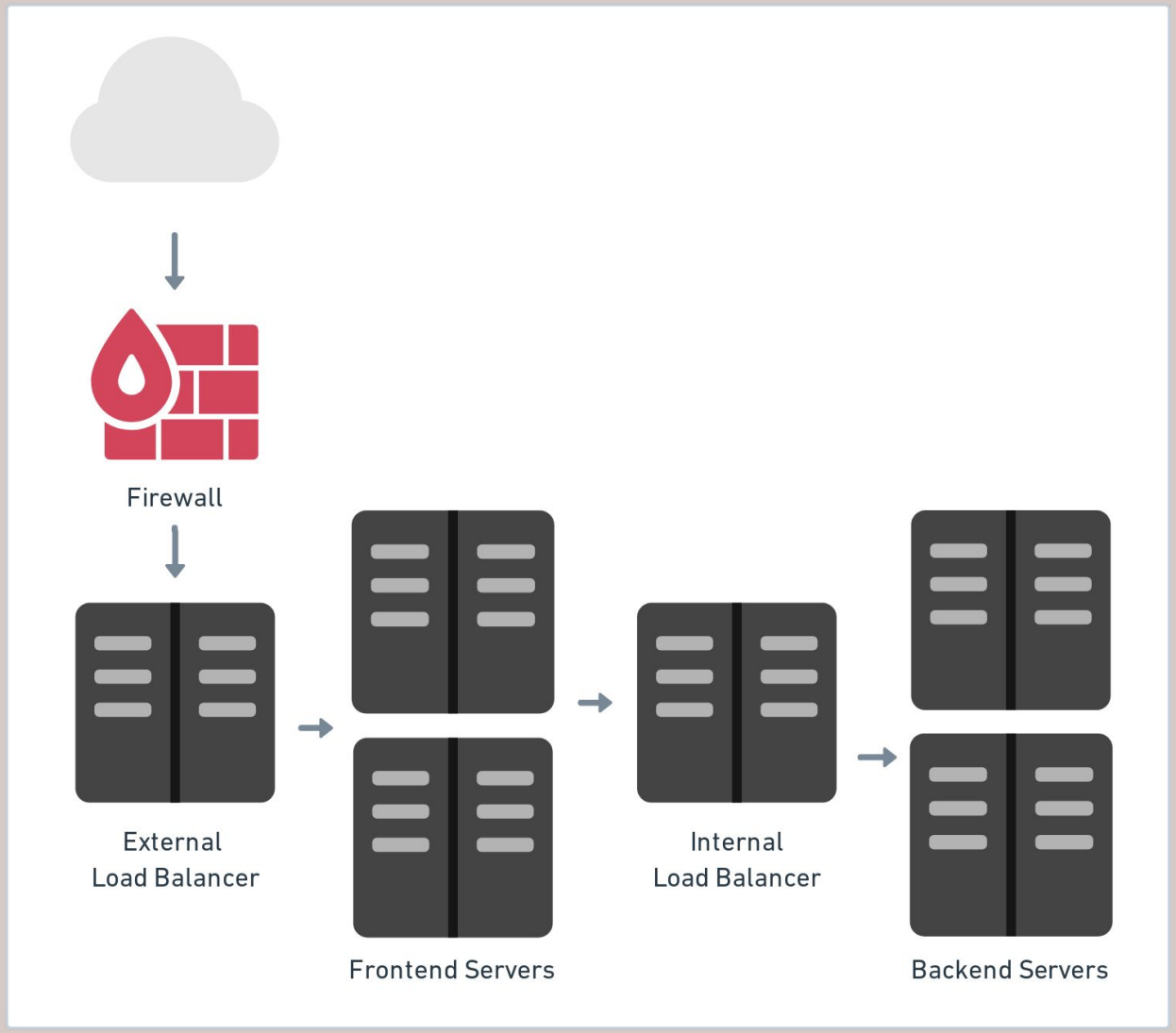

KubeCon
CloudNativeCon
Europe 2023
TiKV

Container is the new VM:
The paradigm change no one explained to you

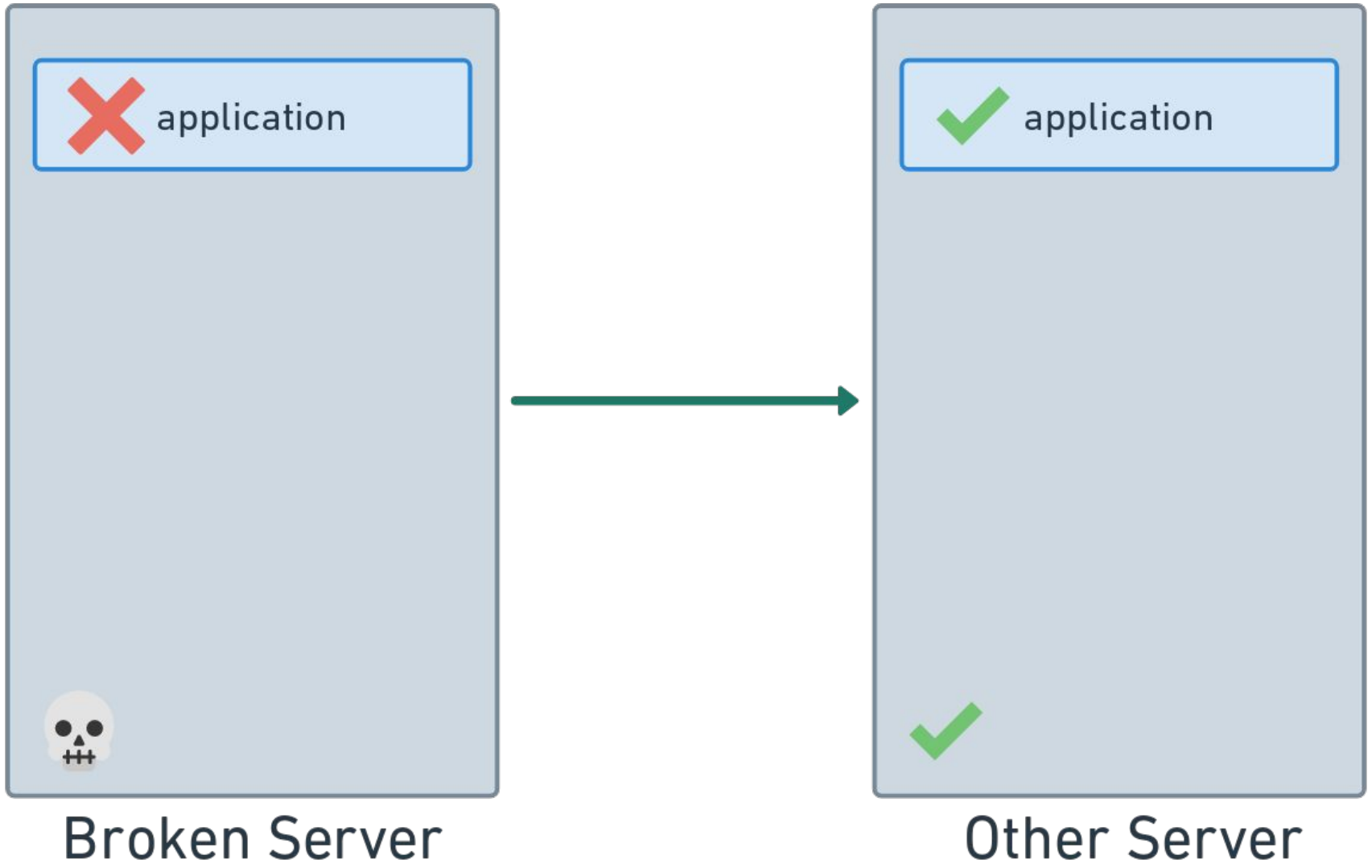
Rodrigo Campos Catelin, Microsoft
github.com/rata
Marga Manterola, Isovalent
@marga@hachyderm.io

Meet Taylor

Meet Taylor

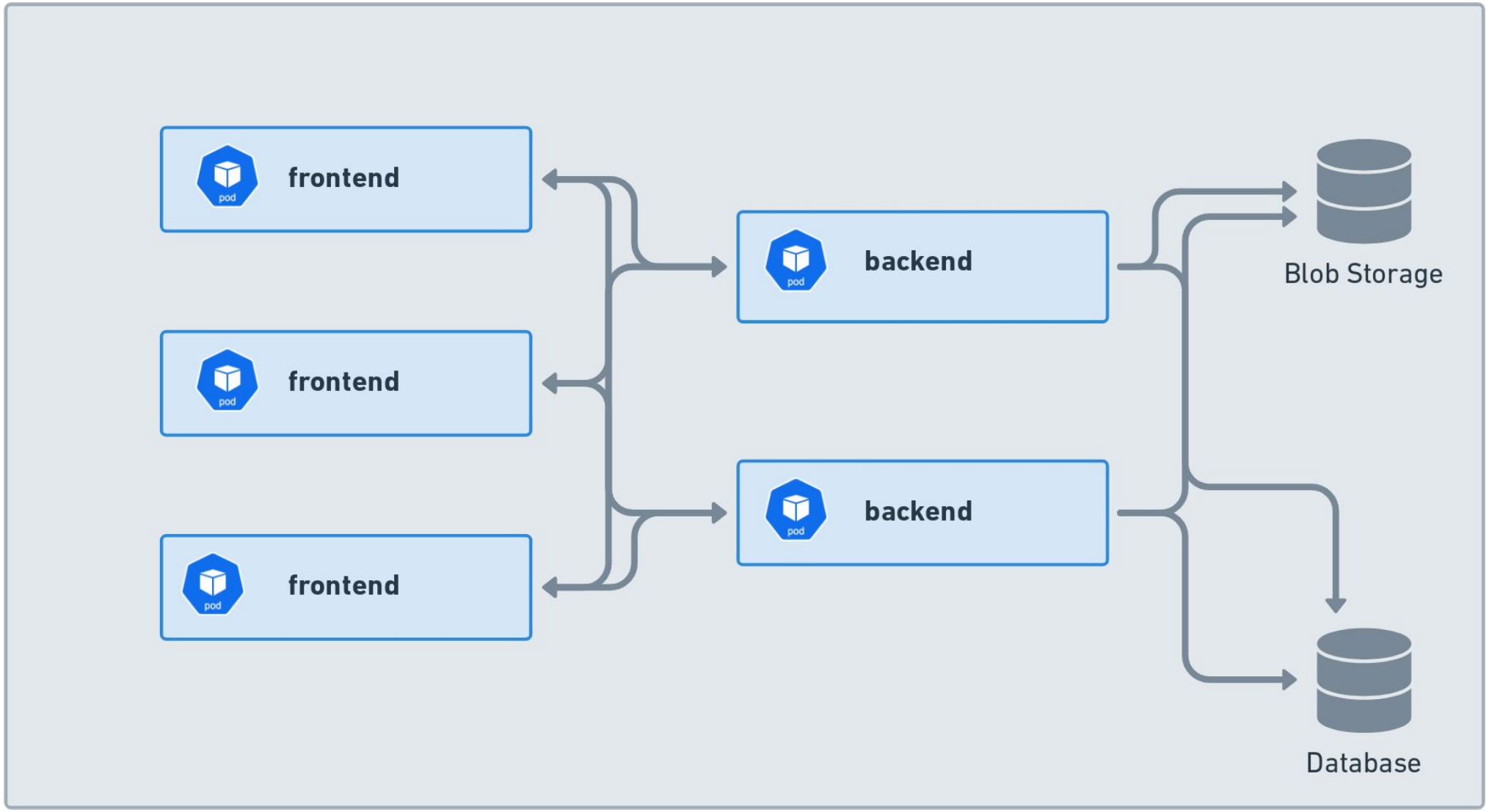

Firewall
External
Load Balancer
Frontend Servers
Internal
Load Balancer
Backend Servers

Lightweight containers



Cattle instead of pets

It can get complex fast



Automate more tasks

$$O(1) = O(n)$$

Self healing and load balancing

Additional abstraction

No free meal

Creating Deployments

Frontend

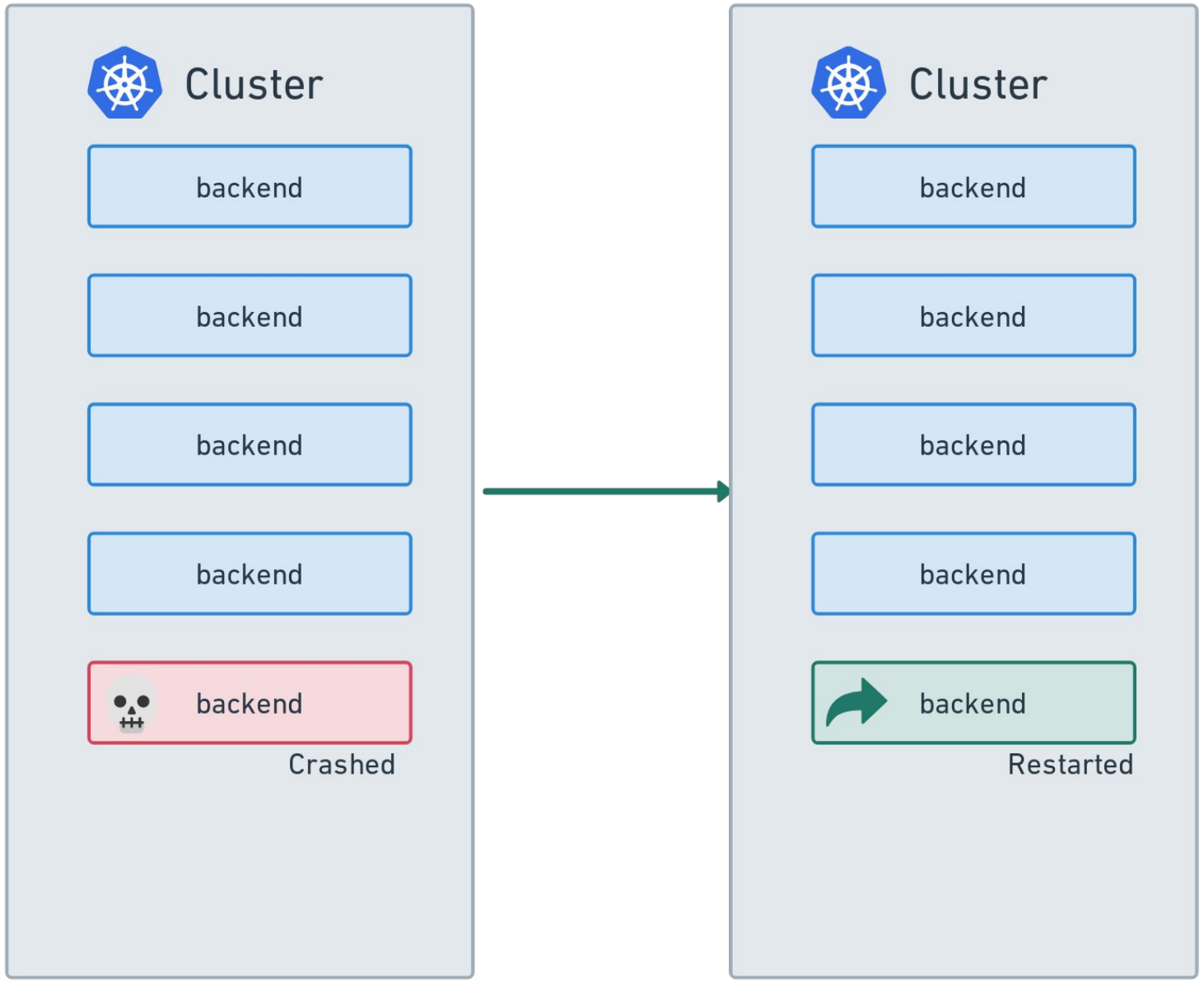
Backend

Taylor's Backend Deployment

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: backend-deployment
spec:
 replicas: 5
 selector:
   matchLabels:
     app-name: backend
 template:
   metadata:
     labels:
       app-name: backend
   spec:
     containers:
     - name: backend
       image: backend:1.2.3
```

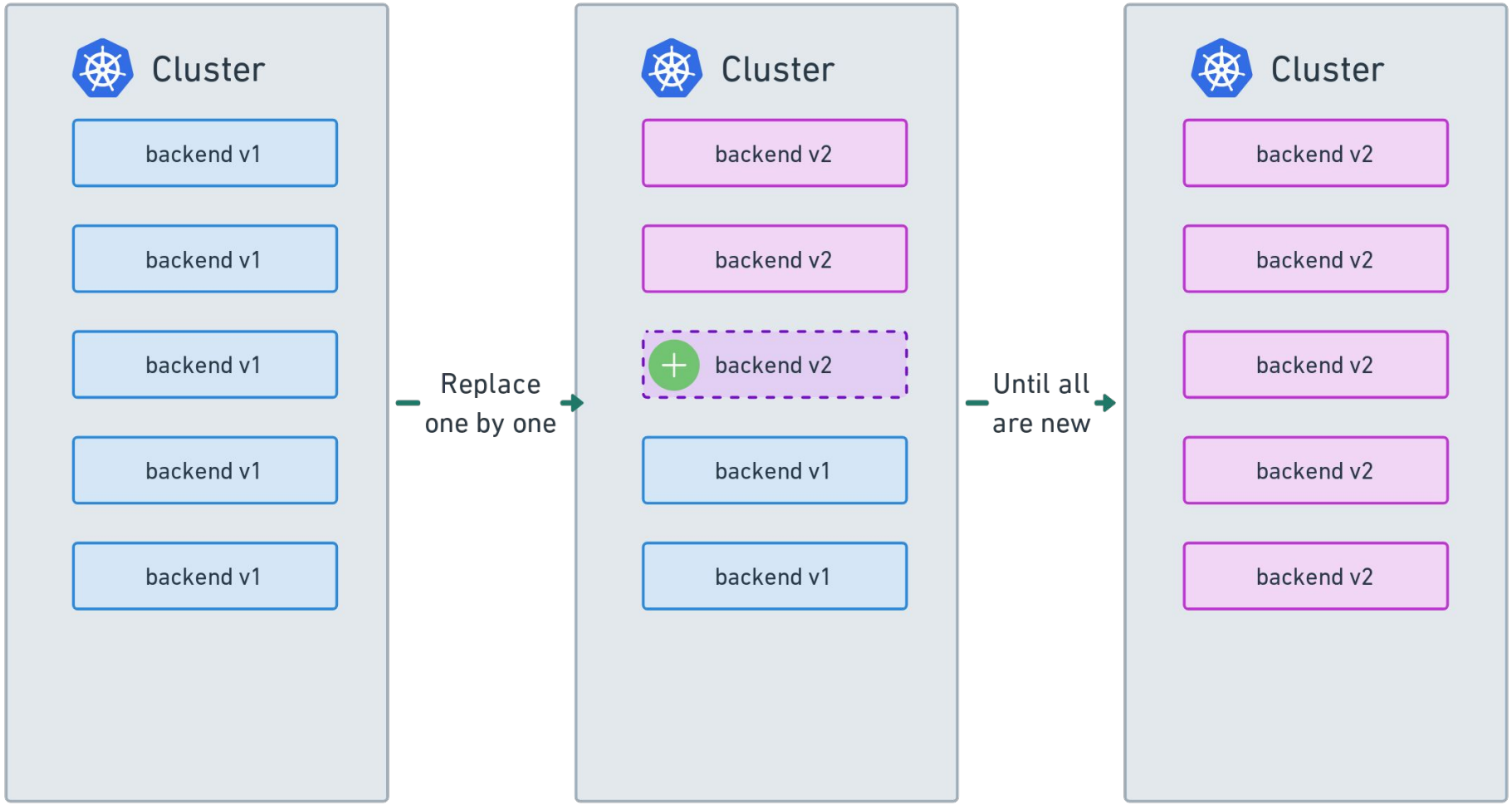
Desired state shapes reality


```
replicas: 5
```

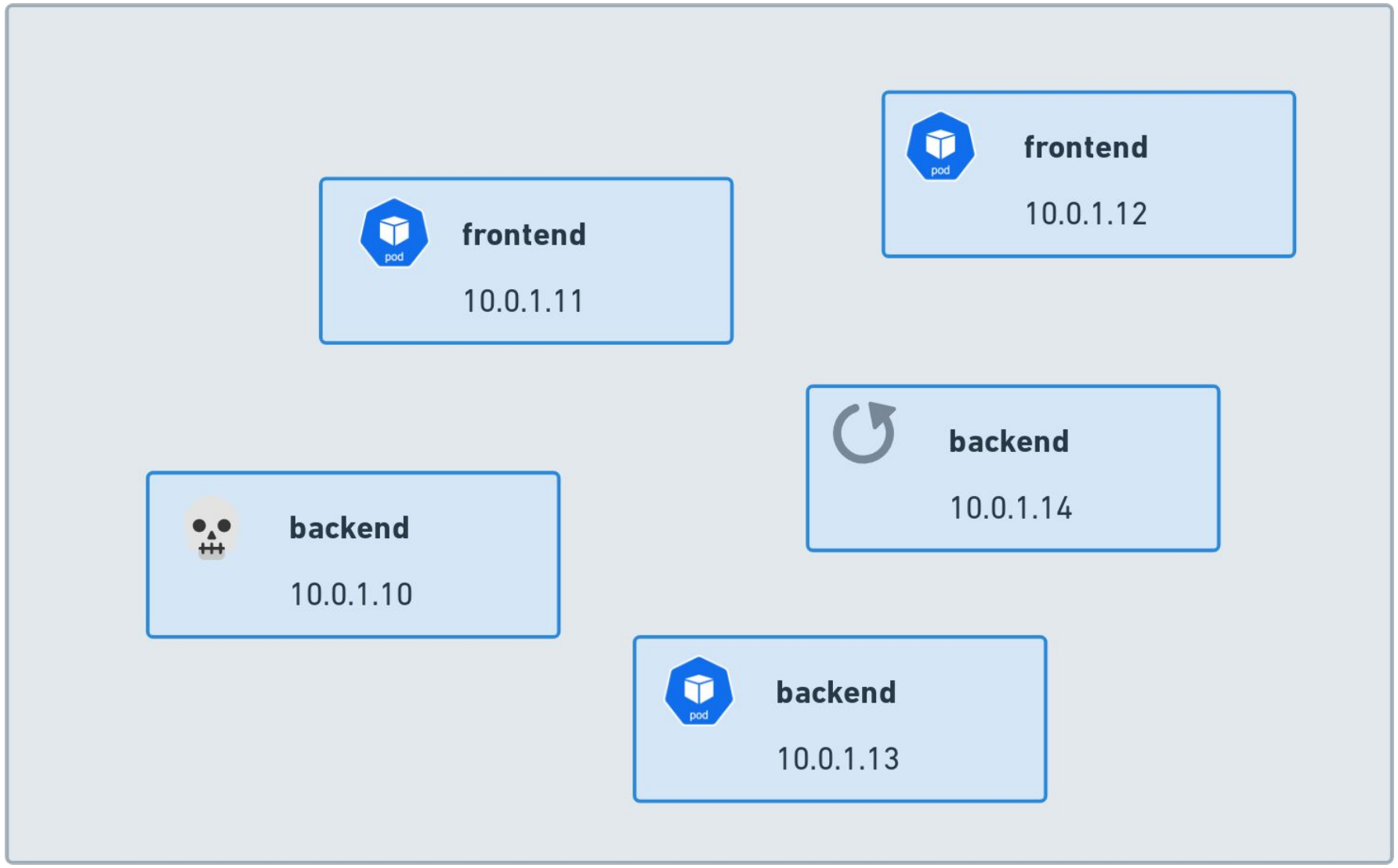


Desired state shapes reality


```
containers:
- name: backend
  image: backend:2.0
```



Container IPs are constantly changing

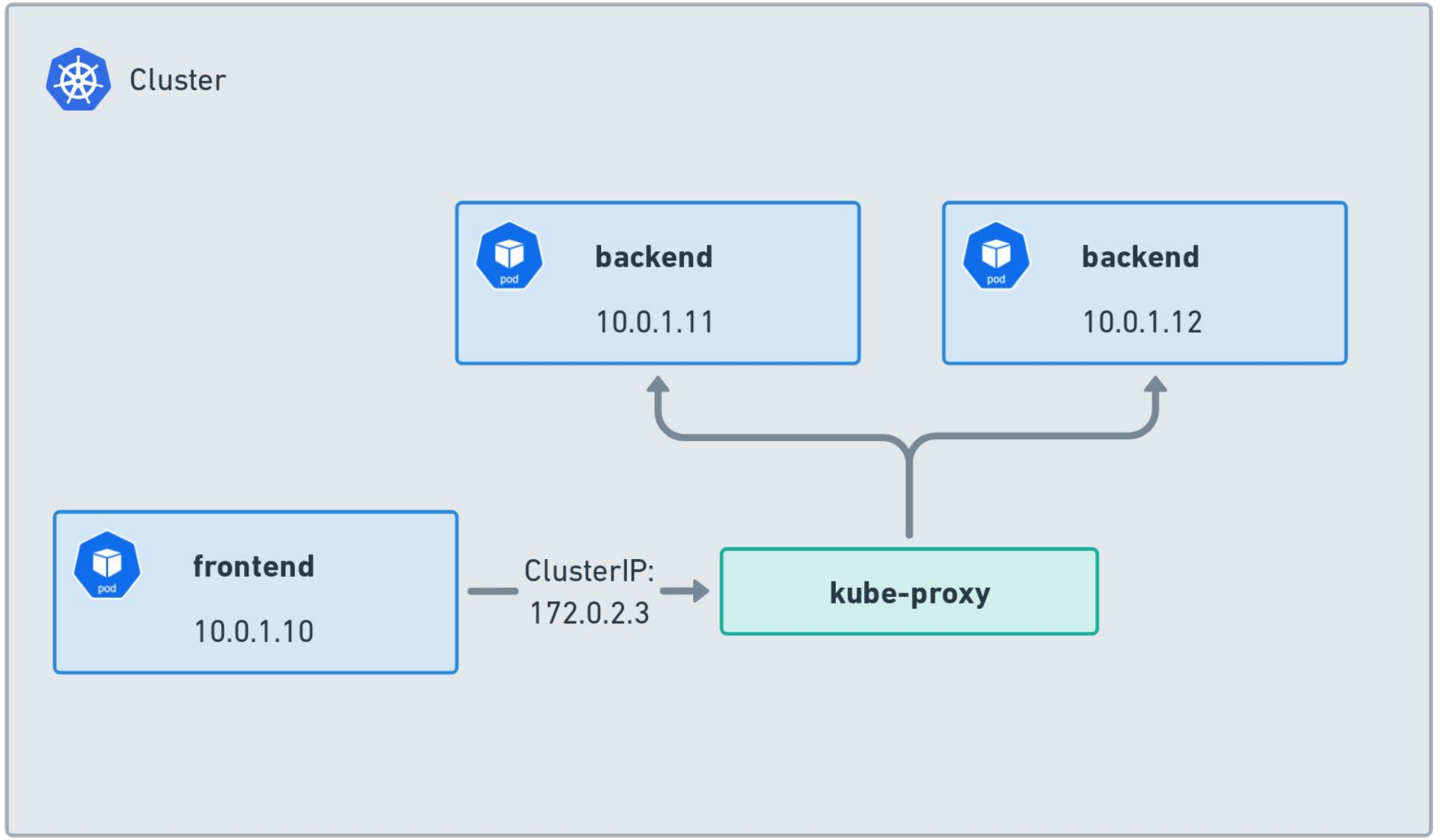


Taylor's services


```yaml
apiVersion: v1
kind: Service
metadata:
 name: frontend-service
spec:
 selector:
   app-name: frontend
 ports:
 - protocol: TCP
     port: 80
```

```yaml
apiVersion: v1
kind: Service
metadata:
 name: backend-service
spec:
 selector:
   app-name: backend
 ports:
 - protocol: TCP
     port: 9376
```

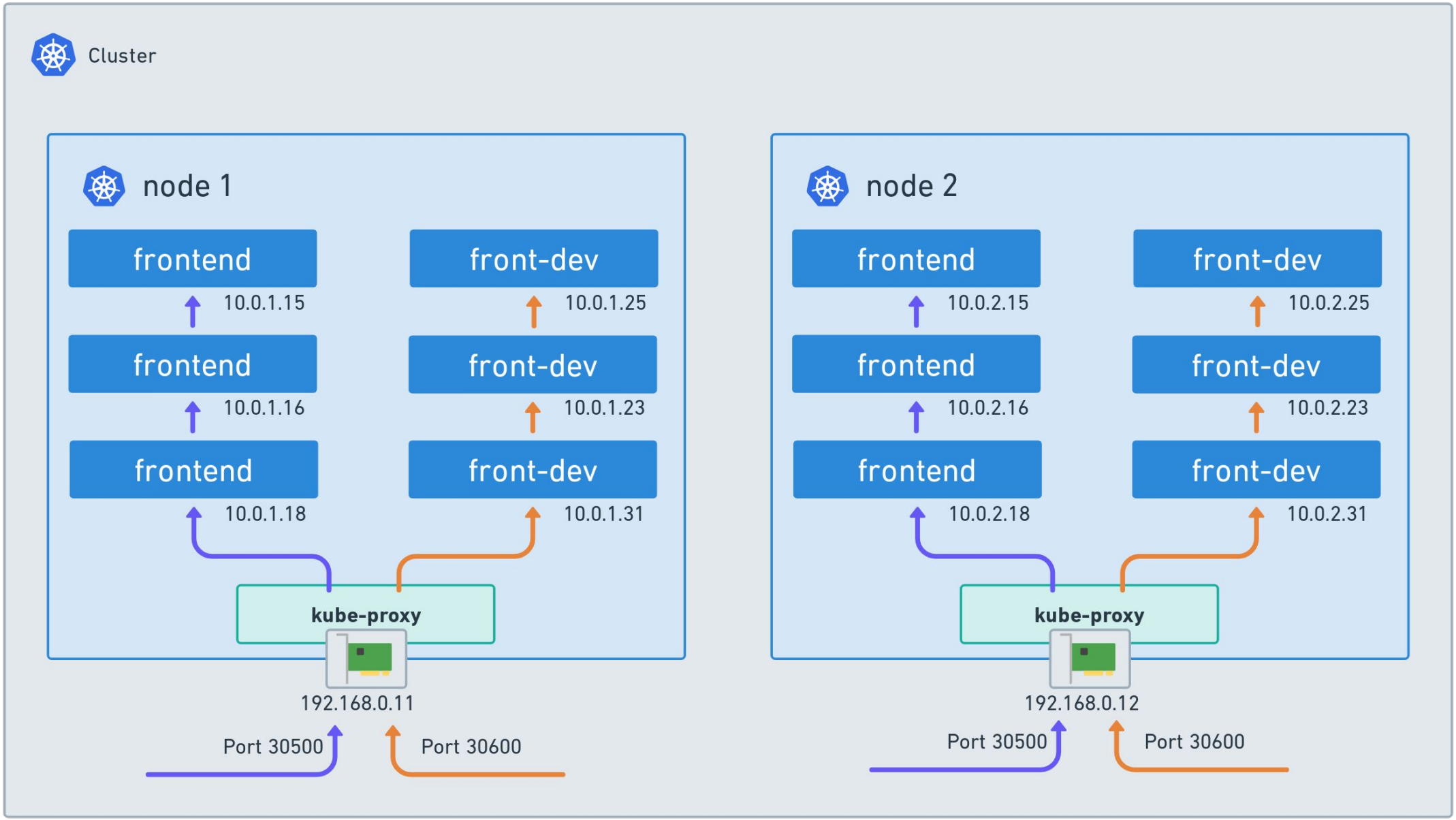
ClusterIP Services



Taylor's backend service

```yaml
apiVersion: v1
kind: Service
metadata:
 name: backend-service
spec:
 type: ClusterIP
 selector:
   app-name: backend
 ports:
 - protocol: TCP
     port: 80
```

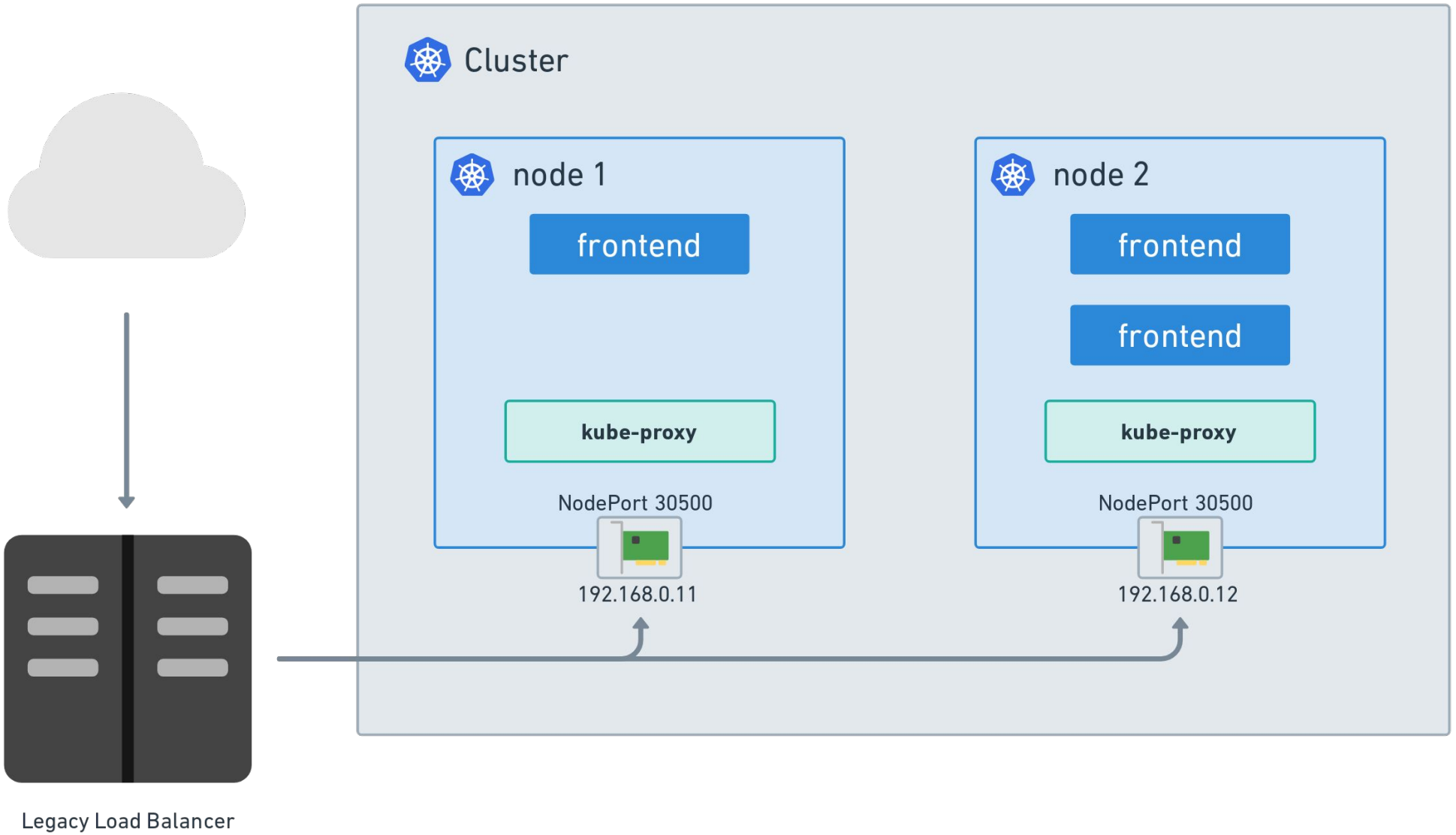
NodePort Services



Taylor's frontend service


```yaml
apiVersion: v1
kind: Service
metadata:
 name: frontend-service
spec:
 type: NodePort
 selector:
   app-name: frontend
 ports:
 - protocol: TCP
     port: 80
   nodePort: 30500
```

Legacy Load Balancer



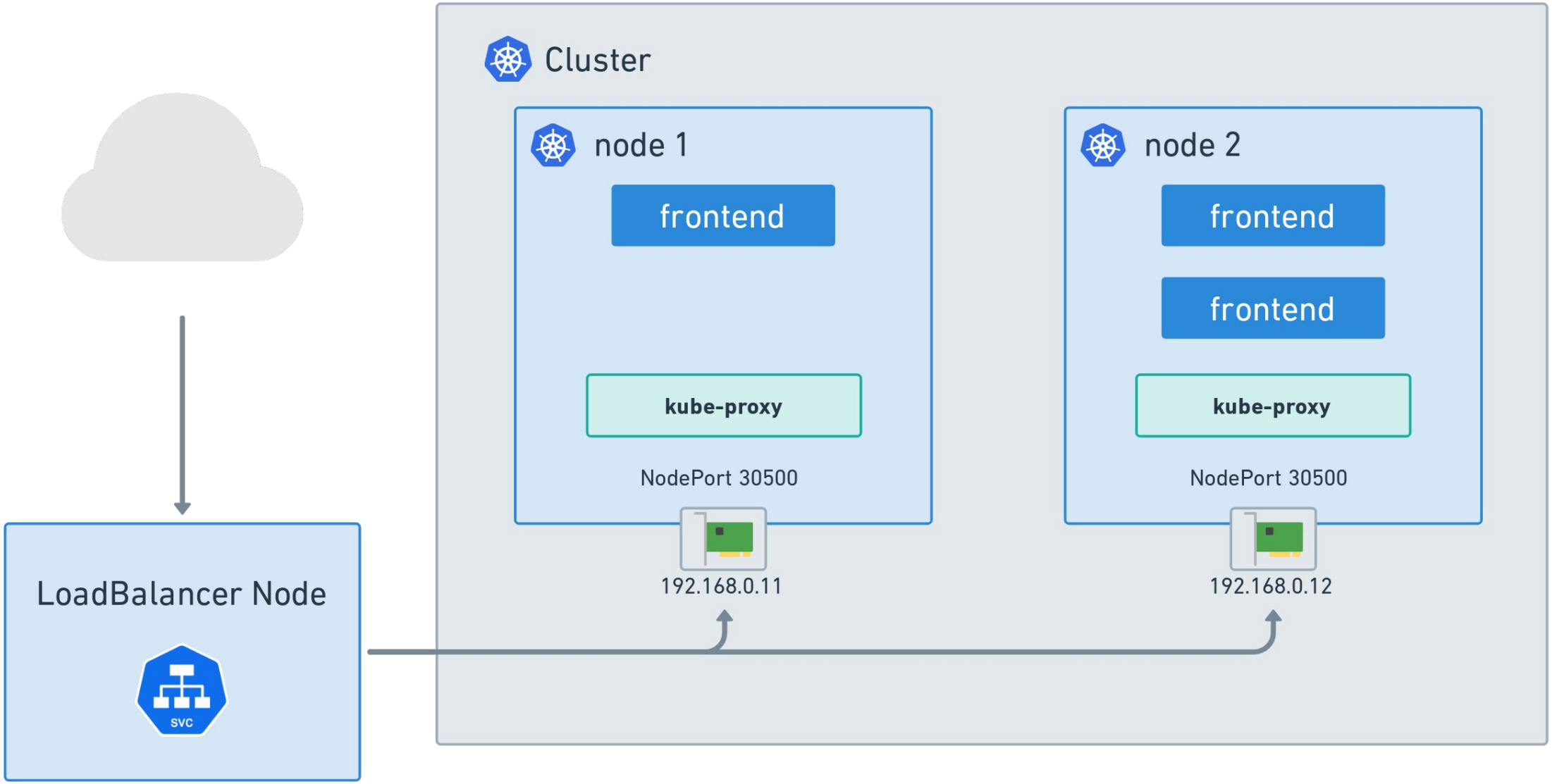
LoadBalancer definition

```yaml
apiVersion: v1
kind: Service
metadata:
 name: frontend-service
spec:
 type: LoadBalancer
 selector:
   app-name: frontend
 ports:
 - protocol: TCP
     port: 80
```

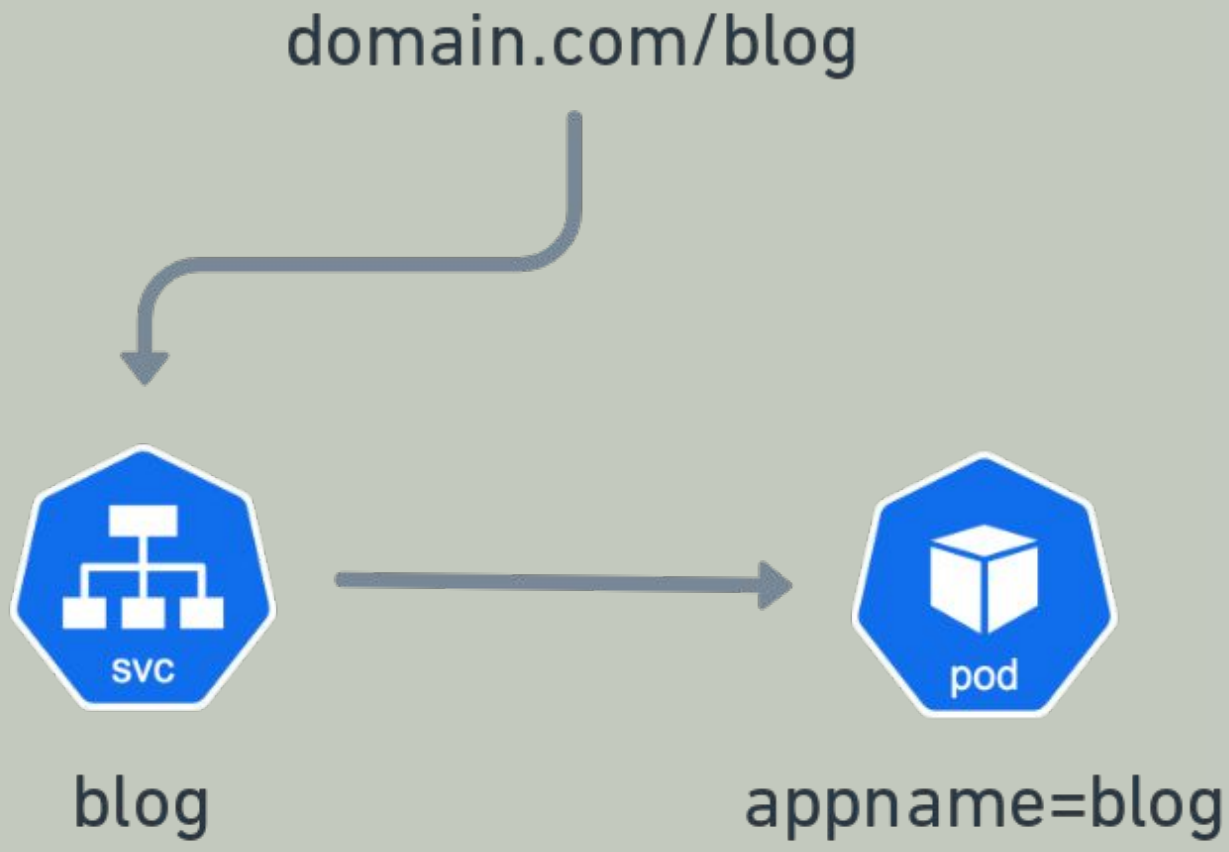
LoadBalancer definition

```
apiVersion: v1
kind: Service
metadata:
 name: my-service
spec:
 type: LoadBalancer
 selector:
   app-name: externally-reachable
 ports:
 - protocol: TCP
     port: 80
 clusterIP: 10.0.171.239
status:
 loadBalancer:
 ingress:
 - ip: 192.0.2.127
```

Cloud provided Load Balancer



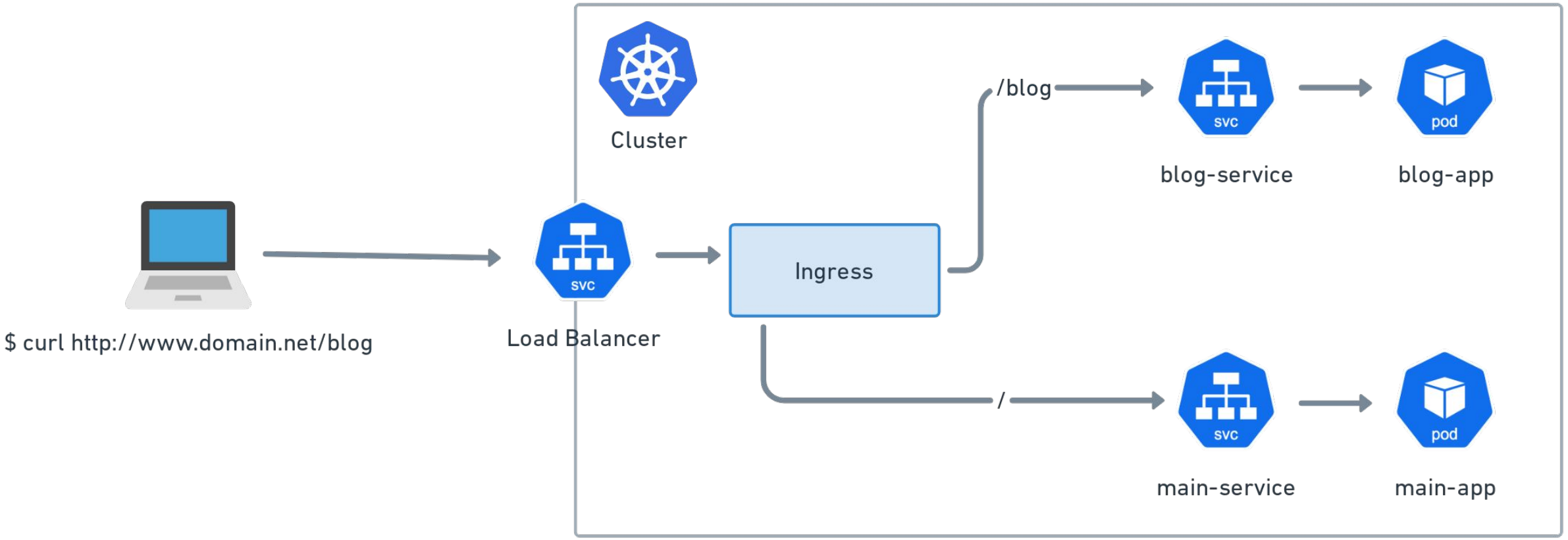
Taylor's app got more complex!



Ingress definition


```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: basic-ingress
spec:
 rules:
 - http:
     paths:
     - backend:
         service:
           name: blog
           port:
             number: 9080
       path: /blog
       pathType: Prefix
     - backend:
         service:
           name: frontend
           port:
             number: 80
       path: /
       pathType: Prefix
```

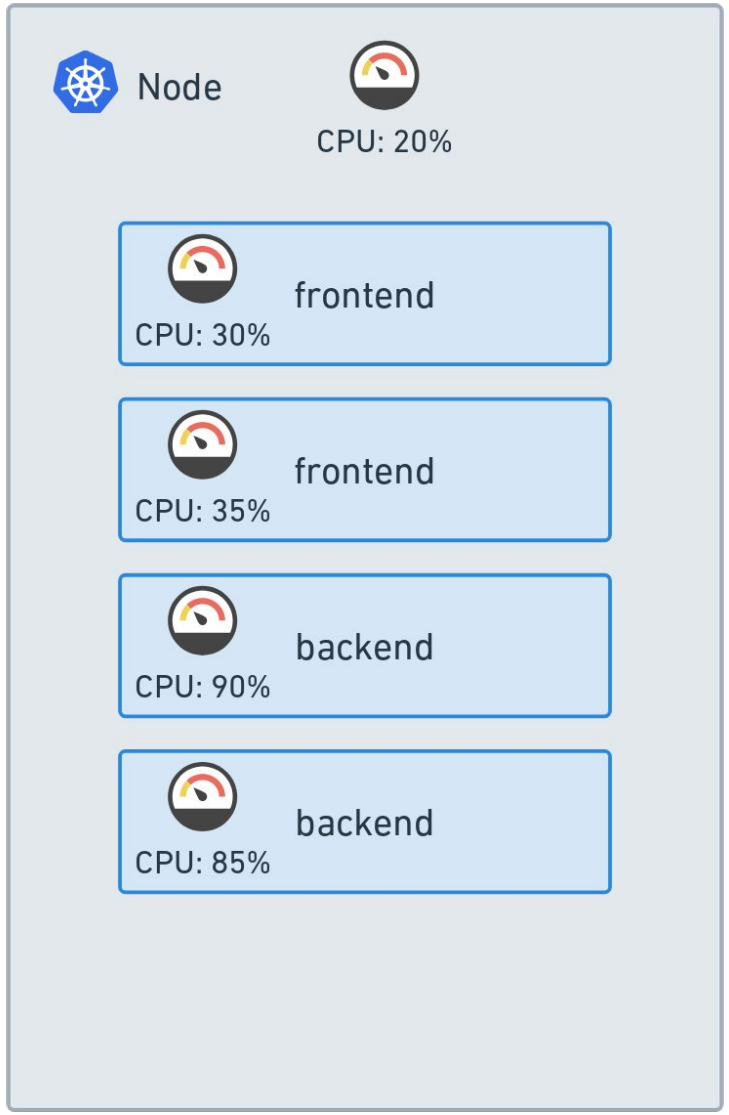
Ingress


Cluster
/blog
svc
pod
blog-service
blog-app
svc
Ingress
$ curl http://www.domain.net/blog
Load Balancer
/
svc
pod
main-service
main-app

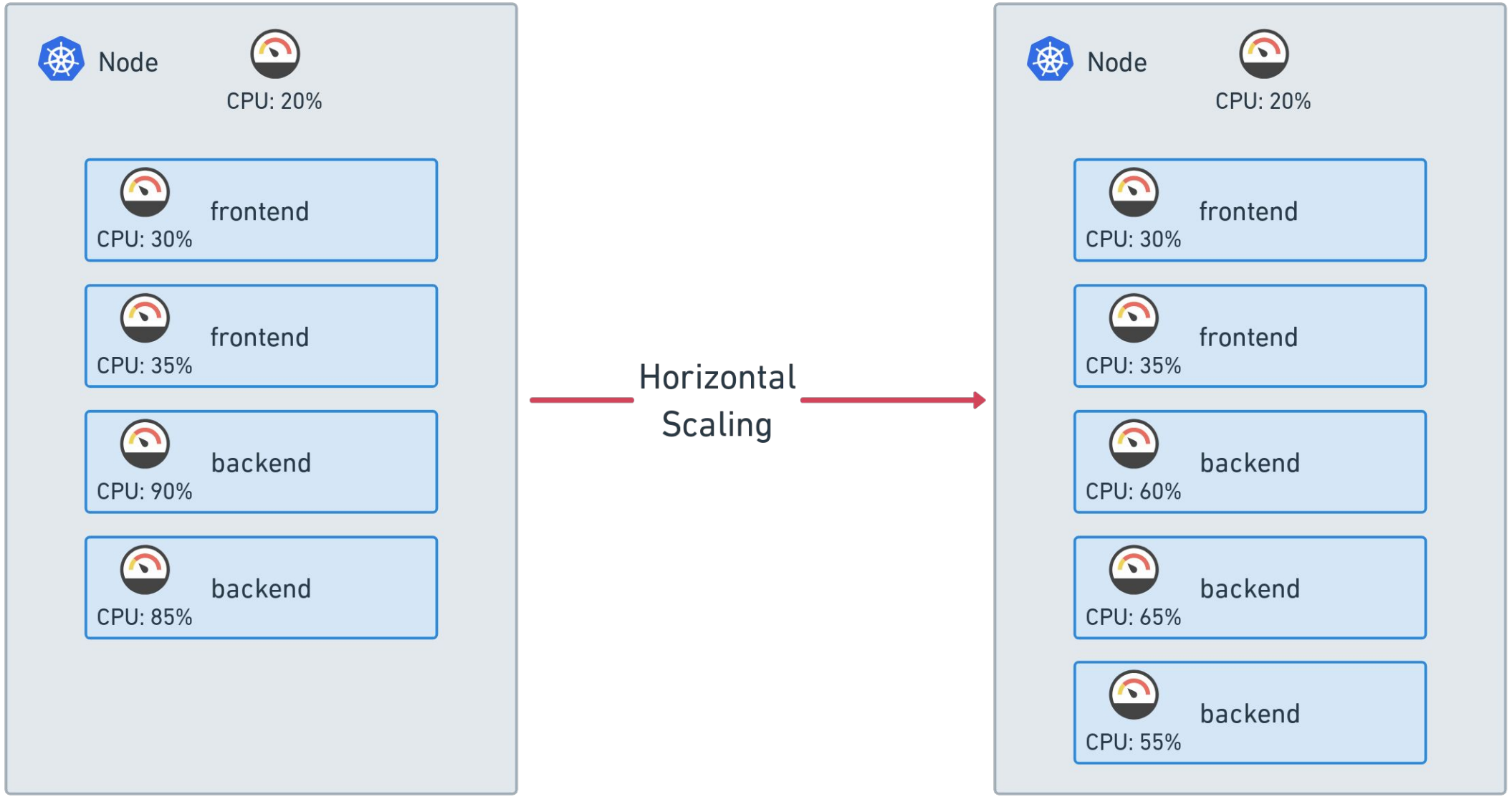
Autoscaling

Autoscaling in the VM world

Horizontal Scaling



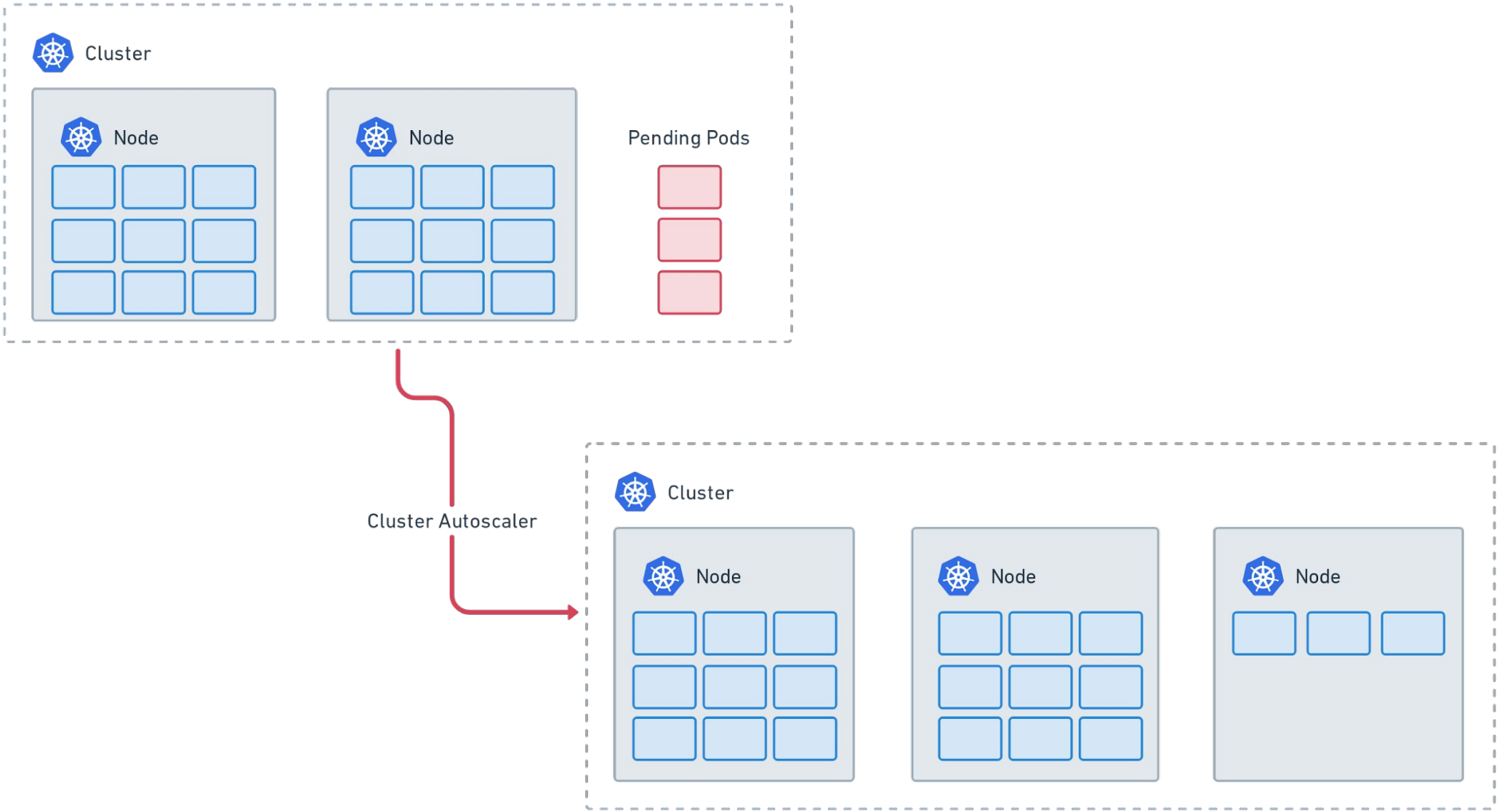
Horizontal Scaling



HorizontalPodAutoscaler definition

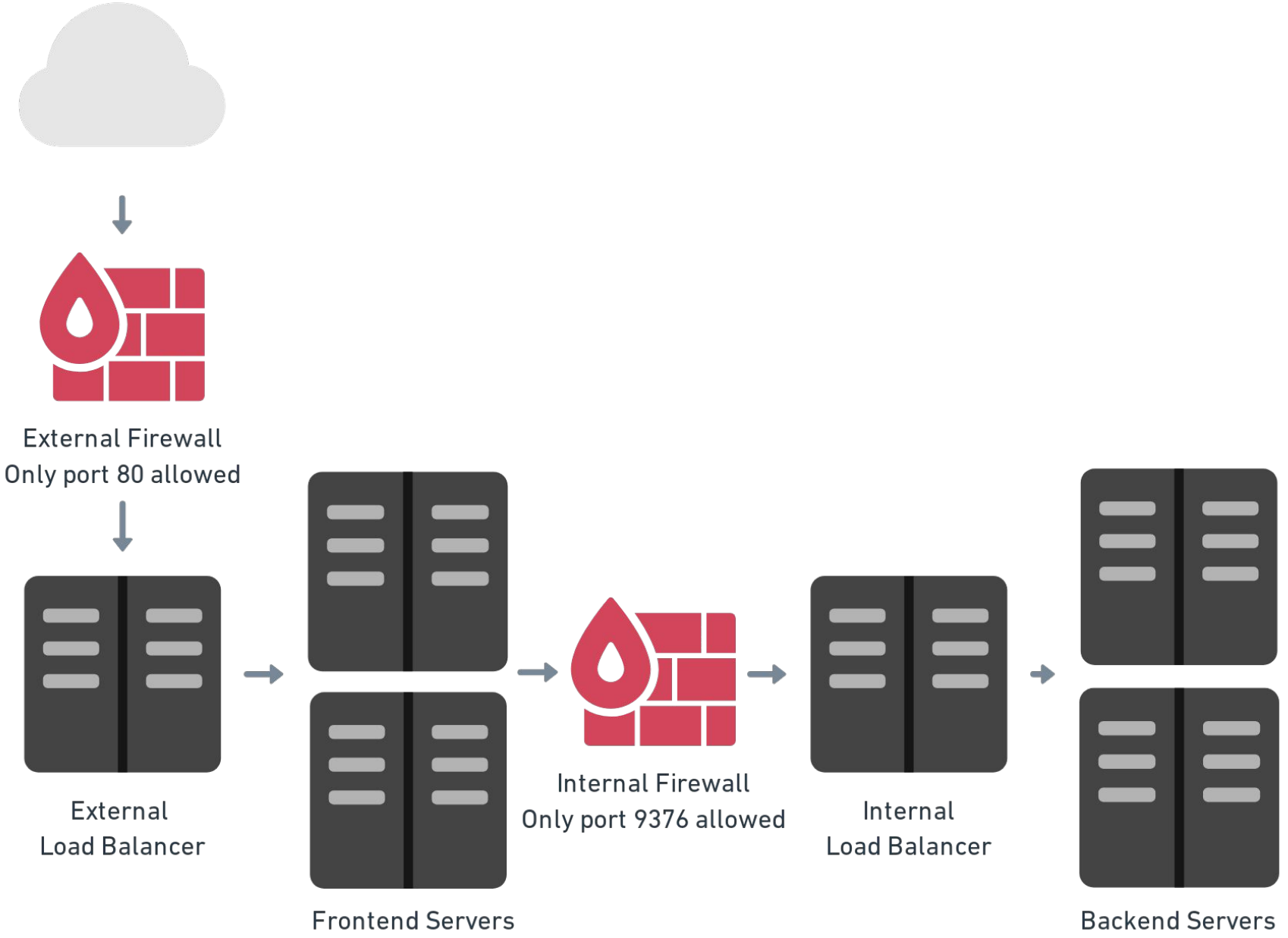

```yaml
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
 name: backend-hpa
spec:
 scaleTargetRef:
   apiVersion: apps/v1
   kind: Deployment
   name: backend-deployment
 minReplicas: 3
 maxReplicas: 10
 metrics:
 - type: Resource
   resource:
     name: cpu
     target:
       type: Utilization
       averageUtilization: 70
```

Cluster autoscaling

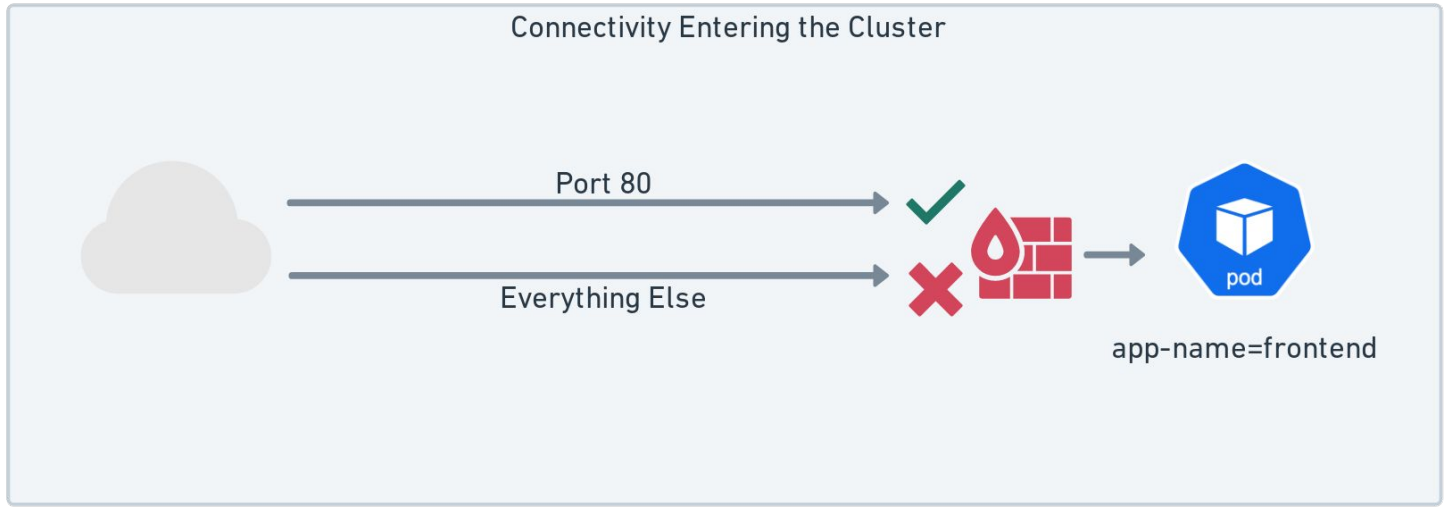


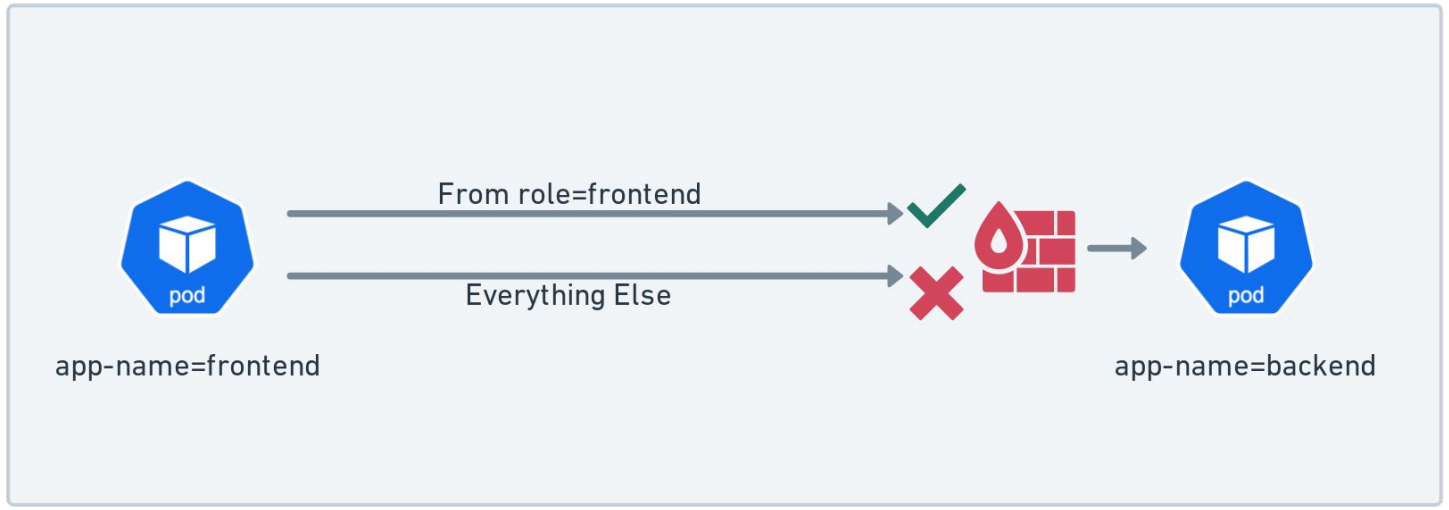
Firewalls

Old Style Firewall



Network Policies





Network Policies


```yaml
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
 name: allow-frontend-to-backend
spec:
 podSelector:
   matchLabels:
     app-name: backend
 policyTypes:
 - Ingress
 ingress:
   - from:
     - podSelector:
         matchLabels:
           app-name: frontend
     ports:
       - protocol: TCP
         port: 9376
```

Security

Taylor's app runs as root!

KubeCon CloudNativeCon Europe 2023

Dockerfile

```
FROM debian:jessie
WORKDIR /app
COPY --from=build /home/lab/target .
ENTRYPOINT ["java", "-Xmx8m", "-Xms8m", "-jar", "/app/words.jar"]
EXPOSE 8080
```

Deploy as non-root

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: backend-deployment
spec:
 replicas: 5
 selector:
   matchLabels:
     app-name: backend
 template:
   metadata:
     labels:
       app-name: backend
   spec:
     securityContext:
       runAsUser: 65534
       runAsGroup: 65534
     containers:
     - name: backend
       image: backend:1.2.3
```

Image Security

Image Security

Dockerfile

```
FROM taylor.azurecr.io/java-base:v1
WORKDIR /app
COPY --from=build /home/lab/target .
ENTRYPOINT ["java", "-Xmx8m", "-Xms8m", "-jar", "/app/words.jar"]
EXPOSE 8080
```

Minimizing access


```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: backend-deployment
spec:
 replicas: 5
 selector:
   matchLabels:
     app-name: backend
 template:
   metadata:
     labels:
       app-name: backend
   spec:
     securityContext:
       seccompProfile:
         type: RuntimeDefault
     containers:
     - name: backend
       image: backend:1.2.3
       securityContext:
         allowPrivilegeEscalation: false
```

Cluster admin = root in the VM

Final words

References

- Kubernetes Service reference.
  - And the rest of the Kubernetes docs, they are really good!
- The dockerfile in the “wordsmith” example from Docker documentation is a case of a common example that runs a root.
- Inspektor Gadget:
  - https://www.inspektor-gadget.io/
- Cilium
  - https://www.cilium.io
- Dockerhub vulnerabilities analysis (link1, link2)
- Kubercon 2022 Detroit - user namespaces talk (video, slides)
- Taylor images were created with MidJourney and Gimp.
- All logos on Taylor's T-shirts are CNCF trademarks

Questions?

KubeCon CloudNativeCon Europe 2023

Please scan
the QR Code
to leave feedback
on this session

Thank you!

KubeCon CloudNativeCon Europe 2023

Please scan
the QR Code
to leave feedback
on this session