



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

クラスタリングを利用すると、複数の Firewall 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 Firewall 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 \(41 ページ\)](#)」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 \(1 ページ\)](#)
- [Threat Defense Virtual クラスタリングのライセンス \(6 ページ\)](#)
- [Threat Defense Virtual クラスタリングの要件および前提条件 \(6 ページ\)](#)
- [Threat Defense Virtual クラスタリングのガイドライン \(8 ページ\)](#)
- [Threat Defense Virtual クラスタリングの設定 \(9 ページ\)](#)
- [クラスタノードの管理 \(24 ページ\)](#)
- [クラスタのモニタリング \(35 ページ\)](#)
- [クラスタリングの参考資料 \(41 ページ\)](#)
- [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 \(55 ページ\)](#)

## 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、Firewall 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）。Firewall 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する必要があります。

- 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リングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

## 個々のインターフェイス

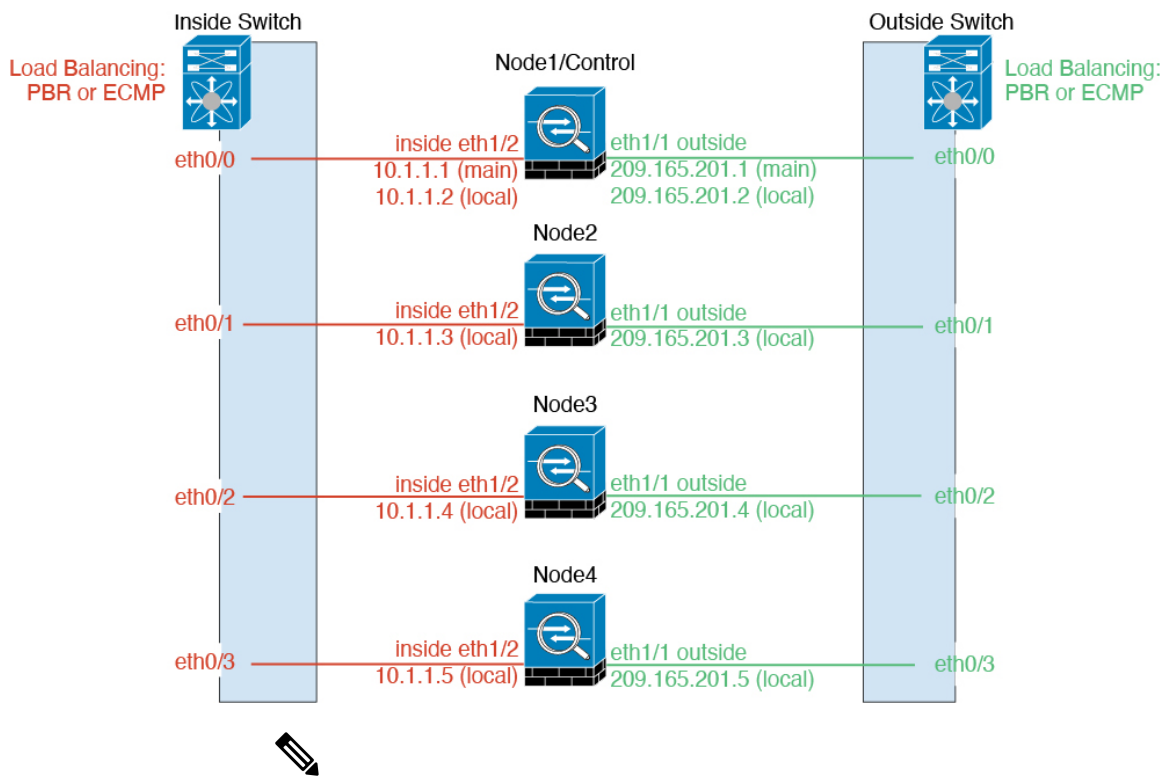
クラスターフェイスを個々のインターフェイスとして設定できます。

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

IPS 専用インターフェイス（インラインセットとパッシブインターフェイス）は、個別インターフェイスとしてサポートされません。

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

アップストリームスイッチ上でロードバランシングを別途する必要があります。



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

## ポリシーベース ルーティング

個別インターフェイスを使用するときは、各 Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense をモニタします。これで、PBR は、特定の Firewall Threat Defense の到達可能性に基づいてルート マップを有効化または無効化できます。詳細については、次の URL を参照してください。

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

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

## 等コスト マルチパス ルーティング

個別インターフェイスを使用するときは、各 Firewall 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、Firewall 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 Firewall 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 Firewall Threat Defense を設定する必要があります。

## クラスタ制御リンク

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

### VXLAN トンネル エンドポイント

VXLAN トンネルエンドポイント (VTEP) デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイスタイプ (VXLAN Network Identifier (VNI) インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、VTEP 間に VNI を

トンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス) があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

### VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、VNI インターフェイスに関連付けられる予定の標準の Firewall 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、Firewall 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。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

## 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 Firewall 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 Firewall 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、[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) Firewall 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、Firewall 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
- 2x2 構成のクラスタで最大4つのノードがサポートされます。最大2つのホストを設定し、各ホストに最大2つの Threat Defense 仮想インスタンスを設定できます。

## 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：

- 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。"DeploymentType": "Cluster" を設定して Firewall Threat Defense Virtual を展開するときに、Day 0 構成でこれを実行します。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。
- (KVM のみ) KVM ホスト上のすべての VM に CPU ハードパーティショニング (CPU ピン留め) を使用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。
- Firewall Management Center 通信の管理インターフェイスを指定する必要があります。データインターフェイス管理はサポートされていません。
- アップグレード時を除き、同じバージョン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 \(41 ページ\)](#)。
- 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。

## Firewall Management Center の要件

Firewall Management Center NTP サーバーをすべてのクラスタノードから到達可能な信頼できるサーバーに設定し、適切にクロックを同期できるようにします。デフォルトでは、デバイスは Firewall Management Center と同じ NTP サーバーが使用されます。すべてのクラスタノードの時刻が同じ時刻に設定されていない場合は、クラスタから自動で削除されます。

### 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

### ハイ アベイラビリティ

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

- 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、Firewall Threat Defense Virtual 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、トポロジ変更の影響を受け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。

## Threat Defense Virtual クラスタリングの設定

Firewall 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、Firewall 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** 『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』[英語] に従って各クラスタノードを展開します。

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。  
"DeploymentType": "Cluster" を設定して Firewall Threat Defense Virtual を展開するときに、Day 0 構成でこれを実行します。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。
- (KVM のみ) KVM ホスト上のすべての VM に CPU ハードパーティショニング (CPU ピン留め) を使用する必要があります。

**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 Firewall Management Center に追加します。

[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。

## クラスタの作成

Firewall 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 (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

Add Cluster Wizard

1 Configuration — 2 Summary

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

Cluster Name\*

cluster1

Cluster Key

....

....

Control Node

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

Node\*

node1

VXLAN Network Identifier (VNI) Network\*

10.10.1.0 / 27 (30 addresses)

Virtual Tunnel Endpoint (VTEP) Network\*

209.165.200.224 / 27 (30 addresses)

Cluster Control Link\*

GigabitEthernet0/7

VTEP IPv4 Address\*

209.165.200.225

Priority\*

1

Data Nodes (Optional)

Data node hardware needs to match the control node hardware.

[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。

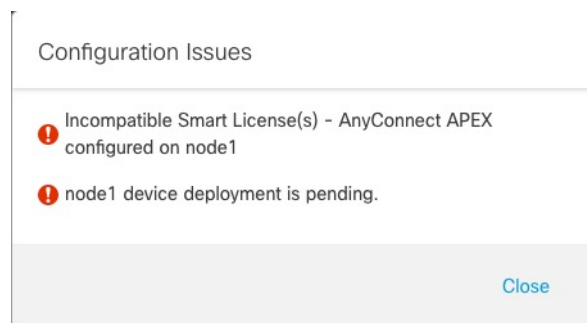
**ステップ 3** [制御ノード (Control Node)] については、次のように設定します。

- [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。Firewall 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** (❗) 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** (❗) 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

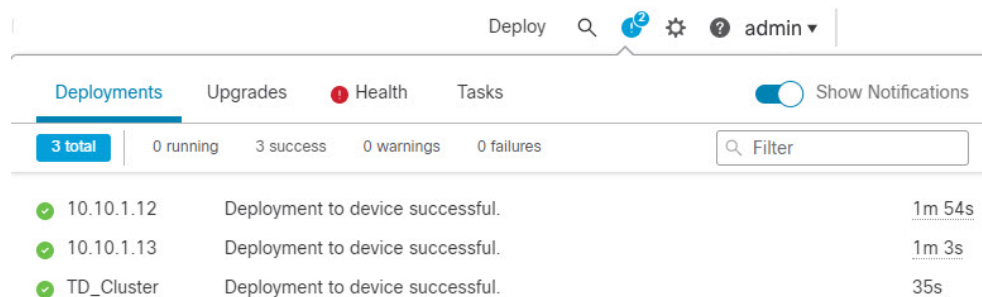
|   |                 |       |        |                          |                   |  |
|---|-----------------|-------|--------|--------------------------|-------------------|--|
| ftdcluster (2)<br>Cluster                             |                 |       |        |                          |                   |  |
| 172.16.0.50 (Control) Snort 3<br>172.16.0.50 - Routed | FTDv for VMware | 7.2.0 | Manage | Base, Threat (2 more...) | Default AC Policy |  |
| 172.16.0.51 Snort 3<br>172.16.0.51 - Routed           | FTDv for VMware | 7.2.0 | N/A    | 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 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。Firewall 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** クラスターの [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 5: クラスタ設定

ftdcluster  
Cisco Secure Firewall 3120 Threat Defense

Cluster
Device
Routing
Interfaces
Inline Sets

General

Name: ftdcluster  
Transfer Packets: No  
Status:   
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  
[Revert to Snort 2](#)

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。

General
✎

Name: ftdcluster  
Transfer Packets: No  
Status:   
Control: 172.16.0.50  
Cluster Live Status: [View](#)

その後に、[名前（Name）] フィールドを設定します。

General

Name: ftdcluster

Transfer Packets: ☐

Compliance Mode:

TLS Crypto Acceleration:

Force Deploy: →

Cancel


Save

- [全般 (General)] > [表示 (View)] : [表示 (View)] リンクをクリックして [クラスステータス (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。

Cluster Status

Overall Status: Cluster has all nodes in sync

Nodes details (2)

Refresh

Reconcile All

Enter node name

|   | Status   | Device Name                      | Unit Name   | Chassis URL |   |
|---|----------|----------------------------------|-------------|-------------|---|
| > | In Sync. | 172.16.0.50 <span>Control</span> | 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 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

ftdcluster

Cisco Secure Firewall 3120 Threat Defense

Cluster Device Routing Interfaces Inline Sets

172.16.0.50

General

Name: 172.16.0.50  
Mode: Transparent  
Compliance Mode: None  
TLS Crypto Acceleration: Enabled  
Device Configuration: Import Export Download

System

Model: Cisco Secure Firewall 3120 Threat Defense  
Serial: FJZ2512139M  
Time: 2021-12-22 19:39:13  
Time Zone: UTC (UTC+0:00)  
Version: 7.1.0  
Time Zone setting for Time based Rules: UTC (UTC+0:00)  
Inventory: View

Health

Status:   
Policy: Initial\_Health\_Policy 2021-10-30 01:21:29  
Excluded: None

Management

Host: 172.16.0.50  
Status:

Inventory Details

CPU Type: CPU Ryzen Zen 2 2800 Mhz  
CPU Cores: 1 CPU (32 cores)  
Memory: 34335 MB RAM  
Storage: N/A  
Chassis URL: N/A  
Chassis Serial Number: N/A  
Chassis Module Number: N/A  
Chassis Module Serial Number: N/A

図 7: ノードの選択


172.16.0.50

172.16.0.50

172.16.0.51




- [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。

| General                  |            |  |
|--------------------------|------------|---|
| Name:                    | 10.89.5.21 |   |
| Transfer Packets:        | Yes        |   |
| Mode:                    | routed     |   |
| Compliance Mode:         | None       |   |
| TLS Crypto Acceleration: | Enabled    |   |

その後に、[名前 (Name)] フィールドを設定します。

| General  |   | ? |
|--|---|---|
| Name:  | <input type="text" value="10.10.1.13"/> |   |
| Transfer Packets:                              | <input checked="" type="checkbox"/>     |   |
| Mode:  | routed                                  |   |
| Compliance Mode:                               | None                                    |   |
| Performance Profile:                           | Default                                 |   |
| TLS Crypto Acceleration:                       | Disabled                                |   |
| Force Deploy:                                  | →                                       |   |
| <div> <div>Cancel</div> <div>Save</div> </div> |   |   |

- [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、Firewall 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:    | ✓          |   |

**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。デバイスのシャットダウンまたは再起動を参照してください。

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。[MTUの設定](#)を参照してください。

（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（[ルーテッドモードのインターフェイスの設定](#)を参照）。




（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。[アドレスプール](#)を参照してください。

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する必要があります。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 (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。変更を展開するまで、変更は有効ではありません。

## 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 8: 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<br>(Timeouts)                           |   |
| 保留時間 (Hold Time)                               | 指定できる範囲は0.3～45秒です。デフォルトは3秒です。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)     | 指定できる範囲は 300 ～ 9000 ミリ秒です。デフォルトは 500 ms です。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見なされ、クラスタからノードが削除されるまでの時間です。  |
| <b>Monitored Interfaces</b> (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。  |
| モニタリング対象外のインターフェイス<br>(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<br>(Auto-Rejoin Settings)             |   |
| クラスタインターフェイス (Cluster Interface)               | クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。  |
| 試行 (Attempts)                                  | 指定できる範囲は -1 ～ 65535 です。デフォルトは -1 (無制限) です。再結合の試行回数を設定します。   |
| 試行の間隔 (Interval Between Attempts)              | 指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。   |
| 間隔のバリエーション (Interval Variation)                | 指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。   |

| フィールド                                | 説明   |
|--------------------------------------|--|
| データインターフェイス<br>(Data Interfaces)     | データインターフェイスに障害が発生した後に自動再結合の設定を表示します。   |
| 試行 (Attempts)                        | 指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。                               |
| 試行の間隔 (Interval<br>Between Attempts) | 指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。                              |
| 間隔のバリエーション<br>(Interval Variation)   | 指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。                        |
| システム (System)                        | 内部エラーが発生した後に自動再結合の設定を表示します。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。 |
| 試行 (Attempts)                        | 指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。                               |
| 試行の間隔 (Interval<br>Between Attempts) | 指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。                              |
| 間隔のバリエーション<br>(Interval Variation)   | 指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。                        |



(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。

これらの設定は、このセクションから変更できます。

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。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

## 手順

- ステップ 1 [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 (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、システムのヘルスチェックを無効にします。

図 9: 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（または VNet）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 10: 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 11: モニタリング対象インターフェイスの設定

▼ Monitored Interfaces

Monitored Interfaces

- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2
- GigabitEthernet0/3
- GigabitEthernet0/4
- GigabitEthernet0/5
- GigabitEthernet0/6
- GigabitEthernet0/7
- Diagnostic0/0

Add

Unmonitored Interfaces 1

☒ Enable Service Application Monitoring

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。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にできます。

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（または VNet）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



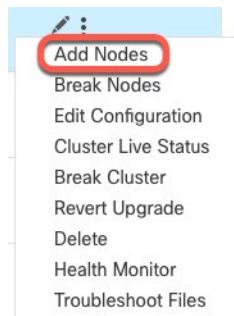
## 新しいクラスタノードの追加

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 (More)] (⋮) をクリックして [ノードを追加 (Add Nodes)] を選択します。

図 12: 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 13: [クラスタの管理 (Manage Cluster)] ウィザード

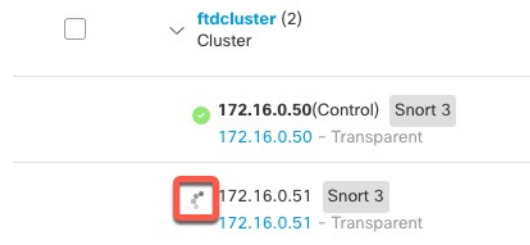
A screenshot of the 'Manage Cluster Wizard' Configuration step. The form includes fields for 'Cluster Name\*' (cluster1), 'Cluster Key' (masked), 'Control Node' (node1), 'VXLAN Network Identifier (VNI) Network\*' (10.10.1.0 / 27 (30 addresses)), 'Virtual Tunnel Endpoint (VTEP) Network\*' (209.165.200.224 / 27 (30 addresses)), 'Cluster Control Link\*' (GigabitEthernet0/7), 'VTEP IPv4 Address\*' (209.165.200.225), and 'Priority\*' (1). Under 'Data Nodes (Optional)', there is a 'Node\*' field with a dropdown menu showing 'Type device name', a 'VTEP IPv4 Address\*' field (209.165.200.226), and a 'Priority\*' field (2). A 'Remove' button is next to the second data node. A red box highlights the 'Node\*' dropdown menu. At the bottom, there is a link '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。

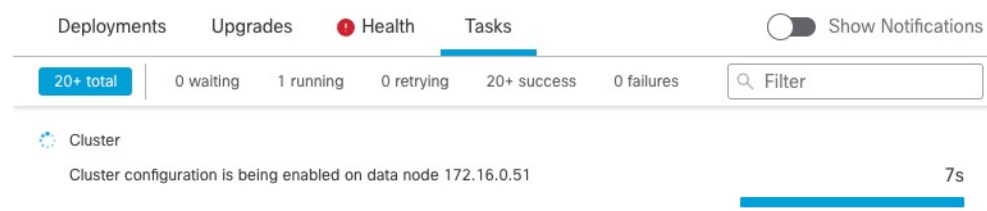
**ステップ 4** [続行（Continue）] をクリックします。[概要（Summary）] を確認し、[保存（Save）] をクリックします。

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 14: 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。



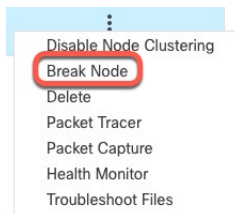
## ノードの除外

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（More）] (⋮) をクリックして [ノードを除外（Break Node）] を選択します。

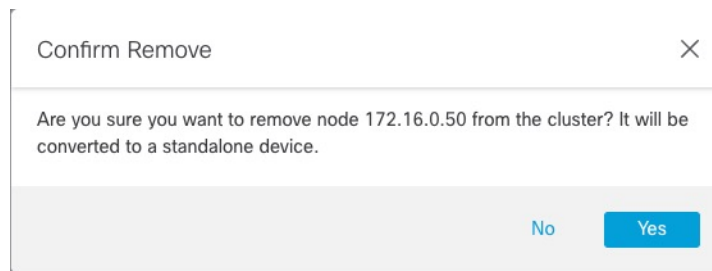
図 15: ノードの除外



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 16: 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。

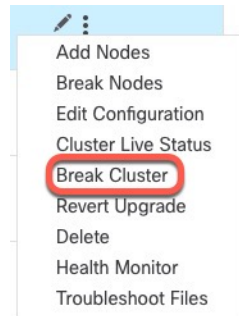
## クラスタの解除

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

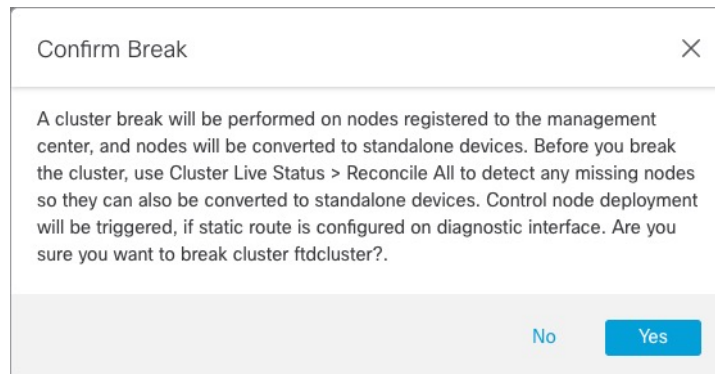
- ステップ 1** ノードを照合することにより、すべてのクラスタノードが Firewall Management Center で管理されていることを確認します。[クラスタノードの照合 \(32 ページ\)](#) を参照してください。
- ステップ 2** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、クラスタの [その他 (More)] (⋮) をクリックして [クラスタを解除 (Break Cluster)] を選択します。

図 17: クラスターの解除



**ステップ 3** クラスター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 18: 解除の確定



クラスター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。

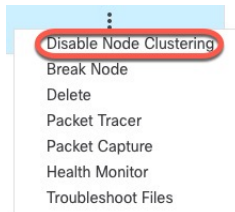
## クラスタリングを無効にする

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 Firewall 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 (More)] (⋮) 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 19: 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 \(29 ページ\)](#) 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 \(49 ページ\)](#)」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 (More)] (⋮) 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 (More)] (⋮) > [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 20: 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
Enter node name

|   | Status   | Device Name                      | Unit Name   | Chassis URL |   |
|---|----------|----------------------------------|-------------|-------------|---|
| > | In Sync. | 172.16.0.50 <span>Control</span> | 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 (More)] (⋮) > [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。

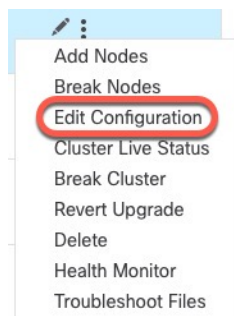
## クラスタ設定の編集

クラスタ設定を編集できます。ノードのVTEPIP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VTEPIP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 (More)] (⋮) をクリックして [設定を編集 (Edit Configuration)] を選択します。

図 21: 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 22:[クラスタの管理 (Manage Cluster) ]ウィザード

Manage Cluster Wizard

1 Configuration
2 Summary

▲ 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.

Cluster Name\*  
ftd\_cluster

Cluster Key  

\*\*\*\*\*

\*\*\*\*\*

Cluster-level changes

Control Node  
You can form the cluster with just the control node to reduce formation time.  
Node\*  
172.16.0.51

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

Cluster Control Link\*  
Ethernet1/7

Cluster Control Link IPv4 Address\*  
10.10.10.2

Priority\*  
2

Site ID  
0

Data Nodes (Optional)  
Data node hardware needs to match the control node hardware.  
Node\*  
172.16.0.50

Cluster Control Link IPv4 Address\*  
10.10.10.1

Priority\*  
1

Site ID  
0

Node-level changes

**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

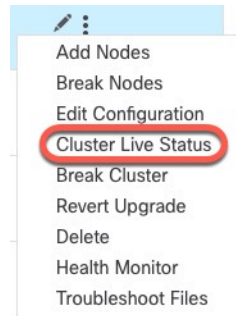
クラスタノードの登録に失敗した場合は、デバイスから Firewall Management Center に対してクラスタメンバーシップを照合できます。たとえば、Firewall Management Center が特定のプロセスで占領されているか、ネットワークに問題がある場合、データノードの登録に失敗することがあります。

### 手順

**ステップ 1** クラスターの [Devices] > [Device Management] > [その他 (More) ] (ⓘ) 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。

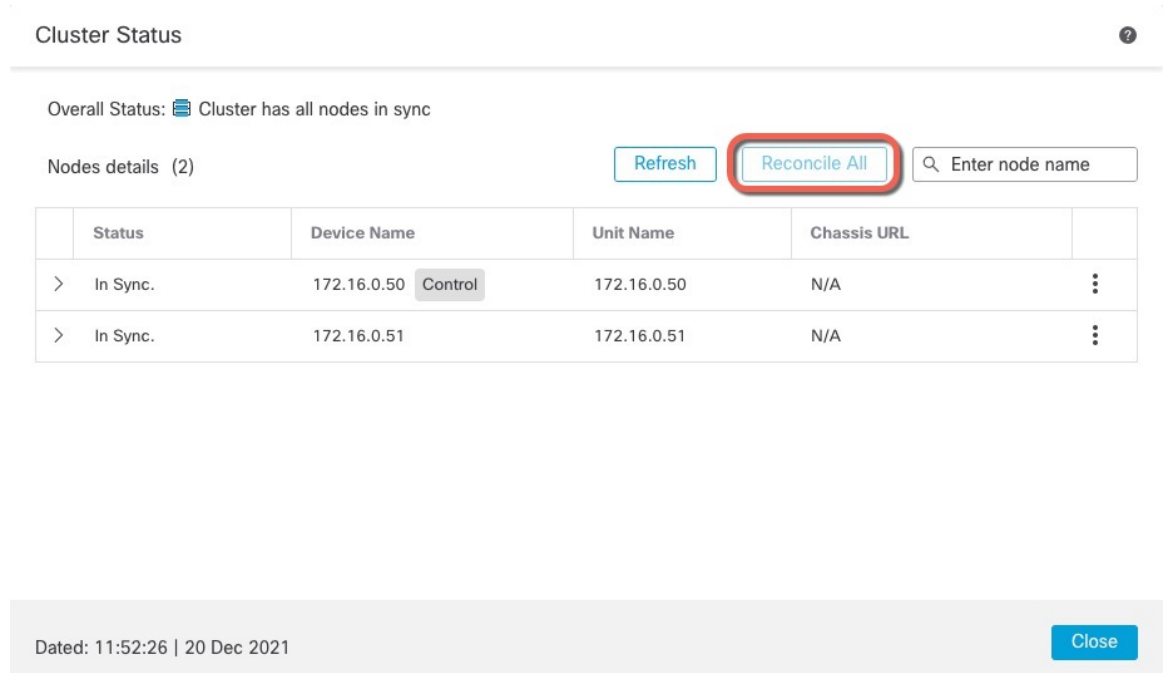


図 23: クラスターのライブステータス



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

図 24: 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（35 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 Firewall Management Center への登録

Firewall 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 Firewall 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、Firewall 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 Firewall 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。Firewall 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：

- Firewall 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 Firewall 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 Firewall 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。

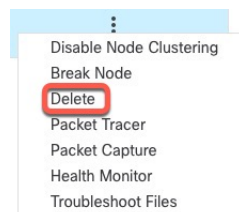
### 始める前に

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 (More)] (⋮) をクリックして [登録解除] [削除 (Delete)] を選択します。

図 25: 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）Firewall Management Center に登録できます。

- 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 Firewall 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、[デバイスの追加 (Add Device)] をクリックします。

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す。

**ステップ4** 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 \(32 ページ\)](#)」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、Firewall Management Center と Firewall 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 (More)] (⚙️ 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 26: 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 <span style="background-color: #d3d3d3;">Control</span> | 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 Firewall 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 Firewall 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 Firewall 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...）：ノードがシャード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 Firewall 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 27: 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         |
| <div>Summary History</div> <div> ID: 0 CCL IP: 10.10.10.1<br/> Site ID: N/A CCL MAC: 6c13.d509.4d9a<br/> Serial No: FJZ2512139M Module: N/A<br/> Last join: 05:41:26 UTC Dec 17 2021 Resource: N/A<br/> Last leave: N/A </div> |                     |             |             |

図 28: 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  |           |            |          |       |                          |        |        |  |                          |        |        |  |                          |        |        |  |                          |        |        |  |
| <div>Summary History</div> <div> <table> <tr> <th>Timestamp</th><th>From State</th><th>To State</th><th>Event</th></tr> <tr> <td>05:56:31 UTC Dec 17 2021</td><td>MASTER</td><td>MASTER</td><td>Event: Cluster new slave enrollment hold for app 1 is relea...</td></tr> <tr> <td>05:56:31 UTC Dec 17 2021</td><td>MASTER</td><td>MASTER</td><td>Event: Cluster new slave enrollment hold for app 1 is relea...</td></tr> <tr> <td>05:56:29 UTC Dec 17 2021</td><td>MASTER</td><td>MASTER</td><td>Event: Cluster new slave enrollment is on hold for app 1 fo...</td></tr> <tr> <td>05:56:29 UTC Dec 17 2021</td><td>MASTER</td><td>MASTER</td><td>Event: Cluster new slave enrollment is on hold for app 1 fo...</td></tr> </table> </div> |                     |             |  | 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... |
| 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（System）] [⚙] > [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 モニター ダッシュボード

### クラスタのヘルスマニター

Firewall Threat Defense がクラスタの制御ノードである場合、Firewall 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 Firewall 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。セレクト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

- Firewall 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 (System)] (⚙️) > [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** 正常性モニターの右上隅にあるプラス記号[新しいダッシュボードの追加 (Add New Dashboard)] (+) 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   | フォーマット (Format) |
|-----------|--|-----------------|
| 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）。 | パーセンテージ         |
| 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）。   | パーセンテージ         |
| 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。                          | バイト             |



| メトリック      | 説明                          | フォーマット<br>(Format) |
|------------|-----------------------------|--------------------|
| 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。 | バイト                |
| 接続         | クラスタ内のアクティブな接続数。            | 番号                 |
| NAT 変換数    | クラスタの NAT 変換数。              | 番号                 |
| 分布         | 1 秒ごとのクラスタ内の接続分布数。          | 番号                 |
| パケット       | クラスタ内の 1 秒ごとのパケット配信の件数。     | 番号                 |

## 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

Firewall 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、Firewall 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
- Firewall Management Center UCAPL/CC モード

- 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。

## 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、Firewall 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

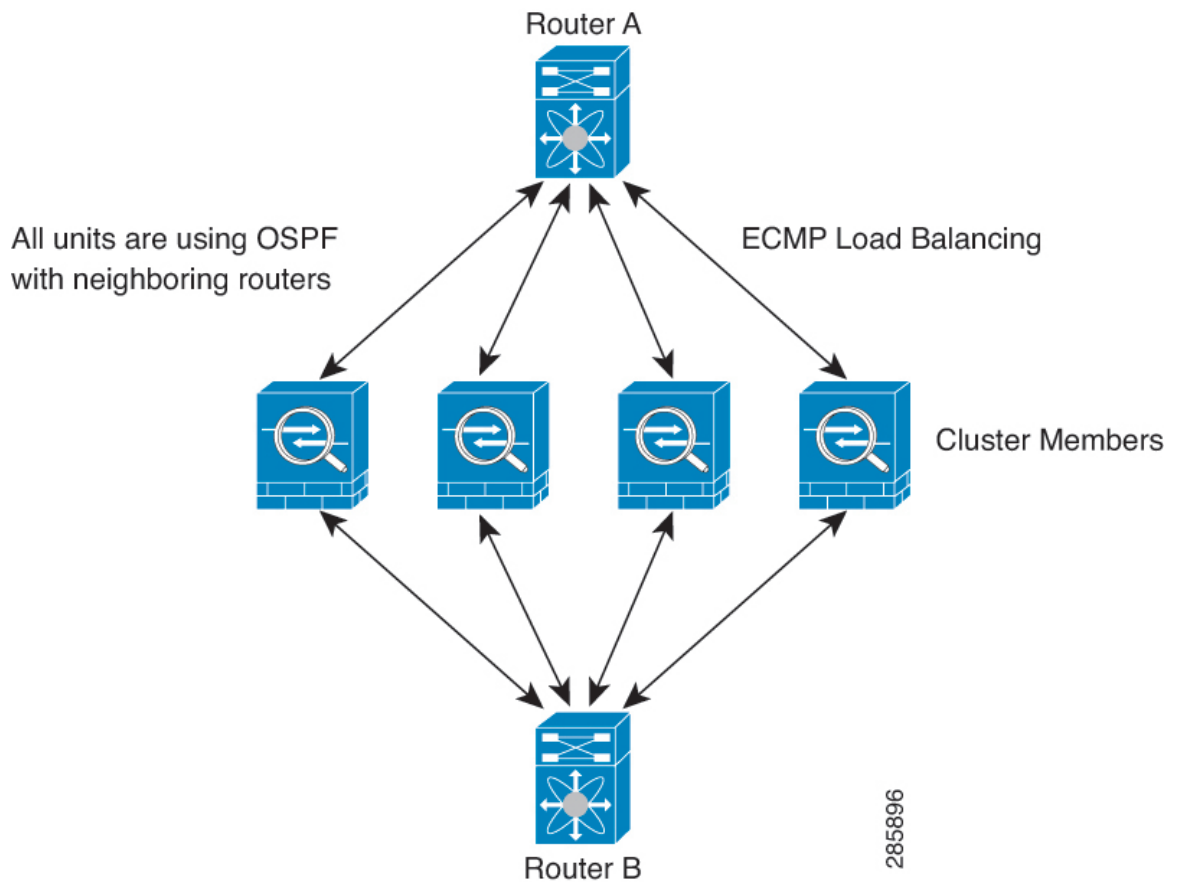
## 接続設定とクラスタリング

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

## 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 Firewall 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 Firewall 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テティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。
- 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まだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード

間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。

- クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての `xlate` をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。
- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT `xlate`：制御ノードが `xlate` テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その `xlate` がテーブル内にない場合、データノードは制御ノードに `xlate` を要求します。データノードが接続を所有します。
- 旧式の `xlate`：接続所有者の `xlate` アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の `xlate` であることを示します。
- 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спек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 Firewall Threat Defense を、その [診断 (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 ユーザは新しいノードに複製されません。SNMPv3 ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

## 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

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。



(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。

## 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。

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。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。

### 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。ヘルスチェックは、インターフェイスごとに、モニタリングをオプションで無効にすることができます。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。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、Firewall Threat Defense は自動的にクラスタへの再参加を試みます。



(注) Firewall 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：FTD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：Firewall 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、Firewall 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。Firewall 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：FMC 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

| Traffic          | 状態のサポート    | 注意                    |
|------------------|------------|-----------------------|
| Up time          | Yes        | システムアップタイムをトラッキングします。 |
| ARP Table        | あり         | —                     |
| MAC アドレス テーブル    | あり         | —                     |
| ユーザ アイデンティティ     | Yes        | —                     |
| IPv6 ネイバー データベース | ○          | —                     |
| ダイナミック ルーティング    | ○          | —                     |
| SNMP エンジン ID     | [いいえ (No)] | —                     |

## 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なります。

クアッパオーナーに問い合わせ、関連するステート情報を取得し、そのノードが新しいオーナーになります。

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

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

- **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 識別子であり、宛先ポートは 0 です。
  - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
  - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。
- **フォワーダ**：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせ、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するのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。



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

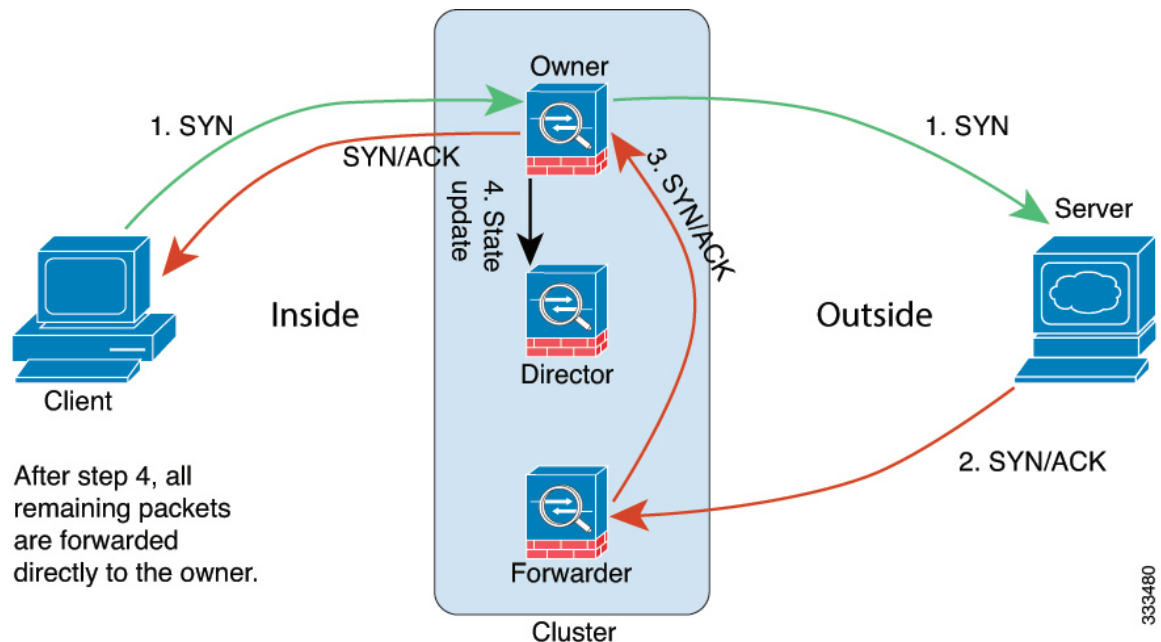
- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先のIPアドレス、およびパケットIDのハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される5タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先IPアドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

## 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。

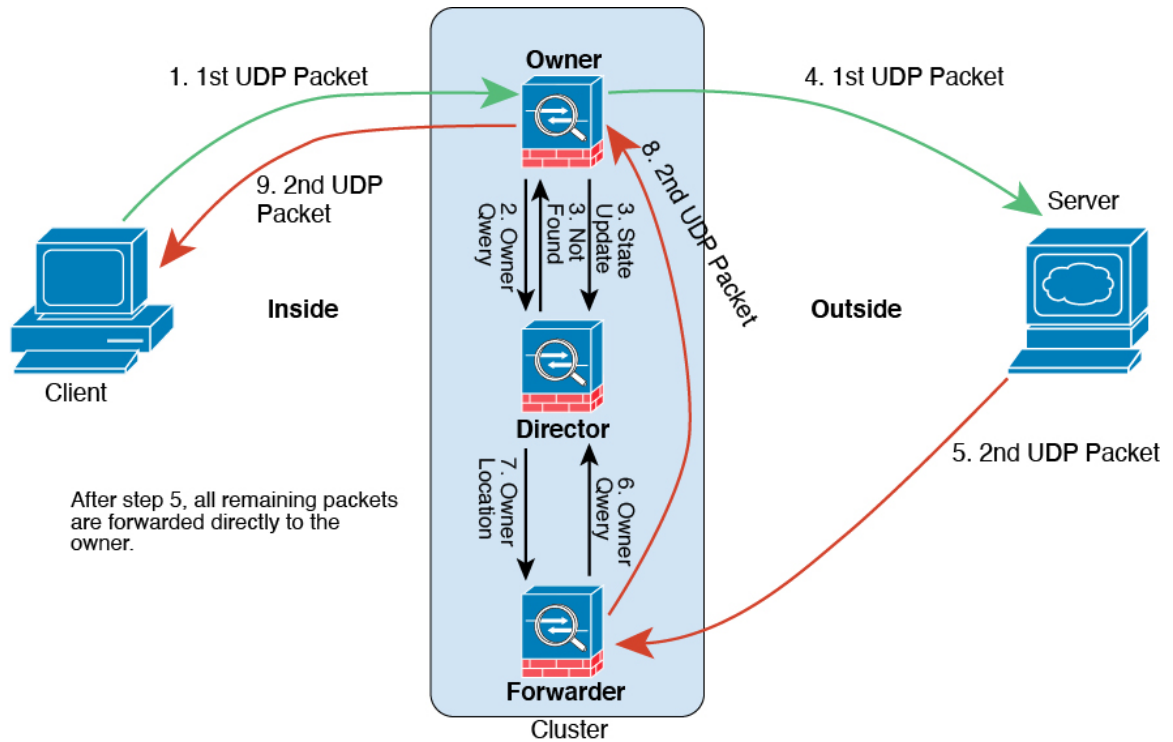


1. SYN パケットがクライアントから発信され、Firewall Threat Defense の1つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firewall Threat Defense（ロードバランシング方法に基づく）に配信されます。この Firewall Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN 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 ステート情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせ、オーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、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 30: 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 Firewall 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、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

# 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  | 最小<br>Firewall<br>Management<br>Center | 最小<br>Firewall<br>Threat<br>Defense | 詳細  |
|---|--|-------------------------------------|---|
| 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）]&gt;[デバイス管理（Device Management）]&gt;クラスタ（Cluster）&gt;[クラスタのヘルスマニターの設定（Cluster Health Monitor Settings）]</p> <p>（注）<br/>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>   |
| 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（System）]&gt;[正常性（Health）]&gt;[モニター（Monitor）]</p>  |
| VMware および KVM の Firewall Threat Defense Virtual のクラスタリング | 7.2.0                                  | 7.2.0                               | <p>Firewall 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이스の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"> <li>• [デバイス（Devices）]&gt;[デバイス管理（Device Management）]&gt;[クラスタの追加（Add Cluster）]</li> <li>• [デバイス（Devices）]&gt;[デバイス管理（Device Management）]&gt;[詳細（More）]メニュー</li> <li>• [Devices]&gt;[Device Management]&gt;[Cluster]</li> </ul> <p>サポートされているプラットフォーム：VMware および KVM 上の Firewall Threat Defense Virtual</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。