



KubeCon



CloudNativeCon

North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2022



Pushkar Joglekar

Tech Lead
CNCF TAG Security

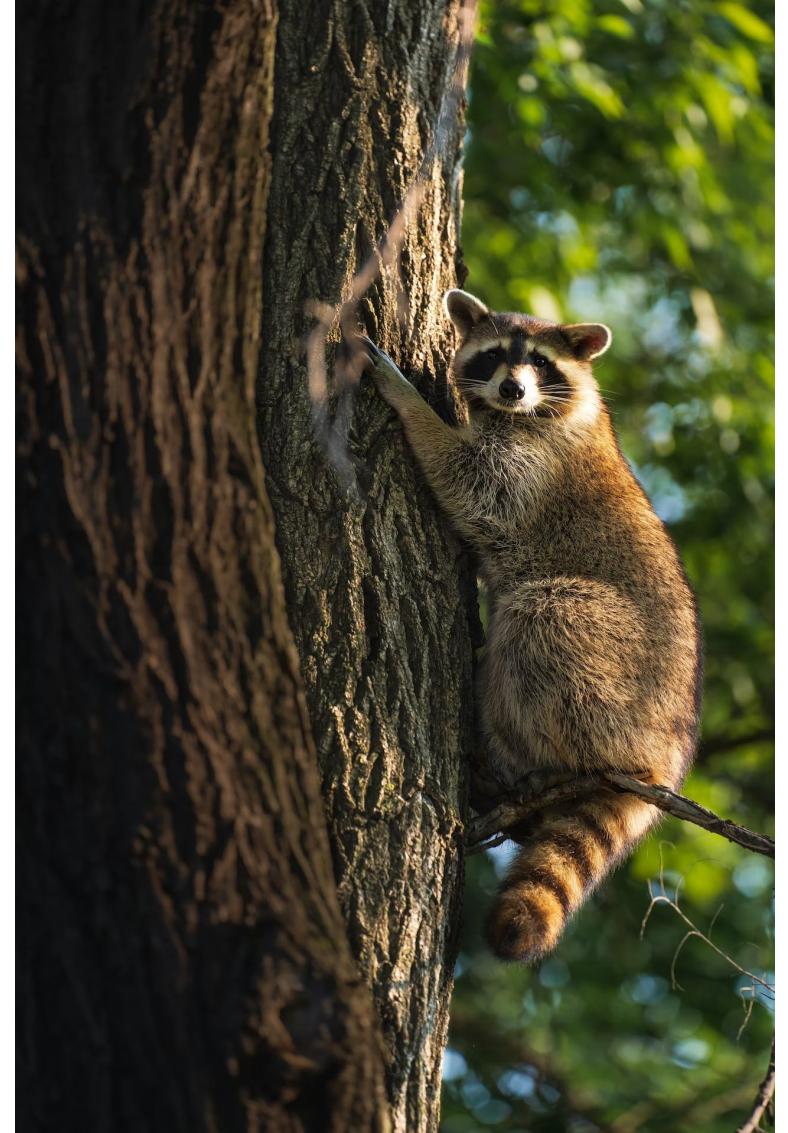


Naadir Jeewa

Staff Engineer for Tanzu Kubernetes
Grid
VMware

What's with the animals?

Raccoon
=
CNCF TAG
Security



What's with the animals?

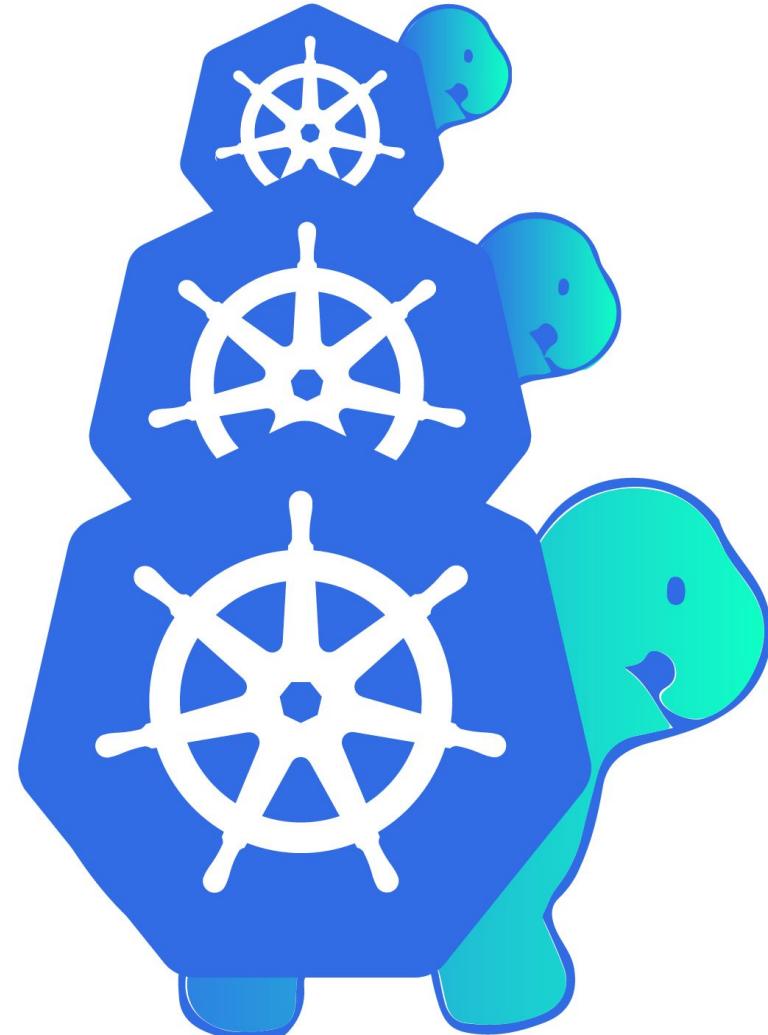
Geese
=

Kubernetes
SIG Security



What's with the animals?

Turtles
=
Kubernetes
Cluster API



How it started?

first 5 security assessments (before process review/improvement) #167

Closed 5 of 10 tasks ultrasaurus opened this issue on 20 May 2019 · 38 comments



ultrasaurus commented on 20 May 2019 · edited

Member ...

We have a target of 5 security assessments, before doing a retrospective on process and addressing (most of) [open issues/questions](#)

This was the initial set of security-related projects, initially [identified by TOC for our SIG](#): SPIFFE, SPIRE, Open Policy Agent, Notary, TUF, Falco. We omitted those that had already had a formal audit or TOC contributor assessment.

Done:

- Harbor
- in-toto
- OPA
- SPIFFE / SPIRE - [\[Assessment\] SPIFFE/SPIRE #308](#)



randomvariable commented on 3 Jul 2019

...
...

Hi, is this the right place to say we would like and are ready for a security audit for [kubeadm](#)? kubeadm is the recommended bootstrapper for Kubernetes and is consumed by a lot of other Kubernetes infrastructure bootstrappers such as Kubespray and Kubernetes Cluster API. cc @timothysc

2

The heady days of 2019...

How it started?

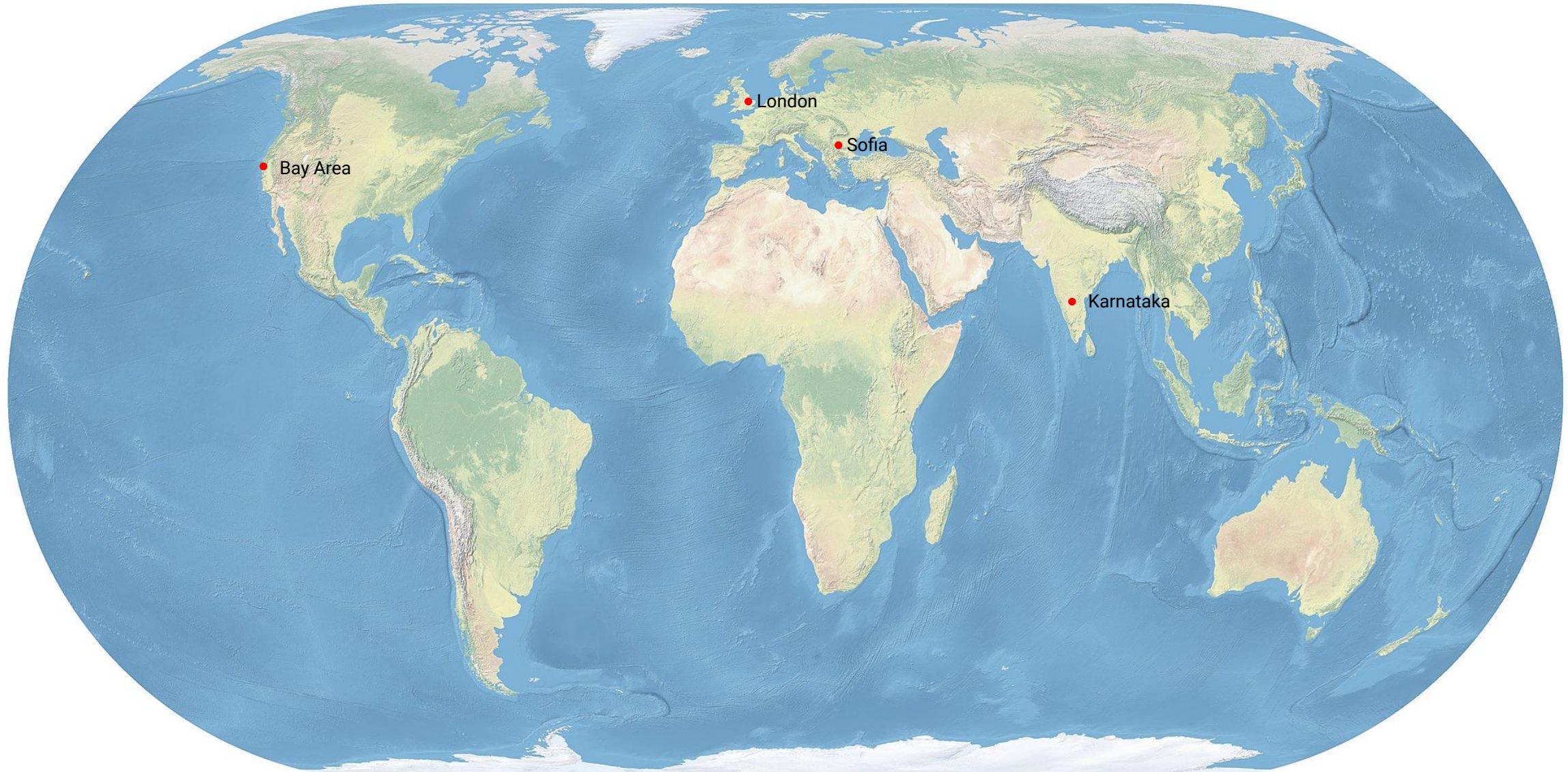
 [kubernetes-sigs / cluster-api](#) Public  Watch 96 ▾ 

 Code  Issues 245  Pull requests 56  Discussions  Actions  Projects  Security  Insights

Complete Cluster API external security audit #4446

 Closed neolit123 opened this issue on Apr 7, 2021 · 23 comments

Time zones



How it started?

The screenshot shows a GitHub repository page for 'cncf/tag-security'. The repository is public, as indicated by the 'Public' badge. The top navigation bar includes options for 'Edit Pins', 'Unwatch' (160), 'Fork' (368), and a dropdown menu. Below the navigation, there are links for 'Code', 'Issues' (132, highlighted in red), 'Pull requests' (13), 'Actions', 'Projects' (8), 'Security', and 'Insights'. The main content area displays an issue titled '[Pilot] Security Self-Assessment of a sub-project of a graduated CNCF project #603'. The issue is labeled 'Open' and shows '7 of 9 tasks'. It was opened by 'PushkarJ' on April 27, 2021, with 19 comments.

How it started?

A screenshot of a GitHub repository page for `kubernetes / sig-security`. The repository is public and was generated from `kubernetes/kubernetes-template-project`. The page includes standard GitHub navigation links: Code, Issues (13), Pull requests (4), Actions, Projects, Security, and Insights. The Issues tab is currently selected.

[Umbrella] Security Assessment Process for Kubernetes sub-projects #2

Open 5 of 7 tasks PushkarJ opened this issue on Jul 29, 2021 · 7 comments

To Sync or Async?

May 22nd, 2021 ▾

Slack channel created



August 26th, 2021 ▾

First Meeting Planned

Async First

New channel for security assessment of cluster api #5792

Merged

k8s-ci-robot merged 2 commits into `kubernetes:master` from `PushkarJ:patch-1` on May 22, 2021

sig-security-assess-capi ×

★ Get Notifications for All Messages Start a Call

[About](#) [Members 80](#) [Integrations](#) [Settings](#)

Topic [Edit](#)
Working doc: <https://bit.ly/3wJMWC>
Minutes: <https://bit.ly/3eXr5AL>

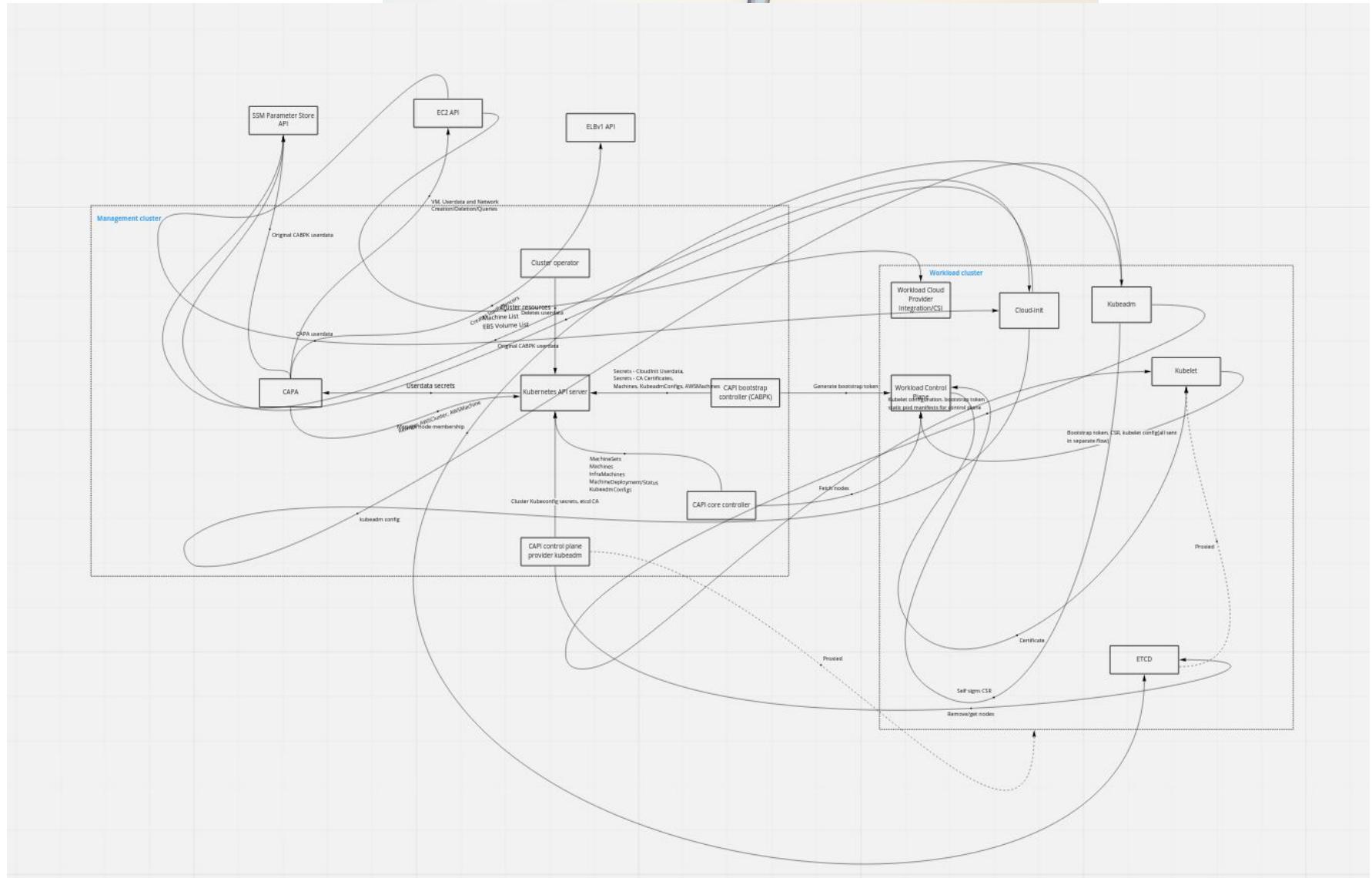
Description [Edit](#)
Affiliated with [#sig-security](#)

Low hanging fruit for OSS projects

The screenshot shows the OpenSSF Best Practices dashboard for the "Kubernetes Cluster API" project. At the top, there's a navigation bar with the OpenSSF logo, the project name, a progress bar indicating 96%, and various actions like Edit, Delete, Projects, Account, and a dropdown menu. Below the header, there's a large circular badge with a trophy icon and the text "CORE INFRASTRUCTURE INITIATIVE BEST PRACTICES". To the right of the badge, the project name "Kubernetes Cluster API" is displayed. Underneath, there are buttons for "Expand panels", "Show all details", and "Hide met & N/A". A callout text states: "Projects that follow the best practices below can voluntarily self-certify and show that they've achieved an Open Source Security Foundation (OpenSSF) best practices badge." It includes a "Show details" button. Another callout shows how to embed the badge: "If this is your project, please show your badge status on your project page! The badge status looks like this: openssf best practices in progress 96% Here is how to embed it: Show details". At the bottom, it says "These are the passing level criteria. You can also view the silver or gold level criteria."

The screenshot shows a detailed view of the "Identification" section of the OpenSSF Best Practices form. The top bar indicates this is the 13th step of 13, with a blue header bar labeled "Basics". The section starts with the question "What is the human-readable name of the project?" followed by a text input field containing "Kubernetes Cluster API". Below that is the question "What is a brief description of the project?", with a larger text area containing the text: "Cluster API is a Kubernetes sub-project focused on providing declarative APIs and tooling to simplify provisioning, upgrading, and operating multiple Kubernetes clusters.". The final visible question at the bottom is "What is the URL for the project (as a whole?)", with a corresponding text input field.

Data Flow Diagrams



Scoping

Some of the possibilities

- The operating system
- All of the cloud providers:
AWS/Azure/Google/vSphere/OpenStack
etc...
- Hardware trust systems
- Tenancy boundaries
- Core Kubernetes components
 - kubelet
 - kube-controller-manager
- Certificates!!

What's already done

- [Kubernetes security review](#)
 - Covers core componentry
- Cloud providers
 - [AWS shared responsibility model](#)

Where do the project contributors skills and primary contributions lie

- kubeadm
- AWS Networking & Security

Reasonable scope

- Take a slice through system:
 - Machine bootstrapping
 - Control plane bootstrapping

In Sync too

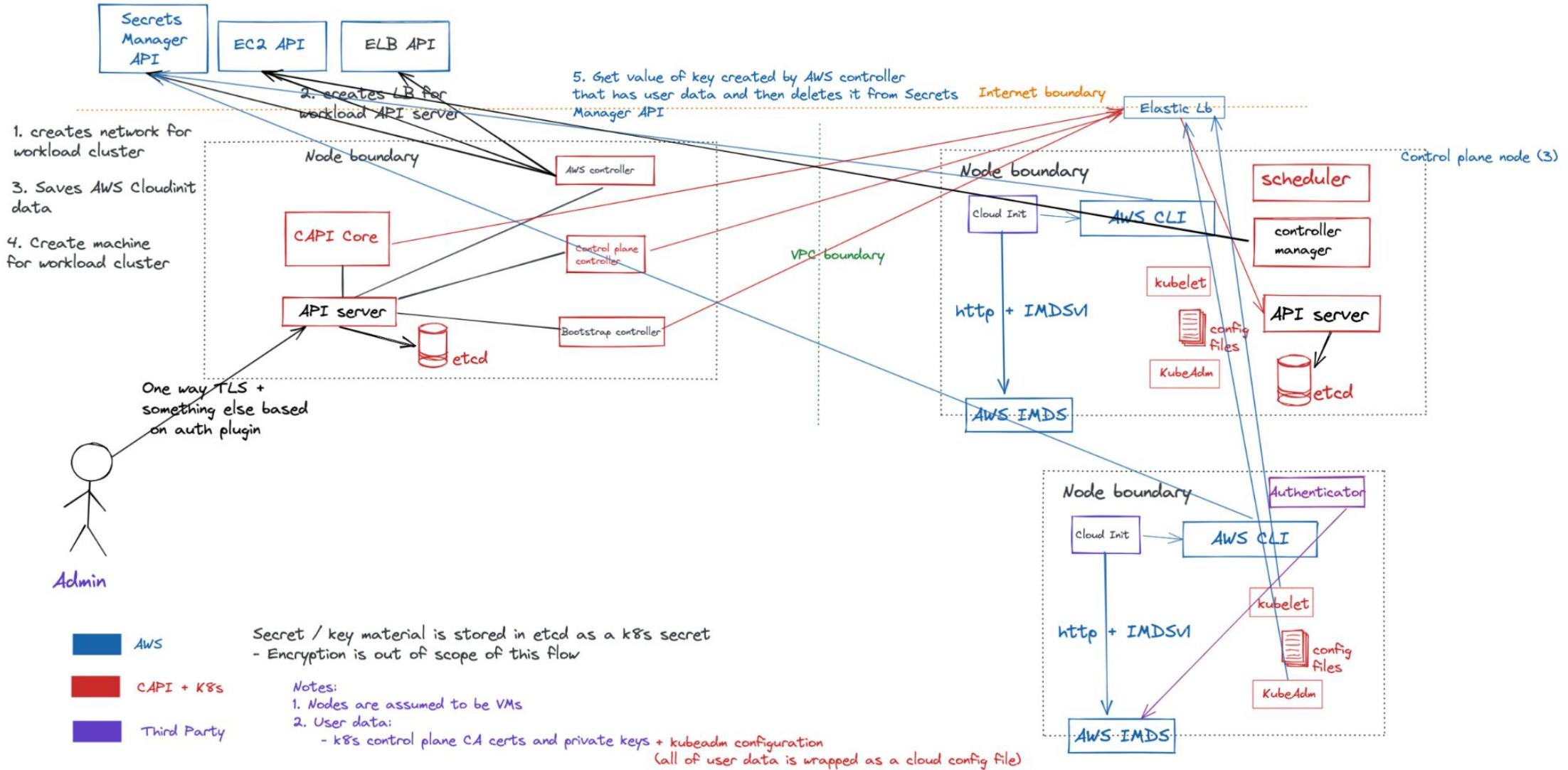
PLAY ALL

Kubernetes SIG Security Self-Assessments

5 videos • 32 views • Last updated on Feb 23, 2022

Public ▼

Data Flow Diagrams



Pre-drafts

A Google doc created, based on a template

<https://bit.ly/capi-sa-draft>

Kubernetes SIG-Security Cluster API Self-Assessment Last edit was on February 16

File Edit View Insert Format Tools Extensions Help

Cluster API Self-Assessment

MetaData

Last Modified: 2022/01/27
Authors: Naadir Jeewa, Ankita Swamy, Pushkar Joglekar, Robert Ficcia
Hackmd version: <https://hackmd.io/g1YUwlfDTlu0o0BLKjPscw?both>

[MetaData](#)
[Overview](#)
[Impact](#)
[Scope](#)
[Process level](#)
[Technical](#)
[Not in Scope](#)

[Communication Channels](#)
[Slack Channel in Kubernetes Workspace](#)
[Github Tracker](#)
[Primary Community Contact:](#)

Pre-drafts

In preparation for the final pull request, we moved to HackMD

<https://bit.ly/capi-sa-hackmd>

The screenshot shows a HackMD editor window with the following content:

```
1 ---  
2 breaks: false  
3 ---  
4 <!-- markdownlint-configure-file { "MD013": { "line_length": 120 } } -->  
5 <!-- markdownlint-disable-file MD034 -->  
6  
7 # Cluster API Security Self-Assessment  
8  
9 ## Metadata  
10  
11 * **Last Modified**: 2022-02-23  
12 * **Youtube Recordings**: [Cluster API Security Self-assessment Playlist](https://www.youtube.com/watch?v=PhIhakKnJGE&list=PLrQN4xC6U5d8jQyZ9uw7RX5Xo0sgcti)  
13 * **Authors** (alphabetical order):  
14   * [Ankita Swamy](https://github.com/Ankitasw)  
15   * [Naadir Jeewa](https://github.com/randomvariable)  
16   * [Pushkar Joglekar](https://github.com/pushkarj)  
17   * [Robert Ficcaiglia](https://github.com/rficcaglia)  
18 * **Github issue**: https://github.com/kubernetes/sig-security/issues/8  
19  
20 ## Overview  
21  
22 This is a working document to describe the security assessment of the [Cluster API](#cluster-api) sub-project of [Kubernetes](#Kubernetes-Security-Review). This is the pilot exercise to enable [Kubernetes SIG Security](#Kubernetes-SIG-Security) to extend the great processes and methodologies from CNCF Security TAG (Technical Advisory Group) on doing [security reviews](#TAG-Security-Reviews)  
23  
24  
25  
26  
27  
28  
29  
30 This is a pilot exercise on how Kubernetes SIG Security can perform a security assessment of sub-projects where there may or may not be a separate working group or a SIG focussed on the sub-project and security. For example in this pilot, we have SIG Cluster Lifecycle focused on cluster-api project and sig-security focused on overall security of the Kubernetes project including its sub-projects.  
31  
32  
33
```

The right side of the screenshot shows the published version of the document on a website:

- Header: CHANGED 7 MONTHS AGO, Sign in, Print
- Title: Cluster API Security Self-Assessment
- Section: Metadata
 - Last Modified: 2022-02-23
 - Youtube Recordings: Cluster API Security Self-assessment Playlist
 - Authors (alphabetical order):
 - Ankita Swamy
 - Naadir Jeewa
 - Pushkar Joglekar
 - Robert Ficcaiglia
 - Github issue: <https://github.com/kubernetes/sig-security/issues/8>- Section: Overview

This is a working document to describe the security assessment of the Cluster API sub-project of Kubernetes. This is the pilot exercise to enable Kubernetes SIG Security to extend the great processes and methodologies from CNCF Security TAG (Technical Advisory Group) on doing security reviews
- Section: Impact

This is a pilot exercise on how Kubernetes SIG Security can perform a security assessment of sub-projects where there may or may not be a separate working group or a SIG focussed on the sub-project and security. For example in this pilot, we have SIG Cluster Lifecycle focused on cluster-api project and sig-security focused on overall security of the Kubernetes project including its sub-projects.
- Section: Scope

Complete an end to end assessment, solicit and incorporate feedback on the process, tools and methodologies to define how this process can be revised after completion of this initial pilot as template for future iterations of CAPI itself, and other future sub-project assessments. As a derivative product of this effort it is hoped that the sub-project community learns new things about secure coding, secure devops, security reviews / assessments, and reporting and resolving security issues so as to become more self-sufficient and proactive in the day-to-day maintenance and development of new features (i.e. instead of relying on discrete and infrequent point-in-time efforts post hoc).

Draft PRs



PushkarJ changed the title ~~Initial Draft for Cluster API Security Assessment~~ Cluster API Security Self Assessment on May 13

- ✓ sig-security-assessments/cluster...
 - ✓ images
 - data-flow-diagram-cluster-...
 - data-flow-diagram-cluster-...
 - excalidraw-data-flow-diagr...
 - mgmt-and-workload-cluste...
 - self-assessment.md

PR Reviews

Cluster API Security Self Assessment #40

Merged k8s-ci-robot merged 2 commits into `kubernetes:main` from `PushkarJ:add-cluster-api-sec-assessment` on Jul 14

Conversation 72 Commits 2 Checks 0 Files changed 5 +1,134 -0

PushkarJ commented on Mar 2 • edited Member

Description

SIG Cluster Lifecycle and SIG Security worked together over several months, inspired from <https://github.com/cncf/tag-security> self-assessment process to write this self-assessment that identifies feature and documentation that needs work to improve the security posture of the sub-project.

Note

This is the first of it's kind effort at CNCF where a sub-project of a graduated project was assessed via collaboration between Security experts and maintainers of this sub-project. Past self-assessments via CNCF TAG Security have been focussed on *graduating* projects.

If you would like to request self-assessment for your sub-project, please create an issue by clicking on this [link](#)

Fixes #8

xref [cncf/tag-security#603](#) and [kubernetes-sigs/cluster-api#4446](#)

Project Tracker

All the issues that are an outcomes of the self-assessment are tracked here:
<https://github.com/orgs/kubernetes/projects/83/views/1>

/sig security cluster-lifecycle
/area security
/kind feature
/cc @sbueringer @Ankitasw @rficcaglia @randomvariable

Reviewers

- neolit123
- sbueringer
- fabriziopandini
- rficcaglia
- randomvariable

Assignees

- aladewberry

Labels

- approved
- cncf-cla: yes
- kind/feature
- lgtm
- sig/cluster-lifecycle
- sig/security
- size/XXL
- tide/merge-method-squash

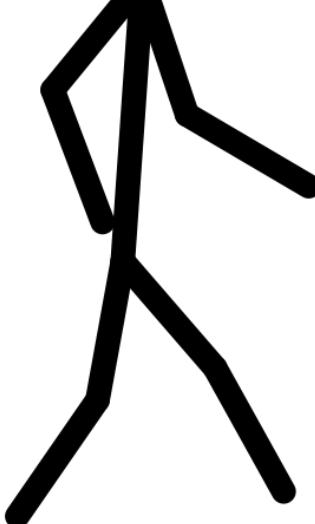
Projects

- sig-security-tracker

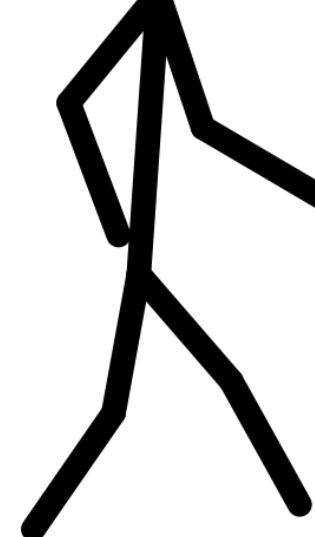
Milestone

No milestone

Changes: Roles and Responsibilities



- Moved from 50/50 downstream + upstream split to 30/70 split in favor of upstream - yay!
- New sub-project was formed to ensure this process can be repeatable for future sub-project self-assessments



- Moved from upstream to work on downstream
- Found replacements who would continue working as SMEs of cluster-api

Fuzz Testing

Security Self Assessment: [DEV-3] Setup Cluster API on oss-fuzz #6059

Closed

randomvariable opened this issue on Feb 3 · 11 comments



randomvariable commented on Feb 3

Member



...

Assignees



AdamKorcz

Labels

area/security

area/testin

sig/security

Projects



sig-security-tracker

Done ▾

See also: "Fuzzing Session: Finding Bugs and Vulnerabilities Automatically" - David & Adam Korczynski, Ada Logics at 4pm on Friday in Room 260:
<https://sched.co/1BvfI>

Final outcome

Ref: <https://github.com/kubernetes/sig-security/tree/main/sig-security-assessments/cluster-api>

main sig-security / sig-security-assessments / cluster-api / self-assessment.md Go to file ...

PushkarJ Cluster API Security Self Assessment (#40) ... Latest commit 1e6f14d on Jul 14 History

1 contributor

1083 lines (832 sloc) | 51.4 KB

<> Raw Blame

main sig-security / sig-security-assessments / cluster-api / capi_2022_fuzzing.pdf Go to file ...

AdamKorcza Add Cluster API fuzzing report ✓ Latest commit f749938 on Jul 13 History

1 contributor

320 KB

Download

What's Next?

⊕ [Cluster API] SIG Security Self-Assessment

[Cluster API] SIG Security Self-Assessment + New view

Filter by keyword or by field

Planned 11

- cluster-api #6151 Security Self Assessment: [DEV-1] Update OWNERS file and associated permissions
- image-builder #803 Security Self Assessment: [STRIDE-TAMPER-2] Produce an SBoM for machine images
- cluster-api #5398 Security Self Assessment: [DEV-2] Verify vulnerability reporting process
- cluster-api #3762 ... Security Self Assessment: [STRIDE-SPOOF-4] [STRIDE-SPOOF-5] Machine attestation for secure kubelet registration
- cluster-api #6153 Security Self-Assessment: [STRIDE-TAMPER-1] Produce a SBoM
- cluster-api #6515 Security Self Assessment: [STRIDE-DOS-1] Misuse of cloud credentials to create unlimited number of cloud resources

To be Implemented 1

- cluster-api #4219 Cluster API Kubelet Authentication

Implemented 3

- cluster-api #5490 Security Self Assessment: [STRIDE-INFODISCLOSE-3] RFE: Improve certificate management in Cluster API
- cluster-api #6059 Security Self Assessment: [DEV-3] Setup Cluster API on oss-fuzz
- cluster-api #6329 Security Self-Assessment: [STRIDE-MULTIPLE] Secure Cluster Class for Cluster API (MVP)

+ Add item

+ Add item

+ Add item

Ref:

<https://github.com/orgs/kubernetes/projects/83/views/1>

What's Next?

Thursday, October 27 • 3:25pm - 4:00pm

[Back To Schedule](#)

SIG Security: Empowerment Through Autonomy - Ala Dewberry, VMware; Savitha Raghunathan, Red Hat; Tabitha Sable, Datadog

[Sign up](#) or [log in](#) to save this to your schedule, view media, leave feedback and see who's attending!

<https://sched.co/182t>

[Tweet](#)

[Share](#)

SIG Security takes a community-building approach to improving Kubernetes security, both for the project itself and our end users. Join organizers Ala, Rey, Savitha, and Tabitha for an overview of how we make space for security collaboration to thrive. We'll share timely updates from our documentation, third-party audit, and tooling subprojects. Security self-assessments will be a special focus, with a deep-dive on this new service offered to Kubernetes by our newest subproject! The Self-Assessments subproject in SIG Security is here to make security introspection accessible to any and all SIGs and subprojects. We aim to give SIGs and subprojects a repeatable and rigorous way to think about their own security, making Kubernetes safer to use as more workloads find their way to it. You'll learn what's been going on, what's next, and how you could join in, regardless of your experience from beginner to expert. We hope to see you there!

Q & A

You ask & we try to answer :)

Thank you!

See you around :)



BUILDING FOR THE ROAD AHEAD

DETROIT 2022



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