ALIBABA CLOUD

阿里云

服务网格
控制台使用指南

文档版本：20210208

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
  - 容器服务
  - 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**页面，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。
地域	选择服务网格所在的地域。

配置项	描述
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，详情请参见创建交换机。
Istio版本	选择Istio版本。
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。
	设置是否开放**使用公网地址暴露Istio Pilot**。 ■ 如果选择开放，会创建一个EIP，并挂载到私网SLB上。Istio Pilot的15011端口会暴露出来，数据平面侧集群中部署的Envoy代理通过该公网地址连接到Istio Pilot。 ■ 如果选择不开放，则不会创建EIP，数据平面侧只能添加与该VPC互连的集群，包括同一VPC下的集群或者通过云企业网连通的跨VPC集群。 **说明** 默认不开放公网地址暴露Istio Pilot，优先通过VPC连通数据平面与控制平面。
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Prometheus监控指标**。

配置项	描述
流量管理	设置是否**启用服务就近访问**。 服务网格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**。 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。
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。

ii. 设置网格高级选项。

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。
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。
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。

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。

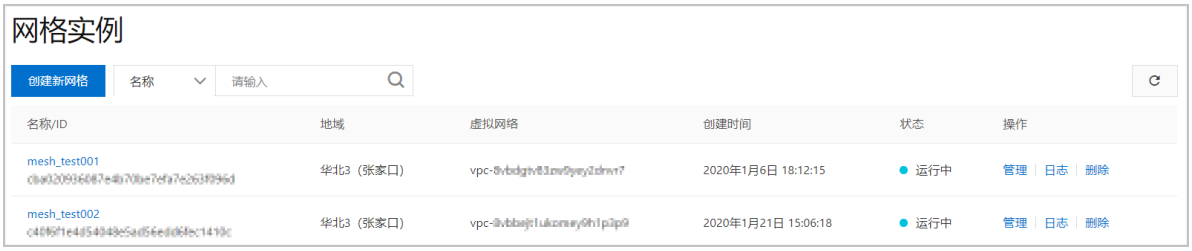
> **说明** 一个ASM实例的创建时间一般约为2到3分钟。

执行结果

实例创建成功后，您可以查看以下信息：

- 在**网格实例**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**网格实例**页面，单击新建实例**操作**列的**日志**，进入网格日志页面查看该实例相关的日志信息。
- 在**网格实例**页面，单击新建实例**操作**列的 **管理**，查看该实例的基本信息、连接配置以及对应数据平面侧的集群信息、控制平面侧定义的命名空间、虚拟服务、目标规则与Istio网格等资源定义信息。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Prometheus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Prometheus监控指标，才可以启用Kialia。

配置项	描述
	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。
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
```

```
  - 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**页面单击目标ASM实例名称或目标ASM实例右侧操作列下的**管理**。
4. 在**数据平面**区域，单击**集群**页签。
5. 在**集群**页签，单击**添加**。
6. 在**添加集群**页面，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。

7. 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**数据平面**区域，可以查看已添加集群的信息。

2.2. 添加入口网关服务

如果部署的应用需要对公网提供访问，需要部署一个入口网关服务到集群中。本文介绍如何为ASM实例中的ACK集群添加入口网关服务。

前提条件

已创建至少一个ASM实例，并已添加至少一个ACK集群到该实例中。

背景信息

入口网关服务（Ingress Gateway）为Kubernetes集群提供了七层网关功能，对外提供一个统一的七层服务入口，根据HTTP请求的内容将来自同一个TCP端口的请求分发到不同的Kubernetes服务。

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**数据平面**区域，单击**入口网关服务**页签。
5. 在**入口网关服务**页签，单击**部署默认入口网关**。

   > **说明** 您也可以通过单击**部署自定义入口网关**来自定义入口网关服务，详情请参见自定义入口网关服务。

6. 在**部署入口网关**页面，为集群添加入口网关服务。
   i. 从**部署集群**列表中选择要部署入口网关服务的集群。
   ii. 指定负载均衡的类型，**公网访问**或**内网访问**。
   iii. 选择负载均衡。
   - 使用已有负载均衡：从已有负载均衡列表中选择。
   - 新建负载均衡：单击**新建负载均衡**，从下拉列表中选择所需的负载均衡规格。

   > **说明** 建议您为每个Kubernetes服务分配一个SLB。如果多个Kubernetes服务复用同一个SLB，存在以下风险和限制：
   > - 使用已有的SLB会强制覆盖已有监听，可能会导致您的应用不可访问。
   > - Kubernetes通过Service创建的SLB不能复用，只能复用您手动在控制台（或调用OpenAPI）创建的SLB。
   > - 复用同一个SLB的多个Service不能有相同的前端监听端口，否则会造成端口冲突。
   > - 复用SLB时，监听的名字以及虚拟服务器组的名字被Kubernetes作为唯一标识符。请勿修改监听和虚拟服务器组的名字。
   > - 不支持跨集群、跨地域复用SLB。

7. 配置端口映射。
   i. 单击**添加端口**。
   ii. 在新增端口行中，输入服务端口和容器端口。

   > **说明**
   > - 建议容器端口与服务端口一致，并在Istio网关资源定义中启用了该端口。
   > - 控制台默认提供了4个Istio常用的端口，但并不意味着必须从中选择，您可以根据需要自行添加或删除端口。

8. 单击**确定**。

执行结果

添加入口网关服务之后，可登录容器服务控制台查看详情。

- 查看新添加的入口网关服务的基本信息。
  i. 登录容器服务管理控制台

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. 在集群管理页左侧导航栏中单击**服务**。
v. 在**服务**页面，从**命名空间**下拉列表中选择istio-system。
vi. 单击目标服务**操作**列的**详情**，查看入口网关服务的详细信息。

- 查看新添加入口网关服务的Pod信息。
  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**应用管理**。
  iv. 在工作负载页面单击**容器组**页签。
  v. 在**容器组**页面，从**命名空间**下拉列表中选择istio-system。
  vi. 单击目标Pod操作列的**详情**，查看入口网关服务的Pod详细信息。

2.3. 修改入口网关服务

服务网格ASM支持修改入口网关服务的配置，本文介绍如何在服务网格ASM修改入口网关服务。

前提条件

已添加入口网关，详情请参见添加入口网关服务。

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**数据平面**区域单击**入口网关服务**页签。
5. 在**入口网关服务**页签单击目标入口网关**操作**列的YAML。
6. 在**编辑**对话框修改参数，单击**确定**。

2.4. 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 > 网格实例**。
3. 在**网格实例**页面，找到待移出集群的实例，单击实例的名称或在**操作**列中单击**管理**。
4. 在**数据平面**区域，勾选待移出的集群。

5. 单击**移出**。
6. 单击**确定**，确认移出集群。
   在**数据平面**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. 管理Namespace

为Kubernetes集群提供虚拟的隔离作用。本文介绍如何新建、定义和删除命名空间。

背景信息

通过服务网格ASM控制台或者使用ASM Kubeconfig定义的命名空间隶属于ASM实例本身，与该ASM管理的数据平面集群是独立的，因此ASM托管的控制平面的命名空间可以与数据平面集群的命名空间存在不同的情况。即在服务网格ASM控制台新增或者删除命名空间，并不会影响数据平面Kubernetes集群的命名空间。

新建命名空间

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**控制平面**区域，选择**Namespace**页签，然后单击**新建**。
5. 在**新建**页面，输入命名空间的基本信息，单击**确定**。

参数	描述
名称	设置命名空间的名称。长度为1~63个字符，只能包含数字、字母、和“-”，且首尾只能是字母或数字。
标签	命名空间可添加多个标签。标签用于标识该命名空间的特点，如标识该命名空间用于测试环境。您可输入变量名称和变量值，单击右侧的添加，为命名空间新增一个标签。

启用自动注入

通过启动自动注入功能，可以在创建Pod的过程中，将Sidecar自动注入Proxy容器，以实现数据平面的网格化。

1. 在**控制平面**区域的**Namespace**页签，找到待注入的命名空间，在**自动注入**列中单击**启用Sidecar自动注入**。
2. 在**确认**对话框，单击**确定**。

定义命名空间

1. 在**控制平面**区域的**Namespace**页签，找到待定义的命名空间，在**操作**列中单击**YAML**。
2. 在**编辑**页面，定义命名空间，单击**确定**。

删除命名空间

1. 在**控制平面**区域的**Namespace**页签，找到待删除的命名空间，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该命名空间。
   单击**刷新**后，在**Namespace**页签下，可以看到该命名空间已被删除。

3.2. 管理VirtualService

在服务网格中，VirtualService是实现流量路由功能的一个关键资源，用于配置如何将请求发送给服务网格中的服务。本文介绍如何新建、修改和删除VirtualService。

新建VirtualService

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**控制平面**区域，选择**VirtualService**页签，然后单击**新建**。
5. 在**新建**页面，输入VirtualService的信息，单击**确定**。
   i. 在**命名空间**下拉列表中，选择待新建VirtualService的命名空间。
   ii. 在文本框中，输入VirtualService的配置信息。

   在**VirtualService**页签，可以看到新建的VirtualService。

修改VirtualService

1. 在**控制平面**区域的**VirtualService**页签，找到待修改的VirtualService，在**操作**列中单击**YAML**。
2. 在**编辑**页面，修改VirtualService，单击**确定**。

删除VirtualService

1. 在**控制平面**区域的**VirtualService**页签，找到待删除的VirtualService，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该VirtualService。
   单击**刷新**后，在**VirtualService**页签下，可以看到该VirtualService已被删除。

3.3. 管理DestinationRule

在服务网格中，DestinationRule是实现流量路由功能的一个关键资源，用于配置目标服务的流量策略，例如指定服务子集以及Envoy代理的流量策略。本文介绍如何新建、修改和删除DestinationRule。

新建DestinationRule

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**控制平面**区域，选择**DestinationRule**页签，然后单击**新建**。
5. 在**新建**页面，输入DestinationRule的信息，单击**确定**。
   i. 在**命名空间**下拉列表中，选择待新建DestinationRule的命名空间。
   ii. 在文本框中，输入DestinationRule的配置信息。

   在**DestinationRule**页签，可以看到新建的DestinationRule。

修改DestinationRule

1. 在**控制平面**区域的**DestinationRule**页签，找到待修改的DestinationRule，在**操作**列中单击**YAML**。
2. 在**编辑**页面，修改DestinationRule，单击**确定**。

删除DestinationRule

1. 在**控制平面**区域的**DestinationRule**页签，找到待删除的DestinationRule，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该DestinationRule。
   单击**刷新**后，在**DestinationRule**页签下，可以看到该DestinationRule已被删除。

3.4. 管理Gateway

Gateway定义了在网格出入口操作的负载均衡器，用于接收传入或传出的HTTP/TCP连接。本文介绍如何新建、修改和删除Gateway。

新建Gateway

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**控制平面**区域，选择**Gateway**页签，然后单击**新建**。
5. 在**新建**页面，输入Gateway的信息，单击**确定**。
   i. 在**命名空间**下拉列表中，选择待新建Gateway的命名空间。
   ii. 在文本框中，输入Gateway的配置信息。

   在**Gateway**页签，可以看到新建的Gateway。

修改Gateway

1. 在**控制平面**区域的**Gateway**页签，找到待修改的Gateway，在**操作**列中单击**YAML**。
2. 在**编辑实例**页面，修改Gateway，单击**确定**。

删除Gateway

1. 在**控制平面**区域的**Gateway**页签，找到待删除的Gateway，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该Gateway。
   单击**刷新**后，在**Gateway**页签下，可以看到该Gateway已被删除。

3.5. 管理EnvoyFilter

EnvoyFilter用于配置Envoy中的过滤条件、监听等信息，为服务网格控制面提供更强大的扩展能力。本文介绍如何新建、修改和删除EnvoyFilter。

新建EnvoyFilter

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**控制平面**区域，选择**EnvoyFilter**页签，然后单击**新建**。
5. 在**新建**页面，输入EnvoyFilter的信息，单击**确定**。
   i. 在**命名空间**下拉列表中，选择待新建EnvoyFilter的命名空间。
   ii. 在文本框中，输入EnvoyFilter的配置信息。

在**EnvoyFilter**页签，可以看到新建的EnvoyFilter。

修改EnvoyFilter

1. 在**控制平面**区域的**EnvoyFilter**页签，找到待修改的EnvoyFilter，在**操作**列中单击**YAML**。
2. 在**编辑实例**页面，修改EnvoyFilter，单击**确定**。

删除EnvoyFilter

1. 在**控制平面**区域的**EnvoyFilter**页签，找到待删除的EnvoyFilter，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该EnvoyFilter。
   单击**刷新**，在**EnvoyFilter**页签下，可以看到该EnvoyFilter已被删除。

3.6. 管理ServiceEntry

ServiceEntry用于将附加服务条目添加到网格内部维护的服务注册表中，描述了服务的域名、端口、协议、端点等信息。本文介绍如何新建、修改和删除ServiceEntry。

新建ServiceEntry

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**控制平面**区域，选择**ServiceEntry**页签，然后单击**新建**。
5. 在**新建**页面，输入ServiceEntry的信息，单击**确定**。
   i. 在**命名空间**下拉列表中，选择待新建ServiceEntry的命名空间。
   ii. 在文本框中，输入ServiceEntry的配置信息。

   在**ServiceEntry**页签，可以看到新建的ServiceEntry。

修改ServiceEntry

1. 在**控制平面**区域的**ServiceEntry**页签，找到待修改的ServiceEntry，在**操作**列中单击**YAML**。
2. 在**编辑实例**页面，修改ServiceEntry，单击**确定**。

删除ServiceEntry

1. 在**控制平面**区域的**ServiceEntry**页签，找到待删除的ServiceEntry，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该ServiceEntry。
   单击**刷新**，在**ServiceEntry**页签下，可以看到该ServiceEntry已被删除。

3.7. 管理Sidecar

Sidecar用于配置Sidecar代理，该代理负责调优与应用实例的出口和入口通信。本文介绍如何新建、修改和删除Sidecar。

新建Sidecar

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**控制平面**区域，选择**Sidecar**页签，然后单击**新建**。
5. 在**新建**页面，输入Sidecar的信息，单击**确定**。
   i. 在**命名空间**下拉列表中，选择待新建Sidecar的命名空间。
   ii. 在文本框中，输入Sidecar的配置信息。

   在**Sidecar**页签，可以看到新建的Sidecar。

修改Sidecar

1. 在**控制平面**区域的**Sidecar**页签，找到待修改的Sidecar，在**操作**列中单击**YAML**。
2. 在**编辑实例**页面，修改Sidecar，单击**确定**。

删除Sidecar

1. 在**控制平面**区域的**Sidecar**页签，找到待删除的Sidecar，在**操作**列中单击**删除**。
2. 单击**确定**，确认删除该Sidecar。
   单击**刷新**，在**Sidecar**页签下，可以看到该Sidecar已被删除。

3.8. 管理WorkloadEntry

WorkloadEntry用于定义非容器化工作负载的属性，支持指定单个非容器化工作负载的属性。本文介绍如何新建、修改和删除WorkloadEntry。

新建WorkloadEntry

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**控制平面**区域，单击**WorkloadEntry**页签，然后单击**新建**。
5. 在**新建**页面，设置WorkloadEntry的信息。
   i. 在**命名空间**下拉列表中，选择待新建WorkloadEntry的命名空间。
   ii. 在文本框中，输入WorkloadEntry的配置信息。
   iii. 单击**确定**。

   在**WorkloadEntry**页签，可以看到新建的WorkloadEntry。

修改WorkloadEntry

1. 在**控制平面**区域的WorkloadEntry页签，找到待修改的WorkloadEntry，在**操作**列中单击**YAML**。
2. 在**编辑**页面，修改WorkloadEntry，单击**确定**。

删除WorkloadEntry

1. 在**控制平面**区域的**WorkloadEntry**页签，找到待删除的WorkloadEntry，在**操作**列中单击**删除**。
2. 在**确认**对话框中单击**确定**。
   单击**刷新**，在**WorkloadEntry**页签下，可以看到该WorkloadEntry已被删除。

3.9. 管理PeerAuthentication

PeerAuthentication用于定义TLS请求认证，本文介绍如何新建、修改和删除PeerAuthentication。

新建PeerAuthentication

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**控制平面**区域，单击**PeerAuthentication**页签，然后单击**新建**。
5. 在**新建**页面，设置PeerAuthentication信息。
   i. 在**命名空间**下拉列表中，选择待新建PeerAuthentication的命名空间。
   ii. 在文本框中，输入PeerAuthentication的配置信息。
   iii. 单击**确定**。

   在**PeerAuthentication**页签，可以看到新建的PeerAuthentication。

修改PeerAuthentication

1. 在**控制平面**区域的**PeerAuthentication**页签，找到待修改的PeerAuthentication，在**操作**列中单击**YAML**。
2. 在**编辑**页面，修改PeerAuthentication，单击**确定**。

删除PeerAuthentication

1. 在**控制平面**区域的**PeerAuthentication**页签，找到待删除的PeerAuthentication，在**操作**列中单击**删除**。
2. 在**确认**对话框中单击**确定**。
   单击**刷新**，在**PeerAuthentication**页签下，可以看到该PeerAuthentication已被删除。

3.10. 管理RequestAuthentication

RequestAuthentication用于定义JWT请求认证，当请求包含无效验证信息时，将根据验证规则拒绝该请求。本文介绍如何新建、修改和删除RequestAuthentication。

前提条件

请确保Istio版本≥1.6，否则将不支持RequestAuthentication功能。

新建RequestAuthentication

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**控制平面**区域，单击**RequestAuthentication**页签，然后单击**新建**。
5. 在**新建**页面，设置RequestAuthentication信息。
   i. 在**命名空间**下拉列表中，选择待新建RequestAuthentication的命名空间。
   ii. 在文本框中，输入RequestAuthentication的配置信息。
   iii. 单击**确定**。

   在**RequestAuthentication**页签，可以看到新建的RequestAuthentication。

修改RequestAuthentication

1. 在**控制平面**区域的**RequestAuthentication**页签，找到待修改的RequestAuthentication，在**操作**列中单击**YAML**。
2. 在**编辑**页面，修改RequestAuthentication，单击**确定**。

删除RequestAuthentication

1. 在**控制平面**区域的**RequestAuthentication**页签，找到待删除的RequestAuthentication，在**操作**列中单击**删除**。
2. 在**确认**对话框中单击**确定**。
   单击**刷新**，在**RequestAuthentication**页签下，可以看到该RequestAuthentication已被删除。

3.11. 管理AuthorizationPolicy

AuthorizationPolicy用于定义授权策略，可对服务网格中的工作负载进行访问控制。本文介绍如何新建、删除和修改AuthorizationPolicy。

新建AuthorizationPolicy

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**控制平面**区域，单击**AuthorizationPolicy**页签，然后单击**新建**。
5. 在**新建**页面，设置AuthorizationPolicy信息。
   i. 在**命名空间**下拉列表中，选择待新建AuthorizationPolicy的命名空间。
   ii. 在文本框中，输入AuthorizationPolicy的配置信息。
   iii. 单击**确定**。

   在**AuthorizationPolicy**页签，可以看到新建的AuthorizationPolicy。

修改AuthorizationPolicy

1. 在**控制平面**区域的**AuthorizationPolicy**页签，找到待修改的AuthorizationPolicy，在**操作**列中单击**YAML**。
2. 在**编辑**页面，修改AuthorizationPolicy，单击**确定**。

删除AuthorizationPolicy

1. 在**控制平面**区域的**AuthorizationPolicy**页签，找到待删除的AuthorizationPolicy，在**操作**列中单击**删除**。
2. 在**确认**对话框中单击**确定**。
   单击**刷新**，在**AuthorizationPolicy**页签下，可以看到该AuthorizationPolicy已被删除。