KubeCon | CloudNativeCon

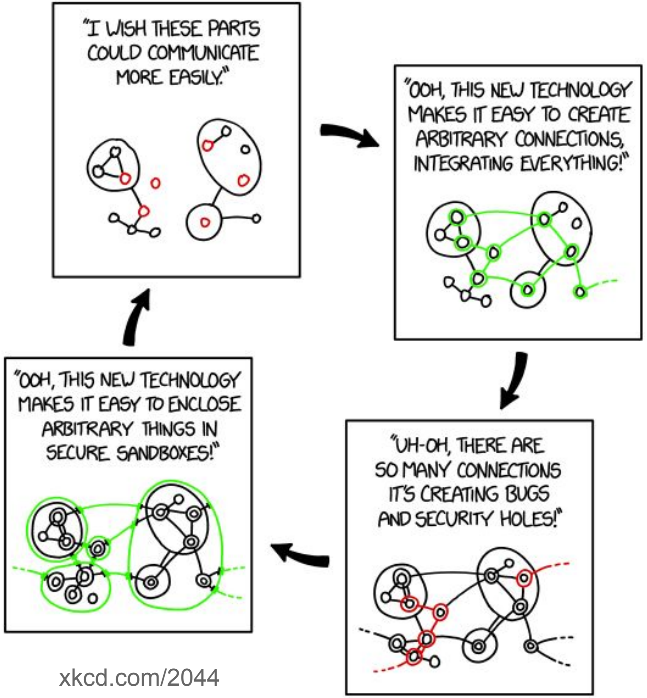
North America 2018

SIG-Auth Intro

Tim Allclair, Mike Danese,
Mo Khan, Jordan Liggitt

SIG-Auth Intro

What do we do?


"I WISH THESE PARTS COULD COMMUNICATE MORE EASILY."
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO CREATE ARBITRARY CONNECTIONS, INTEGRATING EVERYTHING!"
"UH-OH, THERE ARE SO MANY CONNECTIONS IT'S CREATING BUGS AND SECURITY HOLES!"
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO ENCLOSE ARBITRARY THINGS IN SECURE SANDBOXES!"

xkcd.com/2044

SIG-Auth Intro

What do we do?

Scope (https://github.com/kubernetes/community/blob/master/sig-auth/charter.md):

> SIG Auth is responsible for the design, implementation, and maintenance of features in Kubernetes that control and protect access to the API and other core components. This includes authentication and authorization, but also encompasses features like auditing and some security policy

Subprojects (https://github.com/kubernetes/community/blob/master/sig-auth#subprojects):

- Audit
- Authenticators
- Authorizers
- Certificates
- Encryption at rest
- Node identity/isolation
- Policy
- Service accounts

SIG-Auth Intro

Who are we?

Chairs:

Tim Allclair (@tallclair), Mike Danese (@mikedanese), Mo Khan (@enj)

Subproject approvers:

@deads2k, @immutableT, @liggitt, @mikedanese, @smarterclayton, @sttts, @tallclair

Subproject reviewers:

@awly, @caesarxuchao, @CaoShuFeng, @david-mcmahon, @dims, @enj, @erictune, @errordeveloper, @hongchaodeng, @hzxuzhonghu, @jianhuiz, @krmayankk, @krousey, @lavalamp, @mbohlool, @mml, @ncdc, @nikhiljindal, @pweil-, @sakshamsharma, @sttts, @thockin, @timothysc, @wojtek-t

SIG-Auth Intro

Where can you find us?

Slack channel: #sig-auth

Home page: https://github.com/kubernetes/community/tree/master/sig-auth

Mailing list: https://groups.google.com/forum/#!forum/kubernetes-sig-auth

Bi-weekly meetings Wednesday at 11PT (agenda/recordings links on home page)

What happened last year?

- External client-go credential providers (beta in 1.11)
- Better Node isolation in NodeRestriction admission
  - Protection of taints (1.11)
  - Protection of specific labels and self-deletion (1.13)
- Better audit
  - Authorization and admission annotations added to audit events (1.12)
  - Audit event API promoted to v1 (1.12)
  - Dynamic audit sink registration (alpha in 1.13)
- Etcd encryption graduated to stable (1.13)

What happened last year?

- Work started on better service account tokens
  - TokenRequest API (time-, pod-, and audience-bound service account tokens) (beta in 1.12)
  - ServiceAccountTokenVolumeProjection for mounting these tokens into pods (beta in 1.12)
  - BoundServiceAccountTokenVolume to switch the automatically injected token (alpha in 1.13)

- Learn more
  - Deep Dive: Container Identity WG - Greg Castle & Michael Danese
    Thursday, December 13 • 1:45pm - 2:20pm

  - Navigating Workload Identity in Kubernetes - Michael Danese & Spike Curtis
    Wednesday, December 12 • 4:30pm - 5:05pm

What’s coming next year?

- Working on roll out of better service account tokens
  - Updating client libraries to handle tokens that require refreshing
  - Opt-in switch to admission injecting better tokens into pods
  - Looking to make that the default behavior on an API server config version boundary
- Dynamic audit
  - Per-sink policy
  - Work through apiserver -> webhook authentication design
- Refining approach to policy
  - Dynamic admission ecosystem, including a general purpose policy engine
  - New domain-specific policies: scheduling, images, rethinking PodSecurityPolicy
  - Extending node authz & restriction to DaemonSets & workloads

How to get involved

New Contributors

- good first issue labels
- Have a cool idea? Awesome! Prototype it through a plugin.
  Authorization & Authentication webhooks, Dynamic Admission, Dynamic Audit
- Quality is a **top priority** for 2019: expand test coverage & improve documentation

Experienced Contributors

- help wanted labels
- Help with PR reviews! (even if you're not a "sig auth reviewer")
- Help with issue triage, identify "good first issue" and "help wanted"

SIG-Auth Intro

What do you want to talk about?