



における Threat Defense のクラスタの展開 Cisco Secure Firewall 3100/4200 のクラスタ リング

クラスタリングを利用すると、複数の Threat Defense 装置をグループ化して1つの論理デバイスにすることができます。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 \(54 ページ\)](#) を参照してください。

- [Cisco Secure Firewall 3100/4200 のクラスタリングについて \(1 ページ\)](#)
- [クラスタリングのライセンス \(3 ページ\)](#)
- [クラスタリングの要件と前提条件 \(3 ページ\)](#)
- [クラスタリングに関するガイドライン \(4 ページ\)](#)
- [クラスタリングの設定 \(9 ページ\)](#)
- [クラスタノードの管理 \(31 ページ\)](#)
- [クラスタのモニタリング \(42 ページ\)](#)
- [クラスタのトラブルシューティング \(48 ページ\)](#)
- [クラスタリングの例 \(51 ページ\)](#)
- [クラスタリングの参考資料 \(53 ページ\)](#)
- [クラスタリングの履歴 \(67 ページ\)](#)

Cisco Secure Firewall 3100/4200 のクラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

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

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

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータがスパンド EtherChannel。クラスタ内の複数のメンバのインターフェイスをグループ化して1つの EtherChannel とします。この EtherChannel がユニット間のロードバランシングを実行します。

制御ノードとデータノードの役割

クラスタ内のメンバーの1つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、プライオリティ設定によって決まります。プライオリティは1～100の範囲内で設定され、1が最高のプライオリティです。他のすべてのメンバーはデータノードです。最初にクラスタを作成するときに、制御ノードにするノードを指定します。これは、クラスタに追加された最初のノードであるため、制御ノードになります。

クラスタ内のすべてのノードは、同一の設定を共有します。最初に制御ノードとして指定したノードは、データノードがクラスタに参加するときにその設定を上書きします。そのため、クラスタを形成する前に制御ノードで初期設定を実行するだけで済みます。

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

クラスタ インターフェイス

データインターフェイスは、スパンド EtherChannel。詳細については、[クラスタインターフェイスについて \(9 ページ\)](#) を参照してください。



(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。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、[クラスタ制御リンク \(9 ページ\)](#) を参照してください。

コンフィギュレーションの複製

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

管理ネットワーク

管理インターフェイスを使用して各ノードを管理する必要があります。クラスタリングでは、データインターフェイスからの管理はサポートされていません。

クラスタリングのライセンス

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

制御ノードを Management Center に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタを作成する前に、データノードにどのライセンスが割り当てられているのかは問題になりません。制御ノードのライセンス設定は、各データノードに複製されます。クラスタのライセンスは、システム (⚙️) > [ライセンス (Licenses)] > [スマートライセンス (Smart Licenses)] > [ライセンスの編集 (Edit Licenses)] または [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] > [ライセンス (License)] エリアで変更できます。



- (注) Management Center にライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Management Center にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

クラスタリングの要件と前提条件

モデルの要件

- Secure Firewall 3100 : 最大 8 ユニット
- Secure Firewall 4200 : 最大 8 ユニット

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

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ユニット：

- 同じモデルである必要があります。
- 同じインターフェイスを含めること。
- Management Center へのアクセスは管理インターフェイスから行うこと。データインターフェイスの管理はサポートされていません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレスアップグレードがサポートされます。
- ファイアウォールモードが同じであること（ルーテッドまたは透過）。
- 同じドメインに属していること。
- 同じグループに属していること。
- 保留中または進行中の展開がないこと。
- 制御ノードにサポート対象外の機能が設定されていないこと（「[クラスタリングでサポートされない機能（54 ページ）](#)」を参照）。
- データノードに VPN が設定されていないこと。制御ノードにはサイト間 VPN を設定できません。

スイッチ要件

- クラスタリングの設定前にスイッチの設定を完了していること。クラスタ制御リンクに接続されているポートに適切な MTU 値（高い値）が設定されていること。デフォルトでは、クラスタ制御リンクの MTU は、データインターフェイスよりも 100 バイト大きく設定されています。スイッチで MTU が一致しない場合、クラスタの形成に失敗します。

クラスタリングに関するガイドライン

ファイアウォールモード

ファイアウォールモードは、すべてのユニットで一致する必要があります。

高可用性

クラスタリングでは、高可用性はサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

スイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンク インターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンク インターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。
- 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。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経路でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

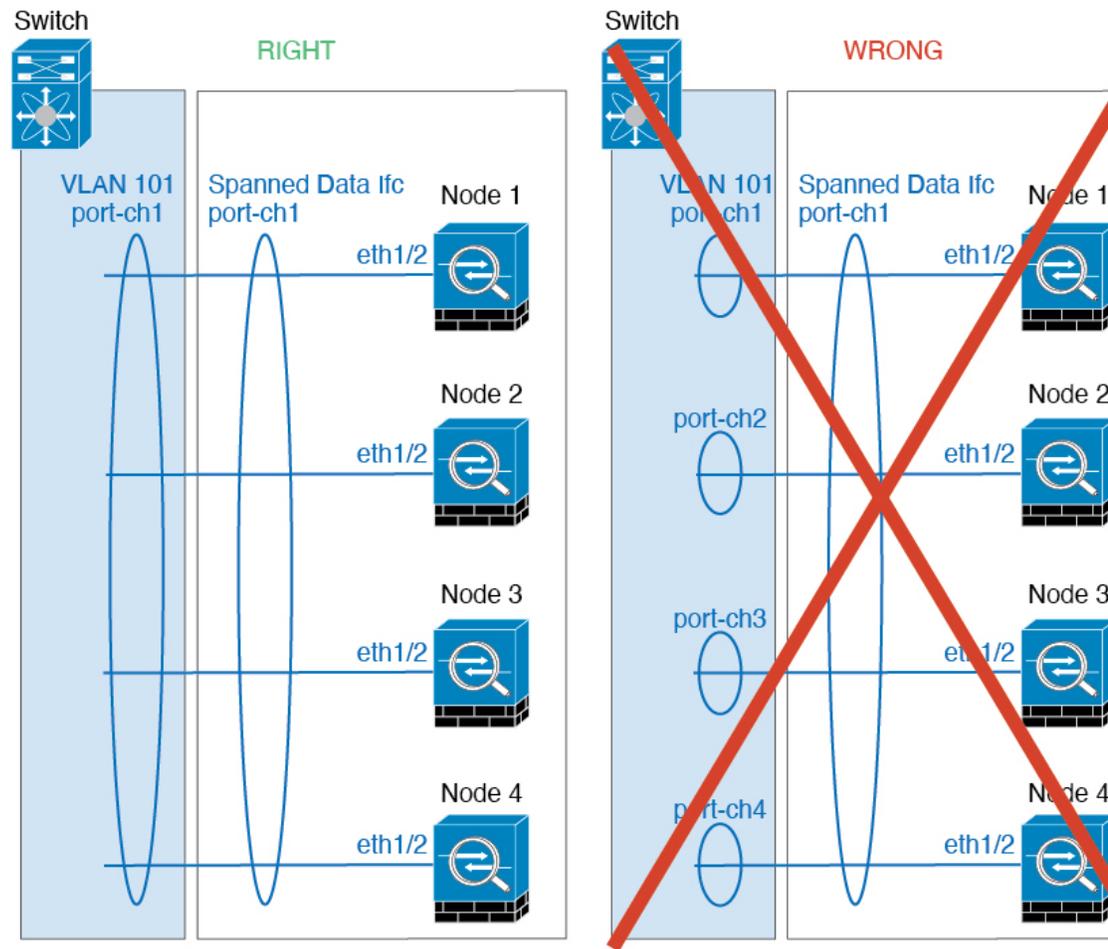
router(config)# **port-channel id hash-distribution fixed**

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

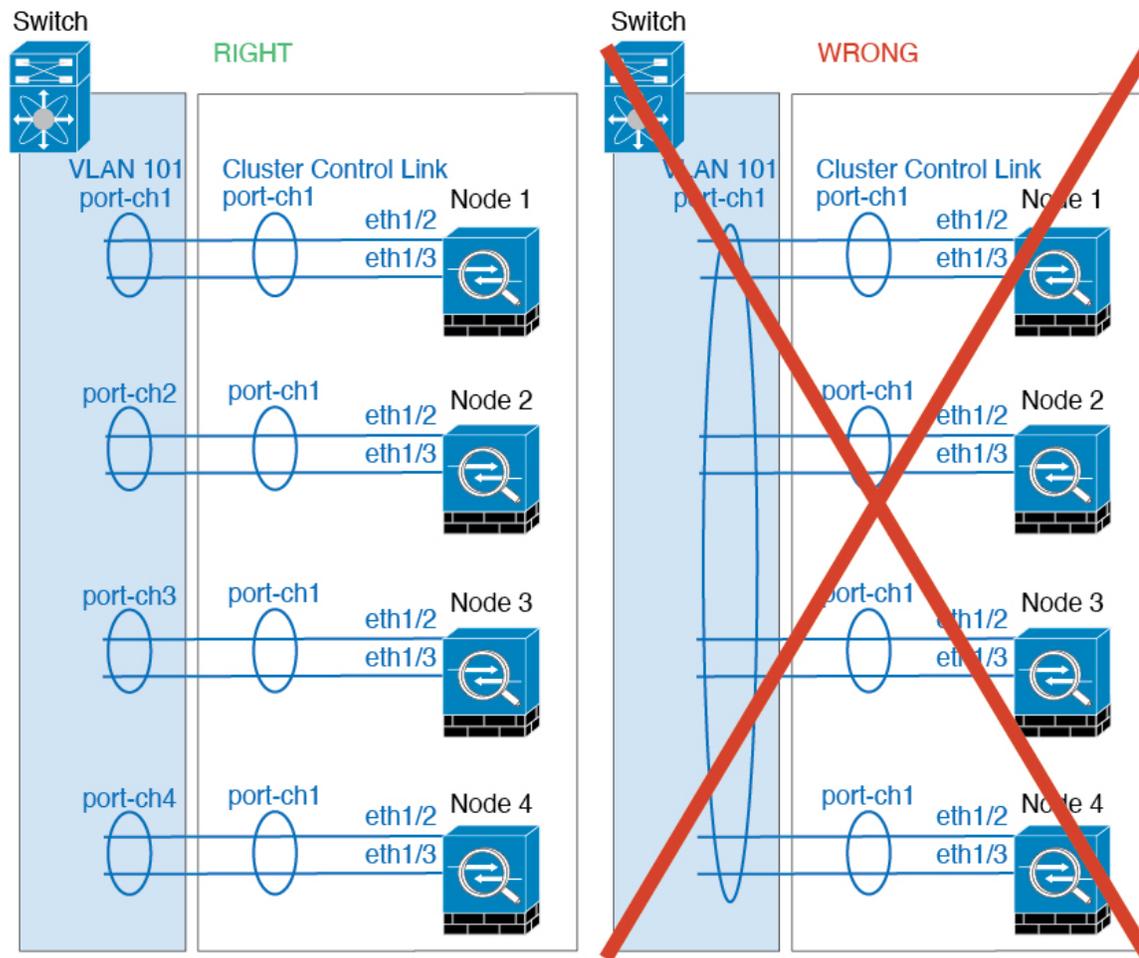
- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能を無効化する必要があります。

EtherChannel

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
 - スパンド EtherChannel：クラスタユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャンネルグループ内にあることを確認してください。



- デバイス ローカル EtherChannel : クラスター ユニット デバイス ローカル EtherChannel (クラスター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ーユニット EtherChannel を結合して1つの EtherChannel としないでください。



その他のガイドライン

- 重要なトポロジの変更（EtherChannel インターフェイスの追加や削除、Threat Defense またはスイッチのインターフェイスの有効化や無効化、VSS または vPC を形成するスイッチの追加など）が発生した場合は、ヘルスチェック機能を無効にし、無効になっているインターフェイスのインターフェイスモニタリングも無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。
- ユニットの既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバー ポートがダウンし、サーバーが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージが ASA クラスタに送信されます。このようなメッセージにより、ASA

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。

- 復号された TLS/SSL 接続の場合、復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新しいユニットへの新しい接続を確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。

クラスタリングのデフォルト

- cLACP システム ID は自動生成され、システムの優先順位はデフォルトでは 1 になっています。
- クラスタのヘルスチェック機能は、デフォルトで有効になり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネットヘルスマonitoringが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 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。

クラスタリングの設定

Management Center にクラスタを追加するには、各ノードをスタンドアロンユニットとして Management Center に追加し、制御ノードにするユニットでインターフェイスを設定してからクラスタを形成します。

クラスタ インターフェイスについて

データインターフェイスは、スパンド EtherChannel など) として設定することはできません。また、各ユニットの、少なくとも 1 つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンク

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

クラスタ制御リンク トラフィックの概要

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

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 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 インターフェイスとネットワーク

クラスタ制御リンクには、任意の物理インターフェイスまたはEtherChannelを使用できます。VLANサブインターフェイスをクラスタ制御リンクとして使用することはできません。管理インターフェイスも使用できません。

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



- (注) 2 メンバークラスタの場合、ノード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。(テスト目的などで) ユニットの直接接続する必要がある場合は、クラスタを形成する前に、両方のノードでクラスタ制御リンクインターフェイスを設定して有効にする必要があります。

クラスタ制御リンクのサイジング

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

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

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

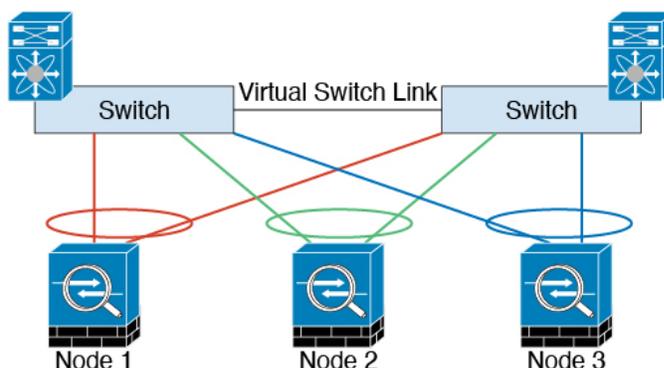
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。



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

クラスタ制御リンクの冗長性

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。



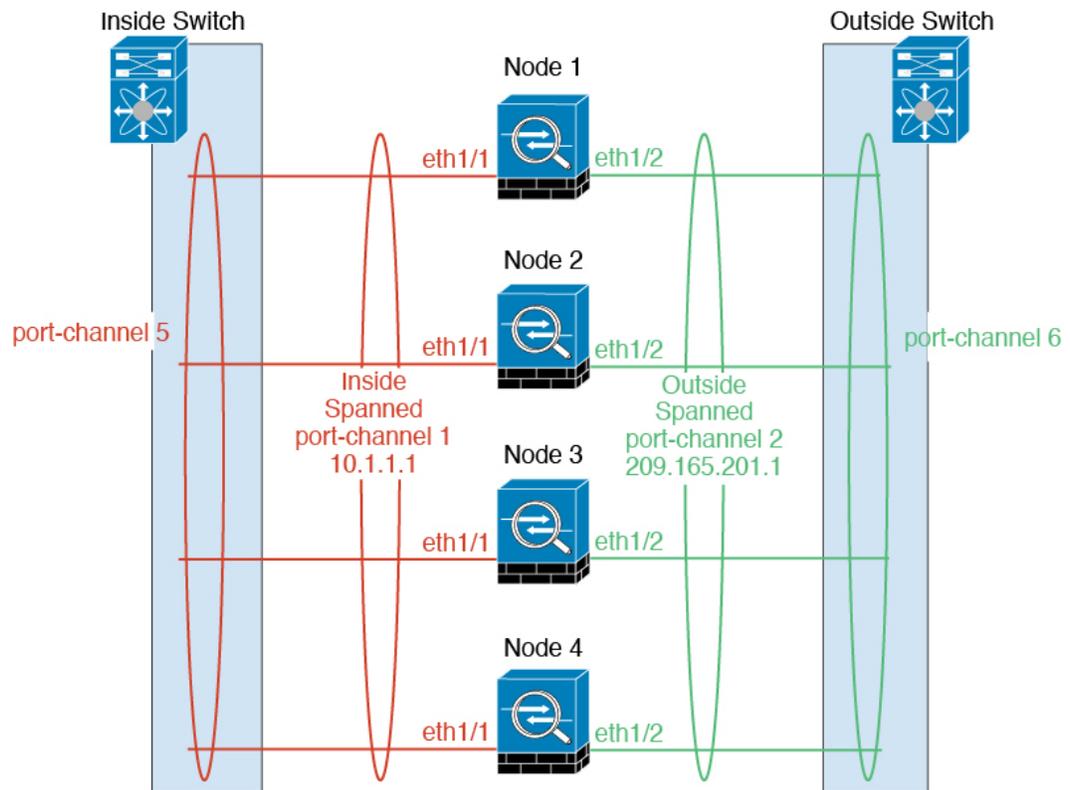
クラスタ制御リンクの信頼性

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。

スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッドモードでは、EtherChannel は単一の IP アドレスを持つルーテッドインターフェイスとして設定されます。トランスペアレントモードでは、IP アドレスはブリッジグループメンバ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。



最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

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

ロードバランシング

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



- (注) スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port** (Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照) を使用することをお勧めします。クラスター内の ASA へのトラフィックが均等に分散されなくなる可能性があるため、ロードバランシングアルゴリズムでは、**vlan** キーワードを使用しないでください。

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

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

EtherChannel の冗長性

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

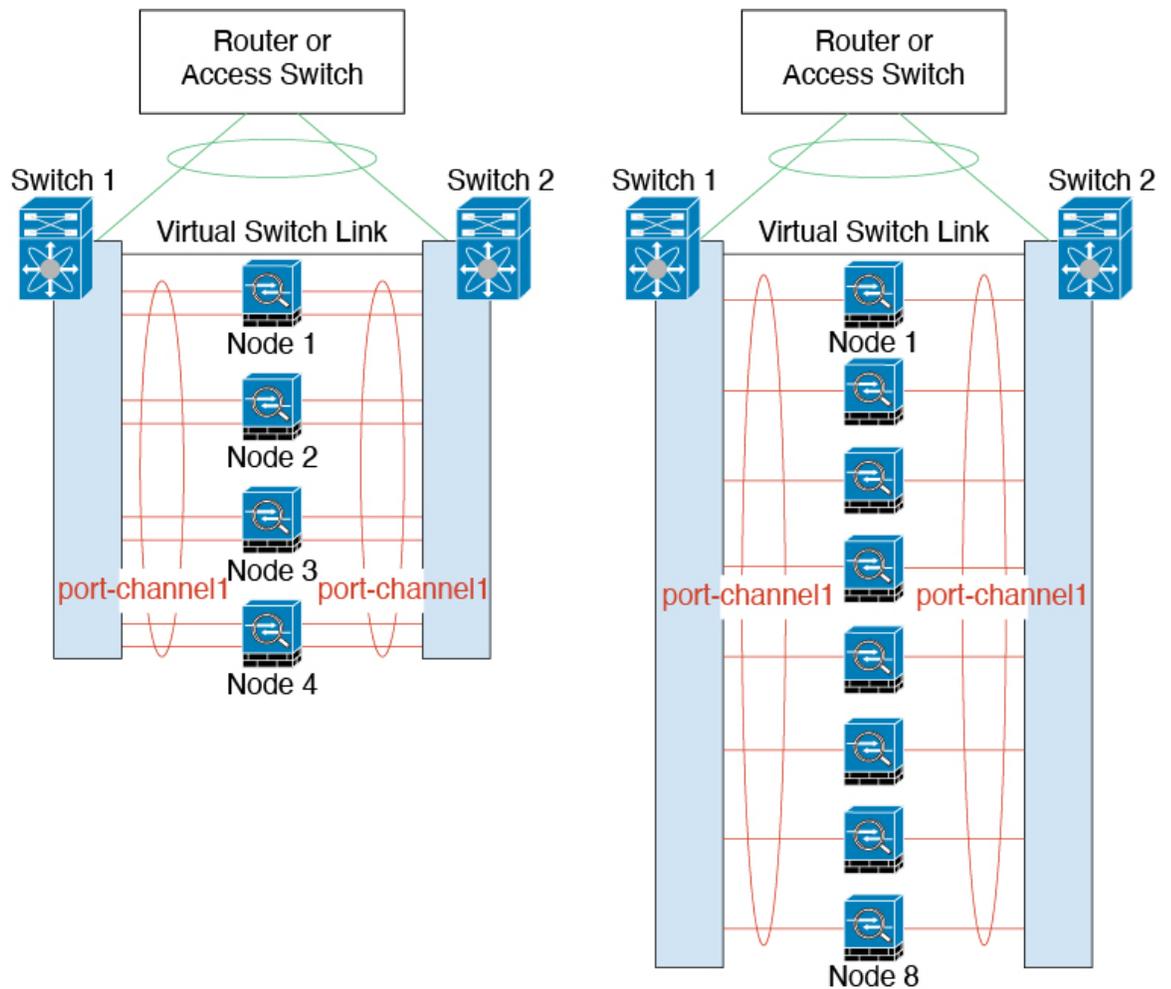
冗長スイッチシステムへの接続

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

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

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

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



Management Center へのデバイスのケーブル接続と追加

クラスタリングを設定する前に、デバイスを準備する必要があります。具体的には、すべてのノードがクラスタ制御リンクを介して通信できない限り、クラスタは起動しません。したがって、クラスタを形成する前に、クラスタ制御リンクの準備ができていなければならない必要があります。

手順

-
- ステップ 1** クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。
 - ステップ 2** アップストリームとダウンストリームの機器を設定します。
 - a) クラスタ制御リンクのネットワークに、データインターフェ이스の最大 MTU より少なくとも 100 バイト高くなるように MTU を設定します。

デフォルトでは、クラスタ制御リンクの MTU は 1500 バイトです。そのため、クラスタノードのクラスタ制御リンクの MTU は 1600 バイトに設定されます。データインターフェイスにより高い MTU を使用する場合は、それに応じて接続スイッチのクラスタ制御リンクの MTU を増やしてください。

- b) オプションの EtherChannel を含め、アップストリームおよびダウンストリーム機器でクラスタ制御リンクインターフェイスを設定します。

クラスタ制御リンクの要件については、「[クラスタ制御リンクインターフェイスとネットワーク \(10 ページ\)](#)」を参照してください。

- c) スパンド EtherChannel を含むアップストリームおよびダウンストリーム機器のデータインターフェイスを設定します。

スパンド EtherChannel のケーブル接続の方法については、「[クラスタインターフェイスについて \(9 ページ\)](#)」を参照してください。

- ステップ 3** 同じドメインおよびグループ内のスタンドアロンデバイスとして、各ノードを Management Center に追加します。

[登録キーを使用した Management Center へのデバイスの追加](#)を参照してください。単一のデバイスでクラスタを作成し、後からノードを追加できます。デバイスを追加したときに行った初期設定（ライセンス、アクセス コントロール ポリシー）は、制御ノードからすべてのクラスタノードに継承されます。クラスタを形成するときに制御ノードを選択します。

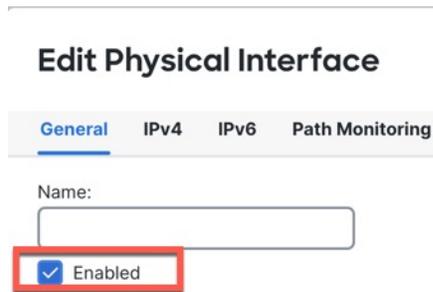
- ステップ 4** 制御ノードにするデバイスでクラスタ制御リンクを有効にします。

他のノードを追加すると、それらのノードはクラスタ制御リンク設定を継承します。

(注) クラスタ制御リンクの名前、または IP アドレスを設定しないでください。クラスタの形成時に、クラスタ制御リンクインターフェイスの MTU が最も高いデータインターフェイス MTU よりも 100 バイト多い値に自動的に設定されるため、設定が必要なくなりました。

- a) 制御ノードにするデバイスで、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、[編集 (Edit)] (✎) をクリックします。
- b) [インターフェイス (Interfaces)] をクリックします。
- c) インターフェイスをイネーブルにします。クラスタ制御リンクに EtherChannel を使用する場合は、すべてのメンバーをイネーブルにします。[物理インターフェイスの有効化およびイーサネット設定の構成](#)を参照してください。

図 1: クラスタ制御リンクインターフェイスの有効化



- d) (任意) EtherChannel を追加します。EtherChannel の設定を参照してください。

クラスタ制御リンクで不要なトラフィックを削減できるように、クラスタ制御リンクのメンバーインターフェイスに対しては On モードを使用することをお勧めします (デフォルトはアクティブモードです)。クラスタ制御リンクは LACP トラフィックのオーバーヘッドを必要としません。これは隔離された、安定したネットワークであるからです。注：データ EtherChannel を Active モードに設定することをお勧めします。

- e) [保存 (Save)] > [展開 (Deploy)] の順にクリックして、インターフェイスの変更を制御ノードに展開します。

クラスタの作成

Management Center 内の 1 台以上のデバイスでクラスタを形成します。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択してから、[追加 (Add)] > [クラスタ (Cluster)] の順に選択します。 > > [クラスタの追加 (Add Cluster)] ウィザードが表示されます。

図 2:[クラスタの追加 (Add Cluster)]ウィザード

Add Cluster Wizard

1 Configuration — 2 Summary

▲ Create a cluster for supported models. Note: For the Firepower 4100/9300, use the Add Device option.

Cluster Name*
ftdcluster

Cluster Key

Control Node
You can form the cluster with just the control node to reduce formation time.

Node*
172.16.0.50

Cluster Control Link Network*
10.10.10.0 / 24 (254 addresses)

Cluster Control Link*
Ethernet1/7

Cluster Control Link IPv4 Address*
10.10.10.1

Priority*
1

Site ID
0

Data Nodes (Optional)
Data node hardware needs to match the control node hardware.

Node*
172.16.0.51

Cluster Control Link IPv4 Address*
10.10.10.2

Priority*
2

Site ID
0

Remove

Add a data node

ステップ 2 制御トラフィックの [クラスタ名 (Cluster Name)]と認証用の [クラスタキー (Cluster Key)]を指定します。

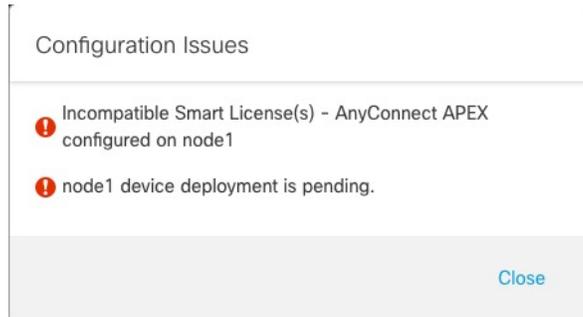
- [クラスタ名 (Cluster Name)] : 1 ~ 38 文字の ASCII 文字列。
- [クラスタキー (Cluster Key)] : 1 ~ 63 文字の ASCII 文字列。 [クラスタキー (Cluster Key)]の値は暗号キーを生成するために使用されます。この暗号は、データパストラフィック (接続状態の更新や転送されるパケットなど) には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

ステップ 3 [制御ノード (Control Node)]については、次のように設定します。

- [ノード (Node)] : 最初に制御ノードにするデバイスを選択します。Management Center がクラスタを形成すると、このノードが最初にクラスタに追加されて制御ノードになります。

- (注) ノード名の横に [エラー (Error)] (❗) アイコンが表示されている場合は、そのアイコンをクリックして設定の問題を表示します。クラスタの形成をキャンセルし、問題を解決してからクラスタの形成に戻る必要があります。次に例を示します。

図 3: 設定の問題



上記の問題を解決するには、サポート対象外の VPN ライセンスを削除し、保留中の設定の変更をデバイスに展開します。

- [クラスタ制御リンクネットワーク (Cluster Control Link Network)] : IPv4 サブネットを指定します。このインターフェイスでは IPv6 はサポートされていません。[24]、[25]、[26]、または [27] サブネットを指定します。
- [クラスタ制御リンク (Cluster Control Link)] : クラスタ制御リンクに使用する物理インターフェイスまたは EtherChannel を選択します。

(注) クラスタ制御リンクインターフェイスの MTU は、最も高いデータインターフェイス MTU よりも 100 バイト多い値に自動的に設定されます。デフォルトでは、MTU は 1,600 バイトです。MTU を増やす場合は、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] ページを参照してください。

クラスタ制御リンクに接続されているスイッチの MTU を適切な値 (高い値) に設定してください。そうしないと、クラスタ形成に失敗します。

- [クラスタ制御リンク IPv4 アドレス (Cluster Control Link IPv4 Address)] : このフィールドには、クラスタ制御リンクネットワークの最初のアドレスが自動的に入力されます。必要に応じてホストアドレスを編集できます。
- [プライオリティ (Priority)] : 制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは 1 ~ 100 であり、1 が最高のプライオリティです。他のノードよりプライオリティを低く設定しても、クラスタが最初に形成されたときは、このノードが引き続き制御ノードになります。
- [サイト ID (Site ID)] : (FlexConfig 機能) このノードのサイト ID を 1 ~ 8 の間で入力します。値を 0 に設定するとサイト間クラスタリングが無効になります。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上

させることを目的としたサイト間クラスタの追加のカスタマイズは、FlexConfig 機能を使用した場合にのみ設定できます。

ステップ 4 [データノード (Data Nodes)] (オプション) で、[データノードを追加 (Add a data node)] をクリックしてクラスタにノードを追加します。

クラスタの形成を高速化するために制御ノードのみでクラスタを形成することも、すべてのノードをここで追加することも可能です。各データノードで以下を設定します。

- [ノード (Node)] : 追加するデバイスを選択します。
 - (注) ノード名の横に [エラー (Error)] (❗) アイコンが表示されている場合は、そのアイコンをクリックして設定の問題を表示します。クラスタの形成をキャンセルし、問題を解決してからクラスタの形成に戻る必要があります。
- [クラスタ制御リンクIPv4アドレス (Cluster Control Link IPv4 Address)] : このフィールドには、クラスタ制御リンクネットワークの次のアドレスが自動的に入力されます。必要に応じてホストアドレスを編集できます。
- [プライオリティ (Priority)] : 制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは 1 ~ 100 であり、1 が最高のプライオリティです。
- [サイトID (Site ID)] : (FlexConfig 機能) このノードのサイトID を 1 ~ 8 の間で入力します。値を 0 に設定するとサイト間クラスタリングが無効になります。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、FlexConfig 機能を使用した場合にのみ設定できます。

ステップ 5 [続行 (Continue)] をクリックします。[概要 (Summary)] を確認し、[保存 (Save)] をクリックします。

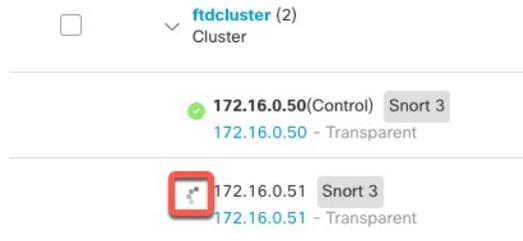
[デバイス (Devices)] > [デバイス管理 (Device Management)] ページにクラスタ名が表示されます。クラスタを展開して、クラスタノードを表示します。

図 4: クラスタの管理

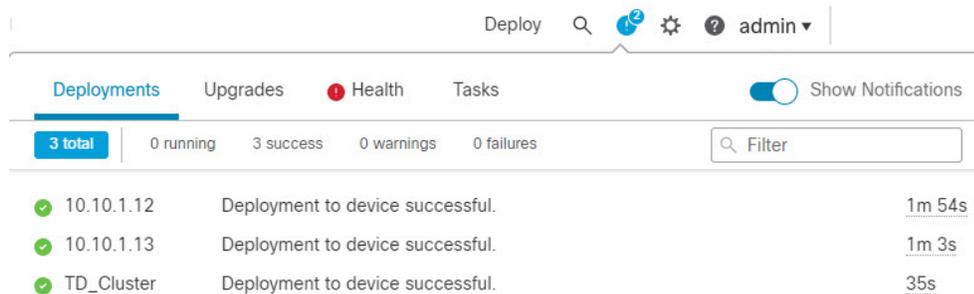
Node Name	Model/Version	Status	Configuration
172.16.0.50 (Control) Snort 3 172.16.0.50 - Transparent	Firewall 3120 Threat Defense 7.1.0	Active (Green)	Base, Threat (2 more...) Default AC Policy
172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense 7.1.0	Warning (Orange)	Base, Threat (2 more...) Default AC Policy

現在登録中のノードには、ロードアイコンが表示されます。

図 5: ノードの登録



クラスタノードの登録をモニターするには、[通知 (Notifications)] アイコンをクリックし、[タスク (Tasks)] を選択します。Management Center は、ノードの登録ごとにクラスタ登録タスクを更新します。



ステップ 6 クラスタの [編集 (Edit)] (✎) をクリックして、デバイス固有の設定を指定します。

ほとんどの設定は、クラスタ内のノードではなく、クラスタ全体に適用できます。たとえば、ノードごとに表示名を変更できますが、インターフェイスはクラスタ全体についてのみ設定できます。

ステップ 7 [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] 画面に、クラスタの [全般 (General)] などの設定が表示されます。

図 6: クラスタ設定

The screenshot displays the configuration page for a cluster named 'ftdcluster'. The top navigation bar includes 'Cluster', 'Device', 'Routing', 'Interfaces', and 'Inline Sets'. The main content is organized into several sections:

- General:** Name: ftdcluster, Transfer Packets: No, Status: (Green dot), Control: 172.16.0.50, Cluster Live Status: View.
- License:** Base: Yes, Export-Controlled Features: No, Malware: Yes, Threat: Yes, URL Filtering: Yes, AnyConnect Apex: N/A, AnyConnect Plus: N/A, AnyConnect VPN Only: N/A.
- Security Engine:** Intrusion Prevention Engine: Snort 3.0, with a 'Revert to Snort 2' button.
- Applied Policies:** Access Control Policy: Default AC Policy, Prefilter Policy: Default Prefilter Policy, SSL Policy, DNS Policy: Default DNS Policy, Identity Policy, NAT Policy, Platform Settings Policy, NGFW QoS Policy, FlexConfig Policy.
- Health:** Policy: Initial_Health_Policy (2021-10-30 01:21:29).
- Advanced Settings:** Application Bypass: No, Bypass Threshold: 3000 ms, Object Group Search: Disabled, Interface Object Optimization: Disabled.

[全般 (General)] 領域には、次のクラスタに固有の項目が表示されます。

- [全般 (General)] > [名前 (Name)] : [編集 (Edit)] (✎) をクリックして、クラスタの表示名を変更します。

This close-up view shows the 'General' section of the configuration page. The 'Name' field is set to 'ftdcluster'. To the right of the 'Name' field, there is a red-bordered edit icon (✎). Other fields include 'Transfer Packets: No', 'Status: (Yellow triangle)', 'Control: 172.16.0.50', and 'Cluster Live Status: View'.

その後に、[名前 (Name)] フィールドを設定します。

General ?

Name:

Transfer Packets:

Compliance Mode:

TLS Crypto Acceleration:

Force Deploy: →

- [全般 (General)] > [クラスタステータスの表示 (View cluster status)] : [クラスタステータスの表示 (View cluster status)] リンクをクリックして [クラスタステータス (Cluster Status)] ダイアログボックスを開きます。

General ✎	
Name:	ftdcluster
Transfer Packets:	No
Status:	▲
Control:	172.16.0.50
Cluster Live Status:	View

[クラスタステータス (Cluster Status)] ダイアログボックスでは、[すべて照合 (Reconcile All)] をクリックしてデータユニットの登録を再試行することもできます。ノードからクラスタ制御リンクに ping を実行することもできます。 [クラスター制御リンクへの ping の実行 \(49 ページ\)](#) を参照してください。

Cluster Status ?

Overall Status: Cluster has all nodes in sync

Nodes details (2)

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 Control	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮

Dated: 11:52:26 | 20 Dec 2021

- [全般 (General)] > [トラブルシューティング (Troubleshoot)] : トラブルシューティングログを生成およびダウンロードしたり、クラスタ CLI を表示したりできます。 [クラスタのトラブルシューティング \(48 ページ\)](#) を参照してください。

図 7: トラブルシューティング

General ✎

Name: ● clusterVFTD

Transfer Packets: Yes

Status: ●

Control: 10.10.43.21

Cluster Live Status: View

Troubleshoot:

ステップ 8 [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Devices)] の右上のドロップダウンメニューで、クラスタ内の各メンバーを選択し、次の設定を指定することができます。

図 8: デバイス設定

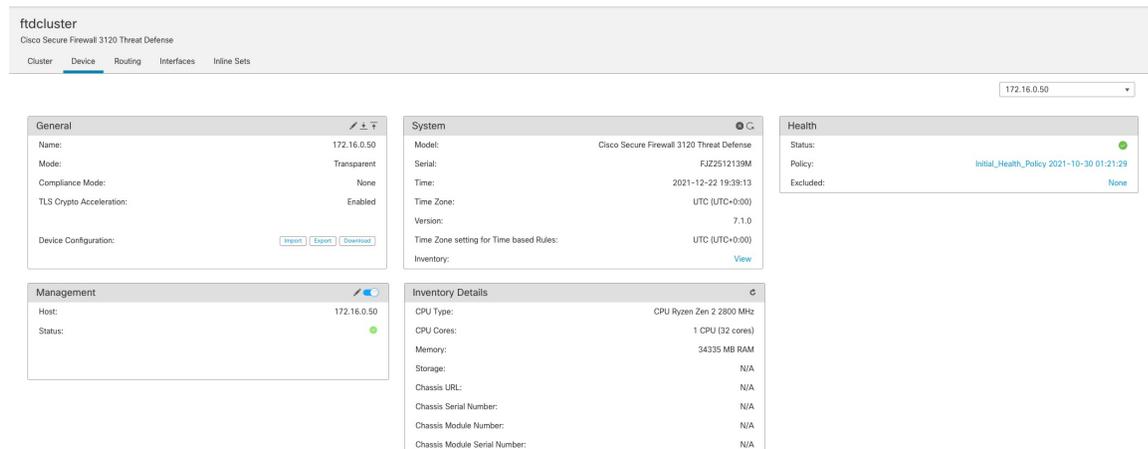
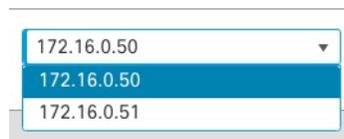
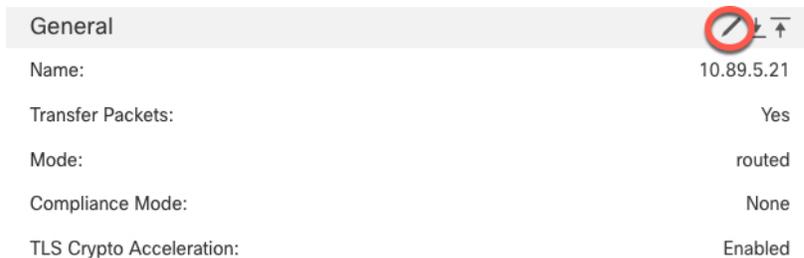


図 9: ノードの選択



- [全般 (General)] > [名前 (Name)] : [編集 (Edit)] (✎) をクリックして、クラスタメンバーの表示名を変更します。



その後に、[名前 (Name)] フィールドを設定します。

General ?

Name:

Transfer Packets:

Mode: routed

Compliance Mode: None

Performance Profile: Default

TLS Crypto Acceleration: Disabled

Force Deploy: →

- [管理 (Management)]>[ホスト (Host)]: デバイス設定で管理 IP アドレスを変更する場合は、Management Center で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにする必要があります。最初に接続を無効にし、[管理 (Management)]領域で[ホスト (Host)]のアドレスを編集してから、接続を再度有効にします。

Management	
Host:	10.89.5.20
Status:	✓

インターフェイスの設定

データインターフェイスをスパンド EtherChannel として設定します。

手順

- ステップ 1 [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択し、クラスタの横にある[編集 (Edit)] () をクリックします。
- ステップ 2 [インターフェイス (Interfaces)]をクリックします。
- ステップ 3 スパンド EtherChannel データインターフェイスを設定します。
 - a) EtherChannel は 1 つ以上設定します。 [EtherChannel の設定](#)を参照してください。

EtherChannel には 1 つ以上のメンバーインターフェイスを含めることができます。この EtherChannel はすべてのノードにまたがっているため、各ノードに必要なメンバーインター

フェイスは1つだけです。ただし、スループットと冗長性を向上させるために、メンバーを複数にすることをお勧めします。

- b) (任意) EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。サブインターフェイスの追加を参照してください。
- c) EtherChannel インターフェイスの **[編集 (Edit)]** (✎) をクリックします。
- d) ルーテッドモードのインターフェイスの設定 (トランスペアレントモードの場合はブリッジグループインターフェイスの設定) に従って、名前、IP アドレス、およびその他のパラメータを設定します。

(注) クラスタ制御リンクインターフェイスの MTU がデータインターフェイスの MTU より 100 バイト以上大きくない場合、データインターフェイスの MTU を減らす必要があるというエラーが表示されます。デフォルトでは、クラスタ制御リンクの MTU は 1,600 バイトです。データインターフェイスの MTU を増やす場合は、まずクラスタ制御リンクの MTU を増やしてください。

- e) EtherChannel の手動グローバル MAC アドレスを設定します。[詳細設定 (Advanced)] をクリックし、[アクティブな MAC アドレス (Active MAC Address)] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャストビットセットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

[スタンバイ MAC アドレス (Standby MAC Address)] は設定しないでください。無視されます。

潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在の制御ユニットに留まります。MAC アドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

- f) [OK] をクリックします。他のデータ インターフェイスについても前述の手順を繰り返します。

ステップ 4 [Save (保存)] をクリックします。

これで、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

クラスタのヘルスマニターの設定

[クラスタ (Cluster)] ページの [クラスタヘルスマニターの設定 (Cluster Health Monitor Settings)] セクションには、次の表で説明されている設定が表示されます。

図 10: クラスタのヘルスマニターの設定

Cluster Health Monitor Settings			
Timeouts			
Hold Time	3 s		
Interface Debounce Time	9000 ms		
Monitored Interfaces			
Service Application	Enabled		
Unmonitored Interfaces	None		
Auto-Rejoin Settings			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

表 1: [クラスタヘルスマニターの設定 (Cluster Health Monitor Settings)]セクションテーブルのフィールド

フィールド	説明
タイムアウト	
保留時間 (Hold Time)	ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間 (Interface Debounce Time)	インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると思われ、クラスタからノードが削除されるまでの時間です。
Monitored Interfaces (モニタリング対象インターフェイス)	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、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、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。
サービスアプリケーション (Service Application)	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。

フィールド	説明
モニタリング対象外のインターフェイス (Unmonitored Interfaces)	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定	
クラスターインターフェイス (Cluster Interface)	クラスター制御リンクの自動再結合の設定の不具合を表示します。
データインターフェイス (Data Interfaces)	データインターフェイスの自動再結合の設定を表示します。
システム (System)	内部エラー時の自動再結合の設定を表示します。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。



(注) システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

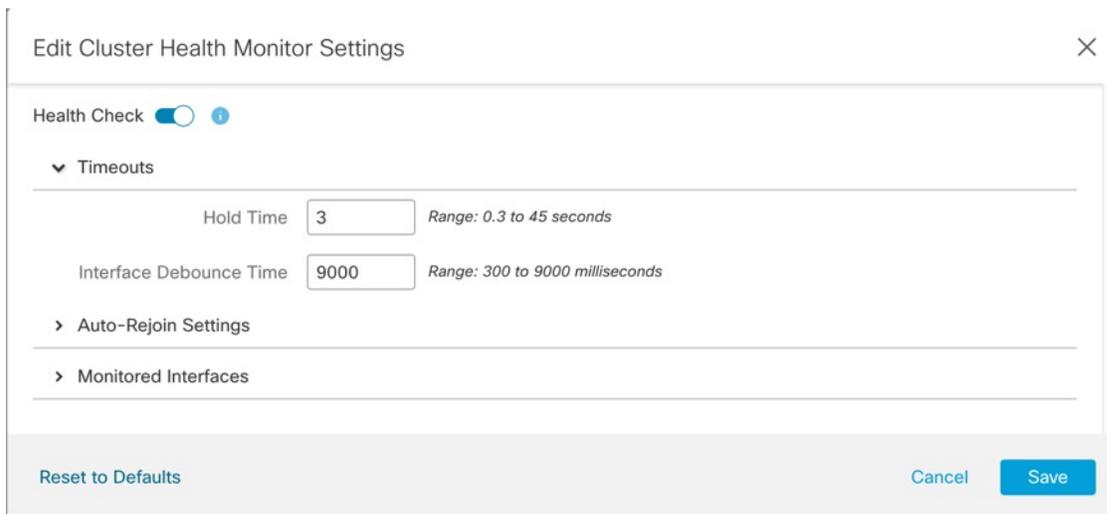
このセクションからこれらの設定を行うことができます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルスマニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスター制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

手順

- ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- ステップ 2 変更するクラスターの横にある [編集 (Edit)] (✎) をクリックします。
- ステップ 3 [クラスター (Cluster)] をクリックします。
- ステップ 4 [クラスタのヘルスマニターの設定 (Cluster Health Monitor Settings)] セクションで、[編集 (Edit)] (✎) をクリックします。
- ステップ 5 [ヘルスチェック (Health Check)] スライダをクリックして、システムのヘルスマニタリングを無効にします。

図 11: システムヘルスチェックの無効化



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、ノードやスイッチのインターフェイスの有効化/無効化、VSSやvPCを形成するスイッチの追加）を行うときには、システムの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。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間 (Hold Time)]: ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ~ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間 (Interface Debounce Time)]: デバウンス時間は 300 ~ 9000 ms の範囲で値を設定します。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、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 12: 自動再結合の設定

▼ Auto-Rejoin Settings

Cluster Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

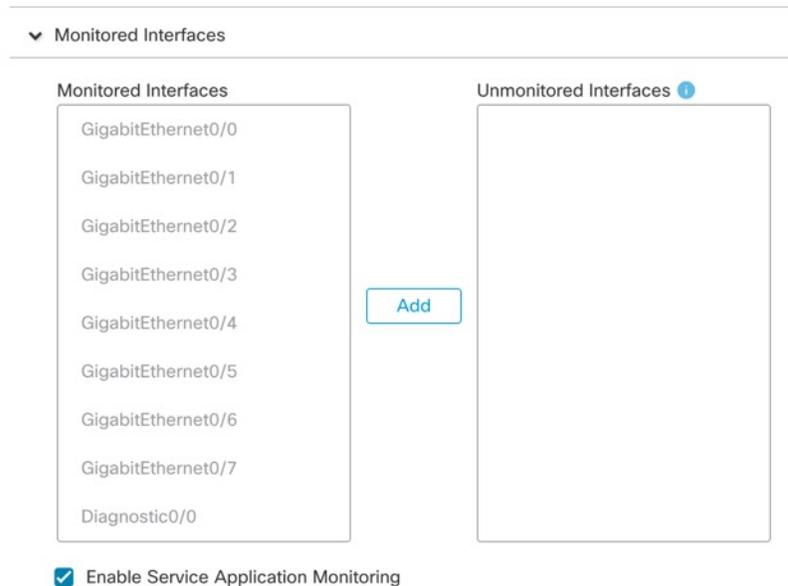
Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

[クラスタインターフェイス (Cluster Interface)]、[データインターフェイス (Data Interface)]、および[システム (System)]に次の値を設定します (内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります)。

- [試行数 (Attempts)]: 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。[クラスタインターフェイス (Cluster Interface)]のデフォルト値は -1 (無制限) です。[データインターフェイス (Data Interface)]と[システム (System)]のデフォルト値は 3 です。
- [試行の間隔 (Interval Between Attempts)]: 再結合試行の間隔を 2 ~ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分 (10 日) に制限されます。
- [間隔のバリエーション (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 (Cluster Interface)]の場合は 1、[データインターフェイス (Data Interface)]および[システム (System)]の場合は 2 です。

ステップ 8 [モニタリング対象のインターフェイス (Monitored Interfaces)]または[モニタリング対象外のインターフェイス (Unmonitored Interfaces)]ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリングを有効にする (Enable Service Application Monitoring)]をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 13: モニタリング対象インターフェイスの設定



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、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、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、および Snort プロセスと disk-full プロセスで有効になっています。

必須以外のインターフェイスのヘルス モニタリングを無効にできます。

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、ノードやスイッチのインターフェイスの有効化/無効化、VSSやvPCを形成するスイッチの追加）を行うときには、システムの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。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存 (Save)] をクリックします。

ステップ 10 設定変更を展開します [設定変更の展開](#) を参照してください。

クラスタノードの管理

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

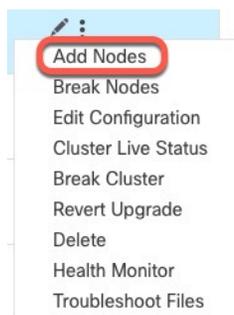
新しいクラスタノードの追加

1 つ以上の新しいクラスタノードを既存のクラスタに追加できます。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、クラスタの **その他 (⋮)** をクリックして [ノードを追加 (Add Nodes)] を選択します。 >

図 14: ノードの追加



[クラスタの管理 (Manage Cluster)] ウィザードが表示されます。

ステップ 2 [ノード (Node)] メニューからデバイスを選択し、必要に応じて IP アドレス、優先順位、およびサイト ID を調整します。

図 15: [クラスタの管理 (Manage Cluster)]ウィザード

Manage Cluster Wizard

1 Configuration — 2 Summary

Cluster Name*
ftdcluster

Cluster Key

Control Node
You can form the cluster with just the control node to reduce formation time.

Node*
172.16.0.50

Cluster Control Link Network*
10.10.10.0 / 24 (254 addresses)

Cluster Control Link*
Ethernet1/7

Cluster Control Link IPv4 Address*
10.10.10.1

Priority*
1

Site ID
0

Data Nodes (Optional)
Data node hardware needs to match the control node hardware.

Node*
172.16.0.51

Cluster Control Link IPv4 Address*
10.10.10.2

Priority*
2

Site ID
0

Node*
Type device name

Cluster Control Link IPv4 Address*
10.10.10.3

Priority*
3

Site ID
0

Remove

Add a data node

ステップ 3 さらにノードを追加するには、[データノードを追加 (Add a data node)]をクリックします。

ステップ 4 [続行 (Continue)]をクリックします。[概要 (Summary)]を確認し、[保存 (Save)]をクリックします。

現在登録されているノードには、ロードアイコンが表示されます。

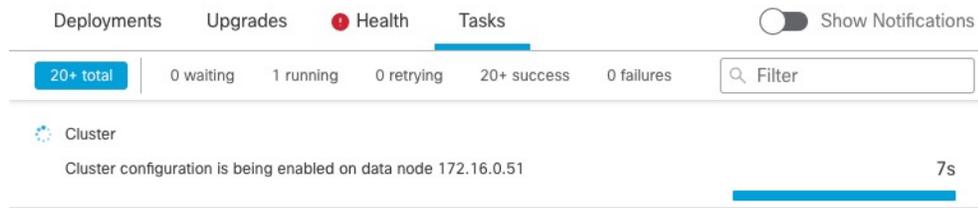
図 16: ノードの登録

ftdcluster (2)
Cluster

172.16.0.50 (Control) Snort 3
172.16.0.50 - Transparent

172.16.0.51 Snort 3
172.16.0.51 - Transparent

クラスタノードの登録をモニターするには、[通知 (Notifications)]アイコンをクリックし、[タスク (Tasks)]を選択します。



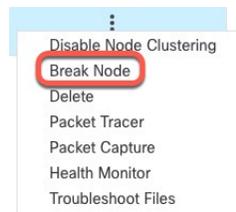
ノードの除外

ノードがスタンドアロンデバイスになるように、クラスからノードを削除できます。クラスタ全体を解除しない限り、制御ノードを除外することはできません。データノードの設定は消去されます。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、除外するノードの **その他** (⋮) をクリックして [ノードを除外 (Break Node)] を選択します。

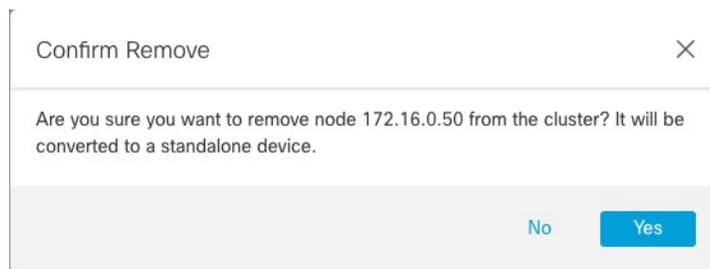
図 17: ノードの除外



オプションで、クラスタの [詳細 (More)] メニューから [ノードを除外 (Break Nodes)] を選択して 1 つ以上のノードを除外できます。

- ステップ 2** 除外の確定を求められたら、[はい (Yes)] をクリックします。

図 18: 解除の確定



クラスタノードの除外をモニターするには、[通知 (Notifications)] アイコンをクリックし、[タスク (Tasks)] を選択します。

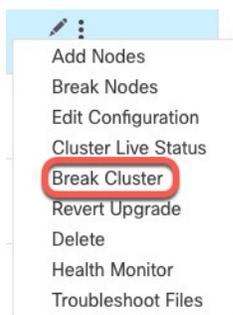
クラスタの解除

クラスタを解除し、すべてのノードをスタンドアロンデバイスに変換できます。制御ノードはインターフェイスとセキュリティポリシーの設定を保持しますが、データノードでは設定が消去されます。

手順

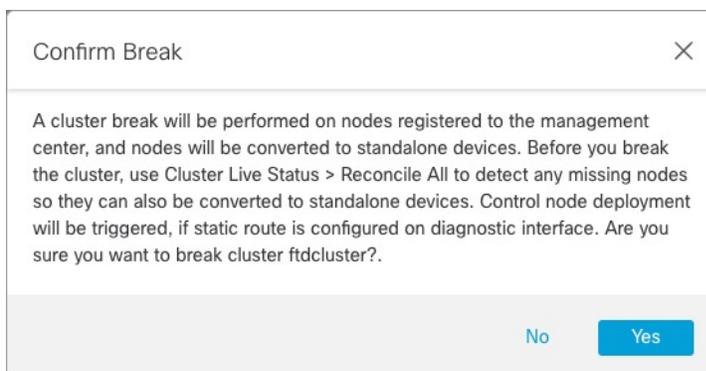
- ステップ 1** ノードを照合することにより、すべてのクラスタノードが Management Center で管理されていることを確認します。[クラスタノードの照合 \(40 ページ\)](#) を参照してください。
- ステップ 2** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、クラスタの **その他 (⋮)** をクリックして [クラスタを解除 (Break Cluster)] を選択します。

図 19: クラスタの解除



- ステップ 3** クラスタを解除するよう求められたら、[はい (Yes)] をクリックします。

図 20: 解除の確定



クラスタの解除をモニターするには、[通知 (Notifications)] アイコンをクリックし、[タスク (Tasks)] を選択します。

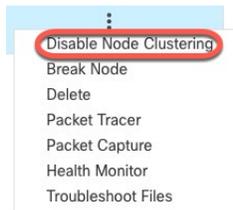
クラスタリングを無効にする

ノードの削除に備えて、またはメンテナンスのために一時的にノードを非アクティブ化する場合があります。この手順は、ノードを一時的に非アクティブ化するためのものです。ノードは引き続き Management Center のデバイスリストに表示されます。ノード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。

手順

- ステップ 1** 無効にするユニットに対して、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択して **その他 (⋮)** をクリックし、[ノードのクラスタリングを無効にする (Disable Node Clustering)] を選択します。

図 21: クラスタリングを無効にする



制御ノードでクラスタリングを無効にすると、データノードの1つが新しい制御ノードになります。なお、中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるため、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。制御ノードがクラスタ内の唯一のノードである場合、そのノードでクラスタリングを無効にすることはできません。

- ステップ 2** ノードのクラスタリングを無効にすることを確認します。

ノードは、[デバイス (Devices)] > [デバイス管理 (Device Management)] リストの名前の横に [(無効 (Disabled))] と表示されます。

- ステップ 3** クラスタリングを再び有効にするには、[クラスタへの再参加 \(36 ページ\)](#) を参照してください。

クラスタへの再参加

(たとえば、インターフェイスで障害が発生したために) ノードがクラスタから削除された場合、または手動でクラスタリングを無効にした場合は、クラスタに手動で再参加する必要があります。

ります。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。ノードをクラスタから削除できる理由の詳細については、「[クラスタへの再参加（62 ページ）](#)」を参照してください。

手順

-
- ステップ 1** 再度有効にするユニットに対して、[デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択して **その他 (⚙)** をクリックし、[ノードのクラスタリングを有効にする (Enable Node Clustering)] を選択します。
- ステップ 2** ユニットでクラスタリングを有効にすることを確認します。
-

制御ノードの変更



注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするユニットを厳密に指定する必要がある場合は、このセクションの手順を使用します。なお、中央集中型機能については、いずれかの方法で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ため、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

手順

-
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] > **その他 (⚙)** > [クラスタのライブステータス (Cluster Live Status)] を選択して [クラスタステータス (Cluster Status)] ダイアログボックスを開きます。

図 22: クラスタのステータス

Cluster Status

Overall Status: Cluster has all nodes in sync

Nodes details (2) Refresh Reconcile All

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 Control	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮

Dated: 11:52:26 | 20 Dec 2021 Close

ステップ 2 制御ユニットにしたいユニットについて、**その他** (⋮) > [ロールを制御に変更 (Change Role to Control)] を選択します。

ステップ 3 ロールの変更を確認するように求められます。チェックボックスをオンにして [OK] をクリックします。

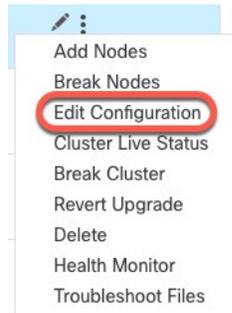
クラスタ設定の編集

クラスタ設定を編集できます。クラスタキー、クラスタ制御リンクインターフェイス、またはクラスタ制御リンクネットワークを変更すると、クラスタは自動的に解除されて再形成されます。クラスタが再形成されるまで、トラフィックの中断が発生する可能性があります。ノードのクラスタ制御リンクの IP アドレス、ノードの優先順位、またはサイト ID を変更すると、影響を受けるノードのみが除外されてクラスタに再追加されます。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、クラスタの **その他** (⋮) をクリックして [設定を編集 (Edit Configuration)] を選択します。

図 23: 設定の編集



[クラスタの管理 (Manage Cluster)] ウィザードが表示されます。

ステップ 2 クラスタ設定を更新します。

図 24: [クラスタの管理 (Manage Cluster)] ウィザード

The screenshot shows the 'Manage Cluster Wizard' interface. It has two tabs: 'Configuration' (active) and 'Summary'. A warning message at the top states: 'Editing the cluster bootstrap configuration results in disabling clustering temporarily. This operation may result in traffic disruption, and you should perform bootstrap changes during the maintenance window.'

The configuration fields are as follows:

- Cluster Name*:** ftd_cluster
- Cluster Key:** Two masked input fields (indicated by red boxes).
- Control Node:**
 - Node*:** 172.16.0.51
 - Cluster Control Link Network*:** 10.10.10.0 / 24 (254 addresses) (indicated by a red box).
 - Cluster Control Link*:** Ethernet1/7 (indicated by a red box).
- Data Nodes (Optional):**
 - Node*:** 172.16.0.50
 - Cluster Control Link IPv4 Address*:** 10.10.10.2, Priority*: 2, Site ID: 0 (indicated by a green box).
 - Cluster Control Link IPv4 Address*:** 10.10.10.1, Priority*: 1, Site ID: 0 (indicated by a green box).

Labels 'Cluster-level changes' and 'Node-level changes' are present in red and green text respectively.

クラスタ制御リンクが EtherChannel の場合、インターフェイスのドロップダウンメニューの横にある **[編集 (Edit)]** (✎) をクリックして、インターフェイスのメンバーシップと LACP の設定を編集できます。

ステップ 3 [続行 (Continue)] をクリックします。[概要 (Summary)] を確認し、[保存 (Save)] をクリックします。

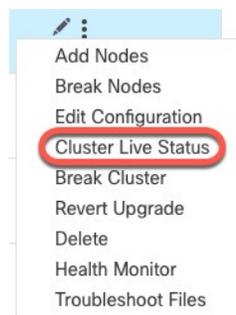
クラスタノードの照合

クラスタノードの登録に失敗した場合は、デバイスから Management Center に対してクラスタメンバーシップを照合できます。たとえば、Management Center が特定のプロセスで占領されているか、ネットワークに問題がある場合、データノードの登録に失敗することがあります。

手順

ステップ 1 クラスタの [Devices] > [Device Management] > その他 (⋮) を選択し、次に [Cluster Live Status] を選択して [Cluster Status] ダイアログボックスを開きます。

図 25: クラスタのライブステータス



ステップ 2 [すべてを照合 (Reconcile All)] をクリックします。

図 26: すべてを照合

A screenshot of the 'Cluster Status' dialog box. At the top, it says 'Cluster Status' with a help icon. Below that, the overall status is 'Cluster has all nodes in sync'. Under 'Nodes details (2)', there are 'Refresh' and 'Reconcile All' buttons, with 'Reconcile All' highlighted by a red circle. A search bar contains the text 'Enter node name'. Below the buttons is a table with columns: Status, Device Name, Unit Name, and Chassis URL. The table contains two rows, both with 'In Sync.' status. The first row has a 'Control' button next to the device name. At the bottom, there is a footer with the date 'Dated: 11:52:26 | 20 Dec 2021' and a 'Close' button.

Status	Device Name	Unit Name	Chassis URL
> In Sync.	172.16.0.50 Control	172.16.0.50	N/A
> In Sync.	172.16.0.51	172.16.0.51	N/A

クラスタ ステータスの詳細については、[クラスタのモニタリング（42 ページ）](#) を参照してください。

クラスタまたはノードの削除（登録解除）と新しい Management Center への登録

Management Center からクラスタを登録解除できます。これにより、クラスタはそのまま維持されます。クラスタを新しい Management Center に追加する場合は、クラスタを登録解除することができます。

クラスタからノードを除外することなく、Management Center からノードを登録解除することもできます。ノードは Management Center に表示されていませんが、まだクラスタの一部であり、引き続きトラフィックを渡して制御ノードになることも可能です。現在動作している制御ノードを登録解除することはできません。Management Center から到達不可能になったノードは登録解除してもかまいませんが、管理接続をトラブルシューティングする間、クラスタの一部として残しておくことも可能です。

クラスタの登録解除：

- Management Center とクラスタとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからクラスタが削除されます。
- クラスタのプラットフォーム設定ポリシーで、NTP を使用して Management Center から時間を受信するように設定されている場合は、クラスタがローカル時間管理に戻されます。
- 設定はそのままになるため、クラスタはトラフィックの処理を続行します。

NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Management Center にクラスタを再登録すると、設定が削除されるため、クラスタはその時点でトラフィックの処理を停止します。クラスタ設定はそのまま維持されるため、クラスタ全体を追加できます。登録時にアクセス コントロール ポリシーを選択できますが、トラフィックを再度処理する前に、登録後に他のポリシーを再適用してから設定を展開する必要があります。

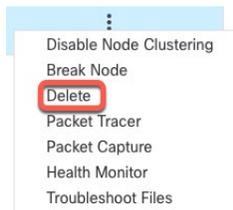
始める前に

この手順では、いずれかのノードへの CLI アクセスが必要です。

手順

ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）]の順に選択し、クラスタかノードの **その他** (ⓘ) をクリックして [登録解除] [削除（Delete）] を選択します。

図 27: クラスタまたはノードの削除



ステップ 2 クラスタかノードを削除するよう求められたら、[はい (Yes)] をクリックします。

ステップ 3 クラスタメンバーの1つを新しいデバイスとして追加することにより、クラスタを新しい（または同じ）Management Center に登録できます。

クラスタノードの1つをデバイスとして追加するだけで、残りのクラスタノードが検出されません。

- a) 1つのクラスタノードのCLIに接続し、**configure manager add** コマンドを使用して新しいManagement Center を識別します。 [Threat Defense 管理インターフェイスのCLIでの変更を参照してください。](#)
- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、[追加 (Add)] > [デバイス (Device)] をクリックします。

ステップ 4 未登録のノードを再度追加するには、[クラスタノードの照合 \(40 ページ\)](#) を参照してください。

クラスタのモニタリング

クラスタは、Management Center と Threat Defense の CLI でモニターできます。

- [クラスタステータス (Cluster Status)] ダイアログボックスには、[デバイス (Devices)] > [デバイス管理 (Device Management)] > **その他** (⚙️) アイコンから、または [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] ページ > [全般 (General)] 領域 > [クラスタのライブステータス (Cluster Live Status)] リンクからアクセスできます。 > > >

図 28: クラスタのステータス

Cluster Status ?

Overall Status: Cluster has all nodes in sync

Nodes details (2) Refresh Reconcile All

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 Control	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮

Dated: 11:52:26 | 20 Dec 2021 Close

制御ノードには、そのロールを示すグラフィックインジケータがあります。

クラスタメンバーステータスには、次の状態が含まれます。

- 同期中 (In Sync) : ノードは Management Center に登録されています。
- 登録の保留中 (Pending Registration) : ノードはクラスタの一部ですが、まだ Management Center に登録されていません。ノードの登録に失敗した場合は、[すべてを照合 (Reconcile All)] をクリックして登録を再試行できます。
- クラスタリングが無効 (Clustering is disabled) : ノードは Management Center に登録されていますが、クラスタの非アクティブなメンバーです。クラスタリング設定は、後で再有効化する予定がある場合は変更せずに維持できます。また、ノードをクラスタから削除することも可能です。
- クラスタに参加中... (Joining cluster...) : ノードがシャーシ上でクラスタに参加していますが、参加は完了していません。参加後に Management Center に登録されます。

ノードごとに [概要 (Summary)] と [履歴 (History)] を表示できます。

図 29: ノードの [概要 (Summary)]

Status	Device Name	Unit Name	Chassis URL
In Sync.	172.16.0.50 Control	172.16.0.50	N/A

Summary		History	
ID:	0	CCL IP:	10.10.10.1
Site ID:	N/A	CCL MAC:	6c13.d509.4d9a
Serial No:	FJZ2512139M	Module:	N/A
Last join:	05:41:26 UTC Dec 17 2021	Resource:	N/A
Last leave:	N/A		

図 30: ノードの [履歴 (History)]

Status	Device Name	Unit Name	Chassis URL
In Sync.	172.16.0.50 Control	172.16.0.50	N/A

Summary		History	
Timestamp	From State	To State	Event
05:56:31 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment hold for app 1 is relea...
05:56:31 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment hold for app 1 is relea...
05:56:29 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment is on hold for app 1 fo...
05:56:29 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment is on hold for app 1 fo...

- システム (⚙️) > [Tasks] ページ。

[タスク (Tasks)]ページには、ノードが登録されるたびにクラスタ登録タスクの最新情報が表示されます。

- [デバイス (Devices)]> [デバイス管理 (Device Management)]> cluster_name。 >

デバイスの一覧表示ページでクラスタを展開すると、IPアドレスの横にそのロールが表示されている制御ノードを含む、すべてのメンバーノードを表示できます。登録中のノードには、ロード中のアイコンが表示されます。

- **show cluster {access-list [acl_name] | conn [count] | cpu [usage] | history | interface-mode | memory | resource usage | service-policy | traffic | xlate count}**

クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info [auto-join | clients | conn-distribution | flow-mobility counters | goid [options] | health | incompatible-config | loadbalance | old-members | packet-distribution | trace [options] | transport { asp | cp}]**

クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタヘルスマニターダッシュボード

Cluster Health Monitor

Threat Defense がクラスタの制御ノードである場合、Management Center はデバイスメトリックデータコレクタからさまざまなメトリックを定期的に収集します。クラスタのヘルスマニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
 - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタで Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
 - クラスタの統計セクションには、CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。



(注) CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

- メトリックチャート、つまり、CPU 使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。
- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。
 - 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
 - ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。
- メンバーパフォーマンスダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できます。メトリックデータには、CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数が含まれます。

- CCL ダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタ ヘルスの表示

この手順を実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリストユーザーである必要があります。

クラスタヘルスマニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスマニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Management Center の 1 つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ 1 システム (⚙️) > [正常性 (Health)] > [モニタ (Monitor)] を選択します。

[モニタリング (Monitoring)] ナビゲーションウィンドウを使用して、ノード固有のヘルスマニターにアクセスします。

ステップ 2 デバイスリストで [展開 (Expand)] (➤) と [折りたたみ (Collapse)] (▼) をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ 3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要 (Overview)]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT 変換情報などが含まれます。
- [負荷分散 (Load Distribution)]：クラスタノード間のトラフィックとパケットの分散。
- [メンバーパフォーマンス (Member Performance)]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。

- [CCL] : インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「[Cisco Secure Firewall Threat Defense Health Metrics](#)」を参照してください。

- ステップ 4** 右上隅のドロップダウンで、時間範囲を設定できます。最短で1時間前（デフォルト）から、最長では2週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を5分に設定するか、自動更新をオフに切り替えます。

- ステップ 5** 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上にあるアイコンをクリックします。

- ステップ 6** （ノード固有のヘルスマニターの場合） ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

- ステップ 7** （ノード固有のヘルスマニターの場合） デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- **Overview** : CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- **CPU** : CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- **Memory** : デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- **Interfaces** : インターフェイスのステータスおよび集約トラフィック統計情報。
- **Connections** : 接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- **[Snort]** : Snort プロセスに関連する統計情報。
- **[ASP ドロップ (ASP drops)]** : さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「[Cisco Secure Firewall Threat Defense Health Metrics](#)」を参照してください。

ステップ 8 ヘルスモニターの右上隅にあるプラス記号 ([+]) をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

クラスタメトリック

クラスタのヘルスモニターは、クラスタとそのノードに関連する統計情報と、負荷分散、パフォーマンス、および CCL トラフィックの統計データの集約結果を追跡します。

表 2: クラスタメトリック

メトリック	説明	書式
CPU	クラスタノード上の CPU メトリックの平均 (データプレーンと snort についてそれぞれ表示)。	percentage
メモリ	クラスタノード上のメモリメトリックの平均 (データプレーンと snort についてそれぞれ表示)。	percentage
データスループット	クラスタの着信および発信データトラフィックの統計。	bytes
CCL スループット	クラスタの着信および発信 CCL トラフィックの統計。	bytes
接続 (Connections)	クラスタ内のアクティブな接続数。	number
NAT Translations	クラスタの NAT 変換数。	number
Distribution	1 秒ごとのクラスタ内の接続分布数。	number
パケット	クラスタ内の 1 秒ごとのパケット配信の件数。	number

クラスタのトラブルシューティング

CCL Ping ツールを使用すると、クラスタ制御リンクが正しく動作していることを確認できます。デバイスとクラスタで使用可能な次のツールを使用することもできます。

- **トラブルシューティングファイル**: ノードがクラスタに参加できない場合、トラブルシューティングファイルが自動的に生成されます。また、**[デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] > [一般 (General)]** エリアからトラ

ブルシューティングファイルを生成してダウンロードすることもできます。 [トラブルシューティング ファイルの生成](#)を参照してください。

その他 (🔍) をクリックし、[トラブルシューティングファイル (Troubleshoot Files)] を選択して、[デバイス管理 (Device Management)] ページからファイルを生成することもできます。

- CLI 出力 : [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] > [一般 (General)] エリアで、クラスタのトラブルシューティングに役立つ一連の定義済み CLI 出力を表示できます。クラスタに対して次のコマンドが自動的に実行されます。

- `show running-config cluster`
- `show cluster info`
- `show cluster info health`
- `show cluster info transport cp`
- `show version`
- `show asp drop`
- `show counters`
- `show arp`
- `show int ip brief`
- `show blocks`
- `show cpu detailed`
- `show interface ccl_interface`
- `ping ccl_ip size ccl_mtu repeat 2`

[コマンド (Command)] フィールドに任意の `show` コマンドを入力することもできます。詳細については、[CLI 出力の表示](#)を参照してください。

クラスタ制御リンクへの ping の実行

ping を実行して、すべてのクラスタノードがクラスタ制御リンクを介して相互に到達できることを確認できます。ノードがクラスタに参加できない主な原因の1つは、クラスタ制御リンクの設定が正しくないことです。たとえば、クラスタ制御リンクの MTU が、接続しているスイッチの MTU よりも大きい値に設定されている可能性があります。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、クラスタの横の **その他** (☰) をクリックして [クラスタのライブステータス (Cluster Live Status)] を選択します。

図 31: クラスタのステータス

Cluster Status

Overall Status: Cluster has all nodes in sync

Nodes details (2) Refresh Reconcile All

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 Control	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮

Dated: 11:52:26 | 20 Dec 2021 Close

ステップ 2 ノードの 1 つを展開し、[CCL Ping] をクリックします。

図 32 : CCL Ping

Cluster Status ?

Overall Status:  Clustering is disabled for 1 node(s)

Nodes details (3) Refresh Reconcile All

Status	Device Name	Unit Name	Chassis URL
In Sync.	10.10.43.21 Control	10.10.43.21	N/A
<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc;"> Summary History CCL Ping </div> <pre> ping 10.10.3.2 size 1654 Sending 5, 1654-byte ICMP Echos to 10.10.3.2, timeout is 2 seconds: ????? Success rate is 0 percent (0/5) ----- --ping 10.10.3.1 size 1654 </pre>			
> Clustering is disabled	10.10.43.22	10.10.43.22	N/A

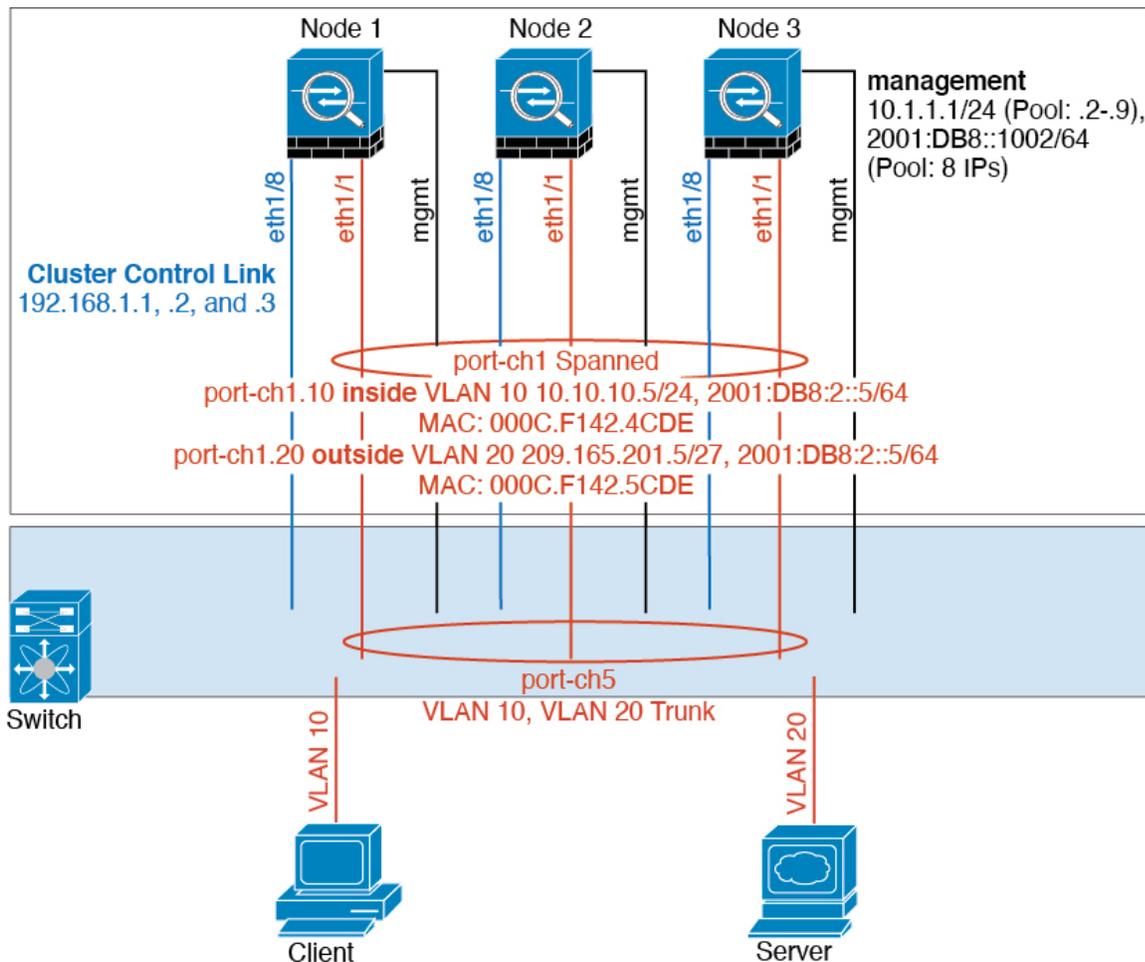
Dated: 18:38:41 | 01 Mar 2023 Close

ノードは、最大 MTU に一致するパケットサイズを使用して、クラスタ制御リンクで他のすべてのノードに ping を送信します。

クラスタリングの例

これらの例には、一般的な展開の例が含まれます。

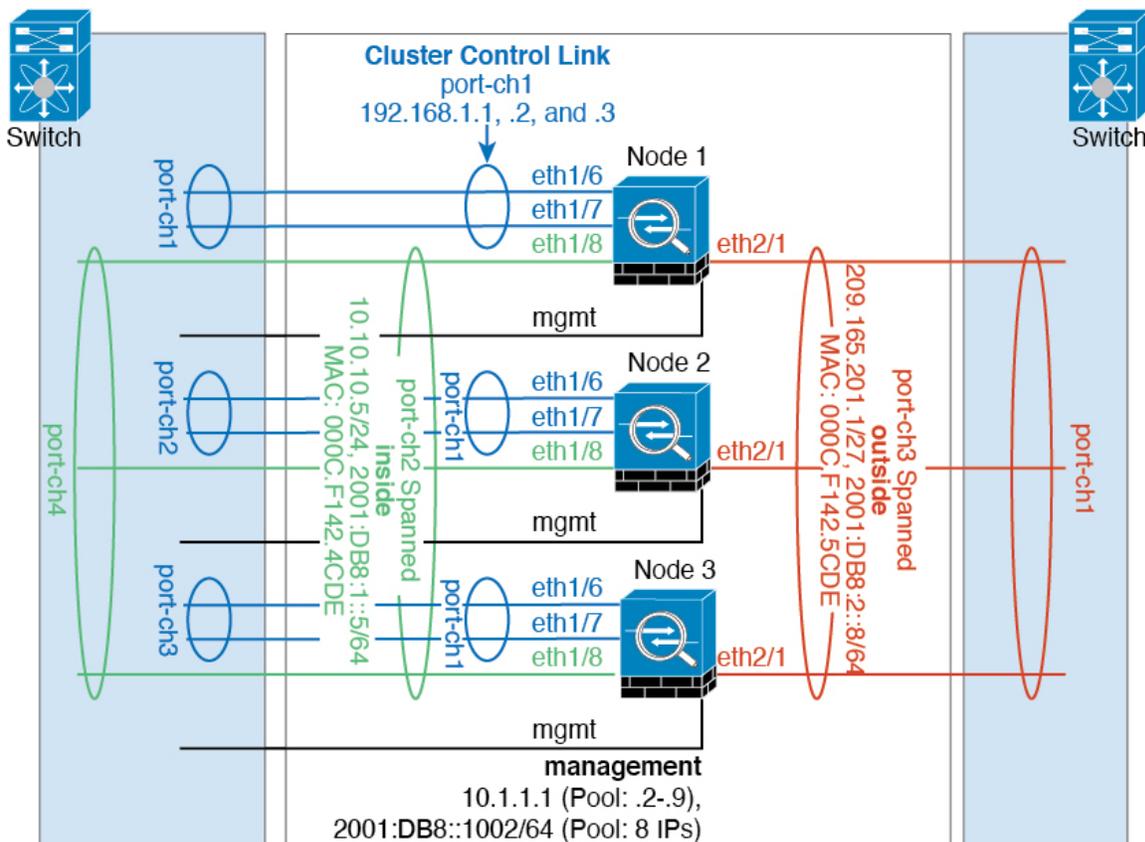
スティック上のファイアウォール



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。は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スバンド 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。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。

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。

Threat Defense の機能とクラスタリング

Threat Defense の一部の機能はクラスタリングではサポートされず、一部は制御ユニットだけでサポートされます。その他の機能については適切な使用に関する警告があります。

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。



(注) クラスタリングでもサポートされていない FlexConfig 機能 (WCCP インспекションなど) を表示するには、[ASA の一般的な操作のコンフィギュレーションガイド](#)を参照してください。FlexConfig では、Management Center GUI にはない多くの ASA 機能を設定できます。[FlexConfig ポリシー](#)を参照してください。

- リモート アクセス VPN (SSL VPN および IPsec VPN)
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされていません。
- 仮想トンネルインターフェイス (VTI)
- 高可用性
- 統合ルーティングおよびブリッジング
- Management Center UCAPL/CC 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。



(注) クラスタリングでも一元化されている FlexConfig 機能 (RADIUS インспекションなど) を表示するには、[ASA の一般的な操作のコンフィギュレーションガイド](#)を参照してください。FlexConfig では、Management Center GUI にはない多くの ASA 機能を設定できます。[FlexConfig ポリシー](#)を参照してください。

- 次のアプリケーション インспекション :
 - DCERPC

- ESMTTP
 - NetBIOS
 - PPTP
 - RSH
 - SQLNET
 - SUNRPC
 - TFTP
 - XDMCP
- スタティック ルート モニタリング
 - サイト間 VPN
 - IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
 - PIM マルチキャスト コントロールプレーンプロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
 - ダイナミックルーティング

接続設定とクラスタリング

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

FTP とクラスタリング

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

個別インターフェイス モードでのマルチキャスト ルーティング

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

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の Threat Defense に送信されることがあります。ロードバランシングアルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合は、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない Threat Defense に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

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

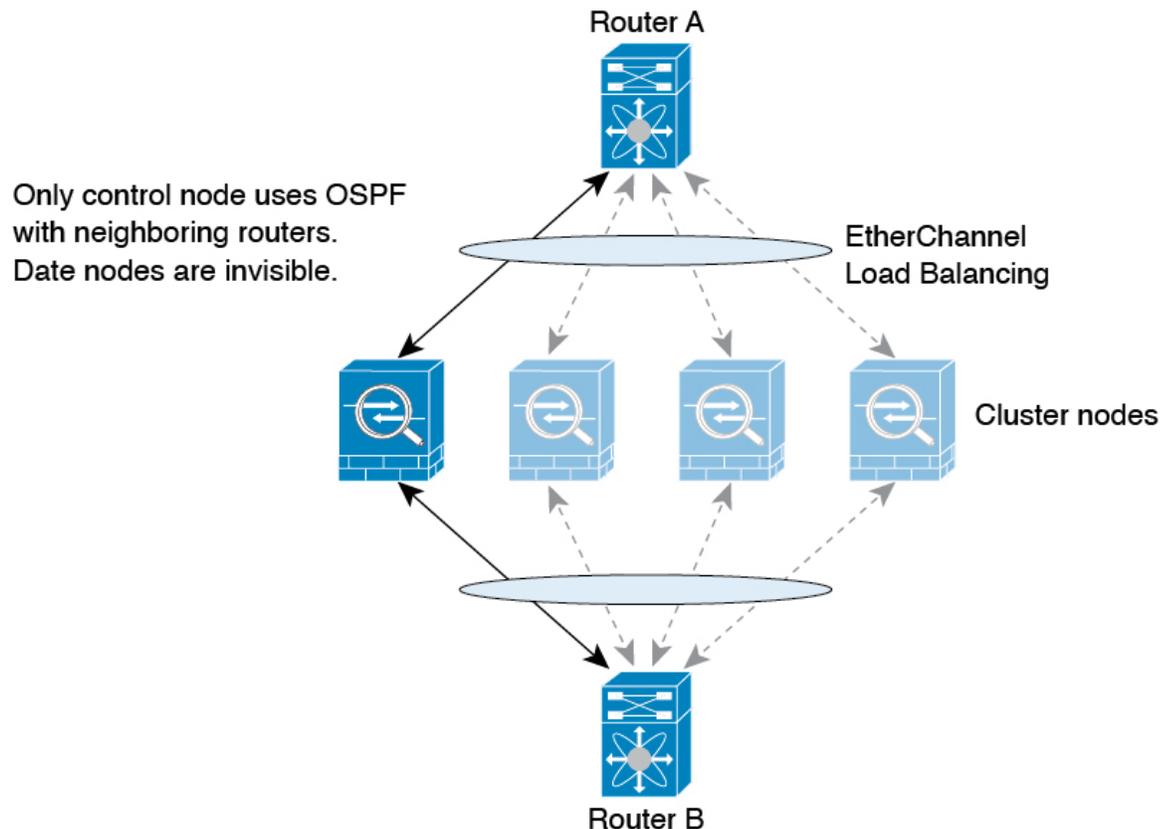
- ポートブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
 - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
 - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
 - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
 - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。
- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ~ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ~ 65535 のポート範囲をカバーします。

- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、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。
- 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
 - 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。

でのダイナミック ルーティング

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

図 33: スパンド EtherChannel モードでのダイナミック ルーティング



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

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

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。

SNMP とクラスタリング

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。ユーザーを削除して再追加し、設定を再展開して、ユーザーを新しいノードに強制的に複製する必要があります。

syslog とクラスタリング

- 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。

Cisco TrustSec とクラスタリング

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

VPN とクラスタリング

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



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

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

VPN トンネルをスパンド EtherChannel アドレスに接続すると、接続が自動的に制御ノードに転送されます。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

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

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

制御ノードの選定

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

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



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

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



(注) ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

クラスタ内のハイアベイラビリティ

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

ノードヘルスマニタリング

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

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

詳細については、[制御ノードの選定 \(60 ページ\)](#) を参照してください。

インターフェイス モニタリング

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

- スパンド EtherChannel : クラスタ Link Aggregation Control Protocol (cLACP) を使用します。各ノードは、リンクステータスおよび cLACP プロトコルメッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスが制御ノードに報告されます。

ヘルスマニタリングを有効にすると、(主要な EtherChannel を含む) すべての物理インターフェイスがデフォルトでモニタされます。オプションでインターフェイスごとにモニタリングを無効にできます。指名されたインターフェイスのみモニターできます。たとえば、指名された EtherChannel に障害が発生している状態と判断されてはなりません。つまり、EtherChannel のすべてのメンバーポートはクラスタ削除のトリガーに失敗する必要があります。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。Threat Defense がメンバーをクラスタから削除するまでの時間は、そのノードが確立済みメンバーであるか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。確立済みメンバーのインターフェイスがダウン状態の場合、Threat Defense はそのメンバーを 9 秒後に削除します。Threat Defense 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、Threat Defense はクラスタから削除されません。EtherChannel 以外の場合は、メンバー状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

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

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高 (番号が最小) のメンバーが制御ノードになります。

障害イベントに応じて、Threat Defense は自動的にクラスタへの再参加を試みます。



- (注) Threat Defense 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。

クラスタへの再参加

クラスタメンバー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。

- 最初に参加するときに障害が発生したクラスタ制御リンク：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、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：Threat Defense は、無限に 5 分ごとに自動的に再参加を試みます。
- データ インターフェイスの障害：Threat Defense 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、Threat Defense アプリケーションはクラスタリングを無効にします。データインターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ノードは再起動するとクラスタに再参加します。Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。
- 障害が発生した設定の展開：Management Center から新しい設定を展開し、展開が一部のクラスタメンバーでは失敗したものの、他のメンバーでは成功した場合、失敗したノードはクラスタから削除されます。クラスタリングを再度有効にして手動でクラスタに再参加する必要があります。制御ノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。すべてのデータノードで展開が失敗した場合、展開はロールバックされ、メンバーは削除されません。

データ パス接続状態の複製

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

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

表 3: クラスタ全体で複製される機能

トラフィック	状態のサポート	注
アップタイム	対応	システムアップタイムをトラッキングします。
ARP テーブル	対応	—
MAC アドレス テーブル	対応	—
ユーザ アイデンティティ	対応	—
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	—

クラスタが接続を管理する方法

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

接続のロール

接続ごとに定義された次のロールを参照してください。

- **オーナー**：通常、最初に接続を受信するノード。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- **バックアップオーナー**：オーナーから受信した TCP/UDP ステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせ、関連するステート情報を取得し、そのノードが新しいオーナーになります。

ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーが自分をディレクタとして選択した場合は、別のバックアップオーナーが選択されます。

1 台のシャーシに最大 3 つのクラスタ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。

- **ディレクタ**：フォワーダからのオーナーバックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、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。

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してから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN キーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないため、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえば DNS や ICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。



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

- **フラグメントオーナー**：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、

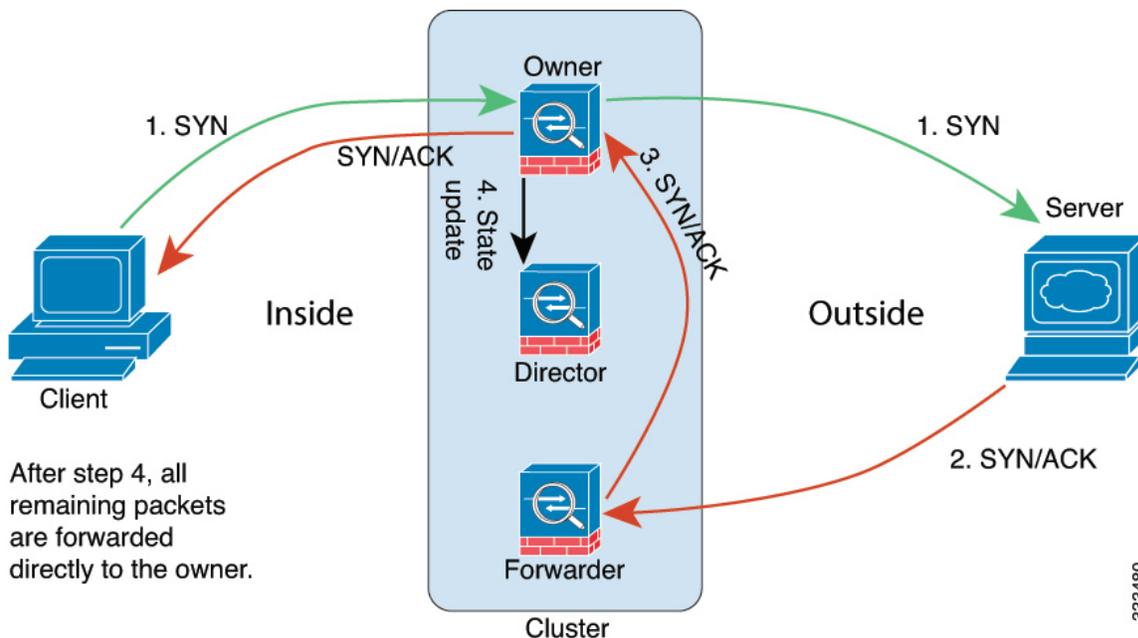
フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを決定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。これが既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続の所有者はすべてのフラグメントを再構築します。

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。



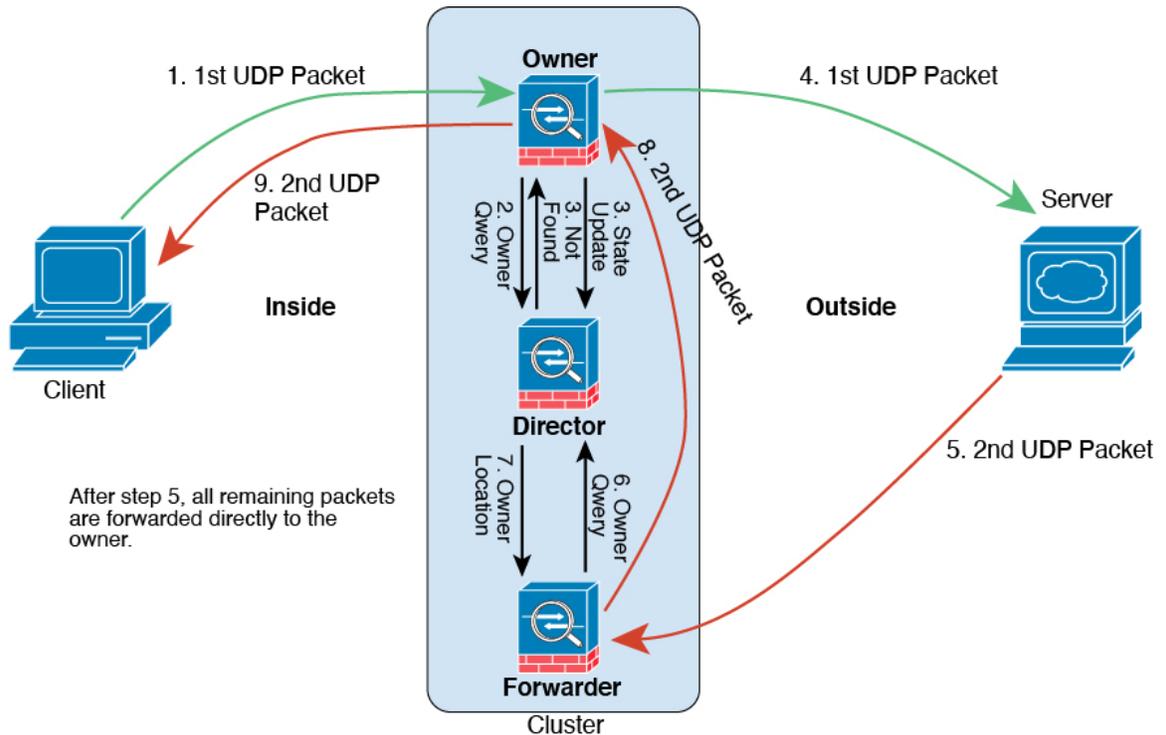
1. SYN パケットがクライアントから発信され、Threat Defense の 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Threat Defense（ロードバランシング方法に基づく）に配信されます。この Threat Defense はフォワーダです。

3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP 状態情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせ、オーナーを特定し、フローを確立します。
8. フローの状態が変化した場合、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

1. 図 34: 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 Threat Defense（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 packets 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 packets 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 packets を転送します。
5. 2 番目の UDP packets 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 packets を即座にディレクタに送信し、ディレクタがその packets 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、packets をオーナーに転送します。
9. オーナーは packets をクライアントに転送します。

クラスタリングの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
クラスタ制御リンク ping ツール。	7.4.1	任意 (Any)	<p>ping を実行して、すべてのクラスタノードがクラスタ制御リンクを介して相互に到達できることを確認できます。ノードがクラスタに参加できない主な原因の 1 つは、クラスタ制御リンクの設定が正しくないことです。たとえば、クラスタ制御リンクの MTU が、接続しているスイッチの MTU よりも大きい値に設定されている可能性があります。</p> <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>その他 (⚙️)>[クラスタのライブステータス (Cluster Live Status)]</p> <p>その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
トラブルシューティングファイルの生成とダウンロードは、[デバイス (Device)]および [クラスタ (Cluster)] ページから実行できます。	7.4.1	7.4.1	<p>[デバイス (Device)] ページの各デバイス、および [クラスタ (Cluster)] ページのすべてのクラスタノードのトラブルシューティングファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。または、[デバイス (Devices)] > [デバイス管理 (Device Management)] > その他 (☺) > [トラブルシューティングファイル (Troubleshoot Files)] メニューからファイル生成をトリガーできます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [全般 (General)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] > [全般 (General)]
クラスタへの参加に失敗した場合のノードでのトラブルシューティングファイルの自動生成。	7.4.1	7.4.1	<p>ノードがクラスタに参加できない場合、そのノードのトラブルシューティングファイルが自動的に生成されます。[タスク (Tasks)] または [クラスタ (Cluster)] ページからファイルをダウンロードできます。</p>
デバイスまたはデバイスクラスタの CLI 出力を表示します。	7.4.1	任意 (Any)	<p>デバイスまたはクラスタのトラブルシューティングに役立つ一連の定義済み CLI 出力を表示できます。また、任意の show コマンドを入力して、出力を確認できます。</p> <p>新規/変更された画面：[デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] > [全般 (General)]</p>
Cisco Secure Firewall 4200 のクラスタリング	7.4.0	7.4.0	<p>Cisco Secure Firewall 4200 は、最大 8 ノードのスパンド EtherChannel クラスタリングをサポートします。</p>
クラスタのヘルスマニターの設定	7.3.0	いずれか	<p>クラスタのヘルスマニター設定を編集できるようになりました。</p> <p>新規/変更された画面：[デバイス (Devices)] > [デバイス管理 (Device Management)] > クラスタ (Cluster) > [クラスタのヘルスマニターの設定 (Cluster Health Monitor Settings)]</p> <p>(注) 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
クラスタヘルスマニターダッシュボード	7.3.0	いずれか	<p>クラスタのヘルスマニターダッシュボードでクラスタの状態を表示できるようになりました。</p> <p>新規/変更された画面：システム (⚙️) > [正常性 (Health)] > [モニター (Monitor)]</p>
クラスタ制御リンク MTU の自動構成	7.2.0	7.2.0	<p>クラスタ制御リンクインターフェイスの MTU が、最も高いデータインターフェイス MTU よりも 100 バイト多い値に自動的に設定されるようになりました。デフォルトでは、MTU は 1,600 バイトです。</p>
Cisco Secure Firewall 3100 のクラスタリング	7.1.0	7.1.0	<p>Cisco Secure Firewall 3100 は、最大 8 ノードのスパンド EtherChannel クラスタリングをサポートします。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタの追加 (Add Cluster)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [詳細 (More)] メニュー • [Devices] > [Device Management] > [Cluster] <p>サポートされるプラットフォーム：Cisco Secure Firewall 3100</p>

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。