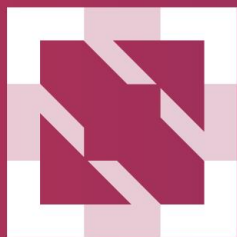




KubeCon



CloudNativeCon

India 2024





KubeCon



CloudNativeCon

India 2024

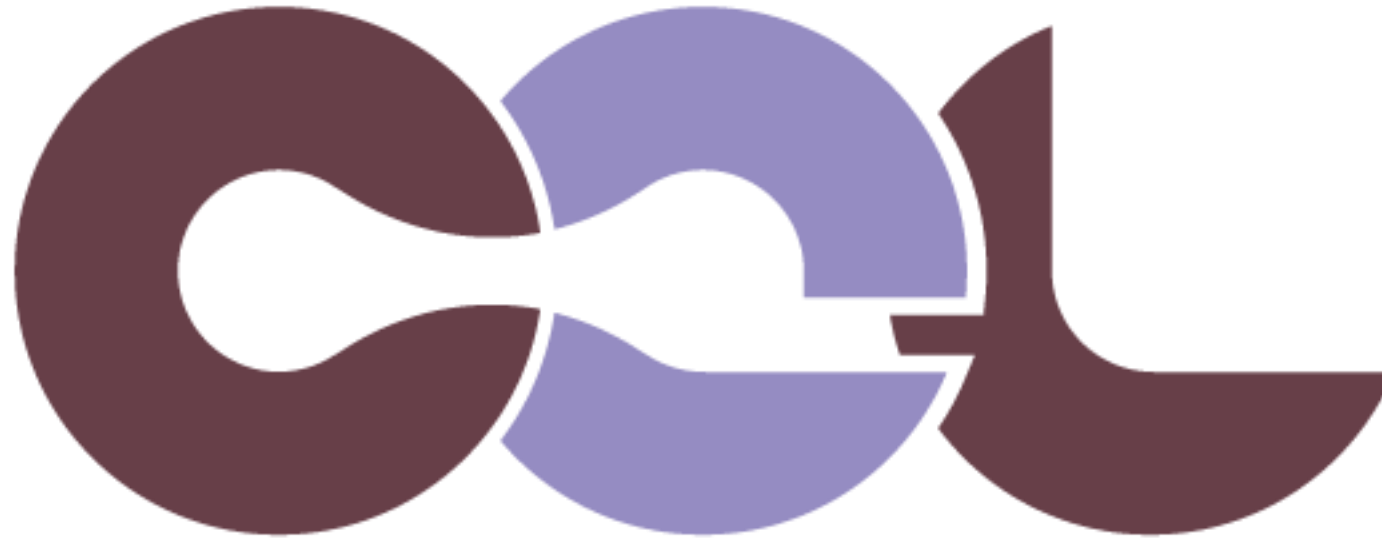
Enhance Kubernetes Security with the Common Expression Language (CEL)

Cloud Solutions Architect / Cloud Native Engineer

{{ CNCF Ambassador, KubeStronaut }}

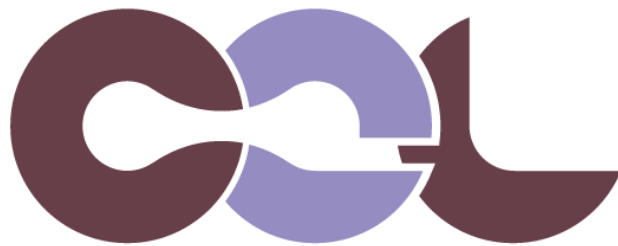
Hoon Jo@Megazone

What I aim to tell you today.



COMMON EXPRESSION LANGUAGE

What I aim to tell you today.



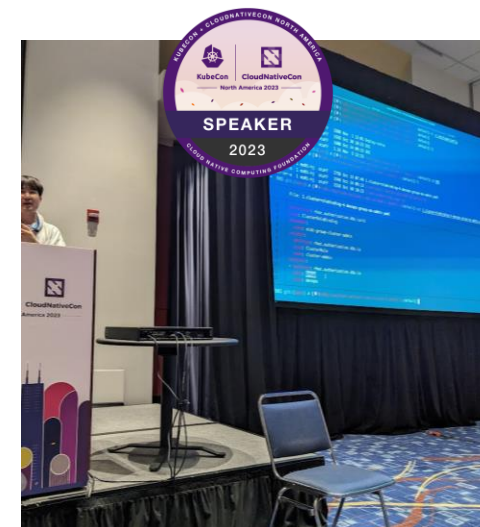
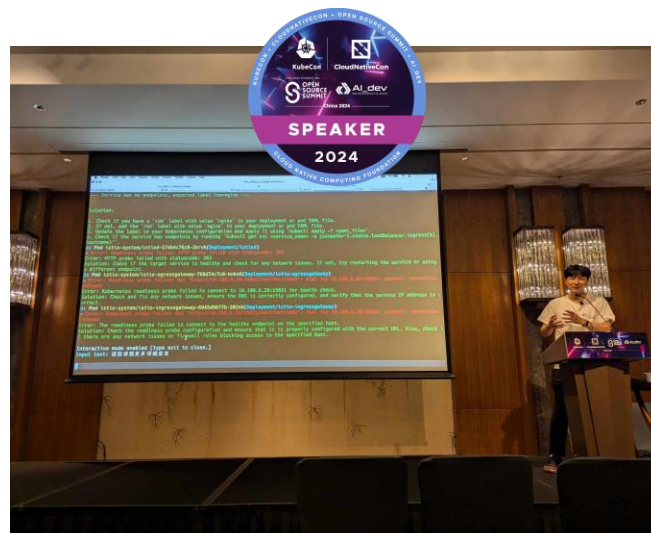
COMMON EXPRESSION LANGUAGE



Open Policy Agent



Kyverno



Who am I ?



<https://github.com/SysNet4Admin>



<https://www.linkedin.com/in/hoonjo/>



KubeCon

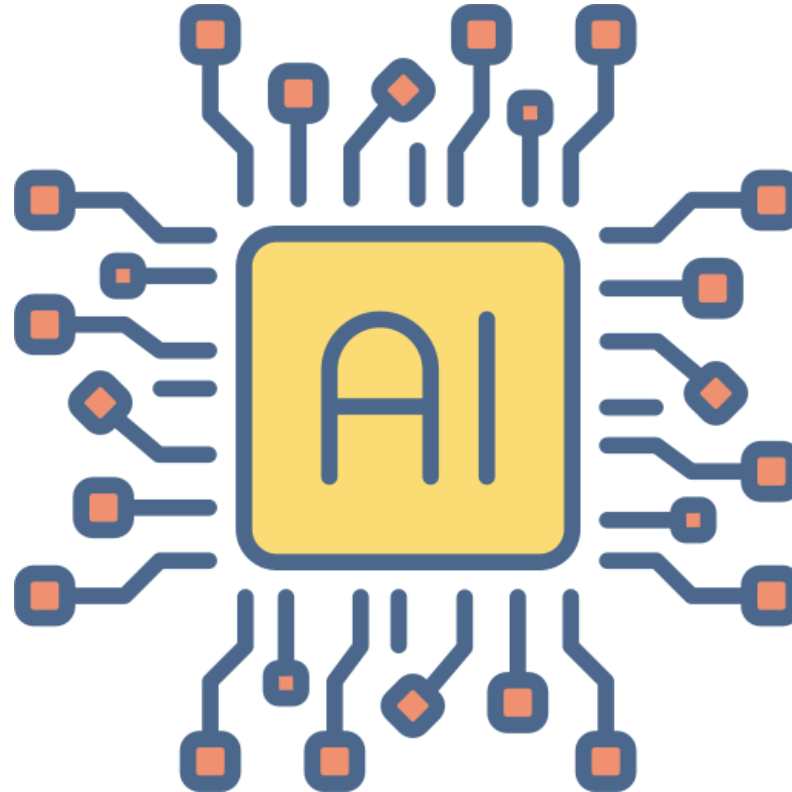


CloudNativeCon

India 2024

PART I - Intro

Why do we know new CODE in the era of AI?

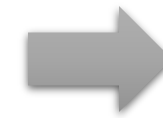


Because... the human is biggest vulnerability

“Social engineering
bypasses all technologies,
including firewalls.”



Who knows the human inside?



AI is good but not perfect for the SECURITY

Junior Programmer: Everything looks perfect but still it doesn't work.

Senior Programmer:





KubeCon

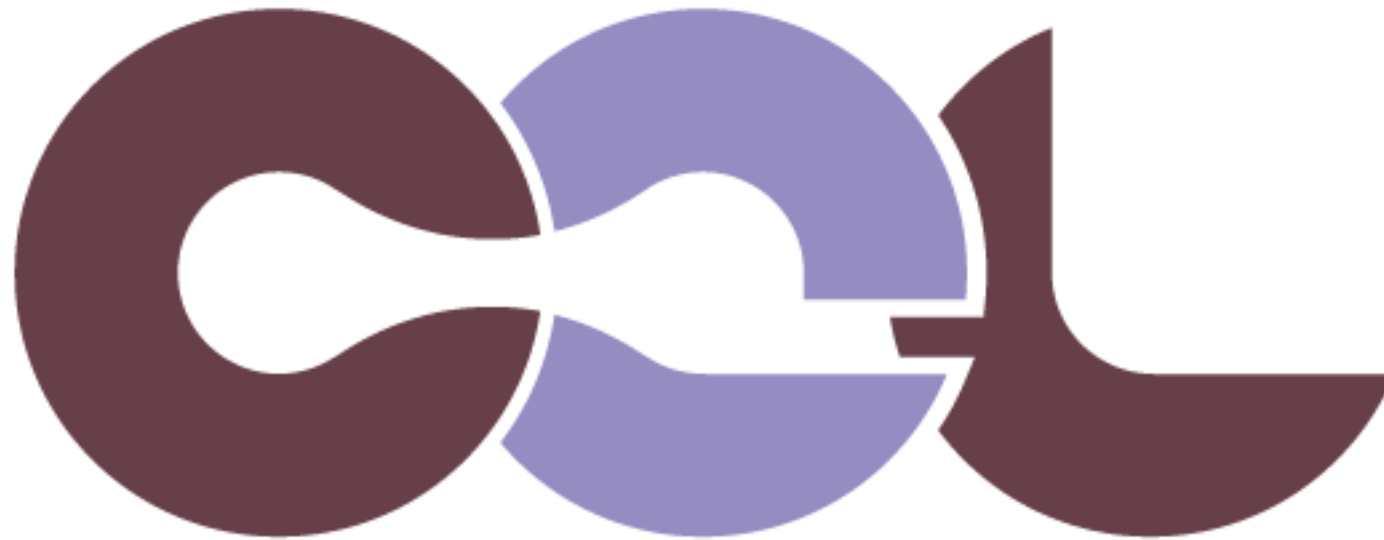


CloudNativeCon

India 2024

PART II - CEL

Easy to learn the CEL



COMMON EXPRESSION LANGUAGE

CEL Condition & Construction



1. Keep it small & fast.


- o CEL evaluates in linear time, is mutation free, and not Turing-complete. This limitation is a feature of the language design, which allows the implementation to evaluate orders of magnitude faster than equivalently sandboxed JavaScript.

2. Make it extensible.

- o CEL is designed to be embedded in applications, and allows for extensibility via its context which allows for functions and data to be provided by the software that embeds it.

3. Developer-friendly.

- o The language is approachable to developers. The initial spec was based on the experience of developing Firebase Rules and usability testing many prior iterations.
- o The library itself and accompanying toolings should be easy to adopt by teams that seek to integrate CEL into their platforms.




```
// Condition
account.balance >= transaction.withdrawal
|| (account.overdraftProtection
    && account.overdraftLimit >= transaction.withdrawal - account.balance)

// Object construction
common.GeoPoint{ latitude: 10.0, longitude: -5.5 }
```

<https://github.com/google/cel-spec>

Into the CEL

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
metadata:
  name: celvalidatingadmissionpolicynohostnetwork
spec:
  matchConstraints:
    resourceRules:
      - apiGroups: [""]
        apiVersions: ["v1"]
        operations: ["CREATE", "UPDATE"]
        resources: ["pods"]
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
        object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```



```
spec:
  containers:
    - image: nginx:1.27.2-alpine-slim
      imagePullPolicy: IfNotPresent
      name: nginx
      resources: {}
      terminationMessagePath:
/dev/termination-log
      terminationMessagePolicy: File
      volumeMounts:
        - mountPath:
/var/run/secrets/kubernetes.io/service
account
          name: kube-api-access-h7dj2
          readOnly: true
      dnsPolicy: ClusterFirst
      enableServiceLinks: true
      hostNetwork: true
      nodeName: w3-k8s
```


The history of CEL into the Kubernetes



📄 1

v1.23
Announcement
CHANGELOG
v1.24
Announcement
CHANGELOG
v1.25
Announcement
CHANGELOG
v1.26 (ValidatingAdmissionPolicy, Alpha)
Announcement
CHANGELOG
Other (Cleanup or Flake)
v1.27
Announcement
CHANGELOG
v1.28 (ValidatingAdmissionPolicy, Beta)
Announcement
CHANGELOG
v1.29
Announcement
CHANGELOG
v1.30 (ValidatingAdmissionPolicy, GA / Muta...
Announcement
CHANGELOG
v1.31
Announcement
CHANGELOG
v1.32
Announcement
CHANGELOG

v1.30 (ValidatingAdmissionPolicy, GA / MutatingAdmissionPolicy, Alpha)

Announcement

Graduations, deprecations and removals for Kubernetes v1.30

- **CEL for Admission Control**
 - Kubernetes Enhancement Proposal:
<https://github.com/kubernetes/enhancements/tree/master/keps/sig-api-machinery/3488-cel-admission-control>
 - Discussion Link: https://groups.google.com/g/kubernetes-sig-api-machinery/c/WBVf_oWm4kU
 - Primary contact (assignee): [cici37](#)
 - Responsible SIGs: sig-apimachinery
 - Enhancement target (which target equals to which milestone):
 - Alpha release target (x.y): 1.28
 - Beta release target (x.y): 1.28
 - Stable release target (x.y): 1.30
- **CEL-based admission webhook match conditions**
 - Kubernetes Enhancement Proposal:
<https://github.com/kubernetes/enhancements/tree/master/keps/sig-api-machinery/3716-admission-webhook-match-conditions>
 - Discussion Link:
<https://docs.google.com/document/d/1x9RNAaayO0gXHLr1y50QFb1x8OWnk2v3XnrkT5Y/eJt#bookmark=id.55kd8uoz25p5>
 - Primary contact (assignee): [@talclair](#)
 - Responsible SIGs: api-machinery
 - Enhancement target (which target equals to which milestone):
 - Alpha release target (x.y): 1.27
 - Beta release target (x.y):
 - Stable release target (x.y):

<https://kubernetes.io/blog/2024/04/17/kubernetes-v1-30-release/>

CHANGELOG

API Change

- Fixed a bug in the API server where empty collections of ValidatingAdmissionPolicies did not have an `items` field. ([#126146](#), [@xyz-li](#)) [SIG API Machinery]
- `ValidatingAdmissionPolicy` was promoted to GA and will be enabled by default. ([#123405](#), [@cici37](#))
- Added the feature gates `StrictCostEnforcementForVAP` and `StrictCostEnforcementForWebhooks` to enforce the `strict` cost calculation for CEL extended libraries. It is strongly recommended to turn on the feature gates as early as possible. ([#124676](#), [@cici37](#)) [SIG API Machinery, Auth, Node and Testing]
- OIDC authentication will now fail if the username asserted based on a CEL expression config is the empty string. Previously the request would be authenticated with the username set to the empty string. ([#123568](#), [@eni](#))
- Promoted `AdmissionWebhookMatchConditions` to GA. The feature is now stable, and the feature gate is now locked to default. ([#123560](#), [@ivelichkovich](#))





KubeCon



CloudNativeCon

India 2024

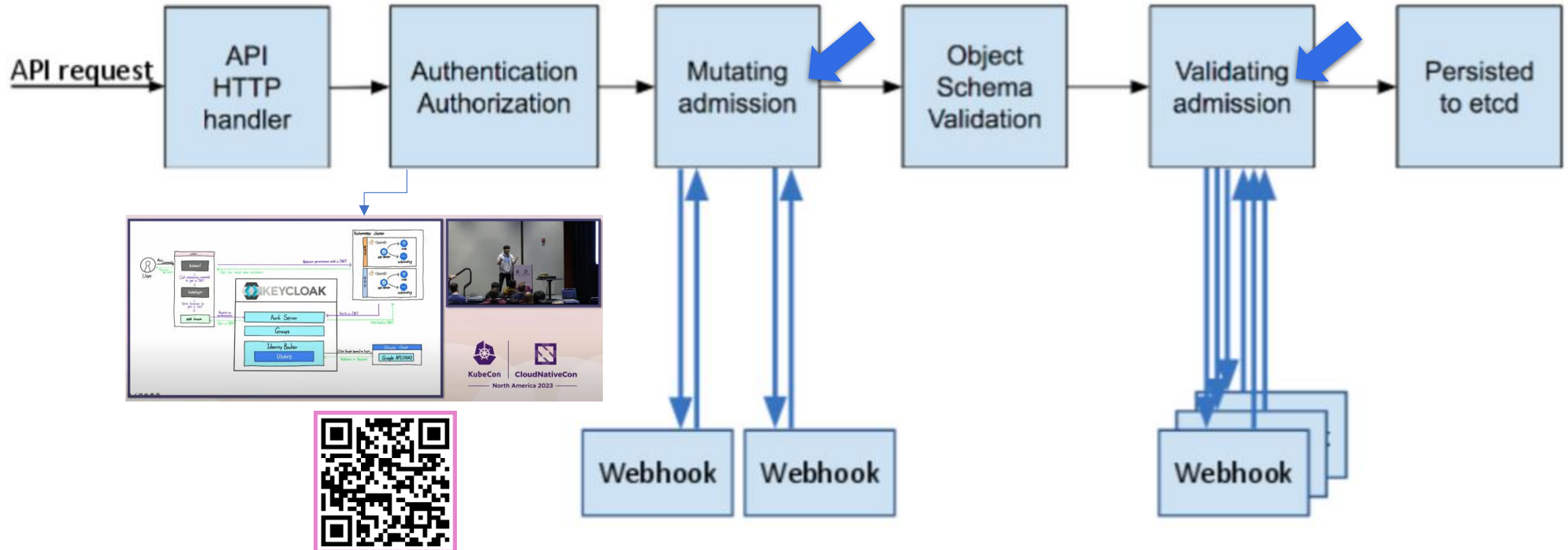
PART III - Admission Control

Admission Controller Phases (2019) > (2024)

OR

apiVersion: admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicy

apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy



Admission Controller Phases (2019) > (2024)

Validating
admission

apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy



apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicyBinding



```
object.spec.hostNetwork != true
```

Mutating
admission

apiVersion: admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicy

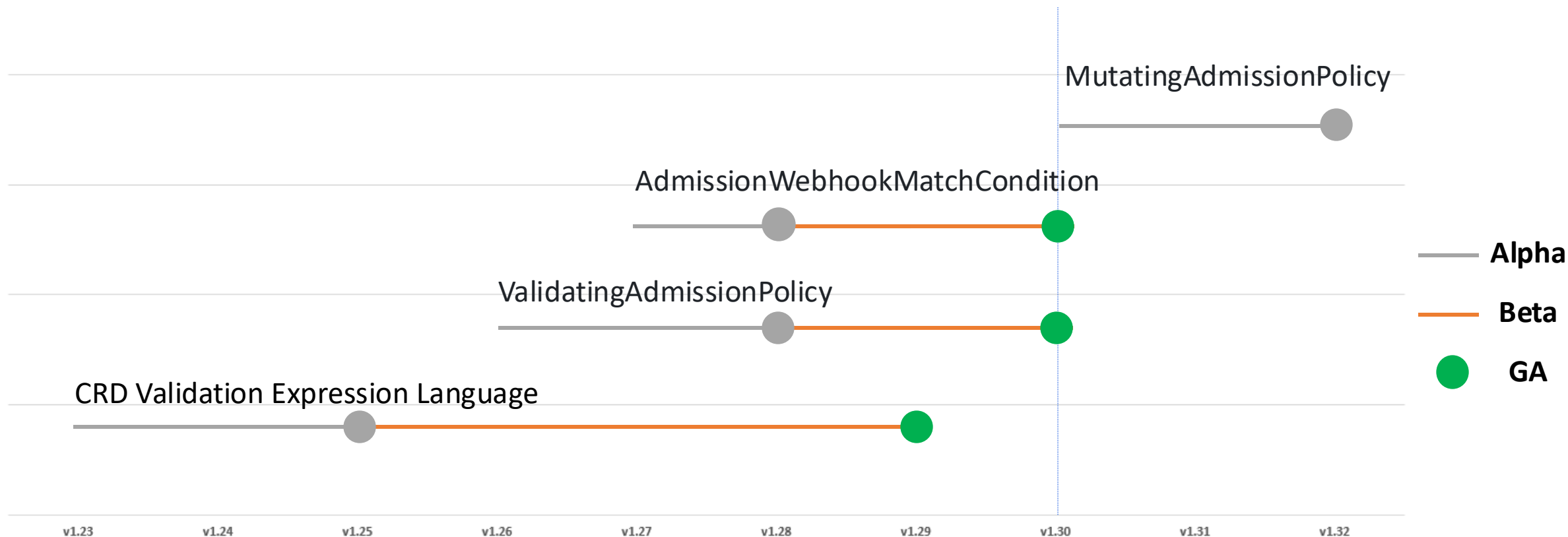


apiVersion: admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicyBinding



```
- (image): "*:latest"  
  imagePullPolicy: "IfNotPresent"
```

Maturity: CEL & Admission





KubeCon



CloudNativeCon

India 2024

PART III - CEL w/ others

Gatekeeper, Kyverno, Native-k8s

Technical & Community Characteristics

| Features / Misc | Gatekeeper | Kyverno | Native-k8s (v1.30~) |
|------------------|-----------------|------------|----------------------------------|
| Validation | Yes | Yes | Yes (GA) |
| Mutation | Yes | Yes | Partly Yes (from 1.30, Alpha) |
| CRD | Yes | Yes | No |
| Language support | Rego, CEL | Yaml, CEL | CEL |
| CNCF Status | Graduated (OPA) | Incubating | - |
| First PR | 2018 Oct | 2019 Mar | 2021 Nov (CEL) |
| GitHub stars | 3.7k | 5.7k | 111k |
| Learning curve | High | Low | Very Low |

Gatekeeper-{{Rego,CEL}}

```
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
  name: regoconstrainttemplatenohostnetwork
spec:
  crd:
    spec:
      names:
        kind: RegoConstraintTemplateNoHostNetwork
  targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package regoconstrainttemplatenohostnetwork

        violation[{"msg": msg}] {
          input.review.kind.kind == "Pod"
          input.review.object.spec.hostNetwork == true
          msg := "HostNetwork is not allowed for the Pod"
        }
```

```
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
  name: celconstrainttemplatenohostnetwork
spec:
  crd:
    spec:
      names:
        kind: CELConstraintTemplateNoHostNetwork
  targets:
    - target: admission.k8s.gatekeeper.sh
      code:
        - engine: K8sNativeValidation
          source:
            validations:
              - expression: "!has(object.spec.hostNetwork) ||
                  object.spec.hostNetwork != true"
                message: "HostNetwork is not allowed for the Pod"
```

Kyverno-{{Yaml,CEL}}

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: yamlclusterpolicynohostnetwork
spec:
  validationFailureAction: Enforce
  rules:
    - name: YamlClusterPolicyNoHostNetwork
      match:
        any:
          - resources:
              kinds:
                - Pod
      validate:
        message: "HostNetwork is not allowed for the Pod"
        pattern:
          spec:
            =(hostNetwork): "false"
```

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: celclusterpolicynohostnetwork
spec:
  validationFailureAction: Enforce
  rules:
    - name: CELClusterPolicyNoHostNetwork
      match:
        any:
          - resources:
              kinds:
                - Pod
              operations:
                - CREATE
                - UPDATE
      validate:
        cel:
          expressions:
            - expression: "!has(object.spec.hostNetwork) ||
                          object.spec.hostNetwork != true"
          message: "HostNetwork is not allowed for the Pod"
```

Native-k8s (v1.30~)

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
metadata:
  name: celvalidatingadmissionpolicynohostnetwork
spec:
  matchConstraints:
    resourceRules:
      - apiGroups: [""]
        apiVersions: ["v1"]
        operations: ["CREATE", "UPDATE"]
        resources: ["pods"]
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
                    object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```

Sum up: Compare with ONLY CEL



Open Policy Agent

```
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
<snipped>
validations:
- expression: "!has(object.spec.hostNetwork) ||
  object.spec.hostNetwork != true"
  message: "HostNetwork is not allowed for the Pod"
```



COMMON EXPRESSION LANGUAGE



Kyverno

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
<snipped>
validate:
  cel:
    expressions:
    - expression: "!has(object.spec.hostNetwork) ||
      object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```



```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
metadata:
  name: celvalidatingadmissionpolicynohostnetwork
spec:
  matchConstraints:
    resourceRules:
    - apiGroups: [""]
      apiVersions: ["v1"]
      operations: ["CREATE", "UPDATE"]
      resources: ["pods"]
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
      object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```





KubeCon



CloudNativeCon

India 2024

PART IV - DEMO on GKE

DEMO on GKE





KubeCon



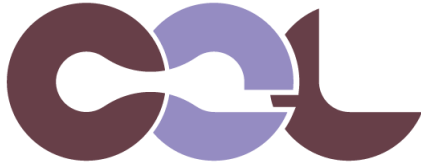













CloudNativeCon

India 2024

PART V - TL; Summary

What is the best choice for your status?

| |  Open Policy Agent |  Kyverno |  COMMON EXPRESSION LANGUAGE |
|---|---|--|---|
|  ValidatingAdmissionPolicy | | |  |
|  ValidatingAdmissionPolicy |  |  | |
|  MutatingAdmissionPolicy | |  |  |
|  MutatingAdmissionPolicy |  |  | |

Any Questions?

KubeCon India 2024's docs

[KubeCon India 2024] #1 History of CEL into the Kubernetes

- ShortURL: <https://m.site.naver.com/1ylkP>



[KubeCon India 2024] #2 PaC(Policy as Code) Source

- ShortURL: <https://m.site.naver.com/1ylkv>



<https://github.com/SysNet4Admin>



<https://www.linkedin.com/in/hoonjo/>