ログインブロックのクワイエットモードが原因で発生する、IOS XEデバイスでの断続的なSSHアクセス障害の解決

内容

問題

IOS XEソフトウェアを実行しているデバイスで、SSHアクセスの障害が断続的に発生します。SSH接続が受け入れられたり、一貫したパターンなしで拒否されたりする場合があります。デバイスへのコンソールアクセスは影響を受けません。失敗したSSHセッションに対して、該当デバイス上でパケットキャプチャを実行し、SSHセッションがネゴシエートを開始する前に、デバイス自体がクライアントのTCP SYNを受信するとすぐにTCP RSTパケットを送信していることを確認します。コマンドdebug ip tcp transactions を有効にすると、TCP RSTの動作が次のデバッグ出力に示されます。

```
Aug 21 19:46:04.697: Reserved port 0 in Transport Port Agent for TCP IP type 0
Aug 21 19:46:04.697: TCP: sending RST, seq 0, ack 1013312911
Aug 21 19:46:04.697: TCP: sent RST to 10.x.x.x:43266 from 10.x.x.x:22
Aug 21 19:46:04.698: Released port 0 in Transport Port Agent for TCP IP type 0 delay 0
Aug 21 19:46:04.698: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
Aug 21 19:46:04.698: TCB destroyed
```

次の項目を確認して、問題の原因として除外します。

- show ip sshコマンドを使用して、デバイスでSSHが有効になっていることを確認します。
- show tcp briefコマンドを使用して、TCPポート22がIOSdプロセス内部でリスニングしていることを確認します。
- show ip trafficコマンドまたはdebug ip errorコマンドの出力に「no port」エラーはありません
- VTY回線は完全には消費されていません。show lineのコマンド出力には、すべての回線がビジーであると表示されません。
- VTY回線のaccess-class設定を削除しても、問題が解決しない。

デバイスのロギングバッファには、非常に大量の認証障害が繰り返し発生しており、quietモードがアクティブであることが示されています。

```
Aug 21 12:24:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: test_user] [Source: LOCAL] [localport: 
Aug 21 12:24:32: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 0 secs, [user: tes
```

障害発生時のshow login出力は、SSH障害時のquiet-modeでデバイスを示します。

環境

- プラットフォーム：Cisco Catalyst 9500シリーズスイッチ（コアスイッチおよびマネージドスイッチスタック）
- デバイスへのリモートアクセスに対してSSHが有効になっている
- デバイスでアクティブなログインブロック設定：login block-for 120 attempts 3 within 60

解決方法

この問題は、大量の認証の失敗によって永続的にトリガーされるログインブロッククワイエットモード機能によって発生します。この問題を解決するには、信頼できるSSH管理デバイスに対してquiet-mode access-class ACLを使用します。

Quiet-Mode Trusted IP Access-Class ACLによるログインブロックの設定

ログインブロック機能を設定し、Quiet-Modeアクセスクラス ACL（アクセスコントロールリスト）を実装する。 このACLにより、信頼できる管理ホストとサブネットは、他のすべてのソースに対してログインブロック保護がアクティブなままの間、クワイエットモードの適用をバイパスできます。

1. 信頼できる管理ホストとサブネットを許可する名前付き拡張ACLを定義します。次の例では、2つの特定のジャンプホストIPと1つの/22管理サブネットを許可しています。環境内の信頼できる管理ソースに合わせてエントリを調整します。

```
device# configure terminal
device(config)# ip access-list extended quietmode_trusted_ip
device(config-ext-nacl)# 10 permit ip host <trusted_host_1_ip> any
device(config-ext-nacl)# 20 permit ip host <trusted_host_2_ip> any
device(config-ext-nacl)# 30 permit ip <subnet_address> <wildcard_mask> any
device(config-ext-nacl)# exit
```

ACLエントリの作成：

- 特定の管理ホスト（ジャンプサーバなど）を許可するには、hostキーワードの後に単一のIPアドレスを使用します。
- サブネット全体を許可するには、ネットワークアドレスを指定し、その後に適切なワイルドカードマスクを指定します。

2. クワイエットモードのアクセスクラスにACLを適用し、ACLに一致する送信元が、クワイエットモードがアクティブであっても接続を許可されるようにします。

```
device(config)# login quiet-mode access-class quietmode_trusted_ip
device(config)# end
```

3. 削除された場合は、login block-for設定コマンドを再度有効にします。

```
device# configure terminal
device(config)# login block-for 120 attempts 3 within 60
device(config)# end
```

4. 設定を保存します。

```
device# write memory
```

5. システムログを監視して、quietモードが引き続きトリガーされているかどうか、および現在のログインモードを確認します。

```
device# show logging
device# show login
```

持続的な認証失敗の根本原因への対処

上記のACLベースの回避策は症状（SSHがQuietモードでブロックされている）に対処しますが、認証エラーが繰り返し発生するという根本的な原因には対処しません。これらの障害は、継続的にquietモードをトリガーします。この問題を完全に解決するには、頻繁に発生する認証の問題を調査して解決する必要があります。

原因

断続的なSSHアクセス障害は、大量の認証の失敗が繰り返し原因で、IOS-XEのログインブロック機能がクワイエットモードに入ることで発生します。設定例login block-for:

```
login block-for 120 attempts 3 within 60
```

この設定では、3回以上のログイン試行の失敗が60秒以内に検出された場合は常に、クワイエットモードに入り、120秒間すべての新規ログイン接続をブロックするようにIOS XEデバイスに指示します。大量の認証の失敗は、ログイン待機モードを常にトリガーします。クワイエットモードの適用はグローバルで、すべてのVTY回線とすべてのTCPポートに適用され、SSHが設定されます。クワイエットモードがアクティブの場合、デバイスは、クワイエットモードのアクセスクラスACLによって明示的に許可されていない発信元から新しいTCP SYNパケットを受信するとすぐにTCP RSTパケットを送信し、SSHセッションの確立を阻止します。

関連コンテンツ

- Cisco IOS XEセキュリティ設定ガイド：ログインの機能拡張（ログインブロック用およびクワイエットモードアクセスクラス）
- シスコのテクニカルサポートとダウンロード

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。