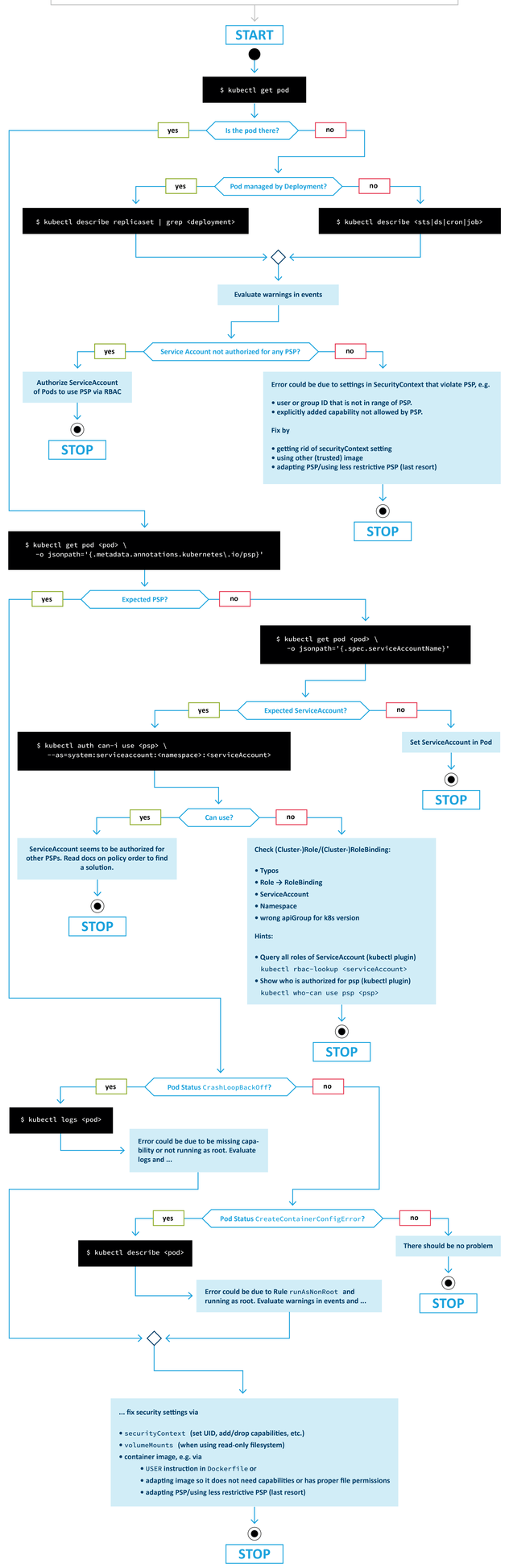
cloudogu

Troubleshooting – Kubernetes PodSecurityPolicies

Before starting – Check if common pitfalls are avoided:

- admission controller active
- PSP, (Cluster-)Role and (Cluster-)RoleBinding applied
- Pods started *after* enabling admission controller, applying PSP, (Cluster-)Role and (Cluster-)RoleBinding
- correct apiGroup for (Cluster-)Role, depending on k8s version
  - < 1.16: `apiGroups: [extensions]`
  - >= 1.16: `apiGroups: [policy]`



Hints for testing if settings are effective:

- Query capabilities of container:
  `capsh --decode="$(kubectl exec <pod> cat /proc/1/status | grep CapBnd| cut -d':' -f2)"`
- Check if seccomp active ("2" means active)
  `kubectl exec <pod> cat /proc/1/status | grep Seccomp`
- Check if privilege escalation is possible:
  `kubectl exec <pod> cat /proc/1/status | grep NoNewPrivs`
- Simple test for read-only filesystem (expected result `touch: cannot touch 'a': Read-only file system`)
  `kubectl exec <pod> touch a`
- Query user and group of container:
  `kubectl exec <pod> id`

cloudogu.com