servicecomb-mesher Documentation

The Apache Software Foundation

Jan 04, 2022

User Documentations

CHAPTER 1

Introductions

1.1 What is mesher

Mesher is a service mesh implementation based on go chassis. So it has all the features of go chassis like service discovery, load balancing, fault tolerance, route management,distributed tracing etc. it makes your service become resilient and observable.

1.2 Concepts

1.2.1 Sidecar

Mesher leverages distributed design pattern, sidecar to work along with service.

1.2.2 go chassis

Mesher is a light weight sidecar proxy developed on top of go-chassis, so it has the same concepts with it and it has all features of go chassis

1.2.3 Destination Resolver

Destination Resolver parses request into a service name

1.2.4 Source Resolver

Source resolver gets remote IP and based on remote IP, it provides a standard way for the applications to create media sources.

1.2.5 Admin API

Admin API listens on isolated port, it gives a way to interact with mesher

CHAPTER 2

Get started

2.1 Before you start

Before you start, you must know what you gonna do if you use mesher as your sidecar proxy.

Assume you launched 2 services, each of service has a dedicated mesher as sidecar proxy.

The network traffic will be: ServiceA->mesherA->mesherB->ServiceB.

To run mesher along with your services, you need to set minimum configurations as below:

1. Give mesher your service name in microservice.yaml file
2. Set service discovery service(service center, Istio etc) configurations in chassis.yaml
3. Export HTTP_PROXY=http://127.0.0.1:30101 as your service runtime environment
4. (optional) Give mesher your service port list by ENV SERVICE_PORTS or CLI –service-ports

After the configurations, assume you serviceB is listening at 127.0.0.1:8080.

The serviceA must use http://ServiceB:8080/{api_path} to access ServiceB.

Now you can launch as many as serviceA and serviceB to make this system become a distributed system.

Notice:

> Consumer need to use http://provider_name:provider_port/ to access provider, instead of http://provider_ip:provider_port/. if you choose to set step4, then you can simply use http://provider_name/ to access provider.

2.2 Quick start

2.2.1 Local

In this case, you will launch one mesher sidecar proxy and one service developed with go-chassis as provider and use curl as a dummy consumer to access this service

The network traffic: curl->mesher->service

1. Install ServiceComb service-center
2. Install go-chassis and run rest server
3. Build and run, use go mod(go 1.11+, experimental but a recommended way)

```
cd mesher
GO111MODULE=on go mod download
#optional
GO111MODULE=on go mod vendor
go build mesher.go
./mesher
```

4. Verify, in this case curl command is the consumer, mesher is consumer's sidecar, and rest server is provider

```
export http_proxy=http://127.0.0.1:30101
curl http://RESTServer:8083/sayhello/peter
```

Notice:

> You don't need to set service registry in chassis.yaml, because by default registry address is 127.0.0.1:30100, just same service center default listen address.
>
> curl command read lower case http_proxy environment variable.

2.2.2 Run on different infrastructures

Mesher does not bind to any platform or infrastructure, please refer to https://github.com/go-mesh/mesher-examples/tree/master/Infrastructure to know how to run mesher on different infrastructures

2.2.3 Sidecar injector

Mesher supply a way to automatically inject mesher configurations in kubernetes

See detail https://github.com/go-chassis/sidecar-injector

CHAPTER 3

User guides

3.1 Mesher command Line

When you start a mesher process, you can use mesher command line to specify configurations as follows:

```
mesher --config=mesher.yaml --service-ports=rest:8080
```

3.1.1 Options

–config

(optional, string) The path to mesher configuration file, default value is {current_bin_work_dir}/conf/mesher.yaml

–mode

(optional, string) Mesher has 2 work modes, sidecar and edge, default is sidecar

–service-ports

(optional, string) Running as sidecar, mesher needs to know local service ports, this is to tell mesher service port list, The value format is {protocol}-{suffix} or {protocol}. If service has multiple protocols, you can separate with comma "rest-admin:8080, grpc:9000", default is empty. In that case mesher will use header X-Forwarded-Port as local service port, if header X-Forwarded-Port is also empty, mesher can not communicate to your local service.

3.2 Profile Mesher

Mesher has a convenience way to enable go pprof, so that you can easily analyze the performance of mesher.

3.2.1 Configurations

```
pprof:
  enable: true
  listen: 127.0.0.0.1:6060
```

enable

(optional, bool) Default is false

listen

(optional, string) Listen IP and port

3.3 Admin API

3.3.1 Configurations

Admin API server leverages protocol server, it listens on isolated port. By default admin is enabled, and default value of goRuntimeMetrics is false.

To start API server, set protocol server config in chassis.yaml:

```
cse:
   protocols:
     rest-admin:
       listenAddress: 0.0.0.0:30102  # listen addr for admin API
```

Tune admin api in mesher.yaml:

```
admin:
  enable: true
```

admin.enable

(optional, bool) Default is false

3.4 Local Health check

You can use health checker to check local service health. When service instance is unhealthy, mesher will update the instance status in registry service to "DOWN" so that other services can not discover this instance. After the service becoming healthy again, mesher will update the status to "UP", then other instance can discover it again. Currently this function works only when using service center as registry.

Examples:

- Check local http service

```
localHealthCheck:
  - port: 8080
    protocol: rest
    uri: /health
    interval: 30s
    match:
```

(continues on next page)

(continued from previous page)

```
      status: 200
      body: ok
```

3.4.1 Options

port

(require, string) Must be a port number, mesher is only responsible to check local services, it use 127.0.0.1:{port} to check services.

protocol

(optional, string) Mesher has a built-in checker "rest",for other protocols, will use default TCP checker unless implementing your own checker.

uri

(optional, string) Uri start with /.

interval

(optional, string) Check interval, you can use number with unit: 1m, 10s.

match.status

(optional, string) The http response status must match status code.

match.body

(optional, string) The http response body must match body.

3.5 Destination Resolver

Destination Resolver is a module to parse each protocol request to get a target service name. You can write your own resolver implementation for different protocols.

3.5.1 Configurations

Example:

```
plugin:
  destinationResolver:
    http: host # host is a build-in and default resolver, it uses host name as␣
↪service name
    grpc: ip
```

plugin.destinationResolver

(optional, map) Define what kind of resolver, a protocol should use

3.6 API gateway

Mesher is able to work as a API gateway to mange traffic, to run mesher as an API gateway:

```
mesher --config=mesher.yaml --mode edge
```

The ingress rule is in mesher.yaml.

3.6.1 Options

mesher.ingress.type

(optional, string) Default is servicecomb, it reads servicecomb ingress rule. It is a plugin, you can custom your own implementation.

mesher.ingress.rule.http

(optional, string) Rule about how to forward http traffic. It holds a yaml content as rule.

Below explaining the content, the rule list is like a filter, all the request will go through this rule list until matching one rule.

apiPath

(required, string) If request's url matches this, it will use this rule.

host

(optional, string) If request HOST matches this, mesher will use this rule. It can be empty. If you set both host and apiPath, the request's host and api path must match them both.

service.name

(required, string) Target back-end service name in registry service (like ServiceComb service center).

service.redirectPath

(optional, string) By default, mesher uses original request's url.

service.port.value

(optional, string) If using java chassis or go chassis to develop back-end service, no need to set it. But if back-end service uses mesher-sidecar, service port must be given here.

3.6.2 example

```
mesher:
  ingress:
    type: servicecomb
    rule:
      http: |
        - host: example.com
          apiPath: /some/api
          service:
            name: example
            redirectPath: /another/api
            port:
              name: http-legacy
              value: 8080
        - apiPath: /some/api
          service:
            name: Server
            port:
```

(continues on next page)

(continued from previous page)

```
            name: http
            value: 8080
```

3.6.3 Enable TLS

Generate private key

```
openssl genrsa -out server.key 2048
```

Sign cert with private key

```
openssl req -new -x509 -key server.key -out server.crt -days 3650
```

Set file path in chassis.yaml

```
ssl:
  mesher-edge.rest.Provider.certFile: server.crt
  mesher-edge.rest.Provider.keyFile: server.key
```

To know advanced feature about TLS configuration, check https://docs.go-chassis.com/user-guides/tls.html

CHAPTER 4

Development guides

mesher is an out of box service mesh and API gateway component, you can use them by simply setting configuration files. But some of user still need to customize a service mesh or API gateway. For example:

- API gateway need to query account system and do the authentication and authorization.
- mesher need to access cloud provider API
- mesher use customized control panel
- mesher use customized config server

4.1 Handler chain

All the traffic will go through the handler chain. A chain is composite of handlers, each handler has a particular logic. Mesher also has lots of feature working in chain, like route management, circuit breaking and rate-limiting. In Summary, handler is the middle ware between clients and servers, it is useful when adding authorization to intercept illegal requests.

4.1.1 How to write a handler

https://docs.go-chassis.com/dev-guides/how-to-implement-handler.html

4.1.2 How to use it in handler chain

In chassis.yaml add your handler name in chain configuration. As sidecar and API gateway, mesher's chain has different meanings.

For example, running as mesher-sidecar, service A call another service B, outgoing chain of service A processes all the service A requests before remote call, incoming chain of service B processes all the requests from service A, before access to service B API.

In summary, outgoing chain works when a service attempt to call other services, incoming chain works when other services call this service.

```
  handler:
    chain:
      Consumer:
        # if a service call other service, it go through this chain, loadbalance and␣
↪transport is must
        outgoing: router, bizkeeper-consumer, loadbalance, transport
      Provider:
        incoming: ratelimiter-provider
```

Running as API gateway, incoming chain processes all the requests from the external network, outgoing chain processes all the the requests between API gateway and back-end services.

```
  handler:
    chain:
      Consumer:
        #loadbalance and transport is must
        outgoing: router, bizkeeper-consumer, loadbalance, transport
      Provider:
        incoming: ratelimiter-provider
```

4.2 Cloud Provider

By default Mesher do not support any cloud provider. But there is plugin that helps mesher do it.

4.2.1 Huawei Cloud

Mesher is able to use huawei cloud ServiceComb engine.

4.2.1.1 Access ServiceComb Engine API

Import auth in cmd/mesher/mesher.go

```
import _ "github.com/huaweicse/auth/adaptor/gochassis"
```

It will sign all requests from mesher to ServiceComb Engine.

4.2.1.2 Use Config Center to manage configuration

Mesher uses servicecomb-kie as config server,

```
_ "github.com/apache/servicecomb-kie"
```

When you need to use ServiceComb Engine, you must replace this line. Import config center in cmd/mesher/mesher.go.

```
_ "github.com/go-chassis/go-chassis/v2-config/configcenter"
```

Set the config center in chassis.yaml

```
config:
  client:
    serverUri: https://xxx #endpoint of servicecomb engine
    refreshMode: 1 # 1: only pull config.
    refreshInterval: 30 # unit is second
    type: config_center
```

4.3 Build mesher

You need to build and release your mesher after customization.

4.3.1 Build binary

You can refer to build/build_proxy to see how we build mesher binary and docker image.

build/docker/proxy/Dockerfile is a example about making a docker image

CHAPTER 5

Protocols

5.1 gRPC Protocol

Mesher support gRPC protocol

5.1.1 Configurations

To enable gRPC proxy you must set the protocol config

```
cse:
  protocols:
    grpc:
      listenAddress: 127.0.0.1:40101 # or internalIP:port
```

5.1.2 How to use mesher as sidecar proxy

Assume you original client is

```
        conn, err := grpc.Dial("10.0.1.1:50051",
                grpc.WithInsecure(),
                )
```

Set http_proxy:

```
export http_proxy=http://127.0.0.1:40100
```

5.1.3 Example

A gRPC example is here

CHAPTER 6

Use Istio as control plane

6.1 Get started

Istio Pilot can be configured as the service discovery component for mesher. By default the Pilot plugin is not compiled into mesher binary. To make mesher work with Pilot, import the plugin in mesher's entrypoint source code:

```
import _ "github.com/apache/servicecomb-mesher/plugins/registry/istiov2"
```

Then the Pilot plugin will be installed when mesher starts. Next step, configure Pilot as service discovery in `chassis.yaml`:

```
cse:
  service:
    registry:
      registrator:
        disabled: true
      serviceDiscovery:
        type: pilotv2
        address: grpc://istio-pilot.istio-system:15010
```

Since mesher doesn't have to register the service to Pilot, the registrator config item should be disabled. Make serviceDiscovery.type to be pilotv2, to get service information by xDS v2 API (the v1 API is deprecated).

6.1.1 The routing tags in Istio

In the original mesher configuration, user can specify tag based route rules, as described below:

```
## router.yaml
router:
  infra: cse
routeRule:
  targetService:
```

(continues on next page)

(continued from previous page)

```
    - precedence: 2
      route:
      - tags:
          version: v1
        weight: 40
      - tags:
          version: v2
          debug: true
        weight: 40
      - tags:
          version: v3
        weight: 20
```

Then in a typical Istio environment, which is likely to be Kubernetes cluster, user can specify the DestinationRules for targetService with the same tags:

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: targetService
spec:
  host: targetService
  subsets:
  - name: v1
    labels:
      version: v1
  - name: v2
    labels:
      version: v2
      debug: "true"
  - name: v3
    labels:
      version: v3
```

Notice that the subsets' tags are the same with those in `router.yaml`, then mesher's tag based load balancing strategy works as it originally does.

6.2 Discovery

6.2.1 Introduction

Istio Pilot can be integrated with Mesher, working as the Service Discovery component.

6.2.2 Configuration

edit chassis.yaml.

registrator.disabled

> Must disable registrator, because registrator is is used in client side discovery. mesher leverage server side discovery which is supported by kubernetes

serviceDiscovery.type

specify the discovery plugin type to "pilotv2", since Istio removes the xDS v1 API support from version 0.7.1, type "pilot" is deprecated.

serviceDiscovery.address

the pilot address, in a typical Istio environment, pilot usually listens on the grpc port 15010.

6.2.3 examples

```
cse: # Using xDS v2 API
  service:
    Registry:
      registrator:
        disabled: true
      serviceDiscovery:
        type: pilotv2
        address: grpc://istio-pilot.istio-system:15010
```

6.3 Route Rule

Instead of using CSE and route config to manage routes, mesher supports Istio as a control plane to set route rules and follows the envoy API reference to manage routes. This page gives the examples to show how requests are routed between micro services.

6.3.1 Mesher Configurations

In **Consumer** router.yaml, you can set router.infra to define which router plugin mesher fetches from. The default router.infra is cse, which means the route rule comes from route config in CSE config-center. If router.infra is set to be pilotv2, the router.address is necessary, such as the in-cluster istio-pilot grpc address.

Notice that `infra: pilot` is deprecated since Istio removes the xDS v1 API from 0.7.1

```
router:
  infra: pilotv2 # pilotv2 or cse
  address: grpc://istio-pilot.istio-system:15010
```

In **Both** consumer and provider registry configurations, the recommended one shows below.

```
cse:
  service:
    registry:
      registrator:
        disabled: true
      serviceDiscovery:
        type: pilotv2
        address: grpc://istio-pilot.istio-system:15010
```

6.3.2 Kubernetes Configurations

The provider applications of v1, v2 and v3 version could be deployed in kubernetes cluster as **Deployment** with differenent labels. The labels of version are necessary now, and you need to set env to generate nodeID in Istio system,

such as **POD_NAMESPACE, POD_NAME** and **INSTANCE_IP**.

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  labels:
    version: v1
    app: pilot
    name: istioserver
  name: istioserver-v1
  namespace: default
spec:
  progressDeadlineSeconds: 600
  replicas: 1
  revisionHistoryLimit: 10
  selector:
    matchLabels:
      app: pilot
      version: v1
      name: istioserver
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 1
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: pilot
        version: v1
        name: istioserver
    spec:
      containers:
      - image: gosdk-istio-server:latest
        imagePullPolicy: Always
        name: istioserver-v1
        ports:
        - containerPort: 8084
          protocol: TCP
        resources: {}
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
        env:
        - name: CSE_SERVICE_CENTER
          value: grpc://istio-pilot.istio-system:15010
        - name: POD_NAME
          valueFrom:
            fieldRef:
              apiVersion: v1
              fieldPath: metadata.name
        - name: POD_NAMESPACE
          valueFrom:
            fieldRef:
              apiVersion: v1
              fieldPath: metadata.namespace
        - name: INSTANCE_IP
          valueFrom:
            fieldRef:
```

(continues on next page)

(continued from previous page)

```
            apiVersion: v1
            fieldPath: status.podIP
      volumeMounts:
      - mountPath: /etc/certs/
        name: istio-certs
        readOnly: true
    dnsPolicy: ClusterFirst
    initContainers:
    restartPolicy: Always
    schedulerName: default-scheduler
    securityContext: {}
    terminationGracePeriodSeconds: 30
    volumes:
    - name: istio-certs
      secret:
        defaultMode: 420
        optional: true
        secretName: istio.default
```

6.3.3 Istio v1alpha3 Router Configurations

Traffic-management gives references and examples of Istio new route rule schema. First, subsets is defined according to labels. Then you can set route rules of different weights for virtual services.

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: istioserver
spec:
  host: istioserver
  subsets:
  - name: v1
    labels:
      version: v1
  - name: v2
    labels:
      version: v2
  - name: v3
    labels:
      version: v3
```

NOTICE: The subsets only support labels of version to distinguish different virtual services, this constrains will be canceled later.

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: istioserver
spec:
  hosts:
    - istioserver
  http:
  - route:
    - destination:
        host: istioserver
```

(continues on next page)

(continued from previous page)

```
        subset: v1
      weight: 25
    - destination:
        host: istioserver
        subset: v2
      weight: 25
    - destination:
        host: istioserver
        subset: v3
      weight: 50
```

6.4 Egress

6.4.1 Introduction

Mesher support Egress for your service, so that you can access any publicly accessible services from your microservices.

6.4.2 Configuration

The egress related configurations are all in egress.yaml.

infra

(optional, string) Specifies from where the egress configuration need to be taken supports two values CSE or pilot , CSE means the egress configurations from egress.yaml file, pilot means egress configurations are taken from pilot of Istio, default is *CSE*.

address

(optional, string) The end point of pilot from which configuration need to be fetched.

hosts

(optional, []string) Host associated with external service, could be a DNS name with wildcard prefix.

ports.port

(optional, int) The port associated with the external service, default is *80*.

ports.protocol

(optional, int) The protocol associated with the external service, supports only HTTP, default is *HTTP*.

6.4.3 Example

Edit egress.yaml

```
egress:
  infra: cse  # pilot or cse
  address: http://istio-pilot.istio-system:15010
egressRule:
  google-ext:
    - hosts:
```

(continues on next page)

(continued from previous page)

```
    - "www.google.com"
    - "*.yahoo.com"
  ports:
    - port: 80
      protocol: HTTP
```

CHAPTER 7

Sidcar-injector Deployment and Usage

7.1 Introduction

Sidecar is a way to run alongside your service as a second process. The role of the sidecar is to augment and improve the application container, often without the application container's knowledge.

sidecar is a pattern of "Single-node, multi container application".

This pattern is particularly useful when using kubernetes as container orchestration platform. Kubernetes uses pods. A pod is composed of one or more application containers. A sidecar is a utility container in the pod and its purpose is to support the main container. It is important to note that standalone sidecar doesnot serve any purpose, it must be paired with one or more main containers. Generally, sidecar container is reusable and can be paired with numerous type of main containers.

For design pattern please refer

Container Design Pattern

Example: The main container might be a web server, and it might be paired with a "logsaver" sidecar container that collects the web server's logs from local disk and streams them to a cluster.

7.2 Injection

Two types

1. Manual sidecar injection
2. Automatic sidecar injection

7.3 Manual sidecar injection

In manual sidecar injection user has to provide sidecar information in deployment.

```
kubectl get deployment client -o wide
NAME      DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE       CONTAINERS
client    1         1         1            1           13s       client,mesher
```

7.4 Automatic sidecar injection

Sidecars can be automatically added to applicable Kubernetes pods using

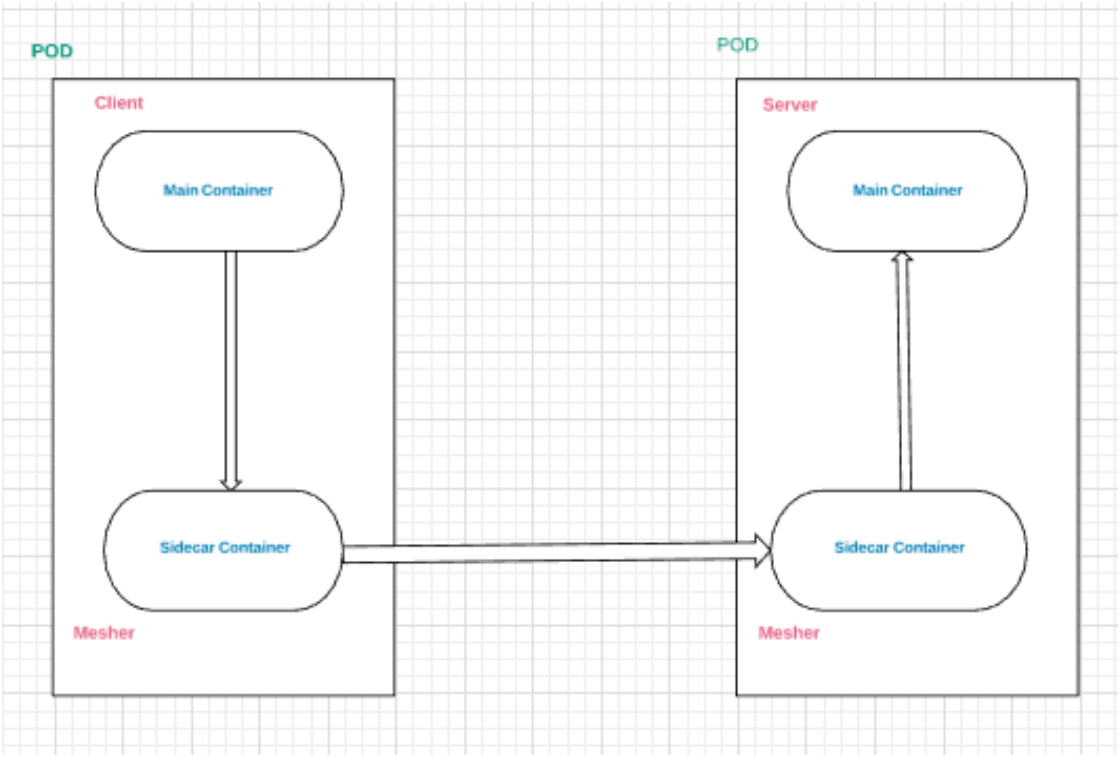
mutating webhook admission controller Note that unlike manual injection, automatic injection occurs at the pod-level. You won't see any change to the deployment itself.

Verify

7.5 How it works

sidecar will deploy along side with main container as shown below

The figure shows the client and server communication using mesher as a sidecar.



Explanation:

Mesher is deployed as a sidecar along with main container of server and client in a pod.

client and server will implement some rest api's and functionalities like loadbalance, circuit-breaker, fault-injection, routerule, discovery etc... will be provided by mesher(sidecar).

workflow:

user/curl——>client(main container)——>mesher(sidecar container)——>mesher(sidecar container)——>server(main container).

7.6 Deployment Of Sidecar-Injector

Prerequisites

Quick start

Use below links to build and Install sidecar

build install

7.7 Annotations

Refer k8s document

Annotation

7.8 Deployment of application

The Sidecar-injector will automatically inject mesher containers into your application pods.

Following are the annotations used to inject mesher sidecar into the user pod

1. sidecar.mesher.io/inject:

   The allowed values are “yes” or “y”

   If “yes” or “y” provided the sidecar will inject in the main container. If not, sidecar will not inject in the main container.

2. sidecar.mesher.io/discoveryType:

   The allowed values are “sc” and “pilot”

   If value is “sc” it will use serviecComb service-center as a registry and discovery. If value is “pilot” it will use the istio pilot as a discovery.

3. sidecar.mesher.io/servicePorts:

   serviceports are the port values of actual main server container append with “rest or grps”

   ex: sidecar.mesher.io/servicePorts: rest:9999

Required annotation for client and server sidecar.mesher.io/inject:

Optional annotation for client and server sidecar.mesher.io/discoveryType:

Optional annotation for server sidecar.mesher.io/servicePorts:

7.9 Prerequisites before deploying application

Label the chassis namespace with sidecar-injector=enabled

kubectl label namespace chassis sidecar-injector=enabled

kubectl get namespace -L sidecar-injector

```
NAME          STATUS    AGE       SIDECAR-INJECTOR
default       Active    18h
kube-public   Active    18h
kube-system   Active    18h
chassis       Active    3m        enabled
```

7.10 Usage of istio

To use istio following are the required annotation to be given in client and server yaml file sidecar.mesher.io/inject: “yes” and sidecar.mesher.io/discoveryType:”pilot”

Example to use pilot registry

deploy the examples using kubectl command line

kubectl create -f <filename.yaml> -n chassis

7.11 Usage of serviceComb

To use service-center following are the required annotation to be given in client and server yaml file sidecar.mesher.io/inject: “yes” and sidecar.mesher.io/discoveryType:”sc”

Example to use sc registry

deploy the examples using kubectl command line

kubectl create -f <filename.yaml> -n chassis

7.12 Verification

Follow