

零信任訪問配置檔案刪除導致使用者訪問丟失

目錄

問題

在刪除被認為未使用的零信任訪問(ZTA)配置檔案後，所有使用ZTNA模組的使用者都完全無法訪問專用資源和網際網路導航。此配置檔案的刪除導致所有ZTNA使用者的服務立即中斷，阻止他們通過零信任網路訪問基礎設施訪問任何資源。

受影響的使用者無法建立連線：

- 專用內部資源
- 通過ZTNA模組進行網際網路導航

環境

- 安全訪問 (零信任網路訪問)
- 部署有多個使用者配置檔案的ZTNA模組
- 配置了ZTNA控制的預設策略
- 為使用者訪問管理配置多個ZTA配置檔案

解析

瞭解ZTA配置檔案匹配邏輯

零信任訪問配置檔案根據特定的匹配順序和邏輯應用：

- 配置檔案匹配順序：ZTA配置檔案根據使用者和目標匹配條件按順序評估
- 預設配置檔案行為：當沒有特定配置檔案與使用者或目標條件匹配時，系統回退到預設配置檔案
- 配置檔案相關性：刪除充當有效預設設定的配置檔案會導致服務中斷，即使該配置檔案看起來未使用

刪除的配置檔案可能充當使用者匹配的有效預設配置檔案，儘管在配置介面中出現未使用的配置檔案。刪除此配置檔案後，使用者會丟失通過ZTNA基礎設施的主要訪問路徑。

驗證步驟

為了防止將來出現類似問題，需要實施此驗證方法：

1. — 刪除前，檢查所有配置的ZTA配置檔案及其匹配條件。
2. — 確定哪個配置檔案是使用者訪問的有效預設配置檔案。
3. — 通過配置螢幕截圖和策略檢查驗證使用者到配置檔案的對映。
4. — 在申請生產前測試輪廓以受控方式變化。

原因

根本原因是刪除了作為ZTNA使用者訪問的有效預設配置檔案的ZTA配置檔案，儘管該配置檔案在配置介面中未被使用。刪除此配置檔案後，系統丟失使用者訪問的主要匹配條件，導致所有ZTNA使用者失去與專用資源和網際網路導航的連線。配置檔案匹配邏輯取決於當其他已配置的配置檔案未滿足特定使用者或目標條件時，是否有一個有效的預設配置檔案可供回退。

相關內容

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。