

Istio - Sidecar and Service Entry

Linus
2020/7/1

Outline

- Environment
- SSHD container dockfile
- SSHD pod yaml
- SSHD service yaml
- Minikube service list
- Add sidecar manually
- Sidecar yaml
- Service Entry yaml
- Result

Environment

- Host: CentOS 7
 - docker
 - kubectl
 - istioctl
- Minikube in KVM2
 - # minikube config set driver kvm2
- Local Docker Registry
 - <https://10.206.79.138/>
 - #minikube start --insecure-registry=[]

SSHD container dockfile

```
FROM centos:centos6
```

```
MAINTAINER Linus Chien <linus_chien@commscope.com>
```

```
RUN yum install -y openssh-server
```

```
# setup root's password
```

```
RUN echo 'root:root' | chpasswd
```

```
# SSH login fix. Otherwise user is kicked off after login
```

```
RUN sed 's@session\s*required\s*pam_loginuid.so@session  
optional pam_loginuid.so@g' -i /etc/pam.d/sshd
```

```
# init SSH keys
```

```
RUN /sbin/service sshd start && /sbin/service sshd stop
```

```
EXPOSE 22
```

```
CMD ["/usr/sbin/sshd", "-D"]
```

SSHD pod yaml

```
apiVersion: v1
kind: Pod
metadata:
  name: sshd-pod
  labels:
    app: sshd-pod
spec:
  containers:
    - name: sshd
      image: 10.206.79.138/linus:sshd
      ports:
        - containerPort: 22
```

SSHD service yaml

```
apiVersion: v1
kind: Service
metadata:
  name: sshd-service
spec:
  selector:
    app: sshd-pod
  ports:
    - protocol: TCP
      port: 22
  type: LoadBalancer
```

Minikube service list

NAMESPACE	NAME	TARGET PORT	URL
default	kubernetes	No node port	
default	sshd-service	22	http://192.168.39.92:32523
istio-system	grafana	No node port	
istio-system	istio-egressgateway	No node port	
istio-system	istio-ingressgateway	status-port/15020	http://192.168.39.92:31683
		http2/80	http://192.168.39.92:32697
		https/443	http://192.168.39.92:30104
		tcp/31400	http://192.168.39.92:30280
		tls/15443	http://192.168.39.92:31426
istio-system	istiod	No node port	
istio-system	jaeger-agent	No node port	
istio-system	jaeger-collector	No node port	
istio-system	jaeger-collector-headless	No node port	
istio-system	jaeger-query	No node port	
istio-system	kiali	No node port	
istio-system	prometheus	No node port	
istio-system	tracing	No node port	
istio-system	zipkin	No node port	
kube-system	kube-dns	No node port	

Add sidecar manually

- `# istioctl kube-inject -f pod.yaml | kubectl apply -f -`

NAME	READY	STATUS	RESTARTS	AGE
sshd-pod	2/2	Running	0	22h

Sidecar yaml

```
kind: Sidecar
metadata:
  name: no-ip-tables
  namespace: default
spec:
  workloadSelector:
    labels:
      app: sshd-pod
  egress:
    - port:
        number: 8888
        protocol: TCP
        name: egress
      captureMode: NONE # not needed if metadata is set for
entire proxy
      bind: 127.0.0.1
      hosts:
        - "*/mysql.foo.com"
```

Service Entry yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: external-http
spec:
  hosts:
    - mysql.foo.com
  # addresses:
  # - 127.0.0.1/32 # VIPs
  ports:
    - number: 8888
      name: https
      protocol: TCP
  location: MESH_EXTERNAL
  resolution: DNS
  endpoints:
    - address: www.google.com
      ports:
        https: 443
```

Result

- `ssh root@192.168.39.92 -p 32523 -L 7777:127.0.0.1:8888`
- `curl -k https://localhost:7777/`

```
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 404 (Not Found)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-
    serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-
    height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px
    no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a
    img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-
    right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png)
    no-repeat;margin-left:-5px}@media only screen and (min-
    resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150
    x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-
    image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only
    screen and (-webkit-min-device-pixel-
    ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png)
    no-repeat;-webkit-background-size:100% 100%}}#logo{display:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>404.</b> <ins>That's an error.</ins>
  <p>The requested URL <code></code> was not found on this server. <ins>That's all we know.</ins>
```

Q&A