aws

KUBECON EUROPE 2025

Cedar Access Control For Kubernetes

Simplify security with powerful, flexible policies.

Micah Hausler

Principal Kubernetes Software Engineer

Rodrigo Bersa

Sr. WW Containers Specialist SA

What is Cedar for K8s?

SINGLE POLICY LANGUAGE FOR KUBERNETES AUTHORIZATION AND ADMISSION CONTROL

Unified Policy Language

One language for both authorization and admission policies

Dynamic control

Create rules based on user attributes and request details

Feature Rich

Supports label-based access, conditions, denial policies

The Current Challenge

Multiple Languages

Admins must learn different policy languages

Fragmented Security

Permits in one file, restrictions in another

Risk of Gaps

Hard to see complete picture during reviews

Cognitive Overhead

Difficult to reason about overall security posture

1

2

3

4

aws

Cedar's Solution

UNIFIED SECURITY POLICY

1 **Single Policy File**

Both permissions and restrictions in one place

2 **Clear Reasoning**

Easily understand what's allowed and what's restricted

3 **Fleet Management**

Apply policies across multiple clusters

4 **Powerful Controls**

Reference requesters, attributes, and add conditions

Cedar and Kubernetes RBAC

RBAC

Built-in framework

Allow-only policies

Resource-focused access

Limited conditions

Cedar

Flexible policy language

Allow and deny policies

Requester-attribute based

Full request evaluation

Demo time!

Cedar Authorization Policy

```
→ cedar-access-control-for-k8s git:(main) × []
```

Cedar Impersonation Policy

```
→ cedar-access-control-for-k8s git:(main) × []
```

Cedar Admission Policy

```
→ cedar-access-control-for-k8s git:(main) ✗ []
```

Get involved

CEDAR ACCESS CONTROL FOR KUBERNETES

Current Status

Active development, not yet production-ready

github.com/awslabs/cedar-access-control-for-k8s

Community

Join #cedar-for-k8s Slack channel

Thank you!

Micah Hausler
mhausler@amazon.com
linkedin.com/in/micahhausler

Rodrigo Bersa
bersr@amazon.com
linkedin.com/in/bersa/