

Kubernetes Security Checklist

15 best practices for clusters and pods, with a way to check each one. By Olivia Harper, Android Corner.
Updated October 2026.

Run this checklist as a quarterly assessment and after every cluster upgrade. Rows 1 to 13 use read-only commands. Rows 14 and 15 are tests: they prove a control works by trying to break it, so run them only in a test namespace. Replace prod and <name> with your own cluster and pod names.

#	Practice	How to check it	Done
CONTROL PLANE			
1	API server off the public internet	aws eks describe-cluster --name prod --query cluster.resourcesVpcConfig (or the AKS/GKE equivalent): public access is off or limited to listed IPs.	☐
2	Least-privilege RBAC	kubectl get clusterrolebindings -o wide grep cluster-admin lists only expected admin groups.	☐
3	Secrets encrypted at rest	aws eks describe-cluster --name prod --query cluster.encryptionConfig returns a KMS key. Self-managed clusters set --encryption-provider-config.	☐
4	Audit logging on	aws eks describe-cluster --name prod --query cluster.logging shows audit enabled, and logs reach a store outside the cluster.	☐
WORKER NODES			
5	Supported Kubernetes version	kubectl version and kubectl get nodes match a release still inside its patch window.	☐
6	Hardened nodes (CIS Benchmark)	A kube-bench job report shows no unexplained FAIL results.	☐
PODS AND WORKLOADS			
7	Pod Security Standards enforced	kubectl get ns -L pod-security.kubernetes.io/enforce shows restricted on every app namespace.	☐
8	Strict security context	kubectl get pod <name> -o yaml shows non-root, no privilege escalation, dropped capabilities and seccomp.	☐
9	User namespaces (v1.36+)	kubectl get pod <name> -o jsonpath='{.spec.hostUsers}' returns false for isolated workloads.	☐
10	No auto-mounted API tokens	kubectl get sa -A -o custom-columns=NS:.metadata.namespace,NAME:.metadata.name,AUTOMOUNT:.automountServiceAccountToken shows false where the API isn't needed.	☐
NETWORKING			
11	Default-deny network policies	kubectl get networkpolicy -A lists a default-deny policy per namespace, and your CNI enforces it.	☐
12	No Ingress NGINX	kubectl get ingressclass -o custom-columns=NAME:.metadata.name,CONTROLLER:.spec.controller shows no k8s.io/ingress-nginx controller.	☐
SOFTWARE SUPPLY CHAIN			
13	Scanned, digest-pinned images	kubectl get pods -A -o jsonpath='{..image}' shows @sha256: digests, and CI fails on fixable critical CVEs.	☐
14	Signed images only	Deploying an unsigned image to a test namespace gets rejected.	☐
RUNTIME DETECTION			
15	Runtime alerts working	A kubectl exec into a test pod triggers an alert within minutes.	☐

Full guide: each practice is explained, with examples and the 2025-2026 changes behind it, at androidcorner.com/kubernetes-security/.