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

网关

8分钟阅读

`Gateway`描述了在接收传入或传出HTTP / TCP连接的网状网边缘操作的负载平衡器。规范描述了应该公开的一组端口，要使用的协议类型，负载平衡器的SNI配置等。

例如，以下网关配置设置代理以充当负载平衡器，为入口公开端口80和9080（http），443（https），9443（https）和端口2379（TCP）。网关将应用于在带有标签的pod上运行的代理`app: my-gateway-controller`。虽然Istio将配置代理以侦听这些端口，但用户有责任确保允许这些端口的外部流量进入网状网。

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: my-gateway
  namespace: some-config-namespace
spec:
  selector:
    app: my-gateway-controller
  servers:
  - port:
      number: 80
      name: http
      protocol: HTTP
    hosts:
    - uk.bookinfo.com
    - eu.bookinfo.com
    tls:
      httpsRedirect: true # sends 301 redirect for http requests
  - port:
      number: 443
      name: https-443
      protocol: HTTPS
    hosts:
    - uk.bookinfo.com
    - eu.bookinfo.com
    tls:
      mode: SIMPLE # enables HTTPS on this port
      serverCertificate: /etc/certs/servercert.pem
      privateKey: /etc/certs/privatekey.pem
  - port:
      number: 9443
      name: https-9443
      protocol: HTTPS
    hosts:
    - "bookinfo-namespace/*.bookinfo.com"
    tls:
      mode: SIMPLE # enables HTTPS on this port
      credentialName: bookinfo-secret # fetches certs from Kubernetes secret
  - port:
      number: 9080
      name: http-wildcard
      protocol: HTTP
    hosts:
    - "*"
  - port:
      number: 2379 # to expose internal service via external port 2379
      name: mongo
      protocol: MONGO
    hosts:
    - "*"
```

上面的网关规范描述了负载平衡器的L4-L6属性。`VirtualService`然后，可以将A 绑定到网关，以控制到达特定主机或网关端口的流量的转发。

例如，下面的VirtualService分裂流量 `https://uk.bookinfo.com/reviews`，`https://eu.bookinfo.com/reviews`， `http://uk.bookinfo.com:9080/reviews`，`http://eu.bookinfo.com:9080/reviews`进入端口9080的内部的评论服务的两个版本（PROD和QA）另外，包含cookie请求“用户：DEV-123”将被发送到特定的端口7777在qa版本中。对于“reviews.prod.svc.cluster.local”服务的请求，同样的规则也适用于网格内部。此规则适用于端口

443,9080。请注意，`http://uk.bookinfo.com` 重定向到`https://uk.bookinfo.com`（即80重定向到443）。

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: bookinfo-rule
  namespace: bookinfo-namespace
spec:
  hosts:
  - reviews.prod.svc.cluster.local
  - uk.bookinfo.com
  - eu.bookinfo.com
  gateways:
  - some-config-namespace/my-gateway
  - mesh # applies to all the sidecars in the mesh
  http:
  - match:
    - headers:
        cookie:
          exact: "user=dev-123"
    route:
    - destination:
        port:
          number: 7777
        host: reviews.qa.svc.cluster.local
  - match:
    - uri:
        prefix: /reviews/
    route:
    - destination:
        port:
          number: 9080 # can be omitted if it's the only port for reviews
        host: reviews.prod.svc.cluster.local
      weight: 80
    - destination:
        host: reviews.qa.svc.cluster.local
      weight: 20
```

以下VirtualService将到达（外部）端口27017的流量转发到端口5555上的内部Mongo服务器。此规则不适用于网状网内部，因为网关列表省略了保留名称`mesh`。

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: bookinfo-Mongo
  namespace: bookinfo-namespace
spec:
  hosts:
  - mongosvr.prod.svc.cluster.local # name of internal Mongo service
  gateways:
  - some-config-namespace/my-gateway # can omit the namespace if gateway is in same
                                     namespace as virtual service.
  tcp:
  - match:
    - port: 27017
    route:
    - destination:
        host: mongo.prod.svc.cluster.local
        port:
          number: 5555
```

可以使用hosts字段中的namespace / hostname语法限制可以绑定到网关服务器的虚拟服务集。例如，以下网关允许ns1命名空间中的任何虚拟服务绑定到它，同时仅限制ns2命名空间中foo.bar.com主机的虚拟服务绑定到它。

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: my-gateway
  namespace: some-config-namespace
spec:
  selector:
    app: my-gateway-controller
  servers:
  - port:
      number: 80
      name: http
      protocol: HTTP
    hosts:
    - "ns1/*"
    - "ns2/foo.bar.com"
```

网关

领域	类型	描述
servers	Server[]	必需：服务器规范列表。
selector	map<string, string>	必需：一个或多个标签，指示应在其上应用此网关配置的一组特定pod / VM。标签搜索的范围仅限于资源所在的配置命名空间。换句话说，Gateway资源必须与网关工作负载实例位于同一名称空间中。

港口

端口描述服务的特定端口的属性。

领域	类型	描述
number	uint32	REQUIRED：有效的非负整数端口号。

领域	类型	描述
protocol	string	要求：端口上暴露的协议。必须是HTTP | HTTPS | GRPC | HTTP2 | MONGO | TCP | TLS之一。TLS意味着连接将基于SNI报头路由到目的地，而不终止TLS连接。
name	string	分配给端口的标签。

服务器

Server描述给定负载均衡器端口上代理的属性。例如，

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: my-ingress
spec:
  selector:
    app: my-ingress-gateway
  servers:
  - port:
      number: 80
      name: http2
      protocol: HTTP2
    hosts:
    - "*"
```

另一个例子

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: my-tcp-ingress
spec:
  selector:
    app: my-tcp-ingress-gateway
  servers:
  - port:
      number: 27018
      name: mongo
      protocol: MONGO
    hosts:
    - "*"
```

以下是端口443的TLS配置示例

```yaml
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: my-tls-ingress
spec:
  selector:
    app: my-tls-ingress-gateway
  servers:
  - port:
      number: 443
      name: https
      protocol: HTTPS
    hosts:
    - "*"
    tls:
      mode: SIMPLE
      serverCertificate: /etc/certs/server.pem
      privateKey: /etc/certs/privatekey.pem
```

领域	类型	描述
port	Port	必需：代理应侦听传入连接的端口。
hosts	string[]	需要。此网关公开的一个或多个主机。虽然通常适用于HTTP服务，但它也可以用于使用带有SNI的TLS的TCP服务。主机被指定为dnsName带有可选namespace/前缀的主机。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VirtualService从指定的命名空间中选择所有主机（例如，prod/*）。如果未namespace/指定，VirtualService则将从任何可用的命名空间中选择主机。DestinationRule还将使用相同名称空间中的任何关联。 A VirtualService必须绑定到网关，并且必须具有一个或多个与服务器中指定的主机匹配的主机。匹配可以是与服务器主机的完全匹配或后缀匹配。例如，如果服务器的主机指定*.example.com，则a VirtualService与主机dev.example.com或prod.example.com将匹配。但是，VirtualService与主机example.com或 newexample.com将不匹配。 注意：只能引用导出到网关名称空间的虚拟服务（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。
tls	Server.TLSOptions	一组TLS相关选项，用于管理服务器的行为。使用这些选项可以控制是否应将所有http请求重定向到https，以及要使用的TLS模式。

领域	类型	描述
defaultEndpoint	string	默认情况下应将流量转发到的环回IP端点或Unix域套接字。格式应为127.0.0.1:PORT或 unix:///path/to/socket 或unix://@foobar（Linux的抽象命名空间）。

Server.TLSOptions

领域	类型	描述
httpsRedirect	bool	如果设置为true，则负载均衡器将为所有http连接发送301重定向，要求客户端使用HTTPS。
mode	Server.TLSOptions.TLSmode	可选：指示是否应使用TLS保护与此端口的连接。此字段的值确定如何强制执行TLS。
serverCertificate	string	如果模式是SIMPLE或，则需要MUTUAL。保存服务器端TLS证书的文件的路径。
privateKey	string	如果模式是SIMPLE或，则需要MUTUAL。保存服务器私钥的文件的路径。
caCertificates	string	如果模式是必需的MUTUAL。包含证书颁发机构证书的文件的路径，用于验证提供的客户端证书。

领域	类型	描述
credentialName	string	credentialName代表唯一标识符，可用于标识serverCertificate和privateKey。附加后缀“-cacert”的credentialName用于标识与此服务器关联的CaCertificates。能够从远程凭证存储（例如Kubernetes secrets）获取凭据的网关工作负载将配置为使用凭证名称检索serverCertificate和privateKey，而不是使用上面指定的文件系统路径。如果使用相互TLS，网关工作负载实例将使用credentialName-cacert检索CaCertificates。名称的语义取决于平台。在Kubernetes中，默认的Istio提供的凭据服务器期望credentialName与保存服务器证书的Kubernetes秘密的名称（私钥，和CA证书（如果使用相互TLS）。设置 ISTIO_META_USER_SDS 网关代理中的元数据变量，用于启用动态凭据提取功能。
subjectAltNames	string[]	用于验证客户端提供的证书中的主题标识的备用名称列表。
minProtocolVersion	Server.TLSOptions.TLSProtocol	可选：最小TLS协议版本。
maxProtocolVersion	Server.TLSOptions.TLSProtocol	可选：最大TLS协议版本。
cipherSuites	string[]	可选：如果已指定，则仅支持指定的密码列表。否则默认为Envoy支持的默认密码列表。

Server.TLSOptions.TLSProtocol

TLS协议版本。

名称	描述
TLS_AUTO	自动选择最佳TLS版本。
TLSV1_0	TLS版本1.0

名称	描述
TLSV1_1	TLS版本1.1
TLSV1_2	TLS版本1.2
TLSV1_3	TLS版本1.3

Server.TLSOptions.TLSmode

代理强制执行的TLS模式

名称	描述
PASSTHROUGH	客户端提供的SNI字符串将用作VirtualService TLS路由中的匹配条件，以确定服务注册表中的目标服务。
SIMPLE	使用标准TLS语义保护连接。
MUTUAL	通过提供客户端证书进行身份验证，使用相互TLS保护与上游的连接。
AUTO_PASSTHROUGH	与直通模式类似，除了具有此TLS模式的服务器不需要关联的VirtualService从SNI值映射到注册表中的服务。诸如服务/子集/端口的目的地细节以SNI值编码。代理将转发到由SNI值指定的上游（Envoy）集群（一组端点）。该服务器通常用于提供不同L3网络中的服务之间的连接，否则这些服务在其各自的端点之间没有直接连接。使用此模式假定源和目标都使用Istio mTLS来保护流量。