ハイ アベイラビリティ（フェールオーバー）

ここでは、アクティブ/スタンバイ フェールオーバーを設定および管理して、Firepower Threat Defense システムのハイ アベイラビリティを実現する方法について説明します。

ハイ アベイラビリティ（フェールオーバー）について

ハイ アベイラビリティまたはフェールオーバー セットアップは、プライマリ デバイスの障害時にセカンダリ デバイスで引き継ぐことができるように、2 つのデバイスを結合します。これにより、デバイスの障害時にネットワーク運用を維持できます。

ハイ アベイラビリティを設定するには、同じ Firepower Threat Defense デバイスが 2 台、専用のフェールオーバー リンク（オプションで、ステート リンク）で相互に接続されている必要があります。2 台の装置はフェールオーバー リンクを介して常に通信し、各装置の動作状態を判断して、展開された設定の変更を同期します。システムでは、フェールオーバーが発生したときにユーザ接続が維持されるように、ステート リンクを使用して接続状態の情報をスタンバイ デバイスに渡します。

この装置はアクティブ/スタンバイ ペアを形成します。1 台の装置がアクティブ装置となり、トラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニタされま

す。これらの条件が満たされると、アクティブ装置がスタンバイ装置にフェールオーバーし、スタンバイ装置がアクティブになります。

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firepower Threat Defense デバイス に引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリ ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニットが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ ユニットが常にアクティブ ユニットになります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ ユニットの MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ ユニットが行うアクション、スタンバイ ユニットが行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *1:* フェールオーバー イベント

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記（**Notes**）
アクティブユニットが故障（電源またはハードウェア）	フェールオーバー	適用対象外	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであったユニットの復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。
スタンバイ ユニットが故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	適用対象外	スタンバイ ユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー リンクに故障とマークする	フェールオーバー リンクに故障とマークする	フェールオーバー リンクがダウンしている間、ユニットはスタンバイ ユニットにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー リンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方のユニットがアクティブになります。
ステート リンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記（Notes）
アクティブユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクは 2 つの装置の間の専用接続です。ステートフル フェールオーバー リンクも専用接続ですが、1 つのフェールオーバー リンクをフェールオーバー リンクとステート リンクが組み合わされたものとして使用することも、個別の専用ステート リンクを作成することもできます。フェールオーバー リンクだけを使用する場合は、ステートフルな情報もそのリンクを経由し、ステートフル フェールオーバー機能は失われません。

デフォルトでは、フェールオーバー リンクおよびステートフル フェールオーバー リンク上の通信はプレーン テキスト（暗号化されない）です。IPsec 暗号キーを設定することにより、通信を暗号化してセキュリティを強化できます。

ここでは、これらのインターフェイスについて詳しく説明するとともに、最良の結果を得るためのデバイスの配線方法に関する推奨事項を示します。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認し、設定の変更を同期します。

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- Hello メッセージ（キープアライブ）
- ネットワーク リンク ステータス
- MAC アドレス交換
- 設定の複製と同期化

- システム データベースの更新。これには、VDB やルールは含まれますが、地理位置情報データベースやセキュリティ インテリジェンス データベースは含まれません。各システムは、地理位置情報の更新やセキュリティインテリジェンスの更新を個別にダウンロードします。更新スケジュールを作成する場合は、これらの同期が維持されます。ただし、アクティブ デバイスで地理位置情報やセキュリティ インテリジェンスを手動更新する場合は、スタンバイ デバイスでも更新する必要があります。

（注） イベント、レポート、および監査ログデータは同期されません。イベント ビューアとダッシュボードには、特定の装置に関連するデータのみが表示されます。また、展開履歴、タスク履歴、およびその他の監査ログ イベントも同期されません。

ステートフル フェールオーバー リンク

システムは、ステート リンクを使用して接続状態の情報をスタンバイ デバイスに渡します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。

フェールオーバー リンクとステートフル フェールオーバー リンクの両方に単一のリンクを使用することは、インターフェイスを節約する最善の方法です。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステート リンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

ステートフル フェールオーバー リンクの帯域幅は、デバイス上のデータ インターフェイスの最大帯域幅と一致させることをお勧めします。

フェールオーバー リンクとステート リンクのインターフェイス

使用されていないが有効になっているデータインターフェイス（物理）は、いずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバーリンクインターフェイスは、通常のネットワークインターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。管理インターフェイスまたはサブインターフェイスをフェールオーバーに使用することはできません。

FTD は、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。

フェールオーバーおよびステートフル フェールオーバー インターフェイスの接続

未使用のデータ物理インターフェイスは、フェールオーバー リンクやオプションの専用ステートリンクとして使用できます。ただし、現在名前が設定されているインターフェイスやサブインターフェイスを持つインターフェイスは選択できません。フェールオーバーおよびステートフル フェールオーバー リンク インターフェイスは、通常のネットワーキング インターフェイ

スとして設定されません。フェールオーバー通信用にのみ存在し、通過トラフィックや管理アクセスに使用することはできません。

設定がデバイス間で同期されるため、リンクの両端に同じポート番号を選択する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで GigabitEthernet 1/3 を使用します。

次のいずれかの方法で、フェールオーバー リンクおよび専用ステート リンク（使用する場合）を接続します。

- Firepower Threat Defense デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。専用ステート リンクの要件は同じですが、フェールオーバー リンクとは異なるネットワーク セグメントに存在する必要があります。

（注） スイッチを使用する利点は、装置のいずれかのインターフェイスがダウンした場合、障害が発生したインターフェイスのトラブルシューティングが容易であることです。直接ケーブル接続を使用する場合、1 つのインターフェイスに障害が発生すると、リンクが両方のピアでダウンし、どのデバイスで障害が発生しているのかを判別することが困難になります。

- イーサネット ケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。Firepower Threat Defense デバイスは銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているので、クロス ケーブルまたはストレート ケーブルのどちらでも使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバー リンクとデータ リンクの中断の回避

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、Firepower Threat Defense デバイスはデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクの正常性が復元されるまで停止されます。

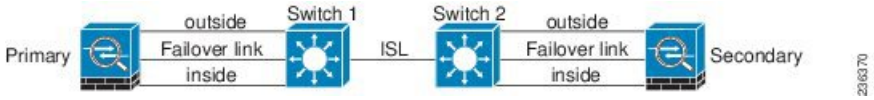
耐障害性フェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

2 つの Firepower Threat Defense デバイス間のフェールオーバーとデータ インターフェイスの両方を接続するために 1 つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の Firepower Threat Defense デバイスがアクティブになります。したがって、次の図で示されている 2 つの接続方式は推奨**しません**。

図 *1:* 単一のスイッチを使用した接続：非推奨

図 *2:* 2 つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *3:* 異なるスイッチを使用した接続

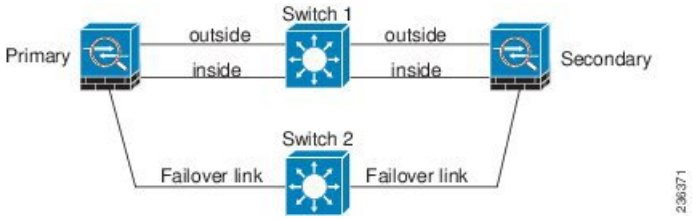
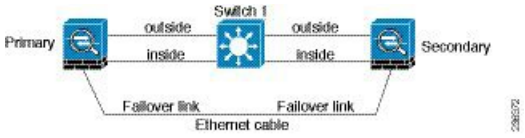


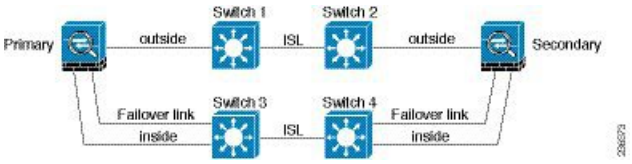
図 *4:* ケーブルを使用した接続



シナリオ 3：推奨

Firepower Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *5:* セキュア スイッチを使用した接続



ステートフル フェールオーバーがユーザ接続に与える影響

アクティブ装置は、接続状態情報をスタンバイ装置と共有します。これは、スタンバイ装置がユーザに影響を与えずに特定のタイプの接続を維持できることを意味します。

ただし、ステートフルフェールオーバーをサポートしないタイプの接続もあります。これらの接続については、フェールオーバーが発生した場合、ユーザが接続を再確立する必要があります。多くの場合、これは、接続で使用されているプロトコルの動作に基づいて自動的に実行されます。

ここでは、ステートフルフェールオーバーに関してサポートされる機能またはサポートされない機能について説明します。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ Firepower Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および HTTP 接続状態を含む状態。他のタイプの IP プロトコルおよびICMPは、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- 厳密な TCP 強制を含む、Snort の接続状態、インスペクション結果、およびピンホール情報。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションとピンホール。
- スタティックおよびダイナミック ルーティングテーブル：ステートフルフェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリ ユニットには最初にプライマリ ユニットをミラーリングするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。

フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIBテーブルのエポック番号が増加します。再コンバージェンス中に、OSPFおよびEIGRPルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIBには新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。

（注） ルートは、アクティブ装置上のリンクアップまたはリンクダウンイベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCPサーバ：DHCPアドレス リースは複製されません。ただし、インターフェイスで設定されたDHCPサーバは、DHCPクライアントにアドレスを付与する前にアドレスが使用されていないことを確認するためにpingを送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたはDDNSとは関連性がありません。
- アクセス コントロール ポリシーの判断：フェールオーバー時には、トラフィックの照合（URL、URL カテゴリ、地理位置情報など）、侵入検知、マルウェア、ファイル タイプに関する判断が保持されます。ただし、フェールオーバーの時点で評価される接続には、次のような注意事項があります。
  - AVC：App-ID判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に、App-ID 判定が完了および同期されていれば、正常に同期は行われます。
  - 侵入検知状態：フェールオーバーの際、フロー中にピックアップが発生すると、新しいインスペクションは完了しますが、古い状態は失われます。
  - ファイル マルウェア ブロッキング：ファイルの処分は、フェールオーバー前にできるようになる必要があります。
  - ファイル タイプ検出とブロッキング：ファイル タイプは、フェールオーバー前に特定される必要があります。元のアクティブ デバイスでファイルを特定している間にフェールオーバーが発生すると、ファイル タイプの同期は失われます。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。
- アイデンティティ ポリシーからのパッシブなユーザ識別の判断（キャプティブ ポータルを介したアクティブ認証を通じて収集されたもの以外）。
- セキュリティ インテリジェンス判断。
- RA VPN：リモート アクセスVPNエンドユーザは、フェールオーバー後にVPNセッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリ

ケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ Firepower Threat Defense デバイスに渡されません。

- GREやIP-in-IPなどのプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されず、新しいアクティブ ノードは、既存のインスペクションの判定を再利用して、正しいポリシー ルールを照合することができません。
- SSL復号ポリシーにより復号された接続：復号状態は同期されず、現在の復号された接続はリセットされ、ブロックされます。新しい接続が適切に機能します。（復号しないルールと一致する）復号されない接続は影響を受けず、他の TCP 接続と同様に正しく複製されます。
- マルチキャスト ルーティング。

スタンバイ装置で許可される設定の変更とアクション

ハイ アベイラビリティ モードで運用している場合は、アクティブ装置にのみ設定の変更を加えます。設定を展開すると、新しい変更はスタンバイ装置にも送信されます。

ただし、一部のプロパティはスタンバイ装置固有です。スタンバイ装置では次の設定を変更できます。

- 管理 IP アドレスとゲートウェイ。
- （CLI のみ）管理ユーザ アカウントのパスワード。この変更を行うことができるのはCLIのみで、FDM で行うことはできません。

さらに、スタンバイ デバイスでは次のアクションを実行できます。

- HAの一時停止、再開、リセット、解除などのハイ アベイラビリティ アクションと、アクティブ モードとスタンバイ モードの切り替え。
- ダッシュボードとイベントデータはデバイスごとに一意であり、同期されません。これには、イベント ビューアのカスタム ビューが含まれます。
- 監査ログ情報はデバイスごとに一意です。
- スマートライセンスの登録。ただし、アクティブ装置でオプションのライセンスを有効または無効にする必要があります。このアクションはスタンバイ装置と同期され、適切なライセンスが要求または解放されます。
- バックアップ（ただし復元ではない）。バックアップを復元するには装置でHAを解除する必要があります。バックアップにHA設定が含まれている場合、装置はHAグループに再び参加します。

- ソフトウェア アップグレードのインストール。
- トラブルシューティング ログの生成。
- 地理位置情報データベースまたはセキュリティ インテリジェンス データベースの手動更新。これらのデータベースは、装置間で同期されません。更新スケジュールを作成する場合、装置は独立して一貫性を維持できます。
- **[モニタリング（Monitoring）]**>**[セッション（Sessions）]**ページからアクティブなFirepower Device Manager のユーザ セッションを表示したり、セッションを削除できます。

ハイ アベイラビリティのシステム要件

ここでは、ハイ アベイラビリティ設定に2台のデバイスを実装する前に満たさなくてはならない要件について説明します。

HA のハードウェア要件

ハイ アベイラビリティ設定で2つのデバイスを結び付けるには、次のハードウェア要件を満たす必要があります。

- デバイスはまったく同じハードウェア モデルである必要があります。
- デバイスは同じ数の同じタイプのインターフェイスを備えている必要があります。
- デバイスには同じモジュールが取り付けられている必要があります。たとえば、一方にオプションのネットワーク インターフェイス モジュールがある場合は、もう一方のデバイスに同じモジュールを取り付ける必要があります。

HA のソフトウェア要件

ハイ アベイラビリティ設定で2つのデバイスを結び付けるには、次のソフトウェア要件を満たす必要があります。

- デバイスは、まったく同じバージョンのソフトウェア（つまり、1 番目のメジャー番号、2 番目のマイナー番号、および 3 番目のメンテナンス番号が同じ）を実行する必要があります。バージョンは、Firepower Device Manager の [デバイス（Devices）] ページで確認できます。また、CLI で **show version** コマンドを使用して確認することもできます。異なるバージョンを実行するデバイスでも参加できますが、設定がスタンバイ装置にインポートされず、装置を同じソフトウェア バージョンにアップグレードしないとフェールオーバーは機能しません。
- 両方のデバイスがローカル マネージャ モードになっている（つまり、Firepower Device Manager を使用して設定されている）必要があります。両方のシステムでFirepower Device Managerにログインできる場合は、それらがローカルマネージャ モードになっています。CLI で **show managers** コマンドを使用して確認することもできます。

- 各デバイスの初期セットアップ ウィザードを完了する必要があります。
- 各デバイスに固有の管理 IP アドレスが必要です。管理インターフェイスの設定は、デバイス間で同期されません。
- デバイスの NTP 設定が同じである必要があります。
- DHCP を使用してアドレスを取得するようにインターフェイスを設定することはできません。つまり、すべてのインターフェイスに静的 IP アドレスが必要です。
- Cisco Defense Orchestrator への登録が両方のデバイスで同じステータスになっている必要があります（両方登録済みまたは両方未登録）。
- 次のクラウド サービスでは、プライマリ デバイスとセカンダリ デバイスの両方を有効にする必要があります。または、セカンダリが有効になっている間はプライマリを無効にすることができます（セカンダリは HA への参加後に無効になります）。
  - Cisco Success Network
  - Cisco Threat Response
- ハイ アベイラビリティを設定する前に、保留中の変更を展開する必要があります。

HA のライセンス要件

ハイ アベイラビリティを設定する前に、装置が同じ状態（両方とも基本ライセンスに登録されているか両方とも評価モードになっている）である必要があります。デバイスが登録されている場合は、それらを異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態（両方有効または両方無効）である必要があります。ただし、装置ごとに異なるオプション ライセンスを有効にすることは可能です。

運用時には、ハイ アベイラビリティ ペアの装置に同じライセンスが必要です。アクティブ装置で行ったライセンスの変更は、展開時にスタンバイ装置で繰り返されます。

ハイ アベイラビリティ構成には、2 つのスマート ライセンス資格（ペアを構成するデバイスごとに 1 つ）が必要です。各デバイスに適用するためにアカウントに十分なライセンスがあることを確認する必要があります。ライセンスが不足している場合は、一方のデバイスが準拠状態でも、もう一方のデバイスが非準拠になる可能性があります。

たとえば、アクティブデバイスに基本ライセンスと脅威ライセンスが割り当てられており、スタンバイ デバイスに基本ライセンスのみが割り当てられている場合、スタンバイ装置は Cisco Smart Software Manager と通信してアカウントから利用可能な脅威ライセンスを取得します。スマート ライセンス アカウントに購入済みの十分な権限付与が含まれていない場合は、正しい数のライセンスが購入されるまで、アカウントがコンプライアンス適用外（そのため、アクティブ デバイスにコンプライアンスが適用されていてもスタンバイ デバイスはコンプライアンス適用外）になります。

（注） 輸出規制対象の機能の設定が異なるアカウントにデバイスを登録した場合、または1つの装置が登録済みで、もう 1 つが評価モードにある HA ペアを作成しようとした場合、HA の参加が失敗する可能性があります。輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワークセグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置で HA を手動で中断する必要があります。

ハイ アベイラビリティのガイドライン

その他のガイドライン

- 169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、それらをフェールオーバーまたはステート リンクに使用することはできません。
- アクティブ装置からの設定は、アクティブ装置で展開ジョブを実行したときに、スタンバイ装置に同期されます。ただし、一部の変更は、変更を展開するまでスタンバイ装置で同期されていなくても、保留中の変更に表示されない場合があります。次のいずれかを変更した場合、変更は隠され、これらがスタンバイ装置で設定される前に展開ジョブを実行する必要があります。変更をすぐに適用する必要がある場合は、保留中の変更に表示されるその他の変更を行う必要があります。非表示となる変更には、ルール、ジオデータベース、セキュリティ インテリジェンスまたは VDB 更新のスケジュール、バックアップのスケジュール、NTP、管理インターフェイスの DNS、ライセンス権限付与、クラウド サービス オプション、URL フィルタリング オプションの編集が含まれます。
- プライマリ装置とセカンダリ装置の両方でバックアップを実行する必要があります。バックアップを復元するには、まず HA を解除する必要があります。両方のユニットで同じバックアップを復元しないでください（両方のユニットがアクティブになってしまうため）。代わりに、まず、アクティブにする装置でバックアップを復元し、その後に、別のユニットで同等のバックアップを復元してください。
- さまざまなアイデンティティ ソースの [テスト（Test）] ボタンは、アクティブ装置でのみ機能します。スタンバイ デバイスのアイデンティティ ソース接続をテストする必要がある場合は、まず、モードを切り替えてスタンバイ ピアをアクティブ ピアにする必要があります。
- ハイ アベイラビリティ設定を作成または解除すると、設定の変更が展開されたときに両方のデバイスで Snort 検査プロセスが再開されます。これにより、プロセスが完全に再開されるまでに通過トラフィックの中断が発生する可能性があります。
- ハイ アベイラビリティの初期設定時に、セカンダリ上のセキュリティ インテリジェンスおよび地理位置情報データベースのバージョンがプライマリ上のバージョンと異なる場合、データベースを更新するジョブはセカンダリ装置でスケジュールされます。これらのジョブは、次の展開時にアクティブ装置から実行されます。HA結合に失敗した場合でも、これらのジョブはそのまま残り、次の展開時に実行されます。

- ユーザが外部アイデンティティ ソースに対して認証される場合（つまり、ローカル**管理者**ユーザではない場合）、そのユーザはスタンバイ装置にログインできなくなる可能性があります。アクティブ装置に少なくとも一度ログインし、設定を展開すると、スタンバイ装置にログインできます。この制限は、ローカル**管理者**ユーザには適用されません。
- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行している接続済みスイッチ ポートが、トポロジの変化を検出すると 30 ～ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング ステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

  interface *interface_id* **spanning-tree portfast**

  この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。
- ハイ アベイラビリティ ペアに接続されているスイッチでポート セキュリティを設定すると、フェールオーバーイベントが発生したときに通信上の問題が発生する可能性があります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動するときに、スイッチのポート セキュリティ機能によって違反フラグが付けられるために発生します。
- アクティブ/スタンバイ ハイ アベイラビリティと VPN IPsec トンネルの場合、VPN トンネル経由で SNMP を使用してアクティブ装置とスタンバイ装置の両方をモニタすることはできません。スタンバイ装置にはアクティブ VPN トンネルがなく、ネットワーク管理システム（NMS）宛てのトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

ハイ アベイラビリティの設定

ハイ アベイラビリティのセットアップを使用して、デバイスで障害が発生している場合でもネットワーク接続を確保します。アクティブ/スタンバイ ハイ アベイラビリティを使用して、2 台のデバイスがリンクされます。そのため、アクティブ デバイスが故障した場合、スタンバイ デバイスが引き継ぎ、ユーザは接続の問題をほとんど感じません。

次の手順で、アクティブ/スタンバイ ハイ アベイラビリティ（HA）ペアをセットアップするエンドツーエンド プロセスについて説明します。

手順

ステップ 1 2 台の装置でのハイ アベイラビリティの準備 （15 ページ）。

ステップ 2 ハイ アベイラビリティ用のプライマリ装置の設定 （17 ページ）。

ステップ 3 ハイ アベイラビリティ用のセカンダリ装置の設定 （20 ページ）。

ステップ 4 ヘルス モニタリングのフェールオーバー基準の設定 （21 ページ）。

基準には、ピア モニタリングとインターフェイス モニタリングが含まれます。すべてのフェールオーバー基準にはデフォルト設定がありますが、デフォルト設定を調べて、それらがネットワークで機能していることを確認する必要があります。

- ピア装置のヘルス モニタリング フェールオーバー基準の設定 （22 ページ）。
- インターフェイスのヘルス モニタリング フェールオーバー基準の設定 （23 ページ）。

  インターフェイス テストの詳細については、システムがインターフェイス ヘルスをテストする方法 （26 ページ）を参照してください。

ステップ 5 （オプション。ただし推奨。）スタンバイ IP および MAC アドレスの設定 （27 ページ）。

ステップ 6 （オプション）ハイ アベイラビリティ設定の確認 （28 ページ）。

2 台の装置でのハイ アベイラビリティの準備

ハイ アベイラビリティを正常に設定するには、多くのことを事前に正しく準備する必要があります。

手順

ステップ 1 デバイスがHA のハードウェア要件 （11 ページ）に説明されている要件を満たしていることを確認します。

ステップ 2 単一のフェールオーバー リンクを使用するのか、別のフェールオーバー リンクとステートフル フェールオーバー リンクを使用するのかを決め、使用するポートを特定します。

各リンクのそれぞれのデバイスで同じポート番号を使用する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで GigabitEthernet 1/3 を使用します。使用する内容を把握しておくことで、誤ってその他の目的で使用することがなくなります。詳細については、フェールオーバー リンクとステートフル フェールオーバー リンク （4 ページ）を参照してください。

ステップ 3 デバイスをインストールしてネットワークに接続し、各デバイスで初期セットアップ ウィザードを完了します。

a) フェールオーバー リンクとデータ リンクの中断の回避 （6 ページ）で推奨のネットワーク設計を確認します。

b) インターフェイスの接続の説明に従い、少なくとも外部インターフェイスだけは接続します。

その他のインターフェイスも接続できますが、特定のサブネットへの接続には各デバイスで同じポートを使用する必要があります。各デバイスでは同じ設定が共有されるため、デバイスは同じ方法でネットワークに接続する必要があります。

（注） セットアップ ウィザードでは、管理インターフェイスと内部インターフェイスの IP アドレスを変更できません。そのため、プライマリ デバイス上のそれらのインターフェイスのいずれかをネットワークに接続する場合、セカンダリ デバイスのインターフェイスは接続しないでください。接続すると IP アドレスの競合が発生します。ワークステーションをそれらのインターフェイスのいずれかに直接接続し、DHCP を介してアドレスを取得できるため、Firepower Device Manager に接続して、デバイスを設定できます。

c) 各デバイスで初期セットアップ ウィザードを完了します。外部インターフェイスの静的 IP アドレスを指定していることを確認します。さらに、同じ NTP サーバを設定します。詳細については、初期設定の完了を参照してください。

各装置で同じライセンスと Cisco Success Network オプションを選択します。たとえば、それぞれに評価モードを選択したり、デバイスを登録したりします。

d) セカンダリ デバイスで、**[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]** を選択して一意の IP アドレスを設定し、必要に応じてゲートウェイを変更します。また、ニーズに合わせて DHCP サーバの設定を無効化または変更します。

e) セカンダリ デバイスで、**[デバイス（Device）] > [インターフェイス（Interface）]** を選択し、内部インターフェイスを編集します。IP アドレスを削除するか、または変更します。また、同じネットワーク上に 2 つの DHCP サーバは定義できないため、インターフェイスに定義されている DHCP サーバを削除します。

f) 設定をセカンダリ デバイスに展開します。

g) ネットワーク トポロジに基づいて必要な場合は、プライマリ デバイスにログインして、管理アドレス、ゲートウェイ、DHCP サーバの設定、および内部インターフェイスの IP アドレスを変更します。変更を加えた場合は、設定を展開します。

h) 内部インターフェイス、または管理インターフェイス（別の管理ネットワークを使用する場合）を接続していない場合は、ここでそれらのインターフェイスをスイッチに接続できます。

ステップ 4 デバイスのソフトウェア バージョンが完全に同じである（つまり、同じメジャー（1 番）、マイナー（2 番）、メンテナンス（3 番）の番号が付いている）ことを確認します。バージョンは、Firepower Device Manager の [デバイス（Devices）] ページで確認できます。また、CLI で **show version** コマンドを使用して確認することもできます。

同じソフトウェア バージョンが実行されていない場合は、Cisco.com から推奨のソフトウェア バージョンを取得して、各デバイスにインストールします。詳細は、Firepower Threat Defense ソフトウェアのアップグレードを参照してください。

ステップ 5 接続して、フェールオーバー リンクとステートフル フェールオーバー リンクを設定します。

a) （フェールオーバー リンクとデータ リンクの中断の回避 （6 ページ）で選択した）推奨のネットワーク設計に従い、適切に各デバイスのフェールオーバーインターフェイスをスイッチに接続するか、デバイス間で直接接続します。

b) 別のステート リンクを使用している場合は、各デバイスのステートフル フェールオーバーインターフェイスも適切に接続します。

c) 次に各デバイスにログインして、**[デバイス（Device）]** > **[インターフェイス（Interface）]** にアクセスします。各インターフェイスを編集し、インターフェイス名やIPアドレスが設定されていないことを確認します。

名前付きのインターフェイスが設定されている場合、その名前を削除する前に、セキュリティゾーンからそれらのインターフェイスを削除して、その他の設定を削除する必要がある場合があります。名前の削除に失敗した場合は、エラーメッセージを調べて、加える必要があるその他の変更を確認します。

ステップ 6 プライマリ デバイスで、残りのデータ インターフェイスを接続してデバイスを設定します。

a) **[デバイス（Device）]** > **[インターフェイス（Interface）]** を選択し、トラフィックの通過に使用される各インターフェイスを編集し、プライマリ静的 IP アドレスを設定します。

b) セキュリティゾーンにインターフェイスを追加し、接続されたネットワーク上のトラフィックの処理に必要な基本的なポリシーを設定します。設定例については、Firepower Threat Defense の使用例にリストされているトピックを参照してください。

c) 設定を展開します。

ステップ 7 HA のソフトウェア要件 （11 ページ）で説明されているすべての要件を満たしていることを確認します。

ステップ 8 一貫性のあるライセンス（登録済みまたは評価モード）を保有していることを確認します。詳細については、HA のライセンス要件 （12 ページ）を参照してください。

ステップ 9 セカンダリ デバイスで、残りのデータ インターフェイスをプライマリ デバイスの同等のインターフェイスと同じネットワークに接続します。インターフェイスは設定しないでください。

ステップ 10 各デバイスで **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** を選択し、Cisco Defense Orchestrator の設定および Cisco Success Network や Cisco Threat Defense などのその他のクラウド サービスの設定が同じであることを確認します。

これで、プライマリ デバイスでハイ アベイラビリティを設定する準備が整いました。

ハイ アベイラビリティ用のプライマリ装置の設定

アクティブ/スタンバイ ハイ アベイラビリティ ペアをセットアップするには、まず、プライマリ デバイスを設定する必要があります。プライマリ デバイスは、通常の状況下でアクティブにする予定の装置です。セカンダリ デバイスは、プライマリ装置が使用できなくなるまでスタンバイ モードのままです。

プライマリにするデバイスを選択し、そのデバイス上の Firepower Device Manager にログインして次の手順に従います。

（注） いったんハイ アベイラビリティ ペアを確立すると、この手順で説明する設定を編集するにはペアを破棄する必要があります。

始める前に

フェールオーバー リンクとステートフル フェールオーバー リンク用に設定するインターフェイスに名前が付いていないことを確認します。名前が付いている場合は、セキュリティゾーンオブジェクトを含め、それらを使用するポリシーからインターフェイスを削除してインターフェイスを編集し、名前を削除する必要があります。また、インターフェイスはパッシブモードではなくルーテッドモードにする必要もあります。これらのインターフェイスは、HA 設定での使用専用にする必要があります。他のプロセスに使用することはできません。

保留中の変更がある場合は、それらを展開してから HA を設定する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側で、[ハイアベイラビリティ（High Availability）] グループの横にある [設定（Configure）] をクリックします。

デバイスで初めて HA を設定する場合、グループは次のように表示されます。

ステップ 3 [ハイアベイラビリティ（High Availability）] ページで、[プライマリデバイス（Primary Device）] ボックスをクリックします。

セカンダリ デバイスが既に設定されていて、その設定をクリップボードにコピーする場合は、[クリップボードから貼り付け（Paste from Clipboard）] ボタンをクリックすると設定を貼り付けることができます。これにより、適切な値でフィールドが更新され、後で確認できます。

ステップ 4 [フェールオーバーリンク（Failover Link）] プロパティを設定します。

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認し、設定の変更を同期します。詳細については、フェールオーバーリンク （4 ページ）を参照してください。

- [物理インターフェイス（Physical Interface）] フェールオーバー リンクとして使用するセカンダリ デバイスに接続するインターフェイスを選択します。名前が付いていないインターフェイスにする必要があります。
- [タイプ（Type）]：インターフェイスに IPv4 アドレスまたは IPv6 アドレスを使用するかどうか選択します。設定できるアドレス タイプは 1 つのみです。
- [プライマリ IP（Primary IP）]：このデバイス上のインターフェイスの IP アドレスを入力します。たとえば、192.168.10.1 と入力します。IPv6 アドレスの場合、標準表記にプレフィックス長を含める必要があります（2001:a0a:b00::a0a:b70/64 など）。
- [セカンダリ IP（Secondary IP）]：セカンダリ デバイス上のインターフェイスについて、リンクのもう一方の端に設定する必要がある IP アドレスを入力します。このアドレスはプライマリ アドレスと同じサブネット上に存在し、プライマリ アドレスとは異なるアドレスである必要があります（192.168.10.2 または 2001:a0a:b00::a0a:b71/64 など）。

- [ネットマスク（Netmask）]（IPv4 のみ）：プライマリ/セカンダリ IP アドレスのサブネット マスクを入力します。

ステップ 5 [ステートフルフェールオーバーリンク（Stateful Failover Link）] プロパティを設定します。

システムは、ステート リンクを使用して接続状態の情報をスタンバイ デバイスに渡します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。フェールオーバー リンクと同じリンクを使用するか、別のリンクを設定することができます。

- [フェールオーバーリンクと同じインターフェイスを使用する（Use the Same Interface as the Failover Link）]：フェールオーバー通信およびステートフル フェールオーバー通信に単一のリンクを使用する場合は、このオプションを選択します。このオプションを選択する場合は、次の手順に進みます。
- [物理インターフェイス（Physical Interface）]：別のステートフル フェールオーバー リンクを使用する場合は、ステートフル フェールオーバー リンクとして使用するセカンダリ デバイスに接続したインターフェイスを選択します。名前が付いていないインターフェイスにする必要があります。次のプロパティを設定します。
  - [タイプ（Type）]：インターフェイスに IPv4 アドレスまたは IPv6 アドレスを使用するかどうか選択します。設定できるアドレス タイプは 1 つのみです。
  - [プライマリIP（Primary IP）]：このデバイス上のインターフェイスの IP アドレスを入力します。アドレスは、フェールオーバー リンクに使用されるものとは別のサブネット上にある必要があります。たとえば、192.168.11.1 と入力します。IPv6 アドレスの場合、標準表記にプレフィックス長を含める必要があります（2001:a0a:b00:a::a0a:b70/64 など）。
  - [セカンダリIP（Secondary IP）]：セカンダリ デバイス上のインターフェイスについて、リンクのもう一方の端に設定する必要がある IP アドレスを入力します。このアドレスはプライマリ アドレスと同じサブネット上に存在し、プライマリ アドレスとは異なるアドレスである必要があります（192.168.11.2 または 2001:a0a:b00:a::a0a:b71/64 など）。
  - [ネットマスク（Netmask）]（IPv4 のみ）：プライマリ/セカンダリ IP アドレスのサブネット マスクを入力します。

ステップ 6 （オプション）ペアの 2 台の装置間での通信を暗号化する場合は、[IPsec暗号キー（IPsec Encryption Key）] 文字列を入力します。

セカンダリ ノードでまったく同じキーを設定する必要があるため、入力した文字列をメモしてください。

キーを入力しなければ、フェールオーバー リンクとステートフル フェールオーバー リンクでのすべての通信はプレーンテキストで実行されます。インターフェイス間をケーブルで直接接続していない場合、これによってセキュリティの問題が発生することがあります。

ステップ 7 [HAの有効化（Activate HA）] をクリックします。

システムは、すぐにデバイスに設定を展開します。展開ジョブを開始する必要はありません。設定が保存され、展開が進行中であるというメッセージが表示されない場合は、ページ上部にスクロールして、エラー メッセージを確認します。

設定はクリップボードにもコピーされます。コピーを使用すると、簡単にセカンダリ装置を設定できます。セキュリティを強化するため、暗号キーはクリップボードのコピーには含まれません。

設定が完了すると、実行する必要がある次の手順を説明するメッセージが表示されます。情報を確認したら、[了解（Got It）] をクリックします。

この時点で、[ハイアベイラビリティ（High Availability）]ページが表示され、デバイス ステータスが [ネゴシエーション中（Negotiating）] になっている必要があります。ステータスはピアの設定前でも [アクティブ（Active）] に変わります。設定するまで [故障（Failed）] と表示されます。

これで、セカンダリ装置を設定できるようになりました。ハイ アベイラビリティ用のセカンダリ装置の設定 （20 ページ）を参照してください。

（注） 選択したインターフェイスは直接設定されません。ただし、CLI に **show interface** と入力すると、インターフェイスが特定の IP アドレスを使用していることが表示されます。インターフェイスには「failover-link」という名前が付いています。別のステート リンクを設定する場合は「stateful-failover-link」になります。

ハイ アベイラビリティ用のセカンダリ装置の設定

プライマリ デバイスをアクティブ/スタンバイ ハイ アベイラビリティ向けに設定した後、セカンダリ デバイスを設定する必要があります。そのデバイス上の Firepower Device Manager にログインして、次の手順に従います。

（注） まだそのように設定していな場合は、プライマリ デバイスからクリップボードにハイ アベイラビリティ設定をコピーします。手動でデータを入力するより、コピーと貼り付けを使用してセカンダリ デバイスを設定するほうがはるかに簡単です。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側で、[ハイアベイラビリティ（High Availability）] グループの横にある [設定（Configure）] をクリックします。

デバイスで初めて HA を設定する場合、グループは次のように表示されます。

ステップ 3 [ハイアベイラビリティ（High Availability）] ページで、[セカンダリデバイス（Secondary Device）] ボックスをクリックします。

ステップ 4 次のいずれかを実行します。

- [簡単な方法（Easy method）] : [クリップボードから貼り付け（Paste from Clipboard）] ボタンをクリックして設定に貼り付け、[OK] をクリックします。これにより、適切な値でフィールドが更新され、後で確認できます。
- [手動の方法（Manual method）] : フェールオーバー リンクとステートフル フェールオーバー リンクを直接設定します。プライマリ デバイスに入力したのとまったく同じ設定をセカンダリ デバイスに入力します。

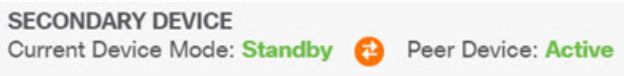
ステップ 5 プライマリ デバイスで [IPSec暗号キー（IPSec Encryption Key）] を設定した場合、まったく同じキーをセカンダリ デバイスに入力します。

ステップ 6 [HAの有効化（Activate HA）] をクリックします。

システムは、すぐにデバイスに設定を展開します。展開ジョブを開始する必要はありません。設定が保存され、展開が進行中であるというメッセージが表示されない場合は、ページ上部にスクロールして、エラー メッセージを確認します。

設定が完了すると、HA が設定されたことを示すメッセージが表示されます。[了解（Got It）] をクリックして、メッセージを閉じます。

この時点で、[ハイアベイラビリティ（High Availability）]ページが表示され、デバイス ステータスにこれがセカンダリ デバイスであることが示されている必要があります。プライマリ デバイスとの結合が成功した場合、デバイスはプライマリと同期して、最終的にはスタンバイ モードになります。ピアがアクティブになります。



（注） 選択したインターフェイスは直接設定されません。ただし、CLI に **show interface** と入力すると、インターフェイスが特定の IP アドレスを使用していることが表示されます。インターフェイスには「failover-link」という名前が付いています。別のステート リンクを設定する場合は「stateful-failover-link」になります。

ヘルス モニタリングのフェールオーバー基準の設定

ハイ アベイラビリティ設定の装置は、全体的な健全性とインターフェイスの健全性をモニタします。

フェールオーバー基準により、ピアに障害が発生したかどうかを判断するヘルス モニタリング メトリックが定義されます。アクティブ ピアが基準に違反した装置である場合、スタンバイ装置へのフェールオーバーがトリガーされます。スタンバイ ピアが基準に違反した装置である場合、スタンバイ ピアは障害が発生した装置としてマークされ、フェールオーバーに使用できなくなります。

アクティブ デバイスでのみフェールオーバー基準を設定できます。

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。

表 *2:* フェールオーバー基準に基づくフェールオーバー時間

フェールオーバー トリガー イベント	最小	デフォルト	最大数
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ装置のインターフェイスの物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

ここでは、フェールオーバー ヘルス モニタリング基準をカスタマイズする方法と、システムがインターフェイスをテストする方法について説明します。

ピア装置のヘルス モニタリング フェールオーバー基準の設定

ハイ アベイラビリティ設定の各ピアは、hello メッセージを使用してフェールオーバー リンクをモニタすることによって相手装置の状態を判断します。装置がフェールオーバー リンクで3回連続して hello メッセージを受信しない場合、装置はフェールオーバー リンクを含む各データ インターフェイスにLANTESTメッセージを送信し、ピアが応答するかどうか検証します。デバイスが行うアクションは、相手装置からの応答によって異なります。

- デバイスがフェールオーバー リンクで応答を受信した場合は、フェールオーバーを行いません。
- デバイスがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- デバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

hello メッセージのポーリング時間および保留時間を設定できます。

手順

ステップ 1 アクティブ デバイスで、[デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

フェールオーバー条件は、[ハイアベイラビリティ（High Availability）] ページの右側の列に表示されます。

ステップ 3 [ピアのタイミング設定（Peer Timing Configuration）] を定義します。

これらの設定では、アクティブ デバイスがスタンバイ デバイスにフェールオーバーできる早さを決定します。ポーリング時間が短いほど、デバイスは短時間で障害を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。ほとんどの場合、デフォルト設定が適切です。

1 回のポーリング期間中に装置がフェールオーバー インターフェイスで hello パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

- [ポーリング時間（Poll Time）] : hello メッセージ間の間隔。1 ～ 15 秒または 200 ～ 999 ミリ秒を入力します。デフォルト値は 1 秒です。
- [保留時間（Hold Time）] : 装置が、フェールオーバー リンクで hello メッセージを受信する間隔。この時間を経過すると、ピア装置で障害が発生したと見なされます。保留時間は、ポーリング時間の 3 倍以上にする必要があります。1 ～ 45 秒または 800 ～ 999 ミリ秒を入力します。デフォルトは 15 秒です。

ステップ 4 [保存（Save）] をクリックします。

インターフェイスのヘルス モニタリング フェールオーバー基準の設定

デバイス モデルに応じて、最大 211 のインターフェイスをモニタできます。重要なインターフェイスをモニタする必要があります。たとえば、重要なネットワーク間のスループットを保証するインターフェイスなどです。スタンバイ IP アドレスを設定する場合、さらにインターフェイスを常にアップ状態にする必要がある場合にのみインターフェイスをモニタします。

装置が、2回のポーリング期間中にモニタ対象のインターフェイス上でhelloメッセージを受信しない場合、インターフェイステストを実行します。1つのインターフェイスに対するすべてのインターフェイステストがすべて失敗したが、相手装置のこの同じインターフェイスが正常にトラフィックを渡し続けている場合、そのインターフェイスは故障していると見なされます。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われます。相手装置のインターフェイスもすべてのネットワークテストに失敗した場合、両方のインターフェイスが「Unknown」状態になり、フェールオーバー制限に向けてのカウントは行いません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したデバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

show monitor-interface コマンドを使用して、CLI または CLI コンソールからインターフェイスの HA ステータスをモニタできます。詳細については、HA モニタ対象インターフェイスのステータスのモニタリング （42 ページ）を参照してください。

（注） のインターフェイスの 1 つがダウンしたときも、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスがダウンしていることを装置が検出すると、インターフェイスの保留時間を待たずにすぐにフェールオーバーが発生します（1 インターフェイスのデフォルトしきい値を維持している場合）。インターフェイスの保留時間が有効であるのは、装置が自身のステータスを OK と見なしているときだけです（ピアから hello パケットを受信していなくても）。

始める前に

デフォルトでは、すべての名前付き物理インターフェイスが HA モニタリングに選択されています。したがって、重要ではない物理インターフェイスのモニタリングを無効にする必要があります。サブインターフェイスまたはブリッジグループでは、手動でモニタリングを有効にする必要があります。

インターフェイス モニタリングを完全に無効にしてインターフェイスの故障によるフェールオーバーを防止するには、単純に、HA モニタリングが有効になっているインターフェイスがないことを確認します。

手順

ステップ 1 アクティブ デバイスで、[デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

フェールオーバー条件は、[ハイアベイラビリティ（High Availability）] ページの右側の列に表示されます。

ステップ 3 [インターフェイス障害しきい値（Interface Failure Threshold）] を定義します。

故障したインターフェイスの数がしきい値を満たすと、装置は自身を故障としてマークします。装置がアクティブ装置の場合、スタンバイ装置にフェールオーバーします。装置がスタンバイ装置の場合、自身を故障としてマークすることによって、アクティブ装置はその装置をフェールオーバーに利用できると見なさなくなります。

この条件を設定する場合、モニタするインターフェイスの数を考慮します。たとえば、2 つのインターフェイスでのみモニタリングを有効にすると、10 個のインターフェイスのしきい値に到達することはありません。インターフェイスのプロパティを編集するときに [詳細オプショ

ン（Advanced Options）] タブの [HAモニタリングの有効化（Enable for HA Monitoring）] オプションを選択することで、インターフェイスのモニタリングを設定します。

デフォルトでは、1 つのモニタ対象インターフェイスが故障すると、装置は自身を故障としてマークします。

次の [フェールオーバー条件（Failover Criteria）] オプションのいずれかを選択して、インターフェイス障害のしきい値を設定できます。

- [故障したインターフェイスの数を超える（Number of failed interfaces exceeds）]：インターフェイスの生の数字を入力します。デフォルトは1です。実際には、最大値はデバイス モデルに依存して変わりますが、211 以上を入力することはできません。この条件を使用すると、デバイス サポートよりも大きい数を入力すると展開エラーが発生します。より小さい数を試すか、代わりにパーセンテージを使用します。
- [故障インターフェイスのパーセンテージを超える（Percentage of failed interfaces exceeds）]：1 ～ 100 の数値を入力します。たとえば、50% と入力して 10 個のインターフェイスをモニタする場合、5 個のインターフェイスが故障するとデバイスは自身を故障としてマークします。

ステップ 4 [インターフェイスタイミング設定（Interface Timing Configuration）] を定義します。

これらの設定では、インターフェイスで障害が発生したかどうかをアクティブデバイスが判断できる早さを決定します。ポーリング時間が短いほど、デバイスは短時間でインターフェイスの障害を検出できます。ただし、検出が早いほど、実際には健全な状態でもビジー状態のインターフェイスが障害発生とマークされ、必要以上に頻繁にフェールオーバーが生じる可能性があります。ほとんどの場合、デフォルト設定が適切です。

インターフェイス リンクがダウンしていると、インターフェイスのテストは実行されません。また、故障したインターフェイスの数が設定されたインターフェイス フェールオーバーしきい値に合致するかまたはそれを超過すると、スタンバイ装置は1回のインターフェイス ポーリング期間でアクティブになります。

- [ポーリング時間（Poll Time）]：helloパケットがデータ インターフェイスで送信される頻度。1 ～ 15 秒または 500 ～ 999 ミリ秒を入力します。デフォルトは 5 秒です。
- [保留時間（Hold Time）]：保留時間によって、helloパケットを受信できなかったときからインターフェイスが故障とマークされるまでの時間が決まります。5 ～ 75 秒を入力します。ポーリング時間の 5 倍に満たない保持時間は入力できません。

ステップ 5 [Save] をクリックします。

ステップ 6 モニタする各インターフェイスの HA モニタリングを有効にします。

a) **[デバイス（Device）] > [インターフェイス（Interfaces）]** を選択します。

インターフェイスをモニタしている場合、[HAのモニタ（Monitor for HA）] 列は [有効（Enabled）] になります。

b) モニタリング ステータスを変更するインターフェイスの編集アイコン（）をクリックします。

フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスは編集できません。インターフェイス モニタリングはそれらに適用されません。

c) [詳細オプション（Advanced Options）] タブをクリックします。
d) 必要に応じて、[HAモニタリングの有効化（Enable for HA Monitoring）] チェックボックスを選択または選択解除します。
e) [OK] をクリックします。

ステップ 7 （オプション。ただし推奨。）モニタ対象インターフェイスのスタンバイ IP アドレスおよび MAC アドレスを設定します。スタンバイ IP および MAC アドレスの設定 （27 ページ）を参照してください。

システムがインターフェイス ヘルスをテストする方法

システムは、ユーザがハイ アベイラビリティ ヘルスをモニタしているインターフェイスを継続的にテストします。インターフェイスのテストに使用されるアドレスは、ユーザが設定するアドレス タイプに基づきます。

- インターフェイスに IPv4 アドレスと IPv6 アドレスの両方が設定されている場合、デバイスは IPv4 アドレスを使用してヘルス モニタリングを実行します。
- インターフェイスに IPv6 アドレスだけが設定されている場合、デバイスは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャスト ping テストの場合、デバイスは IPv6 全ノード アドレス（FE02::1）を使用します。

システムは、各装置で次のテストを実行します。

1. リンクアップ/ダウンテスト：インターフェイス ステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、装置はそれに障害が発生していると見なします。ステータスが Up（稼働中）の場合、装置はネットワーク動作のテストを実行します。

2. ネットワーク アクティビティ テスト：ネットワークの受信アクティビティのテストです。このテストの目的は、LANTEST メッセージを使用してネットワーク トラフィックを生成し、障害が発生しているユニット（いずれか 1 つ）を特定することです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。ユニットがテスト中にパケットを受信したらすぐに（最大 5 秒）、そのインターフェイスは動作可能と見なされます。いずれか一方の装置だけがトラフィックを受信している場合は、トラフィックを受信しなかった装置が故障していると見なされます。いずれの装置もトラフィックを受信しなかった場合、装置は ARP テストを開始します。

3. ARP テスト：取得したエントリの最後の 2 つの装置 ARP キャッシュの読み取り。ネットワーク トラフィックを発生させるため、ユニットから 1 回に 1 つずつ、これらのデバイスに ARP 要求が送信されます。各要求後、装置は最大 5 秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると見なされます。トラフィックが受信されなければ、次のデバイスに ARP 要求が送信され

ます。リストの最後まで来てもトラフィックが受信されない場合は、pingテストが実行されます。

4. ブロードキャスト ping テスト：このテストでは、ブロードキャスト ping 要求が送信されます。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなければ、ARPテストからやり直します。

スタンバイ IP および MAC アドレスの設定

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。スタンバイ アドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IPアドレスがないと、アクティブ装置はスタンバイインターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

1. プライマリ装置に障害が発生すると、セカンダリ装置はプライマリ ユニットの IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
2. 現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。しかし、プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスは手動で設定できます。

仮想MACアドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータのARPテーブルをクリアする必要がある場合があります。Firepower Threat Defense デバイス は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスのMACアドレスの変更を認識できません。

手順

ステップ 1 **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** を選択します。

少なくとも、HA をモニタしているインターフェイスのスタンバイ IP アドレスと MAC アドレスを設定する必要があります。インターフェイスをモニタしている場合、[HAのモニタ（Monitor for HA）] 列は [有効（Enabled）] になります。

ステップ 2 スタンバイ アドレスを設定するインターフェイスの編集アイコン（）をクリックします。

フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスは編集できません。ハイ アベイラビリティを設定する場合、これらのインターフェイスの IP アドレスを設定します。

ステップ 3 [IPv4アドレス（IPv4 Address）] タブおよび [IPv6アドレス（IPv6 Address）] タブでスタンバイ IP アドレスを設定します。

スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。使用している IP バージョンごとにスタンバイ アドレスを設定します。

ステップ 4 [詳細オプション（Advance Options）] タブをクリックして、MAC アドレスを設定します。

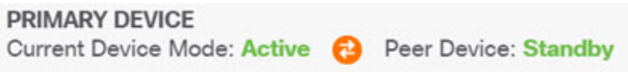
デフォルトでは、システムはインターフェイスのネットワークインターフェイスカード（NIC）に焼き込まれた MAC アドレスを使用します。したがって、インターフェイスのすべてのサブインターフェイスは同じ MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、ハイ アベイラビリティを設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MACアドレス（MAC Address）]：H.H.H 形式の Media Access Control アドレス。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は 000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。
- [スタンバイMACアドレス（Standby MAC Address）]：ハイ アベイラビリティで使用します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 5 [OK] をクリックします。

ハイ アベイラビリティ設定の確認

ハイ アベイラビリティの設定が完了したら、両方のデバイスが「動作中」でアクティブ/スタンバイ モードであることが、デバイスのステータスに示されていることを確認します。



次の手順を使用して、ハイ アベイラビリティの設定が機能していることを確認できます。

手順

ステップ 1 FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

設定済みの各インターフェイスに接続されている、少なくとも 1 つのワークステーションからシステムへの接続をテストします。

ステップ 2 次のいずれかを実行して、モードを切り替え、アクティブな装置をスタンバイ装置にします。

- Firepower Device Manager で、**[デバイス（Device）]** > **[ハイアベイラビリティ（High Availability）]** ページの歯車メニューから [モードの切り替え（Switch Mode）] を選択します。
- アクティブな装置の CLI で、**no failover active** を入力します。

ステップ 3 接続テストを繰り返して、ハイ アベイラビリティ ペア内のその他の装置からも同じ接続を確立できることを確認します。

テストが失敗する場合は、他の装置の同等インターフェイスと同じネットワークにその装置のインターフェイスを接続していることを確認します。

HA ステータスは [ハイアベイラビリティ（High Availability）] ページから確認できます。CLI または装置の CLI コンソールを使用し、**show failover** コマンドを入力して、フェールオーバーステータスを確認することもできます。また、**show interface** コマンドを使用して、失敗した接続テストで使用されたインターフェイスのインターフェイス設定を確認できます。

これらの操作で問題を特定できない場合は、他の手順を実行することができます。ハイ アベイラビリティ（フェールオーバー）のトラブルシューティング （43 ページ）を参照してください。

ステップ 4 完了したら、モードを切り替えて、元々アクティブだった装置をアクティブ ステータスに戻します。

ハイ アベイラビリティの管理

ハイ アベイラビリティ ペアを管理するには、[デバイス概要（Device Summary）] ページの [ハイアベイラビリティ（High Availability）] リンクをクリックします。

[ハイアベイラビリティ（High Availability）] ページには次のものがあります。

- [ロールおよびモードステータス（Role and Mode Status）]：左側のステータスエリアには、デバイスがグループ内のプライマリ デバイスかセカンダリ デバイスかが示されます。モードは、このデバイスがアクティブかスタンバイかや、HA が一時停止されているかデバイスがピア デバイスの参加を待っているかが示されます。また、ピア デバイスのステータ

ス（アクティブ、スタンバイ、一時停止、または障害）も示されます。たとえば、現在ログインしているデバイスがプライマリ デバイスであり、アクティブ デバイスでもある場合、セカンダリ デバイスが正常で、必要に応じてフェールオーバーできる状態であれば、ステータスは次のように表示されます。ピアの間のアイコンをクリックすると、デバイス間の設定同期ステータスに関する情報を取得できます。

- [フェールオーバー履歴（Failover History）] リンク：このリンクをクリックすると、ペアに含まれるデバイスのステータスの詳細な履歴を確認できます。CLI コンソールが開き、**show failover history details** コマンドが実行されます。
- [展開履歴（Deployment History）] リンク：このリンクをクリックすると、イベントがフィルタリングされて展開ジョブだけが表示された監査ログに移動します。
- 歯車ボタン：このボタンをクリックすると、デバイス上でアクションが実行されます。
  - [HAの一時停止（Suspend HA）]/[HAの再開（Resume HA）]：HA を一時停止すると、HA 設定を削除しなくても、デバイスがハイ アベイラビリティ ペアとして機能しなくなります。その後、デバイスで HA を再開（つまり再有効化）することができます。詳細は、ハイ アベイラビリティの中断または再開 （31 ページ）を参照してください。
  - [HAの解除（Break HA）]：HA を解除すると、両方のデバイスからハイ アベイラビリティ設定が削除され、それらがスタンドアロン デバイスに戻ります。詳細は、ハイ アベイラビリティの破棄 （32 ページ）を参照してください。
  - [モードの切り替え（Switch Mode）]：モードを切り替えることにより、アクションを実行するデバイスに応じて、強制的にアクティブデバイスをスタンバイにしたりスタンバイ デバイスをアクティブにすることができます。詳細は、アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー） （33 ページ）を参照してください。
- [ハイアベイラビリティ設定（High Availability Configuration）]：このパネルには、フェールオーバー ペアの設定が表示されます。[クリップボードにコピー（Copy to Clipboard）] ボタンをクリックすると情報をクリップボードにロードできます。そこから、セカンダリ デバイスの設定に貼り付けることができます。情報を記録するために別のファイルにコピーすることもできます。この情報には、IPsec 暗号キーを定義したかどうかは示されません。

（注） HA のインターフェイス設定は、インターフェイスのページ（**[デバイス（Device）]>[インターフェイス（Interfaces）]**）に反映されません。HA 設定で使用しているインターフェイスは編集できません。

- [フェールオーバー基準（Failover Criteria）]：このパネルには、「アクティブ装置に障害が発生したためにスタンバイ装置がアクティブ装置になる必要がある」かどうかを評価する際に使用される健全性の基準を決定する設定が含まれます。これらの基準を調整して、ネットワークで必要なフェールオーバーパフォーマンスを実現してください。詳細は、ヘルス モニタリングのフェールオーバー基準の設定 （21 ページ）を参照してください。

ここでは、ハイ アベイラビリティ設定に関連するさまざまな管理タスクについて説明します。

ハイ アベイラビリティの中断または再開

ハイ アベイラビリティ ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。
- スタンバイデバイスのソフトウェアアップグレードをインストール中のフェールオーバーを防ぎたい場合。

ハイ アベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイ アベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムで HA を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバー ペアとして再び機能します。

アクティブ装置からハイ アベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピアユニットとアクティブ/スタンバイ ステータスをネゴシエートします。

（注） 必要に応じて、**configure high-availability suspend** コマンドを入力して、CLI から HA を中断できます。HA を再開するには、**configure high-availability resume** と入力します。

始める前に

Firepower Device Manager を使用してハイ アベイラビリティを中断した場合、装置をリロードした場合でも、再開するまで中断のままになります。ただし、CLI を使用して中断した場合は

一時的な状態なので、リロード時に装置のハイ アベイラビリティの設定が自動的に再開され、ピアとアクティブ/スタンバイ状態がネゴシエートされます。

スタンバイ装置のハイ アベイラビリティを中断する場合は、展開ジョブがアクティブな装置で実行中かどうかを確認してください。展開ジョブの進行中にモードを切り替えると、ジョブが失敗し、設定の変更は失われます。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

ステップ 3 歯車アイコン（⚙）から適切なコマンドを選択します。

- [HAの中断（Suspend HA）]：アクションの確認を求められます。メッセージを読んで、[OK] をクリックします。HA ステータスにデバイスが中断モードであることが表示されます。
- [HAの再開（Resume HA）]：アクションの確認を求められます。メッセージを読んで、[OK] をクリックします。HA ステータスは、装置がピアとネゴシエートした後に正常（アクティブまたはスタンバイ）に戻ります。

ハイ アベイラビリティの破棄

2 台のデバイスをハイ アベイラビリティ ペアとして稼働させない場合は、HA 設定を破棄できます。HA を破棄すると、各デバイスはスタンドアロン デバイスになります。これらの設定は、次のように変更されます。

- アクティブ デバイスは破棄される前と変わらずすべての設定を維持し、HA 設定が削除されます。
- スタンバイ デバイスではHA設定だけでなくすべてのインターフェイス設定が削除されます。すべての物理インターフェイスは無効になりますが、サブインターフェイスは無効になりません。管理インターフェイスはアクティブなままであるため、デバイスにログインして再設定することができます。

破棄が装置にどのように影響するのかは、破棄を実行するときの各装置の状態によって変わります。

- 装置が健全なアクティブ/スタンバイ状態である場合、アクティブ装置から HA を破棄します。これにより、HA ペアの両方のデバイスから HA 設定が削除されます。スタンバイ装置でのみ HA を破棄する場合は、スタンバイ装置にログインして HA を中断した後に HA を破棄できます。

- スタンバイ装置が中断状態または障害状態になっている場合、アクティブ装置からHAを破棄するとアクティブ装置からのみHA設定が削除されます。スタンバイ装置にログインして、スタンバイ装置のHAも破棄する必要があります。
- ピアがHAをネゴシエーションしていたり設定を同期している場合、HAを破棄することはできません。ネゴシエーションまたは同期が完了するか、タイムアウトになるまで待ちます。システムがこの状態でスタックしていると思われる場合は、HAを中断してからHAを破棄することができます。

（注） Firepower Device Managerを使用する場合、**configure high-availability disable** コマンドを使用してCLIからHAを破棄することはできません。

始める前に

理想的な結果を得るために、デバイスを健全なアクティブ/スタンバイ状態にして、アクティブ デバイスからこの操作を実行します。

手順

ステップ1 [デバイス（Device）] をクリックします。

ステップ2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

ステップ3 歯車アイコン（⚙）から、[HAの破棄（Break HA）] を選択します。

ステップ4 確認メッセージを読み、オプションを選択してインターフェイスを無効にするかどうかを決定し、[OK] をクリックします。

スタンバイ装置からHAを破棄する場合は、インターフェイスを無効にするオプションを選択する必要があります。

システムはすぐに、このデバイスとピアデバイスの両方で変更を展開します（可能な場合）。各デバイスで展開が完了して、各デバイスが依存しなくなるまで数分かかることがあります。

アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー）

機能しているハイ アベイラビリティ ペア（つまり、1つのピアがアクティブで、もう1つがスタンバイ）のアクティブ/スタンバイ モードを切り替えることができます。たとえば、ソフトウェアアップグレードをインストールしている場合は、アクティブな装置をスタンバイに切り替えて、アップグレードがユーザ トラフィックに影響を及ぼさないようにできます。

モードはアクティブまたはスタンバイ装置から切り替えることができますが、ピア装置はその他の装置の観点から機能している必要があります。中断中の装置がある場合、モードを切り替えることはできません（最初に HA を再開する必要があります）。そうしないと、失敗します。

（注） 必要に応じて、CLIからアクティブモードとスタンバイ モードを切り替えることができます。スタンバイ装置から **failover active** コマンドを入力します。アクティブな装置から **no failover active** コマンドを入力します。

始める前に

モードを切り替える前に、アクティブな装置で展開ジョブが進行中でないことを確認します。展開ジョブの完了を待ってから、モードを切り替えます。

アクティブな装置に保留中の展開していない変更がある場合は、モードを切り替える前に展開します。そうしないと、新しいアクティブな装置から展開ジョブを実行した場合に変更内容が失われます。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

ステップ 3 歯車アイコンから（⚙）から、[モードの切り替え（Switch Mode）] を選択します。

ステップ 4 確認メッセージを読んで、[OK] をクリックします。

強制的にフェールオーバーが行われ、アクティブな装置がスタンバイになり、スタンバイ装置が新しいアクティブな装置になります。

フェールオーバー後の未展開の設定変更の保持

ハイ アベイラビリティ ペアの装置の設定を変更する場合は、アクティブ装置で設定を編集します。その後、変更を展開すると、アクティブ装置とスタンバイ装置の両方が新しい設定で更新されます。アクティブ装置がプライマリ デバイスであるかセカンダリ デバイスであるかは関係ありません。

ただし、未展開の変更は装置間で同期されません。未展開の変更は、変更を行った装置でのみ利用できます。

そのため、未展開の変更があるときにフェールオーバーが発生すると、その変更は新しいアクティブ装置で利用できません。ただし、現在のスタンバイになっている装置では、変更が保持されています。

未展開の変更を取得するには、モードを切り替えてフェールオーバーを強制的に実行し、そのもう一方の装置をアクティブステータスに戻す必要があります。新しくアクティブになった装置にログインすると、未展開の変更が利用可能になり、それらを展開できます。[ハイアベイラビリティ（High Availability）] 設定の歯車メニュー（⚙）から [モードの切り替え（Switch Modes）] コマンドを使用します。

次の点に注意してください。

- スタンバイ装置上に未展開の変更があるときにアクティブ装置から変更を展開すると、スタンバイ装置上の未展開の変更が削除されます。そのため、それらを取得できなくなります。
- スタンバイ装置がハイアベイラビリティペアに参加すると、そのスタンバイ装置上の未展開の変更が削除されます。装置がペアに参加または再参加するたびに、設定が同期されます。
- 未展開の変更を持つ装置に致命的な障害が発生し、その装置を置き換えたり再イメージ化する必要があった場合は、未展開の変更が完全に失われます。

ハイ アベイラビリティ モードでのライセンスと登録の変更

ハイ アベイラビリティ ペアの装置は、ライセンスと登録ステータスが同じである必要があります。変更するには、次の手順に従います。

- アクティブ装置でオプションのライセンスを有効または無効にします。その後、設定を展開すると、スタンバイ装置が必要なライセンスを要求（または解放）します。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。
- 装置を個別に登録または登録解除します。正しく機能させるには、両方の装置を評価モードにするか、両方の装置を登録する必要があります。装置を異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態（両方有効または両方無効）である必要があります。装置の登録ステータスに一貫性がない場合は、設定の変更を展開できません。

HA IPsec 暗号キーまたは HA 設定の編集

フェールオーバー基準を変更するには、アクティブ装置にログインし、変更を加えて、それらを展開します。

ただし、フェールオーバー リンクで使用される IPsec 暗号キーを変更したり、フェールオーバーまたはステートフル フェールオーバー リンクのインターフェイスや IP アドレスを変更する必要がある場合は、まず HA 設定を解除する必要があります。その後、新しい暗号キーまたはフェールオーバー/ステートフル フェールオーバー リンク設定を使用してプライマリおよびセカンダリ装置を再設定できます。

障害のある装置の正常な装置としてのマーキング

ハイ アベイラビリティ設定の装置は、定期的なヘルス モニタリングによって、障害が発生した装置としてマーキングされる場合があります。この装置が正常である場合は、ヘルス モニタリング要件を再度満たすと正常なステータスに戻ります。正常なデバイスが、頻繁に、障害が発生したデバイスとしてマーキングされる場合は、ピア タイムアウトの値を増やしたり、重要性の低い特定のインターフェイスのモニタリングを停止したり、インターフェイスのモニタリング タイムアウトを変更することができます。

CLI から **failover reset** コマンドを入力することにより、障害が発生した装置を強制的に正常な装置として表示させることができます。このコマンドは、アクティブ装置から入力することをお勧めします。それにより、スタンバイ装置のステータスがリセットされます。**show failover** コマンドまたは **show failover state** コマンドを使用することにより、装置のフェールオーバー ステータスを表示できます。

障害が発生した装置を障害のない状態に復元しても、その装置は自動的にはアクティブになりません。復元された装置は、（強制または通常の）フェールオーバーによってアクティブになるまではスタンバイ状態のままです。

デバイス ステータスをリセットしても、障害が発生したデバイスとしてマーキングされる原因となった問題は解決されません。問題に対処しなかったり、モニタリング タイムアウトを緩和したりすると、そのデバイスは、障害が発生したデバイスとして再びマーキングされます。

HA デバイスでのソフトウェア アップグレードのインストール

ネットワーク内のトラフィックを中断することなく、ハイ アベイラビリティ ペアのデバイスで実行中のシステム ソフトウェアをアップグレードできます。基本的にはスタンバイ デバイスをアップグレードして、アクティブデバイスでトラフィックの処理を続行できるようにします。アップグレードが完了したら、役割を切り替えて、スタンバイ装置をもう一度アップグレードします。

ハイ アベイラビリティ グループ内の装置で異なるソフトウェア バージョンが実行されている間は、フェールオーバーはできません。通常の状況では、各装置で同じソフトウェア バージョンを実行する必要があります。別バージョンの実行が有効なのは、ソフトウェア アップグレードのインストールの進行中だけです。

この手順はアップグレード プロセスを要約したものです。詳細については、Firepower Threat Defenseソフトウェアのアップグレードを参照してください。

（注） アップグレード中、システムはシステムライブラリの更新中（自動展開を含む）にHAを一時停止します。このプロセスの最後の部分で、システムは SSH 接続が可能になります。そのため、アップグレードの適用後すぐにログインすると、HA が一時停止ステータスとして表示される場合があります。システムがスタンバイ完了状態に戻らず、FDM が使用可能になり自動展開が成功した後もこの問題が解消されない場合、[HA]ページに移動し、HAを手動で再開してください。

始める前に

アップグレード プロセスを開始する前に保留中の変更をアクティブ ノードから展開していることを確認します。デバイスのアップグレード時には、設定を変更したり、1 台のデバイスのアップグレード後かつ他のデバイスのアップグレード前に展開を開始したりしないでください。展開が失敗し、変更内容が失われる可能性があります。

タスク リストを確認し、実行中のタスクがないことを確認します。アップグレードをインストールする前に、データベースの更新など、すべてのタスクが完了するまで待機してください。また、スケジュールされたタスクについても確認します。アップグレード タスクにスケジュール タスクが重複しないようにしてください。

更新を実行する前に、アプリケーション フィルタ、アクセス ルール、または SSL 復号ルールに廃止されているアプリケーションが存在しないことを確認してください。これらのアプリケーションには、アプリケーション名の後に「（廃止）(Deprecated)」が付加されています。これらのオブジェクトに廃止されたアプリケーションを追加することはできませんが、後続の VDB 更新により、以前に有効になっていたアプリケーションが廃止される可能性があります。この場合、アップグレードは失敗し、デバイスは使用不能状態のままになります。

Cisco.com にログインし、アップグレード イメージをダウンロードします。

- 適切なアップグレード ファイル（ファイル タイプが REL.tar）を入手していることを確認します。システム ソフトウェア パッケージまたはブート イメージをダウンロードしないでください。
- アップグレードファイルの名前を変更しないでください。名前が変更されたファイルは無効だと見なされます。
- パッチをダウングレードまたはアンインストールすることはできません。
- アップグレードに必要なベースラインイメージを実行していることを確認します。互換性の情報については、『 *Cisco Firepower Compatibility Guide*』、http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html を参照してください。
- 新しいバージョンの場合は、リリース ノートをお読みください。リリース ノートは http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html をご覧ください。

手順

ステップ 1 スタンバイ装置にログインして、アップグレードをインストールします。

a) [デバイス（Device）] をクリックし、[更新サマリー（Updates summary）] の [設定の表示（View Configuration）] をクリックします。
b) [システムアップグレード（System Upgrade）] グループで、[参照（Browse）] または [別のファイルのアップロード（Upload Another File）] をクリックして、イメージをアップロードします。
c) [インストール（Install）] をクリックして、インストール プロセスを開始します。

インストールが完了するまで待機したら、再度ログインして、システムが正常に機能していることを確認できます。

（注） ハイ アベイラビリティのステータスを確認すると、アプリケーションの同期エラーが表示されることがあります。このエラーは、スタンバイデバイスのソフトウェアをアップグレードしている間に、アクティブデバイスから変更を展開した場合にのみ発生します。

ステップ 2 スタンバイ装置で**[デバイス（Device）]** > **[ハイ アベイラビリティ（High Availability）]** をクリックし、歯車メニュー（⚙）から [モードの切り替え（Switch Mode）] を選択します。

この操作により、強制的にフェールオーバーが行われ、ログインしている装置がアクティブな装置になります。装置のステータスが「アクティブ」に変わるまで待ちます。

続行する前に、必要に応じてネットワークをテストして、デバイスの接続先ネットワークをトラフィックが通過していることを確認できます。

ステップ 3 元々はアクティブな装置だった新しいスタンバイ装置にログインして、アップグレードをインストールします。

このプロセスは前述のプロセスと同じです。ソフトウェアアップグレードは、他の装置からはコピーされないため、アップロードする必要があります。

インストールが完了したら、スタンバイ装置に再度ログインして、インストールが成功したこと、装置が通常のアクティブ/スタンバイ状態に戻っていることを確認します。装置のアクティブ ステータスは自動的には再開しません。

（注） ハイアベイラビリティのステータスを確認すれば、アプリケーションの同期エラーが発生することはありません。各装置で同じソフトウェアバージョンが実行されているため、アクティブな装置からの設定のインポートが成功します。自動展開に失敗した場合、またはデバイスがスタンバイ完了状態に移行しない場合は、歯車メニューから [HA の再開（Resume HA）] をクリックします。

ステップ 4 現在アクティブな装置にログインします。保留中の変更がある場合は、それらの変更を展開し、展開が正常に完了するまで待ちます。

ステップ 5 （オプション）現在のスタンバイ装置のアクティブ ステータスを再開させる場合は、**[デバイス（Device）]** > **[ハイ アベイラビリティ（High Availability）]** をクリックして、いずれかの装置の歯車メニューから [モードの切り替え（Switch Mode）] を選択します。

たとえば、このプロセスの開始時点ではプライマリ装置がアクティブな装置であり、その状態にする場合はモードを切り替えます。

HA デバイスをアップグレードする際の変更の展開

ハイ アベイラビリティ グループ内のデバイスのシステム ソフトウェアをアップグレードするプロセスの間は、ある時点において、スタンバイ デバイスでアクティブ デバイスより新しい

ソフトウェアバージョンが実行されています。通常は、この時点でモードを切り替え、スタンバイ デバイスをアクティブ デバイスにしてから、2番目のデバイスをアップグレードします。

ただし、こうしたアップグレード途中の状態でアクティブデバイスの設定を変更する必要が生じた場合は、次の手順を実行して変更を展開できるようにする必要があります。

手順

ステップ 1 スタンバイ デバイス（新しいソフトウェア バージョンを実行しているデバイス）で、[ハイアベイラビリティ（High Availability）] ページの歯車メニュー（⚙）から [HAの中断（Suspend HA）] を選択します。

ステップ 2 アクティブ デバイスで、変更を展開します。展開が正常に完了するまで待機します。

ステップ 3 中断したスタンバイ デバイスで、[ハイアベイラビリティ（High Availability）]ページの歯車メニュー（⚙）から [HAの再開（Resume HA）] を選択します。デバイスがアクティブ デバイスから自身の設定を同期し、最新の変更を取得します。

ステップ 4 再開したスタンバイ デバイスで、[ハイアベイラビリティ（High Availability）]ページの歯車メニュー（⚙）から [スイッチモード（Switch Mode）] を選択します。これで、スタンバイ デバイスがアクティブデバイスになり、アップグレードを進めることができます。HA デバイスでのソフトウェア アップグレードのインストール （36 ページ）を参照してください。

ハイ アベイラビリティ ペアでの装置交換

必要に応じて、ネットワーク トラフィックを中断することなくハイ アベイラビリティ グループ内の装置を交換できます。

手順

ステップ 1 交換する装置が機能している場合は、ピア装置にフェールオーバーするようにし、デバイス CLI の **shutdown** コマンドを使用して、デバイスをグレースフル シャットダウンします。装置が機能していない場合は、ピアがアクティブ モードで動作していることを確認します。

管理者権限を持っている場合は、FDM CLI コンソールから **shutdown** コマンドを入力することもできます。

ステップ 2 装置をネットワークから取り除きます。

ステップ 3 交換装置を設置して、インターフェイスを再接続します。

ステップ 4 交換装置でデバイス セットアップ ウィザードを完了します。

ステップ 5 ピア装置で[ハイアベイラビリティ（High Availability）]ページにアクセスし、設定をクリップボードにコピーします。装置がプライマリ装置か、セカンダリ装置かに注意してください。

保留中の変更がある場合は、それらの変更を展開し、展開が完了するまで待ってから続行します。

ステップ 6 交換装置で [ハイアベイラビリティ（High Availability）] グループで [設定（Configure）] をクリックして、ピアから反対側の装置タイプを選択します。つまり、ピアがプライマリの場合は [セカンダリ（Secondary）] を選択し、ピアがセカンダリの場合は [プライマリ（Primary）] を選択します。

ステップ 7 ピアから HA の設定を貼り付け、IPsec キーを入力します（使用する場合）。[HAの有効化（Activate HA）] をクリックします。

展開が完了すると、装置はピアに連絡して HA グループに参加します。アクティブなピアの設定がインポートされ、選択内容に基づいて、交換装置がグループ内のプライマリ装置またはセカンダリ装置になります。これで、HA が正常に動作していることを確認し、必要に応じてモードを切り替えて、新しい装置をアクティブな装置にできます。

ハイ アベイラビリティのモニタ

ここでは、ハイ アベイラビリティをモニタする方法について説明します。

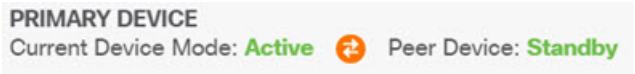
イベント ビューアとダッシュボードには、ログインしているデバイスに関するデータだけが表示されることに注意してください。両方のデバイスの統合された情報は表示されません。

フェールオーバーの全般的なステータスと履歴のモニタリング

次の方法で、ハイ アベイラビリティの全般的なステータスと履歴をモニタできます。

- [デバイス概要（Device Summary）]（[デバイス（Device）] をクリック）の [ハイアベイラビリティ（High Availability）] グループに装置のステータスが表示されます。

- [ハイアベイラビリティ（High Availability）] ページ（**[デバイス（Device）]** > **[ハイアベイラビリティ（High Availability）]** をクリック）に両方の装置のステータスが表示されます。それらの間にある同期のアイコンをクリックすると、追加のステータスが表示されます。



- [ハイアベイラビリティ（High Availability）] ページで、ステータスの横にある [フェールオーバー履歴（Failover History）] リンクをクリックします。CLI コンソールが開き、**show failover history details** コマンドが実行されます。このコマンドを CLI または CLI コンソールに直接入力することもできます。

CLI コマンド

CLI または CLI コンソールで次のコマンドを使用できます。

- **show failover**

  装置のフェールオーバー状態についての情報を表示します。

- **show failover history** ［**details**］

  過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。**details** キーワードを追加すると、ピア装置のフェールオーバー履歴が表示されます。この情報は、トラブルシューティングに役立ちます。

- **show failover state**

  両方の装置のフェールオーバー状態が表示されます。この情報には、装置のプライマリまたはセカンダリ ステータス、装置のアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などが含まれます。

- **show failover statistics**

  フェールオーバー インターフェイスの送信（tx）パケット数と受信（rx）パケット数が表示されます。たとえば、装置がパケットを送信しているのに受信パケットがないことが出力に示されている場合は、リンクに問題があります。ケーブルに問題がある、ピアで正しくない IP アドレスが設定されている、装置によってフェールオーバー インターフェイスが異なるサブネットに接続されているといった可能性があります。

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

  フェールオーバーおよびステートフル フェールオーバー リンクの設定が表示されます。次に例を示します。

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  ハイ アベイラビリティに関してモニタされているインターフェイスに関する情報が表示されます。詳細は、HAモニタ対象インターフェイスのステータスのモニタリング（42ページ）を参照してください。

- **show running-config failover**

実行コンフィギュレーション内のフェールオーバー コマンドを表示します。これらは、ハイ アベイラビリティを設定するコマンドです。

HA モニタ対象インターフェイスのステータスのモニタリング

いずれかのインターフェイスの HA モニタリングを有効にしている場合は、CLI または CLI コンソールで **show monitor-interface** コマンドを使用して、モニタ対象インターフェイスのステータスを確認できます。

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

モニタ対象のインターフェイスには、次のステータスがあります。

- (Waiting)（Unknown (Waiting) などのように他のステータスと結合）：インターフェイスはピア装置上の対応するインターフェイスから hello パケットをまだ受信していません。
- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理上ダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

HA 関連の Syslog メッセージのモニタリング

システムは、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の Syslog メッセージを発行します。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。Syslogメッセージの説明については、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html にある『*Cisco Firepower Threat Defense Syslog Messages*』を参照してください。

（注） フェールオーバー時には、システムが論理的にシャットダウンされた後にインターフェイスが起動し、Syslog メッセージ 411001 および 411002 が生成されます。これは通常のアクティビティです。

Syslog メッセージを表示するには、**[デバイス（Device）]** > **[ロギング設定（Logging Settings）]** で診断ロギングを設定する必要があります。メッセージを確実にモニタできるように、外部 Syslog サーバを設定してください。

ピア装置での CLI コマンドのリモート実行

CLI から failover exec コマンドを使用することにより、ピアにログインすることなく、ピア デバイスに show コマンドを入力できます。

failover exec {**active** | **standby** | **mate**} コマンド

コマンドを実行する装置（active または standby のどちらか）を指定するか、「ログインしている装置ではない方の装置が応答する」ことを指定する **mate** を入力します。

たとえば、ピアのインターフェイス設定と統計情報を表示するには、次のように入力します。

```
> failover exec mate show interface
```

configure コマンドを入力することはできません。この機能は **show** コマンドと一緒に使用します。

（注） アクティブ装置にログインしている場合は、**failover reload-standby** コマンドを使用してスタンバイ装置をリロードできます。

これらのコマンドは、Firepower Device Manager CLI コンソールからは入力できません。

ハイアベイラビリティ（フェールオーバー）のトラブルシューティング

ハイ アベイラビリティ グループ内の装置が期待どおりに機能していない場合は、次の手順による設定のトラブルシューティングを検討します。

アクティブな装置にピア装置が「障害（Failed）」と表示されている場合は、装置の障害状態のトラブルシューティング （46 ページ）を参照してください。

手順

ステップ 1 各デバイス（プライマリとセカンダリ）から次の手順を実行します。

- フェールオーバー リンクのその他のデバイスの IP アドレスに ping を実行します。
- 別のリンクを使用する場合は、ステートフル フェールオーバー リンクのその他のデバイスの IP アドレスに ping を実行します。

ping が失敗する場合は、各デバイス上のインターフェイスが同じネットワーク セグメントに接続されていることを確認します。直接ケーブル接続を使用している場合は、ケーブルを確認します。

ステップ 2 次の一般的なチェックを行います。

- プライマリとセカンダリで重複している管理 IP アドレスを確認します。
- 装置の重複しているフェールオーバー IP アドレスとステートフル フェールオーバー IP アドレスを確認します。
- 各デバイスの同等のインターフェイス ポートが同じネットワーク セグメントに接続されていることを確認します。

ステップ 3 スタンバイ デバイスのタスク リストまたは監査ログを確認します。アクティブなデバイスで展開が成功するごとに、「アクティブ ノードからの設定のインポート（Configuration import from Active node）」タスクの成功を確認できる必要があります。タスクが失敗する場合は、フェールオーバー リンクを確認して、展開を再度実行してください。

（注） 展開タスクの失敗がタスク リストに示されている場合は、展開ジョブ中にフェールオーバーが発生した可能性があります。展開タスクを開始した時点でスタンバイデバイスがアクティブユニットだったものの、タスク中にフェールオーバーが発生した場合には、展開は失敗します。この問題を解決するには、モードを切り替えて再度スタンバイユニットをアクティブユニットに設定してから、設定の変更を再展開します。

ステップ 4 **show failover history** コマンドを使用して、デバイスの状態変更に関する詳細情報を取得します。

以下の点を確認します。

- アプリケーションの同期エラー。

```
12:41:24 UTC Dec 6 2017

App Sync     Disabled     HA state progression failed due to APP SYNC timeout
```

アプリケーションの同期フェーズは、アクティブ デバイスの設定がスタンバイ デバイスに転送されるフェーズです。アプリケーションの同期エラーが発生するとデバイスは無効状態になり、そのデバイスをアクティブにすることはできなくなります。

アプリケーションの同期の問題により、デバイスが無効状態になっている場合は、フェールオーバー リンクとステートフル フェールオーバー リンクのエンドポイント用に、デバイスの別のインターフェイスを使用することができます。リンクの各端には同じポート番号を使用する必要があります。

show failover コマンドの結果、セカンダリ デバイスが疑似スタンバイ状態にあると表示される場合は、セカンダリ デバイスのフェールオーバー リンクに、プライマリ デバイスに設定したアドレスとは異なるIPアドレスを設定している可能性があります。フェールオーバー リンクの両方のデバイスで同じプライマリ/セカンダリ IP アドレスを使用していることを確認します。

疑似スタンバイ状態は、プライマリとセカンダリで異なる IPsec キーが設定されている可能性も示しています。

その他のアプリケーションの同期の問題については、HA アプリケーション同期障害のトラブルシューティング （47 ページ）を参照してください。

- （アクティブからスタンバイに移行して戻る）フェールオーバーの頻度が異常に高い場合、フェールオーバー リンクに問題がある可能性があります。最悪のシナリオでは、両方の装置がアクティブになり、トラフィックの通過が中断されます。リンクの各端に ping を実行して接続を確認します。**show arp** を使用して、フェールオーバー IP アドレスと ARP マッピングが適切であるか確認することもできます。

  フェールオーバー リンクが正常で正しく設定されている場合は、ピアのポーリング時間とホールド時間、インターフェイスのポーリング時間とホールド時間を増やし、HA の監視対象インターフェイスの数を減らし、インターフェイスのしきい値を増やすことを検討してください。

- インターフェイスチェックが原因のエラー。[インターフェイスチェック（Interface Check）] 理由には、障害が発生したと見なされるインターフェイスの一覧が含まれています。それらのインターフェイスをチェックして、正しく設定されていること、ハードウェアの問題がないことを確認します。リンクの反対側のスイッチの設定に問題がないことを確認します。問題がない場合は、それらのインターフェイスに対する HA モニタリングの無効化を検討します。または、インターフェイス障害のしきい値やタイミングを増やすこともできます。

```
06:17:51 UTC Jan 15 2017

Active     Failed     Interface check

                          This Host:3

                             admin: inside

                             ctx-1: ctx1-1

                             ctx-2: ctx2-1

                          Other Host:0
```

ステップ 5 スタンバイ装置を検出できず、フェールオーバー リンクの LAN またはケーブル接続の不良など、具体的な理由を見つけられない場合は、次の手順を実行します。

a) スタンバイ装置で CLI にログインし、**failover reset** コマンドを入力します。このコマンドにより、装置の状態が「障害」から「非障害」に変わります。次に、アクティブデバイスの HA ステータスを確認します。スタンバイ ピアが検出される場合は、これで終了です。

b) アクティブな装置で CLI にログインし、**failover reset** コマンドを入力します。アクティブとスタンバイの両方の装置で HA ステータスがリセットされます。デバイス間のリンクが再確立されるのが理想的です。HA のステータスを確認します。正しくない場合は手順を続行します。

c) アクティブ デバイスの CLI から、または Firepower Device Manager から、まず HA を中断してから HA を再開します。CLI コマンドは **configure high-availability suspend** と **configure high-availability resume** です。

d) これらの手順が失敗する場合は、スタンバイ デバイスを **reboot** します。

装置の障害状態のトラブルシューティング

ピア装置のハイ アベイラビリティ ステータス（[デバイス（Device）] または **[デバイス（Device）] > [ハイアベイラビリティ（High Availability）]** ページ）で装置が故障としてマークされている場合、アクティブ装置である装置 A と故障したピアである装置 B に基づいて、考えられる一般的な原因は次のとおりです

- 装置 B がハイ アベイラビリティ向けに設定されていない場合（スタンドアロン モードのままになっている場合）、装置 A は装置 B を故障として表示します。
- 装置 B で HA を一時停止すると、装置 A は装置 B を故障として表示します。
- 装置 B をリブートすると、装置 B がリブートを完了してフェールオーバー リンク経由で通信を再開するまで装置 A は装置 B を故障として表示します。
- 装置 B でアプリケーションの同期（App Sync）が失敗すると、装置 A は装置 B を故障として表示します。HA アプリケーション同期障害のトラブルシューティング （47ページ）を参照してください。
- 装置 B で装置またはインターフェイスのヘルス モニタリングが失敗すると、装置 A は装置 B を故障として表示します。システム上の問題がないか装置 B を確認します。デバイスをリブートしてみます。装置がおおむね正常な場合は、装置またはインターフェイスのヘルス モニタリング設定を緩和することを検討します。**show failover history** の出力にインターフェイス ヘルス チェックの障害に関する情報が示されます。
- 両方の装置がアクティブな場合、各装置はピアを故障として表示します。通常、これはフェールオーバー リンクに問題があることを示しています。

  ライセンスの問題を示す場合もあります。デバイスには、両方評価モードである、または両方登録済みの一貫性のあるライセンスが必要です。登録されている場合、使用するスマート ライセンス アカウントは別々であっても構いませんが、どちらのアカウントも輸出制限対象の機能で有効または無効のいずれか同じものを選択している必要があります。

輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワーク セグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置でHAを手動で中断する必要があります。

HA アプリケーション同期障害のトラブルシューティング

ピア装置がHAグループへの参加に失敗する場合、またはアクティブ装置からの変更を展開しているときにピア装置で障害が発生する場合は、障害が発生した装置にログインして [ハイアベイラビリティ（High Availability）] ページに移動し、[フェールオーバー履歴（Failover History）] リンクをクリックします。**show failover history** 出力にアプリケーション同期の障害が示されている場合、装置がハイ アベイラビリティ グループとして正しく機能できることをシステムが確認する、HA の検証段階に問題があります。

このタイプの障害は、次のように表示されます。

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
App Sync                  Disabled                  CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

理想としては、From State が App Sync のときに「All validation passed」というメッセージが表示され、ノードが Standby Ready 状態になります。任意の検証で障害が発生すると、ピアは Disabled（Failed）状態になります。問題を解決して、ピアがハイ アベイラビリティ グループとして再度機能するようにする必要があります。アクティブ装置に変更を加えてアプリケーションの同期エラーを修正した場合は、ピア ノードを結合するために、それらを展開してHAを再開する必要があります。

次のメッセージは障害の発生を示しており、問題の解決方法について説明しています。これらのエラーは、ノードの結合と以降の各展開で発生する可能性があります。ノードの結合中は、システムにより、アクティブ装置で最後に展開された設定に対してチェックが実行されます。

- 「ライセンス登録モードがプライマリ ノードとセカンダリ ノードで一致していません。（License registration mode mismatch between Primary and Secondary Node.）」

  ライセンス エラーは、1 つのピアが評価モードになっているときにもう一方のピアが登録されたことを示します。ピアをHAグループに参加させるには、ピアを両方とも登録する

か、両方とも評価モードにする必要があります。登録したデバイスを評価モードに戻すことはできないため、**[デバイス（Device）] > [スマートライセンス（Smart License）]** ページからもう一方のピアを登録する必要があります。

登録するデバイスがアクティブ装置の場合、デバイスの登録後に展開を実行します。展開することで装置は強制的に更新され、設定が同期されます。これにより、セカンダリ装置はハイ アベイラビリティ グループに正しく参加できます。

- 「ライセンス エクスポート コンプライアンスがプライマリ ノードとセカンダリ ノードで一致していません。（License export compliance mismatch between Primary and Secondary Node.）」

  ライセンス コンプライアンス エラーは、デバイスが異なる Cisco Smart Software Manager アカウントに登録されており、1 つのアカウントでは輸出規制された機能が有効で、もう一方のアカウントでは無効になっていることを示します。デバイスは、輸出規制された機能の設定（有効または無効）が同じアカウントに登録される必要があります。**[デバイス（Device）] > [スマートライセンス（Smart License）]** ページでデバイス登録を変更します。

- 「ソフトウェア バージョンがプライマリ ノードとセカンダリ ノードで一致していません。（Software version mismatch between Primary and Secondary Node.）」

  ソフトウェア不一致エラーは、ピアが異なるバージョンの Firepower Threat Defense ソフトウェアを実行していることを示します。一度に 1 台のデバイスにソフトウェア アップグレードをインストールしている場合、システムは一時的にのみ不一致を許容します。ただし、ピアのアップグレードの間に設定変更を展開することはできません。この問題を解決するには、ピアをアップグレードしてから展開をやり直します。

- 「物理インターフェイスの数がプライマリ ノードとセカンダリ ノードで一致していません。（Physical interfaces count mismatch between Primary and Secondary Node.）」

  HA グループ内の装置の物理インターフェイスは、同じ数および同じタイプである必要があります。このエラーは、装置上に異なるインターフェイス セットがあることを示しています。別のピア装置を選択するか、インターフェイス モジュールがないピアに欠落しているインターフェイス モジュールをインストールする必要があります。

- 「フェールオーバー リンク インターフェイスがプライマリ ノードとセカンダリ ノードで一致していません。（Failover link interface mismatch between Primary and Secondary Node.）」

  各装置でフェールオーバー物理インターフェイスをネットワークにリンクする場合、同じ物理インターフェイスを選択する必要があります。たとえば、各装置で GigabitEthernet1/8 にします。このエラーは、異なるインターフェイスを使用したことを示しています。エラーを解決するには、ピア装置のケーブル配線を修正します。

- 「ステートフル フェールオーバー リンク インターフェイスが、プライマリ ノードとセカンダリ ノードで一致していません。（Stateful failover link interface mismatch between Primary and Secondary Node.）」

  別々のステートフル フェールオーバー リンクを使用する場合、各装置でステートフル フェールオーバー インターフェイスをネットワークにリンクするときに、同じ物理インターフェイスを選択する必要があります。たとえば、各装置で GigabitEthernet1/7 にしま

す。このエラーは、異なるインターフェイスを使用したことを示しています。エラーを解決するには、ピア装置のケーブル配線を修正します。

- 「デバイスのモデル番号がプライマリ ノードとセカンダリ ノードで一致していません。（Device Model Number mismatch between Primary and Secondary Node.）」

  HA グループに参加するピアは、まったく同じモデルのデバイスである必要があります。このエラーは、ピアが同じデバイスモデルではないことを示しています。異なるピアを選択して HA を設定する必要があります。

- 「不明なエラーが発生しました。もう一度お試しください。（Unknown error occurred, please try again.）」

  アプリケーションの同期中に問題が発生しましたが、システムが問題を特定できませんでした。もう一度設定を展開してみてください。

- 「ルール パッケージが破損しています。ルール パッケージを更新して、もう一度試してください。（Rule package is corrupted. Please update the rule package and try again.）」

  侵入ルールデータベースに問題があります。障害が発生したピアで、**[デバイス（Device）]**>**[更新（Updates）]** に移動して、[ルール（Rule）] グループの [今すぐ更新（Update Now）] をクリックします。更新が完了するのを待って、変更を展開します。アクティブ装置から展開を再試行できます。

- 「Cisco Success Network はアクティブで有効ですが、スタンバイでは有効になりません。（Cisco Success Network is enabled on Active but not Standby.）」

  評価モードのデバイス向けに HA を設定する場合、ピア装置の Cisco Success Network 参加について同じオプションを選択する必要があります。このエラーを解決するには、**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** に移動して、[Cisco Success Network] を有効にします。

- 「Cisco Defense Orchestrator はアクティブで有効ですが、スタンバイでは有効になりません。（Cisco Defense Orchestrator is enabled on Active but not Standby.）」

  評価モードのデバイス向けに HA を設定する場合、ピア装置の Cisco Defense Orchestrator について同じオプションを選択する必要があります。両方とも登録するか、両方とも登録しない必要があります。このエラーを解決するには、**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** に移動して、[Cisco Defense Orchestrator] グループのデバイスを登録します。

- 「Cisco Threat Response が、アクティブでは有効ですが、スタンバイでは有効になっていません。（Cisco Threat Response is enabled on Active but not Standby.）」

  HA を設定する場合は、ピア ユニットで同じ Cisco Threat Response のオプションを選択する必要があります。このエラーを解決するには、**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** に移動して、[Cisco Threat Response] の [Cisco Cloudにイベントを送信（Send Events to the Cisco Cloud）] を有効にします。

- これはシステム エラーです。展開をもう一度試して、この問題を解決する必要があります。