ASA クラスタのクラスタを展開する

クラスタリングを利用すると、複数の ASA 仮想 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。以下を使用して ASA 仮想 クラスタを展開できます。

- KVM
- VMware

（注） ルーテッド ファイアウォール モードのみがサポートされます。

（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 （46 ページ）」を参照してください。

ASA 仮想クラスタリングについて

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 つのデバイスとして機能します。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、隔離されたネットワーク。VXLAN インターフェイスを使用したクラスタ制御リンクと呼ばれます。レイヤ 3 物理ネットワーク上でレイヤ 2 仮想ネットワークとして機能する VXLAN により、ASA Virtual はクラスタ制御リンクを介してブロードキャスト/マルチキャストメッセージを送信できます。
- 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）。ASA Virtual 導入には、クラスタノードの管理に使用するManagement 0/0 インターフェイスが含まれています。

クラスタをネットワーク内に配置するときは、アップストリームおよびダウンストリームのルータは、レイヤ3の個別インターフェイスおよび次のいずれかの方法を使用して、クラスタとの間で送受信されるデータをロードバランシングできる必要があります。

- ポリシーベースルーティング：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 を使用してノード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：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 ルートを使用してノード間のロードバランシングを実行します。

（注） レイヤ 2 スパンド EtherChannels はサポートされません。

クラスタ ノード

クラスタノードは連携して動作し、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、各ノード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。

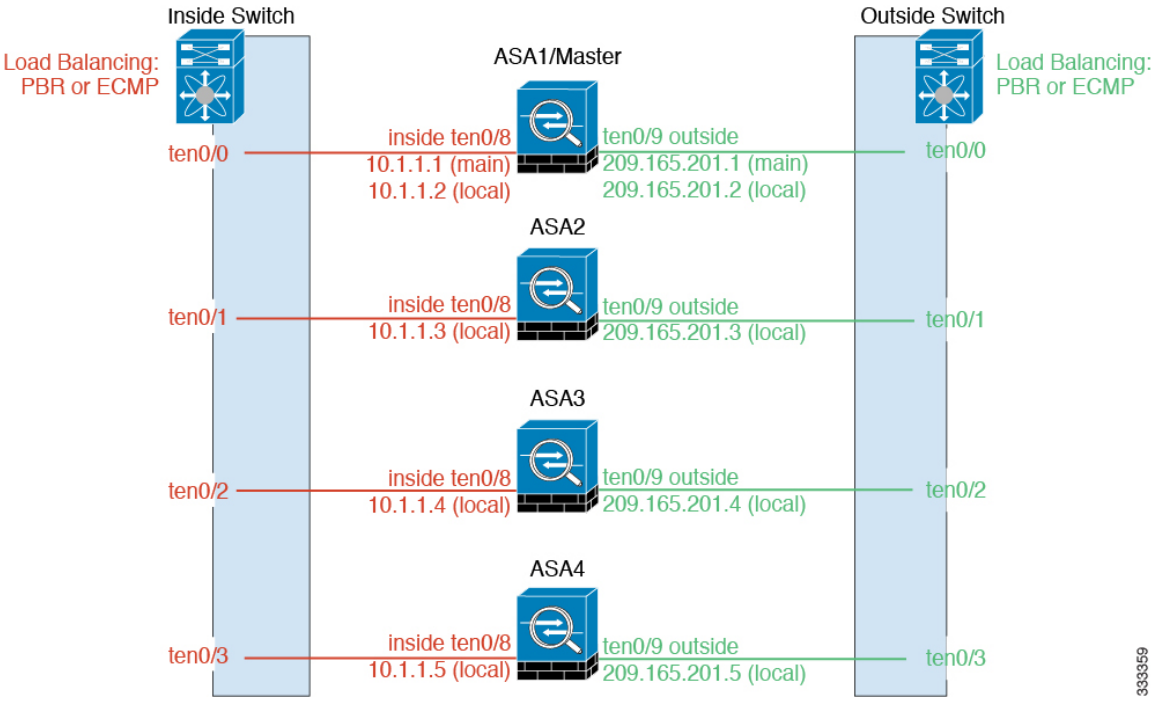
個々のインターフェイス

クラスターフェイスを個々のインターフェイスとして設定できます。

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。



（注） レイヤ 2 スパンド EtherChannels はサポートされません。

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

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。

クラスタ制御リンク

ノードごとに1つのインターフェイスをクラスタ制御リンク専用のVXLAN（VTEP）インターフェイスにする必要があります。VXLAN の詳細については、VXLAN インターフェイスを参照してください。

VXLAN トンネル エンドポイント

VXLANトンネルエンドポイント（VTEP）デバイスは、VXLANのカプセル化およびカプセル化解除を実行します。各VTEPには2つのインターフェイスタイプ（VXLAN Network Identifier（VNI）インターフェイスと呼ばれる1つ以上の仮想インターフェイスと、 VTEP間にVNIをトンネリングするVTEP送信元インターフェイスと呼ばれる通常のインターフェイス）がありますVTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

VTEP 送信元インターフェイス

VTEP送信元インターフェイスは、VNIインターフェイスに関連付けられる予定の標準のASA Virtualインターフェイスです。1 つの VTEP ソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。各 VTEP ソースインターフェイスには、同じサブネット上の IP アドレスがあります。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、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。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持

する仮想インターフェイスです。設定できる VNI インターフェイスは 1 つだけです。各 VNI インターフェイスは、同じサブネット上の IP アドレスを持ちます。

ピア VTEP

単一の VTEP ピアを許可するデータインターフェイス用の通常の VXLAN とは異なり、ASA Virtual クラスタリングでは複数のピアを設定できます。

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 仮想 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 DHCP またはクラスタ 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。クラスタ IP プールを使用している場合、リロードしてもクラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（制御ノードと同じメイン IP アドレスを使用するため）。さらに設定を行う場合は、コンソールポート（使用可能な場合）を使用する必要があります。

コンフィギュレーションの複製

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

ASA 仮想 クラスタの管理

ASA 仮想 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

すべてのノード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

管理用に、管理 0/0 インターフェイスを使用します。

（注） 管理インターフェイスの動的ルーティングを有効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。

管理 IP アドレスには、静的アドレスまたは DHCP を使用できます。

静的 IP アドレスを使用する場合は、常に現在の制御ノードに属するクラスタの固定アドレスであるメインクラスタ IP アドレスを使用できます。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、各ノード（現在の制御ノードも含まれます）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。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、現在の制御ノードに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、制御ノードを含む各ノードは、ローカル IP アドレスを使用してサーバーに接続します。

DHCP を使用する場合、ローカルアドレスのプールを使用したり、メインクラスタの IP アドレスを使用したりしません。

（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。

制御ノードの管理対データノードの管理

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、次の推奨ガイドラインに従う限り、ASA 仮想クラスタリングを利用できます。

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

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 仮想クラスタリングの要件と前提条件 （9 ページ）

- サイト間のガイドライン：ASA 仮想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 （32 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 （26 ページ）
- サイト冗長性の有効化：ASA クラスタの基本パラメータの設定 （26 ページ）
- サイト間での例：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 （45 ページ）

ASA 仮想クラスタリングのライセンス

各クラスタノードには、同じモデルライセンスが必要です。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

（注） ASA 仮想 を登録解除してライセンスを解除した場合、ASA 仮想 をリロードすると、重大なレート制限状態に戻ります。ライセンスのない、パフォーマンスの低いクラスタノードは、クラスタ全体のパフォーマンスに悪影響を及ぼします。すべてのクラスタノードのライセンスを保持するか、ライセンスのないノードを削除してください。

ASA 仮想クラスタリングの要件と前提条件

モデルの要件

- ASAv30、ASAv50、ASAv100
- 次のプライベート クラウド サービス：
  - KVM
  - VMware
- 2x8 展開構成に含まれる「2 つ」のホスト上のクラスタ内で最大 16 ノード。2 つのホストのそれぞれに最大 8 つの ASAv を展開（2x8）することをお勧めします。これにより、16 ノードのクラスタになります。

ASA 仮想プラットフォームおよびソフトウェア要件

クラスタ内のすべてのノード：

- 同じモデルである必要があります。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のノードに一致するようにすべてのノードで制限されます。
- 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。
- 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、制御ノードと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。

ASA 仮想クラスタリングに関するガイドライン

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。

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（ASA 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルスチェック機能を無効にし、無効化し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無効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、インターフェイス ヘルスチェック機能を再度有効にできます。
- ノードを既存のクラスタに追加したときや、ノード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。
- データインターフェイスの VXLAN はサポートしていません。クラスタ制御リンクのみが VXLAN をサポートします。
- クラスタ内のすべてのノード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ノード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。

ASA 仮想クラスタリングのデフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モ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。

Day0 設定を使用した ASA 仮想 クラスタリングの設定

制御ノード Day0 設定

制御ノードの次の Day0 設定には、ブートストラップ設定と、それに続くデータノードに複製されるインターフェイス設定が含まれています。太字のテキストは、データノードの Day0 設定で変更する必要がある値を示しています。

（注） この設定には、クラスタ中心の設定のみが含まれます。Day0 設定には、ライセンス、SSH アクセス、ASDM アクセスなどの他の設定も含める必要があります。Day0 設定の詳細については、スタートアップガイドを参照してください。

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
```

```
security-level 0
ip address 10.6.6.51 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit A
cluster-interface vni1 ip 10.2.2.1 255.255.255.0
priority 1
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

データノード Day0 設定

データノードの次の Day0 設定には、ブートストラップ設定のみが含まれています。太字のテキストは、制御ノードの Day0 設定から変更する必要がある値を示しています。

（注） この設定には、クラスタ中心の設定のみが含まれます。Day0 設定には、ライセンス、SSH アクセス、ASDM アクセスなどの他の設定も含める必要があります。Day0 設定の詳細については、スタートアップガイドを参照してください。

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.52 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
```

```
local-unit B
cluster-interface vni1 ip 10.2.2.2 255.255.255.0
priority 2
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

展開後のASA 仮想クラスタリングの設定

ASA 仮想 の展開後に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。

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。

インターフェイスの設定

のクラスタ インターフェイス モードと、制御ノードのインターフェイスを設定します。インターフェイス構成は、クラスタに参加するときにデータノードに複製されます。クラスタ制御リンクの構成は、ブートストラップコンフィギュレーション手順で説明されていることに注意してください。

の制御ノードでクラスタ インターフェイス モードを設定する

クラスタリングを有効にする前に、個々のインターフェイスを使用するようにファイアウォールを変換する必要があります。クラスタリングによって使用できるインターフェイスの種類が制限されるため、このプロセスでは、既存の設定に互換性のないインターフェイスがあるかどうかを確認し、サポートされていないインターフェイスを設定できないようにします。

（注） 制御ノードからデータノードを追加しない場合は、制御ノードだけでなく全ノード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。制御ノードからデータノードを追加する場合は、ASDMがデータノードのインターフェイスモードを自動的に設定します。

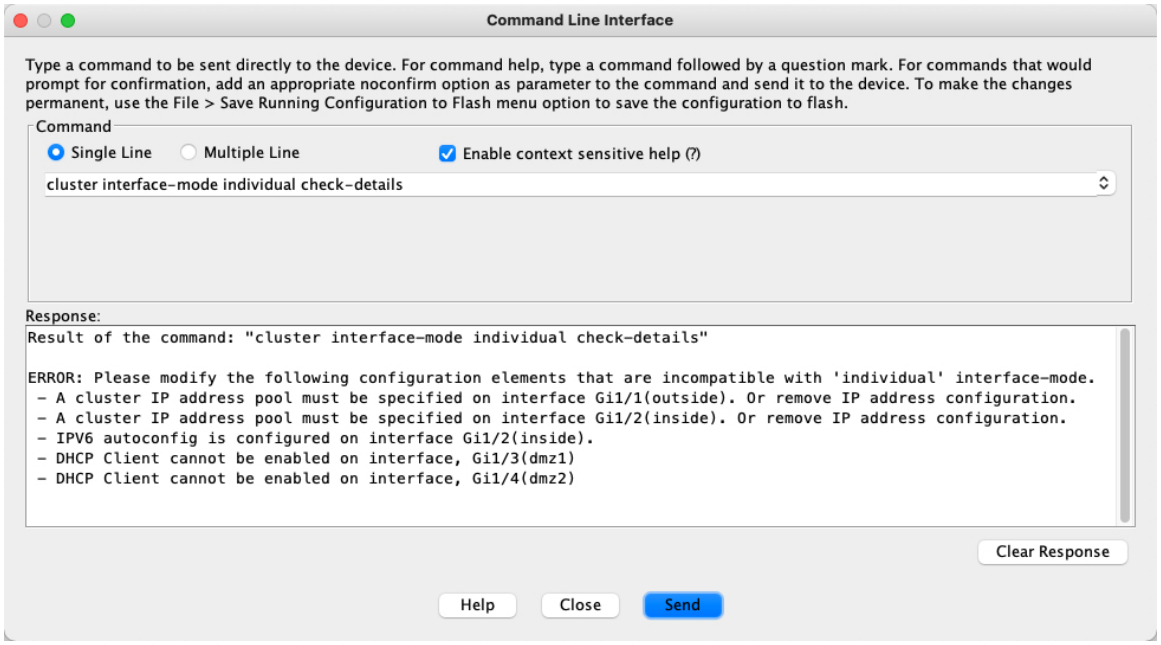
手順

ステップ 1 制御ノードの 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 check-details

例：

図 *1:* コマンド ライン インターフェイス アウトプット



注意

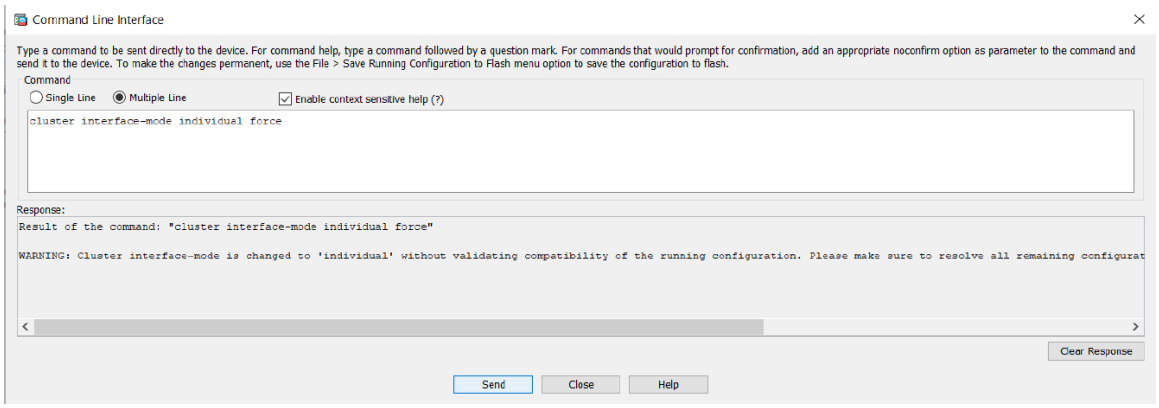
インターフェイス モードを設定した後は、常にインターフェイスに接続できるようになります。ただし、クラスタリング要件に適合するように管理インターフェイスを設定する前にASAをリロードすると（たとえば、クラスタ IP プールを追加するため、または DHCP から IP アドレスを取得するため）、クラスタと互換性のないインターフェイス コンフィギュレーションが削除されるため、再接続できなくなります。その場合は、可能であればコンソールポートに接続してインターフェイス コンフィギュレーションを修正する必要があります。

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 force

例：

図 *2:* インターフェイスモードの設定



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。

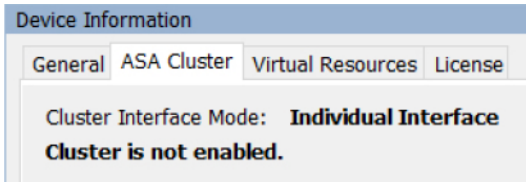
force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

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（可能な場合）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。

図 *3 : ASDM* の更新が必要



制御ノードでのクラスタ制御リンクの設定

クラスタに参加する前に、クラスタ制御リンクインターフェイスのVXLANインターフェイスを実行します。VXLAN およびクラスタ制御リンクの詳細については、クラスタ制御リンク（5 ページ） を参照してください。

始める前に

クラスタ制御リンクで使用するジャンボフレーム予約を有効にして、クラスタ制御リンクの MTU を推奨値に設定できるようにします。ジャンボフレームを有効にすると、ASA がリロードされます。**[設定（Configuration）]** > **[デバイスのセットアップ（Device Setup）]** > **[インターフェイス設定（Interface Settings）]** > **[インターフェイス（Interfaces）]** 画面を確認します。

（注） 各ノードで個別にジャンボフレーム予約を有効にする必要があります。

手順

ステップ 1 ネットワーク オブジェクト グループ内の VXLAN トンネルエンドポイント（VTEP）ピア IP アドレスを識別します。

ネットワーク オブジェクト グループの詳細については、「**Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**」ページ、および ASA ファイアウォール コンフィギュレーション ガイドの「Objects for Access Control」の章を参照してください。

VTEP 間の基礎となる IP ネットワークは、VXLAN ネットワーク識別子（VNI）インターフェイスが使用するクラスタ制御リンクネットワークから独立しています。各 VTEP ソースインターフェイスには、同じサブネット上の IP アドレスがあります。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、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。

ステップ 2 VTEP 送信元インターフェイスを設定します。

VTEP 送信元インターフェイスは、VNI インターフェイスに関連付けられる予定の標準の ASA 仮想 インターフェイスです。1 つの VTEP ソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。

a) **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）]** の順に選択し、VTEP 送信元インターフェイスに使用するインターフェイスを編集します。
b) **インターフェイス名**を設定します。
c) [VTEP Source Interface (cluster)] チェックボックスをオンにします。
d) [Enable Interface] をオンにします。
e) 静的 IPv4 アドレスを設定します。

IP アドレスは、ネットワーク オブジェクト グループのピアの 1 つとして含める必要があります。

f) [Advanced] タブをクリックし、MTU をデータインターフェイスの最大 MTU よりも少なくとも 154 バイト高く設定します。

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（100 バイト）および VXLAN のオーバーヘッド（54 バイト）にも対応する必要があります。MTU を 1554 ～ 9198 バイトの間で設定します。デフォルトの MTU は 1554 バイトです。データインターフェイスが 1500 に設定されている場合は、クラスタ制御リンクの MTU を 1654 に設定することをお勧めします。この値にはリロードが必要なジャンボフレームの予約が必要です。

たとえばジャンボ フレームを使用している場合、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 9044 になり、クラスタ制御リンクは 9198 に設定できます。

g) [**OK**] をクリックします。

ステップ 3 VTEP ソースインターフェイスをネットワーク仮想化エンドポイント（NVE）に関連付けます。

a) **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [VXLAN]** の順に選択します。

b) （任意） デフォルト 4789 から変更する場合は、[VXLAN Destination Port] の値を入力します。

c) [Enable Network Virtualization Endpoint encapsulation using VXLAN] チェック ボックスをオンにします。

d) ドロップダウン リストから [VTEP Tunnel Interface] を選択します。

e) [Configure Packet Recipient] チェックボックスをオンにし、[Peer Group] オプションボタンをクリックして、作成したピアグループを選択します。

f) [Apply] をクリックします。

ステップ 4 VNI インターフェイスを作成します。

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。設定できる VNI インターフェイスは 1 つだけです。

a) **[構成（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）]**の順に選択し、**[追加（Add）] > [VNIインターフェイス（VNI Interface）]**をクリックします。

b) [VNI ID] は 1 ～ 10000 の間で入力します。

この ID は内部インターフェイス識別子です。

c) [VNI Segment ID] は 1 ～ 16777215 の間で入力します。

セグメント ID は VXLAN タギングに使用されます。

d) [NVE Mapped to VTEP Interface] チェック ボックスをオンにします。

この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

e) [OK]、続いて [Apply] をクリックします。

個々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。管理に静的 IP アドレスを使用する場合は、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を変更する必要がある場合があります。他のインターフェイスについては、クラスタリングを有効化する前またはその後に設定で

きます。完全なコンフィギュレーションが新しいクラスタノードと同期するように、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。

ここでは、個々のインターフェイスが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。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、常に現在の制御ノードに属します。すべてのデータインターフェイスは個別インターフェイスである必要があります。

管理インターフェイスでは、IP アドレスプールを設定するか、DHCP を使用できます。管理インターフェイスのみが DHCP からのアドレスの取得をサポートしています。DHCP を使用する場合は、この手順を使用しないでください。代わりに、通常どおりに設定します（ルーテッドモードの一般的なインターフェイス パラメータの設定を参照）。

始める前に

- （オプション）サブインターフェイスを設定します。
- 管理インターフェイスには、静的アドレスを使用するか、DHCP を使用できます。静的 IP アドレスを使用しており、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、将来のデータノードの現在の IP アドレスは一時的なものです。
  - 各メンバには、制御ノード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. 制御ノードに 10.1.1.1 を設定します。
    2. 他のノードには、10.1.1.2、10.1.1.3、10.1.1.4 を使用します。
    3. 制御ノードのクラスタの 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、制御ノード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、現在の制御ノードのものです。

    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す。

手順

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

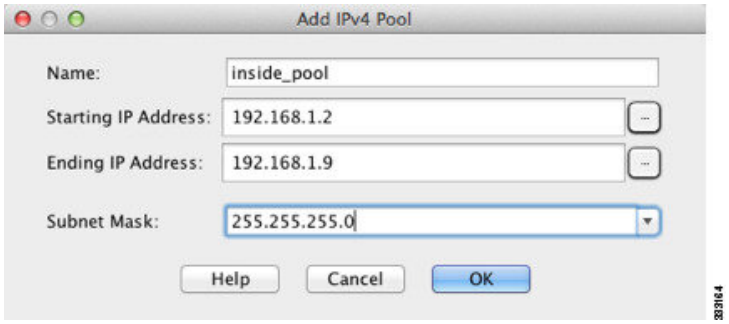
ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。[Static IP] を選択します。DHCP と PPPoE はサポートされません。

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。

a) [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。

b) [Add] をクリックします。

c) 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。



d) [OK] をクリックして、新しいプールを作成します。

e) 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。

f) （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。

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。

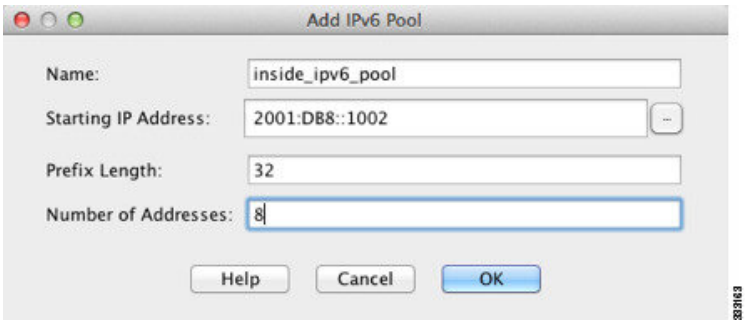
[Enable address autoconfiguration] オプションはサポートされません。リンクローカルアドレスの手動設定もサポートされていません。

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

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、「2001:0DB8::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。

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。

始める前に

- クラスタ制御リンクインターフェイスに使用する VXLAN VTEP ソース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 [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。

- **[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 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有効化または無効化）は、ヘルスチェックを無効にし、無効化したインターフェイスのモニタリングも無効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。

  - [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決定します。範囲は 0.3 ～ 45 秒です。デフォルトは 3 秒です。

- （オプション）[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]：VTEP ソースインターフェイスの最大伝送ユニットを指定します。データインターフェイスの最大 MTU より少なくとも 154 バイト高い値を指定します。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（100 バイト）および VXLAN のオーバーヘッド（54 バイト）にも対応する必要があります。MTU を 1554 ～ 9198 バイトの間で設定します。デフォルトの MTU は 1554 バイトです。データインターフェイスが 1500 に設定されている場合は、クラスタ制御リンクの MTU を 1654 に設定することをお勧めします。この値にはジャンボフレームの予約が必要です。たとえばジャンボ フレームを使用している場合、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 9044 になり、クラスタ制御リンクは 9198 に設定できます。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**：まだ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。

ステップ 3 [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有効化または無効化）は、ヘルスチェックを無効にし、無効化したインターフェイスのモニタリングも無効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 4 [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 5 [Finish] をクリックします。

ステップ 6 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。

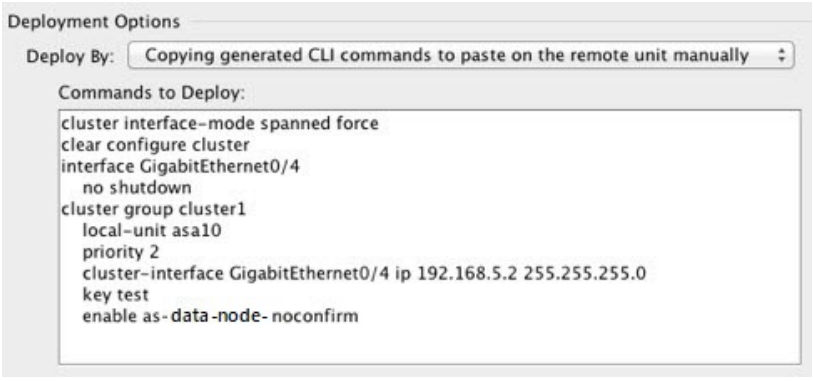
（注）
場合によっては、ウィザードの完了後にクラスタに参加した際にエラーが発生する可能性があります。ASDM が切断されていると、ASDM はそれに続くエラーを ASA から受信しません。ASDM に再接続した後もクラスタリングがディセーブルの場合は、ASA コンソール ポートに接続して、クラスタリングがディセーブルになっている詳細なエラー状況を判断する必要があります。たとえば、クラスタ制御リンクがダウンしている可能性があります。

ステップ 7 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 8 [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

Day 0 設定の一環として、またはクラスタの展開後に、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。

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、各ノードでクラスタ制御リンクを事前設定する必要があります。制御ノードでのクラスタ制御リンクの設定 （17 ページ）を参照してください。

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クラスタ（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 [Cluster Configuration] タブにあります。

ステップ 2 [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 3 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。
- **[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。
- （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）[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ーラビリティ（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）[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見なし、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。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 インスペクションの設定 （34 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。ディレクタローカリゼーションにより、追加のディレクタ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 ディレクタと、任意のサイトに配置できるグローバル ディレクタです。所有者とディレクタ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 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。
  - **インターフェイス**：VNI インターフェイスを指定します。
  - [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]：VTEP ソースインターフェイスの最大伝送ユニットを指定します。データインターフェイスの最大 MTU より少なくとも 154 バイト高い値を指定します。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（100 バイト）および VXLAN のオーバーヘッド（54 バイト）にも対応する必要があります。MTU を 1554 ～ 9198 バイトの間で設定します。デフォルトの MTU は 1554 バイトです。データインターフェイスが 1500 に設定されている場合は、クラスタ制御リンクの MTU を 1654 に設定することをお勧めします。この値にはジャンボフレームの予約が必要です。たとえばジャンボ フレームを使用している場合、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 9044 になり、クラスタ制御リンクは 9198 に設定できます。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。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。**注**：まだジャンボフレームの予約を有効にしていない場合は、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。

ステップ 4 [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 5 [適用（Apply）] をクリックします。

インターフェイス ヘルスモニタリングおよび自動再参加設定の設定

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。ヘルスモニタリングは VLAN サブインターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

手順

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

ステップ 2 [Monitored Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックして [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。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、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。ヘルスモニタリングは VLAN サブインターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

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）を行うときには、ヘルスチェック機能を無効にし（**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**）、無効化したインターフェイスのモニタリングも無効にしてくださいトポロジの変更が完了して、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をルータが更新できる必要があります。Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID、つまりエンドポイント ID（EID）をその場所、つまりルーティング ロケータ（RLOC）から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

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

ASA LISP のサポート

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

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

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。
- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々の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 インスペクション：ASA は、ファーストホップルータと ITR または ETR の間で送信される EID 通知メッセージにおいて、UDP ポート 4342 上の LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。LISP トラフィックにはディレク

タが割り当てられておらず、LISP トラフィック自体はクラスタ状態の共有に参加しないことに注意してください。

3. 指定されたトラフィック上のフロー 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 インスペクションの設定

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 （26 ページ） に従って、各クラスタ ユニットをサイト ID に割り当てます。
- LISP のトラフィックはデフォルト インスペクション 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 インスペクション 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 インスペク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 インスペクションは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービス ポリシーを適用する必要はありません。トラフィックが両方向のクラスに一致する場合、ルールを適用するインターフェイスに出入りするトラフィックのすべてが影響を受けます。

d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)]をオンにします。
e) [Next] をクリックします。
f) インスペクションを行うトラフィックを指定します。ファースト ホップ ルータと UDP ポート 4342 の ITR または ETR の間のトラフィックを指定します。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
g) [Next] をクリックします。
h) [Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。
i) [LISP] チェックボックスをオンにします。
j) （オプション）[Configure] をクリックして、作成したインスペクション マップを選択します。
k) [Finish] をクリックして、サービス ポリシー ルールを保存します。

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

a) **[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。

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

- 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。

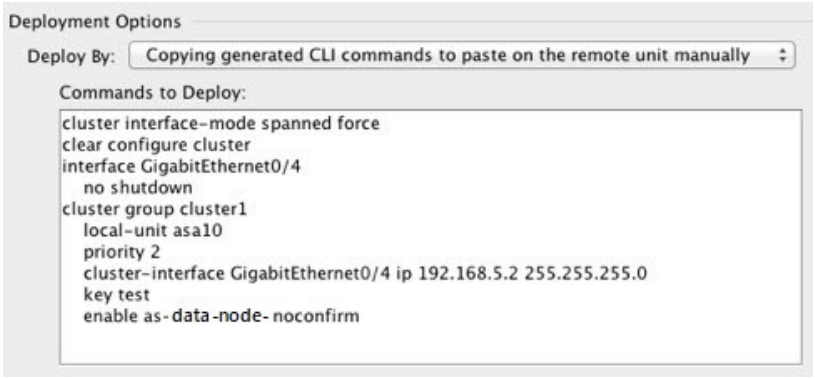
手順

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 [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。



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。

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。

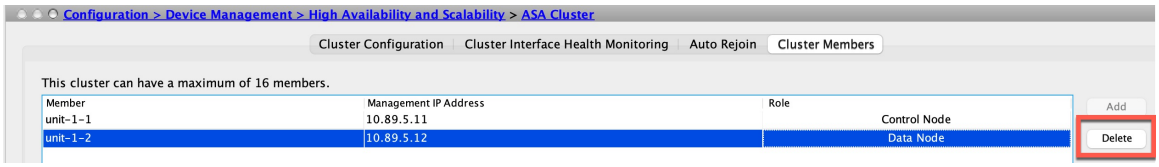
（注） ASA が非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

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。

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。

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。

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。

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

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

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

- **[モニタリング（Monitoring）] > [ASAクラスタ（ASA Cluster）] > [クラスタ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。

クラスタ制御リンクのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

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

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

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次の画面を参照してください。

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

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

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

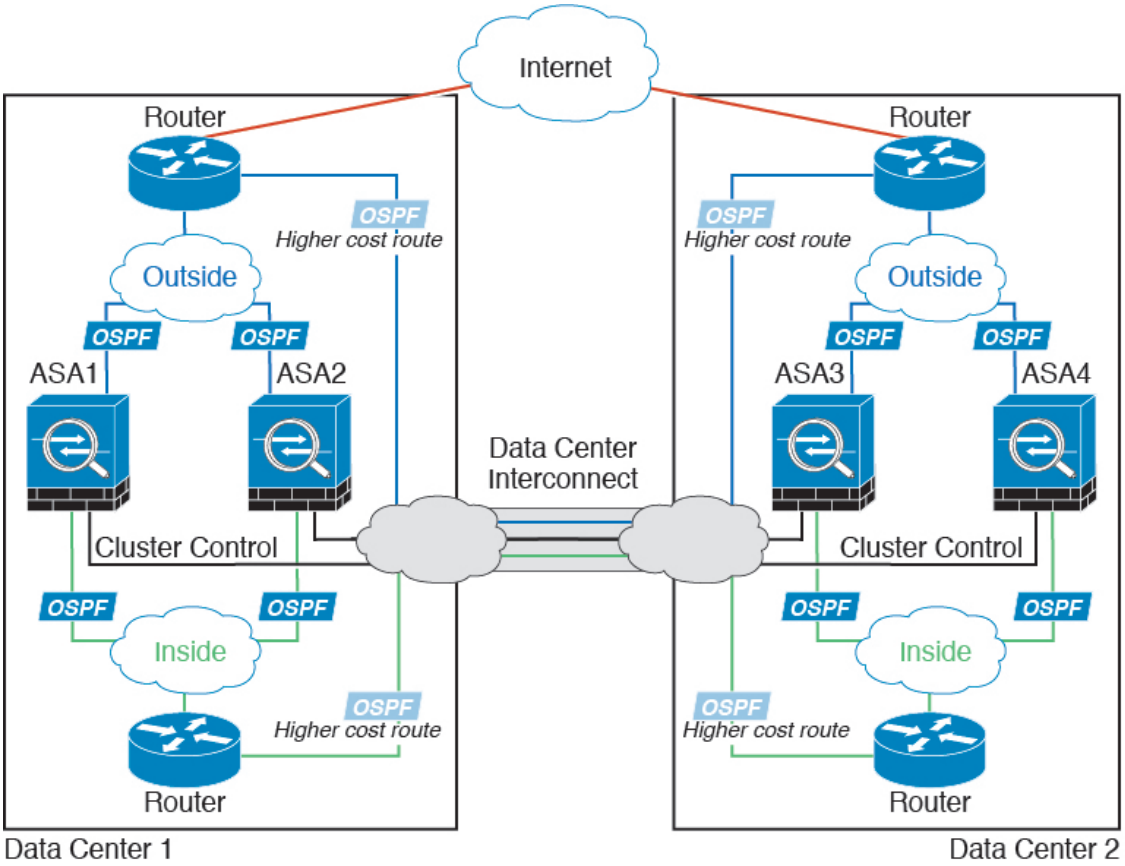
クラスタ内の各ノードは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

ASA 仮想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。

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。



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 インスペクション：
  - 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 インスペクション：
  - 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
- マルチキャスト ルーティング

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ングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て

行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。

- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。
- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 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。

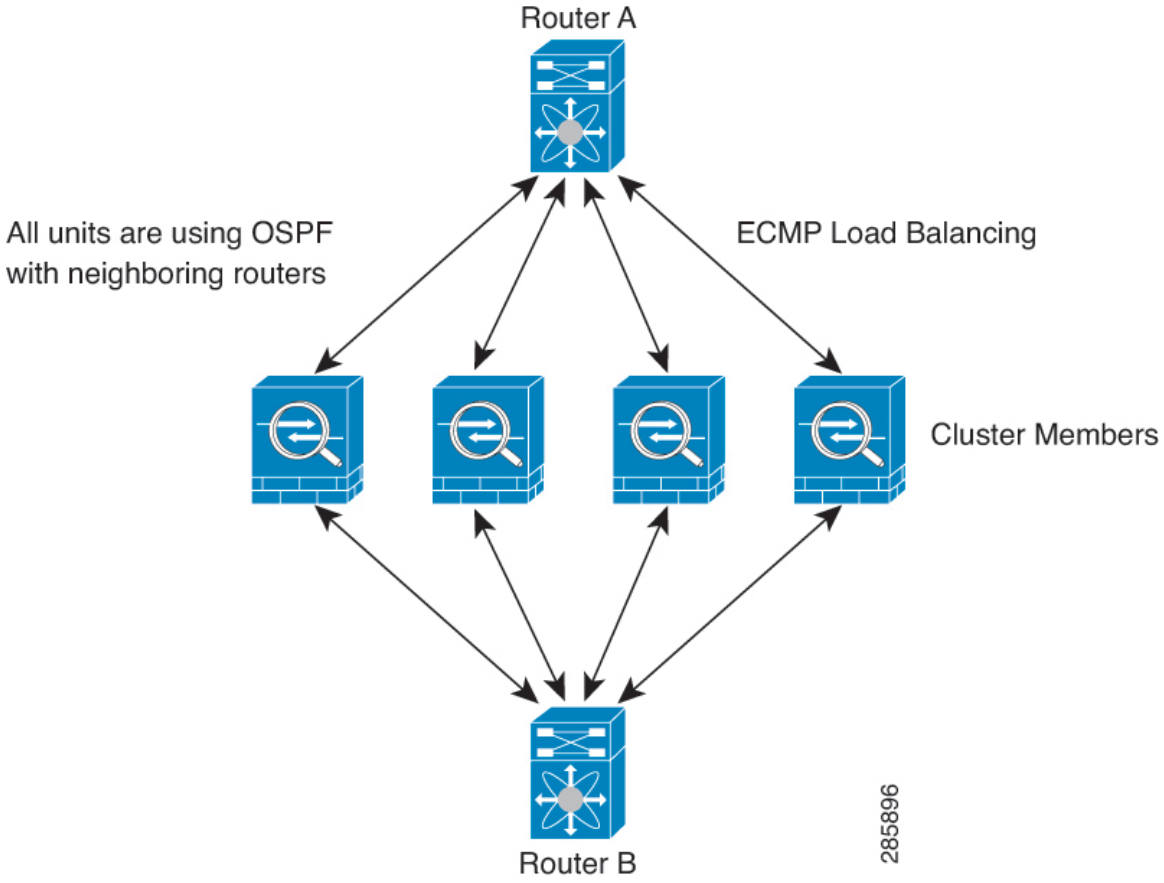
接続設定とクラスタリング

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。

ダイナミック ルーティングおよびクラスタリング

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 *5:* 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。

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す。

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

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 が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

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

- 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タティック 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 がテーブル内にない場合、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。

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に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に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 エクスポータ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。

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。

ASA 仮想クラスタ内のハイアベイラビリティ

ASA仮想クラスタリングは、ノードとインターフェイスの正常性をモニタリングし、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。

ノードヘルスモニタリング

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 （54 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。

ヘルスモニタリングを有効化すると、すべての物理インターフェイスがデフォルトでモニターされるため、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。

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、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。ASAは、ノードがクラスタに参加する最初の90秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。ノード状態に関係なく、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、、クラスタリングを再び有効化することによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASA は、無限に 5 分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディ

セーブルにします。データインターフェイスの問題を解決した後、。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イネ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。

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。
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。

ASA 仮想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て、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ルックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、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（Site Id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クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（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。

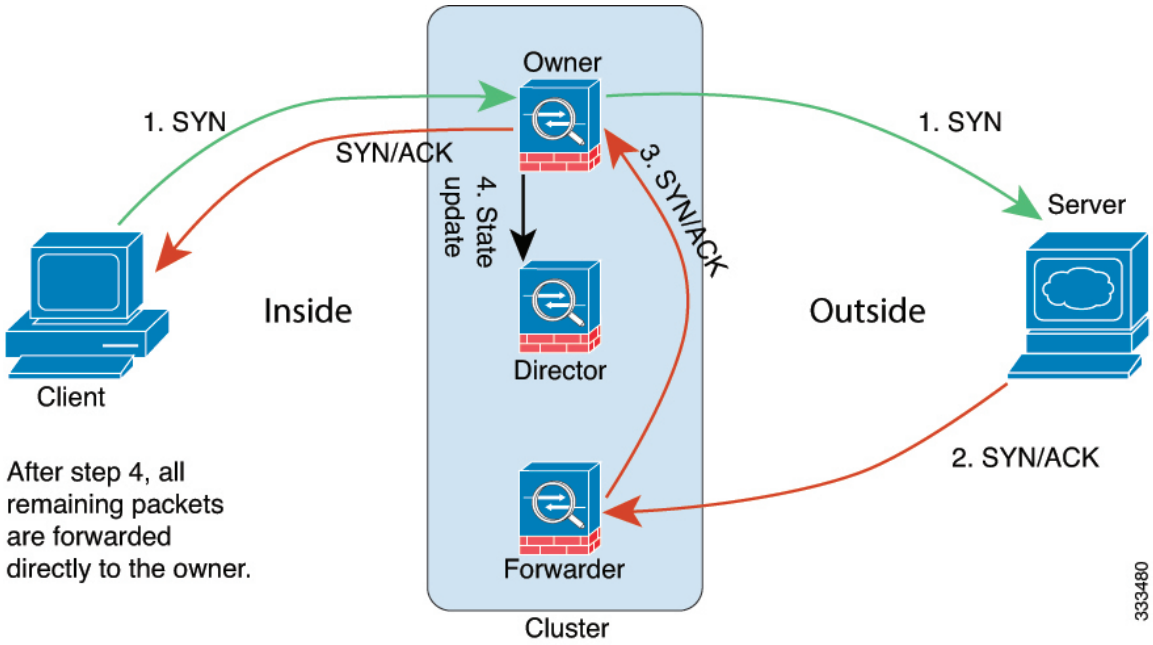
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

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。

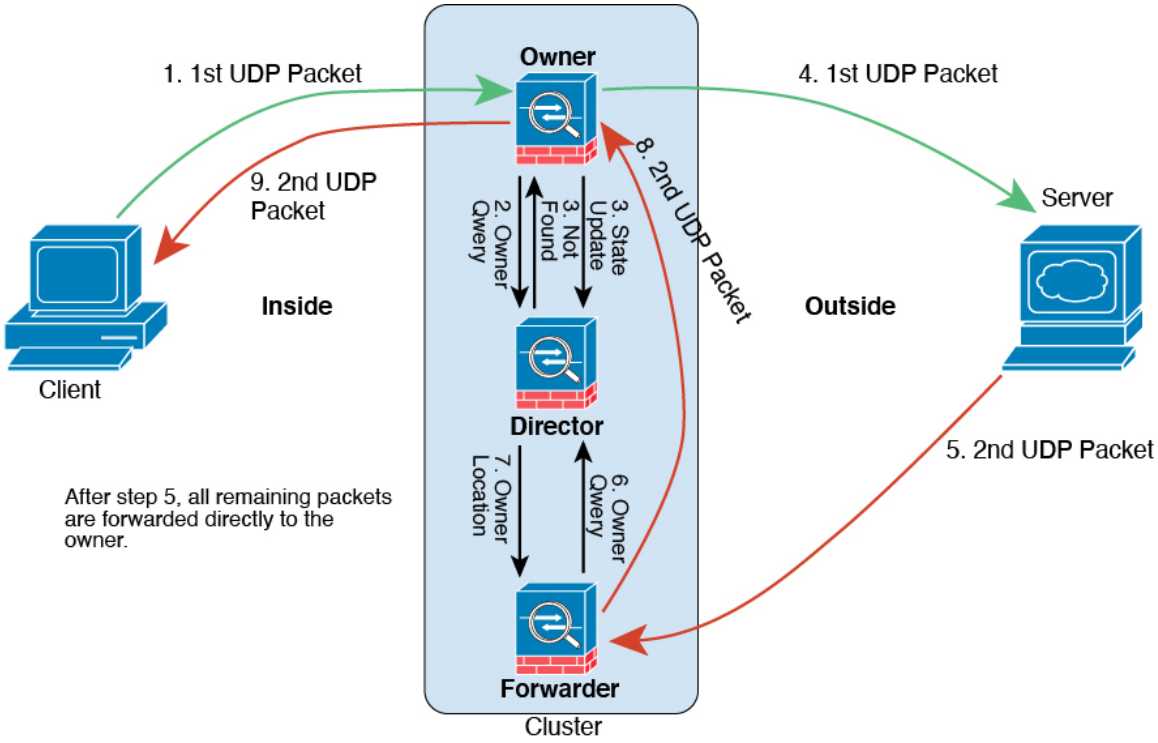


1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. 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てオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

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 *6 : ICMP* および *UDP* データフロー



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

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

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。

ASA 仮想クラスタリングの履歴

機能名	バージョン	機能情報
ノード参加時の MTU ping テスト	9.23(1)	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。
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)	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。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [高可用性と拡張性（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタの設定（Cluster Configuration）]**
バイアス言語の除去	9.19(1)	「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。 新規/変更されたコマンド：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**

機能名	バージョン	機能情報
VMware および KVM 用の ASAv30、ASAv50、および ASAv100 クラスタリング	9.17(1)	ASA 仮想 クラスタリングを使用すると、最大 16 の ASA 仮想 を単一の論理デバイスとしてグループ化できます。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。ASA 仮想 クラスタリングは、ルーテッド ファイアウォール モードで個別インターフェイスモードをサポートします。スパンド EtherChannels はサポートされていません。ASA 仮想 は、クラスタ制御リンクに VXLAN 仮想インターフェイス（VNI）を使用します。 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** • **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

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。