

Firepower 4100/9300 の ASA クラスターの展開

最終更新：2019年4月5日

Firepower 4100/9300 の ASA クラスターの展開

クラスタリングを利用すると、複数の ASA 装置をグループ化して1つの論理デバイスとすることができます。クラスターは、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。ASA ハードウェア モデルでもクラスタリングがサポートされますが、Firepower 4100/9300 は FXOS で別の設定を必要とするため、本書では FXOS および ASA 間の全体的な設定に重点を置いて説明しています。



(注) クラスタリングを使用する場合、一部の機能は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 \(76 ページ\)](#) を参照してください。



(注) 本書では、最新の ASA バージョン機能について網羅しています。機能の変更の詳細については、[Firepower 4100/9300 上の ASA クラスタリングの履歴 \(93 ページ\)](#) を参照してください。古いバージョンのソフトウェアを使用している場合は、お使いのバージョンの FXOS 設定ガイドおよび ASA 設定ガイドの手順を参照してください。

この統合によるメリット

FXOS プラットフォームでは、ASA を含む複数の論理デバイスを実行することができます。スタンドアロンおよびクラスタ化された論理デバイスの展開は、シャーシ内クラスター (Firepower 9300) およびシャーシ間クラスターの両方において簡単に実行できます。FXOS からクラスターを導入する際は、ASA ブートストラップを事前設定しておくこと、ASA アプリケーション内でのカスタマイズがほんのわずかで済みます。FXOS におけるクラスター設定をエクスポートすることにより、その他のクラスター メンバを追加することもできます。

統合された製品

この表では、この統合のために必要な製品の一覧を示します。

表 1: クラスタリング用に統合された製品

製品	機能	最小バージョン	必須かどうか
Firepower 4100 または 9300	ASA を実行するためのハードウェアプラットフォーム	FXOS 1.1.2	必須
Firepower Chassis Manager	FXOS GUI デバイスマネージャ	Firepower Chassis Manager 1.1.2	オプション：代わりに CLI を使用することができます。
ASA	Firewall アプリケーション	ASA 9.4 (1.152)	必須
ASDM	ASA GUI デバイスマネージャ	ASDM 7.4 (3)	オプション：代わりに CLI を使用することができます。

ワークフロー

このワークフローでは、クラスタリングの導入を完了するため、ASA の FXOS および ASDM で Firepower Chassis Manager を使用します。

手順

ステップ 1 FXOS の前提条件：

- スマートライセンスを設定します。スマートライセンスには、NTP サーバー（または少なくとも正確な手動設定時間）および DNS の設定が必要です。

ステップ 2 FXOS タスク：

- a) [FXOS：インターフェイスの設定（20 ページ）](#)。ASA に割り当てる 1 つの管理およびすべてのデータインターフェイスを設定します。クラスタインターフェイスはポートチャンネル 48 としてデフォルトで定義されていますが、シャーシ間のクラスタリングでは、メンバーインターフェイスを追加する必要があります。
- b) [ASA クラスターの作成（25 ページ）](#)。
- c) [クラスターメンバの追加（31 ページ）](#)。

ステップ 3 ASA のタスク。マスターユニットで次の手順のみを実行します。

- a) （任意）キャリアおよびコンテキスト機能のライセンスを設定します。ASA の一般的な操作のコンフィギュレーションガイドを参照してください。
- b) （任意）[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（33 ページ）](#)。デフォルトでは、FXOS シャーシはルーテッド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ーを展開します。

- c) [ASA : データ インターフェイスの設定 \(33 ページ\)](#)。管理インターフェイスは、クラスターを展開したときに事前設定されました。
- d) (任意) [ASA : クラスタ設定のカスタマイズ \(36 ページ\)](#)。サイト間の機能と分散サイト間 VPN を含む、数多くのクラスタリング機能をカスタマイズまたは有効化します。

Firepower 4100/9300 シャーシのクラスタリングについて

Firepower 4100/9300 シャーシにクラスターを展開すると、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。

クラスターを展開すると、クラスター名、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ー設定を含む最小限のブートストラップコンフィギュレーションがシャーシスーパーバイザから各ユニットに対してプッシュされます。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、クラスター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ー内のすべてのユニットに指定します。

ブートストラップコンフィギュレーション

クラスターを展開すると、クラスター名、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ー設定を含む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

シャーシスーパーバイザから各ユニットに対してプッシュされます。クラスター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ーが設定できません。

クラスターメンバー

クラスター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。

クラスター内のメンバーの1つが**制御**ユニットになります。制御ユニットは自動的に決定されます。他のすべてのメンバーは**データ**ユニットになります。

すべてのコンフィギュレーション作業は制御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、データユニットに複製されます。

機能によっては、クラスター内でスケールしないものがあり、そのような機能については制御ユニットがすべてのトラフィックを処理します。[クラスターリングの中央集中型機能 \(77 ページ\)](#) を参照してください。

クラスター制御リンク

クラスター制御リンクはユニット間通信用の EtherChannel (ポートチャネル48) です。シャーシ内クラスターリングでは、このリンクは、クラスター通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスターリングでは、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ーの場合、シャーシと他のシャーシの間をクラスター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、クラスター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ー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ー制御リンクは動作を維持します。

クラスター制御リンク 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。

- 制御ノードの選択。
- 設定の複製。
- 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。

- 状態の複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスター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ー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、クラスター制御リンクが最悪のシナリオを処理できます。

クラスター制御リンク 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。クラスター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制御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、クラスターは大量の接続の再分散を必要とするため、一時的にクラスター制御リンクの帯域幅を大量に使用します。

クラスター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。

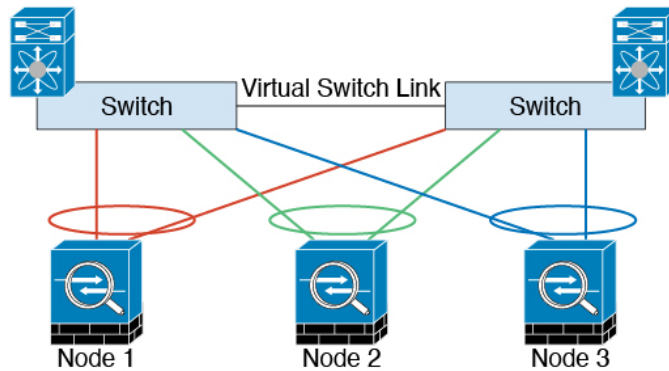


(注) クラスターに大量の非対称（再分散された）トラフィックがある場合は、クラスター制御リンクのサイズを大きくする必要があります。

クラスター制御リンク冗長性

クラスター制御リンクには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）、仮想ポートチャネル（vPC）、StackWise、またはStackWise Virtual環境でクラスター制御リンクとして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。スイッチが冗長システムの一部である場合は、同じEtherChannel内のファイアウォールインターフェイスをそれぞれ、冗長システム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。



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 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。クラスタを展開するときに、この IP アドレスをカスタマイズできます。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。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と 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。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。

冗長スイッチシステムへの接続

インターフェイスに冗長性を持たせるために、EtherChannel を VSS、vPC、StackWise、または StackWise Virtual システムなどの冗長スイッチシステムに接続することをお勧めします。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

Secure Firewall ASA クラスターの管理

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ユニット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、常に現在の制御ユニットに属します。アドレス範囲も設定して、現在の制御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。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。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御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、現在の制御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、制御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ーに接続します。

制御ユニット管理とデータユニット管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。また、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。

- ノードごとの 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

暗号キー複製

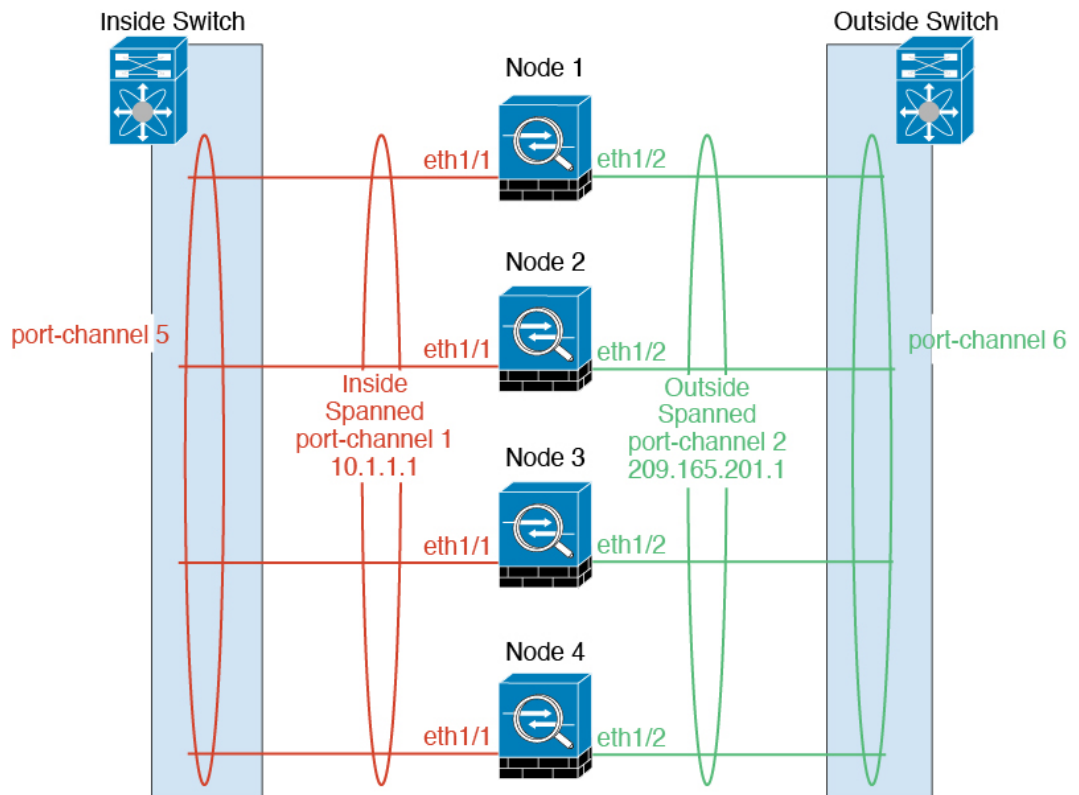
制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH 接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

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と、IP アドレス不一致に関する警告メッセージが表示される場合があります。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 アドレスではないためです。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。詳細については、[「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」](https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html) を参照してください。

スバンド 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。スバンド 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。



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。

各クラスター 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。クラスター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、クラスター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するフローモビリティ、データセンターのサイト間クラスタリングのパフォーマンスを向上し、ラウンドトリップ時間の遅延を減少させるためのディレクター ローカリゼーション、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトにある接続のサイト冗長性を有効にするためにも使用されます。

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。

- Data Center Interconnect のサイジング : [Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 \(10 ページ\)](#)

- サイト間のガイドライン：クラスタリングガイドラインと制限事項（14 ページ）
- クラスターフローモビリティの設定：クラスターフローモビリティの設定（43 ページ）
- ディレクターローカリゼーションの有効化：ASA クラスターの基本パラメータの設定（36 ページ）
- サイト冗長性の実効化：ASA クラスターの基本パラメータの設定（36 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

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ることができます。

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：

- Firepower 4100：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。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 およびアプリケーションソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- 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、同じバンド 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や削除、または 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（データノードから始めて、制御ノードで終わります）。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。時間を手動で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。データノードは追加料金なしで使用できます。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。Threat Defense では、すべてのライセンスは、Management Center によって処理されます。

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特性については、『Cisco FXOS Compatibility』を参照してください。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect (DCI) に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバーの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCIの最小帯域幅は、1つのメンバーに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバーの場合。
 - 合計 4 クラスタ メンバー
 - 各サイト 2 メンバー
 - メンバーあたり 5 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 5 Gbps (2/2 x 5 Gbps)。

- 3 サイトの 6 メンバーの場合、サイズは増加します。
 - 合計 6 クラスタ メンバー
 - サイト 1 は 3 メンバー、サイト 2 は 2 メンバー、サイト 3 は 1 メンバー
 - メンバーあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps (3/2 x 10 Gbps)。

- 2 サイトの 2 メンバーの場合。
 - 合計 2 クラスタ メンバー
 - 各サイト 1 メンバー

- メンバーあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 10 Gbps (1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク (10 Gbps) のサイズ未満になってはなりません)。

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

Smart Software Manager Regular およびオンプレミス

クラスタリング機能自体にライセンスは必要ありません。強力な暗号化およびその他のオプションのライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシがライセンス機関または Smart Software Manager の通常およびオンプレミスサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

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 設定で有効化される高度暗号化 (3DES/AES) 機能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、制御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。設定はデータ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、データ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、制御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データユニットにもキャッシュされ、その中の1つが将来制御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:

- **Essentials** : 制御ユニットのみがサーバーから Essentials ライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- **コンテキスト** : 制御ユニットのみがサーバー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 Essentials 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 Essentials ライセンスの値と、制御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 Firepower 9300 モジュールがある場合を考えます。Essentials 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。制御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、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、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 Firepower 4112 が 3 台あるとします。Essentials 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。制御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

約されたクラスターライセンスは 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、制御ユニット上で最大 250 のコンテキストのみを設定できます。各データユニットも、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になります。この場合では、制御ユニット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ーから各自のライセンスを要求します。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager オンプレミス展開用、または管理目的用）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ーから各自のライセンスを要求します。

新しい制御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、制御ユニットの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。古い制御ユニットがデータユニットとしてクラスターに再度参加すると、制御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、データユニットがライセンスを解放する前に、制御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ーから離れた場合、キャッシュされた制御ユニットの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、クラスター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。

永続ライセンスの予約

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し、クラスターリングを設定する前にライセンスを有効にする必要があります。

分散型 S2S VPN のライセンス

キャリアライセンスは、クラスターの各メンバーで、分散型 S2S VPN に必要です。

各 VPN 接続には、2 つの *Other VPN* ライセンス済みセッションが必要です (*Other VPN* ライセンスは *Essentials* ライセンスの一部です)。1 つはアクティブセッション用、もう 1 つはバックアップセッション用です。クラスターの最大 VPN セッション容量は、セッションごとに 2 つのライセンスを使用するため、ライセンス済み容量の半分以下にすることができます。

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

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンク インターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンク インターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。
- Cisco IOS XR システム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 IOS XR インターフェイスの 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 MTU は、IOS XR IPv4 MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。
- 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-XE 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るので、ロード バランス 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化することで、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。

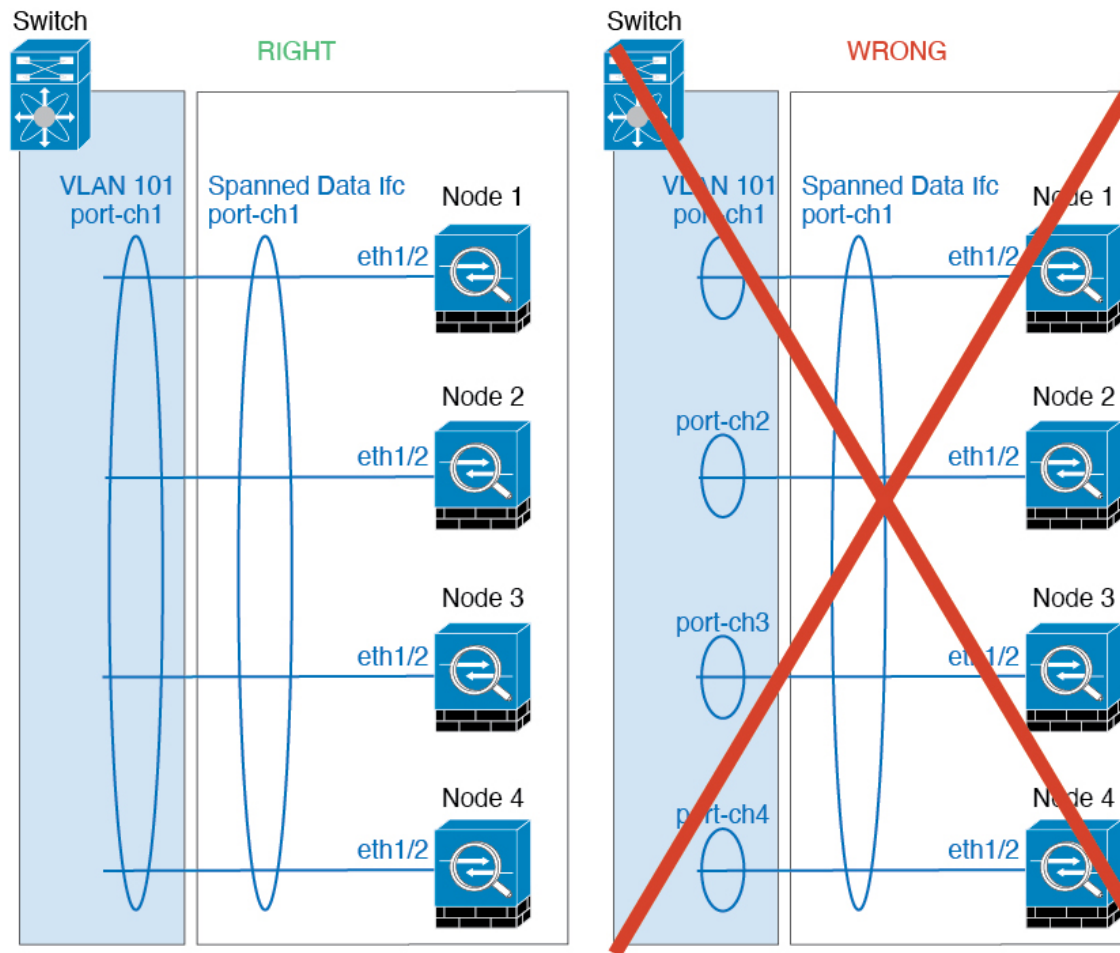
```
router(config)# port-channel id hash-distribution fixed
```

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。

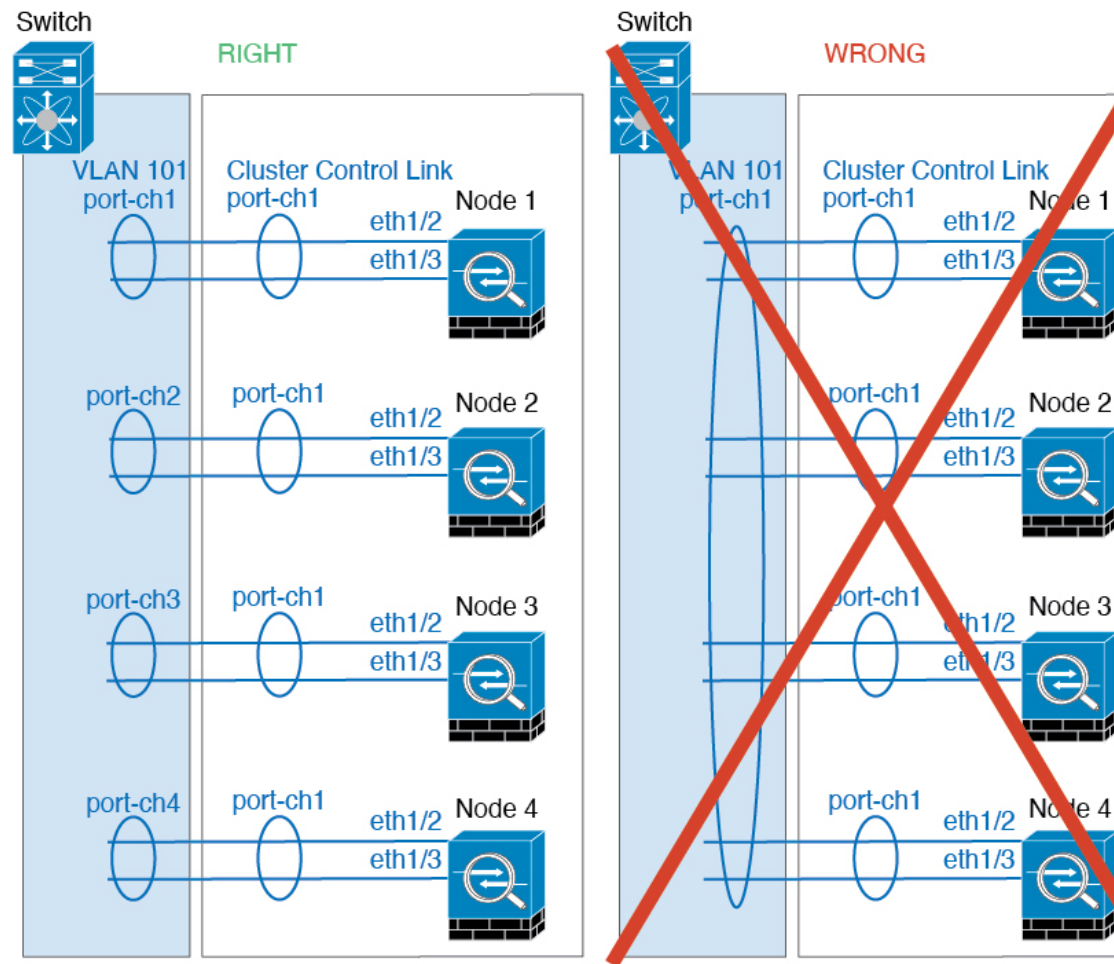
- ASA ハードウェアクラスタとは異なり、Firepower 4100/9300 クラスタは LACP グレースフルコンバージェンスをサポートしています。したがって、プラットフォームでは、接続されている Cisco Nexus スイッチで LACP グレースフルコンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速 (fast)] に設定されている LACP レートがあります。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。

シャーン間クラスタリングの EtherChannel

- 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、制御ユニットの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。
- ASAは専用リンクであるため、データセンター相互接続 (DCI) で使用されている場合でも、クラスタ制御リンクで転送されるデータトラフィックを暗号化しません。オーバーレイトランスポート仮想化 (OTV) を使用する場合、またはローカル管理ドメインの外部でクラスタ制御リンクを拡張する場合は、OTE を介した 802.1AE MacSec などの境界ルータで暗号化を設定できます。

- 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ロ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。ただし、ディレクタローカリゼーションを有効にすると、ローカルディレクタのロールは（サイト ID に従って）常に接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。
- ディレクタローカリゼーションでは、次のトラフィックタイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーションクエリ。
- 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 のクラスタメンバーがサイト 2 のメンバー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アウォー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 つのサイトで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。
- トランスペアレントモードでは、クラスタが HSRP ルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして ASA。隣接ルータで HSRP が使用される場合、HSRP IP アドレス宛てのトラフィックは HSRP MAC アドレスに送信されますが、リターントラフィックは特定のルータのインターフェイスの MAC アドレスから HSRP ペアで送信されます。したがって、ASA MAC アドレステーブルは通常、HSRP IP アドレスの ASA ARP テーブルエントリが期限切れになり、ASA が ARP 要求を送信して応答を受信した場合にのみ更新されます。ASA の ARP テーブルエントリはデフォルトで 14400 秒後に期限切れになりますが、MAC アドレステーブルエントリはデフォルトで 300 秒後に期限切れになるため、MAC アドレステーブルの期限切れトラフィックのドロップを回避するために静的 MAC アドレスエントリが必要です。
- 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 つのサイトで到達不能になった場合、トラフィックが他のサイトのクラスタノードに正常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、vPC、StackWise、または StackWise Virtual 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 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、vPC、StackWise、または StackWise Virtual 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、デフォルトで有効になり、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ニタリングが有効になっています。
- 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。

での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用に自動生成されます。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 \(33 ページ\)](#)
 - ステップ 3 [ASA : データ インターフェイスの設定 \(33 ページ\)](#)
 - ステップ 4 [ASA : クラスタ設定のカスタマイズ \(36 ページ\)](#)
 - ステップ 5 [ASA : クラスタ メンバの管理 \(55 ページ\)](#)
-

FXOS : インターフェイスの設定

クラスタの場合は、次のタイプのインターフェイスを設定する必要があります。

- 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 (ポートチャンネルとも呼ばれる) を追加します。[EtherChannel \(ポート チャンネル\) の追加 \(22 ページ\)](#) または [物理インターフェイスの設定 \(21 ページ\)](#) を参照してください。

シャーシ間クラスタリングの場合は、すべてのデータインターフェイスが、少なくとも 1 つ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 \(14 ページ\)](#) を参照してください。

- 管理タイプのインターフェイスまたは EtherChannel を追加します。[EtherChannel \(ポート チャンネル\) の追加 \(22 ページ\)](#) または [物理インターフェイスの設定 \(21 ページ\)](#) を参照してください。

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。

- シャーシ間クラスタリングでは、メンバーインターフェイスをクラスタ制御リンクの EtherChannel (デフォルトではポートチャンネル 48) に追加します。EtherChannel (ポートチャンネル) の追加 (22 ページ) を参照してください。

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ー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。

[インターフェイス (Interfaces)] タブで、ポートチャンネル 48 クラスター 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。

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。クラスター制御リンクは、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 \(14 ページ\)](#) を参照してください。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。



- (注) QSFPH40G-CUxM の場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

- ステップ 1** [インターフェイス (Interfaces)] を選択して、[インターフェイス (Interfaces)] ページを開きます。

[All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

- ステップ 2** 編集するインターフェイスの行で[編集 (Edit)] をクリックし、[インターフェイスを編集 (Edit Interface)] ダイアログボックスを開きます。

- ステップ 3** インターフェイスを有効にするには、[有効化 (Enable)] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。

ステップ 4 インターフェイスの [タイプ (Type)] を選択します。

- データ
- 管理
- [クラスター (Cluster)]: [クラスター (Cluster)] タイプは選択しないでください。デフォルトでは、クラスター制御リンクはポートチャネル 48 に自動的に作成されます。

ステップ 5 (任意) [速度 (Speed)] ドロップダウンリストからインターフェイスの速度を選択します。

ステップ 6 (任意) インターフェイスで [自動ネゴシエーション (Auto Negotiation)] がサポートされている場合は、[はい (Yes)] または [いいえ (No)] オプションボタンをクリックします。

ステップ 7 (任意) [Duplex] ドロップダウンリストからインターフェイスのデュプレックスを選択します。

ステップ 8 (任意) デバウンス時間 (ミリ秒) を明示的に設定します。0 から 15000 ミリ秒の値を入力します。

ステップ 9 [OK] をクリックします。

EtherChannel (ポートチャネル) の追加

EtherChannel (ポートチャネルとも呼ばれる) は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ (銅と光ファイバ) の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量 (1GB インターフェイスと 10GB インターフェイスなど) を混在させることはできません。リンク集約制御プロトコル (LACP) では、2 つのネットワークデバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データインターフェイスを次のように設定できます。

- アクティブ: LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブモードを使用する必要があります。
- オン: EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。



(注) モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データインターフェイスのみがアクティブモードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバーインターフェイスの両端

が正しいチャネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネルグループ内のスタンバイインターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止 (Suspended)] 状態 (Active LACP モードの場合) または [ダウン (Down)] 状態 (On LACP モードの場合) になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止 (Suspended)] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータインターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止 (Suspended)] または [ダウン (Down)] 状態に戻ります。

手順

-
- ステップ 1** [インターフェイス (Interfaces)] を選択して、[インターフェイス (Interfaces)] ページを開きます。
- [All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** インターフェイステーブルの上にある [ポートチャネルの追加 (Add Port Channel)] をクリックし、[ポートチャネルの追加 (Add Port Channel)] ダイアログボックスを開きます。
- ステップ 3** [ポートチャネル ID (Port Channel ID)] フィールドに、ポートチャネルの ID を入力します。有効な値は、1 ~ 47 です。
- クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、ポートチャネル 48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスを追加できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。
- ステップ 4** ポートチャネルを有効にするには、[有効化 (Enable)] チェックボックスをオンにします。ポートチャネルをディセーブルにするには、[Enable] チェックボックスをオフにします。
- ステップ 5** インターフェイスの [タイプ (Type)] を選択します。
- データ
 - 管理

・クラスター

- ステップ 6** ドロップダウンリストでメンバーインターフェイスに適した [管理速度 (Admin Speed)] を設定します。
- 指定した速度ではないメンバーインターフェイスを追加すると、ポートチャンネルに正常に参加できません。
- ステップ 7** データインターフェイスに対して、LACP ポート チャンネル [Mode]、[Active] または [On] を選択します。
- インターフェイスの場合、モードは常にアクティブです。
- ステップ 8** メンバーインターフェイスに適した [管理デュプレックス (Admin Duplex)] を設定します ([全二重 (Full Duplex)] または [半二重 (Half Duplex)])。
- 指定したデュプレックスのメンバーインターフェイスを追加すると、ポートチャンネルに正常に参加されます。
- ステップ 9** ポート チャンネルにインターフェイスを追加するには、[Available Interface] リストでインターフェイスを選択し、[Add Interface] をクリックしてそのインターフェイスを [Member ID] リストに移動します。
- 同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があり、このポートチャンネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ (銅と光ファイバ) の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量 (1GB インターフェイスと 10GB インターフェイスなど) を混在させることはできません。
- ヒント** 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、Ctrl キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、Shift キーを押しながら最後のインターフェイスをクリックして選択します。
- ステップ 10** ポートチャンネルからインターフェイスを削除するには、[Member ID] リストでそのインターフェイスの右側にある [Delete] ボタンをクリックします。
- ステップ 11** [OK] をクリックします。

FXOS : ASA クラスターの追加

単独の Firepower 9300 シャーシをシャーシ内クラスター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ーリングに追加することもできます。シャーシ間クラスターリングでは、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ーを追加したら、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 クラスターの作成

範囲をイメージバージョンに設定します。

クラスターは、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。導入を容易にするために、1つのシャーシにクラスターを導入し、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。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3つのすべてのモジュール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、クラスターは機能しません。

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。

クラスターを導入すると、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#>
    site-id <number>
    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。 [FXOS : インターフェイスの設定 \(20 ページ\)](#) 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** [追加 (Add)] > [クラスタ (Cluster)] をクリックし、次のパラメータを設定します。

- [必要な操作 (I want to:)] > [新しいクラスタの作成 (Create New Cluster)] を選択します。
- 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内部で使用します。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。
- [テンプレート (Template)] には、[Cisco 適応型セキュリティ アプライアンス (Cisco Adaptive Security Appliance)] を選択します。
- [Image Version] を選択します。
- [Instance Type] では、[Native] タイプのみがサポートされます。
- [OK] をクリックします。

[Provisioning - device name] ウィンドウが表示されます。

- ステップ 4** このクラスタに割り当てるインターフェイスを選択します。
デフォルトでは、すべての有効なインターフェイスが割り当てられています。マルチクラスタタイプのインターフェイスを定義した場合は、すべての選択を解除し、1 つのみ選択します。

ステップ 5 画面中央のデバイスアイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。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 6 [クラスター情報 (Cluster Information)] ページで、次の手順を実行します。

The screenshot shows the 'Cisco: Adaptive Security Appliance - Bootstrap Configuration' dialog box with the 'Cluster Information' tab selected. The 'Security Module' field contains 'Security Module-1,Security Module-2,Security Module-3'. Under 'Interface Information', 'Chassis ID' is 1, 'Site ID' is 1, 'Cluster Key' and 'Confirm Cluster Key' are masked with dots, 'Cluster Group Name' is 'asa_cluster', 'Management Interface' is 'Ethernet1/4', and 'CCL Subnet IP' is 'Eg:x.x.0.0'. Under 'DEFAULT', 'Address Type' is 'IPv4 only'. Under 'IPv4', 'Management IP Pool' is '10.89.5.10 - 10.89.5.22', 'Virtual IPv4 Address' is '10.89.5.25', 'Network Mask' is '255.255.255.192', and 'Network Gateway' is '10.89.5.1'. 'OK' and 'Cancel' buttons are at the bottom.

- 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。クラスター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、クラスター制御リンク 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) サイト間クラスタリングの場合、[サイト ID (Site ID)] フィールドに、このシャーシのサイト ID を 1 ~ 8 の範囲で入力します。

- c) [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。

- d) [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文字列である必要があります。

- e) [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、シャージ管理ポートとは別のものです。

- f) 管理インターフェイスの [アドレスタイプ (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。

- [管理IPプール (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。

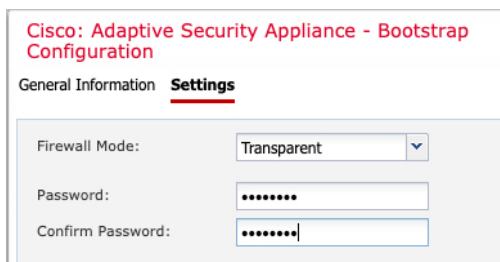
最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300の場合、すべてのモジュールスロットが埋まっていないとしても、シャージごとに3つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在の制御ユニットに属する仮想IPアドレス（メインクラスタIPアドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークのIPアドレスの1つをメインクラスタIPアドレス用に確保してください。IPv4アドレスとIPv6アドレス（どちらか一方も可）を使用できます。

- 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

- [仮想IPアドレス (Virtual IP address)] : 現在の制御ユニットの管理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、プールに含まれてはなりません。

ステップ 7 [Settings] ページで、以下を実行します。



Cisco: Adaptive Security Appliance - Bootstrap Configuration

General Information **Settings**

Firewall Mode:

Password:

Confirm Password:

- a) [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。

ルーテッドモードでは、Threat Defense はネットワーク内のルータホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。

ファイアウォールモードは初期展開時のみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

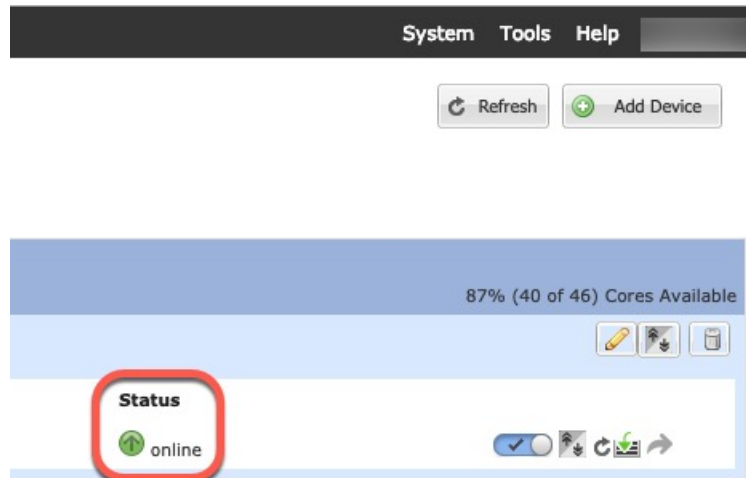
- b) 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

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 8 [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 9 [保存 (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 [ステータス (Status)] に [オンライン (Online)] と表示されている場合、残りのクラスタシャーシを追加するか、シャーシ内クラスタリングでアプリケーションのクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 10 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) Chassis Manager の最初のシャーシで、右上の [設定の表示 (Show Configuration)] 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 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) [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。
- d) **[OK]** をクリックします。
- 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。

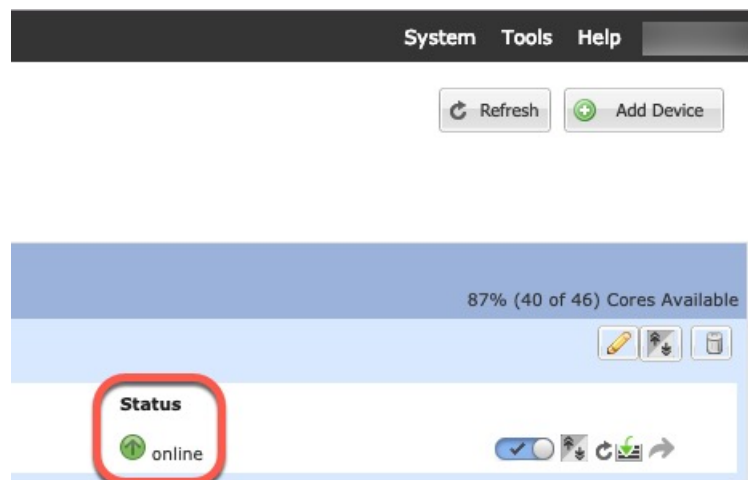
- **サイト ID (Site ID)** : 正しいサイト ID を入力します。

- **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。

[OK] をクリックします。

- g) [保存 (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。各クラスタメンバーの [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。各クラスタメンバーの論理デバイスの [ステータス (Status)] に [オンライン (Online)] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 11 制御ユニット 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。

クラスターメンバの追加

ASA クラスターメンバーを追加または置き換えます。




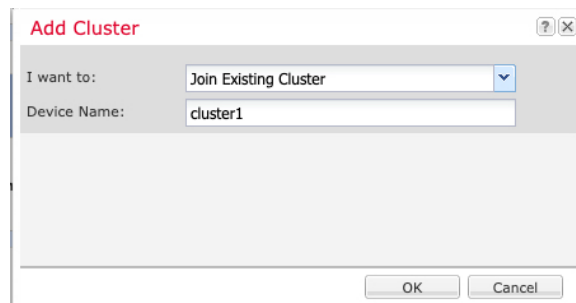
(注) この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

始める前に

- 既存のクラスターに、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ー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、最初のクラスターメンバの 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。追加のクラスター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** 既存のクラスタの Chassis Manager で、[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。
- ステップ 2** 右上の [設定を表示 (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 Chassis Manager に接続して、[追加 (Add)] > [クラスタ (Cluster)] をクリックします。

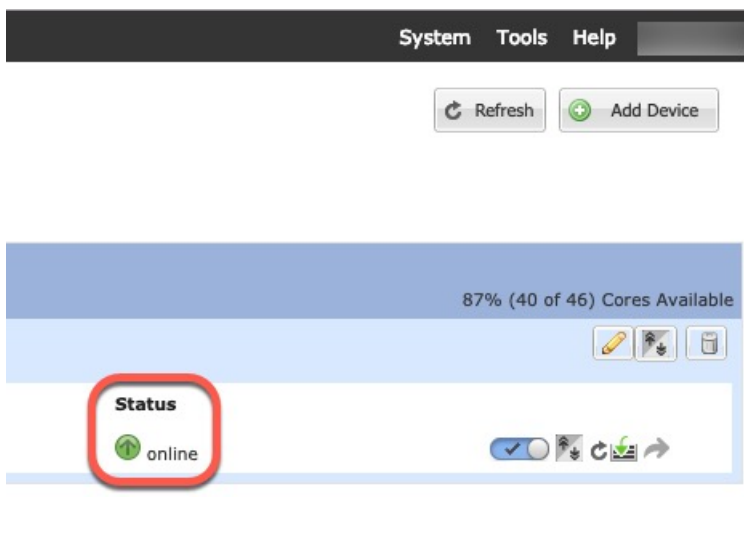


- ステップ 4** [I want to:] > [Join an Existing Cluster] を選択します。
- ステップ 5** [Device Name] に論理デバイスの名前を入力します。
- ステップ 6** [OK] をクリックします。
- ステップ 7** [クラスタ詳細のコピー (Copy Cluster Details)] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。
- ステップ 8** 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。
- [シャーシ ID (Chassis ID)] : 一意のシャーシ ID を入力します。
 - サイト ID (Site ID) : 正しいサイト 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。

[OK] をクリックします。

- ステップ 9** [保存 (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。各クラスタメンバーの [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。各クラスタメンバーの論理デバイスの [ステータス (Status)] に [オンライン (Online)] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



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、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが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。ASA の一般的な操作のコンフィギュレーションガイド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、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。ASA の一般的な操作のコンフィギュレーションガイド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 \(7 ページ\)](#)」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パンド 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、ポートチャン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せん。

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、スパンド 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 アドレスは現在の制御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、制御ユニットが変更された場合、新しい制御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。

- a) [OK] をクリックして変更内容を確定します。
- b) インターフェイスを割り当てます。
- c) ユーザー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。
- d) [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。ポイントツーポイント接続の場合、31 ビットのサブネットマスク (255.255.255.254) を指定できます。この場合、ネットワークまたはブロードキャストアドレス用の IP アドレスは予約されません。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。

- a) [Enable IPv6] チェックボックスをオンにします。
- b) [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。

- c) [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 [適用 (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、制御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

制御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、制御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。

- **[クラスタメンバの制限 (Cluster Member Limit)]** : クラスタメンバの最大数を 2 ~ 16 に設定します。デフォルトは 16 です。クラスタが最大の 16 ユニットよりも少ないことがわかっている場合は、実際の計画ユニット数を設定することを推奨します。最大ユニット数を設定すると、クラスタのリソース管理が向上します。たとえば、ポートアドレス変換 (PAT) を使用する場合は、制御ユニットは計画されたメンバー数にポートブロックを割り

当てることができ、使用する予定のない追加のユニット用にポートを予約する必要がなくなります。

- **Site Periodic GARP**—The ASA generates gratuitous ARP (GARP) packets to keep the switching infrastructure up to date: the highest priority member at each site periodically generates GARP traffic for the global MAC/IP addresses. 各スパンド EtherChannel のユニットと、サイト MAC および IP アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。GARP 間隔を 1 ~ 1000000 秒に設定します。デフォルトは 290 秒です。

クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の 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。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

- **[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。有効の場合は、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、制御ユニットからデータユニットに複製されます。
- **[Enable cluster load monitor]** : クラスタメンバのトラフィック負荷をモニターできるようになりました。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティモジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティモジュールがクラスタを離れると、そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ユニットでクラスタリングを手動で無効にすることを選択できます。

次の値を設定します。

- **[Time Interval]**: モニタリングメッセージ間の時間を、10 ~ 360 秒の範囲で設定します。デフォルトは 20 秒です。
- **[Number Of interval]**: ASA がデータを保持する間隔の数を 1 ~ 60 の範囲で設定します。デフォルトは 30 です。

トラフィック負荷を表示するには、**[Monitoring]>[ASA Cluster]>[Cluster Load-Monitoring]** を参照してください。

- **[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、ユニットハートビートステータスメッセージ間の間隔を .3 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ーに追加して、ASA またはスイッチのトポロジが変更される場合、クラスター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**])。クラスター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 のクラスター ユニットのクラスター制御リンクで他のユニットにハートビート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ハートビート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。

- [**Debounce Time**] : ASA がインターフェイスに障害が発生していると思われ、クラスターからユニットが削除されるまでのデバウンス時間を設定します。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスターからユニットを削除するまで指定されたミリ秒数待機します。ダウン状態から稼働状態に移行している EtherChannel の場合 (スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など)、デバウンス時間を長くすることで、他のクラスターユニットの方がポートのバンドルが速いという理由だけで、クラスターユニット上でインターフェイスがエラー表示されるのを防ぐことができます。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ~ 9 秒です。
- [**Replicate console output**] : データユニットから制御ユニットへのコンソール複製を有効にします。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、データユニットから制御ユニットにコンソールメッセージが送信されるので、モニターが必要になるのはクラスター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、制御ユニットからデータユニットに複製されます。
- **クラスターリング 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 (45 ページ)** を参照してください。
- [**Enable Director Localization for inter-DC cluster**] : データセンターのサイト間クラスターリングでパフォーマンスを向上させてラウンドトリップ時間の遅延を短縮するには、ディレクター ローカリゼーションを有効にします。通常、新しい接続はロード バランスされて、特定のサイト内のクラスター メンバーにより所有されます。ただし、ASA はディレクターの役割を任意のサイトでメンバーに割り当てます。ディレクター ローカリゼーションにより、追加のディレクター役割がイネーブルになります。これは、所有者と同じサイトに存在するローカル ディレクターと、任意のサイトに配置できるグローバル ディレクターです。所有者とディレクターを同じサイトに配置することで、パフォーマンスが向上します。また、元の所有者で障害が発生した場合、ローカル ディレクターは、同じサイトで新しい接続所有者を選択します。クラスター メンバーが別のサイトで所有されている接続のパケットを受信する場合は、グローバル ディレクターが使用されます。

- [Site Redundancy] : サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップオーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップオーナーが別のサイトから選択されます。ディレクタローカリゼーションとサイトの冗長性は別々の機能です。そのうちの1つまたは両方を設定することができます。
- [Enable config sync acceleration] : データユニットが制御ユニットと同じ構成の場合、構成の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。

(注) 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。 **show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。
- [Enable parallel configuration replicate] : データユニットと並行して設定変更が同期化されるように、制御ユニットを有効にします。そうしないと、同期が順番に実行され、多くの時間がかかることがあります。

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。データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。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。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。

たとえば、最大 MTU は 9184 バイトであるため、データインターフェイスの最大 MTU は 9084 になり、クラスタ制御リンクは 9184 に設定できます。

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パンド 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、制御ユニットからデータユニットに複製されます。

ステップ 5 (任意) (Firepower 9300 のみ) [Parallel Join of Units Per Chassis] 領域で、シャーシ内のセキュリティモジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されていることを確認できます。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。

- **num_of_units** : モジュールがクラスタに参加する前に準備する必要がある同じシャーシ内のモジュールの最小数 (1 ~ 3) を指定します。デフォルトは 1 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。たとえば、値を 3 に設定した場合、各モジュールは最大遅延時間の間、または 3 つすべてのモジュールの準備が完了するまで待機してからクラスタに参加します。3 つすべてのモジュールがほぼ同時にクラスタの参加を要求し、同時期にトラフィックの受信を開始します。
- [Maximum Join Delay] : 最大遅延時間を分単位 (0 ~ 30 分) で指定します。この時間が経過すると、モジュールは他のモジュールの準備が完了するのを待つことをやめて、クラスタに参加します。デフォルトは 0 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。最小単位を 1 に設定した場合、この値は 0 にする必要があります。最小単位を 2 または 3 に設定した場合、この値は 1 以上にする必要があります。このタイマーはモジュールごとのタイマーですが、最初のモジュールがクラスタに参加すると、その他すべてのモジュールのタイマーが終了し、残りのモジュールがクラスタに参加します。

たとえば、最小単位を 3、最大遅延を 5 分を設定します。モジュール 1 が起動すると、その 5 分間のタイマーが開始されます。モジュール 2 が 2 分後に起動すると、その 5 分間のタイマーが開始されます。モジュール 3 が 1 分後に起動し、すべてのモジュールが 4 分符号でクラスタに参加します。モジュールはタイマーが完了するまで待機しません。モジュール 3 が起動しない場合、モジュール 1 は 5 分間タイマーの終了時にクラスタに参加し、モジュール 2 も参加します。モジュール 2 はタイマーがまだ 2 分残っていますが、タイマーが完了するまで待機しません。

ステップ 6 [適用 (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 をモニターできます。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ーされています。

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ーから削除されます。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ー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、またはクラスター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。クラスター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ーされています。

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、vPC、StackWise、または StackWise Virtual 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（[設定（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASA クラスター（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、システム、またはクラスター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] : クラスター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、クラスター インターフェイスの場合は [Unlimited]、データ インターフェイスおよびシステムの場合は [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。クラスター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、クラスターインターフェイスの場合は [1]、データ インターフェイスおよびシステムの場合は [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 [適用 (Apply)] をクリックします。

クラスター TCP 複製の遅延の設定

TCP 接続のクラスター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、サーバー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спек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する必要があります。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。

Secure Firewall 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、「トロンボーニング」または「ヘアピンニング」と呼ばれます。

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 の間に存在する必要があります。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、または個々のノードに属しているフローは新しいオーナーには移動されません。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、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、最初のホップルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ 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、各クラスタノードのサイト ID を使用して新しいオーナーを特定します。
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、サーバー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

- Firepower 4100/9300 シャーシ スーパーバイザ上のシャーシのサイト ID を設定します。
- 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 クラスター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、クラスターに関連するサーバーまたはネットワークのみに EID を制限できます。たとえば、クラスターが 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、クラスターに関与している 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) **[追加 (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) インスペク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、作成したインスペク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) [追加 (Add)] をクリックします。
- c) [Service Policy] ページで、LISP インスペク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) サーバー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ー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 [適用 (Apply)] をクリックします。

分散型サイト間 VPN の設定

デフォルトでは、ASA クラスタは集中型サイト間 VPN モードを使用します。クラスタリングの拡張性を活用するために、分散型サイト間 VPN モードを有効にできます。このモードでは、

S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

分散型サイト間 VPN について

分散型 VPN 接続の役割

分散型 VPN モードで実行すると、次の役割がクラスタメンバーに割り当てられます。

- **アクティブセッションオーナー**：最初に接続を受信したユニット、またはバックアップセッションをアクティブセッションに移行したユニット。オーナーは、IKE と IPsec トンネル、およびそれらに関連付けられたすべてのトラフィックを含む、完全なセッションの状態を維持し、パケットを処理します。
- **バックアップセッションオーナー**：既存のアクティブセッションのバックアップセッションを処理しているユニット。選択されたバックアップ戦略によっては、アクティブセッションオーナーと同じシャーシ内のユニット、または別のシャーシ内のユニットである可能性があります。アクティブセッションオーナーに障害が発生すると、バックアップセッションオーナーがアクティブセッションオーナーになり、新しいバックアップセッションが別のユニットで確立されます。
- **フォワーダ**：VPN セッションに関連付けられたトラフィックが VPN セッションを所有していないユニットに送信された場合、そのユニットは VPN セッションを所有しているメンバーにトラフィックを転送するために Cluster Control Link (CCL) を使用します。
- **オーケストレータ**：オーケストレータ（常にクラスタの制御ユニット）は、アクティブセッションの再配布 (ASR) を実行する際に、移動するセッションとその移動先を計算する役割があります。オーケストレータは、オーナーメンバー X に N セッションをメンバー Y に移動する要求を送信します。メンバー X は、完了時に移動できたセッション数を指定して、オーケストレータに応答を返します。

分散型 VPN セッションの特性

分散型 S2S VPN セッションには、次の特性があります。それ以外の場合、VPN 接続は、ASA クラスタ上にない場合に通常動作するように動作します。

- VPN セッションは、セッションレベルでクラスタ全体に分散されます。つまり、1つの VPN 接続に対し、同じクラスタメンバーが IKE および IPsec トンネルと、そのすべてのトラフィックを処理します。VPN セッショントラフィックが、その VPN セッションを所有していないクラスタメンバーに送信された場合、トラフィックは VPN セッションを所有しているクラスタメンバーに転送されます。
- VPN セッションには、クラスタ全体で一意的なセッション ID があります。セッション ID を使用して、トラフィックが検証され、転送の決定が行われ、IKE ネゴシエーションが完了します。

- S2S VPN ハブアンドスポーク構成では、クライアントが ASA クラスタを介して接続する場合（ヘアピニングと呼ばれる）、流入するセッショントラフィックと流出するセッショントラフィックは、異なるクラスタメンバー上にある可能性があります。
- バックアップセッションを別のシャーシのセキュリティ モジュールに割り当てるように要求することができます。これにより、シャーシの障害を防止します。または、クラスタ内の任意のノードにバックアップセッションを割り当てることもできます。これはノードの障害のみを防止します。クラスタにシャーシが2つある場合は、リモートシャーシバックアップを強く推奨します。
- 分散型 S2S VPN モードでは IKEv2 IPsec S2S VPN のみがサポートされ、IKEv1 はサポートされていません。IKEv1 S2S は、集中型 VPN モードでサポートされています。
- 各セキュリティ モジュールは、6 つのメンバーにわたる最大約 36,000 のセッションに対し、最大 6,000 の VPN セッションをサポートします。クラスタメンバーでサポートされる実際のセッション数は、プラットフォームの容量、割り当てられたライセンス、コンテキストごとのリソース割り当てによって決まります。使用率が制限値に近い場合、各クラスタユニットで最大容量に達していても、セッションの作成が失敗することがあります。これは、アクティブセッションの割り当てが外部スイッチングによって決定され、バックアップセッションの割り当てが内部クラスタ アルゴリズムによって決定されるためです。顧客は、使用率を適宜調整し、不均一な配布に対するスペースを確保することが推奨されます。

クラスタ イベントの分散型 VPN の処理

表 2:

イベント	分散型 VPN
メンバーの障害	この障害が発生したメンバー上のすべてのアクティブセッションに対し、（別のメンバー上の）バックアップセッションがアクティブになり、バックアップセッションはバックアップ戦略に従って別のユニットに再割り当てされます。
シャーシ障害	<p>リモートシャーシバックアップ戦略が使用されている場合、障害が発生したシャーシ上のすべてのアクティブセッションに対し、（他のシャーシのメンバー上の）バックアップセッションがアクティブになります。ユニットが交換されると、これらの現在アクティブなセッションに対するバックアップセッションが、交換されたシャーシのメンバーに再割り当てされます。</p> <p>フラットバックアップ戦略が使用されている場合、アクティブセッションとバックアップセッションの両方が障害の発生したシャーシ上にあると、接続は切断されます。他のシャーシのメンバー上にバックアップセッションがあるアクティブセッションはすべて、これらのセッションにフォールバックします。新しいバックアップセッションは、残存しているシャーシ内の別のメンバーに割り当てられます。</p>

イベント	分散型 VPN
クラスタ メンバーの非アクティブ化	非アクティブになっているクラスタメンバー上のすべてのアクティブセッションに対し、（別のメンバー上の）バックアップセッションがアクティブになり、バックアップ戦略に従って別のユニットにバックアップセッションを再割り当てします。
クラスタ メンバーの参加	VPN クラスタモードが分散型に設定されていない場合、制御ユニットはモード変更を要求します。 VPN モードに互換性がある場合、または以前互換性があった場合、クラスタメンバーには、通常の操作の流れでアクティブセッションとバックアップセッションが割り当てられます。

サポートされていないインスペクション

次のタイプの検査は、分散型 S2S VPN モードではサポートされていないか、または無効になっています。

- CTIQBE
- DCERPC
- H323、H225、および RAS
- IPSec パススルー
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP (Skinny)
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

IPsec IKEv2 の変更

IKEv2 は、分散型 S2S VPN モードでは次のように変更されます。

- IP/ポート タプルの代わりに ID が使用されます。これにより、パケットの適切な転送の決定、および他のクラスタメンバー上にある可能性がある以前の接続のクリーンアップが可能になります。
- 単一の IKEv2 セッションを識別する (SPI) 識別子は、ローカルで生成されたランダムな 8 バイトの値で、クラスタ全体で一意です。SPI には、タイムスタンプとクラスタメンバー ID が埋め込まれています。IKE ネゴシエーションパケットの受信時に、タイムスタンプまたはクラスタメンバー ID のチェックに失敗すると、パケットがドロップされ、理由を示すメッセージが記録されます。
- NAT-T ネゴシエーションがクラスタメンバー間で分割されることによって失敗しないように IKEv2 処理が変更されました。新しい ASP 分類ドメインである *cluster_isakmp_redirect*、およびルールは、IKEv2 がインターフェイスで有効になっている場合に追加されます。

サポート モデル

分散型 VPN でサポートされる唯一のデバイスは、Firepower 9300 です。分散型 VPN では、最大 2 シャーシで、最大 6 モジュールをサポートしています。各シャーシで異なる数のセキュリティモジュールを設置することができますが、均等な分配を推奨しています。

サイト間クラスタリングはサポートされていません。

ファイアウォール モード

分散型 S2S VPN は、ルーテッドモードでのみサポートされています。

コンテキストモード

分散型 S2S VPN は、シングルコンテキストモードおよびマルチコンテキストモードの両方で動作します。ただし、マルチコンテキストモードでは、アクティブセッションの再配布はコンテキストレベルではなくシステムレベルで行われます。これにより、コンテキストに関連付けられたアクティブセッションが、異なるコンテキストに関連付けられたアクティブセッションを含むクラスタメンバーに移動し、予期せずに持続不可能な負荷が発生するのを防ぎます。

ハイアベイラビリティ

次の機能により、セキュリティモジュールまたはシャーシの単一障害に対する復元力が提供されます。

- 任意のシャーシ上のクラスタ内にある別のセキュリティモジュールにバックアップされた VPN セッションは、セキュリティモジュールの障害に耐性があります。
- 別のシャーシにバックアップされた VPN セッションは、シャーシの障害に耐性があります。
- 制御ユニットは、VPN S2S セッションを失うことなく変更できます。

クラスタが安定する前に追加の障害が発生すると、アクティブセッションとバックアップセッションの両方が障害の発生したユニットにある場合、接続が失われる可能性があります。

VPN クラスタ モードの無効化、クラスタ メンバーのリロード、およびその他の予想されるシャーシの変更など、メンバーが正常な状態でクラスタを離れるときにセッションが失われないように、すべての試行が行われます。これらのタイプの操作では、操作間でセッションのバックアップを再確立する時間がクラスタに与えられている限り、セッションは失われません。最後のクラスタメンバーで正常な終了がトリガーされた場合、既存のセッションが正常に切断されます。

ダイナミック PAT

分散型 VPN モードでは使用できません。

CMPv2

CMPv2 ID 証明書とキーペアはクラスタメンバー間で同期されます。ただし、クラスタ内の制御ユニットのみが CMPv2 証明書を自動的に更新してキーの再生成を行います。制御ユニットは更新時に、これらの新しい ID 証明書とキーをすべてのクラスタメンバーに同期させます。このようにして、クラスタ内のすべてのメンバーは CMPv2 証明書を利用して認証を行い、また、すべてのメンバーが制御ユニットを継承することができます。

分散型 S2S VPN の有効化

分散型サイト間VPNを有効にして、VPNセッションのクラスタリングの拡張性を活用します。



- (注) VPN モードを集中型と分散型の間で変更すると、既存のすべてのセッションが切断されます。バックアップ モードの変更は動的で、セッションは終了しません。

始める前に

- クラスタのすべてのメンバーにキャリア ライセンスが設定されている必要があります。
- S2S VPN 設定を行う必要があります。

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 [VPN Cluster Mode] 領域で、クラスタの [VPN Mode] を [Centralized] または [Distributed] から選択します。

ステップ 3 [Backup Distribution Mode] を [Flat] または [Remote-chassis] から選択します。

フラットバックアップモードでは、他のクラスタメンバーにスタンバイセッションが確立されます。これにより、ユーザーはブレード障害から保護されますが、シャーシ障害の保護は保証されません。

リモートシャーシバックアップモードでは、クラスタ内の別のシャーシのメンバーにスタンバイセッションが確立されます。これにより、ユーザーはブレード障害とシャーシ障害の両方から保護されます。

リモートシャーシが単一のシャーシ環境（意図的に構成されたものまたは障害の結果）で構成されている場合、別のシャーシが結合されるまでバックアップは作成されません。

分散型 S2S VPN セッションの再配布

アクティブセッションの再配布（ASR）では、アクティブな VPN セッションの負荷がクラスタメンバー全体に再配布されます。セッションの開始と終了の動的な性質のため、ASR は、すべてのクラスタメンバー間でセッションのバランスを取るためのベストエフォートです。繰り返される再配布アクションによってバランスが最適化されます。

再配布はいつでも実行でき、クラスタ内のトポロジ変更後に実行する必要があります。また、新しいメンバーがクラスタに参加した後に実行することを推奨します。再配布の目的は、安定した VPN クラスタを作成することです。安定した VPN クラスタには、ノード間でほぼ同数のアクティブセッションとバックアップセッションがあります。

セッションを移動するには、バックアップセッションがアクティブセッションになり、別のノードが新しいバックアップセッションをホストするように選択されます。移動セッションは、アクティブセッションのバックアップの場所と、その特定のバックアップノード上にすでに存在するアクティブセッションの数に依存します。何らかの理由でバックアップセッションノードがアクティブセッションをホストできない場合、元のノードはセッションのオーナーのままです。

マルチコンテキストモードでは、アクティブセッションの再配布は、個々のコンテキストレベルではなくシステムレベルで行われます。コンテキストレベルで実行されない理由は、あるコンテキスト内のアクティブセッションが別のコンテキスト内のより多くのアクティブセッションを含むメンバーに移動され、そのクラスタメンバーに多くの負荷がかかるためです。

始める前に

- 再配布アクティビティをモニターする場合は、システムログを有効にします。
- この手順は、クラスタの制御ユニットで実行する必要があります。

手順

ステップ 1 [Monitoring] > [ASA Cluster] > [ASA Cluster] > [Cluster Summary] > [VPN Cluster Summary] を選択して、アクティブセッションとバックアップセッションがクラスタ全体にどのように配布されているかを表示します。

再配布するセッションの数とクラスタの負荷に応じて、これには時間がかかることがあります。再配布アクティビティが発生すると、次のフレーズ（およびここには表示されていない他のシステムの詳細）を含む Syslog が提供されます。

Syslog フレーズ	注
VPN session redistribution started	制御ユニットのみ
Sent request to move <i>number</i> sessions from <i>orig-member-name</i> to <i>dest-member-name</i>	制御ユニットのみ
Failed to send session redistribution message to <i>member-name</i>	制御ユニットのみ
Received request to move <i>number</i> sessions from <i>orig-member-name</i> to <i>dest-member-name</i>	データユニットのみ
Moved <i>number</i> sessions to <i>member-name</i>	名前付きクラスタに移動したアクティブセッションの数。
Failed to receive session move response from <i>dest-member-name</i>	制御ユニットのみ
VPN session completed	制御ユニットのみ
Cluster topology change detected. VPN session redistribution aborted.	

ステップ 2 [Re-Distribute] をクリックします。

ステップ 3 [Monitoring] > [ASA Cluster] > [ASA Cluster] > [ClusterSummary] > [VPN Cluster Summary] を更新して、再配布アクティビティの結果を確認します。

再配布が成功し、実質的なシステムまたはセッションアクティビティがなかった場合、システムのバランスが取られ、このアクションは完了します。

それ以外の場合は、再配布プロセスを繰り返して、バランスの取れた安定したシステムを取得します。

FXOS : クラスタユニットの削除

ここでは、ユニットをクラスタから一時的に、または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、クラスタユニット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、手動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存在するか確認するには、Chassis Manager [論理デバイス (Logical Devices)] ページで、**show cluster info** コマンドを使用してアプリケーション内のクラスタステータスを確認します。



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

- 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、制御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。制御ユニットを削除するためにデータユニットでこのコマンドを入力した場合は、新しい制御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。

- アプリケーション インスタンスの無効化：Chassis Manager の [論理デバイス (Logical Devices)] ページで 有効なスライダ () をクリックします。無効なスライダ () 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：Chassis Manager の [セキュリティ モジュール/エンジン (Security Module/Engine)] ページで、[電源オフ (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：Chassis Manager の [概要 (Overview)] ページで、[シャットダウン (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。

- 論理デバイスの削除 : Chassis Manager の [論理デバイス (Logical Devices)] ページで、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ン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、そのノード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、そのノード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、そのノードがクラスタ 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、リロードしてもノード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 [構成 (Configuration)] > [デバイス管理 (Device Management)] > [高可用性とスケーラビリティ (High Availability and Scalability)] > [ASA クラスタ (ASA Cluster)] > [クラスタ設定 (Cluster Members)] 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、すべてのクラスター 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 [適用 (Apply)] をクリックします。

制御ユニットからのデータユニットの非アクティブ化

データノードを非アクティブにするには、次の手順を実行します。



- (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、クラスターリングを再度有効にします。管理インターフェイスは、そのノードがクラスター 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、リロードしてもノードがクラスター内でまだアクティブではない場合（クラスター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 [構成 (Configuration)] > [デバイス管理 (Device Management)] > [高可用性とスケーラビリティ (High Availability and Scalability)] > [ASA クラスター (ASA Cluster)] の順に選択します。

ステップ 2 削除するデータノードを選択して [削除 (Delete)] をクリックします。

データノードの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データノードを再追加できます。

ステップ 3 [適用 (Apply)] をクリックします。

クラスタへの再参加

ノード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ノードに 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、データノードのクラスタリングを制御ノードから再び有効にすることはできません。

- a) [構成 (Configuration)] > [デバイス管理 (Device Management)] > [高可用性とスケーラビリティ (High Availability and Scalability)] > [ASAクラスタ (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
```

制御ユニットの変更



注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニット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。制御ノードにするノード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制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、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** ドロップダウンリストから制御ノードにするデータノードを選択し、制御ノードにするボタンをクリックします。
 - ステップ 3** 制御ノードの変更を確認するように求められます。[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、制御ユニットで **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 サーバーにコピーするには、制御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 サーバーにコピーされます。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ー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ーできます。

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、制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

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、クラスター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、クラスター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。

- **[Monitoring] > [ASA Cluster] > [Cluster Load-Monitoring]**

ここでは、[Load Monitor-Information] ペインと [Load-Monitor Details] ペインについて説明します。ロードモニター情報には、最後のインターバルのクラスターメンバのトラフィック負荷、および設定された間隔の合計数の平均（デフォルトでは30）が表示されます。各間隔の各測定値を表示するには、[Load-Monitor Details] ペインを使用します。

クラスター制御リンクのモニタリング

クラスター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、クラスター制御リンクの [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。

クラスターのルーティングのモニタリング

クラスター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。

分散型 S2S VPN のモニタリング

VPN クラスター ステータ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] > [ASA Cluster] > [Cluster Summary] > [VPN Cluster Summary]**

クラスター全体のセッションの分布を表示し、セッションを再配布する機能を提供します。

- **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]**

クラスターの制御ユニットとデータユニットの両方が表示されます。詳細については、任意のメンバーをクリックしてください。

クラスターリングのロギングの設定

クラスター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]

クラスタ内の各ノードは、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ノードからのメッセージのように見せることができます。

分散型 S2S VPN のトラブルシューティング

分散型 VPN の通知

分散型 VPN を実行しているクラスタで、次のエラー状況が発生した場合、識別されたフレーズを含むメッセージが通知されます。

状況	通知
クラスタに参加しようとしているときに、既存のまたは参加しているクラスタデータユニットが分散型 VPN モードにない場合は、次のメッセージが通知されます。	New cluster member (<i>member-name</i>) rejected due to vpn mode mismatch. および 制御ノード (<i>control-name</i>) は、VPN モード機能に制御ノードの設定との互換性がないという理由でユニット (<i>unit-name</i>) からの登録要求を拒否します。
分散型 VPN のクラスタメンバーでライセンスが正しく設定されていない場合は、次のメッセージが通知されます。	ERROR: Control node requested cluster vpn-mode change to distributed. Unable to change mode due to missing Carrier License.
受信した IKEv2 パケットの SPI でタイムスタンプまたはメンバー ID が無効な場合は、次のメッセージが通知されます。	Expired SPI received または Corrupted SPI detected
クラスタがバックアップセッションを作成できない場合は、次のメッセージが通知されます。	Failed to create the backup for an IKEv2 session.
IKEv2 初期接点 (IC) 処理エラーの場合は、次のメッセージが通知されます。	IKEv2 Negotiation aborted due to ERROR: Stale backup session found on backup
再配布の問題の場合は、次のメッセージが通知されます。	Failed to send session redistribution message to <i>member-name</i> Failed to receive session move response from <i>member-name</i> (control node only)
セッションの再配布中にトポロジが変更された場合は、次のメッセージが通知されます。	Cluster topology change detected. VPN session redistribution aborted.

次のいずれかの状況が発生している可能性があります。

- **port-channel load-balance src-dst l4port** コマンドを使用して N7K スイッチにロードバランシング アルゴリズムとして L4port が設定されている場合、L2L VPN セッションはクラスター内のシャーシの 1 つにのみ配布されます。クラスターセッションの割り当ての例を次に示します。

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

L2L IKEv2 VPN は送信元ポートと宛先ポートの両方にポート 500 を使用するため、IKE パケットは N7K とシャーシ間に接続されたポート チャンネル内のリンクの 1 つにのみ送信されます。

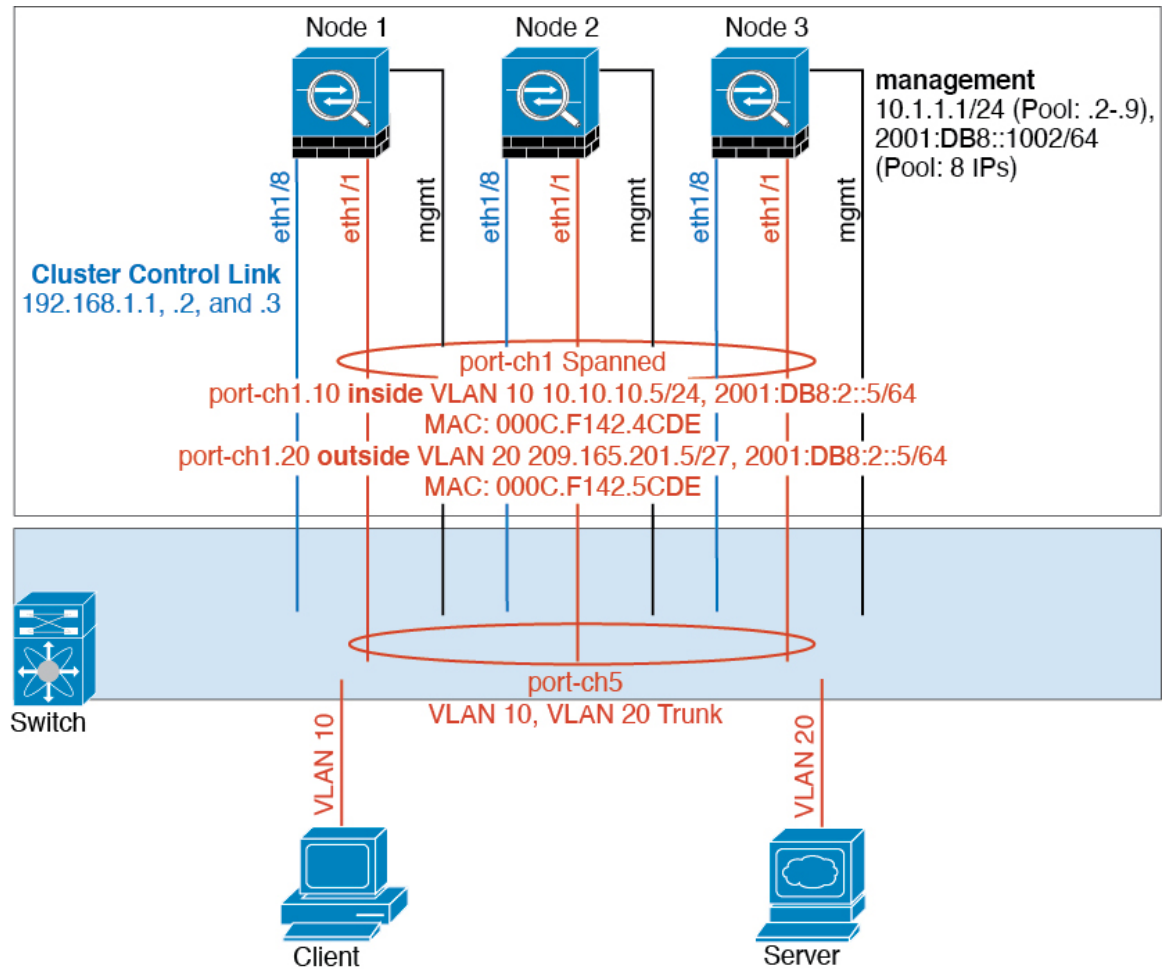
port-channel load-balance src-dst ip-l4port を使用して、N7K ロードバランシング アルゴリズムを IP および L4 ポートに変更します。その後、IKE パケットはすべてのリンクに送信されるので、両方の Firepower9300 シャーシに送信されます。

より即座に調整するには、ASA クラスターの制御ユニットで **cluster redistribute vpn-sessiondb** を実行することで、アクティブな VPN セッションを他のシャーシのクラスタメンバーに再配布できます。

ASA クラスタリングの例

これらの例には、一般的な導入が含まれます。

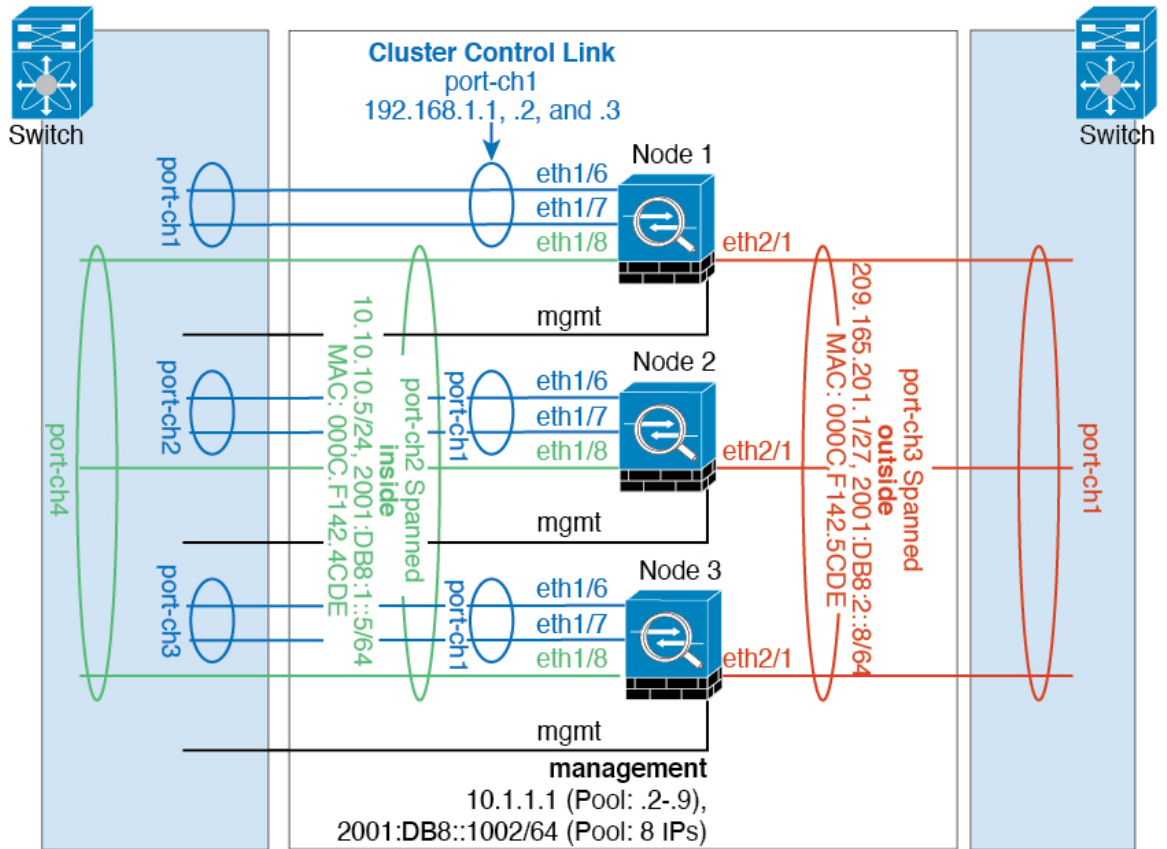
スティック上のファイアウォール



異なるセキュリティドメインからのデータトラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランッキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータリンクがグループ化されて 1 つの EtherChannel となります。ASA が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

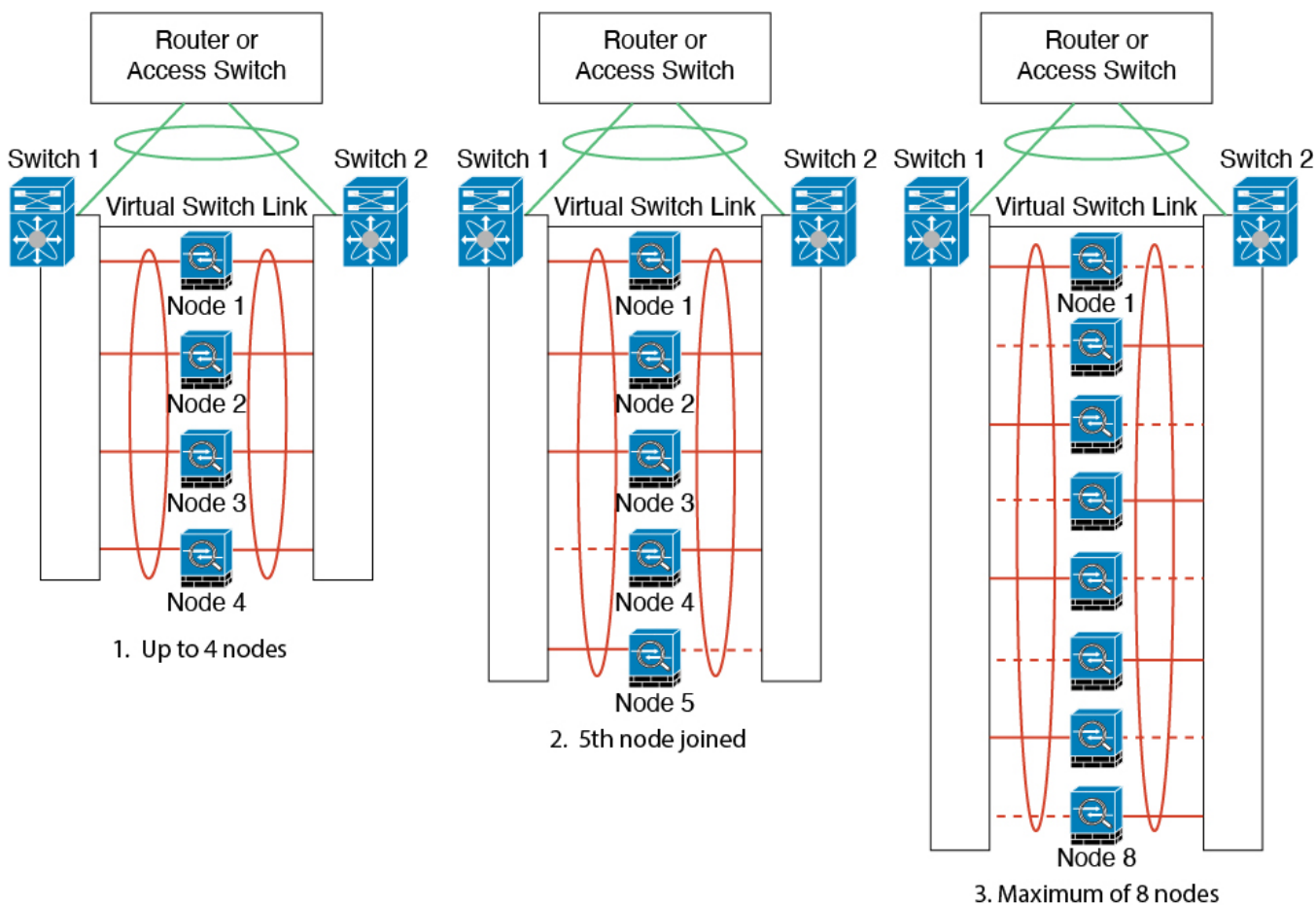
上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上に VLAN サブインターフェイスを作成することもできます。

スパンド EtherChannel とバックアップリンク（従来の 8 アクティブ/8 スタンバイ）

従来の EtherChannel のアクティブポートの最大数は、スイッチ側からの 8 に制限されます。8 ユニットから成るクラスターがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイモードにする必要があります。ASA は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。

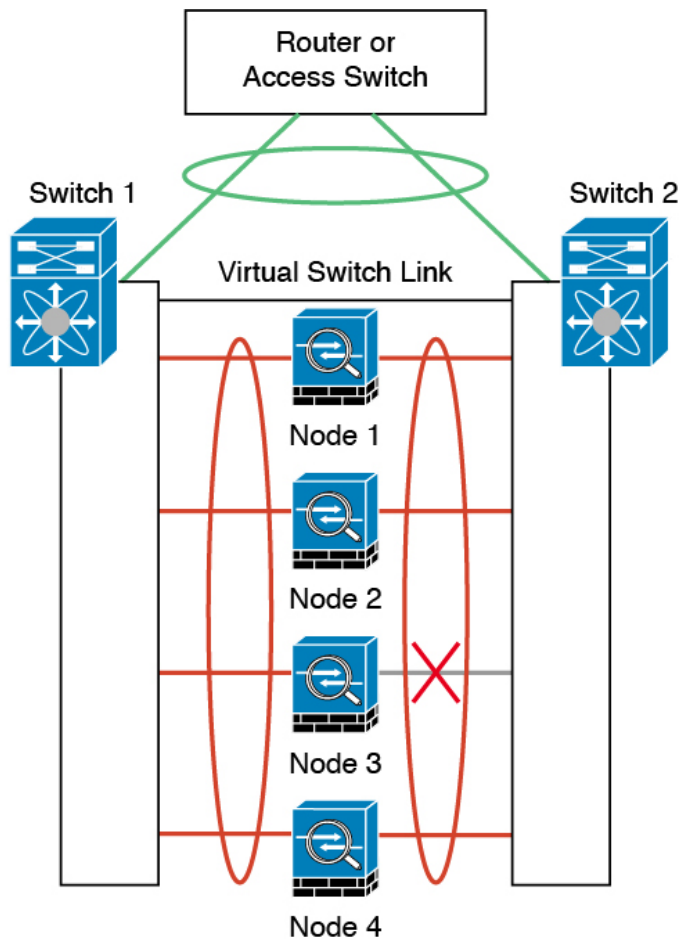
VSS、vPC、StackWise、または StackWise Virtual を使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASA では、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「制御」ポートとなり（たとえば Ethernet 1/1）、他方が「データ」ポートとなります（たとえば Ethernet 1/2）。ハードウェア接続の対称性を保証する必要があります。つまり、すべての制御リンクは 1 台のスイッチが終端となり、すべてのデータリンクは別のスイッチが終端となっている必要があります（冗長スイッチシステムが使用されている場合）。次の図は、クラ

スタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。

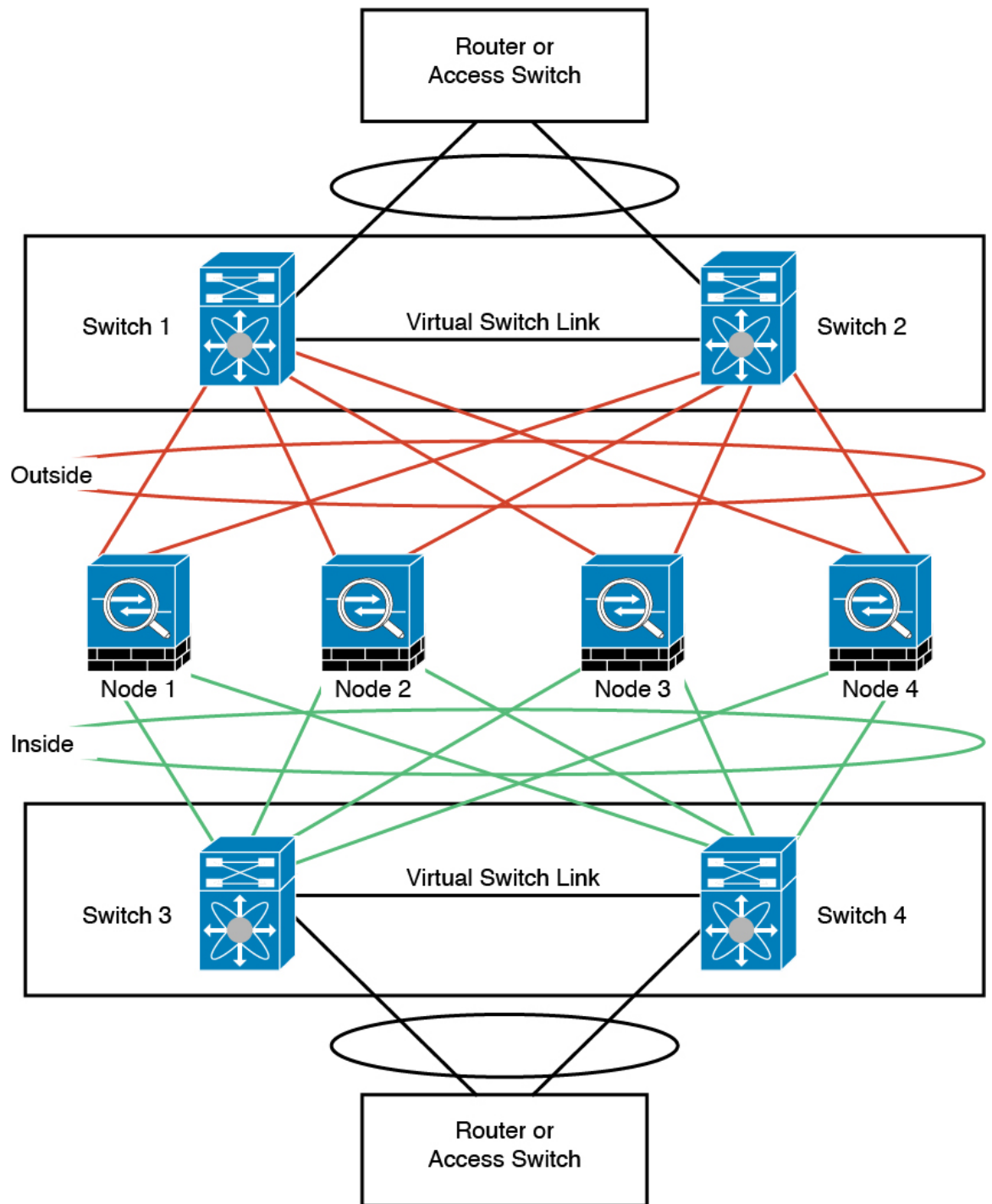


原則として、初めにチャンネル内のアクティブポート数を最大化し、そのうえで、アクティブな制御ポートとアクティブなデータポートの数のバランスを保ちます。5番目のユニットがクラスターに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

リンクまたはデバイスの障害が発生したときも、同じ原則で処理されます。その結果、ロードバランシングが理想的な状態にはならないこともあります。次の図は、4ユニットのクラスターを示しています。このユニットの1つで、単一リンク障害が発生しています。



ネットワーク内に複数の EtherChannel を設定することも考えられます。次の図では、EtherChannel が内部に 1 つ、外部に 1 つあります。ASA は、一方の EtherChannel で制御とデータの両方のリンクが障害状態になった場合にクラスターから削除されます。これは、その ASA がすでに内部ネットワークへの接続を失っているにもかかわらず、外部ネットワークからトラフィックを受信するのを防ぐためです。



ルーテッドモードサイト間クラスタリングの OTV 設定

スバンド EtherChannel を使用したルーテッドモードに対するサイト間クラスタリングの成功は、OTV の適切な設定とモニタリングによって異なります。OTV は、DCI 全体にパケットを転送することで、重要な役割を果たします。OTV は、転送テーブルに MAC アドレスを学習す

るときにのみ、DCI 全体にユニキャスト パケットを転送します。MAC アドレスが OTV 転送テーブルに学習されていない場合、ユニキャスト パケットはドロップされます。

OTV 設定の例

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
 10 permit any any
mac access-list HSRP_VMAC
 10 permit aaaa.1111.1234 0000.0000.0000 any
 20 permit aaaa.2222.1234 0000.0000.0000 any
 30 permit any aaaa.1111.1234 0000.0000.0000
 40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
 match mac address HSRP_VMAC
 action drop
vlan access-map Local 20
 match mac address ALL_MACs
 action forward
vlan filter Local vlan-list 3151-3152

//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
 10 deny aaaa.1111.1234 0000.0000.0000 any
 20 deny aaaa.2222.1234 0000.0000.0000 any
 30 deny any aaaa.1111.1234 0000.0000.0000
 40 deny any aaaa.2222.1234 0000.0000.0000
 50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
 match mac-list GMAC_DENY

interface Overlay1
 otv join-interface Ethernet8/1
 otv control-group 239.1.1.1
 otv data-group 232.1.1.0/28
 otv extend-vlan 202, 3151
 otv arp-nd timeout 60
 no shutdown

interface Ethernet8/1
 description uplink_to_OTV_cloud
 mtu 9198
 ip address 10.4.0.18/24
 ip igmp version 3
 no shutdown
```

```

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151

```

サイト障害のために必要な OTV フィルタの変更

サイトがダウンした場合は、グローバル MAC アドレスをそれ以上ブロックしなくて済むように、フィルタを OTV から削除する必要があります。必要ないいくつかの追加設定があります。

機能しているサイトで OTV スイッチ上の ASA グローバル MAC アドレスに対するスタティック エントリを追加する必要があります。このエントリによって、反対側の OTV はオーバーレイ インターフェイスにこれらのエントリを追加できます。サーバとクライアントに ASA 用の ARP エントリがすでにある場合（これは既存の接続の場合です）、ARP は再送信されないため、この手順が必要になります。したがって、OTV は転送テーブルに ASA グローバル MAC アドレスを学習する機会はありません。OTV には転送テーブル内にグローバル MAC アドレスがなく、OTV の設計ごとに OTV はオーバーレイ インターフェイスを介してユニキャスト パケットをフラディングしないので、ユニキャスト パケットはサーバからのグローバル MAC アドレスにドロップされ、既存の接続は切断されます。

```

//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site

```

他のサイトが復元した場合は、フィルタを再度追加して、OTV でこのスタティック エントリを削除する必要があります。グローバル MAC アドレスのオーバーレイ エントリをクリアする

には、両方の OTV でダイナミック MAC アドレス テーブルをクリアすることが非常に重要です。

MAC アドレス テーブルのクリア

サイトがダウンし、グローバル MAC アドレスへのスタティック エントリが OTV に追加される場合は、他の OTV がオーバーレイ インターフェイスのグローバル MAC アドレスを学習できるようにする必要があります。他のサイトが起動したら、これらのエントリをクリアする必要があります。OTV の転送テーブルにこれらのエントリがないことを確認するために、MAC アドレス テーブルを必ず消去してください。

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----+-----
G -      d867.d900.2e42 static   - F F sup-eth1(R)
O 202   885a.92f6.44a5 dynamic  - F F Overlay1
* 202   885a.92f6.4b8f dynamic  5 F F Eth8/3
O 3151  0050.5660.9412 dynamic  - F F Overlay1
* 3151  aaaa.1111.1234 dynamic  50 F F Eth8/3
```

OTV ARP キャッシュのモニタリング

OTV は、OTV インターフェイス全体で学習した IP アドレスに対するプロキシ ARP への ARP キャッシュを維持します。

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

サイト固有の MAC アドレスおよび IP アドレスを使用したスバンド EtherChannel ルーテッド モードの例

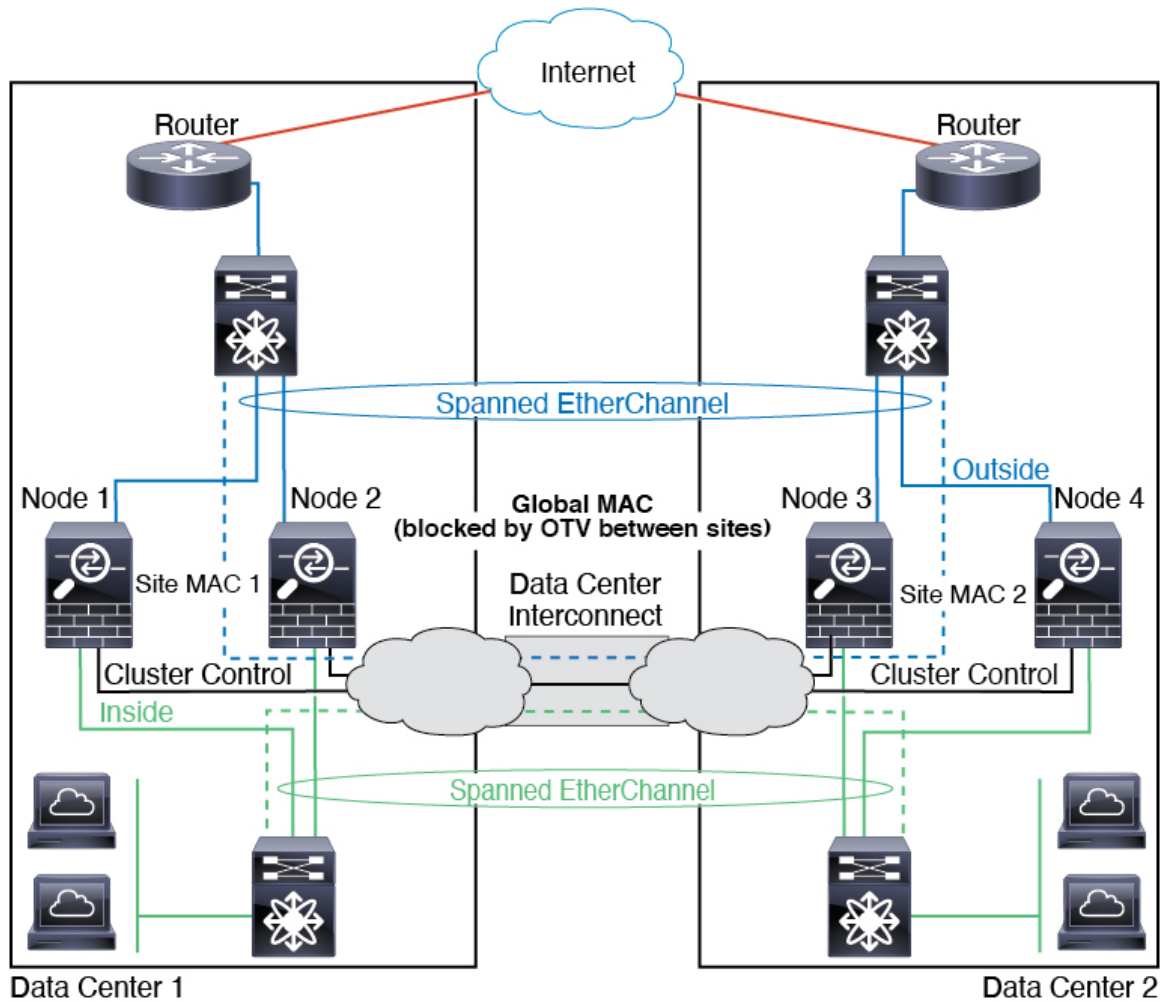
次の例では、各サイトのゲートウェイ ルータと内部ネットワーク間に配置された（イースト ウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタ メンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部両方のネットワークに対しスバンド EtherChannel を使用してローカルスイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

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) を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロックするフィルタを追加する必要があります。1 つのサイトのクラスタノードが到達不能になった場合、トラフィックが他のサイトのクラスタノードに送信されるようにフィルタを削除する必要があります。Vacl を使用して、グローバルの MAC アドレスのフィルタリングする必要があります。F3 シリーズラインカードが搭載された Nexus などの一部のスイッチでは、グローバル MAC アドレスからの ARP パケットをブロックするために ARP インスペクションも使用する必要があります。ARP インスペクションでは、ASA でサイトの MAC アドレスとサイトの IP アドレスの両方を設定する必要があります。サイトの MAC アドレスのみを設定する場合は必ず ARP インスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタノード間で共有されるグローバルな仮想 MAC は、パケットを受信するためだけに使用されます。発信パケットは、各 DC クラスタからのサイト固有の MAC アドレスを使用します。この機能により、スイッチが 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 アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。

この場合のシナリオは次のとおりです。

- クラスタから送信されるすべての出力パケットは、サイトの MAC アドレスを使用し、データセンターでローカライズされます。
- クラスタへのすべての入力パケットは、グローバル MAC アドレスを使用して送信されるため、両方のサイトにある任意のノードで受信できます。OTV のフィルタによって、データセンター内のトラフィックがローカライズされます。



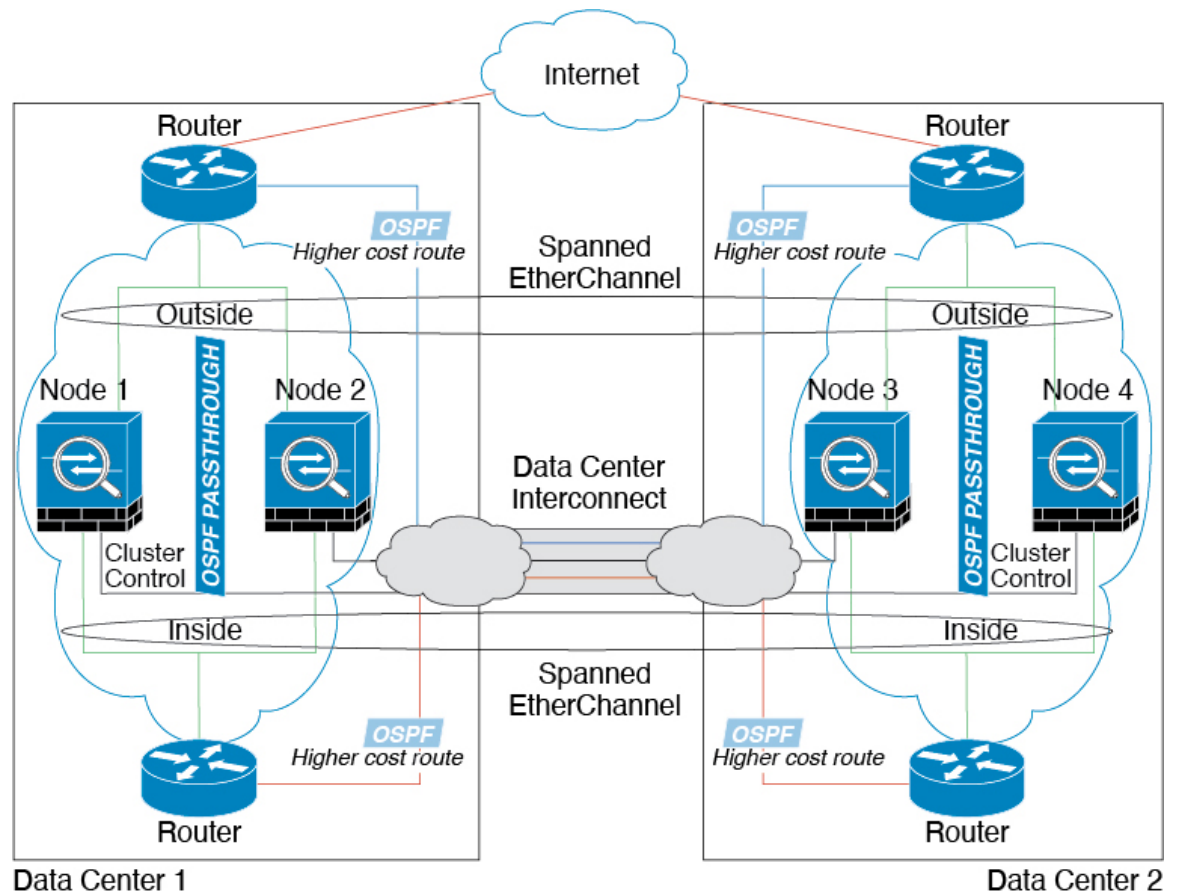
スパンド EtherChannel トランスペアレントモード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2つのデータセンターのそれぞれに2つのクラスタメンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部のスパンド EtherChannels を使用してローカルスイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャージにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コストルートを割り当てることにより、特定のサイトですべてのクラスタメンバーがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジグループを横断する必要があります。1つのサイトのすべてのクラスタメンバーに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタメンバーに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

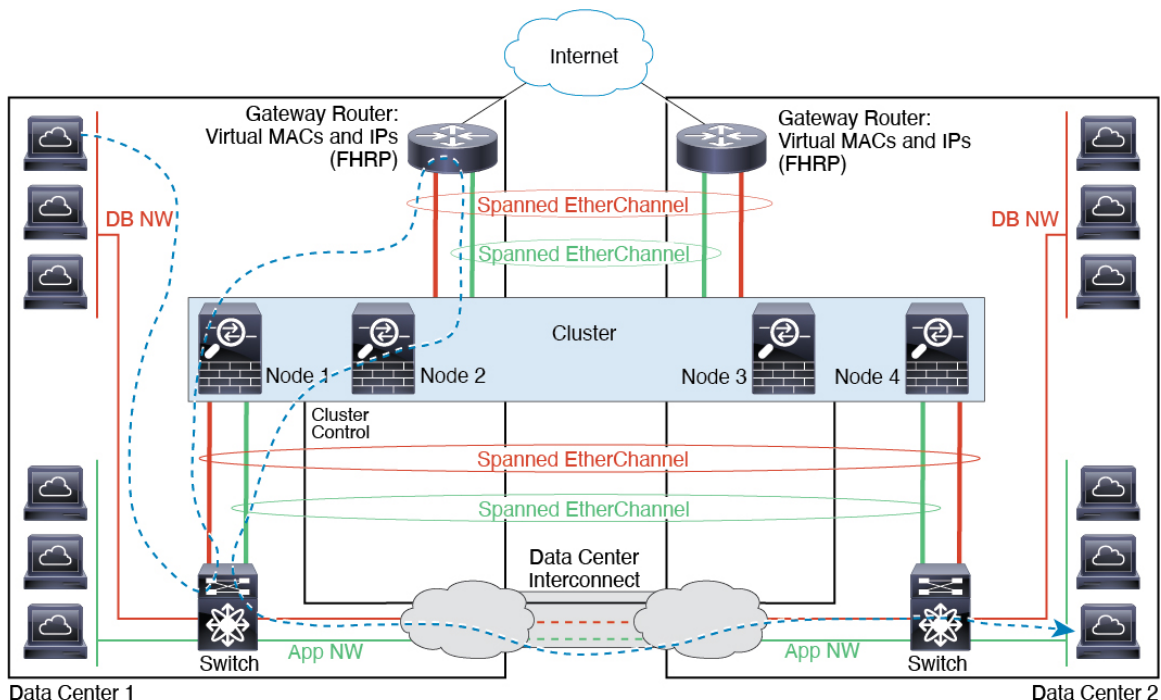
- サイト間 VSS、vPC、StackWise、StackWise Virtual : このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、冗長スイッチトラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCI が余分なトラフィックを処理できる場合、必要に応じて、各ノードを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS、vPC、StackWise、StackWise Virtual : スイッチの冗長性を高めるには、各サイトに 2 つの異なる冗長スイッチペアをインストールできます。この場合、クラスタノードは、両方のローカルスイッチだけに接続されたデータセンター 1 のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター 2 のシャーシではスバンド EtherChannel を使用しますが、スバンド EtherChannel は基本的に「分離」しています。各ローカル冗長スイッチは、スバンド EtherChannel をサイトローカルの EtherChannel として認識します。



スパンド EtherChannel トランスペアレントモード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイルータと2つの内部ネットワーク（アプリケーションネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタメンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部のアプリケーションネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカルスイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレスと IP アドレスを提供します。MAC アドレスの予期せぬフラッピングを避けるため、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト1のゲートウェイがサイト2のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト2に到達しようとして、問題が発生する可能性があります。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）を使用してサイト間に拡張されます。トラフィックがゲートウェイルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1つのサイトのゲートウェイルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



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。

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、一部の機能は制御ノード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

次の各機能は、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。

- 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)
- 仮想トンネルインターフェイス (VTI)
- 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
- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされていません。
- VPN ロード バランシング
- フェールオーバー
- 統合ルーティングおよびブリッジング
- デッド接続検出 (DCD)
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード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ノードから制御ノードに転送されます。

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、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノード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、新しい制御ノード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
- ESMTP
- IM
- NetBIOS
- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- スタティック ルート モニタリング
- 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 VPN

集中モードでは、VPN 接続はクラスタの制御ノード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、分散 VPN モードでも展開できます。この場合、S2S IKEv2 VPN 接続がノード間で分散されます。

- 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 転送は 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）
- ダイナミック ルーティング

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制御ノードではなく、各 ASA ノードに適用されます。

- 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、ポリシーは各ノードに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 ノード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、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 : 脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。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ノード間でロードバランシングされ、1つのノードですべてのトラフィックを確認できないためです。
- 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ノード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、各受信ノード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。各ノードは、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。認証と許可は、クラスタリング制御ノード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データノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザーおよびユーザーに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザー認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウントING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ため、フローに対するアカウントINGが設定されている場合、そのフローを所有するクラスタノードがアカウントING開始と停止のメッセージを AAA サーバーに送信します。

接続設定

接続制限は、クラスタ全体に適用されます（[構成（Configuration）]>[ファイアウォール（Firewall）]>[サービスポリシー（Service Policy）] ページを参照）。各ノードには、ブロー

ドキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

FTP とクラスタリング

- FTPD 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ーによって所有されている場合は、D 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 を使用する場合、制御チャンネルのフローは制御ノードに集中されません。

ICMP インспекション

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインспекションが有効かどうかによって異なります。ICMP インспекションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インспекションを使用する場合、ICMP フローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットのディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

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、制御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、各データユニット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。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA 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。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ため、クラスタ制御リンクに大量のトラフィックが発生します。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できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

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。

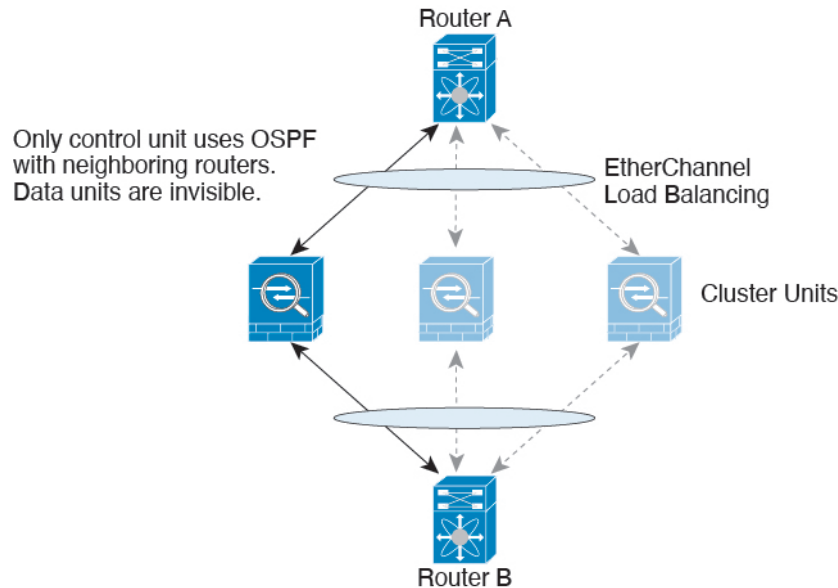
- ポート ブロック 割り当てによる PAT：この機能については、次のガイドラインを参照してください。
 - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
 - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
 - PAT プールが完全に新しい IP 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ノード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。
 - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。
- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- 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。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。

- 制御ノードによって管理されるダイナミック NAT xlate : 制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内がない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlates : 接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- 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 の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノード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設定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
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクションコミットモデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

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制御ユニット上だけで実行されます。ルートは制御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データユニットに到着した場合は、制御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



データユニットが制御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、制御ユニットからデータユニットに同期されません。制御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 アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノード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、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノード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 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、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングで SNMPv3 を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3 ユーザーは新しいノードに複製されません。SNMPv3 ユーザーは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。

STUN とクラスタリング

ピンホールが複製される時、STUN インスペク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 はノード間で複製されません。STUN 要求の受信後にノードに障害が発生し、別のノードが 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** : クラスターの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノード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、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。
- **NetFlow** : クラスターの各ノードは自身の 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

制御ノードだけがセキュリティグループタグ (SGT) 情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

Secure Firewall eXtensible オペレーティングシステム (FXOS) シャーシ上の VPN とクラスタリング

ASA FXOS クラスターは、S2S VPN に対する相互排他的な 2 つのモード (集中型または分散型) のいずれかをサポートしています。

- **集中型 VPN モード**。デフォルトモードです。集中モードでは、VPN 接続はクラスターの制御ユニットとのみ確立されます。

VPN 機能を使用できるのは制御ユニットだけであり、クラスターの高可用性機能は活用されません。制御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 接続されたユーザーにとってはサービスの中断となります。新しい制御ユニット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、接続が自動的に制御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。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスターのメンバー全体に分散され、拡張性が提供されます。クラスターのメンバー全体に VPN 接続を分散することで、クラスターの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。



- (注) 集中型 VPN クラスタリングモードは、S2S IKEv1 と S2S IKEv2 をサポートしています。
- 分散型 VPN クラスタリングモードは、S2S IKEv2 のみをサポートしています。
- 分散型 VPN クラスタリングモードは、Firepower 9300 でのみサポートされています。
- リモートアクセス VPN は、集中型または分散型の VPN クラスタリングモードではサポートされていません。

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ーに結合すると、期待できる合計クラスターパフォーマンスは、最大合計スループットの約 80% になります。

たとえば、TCP スループットについては、3 つの SM-40 モジュールを備えた Firepower 9300 が処理できる実際のファイアウォールトラフィックは、単独動作時は約 135 Gbps となります。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。

制御ユニットの選定

クラスターのメンバーは、クラスター制御リンクを介して通信して制御ユニットを選定します。方法は次のとおりです。

1. クラスターを展開すると、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ー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、そのユニットが制御ユニットになります。



- (注) 最高のプライオリティを持つユニットが複数ある場合は、クラスターユニット名、次にシリアル番号を使用して制御ユニットが決定されます。

4. 後からクラスター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制御ユニットになることはありません。既存の制御ユニットは常に制御ユニットのままです。ただし、制御ユニットが応答を停止すると、その時点で新しい制御ユニットが選定されます。

5. 「スプリットブレイン」シナリオで一時的に複数の制御ユニットが存在する場合、優先順位が最も高いユニットが制御ユニットの役割を保持し、他のユニットはデータユニットの役割に戻ります。



(注) 特定のユニットを手動で強制的に制御ユニットにすることができます。中央集中型機能については、制御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、新しい制御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ーリング

シャーシ アプリケーションのヘルス モニター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。

装置のヘルス モニターリング

各ユニットは、クラスタ制御リンクを介してブロードキャストキープアライブハートビートパケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからキープアライブハートビートパケット、またはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2つのクラスタロケーション間でルータに障害が発生した場合、ロケーション1の元の制御ノードは、ロケーション2のデータノードをクラスタから削除します。一方、ロケーション2のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。詳細については、[制御ユニットの選定 \(84 ページ\)](#) を参照してください。

インターフェイス モニターリング

各ノードは、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監視し、ステータスの変更を制御ノードに報告します。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。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニターして 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。ヘルスマ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ーされます (EtherChannel インターフェイスのメイン EtherChannel を含む)。アップ状態の名前付きインターフェイスのみモニターできます。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 (最小ポートバンドル設定により異なる)。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。

特定のノードで監視対象のインターフェイスに障害が発生し、その他のノードでそのインターフェイスがアクティブになっている場合、そのノードはクラスタから削除されます。ASA によってノードがクラスタから削除されるまでの時間は、そのノードが確立済みのメンバーであるか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、ノード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。確立済みのメンバーの場合は、500 ミリ秒後にノードが削除されます。

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マニタリングは 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。いったん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 秒ごとにモニターします。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

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステータス情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、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) のメンバーが制御ノードになります。

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、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、そのノードがクラスタ 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、クラスタでノード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無効になります。さらに設定を行う場合は、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、クラスタに再参加するための方法は、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。ユニットは5分、10分、および20分の間隔でクラスタに自動的に再参加を試行します。この動作は設定可能です。

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 3: 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
アップタイム	対応	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	対応	—
MAC アドレス テーブル	対応	—
ユーザ アイデンティティ	対応	AAA ルール (uauth) が含まれます。
IPv6 ネイバー データベース	対応	—
ダイナミック ルーティング	対応	—
SNMP エンジン ID	なし	—
Firepower 4100/9300 の分散型 VPN (サイト間)	対応	バックアップセッションがアクティブセッションになると、新しいバックアップセッションが作成されます。

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ノードにロードバランシングできます。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ノード。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、新しいノードが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ノード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ノード。障害が発生した場合、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、(ロードバランシングに基づき) その接続からのパケットを受信する最初のノード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、そのノードが新しいオーナーになります。

ディレクタ (下記参照) がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーが自分をディレクタとして選択した場合は、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 つのクラスターノードを搭載できる Firepower 9300 のクラスターリングでは、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。

サイト間クラスターリングのディレクターローカリゼーションを有効にすると、ローカルバックアップとグローバルバックアップの 2 つのバックアップオーナー権限があります。オーナーは、常に同じサイトのローカルバックアップをオーナー自身として選択します（サイト ID に基づいて）。グローバルバックアップはどのサイトにも配置でき、ローカルバックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステータスを送信します。

サイトの冗長性が有効になっており、バックアップオーナーがオーナーと同じサイトに配置されている場合は、サイトの障害からフローを保護するために、別のサイトから追加のバックアップオーナーが選択されます。シャーシバックアップとサイトバックアップは独立しているため、フローにはシャーシバックアップとサイトバックアップの両方が含まれている場合があります。

- **ディレクター**：フォワーダからのオーナーバックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、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ーを選択し、新しい接続を登録するためにそのディレクターにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクターに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクターは 1 つだけです。ディレクターが失敗すると、オーナーは新しいディレクターを選択します。

ディレクターがオーナーと同じノードでない限り、ディレクター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ー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。

サイト間クラスターリングのディレクターローカリゼーションを有効にすると、ローカルディレクターとグローバルディレクターの 2 つのディレクター権限が区別されます。オーナーは、同一サイト（Site Id に基づき）のローカルディレクターとして、常にオーナー自身を選択します。グローバルディレクターはどのサイトにも配置でき、ローカルディレクターと同一ノードとすることもできます。最初のオーナーに障害が発生すると、ローカルディレクターは、同じサイトの新しい接続オーナーを選択します。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子で、宛先ポートは 0 です。
 - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
 - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。
- **フォワーダ**：パケットをオーナーに転送するノード。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ーにオーナーを問い合わせるから、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。ディレクターは、フォワーダにもなることができます。ディレクターローカリゼーションを有効にすると、フォワーダは常にロー

カルディレクタに問い合わせを行います。フォワーダがグローバルディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタメンバーが受信する場合などです。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 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無効にした場合は、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。



(注) クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを決定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。これが既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続の所有者はすべてのフラグメントを再構築します。

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ノードです。
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：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。
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 を使用するため、それらの接続は常に制御ノードによって所有されています。

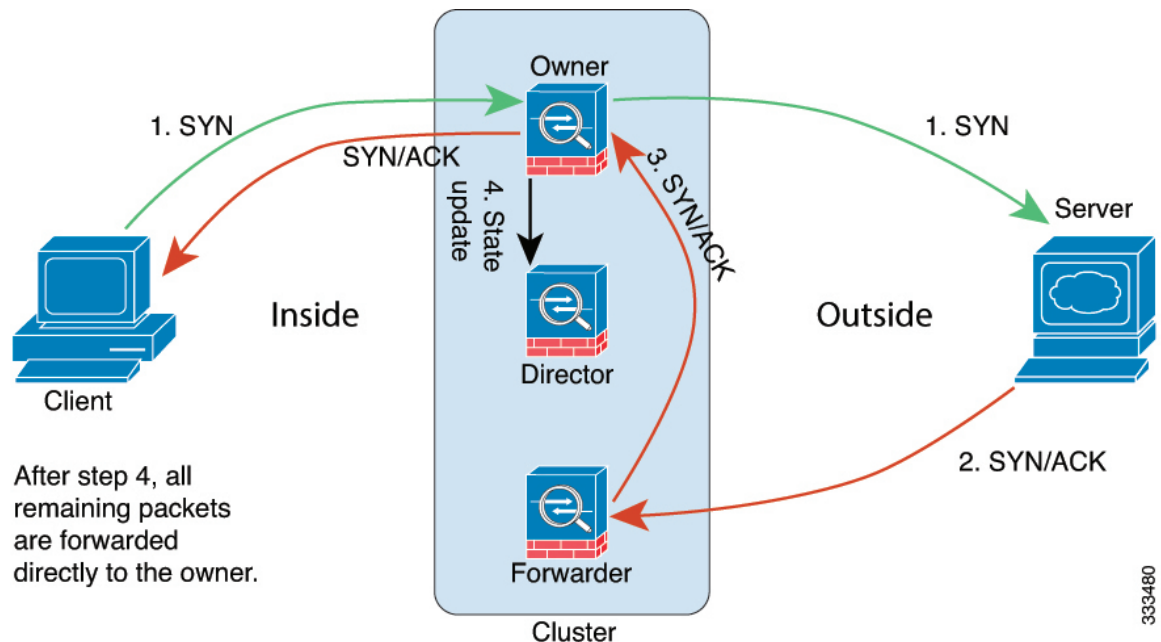
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

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ーのノードに送信される場合は、そのノード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ノードに到着した場合は、そのパケットはクラスター制御リンクを介してオーナーノードに転送されます。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP の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。



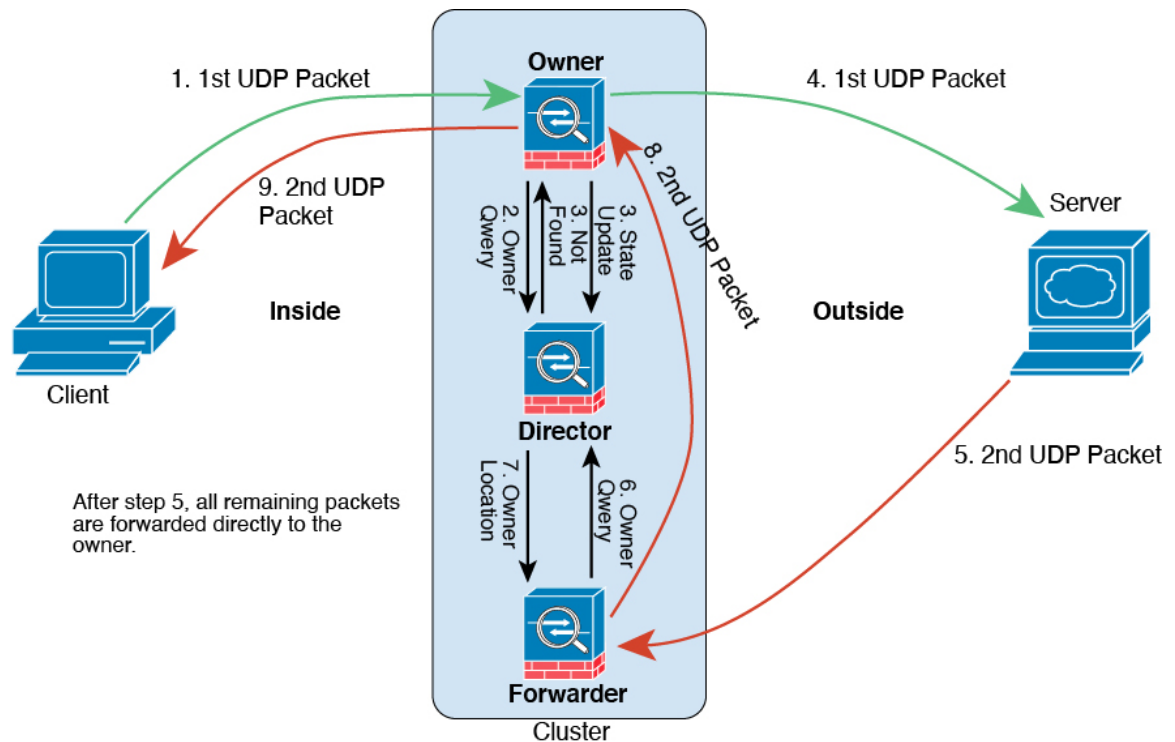
1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロードバランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オー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 状態情報を記録します。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ノードに配信された場合、そのノードはディレクタに問い合わせ、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。

ICMP および UDP の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. 図 2: ICMP および UDP データフロー



UDP パケットがクライアントから発信され、1つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。

4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバーにパケットを転送します。
5. 2 番目の UDP パケットはサーバーから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする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。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

Firepower 4100/9300 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
バイアス言語の除去	9.19(1)	<p>「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。</p> <p>新規/変更されたコマンド：cluster control-node、enable as-data-node、prompt、show cluster history、show cluster info</p>
Firepower 4100/9300 でのクラスタリング用の PAT ポートブロック割り当ての改善	9.16(1)	<p>PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するために、cluster-member-limit コマンドを使用して、クラスタ内に配置する予定の最大ノードを設定できます。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。</p> <p>新規/変更された画面：[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Cluster Member Limit] フィールド</p>
show cluster history コマンドの改善	9.16(1)	<p>show cluster history コマンドの出力が追加されました。</p> <p>新規/変更されたコマンド：show cluster history brief、show cluster history latest、show cluster history reverse、show cluster history time</p>

機能名	バージョン	機能情報
データユニットとの設定の並列同期	9.14(1)	<p>制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。</p> <p>新規/変更された画面：[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Enable parallel configuration replicate] チェックボックス</p>
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 show cluster history	9.14(1)	<p>クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 show cluster history コマンドに追加されました。</p> <p>新規/変更されたコマンド： show cluster history</p> <p>新規/変更された画面：なし。</p>
デッド接続検出 (DCD) の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	<p>デッド接続検出 (DCD) を有効にした場合は、 show conn detail コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。 show conn の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。</p> <p>変更された画面はありません。</p>
クラスタのトラフィック負荷のモニター	9.13(1)	<p>クラスタメンバのトラフィック負荷をモニターできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。</p> <p>新しい/変更された画面：</p> <ul style="list-style-type: none"> • [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Enable Cluster Load Monitor] チェックボックス • [Monitoring] > [ASA Cluster] > [Cluster Load-Monitoring]

機能名	バージョン	機能情報
クラスタ結合の高速化	9.13(1)	<p>データユニットが制御ユニットと同じ設定の場合、設定の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。</p> <p>(注) 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。 show cluster info unit-join-acceleration incompatible-config を使用して、互換性のない設定を表示します。</p> <p>新規/変更された画面 : [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Enable config sync acceleration] チェックボックス</p>
サイトごとのクラスタリング用 Gratuitous ARP	9.12(1)	<p>ASA では、Gratuitous ARP (GARP) パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の 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。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチング インフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。</p> <p>新規/変更された画面 : [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Site Periodic GARP] フィールド</p>
Firepower 9300 シャーシごとのユニットの平行クラスタ参加	9.10(1)	<p>Firepower 9300 の場合、この機能により、シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されるようになります。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。</p> <p>新規/変更された画面 :</p> <p>[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]</p> <p>新規/変更されたオプション : [Parallel Join of Units Per Chassis] エリア</p>

機能名	バージョン	機能情報
Firepower 4100/9300 のクラスター制御リンクのカスタマイズ可能な IP アドレス	9.10(1)	<p>クラスター制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスターを展開するときにネットワークを設定できます。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ー制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック (127.0.0.0/8) およびマルチキャスト (224.0.0.0/4) アドレスを除き、FXOS にクラスター制御リンクのカスタム /16 サブネットを作成できるようになりました。</p> <p>新規/変更された Chassis Manager 画面： [Logical Devices] > [Add Device] > [Cluster Information]</p> <p>新規/変更されたオプション：[CCL Subnet IP] フィールド</p>
クラスターインターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。	9.10(1)	<p>インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスターからユニットを削除するまで health-check monitor-interface debounce-time コマンドまたは ASDM [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスターユニットの方がポートのバンドルが速いという理由だけで、クラスターユニット上でインターフェイスがエラー表示されるのを防ぐことができます。</p> <p>変更された画面はありません。</p>
内部障害発生後に自動的にクラスターに再参加する	9.9(2)	<p>以前は、多くのエラー状態によりクラスターユニットがクラスターから削除されていました。この問題を解決した後、手動でクラスターに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスターに自動的に再参加を試行します。これらの値は設定できます。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。</p> <p>新規または変更された画面：[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Auto Rejoin]</p>
クラスターの信頼性の高いトランスポートプロトコルメッセージのトランスポートに関連する統計情報の表示	9.9(2)	<p>ユニットごとのクラスターの信頼性の高いトランスポートバッファ使用率を確認して、バッファがコントロールプレーンでいっぱいになったときにパケットドロップの問題を特定できるようになりました。</p> <p>新規または変更されたコマンド：show cluster info transport cp detail</p>

機能名	バージョン	機能情報
動作と一致する cluster remove unit コマンドの動作 no enable	9.9(1)	<p>cluster remove unit コマンドは、no enable コマンドと同様に、クラスタリングまたはリロードを手動で再度有効にするまで、クラスタからユニットを削除するようになりました。以前は、FXOS からブートストラップ設定を再展開すると、クラスタリングが再度有効になりました。無効化されたステータスは、ブートストラップ設定の再展開の場合でも維持されるようになりました。ただし、ASA をリロードすると、クラスタリングが再度有効になります。</p> <p>新規または変更された画面 : [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]</p>
シャーシのシャーシヘルスチェックの障害検出の向上	9.9(1)	<p>シャーシヘルスチェックの保留時間をより低い値 (100 ms) に設定できるようになりました。以前の最小値は 300 ms でした。最小の結合時間 (<i>interval x retry-count</i>) は、600 ミリ秒未満にすることはできないことに注意してください。</p> <p>新規または変更されたコマンド : app-agent heartbeat interval</p> <p>ASDM サポートはありません。</p>
クラスタリングのサイト間冗長性	9.9(1)	<p>サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。</p> <p>新規または変更された画面 : [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]</p>

機能名	バージョン	機能情報
Firepower 9300 上のクラスターリングによる分散型サイト間 VPN	9.9(1)	<p>Firepower 9300 上の ASA クラスターは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ユニットだけでなく、ASA クラスターのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスター（合計 6 つのクラスターメンバー）上で動作し、各モジュールは最大約 36,000 のアクティブセッション（合計 72,000）に対し、最大 6,000 のアクティブセッション（合計 12,000）をサポートします。</p> <p>新規または変更された画面：</p> <p>[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]</p> <p>[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]</p> <p>[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]</p> <p>[Wizards] > [Site-to-Site]</p> <p>[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]</p> <p>[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]</p> <p>[Monitoring] > [ASA Cluster] > [ASA Cluster] > [System Resource Graphs] > [CPU/Memory]</p> <p>[Monitoring] > [Logging] > [Real-Time Log Viewer]</p>
クラスターユニットヘルスチェック障害検出の改善	9.8(1)	<p>ユニットヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニットヘルスチェックメッセージングスキームを、コントロールプレーンのキープアライブからデータプレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッピングやスケジューリングの遅延の影響を受けないため、クラスターリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスター制御リンクのメッセージングアクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビートメッセージが存在するため、クラスター制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に帰ることを確認します。保留時間を 0.3 ~ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。</p> <p>次の画面を変更しました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]</p>

機能名	バージョン	機能情報
に対してインターフェイスを障害としてマークするために設定可能なデバウンス時間 Firepower 4100/9300 シャーシ	9.8(1)	ASA がインターフェイスを障害が発生していると思われ、クラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。 新規または変更された画面 : [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]
Firepower 4100/9300 シャーシ上の ASA の サイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト 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。 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	9.7(1)	データセンターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次の画面を変更しました。 [Configuration] > [Device Management] > [High Availability and Scalability] > [Cluster Configuration]
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。

機能名	バージョン	機能情報
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)	<p>スパンド EtherChannel のルーテッドモードでのサイト間クラスターリングの場合、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。</p> <p>次の画面を変更しました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced]</p>
16 のモジュールのシャーシ間クラスターリング、および Firepower 9300 ASA アプリケーションのサイト間クラスターリング	9.5(2.1)	<p>FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスター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。</p> <p>変更された画面はありません。</p>
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ーリングサポートのサイト別 MAC アドレス	9.5(2)	<p>ルーテッドモードでは、スパンド EtherChannel サイト間クラスター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、各クラスターメンバーのサイト ID を設定します。</p> <p>次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]</p>
インターフェイスまたはクラスター制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスターのカスタマイズ	9.5(2)	<p>インターフェイスまたはクラスター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。</p> <p>次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Auto Rejoin]</p>
ASA クラスターは、GTPv1 と GTPv2 をサポートします	9.5(2)	<p>ASA クラスターは、GTPv1 および GTPv2 インспекションをサポートします。</p> <p>変更された画面はありません。</p>
TCP 接続のクラスター複製遅延	9.5(2)	<p>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。</p> <p>次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]</p>

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、サーバー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 の強化がフェールオーバーおよび ASA クラスタリングでサポート	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 つの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>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。