
KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

Empowerment Through Autonomy

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2021

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Ala Dewberry
Senior Product Manager
VMware

Savitha Raghunathan
Senior Software Engineer
Red Hat

Tabitha Sable
Staff Engineer
Datadog

Agenda

- SIG Security Overview
- Sub-projects + Updates
- Introducing - Self-Assessments!
  - Self-Assessments History
  - Current Day & How It Works
  - Future Directions
- Wrap Up

SIG Security

- What is SIG Security?
  - Horizontal SIG covering security initiatives for the entire Kubernetes project
- What do we do?
  - Feature, process, and documentation improvements
  - Security-related services within Kubernetes
  - Public forum for Security Response Committee
- How do we do it?
  - Community!
  - Collaboration with sibling SIGs

To The Subprojects!

Docs

- Sub Project Goals:

  - Collaborate and create/improve existing security content for Kubernetes documentation.
  - Keep the documentation and security examples up to date.
  - Create security awareness through documentation.

- Highlights:
  - Kubernetes Security Checklist
  - API Server bypass risks
  - Historical context on PSP

Docs

- Upcoming Projects:

  - Hardening guide
  - Confidential Kubernetes blog
  - Add more tutorials & examples

- sig-security-docs project is looking for volunteers!

- If you are interested in improving the security content, please feel free to reach out to us in the sig-security-docs slack channel

Audit

Subproject Goals:

- Coordinate regular, comprehensive, third-party security audits

Audit Goals:

- Identify vulnerabilities or weaknesses in Kubernetes
- Make Kubernetes more secure

Blog on the current state from the 2019 audit published:

- https://kubernetes.io/blog/2022/10/05/current-state-2019-third-party-audit/
- Reviews the status of the 37 issues filed from the 2019 audit
- Thank you to Cailyn Edwards, Pushkar Joglekar, Rory McCune and Rey Lejano

2021/2022 Audit:

- Report to be published soon
- Learnings shared with the security self-assessment subproject

Tooling

- Every other week: Working OR Learning sessions
- Continue with KEP-3203: Official K8s CVE Feed
- Vulnerability Scanning: Images, Build time Dependencies
- Help other sub-projects and SIGs

And Now for Something Completely Different

Self Assessments!

- Brief History - CAPI
- What is the goal?
- How do you do a Self Assessment?
- How does it Empower through Autonomy?
- Future Directions

Brief History

- Foundation is Learning & Consent
- CAPI asked for help
- Pushkar had experience from CNCF TAG Security Self Assessments
- Pushkar rallied the troops and we tried it!
- Positive experience - let’s make it a process

What is the goal?

For a Single Self Assessment:

To answer two questions -

- What is the security posture of the workflow modelled?
- How can we improve it?

…And capture actions to take to improve the security posture

For the Project:

- Self Assessments for all Projects and Subprojects

How do you do a Self Assessment? Pt 1

The process of:

- Mapping out a targeted workflow in use by the community
- Building a threat model for the workflow
- Evaluating the security posture of the workflow on the threat model

How do you do a Self Assessment? Pt 2

- Receive Request!
- Find your people
- Map out Architecture
- Prioritize what you want to model
- Map out the workflow
- Build your threat model
- Evaluate weaknesses
- Capture + Prioritize Action items

How does it Empower through Autonomy?

Making Security Accessible & Repeatable

Federating Security Knowledge

Future Directions or…Roadmap!

How will we keep Empowering through Autonomy?

- Socialize this tool - who needs one?
- Refine with feedback and usage
- Get rolling on vSphere CSI Driver - come join us!
- Complete retro for CAPI Self Assessment
- Trade learnings with CNCF

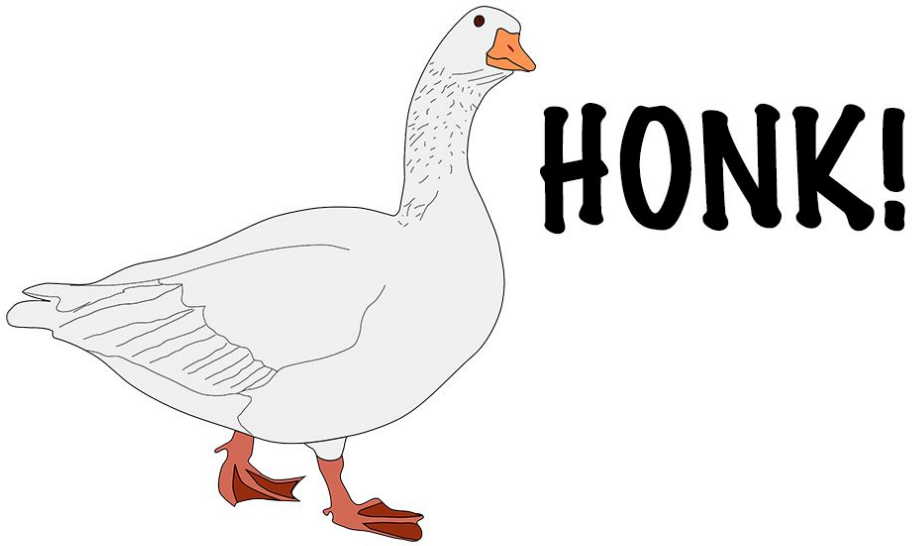
Wrap Up

Come Join the Fun!

Slack

Meetings

Thank you!



KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Please scan the QR Code above to leave feedback on this session