安全訪問AWS Direct Connect整合中路由字首限制導致BGP會話抖動

目錄

問題

BGP會話在Cisco Secure Access和AWS Direct Connect之間的站點到站點通道上遇到抖動。之所以會出現這種不穩定性，是因為從Secure Access通告的路由字首數量超過了AWS Direct Connect的限制，從而阻止了穩定的路由交換，並影響了Secure Access與AWS之間建立一致連線的能力。

環境

- 思科安全存取(CSA)
- 採用BGP路由的AWS Direct Connect
- Secure Access和AWS之間的站點到站點隧道配置
- AWS Direct Connect BGP字首限製為100個路由

解析

解決方法涉及多種方法來解決BGP字首限制約束。

網路資料包分析顯示BGP NOTIFICATION消息，指示已達到最大字首數：

```
Border Gateway Protocol - NOTIFICATION Message
    Length: 28
    Type: NOTIFICATION Message (3)
    Major error Code: Cease (6)
```

```
Minor error Code (Cease): Maximum Number of Prefixes Reached (1)
```

即時解決方法

選項 1:AWS端路由過濾

評估AWS端選項，以忽略或過濾來自Secure Access的傳入路由字首，使其保持在AWS Direct Connect規定的100字首限制範圍內。

選項 2:AWS Transit Gateway實施

考慮遷移到AWS Transit Gateway作為替代連線模式。此方法可以提供更靈活的路由選項，並有助於規避直接連線字首限制。

長期解決方案

功能請求實施

已提交功能請求(CSE-I-4783)，以允許安全訪問上的路由過濾或總結功能。此增強功能將實現：

- 路由總結可減少通告字首的數量
- 路由過濾，控制向AWS Direct Connect通告哪些字首
- 從安全訪問端更好地控制BGP通告

實施步驟

1:檢視AWS Direct Connect限制。請參考AWS Direct Connect限制文檔以瞭解具體的限制條件。

2:評估當前路由通告。分析當前從Secure Access通告的路由數量，以確定有多少路由超過100字首的AWS限制。

3:實施即時因應措施。根據網路架構要求和業務需求，在AWS端過濾或Transit Gateway實施之間選擇。

4:監視功能請求進度。與適用的思科客戶團隊合作，審查推薦的路由過濾/總結功能請求的可行性和影響。

原因

根本原因是AWS Direct Connect中的基本限制，此限制將BGP路由通告限製為最多100個字首。Cisco Secure Access正在通告100多個路由字首，從而導致AWS Direct Connect傳送BGP NOTIFICATION消息，其中顯示錯誤代碼「Maximum Number of Prefixes Reached」，然後中斷BGP會話。這會建立一個會話建立和拆除的循環，導致觀察到的BGP會話擺動行為。

相關內容

- AWS Direct Connect Limits文檔
- 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）。