

客户名称：北京完美创意科技有限公司

故障时间：

2020-06-05

报告类型：故障报告

故障报告

故障时段：

2020-06-05 22:09 ~ 22:53 及次日 1:09 ~ 1:50

故障影响：

2020-06-05 22:09 ~ 22:53 及次日 1:09 ~ 1:50 期间，按需在控制台调整 TKE Service 的访问模式后，该 Service 的 Port name 命名中协议由 HTTP 不符合预期的变为了 TCP，导致服务端口命名不符合 Istio 规范，Istio 默认按照 TCP 协议下发 filter，将 HTTP 流量作为 TCP 流量管理，请求异常。给您的业务造成影响，对此我们表示诚挚的歉意。同时，我们对本次故障的整个过程进行了深入的技术复盘。

故障处理及复盘过程：

- 23:50 腾讯云工程师收到报障，快速电话对齐故障相关信息；
- 23:57 搜集到足够的信息后，拉起腾讯会议紧急升级排查；
- 01:40 线上问题复现，通过日志，抓包等方式抓取现场信息；
- 01:47 发现故障原因为 Service 的端口命名不符合 Istio 规范；
- 01:50 紧急调整 Service 端口命名，线上恢复；
- 02:00 沟通临时解决方案和后续规避措施；

原因分析：

TKE 关联版本特性更新发布，对编辑 Service 访问方式及端口映射的前端适配覆盖不完全，会同步更新 Service 的端口名称，而 Istio 1.5 以前的版本默认通过 Service 端口名称的前缀识别协议，并下发对应协议 filter 至服务的 sidecar，sidecar 据此执行指定协议的服务通信流量的解析与管控能力。Service 端口名称更新后，Istio 无法从名称中正确识别对应端口的协议，默认按照 TCP 协议下发 filter 至服务的 sidecar 进行流量管理，导致请求异常。

Istio 1.1 官方文档相关描述截图：

The screenshot shows the Istio 1.1 documentation page for 'Pods and Services'. The page title is 'Pods and Services' with a sub-header '3 MINUTE READ'. The main content area explains that pods and services in a Kubernetes cluster must satisfy certain requirements. A red box highlights the 'Named service ports' requirement: 'Service ports must be named. The port name key/value pairs must have the following syntax: `name: <protocol>[-<suffix>]`. To take advantage of Istio's routing features, replace `<protocol>` with one of the following values:'. Below this, a list of protocols is provided: `grpc`, `http`, `http2`, `https`, `mongo`, `mysql`, `redis`, `tcp`, `tls`, and `udp`. Another red box highlights a note: 'For example, `name: http2-foo` or `name: http` are valid port names, but `name: http2foo` is not. If the port name does not begin with a recognized prefix or if the port is unnamed, traffic on the port is treated as plain TCP traffic unless the port explicitly uses Protocol: UDP to signify a UDP port.' A third red box highlights the 'Pod ports' requirement: 'Pods must include an explicit list of the ports each container listens on. Use a `containerPort`'.

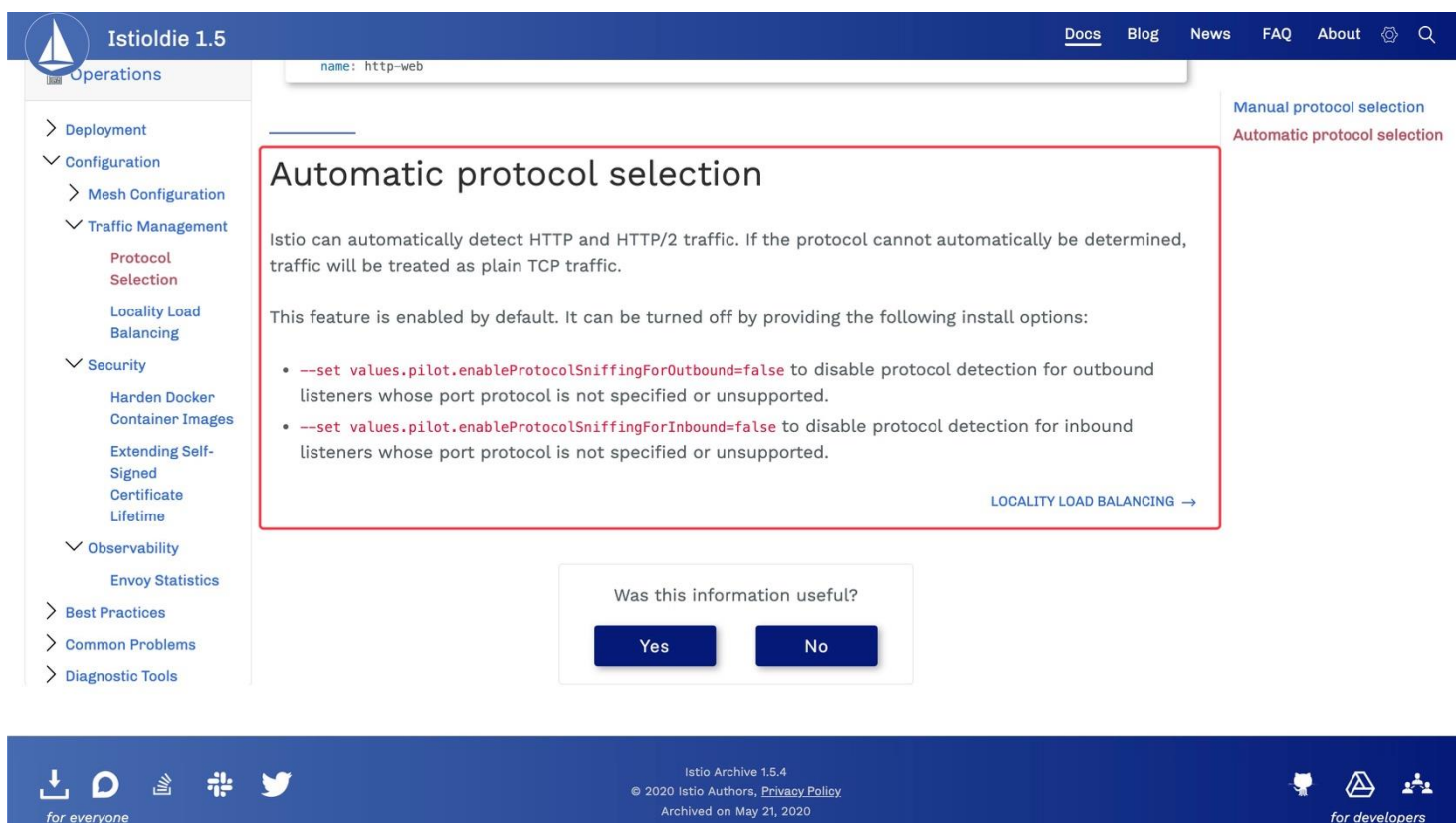
Istio1.1 官方文档相关描述链接: <https://archive.istio.io/v1.1/docs/setup/kubernetes/prepare/requirements/>

规避措施:

经过分析, 我们将从以下 3 个方面加强和改进:

1. 调整 TKE 前端编辑 Service 访问方式及端口映射的适配逻辑, 彻底规避问题, 已于 2020-06-06 凌晨修复完成上线。
2. 后续增强相关联产品依赖特性的检查和代码 Review。
3. 推动优化 Istio 开源版本:
 - a) Istio 1.5 版本可采用协议嗅探的方式自动探测和设置 HTTP 和 HTTP2 流量, 且默认开启 (相关配置项为 `values.pilot.enableProtocolSniffingForOutbound/Inbound`), Istio 1.5 版本上线后, 默认可自动通过嗅探的方式探测 HTTP 和 HTTP2 协议并下发对应协议的 filter 至 sidecar, 设置服务的端口协议。

Istio1.5 官方文档相关描述截图:



Istio 1.5 官方文档相关描述链接：<https://archive.istio.io/v1.5/docs/ops/configuration/traffic-management/protocol-selection/#automatic-protocol-selection>

- b) 推动开源版本通过控制面注册服务端口协议信息的方式，将 sidecar 通信协议 filter 的下发与 Kubernetes Service 端口名称解藕。

建议同步考虑 Istio 版本的升级，当前产品化流程已支持升级至 1.3.6，1.5 版本的升级也会在近期开放，升级工作腾讯云团队将会高优支持。

对于此次故障给贵司带来的困扰，项目组深表歉意，我们已经对事件进行了复盘升级，坚决杜绝此类事件的再次发生，感谢贵司对腾讯云一如既往的支持和信任！

腾讯云项目组

2020 年 06 月 06 日