

安全訪問ZTNA RDP專用資源訪問某一特定資源失敗

目錄

問題

使用者無法通過Cisco Secure Access Zero Trust Network Access(ZTNA)訪問一個特定RDP專用資源。嘗試連線時，使用者收到「內部錯誤」消息。該問題影響了多個使用者（包括新新增的使用者），並阻止在家工作使用者訪問所需的案頭資源。其他RDP資源和非RDP專用資源仍然可供訪問，這表明問題特定於此特定資源配置。

環境

- 思科安全存取 — 零信任網路存取(ZTNA)
- 使用RDP協定的專用資源配置
- Active Directory(AD)基於組的訪問策略
- IP地址重疊的多個專用資源配置
- 基於客戶端的註冊和狀態評估

解析

通過識別並糾正專用資源設定中的配置衝突解決了此問題。下面各節中介紹的步驟已用於解決此問題。

確定配置衝突

調查顯示特定的RDP資源配置在多個專用資源下：登入到CSA Dashboard > Connect > End User Connectivity > Under Zero Trust Access > Add a ZTA profile > Give a Name，然後搜尋特定目標。

刪除衝突的IP地址分配

已從衝突的專用資源中刪除IP地址172.26.106.136。

IP地址僅保留在與使用者的Active Directory組成員資格和訪問策略要求相匹配的適當資源下。

驗證使用者組成員身份

已確認，遇到訪問問題的新新增使用者不是根據配置的訪問策略進行訪問所需的正確Active Directory(AD)組的成員。

此外，請確保正確的AD組或使用者與零信任訪問配置檔案關聯。

配置更改後測試訪問

實施配置更改後，使用者能夠根據需要成功訪問RDP資源。已確認問題已解決，並且使用者可以在不收到「內部錯誤」消息的情況下進行連線。

原因

問題的根本原因是配置衝突，其中將特定資源分配給具有不同訪問策略的多個專用資源。這造成了一種情況，即根據使用者沒有適當Active Directory組成員資格的策略對使用者進行評估，導致拒絕訪問和「發生內部錯誤」消息。新新增的使用者不是衝突策略所需的正確AD組的成員，這阻止了他們訪問資源，即使他們必須通過相應的策略具有訪問許可權。

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）。