



# Cisco Secure Firewall 3100/4200 の ASA クラスタ

クラスタリングを利用すると、複数の ASA 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。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。



(注) 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（84 ページ）](#)」を参照してください。

- [ASA クラスタリングの概要（1 ページ）](#)
- [ASA クラスタリングのライセンス（6 ページ）](#)
- [ASA クラスタリングの要件と前提条件（8 ページ）](#)
- [クラスタリングに関するガイドライン（10 ページ）](#)
- [ASA クラスタリングの設定（16 ページ）](#)
- [クラスタノードの管理（58 ページ）](#)
- [ASA クラスタのモニタリング（66 ページ）](#)
- [分散型サイト間 VPN のトラブルシューティング（68 ページ）](#)
- [ASA クラスタリングの例（69 ページ）](#)
- [クラスタリングの参考資料（84 ページ）](#)
- [Cisco Secure Firewall 3100/4200 の ASA クラスタリングの履歴（103 ページ）](#)

## ASA クラスタリングの概要

ここでは、クラスタリングアーキテクチャとその動作について説明します。

## クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは1つのユニットとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーンネットワーク。クラスタ制御リンクと呼ばれます。
- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータが次のいずれかの方法でできる必要があります：

- スパンド EtherChannel（推奨）：クラスタ内の複数のメンバのインターフェイスをグループ化して1つの EtherChannel とします。この EtherChannel がユニット間のロードバランシングを実行します。
- ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してユニット間のロードバランシングを実行します。
- 等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミック ルートを使用してユニット間のロードバランシングを実行します。

## クラスタ メンバー

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

### ブートストラップ設定

各デバイスで、最小限のブートストラップコンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。通常、クラスタリングを有効にする最初のノードが制御ノードになります。以降のノードに対してクラスタリングをイネーブルにすると、そのノードはデータノードとしてクラスタに参加します。

### 制御ノードとデータノードの役割

クラスタ内のメンバーの1つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは1～100の範囲内で設定され、1が最高のプライオリティです。他のすべてのメンバーはデータノードです。一般的には、クラスタを作成

した後で最初に追加したノードが制御ノードとなります。これは単に、その時点でクラスタに存在する唯一のノードであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ノード上のみで実行する必要があります。コンフィギュレーションは、データノードに複製されます。物理的アセット（たとえばインターフェイス）の場合は、制御ノードのコンフィギュレーションがすべてのデータノード上でミラーリングされます。たとえば、内部インターフェイスとしてイーサネット 1/2 を設定し、外部インターフェイスとしてイーサネット 1/1 を設定した場合、これらのインターフェイスは内部および外部インターフェイスとしてデータノードでも使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

## クラスタ インターフェイス

データインターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。1 つのクラスタ内のすべてのデータインターフェイスのタイプが同一であるか。詳細については、[クラスタ インターフェイスについて（17 ページ）](#)を参照してください。

## クラスタ制御リンク

各ユニットの、少なくとも 1 つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、[クラスタ制御リンク（17 ページ）](#)を参照してください。

## 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。

## ASA クラスタ管理

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

管理インターフェイスについては、専用管理インターフェイスの1つを使用することを推奨します。管理インターフェイスは、個別インターフェイスとして設定することも（ルーテッドモードとトランスペアレントモードの両方）、スパンドEtherChannelインターフェイスとして設定することもできます。

、管理用には、個別インターフェイスを使用することを推奨します。個別インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンドEtherChannelインターフェイスでは、現在の制御ユニットへのリモート接続しかできません。



- (注) スパンドEtherChannelインターフェイスモードを使用して、管理インターフェイスを個別インターフェイスとして構成する場合は、管理インターフェイスに対してダイナミックルーティングをイネーブルにすることはできません。スタティック ルートを使用する必要があります。

個別インターフェイスの場合は、メインクラスタ IP アドレスはそのクラスタ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。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ユニット（現在の制御ユニットも含まれます）がその範囲内のローカルアドレスを使用できるようになります。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。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

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。



- (注) to-the-box トラフィックをノードの管理 IP アドレスに転送する必要があります。to-the-box トラフィックは、クラスタ制御リンクを介して他のノードに転送されません。

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。

スパンド EtherChannel インターフェイスの場合は、IP アドレスは1つだけ設定でき、その IP アドレスは常に制御ユニットに関連付けられます。EtherChannel インターフェイスを使用してデータユニットに直接接続することはできません。管理インターフェイスは個別インターフェイスとして設定することを推奨します。各ユニットに接続できるようにするためです。デバイス ローカル EtherChannel を管理に使用できます。

## 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>」を参照してください。

## サイト間クラスタリング

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

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

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

トの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト ID は、LISP インスペクションを使用したフロー モビリティの有効化、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向上とラウンドトリップ時間の遅延短縮のためのディレクタ ローカリゼーションの有効化、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存在する接続に対するサイト冗長性のある有効化の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 : [ASA クラスタリングの要件と前提条件](#) (8 ページ)
- サイト間のガイドライン : [クラスタリングに関するガイドライン](#) (10 ページ)
- クラスタ フロー モビリティの設定 : [クラスタ フロー モビリティの設定](#) (48 ページ)
- ディレクタ ローカリゼーションの有効化 : [ASA クラスタの基本パラメータの設定](#) (38 ページ)
- サイト冗長性のある有効化 : [ASA クラスタの基本パラメータの設定](#) (38 ページ)
- サイト間での例 : [サイト間クラスタリングの例](#) (79 ページ)

## ASA クラスタリングのライセンス

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

各ユニットには、Essentials ライセンス (デフォルトで有効) と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンス サーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

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。データユニットのコンテキストライセンスに追加料金はかかりません。

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。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、Essentials ライセンスはすべてのユニットで常にデフォルトで有効になっています。制御ユニットにのみスマートライセンスを設定できます。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 : 各ユニットには、サーバーからの Essentials のライセンスが必要です。

- 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 2 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。
  - クラスタ内に 6 つの Secure Firewall 3100 があります。Essentials ライセンスは 2 のコンテキストを含みます。6 ユニットの場合、合計で 12 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 32 のコンテキストを含みます。シャーンゴとのプラットフォームの制限が 100 であるため、結合されたライセンスでは最大 100 のコンテキストが許容されます。32 コンテキストは制限の範囲内です。したがって、制御ユニット上で最大 32 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 32 コンテキストを持つことになります。
  - クラスタ内に 3 つの Secure Firewall 3100 があります。Essentials ライセンスは 2 のコンテキストを含みます。3 ユニットの場合、合計で 6 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 100 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 106 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 100 であるため、統合されたライセンスでは最大 100 のコンテキストが許容されます。106 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 100 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、設定の複製を介して 100 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 94 のコンテキストのみを設定する必要があります。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

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。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた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。

## ASA クラスタリングの要件と前提条件

### モデルの要件

- Secure Firewall 3100 : 最大 16 ユニット
- Secure Firewall 4200 : 最大 16 ユニット

### ASA のハードウェアおよびソフトウェア要件

クラスタ内のすべてのユニット :

- 同じ DRAM を使用する同じモデルである必要があります。フラッシュ メモリの容量は同一である必要はありません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレスアップグレードがサポートされます。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。
- セキュリティ コンテキスト モードが一致している必要があります（シングルまたはマルチ）。
- （シングル コンテキスト モード）ファイアウォール モードが一致している必要があります（ルーテッドまたはトランスペアレント）。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタメンバーは、制御ユニットと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。

### スイッチ要件

- ASA でクラスタリングを設定する前に、スイッチのコンフィギュレーションを完了する必要があります。
- サポートされているスイッチのリストについては、『[Cisco ASA Compatibility](#)』[英語]を参照してください。

### ASA の要件

- ユニットを管理ネットワークに追加する前に、一意の IP アドレスを各ユニットに提供します。
  - ASA への接続および管理 IP アドレスの設定に関する詳細については、「使用する前に」の章を参照してください。

- 制御ユニット（通常は最初にクラスタに追加されたユニット）で使用する IP アドレスを除き、これらの管理 IP アドレスは一時的に使用されるだけです。
- データユニットがクラスタに参加すると、管理インターフェイス設定はマスターユニットからの複製に置き換えられます。

### 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 メンバの場合。

- 合計 4 クラスタ メンバ
- 各サイト 2 メンバ
- メンバあたり 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 メンバの場合、サイズは増加します。

- 合計 6 クラスタ メンバ
- サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
- メンバあたり 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 メンバの場合。

- 合計 2 クラスタ メンバ
- 各サイト 1 メンバ
- メンバあたり 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)。

### その他の要件

ターミナル サーバーを使用して、すべてのクラスタ メンバユニットのコンソール ポートにアクセスすることをお勧めします。初期設定および継続的な管理（ユニットがダウンしたときなど）では、ターミナル サーバーがリモート管理に役立ちます。

## クラスタリングに関するガイドライン

### コンテキスト モード

モードは、各メンバー ユニット上で一致している必要があります。

### ファイアウォール モード

シングル モードの場合、ファイアウォール モードがすべてのユニットで一致している必要があります。

### フェールオーバー

フェールオーバーは、クラスタリングではサポートされません。

### IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

### 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。さらに、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
- 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 **src-dst-mixed-ip-port** を使用することをお勧めします（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）。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。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。  

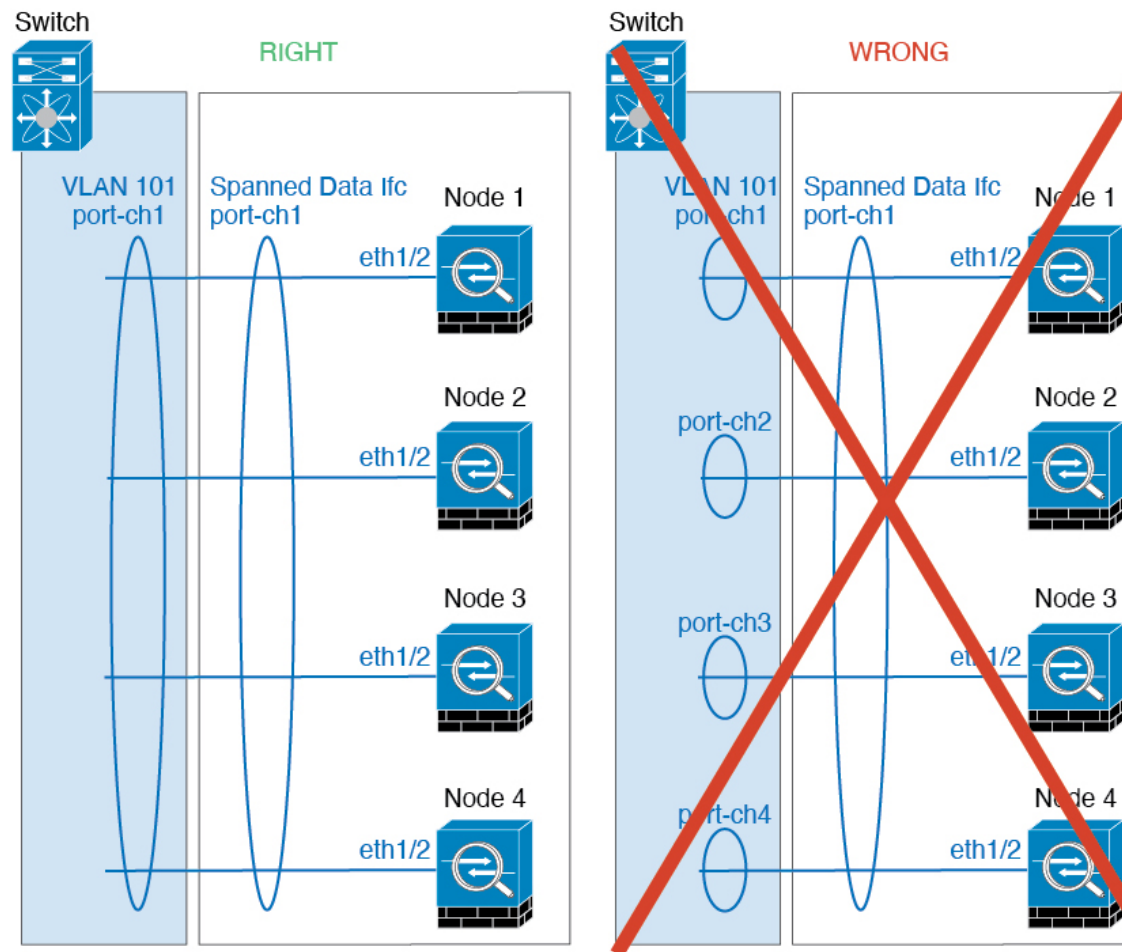
```
router(config)# port-channel id hash-distribution fixed
```

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。
- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能を無効化する必要があります。

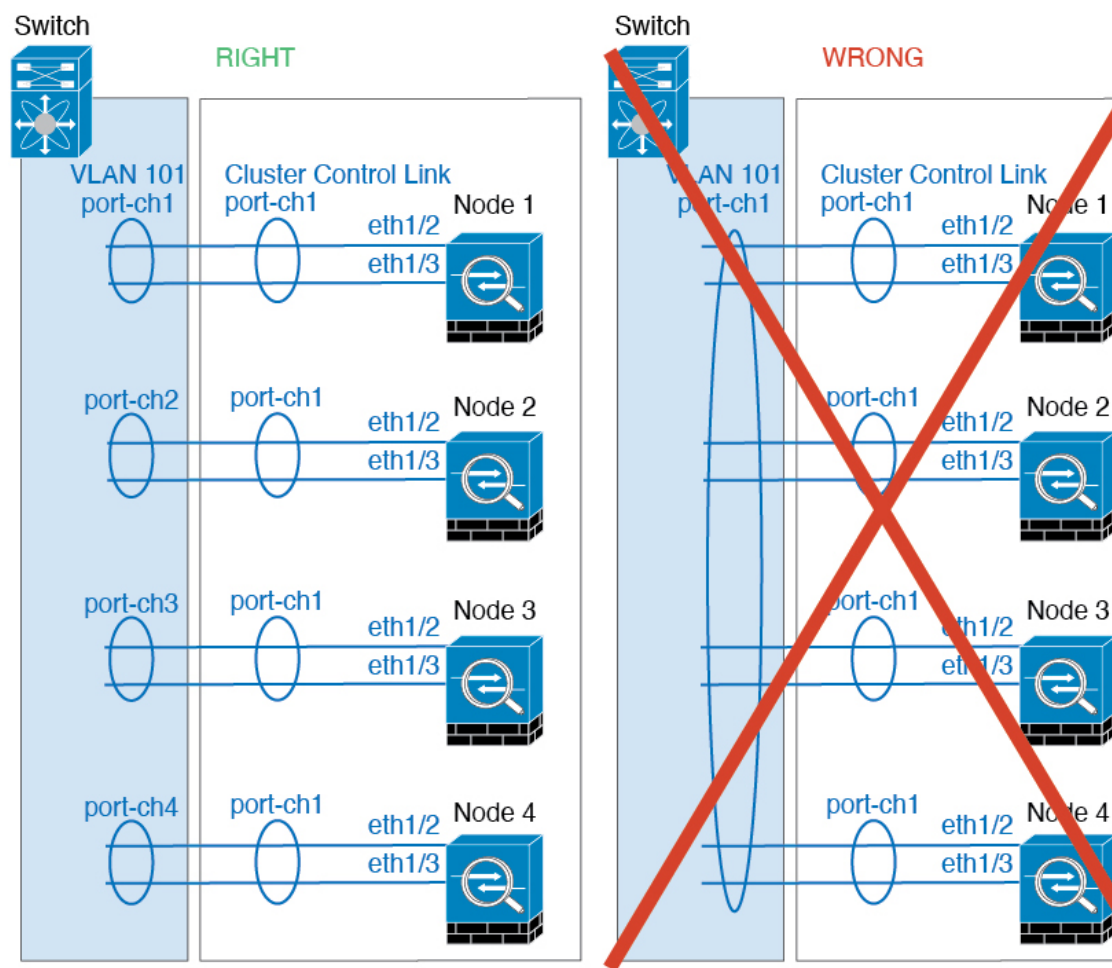
## EtherChannel

- 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。



### サイト間のガイドライン

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。

- 次のインターフェイスおよびファイアウォールモードで Inter-Site クラスタリングをサポートします。

| インターフェイス モード      | ファイアウォール モード |             |
|-------------------|--------------|-------------|
|                   | ルーテッド        | Transparent |
| 個別インターフェイス        | 対応           | N/A         |
| スパンド EtherChannel | ○            | ○           |

- 個別インターフェイスモードでは、マルチキャストランデブーポイント（RP）に向けて ECMP を使用する場合、ネクストホップとしてメインクラスタ IP アドレスを使用する RP IP アドレスのスタティックルートを使用することをお勧めします。このスタティックルートは、データユニットにユニキャスト PIM 登録パケットが送信されるのを防ぎます。デー

タユニットがPIM登録パケットを受け取った場合、パケットはドロップされ、マルチキャストストリームは登録できません。

- 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、ディレクタの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常に（サイト ID に従って）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。
- ノースサウス展開での UDP の長期的フローでは、元のフローの所有者サイトのノードに障害が発生してから復帰し、その後フローが元のサイトに戻されると、ルーティンググループが発生する可能性があります。他のサイトの新しい所有者に宛先へのルートがない場合、フローがインターネットに戻され、ループが発生します。この場合、新しい所有者に対して **clear conn** コマンドを使用して、強制的にフローを再確立します。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じMACアドレスを共有し、両方の外部ルータが同じMACアドレスを共有する必要があります。サイト1のクラスタメンバがサイト2のメンバに接続を転送するとき、宛先MACアドレスは維持されます。MACアドレスがサイト1のルータと同じである場合にのみ、パケットはサイト2のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイル用に各サイトのデータネットワークとゲートウェイルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ

VLAN は、オーバーレイ トランスポート仮想化 (OTV) または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが1つのサイト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 に追加する必要があります (ブリッジグループのスタティック MAC アドレスの追加を参照)。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、ファイアウォール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、インターフェイスのヘルスチェック機能を再度有効にできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバーポートがダウンし、サーバーが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージがクラスタに送信されます。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。

- 個別インターフェイスモードの VXLAN はサポートされていません。スパンド EtherChannel モードでのみ VXLAN をサポートしています。
- シスコは、スパンド EtherChannel モードの IS-IS をサポートしません。個別インターフェイスモードのみが IS-IS をサポートします。
- クラスタ内のすべてのユニットに変更が複製されるまでには時間がかかります。たとえば、オブジェクトグループを使用するアクセスコントロールルール（展開時に複数のルールに分割される）を追加するなどの大きな変更を行うと、変更の完了に必要な時間がクラスタユニットが成功メッセージで応答できるタイムアウトを超える可能性があります。この場合、「failed to replicate command」というメッセージが表示されることがあります。このメッセージは無視できます。

### クラスタリングのデフォルト

- スパンド EtherChannel を使用するときは、cLACP システム ID は自動生成され、システムプライオリティはデフォルトで 1 です。
- 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。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 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。
- 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。

## ASA クラスタリングの設定

クラスタリングを設定するには、次のタスクを実行します。



- (注) クラスタリングを有効または無効にするには、コンソール接続（CLI の場合）または ASDM 接続を使用します。

## コンフィギュレーションのバックアップ（推奨）

データユニットでクラスタリングをイネーブルにすると、現在のコンフィギュレーションは同期したアクティブユニットの設定に置き換えられます。クラスタ全体を解除する場合、使用可

能な管理インターフェイス コンフィギュレーションのバックアップ コンフィギュレーションを取っておくと役立つ場合があります。

#### 始める前に

各ユニットのバックアップを実行します。

#### 手順

**ステップ 1** [ツール (Tools) ] > [バックアップ設定 (Backup Configurations) ] を選択します。

**ステップ 2** 最低でも実行コンフィギュレーションをバックアップします。詳細な手順については、[コンフィギュレーションまたはその他のファイルのバックアップと復元](#)を参照してください。

## ユニットのケーブル接続およびインターフェイスの設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。次に、インターフェイスを設定します。

### クラスタ インターフェイスについて

データインターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータ インターフェイスのタイプが同一であることが必要です。イーサネット 1/1 をスパンド EtherChannel として設定し、イーサネット 1/2 を同じクラスタ内の個別インターフェイス（など）として設定することはできません。

また、各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

#### クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。可能な場合は、クラスタ制御リンクに EtherChannel を使用することを推奨します。

#### クラスタ制御リンク トラフィックの概要

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

制御トラフィックには次のものが含まれます。

- 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。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

#### クラスタ制御リンク インターフェイスとネットワーク

次の例外を除き、クラスタ制御リンクには任意のデータ インターフェイスを使用できます。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。
- 管理  $x/x$  インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。

EtherChannel インターフェイスを使用できます。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、ASA クラスタ制御リンク インターフェイスだけが含まれるようにしてください。

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

#### クラスタ制御リンクのサイジング

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

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

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

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

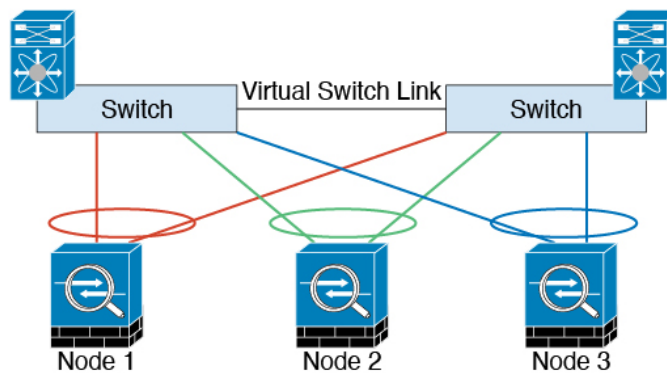


- (注) クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

### クラスタ制御リンクの冗長性

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

次の図は、仮想スイッチングシステム（VSS）、仮想ポートチャネル（vPC）、StackWise、または StackWise Virtual 環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが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の障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャットダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。



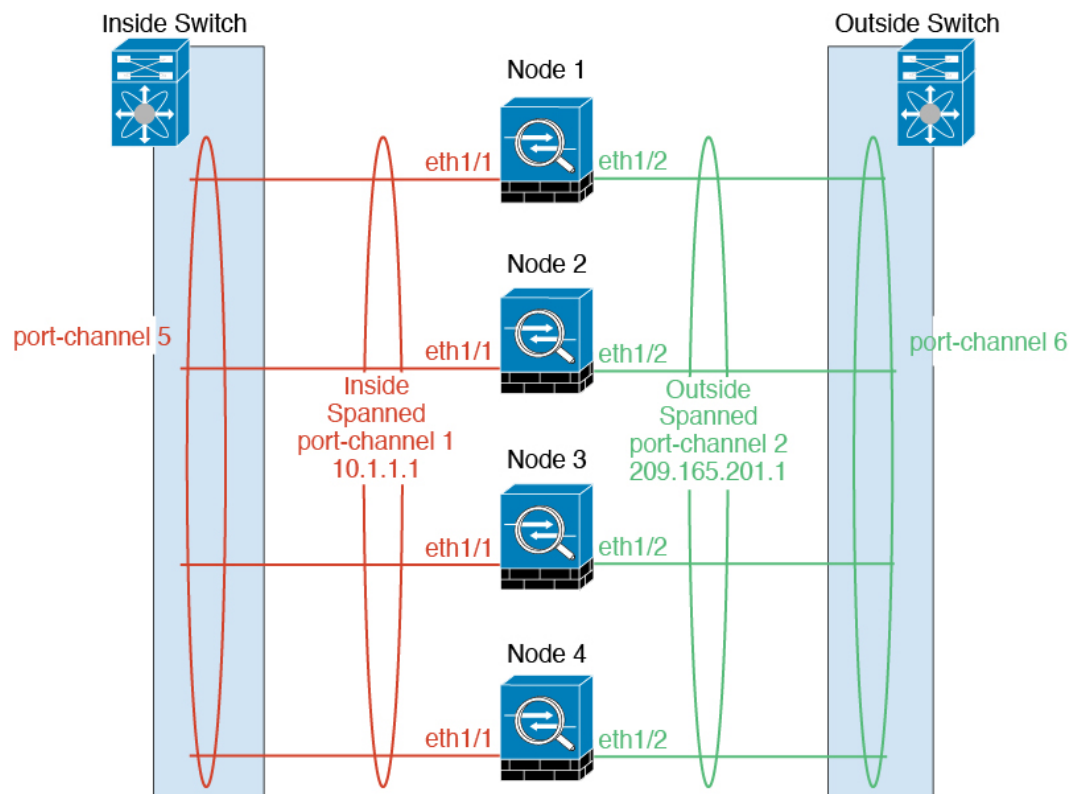
- (注) ASA が非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスター IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスターでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（制御ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

## 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、クラスター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ーではなく BVI に割り当てられます。

EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



## スパンド EtherChannel の利点

EtherChannel 方式のロードバランシングは、次のような利点から、他の方式よりも推奨されます。

- 障害検出までの時間が短い。
- コンバージェンス時間が短い。個別インターフェイスはルーティングプロトコルに基づきトラフィックをロードバランシングしますが、ルーティングプロトコルはリンク障害時にコンバージェンスが遅くなることがよくあります。
- コンフィギュレーションが容易である。

## 最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロードバランシングハッシュアルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内の同じ ASA に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュアルゴリズムとして使用することを推奨します。
- ASA をスイッチに接続するときは、同じタイプのラインカードを使用します。すべてのパケットに同じハッシュアルゴリズムが適用されるようにするためです。

## ロードバランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュアルゴリズムを使用して選択されます。



- (注) スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのノード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。

EtherChannel 内のリンク数はロードバランシングに影響を及ぼします。

対称ロードバランシングは常に可能とは限りません。NAT を設定する場合は、フォワードパケットとリターンパケットとで IP アドレスやポートが異なります。リターントラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターントラフィックを正しいユニットにリダイレクトする必要があります。

## EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコルステータスをモニターします。リンクの1つで障害が発生すると、トラフィックは残りのリンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

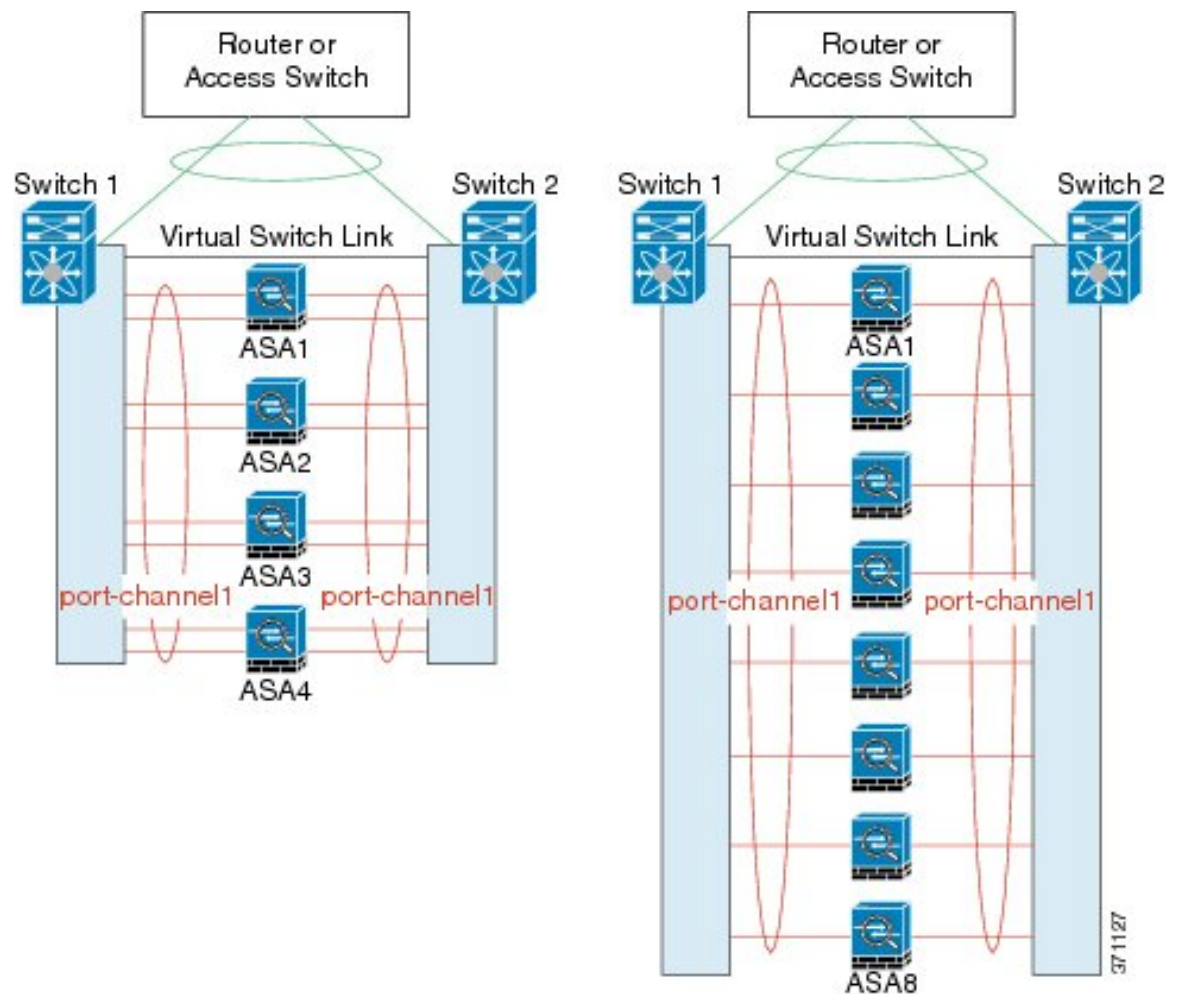
## 冗長スイッチシステムへの接続

1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS、vPC、StackWise、または StackWise Virtual の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブリンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブリンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビットイーサネットモジュール）。

EtherChannel で 8 個のアクティブリンクをサポートするスイッチの場合、冗長システムで 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブリンクを設定できます。

次の図では、4 ノードクラスタおよび 8 ノードクラスタでの 16 アクティブリンクのスパンド EtherChannel を示します。

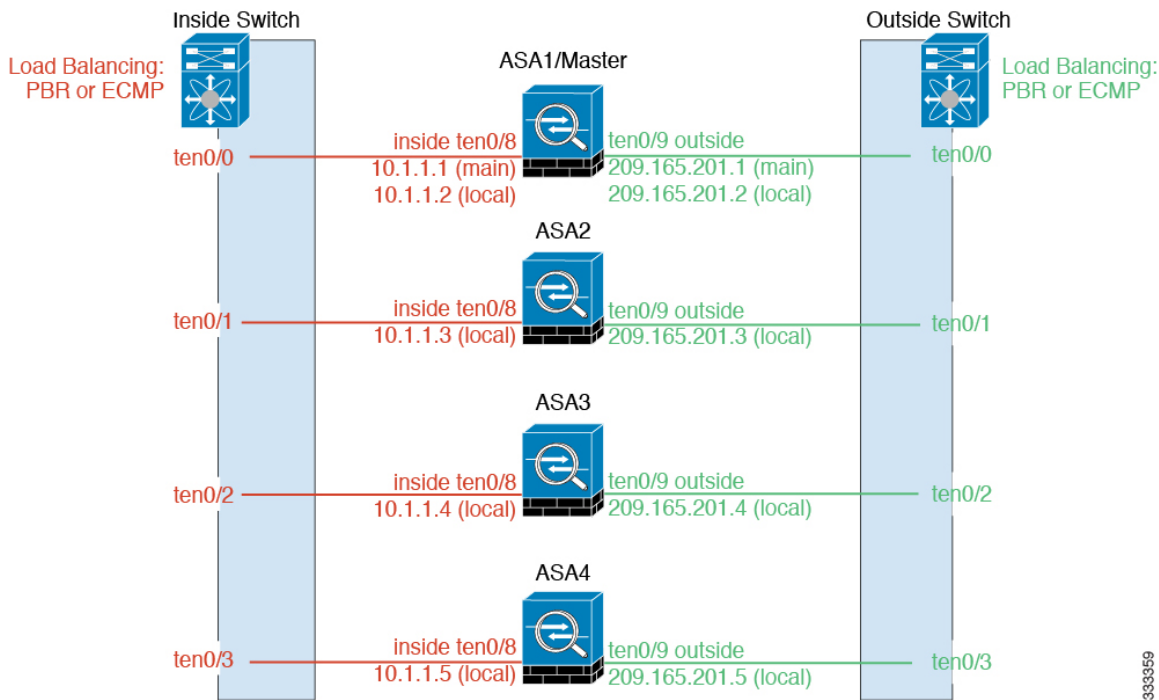


## 個別インターフェイス（ルーテッドファイアウォール モードのみ）

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル IP アドレスを持ちます。各インターフェイスのメインクラスタ IP アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。

インターフェイス コンフィギュレーションは制御ノード上だけで行う必要があるため、IP アドレスプールを設定して、このプールのアドレスがクラスタノード（制御ノード用を含む）の特定のインターフェイスに使用されるようにします。

アップストリームスイッチ上でロードバランシングを別途する必要があります。



## ポリシーベース ルーティング

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA に分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクトトラッキングとともに使

用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 ASA をモニタします。これで、PBR は、特定の ASA の到達可能性に基づいてルート マップを有効化または無効化できます。詳細については、次の URL を参照してください。

<http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html>

[http://www.cisco.com/en/US/products/ps6599/products\\_white\\_paper09186a00800a4409.shtml](http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml)

## 等コスト マルチパス ルーティング

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の1つが、等コストマルチパス (ECMP) ルーティングです。

この方法が推奨されるのは、すでに ECMP を使用しており、既存のインフラストラクチャを活用したい場合です。

ECMP ルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクストホップの1つにパケットを送信できます。ECMP ルーティングにスタティックルートを使用する場合は、ASA の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA を設定する必要があります。

## Cisco Intelligent Traffic Director (ルーテッドファイアウォール モードのみ)

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。Intelligent Traffic Director (ITD) とは、Nexus 5000、6000、7000 および 9000 スイッチシリーズの高速ハードウェアロードバランシングソリューションです。従来の PBR の機能を完全に網羅していることに加え、簡略化された構成ワークフローを提供し、粒度の細かい負荷分散を実現するための複数の追加機能を備えています。

ITD は、IP スティック性、双方向フロー対称性のためのコンシステント ハッシュ法、仮想 IP アドレッシング、ヘルス モニタリング、高度な障害処理ポリシー (N+M 冗長性)、加重ロードバランシング、およびアプリケーション IP SLA プロブ (DNS を含む) をサポートします。ロードバランシングの動的な性質により、PBR に比べて、すべてのクラスタノードでより均一なトラフィック分散を実現します。双方向フロー対称性を実現するために、接続のフォワードおよびリターンパケットが同じ ASA に送信されるように ITD を設定することを推奨します。詳細については、次の URL を参照してください。

[https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/itd\\_deployment/ITD\\_ASA\\_Deployment\\_Guide.pdf](https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/itd_deployment/ITD_ASA_Deployment_Guide.pdf)

## クラスタユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

### 手順

**ステップ 1** クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

(注)

クラスタに参加するようにノードを設定する前に、少なくとも、アクティブなクラスタ制御リンクネットワークが必要です。

**ステップ 2** アップストリームとダウンストリームの機器も設定する必要があります。たとえば、EtherChannel を使用する場合は、EtherChannel のアップストリーム/ダウンストリーム機器を設定する必要があります。

## 制御ユニットでのクラスタ インターフェイス モードの設定

クラスタリング用に設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのいずれか一方のみです。1つのクラスタ内でインターフェイスタイプを混在させることはできません。



(注) 制御ユニットからデータユニットを追加しない場合は、制御ユニットだけでなく全ユニットのインターフェイスモードをこの項の説明に従って手動で設定する必要があります。制御ユニットからセカンダリユニットを追加する場合は、ASDM がデータユニットのインターフェイスモードを自動的に設定します。

### 始める前に

- 管理専用インターフェイスはいつでも、スパンド EtherChannel モードのときでも個別インターフェイス（推奨）として設定できます（スパンド EtherChannel モードのときでも管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレントファイアウォール モードのときでも））。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミックルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。
- マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのインターフェイスタイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッ

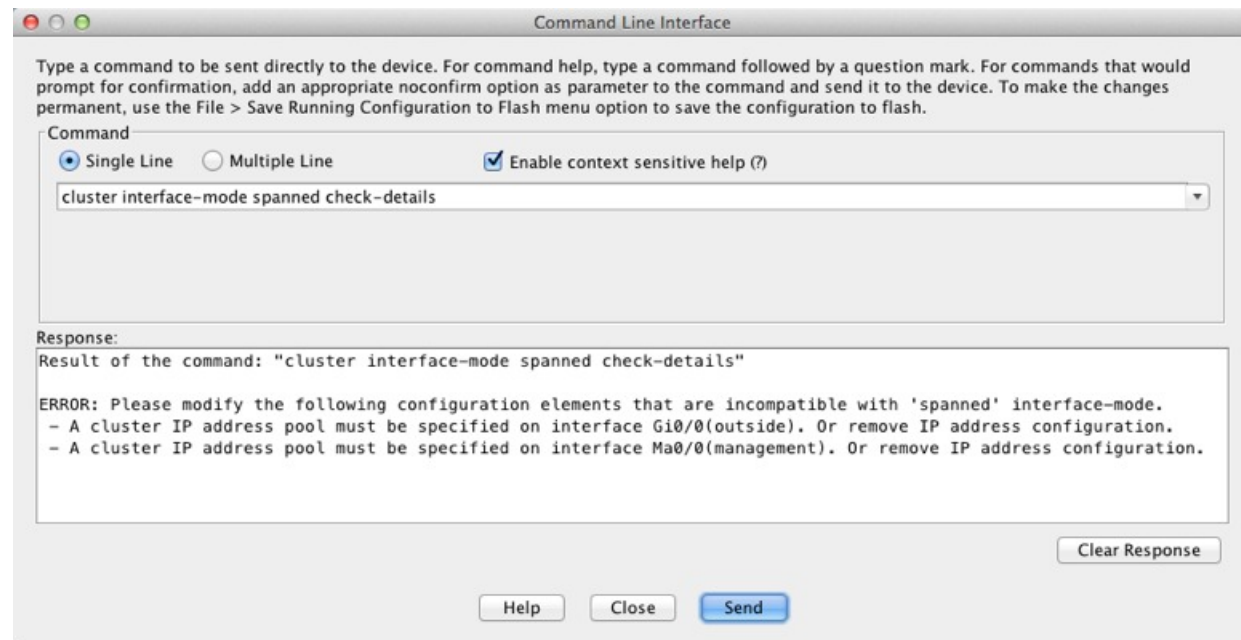
ドモードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレントモードで許可される唯一のインターフェイス タイプであるからです。

## 手順

**ステップ 1** 制御ユニットの ASDM で、**[Tools] > [Command Line Interface]** の順に選択します。互換性のないコンフィギュレーションを表示し、強制的にインターフェイス モードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

**cluster interface-mode {individual | spanned} check-details**

例 :



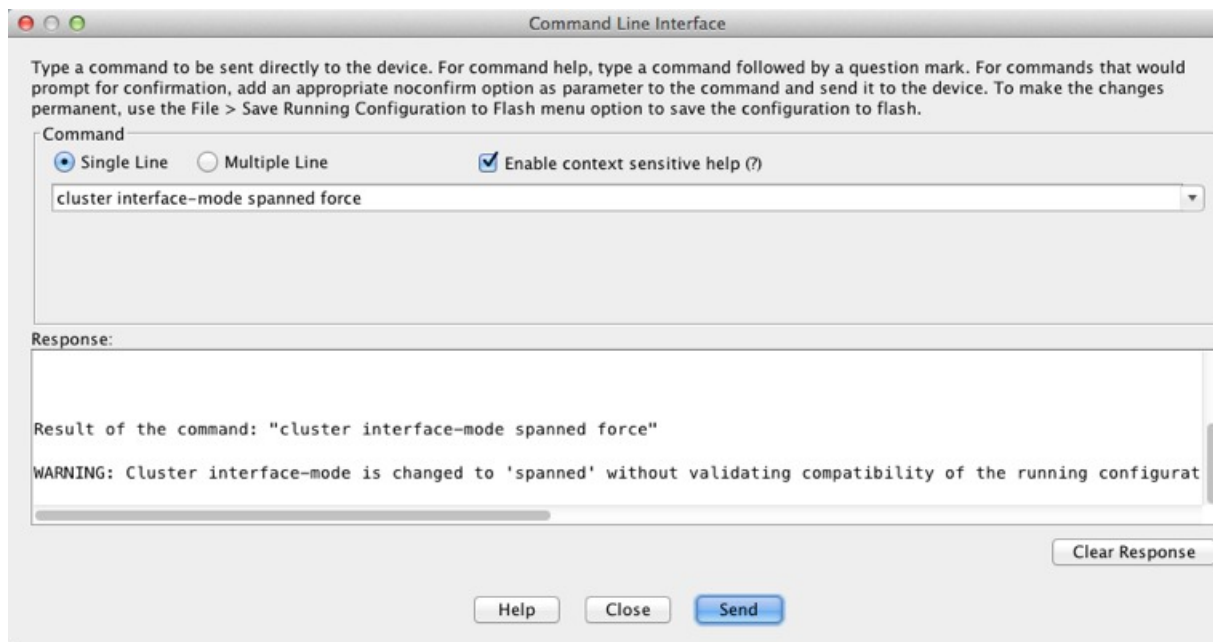
### 注意

インターフェイス モードを設定した後は、常にインターフェイスに接続できるようになります。ただし、クラスタリング要件に適合するように管理インターフェイスを設定する前に ASA をリロードすると（たとえば、クラスタ IP プールを追加するため）、クラスタと互換性のないインターフェイス コンフィギュレーションが削除されるため、再接続できなくなります。その場合は、コンソール ポートに接続してインターフェイス コンフィギュレーションを修正する必要があります。

**ステップ 2** クラスタリング用にインターフェイス モードを設定します。

**cluster interface-mode {individual | spanned} force**

例 :



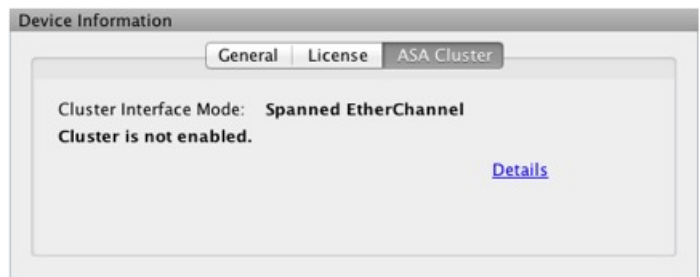
デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

**force** オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

**force** オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソールポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

- ステップ 3** ASDM を終了し、リロードします。クラスタ インターフェイス モードに正しく対応するように ASDM を再起動する必要があります。リロードの後、ホーム ページに [ASA Cluster] タブが表示されます。



## (推奨、マルチコンテキストモードでは必須) 制御ノードでのインターフェイスの設定

クラスタリングを有効にする前に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。少なくとも、ASDM が現在接続されている管理インターフェイスは変更する必要があります。他のインターフェイスについては、クラスタリングの有効化の前後で設定できます。すべての設定が新しいクラスタメンバーと同期するように、すべてのインターフェイスを事前に設定することを推奨します。マルチコンテキストモードでは、この項の手順を使用して、既存のインターフェイスを修正するか、新しいインターフェイスを設定する必要があります。一方、シングルモードでは、この項を省略し、高可用性と拡張性のウィザードで共通インターフェイスパラメータを設定できます ([高可用性ウィザードを使用したクラスタの作成または参加 \(34 ページ\)](#) を参照)。個別インターフェイス用の EtherChannel の作成などの高度なインターフェイス設定はウィザードでは実行できないことに注意してください。

ここでは、クラスタリング互換となるようにインターフェイスを設定する方法について説明します。データ インターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。各方式では異なるロードバランシングメカニズムが使用されます。同じコンフィギュレーションで両方のタイプを設定することはできません。ただし、管理インターフェイスは例外で、スパンド EtherChannel モードであっても個別インターフェイスにできます。

### 個々のインターフェイスを設定する (管理用インターフェイスの場合推奨)

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。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、常に制御ノードに属します。

スパンド EtherChannel モード個別管理インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、制御ノードへの接続しかできません。

### 始める前に

- 管理専用インターフェイスの場合を除き、個別インターフェイスモードであることが必要です。
- マルチ コンテキスト モードの場合は、この手順を各コンテキストで実行します。まだコンテキスト コンフィギュレーションモードに入っていない場合は、**changeto context name**

コマンドを入力します。[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コンテキスト名をダブルクリックします。

- 個別インターフェイスの場合は、ネイバー デバイスでのロード バランシングを設定する必要があります。管理インターフェイスには、外部のロードバランシングは必要ありません。
- （オプション）インターフェイスをデバイスローカル EtherChannel インターフェイスとして設定する、およびサブインターフェイスを設定する作業を必要に応じて行います。
  - EtherChannel の場合、この EtherChannel はユニットに対してローカルであり、スパン ド EtherChannel ではありません。
- ASDM を使用して管理インターフェイスにリモートに接続している場合は、将来のセカンダリ ユニットの現在の IP アドレスは一時的なものです。
  - 各メンバには、プライマリ ユニットで定義されたクラスタ IP プールから IP アドレスが割り当てられます。
  - クラスタ IP プールには、将来のセカンダリ IP アドレスを含む、ネットワークですでに使用中のアドレスを含めることはできません。

次に例を示します。

1. プライマリ ユニットに 10.1.1.1 を設定します。
2. 他のユニットには、10.1.1.2、10.1.1.3、10.1.1.4 を使用します。
3. プライマリ ユニットのクラスタの IP プールを設定する場合、使用中であるために .2、.3、.4 のアドレスをプールに含めることはできません。
4. 代わりに、.5、.6、.7、.8 のような、ネットワークの他の IP アドレスを使用する必要があります。



(注) プールには、プライマリ ユニットを含むクラスタのメンバ数分のアドレスが必要です。元の .1 アドレスはメイン クラスタ IP アドレスであり、現在のプライマリ ユニットのものです。

5. クラスタに参加すると古い一時的なアドレスは放棄され、他の場所で使用できません。

## 手順

**ステップ 1** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。

**ステップ 2** インターフェイス行を選択して、[Edit] をクリックします。インターフェイスのパラメータを設定します。次のガイドラインを参照してください。

- （スパンド EtherChannel モードの管理インターフェイスでは必須）**[このインターフェイスを管理専用にする（Dedicate this interface to management only）]**：インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。デフォルトでは、管理タイプのインターフェイスは管理専用として設定されます。トランスペアレントモードでは、このコマンドは管理タイプのインターフェイスに対して常にイネーブルになります。
- [Use Static IP]：DHCP と PPPoE はサポートされません。

**ステップ 3** IPv4 クラスタ IP プール、MAC アドレス プール、およびサイト別の MAC アドレスを追加するには、[Advanced] タブをクリックして、[ASA Cluster] エリア パラメータを設定します。

- [IP Address Pool] フィールドの横にある [...] ボタンをクリックしてクラスタ IP プールを作成します。表示される有効範囲は、[General] タブで設定するメイン IP アドレスにより決定します。
- [Add] をクリックします。
- メインクラスタの IP アドレスを含まないアドレス範囲を設定します。ネットワーク内で現在使用されているアドレスも含みません。範囲は、たとえば 8 アドレスというように、クラスタのサイズに合わせて十分に大きくする必要があります。

- [OK] をクリックして、新しいプールを作成します。
- 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。プール名が [IP Address Pool] フィールドに表示されます。
- （任意）（オプション）MAC アドレスを手動で設定する場合は、[MAC Address Pool] を設定します。

**ステップ 4** IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

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

[Enable address autoconfiguration] オプションはサポートされません。リンクローカルアドレスの手動設定もサポートされていません。

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

- [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、「2001:0DB8::BA98:0:3210/48」のように入力します。

- d) [...] ボタンをクリックして、クラスタ IP プールを設定します。
- e) [Add] をクリックします。

- f) プールの開始 IP アドレス（ネットワーク プレフィックス）、プレフィックス長、アドレス数を設定します。
- g) [OK] をクリックして、新しいプールを作成します。
- h) 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。  
[ASA Cluster IP Pool] フィールドにプールが表示されます。
- i) [OK] をクリックします。

**ステップ 5** [OK] をクリックして、[Interfaces] ペインに戻ります。

**ステップ 6** [Apply] をクリックします。

## スパンド EtherChannel の設定

スパンド EtherChannel は、クラスタ内のすべての ASA に広がるものであり、EtherChannel の動作の一部としてロード バランシングを行うことができます。

### 始める前に

- スパンド EtherChannel インターフェイス モードにする必要があります。
- 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。[ブリッジ仮想インターフェイス \(BVI\) の設定](#)を参照してください。
- 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イネーブルになるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

## 手順

- ステップ 1** コンテキスト モードによって次のように異なります。
- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
  - マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。
- ステップ 2** [Add] > [EtherChannel Interface] の順に選択します。
- [Add EtherChannel Interface] ダイアログボックスが表示されます。
- ステップ 3** 次をイネーブルにします。
- [Port Channel ID]
  - [Enable Interface] (デフォルトでオンになります)
  - [Members in Group] : [Members in Group] リストに、インターフェイスを少なくとも 1 つ追加する必要があります。ユニットごとに複数のインターフェイスが EtherChannel に含まれていると、VSS、vPC、StackWise、または StackWise Virtual のスイッチに接続する場合に役立ちます。
- すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。
- 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。

- (ルーテッドモード) 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**および 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。リンクローカルアドレスの手動設定もサポートされていません。

- 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。

## 高可用性ウィザードを使用したクラスタの作成または参加

クラスタ内の各ノードがクラスタに参加するには、ブートストラップ設定が必要です。(制御ノードになる) 1 台のノード上で High Availability and Scalability ウィザードを実行してクラスタを作成し、データノードを追加します。



(注) このウィザードでは、デフォルトの cLACP システム ID およびプライオリティを変更できません。これらは、クラスタリングが無効のときにのみ構成できます。したがって、ウィザードを使用してからクラスタリングを無効にするか、[ASA クラスタの基本パラメータの設定 \(38 ページ\)](#) を参照してクラスタを手動で構成してください。

### 始める前に

- マルチ コンテキスト モードでは、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。
- クラスタ制御リンク インターフェイスに使用するインターフェイスは、接続されたスイッチでアップ状態になっている必要があります。
- 稼働中のクラスタにノードを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがありますが、これは想定内の動作です。

### 手順

**ステップ 1** [Wizards] > [High Availability and Scalability Wizard] の順に選択します。次の手順でこのウィザードのガイドラインを確認してください。

**ステップ 2** [インターフェイス (Interfaces)] 画面では新しい EtherChannel を作成できません (クラスター制御リンクを除く)。

**ステップ 3** [ASA Cluster Configuration] 画面で、ブートストラップの設定を構成します。

- [メンバーの優先順位 (Member Priority)] : 制御ノード選定用に、このノードの優先順位を 1 ～ 100 の範囲内で設定します。1 が最高の優先順位です。
- [ (ルーテッドモード、スパンド EtherChannel モード) サイトインデックス ((Routed mode; Spanned EtherChannel mode) Site Index) ] : サイト間クラスタリングを使用する場合は、このノードのサイト ID を設定して、サイト固有の MAC アドレス (1 ～ 8) が使用されるようにします。
- (任意) [共有キー (Shared Key)] : クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパストラフィック (接続状態の更新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。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。
- (オプション) [Enable connection rebalancing for TCP traffic across all the ASAs in the cluster] : 接続の再分散を有効化します。このパラメータはデフォルトでは無効になっています。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、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。

(注)

サイト間トポロジに対しては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。

- (オプション) [クラスタ内のこのデバイスのヘルスマonitoringを有効にする (Enable health monitoring of this device within the cluster)] : クラスタノードヘルスチェック機能を有効にします。ノードのヘルスを確認するため、ASA のクラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。

(注)

何らかのトポロジ変更を行うとき (たとえば、データインターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加など) は、ヘルスチェックをディセーブルにし、ディセーブルにしたインターフェイスのモニタリングもディセーブルにする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェックを再度有効にできます。

- [デバイスが障害状態だと見なされるまでの待機時間 (Time to Wait Before Device Considered Failed)] : この値は、ノードのキープアライブステータスメッセージの間隔を指定します。範囲は 0.3 ～ 45 秒です。デフォルトは 3 秒です。
- (オプション) [Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support] : クラスタ制御リンクが EtherChannel として設定されていて (推奨)、VSS または vPC ペアに接続されている場合は、このオプションをイネーブル

にすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのノードがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバーインターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値 (0.8 秒など) に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はハートビートメッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。このオプションをイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでハートビートメッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。

- (オプション) [コンソール出力を複製する (Replicate console output)] : データノードから制御ノード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。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート 1 つだけです。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。
- [Cluster Control Link] : クラスタ制御リンク インターフェイスを指定します。
  - [MTU] : クラスタ制御リンクインターフェイスの最大伝送ノードを指定します。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 (2561 ~ 8362 でなく、1400 ~ 9198 バイトの範囲) を指定します。ブロックプールの処理により、この MTU サイズはシステム動作に最適ではありません。デフォルトの MTU は 1500 バイトです。すでにジャンボフレームの予約を有効にしている場合は、MTU を最大値に設定することを推奨します。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 9198 バイトであるため、データインターフェイスの最大 MTU は 9098 になり、クラスタ制御リンクは 9198 に設定できます。注 : ジャンボフレームの予約を有効にしていない場合は、ウィザードを終了し、ジャンボフレームを有効にしてから、この手順を再開する必要があります。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。

**ステップ 4** [ヘルスモニタリング対象のインターフェイス (Interfaces for Health Monitoring)] 画面で、一部のインターフェイスを障害のモニタリング対象から除外できます。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。

(注)

何らかのトポロジ変更を行うとき (たとえば、データ インターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加など) は、ヘルス チェックをディセーブルにし、ディセー

ブルにしたインターフェイスのモニタリングもディセーブルにする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェックを再度有効にできます。

**ステップ 5** [インターフェイス自動再結合設定 (Interface Auto Rejoin settings)] 画面で、インターフェイスまたはクラスタ制御リンクで障害が発生した場合の自動再結合設定をカスタマイズします。タイプごとに、次のオプションを設定できます。

- [Maximum Rejoin Attempts] : クラスタへの再結合の試行回数を定義するために、[Unlimited] または 0 ～ 65535 の範囲で値を設定します。0 は自動再結合を無効化します。デフォルト値は、クラスタ インターフェイスの場合は [Unlimited]、データ インターフェイスの場合は 3 です。
- [Rejoin Interval] : 再結合試行間隔の時間を定義するために、2 ～ 60 の範囲で間隔を設定します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分 (10 日) に制限されます。
- [Interval Variation] : 1 ～ 3 の範囲で設定して、間隔を増加させるかどうかを定義します (1 : 変更なし、2 : 直前の間隔の 2 倍、3 : 直前の間隔の 3 倍)。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後 (2 x 5)、3 階目の試行が 20 分後 (2 x 10) となります。デフォルト値は、クラスタインターフェイスの場合は 1、データインターフェイスの場合は 2 です。

**ステップ 6** [Finish] をクリックします。

**ステップ 7** ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルトコンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するには、[OK] をクリックします。[Cancel] をクリックすると、クラスタリングは有効になりません。

しばらくすると、ASDM がクラスタを有効化して ASA に再接続し、ASA がクラスタに追加されたことを確認する [Information] 画面が表示されます。

(注)

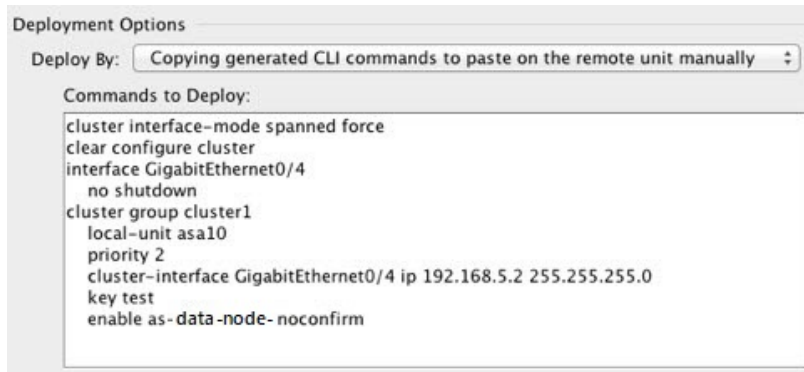
場合によっては、ウィザードの完了後にクラスタに参加した際にエラーが発生する可能性があります。ASDM が切断されていると、ASDM はそれに続くエラーを ASA から受信しません。ASDM に再接続した後もクラスタリングがディセーブルの場合は、ASA コンソール ポートに接続して、クラスタリングがディセーブルになっている詳細なエラー状況を判断する必要があります。たとえば、クラスタ制御リンクがダウンしている可能性があります。

**ステップ 8** データノードを追加するには、[はい (Yes)] をクリックします。

制御ノードからウィザードを再実行する場合、ウィザードを最初に開始するときに [クラスタに別のメンバーを追加する (Add another member to the cluster)] オプションを選択してデータノードを追加できます。

**ステップ 9** [Deployment Options] 領域で、次の [Deploy By] オプションのいずれかを選択します。

- [今すぐリモートユニットにCLIコマンドを送信する (Sending CLI commands to the remote unit now)] : ブートストラップ設定をデータノード (一時) 管理 IP アドレスに送信します。データノード管理 IP アドレス、ユーザ名、パスワードを入力します。
- [生成されたCLIコマンドを手動でコピーして、リモートユニットに貼り付ける (Copying generated CLI commands to paste on the remote unit manually)] : データノードの CLI でコマンドをカットアンドペーストできる、または ASDM の CLI ツールを使用できるようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。



## クラスタリング動作のカスタマイズ

クラスタリングヘルス モニタリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

制御ノードで次の手順を実行します。

### ASA クラスタの基本パラメータの設定

制御ノード上のクラスタ設定をカスタマイズできます。クラスタへのノードの追加にウィザードを使用しない場合は、クラスタパラメータを手動で設定できます。すでにクラスタリングがイネーブルであれば、いくつかのクラスタパラメータを編集できます。クラスタリングがイネーブルになっている間は編集できないものは、グレイ表示されます。この手順には、ウィザードに含まれていない高度なパラメータも含まれます。

クラスタリングが無効である間のみ変更できるパラメータについては、すべてのノードでクラスタリングが無効にしてから、クラスタリングを再度有効にする必要があります。これには、コンソール CLI アクセスが必要です。

#### 始める前に

- ウィザードを使用せず、手動でクラスタに参加する場合は、クラスタに参加する前に、各ノードで `cluster-control-link` インターフェイスを事前設定する必要があります。シングルインターフェイスの場合、イネーブルにする必要があります。他の設定を構成しないでく

ださい。EtherChannel インターフェイスの場合は、イネーブルにして、EtherChannel モードをオンに設定します。

- マルチコンテキストモードでは、制御ノード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。

## 手順

---

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

すでにクラスタにデバイスが追加されていて、それが制御ノードの場合は、このペインは **[クラスタ構成 (Cluster Configuration)]** タブにあります。

図 1: クラスタの設定

Configuration > Device Management > High Availability and Scalability > ASA Cluster

Cluster Configuration | Cluster Interface Health Monitoring | Auto Rejoin | Cluster Members

Configure cluster settings to enable this ASA to participate in a cluster. The name of the cluster and the management interface configuration must be the same for all devices in the cluster.

☒ Participate in ASA cluster

☒ Configure ASA cluster settings

Cluster Name: cluster1

Member Name: unit-1-1

Member Priority: 9 (1 - 100)

Site Index: 1 (1 - 8) (optional)

Site Periodic GARP: (1 - 1000000) (optional)

Shared Key: \*\*\*\* (optional)

☐ Cluster Member Limit 16 (2 - 16)

☐ Enable connection rebalancing across all the ASA in the cluster

Interval Between Connection Rebalancing: 5 seconds (1 - 360)

☒ Enable cluster load monitor

Time Interval: 20 seconds (10 - 360)

Number of Intervals: 30 (1 - 60)

☒ Enable health monitoring of this device within the cluster

Time to Wait Before Device Considered Failed: 3 seconds (0.3 - 45)

☐ Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support

☐ Replicate console output to the control-node's console

☐ Enable Clustering flow mobility

☐ Enable director localization for inter-DC cluster

☐ Site Redundancy

☒ Enable parallel configuration replicate

☐ Flow State Refresh Keepalive Interval 15 seconds (15 - 55)

Cluster Control Link

Interface: Port-channel48

IP Address: 127.2.1.1 Subnet Mask: 255.255.0.0

MTU: 1500 (1400 - 9184)

Cluster LACP

☐ Enable static port priority

Virtual System MAC Address: ☒ Auto-generate ☐ Specify:

System Priority: 1 (1 - 65535)

VPN Grouping Mode

VPN Mode: ☒ Centralized ☐ Distributed

Parallel Join of Units Per Chassis

Minimum Units Required to Join: Default (1)

Maximum Join Delay: 0 (0 - 30 Minutes)

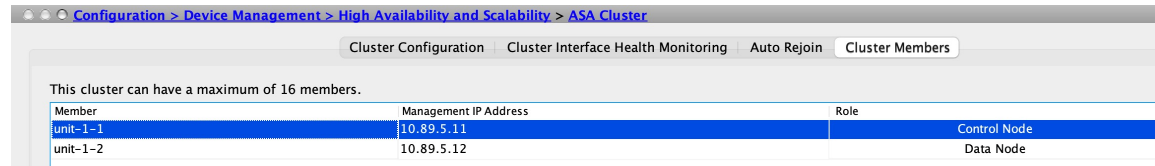
Reset Apply

**ステップ 2** クラスタリングがすでに有効なため、グレースアウトになっている設定を構成する場合は、すべてのノードでクラスタリングを無効にします。

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。管理インターフェイスは、そのノードがメイン IP アドレスではなく、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。

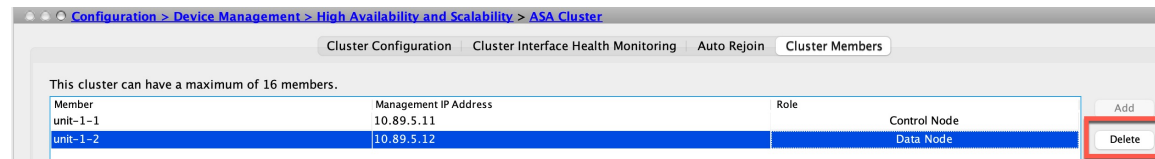
- a) **[クラスタメンバー (Cluster Members)]** タブをクリックすると、制御ノードのローカル IP アドレスを表示できます。クラスタリングを無効にした後、このアドレスに再接続する必要がありますため、制御ノードの IP アドレスをメモしておいてください。

図 2: 制御ノードの管理 IP アドレス



- b) [クラスタ メンバー (Cluster Members)] タブで、各データノードを選択して、[削除 (Delete)] をクリックします。

図 3: ノードの削除



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。

- c) [クラスタ構成 (Cluster Configuration)] タブで、[ASA クラスタに参加 (Participate in ASA cluster)] チェックボックスをオフにして、[適用 (Apply)] をクリックします。  
ASDM から切断されます。
- d) 制御ノードのローカル IP アドレスに ASDM を再接続します。
- e) この手順の残りの部分に従って、変更を続けます。この手順の完了後に各データノードがクラスタに再接続するように設定するには、各ノードを新しいノードとして追加するか、各データ ノードのコンソール ポートに移動して CLI でクラスタリングを再度有効にします。

例：

```
node2(config)# cluster group cluster1
node2(cfg-cluster)# enable
```

### ステップ 3 [Configure ASA cluster settings] チェックボックスをオンにします。

チェックボックスをオフにすると、設定が消去されます。パラメータの設定がすべて完了するまで、[Participate in ASA cluster] をオンにしないでください。

(注)

クラスタリングをイネーブルにした後、[Configure ASA cluster settings] チェックボックスをオフにする場合は、結果をよく理解したうえで行ってください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

### ステップ 4 次のブートストラップ パラメータを設定します。

- **[Cluster Name]** : クラスタに名前を付けます。名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。ノードごとに設定できるクラスタは 1 つだけです。クラスタのすべてのメンバが同じ名前を使用する必要があります。
- **[Member Name]** : このクラスタ メンバの固有の名前を 1 ～ 38 文字の ASCII 文字列で指定します。
- **[メンバーの優先順位 (Member Priority)]** : 制御ノード選定用に、このノードの優先順位を 1 ～ 100 の範囲内で設定します。1 が最高の優先順位です。
- **(ルーテッドモード、スパンド EtherChannel モード) [サイトインデックス (Site Index)]** : サイト間クラスタリングを使用している場合、このノードのサイト ID を設定し、1 ～ 8 のサイト固有の MAC アドレスが使用されるようにします。
- **(オプション) [Site Periodic GARP]** : 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ちます。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。各スパンド EtherChannel のノードと、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。

- **(オプション) [Shared Key]** : クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパストラフィック（接続状態の更新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。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。
- **(オプション) [Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]** : 接続の再分散を有効化します。このパラメータはデフォルトでは無効になっています。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。有効化されている場合、ASA は、1 秒あたりの接続数に関する情報を定期的に交換し、新しい接続を、1 秒あたりの接続数が多いデバイスから低負荷のデバイスにオフロードします。既存の接続は移動されません。さらに、このコマンドは 1 秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。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。デフォルトは 5 秒です。

接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては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新しい接続を再分散できません。

- **[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、残りのノードが負荷を処理できる場合は、ノード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。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、ノード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。

- (オプション) **[クラスタ内でこのデバイスのヘルスモニタリングを有効にする (Enable health monitoring of this device within the cluster)]** : クラスタノードのヘルスチェック機能を有効にして、ノードハートビートステータスメッセージ間の時間間隔を決定します。0.3 から 45 秒の間で選択できます。デフォルトは 3 秒です。**注** : 新しいノードをクラスタに追加していて、ASA またはスイッチのトポロジが変更される場合、クラスタが完成するまでこの機能を一時的にディセーブルにし、ディセーブルにされたインターフェイスのインターフェイスモニタリングもディセーブルにする必要があります (**[構成 (Configuration)]>[デバイス管理 (Device Management)]>[ハイアベイラビリティとスケラビリティ (High Availability and Scalability)]>[ASA クラスタ (ASA Cluster)]>[クラスタインターフェイスヘルスモニタリング (Cluster Interface Health Monitoring)]**)。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ノードのヘルスを確認するため、ASA のクラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
- (オプション) **[Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support]** : クラスタ制御リンクが EtherChannel として設定されていて (推奨)、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのノードがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバーインターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値 (0.8 秒など) に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はハートビートメッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。このオプションをイネーブルにすると、ASA はクラ

スタ制御リンクのすべての EtherChannel インターフェイスでハートビートメッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。

- (オプション) [デバウンス時間 (Debounce Time)] : ASA がインターフェイスを障害が発生していると思われ、クラスタからノード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、クラスタからノードを削除するまで指定されたミリ秒数待機します。EtherChannel がダウン状態からアップ状態に移行する場合 (スイッチがリロードされた、スイッチで EtherChannel が有効になったなど)、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。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。
- (オプション) [コンソール出力を複製する (Replicate console output)] : データノードから制御ノード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。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート 1 つだけです。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。
- (オプション) クラスタリング フロー モビリティをイネーブルにします。 [LISP インスタレーションの設定 \(50 ページ\)](#) を参照してください。
- (オプション) [Enable Director Localization for inter-DC cluster] : データセンターのサイト間クラスタ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イネーブルにします。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。
- (オプション) [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。ディレクター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。
- (オプション) [構成同期アクセラレーションを有効にする (Enable config sync acceleration)] : データノードが制御ノードと同じ構成の場合、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なっています。この機能は各ノードで設定され、制御ノードからデータノードに複製されません。

(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ノードに存在する場合、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。

- [並列構成のレプリケートを有効にする (Enable parallel configuration replicate)] : データノードと並行して設定変更が同期化されるように、制御ノードを有効にします。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。
- [フロー状態更新のキープアライブ間隔 (Flow State Refresh Keepalive Interval)] : フローオーナーからディレクタおよびバックアップオーナーへのフロー状態更新メッセージ (**clu\_keepalive** および **clu\_update** メッセージ) のキープアライブ間隔を 15 ～ 20 秒の範囲で設定します。デフォルトは 15 です。クラスタ制御リンクのトラフィック量を減らすために、デフォルトよりも長い間隔を設定することもできます。
- [Cluster Control Link] : クラスタ制御リンクインターフェイスを指定します。このインターフェイスは、設定されている名前を使用できません。使用可能なインターフェイスがドロップダウンリストに表示されます。
  - [Interface] : インターフェイス ID、できれば EtherChannel を指定します。サブインターフェイスと管理タイプインターフェイスは許可されません。
  - [IP Address] : IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。
  - [Subnet Mask] : サブネット マスクを指定します。
- [MTU] : クラスタ制御リンクインターフェイスの最大伝送ノードを指定します。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 (1400 ～ 9198 バイトの範囲) を指定します。デフォルトの MTU は 1500 バイトです。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。クラスタ制御リンクの MTU を最大値。たとえば、最大 MTU は 9198 バイトであるため、データインターフェイスの最大 MTU は 9098 になり、クラスタ制御リンクは 9198 に設定できます。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
- (オプション) [Cluster LACP] : スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel 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。

- [Virtual System MAC Address] : MAC アドレス形式である cLACP システム ID を設定します。すべての ASA が同じシステム ID を使用します。これは制御ノードによって自動生成され（デフォルト）、すべてのセカンダリノードに複製されます。あるいは *H.H.H* の形式で手動で指定することもできます。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。ただし、この値は、クラスタリングを無効にした場合にのみ変更できます。
- [System Priority] : 1 ～ 65535 の範囲でシステム プライオリティを設定します。プライオリティは意思決定を担当するノードの決定に使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。ただし、この値は、クラスタリングを無効にした場合にのみ変更できます。
- （オプション、Secure Firewall 4200）[VPN グループ化モード（VPN Grouping Mode）]。  
「分散型サイト間 VPN の設定（52 ページ）」を参照してください。

**ステップ 5** [Participate in ASA cluster] チェックボックスをオンにして、クラスタに参加します。

**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。任意のポート チャネル ID、冗長 ID、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 [Unmonitored Interfaces] ボックスにそのインターフェイスを移動します。

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、特定のノード上では障害が発生したが、別のノード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、そのノードはクラスタから削除されます。ノード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 がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みメンバであるか、またはクラスタに参加しようとしているかに

よって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。

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

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、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（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、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

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

- [Maximum Rejoin Attempts]：クラスタへの再結合の試行回数を定義するために、[Unlimited] または 0 ～ 65535 の範囲で値を設定します。0 は自動再結合を無効化します。デフォルト値は、クラスタ インターフェイスの場合は [Unlimited]、データ インターフェイス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。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [Interval Variation]：1 ～ 3 の範囲で設定して、間隔を増加させるかどうかを定義します（1：変更なし、2：直前の間隔の 2 倍、3：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタ インターフェイスの場合は [1]、データ インターフェイス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** [Apply] をクリックします。

## クラスタ TCP 複製の遅延の設定

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

## 手順

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

**ステップ 2** [Add] をクリックして次の値を設定します。

- [Replication delay] : 1 ～ 15 の範囲で秒数を設定します。
- [HTTP] : すべての HTTP トラフィックの遅延を設定します。
- [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す。

### 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 インスペクションについて

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

#### LISP について

VMware VMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンター サーバ モビリティをサポートするには、サーバの移動時にサーバへの入力ルートがルータが更新できる必要があります。Cisco Locator/ID Separation Protocol (LISP) のアーキテクチャ

は、デバイス ID、つまりエンドポイント ID (EID) をその場所、つまりルーティング ロケータ (RLOC) から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

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

## ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISP の統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフロー オーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーン」または「ヘアピン」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に、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

## ASA LISP の実装

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

1. (任意) ホストまたはサーバ IP アドレスに基づく検査対象 EID の制限：ファースト ホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。
2. LISP トラフィック インспек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上のフロー モビリティを有効にするサービス ポリシー：フロー モビリティはビジネスクリティカルなトラフィックに対して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 トラフィックおよび/または特定のサーバへのトラフィックのみに制限できます。
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 モビリティをイネーブルにするためのクラスタレベル設定：フロー モビリティは、クラスタ レベルでも有効にする必要があります。このオン/オフ トグルを使用すると、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

- [ASA クラスタの基本パラメータの設定 \(38 ページ\)](#) に従って、各クラスタ ユニットのサイト ID に割り当てます。
- LISP のトラフィックはデフォルト インспекション トラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

### 手順

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

- a) **[構成 (Configuration)] > [ファイアウォール (Firewall)] > [オブジェクト (Objects)] > [検査マップ (Inspect Maps)] > [LISP]**を選択します。
- b) **[Add]** をクリックして、新しいマップを追加します。
- c) 名前 (最大 40 文字) と説明を入力します。
- d) **Allowed-EID access-list** については、**[Manage]** をクリックします。

[ACL Manager] が開きます。

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

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

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

- g) **[OK]** をクリックします。

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

- a) **[構成 (Configuration)] > [ファイアウォール (Firewall)] > [サービスポリシールール (Service Policy Rules)]**を選択します。
- 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спекションを行うトラフィックを指定します。ファースト ホップ ルータと UDP ポート 4342 の ITR または ETR の間のトラフィックを指定します。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
- g) **[Next]** をクリックします。
- h) **[Rule Actions]** ウィザード ページまたはタブで、**[Protocol Inspection]** タブを選択します。
- i) **[LISP]** チェックボックスをオンにします。
- j) (オプション) **[Configure]** をクリックして、作成したインспекションマップを選択します。
- k) **[Finish]** をクリックして、サービス ポリシー ルールを保存します。

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

- a) **[構成 (Configuration)] > [ファイアウォール (Firewall)] > [サービスポリシールール (Service Policy Rules)]**を選択します。
- 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** **[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、**[クラスタリングフローモビリティを有効にする (Enable Clustering flow mobility)]** チェックボックスをオンにします。

**ステップ 5** **[Apply]** をクリックします。

## 分散型サイト間 VPN の設定

デフォルトでは、クラスタは集中型のサイト間 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。

### 分散型サイト間 VPN について

この分散モードでは、サイト間 IPsec IKEv2 VPN 接続がクラスタのノード全体に分散されます。VPN 接続をクラスタのノード間に分散させると、クラスタのキャパシティ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 機能を超えて VPN サポートを大幅に拡張できます。

### 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 ノード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ノード、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ノード。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ノード。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ノードで確立されます。
- **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ノードに送信された場合、そのノードは VPN セッションを所有しているノードにトラフィックを転送するために クラスタ制御リンクを使用します。
- **オーケストレータ**：オーケストレータ（常にクラスタ制御ノード）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 ノード 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。ノード 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

分散型サイト間 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、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 ノードが 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 ノードに送信された場合、トラフィックは VPN セッションを所有しているクラスタ ノードに転送されます。
- **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。
- **サイト間 VPN ハブ アンドスポーク構成**では、クライアントが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 ノード上にある可能性があります。

### クラスタ イベントの分散型 VPN の処理

| イベント             | 分散型 VPN                                                                                                       |
|------------------|---------------------------------------------------------------------------------------------------------------|
| ノード障害            | この障害が発生したノード上のすべてのアクティブセッションに対し、（別のノード上の）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別のノードに再割り当てされます。                    |
| クラスタ ノードの非アクティブ化 | 非アクティブになっているクラスタ ノード上のすべてのアクティブセッションに対し、（別のノード上の）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ノードにバックアップセッションを再割り当てします。 |

| イベント        | 分散型 VPN                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| クラスタ ノードの参加 | <p>新しいノードの VPN クラスタモードが分散型に設定されていない場合、制御ノードはモード変更を要求します。</p> <p>VPN モードに互換性があった後で、クラスタ ノードには、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。</p> |

## IPsec IKEv2 の変更

IKEv2 は、分散型サイト間 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、クラスタ全体で一貫しています。SPI には、タイムスタンプとクラスタ ノード 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 ノード 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。

## CMPv2

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

## 分散型サイト間 VPN のライセンスング

キャリア ライセンスは、クラスタの各メンバーで、分散型サイト間 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上にすることができます。

## 分散型サイト間 VPN の前提条件

### モデルのサポート

- Cisco Secure Firewall 4200

## クラスタの要件

- スパンド EtherChannel モード。
- ルーテッド ファイアウォール モード。

## 分散型サイト間 VPN のガイドライン

### ファイアウォールモード

分散型サイト間 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

分散型サイト間 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。

### 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、分散型サイト間 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

### その他のガイドライン

- 分散型サイト間 VPN モードでは IKEv2 IPsec サイト間 VPN のみがサポートされています。IKEv1 はサポートされていません。IKEv1 サイト間は、集中型 VPN モードでサポートされています。
- サイト間クラスタリングはサポートされていません。
- ダイナミック PAT は、分散型サイト間 VPN モードでは使用できません。

## 分散型サイト間 VPN を有効にします

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) 集中型または分散型の間で VPN モードを変更するには、クラスタ内のすべてのノードをリロードする必要があります。

### 始める前に

『VPN Configuration Guide』に従って、サイト間 VPN を設定します。

### 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** [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** [適用 (Apply)] をクリックします。

リロードするよう求められます。この設定は、リロード前にすべてのデータノードに複製されます。クラスタ内のすべてのノードがリロードされます。

## 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** [モニタリング (Monitoring)] > [ASA クラスタ (ASA Cluster)] > [ASA クラスタ (ASA Cluster)] > [クラスタ要約 (Cluster Summary)] > [VPN クラスタ要約 (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                                                                      | 制御ノードのみ                    |
| Sent request to move <i>number</i> sessions from <i>orig-member-name</i> to <i>dest-member-name</i>     | 制御ノードのみ                    |
| Failed to send session redistribution message to <i>member-name</i>                                     | 制御ノードのみ                    |
| Received request to move <i>number</i> sessions from <i>orig-member-name</i> to <i>dest-member-name</i> | データノードのみ                   |
| 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>                                    | 制御ノードのみ                    |

| Syslog フレーズ                                                           | 注       |
|-----------------------------------------------------------------------|---------|
| VPN session completed                                                 | 制御ノードのみ |
| 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。

## クラスタノードの管理

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、クラスタノードを管理できます。

### 制御ノードからの新しいデータノードの追加

制御ノードからクラスタにデータノードを追加できます。High Availability and Scalability ウィザードを使用してデータノードを追加することもできます。制御ノードからデータノードを追加すると、クラスタ制御リンクを設定でき、追加する各データノードにクラスタインターフェイス モードを設定できるというメリットがあります。

または、データノードにログインし、ノード上で直接クラスタリングを設定することもできます。ただし、クラスタリングをイネーブルにした後は、ASDMセッションが切断されるので、再接続する必要があります。

#### 始める前に

- マルチ コンテキスト モードでは、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。
- 管理ネットワーク上でブートストラップコンフィギュレーションを送信する場合は、データノードにアクセス可能な IP アドレスがあることを確認してください。

## 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 (ASA Cluster)] > [クラスタメンバー (Cluster Members)] の順に選択します。

**ステップ 2** [追加 (Add)] をクリックします。

**ステップ 3** 次のパラメータを設定します。

- [Member Name] : このクラスタ メンバの固有の名前を 1 ～ 38 文字の ASCII 文字列で指定します。
- [メンバーの優先順位 (Member Priority)] : 制御ノード選定用に、このノードの優先順位を 1 ～ 100 の範囲内で設定します。1 が最高の優先順位です。
- [クラスタ制御リンク (Cluster Control Link)] > [IP アドレス (IP Address)] : 制御ノードのクラスタ制御リンクと同じネットワーク上で、クラスタ制御リンクのこのメンバーに一意の IP アドレスを指定します。
- [展開オプション (Deployment Options)] 領域で、次の [Deploy By] オプションのいずれかを選択します。
  - [今すぐリモートユニットに CLI コマンドを送信する (Sending CLI commands to the remote unit now)] : ブートストラップ設定をデータノード (一時) 管理 IP アドレスに送信します。データノード管理 IP アドレス、ユーザ名、パスワードを入力します。
  - [生成された CLI コマンドを手動でコピーして、リモートユニットに貼り付ける (Copying generated CLI commands to paste on the remote unit manually)] : データノードの CLI でコマンドをカットアンドペーストできる、または ASDM の CLI ツールを使用できるようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。

Deployment Options

Deploy By: Copying generated CLI commands to paste on the remote unit manually

Commands to Deploy:

```
cluster interface-mode spanned force
clear configure cluster
interface GigabitEthernet0/4
no shutdown
cluster group cluster1
local-unit asa10
priority 2
cluster-interface GigabitEthernet0/4 ip 192.168.5.2 255.255.255.0
key test
enable as-data-node-noconfirm
```

**ステップ 4** [OK] をクリックし、さらに [Apply] をクリックします。

## 非アクティブノードになる

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 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。

## 制御ノードからのデータノードの非アクティブ化

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 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

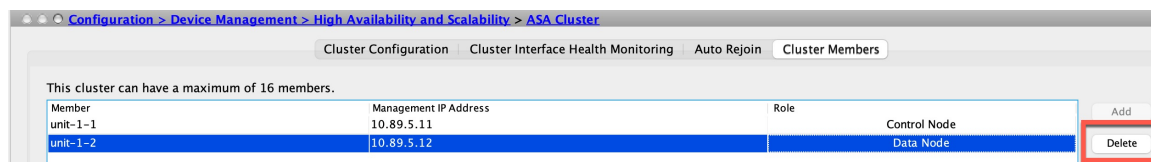
マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステムコンフィギュレーションモードに入っていない場合は、[Configuration]>[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

### 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)]>[クラスタメンバー (Cluster Members)] 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。

図 4: ノードの削除



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にするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。ただし、ASDMでクラスタリングを手動で無効にした場合、設定を保存してリロードしなかった場合は、ASDMでクラスタリングを再び有効にできます。リロード後、管理インターフェイスは無効になるため、コンソール アクセスがクラスタリングを再び有効にする唯一の方法です。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

### 手順

**ステップ 1** ASDM にまだアクセスしている場合は、再イネーブル化するノードに 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**

## クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各ノードの現在のコンフィギュレーションは（アクティブユニッ

トから同期されて) 同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IP アドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

### 始める前に

コンソールポートを使用する必要があります。クラスタのコンフィギュレーションを削除すると、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスがシャットダウンされます。

## 手順

**ステップ 1** データノードの場合、クラスタリングを次のように無効化します。

**cluster group cluster\_name no enable**

例 :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがデータノード上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

**ステップ 2** クラスタ コンフィギュレーションをクリアします。

**clear configure cluster**

ASA は、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

**ステップ 3** クラスタ インターフェイス モードをディセーブルにします。

**no cluster interface-mode**

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

**ステップ 4** バックアップコンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

**copy backup\_cfg running-config**

例 :

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

**ステップ 5** コンフィギュレーションをスタートアップに保存します。

**write memory**

**ステップ 6** バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

## 制御ノードの変更



**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ノードに、または特定のノードに送信するには、次の手順を実行します。**show** コマンドをすべてのノードに送信すると、すべての出力が収集されて現在のノードのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** 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

すべてのノードにコマンドを送信します。ノード名を指定した場合は、特定のノードに送信します。

**cluster exec [unit node\_name]** コマンド

例 :

```
ciscoasa# cluster exec show xlate
```

ノード名を表示するには、**cluster exec unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**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ノードから同時に TFTP サーバにコピーするには、制御ノードで次のコマンドを入力します。

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

複数の PCAP ファイル（各ノードから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にノード名が付加され、capture1\_asa1.pcap、capture1\_asa2.pcap などとなります。この例では、asa1 と asa2 はクラスタノード名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各ノードの EtherChannel 情報が表示されています。

```
ciscoasa# cluster exec show port-channel summary
control node(LOCAL):*****
Number of channel-groups in use: 2
Group Port-channel Protocol Span-cluster Ports
-----+-----+-----+-----+-----
1      Po1          LACP      Yes   Gi0/0 (P)
2      Po2          LACP      Yes   Gi0/1 (P)
slave:*****
Number of channel-groups in use: 2
Group Port-channel Protocol Span-cluster Ports
-----+-----+-----+-----+-----
1      Po1          LACP      Yes   Gi0/0 (P)
2      Po2          LACP      Yes   Gi0/1 (P)
```

# ASA クラスタのモニタリング

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、接続相手のノードとクラスタのその他のノードの情報が表示されます。また、このペインでプライマリノードを変更することができます。

- **[Cluster Dashboard]**

プライマリノードのホームページの [クラスタダッシュボード (Cluster Dashboard)] と [クラスタファイアウォールダッシュボード (Cluster Firewall Dashboard)] を使用してクラスタをモニタできます。

## クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

- **[Wizards] > [Packet Capture Wizard]**

クラスタ全体のトラブルシューティングをサポートするには、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、クラスタノード全体の 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、クラスタノード全体の [空きメモリ (Free Memory)] と [使用済みメモリ (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。

- [モニタリング (Monitoring)] > [ASA クラスター (ASA Cluster)] > [クラスター負荷のモニタリング (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。

## 分散型サイト間 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]

クラスターの制御ノードとデータ ノードの両方が表示されます。詳細については、任意のノード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。

## 分散型サイト間 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ー データ ノードが分散型 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.<br><br>および<br><br>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<br><br>または<br><br>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><br><br>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。

- サイト間 VPN セッションは **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レイヤ 4 ポートが設定されている場合、クラスターのシャーシの 1 つにのみ配布されます。クラスタ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
```

サイト間 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 Nexus 7K 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 およびレイヤ 4 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、そしてすべてのノード送信されます。

より即座に調整するには、クラスターの制御ノードで **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ー ノードに再配布できます。

## ASA クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

### ASA およびスイッチのコンフィギュレーションの例

次のコンフィギュレーション例は、ASA とスイッチ間の次のインターフェイスを接続します。

| ASA インターフェイス | スイッチインターフェイス           |
|--------------|------------------------|
| イーサネット 1/2   | GigabitEthernet 1/0/15 |
| イーサネット 1/3   | GigabitEthernet 1/0/16 |
| イーサネット 1/4   | GigabitEthernet 1/0/17 |
| イーサネット 1/5   | GigabitEthernet 1/0/18 |

## ASA の設定

### 各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

### ASA1 制御ユニットのブートストラップ設定

```
interface Ethernet1/6
  channel-group 1 mode on
  no shutdown
!
interface Ethernet1/7
  channel-group 1 mode on
  no shutdown
!
interface Port-channel1
  description Clustering Interface
!
cluster group Moya
  local-unit A
  cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
  priority 10
  key emphyri0
  enable noconfirm
```

### ASA2 データユニットのブートストラップ設定

```
interface Ethernet1/6
  channel-group 1 mode on
  no shutdown
!
interface Ethernet1/7
  channel-group 1 mode on
  no shutdown
!
interface Port-channel1
  description Clustering Interface
!
cluster group Moya
  local-unit B
  cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
  priority 11
  key emphyri0
  enable as-data-node
```

### 制御ユニットのインターフェイス設定

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface Ethernet1/2
  channel-group 10 mode active
  no shutdown
!
```

```
interface Ethernet1/3
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/4
 channel-group 11 mode active
 no shutdown
!
interface Ethernet1/5
 channel-group 11 mode active
 no shutdown
!
interface Management1/1
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

## Cisco IOS スイッチのコンフィギュレーション

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

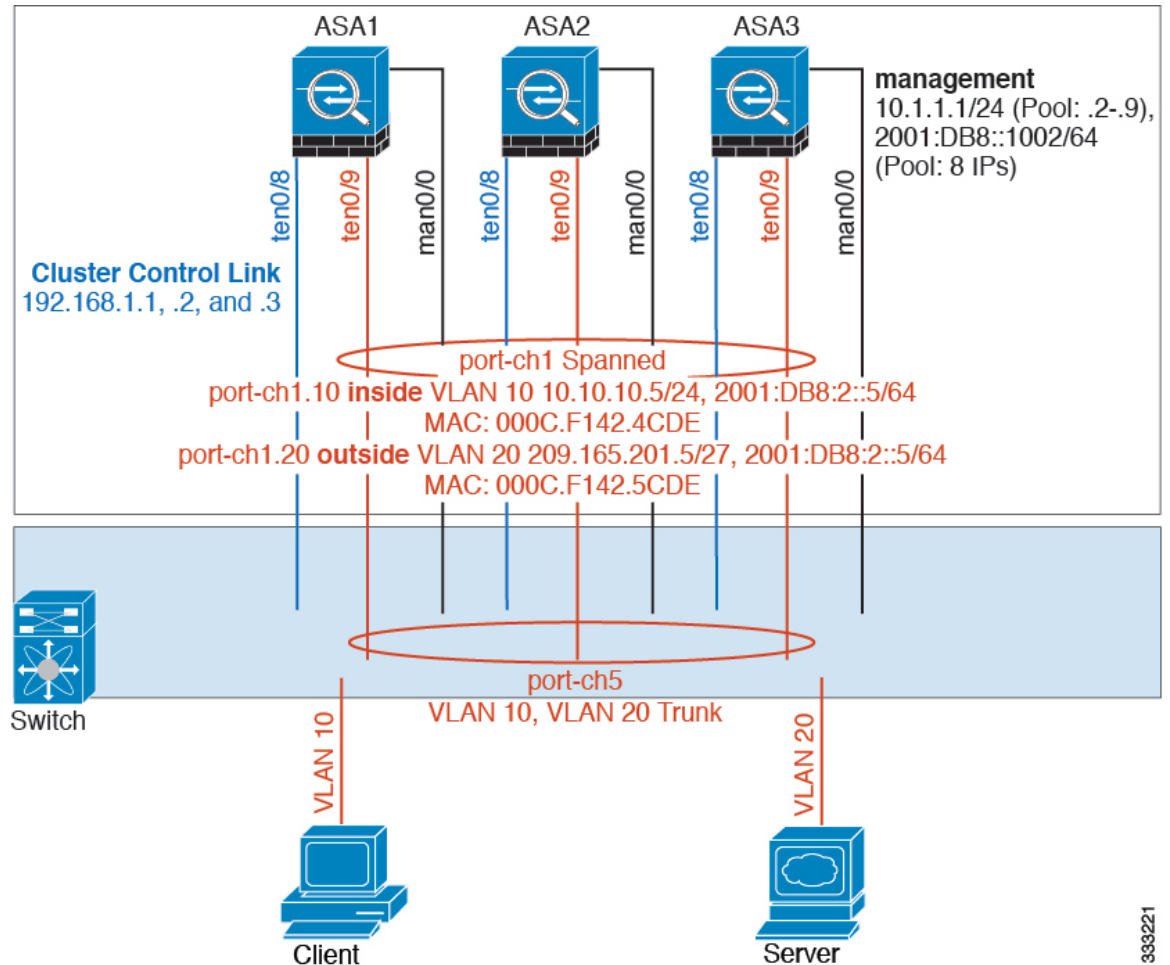
interface Port-channel11
```

```

switchport access vlan 401
switchport mode access

```

## 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。

## 各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

## ユニット 1 制御ユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asal
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

## ユニット 2 データユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

## ユニット 3 データユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-data-node
```

## 制御ユニットのインターフェイス設定

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
```

```

management-only
no shutdown

interface ethernet1/1
channel-group 1 mode active
no shutdown

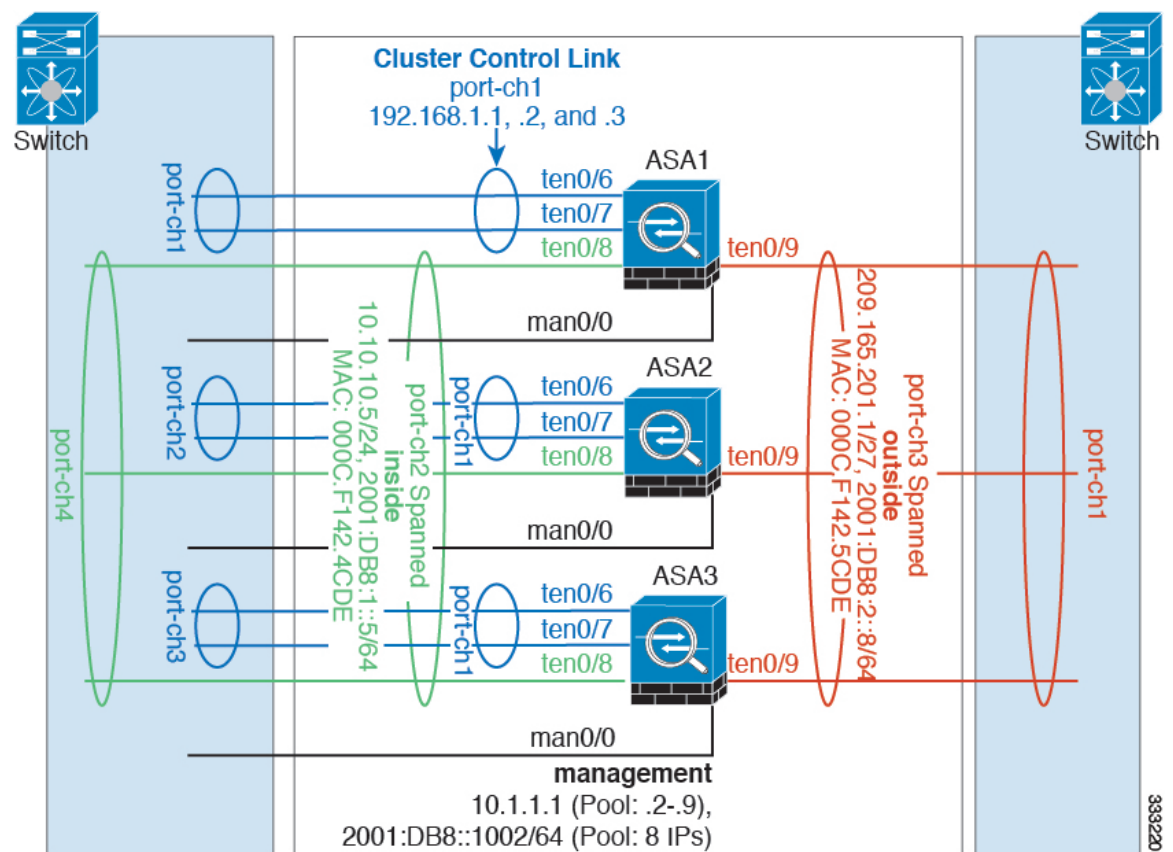
interface port-channel 1

interface port-channel 1.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE

```

## 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。

### 各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

### ユニット1 制御ユニットのブートストラップ設定

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa1
 cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
 priority 1
 key chuntheunavoidable
 enable noconfirm
```

### ユニット2 データユニットのブートストラップ設定

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa2
 cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
 priority 2
 key chuntheunavoidable
 enable as-data-node
```

### ユニット3 データユニットのブートストラップ設定

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown
```

```

interface ethernet 1/7
  channel-group 1 mode on
  no shutdown

interface port-channel 1
  description CCL

cluster group cluster1
  local-unit asa3
  cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
  priority 3
  key chuntheunavoidable
  enable as-data-node

```

### 制御ユニットのインターフェイス設定

```

ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
  nameif management
  ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
  ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
  security-level 100
  management-only
  no shutdown

interface ethernet 1/8
  channel-group 2 mode active
  no shutdown

interface port-channel 2
  nameif inside
  ip address 10.10.10.5 255.255.255.0
  ipv6 address 2001:DB8::1::5/64
  mac-address 000C.F142.4CDE

interface ethernet 2/1
  channel-group 3 mode active
  no shutdown

interface port-channel 3
  nameif outside
  ip address 209.165.201.1 255.255.255.224
  ipv6 address 2001:DB8::2::8/64
  mac-address 000C.F142.5CDE

```

## ルーテッドモードサイト間クラスタリングの OTV 設定

スパンド 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 は再送信されないのので、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 パケットをフラッ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 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

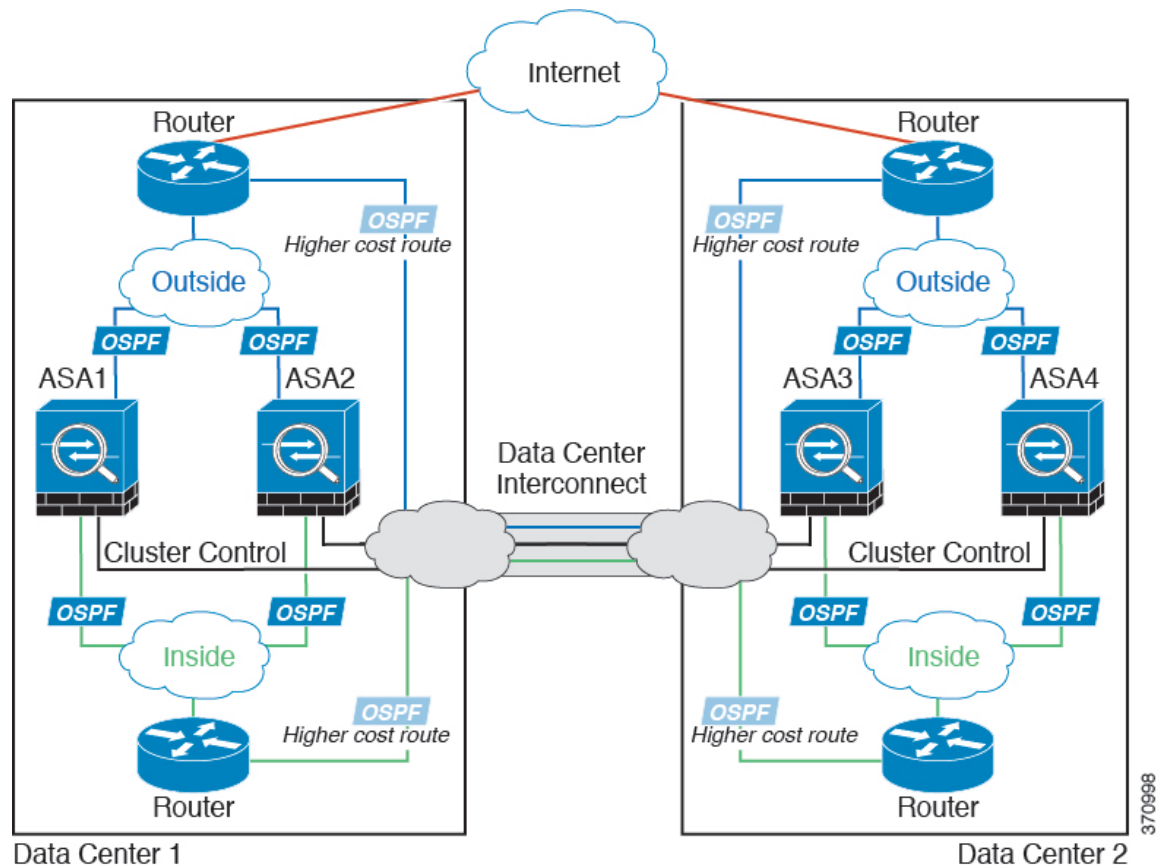
Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

# 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。

## 個別インターフェイス ルーテッド 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 ASA クラスタノードがある場合を示します。クラスタノードは、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。各データセンターの内部ルータと外部ルータは、OSPFとPBRまたはECMPを使用してクラスタメンバ間でトラフィックをロードバランスします。DCIに高コストルートを割り当てることにより、特定のサイトのすべての ASA クラスタノード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。1つのサイトのすべてのクラスタノード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 ASA クラスタノードに送られます。



## 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パンド 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 メンバがある場合を示します。クラスタ メンバは、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 メンバは、内部および外部両方のネットワークに対しスパンド 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。

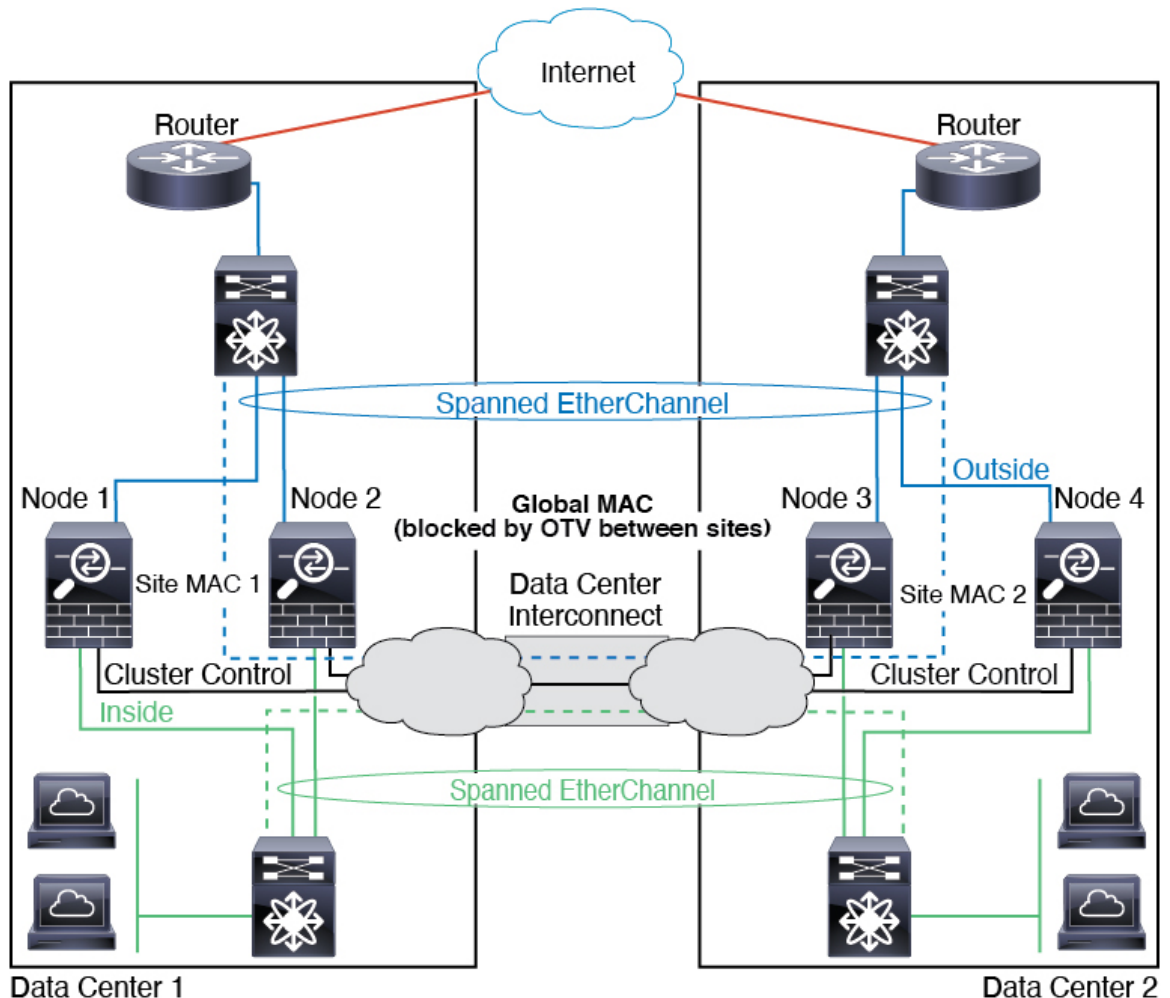
データ VLAN は、オーバーレイ トランスポート 仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロックするフィルタを追加する必要があります。1つのサイトのクラスタ ノードが到達不能になった場合、トラフィックが他のサイトのクラスタ ノードに送信されるようにフィルタを削除する必要があります。Vacl を使用して、グローバルの MAC アドレスのフィルタリングする必要があります。F3 シリーズラインカードを使用した Nexus など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、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。

このシナリオでは、次のようになります。

- 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。



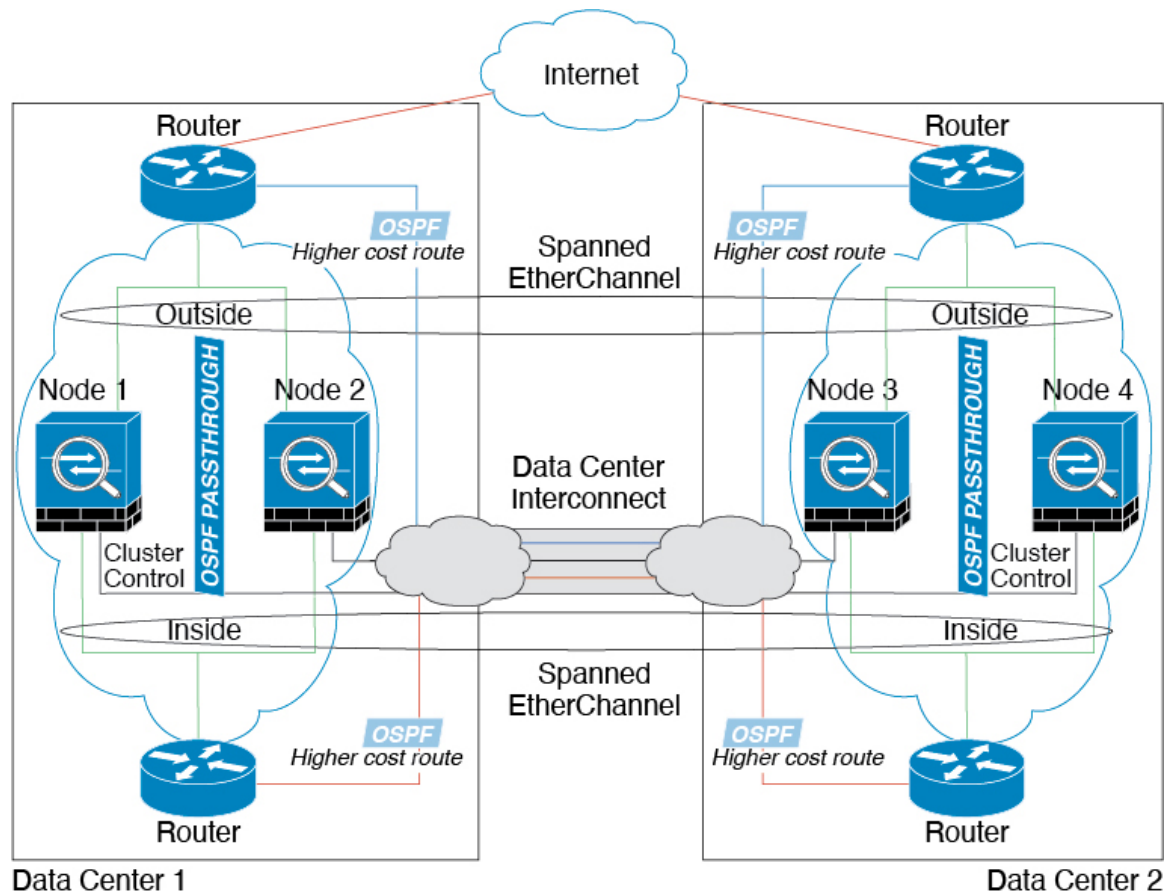
## スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

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がある場合を示します。クラスタメンバは、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シにスパンドされます。

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のシャーシではスパンドEtherChannelを使用しますが、スパンド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、スパンドEtherChannelをサイトローカルのEtherChannelとして認識します。

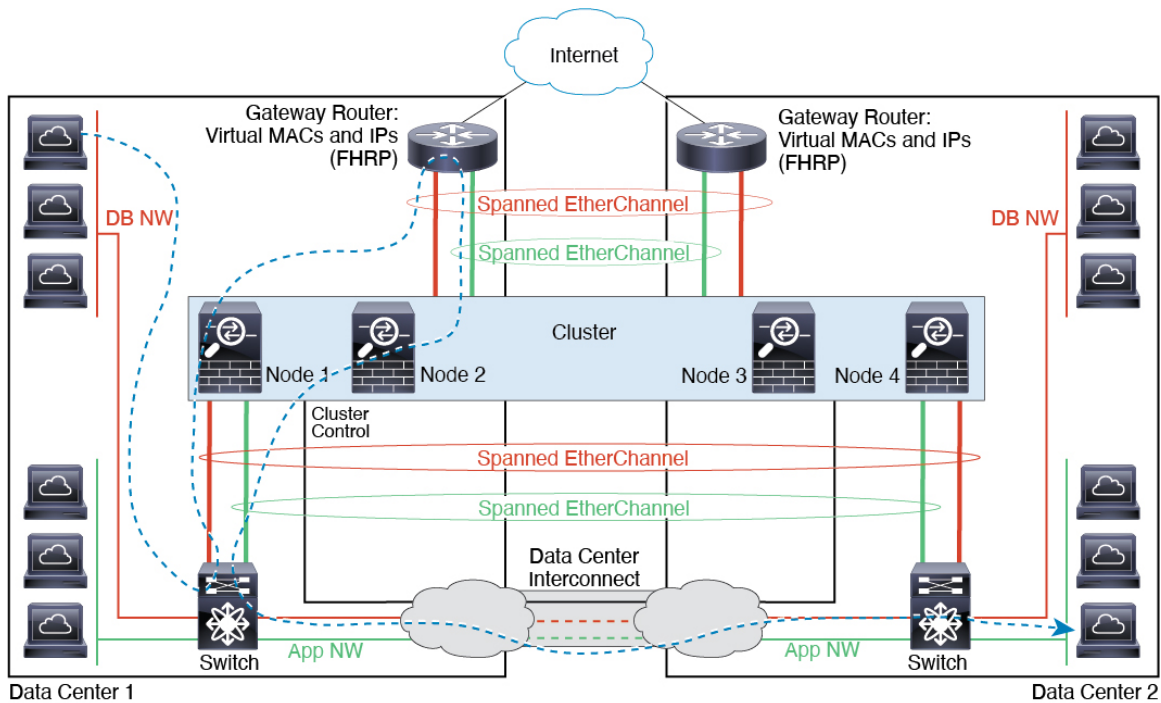


## スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

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 メンバがある場合を示します。クラスタ メンバは、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)
- 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す。
  - VPN ロード バランシング
  - Azure でのフェールオーバー
  - 統合ルーティングおよびブリッジング
  - 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。アカウンティ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
  - 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（スパンド EtherChannel モードのみ）

## 個々のノードに適用される機能

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ーを設定する場合は、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、アカウンティングの 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およびユーザに関連付けられた許可を引き続き中断なく運用する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。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティング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ティング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ティング開始と停止のメッセージを AAA サーバに送信します。

## 接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます ([Configuration] > [Firewall] > [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

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

## ICMP インスペクションとクラスタリング

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 エラーインスペクションが有効かどうかによって異なります。ICMP インスペク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 インスペク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

マルチキャスト ルーティングは、インターフェイス モードによって動作が異なります。

### スパンド EtherChannel モードでのマルチキャストルーティング

スパンド EtherChannel モードでは、ファストパス転送が確立されるまで、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。

### 個別インターフェイス モードでのマルチキャスト ルーティング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべて制御ユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

## 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 が使用される場合は、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。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリームルータは、メインクラスタ IP アドレスを指すマッピングアドレスについてはステティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。これは、スパンド EtherChannel の問題ではありません。クラスタインターフェイスには関連付けられた IP アドレスが 1 つしかないためです。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、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いまだ送信中の `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 `xlate` : 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。たとえば、`TCP/443` の `HTTPS TLS` と比較してずっと優れたパフォーマンスを発揮する代替手段として、`UDP/443` を用いる `Quick` プロトコルの使用が増加している場合、`UDP/443` に対し `per-session PAT` を有効にする必要があります。`H.323`、`SIP`、または `Skinny` などの `multi-session PAT` のメリットを活用できるトラフィックでは、関連付けられている `TCP` ポートに対し `per-session PAT` を無効にできます（それらの `H.323` および `SIP` の `UDP` ポートはデフォルトですでに `multi-session` になっています）。`per-session PAT` の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 次のインスペクション用のスタティック `PAT` はありません。
  - `FTP`
  - `PPTP`
  - `RSH`
  - `SQLNET`
  - `TFTP`
  - `XDMCP`
  - `SIP`
- 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

ここでは、クラスタリングでダイナミックルーティングを使用する方法について説明します。

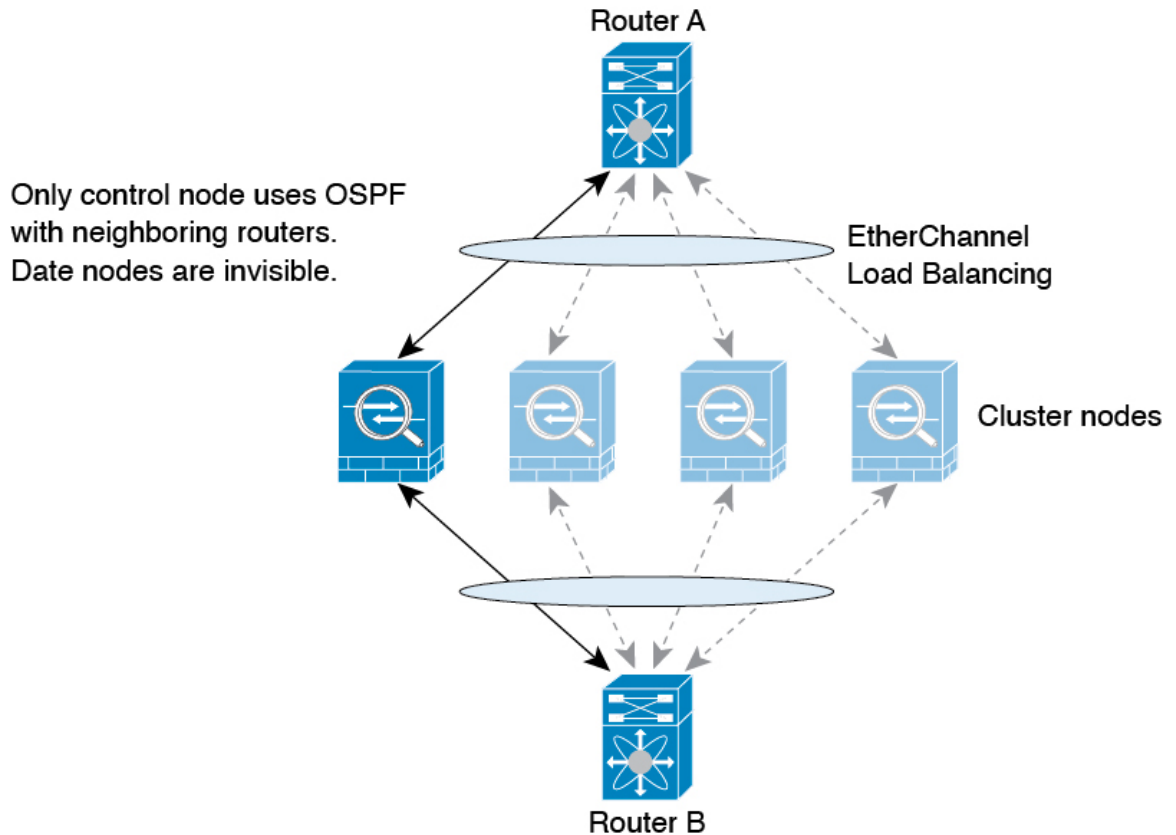
### スパンド `EtherChannel` モードでのダイナミック ルーティング



(注) IS-IS は、スパンド `EtherChannel` モードではサポートされていません。

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 5: スパンド *EtherChannel* モードでのダイナミック ルーティング



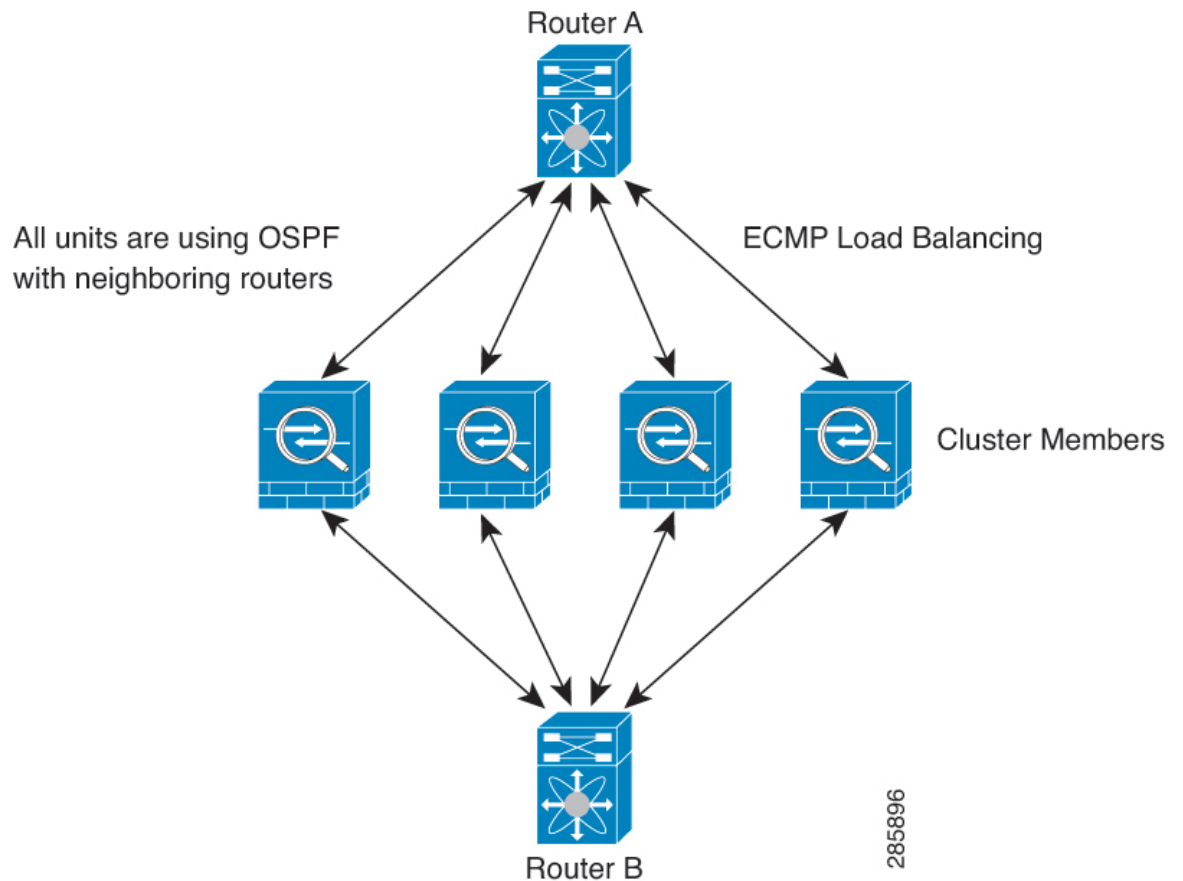
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバー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。

### 個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 6: 個別インターフェイスモードでのダイナミックルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロードバランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイスモードのクラスタピアとのネイバー関係を形成しません。



(注) 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべてのノードインターフェイスをまとめます。 [トラフィックゾーンの設定](#)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 インスペク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 ユーザは新しいノードに複製されません。SNMPv3 ユーザは、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。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製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とき、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 エクスポートア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。

## VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。



(注) リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノード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 EtherChannel アドレスに接続すると、接続が自動的に制御ノードに転送されます。PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカルアドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

## パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80% になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps (8 ユニット x 10 Gbps) の約 80% で 64 Gbps になります。

## 制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。



(注) 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。
5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。



(注) ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、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。

## クラスタ内のハイ アベイラビリティ

クラスタリングは、ノードとインターフェイスの正常性をモニターし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

### ノードヘルスマニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト 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、[制御ノードの選定 \(94 ページ\)](#) を参照してください。

## インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェアインターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

- スパンド EtherChannel：クラスタ Link Aggregation Control Protocol (cLACP) を使用します。各ノードは、リンクステータスおよび cLACP プロトコルメッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスが制御ノードに報告されます。
- 個別インターフェイス（ルーテッドモードのみ）：各ノードが自身のインターフェイスを自己モニタし、インターフェイスのステータスを制御ノードに報告します。

ヘルスモニタリングを有効にすると、すべての物理インターフェイス（主要な EtherChannel インターフェイスを含む）がデフォルトでモニタされるため、オプションでインターフェイスごとのモニタリングを無効化することができます。指名されたインターフェイスのみモニターできます。たとえば、指名された EtherChannel に障害が発生したと判断される必要がある場合、つまり、EtherChannel のすべてのメンバーポートはクラスタ削除をトリガーすることに失敗する必要があります（最小ポート バンドリング設定に応じて）。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済み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。EtherChannel の場合（スパニングかどうかを問わない）：確立済みメンバーのインターフェイスがダウン状態の場合、ASA はそのメンバーを 9 秒後に削除します。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に変化しても、ASA はクラスタから削除されません。EtherChannel 以外の場合は、メンバー状態に関係なく、ノードは 500 ミリ秒後に削除されます。

## 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ト情報は、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

クラスタノード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、。
- 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、。この動作は設定可能です。
- ノードの障害：ノード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て、クラスタリングがまだディセーブルになっているなら、ノードは再起動するとクラスタに再参加することを意味します。ASA は 5 秒ごとにクラスタへの再参加を試みます。
- 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。ノードは、5 分、10 分、20 分の間隔で自動的にクラスタに再参加しようとします。この動作は設定可能です。

「[ASA クラスタの基本パラメータの設定（38 ページ）](#)」を参照してください。

## 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す。

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

表 1: クラスタ全体で複製される機能

| Traffic       | 状態のサポート | 注意                    |
|---------------|---------|-----------------------|
| Up time       | Yes     | システムアップタイムをトラッキングします。 |
| ARP Table     | あり      | —                     |
| MAC アドレス テーブル | あり      | —                     |
| ユーザ アイデンティティ  | Yes     | AAA ルール（uauth）が含まれます。 |

| Traffic                             | 状態のサポート    | 注意                                                |
|-------------------------------------|------------|---------------------------------------------------|
| IPv6 ネイバー データベース                    | ○          | —                                                 |
| ダイナミック ルーティング                       | ○          | —                                                 |
| SNMP エンジン ID                        | [いいえ (No)] | —                                                 |
| Firepower 4100/9300 の分散型 VPN (サイト間) | Yes        | 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。オーナーがディレクタとして自分自身を選択すると、別のバックアップオーナーが選択されます。

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

サイト間クラスタリングのディレクタ 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あってもよく、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ト情報を送信します。

サイトの冗長性を有効にし、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。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**：フォワーダからのオーナーシ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を選択し、新しい接続を登録するためにそのディレクタ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は1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

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

サイト間クラスタリングの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とグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（SiteIdに基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにあってもよく、ローカルディレクタと同一ノードとすることもできます。元のオーナーに障害が発生すると、ローカルディレクタはこのサイトで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 識別子であり、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にオーナーを問い合わせしてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタの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指定できます。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。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。

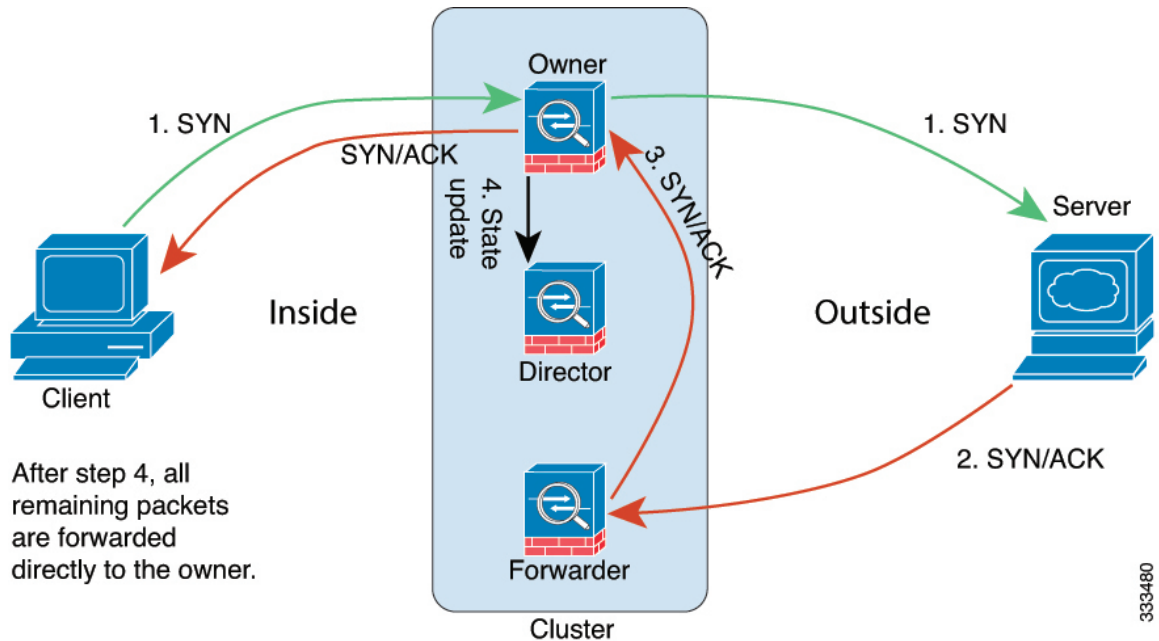
## 新しい接続の所有権

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制御リンクを介してオーナーノードに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1つのフローの両方向が同じノード

ドに到着するとともに、フローがノード間に均等に分散されるようにするためです。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。

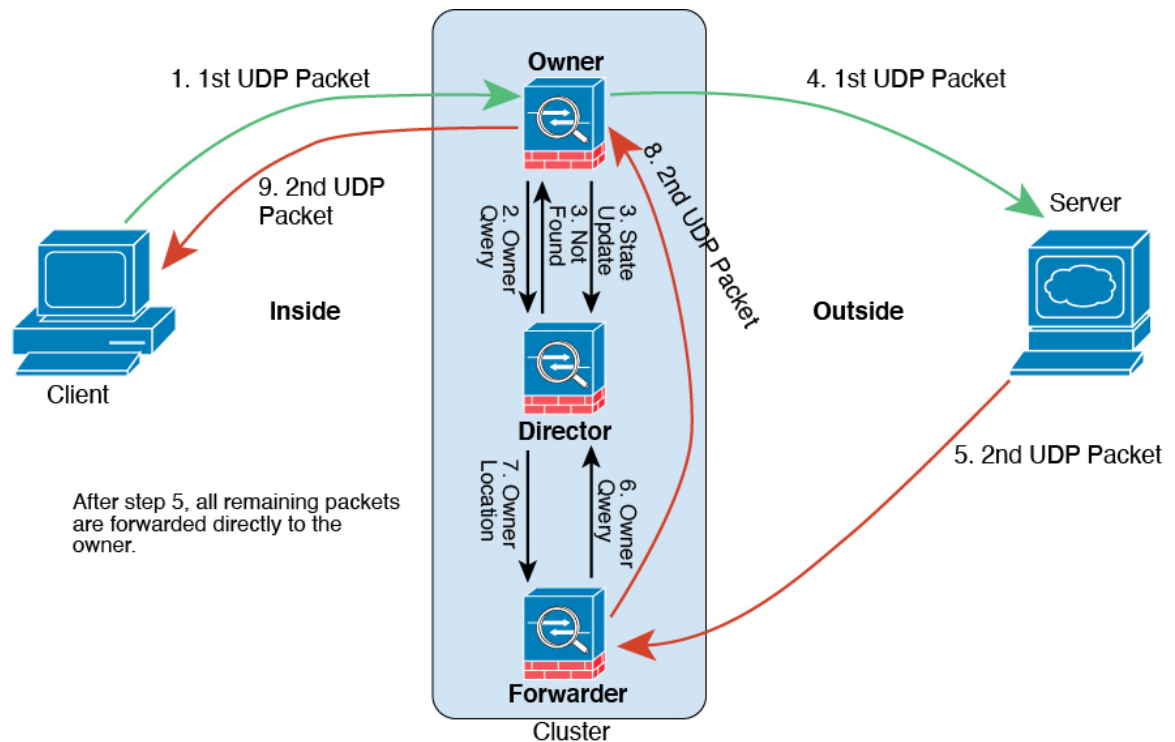


1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. 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 ステート情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他の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 7: 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。

- 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。
- 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。
- 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、サーバにパケットを転送します。
- 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
- 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。
- 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。

## 新しい TCP 接続のクラスタ全体での再分散

アップストリームルータまたはダウンストリームルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しい接続再分散を設定して、1 秒あたりの新しい接続数が多いノードから他のノードに新しい TCP フローをリダイレクトすることができます。既存のフローは他のノードには移動されません。

このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。

接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては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新しい接続を再分散できません。

# Cisco Secure Firewall 3100/4200 の ASA クラスタリングの履歴

| 機能名                                           | バージョン   | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Firewall 4200 のクラスタリングを使用した分散型サイト間 VPN | 9.23(1) | <p>Firepower 4200 上の ASA クラスタは、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）制御ノードだけでなく、ASA クラスタ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。</p> <p>新規または変更された画面：</p> <p>[Monitoring] &gt; [ASA Cluster] &gt; [ASA Cluster] &gt; [VPN Cluster Summary]</p> <p>[Monitoring] &gt; [VPN] &gt; [VPN Statistics] &gt; [Sessions]</p> <p>[Configuration] &gt; [Device Management] &gt; [High Availability and Scalability] &gt; [ASA Cluster]</p> <p>[Wizards] &gt; [Site-to-Site]</p> <p>[Monitoring] &gt; [VPN] &gt; [VPN Statistics] &gt; [Sessions]</p> <p>[Monitoring] &gt; [ASA Cluster] &gt; [ASA Cluster] &gt; [VPN Cluster Summary]</p> <p>[Monitoring] &gt; [ASA Cluster] &gt; [ASA Cluster] &gt; [System Resource Graphs] &gt; [CPU/Memory]</p> <p>[Monitoring] &gt; [Logging] &gt; [Real-Time Log Viewer]</p> |

| 機能名                                                                            | バージョン   | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クラスタリダイレクト: Cisco Secure Firewall 4200 非対称クラスタトラフィックのフローオフロードのサポート             | 9.23(1) | <p>非対称フローの場合、クラスタリダイレクトにより、転送ノードはハードウェアにフローをオフロードできます。この機能はデフォルトで有効になっています。</p> <p>既存のフローのトラフィックが別のノードに送信されると、そのトラフィックはクラスタ制御リンクを介してオーナーノードにリダイレクトされます。非対称フローは、クラスタ制御リンクに大量のトラフィックを作成する可能性があるため、フォワーダにこれらのフローをオフロードさせると、パフォーマンスが向上します。</p> <p>追加/変更された画面: <b>[構成 (Configuration)] &gt; [ファイアウォール (Firewall)] &gt; [高度 (Advanced)] &gt; [オフロードエンジン (Offload Engine)] &gt; [クラスタリダイレクトオフロード (Cluster Redirect Offload)]</b></p> |
| 分散型サイト間 VPN モードの Cisco Secure Firewall 4200 のクラスタ制御リンクのトラフィックの IPsec フローのオフロード | 9.23(1) | <p>分散型サイト間 VPN モードの非対称フローの場合、IPsec フローオフロードにより、フローオーナーは、クラスタ制御リンクを介して転送されたハードウェア内の IPsec トラフィックを復号できます。この機能は構成可能ではありません。IPsec フローのオフロードを有効にすると常に使用できます。</p> <p>追加/変更された画面: <b>[設定 (Configuration)] &gt; [ファイアウォール (Firewall)] &gt; [高度 (Advanced)] &gt; [IPsec オフロード (IPsec Offload)]</b></p>                                                                                                                                 |
| ノード参加時の MTU ping テスト                                                           | 9.23(1) | <p>クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。</p>                                                                                                                                                                                                                                                                                |
| クラスタノードの最大数を 16 に増加                                                            | 9.22(1) | <p>最大ノード数が 8 から 16 に増加しました。</p>                                                                                                                                                                                                                                                                                                                                                                                               |
| 個別インターフェイスモード                                                                  | 9.22(1) | <p>個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル IP アドレスを持ちます。各インターフェイスのメインクラスタ IP アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。</p> <p>アップストリームスイッチ上でロードバランシングを別途する必要があります。</p> <p>新規/変更されたコマンド: <b>cluster interface-mode individual</b></p> <p>新規/変更された画面: <b>Wizards &gt; &gt; High Availability and Scalability Wizard</b></p>                                    |

| 機能名                                         | バージョン   | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フローステータスの設定可能なクラスタキープアライブ間隔                 | 9.20(1) | <p>フローオーナーは、キープアライブ (clu_keepalive メッセージ) と更新 (clu_update メッセージ) をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。</p> <p>新規/変更された画面 : [設定 (Configuration)] &gt; [デバイス管理 (Device Management)] &gt; [高可用性と拡張性 (High Availability and Scalability)] &gt; [ASA クラスタ (ASA Cluster)] &gt; [クラスタの設定 (Cluster Configuration)]</p> |
| Secure Firewall 4200 でのクラスタリングのサポートが導入されました | 9.20(1) | Spanned EtherChannel モードでは、最大 8 つの Cisco Secure Firewall 4200 ノードをクラスタ化できます。                                                                                                                                                                                                                                                                                                                                    |
| 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 : <b>cluster control-node</b>、<b>enable as-data-node</b>、<b>prompt</b>、<b>show cluster history</b>、<b>show cluster info</b></p>                                                                                                                                                                           |
| Secure Firewall 3100 でのクラスタリングのサポートが導入されました | 9.17(1) | Spanned EtherChannel モードでは、最大 8 つの Cisco Secure Firewall 3100 ノードをクラスタ化できます。                                                                                                                                                                                                                                                                                                                                    |



## 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。