ASA/PIX： CLI を使用して、フェールオーバー ペアのソフトウェア イメージをアップグレードする方法

目次

概要

このドキュメントでは、CLI を使用して、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス フェールオーバー ペアのソフトウェア イメージをアップグレードする方法について説明します。

注: セキュリティ アプライアンス ソフトウェアを 7.0 から 7.2 に直接アップグレード（またはダウングレード）する場合、または ASDM ソフトウェアを 5.0 から 5.2 に直接アップグレード（またはダウングレード）する場合、Adaptive Security Device Manager（ASDM）は機能しません。段階的にアップグレード（またはダウングレード）する必要があります。

ASA の ASDM とソフトウェア イメージをアップグレードする方法については、「PIX/ASA： ASDM または CLI を使用したソフトウェア イメージのアップグレードの設定例」を参照してください。

注: マルチコンテキスト モードでは、**copy tftp flash** コマンドを使用してすべてのコンテキストで PIX/ASA イメージのアップグレードまたはダウングレードを行うことはできません。 これは System Exec モードのみでサポートされます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 7.0 以降が稼働する Cisco 適応型セキュリティ アプライアンス (ASA)
- Cisco ASDM バージョン 5.0 以降

注: ASA を ASDM で設定できるようにする方法については、「ASDM での HTTPS アクセスの許可」を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、Cisco PIX 500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.0 以降にも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行

フェールオーバー コンフィギュレーション内の 2 つの装置は、メジャー (最初の番号) およびマイナー (2 番目の番号) のソフトウェア バージョンが同じになるようにします。 ただし、アップグレード プロセス中に装置のバージョン パリティを維持する必要はありません。 それぞれの装置で動作するソフトウェアでバージョンが異なっていても、フェールオーバーはサポートされます。 互換性と安定性を長期にわたって確保するため、可能な限り早く両方の装置を同じバージョンにアップグレードすることを推奨します。

次の 3 種類のアップグレードが あります。

1. **メンテナンス リリース**—どのメンテナンス リリースからでも、マイナー リリース内のその他すべてのメンテナンス リリースにアップグレードできます。 たとえば、中間のメンテナンス リリースをあらかじめインストールしなくても、7.0(1) から 7.0(4) にアップグレードできます。
2. **マイナー リリース**—あるマイナー リリースから次のマイナー リリースにアップグレードできます。 マイナー リリースはスキップできません。 たとえば、7.0 から 7.1 にアップグレードできます。 ゼロ ダウンタイム アップグレードの場合、7.0 から 7.2 に直接アップグレードすることはサポートされません。 まず 7.1 にアップグレードする必要があります。

3. **メジャー リリース**—前のバージョンの最後のマイナー リリースから次のメジャー リリースにアップグレードできます。 たとえば、7.9 が 7.x リリースの最後のマイナー バージョンであれば、7.9 から 8.0 にアップグレードできます。

アクティブ/スタンバイ フェールオーバー コンフィギュレーションのアップグレード

アクティブ/スタンバイ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

1. 両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを boot system コマンドで指定します。詳細については、「CLI を使用したソフトウェア イメージと ASDM イメージのアップグレード」を参照してください。
2. 次のように、アクティブ装置で failover reload-standby コマンドを入力し、スタンバイ装置をリロードして新しいイメージをブートします。`active#failover reload-standby`
3. スタンバイ装置がリロードを終了して Standby Ready 状態になったら、アクティブ装置で no failover active コマンドを入力して、アクティブ装置をスタンバイ装置に強制的にフェールオーバーします。`active#no failover active` **注:** show failover コマンドを使用して、スタンバイ装置が Standby Ready 状態かどうかを検証します。
4. reload コマンドを入力して、前のアクティブ装置（現在の新規スタンバイ装置）をリロードします。`newstandby#reload`
5. 新しいスタンバイ装置がリロードを終了して Standby Ready 状態になったら、failover active コマンドを入力して、元のアクティブ装置をアクティブ ステータスに戻します。`newstandby#failover active`

これで、アクティブ/スタンバイ フェールオーバー ペアをアップグレードするプロセスは終わりです。

アクティブ/アクティブ フェールオーバー コンフィギュレーションのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

1. 両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを boot system コマンドで指定します。詳細については、「CLI を使用したソフトウェア イメージと ASDM イメージのアップグレード」を参照してください。
2. プライマリ装置のシステム実行スペースで failover active コマンドを入力して、プライマリ装置の両方のフェールオーバー グループをアクティブにします。`primary#failover active`
3. プライマリ装置のシステム実行スペースで failover reload-standby コマンドを入力して、セカンダリ装置をリロードして新規イメージをブートします。`primary#failover reload-standby`
4. セカンダリ装置がリロードを終了し、その装置で両方のフェールオーバー グループが Standby Ready 状態になったら、プライマリ装置のシステム実行スペースで no failover active コマンドを使用して、セカンダリ装置の両方のフィールオーバー グループをアクティブにします。`primary#no failover active` **注:** show failover コマンドを使用して、セカンダリ装置の両方のフェールオーバー グループが Standby Ready 状態かどうかを検証します。
5. プライマリ装置の両方のフェールオーバー グループが Standby Ready 状態になっていることを確認してから、reload コマンドを使用してプライマリ装置をリロードします。`primary#reload`

6. フェールオーバー グループは、preempt コマンドを使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。 フェールオーバー グループが preempt コマンドによって設定されていない場合は、failover active group コマンドを使用して、指定された装置でそれらのステータスをアクティブに戻すことができます。

トラブルシューティング

%%ASA-5-720012: ((VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit (または) %ASA-6-720012: ((VPN-unit) Failed to update IPsec failover runtime data on the standby unit

問題

Cisco 適応型セキュリティ アプライアンス (ASA) をアップグレードしようとすると、次のいずれかのエラー メッセージが表示されます。

```
%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit.

%%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
```

解決策

このエラー メッセージは情報伝達のためのエラーです。 このメッセージは、ASA または VPN の機能に影響しません。

このメッセージは、対応する IPSec トンネルがスタンバイ装置で削除されているため、VPN フェールオーバー サブシステムが IPSec 関連のランタイム データをアップデートできないときに表示されます。 これを解決するには、アクティブ装置で **wr standby** コマンドを実行します。

この動作に対処するため、2 つのバグが提起されています。 これらのバグが修正されたソフトウェア バージョンの ASA にアップグレードできます。 詳細は、Cisco Bug ID CSCtj58420 (登録ユーザ専用) および CSCtn56517 (登録ユーザ専用) を参照してください。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Adaptive Security Device Manager
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems