



Firepower 4100/9300 シャーシの ASA クラスタ

クラスタリングを利用すると、複数のFirepower 4100/9300 シャーシ ASA をグループ化して、1つの論理デバイスにすることができます。Firepower 4100/9300 シャーシシリーズには、Firepower 9300 および Firepower 4100 シリーズが含まれます。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 (9 ページ) を参照してください。

- [Firepower 4100/9300 シャーシでのクラスタリングについて \(1 ページ\)](#)
- [ASA の各機能とクラスタリング \(9 ページ\)](#)
- [Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 \(16 ページ\)](#)
- [上のクラスタリングのライセンス Firepower 4100/9300 シャーシ \(17 ページ\)](#)
- [クラスタリング ガイドラインと制限事項 \(19 ページ\)](#)
- [クラスタリングの設定 Firepower 4100/9300 シャーシ \(24 ページ\)](#)
- [FXOS : クラスタ メンバの削除 \(43 ページ\)](#)
- [ASA : クラスタ メンバの管理 \(44 ページ\)](#)
- [ASA : での ASA クラスタのモニタリング Firepower 4100/9300 シャーシ \(49 ページ\)](#)
- [クラスタリングの参考資料 \(51 ページ\)](#)
- [Firepower 4100/9300 シャーシ 上の ASA クラスタリングの履歴 \(58 ページ\)](#)

Firepower 4100/9300 シャーシでのクラスタリングについて

クラスタは、単一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。Firepower 4100/9300 シャーシにクラスタを展開すると、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（デフォルトのポート チャンネル 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、シャーシ間通信のために、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構成が Firepower 4100/9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。
- 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。[クラスタリングの参考資料 \(51 ページ\)](#) も参照してください。

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構成が Firepower 4100/9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部はユーザが設定できます。

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達成します。

クラスタ内のメンバの 1 つが **マスター** ユニットです。マスターユニットは自動的に決定されます。他のすべてのメンバは **スレーブ** ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上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、スレーブユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能（10 ページ）](#) を参照してください。

マスターおよびスレーブユニットの役割

クラスタ内のメンバの1つがマスターユニットです。マスターユニットは自動的に決定されます。他のすべてのメンバはスレーブユニットです。

すべてのコンフィギュレーション作業はマスターユニット上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、スレーブユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能（10 ページ）](#) を参照してください。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポートチャンネル48）です。シャーシ内クラスタリングでは、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、シャーシ間通信のために、Firepower 4100/9300 シャーシのこの 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。

2 シャーシのシャーシ間クラスタの場合、シャーシと他のシャーシ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。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

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。たとえば、ASA 5585-X と SSP-60 を使用する場合は、クラスタのユニットあたり最大 14

Gbpsを通過させることができるので、クラスタ制御リンクに割り当てるインターフェイスも、最低 14 Gbps の通過が可能となるようにしてください。この場合は、たとえば 10 ギガビットイーサネットインターフェイス2つを EtherChannel としてクラスタ制御リンクに使用し、残りのインターフェイスを必要に応じてデータ リンクに使用します。

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。
- ネットワーク アクセスに対する AAA は一元的な機能であるため、すべてのトラフィックがマスターユニットに転送されます。
- 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。

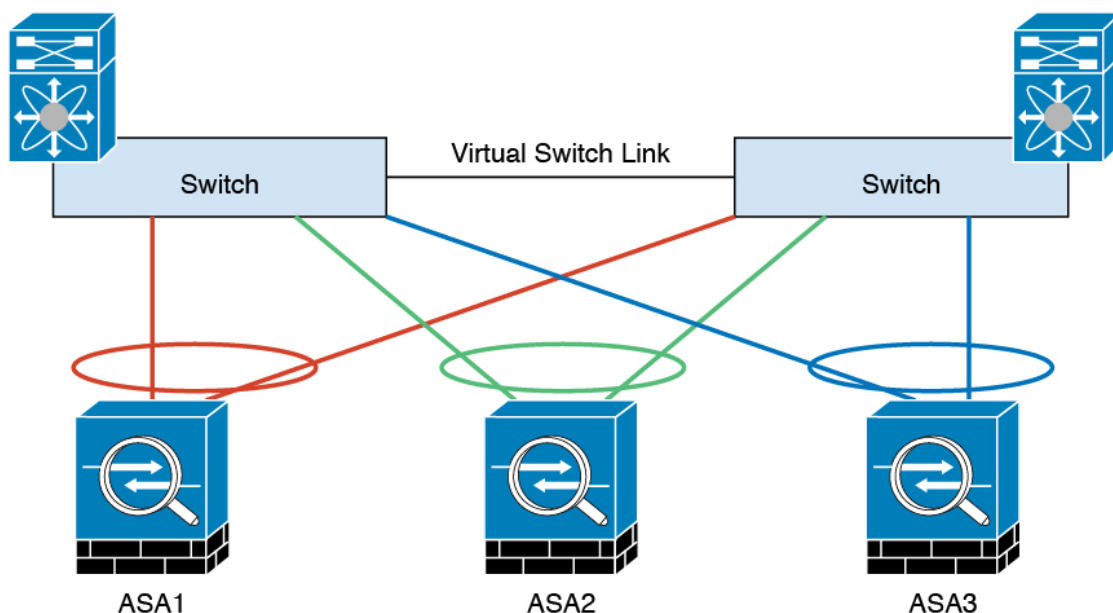


(注) クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンク冗長性

クラスタ制御リンクには EtherChannel を使用することを推奨します。冗長性を実現しながら、EtherChannel 内の複数のリンクにトラフィックを渡すことができます。

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 ASA 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ーです。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。



333222

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 シャーシは、シャーシ ID およびスロット 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 IP アドレスを自動生成します。FXOS とアプリケーション内のどちらでも、この IP アドレスを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には、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。サイト間トラフィックには、オーバーレイ トランスポート 仮想化 (OTV) を使用することをお勧めします。

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、EtherChannel（ポートチャネルとも呼ばれる）の両方を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、各シャーシの同じメンバー インターフェイスを含みます。

アップストリームスイッチでは、これらのインターフェイスはすべて単一の EtherChannel に含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

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。

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。

設定の複製

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マスター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。

ASA クラスタの管理

ASA クラスタリングを使用することの利点の1つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

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単位に直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスターユニットに属します。アドレス範囲も設定して、現在のマスター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。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタの管理をシームレスに続行できます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在のマスターユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

マスターユニット管理とスレーブユニット管理

すべての管理とモニタリングはマスターユニットで実行できます。マスターユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソールメッセージをスレーブユニットからマスターユニットに複製することもできます。

必要に応じて、スレーブユニットを直接モニタできます。マスターユニットからでもできますが、ファイル管理をスレーブユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスターユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング（コンソール レプリケーションが有効な場合にコンソールに送信される syslog を除く）。
- SNMP
- NetFlow

RSA キー複製

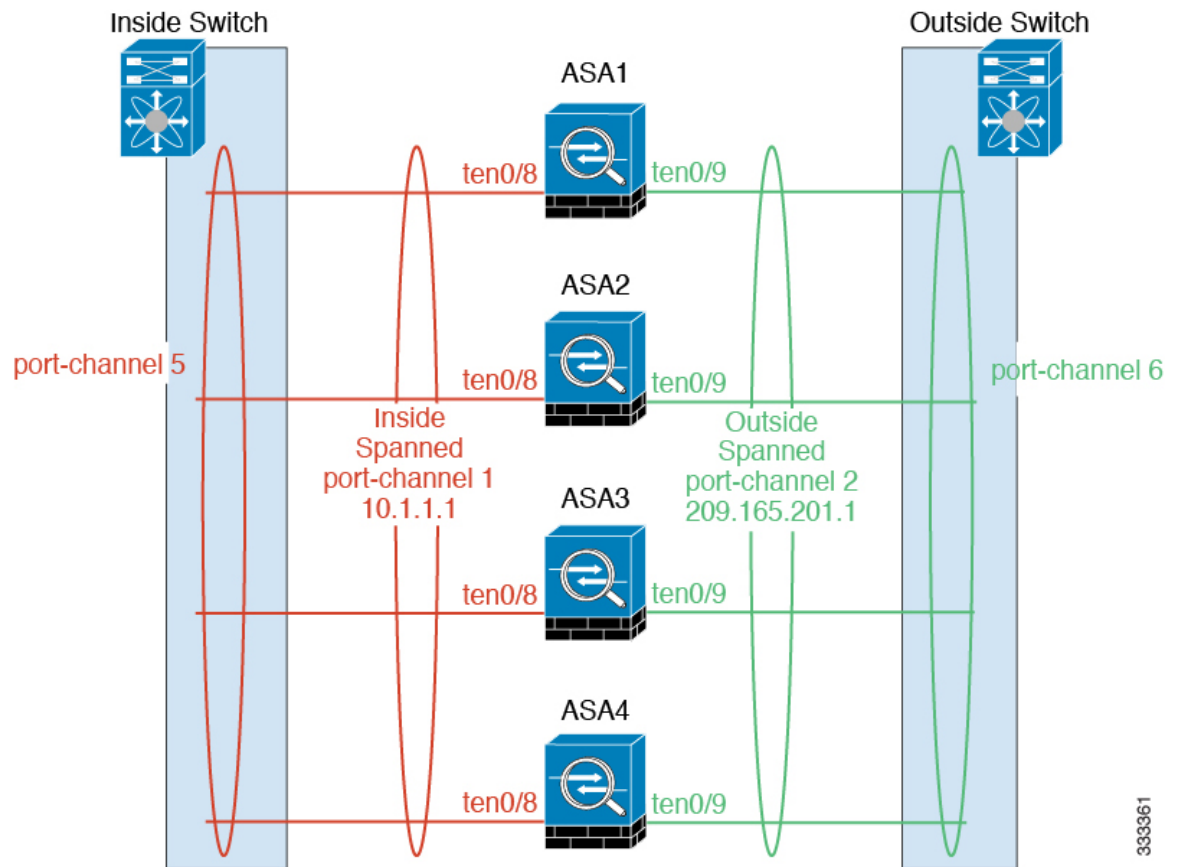
マスターユニット上で RSA キーを作成すると、そのキーはすべてのスレーブユニットに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合に、マスターユニットで障害が発生すると接続が切断されます。新しいマスターユニットは、SSH 接続に対して同じキーを使用するので、新しいマスターユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメインクラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

スパンド EtherChannel（推奨）

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、チャン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ーではなく 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。



333361

サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッドモードでサポートされます。

サイト ID は、LISP インスペクションを使用したフロー モビリティの有効化。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- クラスタ フロー モビリティの設定 : [クラスタ フロー モビリティの設定 \(39 ページ\)](#)

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスターユニットだけでサポートされます。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、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN (SSL VPN および IPsec VPN)
- IS-IS ルーティング
- 次のアプリケーション インспекション：
 - CTIQBE
 - H323、H225、および RAS
 - IPsec パススルー
 - MGCP
 - MMP
 - RTSP
 - SCCP (Skinny)
 - WAAS
 - WCCP
- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- VPN ロード バランシング
- フェールオーバー
- デッド接続検出 (DCD)

クラスタリングの中央集中型機能

次の機能は、マスター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。たとえば、3 ユニットから成るクラスタがあるとします。Other VPN ライセンスでは、許可されるサイト間 IPsec トンネルの最大数は 20,000 です。3 ユニットクラスタ全体で使用できるトンネル数は 20,000 までです。この各機能はスケーリングしません。



(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ユニットからマスター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、トラフィックがマスターユニットに送り返されます。

中央集中型機能については、マスター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、新しいマスター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спекション :

- DCERPC
- NetBIOS
- PPTP
- RADIUS
- 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

• IGMP マルチキャスト コントロールプレーンプロトコル処理 (データプレーンフォワーディングはクラスタ全体に分散されます)

• PIM マルチキャスト コントロールプレーンプロトコル処理 (データプレーン転送はクラスタ全体に分散されます)

• ネットワーク アクセスの認証および許可。アカウントリングは非集中型です。

• フィルタリング サービス

• サイト間 IKEv1/IKEv2 VPN

集中モードでは、VPN 接続はクラスタのマスターとのみ確立されます。これは、VPN クラスタリングのデフォルトモードです。サイト間 VPN は、S2S IKEv2 VPN 接続がメンバー間で分散される分散型 VPN モードでも展開できます。

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスターユニットではなく、各 ASA ユニットに適用されます。

- **QoS** : QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ユニットから成るクラスタがあり、トラフィックが均等に分散している場合は、適合レートは実際にクラスタのレートの3倍になります。
- **脅威検出** : 脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャントラフィックが全ユニット間で分散されるので、1つのユニットがすべてのトラフィックを読み取ることはないからです。
- **リソース管理** : マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。
- **LISP トラフィック** : UDP ポート 4342 上の LISP トラフィックは、各受信ユニットによって検査されますが、ディレクタは割り当てられません。各ユニットは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウントिंगの3つのコンポーネントで構成されます。認証および許可は、クラスタリングマスター上で中央集中型機能として実装されており、データ構造がクラスタスレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスターユニット変更が発生したときも維持されます。

アカウントिंगは、クラスタ内の分散型機能として実装されています。アカウントINGはフロー単位で実行されるので、フローを所有するクラスタユニットがアカウントING開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウントINGが設定されているとき）。

FTP とクラスタリング

- FTPデータチャンネルとコントロールチャンネルのフローがそれぞれ別のクラスタメンバによって所有されている場合は、データチャン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ン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。
- FTPアクセスにAAAを使用している場合、制御チャンネルのフローはマスターユニットに集中化されます。

アイデンティティ ファイアウォールとクラスタリング

マスターユニットのみがADからuser-groupを取得し、ADエージェントからuser-ipマッピングを取得します。マスターユニットからユーザ情報がスレーブに渡されるので、スレーブは、セキュリティポリシーに基づいてユーザIDの一致の決定を行うことができます。

マルチキャストルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、マスターユニットがすべてのマルチキャストルーティングパケットとデータパケットを処理します。接続が確立された後は、各スレーブがマルチキャストデータパケットを転送できます。

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。着信および発信のNATパケットが、クラスタ内のそれぞれ別のASAに送信されることがあります。これは、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が使用される場合、着信と発信でパケットのIPアドレスやポートが異なるためです。NATオーナーではないASA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。NATオーナーはセキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

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。

- ポートブロック割り当てによるPATなし：この機能はクラスタではサポートされていません。
- ポートブロック割り当てによるPAT：この機能については、次のガイドラインを参照してください。
 - ホストあたりの最大制限は、クラスタ全体の制限ではなく、各ユニットで個別に適用されます。したがって、ホストあたりの最大制限が1に設定されている3つのノードを持つクラスタにおいて、ホストからのトラフィックが3つすべてのユニットでロー

ドバランシングされる場合、そのクラスタには3つのブロック（各ユニットに1つずつ）を割り当てることができます。

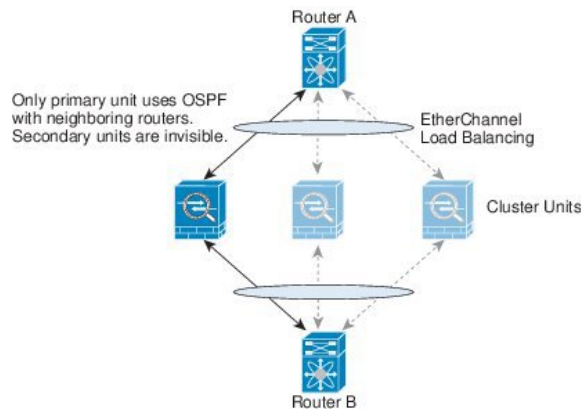
- バックアップ プールからバックアップ ユニットに作成されたポート ブロックは、ホストあたりの最大制限の適用時には含まれません。
- PAT IP アドレスのオーナーがダウンすると、バックアップ ユニットが PAT IP アドレス、対応するポートブロック、および xlate を所有します。ただし、新しい要求を処理するためにこれらのブロックは使用されません。接続が最終的にタイムアウトすると、ブロックは解放されます。
- PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタユニット間でロード バランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
- ダイナミック PAT 用 NAT プールアドレス分散：マスターユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが1つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可能なアドレスがある場合でも）。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。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- 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。
- マスターユニットによって管理されるダイナミック NAT xlate：マスターユニットが xlate テーブルを維持し、スレーブ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スレーブ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、スレーブはマスターユニットに xlate を要求します。スレーブユニットが接続を所有します。
- Per-session PAT 機能：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケーラビリティが向上します。クラスタリングの場合は、各スレーブユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスターユニットに転送する必要があり、マスターユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 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
- PPTP
- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

ダイナミック ルーティングおよびクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター 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 パケットがスレーブに到着した場合は、マスター 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



スレーブ メンバがマスター 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、マスター ユニットからスレーブ ユニットに同期されません。マスター 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。

SCTP とクラスタリング

SCTP 関連付けは、任意のユニットで作成できます（ロード バランシングのため）。そのマルチホーミング接続は同じユニットに存在する必要があります。

SIP インспек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（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。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル 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、新しいマスターが選定されたときに、新しいマスターユニットのポーリングに失敗します。

STUN とクラスタリング

ピンホールが複製される時、STUN インспекションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はユニット間で複製されません。STUN 要求の受信後にユニットに障害が発生し、別のユニットが STUN 応答を受信した場合、STUN 応答はドロップされます。

syslog および NetFlow とクラスタリング

- **Syslog** : 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。
- **NetFlow** : クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポートとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

マスター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。マスターユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティポリシーに基づいて SGT の一致決定を下せます。

VPN とクラスタリング

サイトツーサイト VPN は、中央集中型機能です。マスターユニットだけが VPN 接続をサポートします。



- (注) リモートアクセス VPN は、クラスタリングではサポートされません。分散型サイト間 VPN クラスタリングがサポートされています。詳細については、この [pdf](#) のハイ アベイラビリティ オプションを検索してください。

VPN 機能を使用できるのはマスター 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。マスター 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。新しいマスターが選定されたときに、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、接続が自動的にマスター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。

Firepower4100/9300 シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリングユニット

- Firepower 4100 : 16 シャーシ
- Firepower 9300 : 16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせたことができます。

インター シャーシ クラスタ化に関するハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ :

- Firepower4100 シリーズ : すべてのシャーシが同一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。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。
- 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。

- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成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、インターフェイスが同じバンド EtherChannel に内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイス モジュールの追加または削除、あるいは EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（スレーブユニットから始めて、マスターで終わります）。FXOS でインターフェイスを削除した場合、必要な調整を行うことができるように、ASA 設定では関連するコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。古いインターフェイス設定は手動で削除することができます。
- 同じ NTP サーバを使用する必要があります。手動で時間を設定しないでください。
- ASA : 各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。スレーブユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firepower Threat Defense では、すべてのライセンスは Firepower Management Center で処理されます。

スイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好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。

上のクラスタリングのライセンス Firepower 4100/9300 シャーシ

各 Firepower 4100/9300 シャーシは、License Authority またはサテライト サーバに登録されている必要があります。スレーブユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効になっているオプションの高度暗号化（3DES/AES）機能のライセンスについては、以下を参照してください。

ASA ライセンス設定では、マスターユニットに対するスマートライセンスの設定のみを行えます。設定はスレーブユニットに複製されますが、一部のライセンスに対しては、スレーブユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、マスターユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはスレーブユニットにも

キャッシュされ、その中の1つが将来マスターユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます:

- **標準**: マスターユニットのみがサーバから標準ライセンスを要求します。スレーブユニットにはデフォルトで有効になっている標準ライセンスがあります。そのライセンスを使用するため、サーバに登録を行う必要はありません。
- **コンテキスト**: マスターユニットのみがサーバからコンテキストライセンスを要求します。デフォルトで標準ライセンスは10のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットの標準ライセンスの値と、マスターユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
 - クラスタに6台の Firepower9300 モジュールがある場合を考えます。標準ライセンスは10のコンテキストを含みます。6つユニットの場合、合計で60のコンテキストが加算されます。マスターユニット上で追加の20コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは80のコンテキストを含みます。モジュールごとのプラットフォーム制限は250であるため、統合されたライセンスに最大250のコンテキストが許容されます。80のコンテキストは制限範囲内です。したがって、マスターユニット上で最大80コンテキストを設定できます。各スレーブユニットも、コンフィギュレーションの複製を介して80コンテキストを持つこととなります。
 - クラスタに Firepower4110 が3台あるとします。標準ライセンスは10のコンテキストを含みます。3つユニットの場合、合計で30のコンテキストが加算されます。マスターユニット上で追加の250コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは280のコンテキストを含みます。ユニットごとのプラットフォームの制限が250であるため、統合されたライセンスでは最大250のコンテキストが許容されます。280コンテキストは制限を超えています。したがって、マスターユニット上で最大250のコンテキストのみを設定できます。各スレーブユニットも、コンフィギュレーションの複製を介して250のコンテキストを持つこととなります。この場合では、マスターのコンテキストライセンスとして220のコンテキストのみを設定する必要があります。
- **キャリア**: 分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバから各自のライセンスを要求します。このライセンスの設定はスレーブユニットに複製されます。
- **高度暗号化 (3DES)** (2.3.0 以前の Cisco Smart Software Manager サテライト導入の場合、または追跡目的の場合): このライセンスはユニットごとの権限付与であり、各ユニットはサーバから各自のライセンスを要求します。

新しいマスターユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、マスターライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古いマスターユニットがスレーブユニットとしてクラスタに再度参加すると、マスターユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、スレーブユニットがライセンスを解放する前に、マスターユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは30日間有効です。

が、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされたマスター設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

クラスタリングガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタ デバイス MTU より 14 バイト大きく設定します。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（アジャセンシー）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 MTU は、ASR IPv4 MTU と一致する必要があります。
- 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。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード (ISSU) を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。
- 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。クラスタのデバイスにトラフィックを不均一に配分する場合がありますので、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デフォルトのロードバランシング アルゴリズムは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 プロトコルが再始動します。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。
- 一部のスイッチは、LACP でのダイナミック ポートプライオリティをサポートしていません (アクティブおよびスタンバイ リンク)。ダイナミック ポートプライオリティを無効にすることで、スパンド EtherChannel との互換性を高めることができます。
- 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路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。

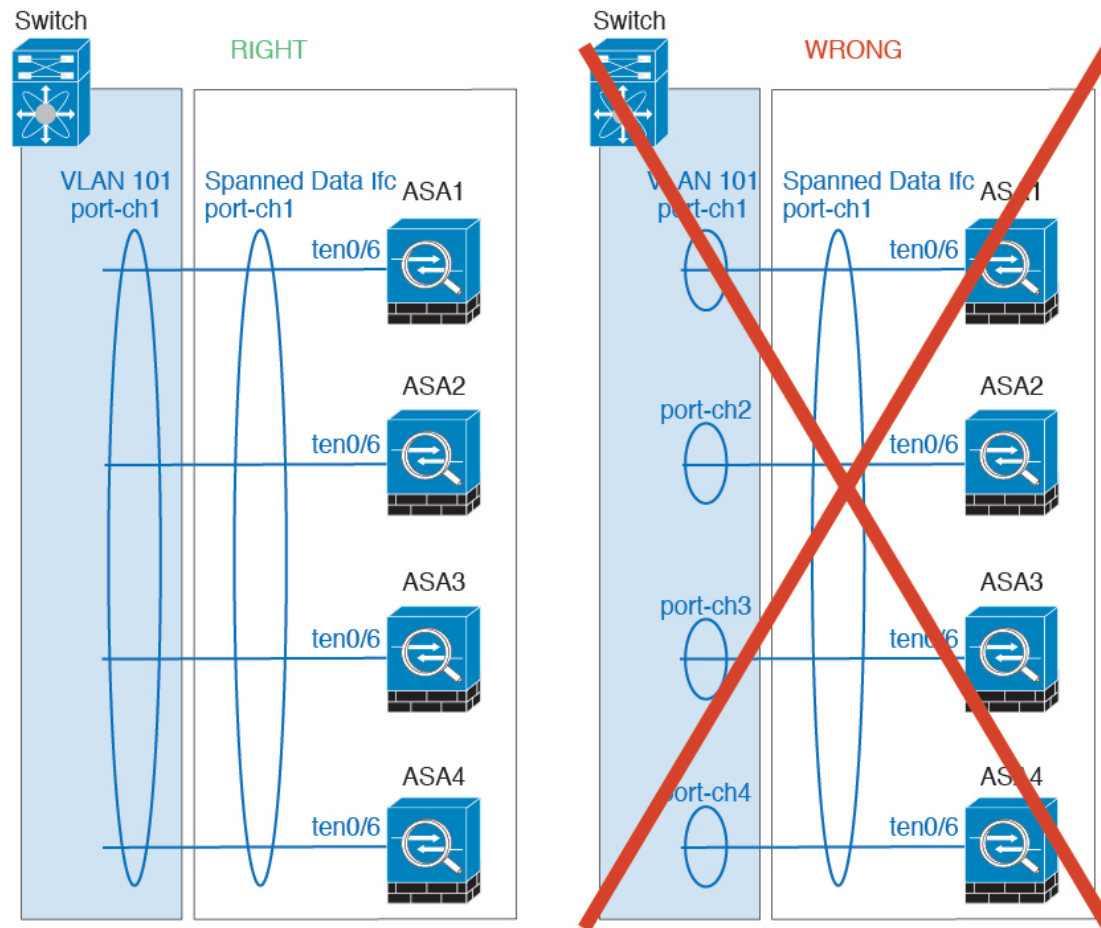
- ポートチャンネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャンネルでのハッシュ アルゴリズムを固定に変更します。

```
router(config)# port-channel id hash-distribution fixed
```

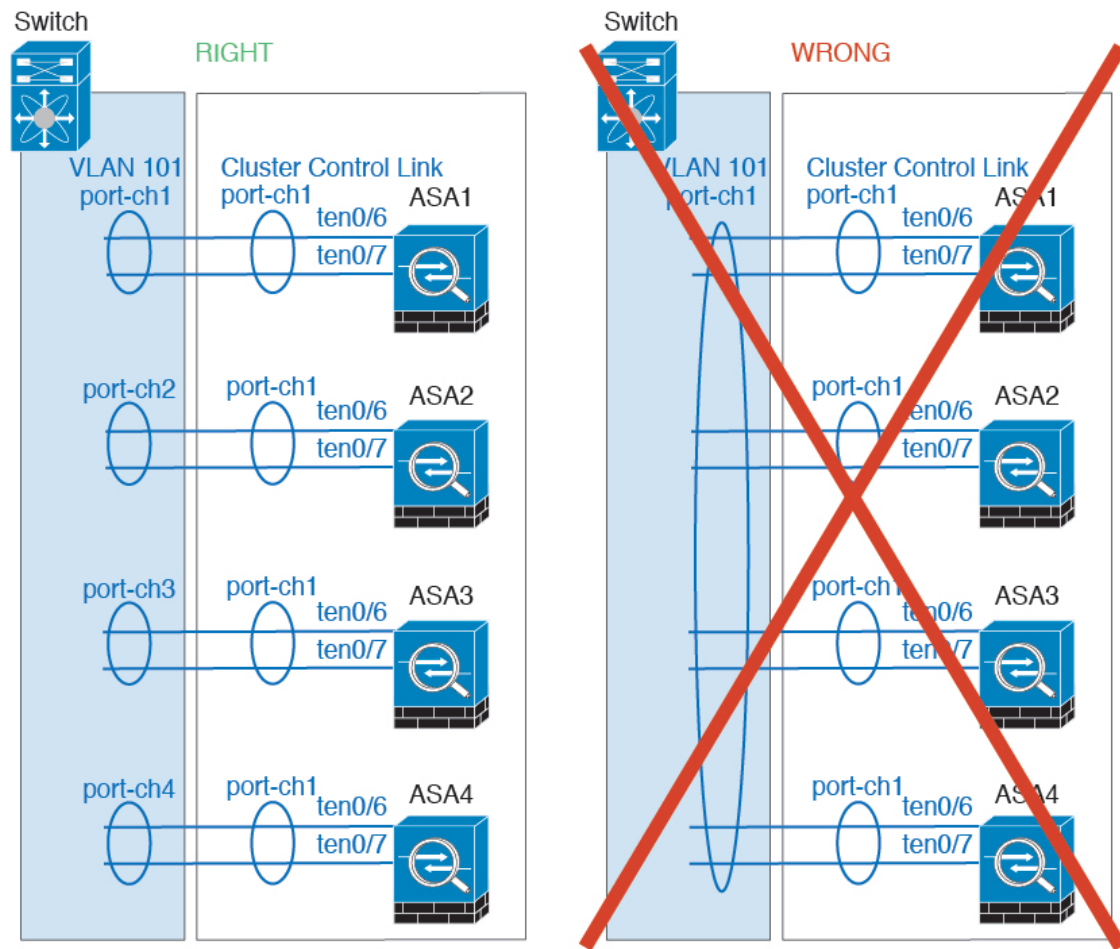
アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

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 シャーシではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [fast] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード (ISSU) を実行する際に LACP 高速レートがサポートされないため、クラスタリングで ISSU を使用することは推奨されません。
- 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ン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。



サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間 (RTT) 20 ms 未満である必要があります。
- 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、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタメンバには接続を再分散できません。
- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のルールが複数のサイトにまたがる場合があります。これは想定されている動作です。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると (AKA ノースサウス挿入)、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタメン

バがサイト2のメンバに接続を転送するとき、宛先MACアドレスは維持されます。MACアドレスがサイト1のルータと同じである場合にのみ、パケットはサイト2のルータに到達します。

- トランスペアレントモードの場合、内部ネットワーク間のファイル用に各サイトのデータネットワークとゲートウェイルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイルータは、HSRP などの First Hop Redundancy Protocol (FHRP) を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイトランスポート仮想化 (OTV) または同様のものを使用してサイト全体にわたって拡張されます。ローカルゲートウェイルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイルータが1つのサイトに到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。
- スパンド EtherChannel を使用したルーテッドモードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが1つのサイトに到達不能になった場合、トラフィックが正常に他のサイトのクラスタユニットに到達できるようにフィルタを削除する必要があります。ダイナミックルーティングは、サイト間クラスタが拡張セグメントのファーストホップルータとして機能する場合はサポートされません。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、Firepower 4100/9300 シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。
- ユニットの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。これは予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 EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることになります。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一部のシャーシセキュリティモジュールをクラスタ化し、他のセキュリティモジュールを実行することはできません。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。

デフォルト

- クラスタのヘルスチェック機能は、デフォルトでイネーブルになり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネットヘルスマonitoringがイネーブルになっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は5秒です。
- 失敗したクラスタ制御リンクのクラスタ自動再結合機能は、5分おきに無制限に試行されるように設定されています。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5分後と、2に設定された増加間隔で合計で3回試行されるように設定されています。
- HTTPトラフィックは、5秒間の接続レプリケーション遅延がデフォルトで有効になっています。

クラスタリングの設定 Firepower 4100/9300 シャーシ

クラスタは、Firepower 4100/9300 シャーシスーパー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に自動的に生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタメンバーを管理する方法についても説明します。クラスタメンバーシップは Firepower 4100/9300 シャーシからも管理できます。詳細については、Firepower 4100/9300 シャーシのマニュアルを参照してください。

手順

-
- ステップ 1 [FXOS : ASA クラスタの追加 \(24 ページ\)](#)
 - ステップ 2 [ASA : ファイアウォールモードとコンテキストモードの変更 \(32 ページ\)](#)
 - ステップ 3 [ASA : データインターフェイスの設定 \(32 ページ\)](#)
 - ステップ 4 [ASA : クラスタ設定のカスタマイズ \(35 ページ\)](#)
 - ステップ 5 [ASA : クラスタメンバの管理 \(44 ページ\)](#)
-

FXOS : ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。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。1つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

ASA クラスタの作成

クラスタは、Firepower 4100/9300 シャーシスーパー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に自動的に生成されます。

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。導入を容易にするために、1つのシャーシにクラスタを導入し、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。

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。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォール モードを変更します。

クラスタを導入すると、Firepower 4100/9300 シャーシスーパーバイザが次のブートストラップ コンフィギュレーションで各 ASA アプライアンスを設定します。ブートストラップ コンフィギュレーションの一部 (**太字**のテキストで示されている部分) は、後から必要に応じて ASA から変更できます。

```
interface Port-channel48
  description Clustering Interface
  cluster group <service_type_name>
  key <secret>
  local-unit unit-<chassis#-module#>

  cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
  priority <auto>
  health-check holdtime 3
  health-check data-interface auto-rejoin 3 5 2
  health-check cluster-interface auto-rejoin unlimited 5 1
  enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
  management-only individual
  nameif management
  security-level 0
  ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
  no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```



(注) **local-unit** 名は、クラスタリングを無効化した場合にのみ変更できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシにアップロードします。
- 次の情報を用意します。
 - 管理インターフェイス ID、IP アドレス、およびネットワーク マスク
 - ゲートウェイ IP アドレス

手順

ステップ 1 インターフェイスを設定します。

- a) 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。

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が1つ以上のメンバーインターフェイスを持つスパンド 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。スイッチ上で、すべてのクラスタユニットからメンバーインターフェイスを1つの EtherChannel へと結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、[クラスタリング ガイドラインと制限事項 \(19 ページ\)](#) を参照してください。

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。シャーシ間クラスタリングでは、EtherChannel のみが割り当てられます。他のインターフェイスタイプを割り当てることはできません。導入後にもクラスタにデータインターフェイスを追加できます。

- b) 管理タイプのインターフェイスまたは EtherChannel を追加します。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません (FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前が表示されます)。

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。

- c) シャーシ間クラスタリングでは、ポートチャネル 48 にメンバー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。

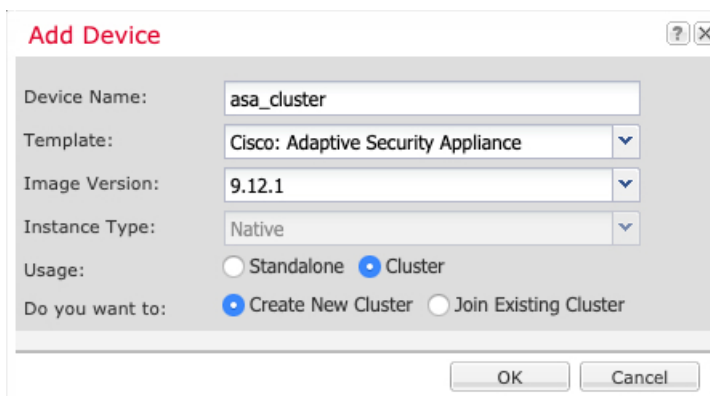
シャーシ内クラスタリングのメンバーインターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタがシャーシ間であると見なし、例えばスパンド Etherchannel のみを使用できるようになります。

[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、メンバーインターフェイスが含まれていない場合は、[Operation State] を [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 はメンバー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。

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。クラスタ制御リンクは、各シャーシのデバイスローカル EtherChannel です。デバイスごとにスイッチで個別の EtherChannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、[クラスタリング ガイドラインと制限事項 \(19 ページ\)](#) を参照してください。

ステップ 2 [論理デバイス (Logical Devices)] を選択します。

ステップ 3 をクリックし、次のパラメータを設定します。



The screenshot shows a dialog box titled "Add Device" with the following configuration:

- Device Name: asa_cluster
- Template: Cisco Adaptive Security Appliance
- Image Version: 9.12.1
- Instance Type: Native
- Usage: Cluster (selected)
- Do you want to: Create New Cluster (selected)

a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理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。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。

c) [Image Version] を選択します。

d) [Instance Type] では、[Native] タイプのみがサポートされます。

e) [Usage] では、[Cluster] オプションボタンをクリックします。

f) [Create New Cluster] ラジオ ボタンをクリックします。

g) [Create New Cluster] ラジオ ボタンをクリックします。

h) [OK] をクリックします。

[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。

ステップ 4 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [Cluster Information] ページで、次の手順を実行します。

Cisco: Adaptive Security Appliance - Bootstrap Configuration ? ×

Cluster Information Settings

Security Module

Security Module-1, Security Module-2, Security Module-3

Interface Information

Chassis ID:

Site ID:

Cluster Key:

Confirm Cluster Key:

Cluster Group Name:

Management Interface:

CCL Subnet IP:

DEFAULT

Address Type:

IPv4

Management IP Pool: -

Virtual IPv4 Address:

Network Mask:

Network Gateway:

- a) シャーシ間クラスタリングでは、**シャーシ 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。
- このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバーインターフェイスを追加した場合にのみ表示されます。
- b) [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) [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) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

- e) 管理インターフェイスの [Address Type] を選択します。

この情報は、ASA 設定で管理インターフェイスを設定するために使用されます。次の情報を設定します。

- [Management IP Pool] : 開始アドレスと終了アドレスをハイフンで区切って入力し、ローカル IP アドレスのプールを設定します。このうちの 1 つがインターフェイス用に各クラスタユニットに割り当てられます。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュールスロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスターユニットに属する仮想 IP アドレス (メインクラスタ IP アドレスと呼ばれる) は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス (どちらか一方も可) を使用できます。

- ネットワーク マスクまたはプレフィックス長

- ネットワーク ゲートウェイ

- [VIRTUAL IP address] : 現在のマスターユニットの管理 IP アドレスを設定します。この IP アドレスは、クラスタプールアドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

ステップ 6 [Settings] ページで、以下を実行します。

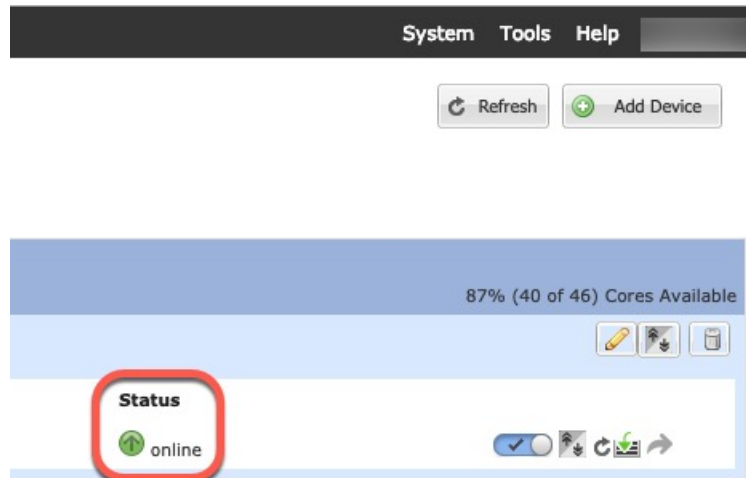
- a) 管理者ユーザの [Password] を入力して確認します。


事前設定されている ASA 管理者ユーザはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザパスワードを忘れたときにリセットできます。

ステップ 7 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[論理デバイス (Logical Devices)] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティポリシーの設定を開始できます。



- ステップ 9** 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。
- 最初のシャーシの Firepower Chassis Manager で、右上にある [Show Configuration] アイコン () をクリックして、表示されるクラスタの設定をコピーします。
 - 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。
 - [必要な操作 (I want to:)] > [既存のクラスタへの参加 (Join an Existing Cluster)] を選択します。
 - [OK] をクリックします。
 - [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。
 - 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。
 - **Chassis ID** : 一意のシャーシ ID を入力します。
 - **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。
- [OK] をクリックします。
- [保存 (Save)] をクリックします。

- ステップ 10** マスターユニット ASA に接続して、クラスタリング設定をカスタマイズします。

クラスタ メンバの追加

ASA クラスタ メンバを追加または置き換えます。




- (注) この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

始める前に

- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。
- マルチコンテキストモードでは、最初のクラスタメンバの ASA アプリケーションでマルチコンテキストモードを有効にします。追加のクラスタメンバはマルチコンテキストモード設定を自動的に継承します。

手順

- ステップ 1** 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。
- ステップ 2** 右上の [Show Configuration] アイコン () をクリックして、表示されるクラスタの設定をコピーします。
- ステップ 3** 新しいシャーシの Firepower Chassis Manager に接続して、[追加 (Add)] > [クラスタ (Cluster)] > をクリックします。
- ステップ 4** [Device Name] に論理デバイスの名前を入力します。
- ステップ 5**
- ステップ 6** [Template] では、[Cisco Adaptive Security Appliance] を選択します。
- ステップ 7**
- ステップ 8** [Image Version] では、ASA のソフトウェアバージョンを選択します。
- ステップ 9**
- ステップ 10** [Device Mode] では、[Cluster] オプション ボタンをクリックします。
- ステップ 11**
- ステップ 12** [既存のクラスタへの参加 (Join an Existing Cluster)] を選択します。
- ステップ 13** [OK] をクリックします。
- ステップ 14** [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。

ステップ 15 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。

- **Chassis ID** : 一意のシャーシ ID を入力します。
- **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。

[OK] をクリックします。

ステップ 16 [保存 (Save)] をクリックします。

ASA : ファイアウォール モードとコンテキスト モードの変更

デフォルトでは、FXOS シャーシはルーテッドまたはトランスペアレント ファイアウォール モード、およびシングル コンテキスト モードでクラスタを展開します。

- **ファイアウォール モードの変更** : 展開後にモードを変更するには、マスター ユニットでモードを変更します。モードは一致するようにすべてのスレーブユニットで自動的に変更されます。を参照してください。 [ファイアウォール モード \(シングル モード\) の設定](#) マルチ コンテキスト モードでは、コンテキストごとにファイアウォール モードを設定します。 [セキュリティ コンテキストの設定](#) を参照してください。
- **マルチ コンテキスト モードに変更** : 展開後にマルチ コンテキスト モードに変更するには、マスター ユニットのモードを変更します。これにより、すべてのスレーブユニットのモードは一致するように自動的に変更されます。 [マルチ コンテキスト モードの有効化](#) を参照してください。

ASA : データ インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。



(注) 管理インターフェイスは、クラスタを展開したときに事前設定されました。ASA で管理インターフェイス パラメータを変更することもできますが、この手順はデータ インターフェイスに焦点を当てています。管理インターフェイスは、スパンドインターフェイスとは対照的に、個別のインターフェイスです。詳細については、「[管理インターフェイス \(6 ページ\)](#)」を参照してください。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] >

[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

- トランスペアレント モードの場合は、ブリッジグループを設定します。
- シャーシ間クラスタリングにスバンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

-
- ステップ 1** コンテキスト モードによって次のように異なります。
- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
 - マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。
- ステップ 2** インターフェイスを選択して、[Edit] をクリックします。
[Edit Interface] ダイアログボックスが表示されます。
- ステップ 3** 次の設定を行います。
- (EtherChannel の場合) [MIO Port-channel ID] : FXOS で使用されるのと同じ ID を入力します。
 - **[Enable Interface]** (デフォルトでオンになります)
- この画面の残りのフィールドは、この手順の後半で説明します。
- ステップ 4** MAC アドレスおよびオプション パラメータを設定するには、[Advanced] タブをクリックします。
- [MAC Address Cloning] 領域で、EtherChannel の手動グローバル MAC アドレスを設定します。スタンバイ MAC アドレスを設定しないでください。無視されます。潜在的なネットワークの接続問題を回避するために、スバンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。MAC アドレスを設定していない場合に、マスター ユニットが変更された場合、新しいマスター ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。
- マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

- サイト間クラスタリングの場合、[ASA Cluster] 領域で、**サイト固有の MAC アドレスを、ルーテッドモードの場合は IP アドレスを設定するために、[Add] をクリックして、サイト ID (1 ~ 8) の MAC アドレスおよび IP アドレスを指定します。**最大 8 つのサイトで上記の手順を繰り返します。サイト固有の IP アドレスは、グローバル IP アドレスと同じサブネット上にある必要があります。ユニットで使用するサイト固有の MAC アドレスおよび IP アドレスは、各ユニットのブートストラップ コンフィギュレーションに指定したサイト ID によって異なります。

ステップ 5 (オプション) この EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 6 (マルチ コンテキスト モード) この手順を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

- [OK] をクリックして変更内容を確定します。
- インターフェイスを割り当てます。
- ユーザが設定するコンテキストを変更します。[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択し、カスタマイズするポートチャネルインターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 7 [General] タブをクリックします。

ステップ 8 (トランスペアレントモード) [Bridge Group] ドロップダウンリストから、このインターフェイスを割り当てるブリッジグループを選択します。

ステップ 9 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 10 [Security level] フィールドに、0 (最低) ~ 100 (最高) のレベルを入力します。

ステップ 11 (ルーテッドモード) IPv4 アドレスに対して [Use Static IP] オプションボタンをクリックし、IP およびマスクを入力します。DHCP と PPPoE はサポートされません。トランスペアレントモードの場合は、EtherChannel インターフェイスではなく、ブリッジグループインターフェイスの IP アドレスを設定します。

ステップ 12 (ルーテッドモード) IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

トランスペアレントモードの場合は、EtherChannel インターフェイスではなく、ブリッジグループインターフェイスの IP アドレスを設定します。

- [Enable IPv6] チェックボックスをオンにします。
- [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

(注) [Enable address autoconfiguration] オプションはサポートされません。

- [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、2001:DB8::BA98:0:3210/64。

- d) (オプション) ホストアドレスとして Modified EUI-64 インターフェイス ID を使用するには、[EUI-64] チェックボックスをオンにします。この場合は、単に [Address/Prefix Length] フィールドにプレフィックスを入力します。
- e) [OK] をクリックします。

ステップ 13 [OK] をクリックして、[Interfaces] 画面に戻ります。

ステップ 14 [Apply] をクリックします。

ASA : クラスタ設定のカスタマイズ

クラスタを展開した後にブートストラップ設定を変更する場合や、クラスタリングヘルスモニタリング、TCP 接続複製の遅延、フローモビリティ、およびその他の最適化など、追加のオプションを設定する場合は、マスターユニットで行うことができます。

ASA クラスタの基本パラメータの設定

マスターユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチ コンテキスト モードでは、マスターユニット上のシステム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。
- local-unit **Member Name** およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合に ASA でのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]** の順に選択します。

ステップ 2 (任意) 次のオプションパラメータを設定します。

- **[Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]** : 接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ~ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスターユニットからスレーブユニットに複製されます。

- **[Enable health monitoring of this device within the cluster]** : クラスタユニットのヘルスチェック機能を有効にして、ユニットキープアライブステータスメッセージ間の間隔を .8 から 45 秒の間で設定します。デフォルトは 3 秒です。**注** : 新しいユニットをクラスタに追加していて、ASA またはスイッチのトポロジが変更される場合、クラスタが完成するまでこの機能を一時的にディセーブルにし、ディセーブルにされたインターフェイスのインターフェイス モニタリングもディセーブルにする必要があります (**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]**)。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブメッセージを送信します。ユニットが保留時間内にピア ユニットからキープアライブメッセージを受信しない場合は、そのピアユニットは応答不能またはデッド状態と見なされます。
- **[Replicate console output to the master's console]** : スレーブ ユニットからマスターユニットへのコンソール複製をイネーブルにします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製をイネーブルにすると、スレーブユニットからマスターユニットにコンソールメッセージが送信されるので、モニタが必要になるのはクラスタのコンソールポート 1 つだけとなります。このパラメータは、ブートストラップコンフィギュレーションの一部ではなく、マスターユニットからスレーブユニットに複製されます。
- **クラスタリング フロー モビリティを有効にします。** [LISP インспекションの設定 \(41 ページ\)](#) を参照してください。

ステップ 3 **[Cluster Control Link]** 領域で、クラスタ制御リンクの MTU を設定できます。この領域のその他のオプションは、ASA では設定できません。

- **[MTU]** : クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。MTU の最大値を 9184 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。

ステップ 4 (任意) **[Cluster LACP]** 領域で、スタティック ポートの優先順位を有効にできます。ASA は cLACP を使用して、EtherChannel とネイバースイッチのネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの (仮想) デバイスであるかのように見えます。この領域のその他のオプションは、クラスタリングを無効化せずに、ASA では設定できません。

- **[Enable static port priority]** : LACP のダイナミック ポートプライオリティをディセーブルにします。一部のスイッチはダイナミック ポートプライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。さらに、8 個より多くのアクティブなスバンド EtherChannel メンバのサポートがイネーブルになります (最大 32 メンバ)。このパラメータを使用しないと、サポートされるのは 8 個のアクティブメンバと 8 個のスタンバイメンバのみです。このパラメータをイネーブルにした場合、スタンバイメンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップコンフィギュレーションの一部ではなく、マスターユニットからスレーブユニットに複製されます。

ステップ 5 [Apply] をクリックします。

インターフェイスのヘルス モニタリングおよび自動再結合の設定

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ポートチャンネル ID、または単一の物理インターフェイス ID をモニタできます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring] の順に選択します。

ステップ 2 [Monitored Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックしてそのインターフェイスを [Unmonitored Interfaces] ボックスに移動します。

インターフェイス ステータス メッセージによって、リンク障害が検出されます。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブポートがある場合、そのユニットはクラスタから削除されます。ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、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。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ポートチャンネル ID、または単一の物理インターフェイス ID を指定できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 4100/9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし ([Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster])、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。

ステップ 3 インターフェイスまたはクラスタ制御リンクに障害が発生した場合の自動再結合の設定をカスタマイズするには、[Auto Rejoin] タブをクリックします。各タイプに関して [Edit] をクリックして次の設定を行います。

- [Maximum Rejoin Attempts] : クラスタへの再結合の試行回数を定義するために、[Unlimited] または 0 ~ 65535 の範囲で値を設定します。0 は自動再結合をディセーブルにします。デ

フォルト値は、クラスタ インターフェイスの場合は [Unlimited]、データ インターフェイスの場合は [3] です。

- **[Rejoin Interval]** : 再結合試行間隔の時間を定義するために、2 ~ 60 の範囲で間隔を設定します。デフォルト値は 5 分です。クラスタへの再結合をユニットが試行する最大合計時間は、最後の失敗から 14,400 分に限られています。
- **[Interval Variation]** : 1 ~ 3 の範囲で設定して、間隔を増加させるかどうかを定義します (1 : 変更なし、2 : 直前の間隔の 2 倍、3 : 直前の間隔の 3 倍)。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後 (2 x 5)、3 階目の試行が 20 分後 (2 x 10) となります。デフォルト値は、クラスタ インターフェイスの場合は [1]、データ インターフェイスの場合は [2] です。

デフォルト設定に戻すには、[Restore Defaults] をクリックします。

ステップ 4 [Apply] をクリックします。

クラスタ TCP 複製の遅延の設定

TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップフロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップフローが作成される前にユニットが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のユニットに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]. の順に選択します。

ステップ 2 [Add] をクリックして次の値を設定します。

- **[Replication delay]** : 1 ~ 15 の範囲で秒数を設定します。
- **[HTTP]** : すべての HTTP トラフィックの遅延を設定します。デフォルトでは、この設定は 5 秒間で有効化されています。
- **[Source Criteria]**
 - **[Source]** : 送信元 IP アドレスを設定します。
 - **[Service]** : (オプション) 送信元ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。
- **[Destination Criteria]**
 - **[Source]** : 宛先 IP アドレスを設定します。

- [Service] : (オプション) 宛先ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。

ステップ3 [OK] をクリックします。

ステップ4 [適用 (Apply)] をクリックします。

サイト間機能の設定

サイト間クラスタリングの場合、冗長性と安定性を高めるために、設定をカスタマイズできません。

クラスタ フロー モビリティの設定

LISP のトラフィックを検査して、サーバがサイト間を移動する時にフロー モビリティを有効にできます。

LISP インスペクションについて

LISP トラフィックを検査することで、サイト間のフローのモビリティを有効にできます。

LISP について

VMware VMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンターサーバモビリティをサポートするには、サーバの移動時にサーバへの入力ルートをルータが更新できる必要があります。Cisco Locator/ID Separation Protocol (LISP) のアーキテクチャは、デバイス ID、つまりエンドポイント ID (EID) をその場所、つまりルーティング ロケータ (RLOC) から2つの異なるナンバリングスペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

LISP では、LISP の出力トンネルルータ (ETR)、入力トンネルルータ (ITR)、ファーストホップルータ、マップリゾルバ (MR)、およびマップサーバ (MS) などのある一定のロールにおいてルータとサーバが必要です。サーバが別のルータに接続されていることをサーバのファーストホップルータが感知すると、そのルータは他のすべてのルータとデータベースを更新し、クライアントに接続されている ITR がトラフィックを代行受信してカプセル化し、新しいサーバの場所に送信できるようにします。

ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISP の統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフローオーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィックフローは最適ではなく、「トロンボーン」または「ヘアピン」呼ばれます。

LISP 統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR 間でやり取りされる LISP トラフィックを検査し、フローの所有者を新しいサイトに変更できます。

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。
- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々のユニットに属しているフローは新しいオーナーに移動されません。半分散されたフローには SIP などのアプリケーションが含まれており、親フローとそのすべての子フローが同じ ASA によって所有されます。
- クラスタはレイヤ 3 および 4 のフロー状態を移動させるだけです。一部のアプリケーション データが失われる可能性があります。
- 短時間のフローまたはビジネスに不可欠でないフローの場合、オーナーの移動は有用でない可能性があります。インスペクションポリシーを設定するときに、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

ASA LISP の実装

この機能には、複数の相互に関係する設定が含まれています（それらについてはすべてこの章で説明します）。

1. （任意）ホストまたはサーバ IP アドレスに基づく検査対象 EID の制限：ファースト ホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。
2. LISP トラフィック インスペクション：ASA は、ファーストホップルータと ITR または ETR の間で送信される EID 通知メッセージにおいて、UDP ポート 4342 上の LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。たとえば、ファーストホップルータの送信元 IP アドレスと ITR または ETR の宛先アドレスで LISP トラフィックを検査する必要があります。LISP トラフィックにはディレクタが割り当てられておらず、LISP トラフィック自体はクラスタ状態の共有に参加しないことに注意してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。
4. サイト ID：ASA は、各クラスタユニットのサイト ID を使用して新しい所有者を特定します。

5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP インспекションの設定

LISP のトラフィックを検査して、サーバがサイト間を移動する時にフロー モビリティを有効にできます。

始める前に

- [ASA クラスタの基本パラメータの設定 \(35 ページ\)](#) に従って、各クラスタ ユニットのサイト ID に割り当てます。
- LISP のトラフィックはデフォルトインспекショントラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

手順

ステップ 1 (任意) LISP インспекションマップを設定して、IP アドレスに基づいて検査済みの EID を制限し、LISP の事前共有キーを設定します。

- a) **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [LISP]** を選択します。
- b) **[Add]** をクリックして、新しいマップを追加します。
- c) 名前 (最大 40 文字) と説明を入力します。
- d) **Allowed-EID access-list** については、**[Manage]** をクリックします。

[ACL Manager] が開きます。

ファースト ホップ ルータまたは ITR/ETR は、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信することがあります。このため、クラスタに関連するサーバまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

- e) ファイアウォールの設定ガイドに従って、少なくとも 1 つの ACE で ACL を追加します。
- f) 必要に応じて、**検証キー**を入力します。

暗号化キーをコピーした場合は、**[Encrypted]** オプション ボタンをクリックします。

- g) **[OK]** をクリックします。

ステップ 2 サービス ポリシー ルールを追加して LISP インспекションを設定します。

- a) **[Configuration] > [Firewall] > [Service Policy Rules]** の順に選択します。
- b) **[Add]** をクリックします。

- c) [Service Policy] ページで、インターフェイスへのルールまたはグローバルなルールを適用します。
既存のサービス ポリシーで使用するものがあれば、そのポリシーにルールを追加します。デフォルトで、ASA には **global_policy** と呼ばれるグローバル ポリシーが含まれます。ポリシーをグローバルに適用しない場合は、インターフェイスごとに 1 つのサービスポリシーを作成することもできます。LISP インспекションは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービスポリシーを適用する必要はありません。トラフィックが両方向のクラスに一致する場合、ルールを適用するインターフェイスに出入りするトラフィックのすべてが影響を受けます。
- d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)] をオンにします。
- e) [Next] をクリックします。
- f) インспекションを行うトラフィックを指定します。ファーストホップルータと UDP ポート 4342 の ITR または ETR の間のトラフィックを指定します。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
- g) [Next] をクリックします。
- h) [Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。
- i) [LISP] チェックボックスをオンにします。
- j) (オプション) [Configure] をクリックして、作成したインспекションマップを選択します。
- k) [Finish] をクリックして、サービス ポリシー ルールを保存します。

ステップ 3 サービス ポリシー ルールを追加して、重要なトラフィックのフロー モビリティを有効化します。

- a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。
- b) [Add] をクリックします。
- c) [Service Policy] ページで、LISP インспекションに使用する同じサービスポリシーを選択します。
- d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)] をオンにします。
- e) [Next] をクリックします。
- f) サーバがサイトを変更するときに最適なサイトに再割り当てする、ビジネスクリティカルなトラフィックを指定します。たとえば、フロー モビリティを HTTPS トラフィック および/または特定のサーバへのトラフィックのみに制限できます。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
- g) [Next] をクリックします。
- h) [Rule Actions] ウィザード ページまたはタブで、[Cluster] タブを選択します。
- i) [Enable Cluster flow-mobility triggered by LISP EID messages] チェックボックスをオンにします。
- j) [Finish] をクリックして、サービス ポリシー ルールを保存します。

ステップ 4 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] の順に選択し、[Enable Clustering flow mobility] チェックボックスをオンにします。

ステップ 5 [Apply] をクリックします。

FXOS : クラスタ メンバの削除

ここでは、メンバを一時的に、またはクラスタから永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタメンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、Firepower Chassis Manager の [Logical Devices] ページで、のクラスタ ステータスを確認します。



The screenshot shows a table with two columns: Management Port and Status. The Management Port is Ethernet1/4 and the Status is online. Below the table, there is an 'Attributes' section with the following information:

Management Port	Status
Ethernet1/4	online

Attributes

- Cluster Operational Status : not-in-cluster
- FIREPOWER-MGMT-IP : 10.89.5.20
- CLUSTER-ROLE : none
- CLUSTER-IP : 127.2.1.1
- MGMT-URL : https://10.89.5.35/
- UUID : 8e459170-451d-11e9-8475-f22f06c32630





FMC を使用した FTD では、FMC デバイス リストにデバイスを残し、クラスタリングを再度有効にした後にすべての機能を再開できるようにする必要があります。

- アプリケーションでのクラスタリングの無効化 : アプリケーション CLI を使用してクラスタリングを無効にすることができます。 **cluster remove unit name** コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスターユニットを削除するためにスレーブユニットでこのコマンドを入力した場合は、新しいマスターユニットが選定されます。

デバイスが非アクティブになると、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。管理専用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。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブでは

ない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。


クラスタリングを再度有効にするには、ASA で **cluster group name** を入力してから **enable** を入力します。クラスタリングを再度有効にするには、FTD で **cluster enable** を入力します。

- アプリケーション インスタンスの無効化：Firepower Chassis Manager の [Logical Devices] ページで [Disable] スライダ () をクリックします。[Enable] スライダ () を使用して後で再度有効にすることができます。
- セキュリティ モジュール/エンジンのシャットダウン：Firepower Chassis Manager の [Module/Engine] ページで、[Power Off] アイコン () をクリックします。
- シャーシのシャットダウン：Firepower Chassis Manager の [Overview] ページで、[Shut Down] アイコン () をクリックします。

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

FMC を使用した FTD の場合、シャーシでクラスタリングを無効にした後でユニットを FMC デバイス リストから削除してください。

- 論理デバイスの削除：Firepower Chassis Manager の [Logical Devices] ページで、[Delete] アイコン () をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティモジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

ASA : クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリングコンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。



- (注) ASAが(手動で、またはヘルスチェックエラーにより)非アクティブになると、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。管理専用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。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合(クラスタリングが無効な状態で設定を保存した場合など)、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] の順に選択します。

ステップ 2 [Participate in ASA cluster] チェックボックスをオフにします。

- (注) [Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソールポートで CLI にアクセスする必要があります。

ステップ 3 [Apply] をクリックします。

マスターユニットからのスレーブメンバーの非アクティブ化

スレーブメンバを非アクティブにするには、次のステップを実行します。



- (注) ASAが非アクティブになると、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。管理専用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。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーションモードに入っていない場合は、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。

ステップ 2 削除するスレーブを選択して [Delete] をクリックします。

スレーブ ブートストラップ コンフィギュレーションは同じであり、その設定を失うことなく以後スレーブを再追加できます。

ステップ 3 [Apply] をクリックします。

クラスタへの再参加

ユニットがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソールポートを使用する必要があります。他のインターフェイスはシャットダウンされます。ただし、ASDMでクラスタリングを手動で無効にした場合、設定を保存してリロードしなかった場合は、ASDMでクラスタリングを再び有効にできます。リロード後、管理インターフェイスは無効になるため、コンソールアクセスがクラスタリングを再び有効にする唯一の方法です。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーションモードに入っていない場合は、[Configuration] >

[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

- ステップ 1** ASDM にまだアクセスしている場合は、再イネーブル化するユニットに ASDM を接続して、ASDM でクラスタリングを再び有効にすることができます。
- 新しいメンバーとして追加していない限り、スレーブユニットのクラスタリングをマスターユニットから再び有効にすることはできません。
- a) [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。
 - b) [Participate in ASA cluster] チェックボックスをオンにします。
 - c) [Apply] をクリックします。
- ステップ 2** ASDM を使用できない場合：コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group name

例：

```
ciscoasa(config)# cluster group pod1
```

- ステップ 3** クラスタリングをイネーブルにします。

enable

マスターユニットの変更



注意 マスターユニットを変更する最良の方法は、マスターユニットでクラスタリングを無効にし、新しいマスターの選択を待ってから、クラスタリングを再度有効にする方法です。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスター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、新しいマスターユニット上で接続を再確立する必要があります。

マスターユニットを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーションモードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

-
- ステップ 1 [Monitoring] > [ASA Cluster] > [Cluster Summary] を選択します。
 - ステップ 2 [Change Master To] ドロップダウン リストから、マスターにするスレーブ ユニットを選択し、[Make Master] をクリックします。
 - ステップ 3 マスター ユニット変更の確認を求められます。[Yes] をクリックします。
 - ステップ 4 ASDM を終了し、メイン クラスタ IP アドレスを使用して再接続します。
-

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。 **show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。（または、マスターユニットで **show** コマンドを入力するとクラスタ全体の統計情報を表示できます。） **capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

始める前に

コマンドライン インターフェイス ツールでこの手順を実行します。[Tools] > [Command Line Interface] を選択します。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit unit_name] コマンド

例 :

```
cluster exec show xlate
```

メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから1つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタユニット名です。

次の **cluster exec show memory** コマンドの出力例では、クラスタの各メンバーのメモリ情報が表示されています。

```
cluster exec show memory
unit-1-1 (LOCAL):*****
Free memory:      108724634538 bytes (92%)
Used memory:      9410087158 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)

unit-1-3:*****
Free memory:      108749922170 bytes (92%)
Used memory:      9371097334 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)

unit-1-2:*****
Free memory:      108426753537 bytes (92%)
Used memory:      9697869087 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)
```

ASA : での ASA クラスタのモニタリング Firepower 4100/9300 シャーシ

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

- [Monitoring] > [ASA Cluster] > [Cluster Summary]

このペインには、接続相手のユニットとクラスタのその他のユニットの情報が表示されます。また、このペインでプライマリ装置を変更することができます。

- **[Cluster Dashboard]**

プライマリ装置のホームページの **[Cluster Dashboard]** と **[Cluster Firewall Dashboard]** を使用してクラスタをモニタできます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

[Wizards] > [Packet Capture Wizard]

クラスタ全体のトラブルシューティングをサポートするには、マスターユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブユニットでも自動的にイネーブルになります。

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [CPU]**

このペインでは、クラスタ メンバ全体の CPU 使用率を示すグラフまたはテーブルを作成することができます。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [Memory]**

このペインでは、クラスタ メンバ全体の **[Free Memory]** と **[Used Memory]** を表示するグラフまたはテーブルを作成することができます。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Connections]**

このペインでは、クラスタメンバ全体の接続を示すグラフまたはテーブルを作成することができます。

- **[Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Throughput]**

このペインでは、クラスタメンバ全体のトラフィックのスループットを示すグラフまたはテーブルを作成することができます。

クラスタ制御リンクのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

[Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link]。

このペインでは、クラスタ制御リンクの [Receival] および [Transmittal] 容量使用率を表示するグラフまたはテーブルを作成することができます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次の画面を参照してください。

- [Monitoring] > [Routing] > [LISP-EID Table]

EIDs と サイト ID を示す ASA EID テーブルを表示します。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

[Configuration] > [Device Management] > [Logging] > [Syslog Setup]

クラスタ内の各ユニットは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

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 の合計スループットの 80 %
- UDP の合計スループットの 90 %
- トラフィックの混在に応じて、イーサネット MIX (EMIX) の合計スループットの 60 %。

たとえば、TCP スループットについては、3つのモジュールを備えた Firepower 9300 は、単独で動作している場合、約 135 Gbps の実際のファイアウォールトラフィックを処理できます。2シャーシの場合、最大スループットの合計は 270 Gbps (2 シャーシ X 135 Gbps) の約 80 %、つまり 216 Gbps です。

マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

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. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティ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、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスターユニットになることはありません。既存のマスターユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスター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マスターにすることができます。中央集中型機能については、マスター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、新しいマスター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監視し、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提供します。

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 シャーシスーパーバイザはASAアプリケーションを定期的に確認します（毎秒）。ASAが作動中で、Firepower 4100/9300 シャーシスーパーバイザと 3 秒間通信できなければASAはsyslogメッセージを生成して、クラスタを離れます。

Firepower 4100/9300 シャーシスーパーバイザが 45 秒後にアプリケーションと通信できなければ、ASAをリロードします。ASAがスーパーバイザと通信できなければ、自身をクラスタから削除します。

ユニットのヘルスモニタリング

マスターユニットは、各スレーブユニットをモニタするために、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送信します（間隔は設定可能です）。各スレーブユニットは、同じメカニズムを使用してマスターユニットをモニタします。ユニットの健全性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、ステータス変更をマスターユニットに報告します。シャーシ間クラスタリングでは、サブバンド 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て EtherChannel でポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には ASA 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、デフォルトでは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メイン EtherChannel を含む)。アップ状態の指名された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前に、EtherChannel のすべてのメンバーポートがエラーとなる必要があります (最小ポート バンドル設定に基づく)。ヘルス チェックは、インターフェイスごとに、モニタリングをオプションで無効にすることができます。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ASA 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。ASA 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監視ししません。この間にインターフェイスのステータスが変化しても、ASA 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、ユニットがクラスタ内にとどまるには ASA、デコレータアプリケーション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。

マスター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、プライオリティが最高 (番号が最小) のものがマスターユニットになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。



- (注) ASA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。管理専用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。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはディセーブルになります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタメンバがクラスタから削除された後、クラスタに再参加できる方法は、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（最初の参加時）：クラスタ制御リンクの問題を解決した後、と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASAは、無限に5分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データインターフェイスの障害：ASAは自動的に最初は5分後、次に10分後、最終的に20分後に再参加を試みます。20分後に参加できない場合、ASAはクラスタリングをディセーブルにします。データインターフェイスの問題を解決した後、と入力して、クラスタリングを手動でイネーブルにする必要があります。この動作は設定可能です。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗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。ユニットは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：ASAが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、ASAは自動的にクラスタの再参加を試みます。
- デコレータアプリケーションの障害：ASAはデコレータアプリケーションが復帰したことを確認すると、クラスタへ再参加します。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーションステータスなどがあります。問題を解決したら、クラスタリングを再び有効にして、クラスタに手動で再参加する必要があります。

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。バックアップオーナーは通常ディレクタでもありません。

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

Traffic	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	Yes	トランスペアレントモードのみ。
MAC アドレス テーブル	Yes	トランスペアレントモードのみ。
ユーザ アイデンティティ	Yes	AAA ルール (uauth) と アイデンティティ ファイアウォールが含まれます。
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—
SNMP エンジン ID	なし	—
集中型 VPN (サイト間)	なし	VPN セッションは、マスター ユニットで障害が発生すると切断されます。

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

接続ごとに定義された次のロールを参照してください。

- **オーナー**：通常、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。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。

- **バックアップ オーナー**：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。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、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。

ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

1 台のシャーシに最大 3 つのクラスタ ユニットの搭載できる Firepower 9300 のシャーシ間クラスタリングでは、バックアップ オーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップ オーナーが選択されます。

- **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。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。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- **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、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 は使用されないため、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。

接続でポート アドレス変換 (PAT) を使用すると、PAT のタイプ (per-session または multi-session) が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- **Per-session PAT**：オーナーは、接続の最初のパケットを受信するユニットです。

デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- **Multi-session PAT** : オーナーは常にマスターユニットです。multi-session PAT 接続がスレーブユニットで最初に受信される場合、スレーブユニットはその接続をマスターユニットに転送します。

デフォルトでは、UDP (DNS UDP を除く) および ICMP トラフィックは multi-session PAT を使用するので、これらの接続は常にマスターユニットによって所有されています。

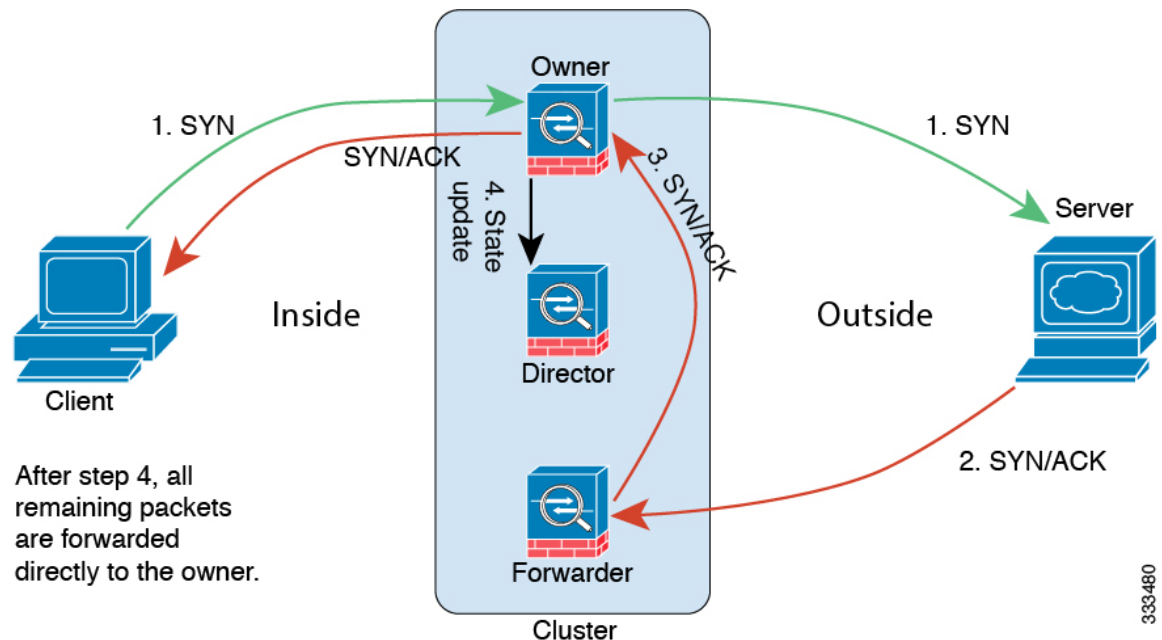
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

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、ASA 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 ASA (ロードバランシング方法に基づく) に配信されます。この ASA 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さ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、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 4100/9300 シャーシ上の ASA クラスタリングの履歴

機能名	バージョン	機能情報
の 16 個のシャーシのサポート Firepower 4100 シリーズ	9.6(2)	Firepower 4100 シリーズでは最大 16 個のシャーシをクラスタに追加できるようになりました。 変更された画面はありません。
Firepower 4100 シリーズのサポート	9.6(1)	FXOS 1.1.4 では、ASA は最大 6 個のシャーシの Firepower 4100 シリーズでサイト間クラスタリングをサポートします。 変更された画面はありません。
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	9.6(1)	スパンド EtherChannel のルーテッドモードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect (DCI) 経由の移動によるオーバーレイトランスポート仮想化 (OTV) デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次の画面を変更しました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced]

機能名	バージョン	機能情報
16 のモジュールのシャーシ間クラスタリング、および Firepower 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 16 のモジュールを搭載することができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。 変更された画面はありません。
ルーテッドファイアウォールモードのスパンド EtherChannel のサイト間クラスタリングサポートのサイト別 MAC アドレス	9.5(2)	ルーテッドモードでは、スパンド EtherChannel サイト間クラスタリングを使用することができます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタメンバーのサイト ID を設定します。 次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]
インターフェイスまたはクラスタ制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスタのカスタマイズ	9.5(2)	インターフェイスまたはクラスタ制御リンクが失敗した場合、auto-rejoin 動作をカスタマイズできます。 次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Auto Rejoin]
ASA クラスタは、GTPv1 と GTPv2 をサポートします	9.5(2)	ASA クラスタは、GTPv1 および GTPv2 インспекションをサポートします。 変更された画面はありません。
TCP 接続のクラスタ複製遅延	9.5(2)	この機能で、ディレクタ/バックアップフロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。 次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]

機能名	バージョン	機能情報
サイト間フローモビリティの LISP インспекション	9.5(2)	<p>Cisco Locator/ID Separation Protocol (LISP) のアーキテクチャは、デバイス ID をその場所から 2 つの異なるナンバリングスペースに分離し、サーバの移行をクライアントに対して透過的にします。ASA は、場所変更の LISP トラフィックを検査し、その情報をシームレスなクラスタリング運用に活用できます。ASA クラスタメンバーは、最初のホップルータと出力トンネルルータまたは入力トンネルルータの間の LISP トラフィックを検査し、フローオーナーの所在場所を新規サイトに変更します。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]</p> <p>[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [LISP]</p> <p>[Configuration] > [Firewall] > [Service Policy Rules] > [Protocol Inspection]</p> <p>[Configuration] > [Firewall] > [Service Policy Rules] > [Cluster]</p> <p>[Monitoring] > [Routing] > [LISP-EID Table]</p>
キャリアグレード NAT の強化は、フェールオーバーおよび ASA クラスタリングでサポートされます。	9.5(2)	<p>キャリアグレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます (RFC 6888 を参照してください)。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。</p> <p>変更された画面はありません。</p>
クラスタリングトレースエントリの設定可能なレベル	9.5(2)	<p>デフォルトで、すべてのレベルクラスタリングイベントは、多くの下位レベルのイベント以外に、トレースバッファに含まれます。より上位レベルのイベントへのトレースを制限するために、クラスタの最小トレースレベルを設定できます。</p> <p>変更された画面はありません。</p>
Firepower 9300 用 シャーシ内 ASA クラスタリング	9.4 (1150)	<p>FirePOWER 9300 シャーシ内では、最大 3 つセキュリティモジュールをクラスタ化できます。シャーシ内の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。</p> <p>次の画面を導入しました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]</p>