使用Umbrella Active Directory聯結器進行身份驗證

目錄

簡介

本文檔介紹如何使用Umbrella Active Directory聯結器通過802.1x、Radius或ISE進行身份驗證。

概觀

Cisco Umbrella Active Directory(AD)Connector的工作方式是將AD使用者/電腦對映到內部IP地址。為使對映正確，AD使用者必須根據配置為與Cisco Umbrella AD聯結器通訊的域控制器進行身份驗證。

如果您的AD使用者通過其他方式進行身份驗證，則可能根本不能在域控制器上生成登入事件，或者可能存在導致應用錯誤策略的意外對映。

通過802.1x、RADIUS或ISE進行身份驗證

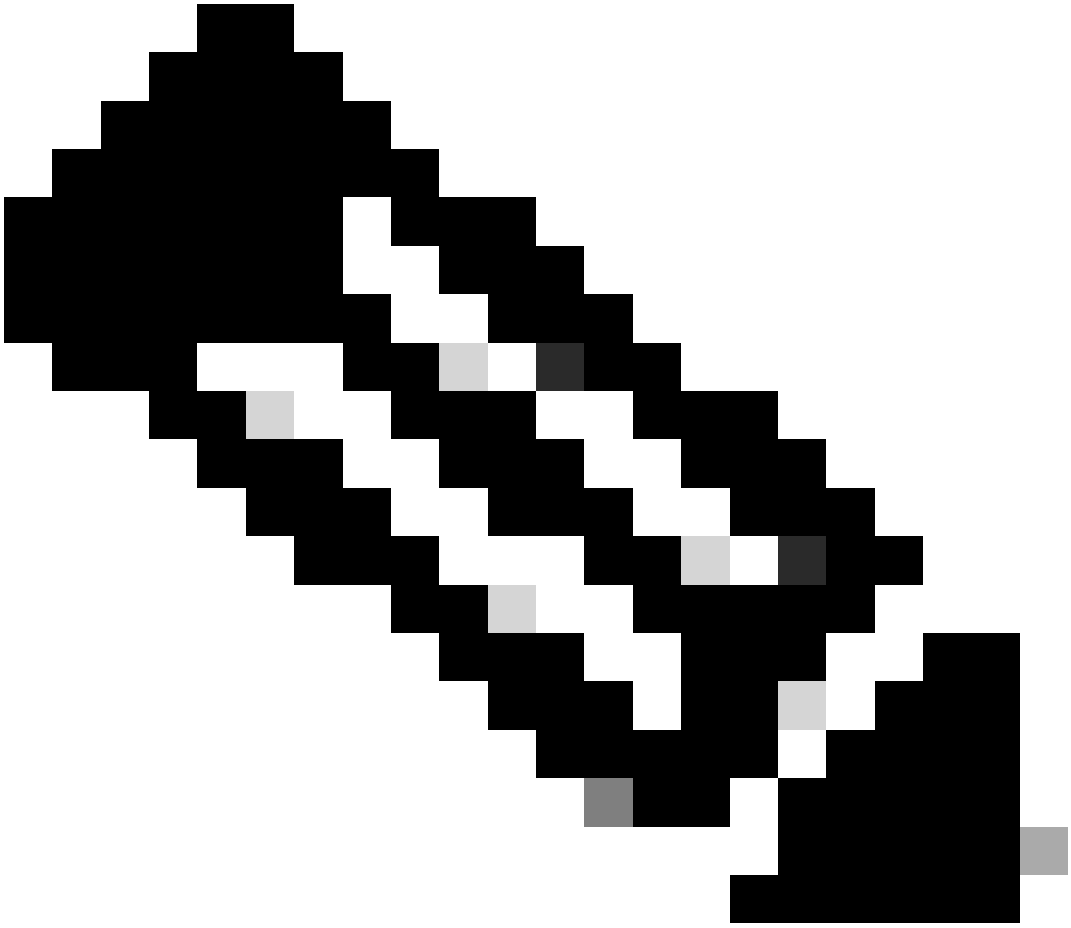
由於Active Directory登入使用這些解決方案的方式存在限制，不支援通過802.1x、RADIUS或ISE進行身份驗證。AD聯結器查詢的登入事件通常不會生成。

在此處瞭解AD聯結器查詢的事件ID:聯結器服務正在查詢哪些視窗事件/事件ID?

最常見的是，身份驗證服務的IP地址對映到AD使用者，而不是使用者電腦的IP地址。

替代解決方案

AD整合也可以通過使用已啟用身份支援功能的漫遊客戶端來實現。有關此功能的詳細資訊，請參閱我們的部署文檔。



附註：此解決方案要求網路上不存在虛擬裝置，因為這會導致漫遊客戶端進入禁用的「VA後」狀態。

如果在網路中使用虛擬裝置，則可以使用內部IP地址進行標識。例如，可以為無線網路的地址範圍建立「內部網路」標識，然後對此標識應用策略。此方法的唯一缺點是此地址範圍內的所有裝置都收到相同的策略。

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）。