CloudKanata
KUBERNETES, HARDENED.

CASE STUDY · NOV 2026
Adari Bain · CKA · CKS · AWS
github.com/planb438

Hardening a Kubernetes platform end to end

I took a Kubernetes cluster from a default install to a hardened, monitored, backed-up platform in 12 phases, all as code. The same playbook is what I run on client clusters: scan, fix in priority order, hand over.

The problem

A freshly installed Kubernetes cluster runs, but it is not locked down. Any pod can talk to any other pod, secrets sit in etcd unencrypted, nothing records who did what, and nobody notices a container doing something it shouldn't. Most teams only find out during an audit or an incident.

What I built

A kubeadm cluster on AWS EC2, provisioned with Terraform and run through GitOps (Argo CD, App of Apps), with security added layer by layer:

1. **Cluster setup:** Terraform IaC, kubeadm "hard way", cert-manager, NGINX ingress
2. **Data protection:** etcd encryption at rest, Sealed Secrets in Git
3. **Accountability:** API audit logging
4. **Policy:** Kyverno: safe pod settings, signed images only
5. **Supply chain:** Cosign signing, Syft SBOMs, Grype + Trivy scans
6. **Runtime detection:** Falco alerts
7. **Recovery:** Velero backups to MinIO
8. **Visibility:** Prometheus + Grafana
9. **Verification:** kube-bench (CIS) and Kubescape scans

Real workloads (WordPress, Nextcloud, invoicing) run on it today. Istio was deliberately left out to keep it simple to operate.

Before and after

Risk	Default cluster	After hardening
Secrets exposure	Unencrypted in etcd; plain in Git	Encrypted at rest; Sealed Secrets in Git
Untrusted images	Any image runs	Only signed images admitted (Cosign + Kyverno)
Known CVEs	Unknown	SBOM + Grype/Trivy scan before deploy
Risky pod settings	Allowed	Blocked by Kyverno policy
Attacks in progress	Unseen	Falco runtime alerts
"Who changed that?"	No record	API audit log
Data loss	No backups	Velero backups to MinIO
Drift	Manual changes	GitOps: Git is the source of truth

What this means for your cluster

Package	What you get	From (USD)
Kubernetes Security Check	Read-only kube-bench + Kubescape + Trivy scan, 1-page risk report, top 10 fixes	$150
Secure Supply Chain Setup	Image signing, verifyImages policy, SBOMs and a CVE gate in your CI	$250
Cluster Hardening Sprint	RBAC, Pod Security, NetworkPolicies, Falco, backups, docs + handover	$900

Start with the Security Check. Nothing changes on your cluster without your OK. Send your setup (EKS, kubeadm, k3s, MicroK8s) and what worries you most.
LinkedIn: linkedin.com/in/adaribain · Upwork: Adari B. · cloudkanata@gmail.com