將安全訪問AD聯結器從傳統身份驗證遷移到API身份驗證

目錄

問題

使用Cisco Secure Access with Active Directory(AD)聯結器的組織會收到通知，指出建議對Active Directory和虛擬裝置使用API身份驗證，並且舊身份驗證設定為於2026年5月29日過期。使用者需要配置幫助才能在到期日期之前從傳統身份驗證遷移到API身份驗證，並希望瞭解遷移過程中對AD和虛擬裝置同步的潛在影響。主要關注點是，在工作時間內實施此更改是否會導致AD和VA同步操作失敗，從而影響身份和策略相關操作。

環境

- 思科安全存取（前身為Cisco Umbrella）
- 已部署Active Directory聯結器
- 當前使用的舊版身份驗證方法
- 2026年5月29日之前需要API身份驗證遷移
- 僅限於AD的環境（某些情況下不使用虛擬裝置）

解析

從傳統身份驗證遷移到API身份驗證涉及在安全訪問門戶中生成API金鑰並正確配置它們。此過程要求為AD聯結器和虛擬裝置建立管理API金鑰和客戶端API金鑰。

步驟 1:生成管理API金鑰

在安全訪問門戶中導航到Admin > API Keys，並生成新的Admin API Key和Admin Key Secret。在生成客戶端API金鑰對時需要安全地儲存這些憑據。

步驟 2:生成客戶端API金鑰對

導航到Users and Groups > Configuration Management > Advanced Settings，然後找到API Authentication部分。輸入步驟1中生成的Admin API Key和Admin Key Secret，然後按一下Generate Client API Key Pair。這會生成AD聯結器和虛擬裝置使用的客戶端API金鑰和客戶端密碼。

步驟 3:在高級設定中配置API身份驗證

將生成的客戶端API金鑰和客戶端金鑰複製到安全訪問門戶的API身份驗證高級設定部分。按照所有AD聯結器和虛擬裝置配置的要求安全地儲存這些憑據。

步驟 4:更新AD聯結器和虛擬裝置

將新生成的客戶端API金鑰和客戶端金鑰應用於所有部署的AD聯結器和虛擬裝置。這可確保他們可以使用新的API身份驗證方法針對註冊和運行狀況檢查正確進行身份驗證。

遷移影響和最佳做法

在安全訪問門戶中生成API金鑰通常不會造成中斷。但是，在切換期間，當AD聯結器和虛擬裝置更新為使用新的客戶端API金鑰和金鑰時，會發生操作影響。

轉換期間的預期影響：

- 對於仍使用舊版身份驗證的元件，可能會發生臨時同步和運行狀況檢查失敗。
- AD/VA同步在轉換視窗期間延遲或失敗。
- 如果同步失敗，依賴於新的身份/組資料的策略決策可能會受到影響。

推薦的實施方法：

- 在非工作時間或可能的情況下在維護時段執行遷移。
- 對於工時實施，請使用控制滾動更新方法。
- 每次更新一個聯結器/VA並在繼續之前驗證健康狀態。
- 避免同時更新所有節點。
- 使用多個聯結器/VA確保足夠的冗餘以進行滾動更新。

相容性和要求：

- API身份驗證適用於僅AD部署，不需要虛擬裝置。
- 在遷移期間，傳統身份驗證方法和API身份驗證方法均保持活動狀態。
- AD聯結器必須能夠通過api.opendns.com與Umbrella同步並過渡到api.umbrella.com。

原因

思科安全訪問正在從傳統身份驗證方法過渡到作為標準身份驗證機制的API身份驗證。傳統身份驗證方法的預定棄用日期為2026年5月29日。API身份驗證最終成為唯一受支援的身份驗證方法，組織必須在舊方法過期之前進行遷移，以避免服務中斷和可能發生的AD/VA同步故障（可能需要完全重新安裝才能恢復）。

相關內容

- Cisco安全存取API驗證檔案
- 思科安全訪問高級配置
- 思科安全存取組態管理
- 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）。