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)
- Web server 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	eno8403	Static 192.168.1.160	No change	Already static
Chimera	enp71s0	DHCP → 192.168.1.150	Static 192.168.1.150	netplan apply
Cerberus	eno2np1	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 web server
- `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: Zero publicly-exposed application ports remain (only SSH).

4.2.3 Cerberus (GPU Worker)

Rules removed:
- `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

Cerberus already had the cleanest firewall configuration.

4.3 Phase 1.3: /etc/hosts Consistency

All 3 nodes already had consistent `/etc/hosts` entries. No changes needed.

5 Phase 2: RKE2 Cluster Health

All checks passed:
- All 3 nodes: `Ready` status
- GPU resources visible: 3 GPUs on Chimera, 2 GPUs on Cerberus
- Control plane components healthy (etcd, scheduler, controller-manager)
- No pending CSRs
- 75 total pods across 5 namespaces — all Running/Completed

K8s namespaces: `default`, `gpu-operator`, `hydra-students` (24 student pods), `hydra-system`, `kube-system`, `local-path-storage`.

6 Phase 3: NFS & Storage Audit

Component	Status
RAID-10 (md0)	Healthy, 6/6 disks [UUUUUU], 21TB at /data
NFS Export	`/data/containers` → 192.168.1.0/24 (rw,sync,no_root_squash)
CSI-NFS	Running on all 3 nodes via DaemonSet
StorageClasses	`hydra-nfs` (nfs.csi.k8s.io) + `hydra-local` (local-path)
Orphaned PVs	None

Table 3: Storage subsystem status.

Note: NFS mounts are handled dynamically via CSI-NFS, not via `/etc/fstab` on workers. Neither Chimera nor Cerberus have static NFS mounts.

7 Phase 4: Service Cleanup

7.1 Docker Cleanup

Node	Action	Result
Hydra	Docker network prune	23 orphaned networks removed
Hydra	Docker image prune	1 dangling image removed (320MB)
Chimera	Docker cleanup (prior session)	Images/volumes pruned
Cerberus	Remove stray `student-gopeen1`	Container removed

Table 4: Docker cleanup actions across all nodes.

7.2 K8s Resource Cleanup

Five orphaned student services were identified (no matching pods): `student-currym6`, `student-degennac1`, `student-escurrad1`, `student-perezd36`, `student-smallg1`. These were successfully deleted. 24 active student services remain with healthy pods.

8 Phase 5: Traefik Routing Audit

The cluster uses K8s Traefik (v2.11) as the primary reverse proxy, exposed via NodePort on ports 80:30080, 443:30443, and 6969:30969. Apache is **not running** — configs exist but are dormant.

8.1 IngressRoute Inventory

IngressRoute	Host/Path	Backend
hydra-main	hydra.newpaltz.edu (catch-all)	hydra-auth:6969
cs-lab-website	/api/ prefix	cs-lab-backend:5001
hackathons	/hackathons/ prefix	hackathons-external:45821
java-executor	/java/ prefix	java-executor-external:55392
git-learning	/git/ prefix	git-learning-external:8080
n8n	n8n.hydra.newpaltz.edu	n8n-external:5678
openwebui	gpt.hydra.newpaltz.edu	openwebui-chimera:3000
hydra-default	HTTP → HTTPS redirect	Redirect scheme

Table 5: IngressRoute summary.

8.2 Critical Findings

1. git-learning route is BROKEN
The `git-learning-external` ExternalName service points to 192.168.1.160:8080, which is the Docker Traefik dashboard port, not the git-learning app. The actual git-learning container (`gg-git-learning-app-1`) exposes port 38765 with no host binding.

2. /api/events priority conflict
Both `cs-lab-website` (priority 20) and `hydra-main` (priority 15) match `/api/events`. The higher-priority cs-lab route wins, which may not be intended.

3. hydra-forward-auth middleware unused
The ForwardAuth middleware is defined but not attached to any IngressRoute.

4. **Dead backend services:** Student proxy (8082), placeframe (6721), and studentmvp (5175) are referenced in legacy Apache configs but have no listeners.

5. **Docker Traefik overlap:** A Docker Traefik (v3.3) instance runs alongside K8s Traefik, handling only the n8n Docker network routing and its own dashboard on port 8080.

9 Phase 6: Backup Automation

Backup Type	Schedule	Status
Cluster OS (rsync to Seagate)	Daily at 1:00 AM	Active (crontab)
Certbot renewal	Weekly (Saturday 2:45 AM)	**Invalid config!**
etcd snapshots	Every 12 hours (automatic)	Working (latest: Feb 5 12:00)

Table 6: Backup and maintenance automation.

The backup script (`/usr/local/bin/backup-cluster.sh`) performs full rsync of all 3 nodes to `/mnt/sdh4/backups/`, excluding transient directories (proc, sys, tmp, docker, cache).

Certbot Issue: The renewal configuration at `/etc/letsencrypt/renewal/hydra.newpaltz.edu.conf` is reported as **invalid**. SSL certificates for `hydra.newpaltz.edu` and `gpt.hydra.newpaltz.edu` may fail to auto-renew. Requires manual investigation.

10 Phase 7: Docker-to-K8s Migration Assessment

14 services are still running as standalone Docker containers across the cluster:

Service	Runtime	Node	K8s Ready?	Priority
Traefik (Docker)	Docker	Hydra	Duplicate	Skip
n8n + Postgres	Docker	Hydra	No	Medium
Hackathon Voting	Docker	Hydra	No	Low
SSHPiper	Docker	Hydra	No	High
Git Learning	Docker	Hydra	No	Low
Java Executor	Docker	Hydra	No	Low
Ollama	Docker	Chimera	No	High
Open WebUI	Docker	Chimera	No	High
OpenWebUI Middleman	Docker	Chimera	No	Medium
Ray Head	Docker	Chimera	No	High
Ray Worker	Docker	Cerberus	No	High

Table 7: Docker container migration inventory.

Recommended migration order:

1. **Phase 1 (High):** Ray cluster (Head + Worker) via KubeRay operator; Ollama + Open WebUI
2. **Phase 2 (Medium):** SSHPiper, n8n stack (requires PVC for Postgres)
3. **Phase 3 (Low):** Git Learning, Java Executor, Hackathon Voting
4. **Decommission:** Docker Traefik (K8s Traefik already primary)

11 Phase 10: Final Validation

Check	Result	Status
K8s nodes Ready (3/3)	All Ready	PASS
All pods Running	0 pods in error state	PASS
GPU visibility (3+2)	5 GPUs total	PASS
Hydra → Chimera ping	0.257ms	PASS
Hydra → Cerberus ping	0.601ms	PASS
Static IPs persisted	.150 and .233 confirmed	PASS
UFW hardened (all nodes)	No public app ports on workers	PASS
RAID-10 healthy	6/6 disks [UUUUUU]	PASS
etcd snapshots	Every 12h, latest today	PASS
Docker containers healthy	All UP across 3 nodes	PASS
Certbot renewal	Config invalid	FAIL
git-learning route	Broken backend	FAIL

Table 8: Final validation results: 10 PASS, 2 FAIL.

12 Recommendations

1. **Fix Certbot:** Investigate and repair `/etc/letsencrypt/renewal/hydra.newpaltz.edu.conf`. Test with `certbot renew -dry-run`.
2. **Fix git-learning route:** Either bind `gg-git-learning-app-1` to a host port and update the ExternalName service, or migrate to K8s.
3. **Begin Ray/Ollama K8s migration:** The GPU operator and multi-node cluster are ready. KubeRay operator would provide proper GPU scheduling.
4. **Resolve /api/events priority conflict:** Adjust IngressRoute priorities to ensure correct routing.
5. **Clean Chimera Docker storage:** Reclaim ~428GB of unused Docker volumes and build cache.
6. **Set up SSH key auth:** Replace password-based SSH between nodes with key-based authentication.
7. **Consider DHCP reservation on router:** As a belt-and-suspenders approach alongside static netplan 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
```