FWSM フェールオーバー トラブルシューティング

内容

概要

このドキュメントでは、Firewall Service Module（FWSM; ファイアウォール サービス モジュール）のフェールオーバー設定の問題の解決に使用できる手順について説明しています。

また、このドキュメントでは、フェールオーバー接続のトラブルシューティングを開始する前に試す一般的な手順のチェックリストも提供しています。

前提条件

要件

このドキュメントに特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、FWSM 2.3 以降に基づくものです。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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。

背景説明

フェールオーバー機能を利用して、障害が発生した FWSM の機能をスタンバイ FWSM で引き継ぐことができます。使用する 2 つの FWSM では、メジャー ソフトウェア バージョン（最初の番号）、マイナー ソフトウェア バージョン（2 番目の番号）、ライセンス、および動作モード（ルーテッドまたは透過、シングルまたはマルチ コンテキスト）が同じである必要があります。 アクティブ ユニットが故障すると、そのユニットはスタンバイ状態に変わり、スタンバイ ユニットがアクティブ状態に変わります。フェールオーバーが発生した後は、同じ接続情報を新しいアクティブ ユニットで使用できます。

その他の情報については、『フェールオーバーの使用方法』の「フェールオーバーの設定」セクションを参照してください。

フェールオーバー チェックリスト

このチェックリストを使用すると、FWSM のフェールオーバーを適切に設定できます。

- インターフェイスの確認
- ライセンス
- コンテキスト モード
- ソフトウェア要件
- ステートフル フェールオーバーのための最小限の FWSM 設定
- 最小限のスイッチ設定

インターフェイスの確認

FWSM のすべてのインターフェイスにスタンバイ IP アドレスが設定されていることを確認してください。まだ設定していない場合は、各インターフェイス（ルーテッド モード）または管理アドレス（透過モード）に、アクティブとスタンバイの IP アドレスを設定します。 スタンバイ IP アドレスは、現在スタンバイ ユニットになっている FWSM で使用されます。これはアクティブ IP アドレスと同じサブネットにある必要があります。

次に設定例を示します。

```
ip address <active-ip> <netmask> standby <standby-ip>
```

注：フェールオーバーリンクまたはステートフルフェールオーバーを使用する場合は、ステートフルリンクのIPアドレスを設定しないでください。

注：スタンバイアドレスのサブネットマスクを特定する必要はありません。フェールオーバー リンクの IP アドレスと MAC アドレスはフェールオーバー時には変化しません。フェールオーバー リンクのアクティブ IP アドレスは常にプライマリ ユニットに存在し、スタンバイ IP アドレスはセカンダリ ユニットに存在します。

ライセンス

アクティブ ユニットとスタンバイ ユニットの両方で同じライセンスを使用する必要があります。

コンテキスト モード

プライマリ ユニットがシングル コンテキスト モードで動作している場合、セカンダリ ユニットもまたシングル コンテキスト モード、およびプライマリ ユニットと同じファイアウォール モードで動作している必要があります。

プライマリ ユニットがマルチ コンテキスト モードで動作している場合、セカンダリ ユニットもマルチ コンテキスト モードで動作している必要があります。フェールオーバー リンクおよびステート リンクはシステム コンテキストに含まれるため、セカンダリ ユニットのセキュリティ コンテキストのファイアウォール モードを設定する必要はありません。セカンダリ ユニットは、プライマリ ユニットからセキュリティ コンテキスト設定を取得します。

注：modeコマンドはセカンダリユニットには複製されません。

注：マルチキャストは、セキュリティアプライアンスのマルチコンテキストモードではサポートされません。詳細は、「サポートされていない機能」セクションを参照してください。

ソフトウェア要件

フェールオーバー構成の 2 つのユニットは、メジャー ソフトウェア バージョン (最初の番号) とマイナー ソフトウェア バージョン (2 番目の番号) が同じである必要があります。ただし、アップグレード プロセスでは、バージョンの異なるソフトウェアを使用できます。たとえば、1 つのユニットをバージョン 3.1(1) からバージョン 3.1(2) にアップグレードしても、フェールオーバーをアクティブに保つことができます。ただし、長期的な互換性を保つために、両方のユニット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。

ステートフル フェールオーバーのための最小限の FWSM 設定

プライマリ FWSM

```
failover lan unit primary
failover lan interface if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr failover link if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr
```

セカンダリ FWSM

```
failover lan unit secondary
failover lan interface if_name vlan vlan failover interface ip if_name ip_addr mask standby
```

ip_addr failover link *if_name* vlan *vlan* failover interface ip *if_name ip_addr mask* standby *ip_addr*

アクティブ/スタンバイ フェールオーバーの設定方法の詳細は、「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。

最小限のスイッチ設定

- プライマリ FWSM を持つ Catalyst によってこのプライマリに送信される VLAN は、セカンダリ FWSM を持つ Catalyst によってそのセカンダリに送信される VLAN と一致している必要があります。（**show run | i firewallコマンド**は同じでなければなりません。)**プライマリ シャーシ**

```
cat6k-7(config)#do sh run | i fire
firewall multiple-vlan-interfaces
firewall module 9 vlan-group 1
firewall vlan-group 1  3,4,100-106
```

セカンダリ シャーシ

```
cat6k-7(config)#do sh run | i fire
firewall multiple-vlan-interfaces
firewall module 9 vlan-group 1
firewall vlan-group 1  3,4,100-106
```

- 送信される VLAN はすべて VLAN データベースに存在し、アクティブである必要があります。このようにするには、コンフィギュレーション モードでスイッチに対して次のコマンドを発行します。

```
vlan 10
no shut
```

VLAN がデータベースに存在し、アクティブであるかどうかを確認するには、両方のシャーシに対する **show vlan コマンドの出力に、FWSM に送信される VLAN が含まれ、かつアクティブとして表示されている必要があります。**次に、出力例を示します。**プライマリ シャーシ**

```
cat6k-7(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----
1    default                               active
3    VLAN0003                         active    Fa4/47
4    VLAN0004                         active    Fa4/48
```

セカンダリ シャーシ

```
cat6k-7(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----
1    default                               active
3    VLAN0003                         active    Fa4/47
4    VLAN0004                         active    Fa4/48
```

- 2 つの FWSM が各 VLAN 上でレイヤ 2 の接続性があることを確認してください（VLAN は同じサブネットにある必要があります）。**透過型ファイアウォール要件**：透過モードでフェールオーバーを使用している場合にループを回避するには、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）フォワーディングをサポートしているスイッチ ソフトウェアを使用する必要があります。また、FWSM で BPDU を使用できるように設定する必要もあります。FWSM を使用して BPDU を許可するには、EtherType?ACL を設定し、これを両方のインターフェイスに適用します。**注**：PIXおよびASAプラットフォームとは異なり、2つのFWSMブレードのハードウェアは常に同じです。異なるモデルやメモリ構成はありません。

トラブルシューティング

FWSM がリロードされると、このセクションで説明しているシナリオに該当する場合、フェールオーバーは無効化されます。

FWSM は、クラッシュ、シャーシからのリセット、FWSM CLI によって発行されたリロードなどが原因でリロードされることがあります。また、単に新しいモジュールが別のスロットに挿入または取り付け直されたり、シャーシから電源が再投入されたりしたことが原因になることもあります。

バージョンのミスマッチ

フェールオーバー構成の 2 つのユニットは、メジャー ソフトウェア バージョン (最初の番号) とマイナー ソフトウェア バージョン (2 番目の番号) が同じである必要があります。

関連 syslog メッセージ：105040

互換性のないライセンス

ライセンスに互換性がないために、次の syslog を受け取る場合があります。

```
FWSM-1-105045: (Primary) Mate license (number contexts) is not compatible
with my license (number contexts).
FWSM-1-105001: (Primary) Disabling failover.
```

関連 syslog メッセージ：105045 および 105001

異なるモード (シングル モードとマルチ コンテキスト モード)

プライマリ FWSM とセカンダリ FWSM は、両方とも同じモード (シングルまたはマルチ) で動作している必要があります。 たとえば、プライマリがシングル モード、セカンダリがマルチ モードに設定されている場合にセカンダリでリロードが発生すると、両方のモジュールのフェールオーバーが無効になります。

シングル モードのプライマリでは、次のメッセージが出力されます。

```
%FWSM-1-103001: (Primary) No response from other firewall (reason code = 1).
%FWSM-1-105044: (Primary) Mate operational mode (Multi) is not compatible
with my mode (Single).
%FWSM-1-105001: (Primary) Disabling failover.
```

マルチ モードのセカンダリ (このブレードでリロードが発生しています) では、次のメッセージが出力されます。

```
%FWSM-5-111008: User 'Config' executed the 'no snmp-server location' command.
%FWSM-5-111008: User 'Config' executed the 'inspect tftp' command.
%FWSM-5-111008: User 'Config' executed the 'service-policy global_policy global'
command.
%FWSM-5-111008: User 'Config' executed the 'config-url disk:/admin.cfg' command.
%FWSM-5-111008: User 'Config' executed the 'prompt hostname context' command.
%FWSM-4-411001: Line protocol on Interface LAN, changed state to up
%FWSM-4-411001: Line protocol on Interface LAN, changed state to up
```

```
%FWSM-1-105044: (Secondary) Mate operational mode (Single) is not compatible
with my mode (Multi).
%FWSM-1-105001: (Secondary) Disabling failover.
%FWSM-6-199002: Startup completed.  Beginning operation.
%FWSM-6-605005: Login permitted from 127.0.0.51/15518 to eobc:127.0.0.91/telnet
for user ""
%FWSM-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
%FWSM-5-111008: User 'enable_15' executed the 'changeto context admin' command.
```

マルチ モードのプライマリでは、次のメッセージが出力されます。

```
%FWSM-1-105044: (Primary) Mate operational mode (Single) is not compatible
with my mode (Multi).
%FWSM-1-105001: (Primary) Disabling failover.
```

関連 syslog メッセージ：105044、103001、105001

2 つの FWSM がアクティブになる

ログに次のエラー メッセージが表示されます。

```
fw_create_pc_sw: fw_create_portchannel failed
```

このエラーの原因は、スイッチの推奨されるポート チャネル数が最大値を超えたためです（Cat6000/6500 の Cisco IOS ソフトウェア リリース 12.2(33)SXH4 の最大値は 128）。 したがって、インターフェイス記述子ブロック（IDB）の制限いっぱいまで使用されます。

このため、次の 2 つの問題が発生する可能性があります。

- それぞれ、アクティブおよびスタンバイとして機能する FWSM モジュールを備えた 2 台のスイッチがある場合に、2 つの FWSM モジュールが同時にアクティブになります。
- すると、追加のポート チャネルを作成できません。

この問題を解決する手順の一部として、不要なポートチャネルを削除し、FWSM をリロードします。

VLAN のミスマッチ

問題

FWSM で次のエラー メッセージを受け取る。「**Detected an Active Mate**」、「**Vlan configuration mismatch**」、「**failover will be disabled**」

または

ファイアウォール サービス モジュールの設定および対応するスイッチの設定が完了したように見える。しかし、FWSM 同士は相互に同期できない。セカンダリ ホストでは、次のエラー メッセージを受け取る。

```
State check detected an Active mate

        Unable to verify vlan configuration with mate.
        Check that mate's failover is enabled

        No Response from Mate
```

または

show failover コマンドの出力で、セカンダリ モジュールのフェールオーバー ステータスが OFF、FWSM フェールオーバー状態が `Failover Off (pseudo-Standby)` と表示される。

```
FWSM-secondary(config)#show failover
Failover Off (pseudo-Standby)
```

解決方法

この問題は、ファイアウォール (FWSM およびスーパーバイザ) にまたがる VLAN の割り当てのミスマッチが原因である可能性があります。 たとえば、firewall vlan-group 1 の設定で、各スイッチにてファイアウォールに割り当てられている同じ数であるべき VLAN の数が異なっている可能性があります。これが問題の原因である可能性があります。ファイアウォールに同じ数の VLAN を割り当てると、フェールオーバーは動作します。

VLAN 設定の不整合エラーが発生するのを防ぐには、**show vlan コマンドの出力が両方の FWSM で同じである必要があります。**このエラー メッセージは、FWSM でフェールオーバーの設定を変更または ロードした場合にのみ生成されます。たとえば、FWSM はブート時にフラッシュ メモリから起動設定を ロードし、フェールオーバーの初期化を試みます。現時点では、これにより、両方のモジュールが正しい VLAN を受信していることを確認できます。VLAN が一致しない場合はエラー メッセージが表示され、フェールオーバーは無効のままです。

注：フェールオーバーが機能するためには、FWSMで同じ設定とポート割り当てが必要です。シャーシ間のフェールオーバーを実行することは可能ですが、ファイアウォールに割り当てられている各 VLAN が、これらの 2 つのシャーシ間のトランクに存在する必要があります。

FWSM には、外部物理インターフェイスは搭載されていません。代わりに、VLAN インターフェイスが使用されます。FWSM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当てと同様に設定します。FWSM には、スイッチ ファブリック モジュール (存在する場合) または共有バスへの内部インターフェイスが組み込まれています。詳細は、「ファイアウォール サービス モジュールへの VLAN の割り当て」を参照してください。

FWSM の設定中に VLAN マッピングが変更され、次の起動時に失敗する場合があることに注意してください。

フェールオーバーが無効

no failover コマンドを使用してフェイルオーバーを無効にすると、装置がリロードされるまで、装置の現在の状態 (アクティブまたはスタンバイ) が維持されます。これはフェールオーバーを無効にするためにのみ使用されます。装置の状態をアクティブからスタンバイに変更する、またスタンバイからアクティブに変更するには、[no] failover active コマンドを使用する必要があります。

関連情報

- FWSM：フェールオーバーの設定
- FWSM：システム ログ メッセージ
- テクニカル サポートとドキュメント – Cisco Systems

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。