1. Istio
2. 文件
3. 参考
4. 组态
5. 交通管理
6. 边门

边门

9分钟阅读

Sidecar描述了sidecar代理的配置，该代理调解与其连接的工作负载实例的入站和出站通信。默认情况下，Istio将为网格中的所有边车代理编程，使其具有到达网格中每个工作负载实例所需的必要配置，并接受与工作负载关联的所有端口上的流量。Sidecar资源提供了一种微调端口集的方法，代理在向工作负载转发流量或从工作负载转发流量时将接受的协议。此外，可以限制代理在从工作负载实例转发出站流量时可以达到的服务集。

网格中的服务和配置被组织成一个或多个名称空间（例如，Kubernetes名称空间或CF组织/空间）。命名空间中的Sidecar资源将应用于使用workloadSelector选择的同一命名空间中的一个或多个工作负载实例。如果没有workloadSelector，它将应用于同一名称空间中的所有工作负载实例。在确定要应用于工作负载实例的Sidecar资源时，将优先使用通过Sidecar资源选择此工作负载实例的workloadSelector的资源，而不使用任何workloadSelector。

注意：*每个命名空间只能有一个Sidecar资源，没有任何工作负载选择器*。如果给定命名空间中存在多个无选择器的Sidecar资源，则系统的行为是不确定的。如果具有工作负载选择器的两个或多个Sidecar资源选择相同的工作负载实例，则系统的行为是不确定的。

下面的示例在prod-us1命名空间中声明了Sidecar资源，该资源配置命名空间中的sidecars以允许出口流量到prod-us1，prod-apis和istio-system命名空间中的公共服务。

```
apiVersion: networking.istio.io/v1alpha3
kind: Sidecar
metadata:
  name: default
  namespace: prod-us1
spec:
  egress:
  - hosts:
    - "prod-us1/*"
    - "prod-apis/*"
    - "istio-system/*"
```

下面的示例在prod-us1命名空间中声明了一个Sidecar资源，该资源接受端口9080上的入站HTTP流量，并将其转发到在Unix域套接字上侦听的连接工作负载实例。在出口方向上，除了istio-system名称空间之外，sidecar仅代理为prod-us1名称空间中的服务绑定到端口9080的HTTP流量。

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: Sidecar
metadata:
  name: default
  namespace: prod-us1
spec:
  ingress:
  - port:
      number: 9080
      protocol: HTTP
      name: somename
    defaultEndpoint: unix:///var/run/someuds.sock
  egress:
  - hosts:
    - "istio-system/*"
  - port:
      number: 9080
      protocol: HTTP
      name: egresshttp
    hosts:
    - "prod-us1/*"
```

如果在没有基于IPTables的流量捕获的情况下部署工作负载，则Sidecar资源是配置连接到工作负载实例的代理上的端口的唯一方法。以下示例在prod-us1名称空间中为所有标签“app：productpage”属于productpage.prod-us1服务的pod声明了Sidecar资源。假设这些pod是在没有IPtable规则的情况下部署的（即Istio init容器），并且代理元数据ISTIO *META* INTERCEPTION_MODE设置为NONE，则下面的规范允许此类pod在端口9080上接收HTTP流量并将其转发到侦听127.0的应用程序.0.1：8080。它还允许应用程序与127.0.0.1:3306上的后备MySQL数据库进行通信，然后在mysql.foo.com:3306上代理到外部托管的MySQL服务。

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: Sidecar
metadata:
  name: no-ip-tables
  namespace: prod-us1
spec:
  workloadSelector:
    labels:
      app: productpage
  ingress:
  - port:
      number: 9080 # binds to 0.0.0.0:9080
      protocol: HTTP
      name: somename
    defaultEndpoint: 127.0.0.1:8080
    captureMode: NONE # not needed if metadata is set for entire proxy
  egress:
  - port:
      number: 3306
      protocol: MYSQL
      name: egressmysql
    captureMode: NONE # not needed if metadata is set for entire proxy
    bind: 127.0.0.1
    hosts:
    - "*/mysql.foo.com"
```

以及用于路由到mysql.foo.com:3306的相关服务条目

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: external-svc-mysql
  namespace: ns1
spec:
  hosts:
  - mysql.foo.com
  ports:
  - number: 3306
    name: mysql
    protocol: MYSQL
  location: MESH_EXTERNAL
  resolution: DNS
```

还可以在单个代理中混合和匹配流量捕获模式。例如，考虑内部服务位于192.168.0.0/16子网上的设置。因此，在VM上设置IP表以捕获192.168.0.0/16子网上的所有出站流量。假设VM在172.16.0.0/16子网上具有用于入站流量的附加网络接口。以下Sidecar配置允许VM在172.16.1.32:80（VM的IP）上公开侦听器，以获取从172.16.0.0/16子网到达的流量。请注意，在此方案中，VM中代理上的ISTIO *META* INTERCEPTION_MODE元数据应包含“REDIRECT”或“TPROXY”作为其值，这意味着基于IP表的流量捕获处于活动状态。

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: Sidecar
metadata:
  name: partial-ip-tables
  namespace: prod-us1
spec:
  workloadSelector:
    labels:
      app: productpage
  ingress:
  - bind: 172.16.1.32
    port:
      number: 80 # binds to 172.16.1.32:80
      protocol: HTTP
      name: somename
    defaultEndpoint: 127.0.0.1:8080
    captureMode: NONE
  egress:
    # use the system detected defaults
    # sets up configuration to handle outbound traffic to services
    # in 192.168.0.0/16 subnet, based on information provided by the
    # service registry
  - captureMode: IPTABLES
    hosts:
    - "*/*"
```

CaptureMode

CaptureMode描述了如何捕获到侦听器的流量。仅在侦听器绑定到IP时才适用。

名称	描述

名称	描述
DEFAULT	环境定义的默认捕获模式
IPTABLES	使用IPtables重定向捕获流量
NONE	没有流量捕获。在egress listener中使用时，应用程序应该与侦听器端口/ unix域套接字明确通信。在ingress侦听器中使用时，需要注意确保侦听器端口未被主机上的其他进程使用。

IstioEgressListener

IstioEgressListener指定附加到工作负载实例的sidecar代理上的出站流量监听器的属性。

领域	类型	描述
port	Port1	与侦听器关联的端口。如果使用Unix域套接字，请使用0作为端口号，并使用有效的协议。端口（如果已指定）将用作与导入的主机关联的默认目标端口。如果省略端口，Istio将根据导入的主机推断侦听器端口。请注意，当指定多个出口侦听器时，其中一个或多个侦听器具有特定端口而其他侦听器没有端口，则侦听器端口上公开的主机将基于具有最特定端口的侦听器。
bind	string	应该绑定侦听器的ip或Unix域套接字。如果bind不为空，则必须指定端口。格式：x.x.x.x或 unix:///path/to/uds或 unix://@foobar（Linux抽象命名空间）。如果省略，Istio将根据导入的服务，应用此配置的工作负载实例以及captureMode自动配置默认值。如果captureMode为NONE，则bind将默认为127.0.0.1。
captureMode	CaptureMode	当绑定地址是IP时，captureMode选项指示如何捕获（或不捕获）到侦听器的流量。对于Unix域套接字绑定，captureMode必须为DEFAULT或NONE。

领域	类型	描述
hosts	string[]	必需：侦听器以namespace/dnsName格式显示的一个或多个服务主机。dnsName将公开指定命名空间匹配中的服务。相应的服务可以是服务注册表中的服务（例如，Kubernetes或云代工服务）或使用ServiceEntry或VirtualService配置指定的服务。DestinationRule还将使用相同名称空间中的任何关联。 在dnsName应该使用FQDN格式指定，可选地包括在通配符最左边的组件（例如，prod/*.example.com）。设置dnsNameto *以从指定的命名空间中选择所有服务（例如，prod/*）。该namespace还可以设置为*选择从任何可用的命名空间的特定服务（例如，“* / foo.example.com”）。 注意：只能引用导出到sidecar命名空间的服务和配置工件（例如，exportTo值*）。私有配置（例如，exportTo设置为.）将不可用。请参阅exportTo在设置VirtualService， DestinationRule以及ServiceEntry配置的详细信息。

IstioIngressListener

IstioIngressListener指定附加到工作负载实例的sidecar代理上的入站流量监听器的属性。

领域	类型	描述
port	Port1	需要。与侦听器关联的端口。如果使用Unix域套接字，请使用0作为端口号，并使用有效的协议。
bind	string	应该绑定侦听器的ip或Unix域套接字。格式：x.x.x.x或unix:///path/to/uds或unix://@foobar（Linux抽象命名空间）。如果省略，Istio将根据导入的服务和应用此配置的工作负载实例自动配置默认值。
captureMode	CaptureMode	当绑定地址是IP时，captureMode选项指示如何捕获（或不捕获）到侦听器的流量。对于Unix域套接字绑定，captureMode必须为DEFAULT或NONE。
defaultEndpoint	string	必需：应将流量转发到的环回IP端点或Unix域套接字。此配置可用于将到达边车上绑定点的流量重定向到应用程序工作负载实例正在侦听连接的端口或Unix域套接字。格式应为127.0.0.1:PORT或unix:///path/to/socket

边门

领域	类型	描述
`workloadSelector`	WorkloadSelector	用于选择应该应用此边车配置的特定pod / VM集的标准。如果省略，则sidecar配置将应用于同一名称空间中的所有工作负载实例。
`ingress`	IstioIngressListener[]	Ingress指定边车的配置，用于处理连接的工作负载实例的入站流量。如果省略，Istio将根据从业务流程平台获得的工作负载信息（例如，公开的端口，服务等）自动配置边车。如果已指定，则当且仅当工作负载实例与服务关联时，才会配置入站端口。
`egress`	IstioEgressListener[]	Egress指定边车的配置，用于处理从连接的工作负载实例到网格中的其他服务的出站流量。如果省略，Istio将自动配置边车，以便能够到达此命名空间可见的网格中的每个服务。

WorkloadSelector

WorkloadSelector指定用于确定Gateway或Sidecar资源是否可以应用于代理的标准。匹配标准包括与代理相关联的元数据，工作负载实例信息（例如附加到pod / VM的标签）或代理在初始握手期间提供给Istio的任何其他信息。如果指定了多个条件，则所有条件都需要匹配，以便选择工作负载实例。目前，仅支持基于标签的选择机制。

领域	类型	描述
`labels`	`map<string, string>`	必需：一个或多个标签，指示应该应用此边车配置的特定pod / VM集合。标签搜索的范围仅限于资源所在的配置命名空间。

Links

1. https://istio.io/docs/reference/config/networking/v1alpha3/gateway.html#Port