

使用SysPrep Golden映像解決安全訪問部署中的重複ZTNA裝置ID

目錄

問題

從SysPrep金色映像部署的多台Windows物理電腦正在生成相同的ZTNA裝置ID，尤其是跨多個終端的同一ztnaDeviceId。這種複製會導致幾個關鍵問題：

- 重複重新註冊具有相同ZTNA裝置ID的裝置
- 在每個重新註冊過程中進行公鑰覆蓋
- 除最近註冊的裝置外，所有電腦上的狀況檢查失敗
- 通過受影響終端的安全訪問發生訪問故障

當隊列中的多台電腦共用同一個ZTNA裝置ID時，將發生觀察到的行為，導致每次註冊都覆蓋上一台電腦的公鑰。除了要註冊的最新電腦外，所有電腦都無法傳送狀態檢查，從而導致通過Secure Access基礎設施拒絕訪問。

有多個主機名和使用者ID對被標識為連結到同一個ZTNA裝置ID，從而演示了整個部署中的重複問題的範圍。

環境

- 思科安全存取（ZTNA實作）
- Windows物理電腦（非虛擬機器）
- SysPrep金色映像部署方法
- 用於映像部署的Windows ADK（評估和部署工具包）工具
- 用於影象捕獲的ESD（電子軟體交付）檔案格式

- 包括強制軟體安裝的標準化作業系統加固流程
- 標準本地管理員和訪客帳戶配置

解析

解決過程包括全面的日誌分析和通過詳細調查查明根本原因。

確定並解決根本原因

調查發現，SysPrep流程在金色映像部署過程中無法正確生成唯一的裝置識別符號。

分析內容包括：

檢查Windows登錄檔項，特別是：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion

使用下列方式收集使用者安全識別符號資訊：

whoami /user

解決方法需要修改SysPrep流程，以確保在部署過程中正確重新生成裝置特定的識別符號，從而防止在多個物理電腦上重複ZTNA裝置ID。

- 通過運行dartcli.exe -nu 命令來續訂UDID，從而更改「HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails」登錄檔路徑下Nounce的值。
- 從C:\ProgramData\Cisco\Cisco刪除JSON檔案安全客戶端\ZTA\enrollments和重新啟動ZTA服務將取消使用者的註冊。您需要手動註冊使用者。這將生成一個新的JSON檔案，並且沒有任何其他影響。
- 只要未在任何伺服器上驗證/評估值，在所有端點上續訂UDID不得有任何影響。

1.以管理員身份啟動命令提示符並轉到「%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART」目錄。

2.運行dartcli.exe -u以檢查當前UDID的值。

3.運行dartcli.exe -nu命令。此命令將更新UDID。

4.重複步驟2中的命令以驗證新值。

5.從C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments目錄刪除JSON檔案

6.重新啟動VPN和ZTA服務。此時，ZTA必須處於未註冊狀態。

7.讓使用者手動註冊ZTA

9.驗證JSON檔案中新ztnaDeviceId的值。

監控和驗證

實施糾正措施以確保唯一的ZTNA裝置ID生成之後：

- 已監視多台電腦的註冊過程
- 已驗證每台電腦生成的唯一ZTNA裝置ID
- 在所有已註冊裝置上確認成功的狀況檢查功能
- 已驗證在註冊期間不再發生公鑰覆蓋

原因

根本原因是未正確為ZTNA註冊生成唯一裝置識別符號的SysPrep金色映像部署過程。當從同一SysPrep金色映像部署多個Windows物理電腦時，用於生成ZTNA裝置ID的特定裝置識別符號在所有已部署電腦中保持相同。

SysPrep流程雖然對標準化作業系統配置和軟體部署有效，但沒有配置為重新生成思科安全客戶端用於建立唯一ZTNA裝置ID的特定識別符號。這導致所有部署於同一黃金映像的機器繼承相同的ZTNA裝置識別引數，從而導致安全訪問基礎架構中的註冊衝突和身份驗證失敗。

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）。