
KubeCon
CloudNativeCon
North America 2024

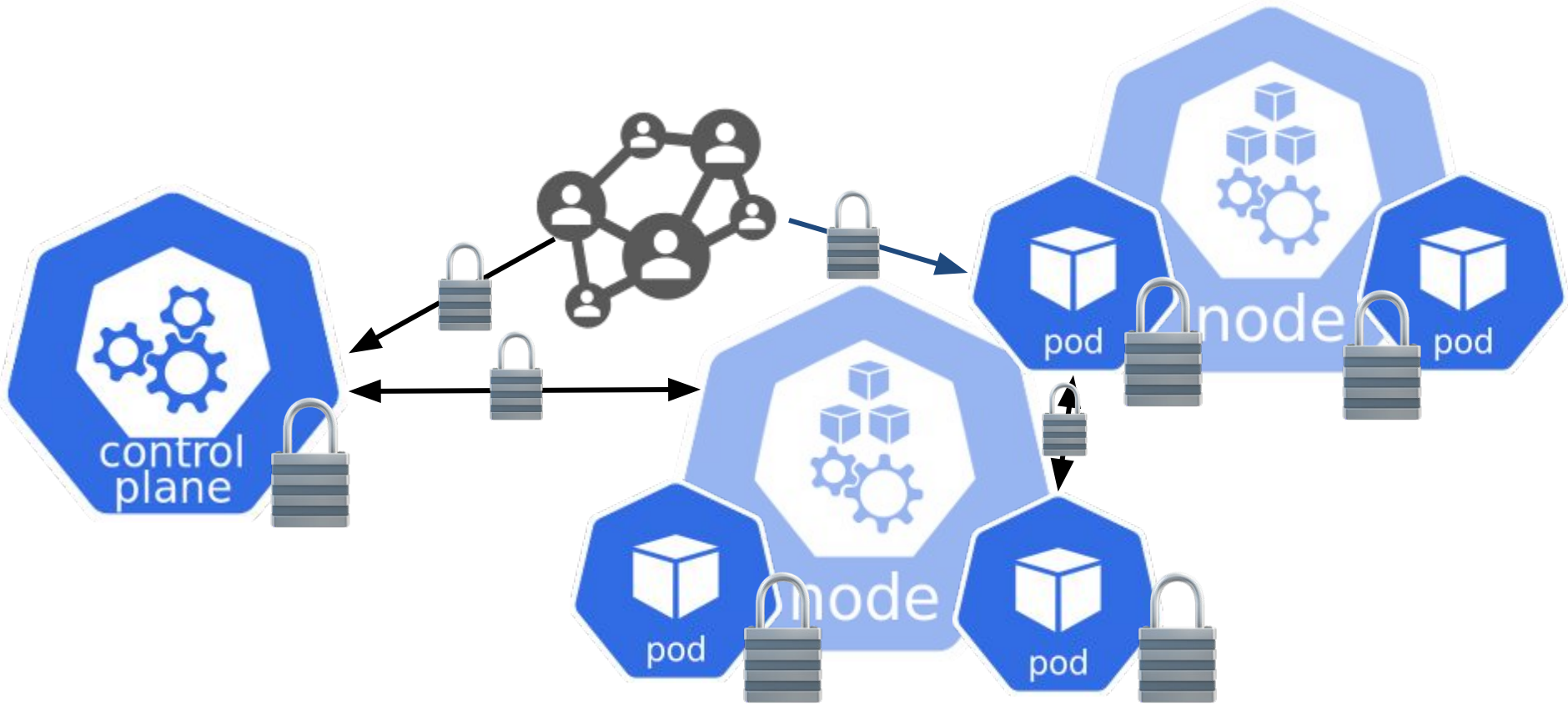
KubeCon | CloudNativeCon

North America 2024

Stop Kubernetes' Revolving Door: A Hands-On Tutorial to Secure a Kubernetes Cluster

Savitha Raghunathan, Red Hat
Mahé Tardy, Isovalent at Cisco
Rey Lejano, Red Hat

Securing Kubernetes



Kubernetes Security Checklist

https://kubernetes.io/docs/concepts/security/security-checklist/

Add a security checklist for clusters #33992

Edit | Code

Merged | k8s-ci-robot merged 16 commits into `kubernetes:main` from `mtardy:security-checklist` on Sep 1, 2022

Conversat 269 | Commits 16 | Checks 0 | Files changed 1 | +408 −0

mtardy ommented on May 27, 2022 • edited | Member

Draft for th @p4ck3t0.

-security repos savitharaghunat Skybound1

issue Create a security checklist for deploying a cluster #28 in

curity checklist guide from the collaborative document w nd

ny people participated in this list via this PR, thanks every !

ument in the form of a checklist with paragraphs that further de ne goal is to centralize many security concerns and form a central place to redirect to other documenta

This checklist is meant to evolve in the future, as the participation on the PR proved, people provided really diverse ideas and this is essential to try to cover as much as possible.

k8s-ci-robot added do-not-merge/work-in-progress cncf-cla: yes size/L labels on May 27, 2022

k8s-ci-robot requested review from bradtopol and jimangel 2 years ago

Reviewers

- rschosser
- sftim
- divya-mohan0209
- NissesSenap
- raesene
- cailyn-codes
- pjbgf
- tengqm
- PushkarJ
- liggitt
- reylejano
- Skybound1
- p4ck3t0

Kubernetes Security Checklist

https://kubernetes.io/docs/concepts/security/security-checklist/

Security Checklist

Baseline checklist for ensuring security in Kubernetes clusters.

This checklist aims at providing a basic list of guidance with links to more comprehensive documentation on each topic. It does not claim to be exhaustive and is meant to evolve.

On how to read and use this document:

- The order of topics does not reflect an order of priority.
- Some checklist items are detailed in the paragraph below the list of each section.

Caution:
Checklists are **not** sufficient for attaining a good security posture on their own. A good security posture requires constant attention and improvement, but a checklist can be the first step on the never-ending journey towards security preparedness. Some of the recommendations in this checklist may be too restrictive or too lax for your specific security needs. Since Kubernetes security is not "one size fits all", each category of checklist items should be evaluated on its merits.

Edit this page
Create child page
Create documentation issue
Print entire section
Authentication & Authorization
Network security
Pod security
Enabling Seccomp
Enabling AppArmor or SELinux
Logs and auditing
Pod placement
Secrets
Images
Admission controllers
What's next

Kubernetes Security Checklist

https://kubernetes.io/docs/concepts/security/security-checklist/

Basic security guidance to improve the security posture of Kubernetes but **is not sufficient**

Security Checklist Topics:

Authentication & Authorization

Network Security

Pod Security

Admission Controllers

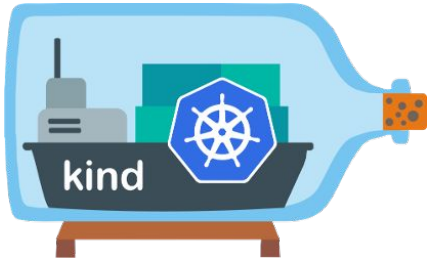
Logs and Auditing

Pod Placement

Secrets

Images

Tutorial Environment



Kubernetes in Docker

- Run local Kubernetes clusters using Docker container “nodes” on MacOS, Windows, or Linux.
- Used by the Kubernetes project to test and run integration tests.
- Pre-reqs:
  - Docker
  - kubectl

Tutorial Environment

instruqt

Browser-based platform for labs with copy or click-to-run functionality

instruqt Stop Kubernetes' Revolving Door

Overview | Invite details | Progress | Hide Instructions

>_ Terminal

```
root@server:~#
```

Instructions | View notes

Introduction

Authentication and Authorization: System Masters Group

This step covers two Kubernetes security checklist items under Authentication & Authorization:

- Check `system:masters` group is not used for user or authentication after bootstrapping
- The Role Based Access Control Good Practices are followed for guidance related to authentication and authorization.

Access the Tutorial on Instruqt

https://cloud-native.us/secure-k8s

Stop Kubernetes' Revolving Door

A Hands-on Tutorial to Secure a Kubernetes Cluster

View details Start

Tutorial - Authentication & Authorization

Authentication & Authorization:

- system:masters group is not used for user or component authentication after bootstrapping
- the Role Based Access Control Good Practices are followed for guidance related to authentication and authorization.

Tutorial - Network Security

Network Security:

- CNI plugins in-use supports network policies.
- Ingress and egress network policies are applied to all workloads in the cluster.
- Default network policies within each namespace, selecting all pods, denying everything, are in place.

Tutorial - Pod Security

Pod Security:

- RBAC rights to create, update, patch, delete workloads is only granted if necessary.
- Appropriate Pod Security Standards policy is applied for all namespaces and enforced.
- For nodes that support it, Seccomp is enabled with appropriate syscalls profile for programs.

Tutorial - Admission Controllers

Admission Controllers:

- A pod security standard policy is enforced by the Pod Security Admission or/and a webhook admission controller.

Tutorial - Authentication & Authorization

Authentication & Authorization:

- Intermediate and leaf certificates have an expiry date no more than 3 years in the future.

Tutorial - Pod Placement

Pod Placement:

- Pod placement is done in accordance with the tiers of sensitivity of the application.
- Sensitive applications are running isolated on nodes or with specific sandboxed runtimes.

Helpful Links

Kubernetes Security Checklist:
https://kubernetes.io/docs/concepts/security/security-checklist/

Application Security Checklist:
https://kubernetes.io/docs/concepts/security/application-security-checklist/

Hardening Guide on Authentication Mechanisms:
https://kubernetes.io/docs/concepts/security/hardening-guide/authentication-mechanisms/

Tutorial Repository:
https://github.com/cloudnativeessentials/kubecon-na-2024-stop-k8s-revolving-door

More tutorials:
https://medium.com/@LachlanEvenson/hands-on-with-kubernetes-pod-security-admission-b6cac495cd11
https://medium.com/@LachlanEvenson/managing-kubernetes-seccomp-profiles-with-security-profiles-operator-c768cff58b0

KubeCon | CloudNativeCon

North America 2024