



KubeCon



CloudNativeCon

# OPEN SOURCE SUMMIT

China 2019





KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

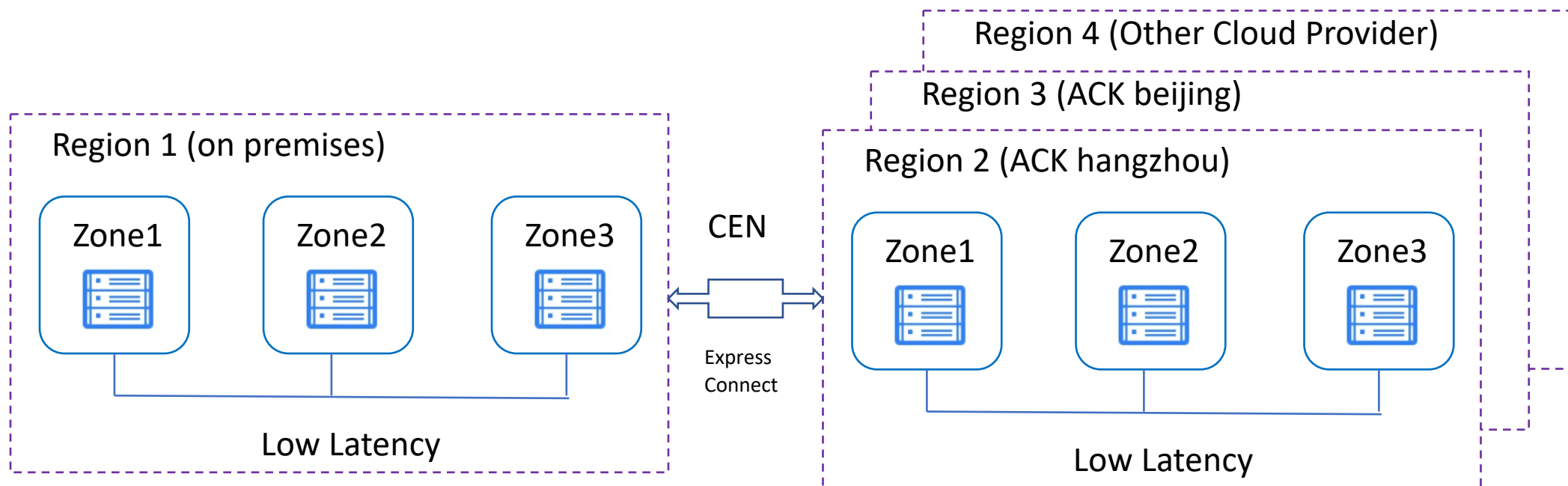
# Using Istio to Manage the Cross-Regional & Cross-Cluster Microservices

Xi Ning Wang(王夕宁), Alibaba Cloud  
Xiao Zhong Liu(刘晓忠), UniCareer



# Why need the multiple regions/clusters?

1. Business Continuity/Disaster Recovery
2. Geographically distributed end users
  - Reduce the access latency
  - Meet local legal and data regulatory compliance
3. Lower barrier to setup the network connectivity b/w regions & clusters



# What does multi-region/cluster mean to ACK?



KubeCon



CloudNativeCon

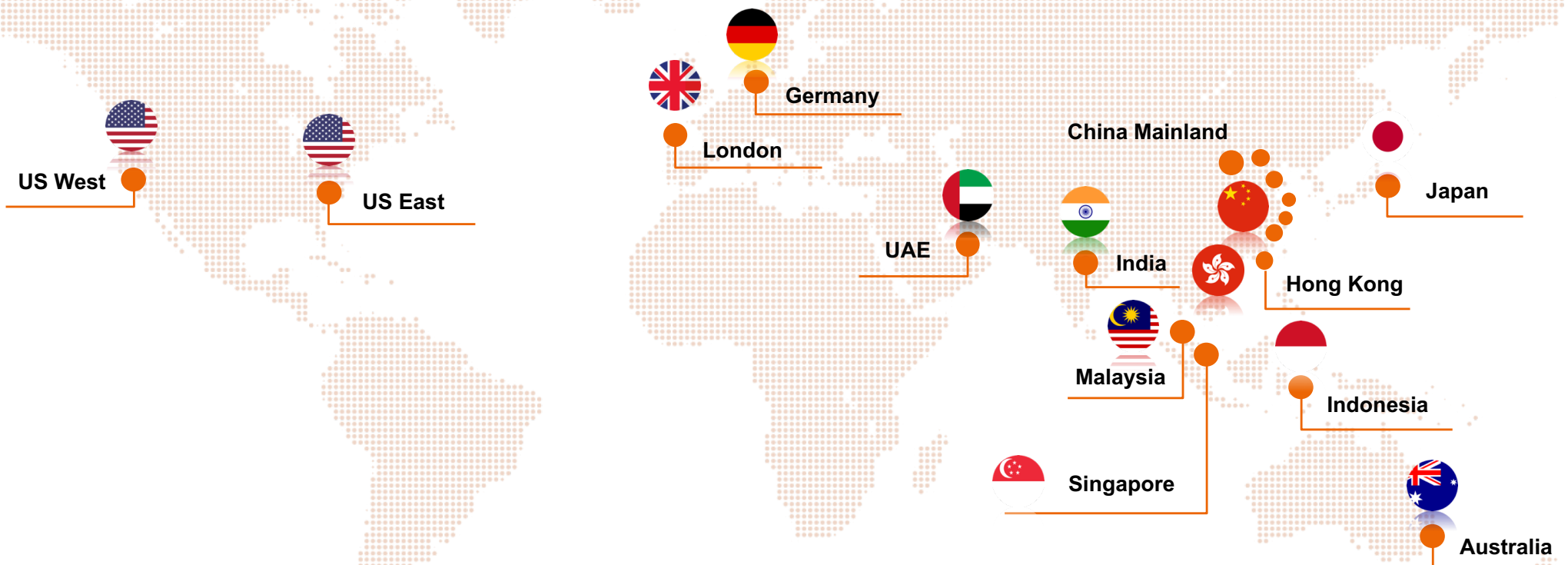


OPEN SOURCE SUMMIT

China 2019

## ACK: Alibaba Container Service for Kubernetes

### Available in 18 Regions





# Istio on ACK



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

Integration with Alibaba Cloud services & open source

Log Service

Tracing Analysis

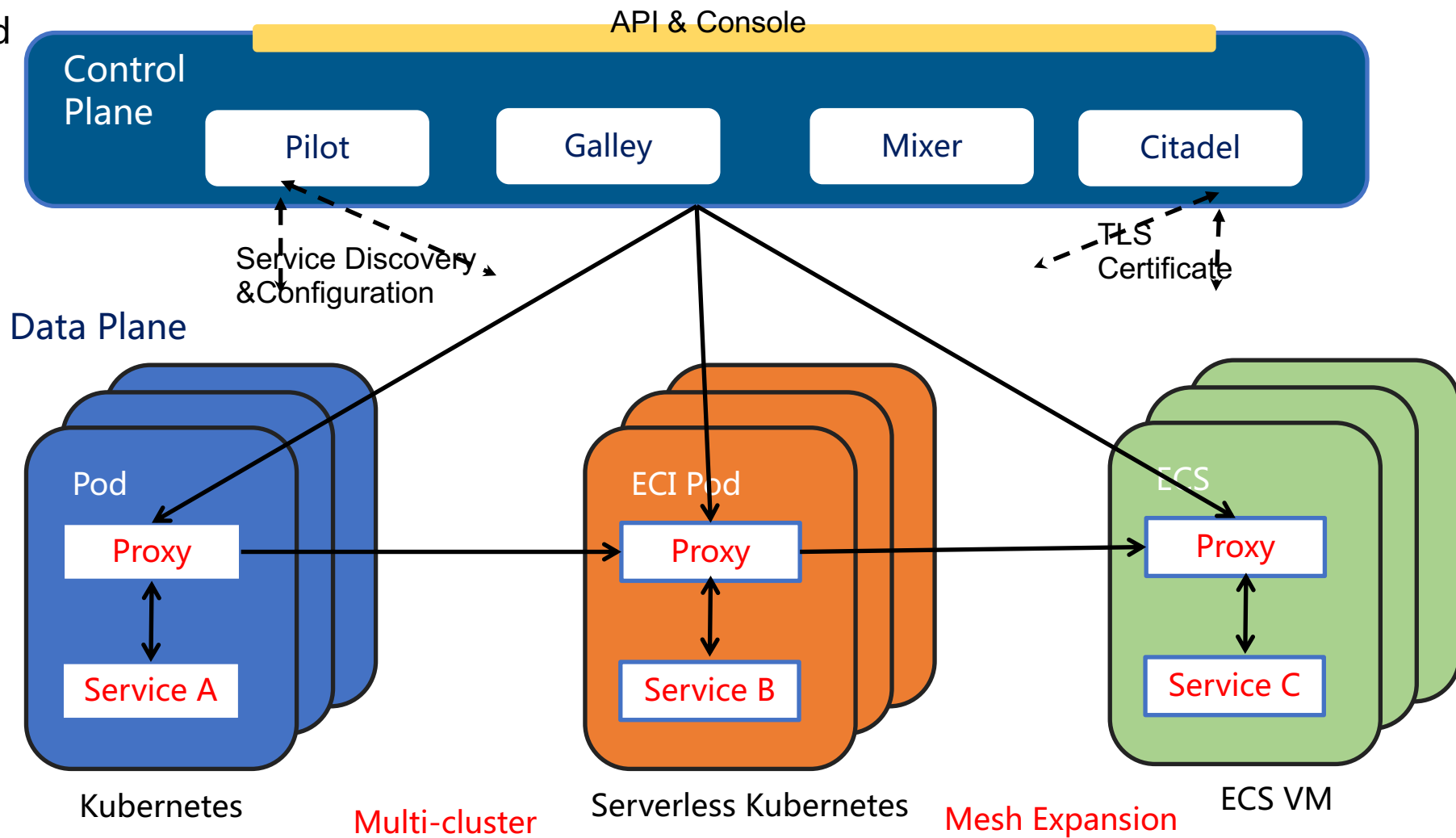
Cloud Monitor

Prometheus+TSDB

Grafana

Kiali

....



# Feature Request for multi-region/cluster

## - Locality based service routing



KubeCon

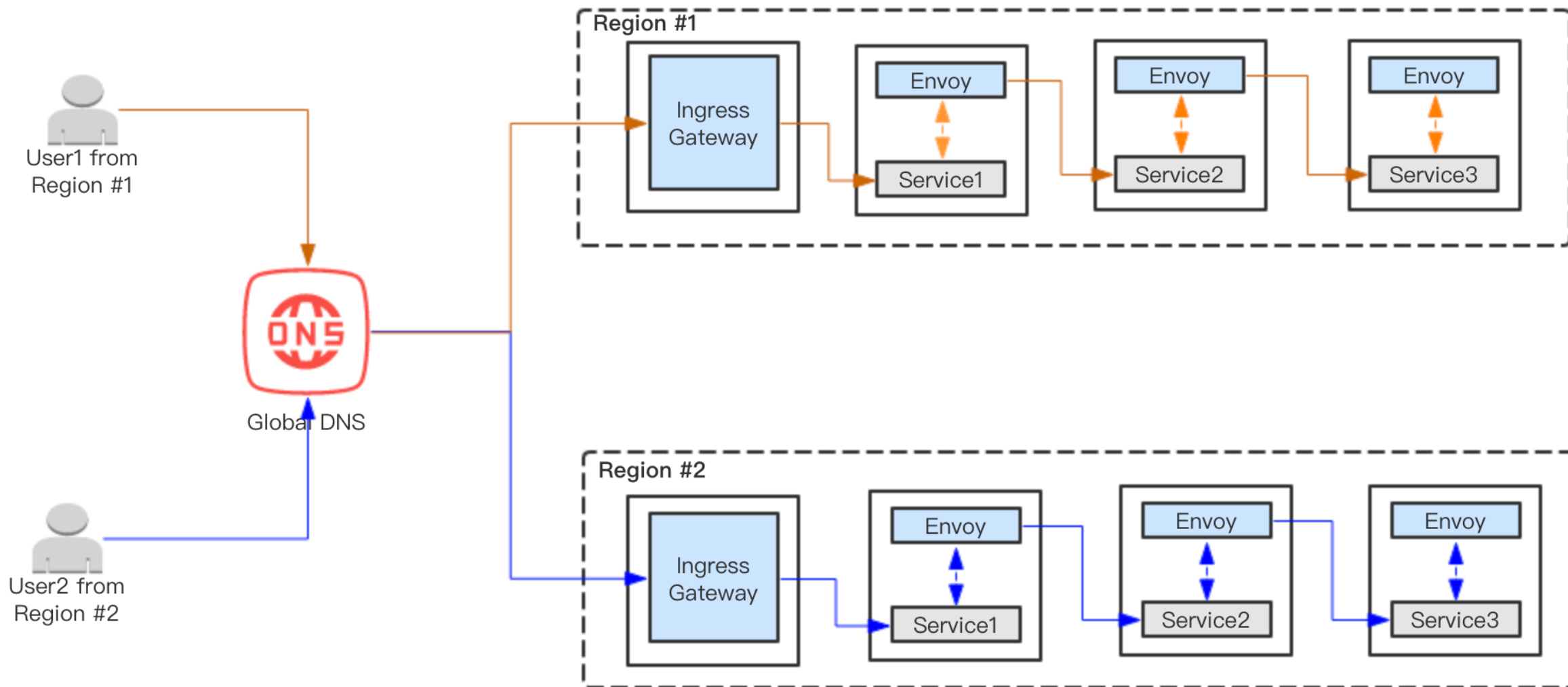


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019



# Feature Request for multi-region/cluster - Automatic Failover



KubeCon

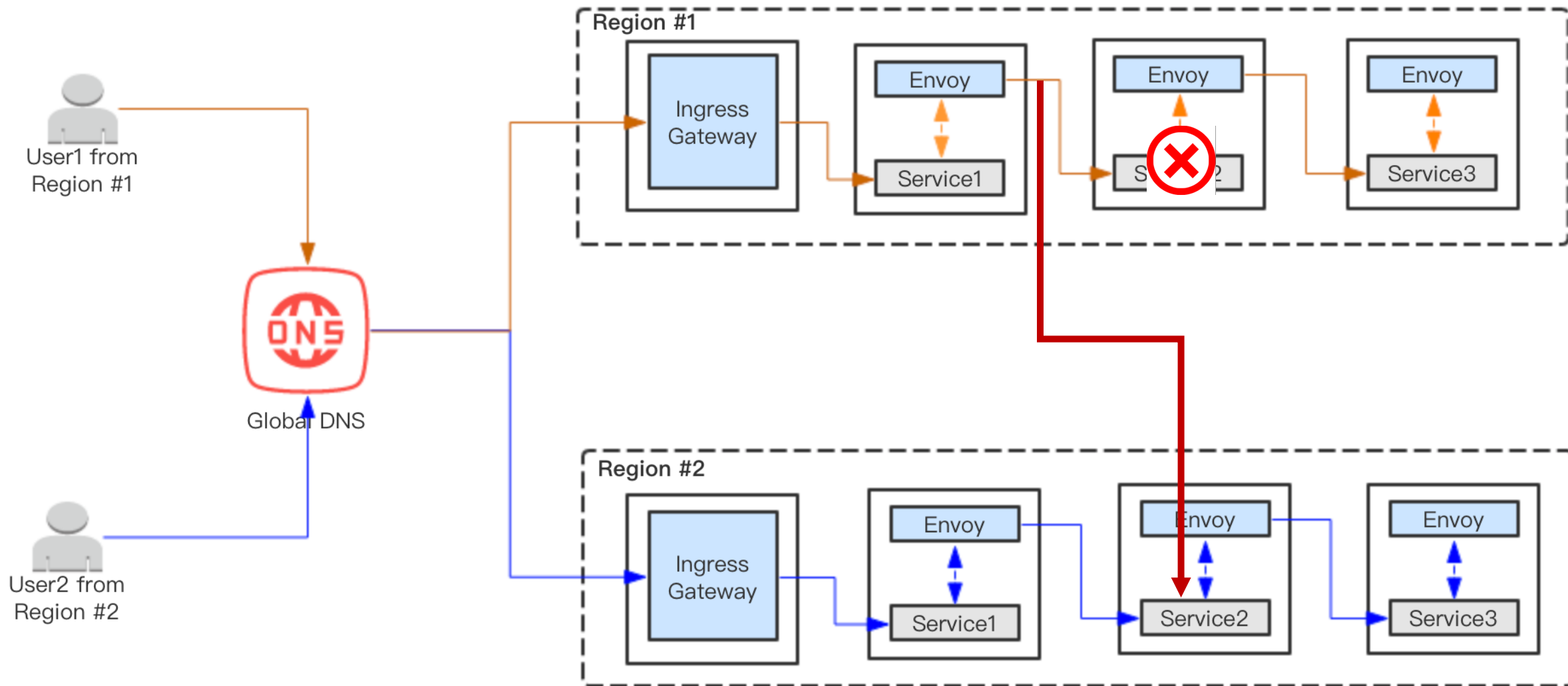


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019









# Istio multi-cluster patterns

	Single Mesh		Mesh Federation
Istio 1.0 * Support for Istio 1.0 ends on June 19th, 2019	<ul style="list-style-type: none"><li>• Single Control Plane</li><li>• Flat network</li><li>• All pod CIDRs in every cluster must be routable to each other</li><li>• Pod/Service CIDR ranges must be unique</li></ul>		
Istio 1.1	<ul style="list-style-type: none"><li>• Same to above in Istio 1.0</li></ul>	<ul style="list-style-type: none"><li>• Single Control Plane</li><li>• No VPN network</li><li>• Inter-connectivity through gateways</li><li>• Pod/Service CIDR ranges may be overlapped</li></ul>	<ul style="list-style-type: none"><li>• Multiple Control Planes</li><li>• No VPN network</li><li>• Inter-connectivity through gateways</li><li>• Pod/Service CIDR ranges may be overlapped</li></ul>



# Simplified Installation and Configuration

 Select resource group ▼ Global  Search Billing Management Enterprise More     English

Container Service - Kubernetes ▼

Overview

Clusters

Clusters

Nodes

Volumes

Namespaces

Authorization

Applications

Deployments

Stateful Sets

Daemon Sets

Jobs

Cron Jobs

Pods

Clusters

managedk8stest1

Namespaces

istio-system

Release Name

istio

Version

1.1.8

Pilot Settings

\* Trace Sampling Percentage (0 to 100)

100

☒ Enable locality based service routing

Control Egress Traffic

Blocked Addresses for External Access

☒ All

Release the address range for external access

This parameter is left empty by default. Use commas (,) to separate multiple addresses.

Gateway settings

☒ Create a default ingress gateway

# Simplified Installation and Configuration (2)



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

## Multi-cluster same control plane mode setting

- ☒ Not enabled
- ☐ Use Flat network or VPN
- ☐ Do not use Flat network or VPN

Step	Status
Pre-Check	pending
Create Istio Resource Definition	pending
Deploy Istio	pending

Deploy Istio



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2019

# Custom Resource for Istio Operator

Each K8s cluster running Istio control plane should have one Istio CR(custom resource)

```

1  apiVersion: istio.alibabacloud.com/v1beta1
2  kind: Istio
3  metadata:
4    labels:
5      controller-tools.k8s.io: "1.0"
6      heritage: Tiller
7      release: istio
8    name: istio-config
9  spec:
10   hub: registry-vpc.cn-hangzhou.aliyuncs.com/aliacs-app
11   version: 1.1.8
12   controlPlaneSecurityEnabled: false
13   mtls:
14     enabled: false
15   security:
16     selfSigned: true
17   meshExpansion:
18     enabled: false
19   includeIPRanges: "*"
20   excludeIPRanges: ""
21   outboundTrafficPolicy:
22     mode: "REGISTRY_ONLY"
23   logging:
24     level: "default:info"
25   dockerImage:
26     region: ""
27   gateways:
28     enabled: true
29   ingress:

```

One RemoteIstio custom resource is created for each remote cluster

```

1  apiVersion: istio.alibabacloud.com/v1beta1
2  kind: RemoteIstio
3  metadata:
4    name: localityaware-bj
5    namespace: istio-system
6  spec:
7    autoInjectionNamespaces:
8      - default
9    dockerImage:
10     region: cn-beijing
11    gateways:
12     enabled: true
13     ingress:
14       - enabled: true
15       k8sIngress: {}
16    hub: registry.cn-beijing.aliyuncs.com/aliacs-app-catalog
17    includeIPRanges: '*'
18    proxy: {}
19    security: {}
20    sidecarInjector:
21     enabled: true
22     replicaCount: 1

```

# Multi-cluster support of Istio on ACK - Flat network



KubeCon

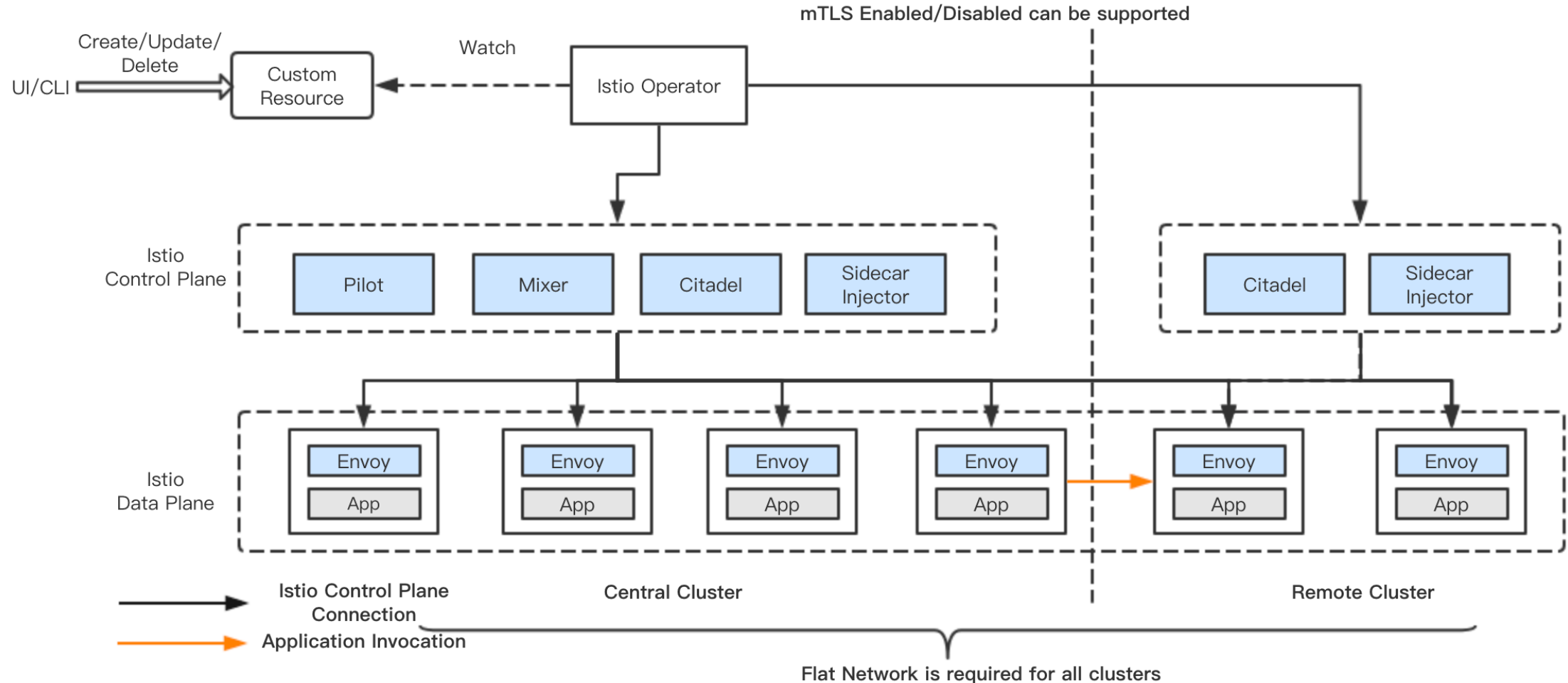


CloudNativeCon



OPEN SOURCE SUMMIT

China 2019





# Multi-cluster support of Istio on ACK - Gateway Connected



KubeCon

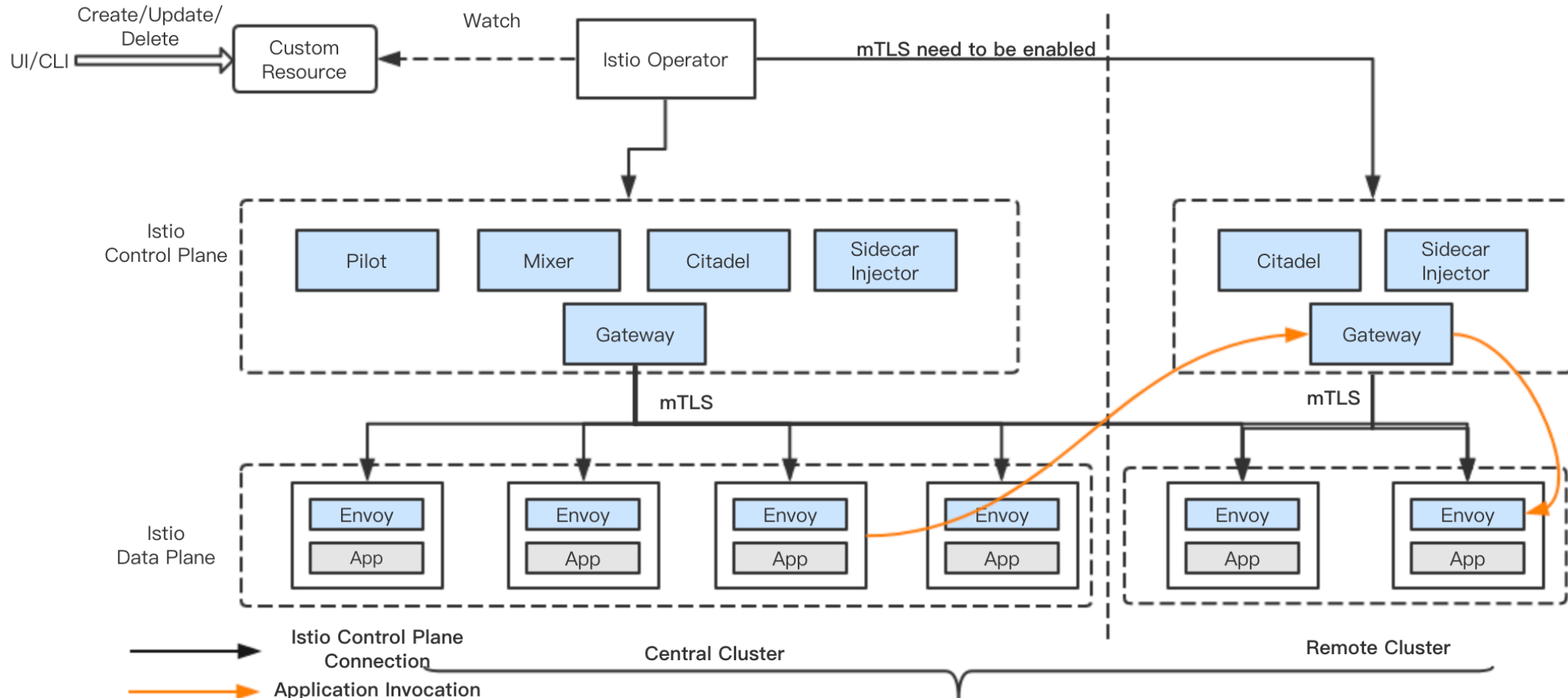


CloudNativeCon



OPEN SOURCE SUMMIT

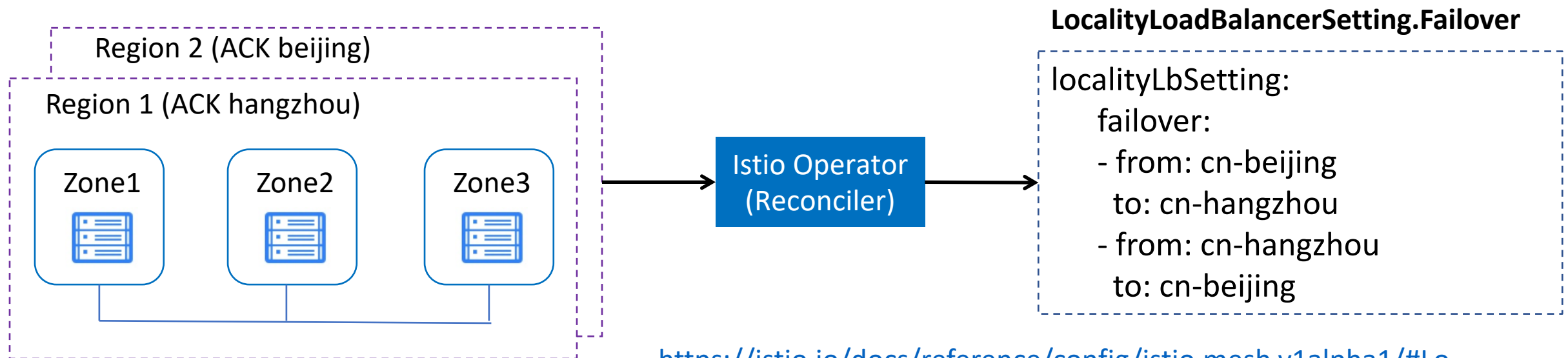
China 2019



1. Flat Network is NOT required for all clusters;
2. Cross cluster mTLS requires one shared Root CA;

# How to enable locality aware & failover?

- Kubernetes reserves the following labels for Nodes:
  - failure-domain.beta.kubernetes.io/region
  - failure-domain.beta.kubernetes.io/zone
- Automatically retrieve the regions and zones info, and populate the preferred failover regions if no specific region is provided



<https://istio.io/docs/reference/config/istio.mesh.v1alpha1/#LocalityLoadBalancerSetting-Failover>

# Customer Case Reference - Unicareer

## Business Scenario

- Serving global users including China Mainland, America, Europe and Australia, etc.
- No dedicated operations team.
- Need one easy-to-use microservice management solution for our full chain of web apps

## Key Problems

- Stable high latency across regions.
- Occasional extreme latency due to cross regional network fluctuation.
- Existing K8s Ingress is weak and inconvenient.
- Multiple programming languages support.
- Decouple application logic from service infrastructure.
- Need to integrate with K8s ecosystem.

# Services running on cross-regional K8s clusters



KubeCon

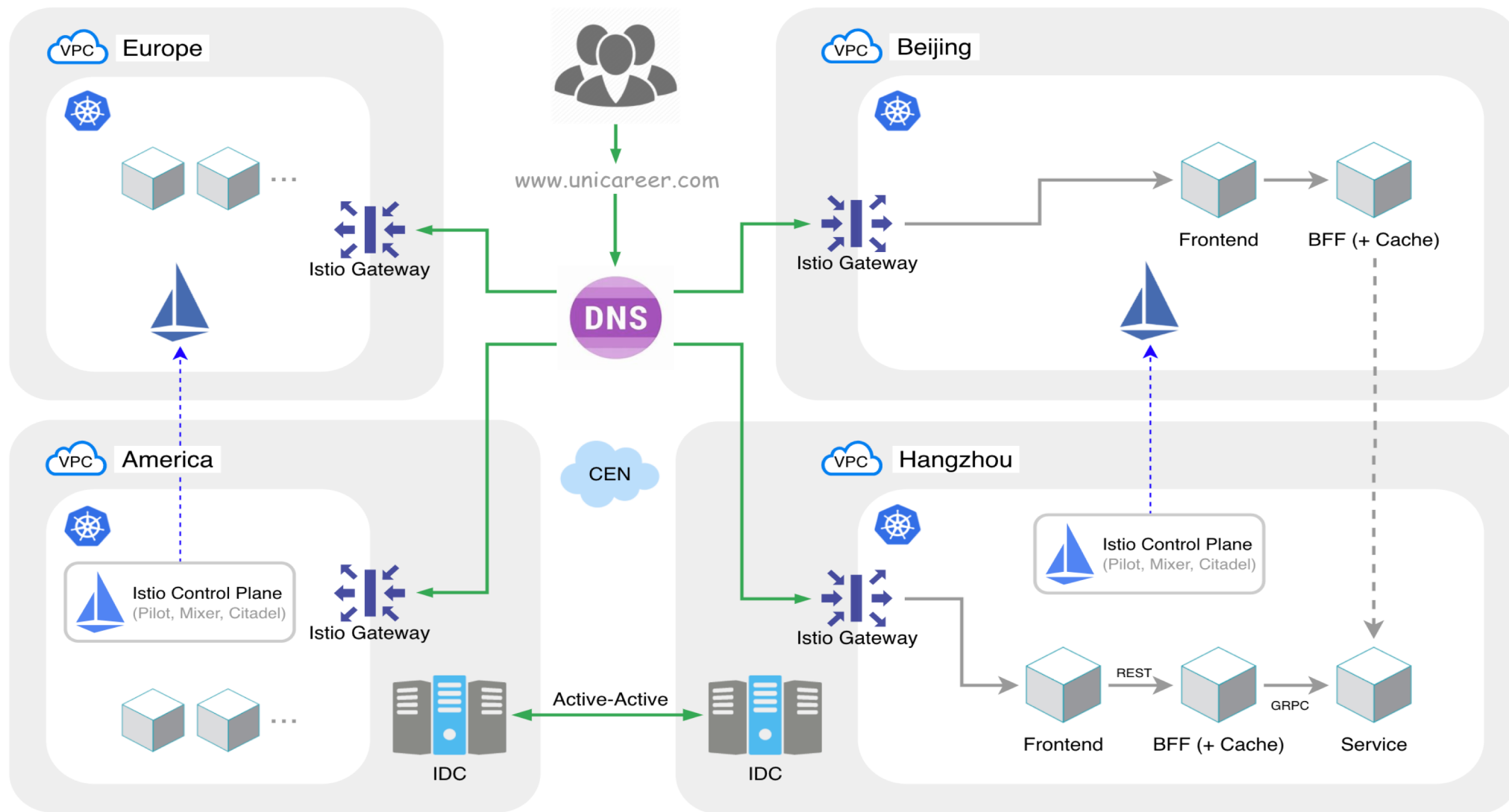


CloudNativeCon



OPEN SOURCE SUMMIT

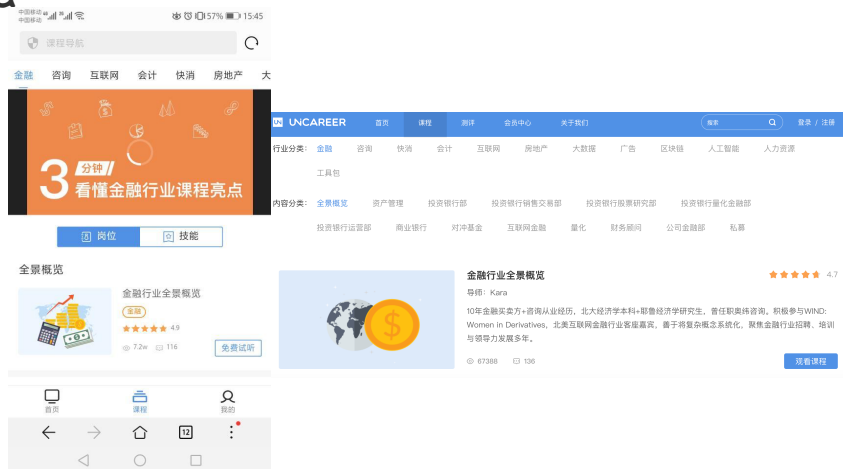
China 2019





# Quick Demo

## North China



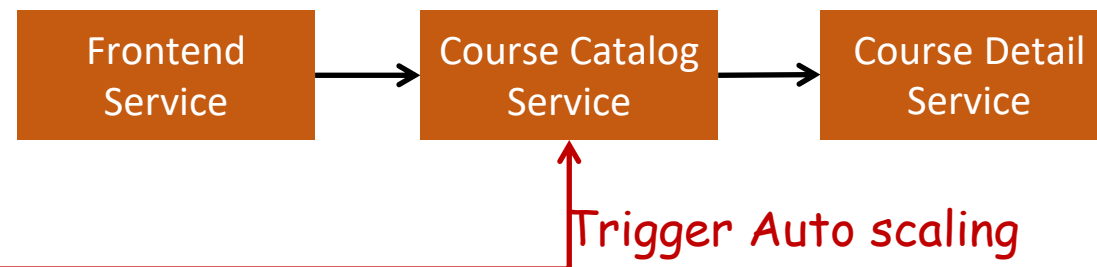
Unicarrer Online Course Service  
running on ACK Beijing Region



## South China



Unicarrer Online Course Service  
running on ACK Hangzhou Region



# Benefits from Istio on ACK



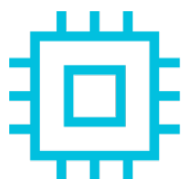
Simplify the Istio deployment and operation, etc.



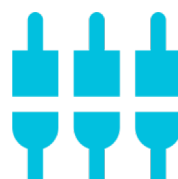
Integrated E2E observability with Alibaba Cloud services



Improved user experience for common scenarios, e.g. canary release, etc.



Assisted problem determination  
- Automatic configuration checking and recovery



Unified traffic management for hybrid-cloud, multi-cloud, and cloud migration



Compatible with open source community

# Recap

Phase 1

Phase 2

Phase 3

Phase 4

Basic Install & Minor Upgrade

Seamless Upgrades

Full Integration & Lifecycle

Auto Pilot



ACK Istio Operator

- Automated provision and configuration management
- ACK provides one-click UI page to simplify the configuration

- Seamless upgrades supported
- ACK provides one-click mode to upgrade

- Istio community version does not cover storage management and maintenance
- ACK provides the full integration with Alibaba Cloud services including storage, tracing, logging, etc.

- ACK provides automatic config tuning, abnormal detection and recovery
- ACK provides the multi-cluster management using CRD



KubeCon



CloudNativeCon

**OPEN SOURCE SUMMIT**

China 2019

