Containers and Kubernetes: could one compromised pod take over the cluster?

This month, take the API server off the internet, enforce the baseline Pod Security Standard in every app namespace after a dry run and start replacing Ingress NGINX, which has had no upstream security fixes since March 2026[13]. Then judge every other setting by whether it stops one compromised pod from reaching its node, the cloud account or a more powerful service account.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for

Platform, DevOps and security teams running Kubernetes on AKS, EKS, GKE or their own servers, from one cluster to many

Latest version

sheets.einblick.dev/containers-kubernetes/

If you only do five things

1. **Take the API server off the internet.**
   EKS, AKS and GKE expose it by default[19,23,28]. Make it private or admin-only: Microsoft finds exposed APIs, default credentials and unpatched images behind most container compromises[18].
2. **Enforce Pod Security baseline in every app namespace.**
   After a dry run, set the label `enforce` to `baseline` to block privileged containers, hostPath and host namespaces[4], and `warn` and `audit` to `restricted`[6]. North Korea-linked UNC4899 broke out through a privileged infrastructure pod[17].
3. **Treat pod creation as a privileged right.**
   Anyone who can create pods in a namespace can mount its Secrets and run as any of its service accounts[3]. Each quarter, list who holds that right, `cluster-admin` or the rights below, and cut the list.
4. **Keep workload credentials short-lived.**
   Set `automountServiceAccountToken: false` unless a pod calls the API[2], avoid non-expiring token Secrets[1] and block pods from the node's cloud role[21]. UNC4899 stole database credentials from a pod's environment variables[17].
5. **Stay on a supported version, add-ons included.**
   Kubernetes patches only its three newest minor versions, for about a year each[10]. Ingress NGINX, in about half of cloud native environments, can read every Secret by default and was retired in March 2026[12,11,13].

Harden a running cluster in this order

1. **Who can reach and administer it?**
   List each cluster's endpoint, version, add-ons and `cluster-admin` bindings. Find Ingress NGINX with `kubectl get pods -A -l app.kubernetes.io/name=ingress-nginx`[12].
2. **Which pods would Pod Security reject?**
   Label namespaces with `--dry-run=server` to list pods that would fail[6], and set the `warn` and `audit` labels first. They also check Deployments, while `enforce` checks only pods, so a noncompliant Deployment is accepted but its pods are rejected[5].
3. **Does your network plugin enforce NetworkPolicy?**
   If not, a NetworkPolicy has no effect. Namespace by namespace, allow the traffic you need, DNS included, then add default-deny ingress and egress policies[8].
4. **What does Pod Security miss?**
   Add admission rules for image sources and digests[1]; signing is in the supply-chain sheet. ValidatingAdmissionPolicy is built in and can `Warn` and `Audit` before it denies[7]; Kyverno and OPA Gatekeeper are add-ons[4].
5. **Would you see a takeover?**
   Turn on audit logs: they are off by default on EKS[20] and need a diagnostic setting with `kube-audit` on AKS[25]. Alert on `exec` into pods, new cluster role bindings and Secrets listed by people. Retention is in the logging sheet.

Defaults to change on EKS, AKS and GKE

Amazon EKS

- **Public endpoint.** Enable private access, then limit or disable public access[19].
- **aws-auth.** Deprecated: move to access entries and remove the creator's `cluster-admin`[21].
- **Support.** 14 months, then 12 of paid extended support, on by default. Extended support for 1.31 ends on 26 November 2026[22].

Azure AKS

- **Public API server.** Use a private cluster or at least authorized IP ranges[23].
- **Local accounts.** On by default and unaudited. Move tools off `--admin`, set `--disable-local-accounts` and rotate certificates off-hours[24].
- **Support.** 12 months per version; 1.34 reaches end of life in November 2026[26].

Google GKE

- **Reachable control plane.** Use only the DNS-based endpoint, or authorized networks[28].
- **Anonymous access.** Set `--anonymous-authentication-config=LIMITED` on clusters created before 1.35.0-gke.1171000[28].
- **Upgrades.** Use a release channel with accelerated patch auto-upgrades[28].

What changed in 2026

- **Ingress NGINX is retired.** Upstream has had no fixes since 24 March 2026[13]; AKS patches its managed NGINX add-on only through November 2026[27]. Move to Gateway API or another controller[12].
- **Kubernetes 1.36 closed old gaps.** It disabled `gitRepo` volumes for good and deprecated Service `externalIPs`[13].
- **AKS will upgrade unsupported clusters itself.** From 1 June 2027, then 60 days after each version's end of life, ignoring maintenance windows[26].
- **Linux root exploits came with public code.** Three flaws disclosed from 29 April to 13 May 2026 gave local users root on major distributions[18]. Patch node images within the patching sheet's deadlines.

RBAC rights that allow escalation

- **`get`, `list` or `watch` on Secrets.** List and watch return the contents too[3].
- **`escalate`, `bind` and `impersonate`.** They bypass RBAC's escalation checks or borrow another user's rights[3].
- **Any right on `nodes/proxy`.** Even `get` runs commands in every pod on the node, unaudited and past admission control[3].
- **Webhook, token and volume rights.** Control of webhook configurations, or `create` on `serviceaccounts/token` or PersistentVolumes, exposes admitted objects, mints tokens or mounts the node's disk[3].
- **`patch` on namespaces.** It lets a user relabel a namespace to a looser Pod Security level[3].

Pod and node settings that stop an escape

- **Non-root, read-only, no escalation.** Restricted requires `runAsNonRoot`, no privilege escalation, seccomp and dropping ALL capabilities[4]. Add `readOnlyRootFilesystem`[2].
- **User namespaces.** Set `hostUsers: false`, GA on Linux since 1.36, to map container root to an unprivileged host user[14].
- **Minimal images by digest.** Ship no shells or debug tools, pin sha256 digests instead of tags and scan at build and deploy[1].
- **Secrets as files.** Environment variables may leak more easily; mount secrets from an external store with the Secrets Store CSI Driver[1].
- **Kubelet API.** On your own nodes, turn off `--anonymous-auth` and set `--authorization-mode=Webhook`: the defaults allow anonymous access[9].

What you can skip

- **A service mesh just for encryption.** The checklist suggests one only if your network plugin can't encrypt traffic[1].
- **Waiting for fixes to old CVEs.** Scanners can flag CVE-2020-8561, CVE-2020-8562 and CVE-2021-25740 on every version since June 2026; they won't be fixed[15]. Mitigate once and accept them.
- **CPU limits on every pod.** They throttle work and can upset autoscaling; the checklist suggests them only for sensitive workloads[1].

Mistakes that cost the most

- **Exempting a controller from Pod Security.** Exempting the ReplicaSet controller exempts everyone who can create a Deployment[5].
- **Giving CI cluster-wide rights.** UNC4899 made CI jobs print service account tokens to logs, then used a highly privileged one to escalate[17].
- **Binding roles to built-in groups.** `system:unauthenticated` is anyone who can reach the API server[3]; on GKE, `system:authenticated` includes any Google account[28].

What this looks like at your size

Small team, no security staff

- Prefer a managed mode with secure defaults: GKE Autopilot blocks privileged pods by default[29].
- Limit the API server to your VPN or office addresses, and turn on audit logs.
- Enforce baseline in every app namespace and turn on automatic patch upgrades.

Growing, with IT or security staff

- Reach a private API server through a VPN or bastion, with SSO groups mapped to RBAC roles.
- Keep admission and network policies in Git, and move each rule from warn to deny.
- Upgrade one minor version every four months, as they ship[26], staging cluster first.

Enterprise or regulated

- Give each trust level its own namespace[3] and untrusted tenants their own cluster.
- On self-managed clusters, load must-have admission policies from disk, beta in 1.37[16].
- Send audit logs and GuardDuty, Defender for Containers or Falco alerts to the SIEM.

Version history

5 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which removed four outage risks from the advice and narrowed 12 statements to what the sources say.

Sources

1. Security Checklist. Kubernetes, 28 Feb 2025. kubernetes.io
2. Application Security Checklist. Kubernetes, 6 Nov 2024. kubernetes.io
3. RBAC Good Practices. Kubernetes, 18 Aug 2026. kubernetes.io
4. Pod Security Standards. Kubernetes, 16 Oct 2026. kubernetes.io
5. Pod Security Admission. Kubernetes, 7 Mar 2024. kubernetes.io
6. Enforce Pod Security Standards with Namespace Labels. Kubernetes, 5 Nov 2022. kubernetes.io
7. Validating Admission Policy. Kubernetes, 28 Sep 2026. kubernetes.io
8. Network Policies. Kubernetes, 14 Apr 2026. kubernetes.io
9. Kubelet authentication/authorization. Kubernetes, 19 Feb 2026. kubernetes.io
10. Releases. Kubernetes, checked 5 Nov 2026. kubernetes.io
11. Ingress-nginx CVE-2025-1974: What You Need to Know. Kubernetes Blog, 24 Mar 2025. kubernetes.io
12. Ingress NGINX: Statement from the Kubernetes Steering and Security Response Committees. Kubernetes Blog, 29 Jan 2026. kubernetes.io
13. Kubernetes v1.36: Haru. Kubernetes Blog, 22 Apr 2026. kubernetes.io
14. Kubernetes v1.36: User Namespaces in Kubernetes are finally GA. Kubernetes Blog, 23 Apr 2026. kubernetes.io
15. Reconciling the Past: Correcting Records for Unfixed Kubernetes CVEs. Kubernetes Blog, 26 May 2026. kubernetes.io
16. Kubernetes v1.37: Garhwal. Kubernetes Blog, 26 Aug 2026. kubernetes.io
17. Cloud Threat Horizons Report H1 2026. Google Cloud, Mar 2026. services.google.com
18. Microsoft Digital Defense Report 2026. Microsoft, Oct 2026. cdn-dynmedia-1.microsoft.com
19. Cluster API server endpoint. AWS, checked 5 Nov 2026. docs.aws.amazon.com
20. Send control plane logs to CloudWatch Logs. AWS, checked 5 Nov 2026. docs.aws.amazon.com
21. EKS Best Practices: Identity and Access Management. AWS, checked 5 Nov 2026. docs.aws.amazon.com
22. Kubernetes version lifecycle on EKS. AWS, checked 5 Nov 2026. docs.aws.amazon.com
23. API server authorized IP ranges in AKS. Microsoft Learn, 3 Aug 2026. learn.microsoft.com
24. Manage local accounts with Microsoft Entra integration. Microsoft Learn, 20 Apr 2023. learn.microsoft.com
25. Monitor Azure Kubernetes Service (AKS). Microsoft Learn, 18 Aug 2026. learn.microsoft.com
26. Supported Kubernetes versions in AKS. Microsoft Learn, 15 Sep 2026. learn.microsoft.com
27. AKS managed NGINX ingress with the application routing add-on. Microsoft Learn, 26 Oct 2026. learn.microsoft.com
28. Best practices for hardening your cluster's security. Google Cloud, 30 Oct 2026. docs.cloud.google.com
29. GKE Autopilot security measures. Google Cloud, 30 Oct 2026. docs.cloud.google.com