Do’s and Don’ts of Kubernetes Security

August 2021
Andy got his start in tech doing IT work while waiting tables in college. Later he took his first SRE role at ReadyTalk back before the video conferencing revolution gave us Zoom and other contenders.

Today Andy leads Research and Development at Fairwinds exploring new nooks and crannies of the Kubernetes ecosystem and pressing the limits of what’s possible with automation in a fast-moving technology like Kubernetes.
Kubernetes
Done Right

Fairwinds provides software and services to help companies ship cloud native applications faster, more cost effectively and with less risk.

- **Software** - policy-driven configuration validation of containers and Kubernetes from CI/CD through production.
- **Open source** - open source projects to address problems that exist with Kubernetes.
- **Services** - expertly managed cloud-native infrastructure leveraging containers and Kubernetes.
Don’t: Expect security by default using native controls
Do: Use Pod Security Context Options
spec:
  securityContext:
    runAsUser: 1000
collectors:
  - name: sec-ctx-demo-2
    image: gcr.io/google-samples/node-hello:1.0
    securityContext:
      runAsUser: 2000
      allowPrivilegeEscalation: false
      readOnlyRootFilesystem: false
      capabilities:
        drop: ["all"]
        add: ["NET_BIND_SERVICE"]
Don’t: Grant access to the host node
Do: Set up Network Policy
Don’t: Run containers with known vulnerabilities
Do: Separate **Node** vs. **Pod** Cloud Access
Do: Create a strategy for role based access control (RBAC)
Do: Use an admission controller to enforce security policies
Security is Now Everyone's Job
69% Reported a Kubernetes misconfiguration incident

Roughly 7 out of 10 companies reported a misconfiguration incident in their Kubernetes environment over the last 12 months -- making it the top Kubernetes security issue.

“Kubernetes by the numbers: 12 stats to see”, July 2020, EnterprisersProject.com
Kubernetes security, policy and governance software, from CI/CD through production

- Shift left security
- Automate Kube and container security
- Enforce policy
- Govern compliance
- Optimize compute resources
Get started on improving your Kubernetes security.

Here are a few of the common mistakes:

- Granting access to the host node
- Assuming operations is aligned with security
- Running containers with known vulnerabilities