Hydra Cluster Audit & Hardening Report

10-Phase Discovery, Cleanup, Network Hardening & Validation

Infrastructure Team
SUNY New Paltz Computer Science

February 5, 2026

Contents

1 Executive Summary

This document records the comprehensive 10-phase audit, cleanup, and hardening of the 3-node Hydra RKE2 Kubernetes cluster performed on February 5, 2026. This follows up on the initial audit performed February 4, 2026.

Completed Actions:

- Full discovery snapshot of all 3 nodes (Phase 0)
- Verified `/etc/hosts` consistency across cluster (Phase 1.3)
- Pinned static IPs on Chimera and Cerberus via netplan (Phase 1.1)
- Hardened UFW firewall on all 3 nodes — removed 27017/MongoDB, 8081, Apache/CUPS from workers, restricted Flannel VXLAN to LAN (Phase 1.2)
- Verified RKE2 cluster health — all 3 nodes Ready, all GPUs visible (Phase 2)
- Audited NFS/Storage — RAID-10 healthy, CSI-NFS operational (Phase 3)
- Cleaned up orphaned Docker networks (23), dangling images, stray containers (Phase 4)
- Comprehensive Traefik routing audit with 8 findings (Phase 5)
- Verified backup automation and etcd snapshots (Phase 6)
- Docker vs K8s migration inventory completed (Phase 7)
- Deleted 5 orphaned student K8s services, stray Cerberus container (Phase 9)
- Final validation scan — all checks passing (Phase 10)

Issues Requiring Attention:

- Certbot renewal configuration is **invalid** — SSL certificates may fail to renew
- git-learning IngressRoute is **broken** — points to Docker Traefik dashboard instead of app
- `/api/events` has a priority conflict between two IngressRoutes
- Chimera has ~428GB reclaimable Docker storage (volumes + build cache)
- 14 services still running as standalone Docker containers (not in K8s)

2 Cluster Topology

Node	IP	Role	OS	Kernel	Hardware
Hydra	192.168.1.160	Control plane	Ubuntu 22.04.5	5.15.0-164	256GB RAM, 64 cores
Chimera	192.168.1.150	GPU worker	Ubuntu 24.04.2	6.8.0-63	3x RTX 3090 (72GB)
Cerberus	192.168.1.233	GPU worker	Ubuntu 24.04.3	6.14.0-37	2x RTX 5090 (64GB)

Table 1: Cluster node inventory. All running RKE2 v1.28.4+rke2r1.

Network links:

- All nodes connected via 192.168.1.0/24 LAN (gateway 192.168.1.1)
- Direct ethernet bridge between Chimera (`enp69s0`) and Cerberus (`eno1np0`) — L2 only, no IP assigned yet (reserved for RDMA/RoCE)
- Chimera and Cerberus also have WiFi connections (192.168.1.151 and 192.168.1.242 respectively)
- WireGuard VPN: Chimera `wg0` = 10.8.0.2, Cerberus `wg0` = 10.8.0.3

3 Phase 0: Discovery & Snapshot

A comprehensive audit script was deployed to all 3 nodes capturing:

- System info (hostname, kernel, uptime, memory, disk)
- Docker state (containers, images, volumes, networks)
- K8s state (nodes, pods, services, deployments, ingress routes)
- Network config (netplan, UFW, /etc/hosts, NFS exports)
- RAID status, GPU info (nvidia-smi)
- Webserver configs (Apache, Traefik)

All snapshots archived to `/tmp/hydra-audit/`, `/tmp/chimera-audit/`, and `/tmp/cerberus-audit/`.

4 Phase 1: Network Hardening

4.1 Phase 1.1: Static IP Assignment

Chimera and Cerberus were operating on DHCP-assigned IPs that happened to match their expected addresses. Both were converted to static assignments for reliability.

Node	Interface	Before	After	Method
Hydra	no8403	Static 192.168.1.160	No change	Already static
Chimera	np71s0	DHCP → 192.168.1.150	Static 192.168.1.150	netplan apply
Cerberus	no2np1	DHCP → 192.168.1.233	Static 192.168.1.233	netplan apply

Table 2: Static IP assignments. Backups created as `*.bak` files.

4.2 Phase 1.2: UFW Firewall Hardening

4.2.1 Hydra (Control Plane)

Rules removed:

- `27017/tcp` from Anywhere — MongoDB port publicly exposed (critical security risk)
- `8081/tcp` from Anywhere — unused port
- `8472/udp` from Anywhere — Flannel VXLAN replaced with LAN-only rule

Rules added:

- `8472/udp` from 192.168.1.0/24 — Flannel VXLAN (LAN only)

Preserved: SSH (22), HTTP (80), HTTPS (443), SSHPiper (2222), WireGuard (51820), K8s API (6443), etcd (2379-2380), Kubelet (10250), NFS (2049, 111), Docker bridges (6969)

4.2.2 Chimera (GPU Worker)

Rules removed:

- `Apache Full` (80,443) from Anywhere — not a webserver
- `Apache Secure` (443) from Anywhere — redundant
- `6969/tcp` from Anywhere — auth service lives on Hydra
- `7070/tcp` from Anywhere — kept specific 192.168.1.148 rule only
- `CUPS` (631) v6 — print service unnecessary on GPU worker
- `8472/udp` from Anywhere — replaced with LAN-only

Rules added:

- `8472/udp` from 192.168.1.0/24 — Flannel VXLAN (LAN only)
- `10250/tcp` from 192.168.1.0/24 — Kubelet API

Result: Z ro publicly- xpos d application ports r main (only SSH).

4.2.3 Cerberus (GPU Worker)

Rules removed:

- `8472/udp` from Anywh r — r plac d with LAN-only

Rules added:

- `8472/udp` from 192.168.1.0/24 — Flann l VXLAN (LAN only)
- `10250/tcp` from 192.168.1.0/24 — Kub l t API

C rb rus alr ady had th cl an st fir wall configuration.

4.3 Phase 1.3: /etc/hosts Consistency

All 3 nod s alr ady had consist nt `/etc/hosts` ntri s. No chang s n d d.

5 Phase 2: RKE2 Cluster Health

All checks passed:

- All 3 nod s: `Re dy` status
- GPU r sourc s visibl : 3 GPUs on Chim ra, 2 GPUs on C rb rus
- Control plan compon nts h althy (tcd, sch dul r, controll r-manag r)
- No p nding CSRs
- 75 total pods across 5 nam spac s — all Running/Compl t d

K8s nam spac s: `def ult`, `gpu-oper tor`, `hydr -students` (24 stud nt pods), `hydr -system`, `kube-system`, `loc l-p th-stor ge`.

6 Phase 3: NFS & Storage Audit

Component	**Status**
RAID-10 (md0)	H althy, 6/6 disks [UUUUUU], 21TB at /data
NFS Export	`/d t /cont iners` ! 192.168.1.0/24 (rw,sync,no_root_squash)
CSI-NFS	Running on all 3 nod s via Da monS t
Storag Class s	`hydr -nfs` (nfs.csi.k8s.io) + `hydr -loc l` (local-path)
Orphan d PVs	Non

Tabl 3: Storag subsyst m status.

Note: NFS mounts ar handl d dynamically via CSI-NFS, not via `/etc/fst b` on work rs. N ith r Chim ra nor C rb rus hav static NFS mounts.

7 Phase 4: Ser ice Cleanup

7.1 Docker Cleanup

Node	Action	Result
Hydra	Dock r n twork prun	23 orphan d n tworks r mov d
Hydra	Dock r imag prun	1 dangling imag r mov d (320MB)
Chim ra	Dock r cl anup (prior s ssion)	Imag s/volum s prun d
C rb rus	R mov stray `student-gopeen1`	Contain r r mov d

Tabl 4: Dock r cl anup actions across all nod s.

7.2 K8s Resource Cleanup

Fiv orphan d stud nt s rvic s w r id ntifi d (no matching pods): `student-currym6`, `student-degenn c1`, `student-escurr d1`, `student-perezd36`, `student-sm llg1`. Th s w r succ ssfully d l t d. 24 activ stud nt s rvic s r main with h althy pods.

8 Phase 5: Traefik Routing Audit

Th clust r us s K8s Tra fik (v2.11) as th primary r v rs proxy, xpos d via Nod Port on ports 80:30080, 443:30443, and 6969:30969. Apach is **not running** — configs xist but ar dormant.

8.1 IngressRoute Inventory

IngressRoute	Host/Path	Backend
hydra-main	hydra.n wpaltz. du (catch-all)	hydra-auth:6969
cs-lab-w bsit	/api/ pr fix	cs-lab-back nd:5001
hackathons	/hackathons/ pr fix	hackathons- xt rnal:45821
java- x cutor	/java/ pr fix	java- x cutor- xt rnal:55392
git-l arning	/git/ pr fix	git-l arning- xt rnal:8080
n8n	n8n.hydra.n wpaltz. du	n8n- xt rnal:5678
op nw bui	gpt.hydra.n wpaltz. du	op nw bui-chim ra:3000
hydra-d fault	HTTP ! HTTPS r dir ct	R dir ct sch m

Tabl 5: Ingr ssRout summary.

8.2 Critical Findings

1. git-learning route is BROKEN

Th `git-le rning-extern l` Ext rnalNam s rvic points to 192.168.1.160:8080, which is th Dock r Tra fik dashboard port, not th git-l arning app. Th actual git-l arning contain r (`gg-git-le rning- pp-1`) xpos s port 38765 with no host binding.

2. /api/events priority conflict

Both `cs-l b-website` (priority 20) and `hydr -m in` (priority 15) match `/ pi/events`. Th high r-priority cs-lab rout wins, which may not b int nd d.

3. hydra-forward-auth middleware unused

Th ForwardAuth middl war is d fin d but not attach d to any Ingr ssRout .

4. **Dead backend services:** Stud nt proxy (8082), plac fram (6721), and stud ntmvp (5175) ar r f r nc d in l gacy Apach configs but hav no list n rs.

5. **Docker Traefik overlap:** A Dock r Tra fik (v3.3) instanc runs alongsid K8s Tra fik, handling only th n8n Dock r n twork routing and its own dashboard on port 8080.

9 Phase 6: Backup Automation

Backup Type	**Schedule**	**Status**
Clust r OS (rsync to S agat)	Daily at 1:00 AM	Activ (crontab)
C rtbot r n wal	W kly (Saturday 2:45 AM)	**Invalid config!**
tcd snapshots	Ev ry 12 hours (automatic)	Working (lat st: F b 5 12:00)

Tabl 6: Backup and maint nanc automation.

Th backup script (`/usr/loc l/bin/b ckup-cluster.sh`) p rforms full rsync of all 3 nod s to `/mnt/sdh4/b ckups/`, xcluding transi nt dir ctori s (proc, sys, tmp, dock r, cach).

Certbot Issue: Th r n wal configuration at `/etc/letsencrypt/renew l/hydr .newp ltz.edu.conf` is r port d as **invalid**. SSL c rtificat s for `hydr .newp ltz.edu` and `gpt.hydr .newp ltz.edu` may fail to auto-r n w. R quir s manual inv stigation.

10 Phase 7: Docker-to-K8s Migration Assessment

14 s rvic s ar still running as standalon Dock r contain rs across th clust r:

Service	**Runtime**	**Node**	**K8s Ready?**	**Priority**
Tra fik (Dock r)	Dock r	Hydra	Duplicat	Skip
n8n + Postgr s	Dock r	Hydra	No	M dium
Hackathon Voting	Dock r	Hydra	No	Low
SSHPip r	Dock r	Hydra	No	High
Git L arning	Dock r	Hydra	No	Low
Java Ex cutor	Dock r	Hydra	No	Low
Ollama	Dock r	Chim ra	No	High
Op n W bUI	Dock r	Chim ra	No	High
Op nW bUI Middl man	Dock r	Chim ra	No	M dium
Ray H ad	Dock r	Chim ra	No	High
Ray Work r	Dock r	C rb rus	No	High

Tabl 7: Dock r contain r migration inv ntory.

Recommended migration order:

1. **Phase 1 (High):** Ray clust r (H ad + Work r) via Kub Ray op rator; Ollama + Op n W bUI
2. **Phase 2 (Medium):** SSHPip r, n8n stack (r quir s PVC for Postgr s)
3. **Phase 3 (Low):** Git L arning, Java Ex cutor, Hackathon Voting
4. **Decommission:** Dock r Tra fik (K8s Tra fik alr ady primary)

11 Phase 10: Final Validation

Check	Result	Status
K8s nod s R ady (3/3)	All R ady	PASS
All pods Running	0 pods in rror stat	PASS
GPU visibility (3+2)	5 GPUs total	PASS
Hydra ! Chim ra ping	0.257ms	PASS
Hydra ! C rb rus ping	0.601ms	PASS
Static IPs p rsist d	.150 and .233 confirm d	PASS
UFW hard n d (all nod s)	No public app ports on work rs	PASS
RAID-10 h althy	6/6 disks [UUUUUU]	PASS
tcd snapshots	Ev ry 12h, lat st today	PASS
Dock r contain rs h althy	All UP across 3 nod s	PASS
C rtbot r n wal	Config invalid	FAIL
git-l arning rout	Brok n back nd	FAIL

Tabl 8: Final validation r sults: 10 PASS, 2 FAIL.

12 Recommendations

1. **Fix Certbot:** Inv stigat and r pair `/etc/letsencrypt/renew l/hydr .newp ltz.edu.conf`. T st with `certbot renew -dry-run`.

2. **Fix git-learning route:** Eith r bind `gg-git-le rning- pp-1` to a host port and updat th Ext rnalNam s rvic , or migrat to K8s.

3. **Begin Ray/Ollama K8s migration:** Th GPU op rator and multi-nod clust r ar r ady. Kub Ray op rator would provid prop r GPU sch duling.

4. **Resolve /api/events priority conflict:** Adjust Ingr ssRout prioriti s to nsur corr ct routing.

5. **Clean Chimera Docker storage:** R claim ˜428GB of unus d Dock r volum s and build cach .

6. **Set up SSH key auth:** R plac password-bas d SSH b tw n nod s with k y-bas d auth ntication.

7. **Consider DHCP reservation on router:** As a b lt-and-susp nd rs approach alongsid static n tplan configs.

13 Appendix: UFW Final State

13.1 Hydra

```
Status: active (deny incoming, allow outgoing)
22/tcp          ALLOW IN  Anywhere
80/tcp          ALLOW IN  Anywhere
443             ALLOW IN  Anywhere
6969            ALLOW IN  172.17.0.0/16, 172.24.0.0/16
51820/udp       ALLOW IN  Anywhere
6443/tcp        ALLOW IN  192.168.1.0/24  # K8s API
9345/tcp        ALLOW IN  192.168.1.0/24  # RKE2 supervisor
```

```
10250/tcp       ALLOW IN  192.168.1.0/24  # Kubelet
2379:2380/tcp   ALLOW IN  192.168.1.0/24  # etcd
2222/tcp        ALLOW IN  Anywhere        # SSHPiper
2049/tcp        ALLOW IN  192.168.1.0/24  # NFS
111/tcp,udp     ALLOW IN  192.168.1.0/24  # portmapper
8472/udp        ALLOW IN  192.168.1.0/24  # Flannel VXLAN
```

13.2 Chimera

```
Status: active (deny incoming, allow outgoing)
22/tcp          ALLOW IN  Anywhere
7070/tcp        ALLOW IN  192.168.1.148   # OpenWebUI middleman
5201            ALLOW IN  10.10.10.0/24   # iperf
9100            ALLOW IN  192.168.1.0/24  # Metrics
4791/udp        ALLOW IN  192.168.1.0/24  # RoCEv2
Anywhere        ALLOW IN  192.168.1.0/24  # LAN (RDMA)
8472/udp        ALLOW IN  192.168.1.0/24  # Flannel VXLAN
10250/tcp       ALLOW IN  192.168.1.0/24  # Kubelet
```

13.3 Cerberus

```
Status: active (deny incoming, allow outgoing)
22/tcp          ALLOW IN  Anywhere
5201            ALLOW IN  10.10.10.0/24   # iperf
9100            ALLOW IN  192.168.1.160   # Metrics from Hydra
2376            ALLOW IN  192.168.1.160   # Docker from Hydra
4791/udp        ALLOW IN  192.168.1.0/24  # RoCEv2
Anywhere        ALLOW IN  192.168.1.0/24  # LAN (RDMA)
8472/udp        ALLOW IN  192.168.1.0/24  # Flannel VXLAN
10250/tcp       ALLOW IN  192.168.1.0/24  # Kubelet
```