由於內部DNS配置，無法通過Azure中的安全訪問虛擬裝置訪問私有連結資源

目錄

問題

當流量通過Azure中部署的Cisco安全訪問虛擬裝置(VA)路由時，無法從Azure工作空間和工作負載訪問Azure專用連結資源。儘管將流量引導異常配置為繞過Azure專用域的安全訪問、啟用DNS回退並在VA上配置專用DNS，但此問題依然存在。

嘗試從Secure Access VA後面的Azure工作負載訪問Azure專用連結終結點會導致解決和連線失敗。

環境

- 在Azure中部署的思科安全訪問虛擬裝置(VA)
- Azure工作區和Azure託管的工作負載
- 已為專用Azure資源連線啟用Azure專用連結
- 配置為繞過Azure私有域的安全訪問的流量控制異常
- 在安全訪問VA內啟用DNS回退
- 在安全訪問VA中配置的專用DNS區域
- 軟體版本:ALL（問題與版本無關）

解析

解決方法涉及更新Cisco Secure Access VA中的DNS配置，以包含能夠解析Azure專用連結域的內部DNS伺服器條目。這些步驟詳細說明了所執行的故障排除和更正操作：

診斷安全訪問VA上的本地DNS配置

1. 要檢查現有DNS配置並確認是否設定了內部DNS伺服器，請在安全訪問VA上使用以下命令：

```
config localdns show
```

1. 輸出示例（替換了裝置名稱）：

```
device# config localdns show
No internal DNS servers configured.
Conditional forwarders present for Azure private domains.
```

將內部DNS伺服器條目新增到安全訪問VA

1. 要啟用Azure專用連結域的正確解析，請使用以下命令新增適當的內部DNS伺服器IP地址：

```
config localdns add <internal-DNS-server-IP>
```

1. 將<internal-DNS-server-IP>替換為可以解析Azure專用連結域的內部DNS伺服器的實際IP地址。

驗證Azure專用連結域的DNS解析

1. 更新DNS配置後，請驗證是否可以通過安全訪問VA解析Azure專用連結域。使用此命令確認DNS伺服器配置：

```
config localdns show
```

1. 輸出示例（替換裝置名稱）：

```
device# config localdns show
Internal DNS servers configured:
- x.x.x.x
Conditional forwarders present for Azure private domains.
```

1. 未找到CLI命令，該命令顯示從config localdns show（沒有DNS伺服器）到已確認解析的工作狀態的更改。

驗證與Azure專用連結資源的連線

在DNS正確解析後，測試從Secure Access VA後面的Azure工作負載到目標Azure專用連結終結點的連線，以確保正確的訪問。

原因

問題的根本原因是思科安全接入VA內沒有內部DNS伺服器配置。VA配置有Azure私有域條件轉發器，但缺少對Azure私有連結域進行正確DNS解析所需的內部DNS伺服器。新增內部DNS伺服器條目解決了問題。

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）。