Firepower 4100/9300 の ASA クラスタ

クラスタリングを利用すると、複数のFirepower 4100/9300 シャーシ ASA をグループ化して、1 つの論理デバイスにすることができます。Firepower 4100/9300 シャーシ シリーズには、Firepower 9300 および Firepower 4100 シリーズ が含まれます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） 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 （88 ページ） を参照してください。

Firepower 4100/9300 シャーシのクラスタリングについて

Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポートチャネル 48）を作成します。

シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通信にFirepower 9300 バックプレーンを使用します。

シャーシ間クラスタリングでは、シャーシ間通信用にこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがシャーシスーパバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

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

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

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ブートストラップ コンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがFirepower 4100/9300シャーシスーパバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部はユーザーが設定できます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

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

すべてのコンフィギュレーション作業は制御ユニット上でのみ実行する必要があります。コンフィギュレーションはその後、データユニットに複製されます。

機能によっては、クラスタ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ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能 （89 ページ）を参照してください。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポート チャネル 48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信のために、Firepower 4100/9300 シャーシ のこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

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

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

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 状態の複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンクのサイズ

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

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

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- 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。

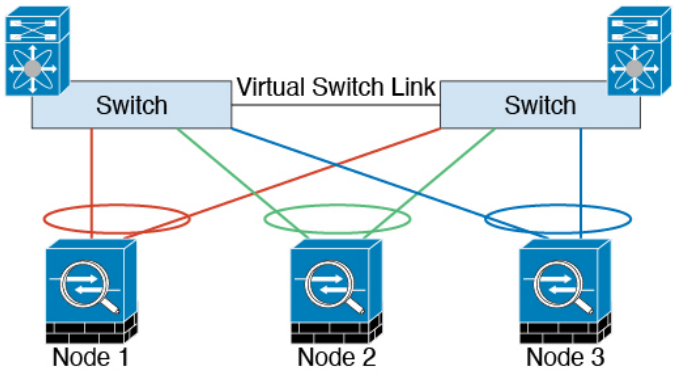
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（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 ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。クラスタを展開するときに、この IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。 サイト間トラフィックには、オーバーレイ トランスポート仮想化（OTV）を使用することをお勧めします。

クラスタ インターフェイス

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

シャーシ間クラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンド EtherChannel は、各シャーシの同じメンバー インターフェイスを含みます。上流に位置するスイッチでは、これらのインターフェイスはすべて単一の EtherChannel に含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

冗長スイッチシステムへの接続

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

コンフィギュレーションの複製

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

Secure Firewall ASA クラスタの管理

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

管理ネットワーク

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

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ユニットに属します。アドレス範囲も設定して、現在の制御ユニットを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタの管理をシームレスに続行できます。

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

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

制御ユニット管理とデータユニット管理

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

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

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

暗号キー複製

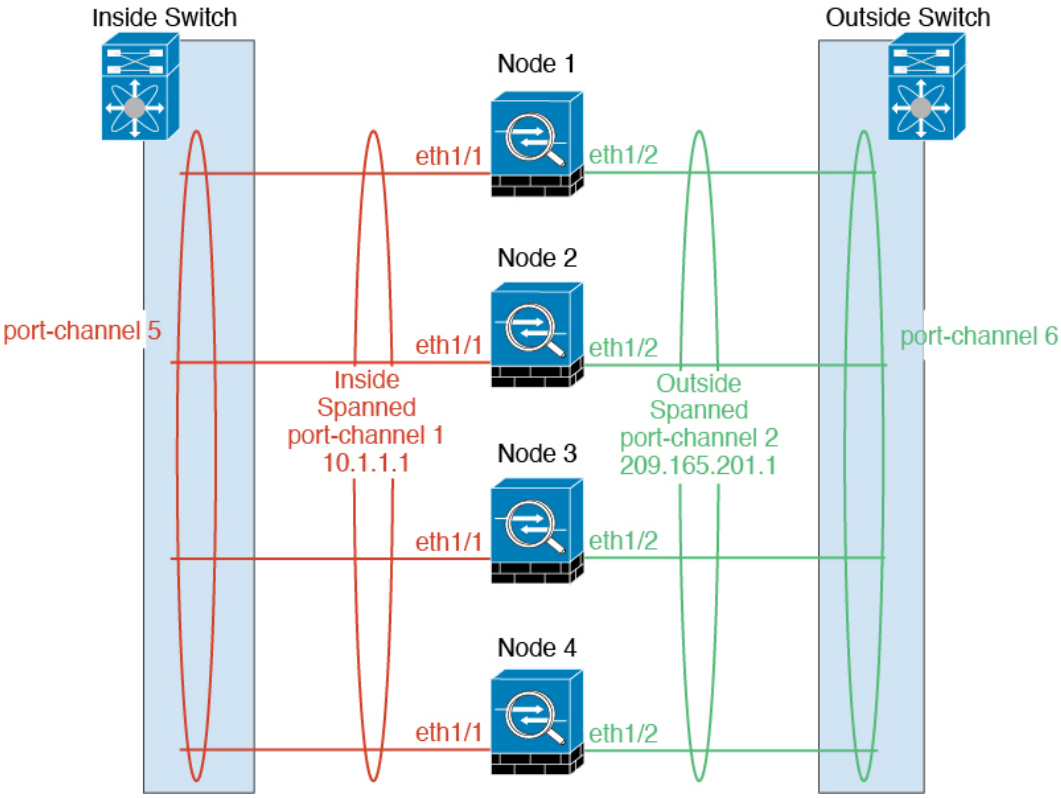
制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH 接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

スパンド EtherChannel（推奨）

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



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も使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 （8 ページ）
- サイト間のガイドライン：クラスタリング ガイドラインと制限事項 （12 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 （43 ページ）
- ディレクタ ローカリゼーションの有効化：ディレクタ ローカリゼーションの有効化 （41 ページ）
- サイト冗長性の有効化：ディレクタ ローカリゼーションの有効化 （41 ページ）

Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリング ユニット

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

インター シャーシ クラスタ化に関するハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower 4100：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。各シャーシに異なる数のセキュリティ モジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。
- イメージアップグレード時を除き、同じ FXOS ソフトウェアを実行する必要があります。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュール タイプを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイスモジュールの追加や削除、または EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データ ノードから始めて、制御ノードで終わります）。FXOS でインターフェイスを削除した場合、必要な調整を行うことができるように、ASA 設定では関連するコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。古いインターフェイス設定は手動で削除することができます。
- 同じ NTP サーバを使用する必要があります。時間を手動で設定しないでください。
- ASA：各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。データ ノードは追加料金なしで使用できます。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Threat Defense では、すべてのライセンスは、Management Center によって処理されます。

スイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチの特性については、『Cisco FXOS Compatibility』を参照してください。

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

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

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

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

次に例を示します。

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

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。
- 3 サイトの 6 メンバーの場合、サイズは増加します。
  - 合計 6 クラスタ メンバー
  - サイト 1 は 3 メンバー、サイト 2 は 2 メンバー、サイト 3 は 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。
- 2 サイトの 2 メンバーの場合。
  - 合計 2 クラスタ メンバー
  - 各サイト 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

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

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

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

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

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

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます:

- 標準：制御ユニットのみがサーバーから標準ライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトで標準ライセンスは 10 のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットの標準ライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタに 6 台の Firepower9300 モジュールがある場合を考えます。標準ライセンスは 10 のコンテキストを含みます。6 つユニットの場合、合計で 60 のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 80 のコンテキストを含みます。モジュールごとのプラットフォーム制限は 250 であるため、統合されたライセンスに最大 250 のコンテキストが許容されます。80 のコンテキストは制限範囲内です。したがって、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して 80 コンテキストを持つことになります。
  - クラスタに Firepower 4112 が 3 台あるとします。標準ライセンスは 10 のコンテキストを含みます。3 つユニットの場合、合計で 30 のコンテキストが加算されます。制御ユニット上で追加の 250 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 280 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大 250 のコンテキストが許容されます。280 コンテキストは制限を超えています。したがって、制御ユニット上で最大 250 のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して 250 のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして 220 のコンテキストのみを設定する必要があります。
- キャリア：分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager オンプレミス展開用、または管理目的用）のライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、

データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、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。

分散型 S2S VPN のライセンス

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

各 VPN 接続には、2 つの *Other VPN* ライセンス済みセッションが必要です（*Other VPN* ライセンスは標準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下にすることができます。

クラスタリング ガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンクインターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンクインターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS XR インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS XR *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。

- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシング アルゴリズムは変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannelインターフェイスは一時的にトラフィックの転送を停止し、スパニングツリープロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル 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。

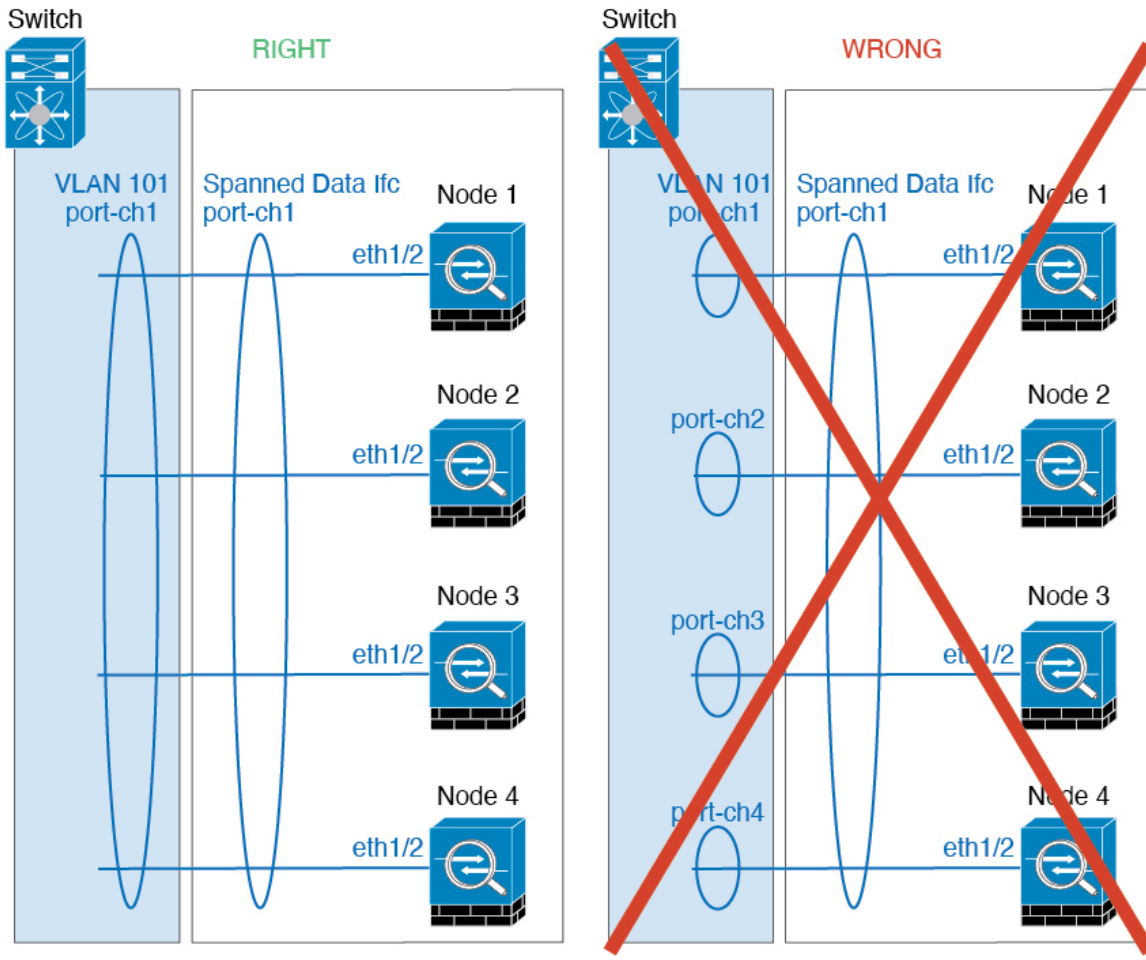
- ASA ハードウェアクラスタとは異なり、Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、プラットフォームでは、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際にLACP高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。

シャーシ間クラスタリングの EtherChannel

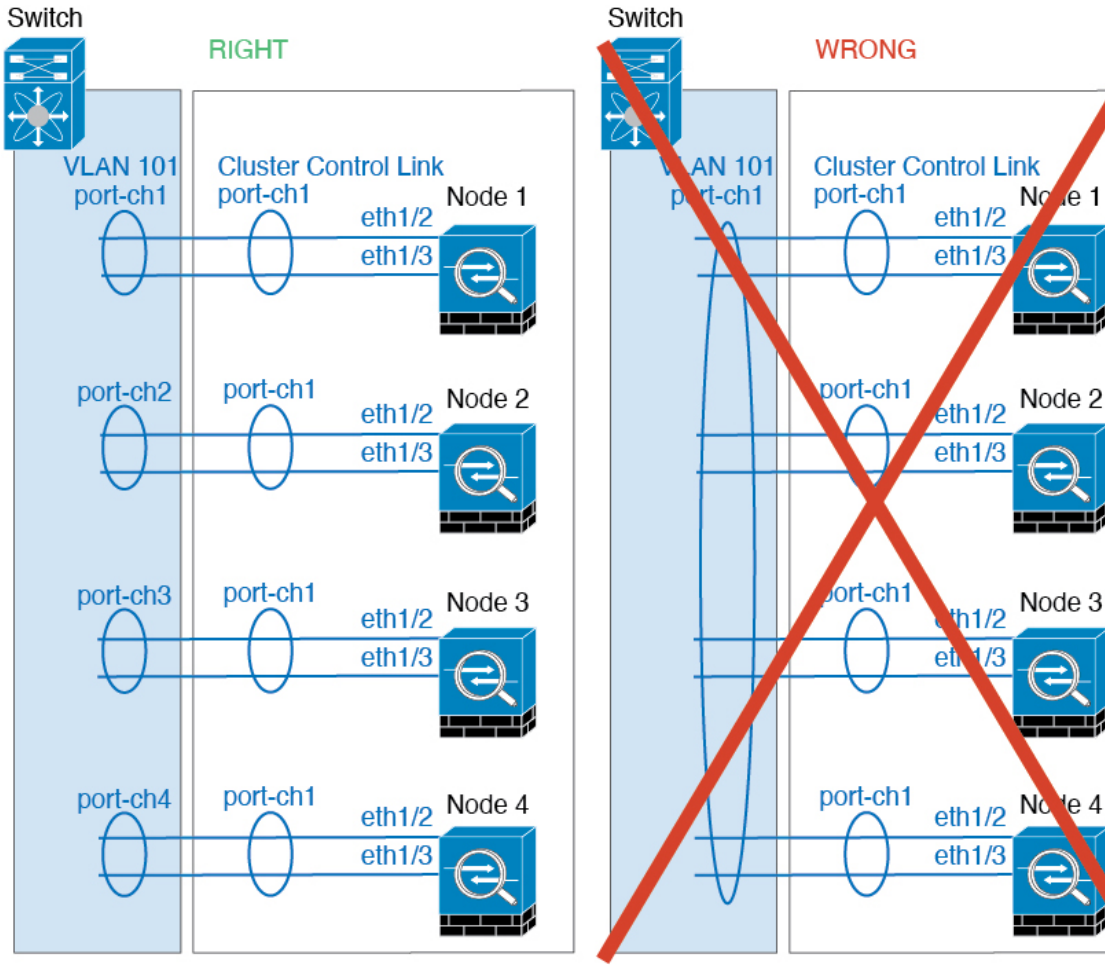
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでし

た。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



  - デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- ASA は専用リンクであるため、データセンター相互接続（DCI）で使用されている場合でも、クラスタ制御リンクで転送されるデータトラフィックを暗号化しません。オーバーレイトランスポート仮想化（OTV）を使用する場合、またはローカル管理ドメインの外部でクラスタ制御リンクを拡張する場合は、OTE を介した 802.1AE MacSec などの境界ルータで暗号化を設定できます。

- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタ ローカリゼーションを有効にすると、ローカル ディレクタのロールは（サイト ID に従って）常に接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。

- ディレクタ ローカリゼーションでは、次のトラフィック タイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション クエリ。

- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じMACアドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバーがサイト 2 のメンバーに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。

- トランスペアレントモードの場合、内部ネットワーク間のファイアウォール用に各サイトのデータ ネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。

- トランスペアレントモードでは、クラスタが HSRP ルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして ASA 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、Firepower4100/9300シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS、vPC、StackWise、またはStackWise Virtualを形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS、vPC、StackWise、または StackWise Virtual に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。
- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5 分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

でのクラスタリングの設定 Firepower 4100/9300 シャーシ

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタ メンバーを管理する方法についても説明します。クラスタ メンバーシップは Firepower 4100/9300 シャーシからも管理できます。詳細については、Firepower 4100/9300 シャーシ のマニュアルを参照してください。

手順

ステップ 1 FXOS：ASA クラスタの追加 （18 ページ）
ステップ 2 ASA：ファイアウォール モードとコンテキスト モードの変更 （29 ページ）
ステップ 3 ASA：データ インターフェイスの設定 （30 ページ）
ステップ 4 ASA：クラスタ設定のカスタマイズ （33 ページ）
ステップ 5 ASA：クラスタ メンバの管理 （58 ページ）

FXOS：ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、次のシャーシにほぼ同じ設定を入力します。

ASA クラスタの作成

範囲をイメージバージョンに設定します。

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。導入を容易にするために、1 つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3 つのすべてのモジュールでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

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

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

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

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

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

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

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

始める前に

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

手順

ステップ 1 インターフェイスを設定します。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。EtherChannel（ポート チャネル）の追加または物理インターフェイスの設定を参照してください。

シャーシ間クラスタリングの場合は、すべてのデータインターフェイスが、少なくとも 1 つのメンバーインターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタユニットからメンバーインターフェイスを 1 つの EtherChannel へと結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （12 ページ） を参照してください。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポートチャネル）の追加または物理インターフェイスの設定を参照してください。

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

シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

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

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

各シャーシに同じメンバインターフェイスを追加します。クラスタ制御リンクは、各シャーシのデバイスローカル EtherChannel です。デバイスごとにスイッチで個別の EtherChannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （12 ページ） を参照してください。

ステップ 2 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 3 アプリケーション インスタンス パラメータ（イメージ バージョンを含む）を設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号を書き留めます。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
```

```
ftd        6.2.3          cisco      Native                Application Yes
ftd        6.3.0          cisco      Native,Container      Application Yes
```

b) 範囲をイメージバージョンに設定します。

scope app asa *application_version*

例：

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) このバージョンをデフォルトとして設定します。

set-default

例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) 終了して ssa モードにします。

exit

例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

ステップ 4 クラスタを作成します。

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name*：Firepower 4100/9300 シャーシスーパバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。この名前は、セキュリティモジュール設定で使用されるクラスタ名ではありません。まだハードウェアをインストールしていない場合でも、3 つすべてのセキュリティ モジュールを指定する必要があります。
- スロット: シャーシ モジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1,2,3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ 5 クラスタ ブートストラップのパラメータを設定します。

これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) シャーシ ID を設定します。

set chassis-id *id*

クラスタの各シャーシは一意の ID が必要です。

c) サイト間クラスタリングの場合、サイト ID は 1 ～ 8 の範囲で設定します。

set site-id *number*.

サイト ID を削除するには、値を **0** に設定します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

set key

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

共有秘密を入力するように求められます。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

e) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

サポートされているモードは、スパンド EtherChannel モードのみです。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) セキュリティ モジュール設定でクラスタ グループ名を設定します。

set service-type *cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （任意） Cluster Control Link IP ネットワークを設定します。

set cluster-control-link network *a*.*b*.**0.0**

クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。この場合、クラスタの固有ネットワークに任意の /16 ネットワーク アドレスを指定できます。

- *a*.*b*.**0.0**：任意の /16 ネットワークアドレスを指定します（ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）のアドレスを除く）。値を 0.0.0.0 に設定すると、デフォルトのネットワーク（127.2.0.0）が使用されます。

シャーシは、シャーシ ID とスロット ID（*a*.*b*.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
 10.10.0.0
```

h) 管理 IP アドレス情報を設定します。

この情報は、セキュリティ モジュール設定で管理インターフェイスを設定するために使用されます。

1. ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、インターフェイス用の各クラスタユニットに割り当てられます。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在の制御ユニットに属する仮想 IP アドレス（メインクラスタ IP アドレスと呼ばれる）は、このプールの一部では

ありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

2. 管理インターフェイスのメインクラスタ IP アドレスを設定します。

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

3. ネットワーク ゲートウェイ アドレスを入力します。

   set ipv4 gateway *ip_address*

   set ipv6 gateway *ip_address*

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11
2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) クラスタ ブートストラップ モードを終了します。

   exit

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 6 管理ブートストラップパラメータを設定します。

これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

a) 管理ブートストラップ オブジェクトを作成します。

   enter mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) admin とイネーブル パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

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

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) ファイアウォール モード（「ルーテッド」または「トランスペアレント」）を指定します。

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

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

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

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 7 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State（管理状態）] が [Enabled（有効）] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- ------------ ------------ ---------------- ------------
ftd        cluster1   1          Enabled     Online           7.3.0.49        7.3.0.49
       Native                   In Cluster      Data Node
ftd        cluster1   2          Enabled     Online           7.3.0.49        7.3.0.49
       Native                   In Cluster      Control Node
ftd        cluster1   3          Disabled    Not Available                    7.3.0.49
       Native                   Not Applicable  None
```

ステップ 8 クラスタに別のシャーシを追加する場合は、この手順を繰り返しますが、固有の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、両方のシャーシで同じ設定を使用します。

インターフェイス コンフィギュレーションが新しいシャーシと同じであることを確認します。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

ステップ 9 制御ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

例

シャーシ 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
```

```
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

シャーシ 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
```

```
commit-buffer
```

クラスタ メンバの追加

ASA クラスタメンバーを追加または置き換えます。

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

始める前に

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

手順

ステップ 1 [OK] をクリックします。

ステップ 2 クラスタに別のシャーシを追加する場合は、ASA クラスタの作成 （18 ページ） の手順を繰り返しますが、一意の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、新しいシャーシに同じ設定を使用します。

ASA：ファイアウォール モードとコンテキスト モードの変更

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

- ファイアウォールモードの変更：展開後にモードを変更するには、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。を参照してください。ファイアウォール モードの設定マルチ コンテキスト モードでは、コンテキストごとにファイアウォール モードを設定します。

- マルチコンテキストモードに変更：展開後にマルチコンテキストモードに変更するには、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。マルチ コンテキスト モードの有効化を参照してください。

ASA：データ インターフェイスの設定

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

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

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- 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。
- シャーシ間クラスタリングにスパンドEtherChannelを使用している場合、クラスタリングが完全に有効になるまで、ポートチャ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 インターフェイス ID を指定します

interface *id*

このクラスタに割り当てられているインターフェイスのFXOSシャーシを参照してください。インターフェイス ID には、次のものがあります。

- **port-channel** *integer*
- **ethernet** *slot/port*

例：

```
ciscoasa(config)# interface port-channel 1
```

ステップ 2 インターフェイスをイネーブルにします。

no shutdown

ステップ 3 （オプション）このインターフェイス上に VLAN サブインターフェイスを作成する予定の場合は、この時点で作成します。

例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

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 4 （マルチ コンテキスト モード）インターフェイスをコンテキストに割り当ててから、コンテキストに変更し、インターフェイス モードを開始します。

例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

マルチ コンテキスト モードの場合は、インターフェイス コンフィギュレーションの残りの部分は各コンテキスト内で行われます。

ステップ 5 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 6 ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード：IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

  （IPv4）

  ip address *ip_address* [*mask*]

  （IPv6）

  ipv6 address *ipv6-prefix*/*prefix-length*

  例：

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
```

DHCP、PPPoE、および IPv6 自動設定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：インターフェイスをブリッジ グループに割り当てます。

  bridge-group *number*

  例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number は、1 ～ 100 の整数です。ブリッジ グループには最大 64 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 7 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 8 （シャーシ間クラスタリング）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 のグローバル MAC アドレスを設定します。

mac-address *mac_address*

- *mac_address*：MAC アドレスは、H.H.H 形式で指定します。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。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

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。

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

ステップ 9 （シャーシ間のクラスタリング）サイトごとにサイト固有の MAC アドレスを、ルーテッドモードの場合は IP アドレスを設定します。

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

例：

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

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。

ASA：クラスタ設定のカスタマイズ

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

ASA クラスタの基本パラメータの設定

制御ユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチコンテキストモードでは、制御ユニット上のシステム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- local-unit name およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合に ASA でのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 このユニットが制御ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
        CCL MAC   : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

別のユニットが制御ユニットの場合は、接続を終了し、正しいユニットに接続します。ASA コンソールへのアクセス方法の詳細については、Cisco ASA for Firepower 4100 クイック スタート ガイド [英語] または Cisco ASA for Firepower 9300 クイック スタート ガイド [英語] を参照してください。

ステップ 2 クラスタ制御リンクインターフェイスの最大伝送ユニットを指定します。データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。

mtu cluster *bytes*

例：

```
ciscoasa(config)# mtu cluster 9184
```

クラスタ制御リンクの MTU を最大値に設定することを推奨します。最小値は 1400 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。たとえば、最大 MTU は 9184 バイトであるため、データインターフェイスの最大 MTU は 9084 になり、クラスタ制御リンクは 9184 に設定できます。

ステップ 3 クラスタの設定モードを開始します。

cluster group *name*

ステップ 4 （任意） データユニットから制御ユニットへのコンソール複製を有効にします。

console-replicate

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します。コンソール複製をイネーブルにすると、データユニットから制御ユニットにコンソールメッセージが送信されるので、モニターが必要になるのはクラスタのコンソールポート 1 つだけとなります。

ステップ 5 クラスタリング イベントの最小トレース レベルを設定します。

trace-level *level*

必要に応じて最小レベルを設定します。

- **critical**：クリティカル イベント（重大度 = 1）
- **warning**：警告（重大度 = 2）
- **informational**：情報イベント（重大度 = 3）
- **debug**：デバッグ イベント（重大度 = 4）

ステップ 6 （任意） LACP のダイナミック ポートの優先順位を無効にします。

clacp static-port-priority

一部のスイッチはダイナミック ポート プライオリティをサポートしていないため、このコマンドはスイッチの互換性を高めます。さらに、このコマンドは、9 ～ 32 のアクティブ スパンドEtherChannelメンバーのサポートをイネーブルにします。このコマンドを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このコマンドをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。

ステップ 7 （任意）（Firepower 9300 のみ）シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されていることを確認します。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。

unit parallel-join*num_of_units* **max-bundle-delay** *max_delay_time*

- *num_of_units*：モジュールがクラスタに参加する前に準備する必要がある同じシャーシ内のモジュールの最小数（1 ～ 3）を指定します。デフォルトは 1 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。たとえば、値を 3 に設定した場合、各モジュールは *max_delay_time* の間、または 3 つすべてのモジュールの準備が完了するまで待機してからクラスタに参加します。3 のすべてのモジュールがほぼ同時にクラスタの参加を要求し、同時期にトラフィックの受信を開始します。

- *max_delay_time*：最大遅延時間を分単位（0 ～ 30 分）で指定します。この時間が経過すると、モジュールは他のモジュールの準備が完了するのを待つことをやめて、クラスタに参加します。デフォルトは 0 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。*num_of_units* を 1 に設定した場合、この値は 0 にする必要があります。*num_of_units* を 2 または 3 に設定した場合、この値は 1 以上にする必要があります。このタイマーはモジュールごとのタイマーですが、最初のモジュールがクラスタに参加すると、その他すべてのモジュールのタイマーが終了し、残りのモジュールがクラスタに参加します。

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

ステップ 8 クラスタメンバの最大数を設定します。

cluster-member-limit *number*

- *number*：2 ー 16。デフォルトは 16 です。

クラスタが最大の 16 ユニットよりも少ないことがわかっている場合は、実際の計画ユニット数を設定することを推奨します。最大ユニット数を設定すると、クラスタのリソース管理が向上します。たとえば、ポートアドレス変換（PAT）を使用する場合、制御ユニットは計画されたメンバー数にポートブロックを割り当てることができ、使用する予定のない追加のユニット用にポートを予約する必要がなくなります。

のヘルス モニタリングおよび自動再結合の設定

この手順では、ユニットとインターフェイスのヘルス モニタリングを設定します。

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

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 クラスタ ユニットのヘルス チェック機能を次のようにカスタマイズします。

health-check [**holdtime** *timeout*]

holdime は、ユニットのハートビート ステータス メッセージの間隔を指定します。指定できる範囲は .3 ～ 45 秒で、デフォルトは 3 秒です。

ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにハートビート メッセージを送信します。ユニットが保留時間内にピア ユニットからハートビート メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 4100/9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし、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（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイス ヘルス チェックを次のように無効化します。

no health-check monitor-interface [*interface_id* | **service-application**]

インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブ ポートがある場合、そのユニットはクラスタから削除されます。ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。

デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブルにすることができます。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。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。**service-application** を指定して、デコレータ アプリケーションのモニタリングをディセーブルにします。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 4100/9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし（**no health-check**）、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

ステップ 4 ヘルス チェック失敗後の自動再結合クラスタ設定を次のようにカスタマイズします。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**：内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
- **unlimited**：（**cluster-interface** のデフォルト）再結合の試行回数を制限しません。
- *auto-rejoin-max*：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。**data-interface**と **system** のデフォルトは 3 です。
- *auto_rejoin_interval*：再結合試行の間隔を 2 ～ 60 の範囲の分単位で定義します。デフォルト値は5分です。クラスタへの再結合をユニットが試行する最大合計時間は、最後の失敗から 14,400 分に限られています。
- *auto_rejoin_interval_variation*：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**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。

例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

ステップ 5 ASAがインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定します。

health-check monitor-interface debounce-time *ms*

デバウンス時間は 300 ～ 9000 ms の範囲の値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASAはインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。 ダウン状態から稼働状態に移行しているEtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっているEtherChannelなど）、デバウンス時間を長くすることで、他のクラスタユニットの方がポートのバンドルが速いという理由だけで、クラスタユニット上でインターフェイスがエラー表示されるのを防ぐことができます。

例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

ステップ 6 シャーシのヘルス チェック間隔を設定します。

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

- **interval** *ms*：ハートビートの時間間隔を 100 ～ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
- **retry-count** *number*：再試行の回数を 1 ～ 30 の範囲の値に設定します。デフォルトの試行回数は 3 回です。

ASA はホストシャーシとのバックプレーンを介して通信できるかどうかをチェックします。

最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできません。たとえば、間隔を 100 に、再試行回数を 3 に設定した場合、合計結合時間は 300 ミリ秒になりますが、これはサポートされていません。たとえば、間隔を 100 に設定し、再試行回数を 6 に設定して最小時間（600 ms）を満たすことができます。

例：

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 300
```

ステップ 7 （任意）トラフィック負荷のモニタリングを設定します。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- seconds: 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。 **frequency** デフォルトは 20 秒です。
- 間隔（ *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。 **intervals** デフォルトは 30 です。

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

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 25 interval:
   0           0            0            12             28
```

```
1           0           0           13              27
```

接続の再分散およびクラスタ TCP 複製の遅延の設定

接続の再分散を設定できます。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 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （オプション）TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合は、ASA は負荷情報を定期的に交換し、新しい接続の負荷を高負荷のデバイスから低負荷のデバイスに移動します。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。デフォルトは 5 秒です。

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 メンバには接続を再分散できません。

ステップ 3 TCP 接続のクラスタ複製の遅延を有効化します。

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

1 ～ 15 の範囲で秒数を設定します。**http** 遅延はデフォルトで 5 秒間有効になります。

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。

ディレクタ ローカリゼーションの有効化

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を向上させ、ラウンドトリップ時間を短縮するために、ディレクターローカリゼーションをイネーブルにすることができます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASAは任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバルディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。

始める前に

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。
- 次のトラフィック タイプは、ローカリゼーションをサポートしていません：NAT および PAT トラフィック、SCTP 検査されたトラフィック、フラグメンテーション所有クエリ。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 次のようにディレクタ ローカリゼーションをイネーブルにします。

director-localization

サイト冗長性の有効化

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。

始める前に

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 サイトの冗長性を有効にします。

site-redundancy

サイトごとの Gratuitous ARP の設定

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。

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

各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。GARP 間隔をカスタマイズするか、または GARP を無効にすることができます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。
- 制御ユニット設定では、スパンド EtherChannel のサイトごとの MAC アドレスを設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 GARP 間隔をカスタマイズします。

site-periodic-garp interval *seconds*

- *seconds*：GARP 生成の間隔を 1 ～ 1000000 秒間の秒単位で設定します。デフォルトは 290 秒です。

GARP を無効にするには、**no site-periodic-garp interval** を入力します。

例：

```
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

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。

Secure Firewall ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISPの統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフローオーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーニング」または「ヘアピニング」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でのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。
4. サイト ID：ASA は、各クラスタノードのサイト ID を使用して新しいオーナーを特定します。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP イン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

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。
- LISP のトラフィックはデフォルト インスペクション 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) 拡張 ACL を作成します。宛先 IP アドレスのみが EID 組み込みアドレスと照合されます。

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) LISP インスペクション マップを作成し、パラメータ モードに移行します。

policy-map type inspect lisp *inspect_map_name*

parameters

c) 作成した ACL を識別して、許可された EID を定義します。

allowed-eid access-list *eid_acl_name*

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。

d) 必要に応じて、事前共有キーを入力します。

validate-key *key*

例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

ステップ 2 ファースト ホップ ルータとポート 4342 の ITR または ETR の間の UDP トラフィック の LISP インスペクションの設定。

a) 拡張 ACL を設定して LISP のトラフィックを特定します。

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

UDP ポート 4342 を指定する必要があります。IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) ACL のクラス マップを作成します。

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) ポリシー マップ、クラス マップを指定し、オプションの LISP インスペクション マップを使用してインスペクションを有効化し、サービス ポリシーをインターフェイスに適用します（新規であれば）。

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

既存のサービス ポリシーある場合は、既存のポリシー マップ名を指定します。デフォルトで、ASA には **global_policy** と呼ばれるグローバル ポリシーが含まれているため、グローバル ポリシーの名前を指定します。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 マップ

に一致する場合、ポリシーマップを適用するインターフェイスに入るまたは存在するトラフィックのすべてが影響を受けます。

例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

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。

ステップ3 トラフィック クラスのフロー モビリティを有効化します。

a) 拡張ACLを設定して、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特定します。

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

IPv4 ACLおよびIPv6 ACLのどちらにも対応しています。厳密な **access-list extended** の構文については、コマンドリファレンスを参照してください。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イネーブルにする必要があります。たとえば、フロー モビリティをHTTPSトラフィックのみ、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。

b) ACLのクラス マップを作成します。

class-map *flow_map_name*

match access-list *flow_acl_name*

c) LISPインスペクションを有効化した同じポリシー マップ、フロー クラス マップを指定して、フロー モビリティを有効にします。

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0
255.255.255.0 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

ステップ 4 クラスタ グループ コンフィギュレーション モードに移行し、クラスタのフローのモビリティを有効化します。

cluster group *name*

flow-mobility lisp

このオン/オフの切り替えにより、フロー モビリティの有効化や無効化を簡単に行えます。

例

次に例を示します。

- EID を 10.10.10.0/24 ネットワーク上の EID に制限します。
- 192.168.50.89（内部）にある LISP ルータと 192.168.10.8（別の ASA インターフェイス上）にある ITR または ETR ルータの間の LISP トラフィック（UDP 4342）を検査します。
- HTTPS を使用して 10.10.10.0/24 のサーバーに送信されるすべての内部トラフィックに対してフロー モビリティを有効化します。
- クラスタに対してフロー モビリティをイネーブルにします。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

分散型サイト間 VPN の設定

デフォルトでは、ASA クラスタは集中型サイト間 VPN モードを使用します。クラスタリングの拡張性を活用するために、分散型サイト間VPNモードを有効にできます。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散されます。クラスタのメン

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

分散型サイト間 VPN について

分散型 VPN 接続の役割

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

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

分散型 VPN セッションの特性

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

- VPN セッションは、セッション レベルでクラスタ全体に分散されます。つまり、1 つの VPN 接続に対し、同じクラスタ メンバーが IKE および IPsec トンネルと、そのすべてのトラフィックを処理します。VPN セッション トラフィックが、その VPN セッションを所有していないクラスタ メンバーに送信された場合、トラフィックは VPN セッションを所有しているクラスタ メンバーに転送されます。
- VPN セッションには、クラスタ全体で一意のセッション ID があります。セッション ID を使用して、トラフィックが検証され、転送の決定が行われ、IKE ネゴシエーションが完了します。
- S2S VPN ハブ アンド スポーク構成では、クライアントが ASA クラスタを介して接続する場合（ヘアピニングと呼ばれる）、流入するセッション トラフィックと流出するセッション トラフィックは、異なるクラスタ メンバー上にある可能性があります。

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

クラスタ イベントの分散型 VPN の処理

表 *1:*

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

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

サポートされていないインスペクション

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

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

IPsec IKEv2 の変更

IKEv2 は、分散型 S2S VPN モードでは次のように変更されます。

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

サポート モデル

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

サイト間クラスタリングはサポートされていません。

ファイアウォール モード

分散型 S2S VPN は、ルーテッド モードでのみサポートされています。

コンテキスト モード

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

ハイ アベイラビリティ

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

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

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

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

ダイナミック PAT

分散型 VPN モードでは使用できません。

CMPv2

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

分散型 S2S VPN の有効化

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

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

始める前に

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

手順

ステップ 1 クラスタの制御ユニットで、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 cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 分散型 S2S VPN を有効にします。

vpn-mode distributed backup flat

または

vpn-mode distributed backup remote-chassis

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

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

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

例：

```
ciscoasa(cfg-cluster)# vpn-mode distributed backup remote-chassis
```

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 クラスタ内の制御ユニットで **show cluster vpn-sessiondb distribution** コマンドを実行して、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でどのように配布されているかを確認します。

例：

配布情報は次のように表示されます。

```
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

各行には、メンバー ID、メンバー名、アクティブ セッション数、およびバックアップ セッションが存在するメンバーが含まれています。上記の例では、次のように情報が読み取れます。

- メンバー 0 には 209 のアクティブ セッションがあり、111 のセッションはメンバー 1 にバックアップされ、98 のセッションはメンバー 2 にバックアップされます。
- メンバー 1 には 204 のアクティブ セッションがあり、108 のセッションはメンバー 0 にバックアップされ、96 のセッションはメンバー 2 にバックアップされます。
- メンバー2にはアクティブセッションがないため、クラスタ メンバーはこのノードのセッションをバックアップしていません。このメンバーは最近クラスタに参加しました。

ステップ 2 **cluster redistribute vpn-sessiondb** コマンドを実行します。

このコマンドは、バックグラウンドで実行中に即座に戻ります（メッセージなしで）。

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

Syslog フレーズ	注
VPN session redistribution started	制御ユニットのみ
Sent request to move *number* sessions from *orig-member-name* to *dest-member-name*	制御ユニットのみ
Failed to send session redistribution message to *member-name*	制御ユニットのみ
Received request to move *number* sessions from *orig-member-name* to *dest-member-name*	データユニットのみ
Moved *number* sessions to *member-name*	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 *dest-member-name*	制御ユニットのみ
VPN session completed	制御ユニットのみ

Syslog フレーズ	注
Cluster topology change detected. VPN session redistribution aborted.	

ステップ 3 **show cluster vpn distribution** の出力を使用して、再配布アクティビティの結果を確認します。

FXOS：クラスタユニットの削除

ここでは、ユニットをクラスタから一時的に、または永続的に削除する方法について説明します。

一時的な削除

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

デバイスが現在クラスタ内に存在するか確認するには、Chassis Manager [論理デバイス（Logical Devices）] ページで、**show cluster info** コマンドを使用してアプリケーション内のクラスタステータスを確認します。

```
ciscoasa# show cluster info
Clustering is not enabled
```

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

  デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。

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

- アプリケーション インスタンスの無効化：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
```

```
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asa1
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

再度有効にするには、次の手順を実行します。

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- セキュリティ モジュール/エンジン のシャットダウン：Chassis Manager の [セキュリティ モジュール/エンジン（Security Module/Engine）] ページで、[電源オフ（Power Off）] アイコンをクリックします。FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

電源を投入するには、次の手順を実行します。

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- シャーシのシャットダウン：Chassis Managerの [概要（Overview）] ページで、[シャットダウン（Shut Down）] アイコンをクリックします。FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

- 論理デバイスの削除：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- サービスからのシャーシまたはセキュリティ モジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

ASA：クラスタ メンバの管理

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

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、その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

- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- 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、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

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

ステップ 2 クラスタリングをディセーブルにします。

no enable

このノードが制御ノードであった場合は、新しい制御ノードの選定が実行され、別のメンバーが制御ノードになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

ユニットの非アクティブ化

ログインしているノード以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ 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、**changeto system** コマンドを入力します。

手順

クラスタからノードを削除します。

cluster remove unit *node_name*

ブートストラップ コンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2
```

```
ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

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。
- 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、**changeto system** コマンドを入力します。
- 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 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 2 クラスタリングをイネーブルにします。

enable

制御ユニットの変更

⚠

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

新しいノードを制御ノードとして設定します。

cluster master unit*node_name*

例：

```
ciscoasa(config)# cluster master unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバー名を表示するには、**cluster master 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。

クラスタ全体でのコマンドの実行

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

手順

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

cluster exec [unit *unit_name*] コマンド

例：

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

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

例

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

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

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

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

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


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


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

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

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info [health], show cluster chassis info**

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバーのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ユニットおよびクラスタ全体の現在の状態を表示します。

  show cluster info コマンドの次の出力を参照してください。

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
        CCL MAC   : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
```

```
        Last leave: 20:24:55 UTC Nov 4 2015
```

- **show cluster info auto-join**

  時間遅延後にクラスタユニットがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルスチェック障害など）がクリアされたかどうかを示します。ユニットが永続的に無効になっている場合、またはユニットがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。

  show cluster info auto-join コマンドについては次の出力を参照してください。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check
failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp**[**detail**]}

  次のトランスポート関連の統計情報を表示します。

  - **asp**：データ プレーンのトランスポート統計情報。
  - **cp**：コントロール プレーンのトランスポート統計情報。

    detail キーワードを入力すると、クラスタで信頼性の高いトランスポート プロトコルの使用状況が表示され、バッファがコントロールプレーンでいっぱいになったときにパケット ドロップの問題を特定できます。**show cluster info transport cp detail** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
```

```
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-----------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
```

```
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

```
MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  クラスタの履歴、およびクラスタユニットが参加できなかった理由や、ユニットがクラスタを離れた理由に関するエラーメッセージが表示されます。

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、次のコマンドを参照してください。

cluster exec capture

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、**cluster exec capture** コマンドを使用して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、次のコマンドを参照してください。

show cluster {cpu | memory | resource} [*options*]、**show cluster chassis [cpu | memory | resource usage]**

クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

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、次のコマンドを参照してください。

- **show conn [detail | count], cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダ フローのいずれであるかを示します。**cluster exec show conn** コマンドを任意のユニットで使用すると、すべての接続が表示されます。このコマンドの表示からは、1つのフローのトラフィックがクラスタ内のさまざまな ASA にどのように到達するかがわかります。クラスタのスループットは、ロード バランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れ

るかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation

          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

  show cluster info conn-distribution および **show cluster info packet-distribution** コマンドは、すべてのクラスタユニット間のトラフィックの分布を表示します。これらのコマンドは、外部ロードバランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

- **show cluster info load-monitor** [**details**]

  この**show cluster info load-monitor**コマンドは、最後の間隔のクラスタメンバのトラフィック負荷と、設定された間隔の合計数（デフォルトでは30）を表示します。各間隔の各測定値を表示するには、**details** キーワードを使用します。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
```

```
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
         0          0          0          0          0          0
         0          0          0          0          0          0
Unit ID  1
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
        25         25         30         30         30         35
        25         25         35         30         30         30
        25         25         30         25         25         35
        30         30         30         25         25         25
        25         20         30         30         30         30
Unit ID  1
        30         25         35         25         30         30
        25         25         35         25         30         35
        30         30         35         30         30         30
        25         20         30         25         25         30
        20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
        25         25         30         30         30         35
        25         25         35         30         30         30
        25         25         30         25         25         35
        30         30         30         25         25         25
        25         20         30         30         30         30
Unit ID  1
        30         25         35         25         30         30
```

```
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [*options*]、**show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

  show cluster access-list コマンドの次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

  使用中の接続の、すべてのユニットでの 合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
```

```
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):*******************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:*******************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

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、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

  クラスタのルーティング情報を表示します。

- **show lisp eid**

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

  cluster exec show lisp eid コマンドからの、次の出力を参照してください。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):*************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  このコマンドは、トラブルシューティングに役立ちます。

分散型 S2S VPN のモニタリング

次のコマンドを使用して、VPN セッションのステータスと分布を監視します。

- セッションの全体的な分布は、**show cluster vpn-sessiondb distribution** を使用して示されます。マルチコンテキスト環境で実行している場合は、このコマンドをシステム コンテキストで実行する必要があります。

  この show コマンドを使用すると、各メンバーで **show vpn-sessiondb summary** を実行する必要なく、セッションのクイック ビューが提供されます。

- **show cluster vpn-sessiondb summary** コマンドを使用して、クラスタ上の VPN 接続の統一されたビューも使用できます。

- **show vpn-sessiondb** コマンドを使用した個々のデバイス モニタリングでは、通常の VPN 情報に加えて、デバイス上のアクティブ セッションとバックアップ セッションの数が表示されます。

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、次のコマンドを参照してください。

logging device-id

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。**logging device-id** コマンドを使用すると、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。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **debug service-module**

  スーパバイザとアプリケーション間のヘルス チェックの問題を含め、ブレード レベルの問題に関するデバッグ メッセージを表示します。

- **show cluster info trace**

  show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

  show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

分散型 S2S VPN のトラブルシューティング

分散型 VPN の通知

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

状況	通知
クラスタに参加しようとしているときに、既存のまたは参加しているクラスタデータユニットが分散型 VPN モードにない場合は、次のメッセージが通知されます。	`New cluster member (member-name) rejected due to vpn mode mismatch.` および マスター（*control-name*）は、VPN モード機能にマスターの設定との互換性がないという理由でユニット（unit-name）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: Master requested cluster vpn-mode change to distributed. Unable to change mode due to missing Carrier License.`

受信した IKEv2 パケットの SPI でタイム スタンプまたはメンバー ID が無効な場合は、次のメッセージが通知されます。	`Expired SPI received`
	または
	`Corrupted SPI detected`

クラスタがバックアップ セッションを作成できない場合は、次のメッセージが通知されます。	`Failed to create the backup for an IKEv2 session.`
IKEv2 初期接点（IC）処理エラーの場合は、次のメッセージが通知されます。	`IKEv2 Negotiation aborted due to ERROR: Stale backup session found on backup`
再配布の問題の場合は、次のメッセージが通知されます。	`Failed to send session redistribution message to` *member-name* `Failed to receive session move response from` *member-name* （マスターのみ）
セッションの再配布中にトポロジが変更された場合は、次のメッセージが通知されます。	`Cluster topology change detected. VPN session redistribution aborted.`

次のいずれかの状況が発生している可能性があります。

- **port-channel load-balance src-dst l4port**コマンドを使用して N7K スイッチにロード バランシング アルゴリズムとして L4port が設定されている場合、L2L VPN セッションはクラス

タ内のシャーシの 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/slave(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
 5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
 5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
 5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

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

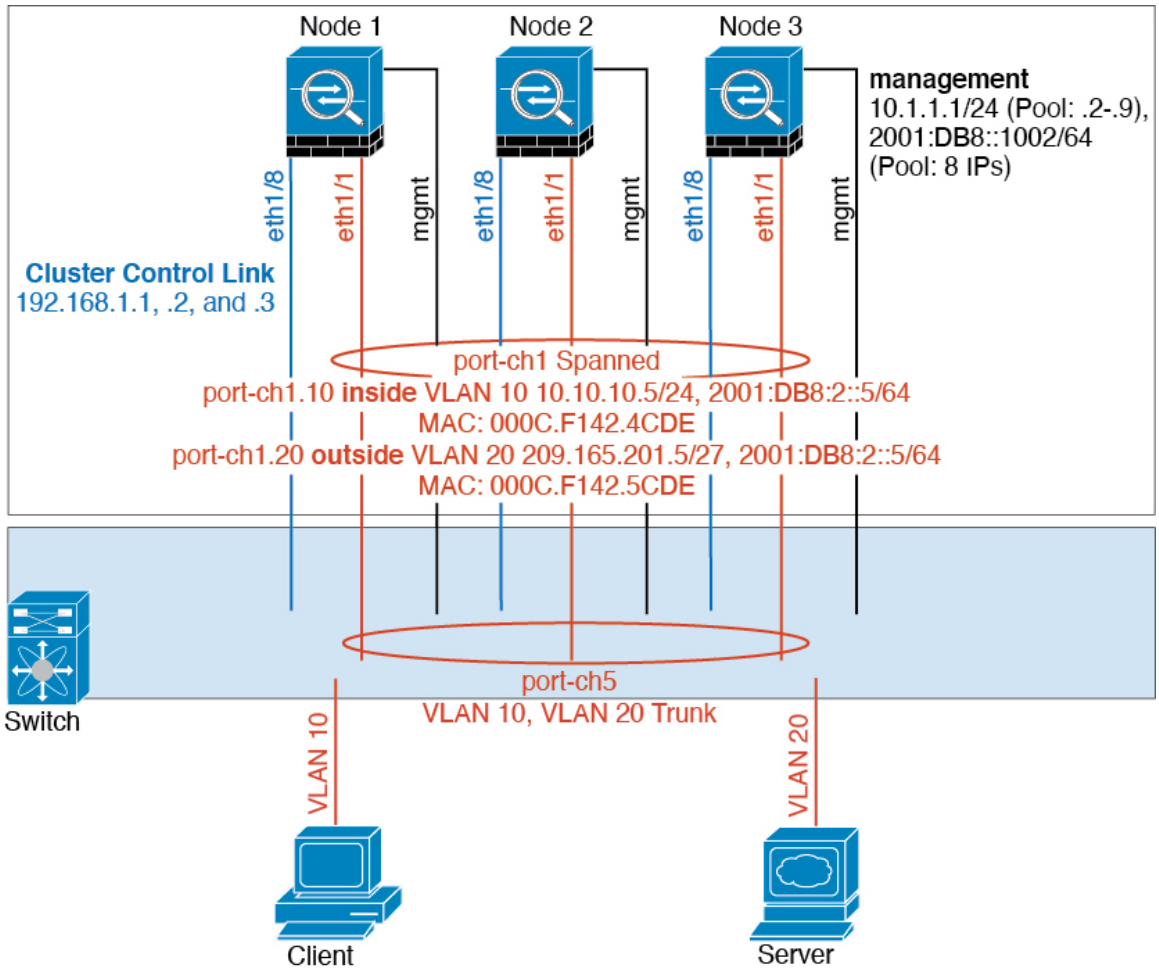
port-channel load-balance src-dst ip-l4port を使用して、N7K ロード バランシング アルゴリズムを IP および L4 ポートに変更します。その後、IKE パケットはすべてのリンクに送信されるので、両方の Firepower9300 シャーシに送信されます。

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

ASA クラスタリングの例

これらの例には、一般的な導入が含まれます。

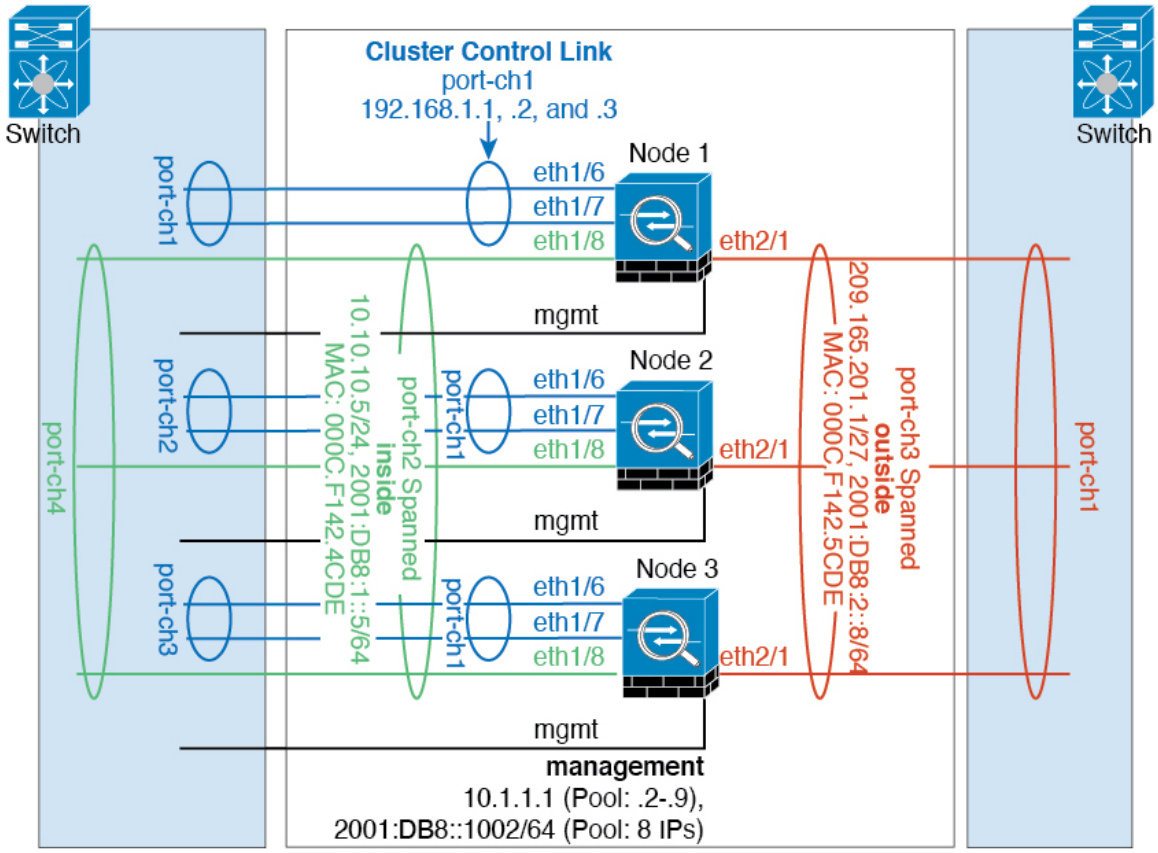
スティック上のファイアウォール



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

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

トラフィックの分離



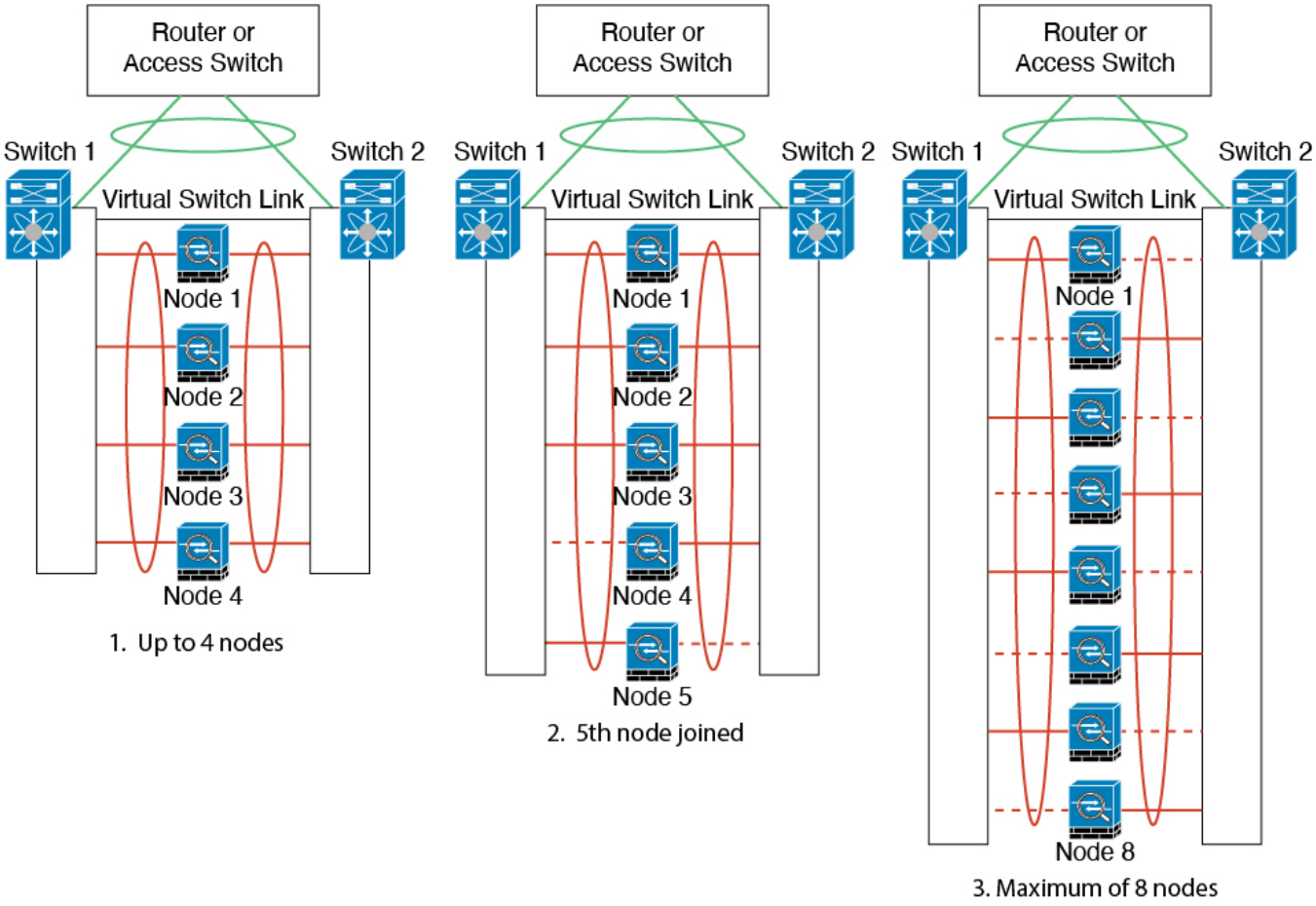
内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

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

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

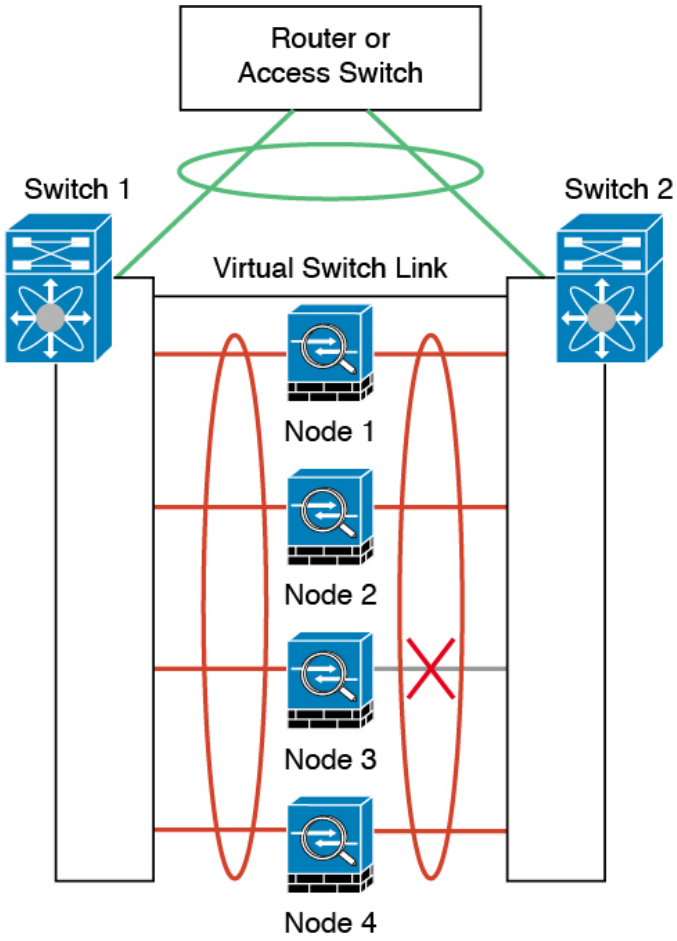
従来の EtherChannel のアクティブ ポートの最大数は、スイッチ側からの 8 に制限されます。8 ユニットから成るクラスタがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイ モードにする必要があります。ASA は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。VSS、vPC、StackWise、または StackWise Virtual を使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASA では、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「制御」ポートとなり（たとえばEthernet 1/1）、他方が「データ」ポートとなります（たとえばEthernet 1/2）。ハードウェア接続の対称性を保証する必要があります。つまり、すべて

の制御リンクは1台のスイッチが終端となり、すべてのデータリンクは別のスイッチが終端となっている必要があります（冗長スイッチシステムが使用されている場合）。次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。

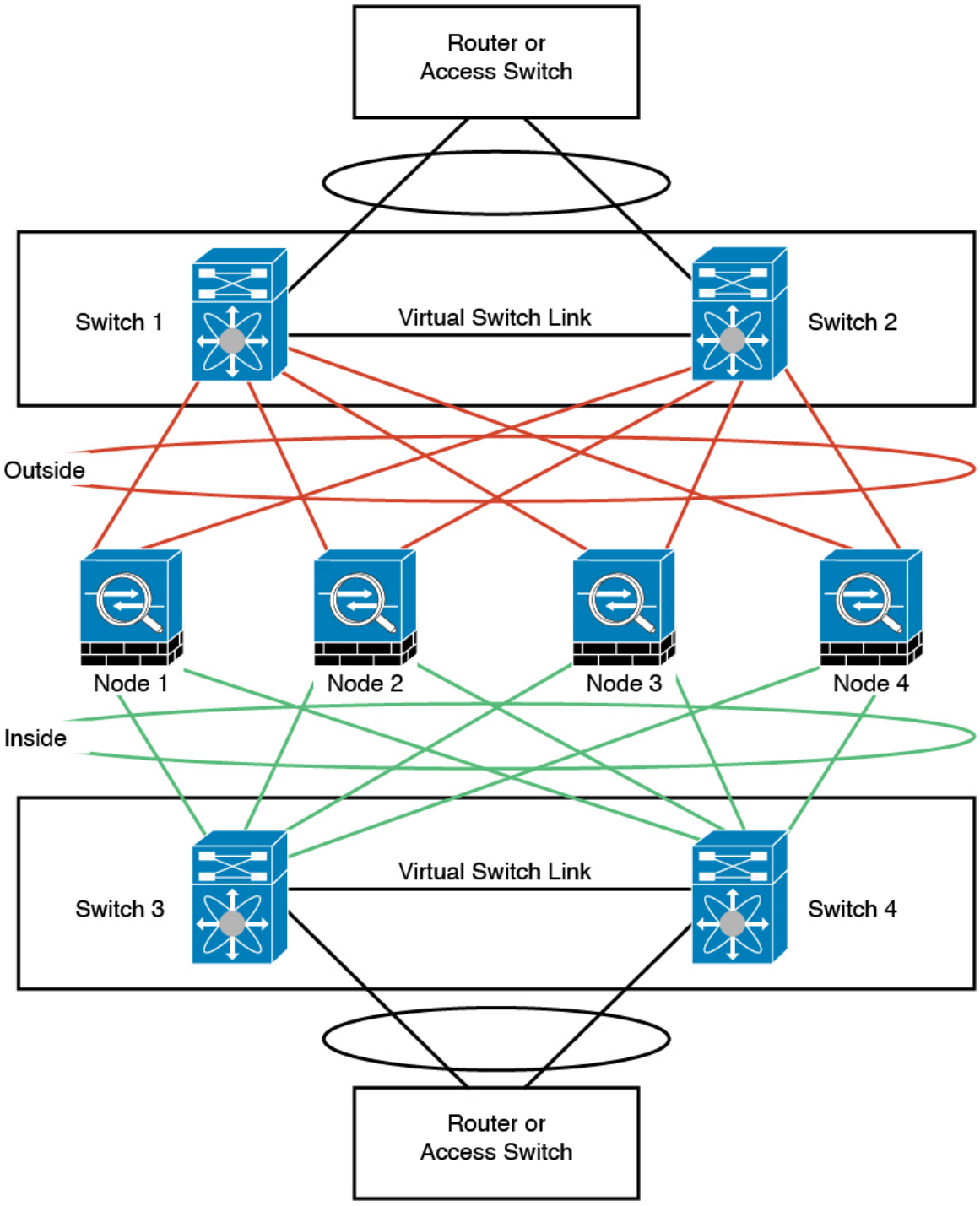


原則として、初めにチャネル内のアクティブポート数を最大化し、そのうえで、アクティブな制御ポートとアクティブなデータポートの数のバランスを保ちます。5 番目のユニットがクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

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



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



ルーテッド モード サイト間クラスタリングの OTV 設定

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

OTV 設定の例

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

feature ospf
feature otv

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


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

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

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

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

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
```

```
  ip igmp version 3
  no shutdown

interface Ethernet8/2

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

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

サイト障害のために必要な OTV フィルタの変更

サイトがダウンした場合は、グローバル MAC アドレスをそれ以上ブロックしなくて済むように、フィルタを OTV から削除する必要があります。必要ない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 Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP キャッシュのモニタリング

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

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

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

サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド 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 メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部両方のネットワークに対しスパンド EtherChannel

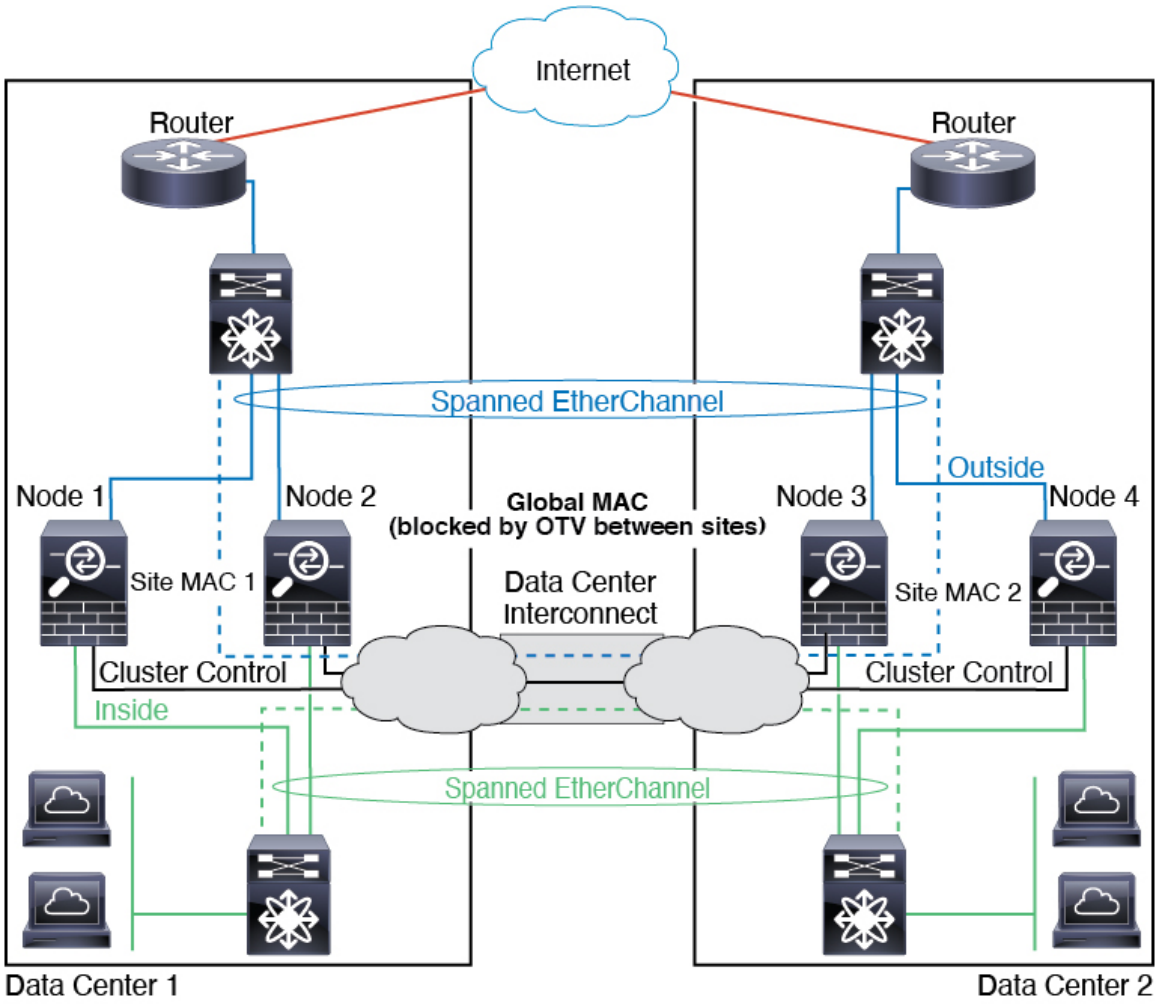
を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

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が搭載された Nexus などの一部のスイッチでは、グローバル MAC アドレスからの ARP パケットをブロックするために ARP インスペクションも使用する必要があります。ARP インスペクションでは、ASA でサイトの MAC アドレスとサイトの IP アドレスの両方を設定する必要があります。サイトの MAC アドレスのみを設定する場合は必ず ARP インスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタノード間で共有されるグローバルな仮想 MAC は、パケットを受信するためだけに使用されます。発信パケットは、各 DC クラスタからのサイト固有の MAC アドレスを使用します。この機能により、スイッチが 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。

この場合のシナリオは次のとおりです。

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



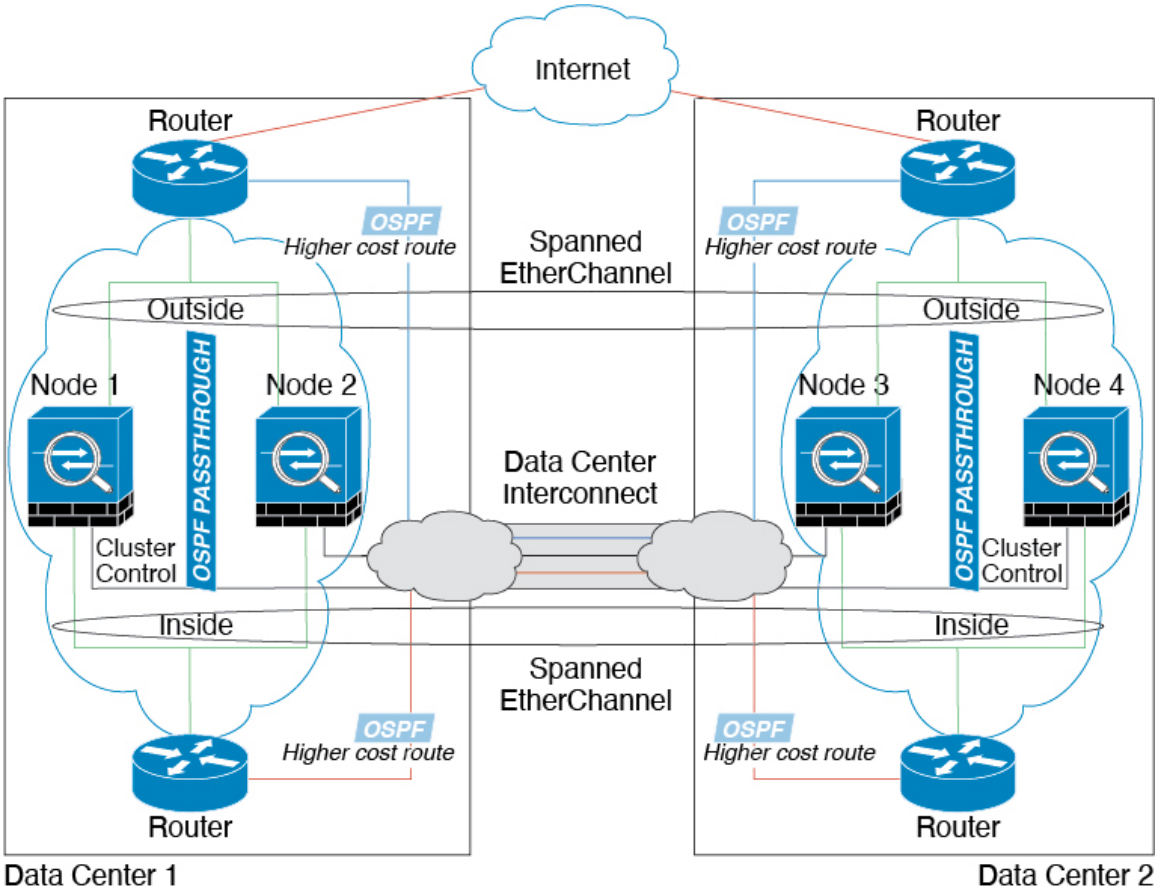
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

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

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

各サイトのスイッチの実装には、次のものを含めることができます。

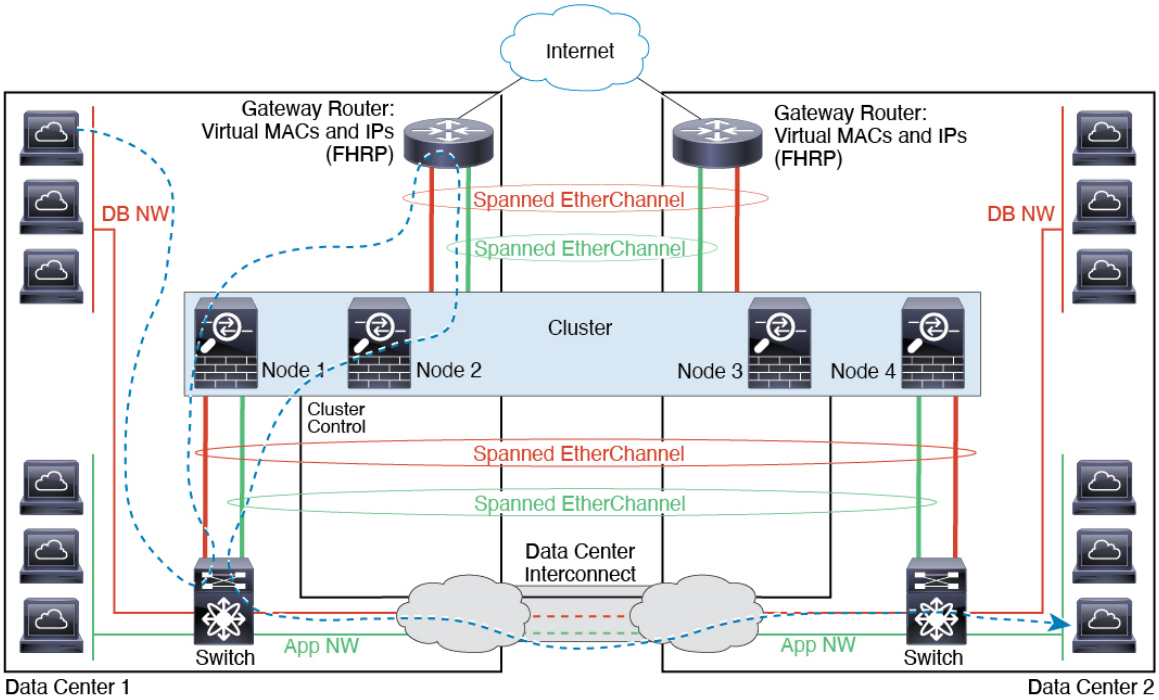
- サイト間 VSS、vPC、StackWise、StackWise Virtual：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、冗長スイッチトラフィックはDCIを経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCIが余分なトラフィックを処理できる場合、必要に応じて、各ノードをDCI経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCIを非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS、vPC、StackWise、StackWise Virtual：スイッチの冗長性を高めるには、各サイトに2つの異なる冗長スイッチペアをインストールできます。この場合、クラスタノードは、両方のローカルスイッチだけに接続されたデータセンター1のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター2のシャーシではスパンド 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 メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

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



クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

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

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- IS-IS ルーティング
- 次のアプリケーション インスペクション：
  - 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
- フェールオーバー

- 統合ルーティングおよびブリッジング
- デッド接続検出（DCD）
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - 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

集中モードでは、VPN 接続はクラスタの制御ノードとのみ確立されます。 これは VPN クラスタリングのデフォルト モードです。サイト間 VPN は、分散 VPN モードでも展開できます。この場合、S2S IKEv2 VPN 接続がノード間で分散されます。

- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ダイナミック ルーティング

個々のユニットに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。
- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 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ーおよびユーザーに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザー認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、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 サーバーに送信します。

接続設定

接続制限は、クラスタ全体に適用されます（**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max** および **set connection per-client-max** コマンドページを参照）。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 D チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバーによって所有されている場合は、D チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- 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

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

ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを処理します。接続が確立された後は、各データユニットがマルチキャスト データ パケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続

を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

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

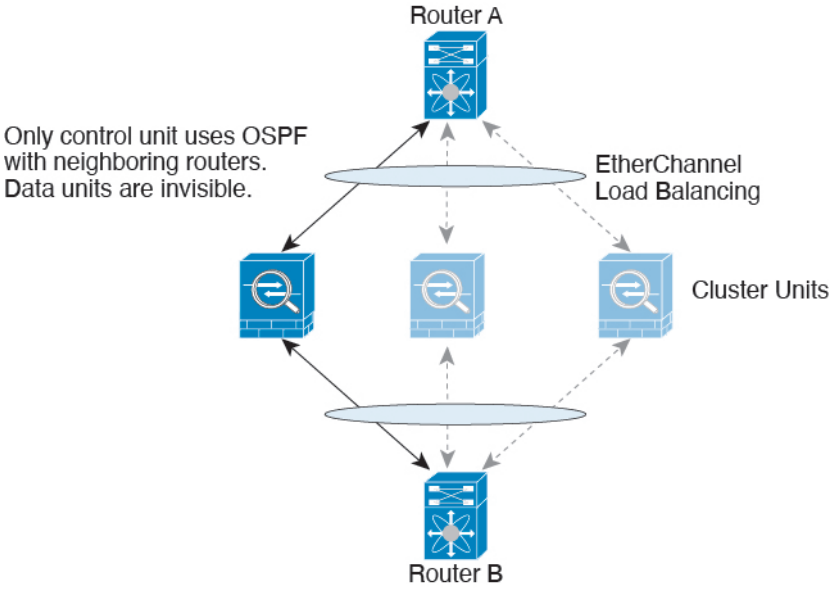
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の 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 xlates：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、ファイアウォールの設定ガイドを参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

ダイナミック ルーティングおよびクラスタリング

ルーティングプロセスは制御ユニット上だけで実行されます。ルートは制御ユニットを介して学習され、セカンダリに複製されます。ルーティングパケットがデータユニットに到着した場合は、制御ユニットにリダイレクトされます。

図 *1:* ダイナミック ルーティング



データユニットが制御ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

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

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP イン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ユーザーは新しいノードに複製されません。SNMPv3ユーザーは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、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。

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

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

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

  VPN機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御ユニットで障害が発生した場合は、すべての既存のVPN接続が失われ、VPN接続されたユーザーにとってはサービスの中断となります。新しい制御ユニットが選定されたときに、VPN 接続を再確立する必要があります。

  VPNトンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

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

（注） 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。

分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。

分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。

リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、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、TCP スループットについては、3 つの SM-40 モジュールを備えた Firepower 9300 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 135 Gbps となります。2 シャーシの場合、最大スループットの合計は 270 Gbps（2 シャーシ X 135 Gbps）の約 80 %、つまり 216 Gbps です。

制御ユニットの選定

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

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。

3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットが制御ユニットになります。

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

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的に制御ユニットになることはありません。既存の制御ユニットは常に制御ユニットのままです。ただし、制御ユニットが応答を停止すると、その時点で新しい制御ユニットが選定されます。

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

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

クラスタ内のハイ アベイラビリティ

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

シャーシ アプリケーションのモニターリング

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

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

装置のヘルス モニターリング

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

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション2のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。詳細については、制御ユニットの選定 （96 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、使用中のすべてのハードウェアインターフェイスのリンクステータスを監視し、ステータスの変更を制御ノードに報告します。シャーシ間クラスタリングでは、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニターして EtherChannel でポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には ASA アプリケーションに通知します。ヘルスモニターリングを有効にすると、デフォルトではすべての物理インターフェイスがモニターされます（EtherChannel インターフェイスのメイン EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニターできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません（最小ポート バンドル設定により異なる）。ヘルス チェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

特定のノードで監視対象のインターフェースに障害が発生し、その他のノードでそのインターフェイスがアクティブになっている場合、そのノードはクラスタから削除されます。ASA によってノードがクラスタから削除されるまでの時間は、そのノードが確立済みのメンバーであるかクラスタに参加しようとしているかによって異なります。ASA は、ノードがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。確立済みのメンバーの場合は、500 ミリ秒後にノードが削除されます。

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

デコレータ アプリケーションのモニタリング

インターフェイスに Radware DefensePro アプリケーションなどのデコレータ アプリケーションをインストールした場合、ユニットがクラスタ内にとどまるには ASA、デコレータ アプリケーションの両方が動作している必要があります。両方のアプリケーションが動作状態になるまで、ユニットはクラスタに参加しません。いったんクラスタに参加すると、ユニットはデコレータ アプリケーションが正しく動作しているか 3 秒ごとにモニターします。デコレータ アプリケーションがダウンすると、ユニットはクラスタから削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、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 メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害（最初の参加時）：クラスタ制御リンクの問題を解決した後、ASA コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASAは、無限に5分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、ASA コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動でイネーブルにする必要があります。この動作は設定可能です。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。ユニットは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシ アプリケーション通信の障害：ASA がシャーシ アプリケーションの状態が回復したことを検出すると、ASA は自動的にクラスタの再参加を試みます。
- デコレータ アプリケーションの障害：ASA はデコレータ アプリケーションが復帰したことを確認すると、クラスタへ再参加します。

- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 ユニットは 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。この動作は設定可能です。

データ パス接続状態の複製

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

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 *2:* クラスタ全体で複製される機能

トラフィック	状態のサポート	注
アップ タイム	対応	システム アップ タイムをトラッキングします。
ARP テーブル	対応	—
MAC アドレス テーブル	対応	—
ユーザ アイデンティティ	対応	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	対応	—
ダイナミック ルーティング	対応	—
SNMP エンジン ID	なし	—
Firepower 4100/9300 の分散型 VPN（サイト間）	対応	バックアップ セッションがアクティブ セッションになると、新しいバックアップ セッションが作成されます。

クラスタが接続を管理する方法

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

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。

- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、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。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタ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も配置でき、ローカルバックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

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

- ディレクタ：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も配置でき、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。最初のオーナーに障害が発生すると、ローカルディレクタは、同じサイトの新しい接続オーナーを選択します。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子で、宛先ポートは 0 です。
- 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
- 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタ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。ディレクタローカリゼーションを有効にすると、フォワーダは常にローカル ディレクタに問い合わせを行います。フォワーダがグローバル ディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタ メンバーが受信する場合などです。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN 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決定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。これが既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続の所有者はすべてのフラグメントを再構築します。

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

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

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

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

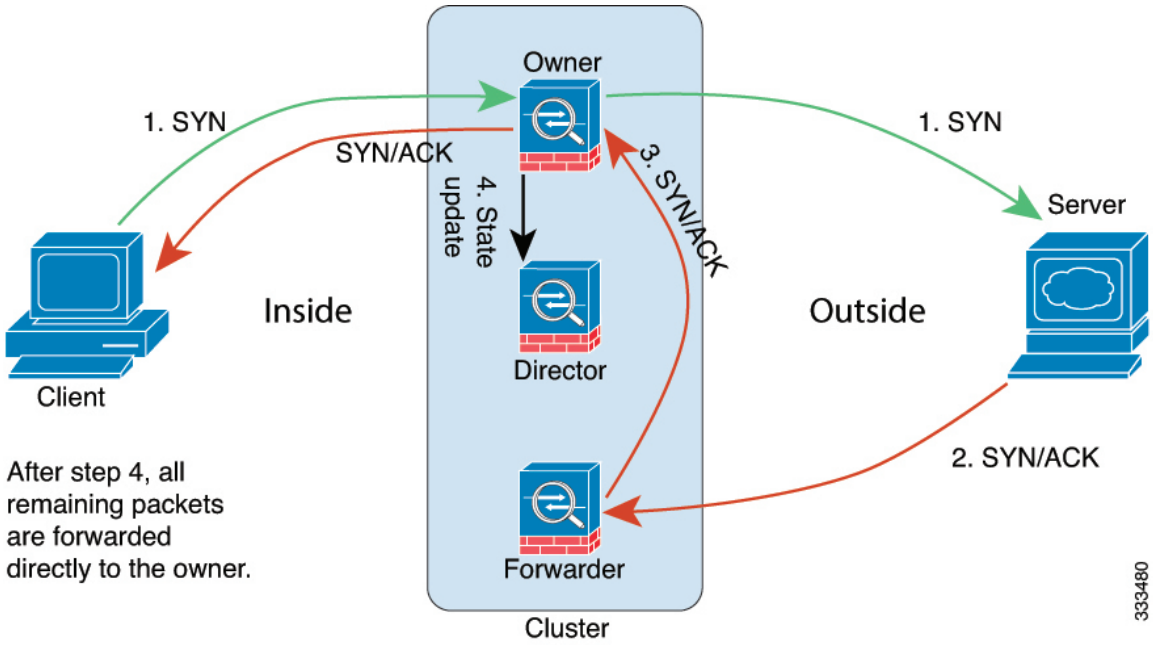
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタ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。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

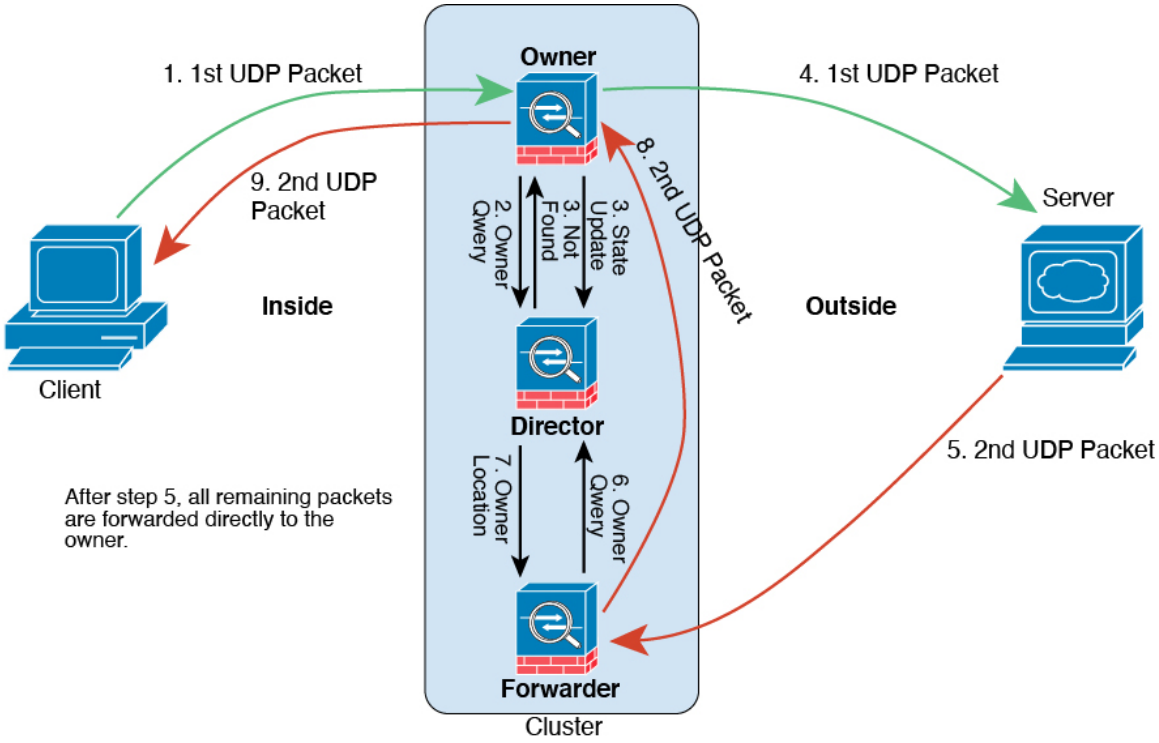


1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. 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



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

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

Firepower 4100/9300 上の ASA クラスタリングの履歴

機能名	バージョン	機能情報
Firepower 4100/9300 でのクラスタリング用の PAT ポートブロック割り当ての改善	9.16(1)	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するために、**cluster-member-limit** コマンドを使用して、クラスタ内に配置する予定の最大ノードを設定できます。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更されたコマンド：**cluster-member-limit**、**show nat pool cluster** [**summary**]、**show nat pool ip detail**
show cluster history コマンドの改善	9.16(1)	**show cluster history** コマンドの出力が追加されました。 新規/変更されたコマンド： **show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
データユニットとの設定の並列同期	9.14(1)	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更されたコマンド： **config-replicate-parallel**
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 **show cluster history**	9.14(1)	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history**
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ）
クラスタのトラフィック負荷のモニター	9.13(1)	クラスタ メンバのトラフィック負荷をモニターできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。 新規/変更されたコマンド：**debug cluster load-monitor**、**load-monitor**、**show cluster info load-monitor**

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

機能名	バージョン	機能情報
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能なIPアドレス	9.10(1)	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された FXOS コマンド： **set cluster-control-link network**
クラスタインターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。	9.10(1)	インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで **health-check monitor-interface debounce-time** コマンドまたは ASDM **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタユニットの方がポートのバンドルが速いという理由だけで、クラスタユニット上でインターフェイスがエラー表示されるのを防ぐことができます。 変更されたコマンドはありません。
内部障害発生後に自動的にクラスタに再参加する	9.9(2)	以前は、多くのエラー状態によりクラスタユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更されたコマンド：**health-check system auto-rejoin**、**show cluster info auto-join**
クラスタの信頼性の高いトランスポートプロトコルメッセージのトランスポートに関連する統計情報の表示	9.9(2)	ユニットごとのクラスタの信頼性の高いトランスポートバッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**

機能名	バージョン	機能情報
動作と一致する**cluster remove unit**コマンドの動作**no enable**	9.9(1)	**cluster remove unit** コマンドは、**no enable** コマンドと同様に、クラスタリングまたはリロードを手動で再度有効にするまで、クラスタからユニットを削除するようになりました。以前は、FXOS からブートストラップ設定を再展開すると、クラスタリングが再度有効になりました。無効化されたステータスは、ブートストラップ設定の再展開の場合でも維持されるようになりました。ただし、ASA をリロードすると、クラスタリングが再度有効になります。 新規または変更されたコマンド：cluster remove unit
シャーシのシャーシヘルスチェックの障害検出の向上	9.9(1)	シャーシヘルスチェックの保留時間をより低い値（100 ms）に設定できるようになりました。以前の最小値は 300 ms でした。最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできないことに注意してください。 新規または変更されたコマンド：**app-agent heartbeat interval**
クラスタリングのサイト間冗長性	9.9(1)	サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更されたコマンド：**site-redundancy**、**show asp cluster counter change**、**show asp table cluster chash-table**、**show conn flag**
Firepower 9300 上のクラスタリングによる分散型サイト間 VPN	9.9(1)	Firepower 9300 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）制御ユニットだけでなく、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 の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスタ（合計 6 つのクラスタ メンバー）上で動作し、各モジュールは最大約 36,000 のアクティブ セッション（合計 72,000)に対し、最大 6,000 のアクティブ セッション（合計 12,000）をサポートします。 新規または変更されたコマンド：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show connection detail**、**show crypto ikev2**

機能名	バージョン	機能情報
クラスタ ユニット ヘルスチェック障害検出の改善	9.8(1)	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージング アクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビート メッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次のコマンドを変更しました。**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details**
に対してインターフェイスを障害としてマークするために設定可能なデバウンス時間 Firepower 4100/9300 シャーシ	9.8(1)	ASA がインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。 新規または変更されたコマンド：**health-check monitor-interface debounce-time**
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次のコマンドが変更されました。**site-id**

機能名	バージョン	機能情報
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	9.7(1)	データ センターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次のコマンドが導入または変更されました。**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail**
の 16 個のシャーシのサポート Firepower 4100 シリーズ	9.6(2)	Firepower 4100 シリーズ では最大 16 個のシャーシをクラスタに追加できるようになりました。 変更されたコマンドはありません。
Firepower 4100 シリーズ のサポート	9.6(1)	FXOS 1.1.4 では、ASA は最大 6 個のシャーシの Firepower 4100 シリーズ でサイト間クラスタリングをサポートします。 変更されたコマンドはありません。
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	9.6(1)	スパンド EtherChannel のルーテッド モードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイ トランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次のコマンドが変更されました。**mac-address**、**show interface**
16 のモジュールのシャーシ間クラスタリング、および Firepower 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 16 のモジュールを搭載することができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。 変更されたコマンドはありません。

機能名	バージョン	機能情報
ルーテッド ファイアウォールモードのスパンド EtherChannel のサイト間クラスタリングサポートのサイト別 MAC アドレス	9.5(2)	ルーテッドモードでは、スパンド EtherChannel サイト間クラスタリングを使用することができます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。 次のコマンドを導入または変更しました。**site-id**、**mac-address site-id**、**show cluster info**、**show interface**
インターフェイスまたはクラスタ制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスタのカスタマイズ	9.5(2)	インターフェイスまたはクラスタ制御リンクが失敗した場合、auto-rejoin 動作をカスタマイズできます。 次のコマンドを導入しました。 **health-check auto-rejoin**
ASA クラスタは、GTPv1 と GTPv2 をサポートします	9.5(2)	ASA クラスタは、GTPv1 および GTPv2 インスペクションをサポートします。 変更されたコマンドはありません。
TCP 接続のクラスタ複製遅延	9.5(2)	この機能で、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。 次のコマンドを導入しました。**cluster replication delay**
サイト間フローモビリティの LISP インスペクション	9.5(2)	Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID をその場所から 2 つの異なるナンバリング スペースに分離し、サーバーの移行をクライアントに対して透過的にします。ASA は、場所変更の LISP トラフィックを検査し、その情報をシームレスなクラスタリング運用に活用できます。ASA クラスタ メンバーは、最初のホップ ルータと出力トンネル ルータまたは入力トンネル ルータの間の LISP トラフィックを検査し、フロー オーナーの所在場所を新規サイトに変更します。 次のコマンドが導入または変更されました。**allowed-eid**、**clear cluster info flow-mobility counters**、**clear lisp eid**、**cluster flow-mobility lisp**、**debug cluster flow-mobility**、**debug lisp eid-notify-intercept**、**flow-mobility lisp**、**inspect lisp**、**policy-map type inspect lisp**、**site-id**、**show asp table classify domain inspect-lisp**、**show cluster info flow-mobility counters**、**show conn**、**show lisp eid**、**show service-policy**、**validate-key**
キャリア グレード NAT の強化がフェールオーバーおよび ASA クラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 次のコマンドが変更されました。**show local-host**

機能名	バージョン	機能情報
クラスタリング トレースエントリの設定可能なレベル	9.5(2)	デフォルトで、すべてのレベルクラスタリング イベントは、多くの下位レベルのイベント以外に、トレースバッファに含まれます。より上位レベルのイベントへのトレースを制限するために、クラスタの最小トレース レベルを設定できます。 次のコマンドが導入されました。**trace-level**
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4 (1.150)	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**

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。