

セキュアなEメールゲートウェイのAWSクラウド移行LDAP接続のタイムアウトの解決

内容

問題

Cisco Secure Email Gateway(SEG)環境をアマゾンウェブサービス(AWS)のクラウドホスト型SEGプラットフォームに移行した後、管理者はログインとパフォーマンスの問題が繰り返し発生します。

含まれる症状：

- GUIインターフェイスとCLIインターフェイスの両方でSEGにアクセスする際に著しい遅延が発生する
- ユーザ名とパスワードの入力後、認証に余分な時間がかかる
- メインダッシュボード/ページのロードが非常に遅い
- プラットフォーム全体の応答性が非常に遅かった
- この問題は、LDAP認証アクセス中に最も顕著でした

パケットキャプチャ分析により、LDAPサーバへのSEG TCPセッションがゲートウェイロードバランサ(GWLB)によって約350秒のアイドル時間後に閉じられ、認証の遅延とタイムアウトが発生することが明らかになりました。

環境

- Cisco Secure Email Gateway(SEG)をAWSクラウドホスト型プラットフォームに移行
- AsyncOS/バージョン：16.0.4-016
- Active Directoryで設定されたLDAP認証

- ネットワークパス内のAWS Gateway Load Balancer (GWLB)
- Cisco Secure Email and Web Managerも同じ問題の影響を受けます
- ポート3269でLDAP接続に対してSSL/TLS暗号化が有効

解決方法

LDAP接続のライフタイム設定を調整して、AWS Gateway Load Balancerが原因で発生するアイドルセッションタイムアウトを防ぐには、次の手順を実行します。

1. SEG CLIに接続し、LDAP設定にアクセスします。

```
device# ldapconfig
```

2. LDAPサーバープロファイルを見つけ、[サーバーへの接続ごとの最長有効期間 (秒)]の設定を変更します。この値を300秒に変更すると、ゲートウェイロードバランサの350秒のアイドルタイムアウトのしきい値の前に、接続が確実に更新されます。

元の設定：

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

更新された設定：

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

3. 構成の変更を確定し、システムが新しい設定を適用できるようにします。

4. 同じ300秒設定を使用して、同じLDAP接続ライフタイム変更をCisco Secure Email and Web Managerに適用します。

5. GUIおよびCLIログイン機能をテストします。変更を実装したら、ログイン時間を約5秒に短縮し、認証の遅延が発生しないようにする必要があります。

6. 環境を監視して問題が再発していないか確認し、問題が解決しない場合はパケットキャプチャを収集します。

原因

パケットキャプチャ分析では、AWS Gateway Load Balancer (GWLB)が約350秒後にアイドル状態のTCPセッションを終了していることが示されました。SEGのデフォルトのLDAP接続ライフタイムは1800秒で、これはGWLBのアイドルタイムアウトのしきい値である350秒を超えています。LDAP接続が350秒を超えてアイドル状態のままになると、GWLBによってTCPセッションが切断され、ユーザがログインを試みた際に認証の遅延とタイムアウトが発生します。LDAP接続のライフタイムを300秒に短縮することで、SEGはGWLBタイムアウトが発生する前に予防的に接続を更新し、認証の遅延を防止します。

関連コンテンツ

- [AsyncOS 16.5 for Cisco Secure Email Cloud Gatewayユーザガイド – GD \(一般導入\)](#)
- [AsyncOS 16.5 for Cisco Secure Email and Web Managerユーザガイド – GD \(一般導入\)](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。