對Umbrella Active Directory中的本地帳戶應用策略

目錄

簡介

本文檔描述了將Umbrella內部部署產品與Active Directory和本地使用者帳戶同步時的預期策略行為。

Umbrella虛擬裝置和本地帳戶標識

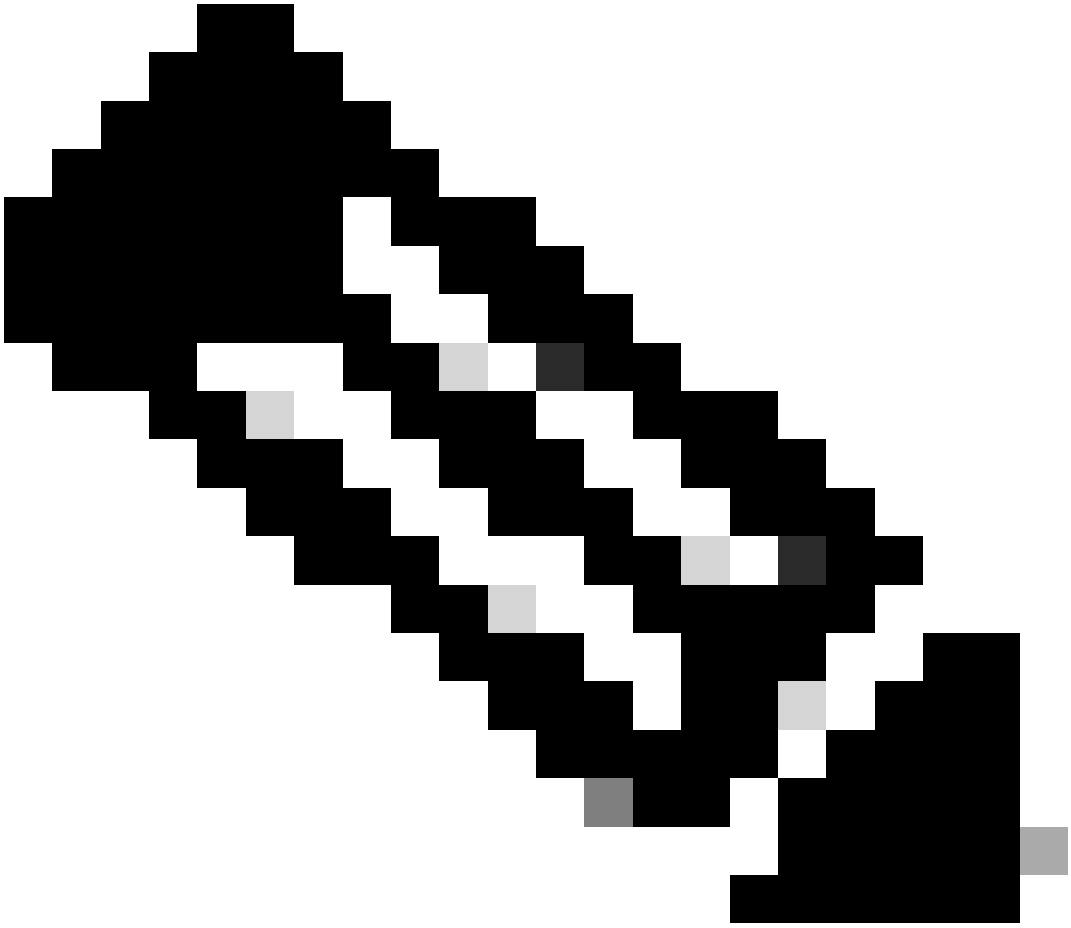
Umbrella虛擬裝置從Windows域控制器接收Active Directory登入資訊。它基於源IP地址快取和標識Active Directory使用者。

- 域控制器不會跟蹤本地使用者登入，因此虛擬裝置無法直接識別這些使用者。
- 如果某個Active Directory使用者最近從IP地址登入，仍可以根據快取使用快取的標識。虛擬裝置無法知道已用本地帳戶替換了AD使用者。
- 如果不存在快取使用者，則虛擬裝置使用預設（非AD）標識。觸發的標識可以是：
  - Umbrella站點名稱（例如，預設站點）
  - 內部網路（內部IP地址）
  - 網路（外部IP地址）

針對Umbrella虛擬裝置的建議

- 限制對本地帳戶和密碼的訪問。
- 為Umbrella站點名稱建立單獨的策略（例如，預設站點）。 將此策略的優先順序分配給低於標準Active Directory使用者策略的優先順序。如果未檢測到AD使用者，則應用此更嚴格的策略。
- 如果本地使用者帳戶需要不同的策略，請考慮部署Umbrella漫遊客戶端。

Umbrella漫遊客戶端和本地帳戶策略



附註：要將Active Directory與漫遊客戶端整合，請導航到Identities > Roaming Computers，並啟用設定Enable Active Directory使用者和組策略實施。

漫遊客戶端從Windows登錄檔中檢測登入使用者，從而允許通過其唯一的AD GUID標識Active Directory使用者。

- 漫遊客戶端無法識別本地使用者名稱以用於策略目的。
- 當檢測到AD使用者時，AD使用者身份適用於策略實施，包括離線時使用快取憑據登入的AD使用者。
- 如果未檢測到任何AD使用者（例如，當本地使用者登入時），則使用漫遊電腦標識執行策略。

Umbrella漫遊客戶端建議

- 限制對本地帳戶和密碼的訪問。
- 為漫遊電腦建立一個單獨的策略，該策略的優先順序低於標準AD使用者策略。此策略適用於未加入域或本地使用者使用的漫遊電腦。

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）。