

在安全訪問中排除專用應用的APP_UNREACHABLE故障

目錄

問題

當嘗試通過Cisco Secure Access訪問零信任網路訪問(ZTNA)應用時，使用者會遇到「Application Unreachable」（應用無法訪問）錯誤消息。

- 聯結器在儀表板中顯示正常/活動，並且應用程式已被其所有者確認正在運行。
- 當由同一聯結器服務的其它應用程式正常工作時，該故障可能影響一個應用程式的所有使用者。
- 在聯結器池部署中，故障可能間歇性出現 — 會話成功或失敗，具體取決於池中的哪個聯結器被選中。

環境

- 採用ZTNA的Cisco安全專用接入部署
- 為ZTNA訪問配置的專用資源
- 用於專用資源訪問的資源聯結器部署

解析

步驟1.測試聯結器網段的直接連通性

- 資源連結器是鎖定的裝置，不提供外殼訪問來直接運行命令，如curl或nc。相反，請從與連結器位於同一子網/VLAN中的測試主機（或臨時VM）執行可達性測試，以便它遵守與應用程式相同的網路路徑、路由和防火牆規則：

```
curl -v http://APP_IP:PORT/health
nc -zv APP_IP PORT
```

- 如果失敗，則問題在網路路徑或應用伺服器上得到確認 — 請先解決此問題，然後再檢視任何安全訪問配置。



附註：來自不同子網的測試不是決定性的 — 防火牆規則和路由是按源評估的，因為測試源必須儘可能密切地映象連結器的IP位置。

步驟2.檢驗專用資源配置

- 在安全訪問控制面板中，導航到Resources > Private Resources，開啟受影響的專用資源，並將配置的IP、FQDN和埠字元與正在運行的應用程式的實際繫結地址和埠進行比較。
- 任何不相符（伺服器遷移後過時的IP、錯誤的埠、HTTP與HTTPS）都會產生APP_UNREACHABLE，即使網路路徑非常健康。

步驟3.驗證連結器的DNS解析

- 如果專用資源由FQDN定義，請驗證分配給連結器的DNS伺服器是否可以解析它。在Resource Connector CLI（VM部署提供帶有支援的標準Linux故障排除命令的診斷CLI）中，運行：

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- 確認返回了正確的專用IP。確保連結器的網路配置點位於可解析專用應用程式FQDN的內部DNS伺服器；使用公共解析程式配置的連結器無法解析內部區域。

步驟4.檢查防火牆路徑

- 確認防火牆規則（網路防火牆和應用伺服器上的主機防火牆）允許從聯結器IP地址到所需埠上的應用伺服器IP的流量。

步驟5.在資源聯結器上使用tcpdump捕獲流量

- 在資源聯結器上運行資料包捕獲，觀察通往應用程式的最後一哩連線嘗試。資源聯結器上提供了tcpdump實用程式 — 請參閱[在資源聯結器上運行tcpdump](#)指南。



提示：要使捕獲在聯結器組部署中成為確定性的，請暫時在組中僅啟用一個Resource Connector，以便資源的所有會話都經過它，然後運行在應用程式伺服器和埠上過濾的捕獲。

- 舉例來說：

```
tcpdump 'host x.x.x.x and tcp port 443'
```

其中x.x.x.x是應用伺服器IP，443是應用埠)

- 解釋結果：沒有SYN-ACK的出站SYN表示防火牆丟棄或應用未偵聽；即時RST表示主機可連線，但沒有任何內容繫結到連線埠；任何指向應用的資料包都表示會話未到達此聯結器或DNS已解析到意外地址。
- 捕獲完成後，重新啟用組中的其餘聯結器。

原因

- 防火牆阻止聯結器到應用流量:基於網路或主機的防火牆阻止聯結器主機IP和應用伺服器IP之間的所需埠。
- 安全訪問中的專用資源配置不匹配:在專用資源定義(Resources > Private Resources)中配置的IP、FQDN或埠與應用程式實際偵聽的內容不匹配（例如，應用程式移動到新的IP，或偵聽配

置了443的8443) 。

- 聯結器的DNS解析故障:專用資源由FQDN定義，但聯結器DNS伺服器無法解析專用應用程式FQDN。
- 應用程式伺服器關閉或未偵聽:按照其他衡量標準，伺服器似乎運行正常，但未繫結到預期的埠，或者服務在主機保持正常狀態時崩潰。
- 聯結器池中的部分可達性:池中的一個或多個聯結器位於無法到達應用程式的網段中，因此只有分配給這些聯結器的會話會失敗。

相關內容

- [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）。