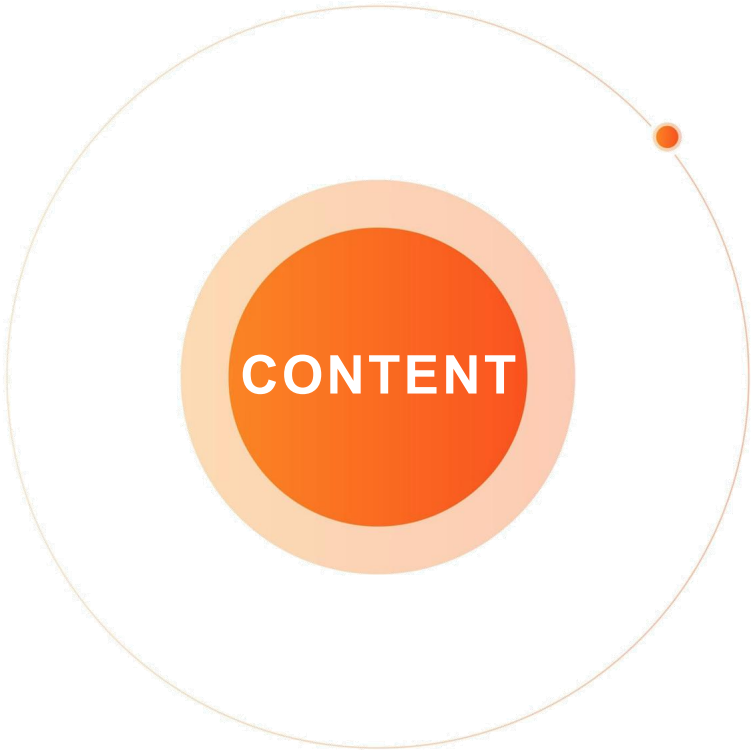

KubeCon
CloudNativeCon
OPEN SOURCE SUMMIT
China 2023

Serverless Service Mesh Based on Istio and Virtual Kubelet

Xi Ning WANG(王夕宁)
Ze Huan SHI(史泽寰)

@Alibaba Cloud

Agenda



① Serverless in Control Plane

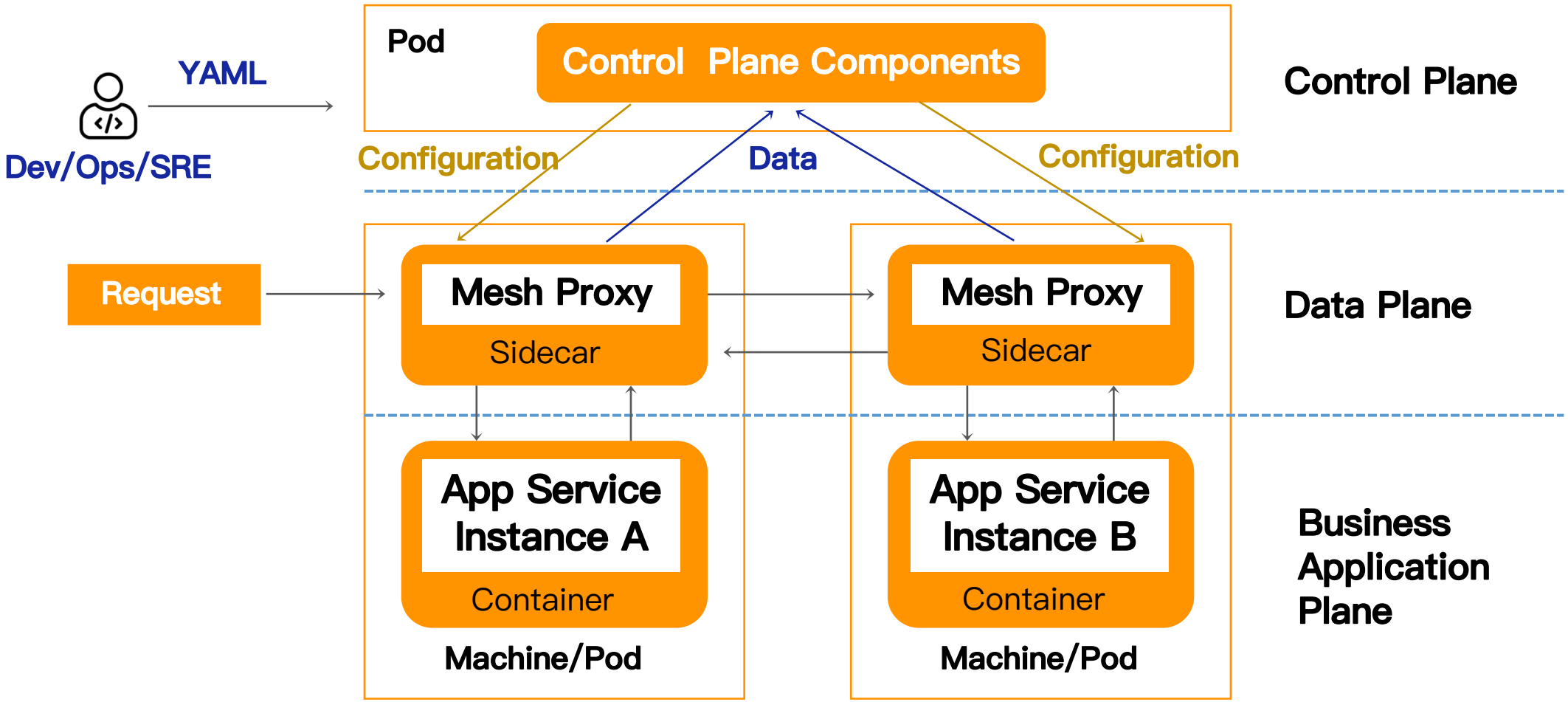
② Serverless support in the data plane with Sidecar mode

③ Serverless support in the data plane with Sidecarless mode

④ Wrap-up

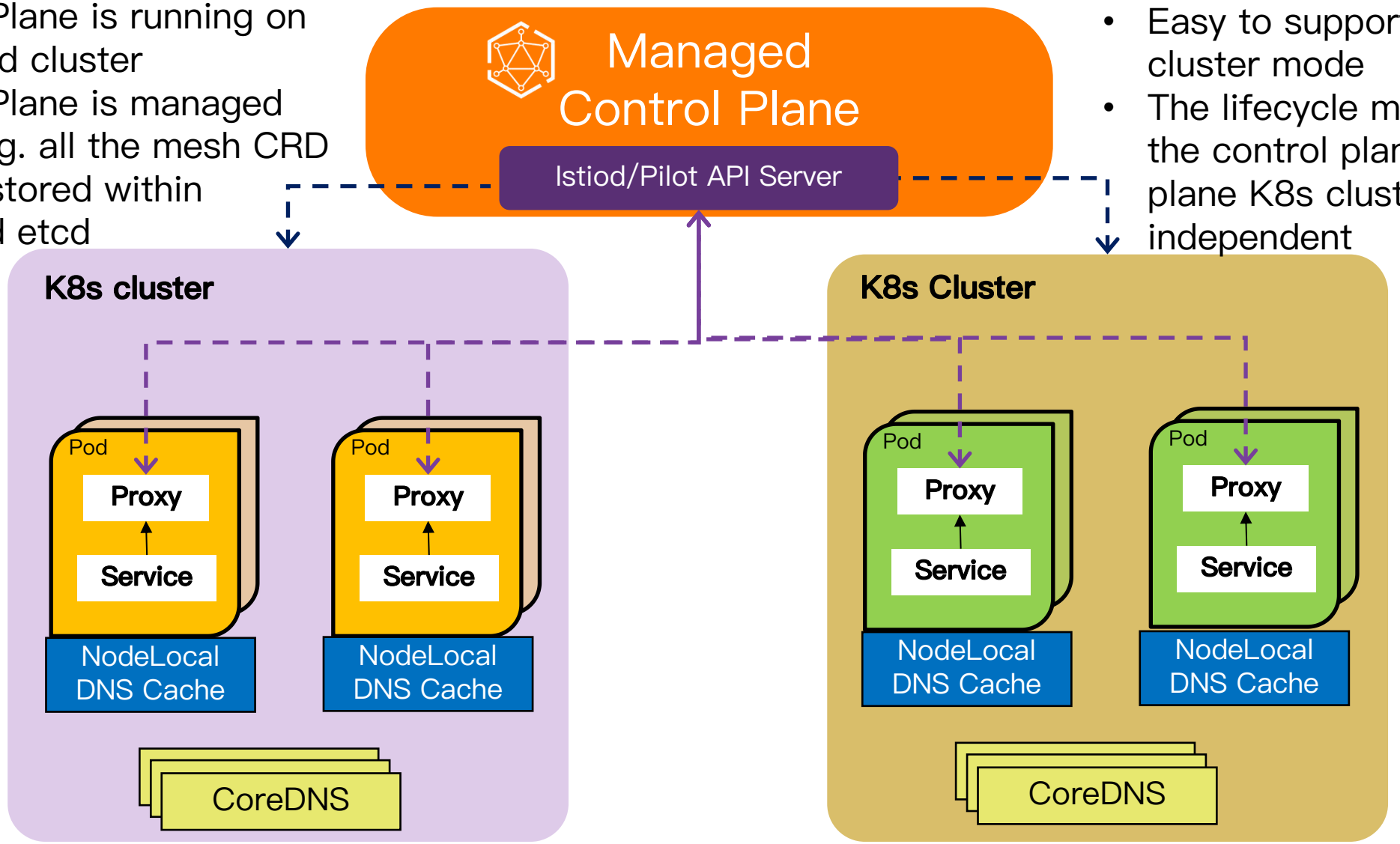
Traditional Sidecar mode in Service Mesh

Both the control plane and data plane components run within a single K8s cluster



Decoupling of the control plane and data plane

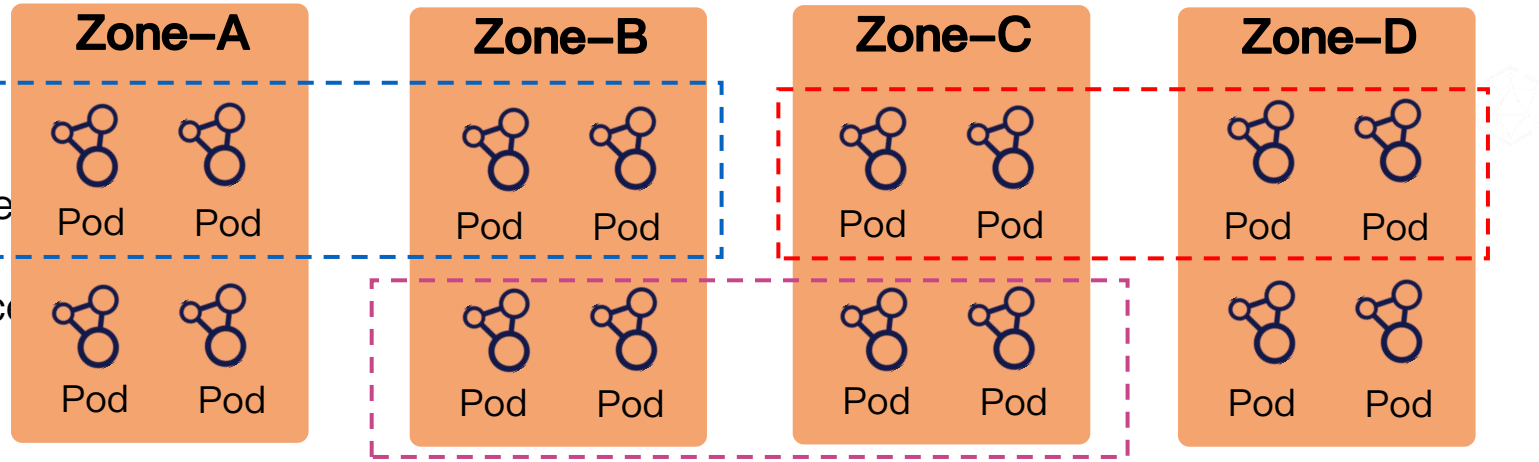
- Control Plane is running on separated cluster
- Control Plane is managed mode, e.g. all the mesh CRD objects stored within managed etcd

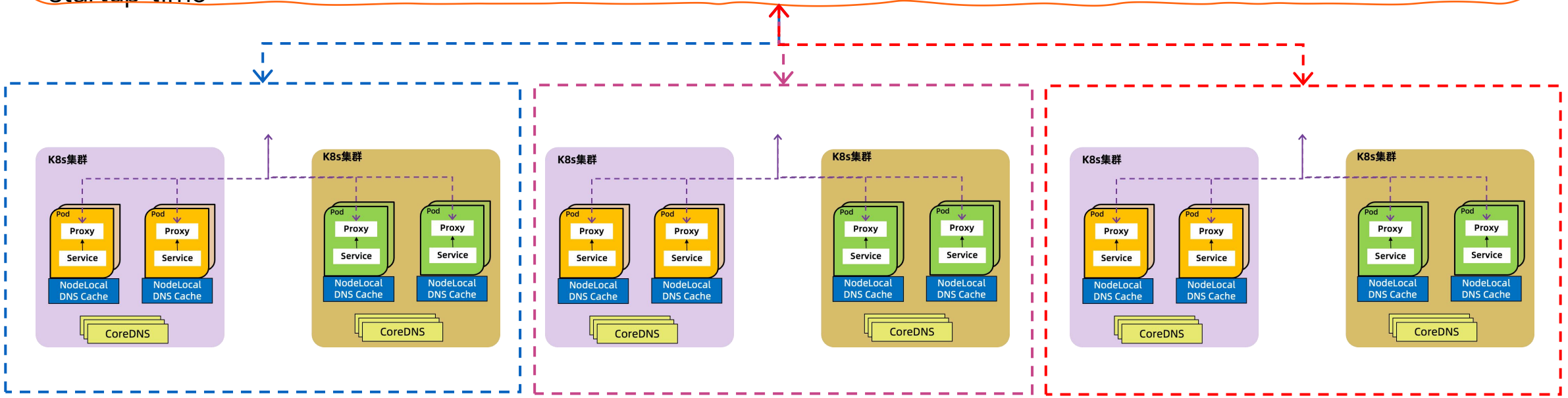


- Easy to support for multi-cluster mode
- The lifecycle management of the control plane and data plane K8s clusters is independent

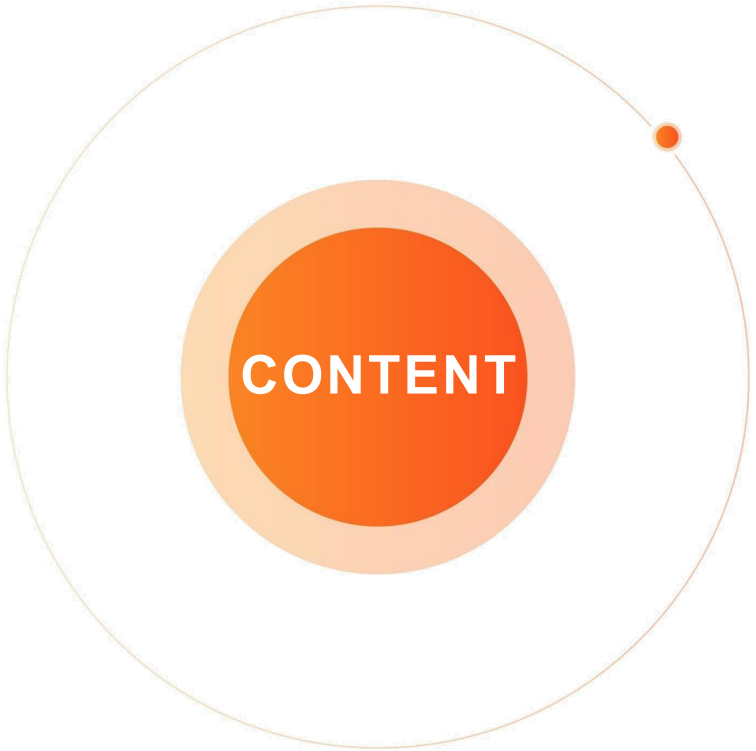
Serverless of the managed control plane.

- ready to use out of the box
- automatic elastic scaling, on-demand usage, and optimized scheduling
- multi-availability zone for improve stability
- Image caching acceleration reduc the time required for readiness, leading to a decrease in overall startup time





Agenda



① Serverless in Control Plane

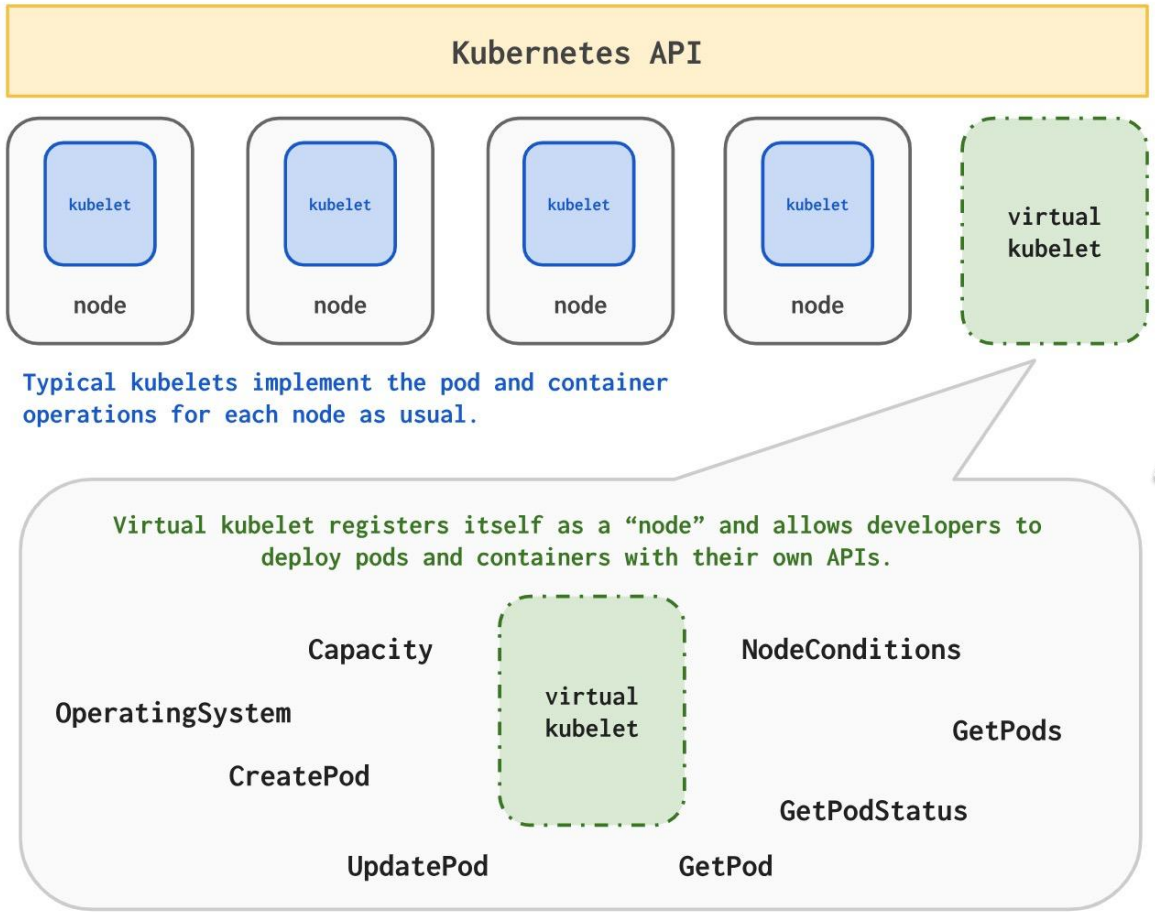
② Serverless support in the data plane with Sidecar mode

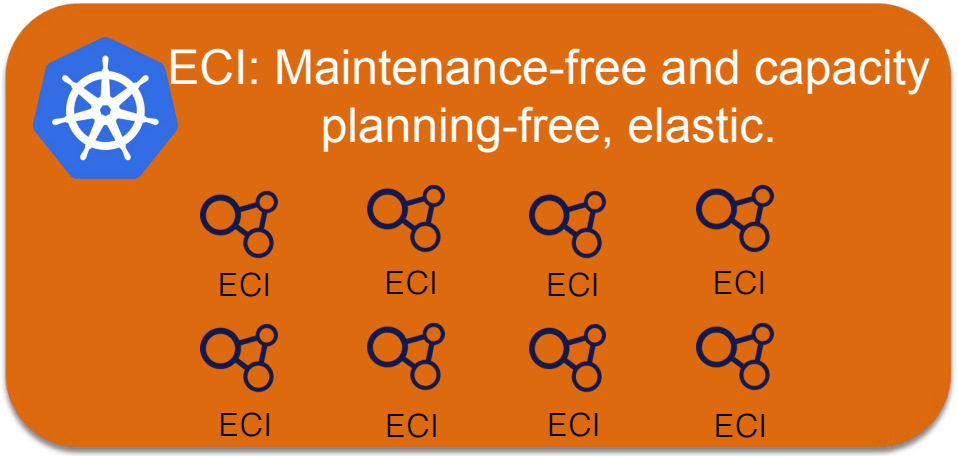
③ Serverless support in the data plane with Sidecarless mode

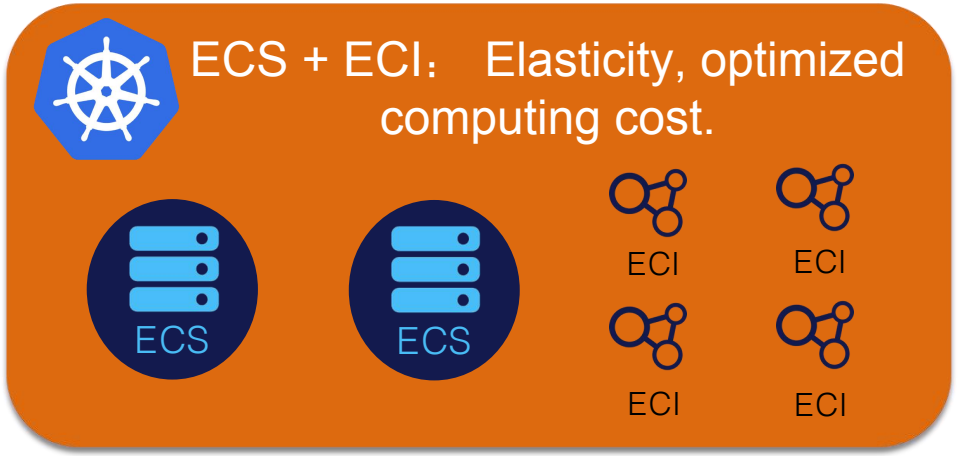
④ Wrap-up

Virtual Kubelet & Serverless Container

- **VK: Decoupling the orchestration layer from the resource pool, fully unleashing resource elasticity.**





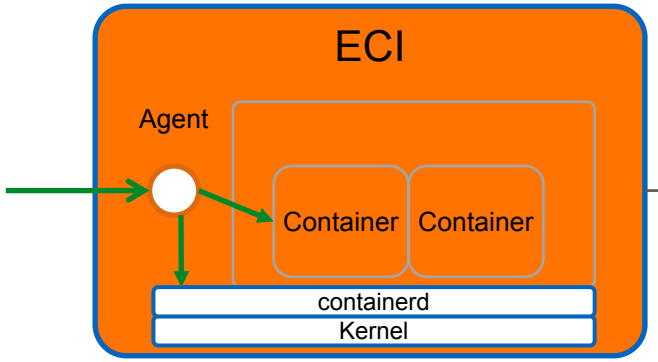


How to make Sidecar and Gateway Pods Serverless

What are the challenges and how to address them?

- **1. Deployment strategy: Running on virtual nodes.**

```yaml
affinity:
  nodeAffinity:
    preferredDuringSchedulingIgnoredDuringExecution:
    - preference:
        matchExpressions:
          - key: type
            operator: In
            values:
              - virtual-kubelet
    requiredDuringSchedulingIgnoredDuringExecution:
    nodeSelectorTerms:
        - matchExpressions:
          - key: type
            operator: In
            values:
              - virtual-kubelet
tolerations:
- effect: NoSchedule
    key: virtual-kubelet.io/provider
    operator: Equal
    value: alibabacloud
```

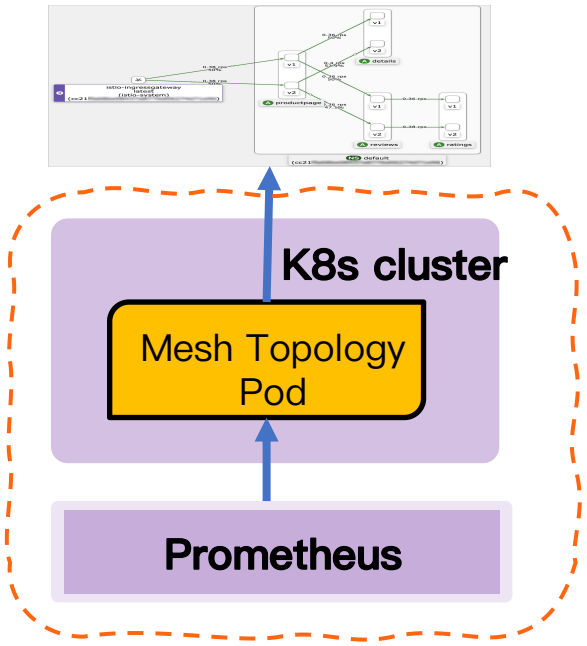


- **2. Security considerations：securityContext**

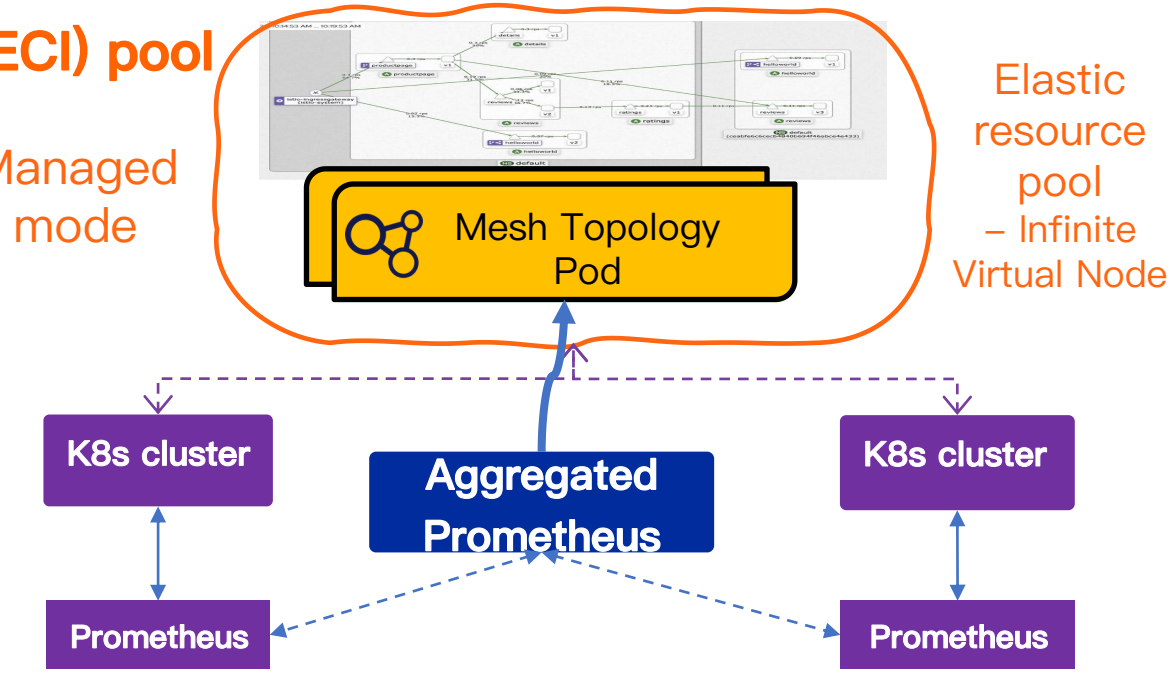
```yaml
securityContext:
      allowPrivilegeEscalation: false
      privileged: false
      capabilities:
        add:
         - NET_ADMIN
        drop:
         - ALL
```

Managed mesh topology within elastic resource pool

- **Running within a Kubernetes cluster**



- **Running within Elastic Container Instances (ECI) pool**



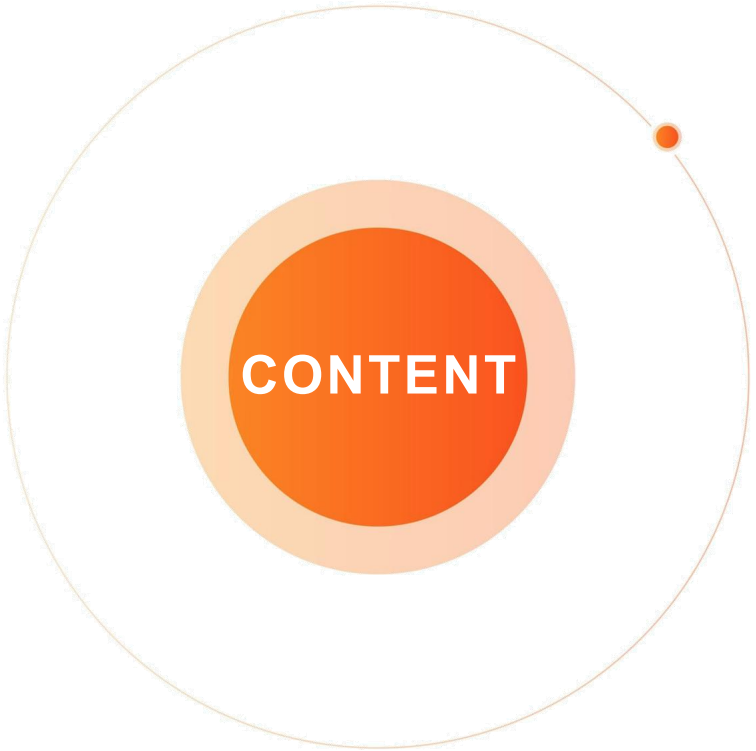
Deployed within a Kubernetes cluster

- The availability of services is affected by the cluster and cannot achieve the elastic capabilities
- In a multi-cluster environment, each topology can only observe the workload-related within its own cluster. Additionally, each cluster needs to be configured and deployed separately, resulting in high complexity.

Deployed in a managed Serverless mode

- Deployed in a managed ECI mode within an elastic resource pool, it has the ability to elastically scale and schedule across multiple availability zones. Resources are used and released on-demand.
- It provides better support for unified observation of traffic topology in a multi-cluster environment, offering centralized configuration for topology observation and a unified service access entry.

Agenda



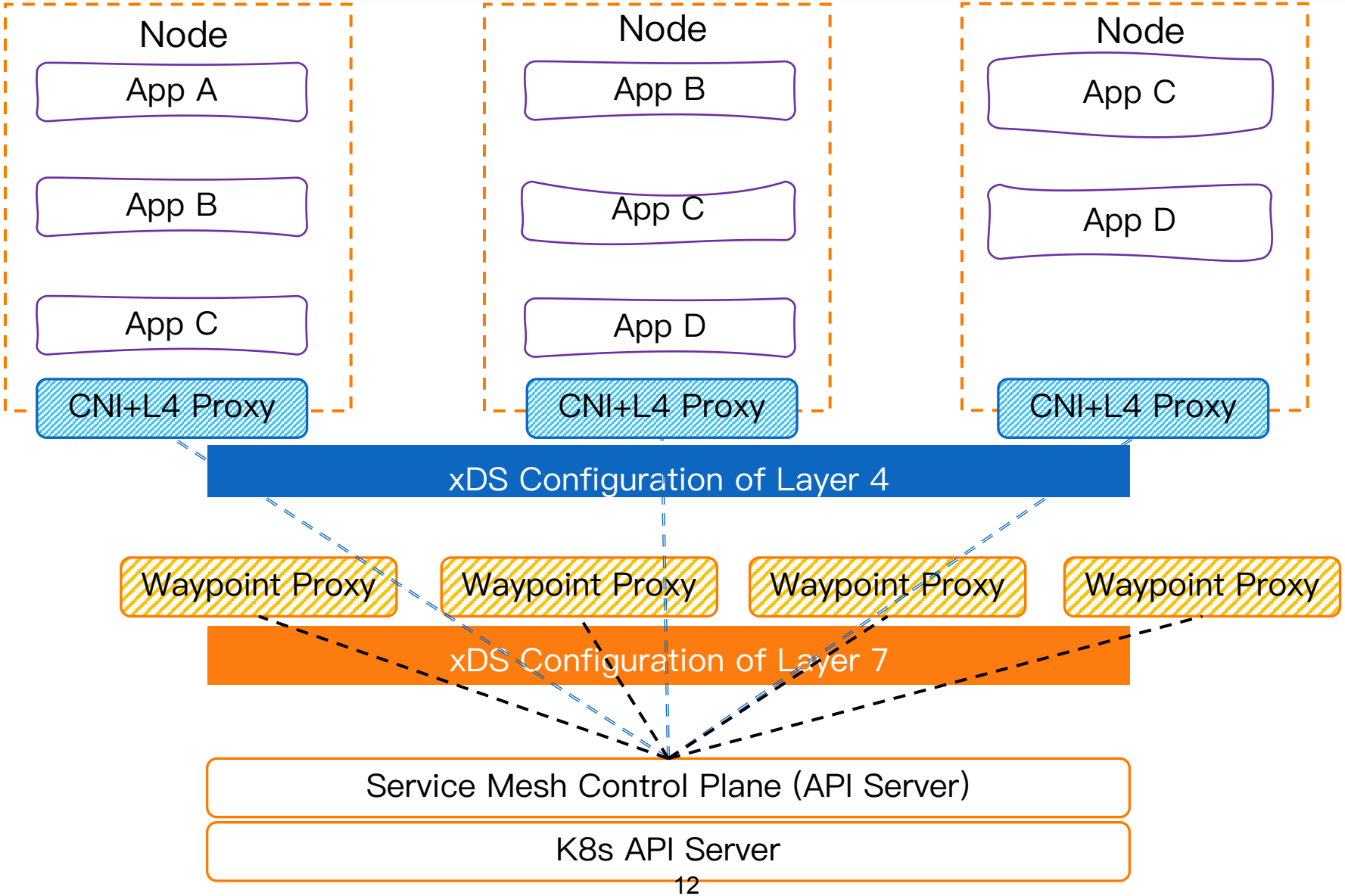
① Serverless in Control Plane

② Serverless support in the data plane with Sidecar mode

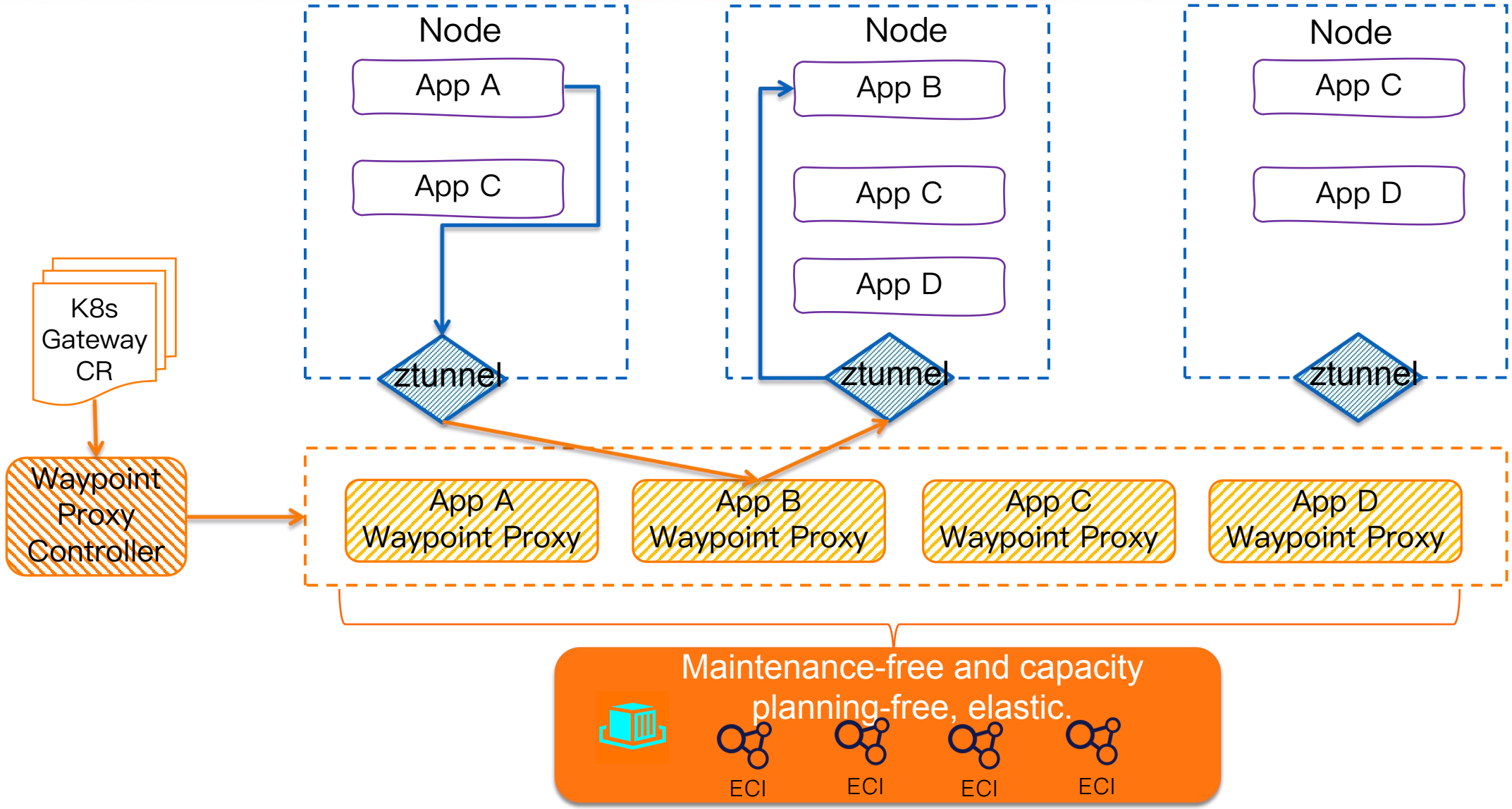
③ Serverless support in the data plane with Sidecarless mode

④ Wrap-up

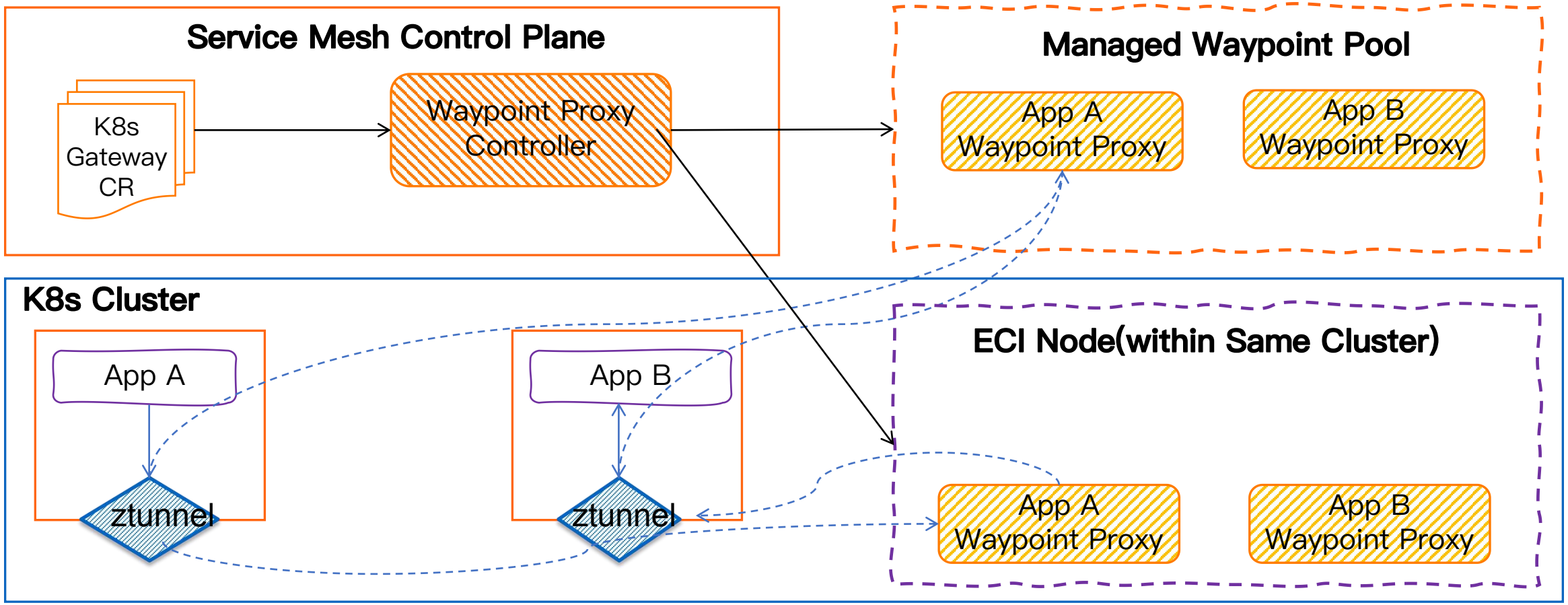
Decoupling of L4 and L7 Proxy



Serverless of L7 proxy in the data plane

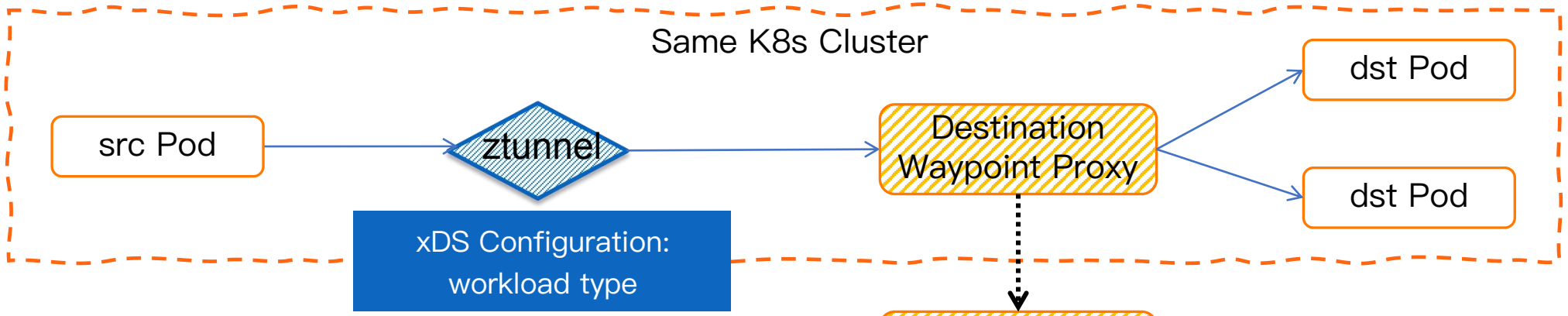


Serverless Waypoint Proxy Architecture



Running Waypoint Proxy within Managed Waypoint Pool or ECI Node within user cluster

Challenges: L4 proxy <--> L7 Proxy

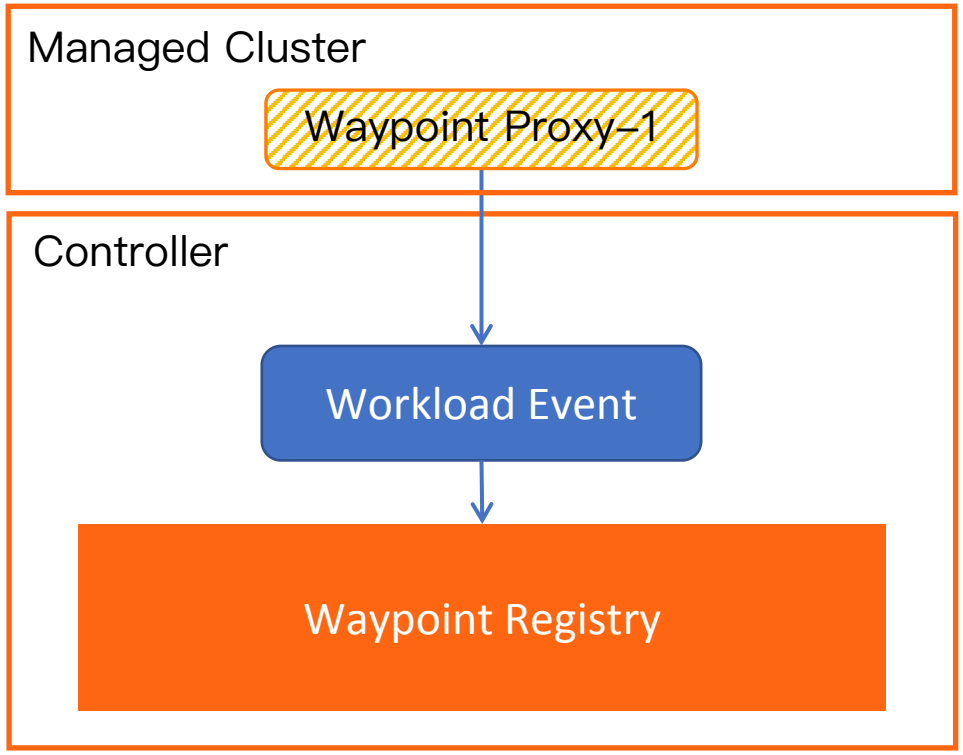


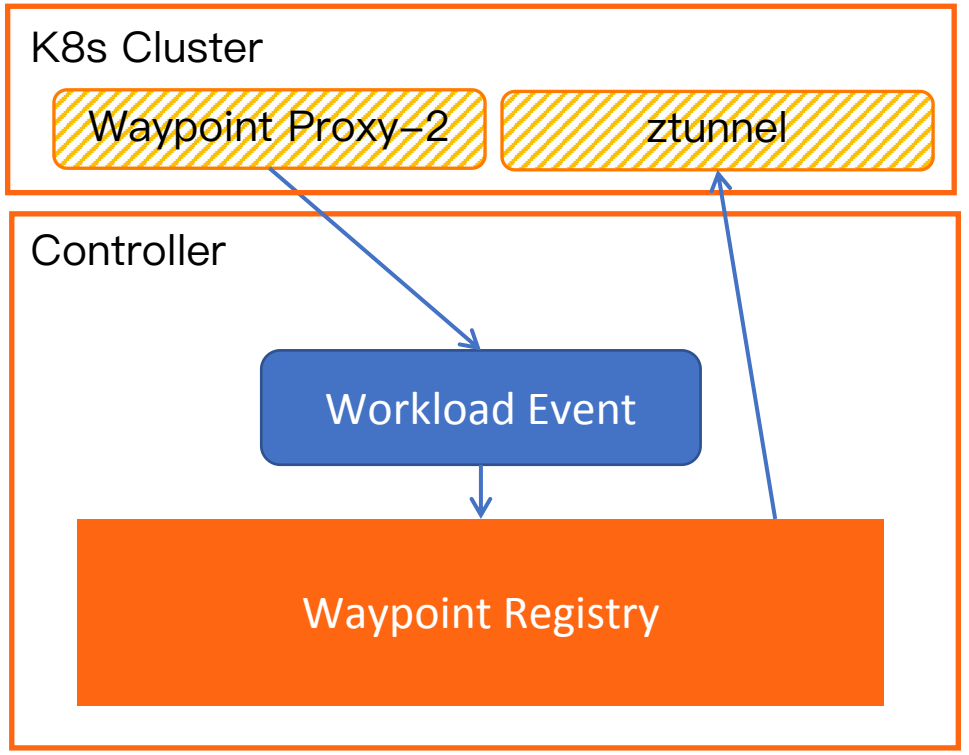

```
{
    "workloadIp": "172.17.0.71",
    "waypointAddresses": [
        "172.17.0.153"
    ],
    "gatewayAddress": null,
    "protocol": "HBONE",
    "name": "helloworld-v1-77dd9697f5-xt7wk",
    "namespace": "default",
    "trustDomain": "cluster.local",
    "serviceAccount": "helloworld",
    "workloadName": "helloworld-v1",
    "workloadType": "deployment",
    "canonicalName": "helloworld",
    "canonicalRevision": "v1",
    "node": "cn-beijing.172.17.0.175",
    "nativeHbone": false,
    "authorizationPolicies": [],
    "status": "Healthy",
    "clusterId": "cbcb410cbf8a44805b065e0dcd1067ee1"
}
```


- L4 proxy cannot be aware of related L7 proxy running on another cluster
- Multiple clusters support issue


```
{
    "workloadIp": "172.17.0.71",
    "waypointAddresses": [],
    "gatewayAddress": null,
    "protocol": "HBONE",
    "name": "helloworld-v1-77dd9697f5-xt7wk",
    "namespace": "default",
    "trustDomain": "cluster.local",
    "serviceAccount": "helloworld",
    "workloadName": "helloworld-v1",
    "workloadType": "deployment",
    "canonicalName": "helloworld",
    "canonicalRevision": "v1",
    "node": "cn-beijing.172.17.0.175",
    "nativeHbone": false,
    "authorizationPolicies": [],
    "status": "Healthy",
    "clusterId": "cbcb410cbf8a44805b065e0dcd1067ee1"
}
```

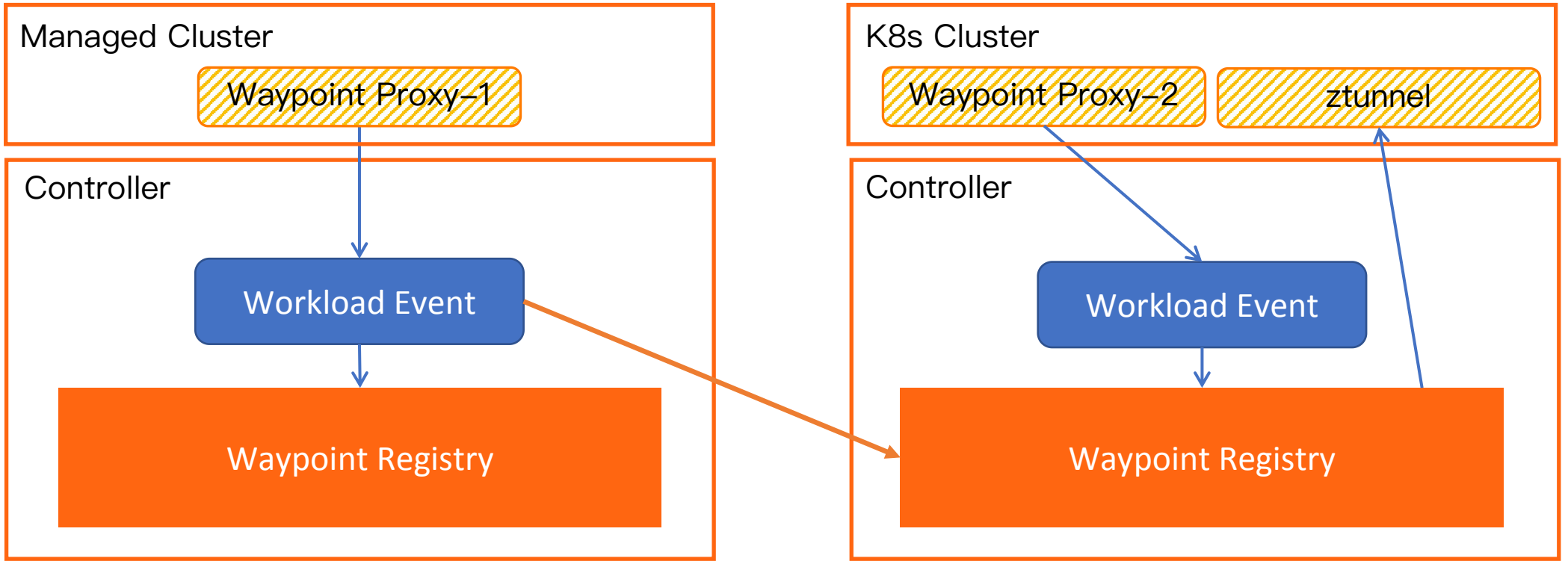
Solution





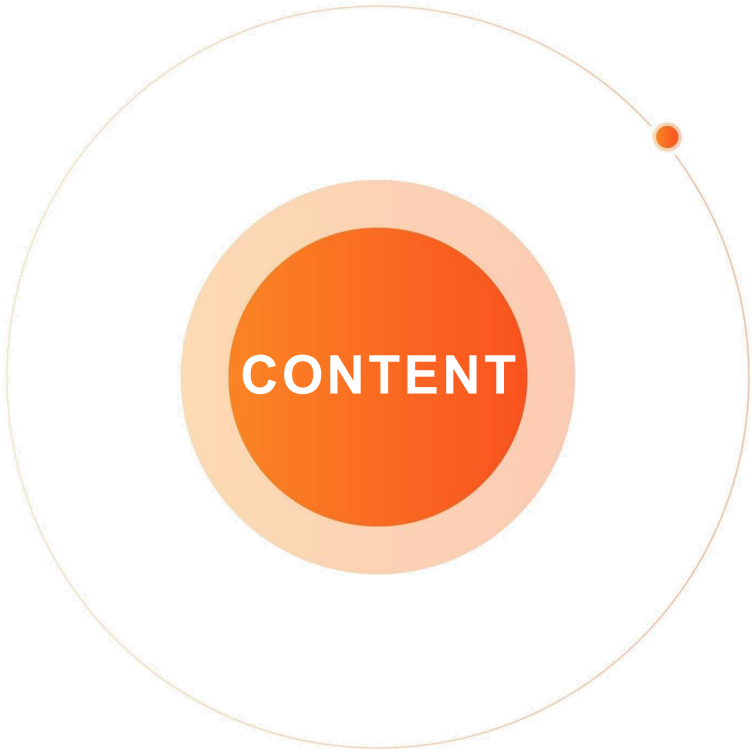
The Istio control plane runs a controller on each cluster and updates the registry when workloads are added or removed. However, the registry between different clusters is not shared.
This means that ztunnel cannot detect Waypoint proxies that are not in the same cluster as itself.

Solution



When the waypoint of the managed cluster starts,
update the Registry in all cluster Controllers and execute the XDS Push

Agenda



① Serverless in Control Plane

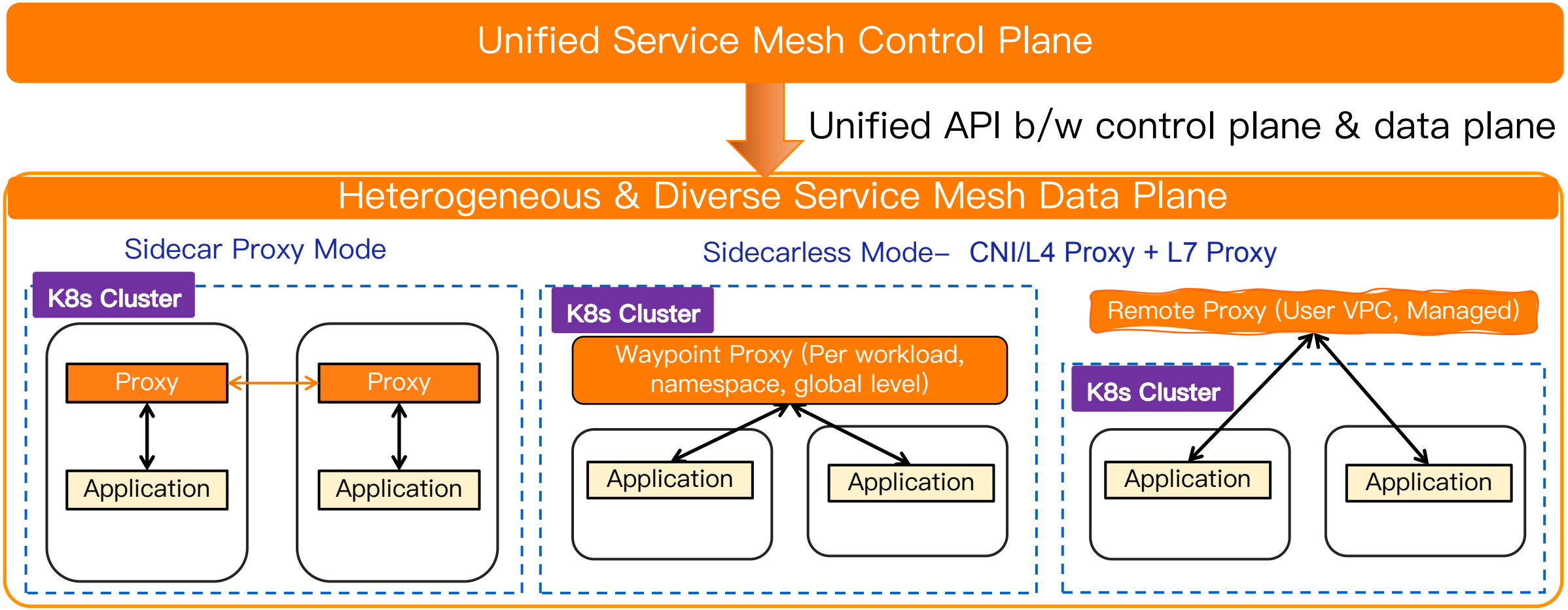
② Serverless support in the data plane with Sidecar mode

③ Serverless support in the data plane with Sidecarless mode

④ Wrap-up

The evolution of Serverless Service Mesh

The fusion of Sidecar Proxy and Sidecarless modes



Diverse data plane forms, supporting a wide range of K8s environments:
(K8s version x form x ECS specifications x OS version)

WWW.ALIYUN.COM