Firepower Threat Defense でのクラスタの展開

初版：2017 年 05 月 01 日

最終更新：2017 年 05 月 01 日

Firepower Threat Defense でのクラスタの展開

クラスタリングを利用すると、複数の Firepower Threat Defense ユニットを 1 つの論理デバイスにグループ化できます。クラスタリングは、Firepower 9300 および Firepower 4100 series 上の Firepower Threat Defense デバイスでのみサポートされています。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） 一部の機能は、クラスタリングを使用する場合、サポートされません。クラスタリングでサポートされない機能, （12 ページ）を参照してください。

Firepower 4100/9300 Chassisでのクラスタリングについて

クラスタは、1 つの論理ユニットとして機能する複数のデバイスから構成されます。クラスタを Firepower 4100/9300 chassis に展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトではポート チャネル 48）を作成します。シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信用にこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。
- アプリケーション内のクラスタ ブートストラップ コンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ コンフィギュレーションが Firepower 4100/9300 chassis スーパバイザからプッシュされます。
- スパンド インターフェイスとして、クラスタにデータ インターフェイスを割り当てます。

  シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンド モードではあらゆるタイプのデータ インターフェ

イスが機能します。シャーシ間クラスタリングでは、すべてのデータ インターフェイスでスパンド EtherChannel を使用します。

（注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタ パフォーマンスの概算値は次のようになります。

- TCP または CPS スループット：0.8 X *number_of_units*
- UDP スループット：0.9 X *number_of_units*
- Ethernet MIX（EMIX）スループット：トラフィック ミックスに応じて、0.6 X *number_of_units*

ブートストラップ コンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ コンフィギュレーションが Firepower 4100/9300 chassis スーパバイザからプッシュされます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を実現します。ここでは、各メンバーのロールの特長について説明します。

標準出荷単位とセカンダリ単位の役割

クラスタのメンバの 1 つが標準出荷単位です。標準出荷単位は自動的に決定されます。他のすべてのメンバはセカンダリ単位です。

すべてのコンフィギュレーション作業は標準出荷単位でのみ実行する必要があります。コンフィギュレーションはその後、セカンダリ単位に複製されます。

一部の機能は、クラスタ内でスケーリングしません。そのような機能のトラフィックすべては、プライマリ ユニットが処理します。。クラスタリングの中央集中型機能, （12 ページ） を参照してください。

プライマリ ユニット選定

クラスタのメンバーは、クラスタ制御リンクを介して通信し、次の方法でプライマリ ユニットを選定します。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. 優先順位が高い他のユニットがこの選定要求に応答します。優先順位はクラスタの展開時に設定され、設定の変更はできません。
3. 45秒経過しても、優先順位の高い他のユニットからの応答を受信しない場合、そのユニットがプライマリになります。
4. より高い優先順位が設定されたクラスタが後から参加した場合でも、そのユニットは自動的にはプライマリ ユニットになりません。既存のプライマリ ユニットは、応答を停止しない限り、常にプライマリのままです。応答を停止すると、その時点で新しいプライマリ ユニットが選定されます。

（注） 特定のユニットを手動で強制的にプライマリにすることができます。中央集中型機能については、プライマリ ユニット変更を強制するとすべての接続がドロップされるので、新しいプライマリ ユニット上で接続を再確立する必要があります。

クラスタ制御リンク

クラスタ制御リンクは、ポートチャネル48インターフェイスを使用して自動的に作成されます。シャーシ内クラスタリングでは、このインターフェイスにメンバ インターフェイスはありません。シャーシ間クラスタリングでは、EtherChannel に 1 つ以上のインターフェイスを追加する必要があります。このクラスタ タイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。

2 メンバー シャーシ間クラスタの場合、シャーシと別のシャーシとの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

シャーシ間クラスタリングのクラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、

ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

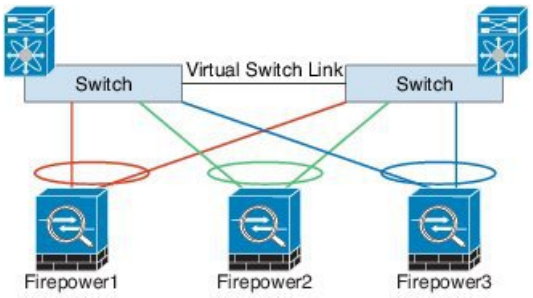
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチング システム（VSS）または仮想ポート チャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の Firepower 4100/9300 chassis インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 chassisは、シャーシ ID とスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。この IP アドレスは、FXOS でもアプリケーション内でも手動で設定することはできません。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンドインターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。この管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。Firepower Management Centerにデバイスを設定し、登録するために使用されます。、独自のローカル認証、IPアドレス、およびスタティック ルーティングを使用します。各クラスタ メンバーは、ブートストラップ コンフィギュレーションの一部としてユーザが設定した管理ネットワークで、それぞれ別個の IP アドレスを使用します。

管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。診断論理インターフェイスはオプションであり、ブートストラップ コンフィギュレーションの一部としては設定されていません。診断インターフェイスは、他のデータ インターフェイスと一緒に設定できます。診断インターフェイスを設定する場合、常に現在のプライマリ ユニットに属するクラスタの固定アドレスとしてメインクラスタIPアドレスを設定します。アドレス範囲も設定して、現在のプライマリユニットを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。メインクラスタIPアドレスを使用することにより、アドレスへの診断アクセスに一貫性を保ことができます。つまり、プライマリ ユニットが変更されると、メイン クラスタ IP アドレスは新しいプライマリ ユニットに移動するので、クラスタへのアクセスをシームレスに継続できます。TFTPやsyslogなどの発信管理トラフィックの場合、標準出荷単位を含む各単位は、ローカル IP アドレスを使用してサーバに接続します。

クラスタ インターフェイス

シャーシ内クラスタリングでは、物理インターフェイスと EtherChannel（ポートチャネルとも呼ばれる）の両方をクラスタに割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロードバランシングを行うスパンドインターフェイスです。

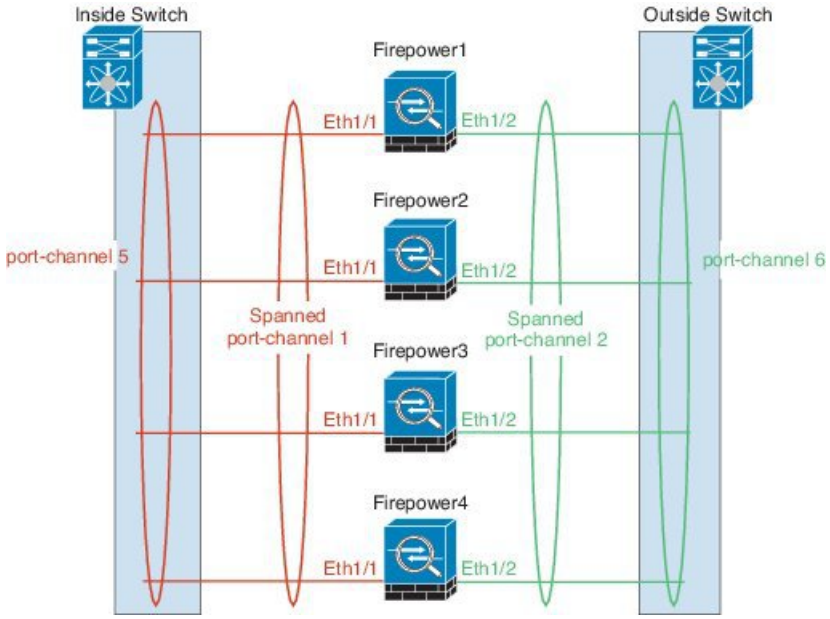
シャーシ間クラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンド EtherChannel は、各シャーシに同じメンバー インターフェイスを含みます。上流に

位置するスイッチでは、これらのインターフェイスがすべて単一の EtherChannel に含まれるため、スイッチは複数のデバイスに接続されていることを認識しません。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジ グループ メンバのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロード バランシング機能を基本的動作の一部として備えています。



VSS または vPC への接続

インターフェイスに冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性をモニタリングし、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを実現します。

シャーシアプリケーションのモニタリング

シャーシアプリケーションのヘルス モニタリングは常に有効になっています。Firepower 4100/9300 chassis スーパバイザは Firepower Threat Defense アプリケーションを定期的に確認します（毎秒）。Firepower Threat Defense device が作動中で Firepower 4100/9300 chassis スーパバイザと 3 秒間通信できない場合、Firepower Threat Defense device は syslog メッセージを生成して、クラスタを離れます。

Firepower 4100/9300 chassis スーパバイザは、45 秒後にアプリケーションと通信できない場合、Firepower Threat Defense device をリロードします。Firepower Threat Defense device は、スーパバイザと通信できない場合、自身をクラスタから削除します。

ユニット ヘルス モニタリング

プライマリ ユニットは、クラスタ制御リンクを介してキープアライブ メッセージを定期的に送信し、各セカンダリ ユニットをモニタします。各セカンダリ ユニットは、同じメカニズムを使用してプライマリ ユニットをモニタします。ユニット ヘルス チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をプライマリ ユニットに報告します。シャーシ間クラスタリングでは、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシは、EtherChannel でポートがアクティブかどうかを判断するためにリンク ステータスと cLACP プロトコル メッセージをモニタします。インターフェイスがダウンしている場合は、Firepower Threat Defense アプリケーションに通知します。ヘルス モニタリングを有効にすると、デフォルトですべての物理インターフェイスがモニタされます（EtherChannel インターフェイスの主要な EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません。

モニタ対象インターフェイスが、ある特定のユニット上では障害が発生し、他のユニットではアクティブな場合、その特定のユニットがクラスタから削除されます。Firepower Threat Defense device がメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。Firepower Threat Defense device は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスをモニタしません。この間にインターフェイスのステータスが変化しても、Firepower Threat Defense device はクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます。

シャーシ間クラスタリングでは、クラスタから EtherChannel を追加または削除した場合、各シャーシに変更を加えられるように、インターフェイス ヘルス モニタリングは 95 秒間中断されます。

デコレータ アプリケーションのモニタリング

インターフェイスに Radware DefensePro アプリケーションなどのデコレータ アプリケーションをインストールした場合、Firepower Threat Defense device とデコレータ アプリケーションがクラス

タ内にとどまるには、その両方が動作している必要があります。両方のアプリケーションが動作状態になるまで、ユニットはクラスタに参加しません。一旦クラスタに参加すると、ユニットはデコレータ アプリケーションが正しく動作しているか3秒ごとにモニタします。デコレータ アプリケーションがダウンすると、ユニットはクラスタから削除されます。

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィック フローのステート情報は、クラスタ制御リンクを介して共有されます。

プライマリ ユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のものがプライマリ ユニットになります。

障害イベントに応じて、Firepower Threat Defense device は自動的にクラスタへの再参加を試みます。

（注） Firepower Threat Defense device が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータ インターフェイスがシャットダウンされます。管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバーがクラスタから削除された後、クラスタに再参加する方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決してから、クラスタリングを再有効化することにより、クラスタを手動で再参加する必要があります。
- データ インターフェイスの障害：Firepower Threat Defense アプリケーションが、5 分後、10 分後、最後に 20 分後に再参加を自動的に試みます。20 分後に参加できない場合、Firepower Threat Defense アプリケーションはクラスタリングを無効化します。データ インターフェイスの問題を解決してから、手動でクラスタリングを有効にする必要があります。
- ユニットの障害：ユニット ヘルス チェックの障害が原因でユニットがクラスタから削除された場合、クラスタへの再参加は障害の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。Firepower Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：Firepower Threat Defense アプリケーションは、シャーシアプリケーションの状態が回復したことを検出すると、自動的にクラスタへの再参加を試みます。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップオーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。

オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップオーナーに問い合わせて、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *1*：クラスタ全体で複製される機能

トラフィック	状態のサポート	注記
アップ タイム	あり	システムアップタイムをトラッキングします。
ARP テーブル	あり	—
MAC アドレス テーブル	あり	—
ユーザ ID	あり	—
IPv6 ネイバー データベース	あり	—
ダイナミック ルーティング	あり	—
SNMP エンジン ID	なし	—
VPN（サイト間）	なし	VPN セッションは、プライマリ ユニットで障害が発生すると切断されます。

コンフィギュレーションの複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはプライマリ ユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

次の 3 種類のロールがあり、各接続に対して定義されます。

- オーナー：最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。最初のオーナーに障害が発生すると、新しいユニットがその接続からパケットを受信したときに、ディレクタがそれらのユニットの中から新しいオーナーを選択します。
- ディレクタ：フォワーダからのオーナールックアップ要求を処理するユニット。また、オーナーが停止した場合はバックアップとなり、接続の状態を保持します。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよび TCP ポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1 つの接続に対してディレクタは 1 つだけです。ディレクタに障害が発生すると、オーナーは新しいディレクタを選択します。
- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化をディセーブルにした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえば DNS や ICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

シャーシ間クラスタリングでは、フローのディレクタがオーナーと同じシャーシにある場合、オーナーのシャーシに障害が発生した場合に備えて、ディレクタのバックアップとして機能する追加のディレクタが別のシャーシで選択されます。他のシャーシにすでにディレクタがある場合、追加のディレクタは不要です。

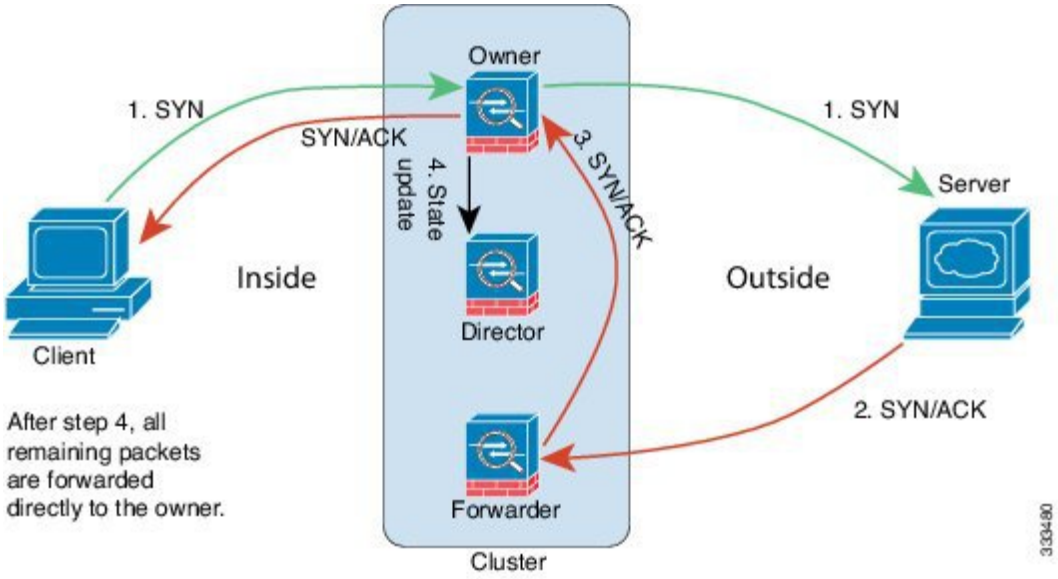
新しい接続の所有権

新しい接続がロード バランシング経由でクラスタのメンバーに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、

そのパケットはクラスタ制御リンクを介してオーナー ユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、Firepower Threat Defense device の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firepower Threat Defense device（ロード バランシング方法に基づく）に配信されます。この Firepower Threat Defense device はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

Firepower Threat Defense の機能とクラスタリング

Firepower Threat Defense には、クラスタリングではサポートされない機能や、プライマリ ユニットだけでサポートされる機能が含まれます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- サイト間 VPN
- DHCP クライアント、サーバ、およびプロキシ。DHCP リレーはサポート対象です。
- 高可用性
- 統合ルーティングおよびブリッジング

クラスタリングの中央集中型機能

次の各機能は、プライマリ ユニット上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバー ユニットからプライマリ ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがプライマリ ユニットに送り返されます。

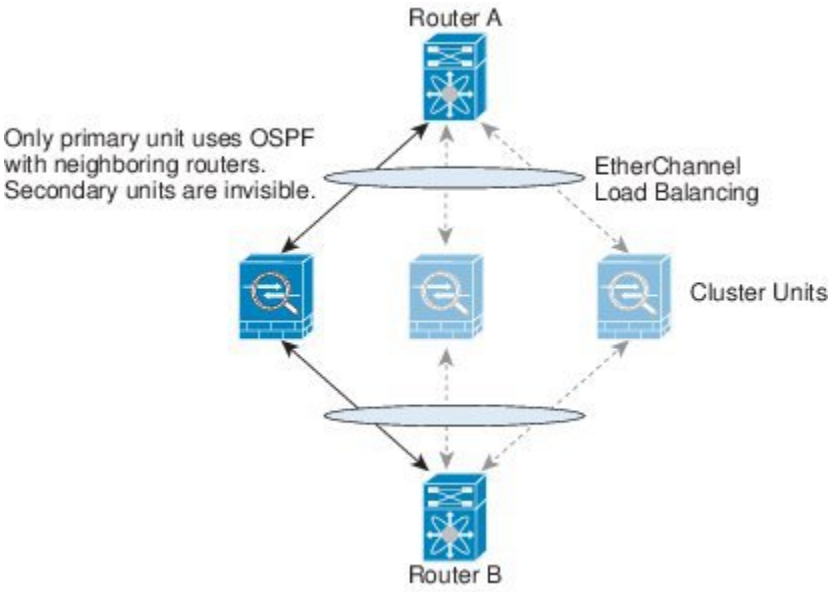
中央集中型機能については、プライマリ ユニットで障害が発生するとすべての接続がドロップされるので、新しいプライマリ ユニット上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング
- スタティック ルート モニタリング

ダイナミック ルーティングとクラスタリング

ルーティング プロセスはプライマリ ユニット上だけで実行されます。ルートはプライマリ ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがセカンダリに到着した場合は、プライマリ ユニットにリダイレクトされます。

図 *1*：ダイナミック ルーティング



セカンダリ メンバがプライマリ ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、プライマリ ユニットからセカンダリ ユニットに同期されません。プライマリ ユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、クラスタ内のそれぞれ別の Firepower Threat Defense device に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。接続のオーナーではない Firepower Threat Defense device に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- ダイナミック PAT 用 NAT プール アドレス分散：プライマリ ユニットは、アドレスをクラスタ全体に均等に分配します。接続を受信したメンバーにアドレスが 1 つも残っていない場合、他のメンバーには使用可能なアドレスがまだ残っていても、接続はドロップされます。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に 1 つのアドレスを受け取るようにするためです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- プライマリ ユニットによって管理されるダイナミック NAT xlate：プライマリ ユニットが xlate テーブルを維持し、セカンダリ ユニットに複製します。ダイナミック NAT を必要とする接続をセカンダリ ユニットが受信したときに、その xlate がテーブル内にない場合は、セカンダリはプライマリ ユニットから xlate を要求します。セカンダリ ユニットが接続を所有します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

SIP インスペクションとクラスタリング

制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データフローは同じユニットに存在する必要があります。

syslog とクラスタリング

- クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタ ブートストラップ コンフィギュレーションで割り当てられたローカル ユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。

SNMP とクラスタリング

SNMP エージェントは、個々の Firepower Threat Defense device を、その診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメイン クラスタ IP アドレスをポーリングする場合は、新しいプライマリが選定されたときに、新しいプライマリ ユニットのポーリングに失敗します。

FTP とクラスタリング

- FTP D チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバーによって所有されている場合は、D チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

Cisco TrustSec とクラスタリング

プライマリ ユニットだけがセキュリティ グループ タグ（SGT）情報を学習します。プライマリ ユニットからこの SGT がセカンダリに渡されるので、セカンダリは、セキュリティ ポリシーに基づいて SGT の一致の決定を行うことができます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。プライマリ ユニットのみが VPN 接続をサポートします。

VPN 機能を使用できるのはプライマリ ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。プライマリ ユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しいプライマリが選定されたら、VPN 接続を再確立する必要があります。

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的にプライマリ ユニットに転送されます。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

クラスタリングの前提条件

シャーシ間のハードウェアとソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower 4100 シリーズ：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシに設置されているセキュリティ モジュールの数はさまざまでかまいません。
- イメージ アップグレード時を除き、同じ FXOS ソフトウェアを実行する必要があります。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュール タイプを使用できます。シャーシ間クラスタリングのすべてのデータ インターフェイスが EtherChannel であることに注意してください。
- 同じ NTP サーバを使用する必要があります。また、Firepower Threat Defense の場合、Firepower Management Center は同じ NTP サーバを使用する必要があります。時間を手動で設定しないでください。

シャーシ間クラスタリングのスイッチの前提条件

- Firepower 4100/9300 chassisでクラスタリングを設定する前に、必ずスイッチの設定を完了し、シャーシからのすべての EtherChannel をスイッチに正常に接続してください。
- サポートされているスイッチのリストについては、「Cisco FXOS Compatibility」を参照してください。

クラスタリングに関するガイドライン

モデル

- Firepower 9300 の Firepower Threat Defense：シャーシ内およびシャーシ間クラスタリングでサポート。
- Firepower 4100 series の Firepower Threat Defense：シャーシ間クラスタリングでサポート。
- Radware DefensePro：Firepower Threat Defense によるシャーシ内クラスタリングでサポート。

シャーシ間クラスタリングのスイッチ

- ASR 9006 でデフォルト以外の MTU を設定する場合は、クラスタ デバイスの MTU よりも 14 バイト大きい ASR インターフェイス MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタ デバイスの MTU と ASR *IPv4* MTU を一致させる必要があることに注意してください。

- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内のデバイスへのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。クラスタ デバイスのロードバランシング アルゴリズムは、デフォルトから変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再起動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id***hash-distributionfixed**

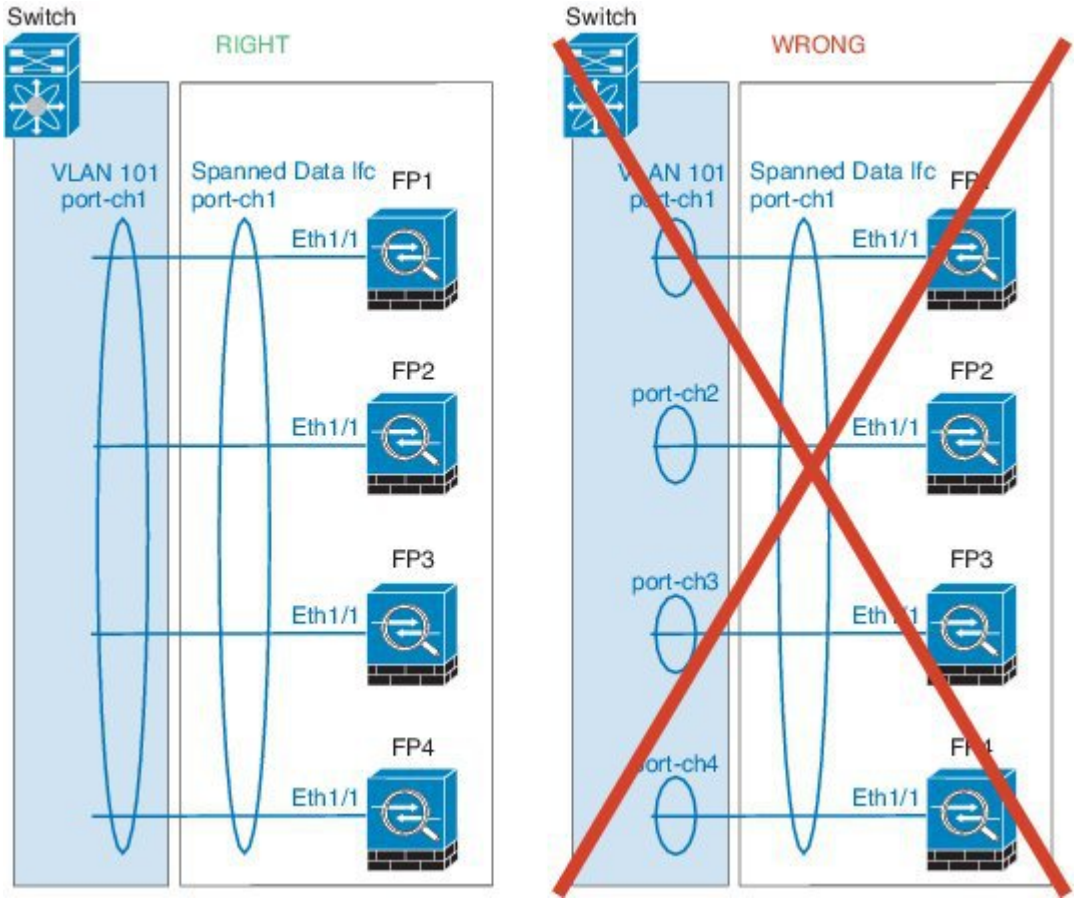
  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

シャーシ間クラスタリングの EtherChannel

- スイッチ接続用に、EtherChannel モードをアクティブに設定します。クラスタ制御リンクであっても、Firepower 4100/9300 chassisではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [標準（normal）] に設定されている LACP レートがあります。この設定ではポート チャネル メンバのバンドルに 30 秒以上かけるように設定できますが、これによりクラスタ ユニット クラスタのヘルスチェックが失敗し、ユニットがクラスタから削除されることがあります。FXOS CLI で LACP レートを [高速（fast）] に変更することを推奨します。次に、「デフォルトの」LACP ポリシーを変更する例を示します。

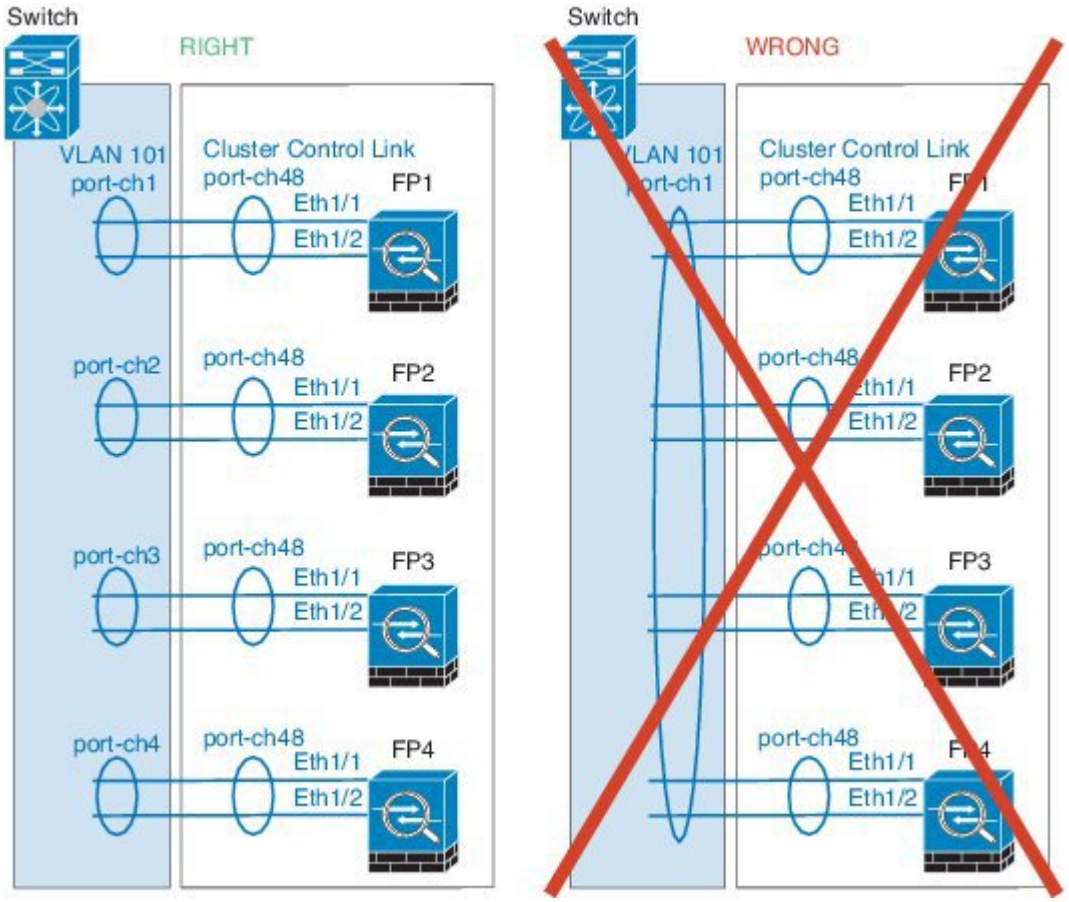
```
firepower# scope org
firepower /org # scope lacppolicy default
firepower /org/lacppolicy# set lacp-rate fast
firepower /org* # commit-buffer
```

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタ ユニット EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



  - デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立

したEtherChannelとしてスイッチ上で設定してください。スイッチ上で複数のクラスタユニットEtherChannelを結合して1つのEtherChannelとしないでください。



その他のガイドライン

- 最大6つのシャーシ内のクラスタに最大6つのモジュールを含めることができます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP接続のFIN/ACKパケットがドロップされると、FTPクライアントがハングします。この場合は、FTP接続を再確立する必要があります。
- スパンドインターフェイスに接続されたWindows 2003サーバを使用している場合、syslogサーバポートがダウンし、サーバがICMPエラーメッセージを制限しないと、大量のICMPメッセージがクラスタに返送されます。このようなメッセージにより、クラスタの一部のユニットでCPU使用率が高くなり、パフォーマンスに影響する可能性があります。ICMPエラーメッセージを調節することを推奨します。
- 冗長性を持たせるため、VSSまたはvPCにEtherChannelを接続することを推奨します。

- シャーシ内では、スタンドアロンモードでクラスタ化できないセキュリティモジュールや、実行できないセキュリティモジュールがあります。空のスロットを含め、クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

Firepower 4100/9300 Chassis のクラスタリングのデフォルト設定

- クラスタのヘルス チェック機能は、デフォルトで有効で、保留時間は 3 秒です。インターフェイス ヘルスモニタリングは、デフォルトで、すべてのインターフェイス上で有効です。
- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5 分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

Firepower 4100/9300 Chassis でのクラスタリング設定

クラスタは、Firepower 4100/9300 chassis スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。その後で、ユニットを Management Center に追加し、クラスタにグループ化できます。

FXOS シャーシ スーパバイザからのクラスタの展開

クラスタは、Firepower 4100/9300 chassis スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。展開を容易にするために、1 つのシャーシにクラスタを展開し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

はじめる前に

- モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。
- [インターフェイス（Interfaces）] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバインターフェイスが含まれていない場合は、[動作状態（Operation State）] を [失敗（failed）] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバ インターフェイスを必要としないため、この動作状態は無視して構いません。

ステップ 1 クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。

また、データ インターフェイスはクラスタを展開した後でも、そのクラスタに追加できます。

シャーシ間クラスタリングでは、全データ インターフェイスは 1 つ以上のメンバ インターフェイスを持つ EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。

ステップ 2 管理タイプのインターフェイスまたは EtherChannel を追加します。
シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

ステップ 3 シャーシ間クラスタリングでは、ポート チャネル 48 にメンバ インターフェイスを追加し、クラスタ制御リンクとして使用します。
メンバ インターフェイスを含めないと、論理デバイスを展開したときに、Firepower Chassis Managerでこのクラスタがシャーシ内クラスタとみなされ、[シャーシID（Chassis ID）] フィールドが表示されません。
各シャーシに同じメンバ インターフェイスを追加します。

ステップ 4 （任意） Firepower-eventing インターフェイスを追加します。
このインターフェイスは、Firepower Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Firepower Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Webイベントなど）から管理トラフィックを分類できます。Firepower Threat Defense コマンド リファレンスの **configure network** コマンドを参照してください。

シャーシ間クラスタリングの場合、各シャーシに同じイベンティング インターフェイスを追加します。

ステップ 5 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。

ステップ 6 [デバイスの追加（Add Device）] をクリックし、[デバイスの追加（Add Device）] ダイアログボックスを表示します。
既存の論理デバイスが存在する場合は、そのデバイスを削除し、新しいクラスタを追加するように求められます。そのデバイス上のすべての設定が新しい情報に置き換えられます。

ステップ 7 [デバイス名（Device Name）] に論理デバイスの名前を入力します。この名前は、Firepower 4100/9300 chassis スーパバイザがクラスタリングまたは管理の設定を行ってインターフェイスを割り当てるために使用します。これは、論理デバイス設定で使用されるクラスタ名ではありません。

ステップ 8 [テンプレート（Template）] には、[Cisco Firepower 脅威に対する防御（Cisco Firepower Threat Defense）] を選択します。

ステップ 9 [イメージ バージョン（Image Version）] では、Firepower Threat Defense ソフトウェア バージョンを選択します。このバージョンが、使用している FXOS のバージョンおよび Firepower Management Center のバージョンと互換性があることを確認します。

ステップ 10 [デバイス モード（Device Mode）] では、[クラスタ（Cluster）] オプション ボタンをクリックします。

ステップ 11 [新しいクラスタの作成（Create a new cluster）] オプション ボタンをクリックします。

ステップ 12 [OK] をクリックします。
スタンドアロン デバイスを設定している場合は、新しいクラスタに置き換えるように求められます。[プロビジョニング - デバイス名（Provisioning - *device name*）] ウィンドウが表示されます。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。Hardware Bypass 対応のポートは次のアイコンで表示されます：  。Hardware Bypass ペアの両方のインターフェイスとも割り当てら

れていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。Hardware Bypass 機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。 ハードウェア バイパス ポートは、EtherChannel のメンバとしてサポートされないため、シャーシ間クラスタリングではサポートされません。

ステップ 13 画面中央のデバイス アイコンをクリックします。
[Cisco Firepower Threat Defense の設定（Cisco Firepower Threat Defense Configuration）] ダイアログボックスが表示されます。

ステップ 14 [クラスタ情報（Cluster Information）] タブで、次の項目を入力します。

a) [シャーシ ID（Chassis ID）] フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。

b) [クラスタ キー（Cluster Key）] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。
共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

c) [クラスタ グループ名（Cluster Group Name）] を設定します。これは、論理デバイス設定のクラスタ グループ名です。
名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

d) [管理インターフェイス（Management Interface）] ドロップダウン リストから、論理デバイスで使用する管理インターフェイスを選択します。
Hardware Bypass 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

ステップ 15 [設定（Settings）] タブで、次の項目を入力します。

a) [登録キー（Registration Key）] フィールドに、登録時に Firepower Management Center とクラスタ メンバー間で共有するキーを入力します。

b) [パスワード（Password）] フィールドに、クラスタの管理者ユーザのパスワードを入力します。

c) [Firepower Management Center の IP（Firepower Management Center IP）] フィールドに、管理側の Firepower Management Center の IP アドレスを入力します。

d) [ドメインの検索（Search Domains）] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。

e) [ファイアウォール モード（Firewall Mode）] ドロップダウン リストから、[トランスペアレント（Transparent）] または [ルーテッド（Routed）] を選択します。

f) [DNS サーバ（DNS Servers）] フィールドに、Firepower Threat Defense デバイスがその管理ネットワーク上で使用する必要がある DNS サーバのカンマ区切りのリストを入力します。

g) [完全修飾ホスト名（Fully Qualified Hostname）] フィールドに、Firepower Threat Defense デバイスの完全修飾名を入力します。

h) [イベンティング インターフェイス（Eventing Interface）] ドロップダウン リストから、Firepower イベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

Firepower イベントに使用する別のインターフェイスを指定するには、*firepower-eventing* インターフェイスとしてインターフェイスを設定する必要があります。Hardware Bypass 対応のインターフェイスを Eventing インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

ステップ 16 [インターフェイス情報（Interface Information）] タブで、クラスタ内の各セキュリティ モジュールの管理 IP アドレスを設定します。[アドレス タイプ（Address Type）] ドロップダウン リストからアドレスのタイプを選択し、セキュリティ モジュールごとに次の手順を実行します。

（注） モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットで IP アドレスを設定する必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

a) [管理 IP（Management IP）] フィールドで、IP アドレスを設定します。
モジュールごとに同じネットワークの IP アドレスを指定します。

b) [ネットワーク マスク（Network Mask）] または [プレフィックス長（Prefix Length）] に入力します。

c) ネットワーク ゲートウェイ アドレスを入力します。

ステップ 17 [利用規約（Agreement）] タブで、エンド ユーザ ライセンス（EULA）を読んで、同意します。

ステップ 18 [OK] をクリックして、[Cisco Firepower Threat Defense の設定（Cisco Firepower Threat Defense Configuration）] ダイアログボックスを閉じます。

ステップ 19 [保存（Save）] をクリックします。
Firepower 4100/9300 chassis スーパバイザは、指定したソフトウェア バージョンをダウンロードし、各セキュリティ モジュールにクラスタ ブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、クラスタを展開します。

ステップ 20 シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

a) 最初のシャーシの Firepower Chassis Manager で、右上の [クラスタ詳細の表示（Show Cluster Details）] アイコンをクリックして、表示されるクラスタ設定をコピーします。

b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。

c) [既存のクラスタへの参加（Join an Existing Cluster）] を選択します。

d) [config のコピー（Copy config）] チェックボックスをクリックして、[OK] をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。

e) [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

f) 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- [クラスタ キー（Cluster Key）]：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理 IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

g）[保存（Save）] をクリックします。

ステップ 21 管理 IP アドレスを使用して各ユニットを個別に Firepower Management Center に追加し、それらを Web インターフェイスでクラスタにグループ化します。
すべてのクラスタ ユニットは、Firepower Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

Add a Cluster to the Management Center

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	N/A	Firepower Threat Defense on the Firepower 4100 and 9300	Any	Access Admin Administrator Network Admin

Add the logical devices to the Management Center, and then group them into a cluster.

はじめる前に

- Refer to the Firepower Chassis Manager Logical Devices screen to see which unit is the primary unit.
- All cluster units must be in a successfully formed cluster on FXOS prior to adding them to the Management Center.

ステップ 1 In the Management Center, choose Devices > Device Management, and choose Add > Add Device to add each unit as a separate managed device using the management IP addresses you assigned when you deployed the cluster.

（注） If you use Management Center High Availability, make sure the standby Management Center also successfully registers each unit before you continue and form the cluster on the active Management Center: Log into the standby Management Center to check the registration status of each unit.

ステップ 2 Choose Add > Add Cluster to group the units into a cluster.

a) Choose the Primary device from the drop-down list.
All other eligible members are added to the Secondary Devices box.

b) Specify a Name for the cluster.

c) Click OK.
The cluster object is added to the Devices screen, with the member units underneath. The current primary unit is indicated by "(primary)" after the unit name.

（注） If you add more units to the cluster later on the FXOS chassis, then you must add each unit to the Management Center, and then add them as secondary nodes of the cluster as soon as possible.

ステップ 3 To configure device-specific settings, click the edit icon ( ) for the cluster; you can only configure the cluster as a whole, and not member units in the cluster.

ステップ 4 On the Devices > Device Management > Cluster tab, you can see General, License, System, and Health settings. This tab is most useful for setting license entitlements. On the Devices tab, you can change the management IP address for the primary unit only.

ステップ 5 （任意） If you want to configure the Diagnostic interface, perform the following steps:
The Diagnostic interface is the only interface that can run in Individual interface mode. You can use this interface for syslog messages or SNMP, for example.

a) Add an IPv4 and/or IPv6 address pool.
b) Click the Interfaces tab to edit the Diagnostic interface.
c) On the IPv4 tab, enter the Virtual IP Address and mask. This IP address is a fixed address for the cluster, and always belongs to the current primary unit.
d) From the IPv4 Address Pool drop-down list, choose the address pool you created.
Include at least as many addresses as there are units in the cluster. The Virtual IP address is not a part of this pool, but needs to be on the same network. You cannot determine the exact Local address assigned to each unit in advance.
e) For the Mask, enter the subnet mask for the cluster IP pool.
f) On the IPv6 > Basic tab, from the IPv6 Address Pool drop-down list, choose the address pool you created.
g) Configure other interface settings as normal.

ステップ 6 Configure other device-level settings as desired.

ステップ 7 Click Save, and then Deploy.

クラスタ メンバーの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
任意	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	アクセス管理者 管理者 ネットワーク管理者

Firepower 9300 デバイスにモジュールを追加する場合や、シャーシを追加する場合などには、既存のクラスタに新しいクラスタ メンバーを追加できます。

はじめる前に

FXOS シャーシのクラスタにさらにユニットを追加する場合、Management Center に各ユニットを追加し、その後すぐにそれらをクラスタのセカンダリ ノードとして追加する必要があります。

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、[追加（Add）] > [デバイスの追加（Add Device）] の順に選択して、新しい論理デバイスを追加します。

ステップ 2 [追加（Add）] > [クラスタの追加（Add Cluster）] の順に選択します。

ステップ 3 ドロップダウンリストから現在の [プライマリ（Primary）] デバイスを選択します。
すでにクラスタに存在するプライマリ デバイスを選択すると、既存のクラスタ名が自動設定され、対象となるすべてのセカンダリ デバイスが [セカンダリ デバイス（Secondary Devices）] ボックスに追加されます。これには、Management Center に追加したばかりの新しいユニットも含まれます。

ステップ 4 [追加（Add）]、[展開（Deploy）] の順にクリックします。
クラスタが更新され、新しいメンバーが追加されます。

セカンダリ メンバーの削除

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
任意	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	アクセス管理者管理者ネットワーク管理者

Firepower 9300 上のモジュールを削除する場合や、シャーシを削除する場合など、クラスタ メンバーを削除する必要がある場合には、Management Center からそのメンバーを削除する必要があります。 Firepower Chassis Manager で、依然としてクラスタの健全な一部として表示されるメンバーは削除しないでください。Management Center から削除しても、そのメンバーはクラスタの動作部分を構成しているため、そのメンバーがプライマリ ユニットになり Management Center で管理できなくなると問題が生じる可能性があります。

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、セカンダリ ユニットの横にあるごみ箱をクリックします。

ステップ 2 ユニットを削除しようとしていることを確認します。
ユニットが、クラスタおよび Management Center のデバイス リストから削除されます。

クラスタへの再参加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン数	アクセス
任意	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意	アクセス管理者 管理者 ネットワーク管理者

障害が発生したインターフェイスなど、ユニットがクラスタから削除された場合、ユニット CLI にアクセスして、クラスタに手動で再参加させる必要があります。クラスタへの再参加を行おうとする前に、障害が解決されていることを確認します。ユニットがクラスタから削除される理由の詳細については、クラスタへの再参加, （8 ページ）を参照してください。

ステップ 1 コンソール ポートか、管理インターフェイスへの SSH を使用して、クラスタに再参加する必要のあるユニットの CLI にアクセスします。ユーザ名 **admin**、および初期セットアップ時に設定したパスワードを使用してログインします。

ステップ 2 クラスタリングを有効にします。
cluster enable

クラスタリングの履歴

機能名	プラットフォームリリース	機能情報
Cisco ASA のシャーシ内クラスタリング	1.1.1	Firepower 9300 シャーシ内のすべての ASA セキュリティ モジュールをクラスタ化できるようになりました。 [論理デバイス（Logical Devices）] > [設定（Configuration）] 画面を導入しました
6 つの ASA モジュールのシャーシ間クラスタリング	1.1.3	ASA のシャーシ間クラスタリングが実現されました。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 次の画面が変更されました。[論理デバイス（Logical Devices）] > [設定（Configuration）]

機能名	プラットフォームリリース	機能情報
Firepower 9300 の Firepower Threat Defense でのシャーシ内クラスタリング サポート	1.1.4	Firepower 9300 が Firepower Threat Defense アプリケーションでシャーシ内クラスタリングをサポートするようになりました。 次の画面が変更されました。[論理デバイス（Logical Devices）] > [設定（Configuration）]
Firepower 4100/9300 chassis 上の ASA のサイト間クラスタリングの改善	2.1.1	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 chassisのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次の画面が変更されました。[論理デバイス（Logical Devices）] > [設定（Configuration）]
6 つの Firepower Threat Defense モジュールのシャーシ間クラスタリング	2.1.1	Firepower Threat Defense のシャーシ間クラスタリングが実現されました。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 次の画面が変更されました。[論理デバイス（Logical Devices）] > [設定（Configuration）]