KubeCon | CloudNativeCon

Europe 2019

# OpenAPI Specs

## Towards Native User Experience of CRDs

Stefan Schimanski – @the_sttts

# Agenda

- Intro to OpenAPI ~~specs~~ schemas
- CRD validation using OpenAPI
- Typical Kubernetes API patterns expressed in OpenAPI
- Towards a standard openapi-spec-gen to extract specs from Go types
- Expressivity and limits of OpenAPI

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          properties:
            command:
              type: string
            schedule:
              type: string
        status:
          type: object
          properties:
            phase:
              type: string
```

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        required: [“spec”]
        spec:
          type: object
          properties:
            command:
              type: string
              minLength: 1 # non-empty
            schedule:
              type: string
              anyOf:
              - pattern: “<ISO8601-regex>”
              - pattern: “<unix-timestamp>
          required: [“command”,”schedule”]
        status:
          type: object
          properties:
            phase:
              type: string
```

value validation

@the_sttts

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          properties:
            command:
              type: string
            schedule:
              type: string
        status:
          type: object
          properties:
            phase:
              type: string
```

pure structural validation

# OpenAPI v3 schemas

**Used in CRDs:** `spec.validation.openAPIV3Schema`

**Standard:** [github.com/OAI/OpenAPI-Specification/versions/3.0.0.md](github.com/OAI/OpenAPI-Specification/versions/3.0.0.md)

**Published by kube-apiserver as v2:** `/openapi/v2` `(beta in 1.15)`
**To be published as v3:** `/openapi/v3`

Used by `kubectl explain` and client-side validation.

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          properties:
            command:
              type: string
            schedule:
              type: string
        status:
          type: object
          properties:
            phase:
              type: string
```

complete
structural
validation

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          - properties:
              command:
                type: string
          anyOf:
          - properties:
              schedule:
                type: string
                pattern: <ISO-8601-regex>
          - properties:
              schedule:
                type: string
                pattern: <unix-timestamp>
        status:
          type: object
          properties:
            phase:
              type: string
```

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          - properties:
              command:
                type: string
          anyOf:
          - properties:
              schedule:
                type: string
                pattern: <ISO-8601-regex>
          - properties:
              schedule:
                type: string
                pattern: <unix-timestamp>
        status:
          type: object
          properties:
            phase:
              type: string
```

⚡

@the_sttts

```
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          - properties:
              command:
                type: string
              schedule:
                type: string
          anyOf:
          - properties:
              schedule:
                pattern: <ISO-8601-regex>
          - properties:
              schedule:
                pattern: <unix-timestamp>
        status:
          type: object
          properties:
            phase:
              type: string
```

```go
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```yaml
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          - properties:
              command:
                type: string
              schedule:
                type: string
          anyOf:
          - properties:
              schedule:
                pattern: <ISO-8601-regex>
          - properties:
              schedule:
                pattern: <unix-timestamp>
        status:
          type: object
          properties:
            phase:
              type: string
```

structural schema

@the_sttts

```
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec    Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          - properties:
              command:
                type: string
              schedule:
                type: string
          anyOf:
          - properties:
              schedule:
                pattern: <ISO-8601-regex>
          - properties:
              schedule:
                pattern: <unix-timestamp>
        status:
          type: object
          properties:
            phase:
              type: string
```

structural schema

@the_sttts

```
type Example struct {
    metav1.TypeMeta
    metav1.ObjectMeta
    Spec   Spec
    Status Status
}

type Spec struct {
    Schedule string
    Command string
}

type Status struct {
    Phase string
}
```

```
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata: examples.kubecon.io
spec:
  validation:
    openAPIV3Schema:
      type: object
      properties:
        spec:
          type: object
          - properties:
              command:
                type: string
              schedule:
                type: string
          anyOf:
          - properties:
              schedule:
                pattern: <ISO-8601-regex>
          - properties:
              schedule:
                pattern: <unix-timestamp>
        status:
          type: object
          properties:
            phase:
              type: string
```

structural schema

@the_sttts

# Kubernetes 1.15+

```
$ kubectl create -f non-structural-crd.yaml -o yaml
...
status:
    conditions:
    - message: '[
        spec.validation.openAPIV3Schema.type: Required value: must not be empty
        spec.validation.openAPIV3Schema.properties[metadata]: Forbidden:
          must not specify anything other than name and generateName,
          but metadata is implicitly specified
      ]'
      reason: Violations
      status: "True"
      type: NonStructuralSchema
      lastTransitionTime: "2019-05-17T19:41:30Z"
```

# The Future of CRDs: current KEPs

KEP Vanilla OpenAPI Subset: Structural Schema – beta in 1.15

**Theme:** Towards CRD GA

# The Future of CRDs: current KEPs

KEP Vanilla OpenAPI Subset: Structural Schema – beta in 1.15

KEP OpenAPI Publishing – beta in 1.15

KEP Conversion Webhooks – beta in 1.15

KEP Pruning – beta in 1.15

KEP Defaulting – alpha in 1.15

KEP Unions

WIP KEP: Unified Golang API Tags

**Theme:** Towards CRD GA

# The Future of CRDs: current KEPs

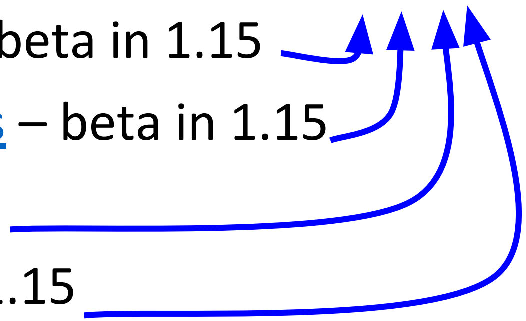
KEP Vanilla OpenAPI Subset: Structural Schema – beta in 1.15

KEP OpenAPI Publishing – beta in 1.15

KEP Conversion Webhooks – beta in 1.15

KEP Pruning – beta in 1.15

KEP Defaulting – alpha in 1.15



all new features require structural schema

KEP Unions

WIP KEP: Unified Golang API Tags

**Theme:** Towards CRD GA

# OpenAPI consumers

OpenAPI publishing →

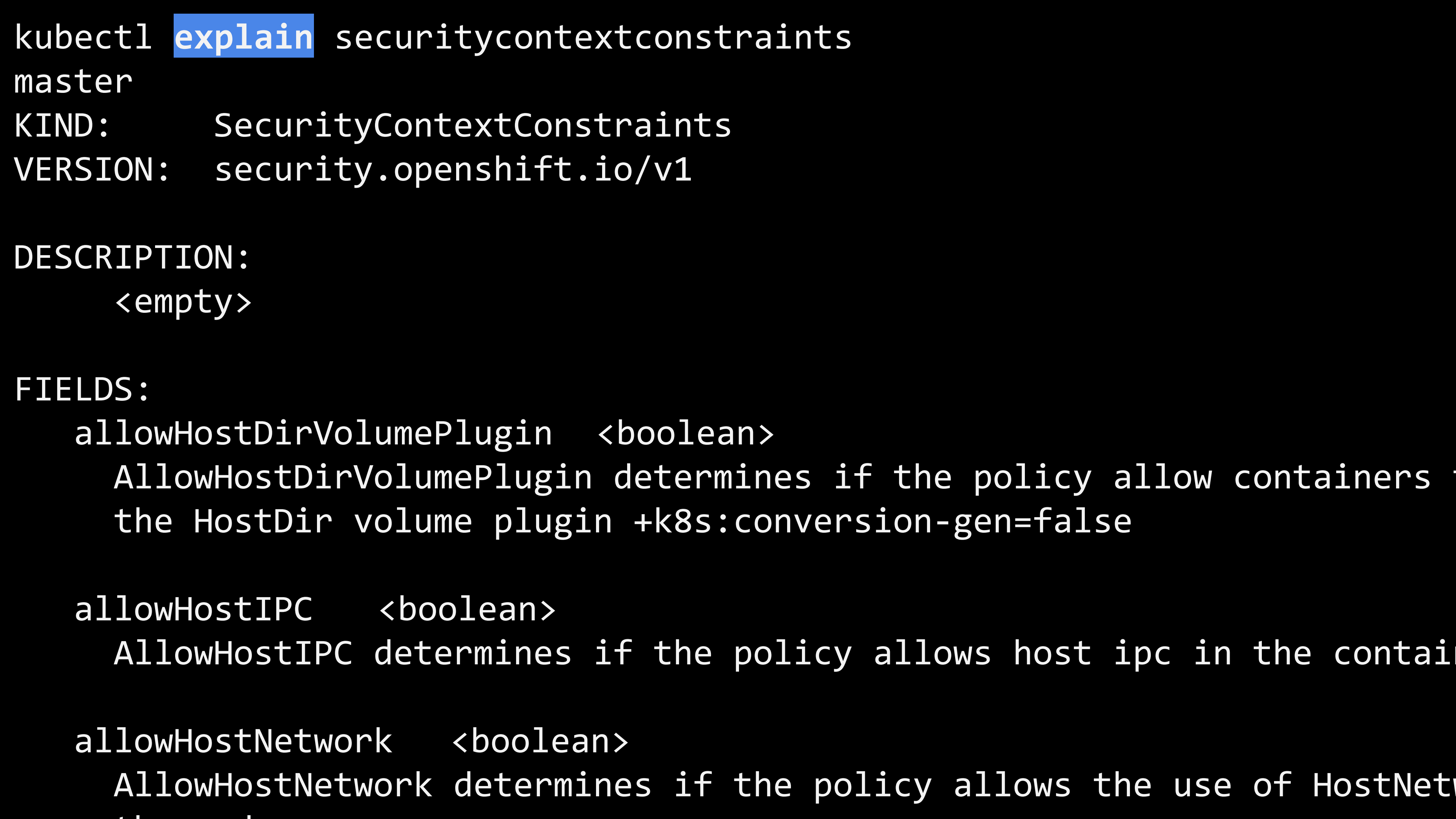
server side apply

CRDs only:

- server-side validation
- Pruning
- Defaulting
- Protobuf[1]
- server-side read-only fields[1]

- client-side validation
- kubectl explain
- client generators
- doc generator
- kube-aggregator
- IDEs like IntelliJ for input completion

1) possibly in the future



```
kubectl explain securitycontextconstraints
master
KIND:     SecurityContextConstraints
VERSION:  security.openshift.io/v1

DESCRIPTION:
     <empty>

FIELDS:
   allowHostDirVolumePlugin  <boolean>
     AllowHostDirVolumePlugin determines if the policy allow containers
     the HostDir volume plugin +k8s:conversion-gen=false

   allowHostIPC   <boolean>
     AllowHostIPC determines if the policy allows host ipc in the contai

   allowHostNetwork   <boolean>
     AllowHostNetwork determines if the policy allows the use of HostNetw
```

# OpenAPI Publishing

/openapi/v2

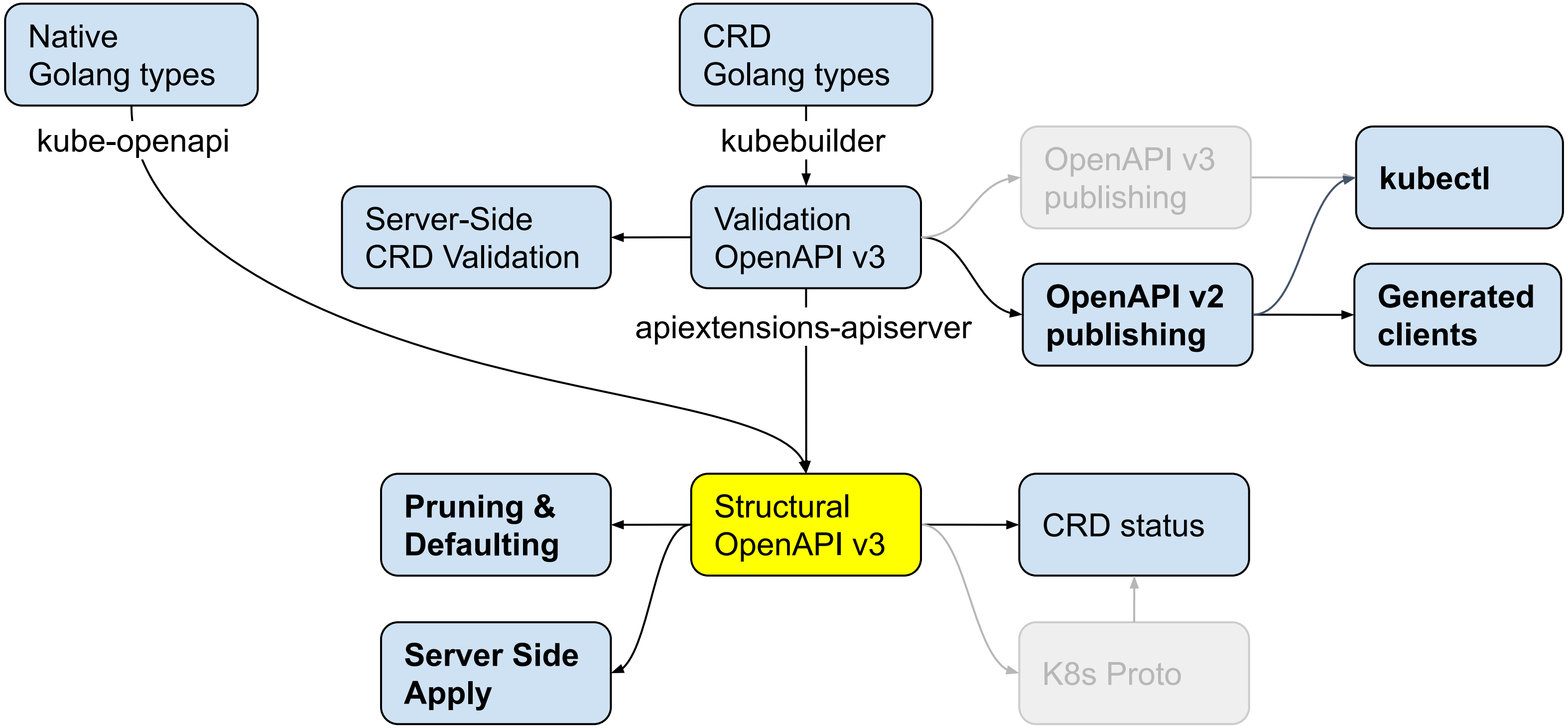
openAPIV3Schema

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
      type: integer
- properties:
    bar:
      type: string
      minLength: 1
      maxLength: 0
```

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
```

OpenAPI v2

# OpenAPI in Kubernetes



# OpenAPI Publishing

/openapi/v2

openAPIV3Schema

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
      type: integer
- properties:
    bar:
      type: string
      minLength: 1
      maxLength: 0
```

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
```

OpenAPI v2

# OpenAPI Publishing

/openapi/v2

openAPIV3Schema

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
      type: integer
- properties:
    bar:
      type: string
      minLength: 1
      maxLength: 0
```

OpenAPI v2

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
    type: undefined
```

no anyOf in v2

# Problematic OpenAPI v3

non-structural schema

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
      type: integer
- properties:
    bar:
      type: string
      minLength: 1
      maxLength: 0
```

mix of types and logic

polymorphic types

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
    type: undefined
```

OpenAPI v2

no anyOf in v2

# Problematic OpenAPI v3

non-structural schema

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
      type: integer
- properties:
    bar:
      type: string
      minLength: 1
      maxLength: 0
```

~~mix of types and logic~~

~~polymorphic types~~

OpenAPI v2

```
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
    type: undefined
```

# OpenAPI v2 at /openapi/v2

~~non~~-structural schema

```yaml
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
    type: integer
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
- properties:
    bar:
      minLength: 1
      maxLength: 0
```

```yaml
type: object
properties:
  foo:
    type: string
  bar:
    minimum: 42
    type: integer
```

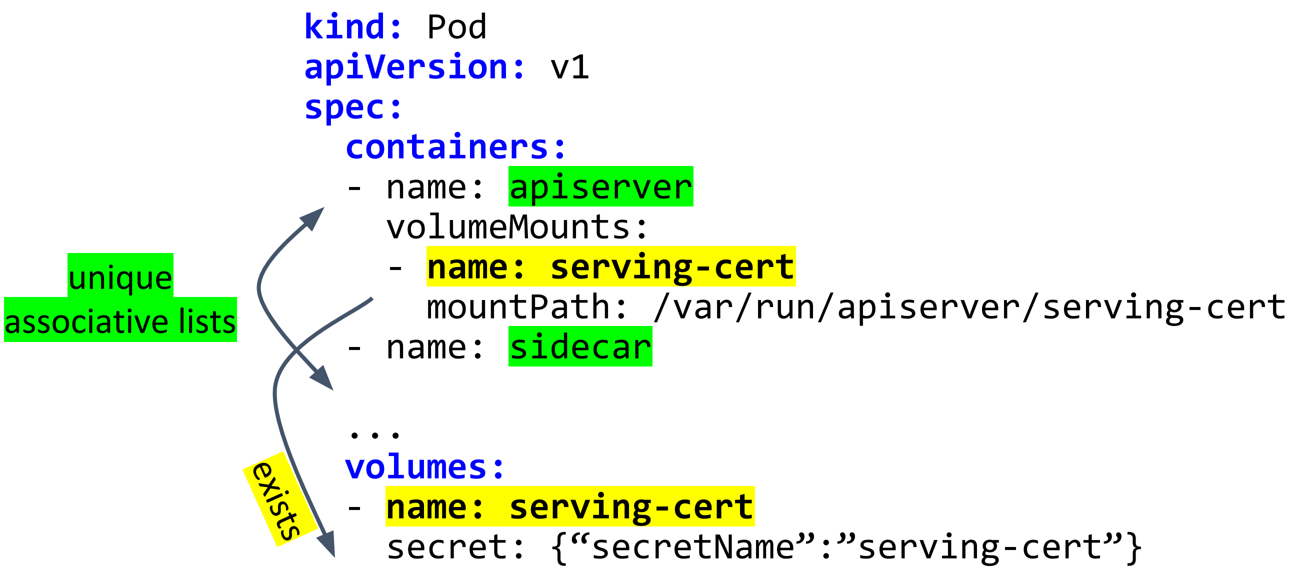
complete structure

# Limits of Expressivity

```
kind: Pod
apiVersion: v1
spec:
  containers:
  - name: apiserver
    volumeMounts:
    - name: serving-cert
      mountPath: /var/run/apiserver/serving-cert
  - name: sidecar

  ...
  volumes:
  - name: serving-cert
    secret: {“secretName”:”serving-cert”}
```

# Limits of Expressivity



unique associative lists

exists

```
kind: Pod
apiVersion: v1
spec:
  containers:
  - name: apiserver
    volumeMounts:
    - name: serving-cert
      mountPath: /var/run/apiserver/serving-cert
  - name: sidecar

  ...
  volumes:
  - name: serving-cert
    secret: {“secretName”:”serving-cert”}
```

# OpenAPI producers

**kube-openapi** — native type schemas compiled into API servers

**controller-tools** — CRD validation schemas

- **controller-gen** — kubebuilder's code-generation tool
- **crd-schema-gen** — work-in-progress non-opinionated tool

**manually written** — CRD validation schemas

# {controller,crd-schema}-gen

- generator for CRD OpenAPIV3Schemas
- github.com/kubernetes-sigs/controller-tools/cmd + PR 183

```
// +optional
// +nullable
// +kubebuilder:validation:pattern=<ISO8601-regex>
// + ...
```

**Work in progress KEP** for a unified tag / marker language

prototype
PR #183

```
$ cd example-project
$ ls manifests/*-crd.yaml
example-crd.yaml
$ crd-schema-gen
    --api-packages ./pkg/apis/...
    --manifest-dir ./manifests
Found 1 CRD manifests.
Updating schema for Example in example.kubecon.io at spec.validation.oper
```

# Pruning

**preserveUnknownFields:** false

possible through structural schemas

# Pruning with a structural schema

```
kind: Example
apiVersion: examples.kubecon.io/v1
metadata:
  name: hello
  foo: bar
spec:
  command: echo ‘Hello world!’
  schedule: 1558125753
  privileged: true
status:
  phase: Running
  conditions:
  - message: Executing
    type: Terminate
    status: False
```

pruning

```
type: object
properties:
  spec:
    type: object
    properties:
      command:
        type: string
      schedule:
        type: string
  status:
    type: object
    properties:
      phase:
        type: string
```

complete structural schema

# Pruning with a structural schema

KubeCon CloudNativeCon Europe 2019

```
kind: Example
apiVersion: examples.kubecon.io/v1
metadata:
  name: hello
  foo: bar
spec:
  command: echo ‘Hello world!’
  schedule: 1558125753
  privileged: true
status:
  phase: Running
  conditions:
  - message: Executing
    type: Terminate
    status: False
```

implicitly specified

pruning

```
kind: Example
apiVersion: examples.kubecon.io/
spec:
  command: echo ‘Hello world!’
  schedule: 1558125753
status:
  phase: Running
```

```
type: object
properties:
  spec:
    type: object
    properties:
      command:
        type: string
      schedule:
        type: string
  status:
    type: object
    properties:
      phase:
        type: string
```

complete structural schema

@the_sttts

# Controlling Pruning

```
kind: CustomResourceDefinition
spec:
  preserveUnknownFields: false

  validation:
    openAPIV3Schema:
      properties:

        embeddedObject:
          type: object
          x-kubernetes-embedded-resource: true
          x-kubernetes-preserve-unknown-fields: true

        rawJSON:
          x-kubernetes-preserve-unknown-fields: true

        intOrString:
          x-kubernetes-int-or-string: true
```

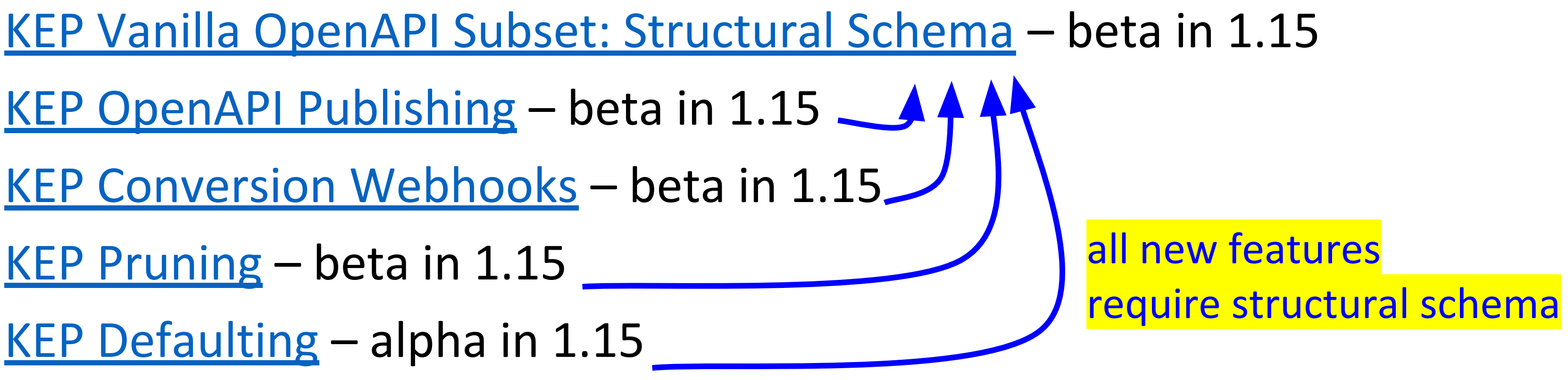
defaults to **true in v1beta1**
**must be false in v1** on creation

runtime.RawExtension

interface{}

intstr.IntOrString

# The Future of CRDs



KEP Vanilla OpenAPI Subset: Structural Schema – beta in 1.15

KEP OpenAPI Publishing – beta in 1.15

KEP Conversion Webhooks – beta in 1.15

KEP Pruning – beta in 1.15

KEP Defaulting – alpha in 1.15

all new features
require structural schema

KEP Unions

WIP KEP: Unified Golang API Tags

**Theme:** Towards CRD GA in 1.16/1.17

# Backup

# Kubernetes patterns: unions

```
type VolumeSource struct {
    HostPath *HostPath
    EmptyDir *EmptyDir
    Secret *SecretVolumeSource
    ...
}
```

```
properties:
    hostPath: …
    emptyDir: …
oneOf:
- required: [“hostPath”]
- required: [“emptyDir”]
```

# Kubernetes patterns: unions

```
// +union
type VolumeSource struct {
    // +discriminator
    Type string
    HostPath *HostPath
    EmptyDir *EmptyDir
    ...
}
```

```
x-kubernetes-unions:
- discriminator: type
  fieldsDiscriminatedBy:
     hostPath: HostPath
     emptyDir: EmptyDir
properties:
     type:
          type: string
     hostPath: …
     emptyDir: …
oneOf:
- required: [“hostPath”]
- required: [“emptyDir”]
```

# Defaulting

```
properties:
  foo:
    type: string
  bar:
    type: integer
    minimum: 42
    default: 100
  slice:
    type: array
    nullable: true
    default: [“a”,”b”]
    items:
      type: string
  logic:
    type: string
    anyOf:
    - default: “nope”
```

```
{}                           => {“bar”:100, “slice”:[“a”,”b”]}
{“bar”:2, “slice”:[]}        => {“bar”:2, “slice”:[]}
{“bar”:0, “slice”:null}      => {“bar”:0, “slice”:null}
```

# Non-structural vs. structural OpenAPI

```
properties:
  foo:
    type: string
  bar:
    type: undefined
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
    bar:
      type: string
- properties:
    bar:
      type: integer
      minimum: 1
      maximum: 0
```

~~mix of types and logic~~

~~polymorphic types~~

```
type: object
properties:
  foo:
    type: string
  bar:
    type: string
    minimum: 42
anyOf:
- properties:
    foo:
      pattern: abc
- properties:
    bar:
      minimum: 1
      maximum: 0
```

structural schema

value validation & logic