

ALIBABA CLOUD

阿里云

服务网格
产品简介

文档版本：20220610

 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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.什么是服务网格ASM?	05
2.产品优势	07
3.功能特性	08
4.应用场景	11
5.基本概念	13
6.开服地域	14
7.使用限制	15
8.路线图	16

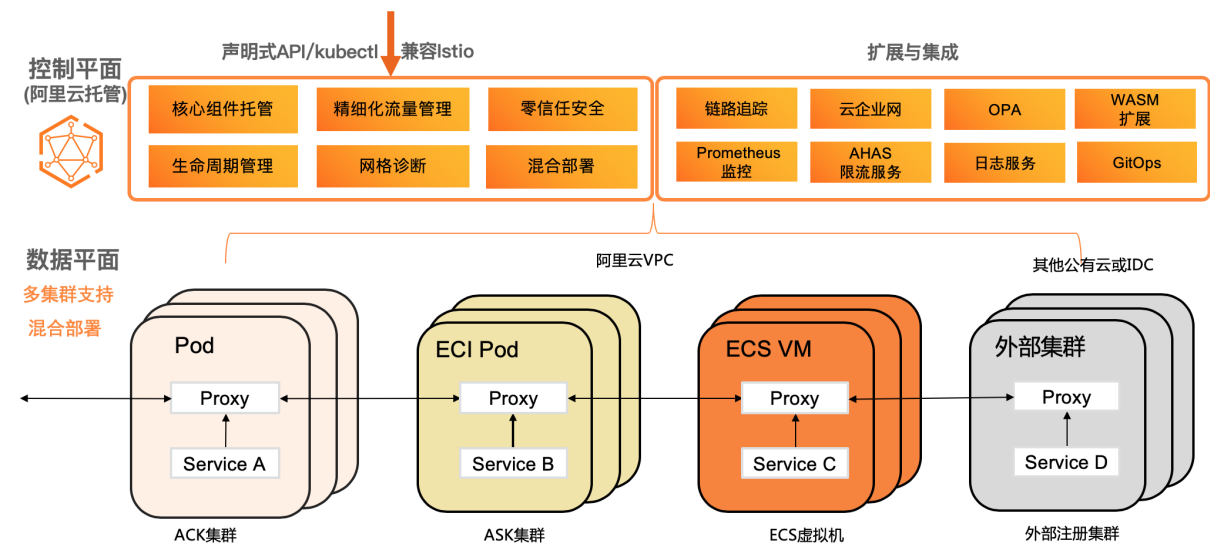
1.什么是服务网格ASM?

阿里云服务网格（Alibaba Cloud Service Mesh，简称ASM）提供一个全托管式的服务网格平台，兼容社区Istio开源服务网格，用于简化服务的治理，包括服务调用之间的流量路由与拆分管理、服务间通信的认证安全以及网格可观测性能力，从而极大地减轻开发与运维的工作负担。

产品简介

产品架构

ASM的产品架构如下图所示。



在ASM中，Istio控制平面的组件全部托管，降低您使用的复杂度，您只需要专注于业务应用的开发部署。同时，保持与Istio社区的兼容，支持声明式的方式定义灵活的路由规则，支持网格内服务之间的统一流量管理。

一个托管了控制平面的ASM实例可以支持来自多个Kubernetes集群的应用服务或者运行于ECI Pod上的应用服务。此外，也可以把一些非Kubernetes服务（例如运行于虚拟机或物理裸机中的服务）集成到同一个服务网格中。

产品功能

ASM定位于混合云、多云、多集群、非容器应用迁移等核心场景中，构建托管式统一的服务网格能力，能够为阿里云用户提供以下功能：

- 一致的管理方式
以一致的方式来管理运行于ACK托管Kubernetes集群、专有Kubernetes集群、Serverless Kubernetes集群、混合云或多云场景下的接入集群上的应用服务，从而提供一致的可观测性和流量控制。
- 统一的流量管理
支持容器或者虚拟机混合环境下统一的流量管理。
- 控制平面核心组件托管化
托管控制平面的核心组件，最大限度地降低用户资源开销和运维成本。

实例规格

服务网格ASM按照规格分为标准版、企业版、旗舰版，其中标准版为免费版，其他两个版本为商业版。商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，并持续提升性能及大规模集群支持能力，降低在生产环境落地服务网格的门槛。商业版适用于有多语言互通，服务精细治理需求，在生产环境大规模使用服务网格的场景。

关于标准版、企业版和旗舰版的详细功能介绍，请参见[功能特性](#)。

 说明 ASM支持升级实例规格。具体操作，请参见[升级ASM商业版规格](#)。

ASM用户交流群

如果您对于ASM有任何疑问，欢迎搜索群号30421250加入钉钉交流群。

学习资源

- [Istio](#)
- [ASM Workshop](#)
- [CNCF × Alibaba 云原生技术公开课](#)
- [阿里云云原生容器工程师ACP认证课程](#)

2.产品优势

本文介绍服务网格 ASM 的优势。

使用便捷

- 通过控制台一键创建服务网格
- 通过控制台一键升级服务网格
- 通过控制台灵活定义 Istio 虚拟服务、目标规则和入口网关资源等

功能强大

功能	说明
完全托管	• 一键安装部署升级 • 控制平面组件托管 • 只需专注于业务应用开发 • 兼容 Istio 社区规范
流量路由	• 自定义流量路由规则 • 跨多个 Kubernetes 集群 • 精细化流量管理 • 开箱即用混沌工程能力
安全功能	• 一键启用或禁用 mTLS • 以渐进方式逐步实现 mTLS • 简单易用的 RBAC 功能 • 易于第三方系统对接
监控诊断	• 提供网格诊断能力 • 集成托管式跟踪、监控和日志服务 • 实现端到端的可见性 • 生态系统对接
高稳定性	• 专门的团队保障托管服务的稳定性
高可用性	• 控制平面分规格，提供不同 SLA 的产品版本面向不同业务需求的客户 • 支持多可用区
技术支持	• 控制平面核心组件托管化，最大限度地降低运维复杂性 • 提供工单技术支持

3. 功能特性

服务网格ASM按照不同的功能及支撑能力划分为标准版、企业版和旗舰版，其中标准版为免费版本，其他两个版本为商业版。本文介绍服务网格ASM各个规格支持的功能。

网格管理

功能	开源社区	标准版	企业版	旗舰版
基于UI控制台的网格实例部署、升级管理等全生命周期管理	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
统一纳管ACK、ASK、ECI、ECS和外部K8s集群	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
生产级的多集群支持（跨VPC、跨地域）	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
对接云平台账号体系（RAM授权等）	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
网格诊断	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
ASM网关高级功能（SLB优雅下线、HPA扩缩容、滚动升级、TLS性能优化）	□	□	✓ [Ⓜ]	✓ [Ⓜ]
多维度的Sidecar代理的配置（全局、命名空间、Workload级）	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
支持Istio资源的历史版本管理	□	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]

流量管理

功能	开源社区	标准版	企业版	旗舰版
Istio社区版核心功能（流量路由、流量治理、可观测性、安全等）	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
本地限流（社区版）	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]	✓ [Ⓜ]
本地限流（优化版）	□	□	✓ [Ⓜ]	✓ [Ⓜ]
支持Dubbo协议	□	□	✓ [Ⓜ]	✓ [Ⓜ]
支持Spring Cloud服务	□	□	✓ [Ⓜ]	✓ [Ⓜ]
服务无损上下线	□	□	✓ [Ⓜ]	✓ [Ⓜ]
全链路标签路由	□	□	✓ [Ⓜ]	✓ [Ⓜ]
AHAS流量防护	□	□	✓ [Ⓜ]	✓ [Ⓜ]

可观测性

功能	开源社区	标准版	企业版	旗舰版
支持与云产品（日志服务、Prometheus服务、链路追踪服务）的融合易用	□	✓☺	✓☺	✓☺
增强的内置常用仪表盘报表	□	✓☺	✓☺	✓☺

安全

功能	开源社区	标准版	企业版	旗舰版
使用OPA实现细粒度访问控制	□	✓☺	✓☺	✓☺
操作审计	□	✓☺	✓☺	✓☺

稳定性与支撑规模

功能	开源社区	标准版	企业版	旗舰版
数据面支撑规模	/	50 Pod ❓ 说明 不推荐生 产使用	1000 Pod	10000 Pod
控制面Istiod组件托管化	/	单个副本	多个副本	多个副本

可扩展性

功能	开源社区	标准版	企业版	旗舰版
EnvoyFilter插件市场	□	✓☺	✓☺	✓☺
对接第三方注册中心（Consul、Nacos）	□	✓☺	✓☺	✓☺

性能

功能	开源社区	标准版	企业版	旗舰版
启用Multi-Buffer实现TLS加速	□	□	✓☺	✓☺
支持选择性服务发现及基于访问日志分析自动推荐的Sidecar资源的配置优化	□	✓☺	✓☺	✓☺

商业版特性相关文档

功能模块	文档
网格管理	启用Multi-Buffer实现TLS加速
ASM网关	• 为域名添加证书 • 为ASM网关启用压缩 • 增强ASM网关高可用性
流量管理	• 使用ASM本地限流功能 • 使用SLB优雅下线功能避免流量损失 • 使用ASM网关的流量路由功能 • 流量打标和标签路由 • 管理Spring Cloud服务 • 通过AHAS对应用进行流量控制 • 基于ASM商业版实现全链路灰度发布
Dubbo服务治理	• 管理Dubbo服务流量 • 集成自建Prometheus实现Dubbo服务可观测性

4. 应用场景

服务网格ASM主要适用于需要对应用服务进行流量管理、安全管理、故障恢复、观测监控以及微服务架构迁移的应用场景。本文介绍ASM的常见应用场景。

流量管理

通过ASM，可以轻松实现基于配置的流量管理：

- 将流量管理与基础设施管理分隔开来，并提供了许多独立于应用代码之外的流量管理功能，在部署规模逐步扩大的过程中帮助简化流量管理。
- 管理服务网格的服务发现、流量路由和负载均衡，简化服务级属性的配置，例如超时和重试等。

服务安全

通过ASM，可以轻松实现服务之间的双向TLS认证：

- 支持以渐进方式实现mTLS双向认证，可以确保服务间通信以及最终用户与服务之间通信的安全。
- 双向TLS认证在实现过程中不需要更改服务代码，可以为每个服务提供基于角色的强大身份认证机制，以实现跨集群、跨云端的交互操作。

通过ASM，可以轻松实现服务之间的授权：

- 借助Istio授权机制，ASM确保只能从经过严格身份认证和授权的客户端访问包含敏感数据的服务。
- 支持对网格中的服务进行基于命名空间级别、服务级别和方法级别的访问权限控制，包括使用基于角色的语义、服务到服务和最终用户到服务的授权，并在角色和角色绑定方面提供灵活的自定义属性支持。

通过ASM，可以轻松实现密钥管理：

- 基于Istio的密钥管理系统，支持自动生成、分发、轮换与撤销密钥和证书。

故障恢复

通过ASM，可以轻松实现开箱即用的故障恢复功能：

- 分布式系统存在高度复杂性，在基础设施、应用逻辑、运维流程等环节都可能存在稳定性风险导致业务系统的失效。
- 提供了基于Istio的混沌工程能力，包括如何使用连接池配置和异常检测实现熔断能力，支持针对服务的重试和故障注入等能力。

服务可观测性

通过ASM，可以轻松实现服务之间的可观测性，借助强大可靠且易于使用的监控功能，快速有效地检测和修复问题。

通过集成的阿里云链路追踪服务，为分布式应用的开发者提供完整的调用链路还原、调用请求量统计、链路拓扑、应用依赖分析等工具，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，提高开发诊断效率。

微服务架构

通过ASM，可以实现敏捷开发和部署落地，加速企业业务迭代。企业生产环境中，通过合理微服务拆分，将每个微服务应用存储在阿里云镜像仓库帮您管理。您只需迭代每个微服务应用，由阿里云提供调度、编排、部署和灰度发布能力。

- 负载均衡和服务发现支持4层和7层的请求转发和后端绑定。
- 丰富的调度和异常恢复策略支持服务级别的亲和性调度，支持跨可用区的高可用和灾难恢复。

- 微服务监控和弹性伸缩支持微服务和容器级别的监控，支持微服务的自动伸缩。

5. 基本概念

本文介绍服务网格所涉及的基本概念，以便于您更好地理解和使用 ASM。

托管服务网格 (Managed Service Mesh)

由服务网格 ASM 创建并托管 Istio 的控制平面。具备简单、低成本、高可用、无需运维管理 Istio 控制平面的特点。

控制平面 (Control Plane)

从架构设计上来看，Istio 服务网格逻辑上分为控制平面和数据平面两部分。控制平面负责管理和配置代理，从而实现路由流量。

数据平面 (Data Plane)

数据平面由一组以 Sidecar 方式部署的智能代理 (Envoy) 组成，负责调节和控制微服务以及 Mixer 之间所有的网络通信。

命名空间 (Namespace)

命名空间为 Kubernetes 集群提供虚拟的隔离作用。Kubernetes 集群初始有 3 个命名空间，分别是默认命名空间 default、系统命名空间 kube-system 和 kube-public，管理员可以创建新的命名空间以满足需求。

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。

虚拟服务 (Virtual Service)

作为 Istio 自定义资源之一，虚拟服务 (VirtualService) 定义了一系列针对指定服务的流量路由规则。每个路由规则都针对特定协议定义流量匹配规则。如果流量符合这些特征，就会根据规则发送到服务注册表中的目标服务（或者目标服务的子集或版本）。

目标规则 (Destination Rule)

作为 Istio 自定义资源之一，目标规则 (DestinationRule) 定义了路由发生后应用于服务的流量策略。这些规则指定负载均衡的配置、来自 Sidecar 代理的连接池大小以及异常检测设置，从而实现从负载均衡池中检测和驱逐不健康的主机。

Istio 网关 (Gateway)

作为 Istio 自定义资源之一，Istio 网关 (Gateway) 定义了在网络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。它描述了需要公开的一组端口、要使用的协议类型、负载均衡器的 SNI 配置等信息。

服务条目 (Service Entry)

作为 Istio 自定义资源之一，服务条目 (ServiceEntry) 是用于将一个服务添加到 Istio 抽象模型或服务注册表中，这些注册的服务是由 Istio 内部维护的。添加服务条目后，Envoy 代理可以将流量发送到该服务，如同这个添加的服务条目是网格中的其他服务一样。

入口网关服务 (IngressGateway Service)

与 Istio 网关 (Gateway) 概念容易混淆的入口网关服务并不是指 Istio 自定义资源，而是指 Kubernetes 服务。它是真实的入口网关服务的抽象，后面由对应的容器来提供支持。通过ASM创建一个入口网关服务时，会部署一个 Kubernetes 服务和 Deployment 资源到用户集群中。

6. 开服地域

地域是指物理的数据中心，资源创建成功后不能更换地域。本文介绍服务网格ASM支持的地域。

ASM免费版和商业版支持相同的地域，支持的地域如下：

云服务	地域	城市	Region ID
公共云	华北2	北京	cn-beijing
	华北3	张家口	cn-zhangjiakou
	华北5	呼和浩特	cn-huhehaote
	华东1	杭州	cn-hangzhou
	华东2	上海	cn-shanghai
	华南1	深圳	cn-shenzhen
	华南2	河源	cn-heyuan
	华南3	广州	guangzhou
	西南1	成都	cn-chengdu
	中国香港	香港	cn-hongkong
	亚太东南1	新加坡	ap-southeast-1
	亚太东南3	吉隆坡	ap-southeast-3
	亚太东南5	雅加达	ap-southeast-5
	亚太南部1	孟买	ap-south-1
	亚太东北1	东京	ap-northeast-1
	美国西部1	硅谷	us-west-1
	美国东部1	弗吉尼亚	us-east-1
	欧洲中部1	法兰克福	eu-central-1
金融云	华东金融云2	上海	cn-shanghai-finance-2
	华南金融云1	深圳	cn-shenzhen-finance-1

7.使用限制

在使用 ASM 之前，您需要提前了解相关的使用限制。本文介绍 ASM 操作限制以及配额限制等。

限制说明

使用 ASM 之前，您需要了解以下限制：

限制项	说明
创建 ASM 实例	网格实例一旦创建后，暂不支持以下操作： • 变更网格所依赖的 VPC 与虚拟交换机 • 如果创建时未开启公网暴露 API Server，暂不支持增加公网 SLB 暴露 API Server • 如果创建时未开启公网暴露 Istio Pilot，暂不支持增加公网 SLB 暴露 Istio Pilot
配额	• 可创建的网格实例数：10；可提交工单申请扩大配额 • 每个网格的 Envoy 代理数：建议 1000 以下；可提交工单申请扩大配额

 **说明** 使用 ASM 之前需要确保能创建标准托管 ACK 集群。关于使用阿里云容器服务 Kubernetes 集群过程中的相关限制，参见[使用限制](#)。

8. 路线图

服务网格ASM路线图中罗列了ASM已经完成的、开发中的和未来规划的功能，帮助您了解未来如何使用服务网格ASM产品。您也可以直接在服务网格ASM路线图的Issues页签下提反馈意见，与阿里云服务网格团队进行产品功能交流。

关于服务网格ASM路线图的更多信息，请参见[ASM Roadmap](#)。