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?

ACK: Alibaba Container Service for Kubernetes

Available in 18 Regions
Istio on ACK

Integration with Alibaba Cloud services & open source

- Log Service
- Tracing Analysis
- Cloud Monitor
- Prometheus+TSDB
- Grafana
- Kiali
- ...

API & Console

Control Plane
- Pilot
- Galley
- Mixer
- Citadel

Service Discovery & Configuration

Data Plane

Pod
- Proxy
- Service A

Kubernetes

Multi-cluster

ECI Pod
- Proxy
- Service B

Serverless Kubernetes

Mesh Expansion

ECS
- Proxy
- Service C

ECS VM
Feature Request for multi-region/cluster - Locality based service routing

- Region #1
  - Ingress Gateway
  - Envoy
  - Service1
  - Envoy
  - Service2
  - Envoy
  - Service3

- Region #2
  - Ingress Gateway
  - Envoy
  - Service1
  - Envoy
  - Service2
  - Envoy
  - Service3

User1 from Region #1

User2 from Region #2

Global DNS
Feature Request for multi-region/cluster - Automatic Failover
## Istio multi-cluster patterns

<table>
<thead>
<tr>
<th></th>
<th>Single Mesh</th>
<th>Mesh Federation</th>
</tr>
</thead>
</table>
| **Istio 1.0**  | • Single Control Plane  
• Flat network  
• All pod CIDRs in every cluster must be routable to each other  
• Pod/Service CIDR ranges must be unique                      |                                                                                |
| * Support for  |                                                                                |                                                                                |
| Istio 1.0 ends |                                                                                |                                                                                |
| on June 19th,  |                                                                                |                                                                                |
| 2019           |                                                                                |                                                                                |
| **Istio 1.1**  | • Same to above in Istio 1.0                                                  | • Single Control Plane  
• No VPN network  
• Inter-connectivity through gateways  
• Pod/Service CIDR ranges may be overlapped                      |
|                |                                                                                | • Multiple Control Planes  
• No VPN network  
• Inter-connectivity through gateways  
• Pod/Service CIDR ranges may be overlapped                      |
## Multi-cluster same control plane mode setting

- [ ] Not enabled
- [ ] Use Flat network or VPN
- [ ] Do not use Flat network or VPN

<table>
<thead>
<tr>
<th>Step</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Check</td>
<td>pending</td>
</tr>
<tr>
<td>Create Istio Resource Definition</td>
<td>pending</td>
</tr>
<tr>
<td>Deploy Istio</td>
<td>pending</td>
</tr>
</tbody>
</table>
Each K8s cluster running Istio control plane should have one Istio CR (custom resource)

One RemoteIstio custom resource is created for each remote cluster
Multi-cluster support of Istio on ACK - Flat network

Custom Resource

Istio Operator

Create/Update/Delete
UI/CLI

Watch

Istio Operator

Pilot

Mixer

Citadel

Sidecar Injector

mTLS Enabled/Disabled can be supported

Istio Control Plane

Istio Data Plane

Envoy

App

Envoy

App

Envoy

App

Envoy

App

Envoy

App

Envoy

App

Envoy

App

Istio Control Plane

Central Cluster

Remote Cluster

Istio Control Plane Connection

Application Invocation

Flat Network is required for all clusters
Multi-cluster support of Istio on ACK - Gateway Connected

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

Istio Operator (Reconciler)

Region 1 (ACK hangzhou)
Region 2 (ACK beijing)

LocalityLoadBalancerSetting.Failover

```
localityLbSetting:
  failover:
    - from: cn-beijing
      to: cn-hangzhou
    - from: cn-hangzhou
      to: cn-beijing
```

https://istio.io/docs/reference/config/istio.mesh.v1alpha1/#LocalityLoadBalancerSetting-Failover
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
Quick Demo

North China

Unicarrer Online Course Service running on ACK Beijing Region

South China

Unicarrer Online Course Service running on ACK Hangzhou Region

Frontend Service → Course Catalog Service → Course Detail Service

Frontend Service → Course Catalog Service → Course Detail Service

Trigger Auto scaling
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
• 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