

解決安全電子郵件網關AWS雲遷移LDAP連線超時

目錄

問題

將Cisco Secure Email Gateway(SEG)環境遷移到Amazon Web Services(AWS)雲託管的SEG平台後，管理員會遇到持續的登入和效能問題。

症狀包括：

- 在GUI和CLI介面中訪問SEG時出現嚴重延遲
- 輸入使用者名稱和密碼後，身份驗證所需的時間過長
- 主儀表板/頁面的載入非常緩慢
- 整體平台響應速度極慢
- 在LDAP身份驗證訪問期間問題最明顯

資料包捕獲分析顯示，網關負載平衡器(GWLB)在大約350秒的空閒時間後關閉了到LDAP伺服器的SEG TCP會話，導致身份驗證延遲和超時。

環境

- Cisco Secure Email Gateway(SEG)遷移到AWS雲託管平台
- AsyncOS版本：16.0.4-016
- 使用Active Directory配置的LDAP身份驗證
- 網路路徑中的AWS網關負載均衡器(GWLB)
- Cisco Secure Email和Web Manager也受到相同問題的影響

- 為埠3269上的LDAP連線啟用SSL/TLS加密

解析

使用以下步驟調整LDAP連線生存期設定，以防止AWS Gateway Load Balancer導致的空閒會話超時：

1.連線到SEG CLI並訪問LDAP配置：

```
device# ldapconfig
```

2.找到LDAP伺服器配置檔案，並修改「每次連線到伺服器時的最大壽命（秒）」設定。將此值更改為300秒，以確保連線在網關負載平衡器的350秒空閒超時閾值之前刷新。

原始配置：

```
Max lifetime per connection: 1800
```

已更新配置：

```
Max lifetime per connection: 300
```

3.提交配置更改並允許系統應用新設定。

4.使用相同的300秒配置將相同的LDAP連線生命週期更改應用到Cisco Secure Email and Web Manager。

5.測試GUI和CLI登入功能。實施更改後，登入時間應減少到大約5秒，並且身份驗證延遲不應再發生。

6.監控環境以發現問題反複出現，並在問題持續時收集資料包捕獲。

原因

資料包捕獲分析顯示，AWS網關負載均衡器(GWLB)在大約350秒後終止空閒TCP會話。SEG的預設LDAP連線生存時間為1800秒，超過了GWLB的空閒超時閾值350秒。當LDAP連線閒置超過350秒時，GWLB將中斷TCP會話，導致使用者嘗試登入時的身份驗證延遲和超時。通過將LDAP連線生存時間縮短到300秒，SEG會在GWLB超時發生之前主動刷新連線，並防止身份驗證延遲。

相關內容

- [思科安全電子郵件雲網關AsyncOS 16.5使用手冊 — GD \(常規部署 \)](#)
- [Cisco Secure Email and Web Manager - GD\(General Deployment\)AsyncOS 16.5使用手冊](#)

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）。