arning (:8080)
- / dmin- pi/ → hydra-back nd (:5002)
- gpt.hydr .newp ltz.edu → chim ra:3000 (Op nW bUI)
- n8n.hydr .newp ltz.edu → n8n (:5678)
- /pl cefr me/ → :6721 (NOT RUNNING)
- /studentmvp/ → :5175 (NOT RUNNING)
- /minecr ftd shbo rd/ → 192.168.1.145:3000 (stal xt rnal IP)

6.3 New K8s IngressRoutes Created

All Apach proxy rul s hav b n conv rt d to K8s Ingr ssRout CRDs:

File: ingressroute-production.y ml

- hydr -m in — All hydra-saml-auth rout s (dashboard, login, auth, s rv rs, API)
- cs-l b-website — All CS Lab API and front nd rout s (20+ path rul s)
- h ck thons — /hackathons/ path (updat d from xisting)
- j v -executor — /java/ path
- git-le rning — /git/ path
- hydr -def ult — Catch-all at priority 1 (CS Lab front nd)

File: ingressroute-subdom ins.y ml

- openwebui — gpt.hydr .newp ltz.edu → chim ra:3000
- n8n — n8n.hydr .newp ltz.edu → n8n:5678

Stale routes removed (s rvic s no long r running):

- /pl cefr me/ — port 6721 not list ning
- /studentmvp/ — port 5175 not list ning
- /minecr ftd shbo rd/ — 192.168.1.145 is not a clust r nod

7 Phase 5: Cleanup Actions

7.1 Static Content Archived & Removed

/v r/www/ (∼436 MB) archiv d to v r-www-b ckup.t r.gz th n r mov d:

- /v r/www/FLAPJS-WebApp/ — JFLAP automata simulator
- /v r/www/interview-co ch/ — Int rvi w practic app
- /v r/www/lccjs/ — LC-3 JavaScript simulator
- /v r/www/LccWebUI/ — LC-3 W b UI
- /v r/www/gpt/ — Old GPT static fil s
- /v r/www/SUNYCAT.png — 772 KB imag
- /v r/www/html/ cont nts (k pt .well-known/ for ACME)

Apach was alr ady inactiv . Non of this cont nt was b ing s rv d.

7.2 Apache Config Archived

Full Apach config archiv d to p che-full-b ckup.t r.gz. Stal fil s r mov d:

- `hydr .newp ltz.edu.conf.b k` — r mov d
- `lccjs.conf` symlink — r mov d

Main config r tain d as r f r nc in `sites- v il ble/`.

7.3 Docker Cleanup

Stal Dock r r sourc s cl an d:

- Stopp d contain rs prun d
- Dangling imag s r mov d
- Unus d n tworks prun d
- Dangling volum s id ntifi d (not r mov d — may contain stud nt data)

8 Phase 6: Backups Created

All backups stor d in `/home/infr /hydr - udit-20260204/b ckups/`:

File	Contents
`cslab-docker-compose.yml`	CS Lab Docker Compose
`hydra-saml-auth-docker-compose.yaml`	Main auth app + Docker Traefik
`sshpiper-docker-compose.yaml`	SSHPiper config
`hackathons-docker-compose.yml`	Hackathon voting app
`java-executor-docker-compose.yml`	Java code executor
`traefik-n8n-docker-compose.yaml`	n8n + Traefik + Postgres
`gg-git-learning-docker-compose.yml`	Git learning app
`apache-hydra.conf`	Apache main vhost config
`apache-lccjs.conf`	Apache lccjs vhost
`traefik-dynamic/`	All Traefik file-provider configs
`cslab.env`	CS Lab environment variables
`hydra-saml-auth.env`	Auth app environment
`hydra-backend.env`	Admin API environment
`cslab-mariadb-full-dump.sql`	Full MariaDB dump (5 MB)
`var-www-backup.tar.gz`	Archived /var/www content
`apache-full-backup.tar.gz`	Archived Apache config

Tabl 4: Compl t backup manif st.

9 Phase 7: Network & Security Findings

9.1 Externally Exposed Ports (Pre-Hardening)

Port	Service	Status	Action
22	SSH	Required	Keep
80	HTTP (Traefik)	Required	Keep
443	HTTPS (Traefik)	Required	Keep
111	rpcbind (NFS)	Exposed	Restrict to cluster
139	Samba	**Closed**	Samba disabled
445	Samba	**Closed**	Samba disabled
2049	NFS	Exposed	Restrict to cluster
2222	SSHPiper	Required	Keep
5001	CS Lab	Exposed	Move behind Traefik
6443	K8s API	Exposed	Restrict to cluster
6969	hydra-auth	Exposed	Move behind Traefik
8081	Traefik Dash	Exposed	Restrict to localhost
8082	Docker Traefik	Exposed	Consolidate to K8s
9345	RKE2 Reg	Exposed	Restrict to cluster
45821	Hackathons	Exposed	Move behind Traefik
55392	Java Executor	Exposed	Move behind Traefik

Table 5: UFW firewall not yet enabled — pending final validation.

9.2 /etc/hosts Verification

All three nodes have consistent `/etc/hosts` entries:

```
192.168.1.160 hydra
192.168.1.150 chimera
192.168.1.233 cerberus
```

10 Remaining Work

1. **CS Lab SQLite migration** — Convert db.js wrapper, import data, test, deploy as single pod
2. **Apply IngressRoutes** — Apply new K8s IngressRoutes, validate all routes work
3. **Docker Traefik removal** — Once K8s IngressRoutes handle student routing, remove Docker Traefik
4. **n8n Traefik consolidation** — Route n8n through K8s Traefik instead of its own instance
5. **UFW firewall** — Enable firewall on all 3 nodes (do last, keep SSH fallback)
6. **Cerberus reboot** — Pending kernel update requires system restart
7. **Backup automation** — Daily etcd snapshots, DB backups, config exports
8. **GPU operator fix** — Add node affinity to skip Hydra (no GPU)
9. **Metrics agents** — Deploy on Chimera and Cerberus
10. **Duplicate `local-path` storage class** — Remove the extra one