SERVICE MESH MEETUP #6 广州站

Service Mesh 在蚂蚁金服生产级安全实践

彭泽文

蚂蚁金服高级开发工程师

2019.8.11

蚂蚁金服 ANT FINANCIAL ServiceMesher

分享内容

- 基于 Secret Discovery Service Sidecar 的证书管理方案
- 使用可信身份服务构建敏感数据下发通道
- Service Mesh Sidecar 的 TLS 生产级落地实践

基于 Secret Discovery Service Sidecar 的证书管理方案

Kubernetes Secret 证书管理流程

在 Kubernetes 场景下，证书是通过 secret 的方式来管理，使用时通过 secret mount 以 Volume 形式挂载。

存在以下三个问题：

- Secret 管理方式与现有密钥管理系统有冲突，需要密钥管理系统强依赖 Kubernetes
- Secret 以明文形式挂载在容器的文件系统中，存在安全隐患
- Secret 更新时，Sidecar 需要通过热重启方式重新加载，成本高昂

基于 Secret Discovery Service Sidecar 的证书管理方案

Envoy SDS 证书管理流程

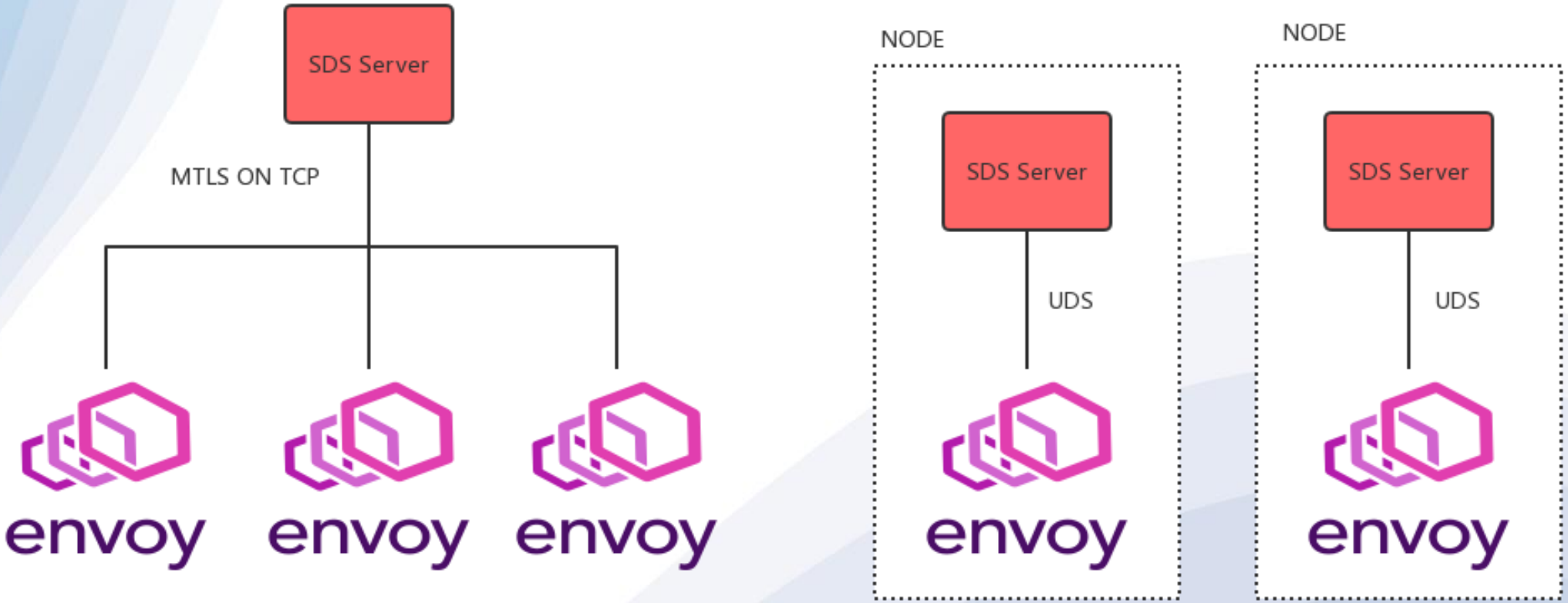
Secret Discovery Service 是 Envoy 提出的 Sidecar 证书管理方案，方案的核心流程在于引入 SDS Server 进行密钥管理和分发，Sidecar 通过 gRPC 请求获取证书，并利用 gRPC stream 能力实现证书动态轮转。

当然，Sidecar 和 SDS Server 的通信也需要保证自身的通信安全，存在以下两种方案：

- Sidecar 与 SDS Server 采用 mTLS 通信，采用静态证书方案，通过 Secret Mount 方式获取通信证书
- Sidecar 与 SDS Server 采用 UDS 方式实现纯内存通信，不需要使用证书。

基于 Secret Discovery Service Sidecar 的证书管理方案

Envoy SDS 证书管理流程



基于 Secret Discovery Service Sidecar 的证书管理方案

Istio With Envoy SDS

Istio 基于 Envoy 的 SDS方案，实现了 SDS Server 和 SDS 配置管理。Istio 方案中选择 UDS 通信方案，Istio的方案证书管理流程由 Citadel , Citadel Agent , Pilot 协同完成

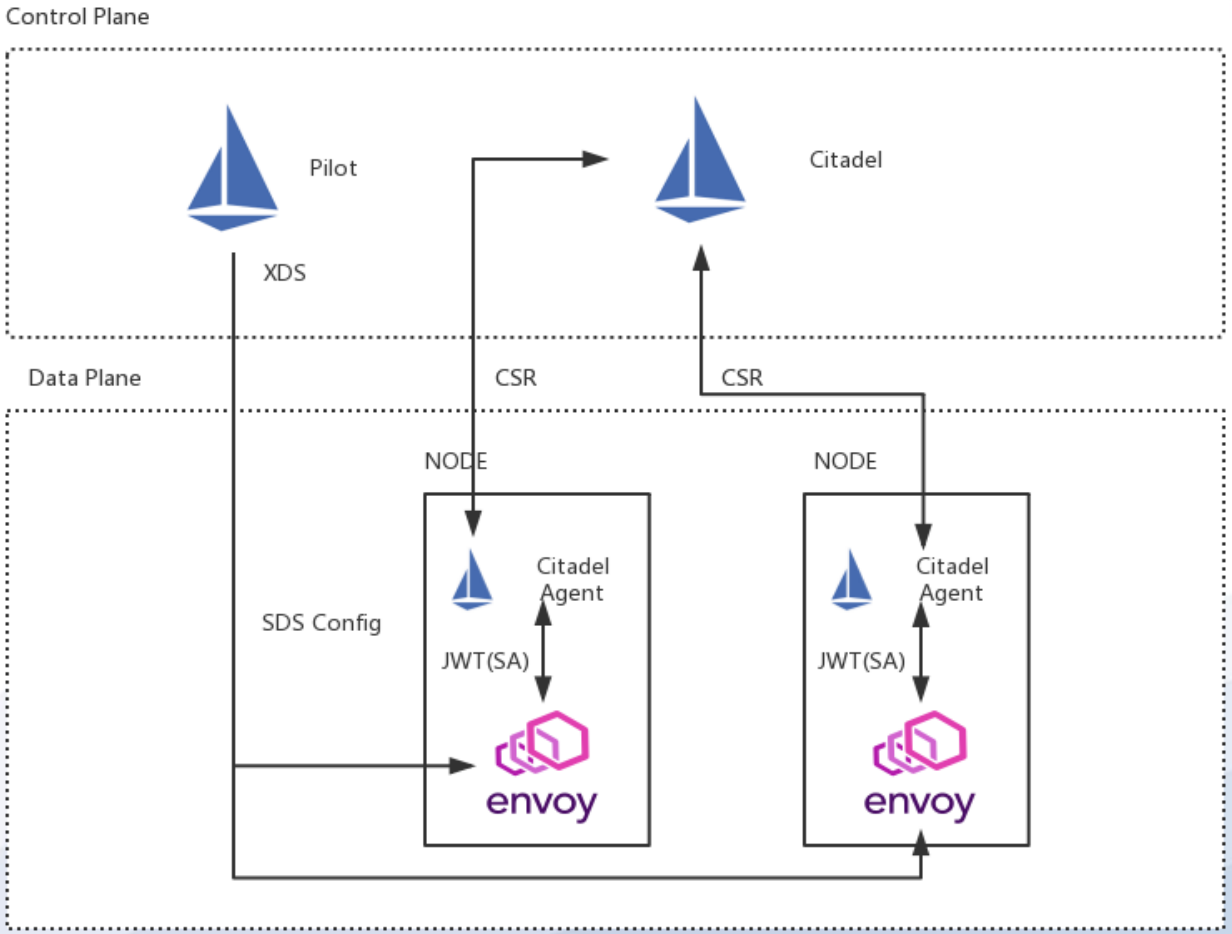
- Pilot 负责 UDS 路径配置下发，用户通过 Policy CRD 和 DestinationRule 来决策需要给哪些 Sidecar 下发
- Sidecar 收到SDS Config 后，然后以 JWT 格式封装身份信息（service account）向Citadel Agent请求证书
- Citadel Agent 会将Sidecar 的请求包装成CSR 请求Citadel ， Citadel 会先检查缓存中是否已有证书，如果不存在的话，会基于Citadel 启动时配置的二级ROOTCA签发证书

基于 Secret Discovery Service Sidecar证书管理方案

Istio With Envoy SDS

Benefits:

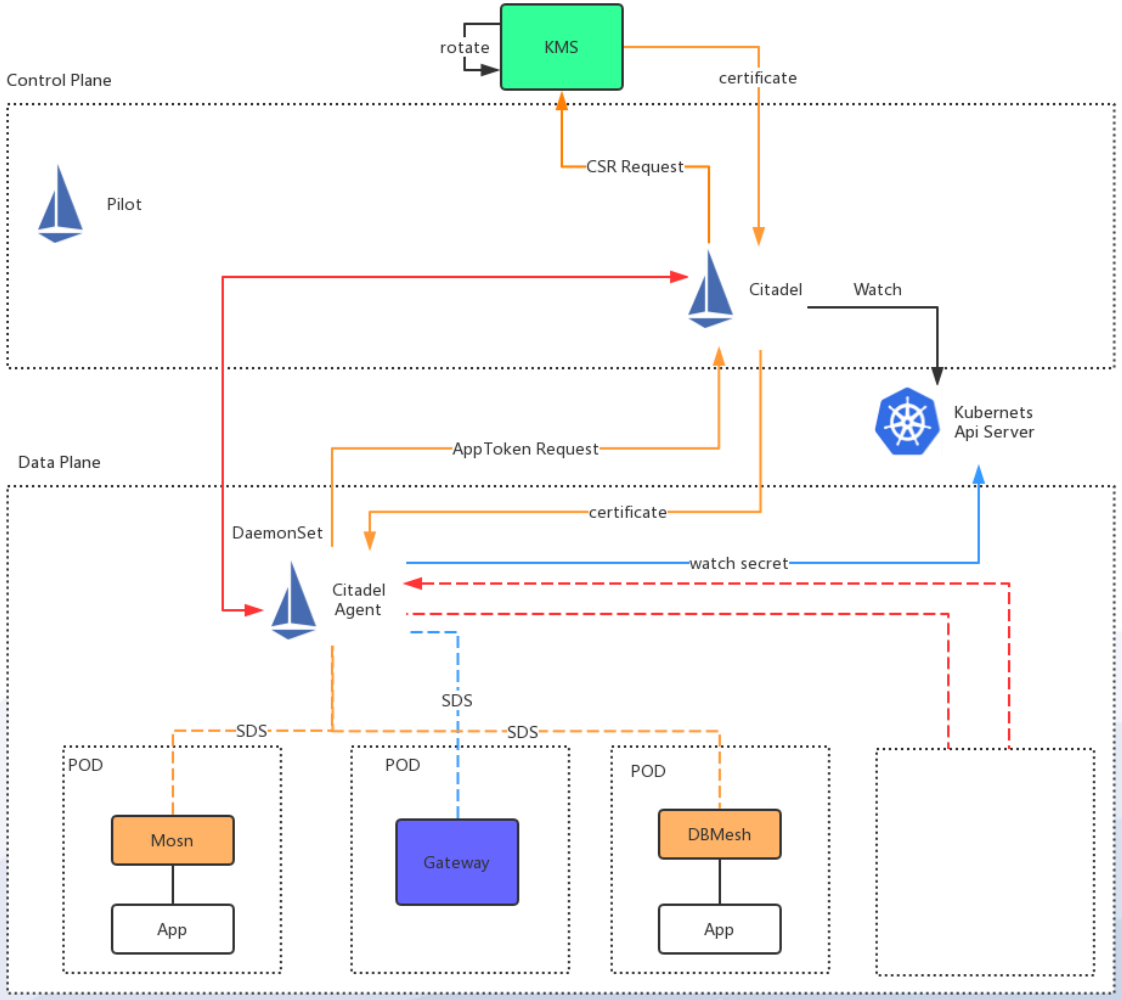
- The private key never leaves the node: It is only in the Citadel agent and sidecar's memory.
- The secret volume mount is no longer needed: The reliance on the Kubernetes secrets is eliminated.
- The sidecar Envoy is able to dynamically renew the key and certificate through the SDS API: Certificate rotations no longer require Envoy to restart.



基于 Secret Discovery Service Sidecar 的证书管理方案

蚂蚁金服证书管理方案

- 基于 Citadel 对接内部密钥管理系统
- 使用 AppLocalToken 替换 Service Account
- 支持多种Sidecar 通过Citadel Agent 获取证书

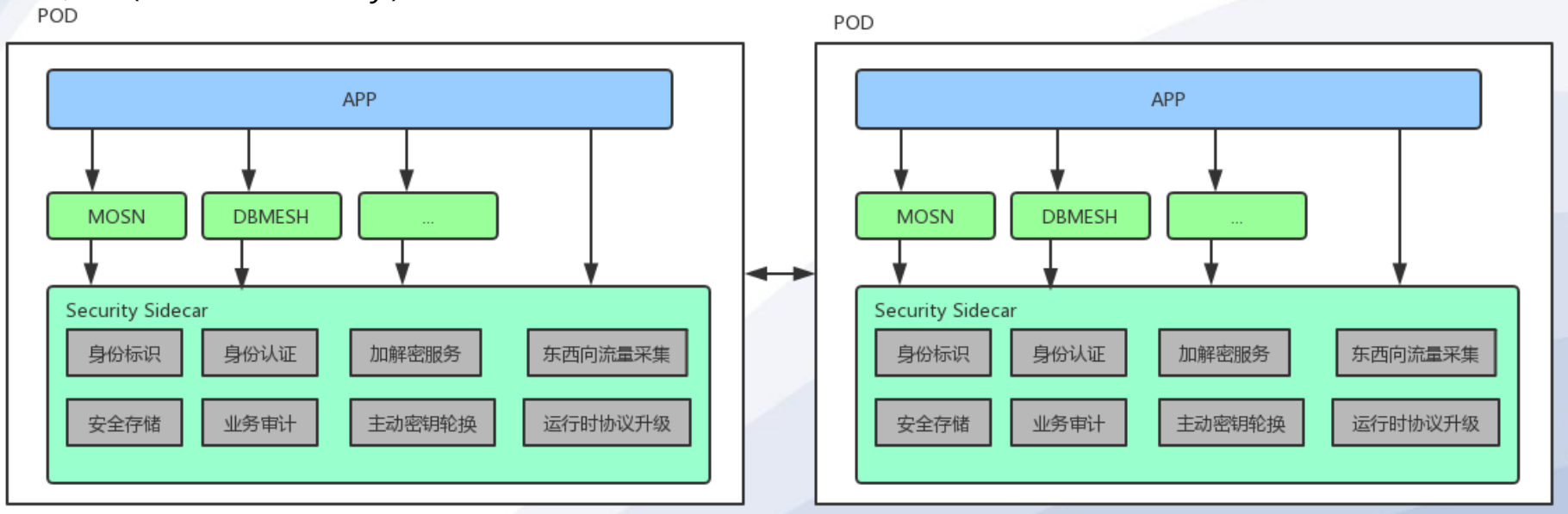


使用可信身份服务构建敏感数据下发通道

背景介绍

通过应用Pod 中增加一个安全 Sidecar，以API接口的形式为APP及其他Sidecar 提供基础的身份颁发、身份验证功能

- 解耦应用的业务逻辑与认证授权逻辑，减少开发量；
- 提供密码学安全的认证授权逻辑，提高安全性；
- 全网统一的认证授权方式，去凭证，减少攻击面；
- 为每个应用建立唯一的全局应用身份标识，提供服务调用全链路溯源能力，及可问责能力（accountability）。



使用可信身份服务构建敏感数据下发通道

身份获取

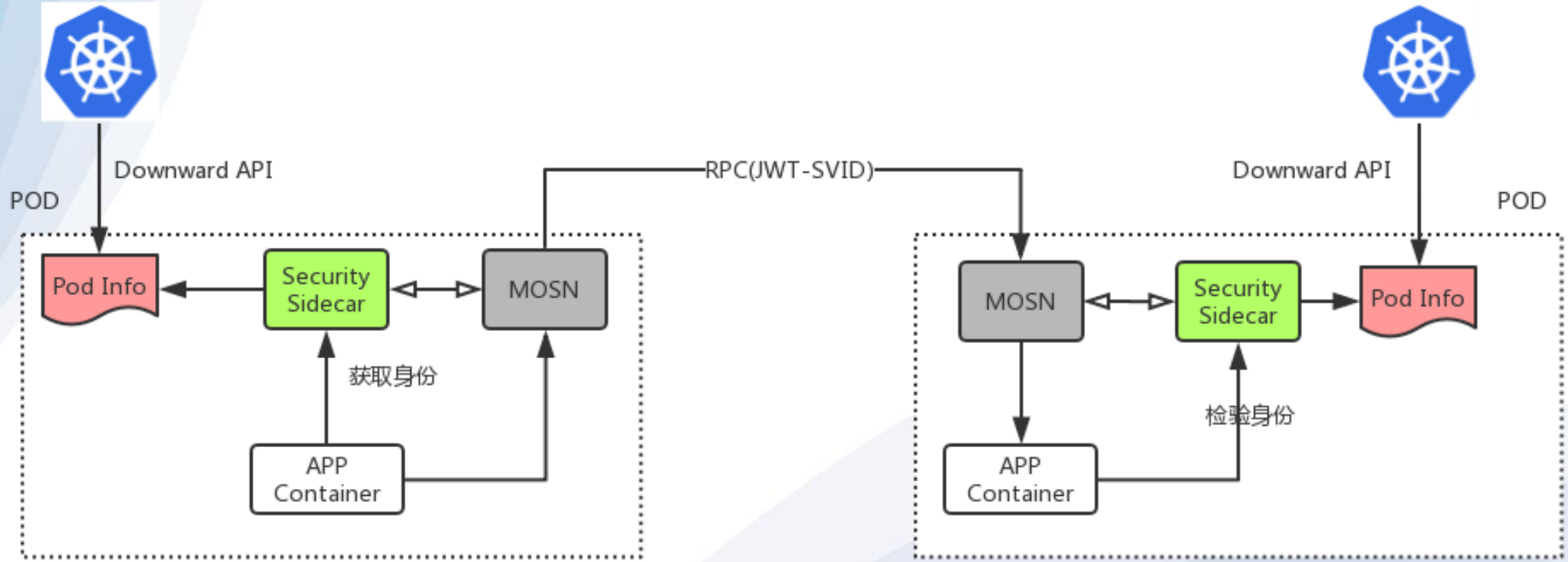
- 应用 A 构造 HTTP 请求，调用 安全Sidecar 提供的 JWT-SVID 颁发接口获取 JWT-SVID。
- 安全Sidecar 通过 Downward API 获取 Pod 身份，并转换成 SPIFFE ID。
- 安全Sidecar 通过密钥将 SPIFFE ID 签发为 JWT-SVID，返回给应用 A。
- 应用 A 在服务调用中带上 JWT-SVID 来声明自己的身份。

使用可信身份服务构建敏感数据下发通道

身份校验

- 从应用 A 发起的调用上下文中获取 JWT-SVID，并构造 HTTP 请求，调用安全Sidecar提供的 JWT-SVID 验证接口。
- 安全Sidecar通过密钥对 JWT-SVID 进行验签。
- 从 JWT-SVID 的 Body 部分中获取 SPIFFE ID。
- 将 SPIFFE ID 内容解释为几个关键属性 (例如租户 ID、应用名等)，并返回给应用 B。
- 应用 B 根据安全Sidecar返回的可信属性，进行权限校验逻辑。

使用可信身份服务构建敏感数据下发通道

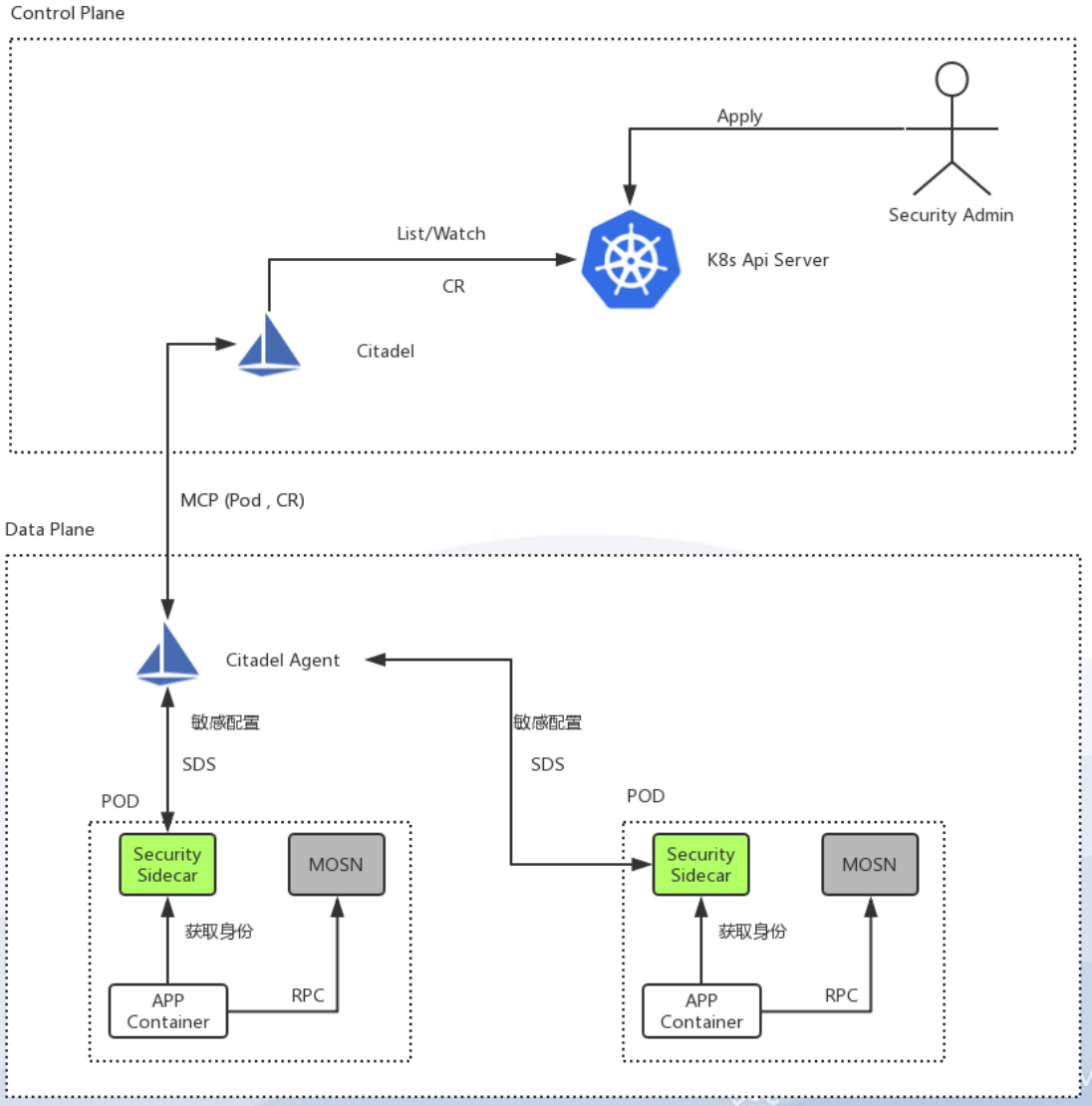


使用可信身份服务构建敏感数据下发通道

密钥更新通道

安全Sidecar 的认证能力中依赖密钥等敏感信息，在参考社区SDS方案的基础上，实现敏感信息的管理及安全下发通道。

- 用户将密钥等信息通过CRD方式提交至K8s，通过K8s的RBAC方式控制访问权限
- 拓展Citadel Watch 密钥相关的CR，筛选后下发至对应的Citadel Agent节点
- 安全Sidecar 与 Citadel Agent 采用基于UDS通信的Grpc服务获取密钥等敏感信息



Service Mesh Sidecar 的TLS 生产级落地实践

TLS 实践难点

证书管理 → SDS 证书管理方案

开关切换 → ISTIO Policy | Mesh Policy

灰度控制 → ScopeConfig

Service Mesh Sidecar 的TLS 生产级落地实践

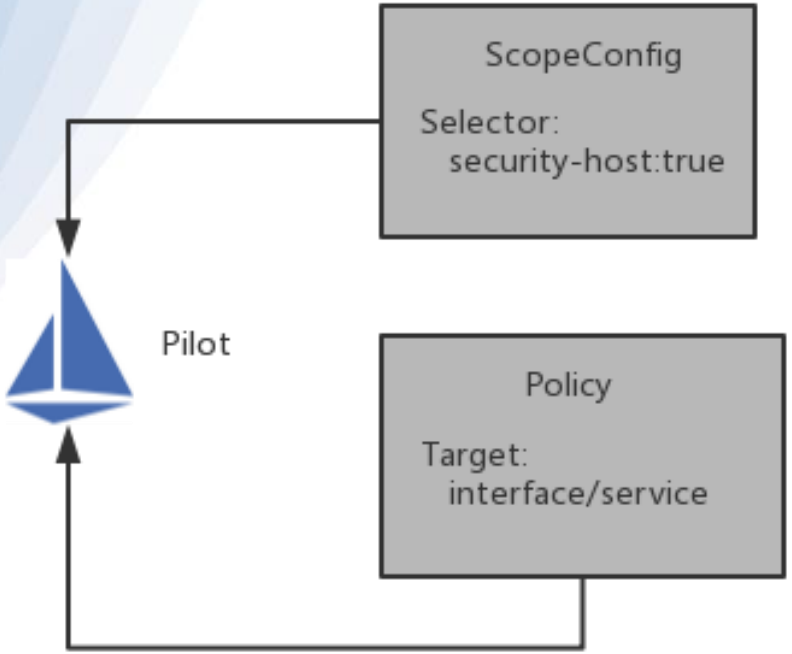
开关切换

RPC 通信场景下，为保证平滑无损的TLS切换能力，需要分别控制 Server (Provider) 和 Client (Consumer)端的 TLS 行为

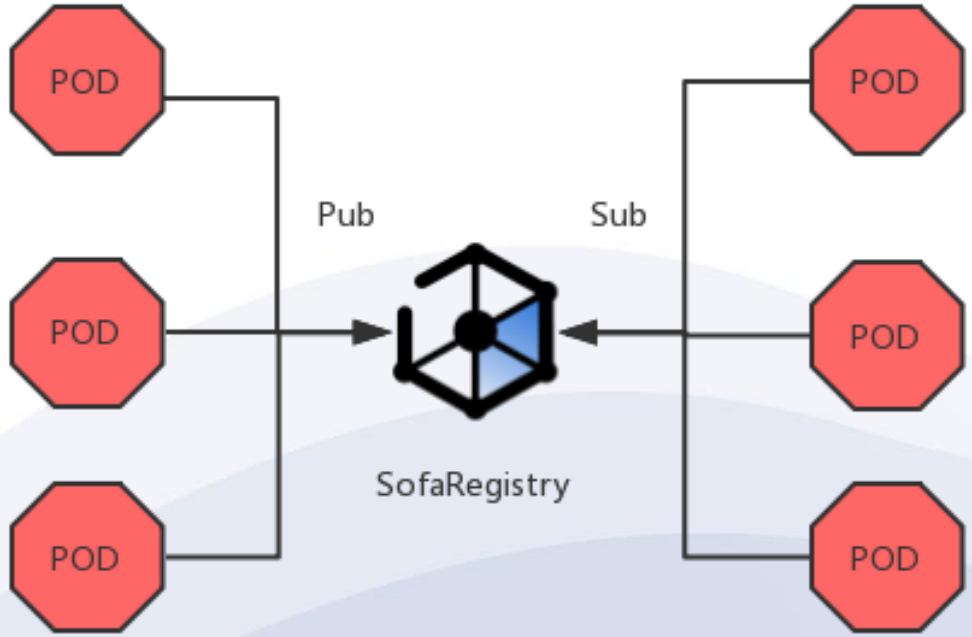
- 对于Server 端利用Istio 的Policy CRD 实现 Namespace + Service 粒度的开关控制
- 对于Client 端理想情况下，希望是通过Istio 的 DestinationRule 和 VirtualService 来控制。但由于相关条件尚未具备，因此通过现有注册中心来控制 Client TLS 能力

Service Mesh Sidecar 的TLS 生产级落地实践

Server Control



Client Control



Service Mesh Sidecar 的TLS 生产级落地实践

灰度控制

新功能总是离不开灰度过程，社区已有的Policy CRD 实现 Namespace + Service 的灰度能力不能满足蚂蚁金服生产落地的要求，需要具备单机灰度、回滚能力。

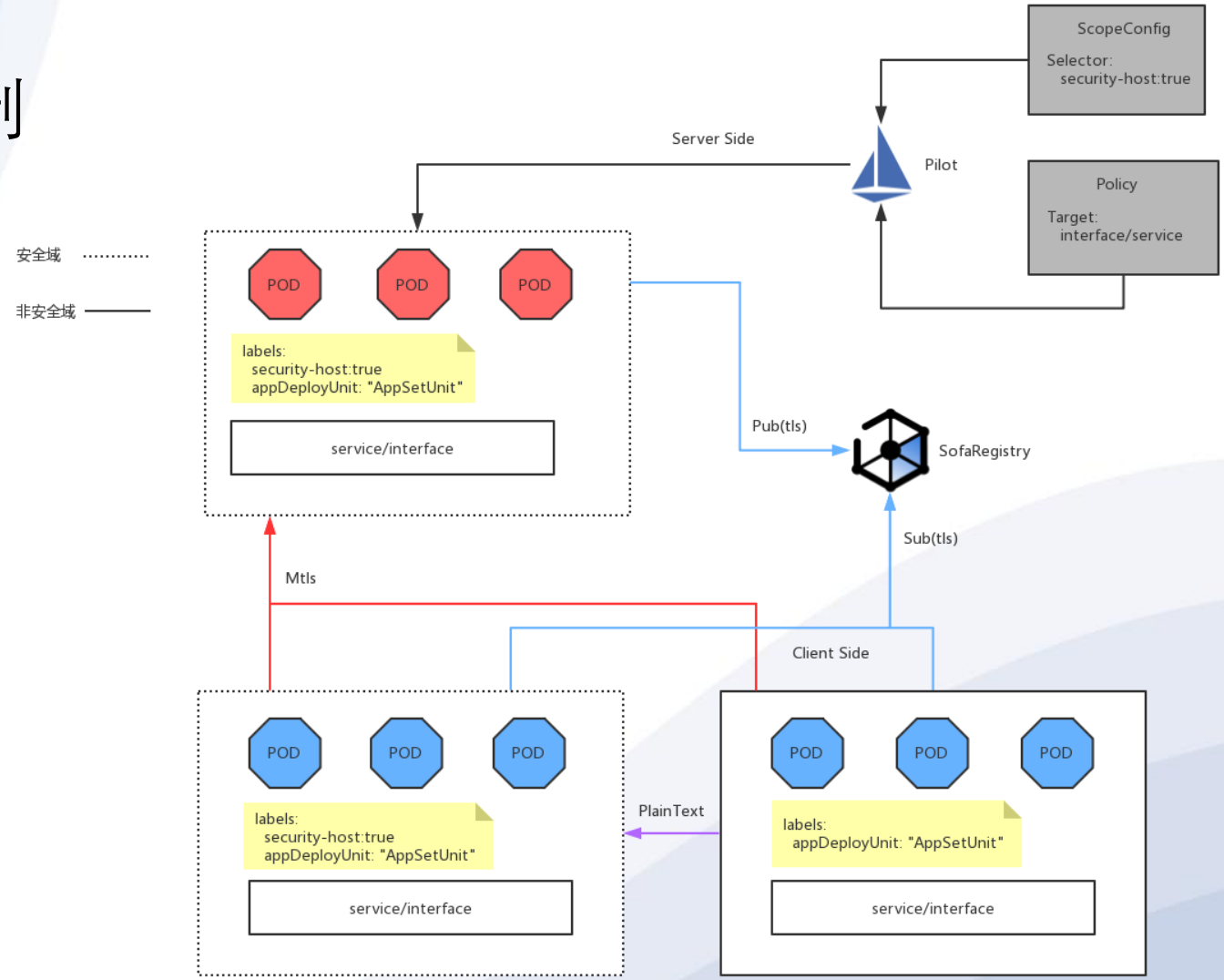
借鉴社区 SourceLabel 和 Sidecar CRD 的设计思路，创造性提出具备“正交”组合能力的ScopeConfig 方案

ScopeConfig 方案是通过label selector 能力选择指定范围内（批量 or 单实例）的Pod 实例，同时关联社区现有CRD，从而实现保留在兼容社区CRD设计方面的灵活性，又能实现任意CRD的更细粒度控制能力

以TLS 开关为例，在发布TLS开关时，先提交 ScopeConfig 通过 Pod IP 这个label 实现单实例开关控制，在观察正常后，逐步调整ScopeConfig 的Selector 范围，实现功能的灰度上线能力

Service Mesh Sidecar 的TLS 生产级落地实践

灰度控制



关注 **ServiceMesher** 微信公众号
获取社区最新信息

关注 金融级分布式架构 微信公众号
获取 **SOFAStack** 最新信息

ServiceMesher 社区是由一群拥有相同价值观和理念的志愿者们共同发起，
于 2018 年 4 月正式成立，致力于成为 Service Mesh 技术在中国的布道者和领航者。
社区官网：https://www.servicemesher.com

蚂蚁金服 ANT FINANCIAL　ServiceMesher