對Azure虛擬案頭連線問題進行故障排除

目錄

問題

當使用者從啟用思科安全訪問的辦公室網路訪問AVD時，Azure虛擬案頭(AVD)連線失敗。觀察到以下特定行為：

- 當從禁用安全訪問的個人網路訪問時，AVD工作正常。
- 從沒有安全訪問的辦公室網路訪問時，AVD工作正常。
- 從任何啟用了安全訪問的網路訪問AVD時，AVD不起作用。

這種連線故障會影響使用者訪問其虛擬案頭的能力並影響生產業務運營。資料包捕獲分析顯示工作和非工作場景中的雙向流量，沒有TCP重置或其他網路級別指示安全訪問正在終止AVD連線。

環境

- 已啟用零信任網路訪問(ZTNA)的思科安全訪問
- ZTNA配置檔案配置為對所有網際網路目標使用ZTA
- 通過Microsoft終結點訪問的Azure虛擬案頭(AVD)部署
- 部署了安全訪問客戶端的辦公室網路環境
- 從辦公室和個人網路訪問AVD的使用者

解析

通過將Microsoft AVD相關域新增到ZTA例外清單來解決了此問題，從而允許安全訪問客戶端繞過

AVD流量的ZTNA。

診斷分析

聯合故障排除分析確定ZTNA配置檔案配置為對所有網際網路目標使用ZTA，這導致安全訪問通過Secure Access雲代理路由AVD的連續WebSocket流量。這種行為會導致會話丟棄，因為Azure虛擬案頭使用複雜的、連續的流量(WebSockets)來即時流式傳輸案頭會話，並且雲代理被設計為檢查標準網頁，而不是處理流協定。

配置更改

這些與Microsoft AVD相關的域已新增到ZTA例外清單：

```
*.wvd.microsoft.com
*.core.windows.net
*.servicebus.windows.net
*.events.data.microsoft.com
```

通過將這些域新增到ZTA例外清單，安全訪問客戶端被指示完全忽略特定於AVD的流量。這允許AVD流量直接進入Microsoft，完全繞過ZTNA代理，這正是Microsoft要求AVD正常運作的。

驗證

應用ZTA Exceptions配置後，在監控期間報告AVD連線正常工作。使用者能夠在啟用安全訪問的情況下，從辦公室網路成功訪問其虛擬案頭。

原因

根本原因是ZTNA配置檔案配置攔截了所有網際網路繫結的流量，包括Azure虛擬案頭連線。當AVD的WebSocket流量通過安全訪問雲代理進行路由檢查時，由於代理不是設計為處理AVD會話的持續流性質，因此會導致連線丟棄。AVD需要直接連線到Microsoft終端以保持穩定的案頭流會話。

相關內容

- Microsoft Azure虛擬機器所需的FQDN終結點
- 排除故障並收集思科安全訪問的基本資訊
- 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）。