

零信任访问配置文件删除导致用户访问丢失

目录

问题

在删除被认为未使用的零信任访问(ZTA)配置文件后，所有具有ZTNA模块的用户都完全无法访问私有资源和互联网导航。此配置文件的删除导致所有ZTNA用户的服务立即中断，阻止他们通过零信任网络访问基础设施访问任何资源。

受影响的用户无法建立连接：

- 私有内部资源
- 通过ZTNA模块进行互联网导航

环境

- 安全访问（零信任网络访问）
- 部署有多个用户配置文件的ZTNA模块
- 配置了ZTNA控制的默认策略
- 为用户访问管理配置多个ZTA配置文件

分辨率

了解ZTA配置文件匹配逻辑

零信任访问配置文件根据特定的匹配顺序和逻辑应用：

- 配置文件匹配顺序：根据用户和目标匹配条件按顺序评估ZTA配置文件
- 默认配置文件行为：当没有特定配置文件匹配用户或目标条件时，系统回退到默认配置文件
- 配置文件依赖关系：删除用作有效默认值的配置文件会导致服务中断，即使它看起来未使用

已删除的配置文件可能充当用户匹配的有效默认配置文件，尽管在配置界面中似乎未使用。删除此配置文件后，用户将失去通过ZTNA基础设施的主要访问路径。

验证步骤

为了防止将来出现类似问题，需要实施以下验证方法：

1. — 在删除之前查看所有已配置的ZTA配置文件及其匹配条件。
2. — 确定哪个配置文件用作用户访问的有效默认值。
3. — 通过配置屏幕截图和策略检查验证用户到配置文件的映射。
4. — 在申请生产前以受控方式测试剖面的变化。

原因

根本原因是删除了充当ZTNA用户访问的有效默认配置文件的ZTA配置文件，尽管该配置文件在配置界面中未被使用。删除此配置文件后，系统丢失用户访问的主要匹配条件，导致所有ZTNA用户失去与专用资源和互联网导航的连接。配置文件匹配逻辑取决于当其他已配置的配置文件未满足特定用户或目标条件时，是否有一个有效的默认配置文件可供回退。

相关内容

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。