dynatrace

Scaling Observability

Harnessing the Power of Kubernetes Operators

chrismuellner

christoph-muellner-at

Christoph Müllner

Sr. Software Engineer & Product Owner at Dynatrace

Agenda

- Background
- Operator
- Webhook
- CSI Driver

dynatrace

Cloud done right.

OneAgent

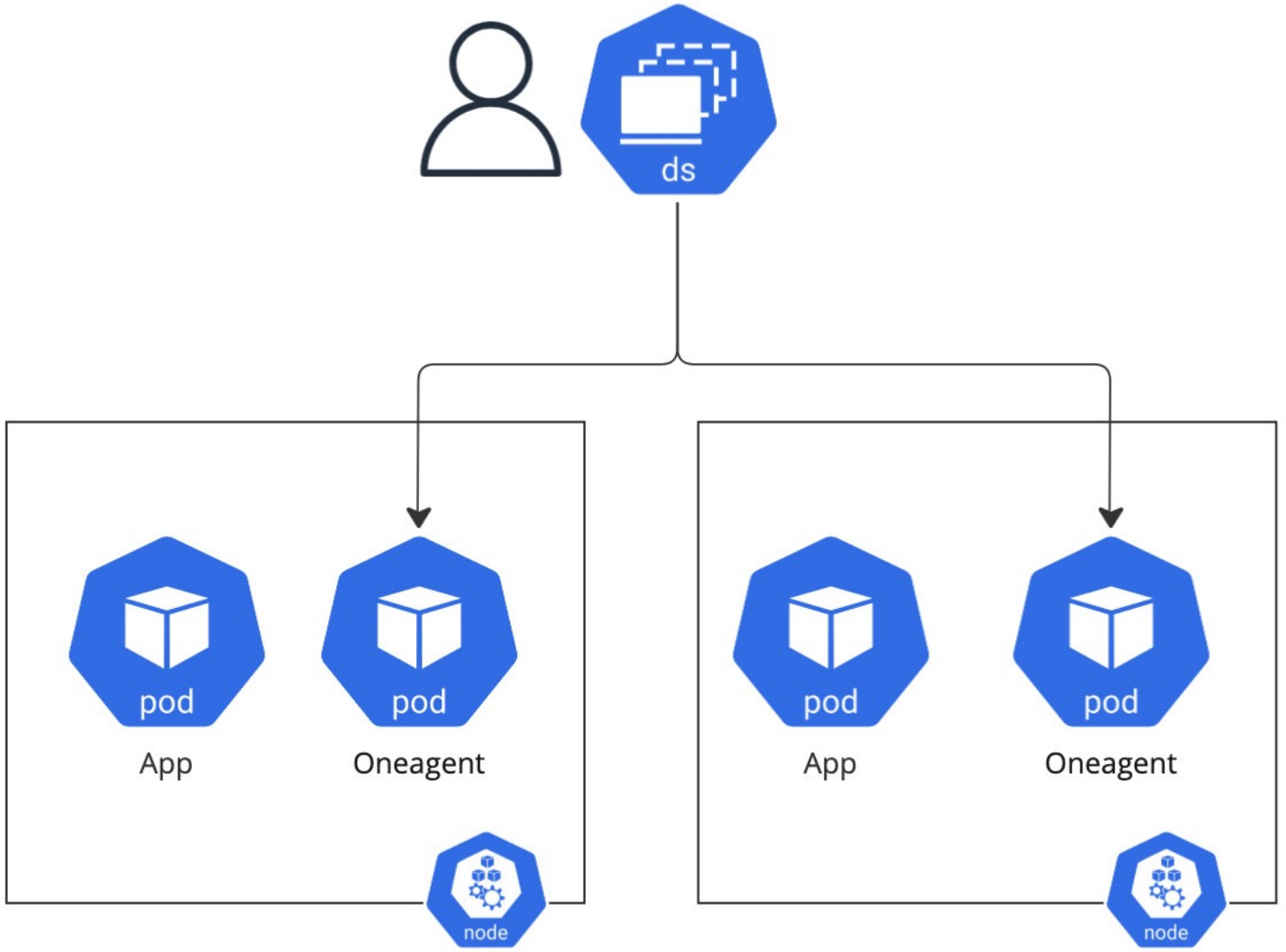
Concept

- Inject applications without manual configuration
- Automatically attach necessary metadata/binaries
  - LD_PRELOAD environment variable
  - binaries via mount points

- *Needs to be present before process startup!*

Deploy OneAgent

- Put container in pod
- Schedule pod on every node via daemonset

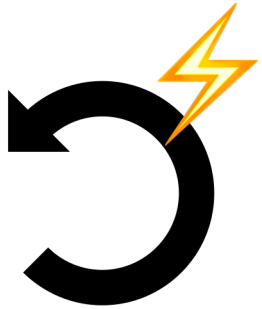


Problems

- Unmanaged manifest

```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    app.kubernetes.io/component: fullstack
    app.kubernetes.io/name: oneagent
    app.kubernetes.io/version: 1.277.0.20230914-094321
  name: oneagent
  namespace: dynatrace
spec:
  revisionHistoryLimit: 10
  selector:
    matchLabels:
      app.kubernetes.io/name: oneagent
  template:
    metadata:
      annotations:
        container.apparmor.security.beta.kubernetes.io/dynatrace-oneagent: unconfined
      labels:
        app.kubernetes.io/component: fullstack
        app.kubernetes.io/name: oneagent
        app.kubernetes.io/version: 1.277.0.20230914-094321
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
            - matchExpressions:
              - key: kubernetes.io/arch
                operator: In
                values:
                - amd64
```

- Manual updates



How to best deploy it on k8s?

Helm

- simple deployment
- single rollout
- basic validation

Operator

- lifecycle management
- fine-grained validation

- *can be used for operator deployment!*

Operator

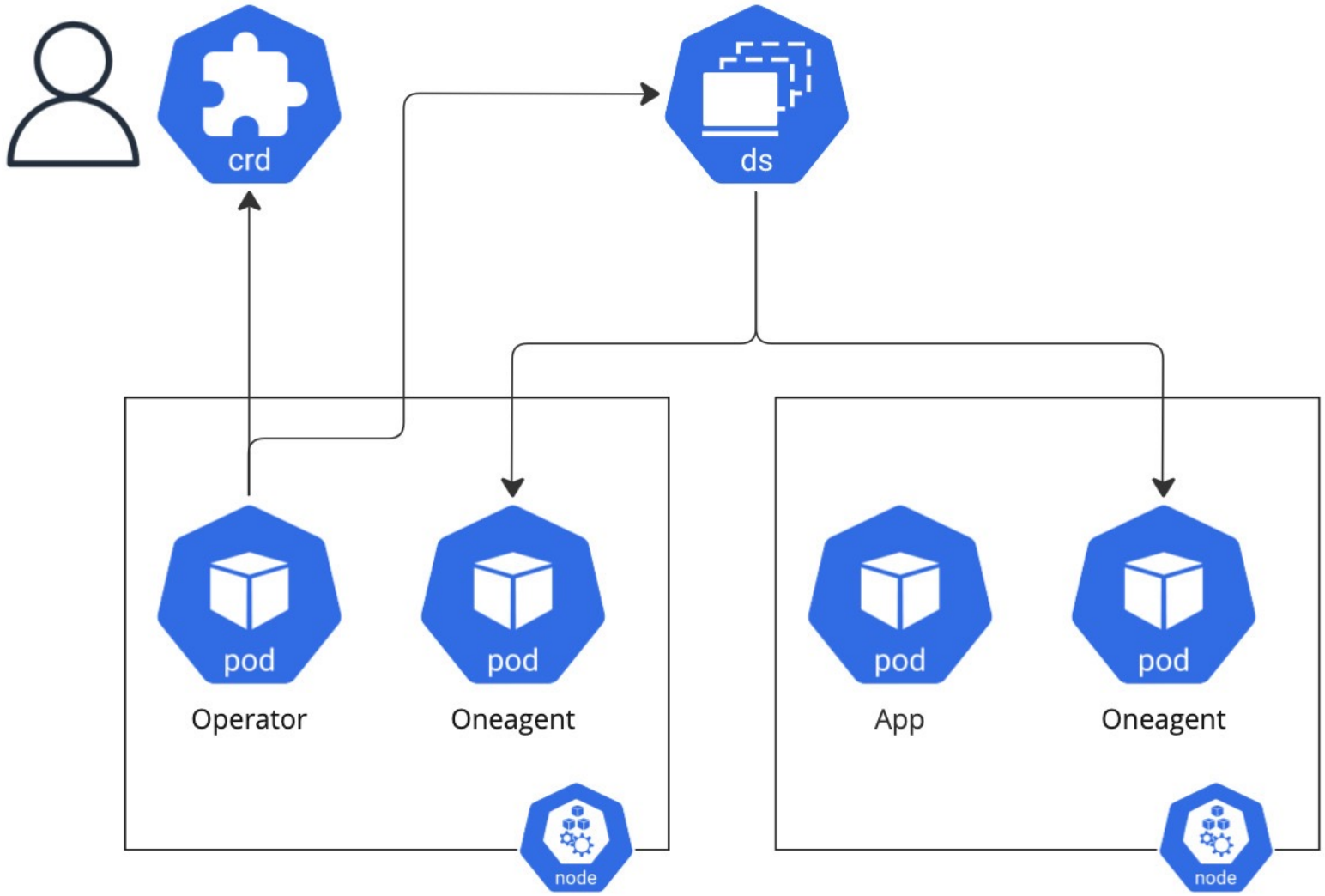
Concept

- Configure via Custom Resource
- Reconcile resources

```yaml
apiVersion: dynatrace.com/v1beta1
kind: DynaKube
metadata:
  name: dynakube
spec:
  apiUrl: TENANT.dynatracelabs.com/api

  oneAgent:
    cloudNativeFullStack: {}
```

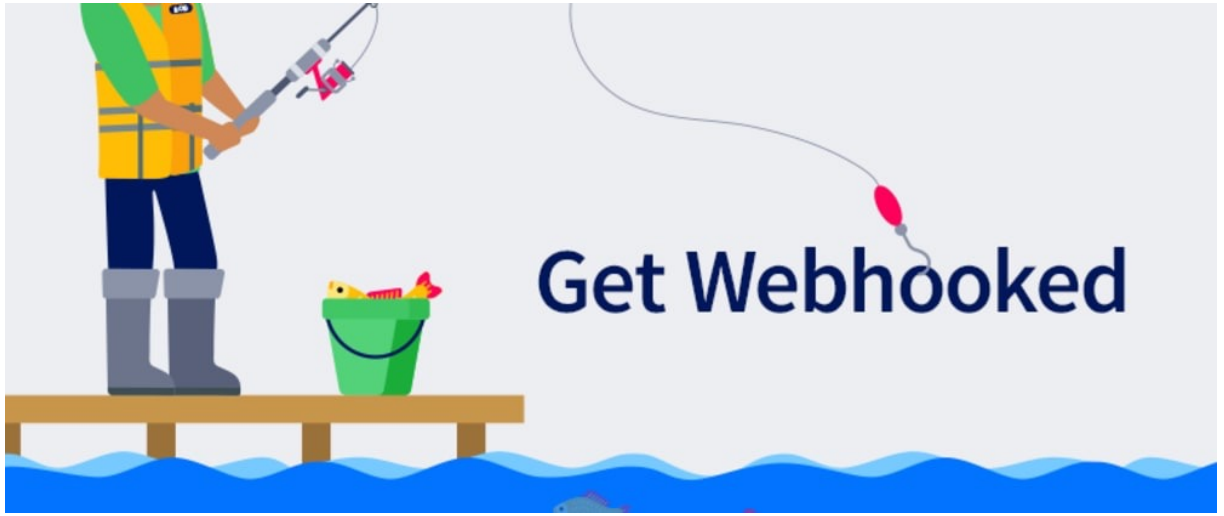
Operator deployment



Problems

- Container runtime injection
  - hidden from Cluster Operators

- Race Condition
  - container needs to be ready on node to inject pods
- No Multi-tenancy
  - single Oneagent per node



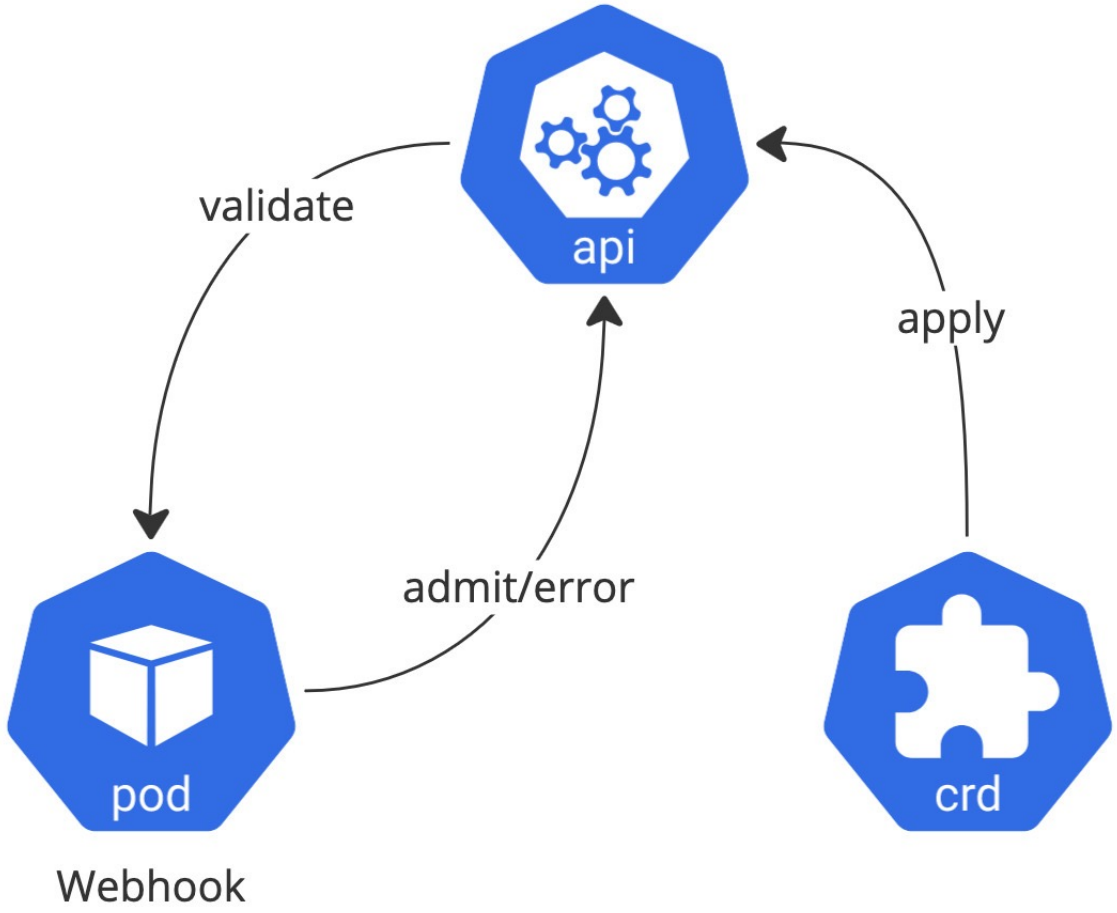
Webhook

Concept

- Event-based
- Different types
  - Validating
  - Mutating
  - Conversion

Validation webhook

- Validate configuration
  - Early feedback
  - Clear error message



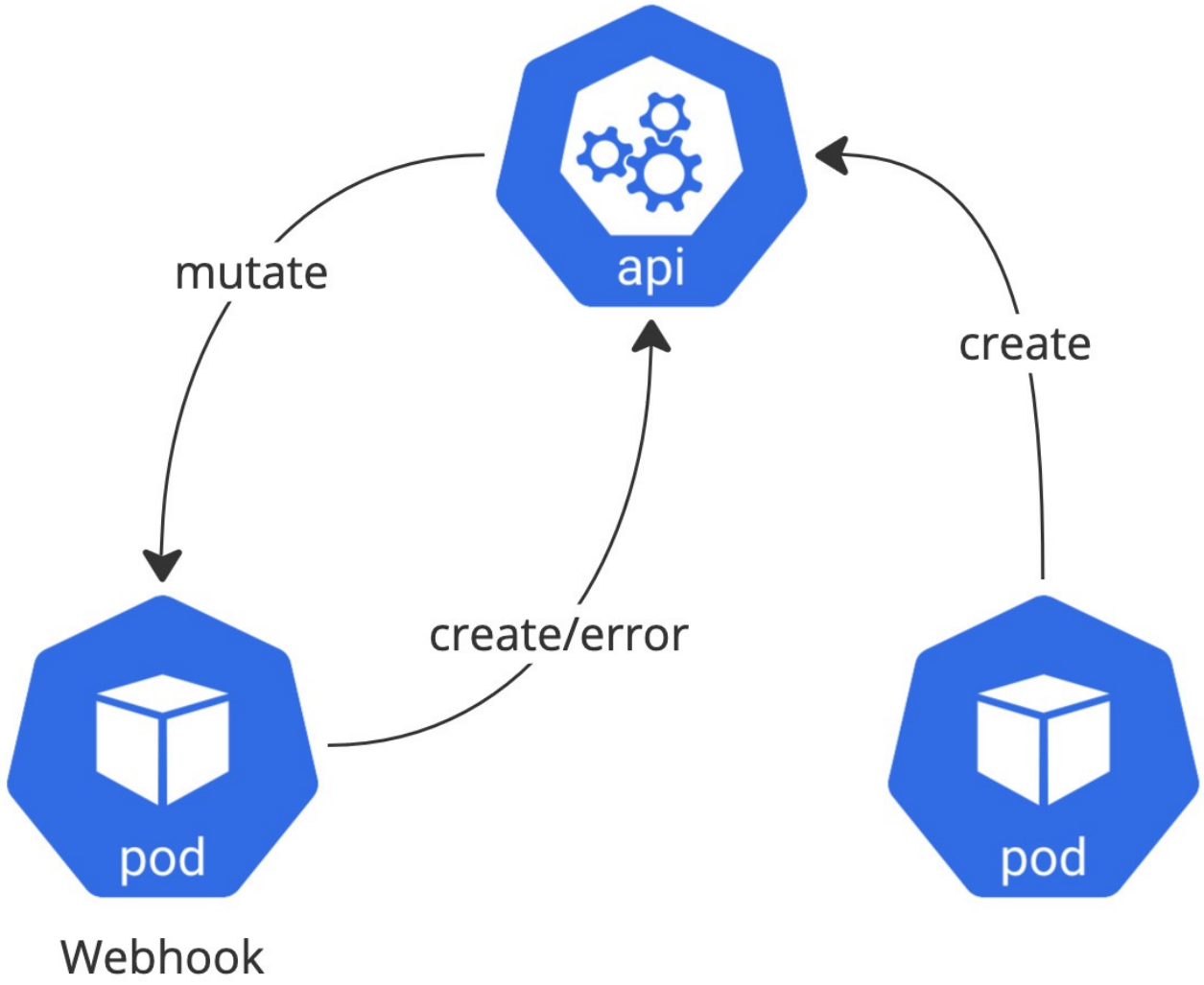
Validation webhook

```yaml
apiVersion: dynatrace.com/v1beta1
kind: DynaKube
metadata:
  name: invalid-dynakube
spec:
  apiUrl: ""
```

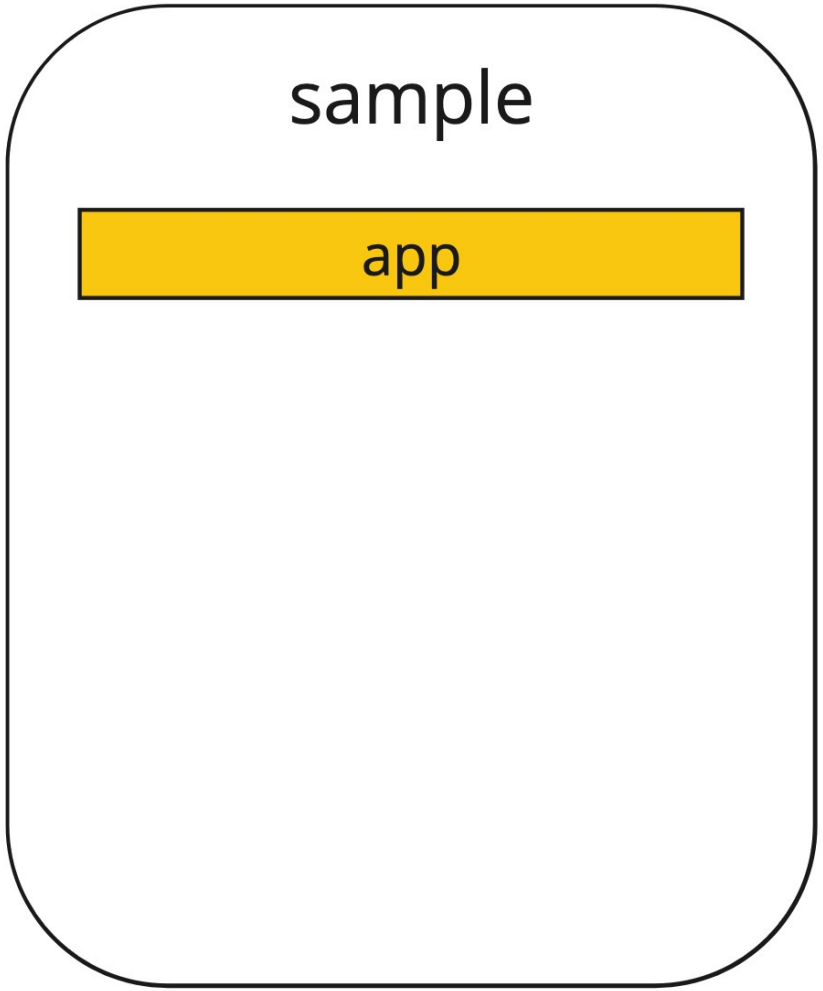
```
Error from server (Forbidden): error when creating "STDIN": admission webhook "webhook.dynatrace.com" denied the
request:
2 error(s) found in the Dynakube
 1. The DynaKube's specification is missing the API URL or still has the example value set.
 Make sure you correctly specify the URL in your custom resource.
 2. The DynaKube's specification has an invalid API URL value set.
 Make sure you correctly specify the URL in your custom resource (including the /api postfix).
```

Mutate pods

- intercept create/update/... events
- mutate/error pod

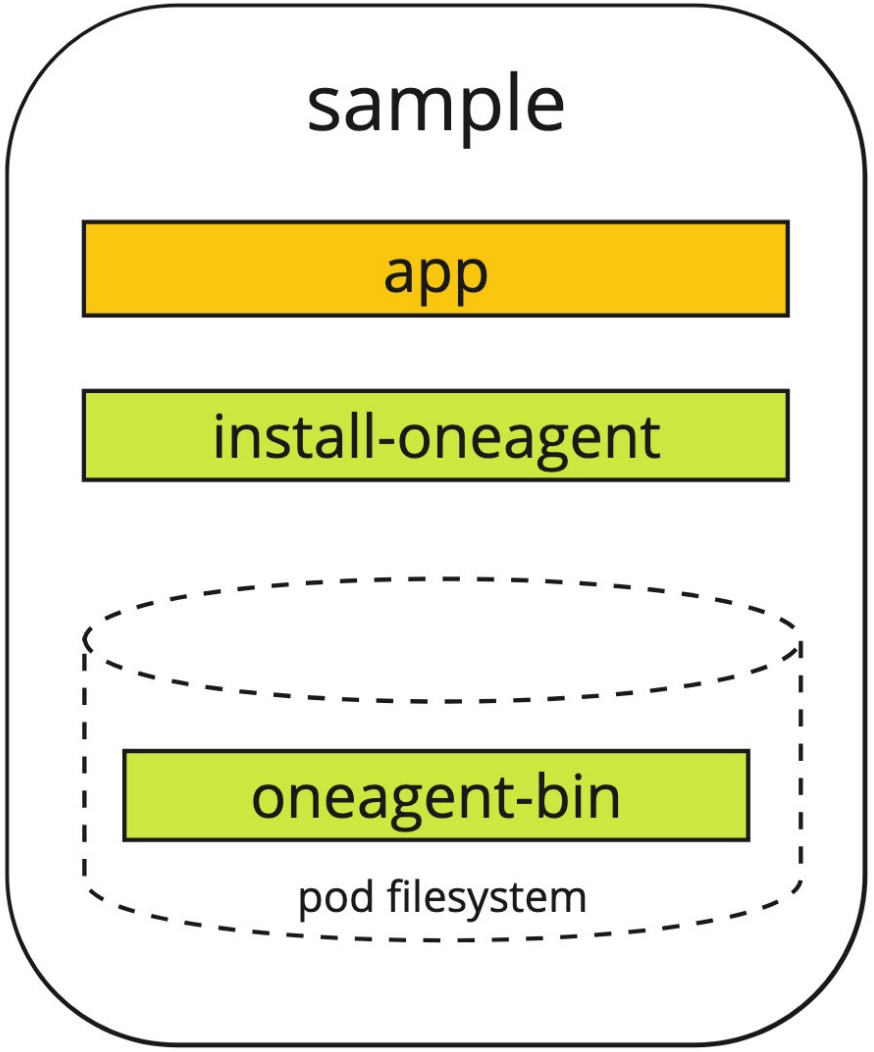


Mutate pods




```yaml
apiVersion: v1
kind: Pod
metadata:
  name: sample
spec:
  containers:
  - image: fancyapp
    name: app
    ports:
    - containerPort: 80
      protocol: TCP
```

Mutate pods




```yaml
apiVersion: v1
kind: Pod
metadata:
 name: sample
spec:
  containers:
  - name: app
    image: fancyapp
    ports:
    - containerPort: 80
    env:
    - name: LD_PRELOAD
      value: /opt/dynatrace/oneagent-paas/agent/lib64/liboneagentproc.so
    volumeMounts:
    - mountPath: /opt/dynatrace/oneagent-paas
      name: oneagent-bin
initContainers:
    image: docker.io/dynatrace/dynatrace-operator
    name: install-oneagent
    volumeMounts:
    - mountPath: /mnt/bin
      name: oneagent-bin
volumes:
  - emptyDir: {}
    name: oneagent-bin
```

Configuration

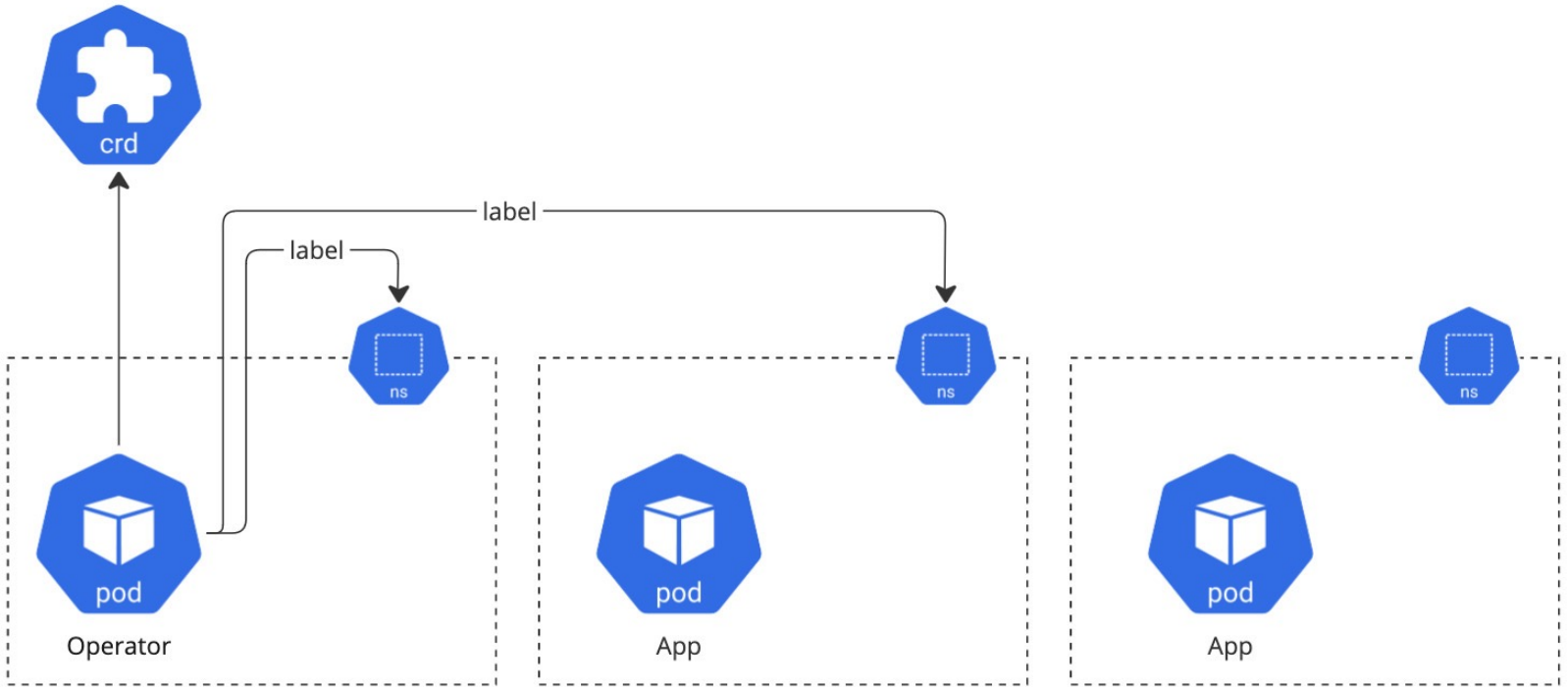
- cluster-wide by default
  - exceptions apply

- namespace selector
  - *manually label every namespace?*

```yaml
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  name: dynatrace-webhook
webhooks:
  - name: webhook.pod.dynatrace.com
...
    namespaceSelector:
      matchExpressions:
        - key: dynakube.internal.dynatrace.com/instance
          operator: Exists
```

Configuration

- namespace selector
  - webhook matches no namespace by default
  - namespace label managed by Operator according to config



Fun with other webhooks

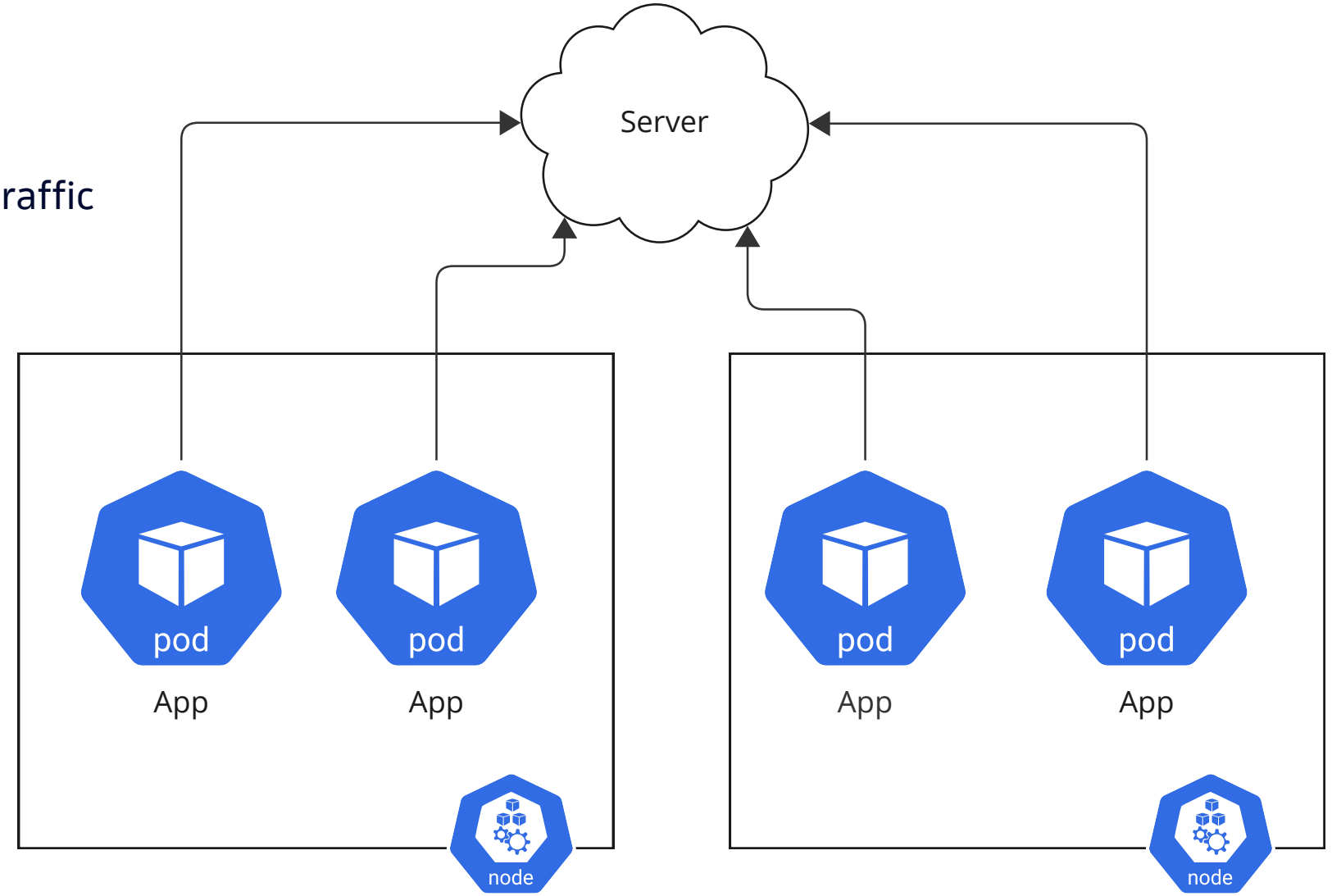
- alphabetical order
  - unknown by webhooks
- reinvocation policy
  - reinvoced if pod is modified by other webhook
  - annotations to optimise reinvoced requests

Resilience

- Webhook
  - topology spread constraints
  - failure policy & timeout
- Init container
  - custom failure policy

Problems

- Download per pod
  - Increased storage & network traffic
  - Increased startup time



CSI Driver

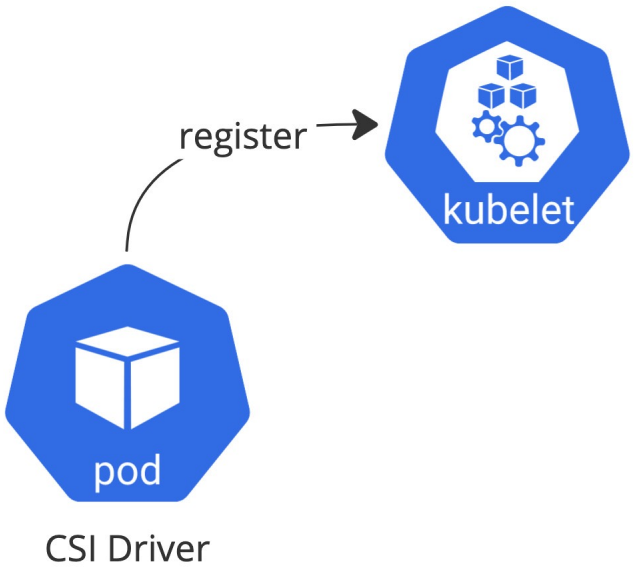
Concept

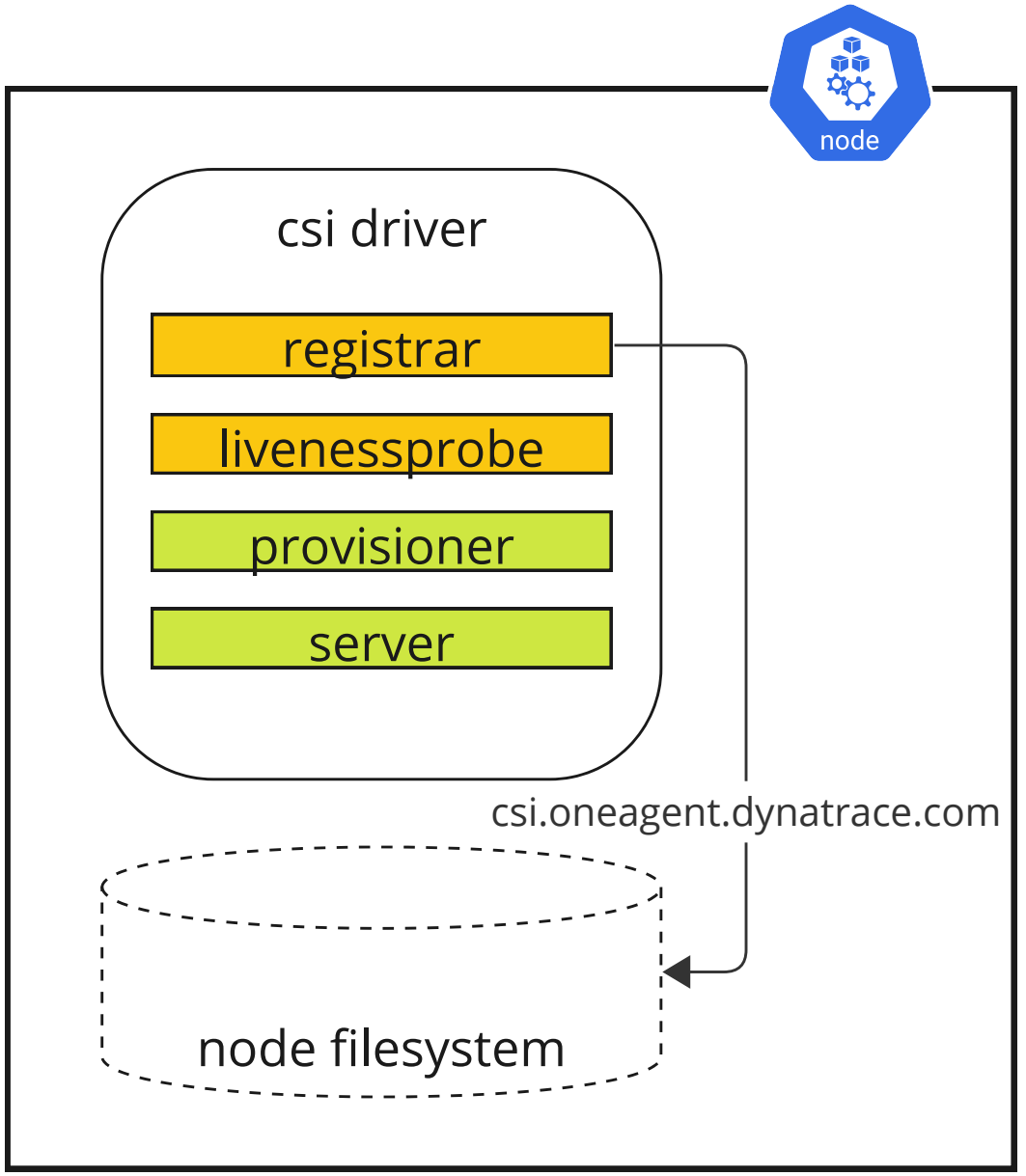
- Container Storage Interface
- CSI object to register

```yaml
apiVersion: storage.k8s.io/v1
kind: CSIDriver
metadata:
 name: csi.oneagent.dynatrace.com
spec:
  attachRequired: false
  podInfoOnMount: true
  volumeLifecycleModes:
    - Ephemeral
```

Concept

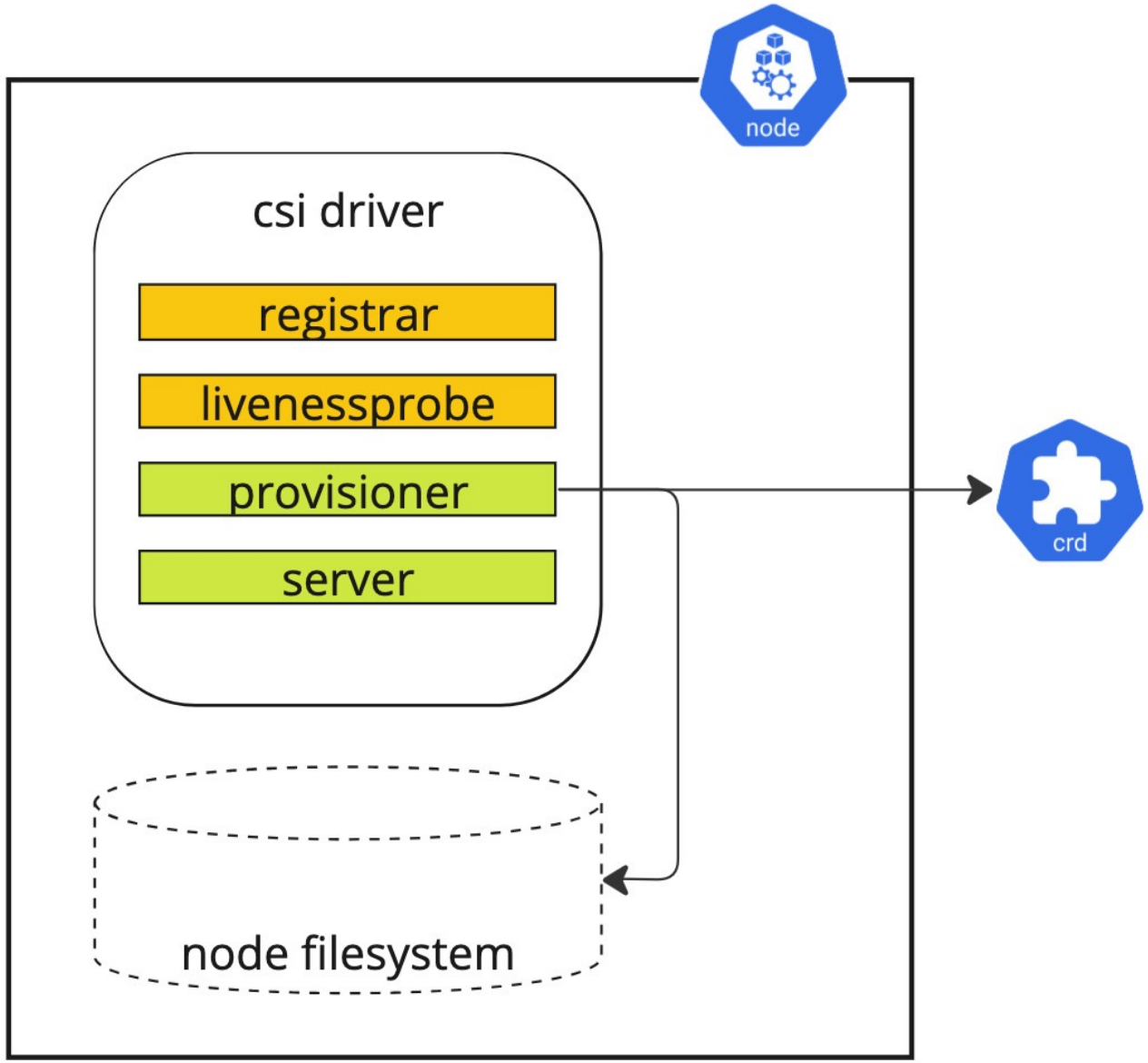
- CSI sidecars
  - registrar
  - liveness probe



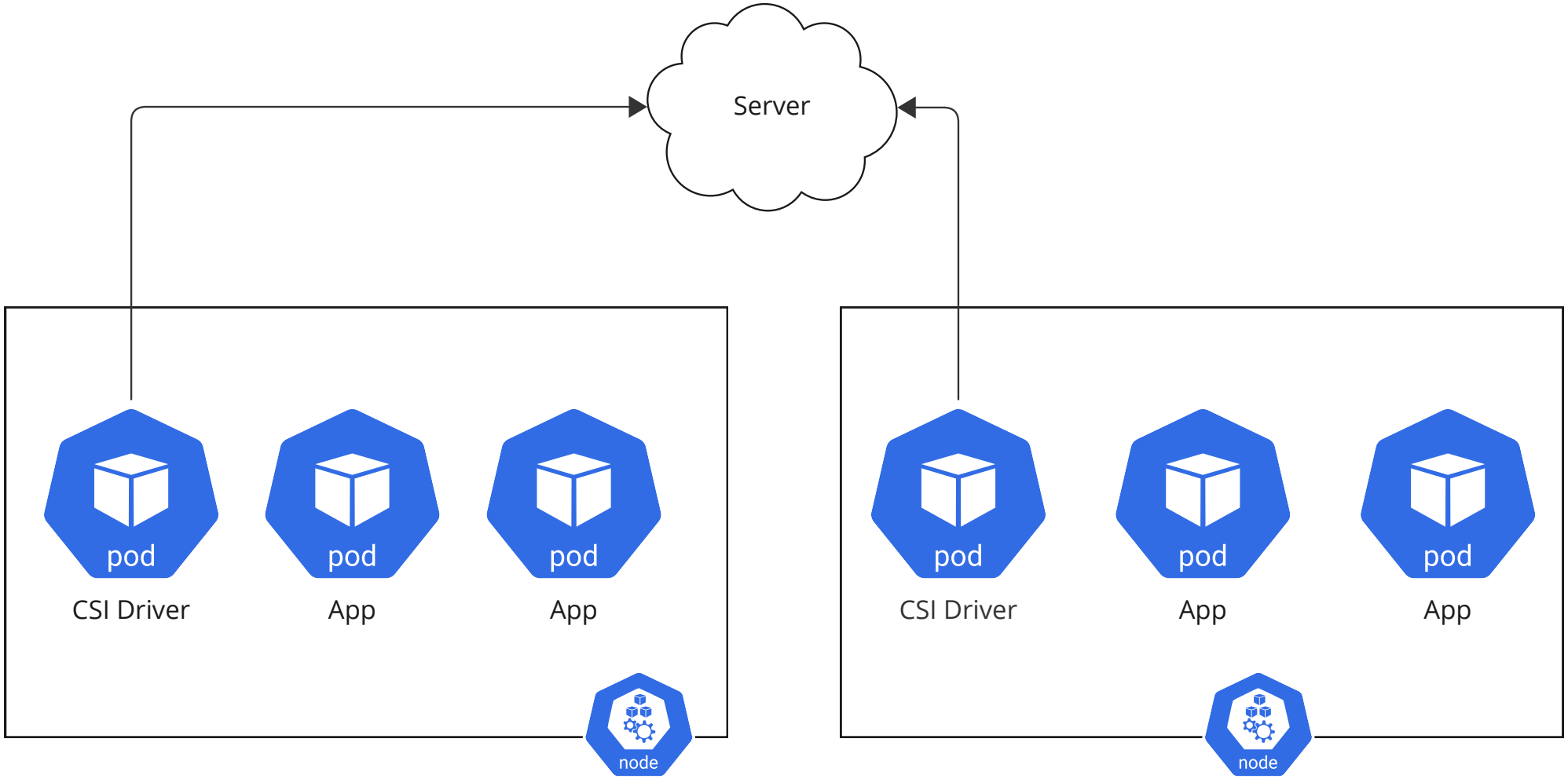


Binaries cached on node

- Watch Custom Resources
- Download required agent versions

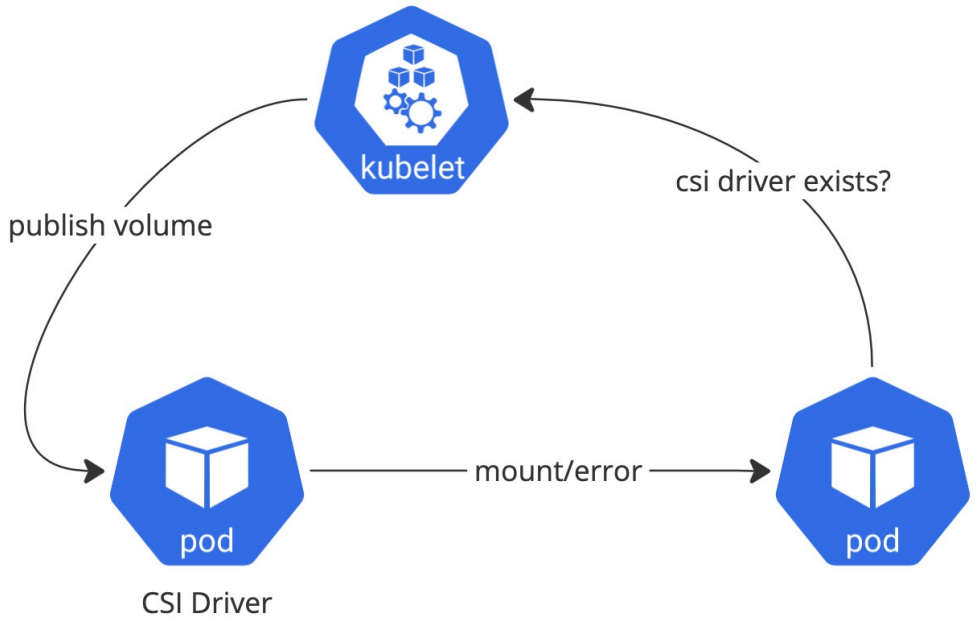


Binaries cached on node



Custom mount logic

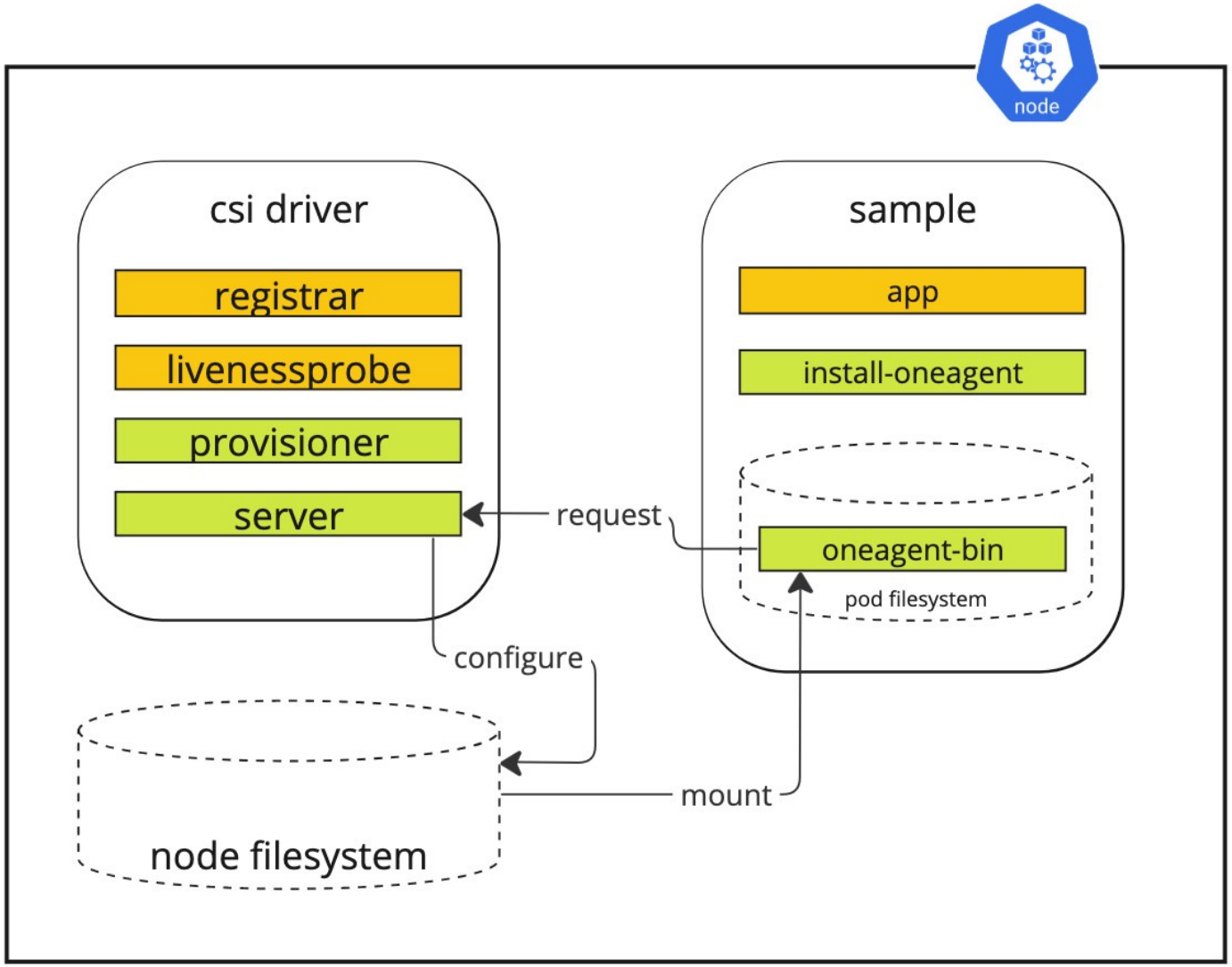
- Volume handled by CSI driver




```yaml
apiVersion: v1
kind: Pod
metadata:
 name: sample
spec:
  containers:
  - name: app
    image: fancyimage
    ports:
    - containerPort: 80
    env:
    - name: LD_PRELOAD
      value: /opt/dynatrace/oneagent-paas/agent/lib64/liboneagentproc.so
    volumeMounts:
    - mountPath: /opt/dynatrace/oneagent-paas
      name: oneagent-bin
initContainers:
    image: docker.io/dynatrace/dynatrace-operator:snapshot
    name: install-oneagent
    volumeMounts:
    - mountPath: /mnt/bin
      name: oneagent-bin
volumes:
  - csi:
      driver: csi.oneagent.dynatrace.com
      readOnly: false
      volumeAttributes:
        dynakube: dynakube
        mode: app
    name: oneagent-bin
```

Custom mount logic

- Mount correct agent version
  - binaries linked via overlayFS
  - configuration adapted per pod



Resilience

- Split containers
  - independantly failing containers
  - server can always handle mount requests
- Custom timeout
  - count failed mount attempts
  - mount empty volume

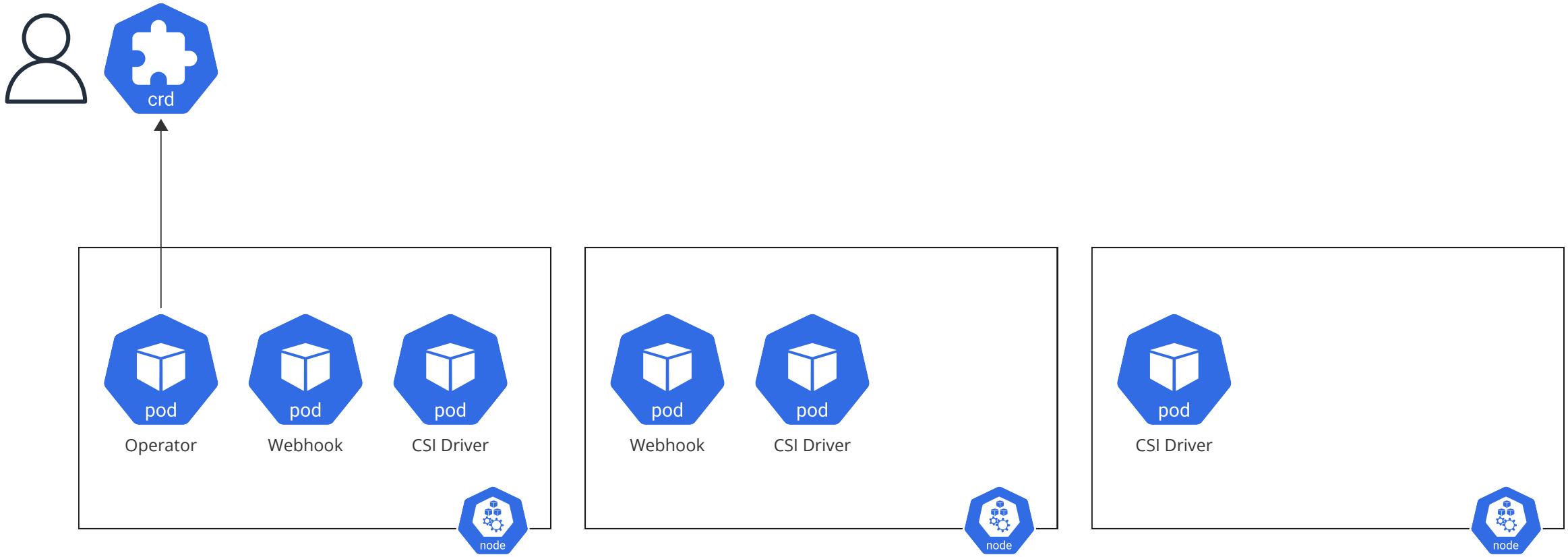
Problems

- requires privileged container
- Security Context Constraints in Openshift
  - Openshift <4.13 does not allow CSI volumes by default

- Need to garbage collect old agents on node filesystem

OPENSHIFT

Overview


crd
pod
Operator
pod
Webhook
pod
CSI Driver
node
pod
Webhook
pod
CSI Driver
node
pod
CSI Driver
node

Thanks!

Scaling Observability