使用VA或CSC整合Active Directory

目錄

簡介

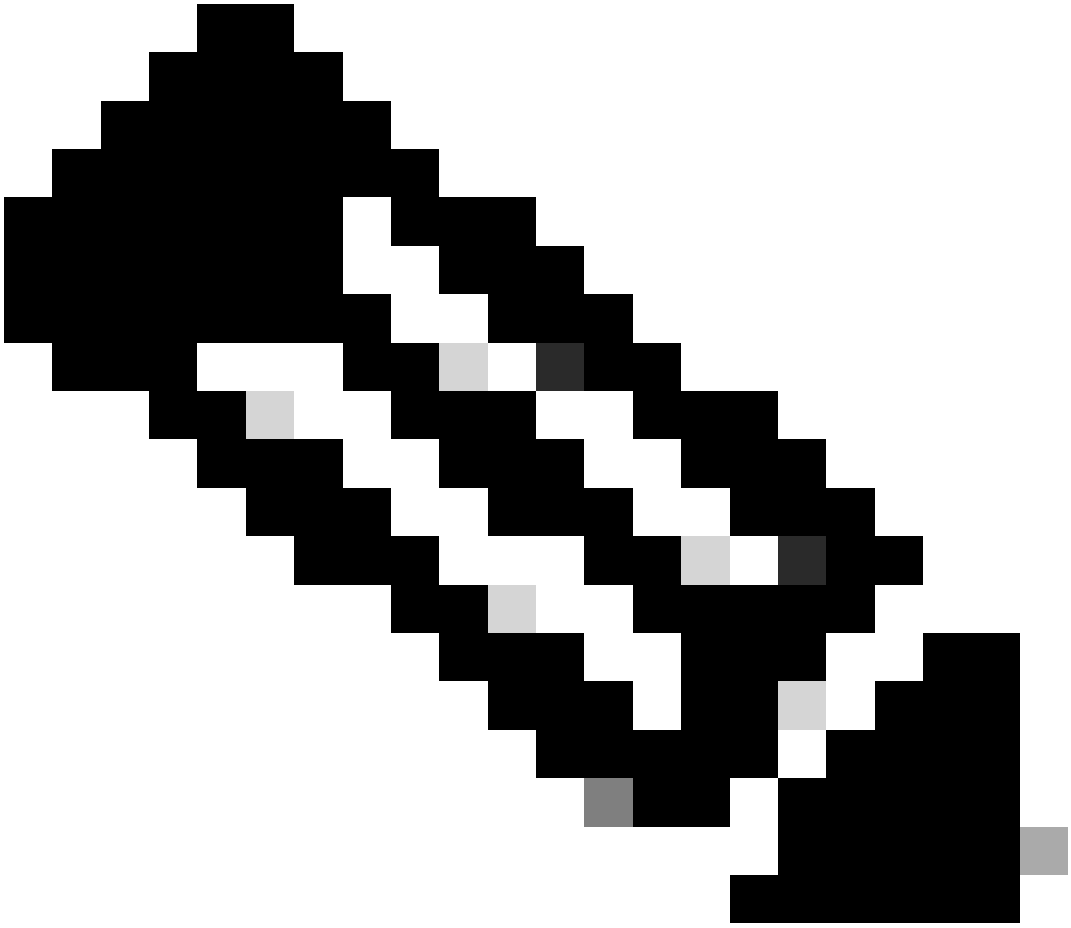
本文檔介紹將Active Directory(AD)與Umbrella整合的兩種方法：虛擬裝置(VA)或思科安全客戶端(CSC)。

必要條件

需求

思科建議您瞭解以下主題：

- AD聯結器:將單個Active Directory域的AD樹同步到儀表板。對於VA實施，它還主動將登入事件從同一Umbrella站點上的DC同步到VA。組織的AD樹通過AD聯結器同步到Umbrella雲，從註冊的DC提取此資料。檢測到樹更新，並在數小時內更新Umbrella雲。
- 域控制器（AD伺服器）:DC通過從儀表板下載的註冊配置.wsf指令碼註冊到儀表板。這會將其名稱、域和內部IP新增到儀表板，以通知聯結器嘗試與哪些IP同步。如果無法運行該指令碼，也可以手動註冊。如需詳細資訊和支援，請聯絡Umbrella支援。
- 虛擬裝置:Umbrella內部部署DNS轉發器。在網路上應用（可選）AD身份，並在報告上應用內部IP。這將觸發其後面的所有漫遊客戶端禁用DNS保護並推遲到「VA保護後面」模式。
- 思科安全使用者端:Umbrella本地軟體服務，為Windows和macOS提供DNS加密以及使用者識別。也作為AnyConnect模組提供。



附註：兩種實施之間的先決條件明顯不同。請參考具體實施以瞭解完整的先決條件。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

本文闡明並探討了將Active Directory與Umbrella Dashboard整合的兩種不同方法。目前，可以通過Umbrella虛擬裝置或思科安全客戶端將AD使用者應用於策略和報告。

安全客戶端實施

需求

- 一個AD聯結器
- 控制面板上有一個DC
- OpenDNS_Connector使用者必須具有只讀域控制器許可權。
- 獨立客戶端（AnyConnect模組）的安全客戶端最低版本：
  - Windows:2.1.0(4.5.01044)
  - OSX:2.0.39(4.5.02033)。

工作方式

- 當前登入的AD使用者由讀取本地登錄檔的漫遊客戶端在本地電腦上直接確定。
- 支援工作站上最多有一個併發登入使用者。
- 兩個併發使用者可能導致沒有AD使用者應用。
- AD使用者GUID和內部IP通過漫遊客戶端的DNS代理中的EDNS0附加到傳送到Umbrella解析器的DNS查詢，以唯一標識AD使用者。
- 所有策略都應用於解析程式端。
- 不需要活動聯結器。但是，AD使用者和組策略應用程式可以反映最近成功的AD樹同步。

工作場所

- 任何全域性網路。
- 在Umbrella虛擬裝置後無法工作，因為DNS層被禁用以服從本地VA。

限制

- 要求終端代理處於活動狀態並在工作站上啟用。
- 不支援伺服器OS。
- 無法基於內部網路IP應用策略。
- 無法為AD電腦應用策略或報告（請改用漫遊主機名）。

聯結器仍可以嘗試從註冊的一個DC拉取AD登入事件。這可能會導致儀表板錯誤，該錯誤與基於漫遊客戶端的AD整合無關。要移除許可權相關的錯誤，而不實際拉入任何事件，請通過此處稽核說明的相反方向禁用登入事件稽核（如果未使用）。

虛擬裝置實施

需求

- 每個Umbrella站點兩個VA
- 每個Umbrella站點一個AD聯結器（冗餘的第二個，可選）
- 每個DC（不是只讀DC）都必須註冊到儀表板。
- OpenDNS_Connector使用者必須擁有完整的先決條件許可權。
- 必須啟用登入事件才能記錄所有DC上的4624安全事件日誌。檢視完整的故障排除提示。

工作方式

- VA接收基於Windows DC的安全登入事件日誌的AD使用者對映。
- 每個工作站登入都將作為唯一登入事件登入到登入伺服器DC的安全事件日誌，並使用AD使用者名稱或AD電腦名稱以及工作站的內部IP。
- 聯結器通過WMI訂閱即時分析這些事件，並通過TCP 443將這些事件同步到Umbrella站點上的每個VA。
- VA在AD使用者/電腦的內部IP與AD使用者/電腦的使用者名稱之間建立即時使用者對映。
- VA僅能檢視DNS查詢的內部源IP，並利用由聯結器同步事件建立的上述對映檔案。VA無法直接檢視當前登入到電腦的人員。這會將AD使用者GUID和通過EDNS0的內部IP附加到VA傳送到Umbrella解析器的DNS查詢，該查詢唯一標識AD使用者。
- AD電腦雜湊以相同方式應用。
- 所有策略都應用於解析程式端。
- 聯結器必須在組織中保持正常運行並處於活動狀態，才能接收AD使用者，並且登入事件必須是最新的。
- 使用者必須是最後一個AD使用者，才能向此電腦進行身份驗證，如事件日誌中所示。

工作場所

在本地公司網路中，所有DNS都指向與使用者驗證的DC屬於同一Umbrella站點的Umbrella虛擬裝置。

限制

- 電腦無法指向屬於其他AD域或Umbrella站點的VA（多個域上的大型部署無法從其基本網路中看到AD應用程式）。
- 大型部署可能需要使用單獨的VA細分到Umbrella站點。
- 服務AD使用者可能需要AD使用者例外。
- 前面提到的聯結器存在每秒最大登入事件吞吐量，該吞吐量可以延遲使用者應用。這是網路延遲和VA數量的因素。

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）。