
KubeCon
CloudNativeCon
North America 2024

KubeCon | CloudNativeCon

North America 2024

Pushing Authorization Further

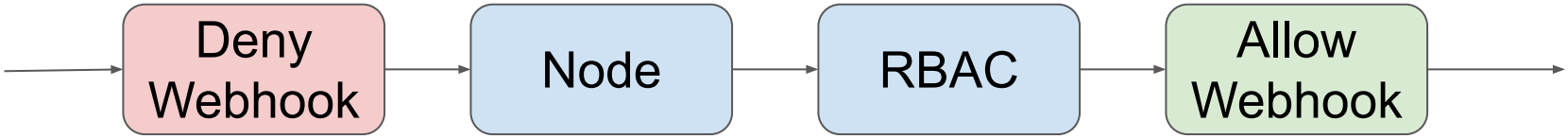
CEL, Selectors (and maybe RBAC++)

Anish Ramasekar & Rita Zhang, Microsoft
Jordan Liggitt, Google

Graduated Features in 2024

Structured Authorization Config

kep.k8s.io/3221, beta in v1.30, stable in v1.32 @liggitt, @palnabarun, @ritazh



1 second timeout
Deny on error
Only kube-system namespace
Exempt system controllers

5 second timeout
NoOpinion on error

2023 Kubecon demo

Structured Authentication Config

kep.k8s.io/3331, beta in v1.30

@aramase, @enj

JWT claims:

```
{
  "username": "jane_doe",
  "sub": "119abc",
  "roles": "admin,user",
  "aud": "kubernetes",
  ...
}
```

Resulting user:

```
username: "jane_doe:external"
uid: "119abc"
groups: ["admin", "user"]
extra:
  other_attributes: ["example"]
  client_name: ["kubernetes"]
```

Graduated Features

Label / Field Selector Authorization

kep.k8s.io/4601, beta in v1.32

@deads2k, @liggitt

- Authorizers see label / field selectors for list / watch requests
- Node authorizer limits nodes to listing/watching their own pods
- Webhook authorizers can limit list and watch requests based on the label or field selector used. Examples:
  - “**`node1`** can only list pods with **`.spec.nodeName=node1`**”
  - “**`myingress`** can watch secrets with **`controller=myingress`**”

Graduated Features

Node Info in Service Account Tokens

kep.k8s.io/4193, beta in v1.30, stable in v1.32 @enj, @munnerz

- Node name included in service account token claims

  `"node":{"name":"my-node","uid":"..."}`
- Node name surfaces as a user attribute

  `"authentication.kubernetes.io/node-name":["my-node"]`
- Usable by authorization / admission (ValidatingAdmissionPolicy)
- Foundation for future work to keep service account credentials being an escalation path for nodes

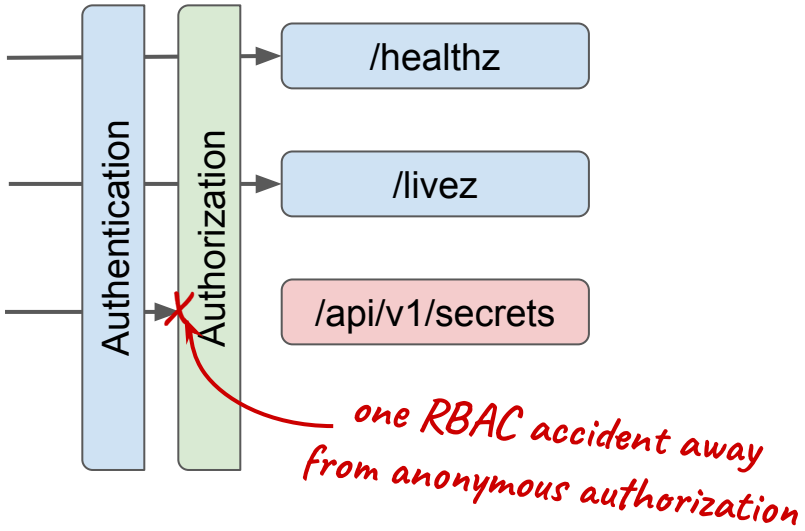
2024 Kubecon demo

Restricted Anonymous Authentication

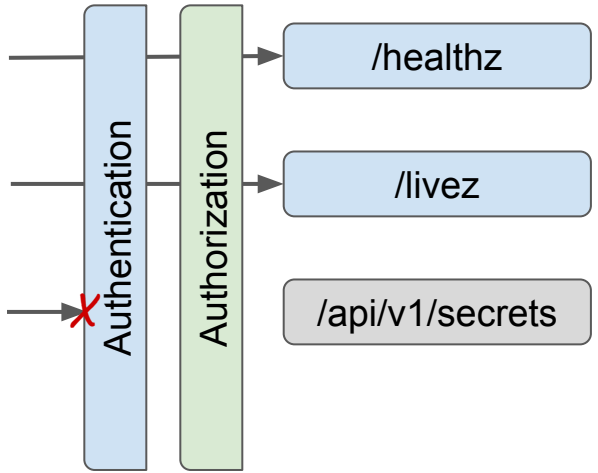
kep.k8s.io/4633, beta in v1.32

@vinayakankugoyal

Before:



After:



Upcoming Features

Upcoming Features

Cluster Trust Bundle

kep.k8s.io/3257, targeting beta in 1.33, @ahmedtd

Publish CA root bundles in API objects, mounted into pods

Pod Certificates

kep.k8s.io/4317, targeting alpha in 1.33, @ahmedtd

x509 client certificates for service account identities, mounted into pods

Upcoming Features

External service account token signing

kep.k8s.io/740, alpha in 1.32, @ahmedtd, @HarshalNeelkamal, @liggitt

Token signing: in-process with local private key file → gRPC call
Token verification keys: local public key files → gRPC call
Removes key signing material from the kube-apiserver
Allows dynamic updates of public verifying keys
Can integrate with cloud KMS signers, external audit of token signatures

Upcoming Features

Fine-grained Kubelet Authorization

kep.k8s.io/2862, alpha in 1.32, @vinayakankugoyal

Authorize *just* the `/configz`, `/healthz`, or `/pods` kubelet API endpoints

Avoid over-granting permissions to local monitoring processes

Upcoming Features

Deleting undecryptable / corrupt resources

kep.k8s.io/3926, alpha in 1.32, @stlaz, @tkashem

The unexpected (both human and cosmic) does happen
Can prevent decoding of an object written to etcd
Failure was *really* bad (unlistable resource type, undeletable object)
Recovery was *really* bad (bypass API and delete directly from etcd)
Allows force delete (with sufficient permissions) of corrupt objects

Upcoming Features

Image pull credential verification

kep.k8s.io/2535, targeting alpha in 1.33, @stlaz

Automatically prevent unauthorized use of images already on the node

Service account image pull credentials

kep.k8s.io/4412, targeting alpha in 1.33, @aramase, @enj

Opt into using service account tokens as image pull credentials

Upcoming Features

Node-restricted service accounts

kep.k8s.io/4935, in design, @vinayakankugoyal

Goal: Constrain a service account so it can’t be a node escalation path

Upcoming Features

Kubelet Serving Certificate Validation

kep.k8s.io/4872, in design, @g-gaston

Additional TLS checks when talking to nodes

Verify node identity in addition to standard IP/DNS validation

Upcoming Features

Secrets Store Sync Controller

sigs.k8s.io/secrets-store-sync-controller, in alpha, @nilekhc

SIG Auth subproject

Controller to sync from external secrets store to Kubernetes secrets

User Stories for Authorization

User stories

- A node can only list pods scheduled to it
  - (already done by node authorizer; this is about being able to express similar policy)
- A node agent can only list a custom resource matching the node it is running on
- A node agent can only get a custom resource with a name matching the node it is running on
- A controller can list all secrets of a particular type
- A controller can list all secrets with a particular label
- Allow access based on extra attributes of user.Info
- Allow access based on namespace or name prefix

these are already achievable
with webhook authorization

but... declarative?

RBAC++

Questions?

https://git.k8s.io/community/sig-auth

Bi-weekly meetings (Wednesday at 11am Pacific Time)
Mailing list: kubernetes-sig-auth@googlegroups.com
Kubernetes Slack: #sig-auth