DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

kube-bench Advanced Training

Run continuous CIS compliance across a fleet of clusters with governance, evidence and drift prevention.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	47 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/kubebench/kubebench-and-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the kube-bench course path, you will be able to:

1

Measure CIS compliance

Scan Kubernetes clusters with kube-bench and interpret every result against the CIS benchmark.

2

Remediate cluster findings

Fix control plane, etcd, kubelet and policy findings and prove the fixes with re-scans.

3

Govern compliance at scale

Automate scanning, reporting and exception handling across a fleet of clusters.

WHAT THE ADVANCED LEVEL ADDS

Fleet compliance, governance and hardening at scale

Hands-on: Build a multi-cluster compliance pipeline. Roll out kube-bench to three clusters with GitOps, aggregate results into one dashboard and enforce fixes with admission policies and waivers.

WHO SHOULD ATTEND

- Experienced kube-bench practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot kube-bench solutions.
- Teams making kube-bench an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Automate kube-bench in CI and on schedules, customise checks and send results to central security tools.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

kube-bench Advanced Training agenda

47 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: CIS Benchmark concepts and first scan

Included from Foundation

1. Kubernetes security posture: why configuration hardening matters and where kube-bench fits
2. CIS Kubernetes Benchmark: control plane, etcd, control plane configuration, worker node and policy sections
3. Check results: PASS, FAIL, WARN and INFO, and automated versus manual recommendations
4. kube-bench overview: Aqua Security's open-source Go tool that checks nodes against the CIS benchmark
5. Installing kube-bench: release binaries, OS packages and the aquasec/kube-bench container image
6. Running in a container: host PID namespace and read-only mounts of /etc and /var for node checks
7. Running as a Kubernetes Job: applying job.yaml and reading results with kubectl logs
8. Targets: kube-bench run --targets master,node,etcd,controlplane,policies
9. Reading the report: section summaries, failing check IDs and remediation text
10. Benchmark detection: how kube-bench maps the Kubernetes version to a CIS benchmark version
11. Lab setup: a kubeadm cluster on local VMs or a kind cluster for safe practice

DAY 2 — Essential: Remediation, output formats and managed clusters

Included from Essential

12. Control plane remediation: kube-apiserver flags such as --anonymous-auth, --audit-log-path and --authorization-mode
13. etcd remediation: client certificate authentication, peer TLS and data directory permissions
14. Worker node remediation: kubelet config file, read-only port, authorization mode and protectKernelDefaults
15. File permission checks: ownership and modes of static pod manifests, kubeconfig files and PKI files
16. Selecting checks: --check for specific IDs and --skip for documented exceptions
17. Choosing a benchmark: --benchmark and --version flags to pin a specific CIS benchmark version
18. Output formats: --json, --junit, --outputfile, --nosummary and --noremediations
19. Managed Kubernetes: job-eks.yaml, job-gke.yaml and job-aks.yaml with the EKS, GKE and AKS benchmarks
20. Distribution benchmarks: OpenShift, k3s and RKE2 configurations shipped with kube-bench
21. Policy section checks: RBAC, Pod Security Standards, network policies and secrets handling
22. Re-scanning: verifying fixes and comparing pass rates per node
23. Team workflow: recording exceptions, owners and remediation tickets

DAY 3 — Intermediate: Automation, CI and custom configuration

Included from Intermediate

24. Configuration files: cfg/config.yaml and the per-benchmark master, node, etcd, controlplane and policies files
25. Custom paths: overriding binary and configuration file locations for non-standard installations
26. Writing custom checks: audit commands, tests with flag and compare operators, and remediation text
27. Scheduled scans: running kube-bench as a CronJob on control plane and worker nodes
28. CI pipelines: scanning ephemeral clusters and failing builds on new FAIL results
29. AWS Security Hub: --asff output and the EKS integration for central findings
30. Collecting results: shipping JSON output to Elasticsearch, Loki or a SIEM

31. Comparing scanners: kube-bench vs trivy k8s with CIS compliance specs and Kubescape frameworks
32. Troubleshooting: wrong benchmark detection, missing processes, containerised control planes and permissions
33. Hardening with kubeadm: applying fixes through ClusterConfiguration and KubeletConfiguration
34. Audit logging: enabling an API server audit policy required by CIS checks
35. Secrets encryption at rest: EncryptionConfiguration with aescbc or KMS v2 providers

DAYS 4-5 **Advanced: Fleet compliance, governance and hardening at scale** **New at this level**

36. Fleet-wide scanning: deploying kube-bench Jobs to many clusters through GitOps
37. Compliance reporting: trend dashboards, pass-rate targets and evidence for auditors
38. Mapping to frameworks: CIS controls alongside NSA/CISA hardening guidance, PCI DSS and SOC 2 needs
39. Hardened node images: building CIS-aligned node images and validating them with kube-bench
40. Drift prevention: Pod Security Admission, Kyverno or OPA Gatekeeper policies
41. Exception governance: risk acceptance, time-bound waivers and approval workflow
42. Upgrades: re-validating after Kubernetes upgrades and new CIS benchmark releases
43. Mixed estates: consistent results across EKS, AKS, GKE, OpenShift and on-premises clusters
44. Defence in depth: combining kube-bench with Falco runtime detection, image scanning and penetration tests
45. Maintaining benchmarks: custom YAML for internal distributions and contributing fixes upstream
46. Security reviews: using benchmark evidence in audits and post-incident analysis
47. Capstone: build a pipeline that scans, reports, remediates and governs a multi-cluster fleet

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION **Run your first CIS scan**
Run kube-bench as a Job on the control plane and a worker node of a kubeadm cluster and list the failing checks by section.

ESSENTIAL **Remediate failing CIS checks on kubeadm**
Fix API server, etcd and kubelet findings on a kubeadm cluster, re-run kube-bench with JSON output and show the before and after pass rate.

INTERMEDIATE **Automate nightly CIS compliance reports**
Schedule kube-bench CronJobs on every node, ship JSON results to a log platform and build a report that flags new failures each night.

ADVANCED **Build a multi-cluster compliance pipeline**
Roll out kube-bench to three clusters with GitOps, aggregate results into one dashboard and enforce fixes with admission policies and waivers.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four kube-bench levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR KUBE-BENCH TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/kubebench/

ENROL OR RESERVE A SEAT
kube-bench Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com