What is Kubernetes RBAC?

Kubernetes RBAC (Role-Based Access Control) is the system that decides what actions each user, group, and service account may perform on the cluster's API. It binds roles (sets of permissions) to subjects through role bindings. Misconfigured RBAC, wildcard permissions, cluster-admin granted to workloads, or rights like creating pods, reading secrets, or impersonating, lets an attacker who compromises one identity escalate to full cluster control. Least-privilege RBAC is the core Kubernetes defense.

HOW IT WORKS

01 How weak RBAC is abused

When a pod or user is compromised, the attacker inherits its RBAC rights and hunts for ways to escalate:

- Wildcards (`verbs: ["*"]`, `resources: ["*"]`) or cluster-admin bound to a workload, instant full control.
- `secrets` read access, dump every secret in a namespace or cluster.
- `create pods`, schedule a privileged pod or one that mounts the node, then escape.
- `impersonate`, `escalate`, or `bind`, grant themselves more rights.
- Token creation for other service accounts.

Documented techniques shown for defenders.

> PERMISSIONS ARE THE EXPLOIT
>
> *In Kubernetes the attack is often just using the permissions you were given. Rights like* `create pods`*-*, `read secrets`*, or* `impersonate` *quietly add up to cluster takeover, so least privilege is everything.*

HOW TO DEFEND

- Apply least privilege: no wildcard verbs/resources, no cluster-admin for workloads.
- Audit dangerous rights: pod creation, secret read, impersonate, escalate, bind, and token creation.
- Use namespaced Roles over ClusterRoles wherever possible.
- Review RBAC regularly and use tooling to surface escalation paths.
- Disable unused service-account token automount so a compromised pod has no key.
- Test the cluster for RBAC escalation paths.

SOURCES

[1] Kubernetes docs: RBAC authorization

[2] MITRE ATT&CK: Containers Matrix

[3] NIST SP 800-190 Application Container Security Guide

Find the container escape paths before an attacker does.

securelayer7.net/learn/containers/what-is-kubernetes-rbac

Open online