プライベートクラウドにおける Threat Defense Virtual クラスタの展開

最終更新：2022 年 5 月 31 日

プライベートクラウドでの Threat Defense Virtual 向けクラスタの展開

クラスタリングを利用すると、複数の Threat Defense Virtual をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。VMware と KVM を使用して、プライベートクラウドに Threat Defense Virtual クラスタを導入できます。ルーテッド ファイアウォール モードのみがサポートされます。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。サポートされていない機能とクラスタリング （29 ページ） を参照してください。

プライベートクラウドでの Threat Defense Virtual 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 つのデバイスとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離されたネットワーク。VXLAN インターフェイスを使用したクラスタ制御リンクと呼ばれます。レイヤ 3 物理ネットワーク上でレイヤ 2 仮想ネットワークとして機能する VXLAN により、threat defense virtual はクラスタ制御リンクを介してブロードキャスト/マルチキャストメッセージを送信できます。
- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。threat defense virtual 導入には、クラスタノードの管理に使用するManagement 0/0 インターフェイスが含まれています。

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

- ポリシーベースルーティング：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してノード間のロードバランシングを実行します。
- 等コスト マルチパス ルーティング：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミック ルートを使用してノード間のロードバランシングを実行します。

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

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。複数のクラスタメンバー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。

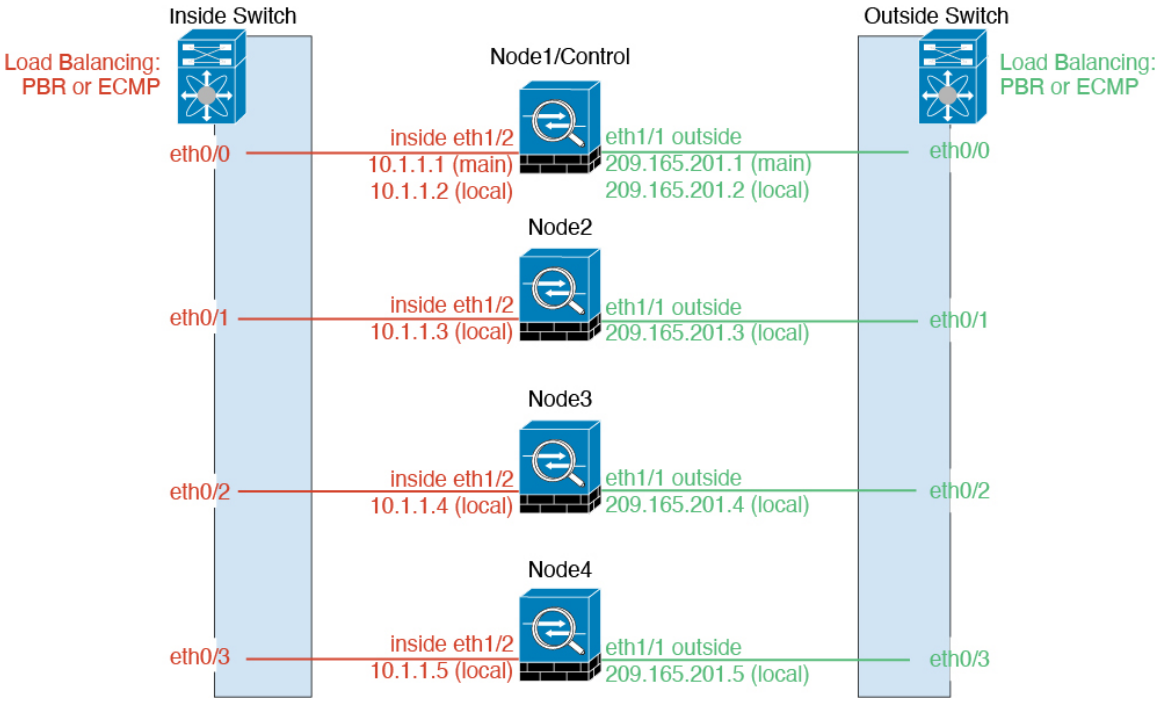
クラスタ内のすべてのノードは、同一の設定を共有します。最初に制御ノードとして指定したノードは、データノードがクラスタに参加するときにその設定を上書きします。そのため、クラスタを形成する前に制御ノードで初期設定を実行するだけで済みます。

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

個々のインターフェイス

クラスターフェイスを個々のインターフェイスとして設定できます。

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のローカル *IP* アドレスを持ちます。インターフェイス コンフィギュレーションは制御ノード上だけで行う必要があるため、このインターフェイス コンフィギュレーションの中で IP アドレスプールを設定して、このプールのアドレスをクラスタノード（制御ノード用を含む）のインターフェイスに使用させることができます。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、常に現在の制御ノードに属します。ローカルIPアドレスは、常にルーティングの制御ノードアドレスです。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。ただし、ロード バランシングを別途する必要があります（この場合はアップストリーム スイッチ上で）。



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

ポリシーベース ルーティング

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

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

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての Threat Defense に分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ Threat Defense に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 Threat Defense をモニタします。これで、PBR は、特定の Threat Defense の到達可能性に基づいてルートマップをイネーブルまたはディセーブルにできます。詳細については、次の URL を参照してください。

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

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

等コスト マルチパス ルーティング

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

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

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

クラスタ制御リンク

ユニットごとに 1 つのインターフェイスをクラスタ制御リンク専用の VXLAN（VTEP）インターフェイスにする必要があります。

VXLAN トンネル エンドポイント

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

VTEP 送信元インターフェイス

VTEP送信元インターフェイスは、VNIインターフェイスに関連付けられる予定の標準の threat defense virtual インターフェイスです。1 つの VTEP ソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。各VTEPソースインターフェイスには、同じサブネット上のIPアドレスがあります。このサブネットは、他のすべてのトラフィックからは隔離し、クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

VNI インターフェイス

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

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

ピア VTEP

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

クラスタ制御リンク トラフィックの概要

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

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 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。

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。

Threat Defense Virtual クラスタリングのライセンス

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

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。クラスタのライセンスは、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[ライセンス（License）]** 領域で変更できます。

（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。

Threat Defense Virtual クラスタリングの要件および前提条件

モデルの要件

- FTDv5、FTDv10、FTDv20、FTDv30、FTDv50、FTDv100
- VMware または KVM
- 最大 4 ノード

ユーザーの役割

- [管理者（Admin）]
- 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：

- クラスタ制御リンクでジャンボフレーム予約を有効にする必要があります。Threat Defense Virtual を展開するときに、ジャンボフレームの予約を有効にできます。それ以外の場合は、クラスタが形成されて正常な状態になった後で、各ノードを再起動してジャンボフレームを有効にする必要があります。
- 同じパフォーマンス層である必要があります。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のノードに一致するようにすべてのノードで制限されます。
- 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。

- 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（「サポートされていない機能とクラスタリング （29 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 を設定できます。

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 154 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。

Threat Defense Virtual クラスタリングのガイドライン

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。

その他のガイドライン

- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- 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。
- データインターフェイスの VXLAN はサポートしていません。クラスタ制御リンクのみが VXLAN をサポートします。

クラスタ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 モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が5分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 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。

Threat Defense Virtual クラスタリングの設定

Threat Defense Virtual の展開後にクラスタリングを設定するには、次のタスクを実行します。

Management Center へのデバイスの追加

クラスタリングを構成する前に、各クラスタノードを展開してから、Management Center でデバイスをスタンドアロンユニットとして追加します。

手順

ステップ 1 ハイパーバイザーのスタートアップガイドに従って、各クラスタノードを展開します。

ステップ 2 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。

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。

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。

始める前に

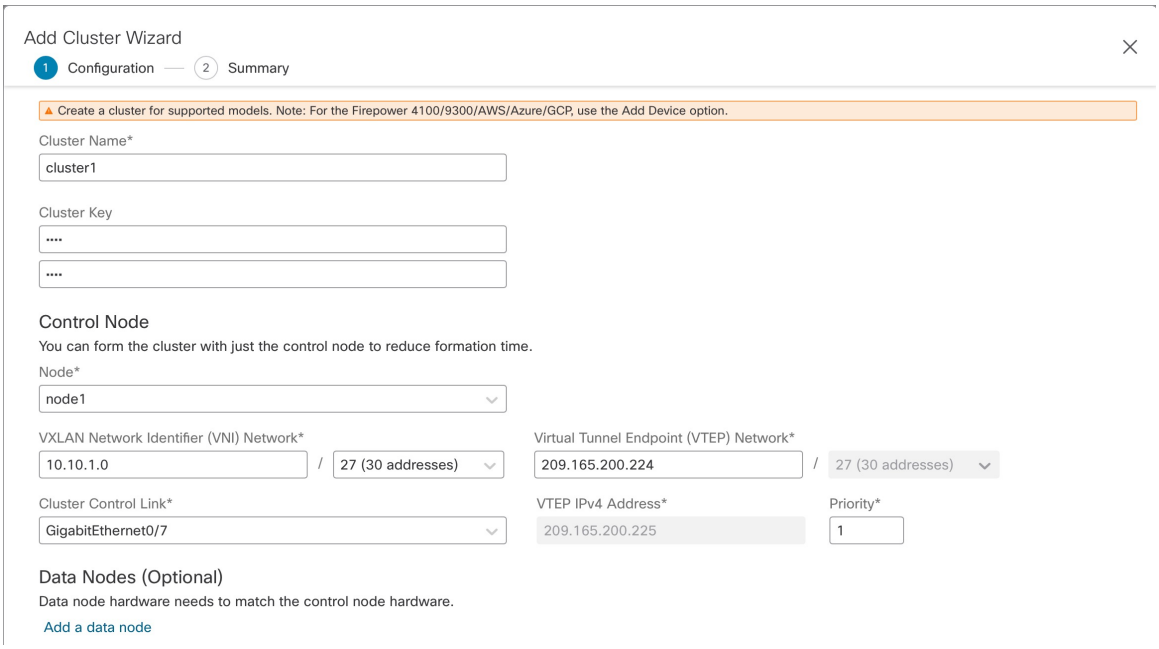
一部の機能はクラスタリングに対応していません。そのため、クラスタリングを有効にしてから、設定を行う必要があります。一部の機能は、設定してしまうとクラスタの作成をブロックします。たとえば、インターフェイスに IP アドレスを設定したり、BVI などのサポート対象外のインターフェイスタイプを設定したりしないでください。

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）] > [クラスタを追加（Add 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 *1 : [クラスタの追加（Add Cluster）]* ウィザード



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。

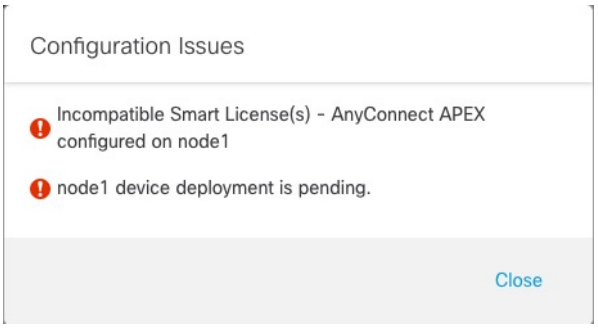
- [クラスタ名（Cluster Name）] : 1 ～ 38 文字の ASCII 文字列。
- [クラスタキー（Cluster Key）] : 1 ～ 63 文字の ASCII 文字列。[クラスタキー（Cluster Key）]の値は暗号キーを生成するために使用されます。この暗号は、データパストラフィック（接続状態の更新や転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

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 2 : 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。

- [VXLANネットワーク識別子(VNI)ネットワーク（VXLAN Network Identifier (VNI) Network）]：VNI ネットワークの IPv4 サブネットを指定します。このネットワークでは 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。IP アドレスは、このネットワーク上の各ノードに自動的に割り当てられます。VNI ネットワークは、物理 VTEP ネットワーク上で稼働する暗号化された仮想ネットワークです。
- [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を選択します。
- [仮想トンネルエンドポイント(VTEP)ネットワーク（Virtual Tunnel Endpoint (VTEP) Network）]：物理インターフェイス ネットワークの IPv4 サブネットを指定します。このネットワークでは IPv6 はサポートされていません。VTEP ネットワークは VNI ネットワークとは別のネットワークであり、物理クラスタ制御リンクに使用されます。
- [VTEP IPv4 アドレス（VTEP IPv4 Address）]：このフィールドには、VTEP 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。
- [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。

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。

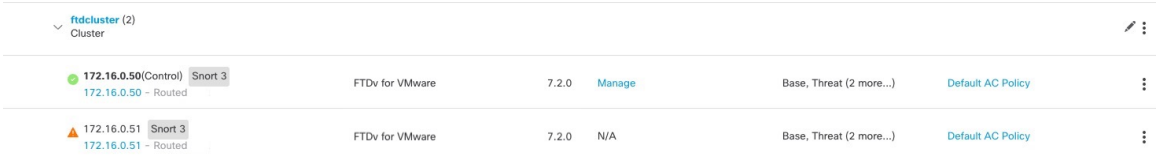
- [VTEP IPv4 アドレス（VTEP IPv4 Address）]：このフィールドには、VTEP ネットワークの次のアドレスが自動的に入力されます。
- [プライオリティ（Priority）]：制御ノードの選択に対するこのノードのプライオリティを設定します。プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。

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。

クラスタブートストラップ構成は、クラスタノードに保存されます。ブートストラップ構成には、クラスタ制御リンクに使用される VXLAN インターフェイスが含まれています。

[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。

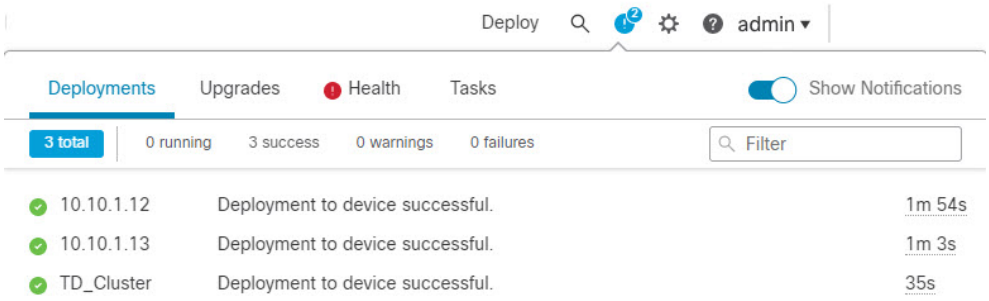
図 *3*：クラスタの管理



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 *4*：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。

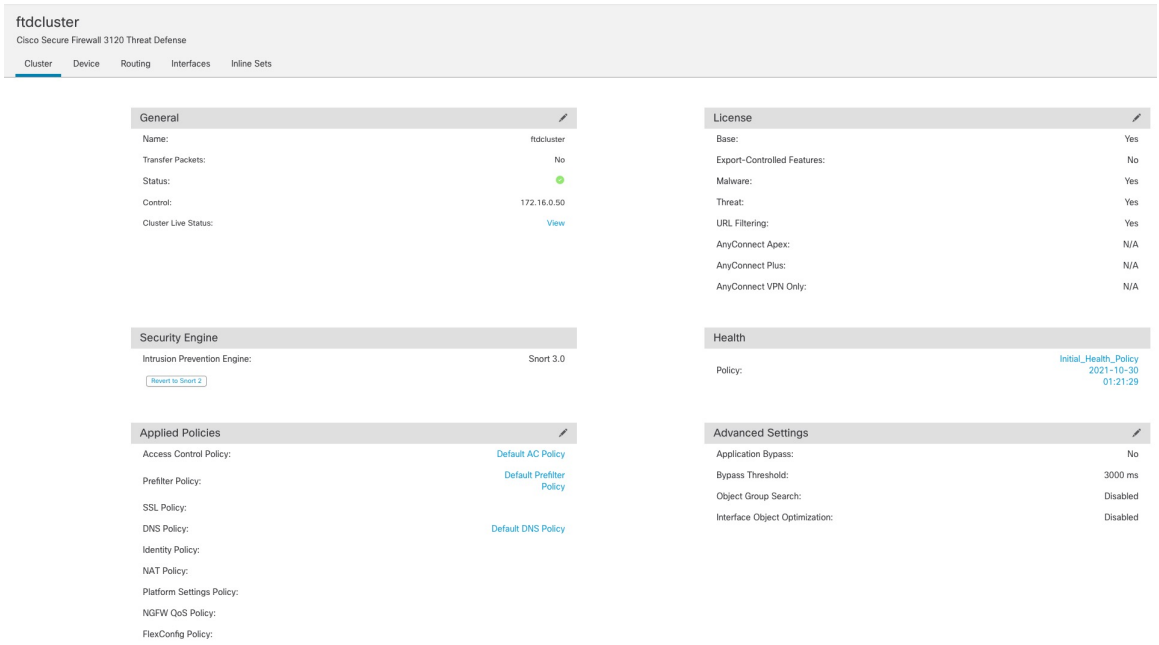


ステップ 6 クラスタの [編集（Edit）]（✎） をクリックして、デバイス固有の設定を指定します。

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。1

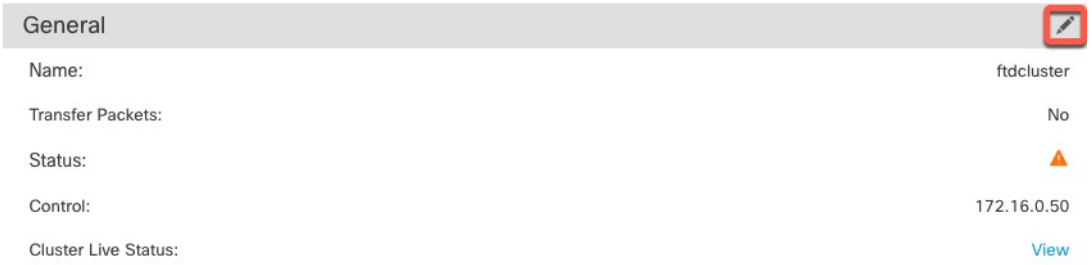
ステップ 7 [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] 画面に、クラスタの [全般（General）] などの設定が表示されます。

図 *5:* クラスタ設定

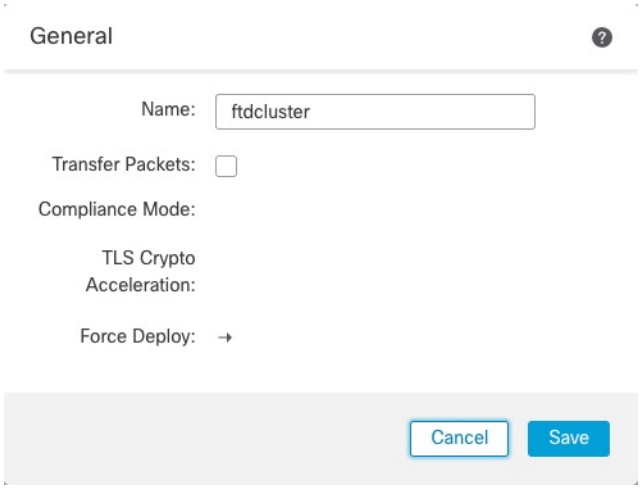


[全般（General）] 領域には、次のクラスタに固有の項目が表示されます。

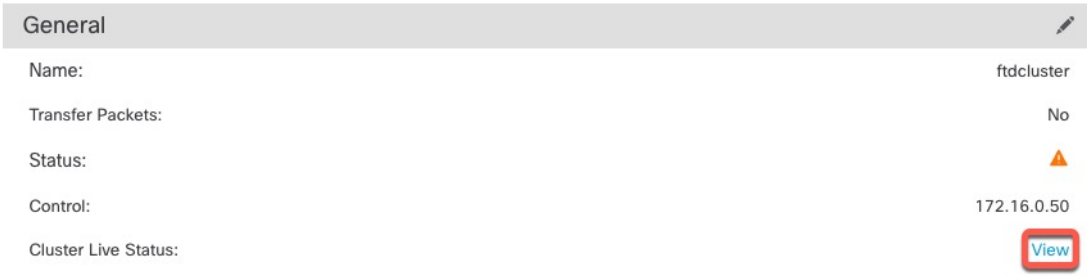
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタの表示名を変更します。



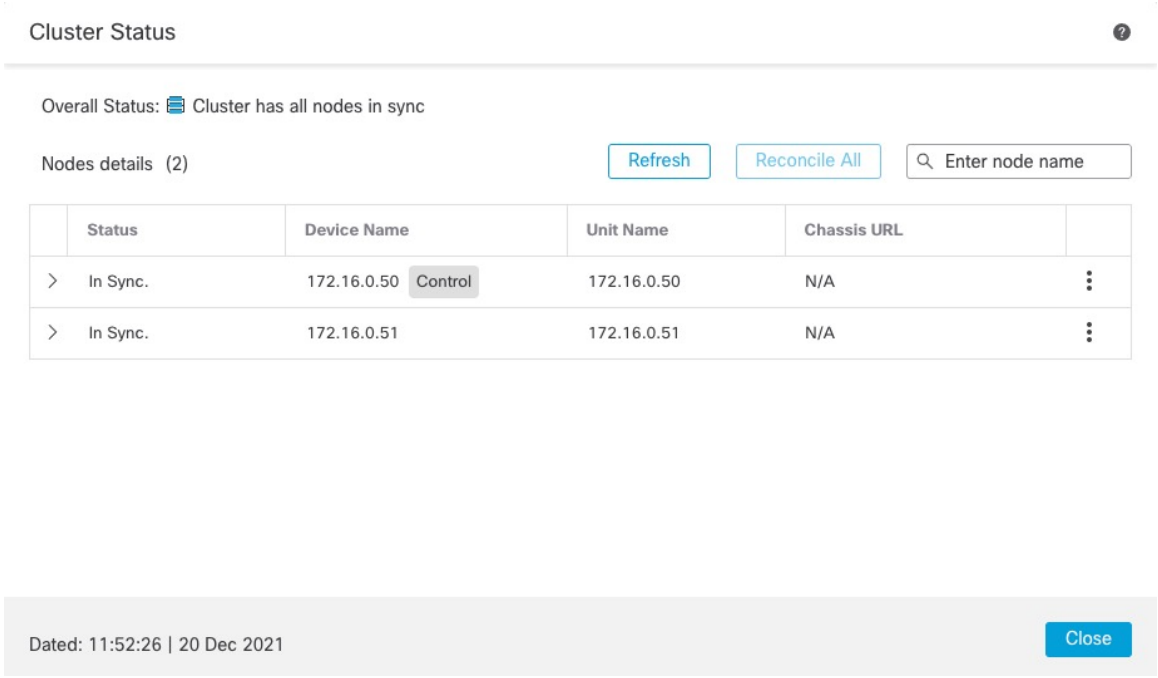
その後に、[名前（Name）] フィールドを設定します。



- [全般（General）] > [表示（View）] : [表示（View）] 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。



[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。



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 *6:* デバイス設定

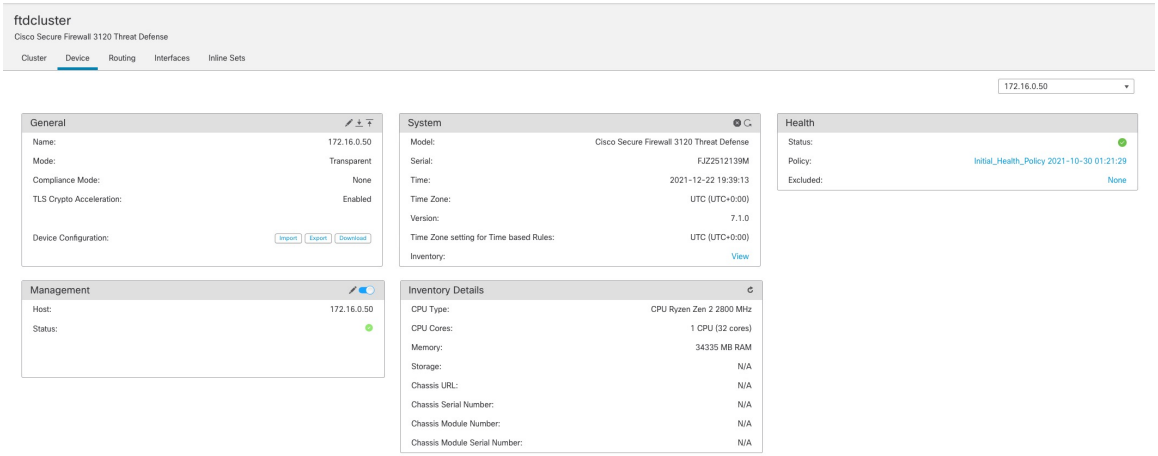
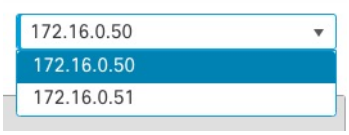
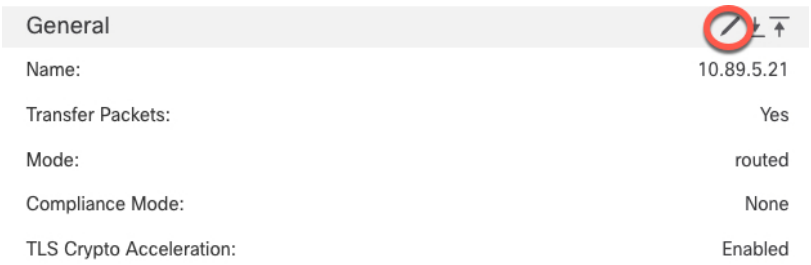


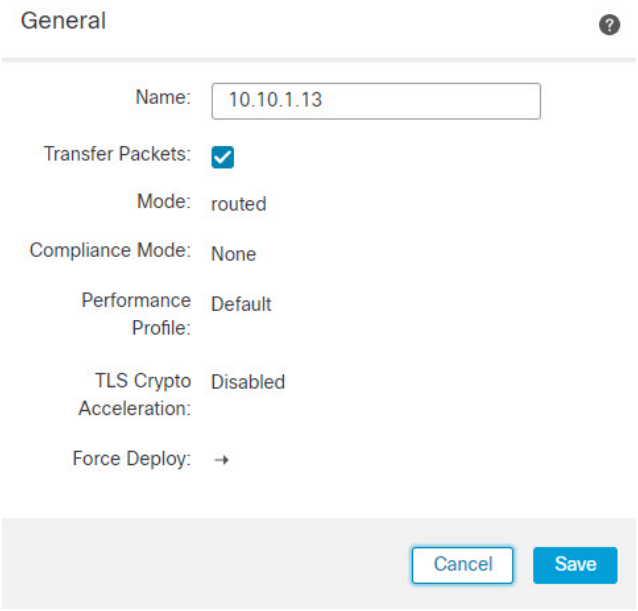
図 *7:* ノードの選択



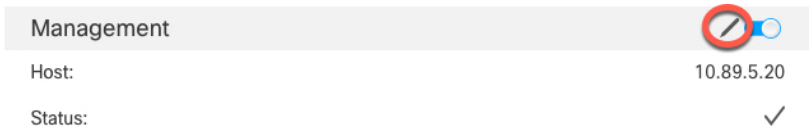
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタメンバーの表示名を変更します。



その後に、[名前（Name）] フィールドを設定します。



- [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。



ステップ 9 ジャンボフレームの予約を有効にせずにクラスタノードを展開した場合は、すべてのクラスタノードを再起動して、クラスタ制御リンクに必要なジャンボフレームを有効にします。

事前にジャンボフレームの予約を有効にした場合は、この手順をスキップできます。

クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッド（100 バ

イト）およびVXLANのオーバーヘッド（54バイト）にも対応する必要があります。クラスタを作成すると、MTU はデータインターフェイスの最大 MTU（デフォルトでは 1654）よりも 154 バイト大きい値が設定されます。後でデータインターフェイスの MTU を増やす場合は、クラスタ制御リンクの MTU も増やすようにしてください。たとえば、最大 MTU は 9198 バイトであるため、データインターフェイスの最大 MTU は 9044 になり、クラスタ制御リンクは 9198 に設定できます。

（注） 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。

インターフェイスの設定

ここでは、個々のインターフェイスがクラスタリング互換となるようにインターフェイスを設定する方法について説明します。個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ノードに属します。すべてのデータインターフェイスは個別インターフェイスである必要があります。

診断インターフェイスでは、IPアドレスプールを設定するか、DHCPを使用できます。診断インターフェイスのみがDHCPからのアドレスの取得をサポートしています。DHCPを使用する場合は、この手順を使用しないでください。代わりに、通常どおりに設定します。

（注） サブインターフェイスは使用できません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[アドレスプール（Address Pools）]** を選択して、IPv4 または IPv6 アドレスプールを追加します。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想IPアドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカルアドレスを事前に決定することはできません。

ステップ 2 **[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 3 [インターフェイス（Interfaces）] をクリックし、データインターフェイスの [編集（Edit）]（✎） をクリックします。

ステップ 4 [IPv4] で [IPアドレス（IP Address）] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在の制御ユニットに属します。

ステップ 5 作成したアドレスプールを [IPv4アドレスプール（IPv4 Address Pool）] ドロップダウンリストから選択します。

（注） このインターフェイスに MAC アドレスを手動で割り当てる場合は、FlexConfig を使用して **mac-address pool** を作成する必要があります。

ステップ 6 [IPv6] > [基本（Basic）] で、[IPv6アドレスプール（IPv6 Address Pool）] ドロップダウンリストから、作成したアドレスプールを選択します。

ステップ 7 通常どおり、他のインターフェイス設定を行います。

ステップ 8 [Save] 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。

クラスタノードの管理

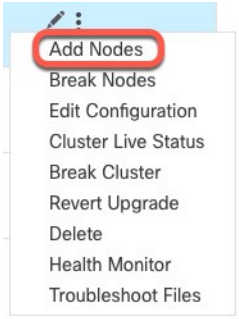
新しいクラスタノードの追加

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。

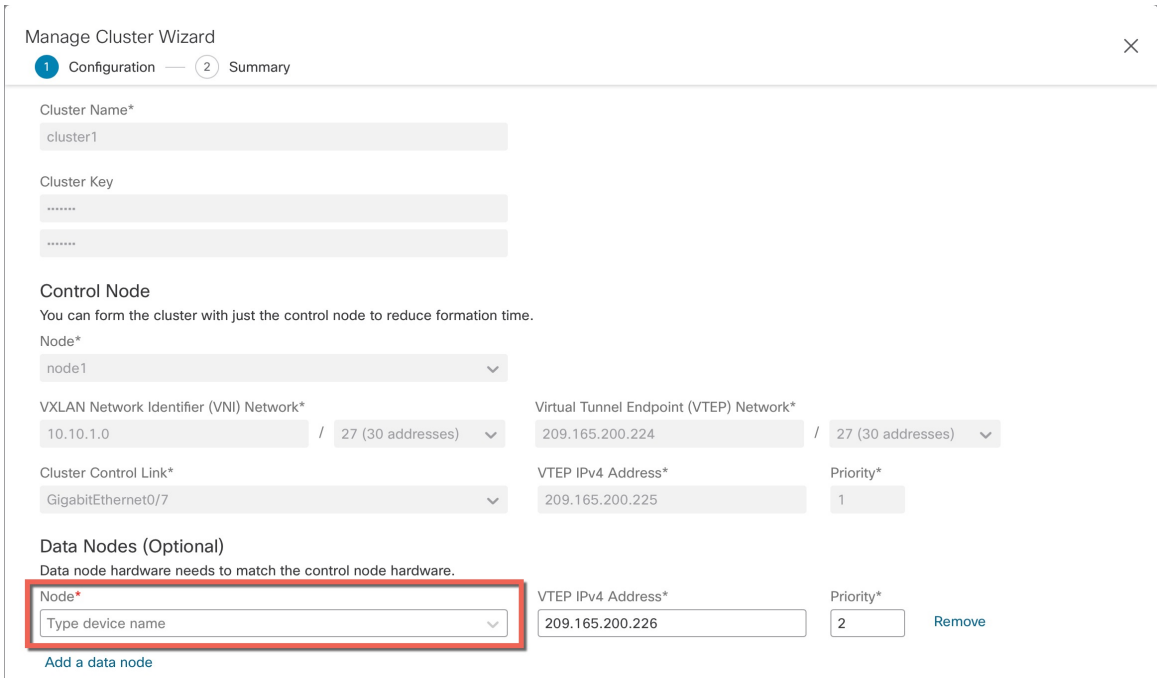
図 *8 :* ノードの追加



[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 アドレスと優先順位を調整します。

図 *9 : [*クラスタの管理（***Manage Cluster***）*]* ウィザード



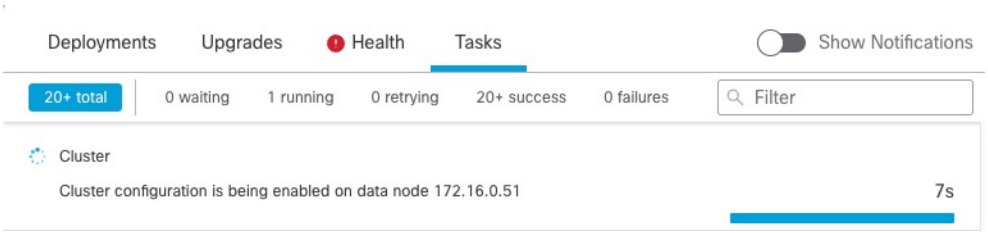
ステップ 3 さらにノードを追加するには、[データノードを追加（Add a data node）] をクリックします。

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 *10 : 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。



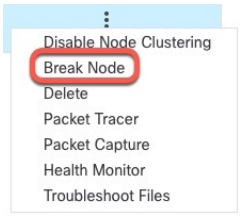
ノードの除外

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。

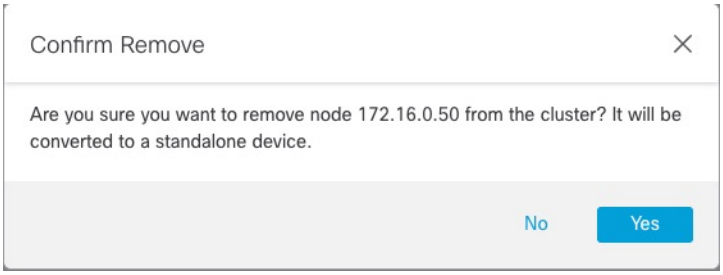
図 *11* : ノードの除外



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 *12* : 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

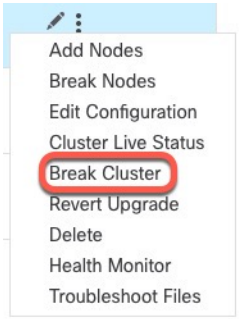
クラスタを解除し、すべてのノードをスタンドアロンデバイスに変換できます。制御ノードはインターフェイスとセキュリティポリシーの設定を保持しますが、データノードでは設定が消去されます。

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 （24 ページ）を参照してください。

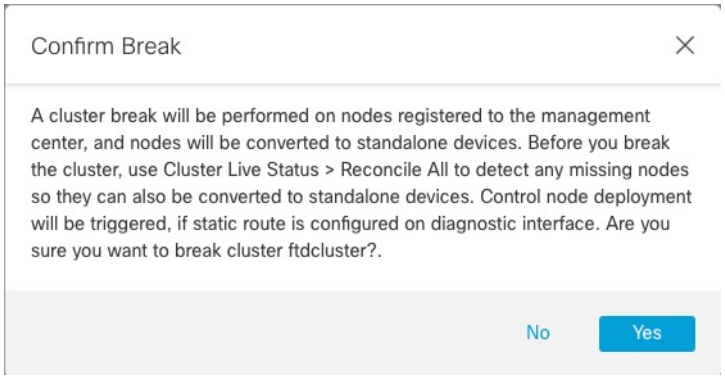
ステップ 2 [デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、クラスタの **その他**（⋮） をクリックして [クラスタを解除（Break Cluster）] を選択します。

図 *13* : 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 *14* : 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。

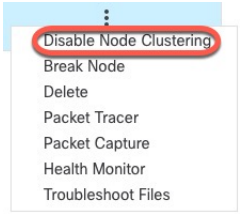
クラスタリングを無効にする

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 *15*：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 （21 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。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 （37 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 ノードの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

⚠

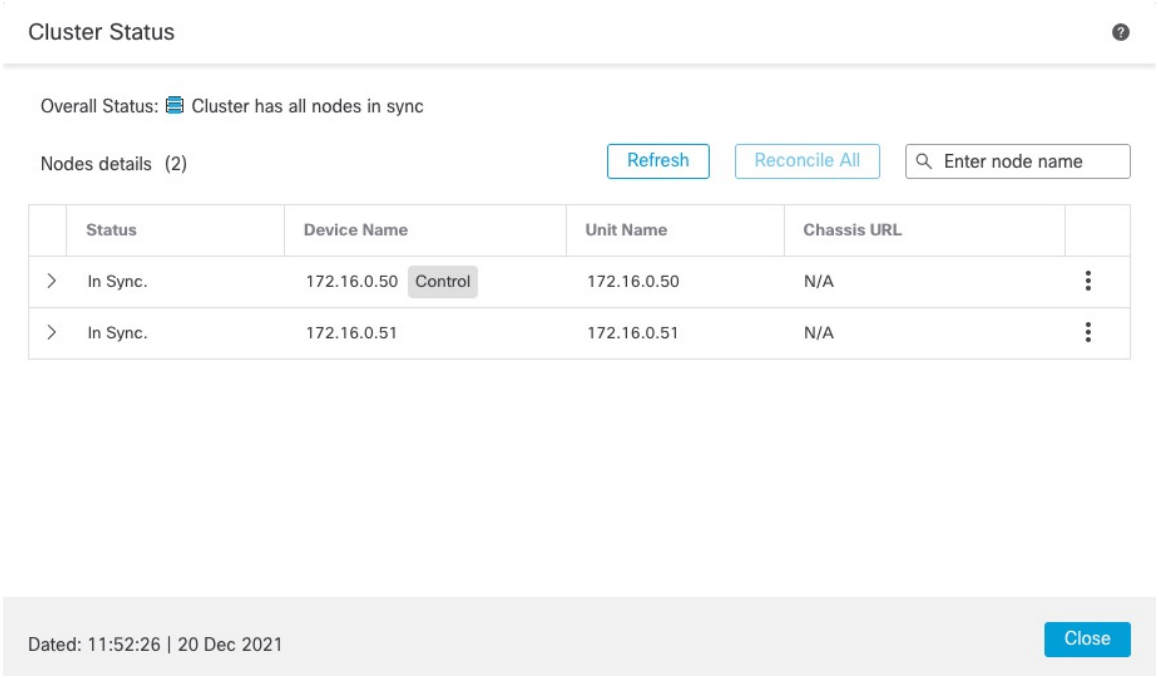
注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするユニットを厳密に指定する必要がある場合は、このセクションの手順を使用します。なお、中央集中型機能については、いずれかの方法で制御ノード変更を強制するとすべての接続がドロップされるため、新しい制御ノード上で接続を再確立する必要があります。

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 *16* : クラスタのステータス



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。

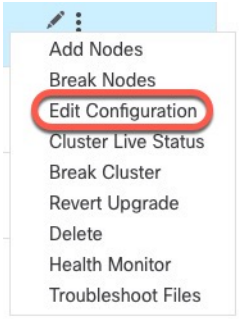
クラスタ設定の編集

クラスタ設定を編集できます。ノードの VTEP IP アドレスまたはノードの優先順位以外の値を変更すると、クラスタは自動的に失われて再構築されます。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 VTEP IP アドレスやノードの優先順位を変更すると、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。

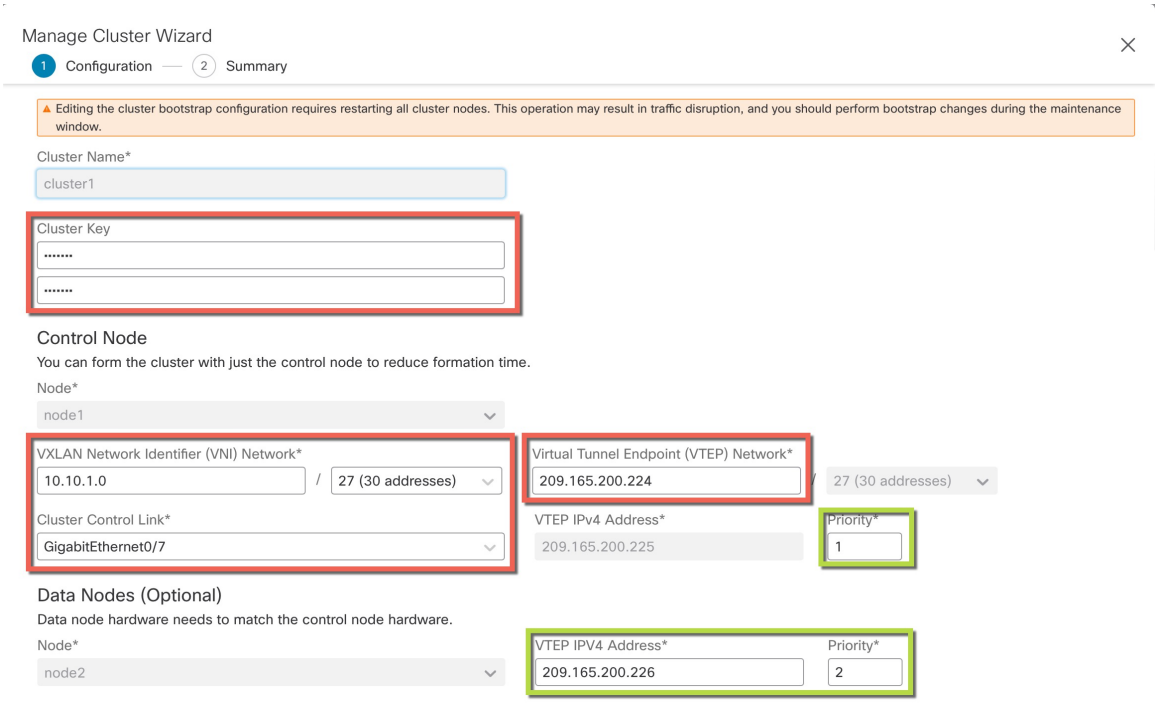
図 *17* : 設定の編集



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



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。

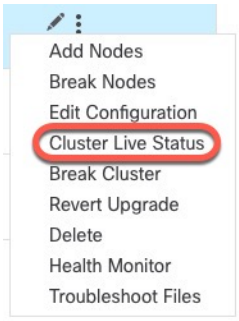
クラスタノードの照合

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

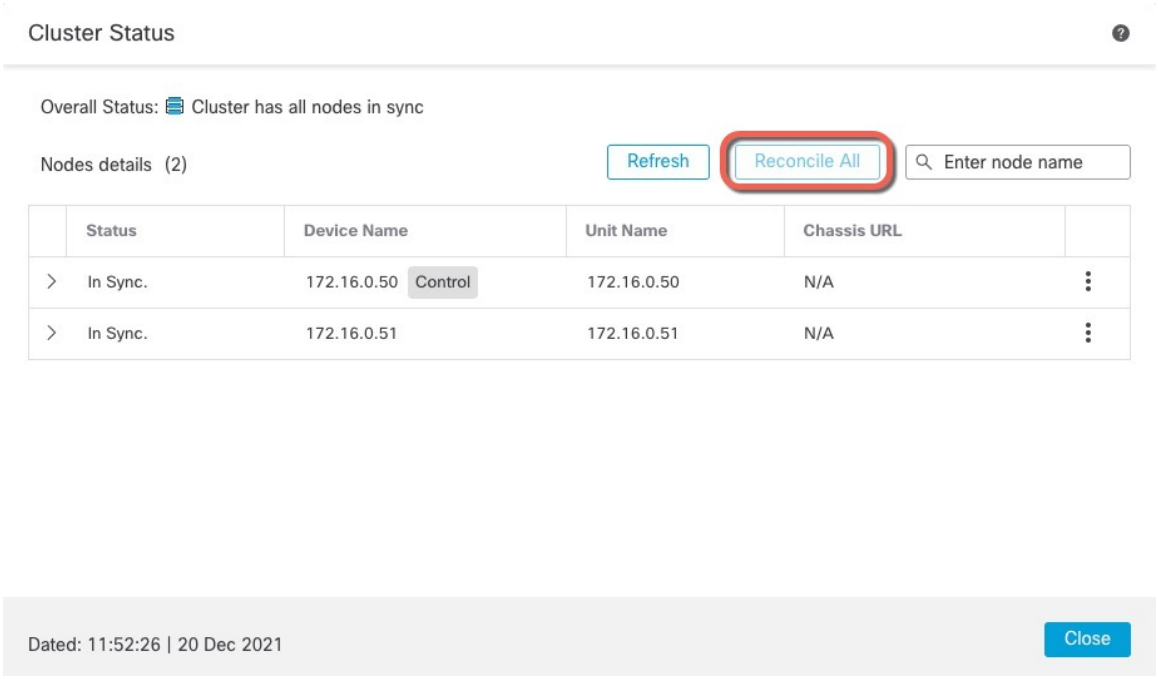
ステップ 1 クラスタの **[Devices]** > **[Device Management]** > **その他** （⋮） を選択し、次に [Cluster Live Status] を選択して [Cluster Status] ダイアログボックスを開きます。

図 *19*：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 *20*：すべてを照合



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 （26 ページ）を参照してください。

Management Center からのノードの削除

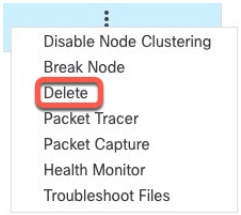
Management Center からクラスタを削除できます。これにより、クラスタはそのまま維持されます。クラスタを新しい Management Center に追加する場合は、クラスタを削除してもかまいません。

クラスタからノードを除外することなく、Management Center からノードを削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削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削除してもかまいませんが、クラスタの一部として残しておくことも可能です。

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 [削除（Delete）] を選択します。

図 *21* : 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 新しい Management Center にクラスタを追加するには、[デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、[デバイスの追加（Add Device）] をクリックします。

クラスタメンバーの 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す。

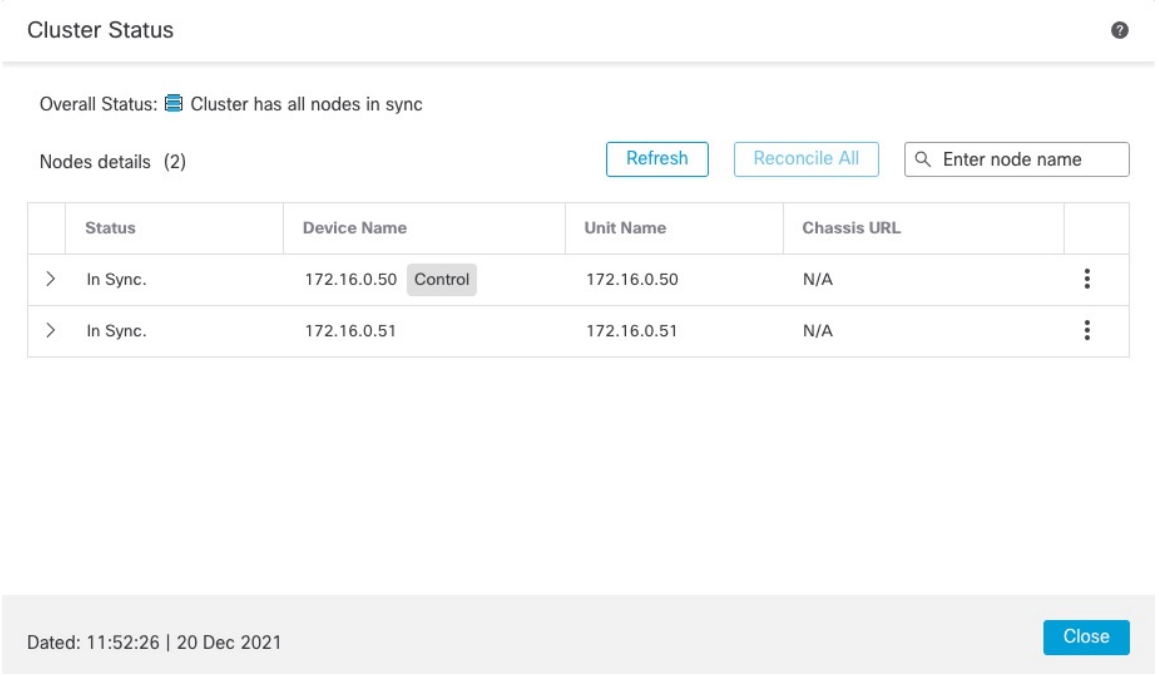
削除したノードを再度追加する方法については、「クラスタノードの照合 （24 ページ）」を参照してください。

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 *22 :* クラスタのステータス



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 *23 : ノードの [*概要（***Summary***）*]*

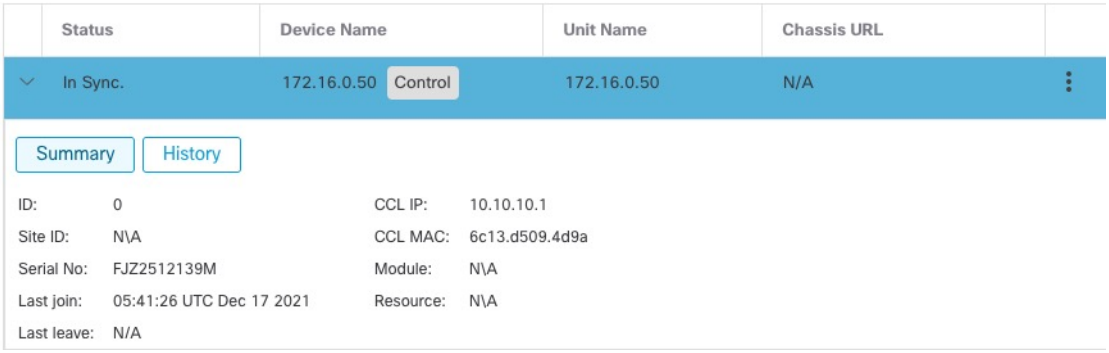
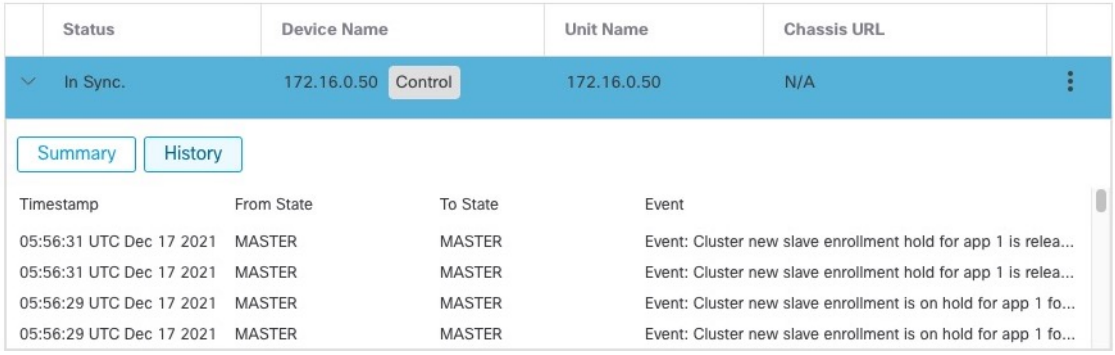


図 *24 : ノードの [*履歴（***History***）*]*



- **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る場合があります。

サポートされていない機能とクラスタリング

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 インスペクションなど）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。

- 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す。
- 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 インスペクションなど）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。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング

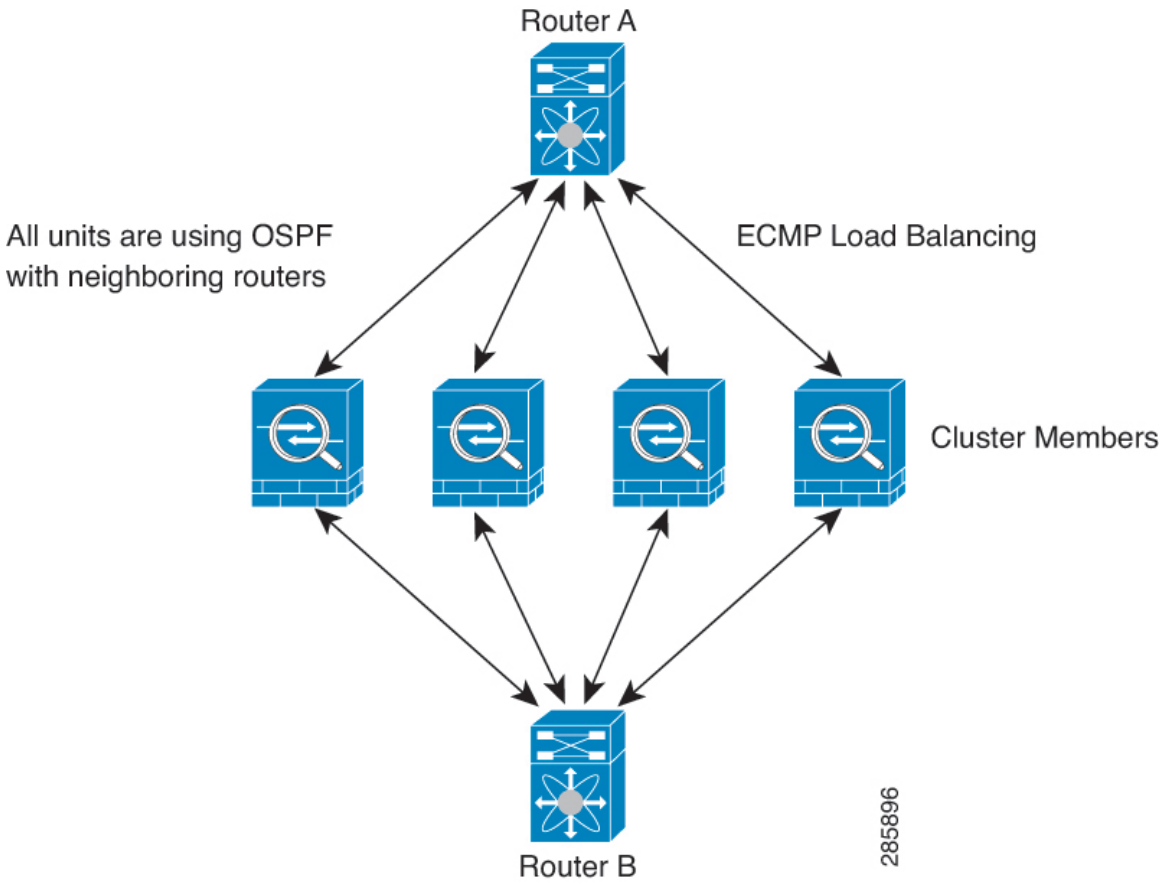
接続設定とクラスタリング

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。

ダイナミック ルーティングおよびクラスタリング

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

図 *25 :* 個別インターフェイス モードでのダイナミック ルーティング



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

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

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。

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 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。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の 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。

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 エージェントは、個々の Threat Defense を、その [Diagnostic] 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。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。

PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットを結合して1つのクラスタとしたときに、期待できるパフォーマンスの概算値は次のようになります。

- 合計スループットの 70 %
- 最大接続数の 60 %
- 接続数/秒の 50 %

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。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。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。

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。

すべての物理インターフェイスがモニタリングされます。ただし、モニタリングできるのは、名前付きインターフェイスのみです。

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。障害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、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。新規ノードがクラスタに参加する最初の 90 秒間は、ノード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、ノードはクラスタから削除されません。ノード状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

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

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

障害イベントに応じて、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/診断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。 問題の解決後、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。
- 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す。

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

表 *1:* クラスタ全体で複製される機能

トラフィック	状態のサポート	注
アップ タイム	○	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	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	○	—
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。

- 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。

  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。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。

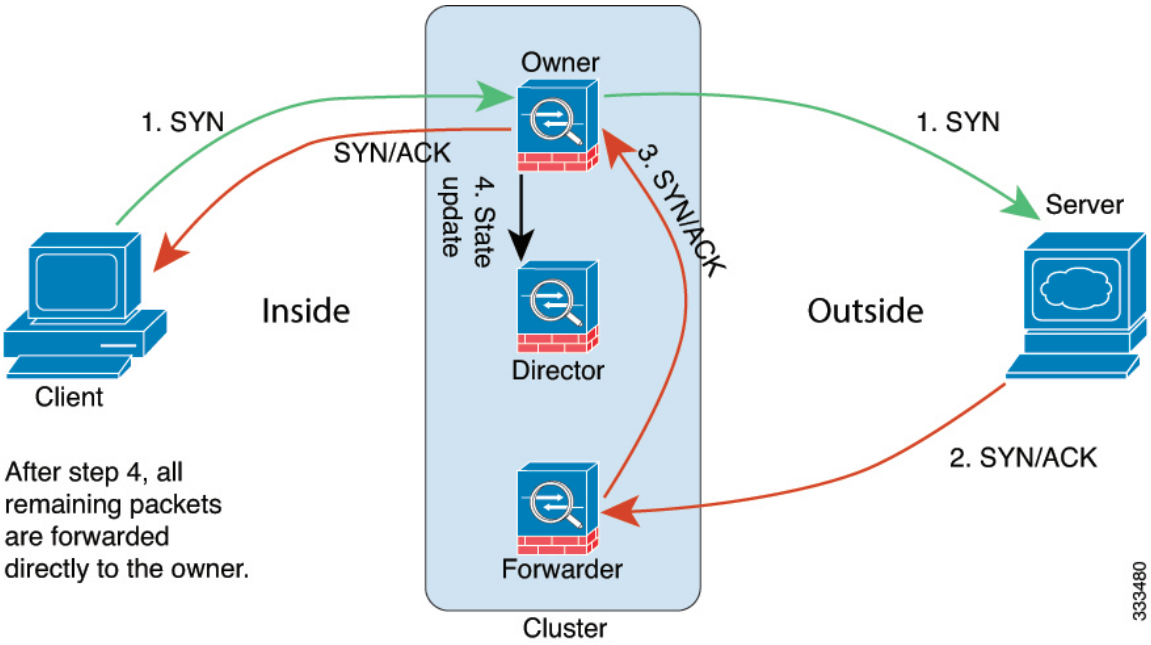
- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合が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

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。

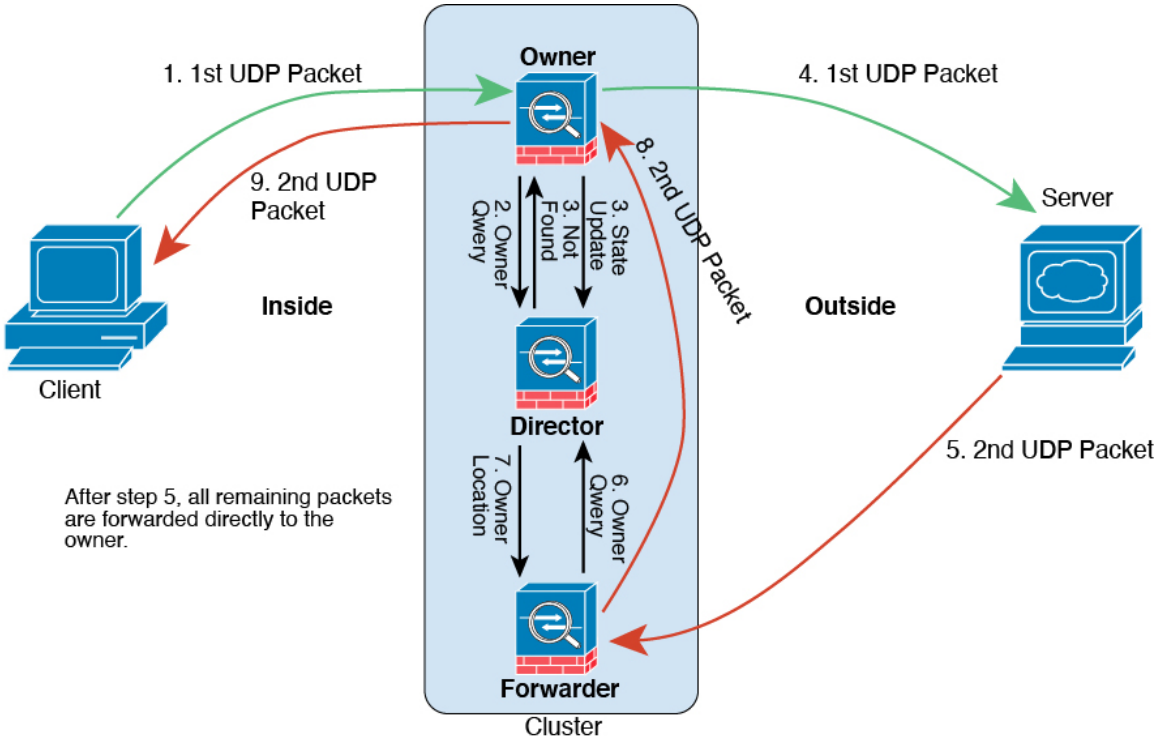


1. SYN パケットがクライアントから発信され、Threat Defense の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Threat Defense（ロードバランシング方法に基づく）に配信されます。この Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、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 *26 : 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。

プライベートクラウドでの Threat Defense Virtual のクラスタリング履歴

機能	バージョン	詳細
VMware および KVM の Threat Defense Virtual のクラスタリング	7.2	Threat Defense Virtual は VMware および KVM で最大 4 ノードの個別インターフェイスのクラスタリングをサポートします。 新規/変更された画面： • **[Devices]** > **[Device Management]** > **[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]** サポートされているプラットフォーム：VMware および KVM 上の Threat Defense Virtual

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。