Firepower 4100/9300 上の Threat Defense クラスタの展開

最終更新：2023 年 4 月 19 日

Firepower 4100/9300 上の Threat Defense のクラスタ展開

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

（注） クラスタリングを使用する場合、一部の機能はサポートされません。クラスタリングでサポートされない機能 （73 ページ） を参照してください。

（注） 本書では、最新の Threat Defense バージョンの機能を取り上げています。機能の変更の詳細については、「クラスタリングの履歴 （87 ページ）」を参照してください。古いバージョンのソフトウェアを使用している場合は、お使いのバージョンの Firepower Management Center 設定ガイドおよび FXOS 設定ガイドの手順を参照してください。

この統合によるメリット

FXOS プラットフォームでは、FTD を含む複数の論理デバイスを実行することができます。スタンドアロンおよびクラスタ化された論理デバイスの展開は、シャーシ内クラスタ（Firepower 9300）およびシャーシ間クラスタの両方において簡単に実行できます。FXOS からクラスタを導入する際は、FTD ブートストラップを事前設定しておくと、FTD アプリケーション内でのカスタマイズがほんのわずかで済みます。FXOS におけるクラスタ設定をエクスポートすることにより、その他のクラスタ メンバを追加することもできます。

統合された製品

この表では、この統合のために必要な製品の一覧を示します。

表 *1:* クラスタリング用に統合された製品

製品	機能	最小バージョン	必須かどうか
Firepower 4100 または 9300	FTD を実行するためのハードウェアプラットフォーム	FXOS 1.1(4)	必須
Firepower Chassis Manager	FXOS GUI デバイスマネージャ	Firepower Chassis Manager 1.1(4)	オプション：代わりに CLI を使用することができます。
FTD	次世代ファイアウォール アプリケーション	FirePOWER 6.0.1	必須
FMC	GUI マルチデバイスマネージャ	FirePOWER 6.0.1	必須

ワークフロー

このワークフローでは、クラスタリングの導入を完了するため、FTD の FXOS および FMC で Firepower Chassis Manager を使用します。

手順

ステップ 1 FXOS タスク：

a) FXOS：インターフェイスの設定 （16 ページ）。FTD に割り当てる 1 つの管理およびすべてのデータインターフェイスを設定します。クラスタインターフェイスはポートチャネル 48 としてデフォルトで定義されていますが、シャーシ間のクラスタリングでは、メンバーインターフェイスを追加する必要があります。マルチインスタンスクラスタリングの場合は、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。

b) FXOS：コンテナインスタンスにリソースプロファイルを追加 （23 ページ）。

c) Threat Defense クラスタの作成 （24 ページ）。

d) クラスタノードの追加 （37 ページ）

ステップ 2 FMC タスク：

a) Management Center：クラスタの追加 （40 ページ）。

b) Management Center：クラスタ、データ、および診断インターフェイスの設定 （46 ページ）。管理インターフェイスは、クラスタを展開したときに事前設定されました。

ステップ 3 FXOS および/または FMC タスク：

a) FMC：クラスタメンバーの管理 （55 ページ）。

Firepower 4100/9300 シャーシのクラスタリングについて

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

- ネイティブインスタンスのクラスタリングの場合：ユニット間通信用のクラスタ制御リンク（デフォルトのポートチャネル 48）を作成します。

  マルチインスタンス クラスタリングの場合：1 つ以上のクラスタタイプの Etherchannel でサブインターフェイスを事前設定する必要があります。各インスタンスには、独自のクラスタ制御リンクが必要です。

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

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

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

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがシャーシ スーパバイザから各ユニットに対してプッシュされます。

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

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

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

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ブートストラップ コンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがFirepower 4100/9300 シャーシスーパバイザから各ユニットに対してプッシュされます。

クラスタ メンバー

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

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

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

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能を参照してください。

クラスタ制御リンク

ネイティブ インスタンス クラスタリングの場合：クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。

マルチインスタンス クラスタリングの場合：1 つ以上のクラスタタイプの EtherChannel でサブインターフェイスを事前設定する必要があります。各インスタンスには、独自のクラスタ制御リンクが必要です。

シャーシ間クラスタリングでは、このインターフェイスにメンバーインターフェイスはありません。このクラスタ タイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。 シャーシ間クラスタリングでは、EtherChannel に 1 つ以上のインターフェイスを追加する必要があります。

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

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

シャーシ間クラスタリングのクラスタ制御リンクのサイズ

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

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

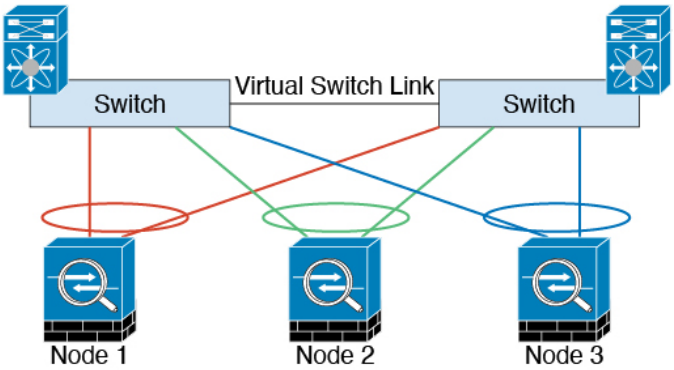
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

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

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

シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチングシステム（VSS）、仮想ポートチャネル（vPC）、StackWise、または StackWise Virtual 環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが冗長システムの一部である場合は、同じ EtherChannel 内のファイアウォールインターフェイスをそれぞれ、冗長システム内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット ID（127.2.*chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。通常、同じ EtherChannel の異なる VLAN サブインターフェイスを使用するマルチインスタンス クラスタの場合は、VLAN の分離によって異なるクラスタに同じ IP アドレスを使用できます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。

管理ネットワーク

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

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。この管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Secure Firewall Management Center にデバイスを設定し、登録するために使用されます。独自のローカル認証、IPアドレス、およびスタティック ルーティングを使用します。クラスタの各メンバーは、管理ネットワーク上で、それぞれに異なる IP アドレスを使用します。これらの IP アドレスは、ブートストラップ構成の一部としてユーザーが設定します。

管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。診断論理インターフェイスはオプションであり、ブートストラップ構成の一部としては設定されません。診断インターフェイスは、他のデータ インターフェイスと併せて設定できます。診断インターフェイスを設定する場合、メインクラスタ IP アドレスを、そのクラスタの固定アドレス（常に現在の制御ユニットに属するアドレス）として設定します。アドレス範囲も設定して、現在の制御ユニットを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、診断アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタへのアクセスをシームレスに続行できます。TFTPやsyslogなどの発信管理トラフィックの場合、制御ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバーに接続します。

クラスタ インターフェイス

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

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

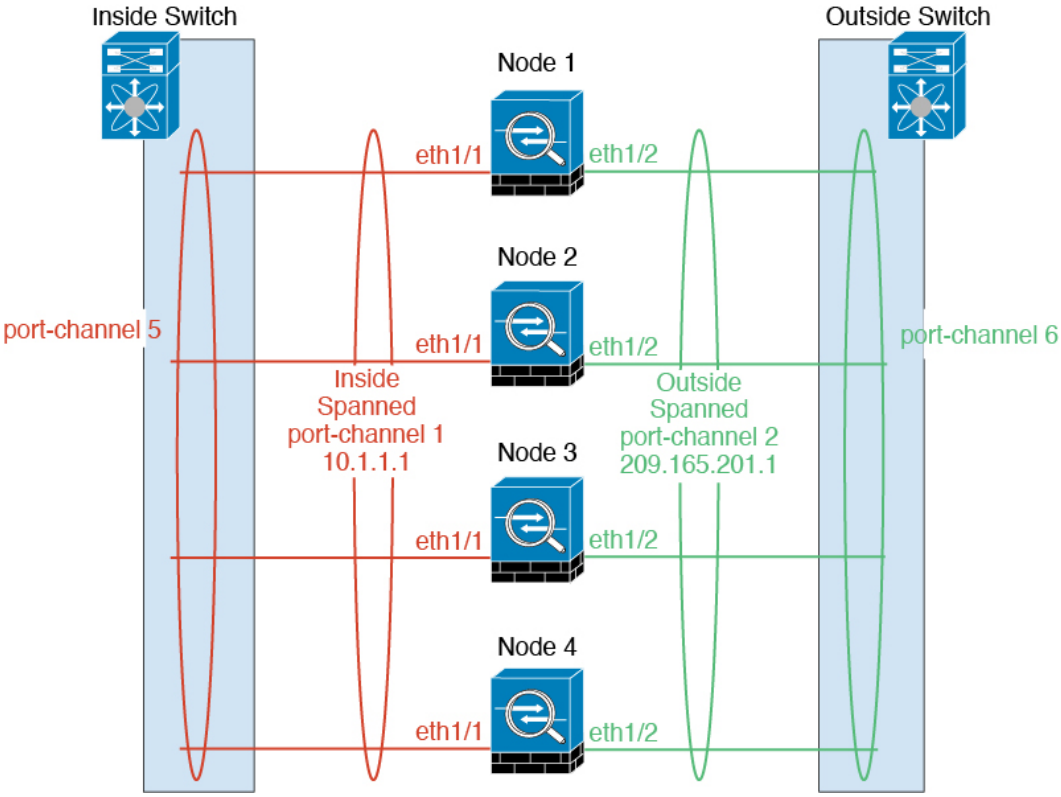
管理インターフェイス以外の個々のインターフェイスはサポートされていません。

スパンド EtherChannel

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

ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジ グループ メンバのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。

マルチインスタンスのクラスタの場合、各クラスタには専用データ Etherchannel が必要です。共有インターフェイスまたは VLAN サブインターフェイスを使用することはできません。



冗長スイッチシステムへの接続

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

コンフィギュレーションの複製

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

クラスタリングのライセンス

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

クラスタノードを 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。

クラスタリングの要件と前提条件

クラスタ モデルのサポート

Threat Defense は、次のモデルでのクラスタリングをサポートしています。

- Firepower 9300：。クラスタには最大 16 ユニットを含めることができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。シャーシ内クラスタリングとシャーシ間クラスタリングをサポートします。
- Firepower 4100：シャーシ間クラスタリングを使用して最大 16 ユニットをサポートします。

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

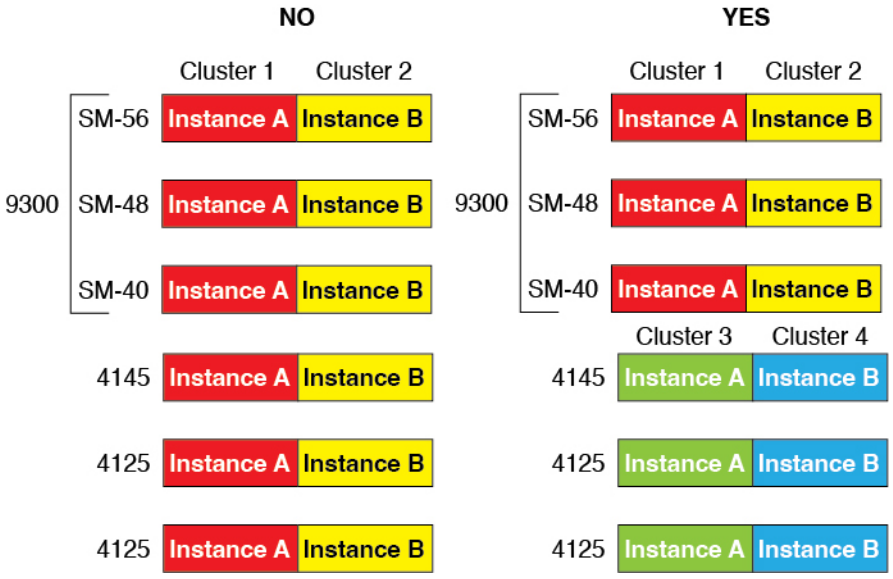
クラスタリングハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- ネイティブインスタンスのクラスタリング—Firepower 4100：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタ

イプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。各シャーシに異なる数のセキュリティ モジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。

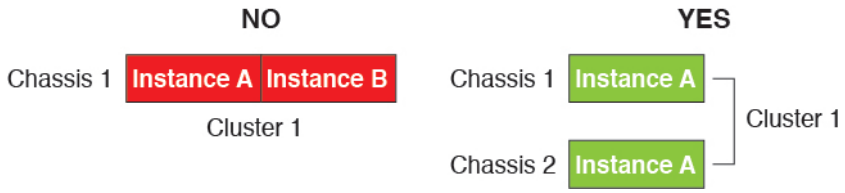
- コンテナインスタンスのクラスタリング—クラスタインスタンスごとに同じセキュリティ モジュールまたはシャーシモデルを使用することをお勧めします。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。



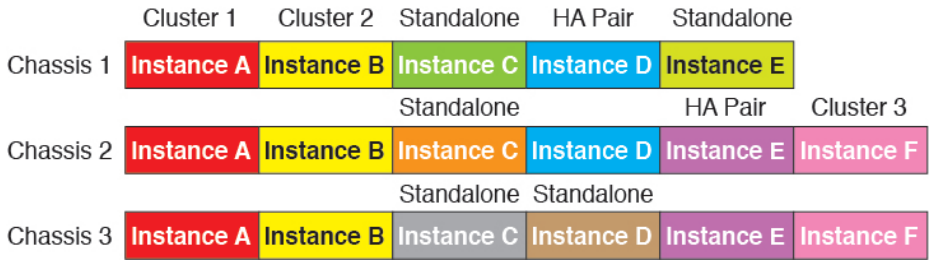
- イメージアップグレード時を除き、同じ FXOS およびアプリケーション ソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュール タイプを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイスモジュールの追加や削除、または EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データ ノードから始めて、制御ノードで終わります）。
- 同じ NTP サーバを使用する必要があります。Threat Defense では、Management Center も同じ NTP サーバーを使用する必要があります。時間を手動で設定しないでください。

マルチインスタンス クラスタリングの要件

- セキュリティモジュール/エンジン間クラスタリングなし：特定のクラスタでは、セキュリティモジュール/エンジンごとに 1 つのコンテナインスタンスのみを使用できます。同じモジュール上で実行されている場合、同じクラスタに 2 つのコンテナインスタンスを追加することはできません。



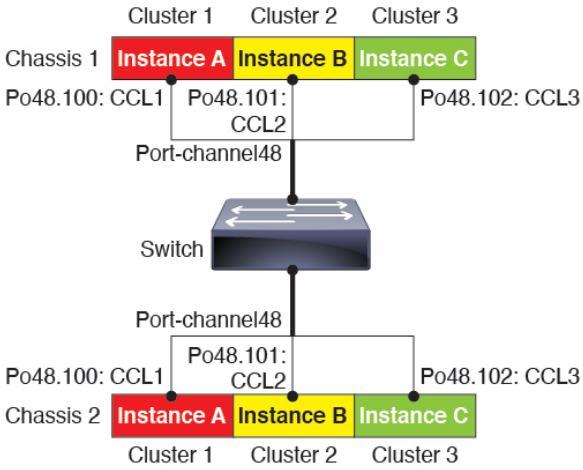
- クラスタとスタンドアロンインスタンスの混在：セキュリティモジュール/エンジン上のすべてのコンテナインスタンスがクラスタに属している必要はありません。一部のインスタンスをスタンドアロンノードまたは高可用性ノードとして使用できます。また、同じセキュリティモジュール/エンジン上で別々のインスタンスを使用して複数のクラスタを作成することもできます。



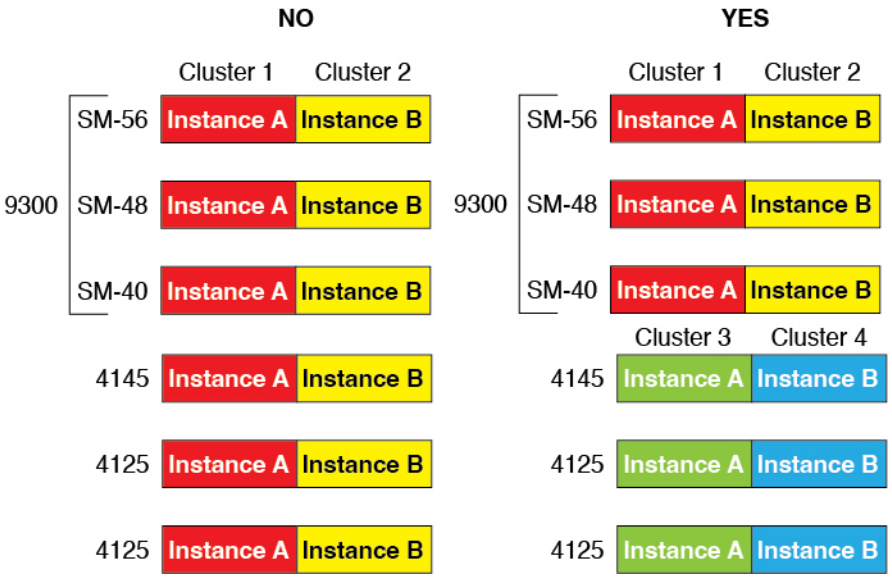
- Firepower 9300 の 3 つすべてのモジュールはクラスタに属している必要があります。Firepower 9300 の場合、クラスタには 3 つすべてのモジュールで 1 つのコンテナインスタンスが必要です。たとえば、モジュール 1 と 2 のインスタンスを使用してクラスタを作成し、モジュール 3 のネイティブインスタンスを使用することはできません。

- リソースプロファイルの一致：クラスタ内の各ノードで同じリソースプロファイル属性を使用することを推奨します。ただし、クラスタノードを別のリソースプロファイルに変更する場合、または異なるモデルを使用する場合は、リソースの不一致が許可されます。

- 専用クラスタ制御リンク：シャーシ間クラスタリングの場合、各クラスタには専用のクラスタ制御リンクが必要です。たとえば、各クラスタは、同じクラスタタイプの EtherChannel で個別のサブインターフェイスを使用したり、個別の EtherChannel を使用したりできます。



- 共有インターフェイスなし：共有タイプのインターフェイスは、クラスタリングではサポートされません。ただし、同じ管理インターフェイスとイベントインターフェイスを複数のクラスタで使用することはできます。
- サブインターフェイスなし：マルチインスタンスクラスタは、FXOS 定義の VLAN サブインターフェイスを使用できません。クラスタ制御リンクは例外で、クラスタ EtherChannel のサブインターフェイスを使用できます。
- シャーシモデルの混在：クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。



- 最大 6 ノード：クラスタ内では最大 6 つのコンテナインスタンスを使用できます。

シャーシ間クラスタリングのスイッチ要件

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

クラスタリング ガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンクインターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンクインターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS XR インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS XR *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリープロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい

L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。

- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

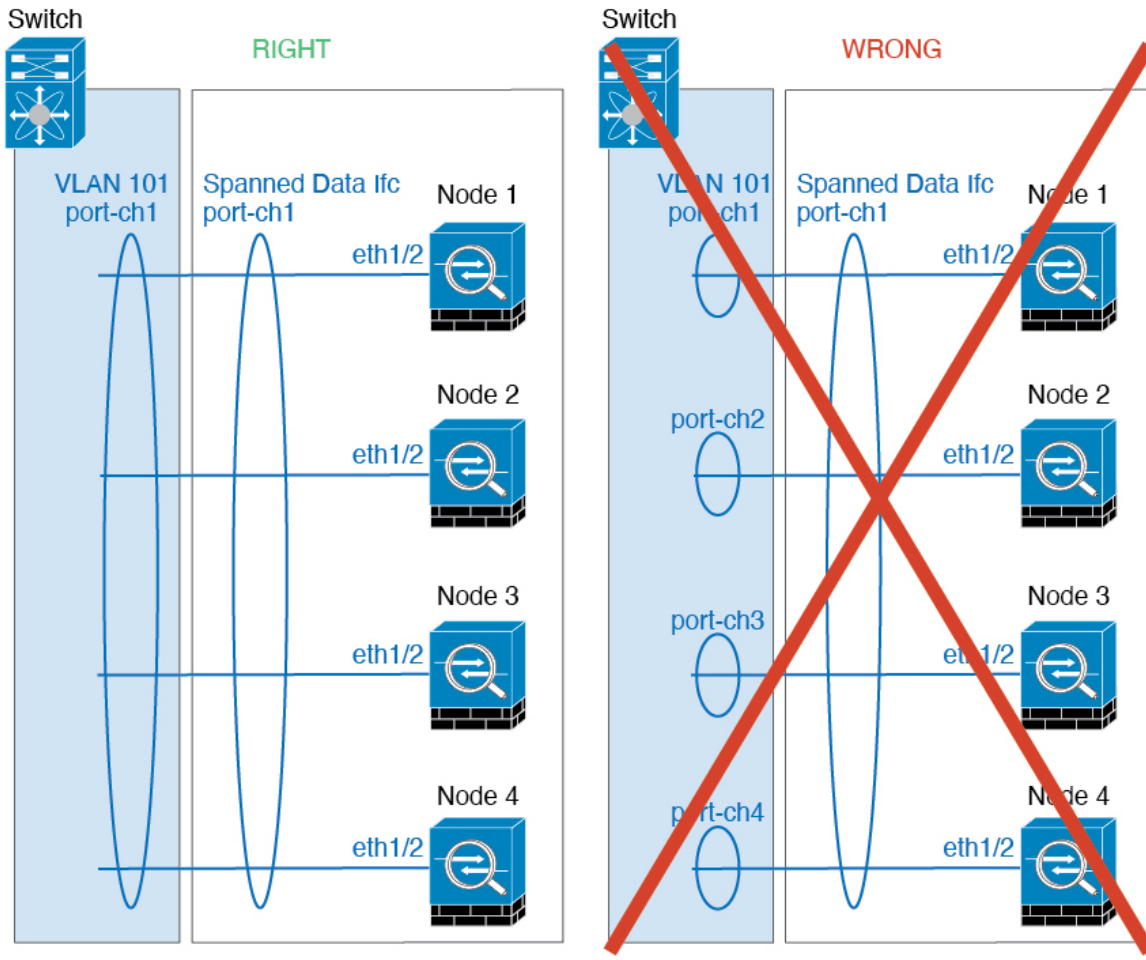
  router(config)# **port-channel** *id* **hash-distribution fixed**

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

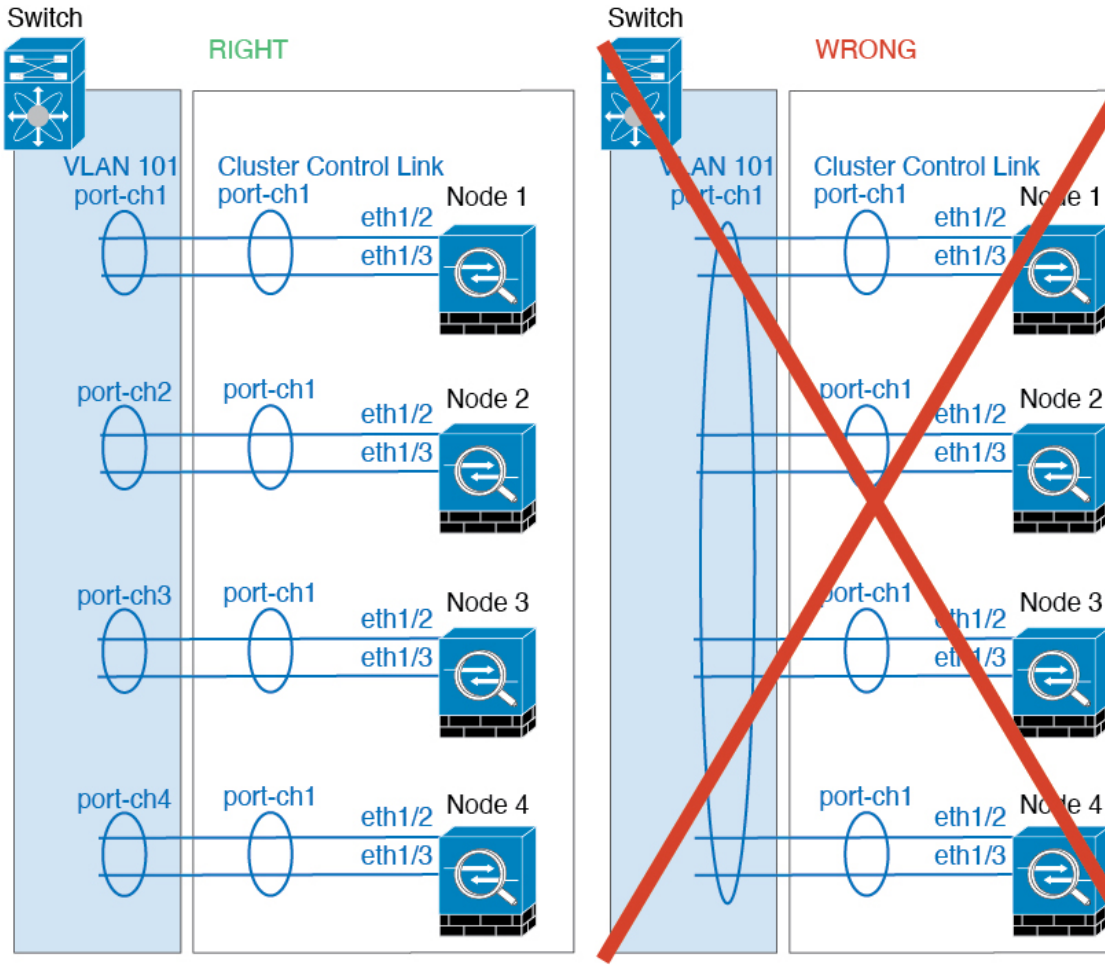
- Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサー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

シャーシ間クラスタリングの EtherChannel

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



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



その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannelインターフェイスの追加または削除、Firepower4100/9300シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS、vPC、StackWise、またはStackWise Virtualを形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制

しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。

- 冗長性を持たせるため、VSS、vPC、StackWise、または StackWise Virtual に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。
- 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。

デフォルト

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

クラスタリングの設定

クラスタは、Firepower 4100/9300 スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。その後、ユニットを Management Center に追加し、1 つのクラスタにグループ化できます。

FXOS：インターフェイスの設定

クラスタの場合は、次のタイプのインターフェイスを設定する必要があります。

- クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。EtherChannel（ポート チャネル）の追加（19 ページ）または物理インターフェイスの設定 （18 ページ）を参照してください。

  シャーシ間クラスタリングの場合は、すべてのデータインターフェイスが、少なくとも 1 つのメンバーインターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタユニットからメンバーインターフェイスを 1 つの EtherChannel へと結合します。 コンテナインスタン

スのデータインターフェイスでは、クラスタ内でVLANサブインターフェイスまたはデータ共有インターフェイスを使用できません。シャーシ間クラスタリングのEtherChannelについての詳細は、クラスタリング ガイドラインと制限事項 （12 ページ） を参照してください。

マルチインスタンス クラスタリングでは、クラスタ内でFXOS定義のVLANサブインターフェイスまたはデータ共有インターフェイスを使用できません。アプリケーション定義のサブインターフェイスのみがサポートされています。

- 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポート チャネル）の追加 （19 ページ）または物理インターフェイスの設定 （18 ページ）を参照してください。

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

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

  マルチインスタンスのクラスタリングでは、同じシャーシ上の複数のクラスタ、またはスタンドアロンインスタンスで同じ管理インターフェイスを共有できます。

- シャーシ間クラスタリングでは、メンバーインターフェイスをクラスタ制御リンクのEtherChannel（デフォルトではポートチャネル48）に追加します。マルチインスタンス クラスタリングの場合は、追加のクラスタタイプのEtherChannelを作成できます。EtherChannel （ポート チャネル）の追加 （19 ページ） を参照してください。

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

  [インターフェイス（Interfaces）] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバ インターフェイスが含まれていない場合は、[動作状態（Operation State）] を [失敗（failed）] と表示します。シャーシ内クラスタリングの場合、このEtherChannelはメンバインターフェイスを必要としないため、この動作状態は無視して構いません。

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

  マルチインスタンス クラスタリングの場合、管理インターフェイスとは異なり、クラスタ制御リンクを複数のデバイスで共有できないため、クラスタごとにクラスタインターフェイスが必要になります。ただし、複数の Etherchannel の代わりに VLAN サブインターフェイスを使用することを推奨します。クラスタインターフェイスにVLANサブインターフェイスを追加するには、次の手順を参照してください。

- マルチインスタンス クラスタリングの場合は、クラスタ EtherChannel に VLAN サブインターフェイスを追加します。コンテナ インスタンスの VLAN サブインターフェイスの追加 （22 ページ） を参照してください。

  クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。

- （オプション）Firepower イベントインターフェイスを追加します。EtherChannel（ポートチャネル）の追加 （19 ページ）または物理インターフェイスの設定 （18 ページ）を参照してください。

  このインターフェイスは、Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Firepower Threat Defense のコマンドリファレンスで **configure network** コマンドを参照してください。

  シャーシ間クラスタリングの場合、各シャーシに同じイベンティング インターフェイスを追加します。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

（注） QSFPH40G-CUxM の場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

ステップ 1 [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ページを開きます。

[**All Interfaces**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの行で[編集（Edit）] をクリックし、[インターフェイスを編集（Edit Interface）] ダイアログボックスを開きます。

ステップ 3 インターフェイスを有効にするには、[有効化（Enable）] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。

ステップ 4 インターフェイスの [タイプ（Type）] を選択します。

- **データ**
- [データ共有（Data-sharing）]：コンテナインスタンスのみ。
- **管理**
- [Firepower-eventing]：Threat Defense のみ。
- [クラスタ（Cluster）]：[クラスタ（Cluster）] タイプは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャネル 48 に自動的に作成されます。

ステップ 5 （任意） [速度（Speed）] ドロップダウンリストからインターフェイスの速度を選択します。

ステップ 6 （任意） インターフェイスで [自動ネゴシエーション（Auto Negotiation）] がサポートされている場合は、[はい（Yes）] または [いいえ（No）] オプション ボタンをクリックします。

ステップ 7 （任意） [Duplex] ドロップダウンリストからインターフェイスのデュプレックスを選択します。

ステップ 8 （任意） **デバウンス時間（ミリ秒）**を明示的に設定します。0 から 15000 ミリ秒の値を入力します。

ステップ 9 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。リンク集約制御プロトコル（LACP）では、2 つのネットワークデバイス間でリンク集約制御プロトコルデータユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データまたはデータ共有インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データ インターフェイスのみがアクティブ モードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止（Suspended）] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータ インターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止（Suspended）] または [ダウン（Down）] 状態に戻ります。

手順

ステップ 1 [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ページを開きます。

[**All Interfaces**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 インターフェイス テーブルの上にある [ポート チャネルの追加（Add Port Channel）] をクリックし、[ポート チャネルの追加（Add Port Channel）] ダイアログボックスを開きます。

ステップ 3 [ポート チャネル ID（Port Channel ID）] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、ポートチャネル 48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN

サブインターフェイスを追加できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。

ステップ 4 ポート チャネルを有効にするには、[有効化（Enable）] チェックボックスをオンにします。ポート チャネルをディセーブルにするには、**[Enable]**チェックボックスをオフにします。

ステップ 5 インターフェイスの [タイプ（Type）] を選択します。

- **データ**
- [データ共有（Data-sharing）]：コンテナインスタンスのみ。
- **管理**
- [Firepower-eventing]：Threat Defense のみ。
- **クラスタ**

ステップ 6 ドロップダウン リストでメンバーインターフェイスに適した [管理速度（Admin Speed）] を設定します。

指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。

ステップ 7 データまたはデータ共有インターフェイスに対して、LACP ポート チャネル [Mode]、[Active] または [On] を選択します。

非データまたはデータ共有インターフェイスの場合、モードは常にアクティブです。

ステップ 8 メンバーインターフェイスに適した [管理デュプレックス（Admin Duplex）] を設定します（[全二重（Full Duplex）] または [半二重（Half Duplex）]）。

指定したデュプックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。

ステップ 9 ポート チャネルにインターフェイスを追加するには、**[Available Interface]**リストでインターフェイスを選択し、**[Add Interface]**をクリックしてそのインターフェイスを [Member ID] リストに移動します。

同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があり、このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

ヒント 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、Ctrl キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、Shift キーを押しながら最後のインターフェイスをクリックして選択します。

ステップ 10 ポートチャネルからインターフェイスを削除するには、[Member ID]リストでそのインターフェイスの右側にある**[Delete]**ボタンをクリックします。

ステップ 11 [OK] をクリックします。

コンテナ インスタンスの VLAN サブインターフェイスの追加

ネットワーク配置に応じて、250 ～ 500 の VLAN サブインターフェイスをシャーシに追加できます。シャーシには最大 500 個のサブインターフェイスを追加できます。

マルチインスタンス クラスタリングの場合、クラスタタイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナ インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

本書では、*FXOS* VLAN サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。

手順

ステップ 1 **[Interfaces]** を選択して **[All Interfaces]** タブを開きます。

[All Interfaces] タブには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

ステップ 2 **[Add New** > **Subinterface]** をクリックして [Add Subinterface] ダイアログボックスを開きます。

ステップ 3 インターフェイスの [タイプ（Type）] を選択します。

- **データ**
- **データ共有**
- [クラスタ（Cluster）]：クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用できません。

データインターフェイスおよびデータ共有インターフェイスの場合：タイプは、親インターフェイスのタイプに依存しません。たとえば、データ共有の親とデータサブインターフェイスを設定できます。

ステップ 4 ドロップダウン リストから親**インターフェイス**を選択します。

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親イ

ンターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できます。

ステップ 5 [Subinterface ID] を 1 ～ 4294967295 で入力します。

この ID は、*interface_id.subinterface_id* のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

ステップ 6 1 ～ 4095 の間で [VLAN ID] を設定します。

ステップ 7 [OK] をクリックします。

親インターフェイスを展開し、その下にあるすべてのサブインターフェイスを表示します。

FXOS：コンテナインスタンスにリソースプロファイルを追加

コンテナインスタンスごとにリソース使用率を指定するには、1つまたは複数のリソースプロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

- コアの最小数は 6 です。

（注） コア数が少ないインスタンスは、コア数が多いインスタンスよりも、CPU使用率が比較的高くなる場合があります。コア数が少ないインスタンスは、トラフィック負荷の変化の影響を受けやすくなります。トラフィックのドロップが発生した場合には、より多くのコアを割り当ててください。

- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、セキュリティモジュール/シャーシモデルによって異なります。「」を参照してください。

シャーシには、「Default-Small」と呼ばれるデフォルトリソースプロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

使用中のリソースプロファイルの設定を変更することはできません。そのリソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。確立されたハイ アベイラビリティ ペ

アまたはクラスタ内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

Threat Defense インスタンスを Management Center に追加した後にリソースプロファイルの設定を変更する場合は、Management Center の [デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [システム（System）] > [インベントリ（Inventory）] ダイアログボックスで各ユニットのインベントリを更新します。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [リソースプロファイル（Resource Profiles）]** を選択し、[追加（Add）] をクリックします。

[リソースプロファイルの追加（Add Resource Profile）] ダイアログボックスが表示されます。

ステップ 2 次のパラメータを設定します。

- [名前（Name）]：プロファイルの名前を 1 ～ 64 文字で設定します。追加後にこのプロファイルの名前を変更することはできません。
- [説明（Description）]：プロファイルの説明を最大 510 文字で設定します。
- [コア数（Number of Cores）]：プロファイルのコア数を 6 ～ 最大数（偶数）で設定します。最大数はシャーシによって異なります。

ステップ 3 [OK] をクリックします。

FXOS：Threat Defense クラスタの追加

ネイティブモード：単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。

マルチインスタンスモード：シャーシ内クラスタとして単一の Firepower 9300 シャーシに 1 つまたは複数のクラスタを追加できます（各モジュールにインスタンスを含める必要があります）。または、シャーシ間クラスタリングのために複数のシャーシに 1 つ以上のクラスタを追加できます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

Threat Defense クラスタの作成

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

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

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3 つのすべてのモジュール、またはコンテナインスタンス、各スロットの 1 つのコンテナインスタンスでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。
- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、FXOS：コンテナインスタンスにリソースプロファイルを追加 （23 ページ）に従ってリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティ モジュール/エンジン を再度初期化する必要があります。[Security Modules] または [Security Engine] を選択して、[再初期化（Reinitialize）] アイコン（  ）をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレス、およびネットワークマスク
  - ゲートウェイ IP アドレス
  - Management Center 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス
  - Threat Defense ホスト名とドメイン名

手順

ステップ 1 インターフェイスを設定します。 FXOS：インターフェイスの設定を参照してください。

ステップ 2 [論理デバイス（Logical Devices）] を選択します。

ステップ 3 **[追加（Add）] > [クラスタ（Cluster）]** をクリックし、次のパラメータを設定します。

図 *1*: ネイティブクラスタ

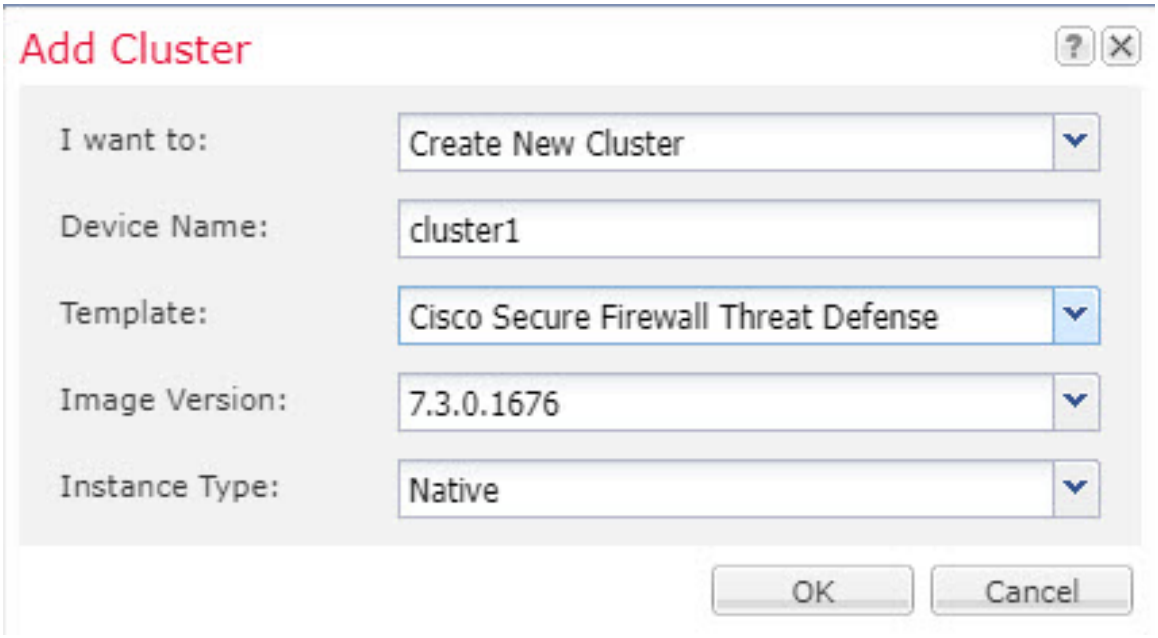
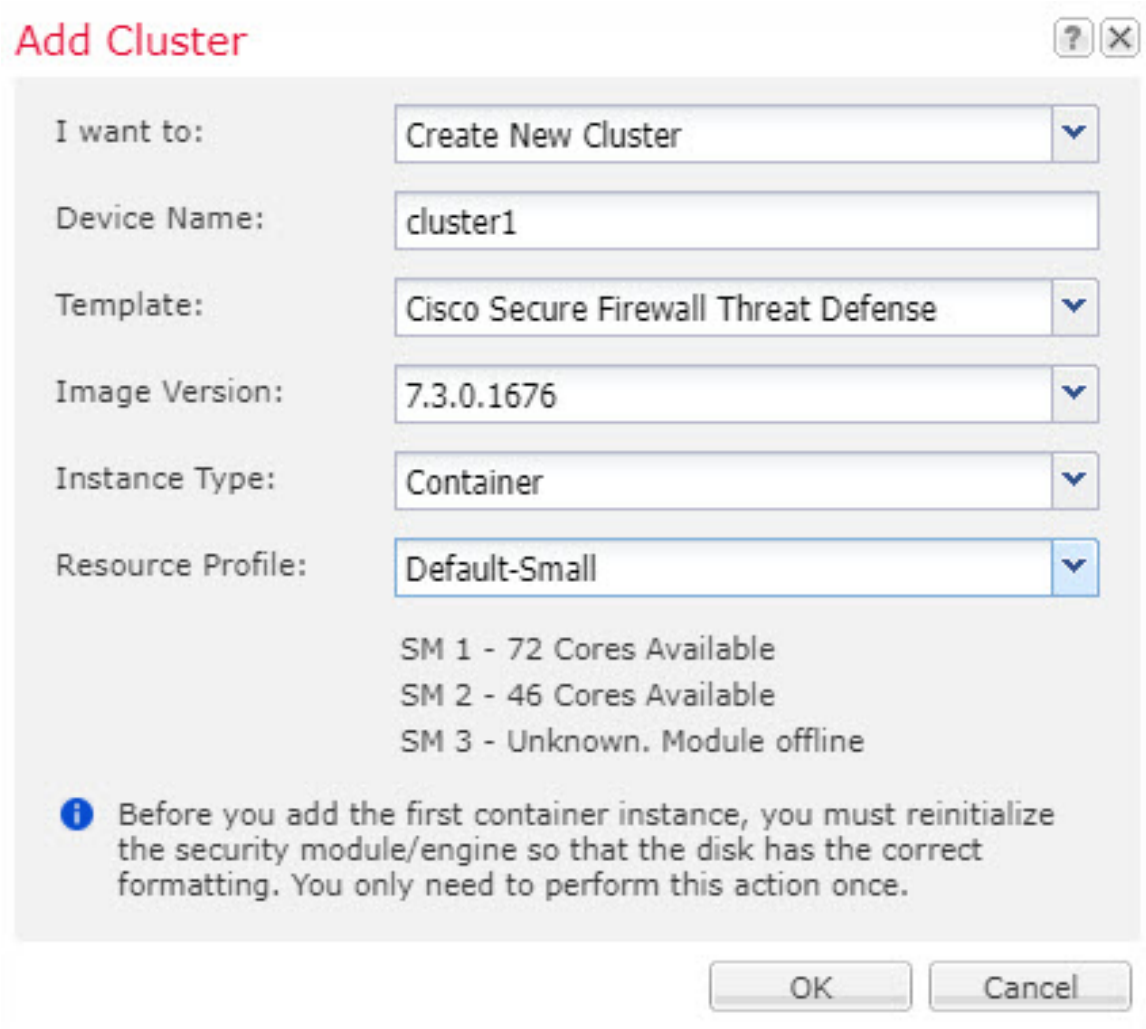


図 *2:* マルチインスタンスクラスタ



a) **[必要な操作（I want to:）] > [新しいクラスタの作成（Create New Cluster）]** を選択します。

b) **デバイス名**を入力します。

この名前は、シャーシスーパバイザが管理設定を行ってインターフェイスを割り当てるために内部で使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

c) [Template] では、[Cisco Firepower Threat Defense] を選択します。

d) [Image Version] を選択します。

e) [Instance Type] の場合、[Native] または [Container] を選択します。

ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブインスタンスを 1 つだけインストールできます。コンテナインスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

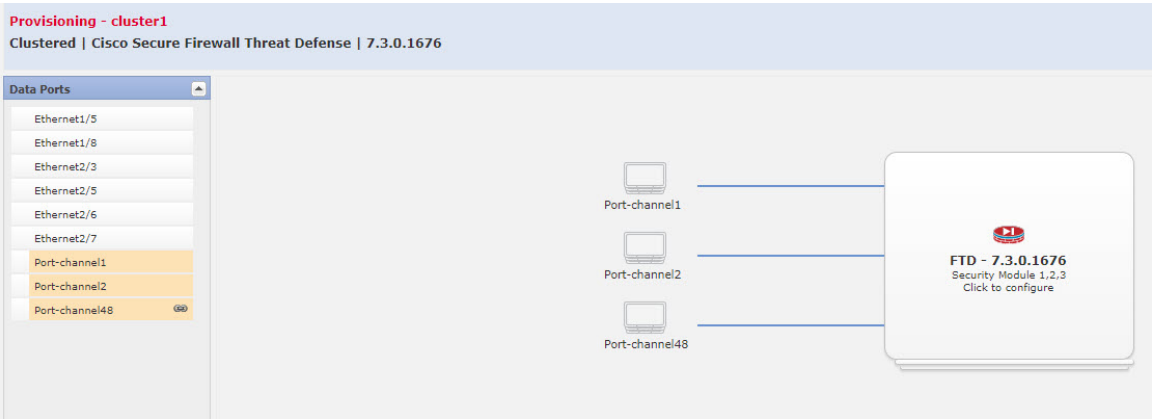
f) （コンテナインスタンスのみ）[リソースタイプ（Resource Type）] で、ドロップダウンリストからいずれかのリソースプロファイルを選択します。

Firepower 9300 の場合、このプロファイルは各セキュリティモジュールの各インスタンスに適用されます。この手順の後半では、セキュリティモジュールごとに異なるプロファイルを設定できます。たとえば、異なるセキュリティモジュールのタイプを使用していて、ローエンドのモデルでより多くの CPU を使用する場合に設定できます。クラスタを作成する前に、正しいプロファイルを選択することを推奨します。新しいプロファイルを作成する必要がある場合は、クラスタの作成をキャンセルし、FXOS：コンテナインスタンスにリソースプロファイルを追加 （23 ページ） を使用して 1 つ追加します。

g) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 4 このクラスタに割り当てるインターフェイスを選択します。



ネイティブモードのクラスタリングの場合：デフォルトでは、すべての有効なインターフェイスが割り当てられます。マルチクラスタタイプのインターフェイスを定義した場合は、すべての選択を解除し、1 つのみ選択します。

マルチインスタンス クラスタリングの場合：クラスタに割り当てる各データインターフェイスを選択し、クラスタタイプのポートチャネルまたはポートチャネルのサブインターフェイスも選択します。

ステップ 5 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 6 [クラスタ情報（Cluster Information）] ページで、次の手順を実行します。

図 *3* : ネイティブクラスタ

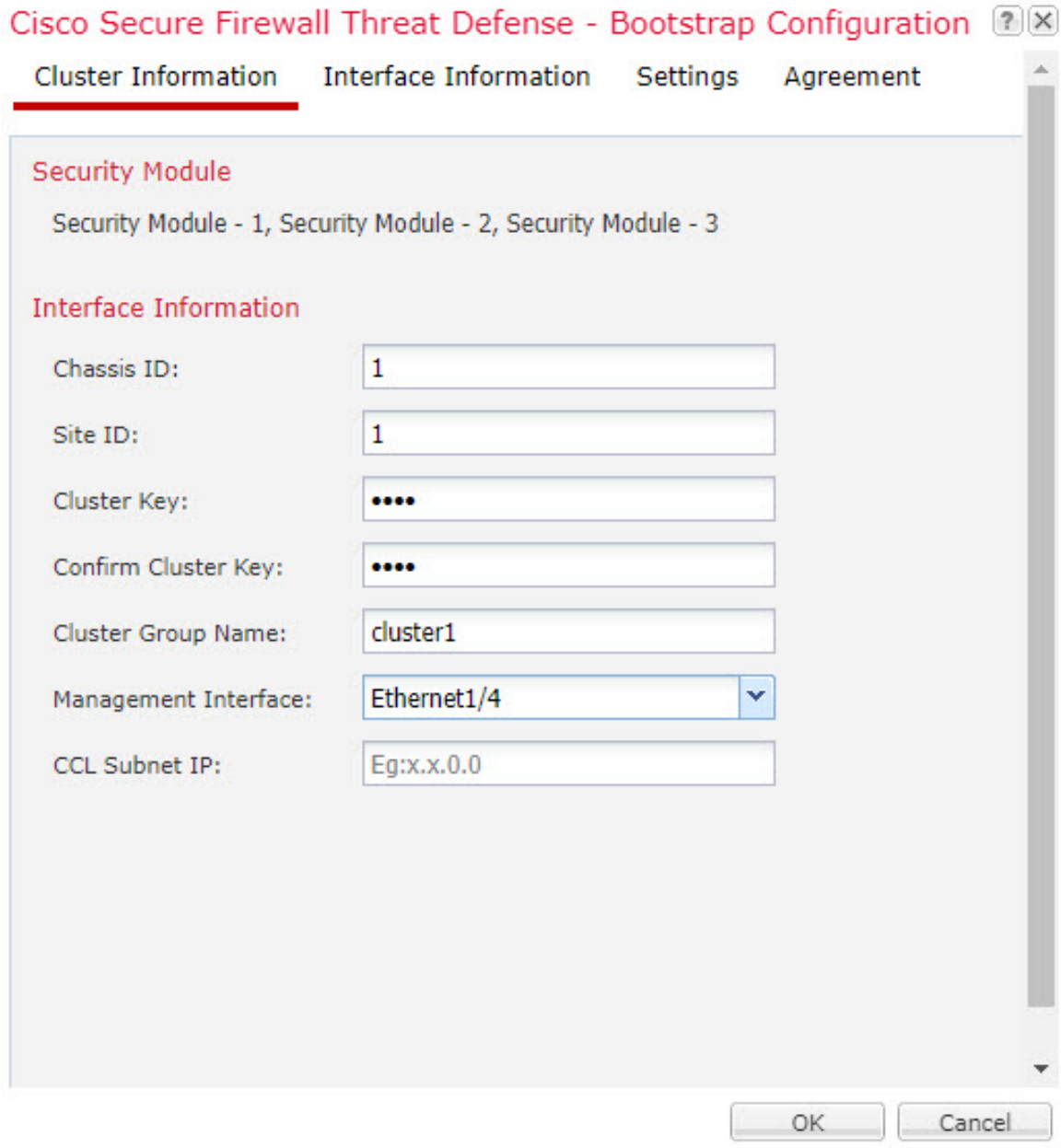
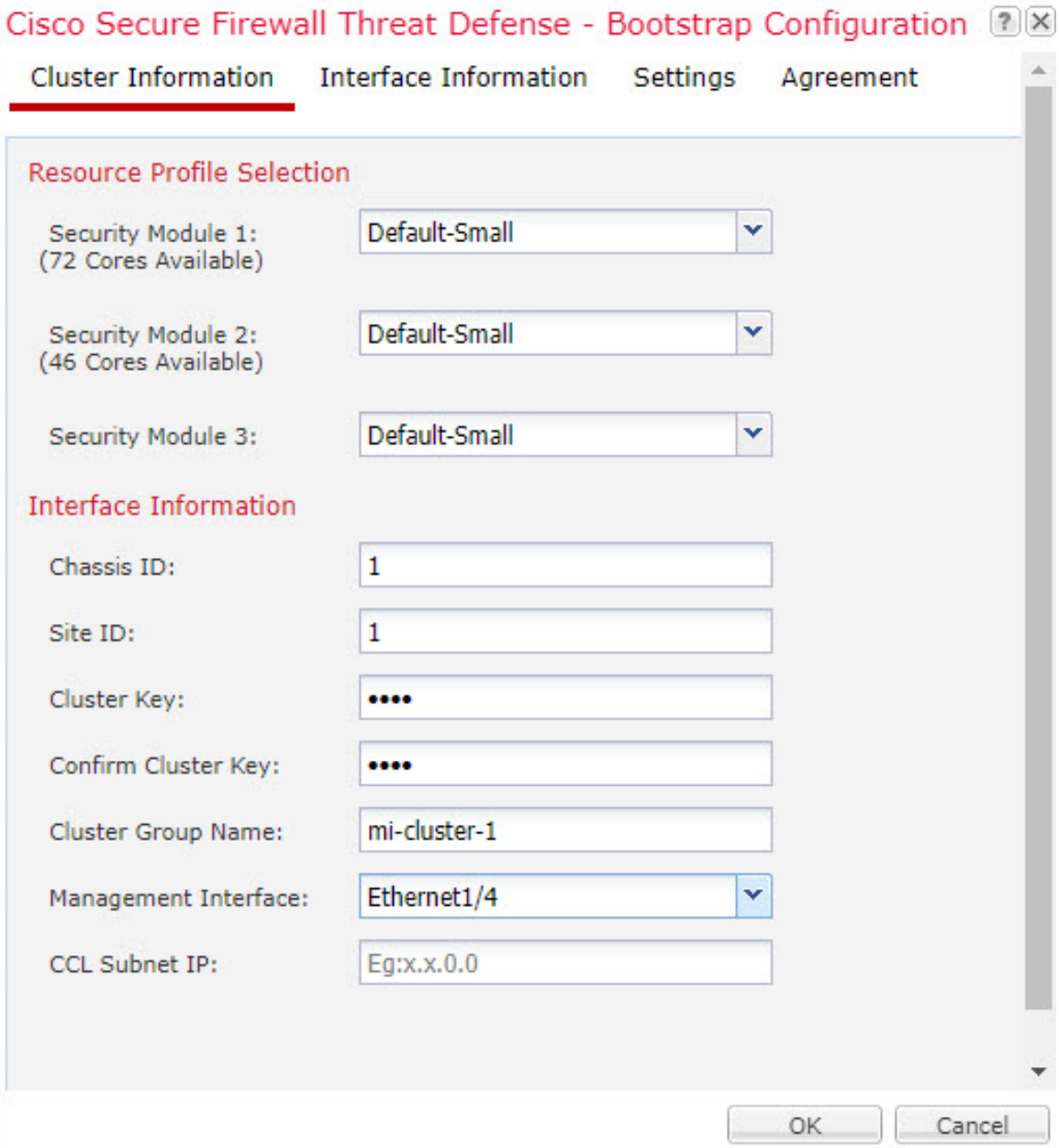


図 *4:* マルチインスタンスクラスタ



a) （Firepower 9300 のコンテナインスタンスのみ）[セキュリティモジュール（SM）とリソースプロファイルの選択（Security Module (SM) and Resource Profile Selection）] エリアで、モジュールごとに異なるリソースプロファイルを設定できます。たとえば、異なるセキュリティモジュールのタイプを使用していて、ローエンドのモデルでより多くの CPU を使用する場合に設定できます。

b) シャーシ間クラスタリングでは、**シャーシ ID** フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバー インターフェイスを追加した場合にのみ表示されます。

c) サイト間クラスタリングの場合、[サイト ID（Site ID）] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。FlexConfig 機能。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、Management Center FlexConfig 機能を使用した場合にのみ設定できます。

d) [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

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

e) [クラスタ グループ名（Cluster Group Name）] を設定します。これは、論理デバイス設定のクラスタ グループ名です。

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

f) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

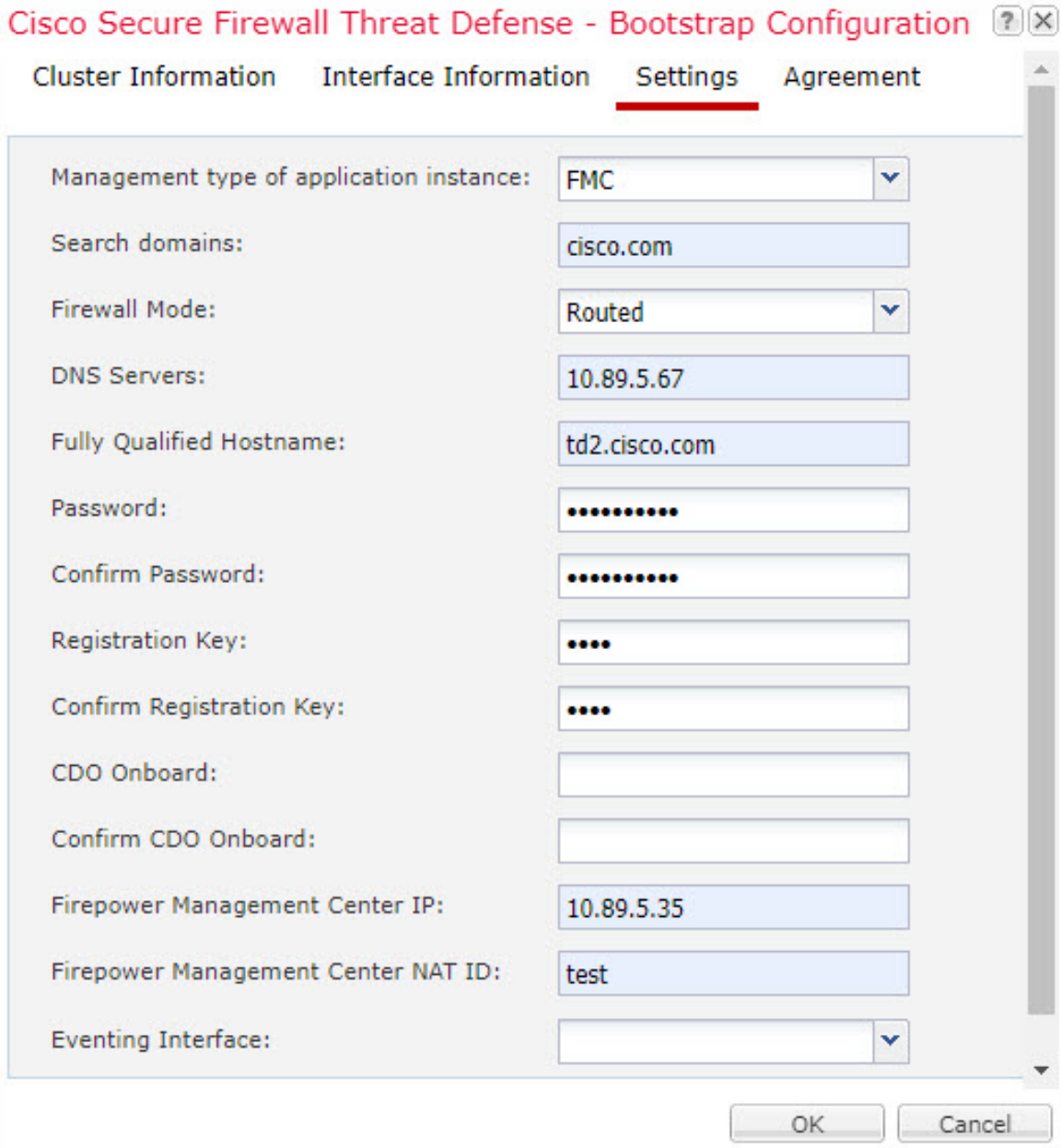
ハードウェア バイパス 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

g) （任意） **CCL サブネット IP** を ***a.b*.0.0** に設定します。

クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。この場合、クラスタの固有ネットワークに任意の/16 ネットワークアドレスを指定します（ループバック（127.0.0.0/8）、マルチキャスト（224.0.0.0/4）、内部（169.254.0.0/16）のアドレスを除く）。値を 0.0.0.0 に設定すると、デフォルトのネットワークが使用されます。

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

ステップ 7 [**設定（Settings**）] ページで、以下を実行します。



a) [登録キー（Registration Key）] フィールドに、登録時に Management Center とクラスタメンバー間で共有するキーを入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。Threat Defense を追加するときに、Management Center に同じキーを入力します。

b) CLI アクセス用の Threat Defense 管理ユーザの [Password] を入力します。

c) [Firepower Management CenterのIP（Firepower Management Center IP）] フィールドに、管理側の Management Center の IP アドレスを入力します。Management Center の IP アドレ

スがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

d) （任意） **FTD SSH セッションからエキスパート モード**、[**Yes**]、または [**No**] を許可します。エキスパート モードでは、高度なトラブルシューティングに Threat Defense シェルからアクセスできます。

このオプションで [Yes] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[いいえ（No）] を選択した場合、FXOS CLI からコンテナインスタンスにアクセスするユーザーのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、Threat Defense CLI で **expert** コマンドを使用します。

e) （任意） [Search Domains] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。

f) （任意） [ファイアウォール モード（Firewall Mode）] ドロップダウン リストから、[トランスペアレント（Transparent）] または [ルーテッド（Routed）] を選択します。

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

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

g) （任意） [**DNSサーバ（DNS Servers**）] フィールドに、DNS サーバのカンマ区切りのリストを入力します。

たとえば、Management Centerのホスト名を指定する場合、Threat Defenseは DNS を使用します。

h) （任意） [Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。このパスフレーズは、新しいデバイスとしてクラスタを追加するときに Management Center でも入力します。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。Management Center がデバイスの IP アドレスを指定し、デバイスが Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。NAT ID として、1 ~ 37 文字の任意のテキスト文字列を指定できます。Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

i) （任意） [Fully Qualified Hostname] フィールドに、Threat Defense デバイスの完全修飾名を入力します。

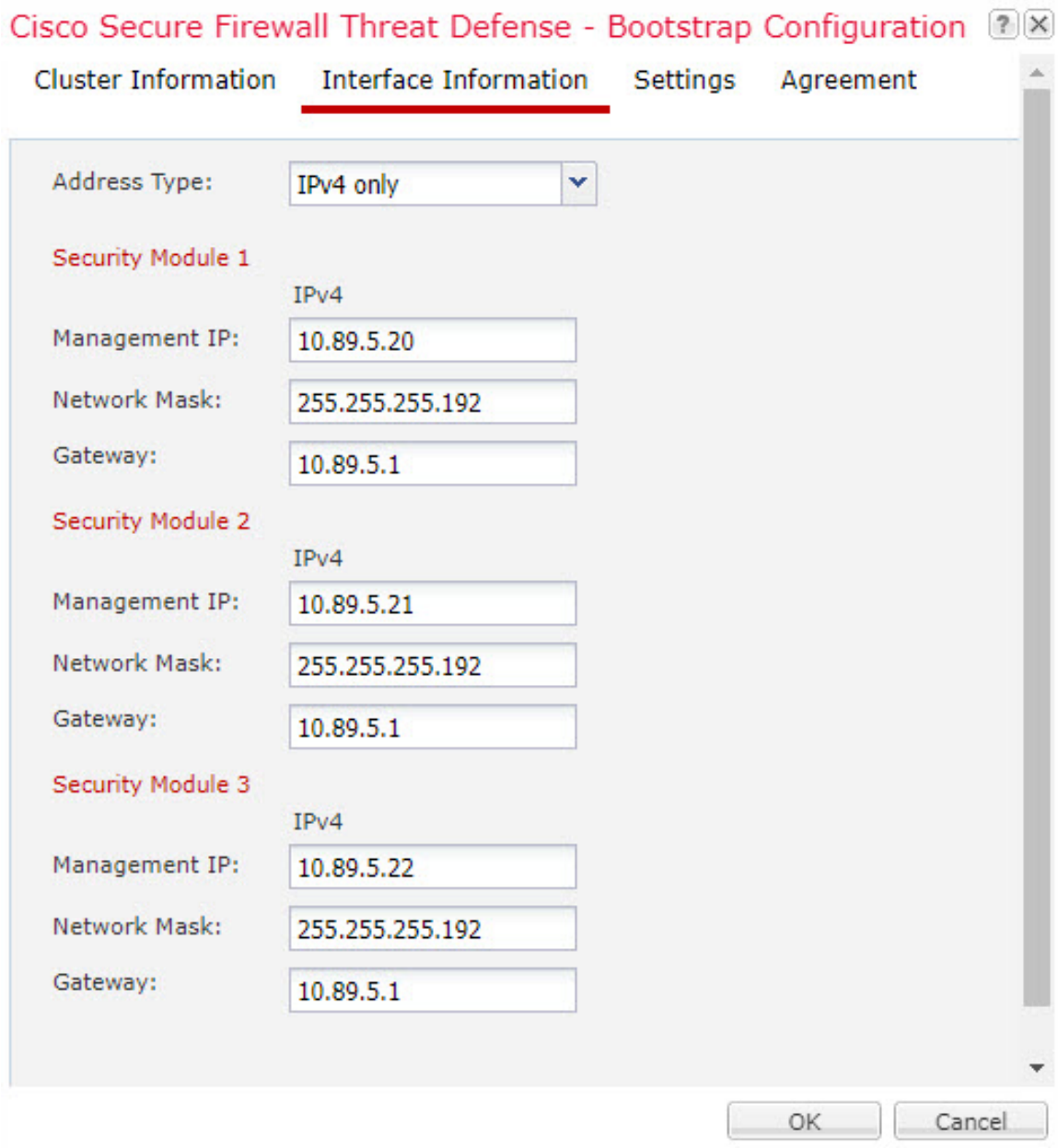
有効な文字は、a ー z の文字、0 ー 9 の数字、ドット（.）、ハイフン（-）です。最大文字数は 253 です。

j) （任意） [イベンティングインターフェイス（Eventing Interface）] ドロップダウンリストから、イベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

イベントに使用する別のインターフェイスを指定するには、*firepower-eventing* インターフェイスとしてインターフェイスを設定する必要があります。ハードウェアバイパス対応のインターフェイスを Eventing インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

ステップ 8 [インターフェイス情報（Interface Information）]ページで、クラスタ内のセキュリティモジュールのそれぞれに管理 IP アドレスを設定します。[アドレス タイプ（Address Type）] ドロップダウン リストからアドレスのタイプを選択し、セキュリティ モジュールごとに次の手順を実行します。

（注） モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットで IP アドレスを設定する必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。



a) [Management IP] フィールドで、IP アドレスを設定します。

モジュールごとに同じネットワーク上の一意の IP アドレスを指定します。

b) [Network Mask] または [Prefix Length] に入力します。

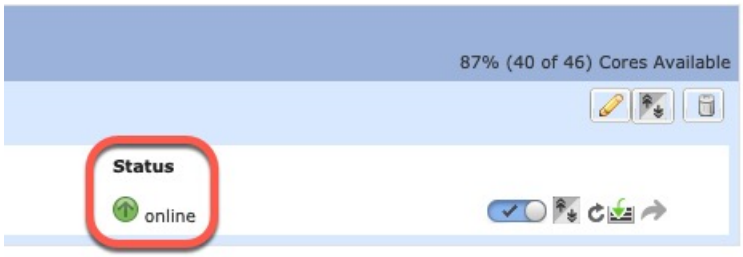
c) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 9 [利用規約（Agreement）] タブで、エンドユーザ ライセンス（EULA）を読んで、同意します。

ステップ 10 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 11 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されている場合、残りのクラスタシャーシを追加するか、シャーシ内クラスタリングでアプリケーションのクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 12 シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

a) Chassis Manager の最初のシャーシで、右上の [設定の表示（Show Configuration）] アイコンをクリックして、表示されるクラスタ設定をコピーします。

b) 次のシャーシの Chassis Manager に接続し、この手順に従って論理デバイスを追加します。

c) [必要な操作（I want to:）] > [既存のクラスタへの参加（Join an Existing Cluster）] を選択します。

d) **[OK]** をクリックします。

e) [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

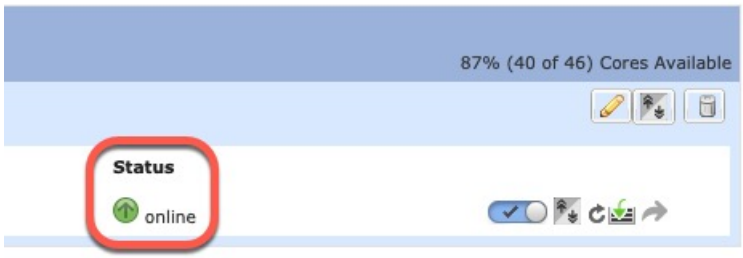
- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、Management Center FlexConfig 機能を使用した場合にのみ設定できます。
- [クラスタ キー（Cluster Key）]：（事前に入力されていない）同じクラスタ キーを入力します。

- [管理IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

g) [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバーの [論理デバイス（Logical Devices）] ページで、新しい論理デバイスのステータスを確認します。各クラスタメンバーの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 13 管理 IP アドレスを使用して、Management Center に制御ユニットを追加します。

すべてのクラスタ ユニットは、Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

Management Center がデータユニットを自動的に検出します。

クラスタノードの追加

既存のクラスタ内の Threat Defense クラスタノードを追加または交換します。FXOS に新しいクラスタノードを追加すると、Management Center によりノードが自動的に追加されます。

（注） このプロシージャにおけるFXOSの手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。

始める前に

- 置き換える場合は、Management Center から古いクラスタノードを削除する必要があります。新しいノードに置き換えると、Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

手順

ステップ 1 以前に Management Center を使用して Threat Defense イメージをアップグレードした場合は、クラスタ内の各シャーシで次の手順を実行します。

Management Center からアップグレードしたときに、FXOS 設定のスタートアップバージョンが更新されておらず、スタンドアロンパッケージがシャーシにインストールされていませんでした。新しいノードが正しいイメージバージョンを使用してクラスタに参加できるように、これらの項目は両方とも手動で設定する必要があります。

（注） パッチリリースのみを適用した場合は、この手順をスキップできます。シスコではパッチ用のスタンドアロンパッケージを提供していません。

a) **[システム（System）]** > **[更新（Updates）]**ページを使用して、実行中の Threat Defense イメージをシャーシにインストールします。

b) [論理デバイス（Logical Devices）] をクリックし、[バージョンの設定（Set Version）] アイコン（ ） をクリックします。複数のモジュールを備えた Firepower 9300 の場合、各モジュールのバージョンを設定します。

[スタートアップバージョン（Startup Version）] には、展開した元のパッケージが表示されます。[現在のバージョン（Current Version）] には、アップグレード後のバージョンが表示されます。

c) [新しいバージョン（New Version）] ドロップダウンメニューで、アップロードしたバージョンを選択します。このバージョンは、表示されている [現在のバージョン（Current Version）] と一致する必要があり、スタートアップバージョンが新しいバージョンと一致するように設定されます。

d) 新しいシャーシに、新しいイメージパッケージがインストールされていることを確認します。

ステップ 2 既存のクラスタシャーシ Chassis Manager で、[論理デバイス（Logical Devices）] をクリックします。

ステップ 3 右上の [設定の表示（Show Configuration）] アイコンをクリックし、表示されるクラスタ設定をコピーします。

ステップ 4 新しいシャーシの Chassis Manager に接続して、**[追加（Add）]** > **[クラスタ（Cluster）]** をクリックします。

ステップ 5 [デバイス名（Device Name）] に論理デバイスの名前を入力します。

ステップ 6 **[OK]** をクリックします。

ステップ 7 [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

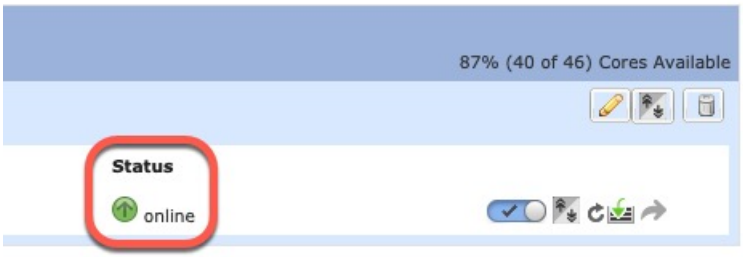
ステップ 8 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。この機能は、Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- [クラスタ キー（Cluster Key）]：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理 IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバーの [論理デバイス（Logical Devices）] ページで、新しい論理デバイスのステータスを確認します。各クラスタメンバーの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



Management Center：クラスタの追加

クラスタ ユニットのいずれかを新しいデバイスとして Secure Firewall Management Center に追加します。Management Center は、他のすべてのクラスタ メンバーを自動検出します。

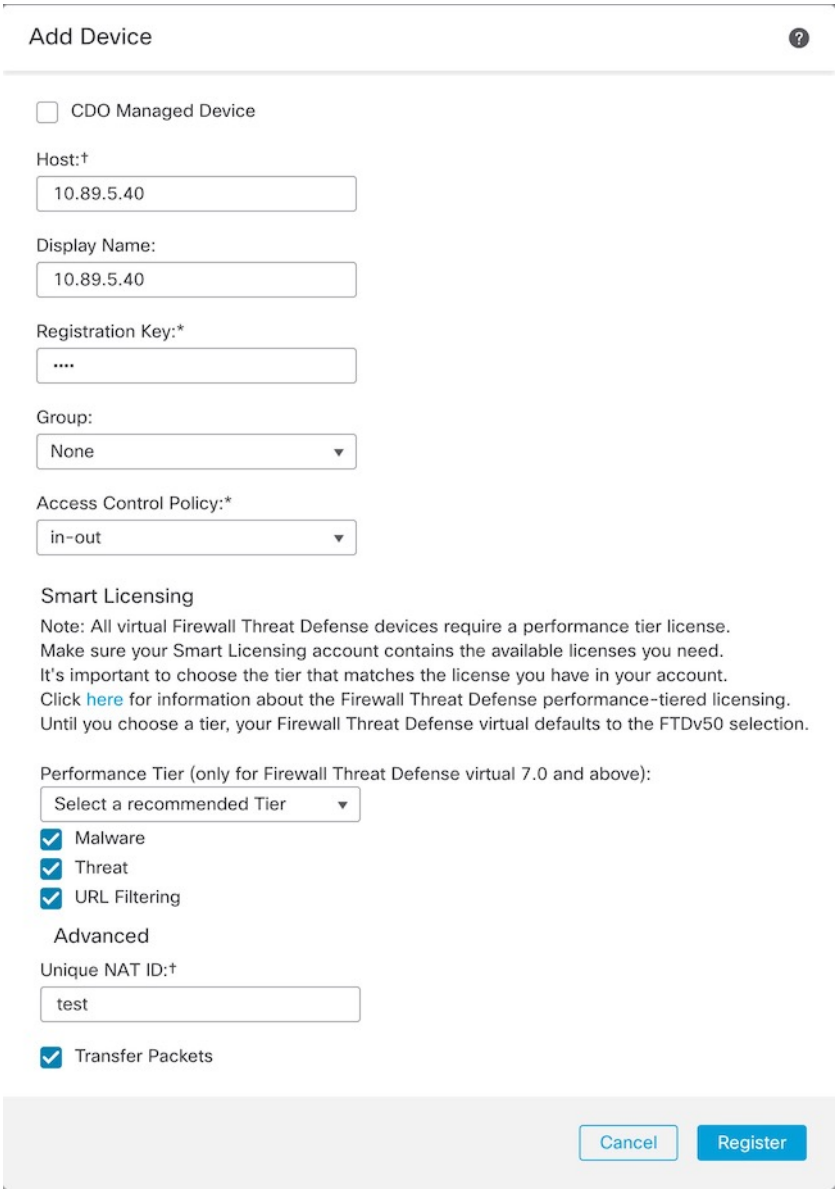
始める前に

- クラスタを追加するためのこの方法には、Threat Defense バージョン 6.2 以降が必要です。以前のバージョンのデバイスを管理する必要がある場合には、そのバージョンの Firepower Management Center コンフィギュレーション ガイドを参照してください。
- すべてのクラスタユニットは、Management Center に追加する前に、FXOS 上にある正常な形式のクラスタ内に存在している必要があります。また、どのユニットが制御ユニットかを確認することも必要です。Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、Threat Defense の **show cluster info** コマンドを使用します。

手順

ステップ 1 Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択してから、**[追加（Add）]** > **[デバイスの追加（Add Device）]** を選択し、クラスタを展開したときに割り当てた制御ユニットの管理 IP アドレスを使用して制御ユニットを追加します。

図 *5 :* デバイスの追加



a) [ホスト（Host）] フィールドに、制御ユニットの IP アドレスまたはホスト名を入力します。

最適なパフォーマンスを得るため、制御ユニットの追加を推奨しますが、クラスタの任意のユニットを追加できます。

デバイスのセットアップ時に NAT ID を使用した場合は、このフィールドを入力する必要がない可能性があります。

b) [表示名（Display Name）] フィールドに、Management Center での制御ユニットの表示名を入力します。

この表示名はクラスタ用ではありません。追加する制御ユニット専用です。後で、他のクラスタメンバーの名前やクラスタ表示名を変更できます。

c) [登録キー（Registration Key）] フィールドに、FXOS にクラスタを展開したときに使用したものと同じ登録キーを入力します。登録キーは、1 回限り使用可能な共有シークレットです。

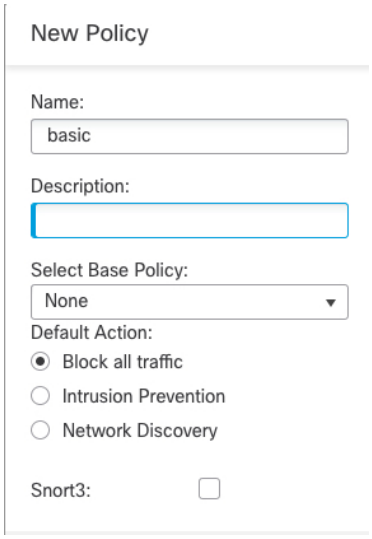
d) マルチドメイン展開では、現在のドメインに関係なく、デバイスをリーフ ドメインに割り当てます。

現在のドメインがリーフ ドメインである場合、デバイスは自動的に現在のドメインに追加されます。現在のドメインがリーフ ドメインでない場合、登録後、デバイスを設定するために、リーフ ドメインに切り替える必要があります。

e) （任意） デバイスをデバイス**グループ**に追加します。

f) 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

新しいポリシーを作成する場合は、基本ポリシーのみを作成します。必要に応じて、後でポリシーをカスタマイズできます。



g) デバイスに適用するライセンスを選択します。

h) デバイスの設定時に、NAT ID を使用した場合、[詳細（Advanced）] セクションを展開し、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

i) [パケットの転送（Transfer Packets）] チェックボックスをオンにし、デバイスで Management Center にパケットを転送することを許可します。

このオプションは、デフォルトで有効です。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベント メタデータ情報とパケット データを Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Management Center に送信され、パケット データは送信されません。

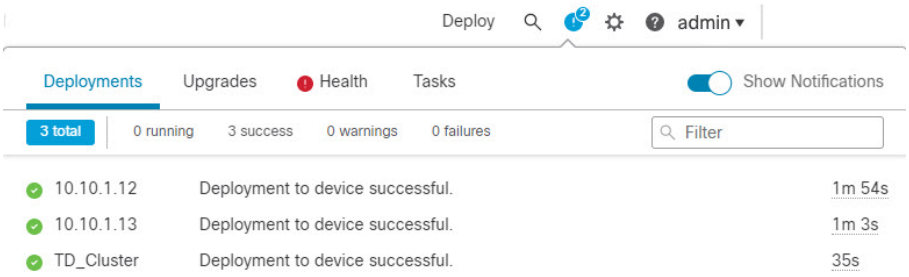
j) [登録（Register）] をクリックします。

Management Center は、制御ユニットを識別して登録した後に、すべてのデータユニットを登録します。制御ユニットが正常に登録されていない場合、クラスタは追加されません。クラスタがシャーシで稼働状態になかったか、その他の接続問題が原因で、登録エラーが発生する場合があります。こうした状況では、クラスタユニットを再度追加することをお勧めします。

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

現在登録されているユニットには、ロード アイコンが表示されます。

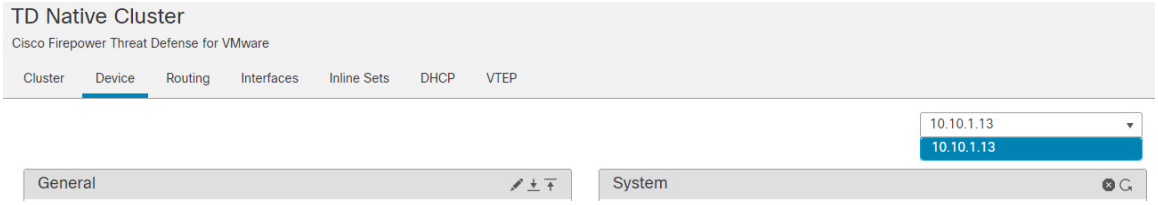
クラスタユニットの登録をモニターするには、[通知（Notifications）] アイコンをクリックし、[タスク（Tasks）] を選択します。Management Center は、ユニットの登録ごとにクラスタ登録タスクを更新します。いずれかのユニットの登録に失敗した場合には、クラスタ メンバーの照合 （61 ページ） を参照してください。



ステップ 2 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。

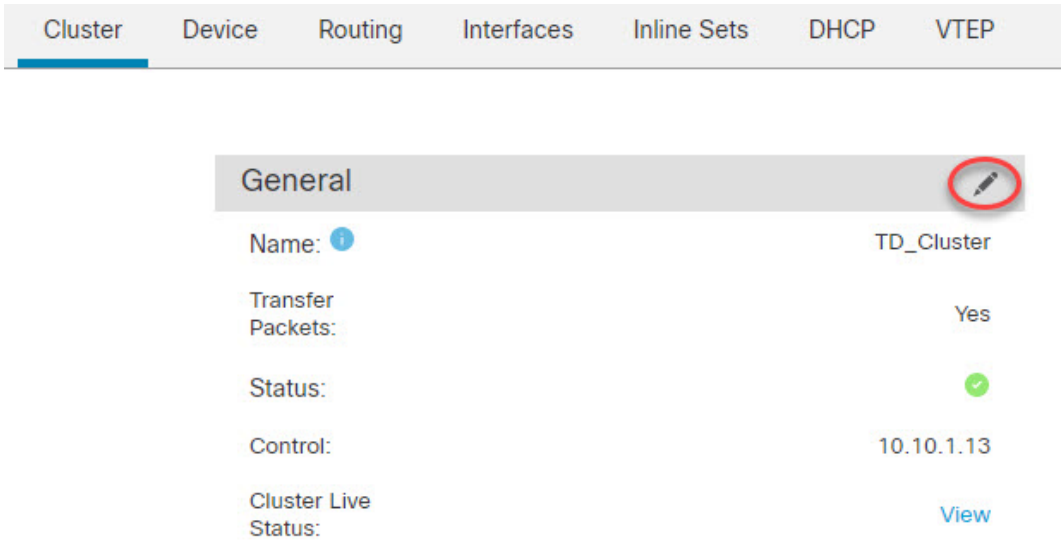
ほとんどの設定は、クラスタ内のメンバーユニットではなくクラスタ全体に適用できます。たとえば、ユニットごとに表示名を変更できますが、インターフェイスはクラスタ全体についてのみ設定できます。

ステップ 3 **[デバイス（Devices）]>[デバイス管理（Device Management）]>[クラスタ（Cluster）]** 画面に、[全般（General）]、[ライセンス（License）]、[システム（System）]、および [ヘルス（Health）] の設定が表示されます。

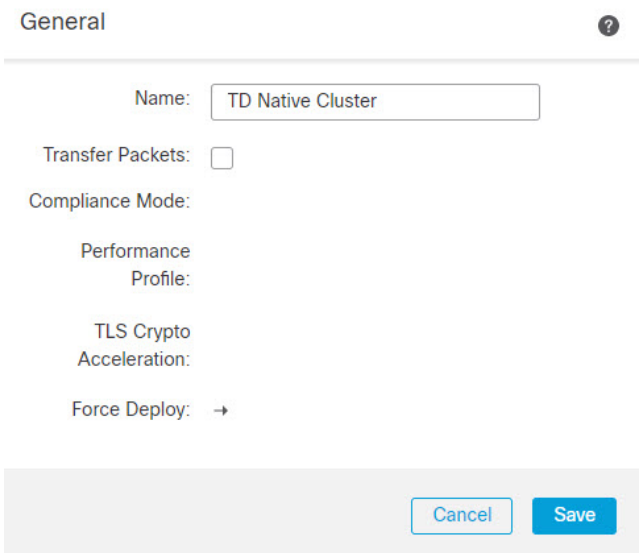


次のクラスタ固有の項目を参照してください。

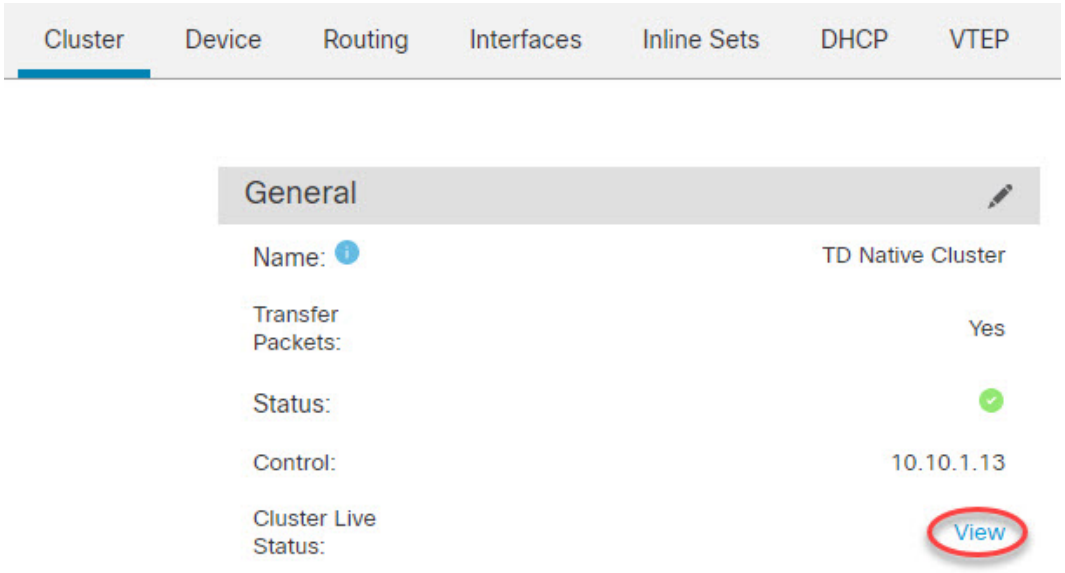
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタの表示名を変更します。



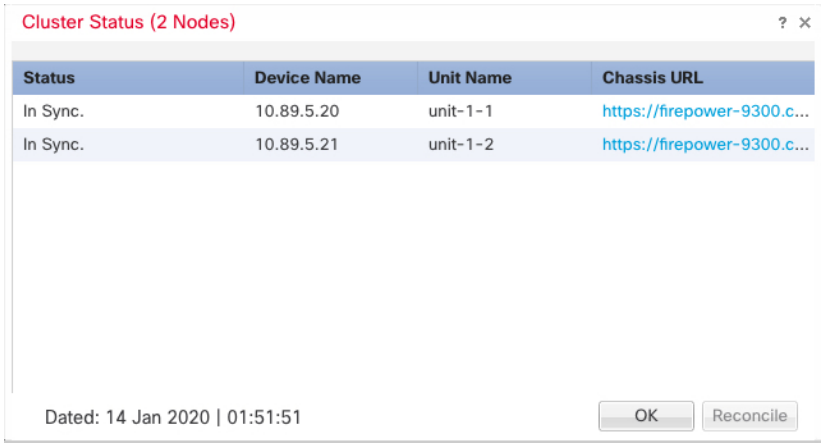
その後に、[名前（Name）] フィールドを設定します。



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



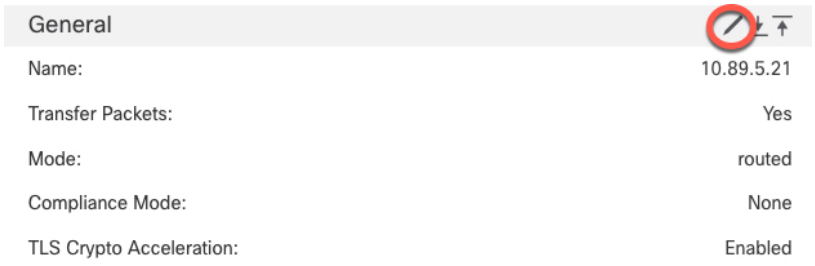
[クラスタステータス（Cluster Status）] ダイアログボックスで、[照合（Reconcile）] をクリックしてデータユニットの登録を再試行することもできます。



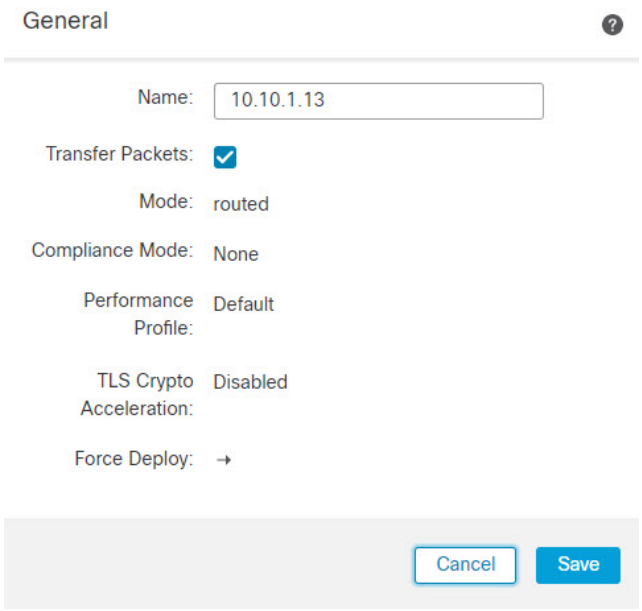
- [ライセンス（License）] : [編集（Edit）]（✎） をクリックして、ライセンス付与資格を設定します。

ステップ 4 **[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。

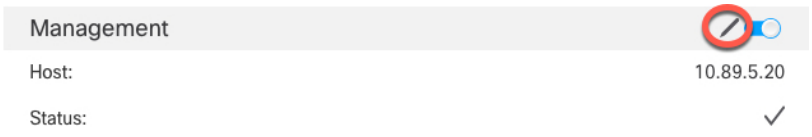
- [全般（General）] > [名前（Name）] : [編集（Edit）]（✎） をクリックして、クラスタメンバーの表示名を変更します。



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、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し、[管理（Management）] 領域で [ホスト（Host）] アドレスを編集します。



Management Center：クラスタ、データ、および診断インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。シャーシ間クラスタリングのクラスタ制御リンクインターフェイスの場合、MTU をデフォルトから増やす必要があ

ります。個別インターフェイスとして実行できる唯一のインターフェイスである診断インターフェイスを設定することもできます。

（注） シャーシ間クラスタリングにスパンドEtherChannelを使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、クラスタの横にある [編集（Edit）]（✎） をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。

ステップ 3 クラスタ制御リンクを設定します。

シャーシ間クラスタリングの場合、クラスタ制御リンク MTU に、データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。MTU の最大値を 9184 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。たとえば、最大 MTU は 9184 バイトであるため、データインターフェイスの最大 MTU は 9084 になり、クラスタ制御リンクは 9184 に設定できます。

ネイティブクラスタの場合：クラスタ制御リンクインターフェイスは、デフォルトで Port-Channel48 です。

a) クラスタ制御リンクインターフェイスの [編集（Edit）]（✎） をクリックします。
b) [全般（General）] ページの [MTU] フィールドに、1400 ～ 9184 の値を入力します。最大の 9184 を使用することをお勧めします。
c) [OK] をクリックします。

ステップ 4 データインターフェイスを設定します。

a) （任意） データインターフェイスに VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。
b) データインターフェイスの [編集（Edit）]（✎） をクリックします。
c) に従い、名前、IP アドレス、およびその他のパラメータを設定します。

（注） クラスタ制御リンクインターフェイスの MTU がデータインターフェイスの MTU より 100 バイト以上大きくない場合、データインターフェイスの MTU を減らす必要があるというエラーが表示されます。手順ステップ 3（47 ページ）を参照して、クラスタ制御リンクの MTU を増やしてください。その後、データインターフェイスの設定を続行できます。

d) シャーシ間クラスタの場合は、EtherChannel の手動グローバル MAC アドレスを設定します。[詳細設定（Advanced）] をクリックし、[アクティブなMACアドレス（Active MAC

Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

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

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

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

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

ステップ 5 （任意） 診断インターフェイスを設定します。

診断インターフェイスは、個別インターフェイスモードで実行できる唯一のインターフェイスです。syslog メッセージや SNMP などに、このインターフェイスを使用できます。

a) **[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。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** で、診断インターフェイスの [編集（Edit）]（✎） をクリックします。

c) [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。

d) 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。

e) [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。

f) 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 6 **[Save（保存）]** をクリックします。

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

Management Center：クラスタのヘルスモニターの設定

[クラスタ（Cluster）]ページの[クラスタヘルスモニターの設定（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 *6 :* クラスタのヘルスモニターの設定

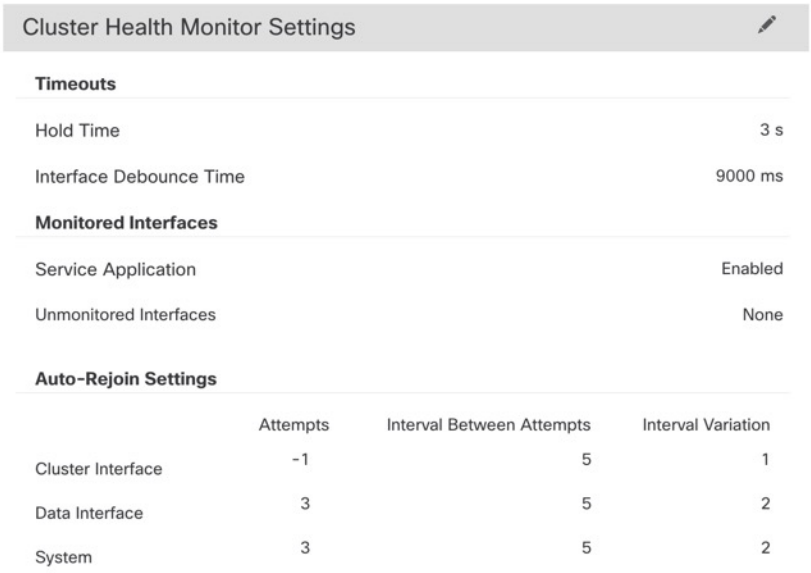


表 *2 : [*クラスタヘルスモニターの設定（*Cluster Health Monitor Settings***）*]* セクションテーブルのフィールド**

フィールド	説明
タイムアウト	
保留時間（Hold Time）	ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間	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。

フィールド	説明
Monitored Interfaces	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	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	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定	
クラスタインターフェイス	クラスタ制御リンクの自動再結合の設定の不具合を表示します。
データインターフェイス	データインターフェイスの自動再結合の設定を表示します。
システム（System）	内部エラー時の自動再結合の設定を表示します。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーションステータスなどがあります。

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

このセクションからこれらの設定を行うことができます。

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

手順

ステップ 1 **[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。

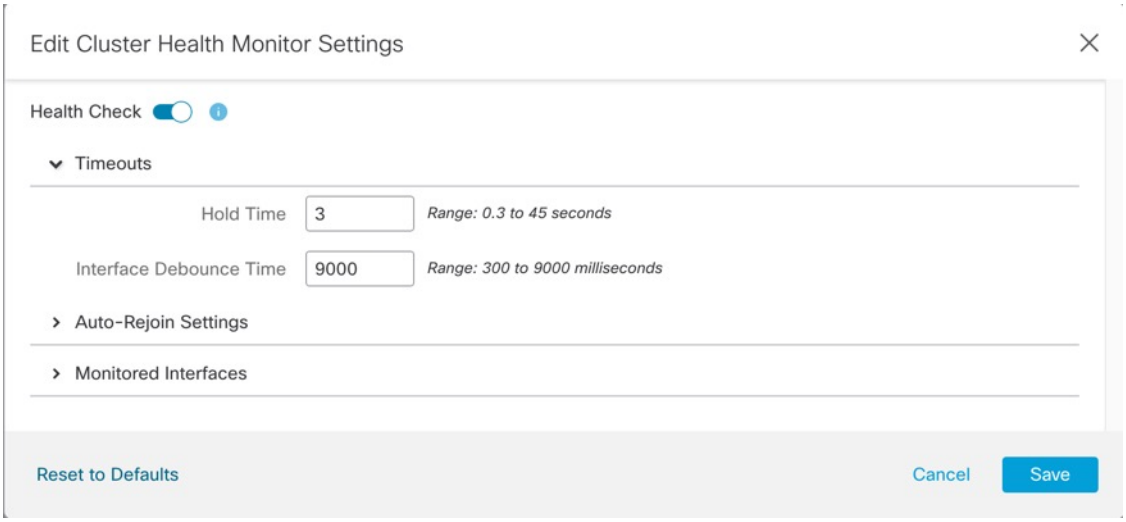
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（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 7: システムヘルスチェックの無効化



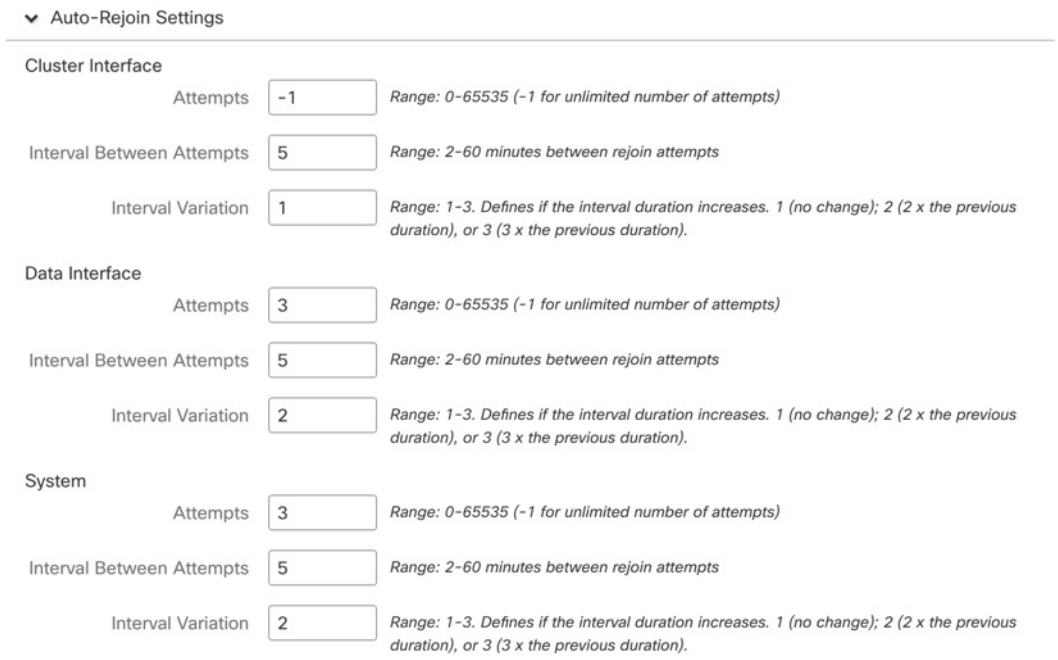
何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS やvPC を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

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

図 *8 :* 自動再結合の設定

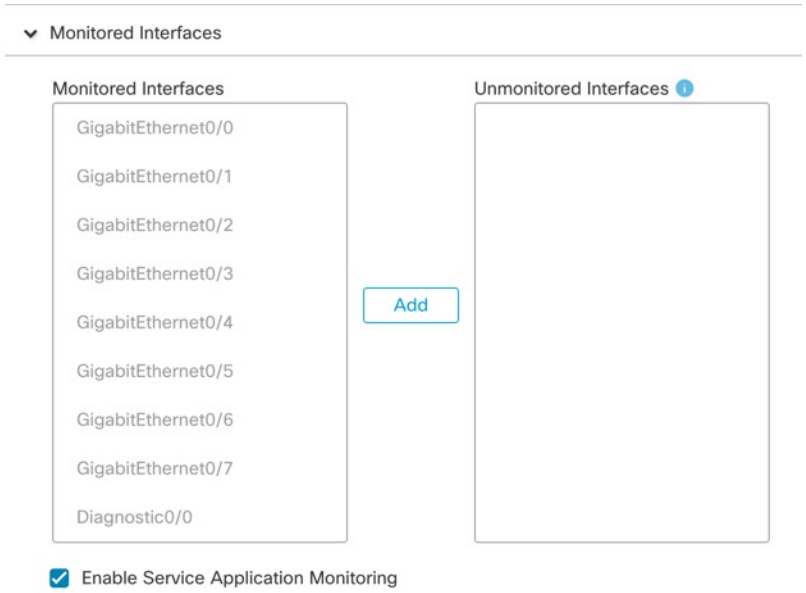


[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [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** は自動再結合をディセーブルにします。[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 *9*：モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

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 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 構成の変更を展開しますを参照してください。

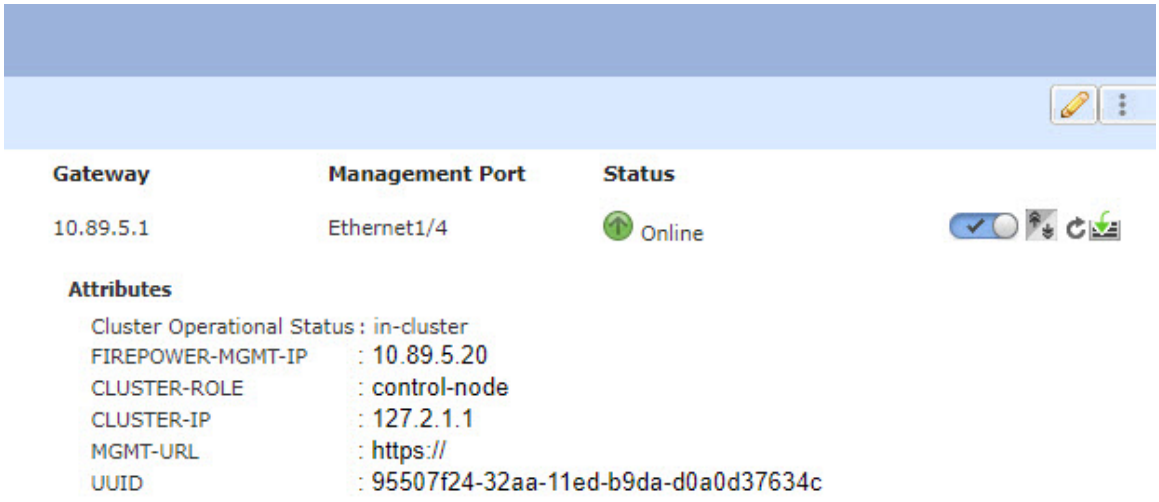
FXOS：クラスタユニットの削除

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

一時的な削除

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

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



Management Center を使用した Threat Defense では、Management Center デバイスリストにデバイスを残し、クラスタリングを再度有効にした後ですべての機能を再開できるようにする必要があります。

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

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

  クラスタリングを再度有効にするには、Threat Defense で **cluster enable** を入力します。

- アプリケーション インスタンスの無効化：Chassis Manager の [論理デバイス（Logical Devices）]ページで**有効なスライダ**（  ）をクリックします。**無効なスライダ**（  ）を使用して後で再度有効にすることができます。

- セキュリティ モジュール/エンジン のシャットダウン：Chassis Manager の [セキュリティ モジュール/エンジン（Security Module/Engine）] ページで、[電源オフ（Power Off）] アイコンをクリックします。
- シャーシのシャットダウン：Chassis Managerの [概要（Overview）] ページで、[シャットダウン（Shut Down）] アイコンをクリックします。

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

Management Center を使用した Threat Defense の場合、シャーシでクラスタリングを無効にした後でユニットを Management Center デバイスリストから削除してください。

- 論理デバイスの削除：Chassis Manager の [論理デバイス（Logical Devices）] ページで、 をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティ モジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

FMC：クラスタメンバーの管理

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

新規クラスタ メンバーの追加

FXOS に新しいクラスタ メンバーを追加すると、Secure Firewall Management Center によりメンバーが自動的に追加されます。

始める前に

- インターフェイスの設定が他のシャーシと交換用ユニットで同じ設定になっていることを確認します。

手順

ステップ 1 FXOS のクラスタに新しいユニットを追加します。『FXOS コンフィギュレーション ガイド』を参照してください。

新しいユニットがクラスタに追加されるまで待機します。Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、または Firepower Threat Defense の **show cluster info** コマンドを使用してクラスタ ステータスを表示します。

ステップ 2 新しいクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニターするには、次のように表示します。

- [クラスタステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** **その他** アイコンまたは **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** タブ > [全般（General）] 領域 > [クラスタステータスの表示（View Cluster Status）]> [クラスタのライブステータス（Cluster Live Status）] リンクから使用可能）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、Management Center はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] をクリックして再登録を強制します。
- [システムステータス（System status）] > [タスク（Tasks）]：Management Center にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

クラスタ メンバーの置換

既存クラスタ内のクラスタ メンバーを置き換えることができます。Management Center は交換ユニットを自動検出します。ただし、Management Center 内の古いクラスタ メンバーは手動で削除する必要があります。また、この手順は再初期化したユニットにも適用されます。その場合は、ハードウェアが同じでも新しいメンバーとして表示されます。

始める前に

- インターフェイス設定が他のシャーシに関する交換ユニットと同じであることを確認します。

手順

ステップ 1 新しいシャーシの場合、可能であれば、FXOS内の古いシャーシの設定をバックアップして復元します。

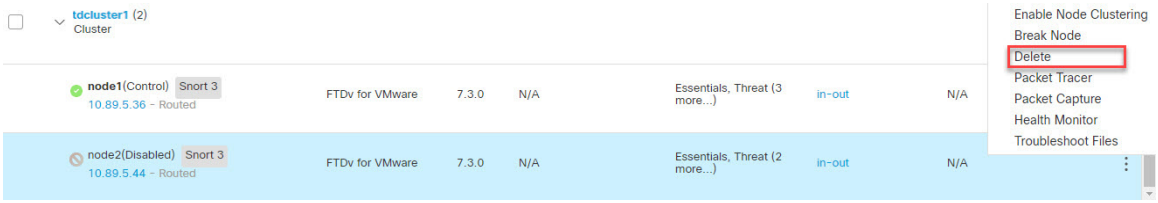
Firepower 9300 のモジュールを交換する場合は、次の手順を実行する必要はありません。

古いシャーシのバックアップ FXOS 設定がない場合は、最初に新規クラスタ メンバーの追加（55 ページ）の手順を実行します。

以下のすべての手順については、FXOS コンフィギュレーション ガイド[英語]を参照してください。

a) 設定のエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォームの構成時の設定を含んでいる XML ファイルをエクスポートします。
b) 交換用シャーシに設定ファイルをインポートします。
c) ライセンス契約に同意します。
d) 必要に応じて、論理デバイスのアプリケーション インスタンス バージョンをアップグレードして、残りのクラスタと一致させます。

ステップ 2 古いユニットの Management Center で、**[デバイス（Devices）] > [デバイス管理（Device Management）] > その他（⋮） > [削除（Delete）]** を選択し。



ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、Management Center デバイス リストからも削除されます。

ステップ 4 新しいクラスタ メンバーまたは再初期化したクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニターするには、次のように表示します。

- [クラスタステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）] > [デバイス管理（Device Management）] その他（⋮）** アイコンまたは **[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 > [クラスタステータスの表示（View Cluster Status）] > [クラスタのライブステータス（Cluster Live Status）] リンク）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、Management Center はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] [すべて（All）] をクリックして再登録を強制します。
- **システム**（⚙）> [タスク（Tasks）]：Management Center にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）] > [デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

メンバーの非アクティブ化

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

（注） ユニットが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールを使用する必要があります。

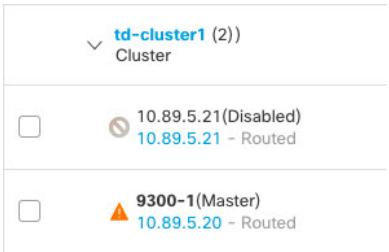
手順

ステップ 1 非アクティブ化するユニットに対し、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** **その他**（⋮） > [クラスタリングを無効にする（Disable Clustering）] を選択します。

[クラスタステータス（Cluster Status）] ダイアログボックスから、ユニットを非アクティブ化することもできます（**[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）]）。

ステップ 2 ユニットのクラスタリングを無効にすることを確認します。

ユニットは、**[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 （59 ページ）を参照してください。

クラスタへの再参加

障害が発生したインターフェイスなど、ユニット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、クラスタに手動で再参加させる必要があります。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。クラスタからユニットが削除される理由の詳細については、クラスタへの再参加 （81 ページ）を参照してください。

手順

ステップ 1 再アクティブ化するユニットに対し、**[デバイス（Devices）] > [デバイス管理（Device Management）] その他**（⋮） > [クラスタリングを有効にする（Enable Clustering）] を選択します。

[クラスタステータス（Cluster Status）] ダイアログボックスから、ユニットを再アクティブ化することもできます（**[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）]）。

ステップ 2 ユニットでクラスタリングを有効にすることを確認します。

データユニットの削除

クラスタ メンバーを完全に削除する必要がある場合（たとえば、Firepower 9300 でモジュールを削除する場合、またはシャーシを削除する場合）は、Management Center からメンバーを削除する必要があります。

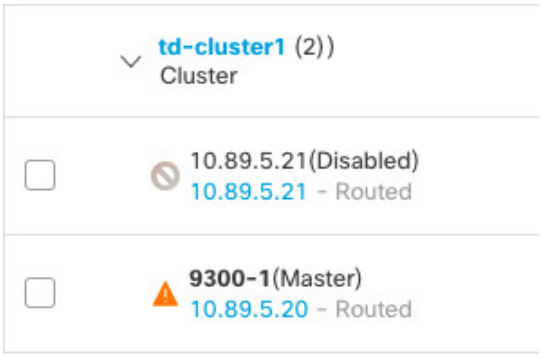
メンバーが正常なクラスタの一部である場合、またはメンバーを一時的に無効にするだけの場合は、メンバーを削除しないでください。FXOS のクラスタから完全に削除するには、FXOS：クラスタユニットの削除 （53 ページ）を参照してください。Management Center から削除しても、まだクラスタの一部である場合、トラフィックを引き続き通過させ、制御ユニット（Management Center が管理できない制御ユニット）になる可能性もあります。

始める前に

ユニットを手動で非アクティブ化するには、メンバーの非アクティブ化 （58 ページ）を参照してください。ユニットを削除する前に、手動で、またはヘルス障害により、ユニットが非アクティブになっている必要があります。

手順

ステップ 1 ユニットが Management Center から削除できる状態であることを確認します。**[デバイス（Devices）] > [デバイス管理（Device Management）]**で、ユニットに [（無効（Disabled））] と表示されていることを確認します。



また、各ユニットのステータスは、**その他**（⋮）から [クラスタステータス（Cluster Status）] ダイアログボックスで確認できます。ステータスが古い場合は、[クラスタステータス（Cluster Status）] ダイアログボックスの [照合（Reconcile）] をクリックして強制的に更新します。

ステップ 2 削除するデータユニットの Management Center で、**[デバイス（Devices）] > [デバイス管理（Device Management）] > その他**（⋮） **> [削除（Delete）]** を選択します。

ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、Management Center デバイス リストからも削除されます。

制御ユニットの変更

⚠

注意 制御ユニットを変更する最良の方法は、制御ユニット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。制御ユニットにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。中央集中型機能については、制御ユニット変更を強制するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

制御ユニットを変更するには、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。

[クラスタステータス（Cluster Status）] ダイアログボックスは、**[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）] リンクからも開くことができます。

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 メンバーの照合

クラスタ メンバーの登録に失敗した場合、シャーシから Secure Firewall Management Center に対してクラスタ メンバーシップを照合することができます。たとえば、Management Center が特定のプロセスで占領されているか、またはネットワークに問題がある場合、データユニット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。

[Cluster Status] ダイアログボックスは、**[Devices] > [Device Management] > [Cluster]** ページ > [General] 領域 > [Cluster Live Status] リンクからも開くことができます。

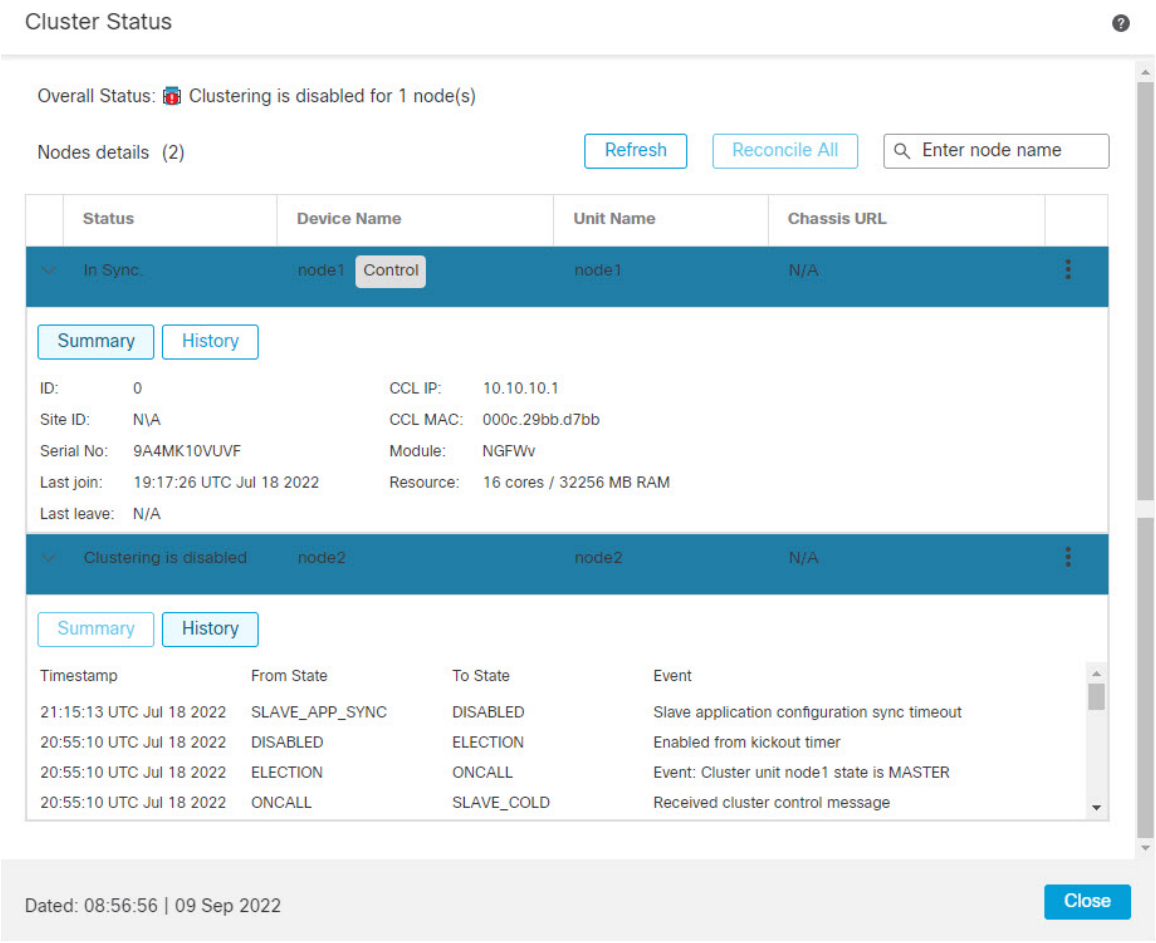
ステップ 2 [**Reconcile All**] をクリックします。

クラスタ ステータスの詳細については、Management Center：クラスタのモニタリング （62 ページ）を参照してください。

Management Center：クラスタのモニタリング

クラスタのモニタリングは、Secure Firewall Management Center および Threat Defense CLI で実行できます。

- [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 > [クラスタステータスの表示（View cluster status）]> [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。



コントロールユニットには、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）：装置は Management Center に登録されています。
- Pending Registration：装置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。装置が登録に失敗した場合、[**Reconcile All**] をクリックして登録を再試行することができます。
- Clustering is disabled：装置は 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。または、装置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）：装置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。

装置ごとに、[Summary] または [History] で、それぞれ概要と履歴を表示できます。

その他（⋮）メニューから、装置ごとに次のステータス変更を実行できます。

- **クラスタリングを無効にする**
- **クラスタリングを有効にする**
- **ロールを Control に変更する**

- **システム**（⚙）> [Tasks] ページ。

  [Tasks] ページには、各装置が登録されるごとに、クラスタ登録タスクの最新の状況が表示されます。

- **[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、制御装置（IP アドレスの横にその役割が示されている）を含め、すべてのメンバ装置を表示できます。登録中の装置には、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

Cluster Health Monitor

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

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

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

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

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

クラスタ ヘルスの表示

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

クラスタヘルスモニターは、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モニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

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

手順

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

[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、ノード固有のヘルスモ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全体のリストについては、クラスタメトリック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、点線の上部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モニターの場合）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モニターの場合）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全体のリストについては、Firepower デバイスのメトリックを参照してください。

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

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

クラスタメトリック

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

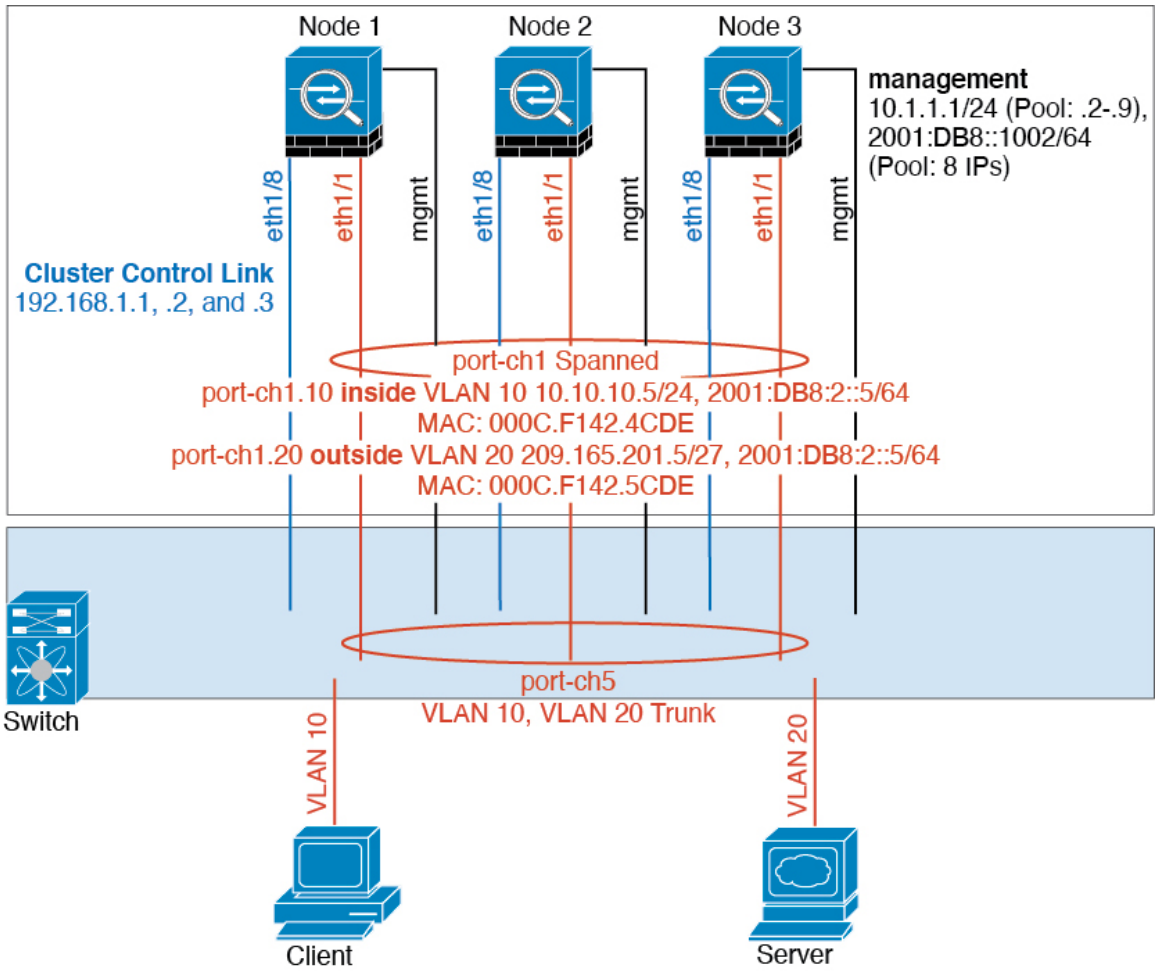
表 *3:* クラスタメトリック

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

クラスタリングの例

これらの例には、一般的な導入が含まれます。

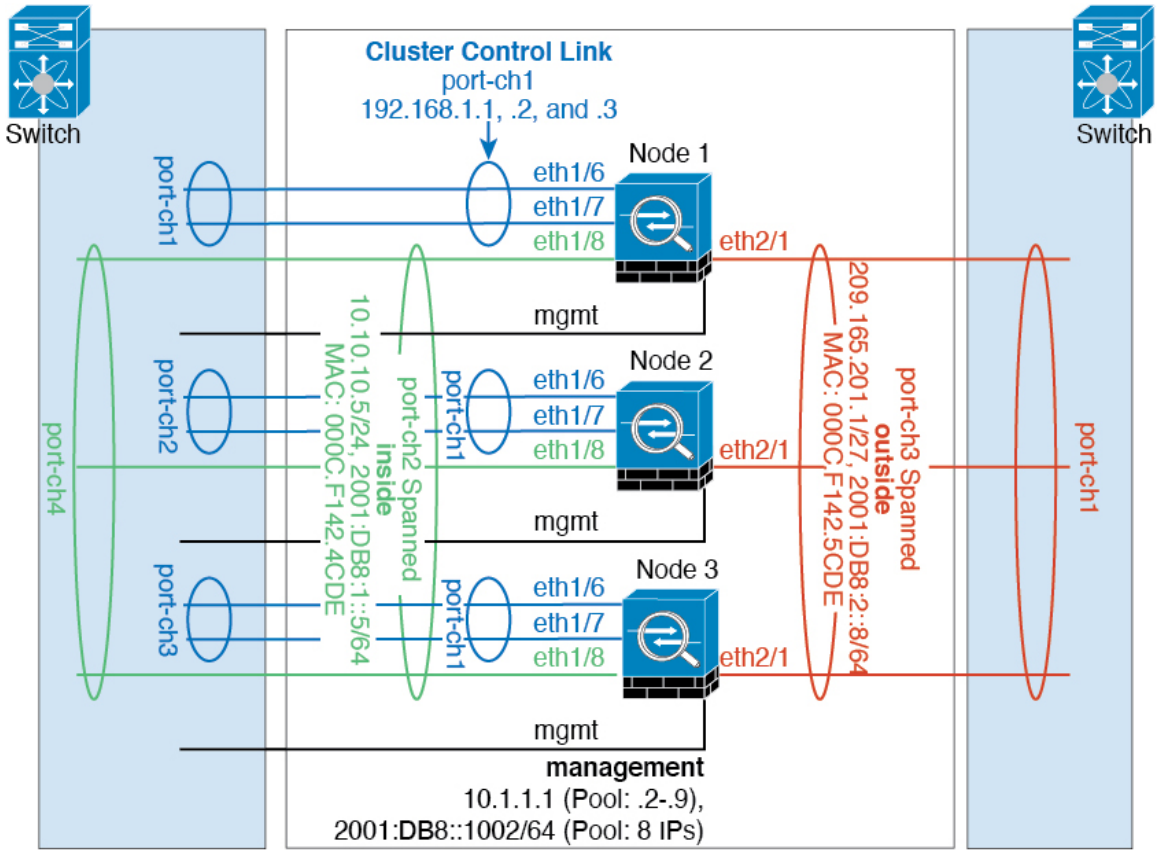
スティック上のファイアウォール



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

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

トラフィックの分離



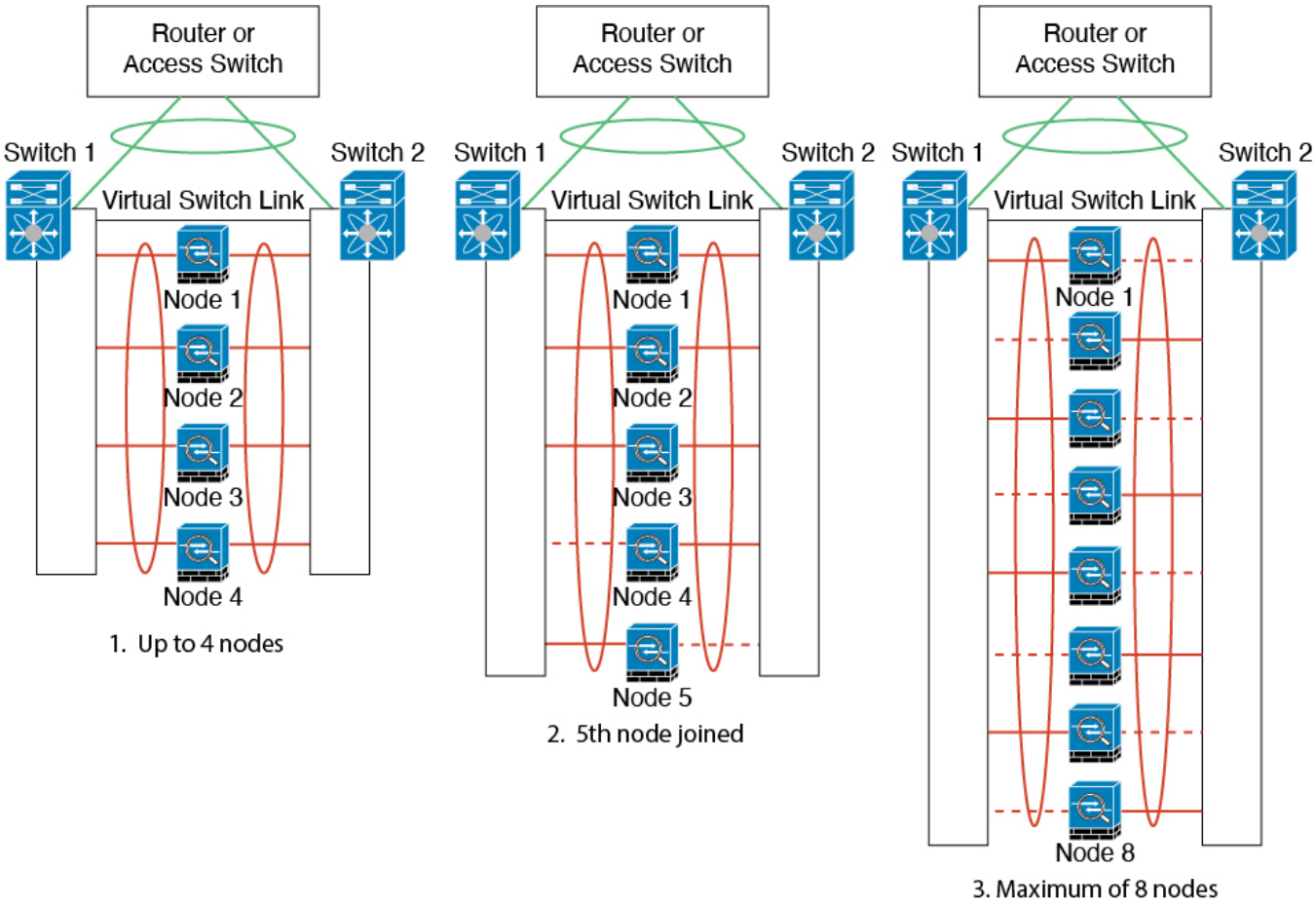
内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

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

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

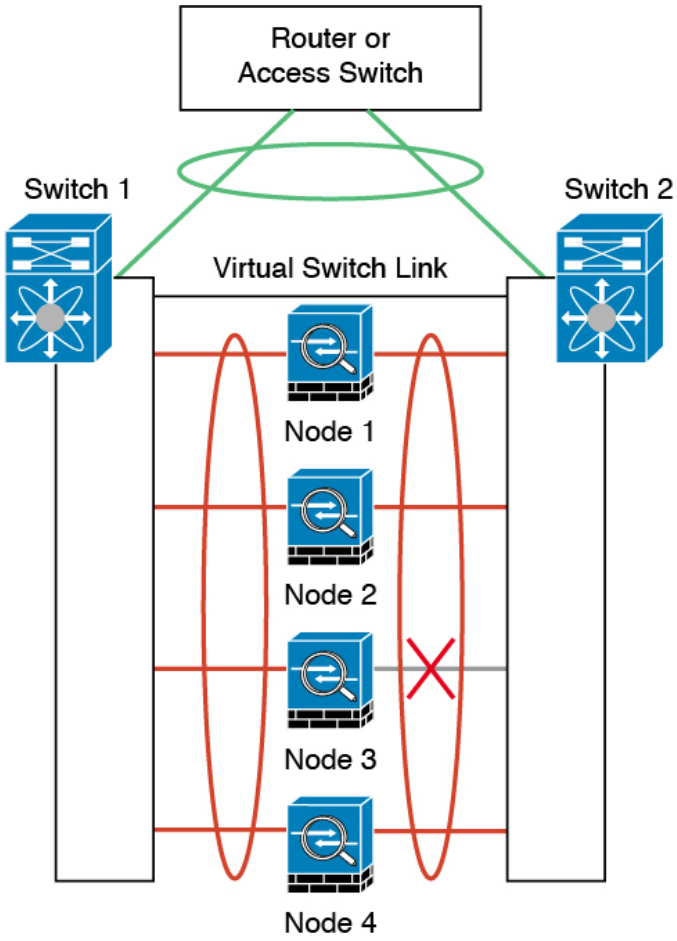
従来の EtherChannel のアクティブ ポートの最大数は、スイッチ側からの 8 に制限されます。8 ユニットから成るクラスタがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイ モードにする必要があります。Threat Defense は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。VSS、vPC、StackWise、またはStackWise Virtualを使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できま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

次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。

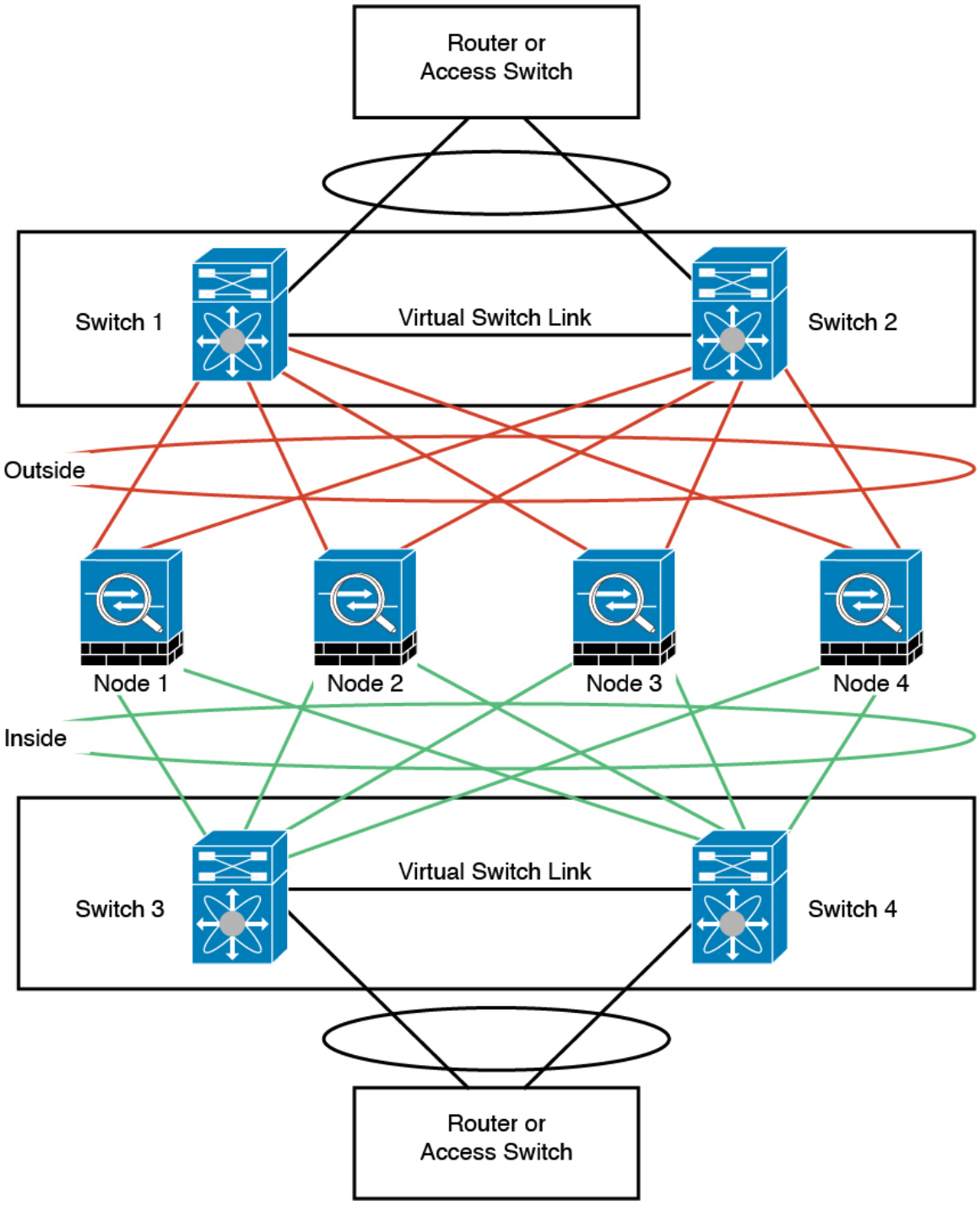


原則として、初めにチャネル内のアクティブポート数を最大化し、そのうえで、アクティブな制御ポートとアクティブなデータポートの数のバランスを保ちます。5 番目のユニットがクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

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



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



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。

クラスタリングでサポートされない機能

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

（注） クラスタリングでもサポートされていないFlexConfig機能（WCCPインスペクションなど）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
- FMC 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
- サイト間 VPN
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ダイナミック ルーティング

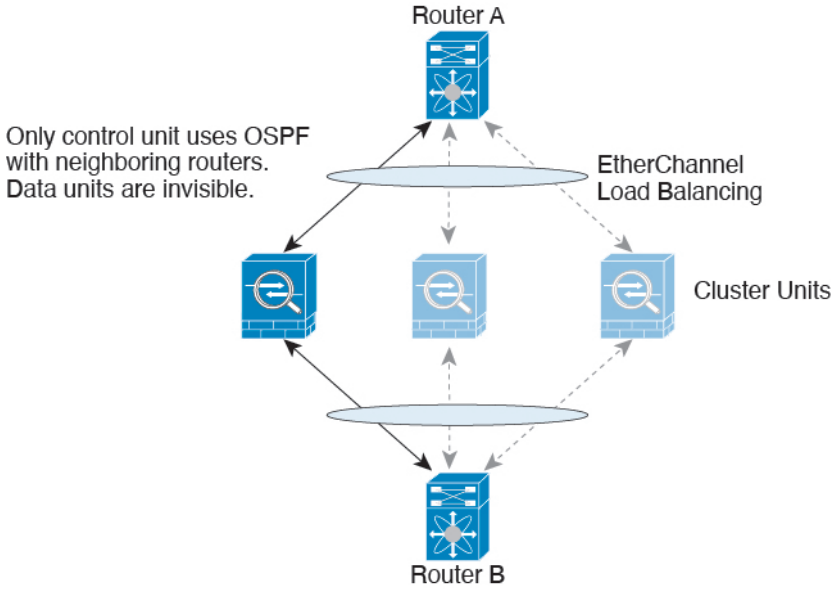
接続設定

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

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

図 *10* : ダイナミック ルーティング



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

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

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。

マルチキャスト ルーティングとクラスタリング

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

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の 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。

- 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 [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。

TLS/SSL 接続とクラスタリング

TLS/SSL接続の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。

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

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

パフォーマンス スケーリング係数

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

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

制御ユニットの選定

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

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットが制御ユニットになります。

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

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

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

クラスタ内のハイ アベイラビリティ

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

シャーシ アプリケーションのモニターリング

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

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

装置のヘルス モニターリング

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

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション2のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。詳細については、制御ユニットの選定 （79 ページ）を参照してください。

インターフェイス モニタリング

各ノードは、使用中のすべてのハードウェアインターフェイスのリンクステータスを監視し、ステータスの変更を制御ノードに報告します。シャーシ間クラスタリングでは、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニターして EtherChannel でポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には Threat Defense アプリケーションに通知します。ヘルスモニターリングを有効にすると、デフォルトではすべての物理インターフェイスがモニターされます（EtherChannel インターフェイスのメイン EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニターできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません。ヘルス チェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

特定のノードで監視対象のインターフェースに障害が発生し、その他のノードでそのインターフェイスがアクティブになっている場合、そのノードはクラスタから削除されます。Threat Defense デバイス によってノードがクラスタから削除されるまでの時間は、そのノードが確立済みのメンバーであるかクラスタに参加しようとしているかによって異なります。Threat Defense

デバイスは、ノードがクラスタに参加する最初の90秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、Threat Defense デバイス はクラスタから削除されません。確立済みのメンバーの場合は、500 ミリ秒後にノードが削除されます。

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

デコレータ アプリケーションのモニタリング

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

障害後のステータス

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

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

障害イベントに応じて、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：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：Threat Defense は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、Threat Defense アプリケーションはクラスタリングを無効にします。データインターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。

- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ノードは再起動するとクラスタに再参加します。Threat Defense アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。
- 障害が発生した設定の展開：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。
- シャーシ アプリケーション通信の障害：Threat Defense アプリケーションはシャーシ アプリケーションの状態が回復したことを検出すると、自動的にクラスタへの再参加を試みます。

データ パス接続状態の複製

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

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

表 *4:* クラスタ全体で複製される機能

トラフィック	状態のサポート	注
アップ タイム	対応	システムアップタイムをトラッキングします。
ARP テーブル	対応	—
MAC アドレス テーブル	対応	—
ユーザ アイデンティティ	対応	—
IPv6 ネイバー データベース	対応	—
ダイナミック ルーティング	対応	—
SNMP エンジン ID	なし	—

クラスタが接続を管理する方法

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

接続のロール

接続ごとに定義された次のロールを参照してください。

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

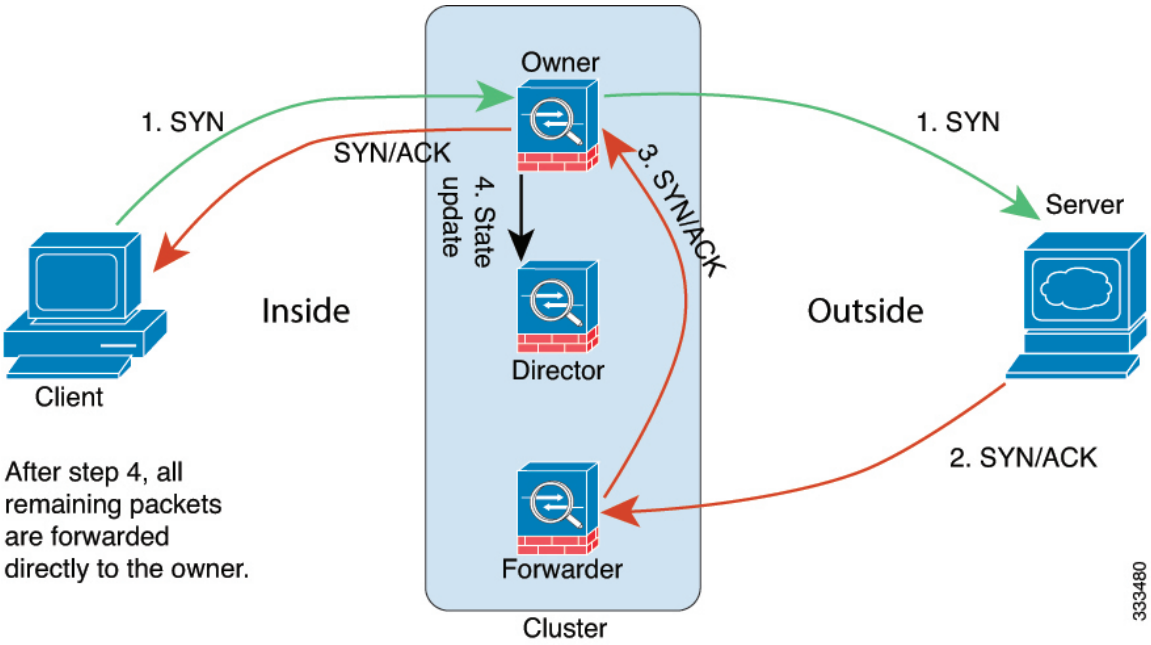
- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合が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

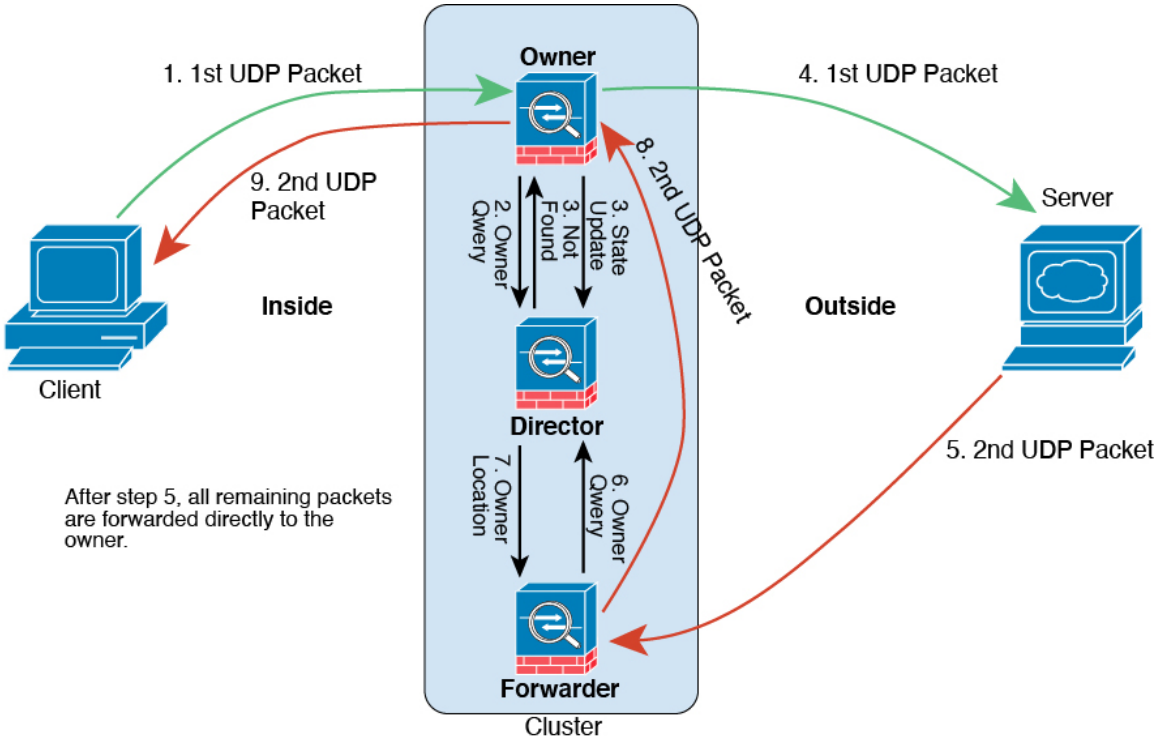


1. SYN パケットがクライアントから発信され、Threat Defense の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Threat Defense（ロードバランシング方法に基づく）に配信されます。この Threat Defense はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、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 *11 : 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。

クラスタリングの履歴

機能	バージョン	詳細
クラスタのヘルスモニターの設定	7.3	クラスタのヘルスモニター設定を編集できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **クラスタ（Cluster）** > **[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前に FlexConfig を使用してこれらの設定を行った場合は、展開前に必ず FlexConfig の設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。
クラスタ ヘルス モニター ダッシュボード	7.3	クラスタのヘルス モニター 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。 新規/変更された画面：**システム**（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]**
16 ノードクラスタのサポート	7.2	Firepower 4100/9300 で 16 ノードクラスタを構成できるようになりました。 新規/変更された画面：なし。 サポートされるプラットフォーム：Firepower 4100/9300
ファイアウォールの変更に対するクラスタの展開がより迅速に完了する	7.1	ファイアウォールの変更に対するクラスタの展開がより迅速に完了するようになりました。 新規/変更された画面：なし。
クラスタリング用の PAT ポートブロック割り当ての改善	7.0	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するには、FlexConfig を使用して **cluster-member-limit** コマンドを実行して、予定しているクラスタ内の最大ノード数を設定します。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更されたコマンド：**cluster-member-limit**（FlexConfig）、**show nat pool cluster** [**summary**]、**show nat pool ip detail**

機能	バージョン	詳細
Snort の変更に対するクラスタの展開がより迅速に完了し、イベントが発生するとより迅速に失敗する	6.7	Snort の変更に対するクラスタの展開がより迅速に完了するようになりました。また、Management Center 展開が失敗する原因となるイベントがクラスタにある場合、エラーがより迅速に発生するようになりました。 新規/変更された画面：なし。
Management Center でのクラスタ管理の改善	6.7	Management Center では、以前は CLI を使用することでしか実現できなかった、次のようなクラスタ管理機能が改善されました。 • クラスタユニットの有効化および無効化 • [デバイス管理（Device Management）]ページからクラスタのステータスを表示（ユニットごとの履歴とサマリーを含む） • ロールの制御ユニットへの変更 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [詳細（More）]**メニュー • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [全般（General）]**エリア > [クラスタのライブステータス（Cluster Live Status）] リンク > [クラスタステータス（Cluster Status）] サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
マルチインスタンスクラスタ	6.6	コンテナインスタンスを使用してクラスタを作成できるようになりました。Firepower 9300 では、クラスタ内の各モジュールに 1 つのコンテナインスタンスを含める必要があります。セキュリティエンジン/モジュールごとに複数のコンテナインスタンスをクラスタに追加することはできません。クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュールタイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。 新規/変更された FXOS コマンド： **set port-type cluster** 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）]** > **[クラスタの追加（Add Cluster）]** • **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] > [タイプ（Type）] フィールド サポートされるプラットフォーム：Firepower 4100/9300 上の Threat Defense
データユニットとの設定の並列同期	6.6	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更された画面：なし。
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。**show cluster history**	6.6	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、**show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history** 新規/変更された画面：なし。

機能	バージョン	詳細
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	6.5	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ） サポートされるプラットフォーム：Firepower 4100/9300 上の Threat Defense
Management Center への Threat Defense クラスタ追加の改善	6.3	Management Center にクラスタの任意のユニットを追加できるようになりました。他のクラスタ ユニットは自動的に検出されます。以前は、各クラスタ ユニットを個別のデバイスとして追加し、Management Center でグループ化してクラスタにする必要がありました。クラスタ ユニットの追加も自動で実行されるようになりました。ユニットは手動で削除する必要があることに注意してください。 新規/変更された画面： **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** > [追加（Add）] ドロップダウンメニュー > [デバイス（Devices）]>[デバイスの追加（Add Device）] ダイアログボックス **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** > [クラスタ（Cluster）] タブ > [全般（General）] 領域 > [クラスタの登録ステータス（Cluster Registration Status）] リンク > [クラスタ ステータス（Cluster Status）] ダイアログボックス サポートされるプラットフォーム：Firepower 4100/9300 上の Threat Defense
中央集中型機能としてのクラスタリングによるサイト間 VPN のサポート	6.2.3.3	クラスタリングを使用してサイト間 VPN を設定できるようになりました。サイト間 VPN は、中央集中型機能です。制御ユニットのみが VPN 接続をサポートします。 サポートされるプラットフォーム：Firepower 4100/9300 上の Threat Defense

機能	バージョン	詳細
内部エラーの発生後に自動的にクラスタに再参加します。	6.2.3	以前は、多くの内部エラー状態によって、クラスタ ユニットがクラスタから削除され、ユーザーが問題を解決した後で、手動でクラスタに再参加する必要がありました。現在は、ユニットが自動的に、5 分、10 分、20 分の間隔でクラスタに再参加しようとします。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。 新しい/変更されたコマンド：**show cluster info auto-join** 変更された画面はありません。 サポートされるプラットフォーム：Firepower 4100/9300 上の Threat Defense
6モジュールのシャーシ間クラスタリング、Firepower 4100 サポート	6.2	FXOS 2.1.1 では、Firepower 9300 および 4100 でシャーシ間クラスタリングを有効化できるようになりました。Firepower 9300 の場合、最大6つのモジュールを含めることができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせたりできます。Firepower 4100 の場合、最大 6 つのシャーシを含めることができます。 （注） サイト間クラスタリングもサポートされていません。しかし、サイト固有の MAC および IP アドレス、ディレクタのローカリゼーション、サイトの冗長性、クラスタフローモビリティなどの冗長性と安定性を向上させるためのカスタマイズは、FlexConfig 機能を使用した場合にのみ設定できます。 変更された画面はありません。 サポートされるプラットフォーム：Firepower 4100/9300 上の Threat Defense

機能	バージョン	詳細
Firepower 9300 用シャーシ内クラスタリング	6.0.1	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [クラスタの追加（Add Cluster）]** **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** サポートされるプラットフォーム：Firepower 9300 上の Threat Defense

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。