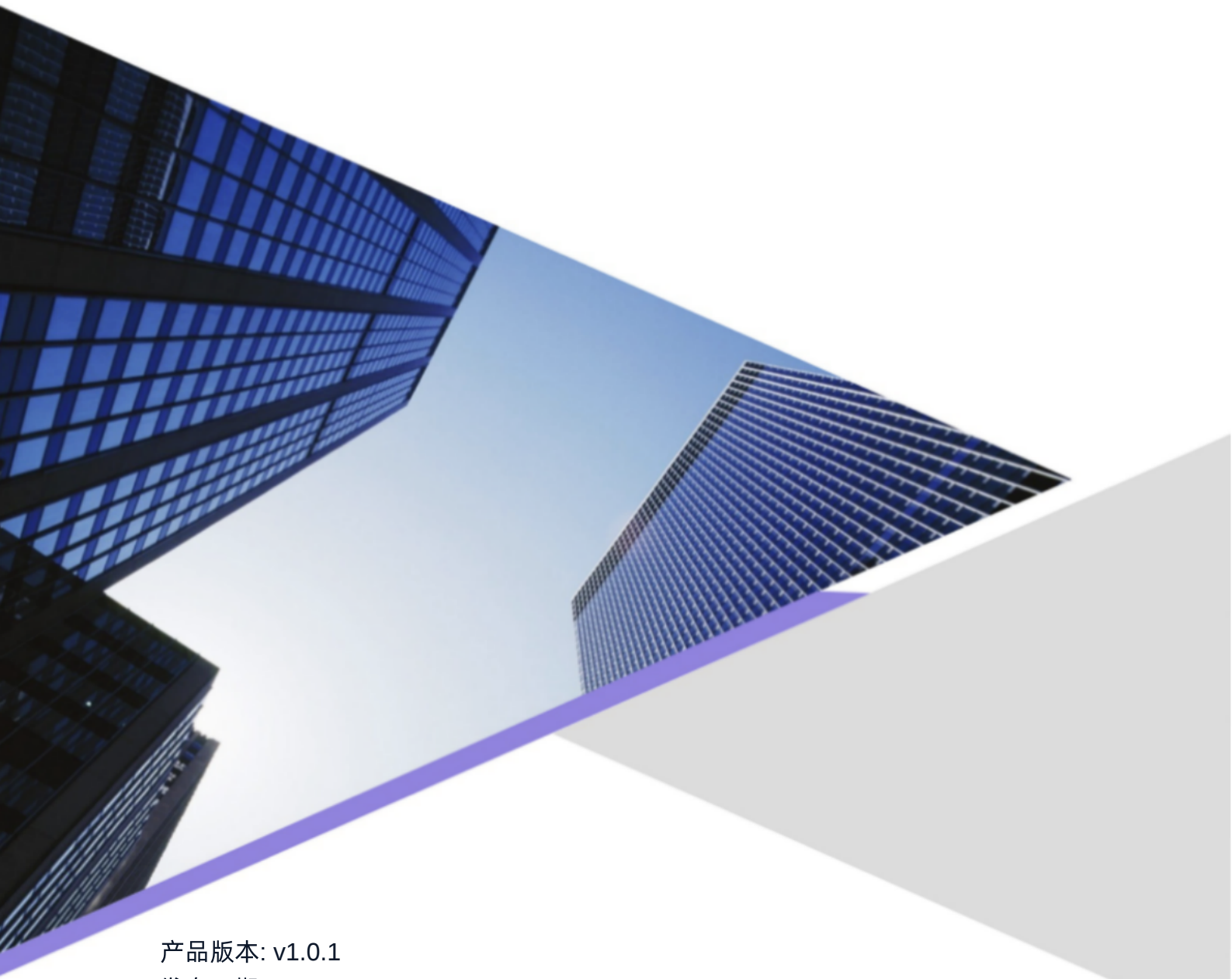
EasyStack
易捷行云

服务网格

产品介绍



产品版本: v1.0.1

发布日期: 2024-06-05

目录

1 产品介绍

1.1 什么是服务网格

服务网格产品基于成熟的 istio 和 cert-manager 实现，提供卓越的基于服务身份的零信任网络,提供微服务应用的流量治理，可观测性和安全基础建设。

让服务间的网络调用更可靠、更安全、更易于监控。像网络中的“交换机”一样,负责处理服务间大量的网络调用，让开发人员更加关注业务逻辑的实现，而基础设施层的网络问题由服务网格组件来处理，以提高微服务应用的性能和稳定性。

产品优势

- **流量控制**

- 支持细粒度的流量控制,如金丝雀发布、A/B 测试、故障注入等
- 提供限流、熔断、重试、负载均衡等能力,提高服务稳定性

- **安全保障**

- 支持服务间 mTLS 认证和加密通信
- 提供细粒度的访问控制和权限管理

- **可观测性**

- 提供聚合的指标、日志和追踪,可以全局观察服务间调用
- 方便定位系统瓶颈和异常,优化服务性能

- **语言无关**

- 作为独立基础层,与业务语言无关
- 降低了语言之间调用的复杂度

- **云原生友好**

- 与 Kubernetes、Istio 等云原生技术无缝集成

- 方便在动态和分布式的环境中管理服务
- **与业务解耦**
- 服务网格独立于业务代码之外,减少了侵入性
- 可以将诸如监控、安全等非业务逻辑提炼出来

1.2 使用场景

多语言应用微服务治理

无需修改代码，服务网格就能为客户提供金丝雀发布、无损上下线、服务鉴权、标签路由等业务应用微服务治理能力，支持与Nacos服务注册中心打通，并提供与异构服务框架如SpringCloud的互通能力。

解决问题：

- 业务代码与治理功能紧耦合，不利于各组件独立快速迭代，服务网格可将治理能力独立出来，实现无侵入的服务治理
- 编程语言及框架的多样化，引入了不同的服务注册中心及治理策略，可利用服务网格实现注册中心的互通，统一治理体系

多集群应用统一流量管理

业务应用部署在多地域或混合云下的Kubernetes集群中，存在一致的可见性和流量管理等需求。服务网格可以为跨类型的计算基础设施构建的服务提供一致的流量管理。

解决问题：

- 部署在异构基础设施上的业务负载涉及Kubernetes、虚拟机等不同的运行环境，可进行统一的流量治理
- 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，可助力用户实现Active-Active的双活方案，或者Active-Standby的灾备方案

应用容器化平滑上云

线下环境有存量应用需要迁移上云，通过部署和配置服务网格，可以将流量动态路由到线下旧版环境或线上新版环境，较好地处理无状态服务迁移。

解决问题：

- 用户在搬站或上云过程中，涉及到测试、灰度、投产等多个阶段，应用流量控制的策略繁杂，可利用简化整个过程
- 对于有多云或混合云战略的用户，为应用服务提供了全局负载均衡能力，同时也支持服务就近访问

服务监控

增强容器、评估API端点的性能，为网格内的服务通信生成详细的遥测，这种遥测技术提供了服务行为的可观察性，允许运营商对其应用程序进行故障排除、维护和优化，而不会给服务开发人员带来任何额外负担。通过应用服务网格，运营商可以全面了解被监控的服务如何与其他服务以及组件本身进行交互。

解决问题：

- 非侵入监控数据采集：在复杂应用的场景下，服务间的访问拓扑，调用链，监控等都是对服务整体运行状况进行管理，服务访问异常时进行定位定界的必要手段。服务网格技术的一项重要能力就是以应用非侵入的方式提供这些监控数据的采集，用户只需关注自己的业务开发，无需额外关注监控数据的生成。
- 灵活的服务运行管理：在拓扑图上通过服务的访问数据，可以直观的观察到服务的健康状况，服务间的依赖情况。并且可以对关心的服务进行下钻，从服务级别下钻到服务版本级别，还可以进一步下钻到服务实例级别。通过实例级别的拓扑可以观察到配置了熔断规则后，网格如何隔离故障实例，使其逐渐接收不到流量。并且可以在故障实例正常时，如何进行实例的故障恢复，自动给恢复的实例重新分配流量

1.3 基本概念

工作负载

工作负载即Kubernetes对一组Pod的抽象模型，用于描述业务的运行载体，包括Deployment、Statefulset、Job、Deamonset等。

- 无状态工作负载（即Kubernetes中的“Deployments”）：Pod之间完全独立、功能相同，具有弹性伸缩、滚动升级等特性。如：Nginx、WordPress。
- 有状态工作负载（即Kubernetes中的“StatefulSets”）：Pod之间不完全独立，具有稳定的持久化存储和网络标示，以及有序的部署、收缩和删除等特性。如：mysql-HA、etcd。

实例（Pod）

Pod是Kubernetes部署应用或服务的最小的基本单位。一个Pod 封装多个应用容器（也可以只有一个容器）、存储资源、一个独立的网络 IP 以及管理控制容器运行方式的策略选项。

健康检查

主要分为主动健康检查和被动健康检查，主动健康检查配置 端点信息，如协议，主机和端口等。被动健康检查又被称为异常值检测，当前众多的协议中，如http ，grpc ，都有专门的配置字段code，表明错误的类型，被动健康检查根据异常值标记节点

金丝雀发布

又称灰度发布，是迭代的软件产品在生产环境安全上线的一种重要手段。在生产环境上引一部分实际流量对一个新版本进行测试，测试新版本的性能和表现，在保证系统整体稳定运行的前提下，尽早发现新版本在实际环境上的问题。

蓝绿发布

蓝绿发布提供了一种零宕机的部署方式。不停老版本，部署新版本进行测试，确认运行正常后，将流量切到新版本，然后老版本同时也升级到新版本。始终有两个版本同时在线，有问题可以快速切换。

流量治理

应用流量治理提供可视化云原生应用的网络状态监控，并实现在线的网络连接和安全策略的管理和配置，当前支持连接池、熔断、负载均衡、HTTP头域、故障注入等能力。

连接池管理

配置TCP和HTTP的连接和请求池相关阈值，保护目标服务，避免对服务的过载访问。

熔断

配置快速响应和隔离服务访问故障，防止网络和服务调用故障级联发生，限制故障影响范围，防止故障蔓延导致系统整体性能下降或者雪崩。

调用链分析

跟踪大规模复杂的分布式系统运行服务调用关系，解决分布式服务故障定位定界问题。

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。

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）定义了在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。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。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。

1.4 产品获取

前提条件

在执行下述产品获取操作步骤前，请确保以下条件均已满足：

- 已成功获取并安装云环境，并且要求云环境版本 >= 6.1.1 。

操作步骤

1. 获取并安装“服务网格”云产品。

在顶部导航栏中，依次选择[产品与服务]-[产品与服务管理]-[云产品]，进入“云产品”页面获取并安装“服务网格”云产品。具体的操作说明，请参考“产品与服务管理”帮助中“云产品”的相关内容。

1.5 权限说明

本章节主要用于说明服务网格各功能的用户权限范围。其中，√ 代表该类用户可对云平台内所有项目的操作对象执行此功能，**XX项目** 代表该类用户仅支持对XX项目内的操作对象执行此功能，未标注代表该类用户无权限执行此功能。

功能		云管理员	部门管理员/项目管理员	普通用户
目标规则（Destination Rule）	信息展示	√	已加入项目	已加入项目
	修改删除	√	已加入项目	已加入项目
虚拟服务（Virtual Service）	信息展示	√	已加入项目	已加入项目
	修改删除	√	已加入项目	已加入项目
Istio 网关（Gateway）	信息展示	√	已加入项目	已加入项目
	修改删除	√	已加入项目	已加入项目
服务条目（Service Entry）	信息展示	√	已加入项目	已加入项目
	修改删除	√	已加入项目	已加入项目

1.6 使用限制

集群限制

- 启用应用服务网格前，您需要创建或已有一个可用集群，并确保集群版本 >= v1.20
- 默认不使用 istio ingress，因此不能管理南北流量。启用 istio ingress 需要开启环境中 loadbalance 控制器
- 重新部署云产品会导致之前正运行 sidecar 因证书问题无法连接，需要重建
- 不支持安全容器类型的负载添加至网格

功能约束

- 服务和工作负载（Deployment）必须是一一对应关系，不允许多个服务对应一个工作负载，因为可能出现灰度发布、网关访问等功能异常。
- 网格实例一旦创建后，不支持变更容器网络。
- 每个网格实例消耗 cpu 0.2 和 memory 256MB 配额。
- 出向网关：使用egressgateway时，因为eks节点默认没有配置外部dns解析，可能无法解析外网域名导致失败，设置步骤：修改coredns配置，添加upstream指向外部DNS，如：”forward . 114.114.114.114”，然后重启coredns(删除pod)，即可正常访问外部DNS进行域名解析。
- 当客户端位于集群内，且配置客户端不连接注册中心时，服务网格支持 dubbo2 协议主要在可观测性上，包括请求, 编解码成功失败指标。 并且提供基础路由方式(当前是基于 interface名称和method名称 路由)，缺乏 dubbo2 的原生流量治理，详见用户指南-多协议和第三方注册中心支持

1.7 与其他服务的关系

服务	关系说明
监控告警服务	平台服务，服务网格会将遥测数据存储在后端的监控告警服务中。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)