ALIBABA CLOUD

Alibaba Cloud

服务网格

控制台使用指南

文档版本：20220121

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.实例管理

1.1. 创建ASM实例

在使用服务网格ASM之前，您需要创建一个ASM实例。本文介绍如何通过ASM管理控制台创建ASM实例。

前提条件

- 已开通以下服务：
  - 服务网格 ASM
  - 弹性伸缩（ESS）服务
  - 访问控制（RAM）服务
  - 链路追踪服务（如需启用链路追踪功能）
- 已获得以下角色授权：AliyunServiceMeshDefaultRole、AliyunCSClusterRole和AliyunCSManagedKubernetesRole。

背景信息

> **说明** 创建服务网格的过程中，根据不同的配置，ASM可能会进行如下操作：
> - 创建安全组，该安全组允许VPC入方向全部ICMP端口的访问。
> - 创建VPC路由规则。
> - 创建EIP。
> - 创建RAM角色及相应策略，该角色拥有SLB的全部权限，云监控的全部权限，VPC的全部权限，日志服务的全部权限。服务网格会根据用户部署的配置相应的动态创建SLB、VPC路由规则等。
> - 创建专有网SLB，暴露6443端口。
> - 创建专有网SLB，暴露15011端口。
> - 在使用服务网格的过程中，ASM会收集被托管管控组件的日志信息用于稳定性保障。

操作步骤

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面单击**创建新网格**。
4. 在**创建新网格**面板，完成网格配置。
   i. 设置网格基础选项。

配置项	描述
名称	设置服务网格的名称。
规格	可选**标准版**和**专业版**实例。专业版在标准版的基础上，增强了多协议支持以及动态扩展能力，提供精细化服务治理，完善零信任安全体系。
Istio版本	选择Istio版本。

配置项	描述
地域	选择服务网格所在的地域。
专有网络	选择服务网格的专有网络，您可以单击**创建专有网络**进行创建，详情请参见创建和管理专有网络。
交换机	选择服务网格的交换机，您可以单击**创建交换机**进行创建，详情请参见使用交换机。
公网访问	设置是否开放**使用公网地址暴露API Server**。ASM实例的运行基于Kubernetes运行时，可以通过API Server定义执行各种网格资源，如虚拟服务、目标规则或者Istio网关等。 ■ 如果选择开放，会创建一个EIP，并挂载到私网SLB上。API Server的6443端口会暴露出来，您可以在公网通过kubeconfig来连接和操作集群，从而定义网格资源。 ■ 如果选择不开放，则不会创建EIP，您只能在VPC下通过kubeconfig来连接和操作集群，从而定义网格资源。
可观测性	设置是否**启用链路追踪**。 ASM集成了阿里云链路追踪服务，为分布式应用的开发者提供了完整的调用链路还原、调用请求量统计、链路拓扑、应用依赖分析等能力，可以帮助开发者快速分析和诊断分布式应用架构下的性能瓶颈，提升开发诊断效率。关于链路追踪的详细介绍，请参见使用链路追踪实现网格内外应用的一体化追踪。 **说明** 启用该配置之前，您需要登录链路追踪管理控制台开通链路追踪服务。
	设置是否**开启采集Prometheus监控指标**。 关于Prometheus的详细介绍，请参见集成ARMS Prometheus实现网格监控和集成自建Prometheus实现网格监控。
	设置是否**启用Kiali提升网格可观测**。 Kiali for ASM是一个服务网格可观测性工具，提供了查看相关服务与配置的可视化界面。ASM从1.7.5.25版本开始支持内置Kiali for ASM。关于启用Kiali提升网格可观测的详细介绍，请参见通过ASM控制台开启Kiali的可观测性。
	设置是否**启用自建Skywalking**。ASM集成了Skywalking，您可以通过Skywalking查看应用的监控指标。 关于Skywalking功能的详细介绍，请参见集成自建Skywalking实现网格可观测性。

配置项	描述
	设置是否**启用访问日志查询**。您可以通过日志服务查看入口网关的访问日志。 关于访问日志的详细介绍，请参见使用日志服务采集数据平面入口网关日志和使用日志服务采集数据平面的AccessLog。
	设置是否**启用控制面日志采集**。 ASM支持采集控制平面日志和日志告警，例如采集ASM控制平面向数据平面Sidecar推送配置的相关日志。关于控制面日志采集的详细介绍，请参见启用控制平面日志采集和日志告警。
策略控制	设置是否**启用OPA插件**。 服务网格ASM集成了开放策略代理（OPA），可用于为您的应用程序实现细粒度的访问控制。启用后，如同Istio Envoy代理容器一样，OPA代理容器也会随之被注入到业务Pod中。然后，在ASM中就可以使用OPA定义访问控制策略，为分布式应用的开发者提供了开箱可用的能力，从而帮助开发者快速定义使用策略，提升开发效率。关于OPA插件的详细介绍，请参见在ASM中使用OPA实现细粒度访问控制。
网格审计	设置是否**启用网格审计**。 网格审计功能可以帮助网格管理人员记录或追溯不同用户的日常操作，是集群安全运维中的重要环节。 关于网格审计功能的详细介绍，请参见使用ASM网格审计。
服务网格资源配置	设置是否**启用Istio资源历史版本**。 当您更新Istio资源的 `spec` 字段中的内容时，ASM会记录更新Istio资源的历史版本，最多记录最近更新的5个版本。关于Istio资源历史版本的详细介绍，请参见回滚Istio资源的历史版本。
	设置是否**启用数据面集群KubeAPI访问Istio资源**。 ASM支持通过数据面集群的Kubernetes API（KubeAPI）对Istio资源进行增删改查操作。关于数据面集群KubeAPI访问Istio资源的详细介绍，请参见使用数据面集群Kubernetes API访问Istio资源。

ii. 设置网格高级选项。

配置项	描述
注入的Istio代理资源设置	设置Istio代理资源。 **说明** ■ 资源限制：默认CPU为2 Core，内存为1024 MiB。 ■ 所需资源：默认CPU为0.1 Core，内存为128 MiB。
集群本地域名	设置服务网格实例使用的集群本地域名，默认为cluster.local。您只能将与网格集群域名相同的K8s集群加入网格实例。 **说明** 当Istio版本≥1.6.4.5，您才可以设置集群本地域名，否则将隐藏集群本地域名。

5. 了解和接受服务协议，并已阅读和同意阿里云服务网格服务条款和免责声明，然后选中该选项。
6. 单击**确定**，开始实例的创建。

> **说明** 一个ASM实例的创建时间一般约为2到3分钟。

执行结果

实例创建成功后，您可以查看以下信息：

- 在**网格管理**页面，查看已创建的实例。

  如需查看最新信息，单击右侧的 按钮。

- 在**网格管理**页面，单击目标实例**操作**列下的**日志**，查看该实例相关的日志信息。
- 在**网格管理**页面，单击目标实例**操作**列下的**管理**，查看该实例的ID、安全组等基本信息。一个新建实例会显示以下默认创建的Istio资源：

- 1个命名空间：default

  > **说明** 系统会为新建实例默认创建5个命名空间，控制台只显示default。通过Kubectl方式可以查询和操作其他命名空间，包括：istio-system、kube-node-lease、kube-public、kube-system。

- 2个目标规则：API-Server（详情请参见 Istio 官网）、default（许可模式的网格范围认证策略，MeshPolicy）

1.2. 查看ASM实例

创建ASM实例之后，可以查看该实例的详细信息以及日志。本文介绍如何查看ASM实例的信息、日志、以及应用部署情况。

查看实例信息

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
   在右侧的**网格管理**页面可以查看已有实例的基本信息。
3. 在**网格管理**页面，找到待查看的实例，单击实例的名称或在**操作**列中单击**管理**。
   在实例的详情页，可以看到基本信息、数据平面信息和控制平面信息。

查看实例日志

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待查看的实例，在**操作**列中单击**日志**。
   在**网格日志**页面，可以查看该网格的详细日志。

查看实例的应用部署

1. 登录ASM控制台。
2. 在左侧导航栏，选择**概览**。
3. 在**概览**页面，从**网格**下拉列表中选择待查看的实例。
   在**概览**页面，可以查看到该实例下所部署的微服务状态。
4. 单击右侧的 按钮，将以可视化图形方式显示实例的应用部署情况。如需返回列表显示样式，单击 按钮。

   > **说明** 如需查看最新信息，单击 按钮。

1.3. 编辑ASM实例

创建ASM实例之后，可以编辑该实例的信息。本文介绍如何编辑ASM实例。

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面单击目标网格**操作**列的**管理**。

4. 在网格管理详情页面右上角单击**功能设置**，在**功能设置更新**对话框中修改参数。

配置项	描述
可观测性	设置是否**启用链路追踪**。 ASM集成了阿里云链路追踪服务，为分布式应用的开发者提供了完整的调用链路还原、调用请求量统计、链路拓扑、应用依赖分析等能力，可以帮助开发者快速分析和诊断分布式应用架构下的性能瓶颈，提升开发诊断效率。 **说明** 启用该配置之前，您需要登录链路追踪管理控制台开通链路追踪服务。
	设置是否**开启采集Promethus监控指标**。
	设置是否**启用Kiali**。 Kiali for ASM是一个服务网格可观测性工具，提供了查看相关服务与配置的可视化界面。 **说明** 您需要先开启采集Promethus监控指标，才可以启用Kialia。
	设置是否**启用访问日志查询**。 容器服务ACK集成了日志服务功能，可对服务网格数据平面集群的AccessLog进行采集。使用日志采集功能前，您需要先在服务网格启用访问日志查询。
流量管理	设置是否**开启支持Http1.0**。 默认启用HTTP2.0。如果您需要使用HTTP1.0，您可以在该页面选中**开启支持Http1.0**开启HTTP1.0。
	设置是否**启用服务就近访问**。 ASM通过Envoy代理为应用服务提供了全局负载均衡能力，您可以在多个跨地域的ACK集群中部署运行应用服务的实例。ASM将这些应用服务的运行状况、路由和后端信息提供给Envoy代理，使其能够以最佳方式将流量路由至某个服务位于多个地域的应用实例。ASM会根据发送请求的Envoy代理位置，针对目标服务的工作负载实例，进行优先级排序。开启该项功能之后，当所有应用实例都正常时，请求将保留在同一位置，即保持服务就近访问。
策略控制	设置是否**启用OPA插件**。 ASM集成了开放策略代理（OPA），可用于为您的应用程序实现细粒度的访问控制。启用后，如同Istio Envoy代理容器一样，OPA代理容器也会随之被注入到业务Pod中。然后，在ASM中就可以使用OPA定义访问控制策略，为分布式应用的开发者提供了开箱可用的能力，从而帮助开发者快速定义使用策略，提升开发效率。

配置项	描述
拦截对外访问的地址范围	设置**拦截对外访问的地址范围**。拦截直接对外访问的地址范围，如果存在多个CIDR，使用英文半角逗号分隔。默认为空时会拦截所有对外访问的地址。
注入的Istio代理资源设置	设置Istio代理资源。 **说明** ○ 资源限制：默认CPU为2 Core，内存为1024 MiB。 ○ 所需资源：默认CPU为0.1 Core，内存为128 MiB。
对外部服务的访问策略OutboundTrafficPolicy	设置外部服务访问策略： ○ ALLOW_ANY：允许网格内应用访问所有外部服务。 ○ REGISTRY_ONLY：允许网格内应用访问在网格内注册的外部服务。
Sidecar代理注入服务资源设置	设置Sidecar代理注入服务资源。 支持设置Sidecar代理注入服务的所需资源和资源限制。
开启自动注入功能	选择开启自动注入的方式，更多信息，请参见多种方式灵活开启自动注入。

5. 单击**确定**。

1.4. 通过kubectl连接ASM实例

如果您需要通过API方式来管理ASM实例，需要建立kubectl命令行客户端与ASM实例的连接。

背景信息

kubectl是Kubernetes集群的命令行工具，通过kubectl能够对集群本身进行管理，并能够在集群上进行容器化应用的安装部署，同时还可以对服务网格进行管理。

服务网格ASM基于Kubernetes提供的RBAC（基于角色的访问权限控制）机制，提供了预定义RBAC角色，可向用户授予访问服务网格的权限范围。

- 提供对控制平面侧命名空间的管理，支持的操作包括create、delete、get、list、patch、update、watch。
- 提供对所有Istio资源类型的管理，支持的操作包括create、delete、get、list、patch、update、watch。
- 提供对 `istiogateways.istio.alibabacloud.com` 类型资源的管理，用于定义入口网关服务，支持的操作包括create、delete、get、list、patch、update、watch
- 提供对 `istio.alibabacloud.com` 类型资源的只读操作，包括get、list。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: istio-admin
rules:
- apiGroups: [""]
  resources: ["namespaces"]
  verbs:
  - create
  - delete
  - get
  - list
  - patch
  - update
  - watch
- apiGroups:
  - config.istio.io
  - networking.istio.io
  - authentication.istio.io
  - rbac.istio.io
  - security.istio.io
  resources: ["*"]
  verbs:
  - create
  - delete
  - get
  - list
  - patch
  - update
  - watch
- apiGroups:
  - istio.alibabacloud.com
  resources: ["istiogateways"]
  verbs:
  - create
  - delete
  - get
  - list
  - patch
  - update
  - watch
- apiGroups:
  - istio.alibabacloud.com
  resources: ["*"]
  verbs:
  - get
  - list
```

操作步骤

1. 从 Kubernetes版本页面安装和设置kubectl客户端，详情参见安装和设置kubectl。
2. 查看ASM实例的连接配置信息。

i. 登录 ASM控制台。

ii. 在左侧导航栏，选择**服务网格 > 网格实例**。

iii. 在**网格实例**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。

iv. 单击右上角的**连接配置**。
在**连接配置**页面的**公网访问**和**内网访问**页签下，可以查看两种网络环境下的连接配置信息。

3. 配置 ASM 实例的连接凭据。
   - 如果您使用公网访问，请选择**公网访问**页签，并单击复制，将内容复制到本地计算机的$HOME/.kube/config（kubectl预期凭据所在的位置）。如果该目录下没有 *config* 文件，请自行创建。
   - 如果您使用内网访问，请选择**内网访问**页签，并单击复制，将内容复制到本地计算机的$HOME/.kube/config（kubectl预期凭据所在的位置）。如果该目录下没有 *config* 文件，请自行创建。
4. 执行以下命令检查是否成功连接。如果显示命名空间信息，则表示连接成功。

```
kubectl get ns
```

1.5. 删除ASM实例

当ASM实例不再需要时，可以删除该实例。

前提条件

已移出该实例下的集群，详情参见移出集群。

操作步骤

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格实例**。
3. 在**网格实例**页面，找到待删除的实例，在**操作**列中单击**删除**。
4. 在**删除网格**对话框中，单击**确定**。

执行结果

待删除网格的状态变为**删除中**，单击**刷新**，成功删除后该实例会从**网格实例**页面消失。

2.数据平面管理

2.1. 添加集群到ASM实例

部署在服务网格中的应用实际上运行于集群之上，因此需要先给ASM实例添加ACK集群。

前提条件

- 已创建至少一个ASM实例。如果没有创建，请参见创建ASM实例。
- 已创建至少一个ACK集群。如果没有创建，请参见创建Kubernetes专有版集群和创建Kubernetes托管版集群。
- 待添加的ACK集群与ASM实例位于同一VPC，或者该ACK集群已开启公网API Server以方便快速接入。

操作步骤

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在网格详情页面左侧导航栏选择**数据平面（服务发现） > Kubernetes集群**，然后在右侧页面单击**添加**。
5. 在**添加集群**面板，选中需要添加的集群，然后单击**确定**。

   > **说明**
   > - 如果应用服务运行于单集群或者同一VPC下的多集群时，建议先选中**与网格处于同一VPC的集群**，筛选出与该网格处于同一VPC的集群。
   > - 请确保添加集群中运行的代理容器能访问ASM实例暴露的Istio Pilot地址。即：如果该ASM实例没有开放Istio Pilot公网地址，请确保能通过VPC进行访问。

6. 在**重要提示**对话框中单击**确定**。

执行结果

添加集群之后，ASM实例的状态变为**更新中**。数秒之后（时长与添加的集群数量有关），单击页面右上方的**刷新**，网格状态会变为**运行中**。在**Kubernetes集群**页面，可以查看已添加集群的信息。

2.2. 添加ECS虚拟机到ASM实例

服务网格ASM支持添加ECS虚拟机到ASM实例，便于您将ECS虚拟机上的工作负载连接到网格中。本文介绍如何添加ECS虚拟机到ASM实例。

前提条件

- 已创建ASM实例。具体操作，请参见创建ASM实例。
- 已创建ECS虚拟机。具体操作，请参见使用向导创建实例。

> **说明** ECS虚拟机必须与ASM实例位于同一VPC。

操作步骤

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在网格详情页面左侧导航栏选择**数据平面（服务发现） > 虚拟机**，然后在右侧页面单击**添加虚拟机**。
5. 在**添加虚拟机**面板选择虚拟机，单击**确定**。
   在**虚拟机**页面可以看到已添加的虚拟机信息。

相关文档

- 在虚拟机上安装Istio Proxy
- 通过ASM管理虚拟机上的Bookinfo应用
- 通过ASM管理VM非容器应用Bookinfo

2.3. 移出集群

当ASM实例中的某个集群不再需要时，可以将该集群从实例中移出。

操作步骤

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在网格详情页面左侧导航栏选择**数据平面（服务发现） > Kubernetes集群**。
5. 在**Kubernetes集群**页面选中待移出的集群，单击**移出**。
6. 单击**确定**，确认移出集群。
   在**Kubernetes集群**页面的集群列表中，可以看到该集群已被移出。

3.控制平面管理

3.1. 回滚Istio资源的历史版本

当您更新Istio资源的 `spec` 字段中的内容时，ASM会记录更新Istio资源的历史版本，最多记录最近更新的5个版本。本文以虚拟服务为例，介绍如何回滚Istio资源的历史版本。

前提条件

- 已创建ASM实例，且ASM实例的Istio为v1.9.7.92-g1d820703-aliyun及以上版本。具体操作，请参见创建ASM实例。
- 已创建虚拟服务。具体操作，请参见管理虚拟服务。

背景信息

Istio资源是指ASM控制台流量管理下的虚拟服务、目标规则、网关规则、服务条目、Envoy过滤器、工作负载组、工作负载条目和Sidecar资源，以及零信任安全下的请求身份认证、对等身份认证及授权策略。

步骤一：启用Istio资源历史版本功能

您可以通过以下两种方式来启用Istio资源历史版本功能：

- 如果您没有创建ASM实例，您可以在创建ASM实例时选中**启用Istio资源历史版本**来启用Istio资源历史版本功能。
- 如果您已创建ASM实例，您可以在ASM实例的网格信息页面启用Istio资源历史版本功能。本文以已创建ASM实例场景为例。

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在**网格信息**页面单击右上角的**功能设置**。
5. 在**功能设置更新**面板选中**启用Istio资源历史版本**，然后单击**确定**。

步骤二：生成虚拟服务的历史版本

> **注意** 只有更新Istio资源的 `spec` 字段中的内容时，ASM才会记录形成历史版本。如果您更新的是Istio资源其他字段，ASM不会记录形成历史版本。

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在网格详情页面左侧导航栏选择**流量管理 > 虚拟服务**。
5. 在**虚拟服务**页面单击目标虚拟服务**操作**列下的**YAML**。
6. 在**编辑**面板修改 `spec` 字段下的内容，例如 `spec` 字段下的 `number` 端口由9080修改为9081，然后单击**确定**。

步骤三：回滚虚拟服务的历史版本

本文以回滚到目标虚拟服务的v2版本为例。

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在网格详情页面左侧导航栏选择**流量管理 > 虚拟服务**。
5. 在**虚拟服务**页面单击目标虚拟服务右侧**操作**列下的**版本管理**。
6. 在**版本管理**面板单击v2版本**操作**列下的**查看**，然后单击**回滚**。
   在**虚拟服务**页面单击目标虚拟服务**操作**列下的**YAML**，在**编辑**面板可以看到目标虚拟服务的YAML内容回滚到v2版本。

FAQ

为什么虚拟服务页面找不到版本管理？

回滚Istio资源的历史版本前，请确保您的Istio版本不能低于v1.9.7.92-g1d820703-aliyun，并且您需要启用Istio资源历史版本功能。

是否只能通过ASM控制台更新Istio资源，ASM才会记录该资源的历史版本？

Istio资源历史版本功能不受操作方式的影响，只要您启用该功能，ASM就会为您记录Istio资源的历史版本。

Istio资源历史版本管理是否有什么限制？

ASM最多为您记录Istio资源最近被更新的5个历史版本。当Istio资源修改超过5次，将清除更新时间最早的历史版本。

ASM记录的Istio资源历史版本与实际更新的YAML内容不完全相同？

ASM记录的Istio资源历史版本会自动省略YAML中冗余的默认值，不会影响该版本的实际使用效果。例如网关规则资源 `spec` 中的 `servers.tls` 字段默认为 `PASSTHROUGH` 。如果您再将此字段设定为PASSTHROUGH，则该设定是冗余的，因此Istio资源历史版本管理功能不会为您记录此字段的设定。

3.2. 使用数据面集群Kubernetes API访问Istio资源

ASM支持通过数据面集群的Kubernetes API（KubeAPI）对Istio资源进行增删改查操作。本文以创建和查看Istio资源为例，介绍如何使用数据面集群KubeAPI访问Istio资源。

前提条件

- 已创建ASM实例，且ASM实例的Istio为1.9.7.93及以上版本。具体操作，请参见创建ASM实例。
- 已创建ACK集群。具体操作，请参见创建Kubernetes托管版集群。
- 添加集群到ASM实例。具体操作，请参见添加集群到ASM实例。

背景信息

Kubernetes API是通过HTTP提供的基于资源的编程接口，支持通过标准HTTP谓词（POST、PUT、PATCH、DELETE、GET）检索、创建、更新和删除集群的主资源，例如Deployment、Service等。更多信息，请参见Kubernetes API。

注意事项

- 强烈建议在单集群模式下使用数据面集群KubeAPI访问Istio资源功能。如果ASM的数据平面有多个集群，则任意一个数据平面集群都可以对ASM上的Istio资源进行增删改查操作。

- 开启数据面集群KubeAPI访问Istio资源功能后，数据面集群将无法删除istio-system命名空间。如果要删除，您需要先从ASM实例中移出数据面集群。
- 删除数据平面的某一命名空间，不会删除ASM控制平面的对应命名空间，以及该命名空间下的Istio资源。
- 如果ASM控制平面有某一命名空间，但是数据平面没有此命名空间，您需要先在数据平面创建出此命名空间，然后才能在这个命名空间下对Istio资源进行增删改查操作。否则会提示以下错误信息：

```
Error from server (NotFound): error when creating "xx.yaml": namespaces "daily-01" not found
```

- 如果在数据平面创建的Istio资源对应的命名空间在ASM控制平面不存在，则会在控制平面自动创建该命名空间。
- Istio资源的增删改查操作不支持缩写，需要使用资源名字的全称，例如 `virtualservice` 。

步骤一：启用数据面集群KubeAPI访问Istio资源功能

您可以通过以下两种方式来启用数据面集群KubeAPI访问Istio资源功能：

- 如果您没有创建ASM实例，您可以在创建ASM实例时选中**启用数据面集群KubeAPI访问Istio资源**来启用数据面集群KubeAPI访问Istio资源功能。具体操作，请参见创建ASM实例。
- 如果您已创建ASM实例，您可以在ASM实例的**网格信息**页面启用数据面集群KubeAPI访问Istio资源功能。本文以已创建ASM实例场景为例。

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在**网格信息**页面单击右上角的**功能设置**。
5. 在**功能设置更新**面板选中**启用数据面集群KubeAPI访问Istio资源**，然后单击**确定**。

   开启数据面集群KubeAPI访问Istio资源后，ASM会创建asm-istio-admin和asm-istio-readonly两个ClusterRole到数据面集群。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  labels:
    api: asm-apiservice-apiserver
    apiserver: "true"
  name: asm-istio-admin
rules:
- apiGroups:
  - networking.istio.io
  - security.istio.io
  resources:
  - '*'
  verbs:
  - '*'
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  labels:
    api: asm-apiservice-apiserver
    apiserver: "true"
  name: asm-istio-readonly
rules:
- apiGroups:
  - networking.istio.io
  - security.istio.io
  resources:
  - '*'
  verbs:
  - get
  - list
  - watch
```

步骤二：获取asm-cr-aggregation配置信息

1. 查看ASM实例ID。
   i. 登录ASM控制台。
   ii. 在左侧导航栏，选择**服务网格 > 网格管理**。
   iii. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
   在**网格信息**页面查看ASM实例ID。
2. 查看集群地域ID。
   i. 登录容器服务管理控制台。
   ii. 在控制台左侧导航栏单击**集群**。
   在**集群**页面查看目标集群的地域，例如您集群地域为华北2（北京），则集群地域ID为cn-beijing。
3. 查看AccessKey ID和AccessKey Secret。具体操作，请参见获取AccessKey。

步骤三：安装asm-cr-aggregation

1. 已通过kubectl连接集群。具体操作，请参见通过kubectl工具连接集群。
2. 在本地安装Helm。具体操作，请参见Helm。

> **说明** 使用kubectl连接集群后，Helm客户端会自动使用KubeConfig连接集群。

3. 下载并解压asm-cr-aggregation至本地。
4. 进入asm-cr-aggregation文件夹中，找到*values.yaml*文件，在*values.yaml*文件中补充ASM ID、集群地域ID、AccessKey ID和AccessKey Secret，然后保存*values.yaml*文件。

> **注意** 如果您的集群位于海外地域，您还需要在*values.yaml*文件中修改asm-cr-aggregation镜像地址的地域为集群所在的地域，例如您的集群位于硅谷，您需要将 `registry.cn-hangzhou.aliyuncs.com/acs/asm-craggregation-apiservice` 修改为 `registry.cn-us-west-1.aliyuncs.com/acs/asm-craggregation-apiservice` 。

5. 执行以下命令，安装asm-cr-aggregation。

```
helm install -f values.yaml asm-cr-aggregation ./
```

6. 验证asm-cr-aggregation是否安装成功。
   i. 登录容器服务管理控制台。
   ii. 在控制台左侧导航栏中，单击**集群**。
   iii. 在**集群列表**页面中，单击目标集群名称或者目标集群右侧**操作**列下的**详情**。
   iv. 在集群管理页面左侧导航栏选择**应用 > Helm**。
   在**Helm**页面可以看到asm-cr-aggregation，说明asm-cr-aggregation安装成功。

步骤四：授予RAM用户权限

使用数据面集群Kubernetes API访问Istio资源之前，您的账号需要拥有在数据面集群访问Istio资源的权限和ASM的自定义资源权限：

> **说明** 您拥有的数据面集群访问Istio资源的权限和ASM的自定义资源权限需要保持一致，即如果您拥有ASM自定义资源的读写权限，那您同时也需要拥有数据面集群访问Istio资源的读写权限。

- 您使用的账号需要拥有控制平面ASM自定义资源的操作权限，即拥有网格管理人员或者网格管理受限人员权限。具体操作，请参见授予RAM用户和RAM角色RBAC权限。
  网格管理人员拥有ASM自定义资源的读写权限，网格管理受限人员拥有ASM自定义资源的只读权限。
- 您使用的账号需要拥有在数据面集群访问Istio资源的权限，否则将访问失败。
  您可以执行以下命令，检查RAM用户是否拥有访问Istio资源的权限。

```
kubectl get VirtualService
```

  预期输出：

```
Error from server (Forbidden): virtualservices.networking.istio.io is forbidden: User "24
869613637716****" cannot list resource "virtualservices" in API group "networking.istio.i
o" in the namespace "default"
```

  返回以上结果，说明RAM用户没用访问Istio资源的权限。您需要授予RAM用户访问Istio资源的权限，具体操作如下：

授予RAM用户访问Istio资源的只读权限。

1. 使用阿里云账号登录容器服务管理控制台。
2. 在控制台左侧导航栏单击**授权管理**。
3. 在**子账号**页签下单击目标RAM用户右侧的**管理权限**。
4. 在**集群RBAC配置**页面中单击图标，选择要授予的集群和命名空间，设置**访问权限**为**自定义**，在文本框中选择asm-istio-readonly，然后单击**下一步**。

   页面提示**授权成功**。

5. 验证RAM用户是否拥有访问Istio资源的只读权限。
   i. 执行以下命令，查看虚拟服务。

   ```
   kubectl get VirtualService
   ```

   预期输出：

   ```
   NAME             CREATED AT
   reviews-route    2021-11-15T07:09:10Z
   ```

   ii. 执行以下命令，编辑虚拟服务。

   ```
   kubectl edit VirtualService reviews-route
   ```

   预期输出：

   ```
   error: virtualservices.networking.istio.io "reviews-route" could not be patched: vi
   rtualservices.networking.istio.io "reviews-route" is forbidden: User "2299278366815
   6****" cannot patch resource "virtualservices" in API group "networking.istio.io" i
   n the namespace "default
   ```

授予RAM用户访问Istio资源的读写权限。

1. 使用阿里云账号登录容器服务管理控制台。
2. 在控制台左侧导航栏单击**授权管理**。
3. 在**子账号**页签下单击目标RAM用户右侧的**管理权限**。
4. 在**集群RBAC配置**页面中单击图标，选择要授予的集群和命名空间，设置**访问权限**为**自定义**，在文本框中选择asm-istio-admin，然后单击**下一步**。

   页面提示**授权成功**。

5. 验证RAM用户是否拥有访问Istio资源的读写权限。
   i. 执行以下命令，查看虚拟服务。

   ```
   kubectl get VirtualService
   ```

   预期输出：

   ```
   NAME             CREATED AT
   reviews-route    2021-11-15T07:09:10Z
   ```

   ii. 执行以下命令，编辑虚拟服务。

   ```
   kubectl edit VirtualService reviews-route
   ```

   预期输出：

   ```
   virtualservice.networking.istio.io/reviews-route edited
   ```

步骤五：使用数据面集群KubeAPI创建和查看Istio资源

本文以Helm Chart方式创建和查看Istio资源为例。

> **说明** 在开启数据面集群KubeAPI访问Istio资源功能后，数据平面集群需要等待1~2分钟，然后才可以使用该功能。

1. 下载并解压Istio-bookinfo至本地。

   Istio-bookinfo文件包含Istio资源和Bookinfo应用的YAML文件。

2. 进入到Istio-bookinfo文件下，执行以下命令，创建Istio资源并安装Bookinfo应用。

   ```
   helm install -f values.yaml istio-bookinfo ./
   ```

3. 验证Istio-bookinfo是否安装成功。

   i. 在ASM控制台查看Istio资源。

      a.

      b.

      c.

      d. 在网格管理页面选择**流量管理 > 网关规则**。

         在**网关规则**页面可以看到bookinfo-gateway网关，说明创建Istio资源成功。

   ii. 在ACK控制台查看Bookinfo应用。

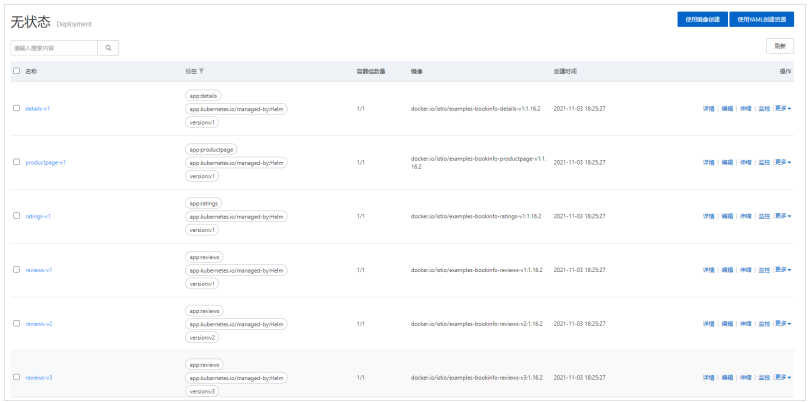
      a. 登录容器服务管理控制台。

      b. 在控制台左侧导航栏中，单击**集群**。

      c. 在**集群列表**页面中，单击目标集群名称或者目标集群右侧**操作**列下的**详情**。

      d. 在集群管理页面可以选择**工作负载 > 无状态**。

         在**无状态**页面可以看到reviews、details等应用，说明安装Bookinfo应用成功。

      根据以上结果，说明Istio-bookinfo安装成功，同时也说明使用数据面集群KubeAPI创建Istio资源成功。

4. 执行以下命令，使用数据面集群KubeAPI查看bookinfo-gateway网关。

```
kubectl get Gateway bookinfo-gateway -o yaml
```

返回bookinfo-gateway网关的YAML文件内容，说明查看bookinfo-gateway网关成功。

3.3. 启用控制平面日志采集和日志告警

ASM支持采集控制平面日志和日志告警，例如采集ASM控制平面向数据平面Sidecar推送配置的相关日志。本文介绍日志告警处理建议，以及如何启用控制平面日志采集和日志告警。

启用控制平面日志采集

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在**网格信息**页面单击**控制面日志采集**右侧的**开启**。
5. 在**启用控制面日志**对话框选择新建Project或使用已有Project，然后单击**确认**。

   如果您选择的是新建Project，您可以使用默认Project名称或者自定义Project名称。

   在**网格信息**页面单击**控制面日志采集**右侧的**查看日志**，然后您可以在Project页面查看详细的控制平面日志。

启用控制平面日志告警

当前只支持数据平面同步失败告警。当控制平面发往数据平面的xDS请求被数据平面拒绝时，数据平面同步失败告警将被触发。此时您的数据平面Sidecar或Ingressgateway将无法得到最新的配置信息，将存在以下两种情况：

> **注意** 启用控制平面日志告警之前必须先启用控制平面日志采集，否则将无法使用该功能。

- 如果数据平面Sidecar在此之前收到过成功的配置推送，则该Sidecar将保持最后一次收到的成功推送的配置。
- 如果数据平面Sidecar在此之前尚未收到过成功的配置推送，则该Sidecar将没有任何配置信息，这意味着该节点可能没有任何监听，也无法处理任何请求和路由规则。

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面，找到待配置的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在**网格信息**页面单击**控制面日志采集**右侧的**告警设置**。
5. 在**控制面日志告警设置**对话框选择行动策略，然后单击**开启告警**。

   行动策略定义了告警触发时的行为，您可以在SLS Project内创建和编辑行动策略。具体操作，请参见创建行动策略。
6. 在**重要提示**对话框单击**确定**。

日志告警处理建议

以下列出了常见的数据面同步失败错误信息和处理建议。如果您没有在下方表格找到对应的错误信息，建议您提交工单。

错误信息	处理建议
Internal:Error adding/updating listener(s) 0.0.0.0_443: Failed to load certificate chain from <inline>, only P-256 ECDSA certificates are supported	该告警信息表示数据面集群不支持您为数据面配置的证书，当前仅支持P-256 ECDSA证书。您需要重新配置证书，具体操作，请参见通过服务网关启用HTTPS安全服务。
Internal:Error adding/updating listener(s) 0.0.0.0_443: Invalid path: ****	该告警信息表示您为数据面配置的证书路径有误或证书不存在，您需要检查证书挂载路径是否与Gateway中配置的路径相符。具体操作，请参见通过服务网关启用HTTPS安全服务。
Internal:Error adding/updating listener(s) 0.0.0.0_xx: duplicate listener 0.0.0.0_xx found	该告警信息表示您为网关配置的监听端口重复，请检查您的Gateway，删除重复的端口。
Internal:Error adding/updating listener(s) 192.168.33.189_15021: Didn't find a registered implementation for name: '***'	该告警信息表示在Sidecar和Ingressgateway中无法找到您通过EnvoyFilter针对15021这个Listener patch的配置中引用的***，您需要删除该引用。
Internal:Error adding/updating listener(s) 0.0.0.0_80: V2 (and AUTO) xDS transport protocol versions are deprecated in grpc_service ***	该告警信息表示即将弃用您数据面的XDS V2协议，这通常是因为您的数据面Sidecar的版本与控制平面不符所致。升级数据平面的Sidecar可以解决该问题，您需要删除Pod，该Pod自动重新创建后会自动注入最新版本的Sidecar。

3.4. 启用Multi-Buffer实现TLS加速

ASM专业版结合Intel的Multi-Buffer加解密技术，可以加速Envoy中TLS的处理过程。本文介绍如何启用Multi-Buffer实现TLS加速。

前提条件

- 已创建ASM专业版实例，且实例为1.10及以上版本。具体操作，请参见创建ASM实例。
- 已创建ACK，且集群节点的实例规格族需要支持Multi-Buffer CPU机型Intel Ice Lake。具体操作，请参见创建Kubernetes托管版集群。

  以下实例规格族支持Multi-Buffer CPU机型Intel Ice Lake：

  > **说明** 关于实例规格的详细介绍，请参见实例规格族。

规格族系列	实例规格族
g7系列	存储增强通用型实例规格族g7se
	通用型实例规格族g7
	安全增强通用型实例规格族g7t
	计算型实例规格族c7
	RDMA增强型实例规格族c7re

c7系列 规格族系列	实例规格族
	存储增强计算型实例规格族c7se
	安全增强计算型实例规格族c7t
r7系列	内存型实例规格族r7p
	存储增强内存型实例规格族r7se
	内存型实例规格族r7
	安全增强内存型实例规格族r7t
其他	内存增强型实例规格族re7p
	GPU虚拟化型实例规格族vgn7i-vws
	GPU计算型实例规格族gn7i
	GPU计算型弹性裸金属服务器实例规格族ebmgn7i
	计算型超级计算集群实例规格族sccc7
	通用型超级计算集群实例规格族sccg7

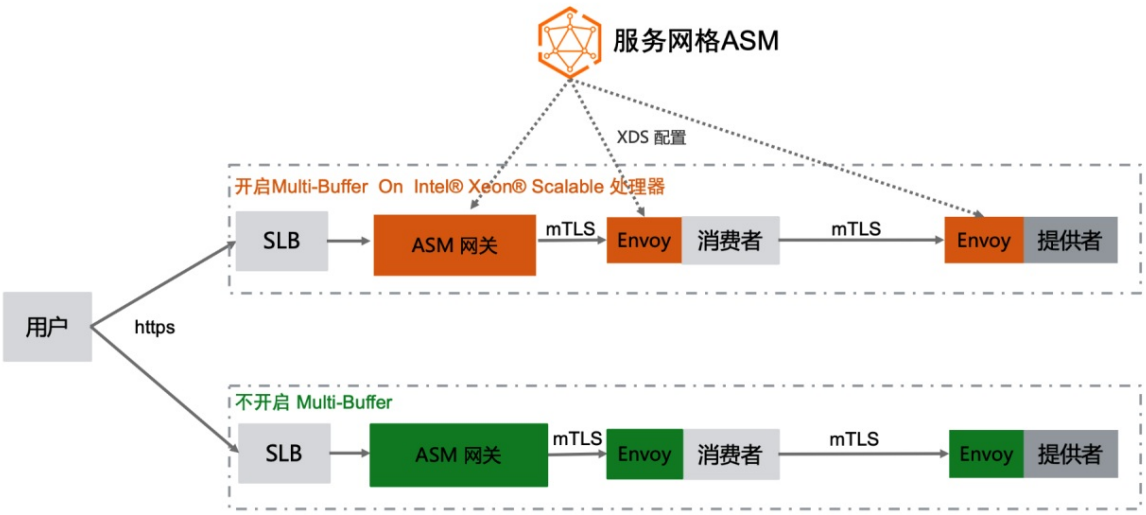
- 添加集群到ASM实例。具体操作，请参见添加集群到ASM实例。

背景信息

随着网络安全技术的发展，TLS已经成为网络通信的基石。一个TLS会话的处理过程总体上可分为握手阶段和数据传输阶段。握手阶段最重要的任务是使用非对称加密技术协商出一个会话密钥，然后在数据传输阶段，使用该会话密钥对数据执行对称加密操作，再进行数据传输。

在微服务场景下，Envoy无论是作为Ingress Gateway还是作为微服务的代理，都需要处理大量的TLS请求，尤其在握手阶段执行非对称加解密的操作时，需要消耗大量的CPU资源，在大规模微服务场景下这可能会成为一个瓶颈。ASM结合Intel的Multi-Buffer加解密技术，可以加速Envoy中TLS的处理过程。

Multi-Buffer加解密技术使用Intel CPU AVX-512指令同时处理多个独立的缓冲区，即可以在一个执行周期内同时执行多个加解密的操作，成倍的提升加解密的执行效率。Multi-Buffer技术不需要额外的硬件，只需要CPU包含特定的指令集。目前阿里云在Ice Lake处理器中已经包含了最新的AVX-512指令集。



操作步骤

您可以通过以下两种方式来启用Multi-Buffer功能：

- 如果您没有创建ASM实例，您可以在创建ASM实例时选中**启用基于MultiBuffer的TLS加解密性能优化**。具体操作，请参见创建ASM实例。
- 如果您已创建ASM实例，您可以在ASM实例的**网格信息**页面启用基于MultiBuffer的TLS加解密性能优化功能。本文以已创建ASM实例场景为例。

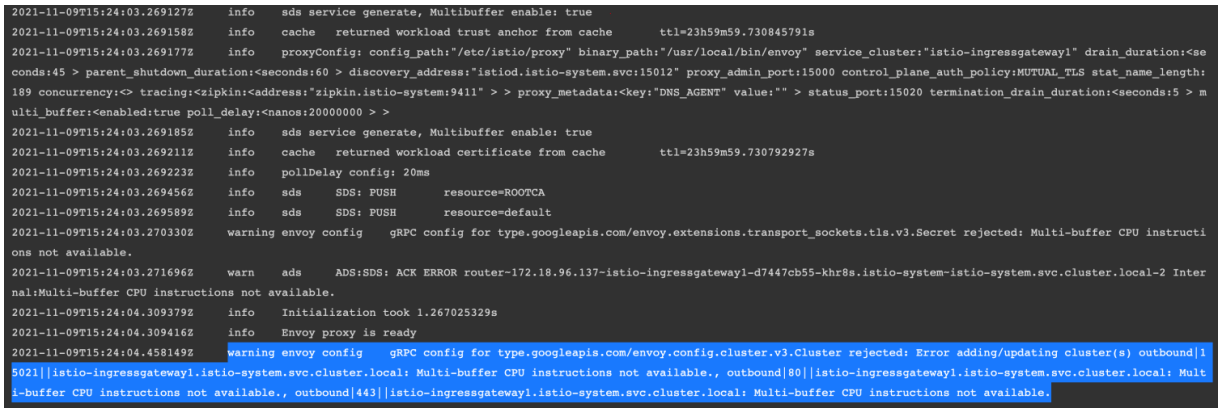
1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 网格管理**。
3. 在**网格管理**页面单击目标ASM专业版实例的名称或**操作**列下的**管理**。
4. 在**基本信息**页面单击右上角的**功能设置**。
5. 在**功能设置更新**面板选中**启用基于MultiBuffer的TLS加解密性能优化**，然后单击**确定**。

   如果您使用通用型实例规格族g7作为Kubernertes节点，启用Multi-Buffer功能后，每秒查询率（QPS）将提升75%的性能。如果您使用的是弹性裸金属节点，提升的性能将更高。

FAQ

如果在控制面启用了MultiBuffer功能，但数据面Kubernetes集群下的节点不是Intel Ice Lake的机型会怎么样？

Envoy会输出告警日志，且MultiBuffer功能将不会生效。



ASM Pro 1.10及以上版本提供了开启TLS加速时的自适应判断能力，若业务或者网关Pod被调度到的Node节点为非Intel Ice Lake机型，则不会下发对应的加速配置，TLS加速不会生效。

如果Kubernetes集群没有支持Multi-Buffer功能类型的节点，那该集群如何才能使用MultiBuffer功能？

1. 在该Kubernetes集群添加新的节点，且节点的实例规格需要支持Multi-Buffer CPU机型Intel Ice Lake。具体操作，请参见添加已有节点。
2. 在新添加的节点上设置 `multibuffer-support：true` 标签。具体操作，请参见管理节点标签。
3. 在ASM网关的YAML配置中添加以下内容。具体操作，请参见修改入口网关服务。

   通过增加节点亲和性，使Gateway实例调度到新添加的支持Multi-Buffer功能的节点上。

   ```
   spec:
     affinity:
       nodeAffinity:
         requiredDuringSchedulingIgnoredDuringExecution:
           nodeSelectorTerms:
             - matchExpressions:
                 - key: multibuffer-support
                   operator: In
                   values:
                     - true
   ```

4. 在ASM专业版启用MultiBuffer功能。具体操作，见上文。

   启用MultiBuffer功能后，该集群新添加的节点即可使用MultiBuffer功能，加速TLS处理过程。