ICS [点击此处添加ICS号]

[点击此处添加中国标准文献分类号]

YD

中华人民共和国通信行业标准

YD/T [×××××]—[××××]

[代替YD/T]

|  |
| --- |
| 服务网格技术能力要求  Service Mesh technical capability requirements  [点击此处添加与国际标准一致性程度的标识]  （征求意见稿）  2021年\*月\*日 |

[××××]-[××]-[××]发布

[××××]-[××]-[××]实施

中华人民共和国工业和信息化部 发 布

服务网格架构通用技术能力要求

1. 范围

本标准规定了服务网格架构的技术规范和能力要求，适用于指导云服务商及企业用户在建设服务网格产品中的技术规范，同时该标准规范了服务网格架构的评估方法。该标准内容包括五个方面：一是服务网格控制层面的技术能力，主要描述针对服务网格框架的控制面板（control plane）相关的技术和规范和要求；二是服务网格数据层面的技术能力，主要描述针对服务网格框架的数据面板（data plane）相关的技术和规范和要求；三是安全方面，针对服务网格架构进行安全方面的技术规范和要求；四是服务网格的服务能力，主要描述服务网格维护所依赖的运维功能；五是性能方面，主要描述服务网格产品的性能要求。

本标准对服务网格架构服务能力进行分级，分为基础级、增强级。

本标准同时适用于公有云服务和私有云软件产品，即面向公共用户提供公有云服务和私有云环境下的软件产品或解决方案；依据交付形式的差异，本标准针对不同的使用场景，其技术指标要求略有不同。

1. 术语和定义

下列术语和定义适用于本文件。

* 1. 服务网格（Service Mesh）

服务网格是一个独立的基础设施层,用于处理服务间的通信。云原生应用有着复杂的服务拓扑，服务网格保证请求可以在这些拓扑中可靠地穿梭。服务网格将服务的通信及相应的管理功能从业务中分离并下沉到基础设施层。在实际应用当中，服务网格通常是由一系列对应用透明的网络代理组成的，作为和服务对等的代理服务。每个服务加上代理组成了网格状的应用系统。第二代服务网格新增的控制面板能够实现对流量、安全性、可视性进行统一的管理。

* 1. 数据面板（Data Panel）

服务网格数据面板的实现方式为服务代理，通过接收控制面发送的路由与控制信息来定向转发或处理数据。数据面板由一系列对应用透明的代理组成，现阶段的代理主要以边车容器或虚机形式实现。每个应用实例都有自己专属的代理，网络流量在到达应用实例之前都会经过该代理。数据面板负责接收系统中每一个请求，提供服务发现，健康检查，路由，负载均衡，保证服务认证/授权，以及监控的功能等。

* 1. 控制面板（Control Panel）

服务网格的控制面板为正在网格中运行的数据面板提供策略和配置，不直接接收系统中的业务流量。第二代服务网格新增的控制面板，能够确保以集中控制的方式，在整个组织中实现对流量的统一管理。服务网格通过其控制面板提供对服务间调用的控制，最终实现组成其数据面板的代理的配置。

1. 服务网格参考模型

控制面板统管安全性、可视性、路由规则等，向数据面板下发配置信息与路由规则，并收集数据面板的代理中的度量监控数据。数据面板通过接收控制面板发送的路由策略与控制信息来定向转发或处理数据。

控制面板

应用服务

数据面板

服务代理

图1：服务网格参考模型

1. 服务网格能力分级

服务网格能力分级划分为基础级和增强级。各级别对应的具体能力要求见第5-9章。各级别服务能力如下：

--基础级：实现服务间通信等基本服务网格流量控制能力，实现集中式管理等增强服务网格治理能力，实现多集群的统一流量管理；

--增强级：在基础级能力上，实现多种基础设施下的统一治理，实现多云混合云的统一流量管理。

1. 控制层面技术能力要求
   1. 流量管理

描述：所有的单机代理组件通过和控制面板交互进行网络拓扑策略的更新和单机数据的上报。

基础级：

--支持多云多集群的统一管理：单一网格实例可管理不同环境下多个集群，实现跨集群跨区域流量统一管理；

--支持灾备；

--支持南北向流量管理：

--支持东西向流量管理。

增强级：

--支持多云混合云应用流量统一管理；

--支持多种基础设施应用的统一管理：拉平不同基础设施上的应用管理，比如容器应用和虚拟机应用间的流量管理，适合容器化上云的平滑迁移场景。

* 1. 多租户管理

描述：实现租户管理、租户数据的隔离存储，解决租户之间的隔离/共享。租户的概念不止局限于集群的用户，它可以包含为一组计算，网络，存储等资源组成的工作负载集合。而在多租户场景中，需要对不同的租户提供尽可能的安全隔离，以最大程度的避免恶意租户对其他租户的攻击，同时需要保证租户之间公平地分配共享集群资源。在这种场景下，各租户只能看到自身的集群资源，包括计算资源、逻辑资源、应用资源等，其它租户创建的集群资源不可见，代理只能从控制端同步到本租户的配置和服务信息。

基础级：

--单控制面单网格：每个租户都有自己的一个控制平面和一个服务网格；

--单控制面多集群网格：每个租户一个网格，集群管理员控制和监控整个控制面以及所有网格，租户管理员只能控制特定的网格；

--每个租户的权限管理。

* 1. 集中监控

描述：负责收集代理上采集的度量数据、处理查询到的服务发现数据。

--协助数据面的业务告警；

--支持无入侵全链路跟踪、应用拓扑、访问日志；

--规则配置。

* 1. 配置数据管理

描述：负责服务发现，路由分流，熔断限流等配置数据的管理和下发，以及配置全系统的认证和授权。

--支持配置灰度下发；

--支持按需配置。

* 1. 任务调度

描述：代理的注入和生命周期管理。服务通过调度系统运行在设备上，调度器负责将一个服务连同它的代理绑定在一起。

基础级：

--当调度器启动或停止服务实例时，将服务的生命状态报告给服务发现系统。

增强级：

--服务代理可兼容不同的虚拟化和容器平台，实现纳管传统部署在虚拟机上的微服务。

* 1. 可扩展性

描述：可对控制面板能力进行了扩展和增强。

--端口监听；

--链路层可扩展；

--协议层可扩展；

--多注册中心支持。

1. 数据层面技术能力要求
   1. 服务接入

描述：服务在启动后自动提供自身的元数据以被请求方发现的能力。

--多服务注册中心配置：同时连接多个不同注册中心；

--多协议支持；

--支持服务自动注册模式；

--动态配置（第三方注册模式）：支持第三方配置中心接入。

* 1. 服务发现

描述：获取已运行的服务及其元数据的能力。数据面代理需要在所有的前后端服务实例中，找出哪些是可用的。服务网格的服务发现机制对应用是无侵入，客户端通过目标服务标识名称的访问方式，需要域名解析能力的支持。

基础级：

--DNS 选型：集中式；

--支持服务节点在注册中心被增加或剔除后，能自动感知；

--支持在10秒以内发现服务状态变化。

增强级：

-- DNS 选型：分布式。

* 1. 服务网关

描述：为客户端提供统一的服务接入，承载南北向流量治理并提供认证鉴权、动态路由、协议转换、服务自动发现等公共功能。

--支持服务发现，负载均衡的能力；

--提供认证鉴权；

--提供流量控制，故障隔离的能力或接口；

--支持服务路由的功能；

--支持API管理的功能；

--支持黑白名单，安全策略，降级等功能或接口。

* 1. 流量治理

描述：承载网格中东西向流量治理，根据预置路由策略将请求转发到服务代理，为服务之间的调用提供流量控制以保障核心业务的可用。

--提供智能路由：实现流量控制；

--实现服务间API调用；

--动态拦截流量；

--支持流量切换；

--协助执行蓝绿部署：在不中断任何服务类型的情况下，安全地推送新的应用升级；

--提供负载均衡：网格中对服务实例进行选择；

--配置超时；

--请求失败后重试；

--熔断机制（容错限流）；

--分布式限流。

* 1. 灰度发布策略

描述：灰度发布是指在黑与白之间，能够平滑过渡的一种发布方式。将功能特性按照控制规则逐步扩大发布范围，以保证在初始灰度期，就可以发现、调整问题，从而控制发布影响范围。

--AB两版流量切换便利；

--提供集中化控制：简化灰度发布的实现流程、降低变更成本、加快产品发布的进度。

* 1. 健康检查

描述：服务本身提供自身运行状态的能力。

--服务发现的前端服务实例是否健康并且可以接受网络通信；

--对后端服务主动健康检查；

--健康检查方式。

* 1. 故障注入

描述：故障注入是一种可靠性验证技术，通过向微服务应用注入故障模拟策略，观察应用程序是否能够处理故障。一般有两种类型的故障：延迟和中止，使用服务网格接口的流量分割API注入应用程序故障。

--中断注入；

--超时注入。

* 1. 可观测性

描述：收集代理的时序数据并集中展示，方便理解分布式通信流，快速定位链路故障以及展示网格间拓扑关系，为分布式系统提高可视性。

--支持Metrics度量统计数据；

--支持链路追踪：埋点，上报；

--支持Logging日志信息和分布式操作记录数据。

* 1. 可扩展性

描述：可对数据面板能力进行了扩展和增强，支持私有协议和自定义报文格式的扩展。

--多协议适配；

--多报文通讯适配。

1. 安全能力要求

描述：基于底层IT基础设施层的安全机制，本标准仅对服务网格涉及到的开发和运营时做出具体的安全能力要求。为了确保网络中流量交互的安全性，服务网格提供了基于策略的身份验证，可以在两个服务之间建立双向的TLS配置，加密服务间流量，以实现服务之间的安全加密通信，和最终用户的身份验证。

* 1. 通信加密

描述：为了确保网络中流交互的安全性，服务网格提供基于策略的身份验证，对于服务间的流量进行加密处理，起到数据保护的功能。

--使用相互传输层安全协议(mTLS)，在两个服务之间建立双向的TLS配置；

--对于访问的请求，访问者需要使用mTLS或者其他方法加密验证；

--支持国密加密。

* 1. 证书和授权

描述：为每个服务生成证书，并透明地管理这些证书的分发、轮换和撤销。有了这些功能，服务可以彼此进行身份验证并实现适当的访问控制。

--密钥/证书定期轮换。

* 1. 集中账号管理

描述：创建用户、添加**资源**和配置策略

--包括用户账号管理和资源账号管理；

--用户的身份验证。

* 1. 集中权限管理

描述：确保以集中控制的方式，在整个组织中实现细粒度的访问控制。

--访问控制和强制执行最小特权级别；

--通过账号管控和权限组管理，实现人员与资产的权限管理；

--能够细粒度地划分不同角色的权限，控制用户对服务器的访问。

* 1. 集中安全审计

描述：对所有运维操作进行审计、监控、控制和历史回放可追溯，对多台资源进行一站式管理和实时记录审计。

--符合“网络安全法”等法律法规，满足合规性规范审查要求；

--满足《萨班斯法案》和《等级保护》系列文件中的技术审计要求；

--满足金融监管部门的技术审计要求；

--满足各类法令法规对运维审计的要求。

* 1. 安全警报

描述：一旦捕获，度量(metrics)和日志(logs)将由服务网格的控制面板收集并传递给后端所选择的监控工具。

--支持用户配置报警规则；

--实时显示微服务集群及实例的健康状态；

--支持服务CPU、内存、网络、磁盘等基础指标。

1. 服务能力要求
   1. 维护

描述：网格平台具备维护能力,提供高质量并且不间断的服务，例如在系统的运行过程中,系统的重配置及资源的维护与更新。服务网格框架属于平台底座，由平台专家团队提供维护；开发人员可以更专注于业务应用而非基础设施运维。

--方便安装，卸载，平滑升级；

--代理独立升级能力：框架扩展升级方面，框架管理面及数据面代理升级用户无感知，不影响业务；

--代理有独立的健康检查。

* 1. 故障隔离

描述：协助切断故障服务，治理逻辑故障不会影响业务进程。

--策略隔离；

--手动隔离。

1. 性能要求

描述：服务网格由于内部实现机制的不同或在不同通信协议下，性能有所差异，在统一环境下，通过固定的服务网格应用验证平台性能指标。性能可参考以下指标：

* 1. 时延

描述：一般是指从客户端发送请求到接收响应的整体耗时，包括：请求的网络耗时，请求在服务端的处理耗时以及响应的网络耗时。

--要求小于5ms。

* 1. 网络跳数

描述：服务间调用的跳数。

--要求小于2跳。

* 1. 网络规模

描述：网格能够管理的实例个数。

* 1. 连接数

描述：并发连接数是指代理（sidecar）对其业务信息流的处理能力,是代理能够同时处理的点对点连接的最大数目,它反映出代理对多个连接的访问控制能力和连接状态跟踪能力。

--控制面支持多少sidecar并发连接数；

--数据面/控制面支持多少稳态下的连接。