部署Secure Access虛擬裝置後離線整合Active Directory

目錄

問題

部署兩個Secure Access虛擬裝置(VA)後，Active Directory(AD)整合在Secure Access儀表板中停止運行。以前，AD整合可正常運行，但在VA部署後，AD聯結器現在在Secure Access儀表板中顯示為離線。需要幫助才能還原AD連線。

環境

- 技術：解決方案支援（SSPT — 需要合約）
- 子技術：安全訪問
- 軟體版本:ALL
- 安全存取(DNS-Advantage/Umbrella)
- 在總部部署兩個安全訪問虛擬裝置(VA)
- 更改事件：在AD聯結器出現故障之前立即安裝VA
- AD聯結器以前可正常運行，現在在Secure Access門戶中顯示為離線

解析

要解決VA部署後AD整合在Secure Access門戶中顯示為離線的問題，請執行以下詳細故障排除步驟：

在聯結器重新啟動期間捕獲網路流量

在重新啟動聯結器服務的同時，在AD聯結器/域控制器的所有介面上運行Wireshark捕獲。這有助於識別在聯結器初始化期間的任何網路通訊故障或未經授權的訪問嘗試。

第1步：在所有相關介面上啟動Wireshark捕獲

啟動Wireshark並開始捕獲所有AD聯結器/域控制器介面。

第2步：通過Windows服務管理器重新啟動聯結器服務

開啟services.msc，找到OpenDNS Connector service，然後按一下Restart。

第3步：儲存捕獲檔案以進行進一步分析

停止捕獲並匯出.pcap檔案。

收集聯結器日誌

從AD聯結器收集日誌，以便更深入地瞭解錯誤或驗證問題：

1. 導航到日誌目錄。

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\vX.X.X
```

1. 收集相關日誌檔案並準備進行檢視。將所有日誌檔案從上述目錄複製到安全位置。

驗證AD聯結器帳戶許可權

引入虛擬裝置後，AD聯結器帳戶需要特定許可權才能正常運行。如果帳戶缺少事件日誌讀取器角色，則可能會遇到未經授權的訪問異常。

1. 為AD聯結器帳戶分配事件日誌讀取器許可權。使用Active Directory使用者和電腦(ADUC)或組策略將AD聯結器帳戶新增到事件日誌讀取器組。
2. 確認帳戶具有新許可權。請檢查AD聯結器帳戶的組成員身份，以驗證是否包含事件日誌讀取器。

發現常見異常

在故障排除過程中，在日誌或聯結器狀態輸出中可能會觀察到此異常：

```
* Exception type: system.unauthorizedaccessexception
message: Attempted to perform an unauthorized operation.
```

這表示AD聯結器帳戶沒有足夠的許可權，尤其是在VA引入後必須使用的事件日誌讀取器角色。

找不到CLI命令，顯示從AD聯結器狀態離線更改為聯機。

原因

根本原因是在部署安全訪問虛擬裝置後，AD聯結器帳戶的許可權不足。該帳戶缺少事件日誌讀取器許可權，這是正常AD聯結器功能所必需的。這將導致「system.unauthorizedaccessexception」錯誤，並阻止聯結器在安全訪問門戶中聯機操作。

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）。