



## 論理デバイス

---

- [論理デバイスについて \(1 ページ\)](#)
- [論理デバイスの要件と前提条件 \(11 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(20 ページ\)](#)
- [スタンドアロン論理デバイスの追加 \(27 ページ\)](#)
- [ハイ アベイラビリティ ペアの追加 \(57 ページ\)](#)
- [クラスタの追加 \(58 ページ\)](#)
- [Radware DefensePro の設定 \(95 ページ\)](#)
- [TLS 暗号化アクセラレーションの設定 \(106 ページ\)](#)
- [論理デバイスの管理 \(109 ページ\)](#)
- [論理デバイスのモニタリング \(121 ページ\)](#)
- [サイト間クラスタリングの例 \(123 ページ\)](#)
- [論理デバイスの履歴 \(128 ページ\)](#)

## 論理デバイスについて

論理デバイスでは、1つのアプリケーションインスタンス（ASA または Firepower Threat Defense のいずれか） および1つのオプションデコレータアプリケーション（Radware DefensePro）を実行し、サービスチェーンを形成できます。

論理デバイスを追加する場合は、アプリケーション インスタンス タイプとバージョンを定義し、インターフェイスを割り当て、アプリケーション設定に送信されるブートストラップ設定を構成することもできます。



- 
- (注) Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および Firepower Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。
-

## スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロンユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、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）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュールデバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3 つすべてのモジュールがネイティブインスタンスとコンテナインスタンスの両方のクラスタに参加する必要があります。FDM はクラスタリングをサポートしていません。

## 論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

アプリケーションインスタンスは次の展開タイプで実行します。

- ネイティブ インスタンス：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：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。マルチインスタンス機能は FMC を使用する Firepower Threat Defense でのみサポートされています。ASA または FDM を使用する Firepower Threat Defense ではサポートされていません。



- 
- (注) マルチインスタンス機能は、実装は異なりますが、ASA マルチコンテキストモードに似ています。マルチコンテキストモードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナインスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェアアップデート、および Firepower Threat Defense のフル機能のサポートが可能です。マルチコンテキストモードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。Firepower Threat Defense ではマルチコンテキストモードは使用できません。
- 

Firepower 9300 の場合、一部のモジュールでネイティブ インスタンスを使用し、他のモジュールではコンテナ インスタンスを使用することができます。

## コンテナ インスタンス インターフェイス

コンテナ インターフェイスでの柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイス (VLAN または物理) を共有することができます。ネイティブのインスタンスは、VLAN サブインターフェイスまたは共有インターフェイスを使用できません。マルチインスタンスクラスタは、VLAN サブインターフェイスまたは共有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。[共有インターフェイスの拡張性](#)および[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](#)を参照してください。



- (注) 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。FTD 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。詳細については、[FXOS インターフェイスとアプリケーションインターフェイス](#)を参照してください。

## シャーシがパケットを分類する方法

シャーシに入ってくるパケットはいずれも分類する必要があります。その結果、シャーシは、どのインスタンスにパケットを送信するかを決定できます。

- 一意のインターフェイス：1つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループメンバー インターフェイス (トランスペアレント モードまたはルーテッド モード)、インラインセット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意の MAC アドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイスに割り当てられた固有の MAC アドレスが使用されます。固有の MAC アドレスがないと、アップストリームルータはインスタンスに直接ルーティングできません。アプリケーション内で各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。



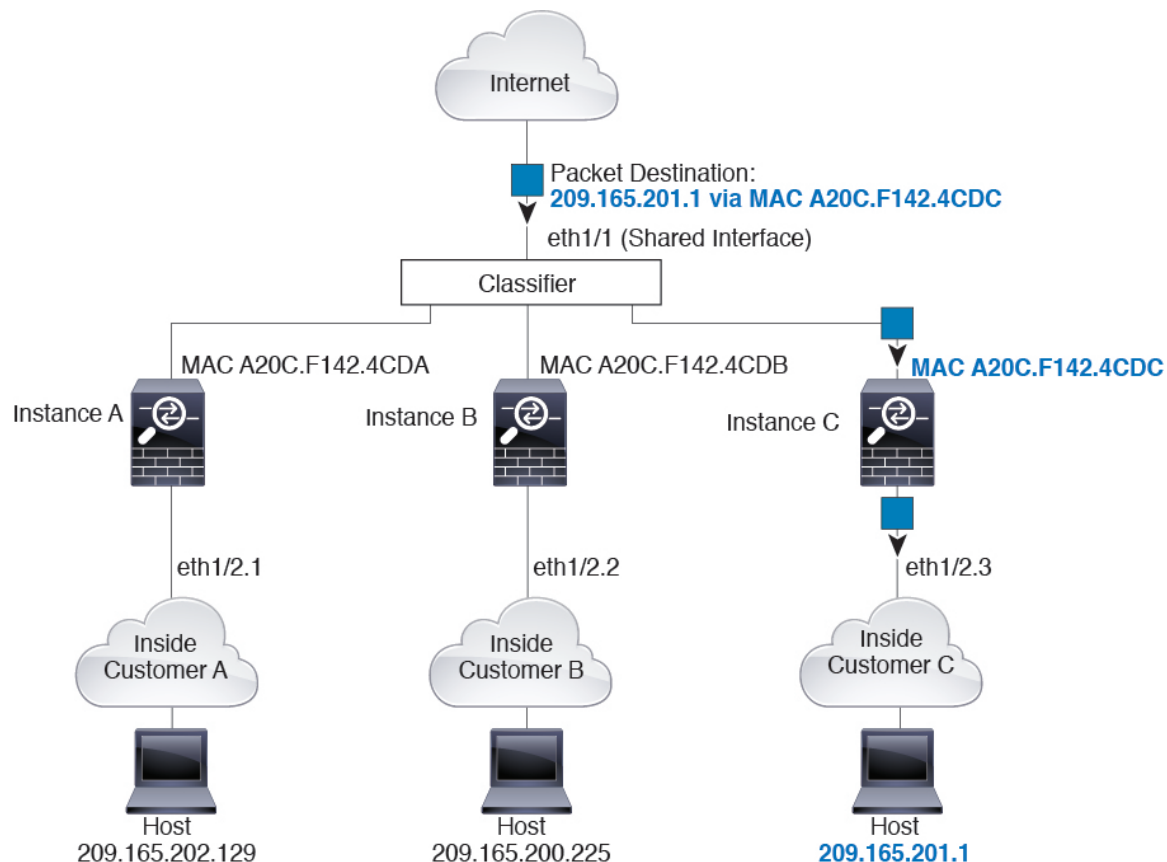
- (注) 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製されて各インスタンスに送信されます。

## 分類例

**MAC アドレスを使用した共有インターフェイスの packets 分類**

次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンス C にはルータが packet を送信する MAC アドレスが含まれているため、分類子は packet をインスタンス C に割り当てます。

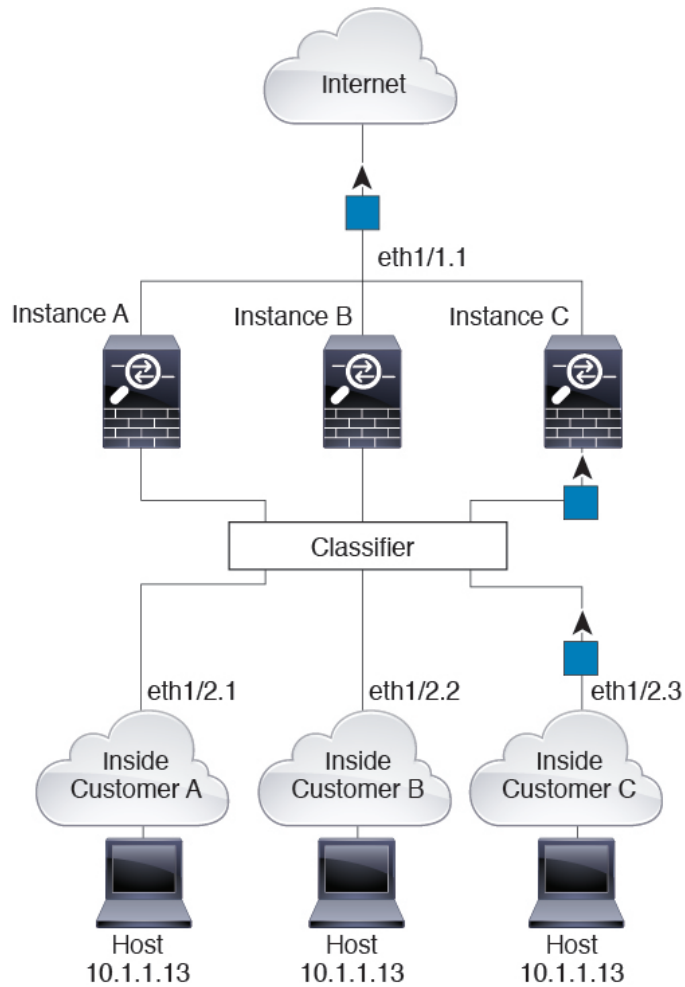
図 1: MAC アドレスを使用した共有インターフェイスの packets 分類

**内部ネットワークからの着信トラフィック**

内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンス C のホストを示します。分類子は、packet をインスタンス C に割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。



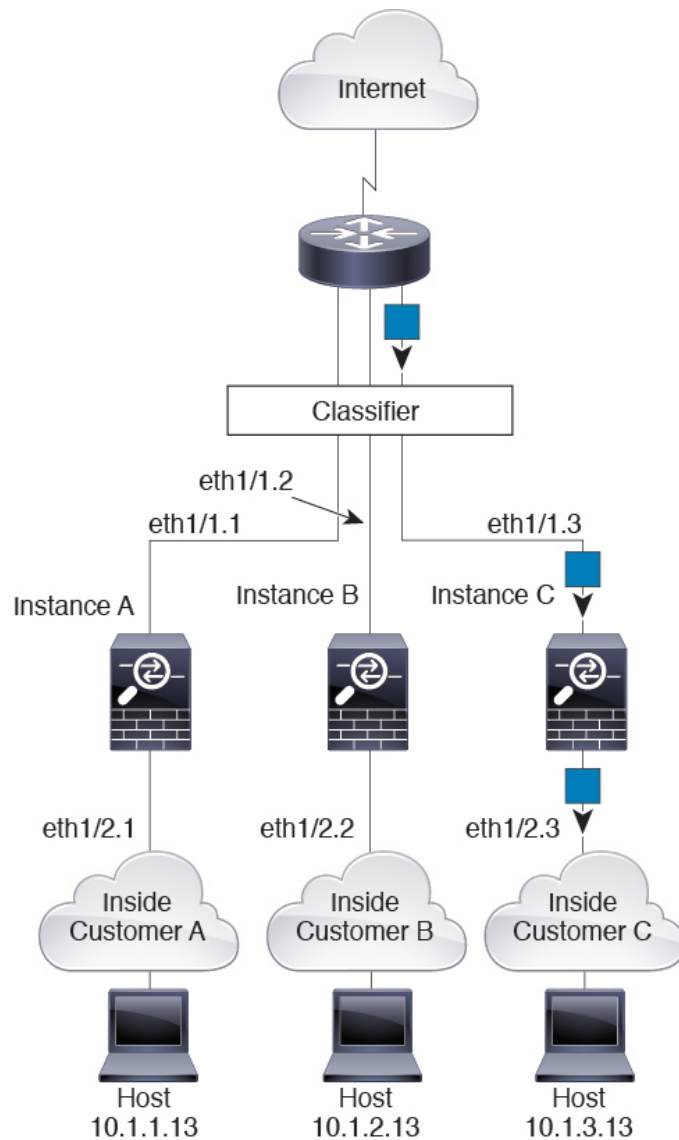
図 2: 内部ネットワークからの着信トラフィック



### トランスペアレント ファイアウォール インスタンス

トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンスCに割り当てられているためです。

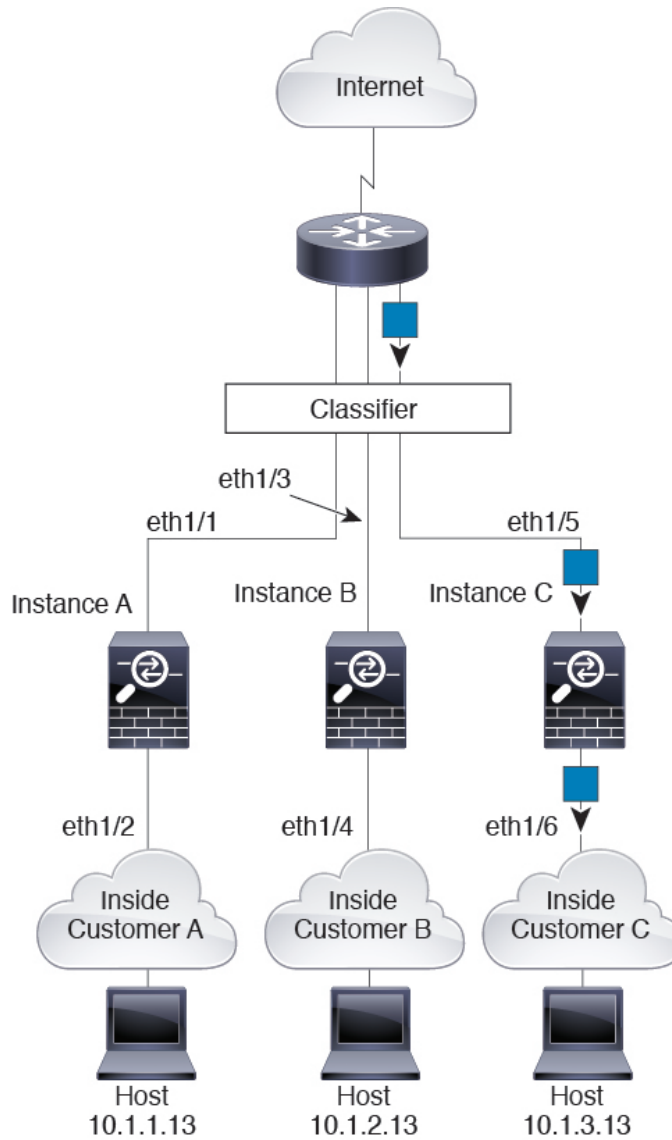
図 3: トランスペアレントファイアウォールインスタンス



### インラインセット

インラインセットの場合は一意のインターフェイスを使用する必要があります。また、それらのセットは物理インターフェイスか、またはEtherChannelである必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/5 で、このイーサネットがインスタンスCに割り当てられているためです。

図 4: インラインセット

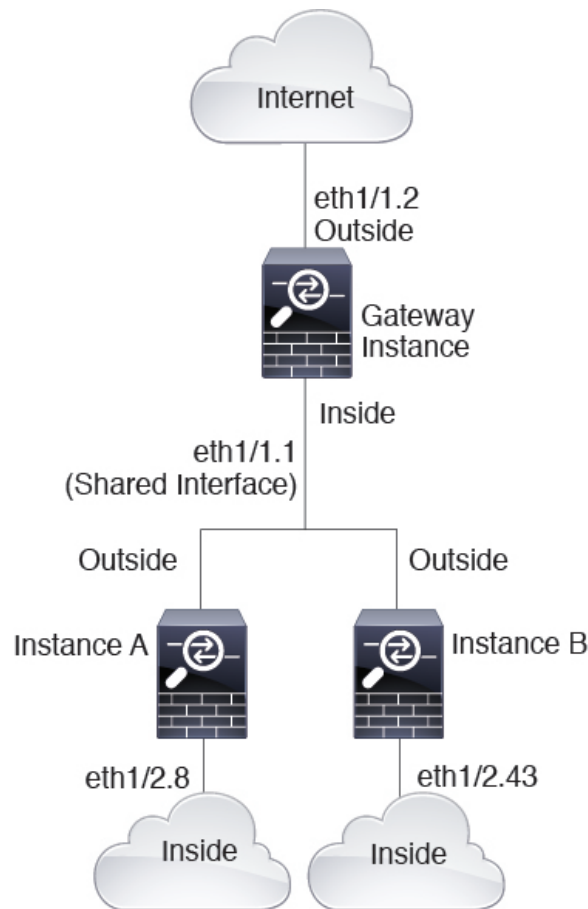


## コンテナ インスタンスのカスケード

別のインスタンスの前にインスタンスを直接配置することをインスタンスのカスケードと呼びます。一方のインスタンスの外部インターフェイスは、もう一方のインスタンスの内部インターフェイスと同じインターフェイスです。いくつかのインスタンスのコンフィギュレーションを単純化する場合、最上位インスタンスの共有パラメータを設定することで、インスタンスをカスケード接続できます。

次の図に、ゲートウェイの背後に2つのインスタンスがあるゲートウェイインスタンスを示します。

図 5: インスタンスのカスケード

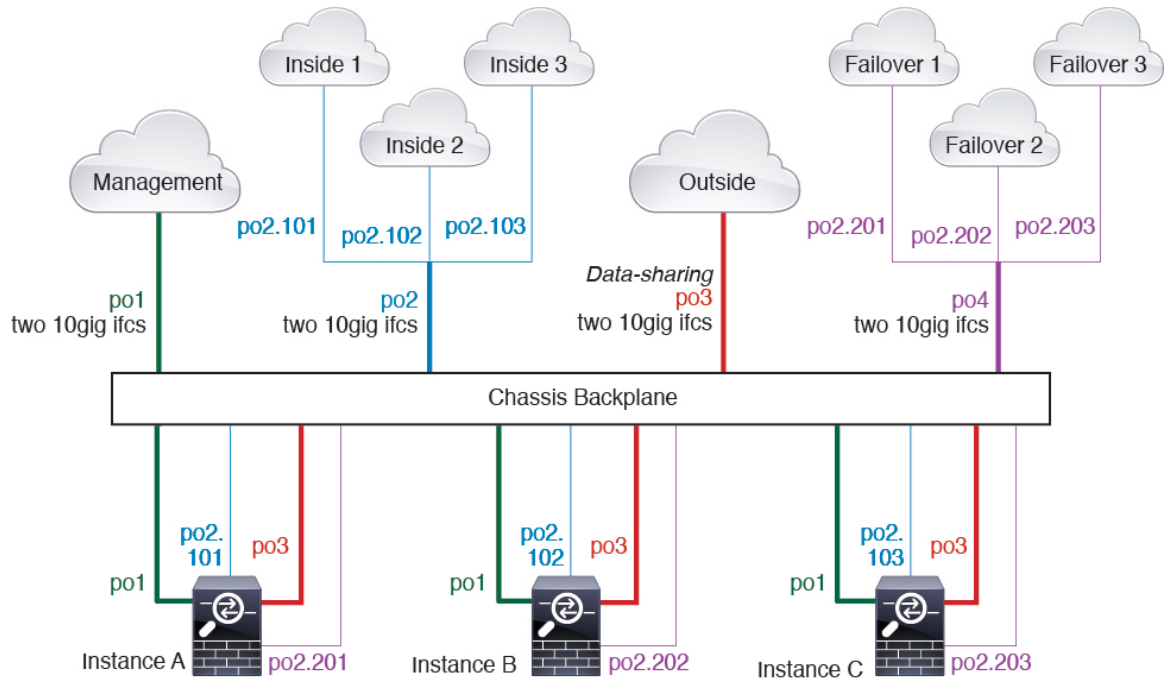


## 一般的な複数インスタンス展開

次の例には、ルーテッドファイアウォールモードのコンテナインスタンスが3つ含まれます。これらには次のインターフェイスが含まれます。

- **管理**：すべてのインスタンスがポートチャネル1インターフェイス（管理タイプ）を使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意的 IP アドレスを使用します。
- **内部**：各インスタンスがポートチャネル2（データタイプ）のサブインターフェイスを使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。
- **外部**：すべてのインスタンスがポートチャネル3インターフェイス（データ共有タイプ）を使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ外部ネットワークで一意的 IP アドレスを使用します。

- フェールオーバー：各インスタンスがポートチャネル4（データタイプ）のサブインターフェイスを使用します。この EtherChannel には2つの 10 ギガビットイーサネットインターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。



## コンテナ インスタンス インターフェイスの自動 MAC アドレス

シャーシは、各インスタンスの共有インターフェイスが一意的な MAC アドレスを使用するように、インスタンス インターフェイスの MAC アドレスを自動的に生成します。

インスタンス内の共有インターフェイスに MAC アドレスを手動で割り当てると、手動で割り当てられた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インスタンス内のインターフェイスの MAC アドレスを手動で設定してください。

自動生成されたアドレスは A2 で始まり、アドレスが重複するリスクがあるため、手動 MAC アドレスの先頭は A2 にしないでください。

シャーシは、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yy はユーザー定義のプレフィックスまたはシステム定義のプレフィックスであり、zz.zzzz はシャーシが生成した内部カウンタです。システム定義のプレフィックスは、IDPROM にプログラムされている Burned-in MAC アドレス内の最初の MAC アドレスの下部 2 バイトと一致します。connect fxos を使用し、次に show module を使用して、MAC アドレスプールを表示します。

たとえば、モジュール 1 について示されている MAC アドレスの範囲が b0aa.772f.f0b0 ~ b0aa.772f.f0bf の場合、システム プレフィックスは f0b0 になります。

ユーザ定義のプレフィックスは、16進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例を挙げます。プレフィックスとして 77 を指定すると、シャースは 77 を 16 進数値 004D (yyxx) に変換します。MAC アドレスで使用すると、プレフィックスはシャースネイティブ形式に一致するように逆にされます (xyyy)。

A24D.00zz.zzzz

プレフィックス 1009 (03F1) の場合、MAC アドレスは次のようになります。

A2F1.03zz.zzzz

## コンテナインスタンスのリソース管理

コンテナインスタンスごとのリソース使用率を指定するには、FXOS で 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 40GB に設定されます。モデルごとに使用可能なリソースを表示するには、[コンテナインスタンスの要件と前提条件 \(19 ページ\)](#) を参照してください。リソース プロファイルを追加するには、[コンテナインスタンスにリソースプロファイルを追加](#) を参照してください。

## マルチインスタンス機能のパフォーマンス スケーリング係数

プラットフォームの最大スループット（接続数、VPN セッション数、および TLS プロキシセッション数）は、ネイティブインスタンスがメモリと CPU を使用するために計算されます（この値は `show resource usage` に示されます）。複数のインスタンスを使用する場合は、インスタンスに割り当てる CPU コアの割合に基づいてスループットを計算する必要があります。たとえば、コアの 50% でコンテナインスタンスを使用する場合は、最初にスループットの 50% を計算する必要があります。さらに、コンテナインスタンスで使用可能なスループットは、ネイティブインスタンスで使用可能なスループットよりも低い場合があります。

インスタンスのスループットを計算する方法の詳細については、<https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html> を参照してください。

## コンテナインスタンスおよびハイ アベイラビリティ

2 つの個別のシャースでコンテナインスタンスを使用してハイアベイラビリティを使用できます。たとえば、それぞれ 10 個のインスタンスを使用する 2 つのシャースがある場合、10 個のハイアベイラビリティ ペアを作成できます。ハイアベイラビリティは FXOS で構成されません。各ハイアベイラビリティ ペアはアプリケーション マネージャで構成します。

詳細な要件については、「[ハイアベイラビリティの要件と前提条件 \(18 ページ\)](#)」と「[ハイアベイラビリティ ペアの追加 \(57 ページ\)](#)」を参照してください。

## コンテナインスタンスおよびクラスタリング

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を使用して、コンテナインスタンスのクラスタを作成できます。詳細な要件については、[クラスタリングの要件と前提条件 \(13 ページ\)](#) を参照してください。

## 論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

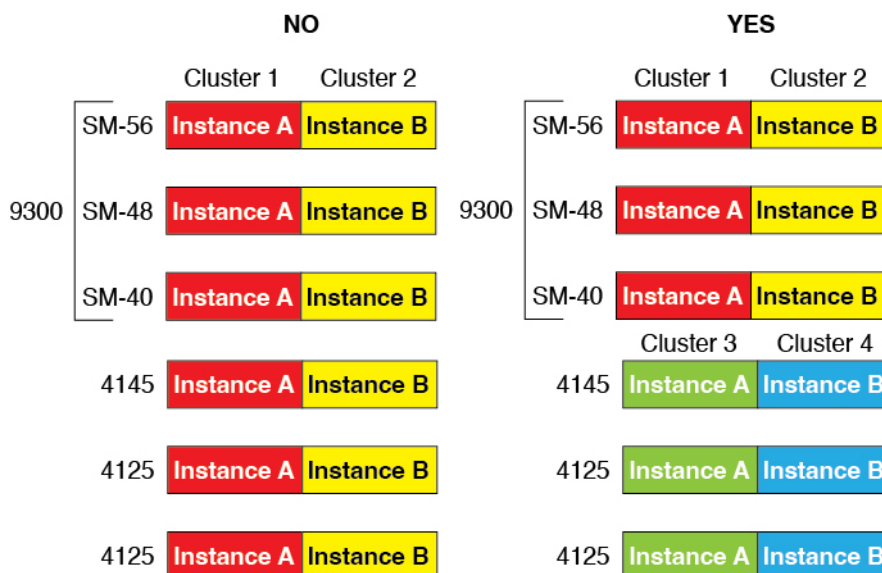
## ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

### Firepower 9300 の要件

Firepower 9300 には、3つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- **セキュリティモジュールタイプ**：Firepower 9300 に異なるタイプのモジュールをインストールできます。たとえば、SM-48 をモジュール 1、SM-40 をモジュール 2、SM-56 をモジュール 3 としてインストールできます。
- **ネイティブインスタンスとコンテナインスタンス**：セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを1つのみインストールできます。一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。たとえば、モジュール 1 とモジュール 2 にネイティブインスタンスをインストールできますが、モジュール 3 にはコンテナインスタンスをインストールできません。
- **ネイティブインスタンスのクラスタリング**：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内の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。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。たとえば、シャーシ 1 に2つの SM-40 を、シャーシ 2 に3つの SM-40 をインストールできます。同じシャーシに1つの SM-48 および2つの SM-40 をインストールする場合、クラスタリングは使用できません。
- **コンテナインスタンスのクラスタリング**：異なるモデルタイプのインスタンスを使用してクラスタを作成できます。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。ただし、同じクラスタ内に Firepower 9300 と Firepower 4100 を混在させることはできません。



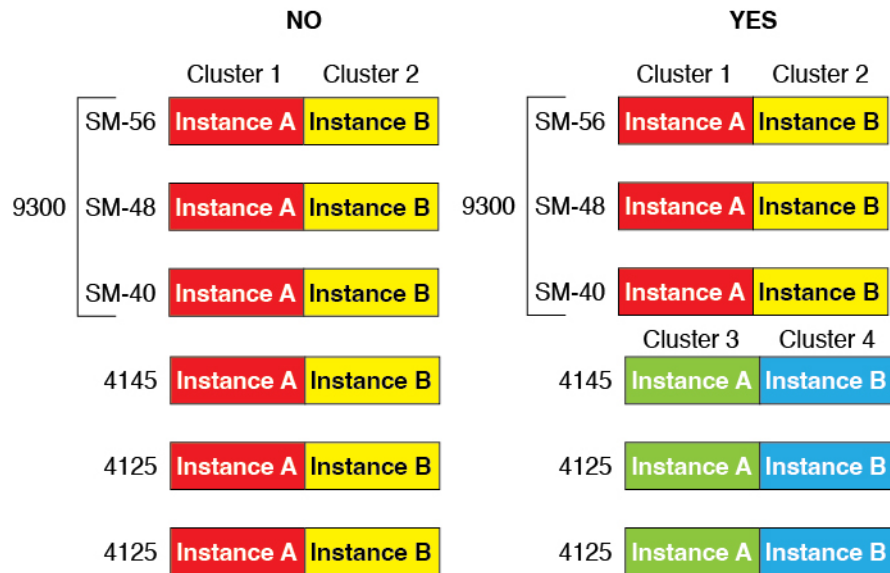
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-40、SM-48、および SM-56 があります。SM-40 モジュール間、SM-48 モジュール間、および SM-56 モジュール間にハイアベイラビリティペアを作成できます。
- ASA および FTD のアプリケーションタイプ：異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール1とモジュール2に ASA をインストールし、モジュール3に FTD をインストールすることができます。
- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーションインスタンスタイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール1に FTD 6.3 を、モジュール2に FTD 6.4 を、モジュール3に FTD 6.5 をインストールできます。

### Firepower 4100 の要件

Firepower 4100 は複数のモデルに搭載されています。次の要件を参照してください。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100 にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブインスタンスを1つのみインストールできます。
- ネイティブインスタンスのクラスタリング：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- コンテナインスタンスのクラスタリング：異なるモデルタイプのインスタンスを使用してクラスタを作成できます。たとえば、Firepower 4145 および 4125 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。ただし、同じクラスタ内に Firepower 9300 と Firepower 4100 を混在させることはできません。





- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。
- ASA および FTD のアプリケーションタイプ：Firepower 4100 は、1つのアプリケーションタイプのみを実行できます。
- FTD コンテナインスタンスのバージョン：同じモジュール上で異なるバージョンの Firepower Threat Defense を個別のコンテナインスタンスとして実行できます。

## 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

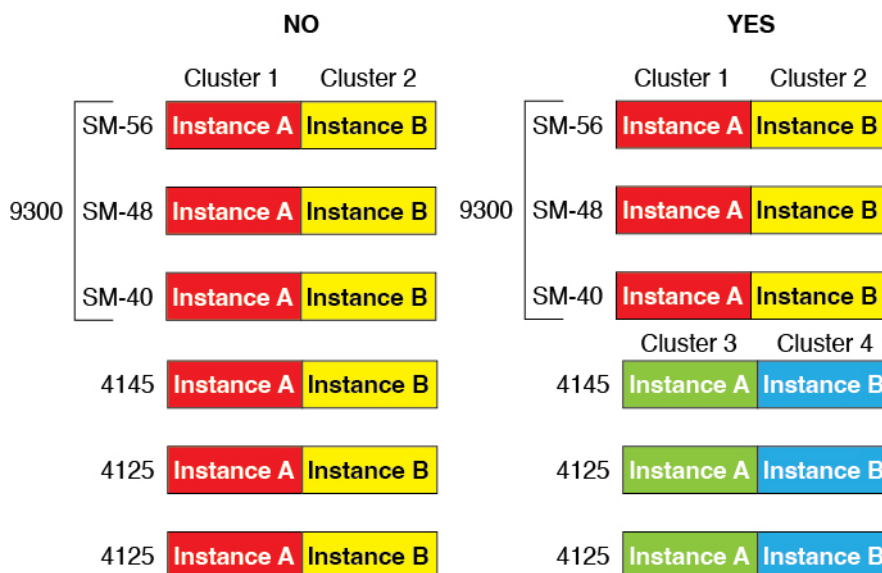
- Firepower 9300 上の ASA：最大 16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用し、最大 16 のモジュールを組み合わせることができます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。シャーシ内、シャーシ間、およびサイト間クラスタリングでサポート。
- Firepower 4100 シリーズ 上の ASA：最大 16 個のシャーシ。シャーシ間、およびサイト間クラスタリングでサポート。
- FTDFirepower 9300 で FMC を使用：1 シャーシ内に最大 3 モジュール。6 モジュールたとえば、3 つのシャーシで 2 つのモジュールを使用したり、2 つのシャーシで 3 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。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。シャーシ内およびシャーシ間クラスタリングでサポート。
- FTDFirepower 4100 シリーズ で FMC を使用：最大 16 シャーシ。シャーシ間クラスタリングでサポート。
- Radware DefensePro：ASA によるシャーシ内クラスタリングでサポート。

- Radware DefensePro : Firepower Threat Defense によるシャーシ内クラスタリングでサポート。マルチインスタンス クラスタリングではサポートされません。

### 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。



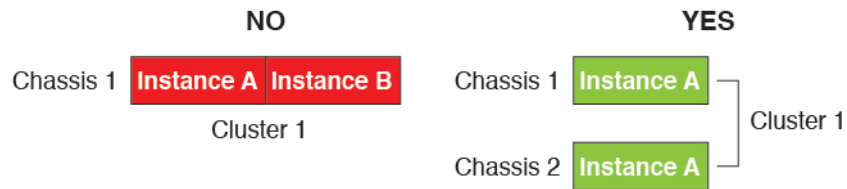
- イメージアップグレード時を除き、同じ FXOS およびアプリケーション ソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じバンド EtherChannel にインターフェイスを正常にバンドルできれば、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）。

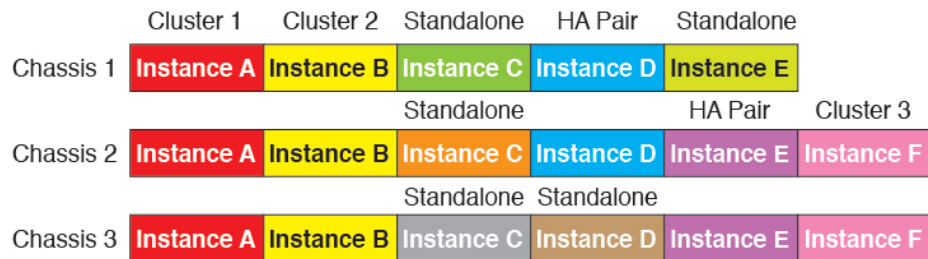
- 同じNTPサーバを使用する必要があります。Firepower Threat Defenseでは、FMCも同じNTPサーバを使用する必要があります。時間を手動で設定しないでください。
- ASA：各FXOSシャーシは、License Authorityまたはサテライトサーバに登録されている必要があります。データノードは追加料金なしで使用できます。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firepower Threat Defenseでは、すべてのライセンスは、FMCによって処理されます。

**マルチインスタンス クラスタリングの要件**

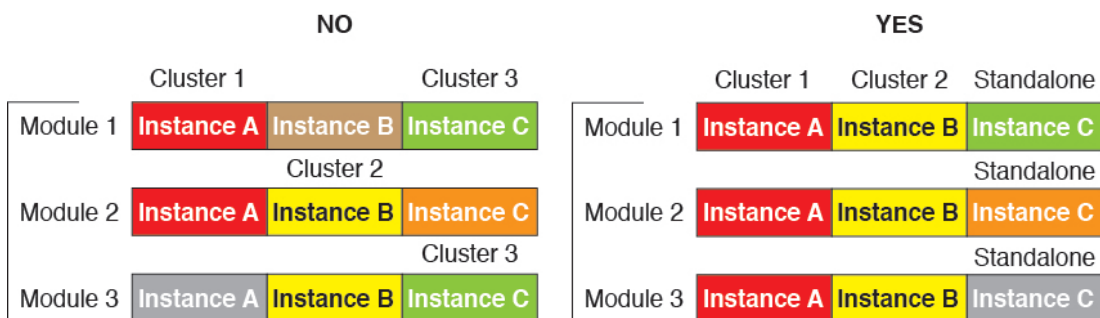
- セキュリティモジュール/エンジン間クラスタリングなし：特定のクラスタでは、セキュリティモジュール/エンジンごとに1つのコンテナインスタンスのみを使用できます。同じモジュール上で実行されている場合、同じクラスタに2つのコンテナインスタンスを追加することはできません。



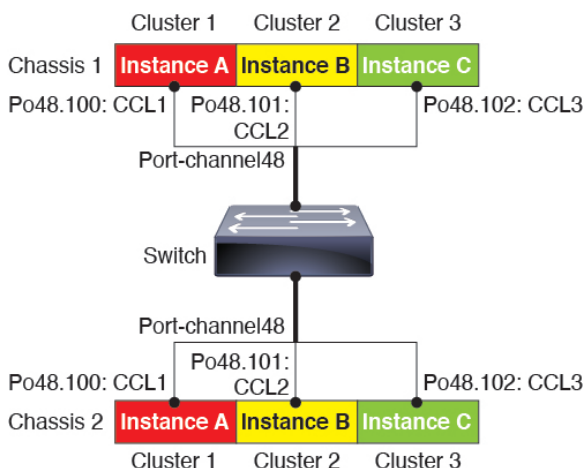
- クラスタとスタンドアロンインスタンスの混在：セキュリティモジュール/エンジン上のすべてのコンテナインスタンスがクラスタに属している必要はありません。一部のインスタンスをスタンドアロンノードまたは高可用性ノードとして使用できます。また、同じセキュリティモジュール/エンジン上で別々のインスタンスを使用して複数のクラスタを作成することもできます。



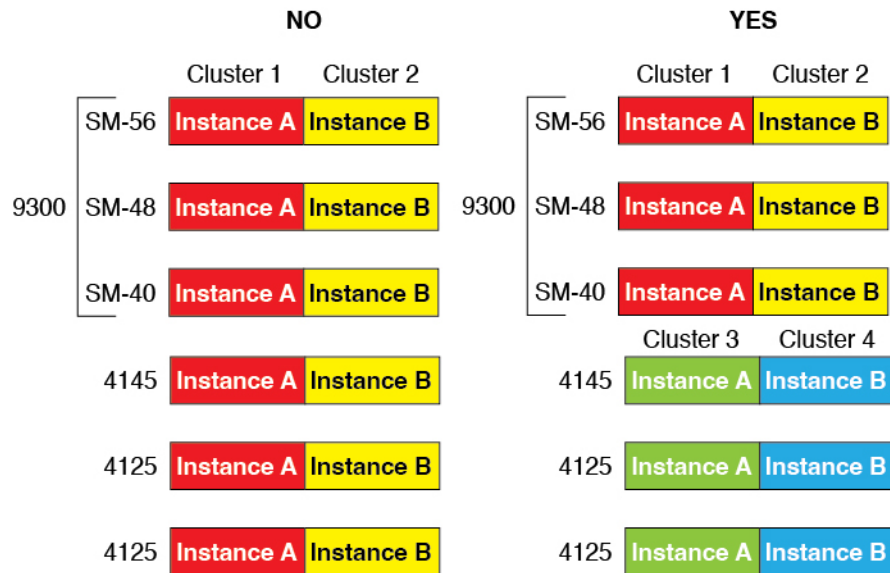
- Firepower 9300の3つすべてのモジュールはクラスタに属している必要があります。Firepower 9300の場合、クラスタには3つすべてのモジュールで1つのコンテナインスタンスが必要です。たとえば、モジュール1と2のインスタンスを使用してクラスタを作成し、モジュール3のネイティブインスタンスを使用することはできません。



- 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。

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

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

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

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

次に例を示します。

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

予約する DCI 帯域幅 = 5 Gbps (2/2 x 5 Gbps)。

- 3 サイトの 6 メンバーの場合、サイズは増加します。
  - 合計 6 クラスタ メンバー
  - サイト 1 は 3 メンバー、サイト 2 は 2 メンバー、サイト 3 は 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps (3/2 x 10 Gbps)。

- 2 サイトの 2 メンバーの場合。
  - 合計 2 クラスタ メンバー
  - 各サイト 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

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

## ハイアベイラビリティの要件と前提条件

- ハイアベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 個別のシャーシ上にあること。Firepower 9300 のシャーシ内ハイアベイラビリティはサポートされません。
  - 同じモデルであること。
  - 高可用性論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。
- コンテナインスタンスでは、各装置で同じリソースプロファイル属性を使用する必要があります。
- 他のハイアベイラビリティ システム要件については、アプリケーションの構成ガイドのハイアベイラビリティに関する章を参照してください。

## コンテナインスタンスの要件と前提条件

### サポートされるアプリケーションタイプ

- FTD FMC を使用

### 最大コンテナ インスタンスとモデルあたりのリソース

各コンテナインスタンスに対して、インスタンスに割り当てる CPU コアの数を指定できます。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あたり 40 GB に設定されます。

表 1: モデルごとの最大コンテナ インスタンス数とリソース

モデル	最大コンテナ インスタンス 数	使用可能な CPU コア	使用可能な RAM	使用可能なディスク スペース
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 セキュリ ティモジュール	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 セキュリ ティモジュール	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 セキュリ ティモジュール	13	78	334 GB	1359 GB
Firepower 9300 SM-44 セキュリ ティモジュール	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 セキュリ ティモジュール	15	94	334 GB	1341 GB
Firepower 9300 SM-56 セキュリ ティモジュール	18	110	334 GB	1314 GB

### FMC の要件

Firepower 4100 シャーシまたは Firepower 9300 モジュール上のすべてのインスタンスに対して、ライセンスの実装のために同じ FMC を使用する必要があります。

## 論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

### 一般的なガイドラインと制限事項

#### ファイアウォールモード

Firepower Threat Defense と ASA のブートストラップ設定でファイアウォールモードをルーテッドまたはトランスペアレントに設定できます。

#### ハイアベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータインターフェイスをフェールオーバーリンクおよびステートリンクとして使用できます。データ共有インターフェイスはサポートされていません。

#### マルチインスタンスとコンテキストモード

- ASA ではマルチコンテキストモードはサポートされていません。
- 展開後に、ASA のマルチコンテキストモードを有効にします。
- コンテナインスタンスによる複数インスタンス機能は FMC を使用する Firepower Threat Defense に対してのみ使用できます。
- Firepower Threat Defense コンテナインスタンスの場合、1 つの FMC でセキュリティモジュール/エンジンのすべてのインスタンスを管理する必要があります。
- 最大 16 個のコンテナインスタンスの で TLS 暗号化アクセラレーションを有効にできます。
- Firepower Threat Defense コンテナインスタンスの場合、次の機能はサポートされていません。
  - Radware DefensePro リンクデコレータ
  - FMC UCAPL/CC モード
  - ハードウェアへのフローオフロード



## 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路でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

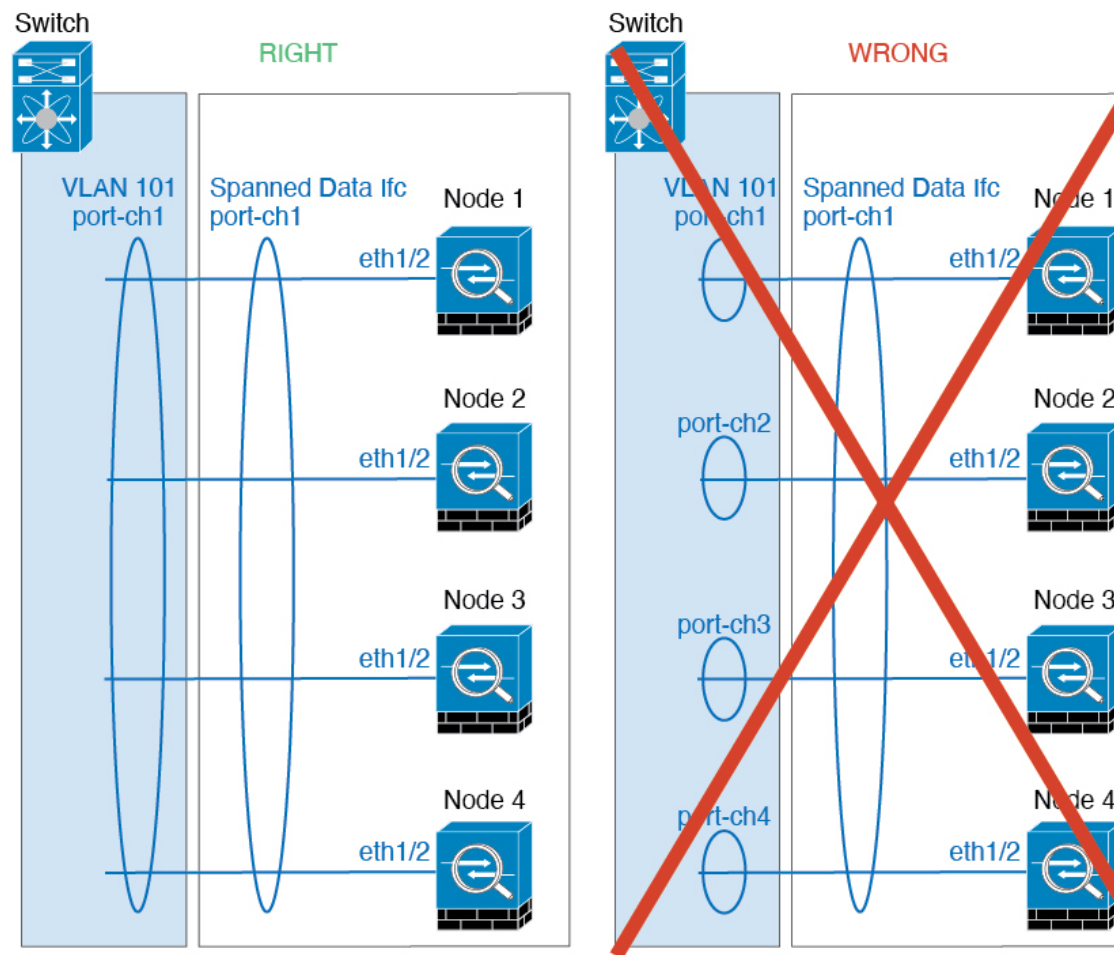
```
router(config)# port-channel id hash-distribution fixed
```

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

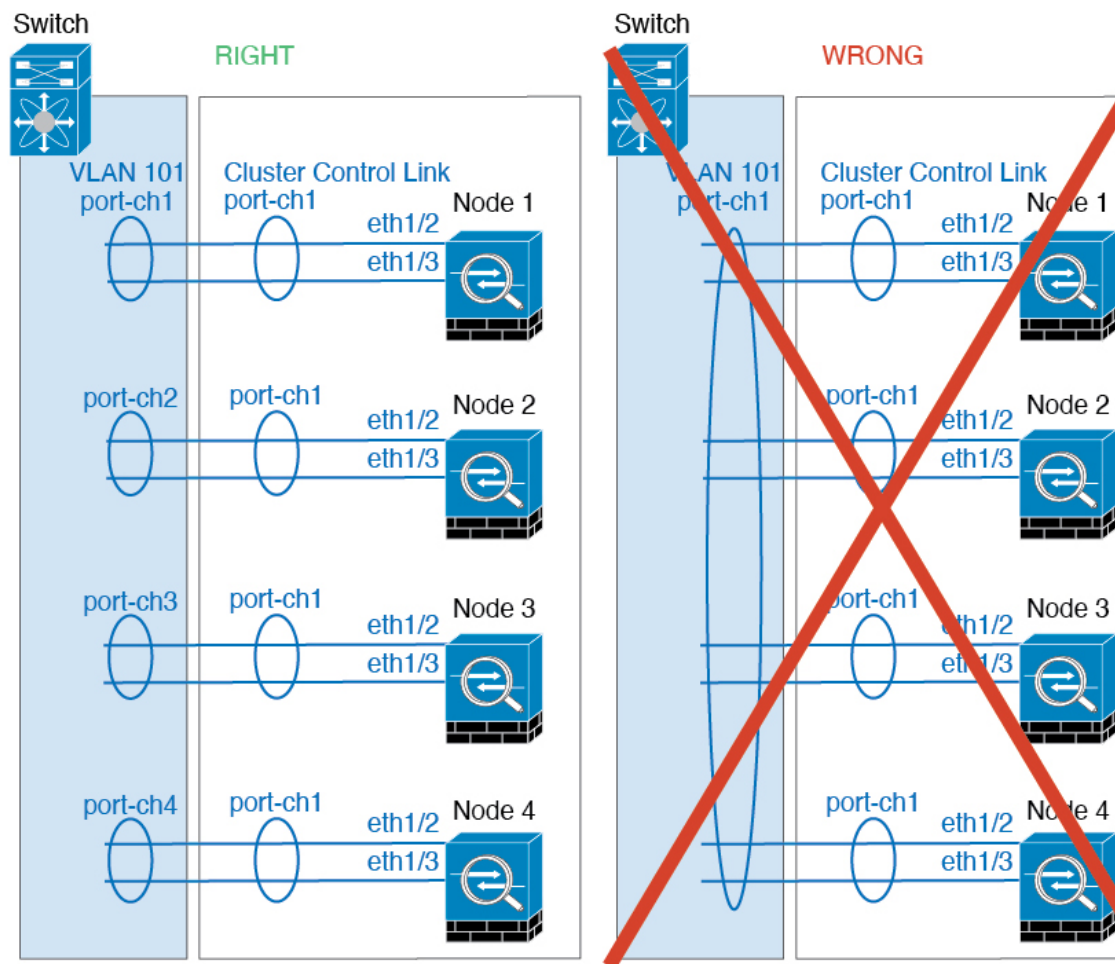
- Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速 (fast)] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサ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

### シャーシ間クラスタリングの EtherChannel

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



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



### サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

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

- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のルールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタローカリゼーションを有効にすると、ローカルディレクタのルールは（サイト ID に従って）常に接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。
- ディレクタローカリゼーションでは、次のトラフィックタイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーションクエリ。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタメンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイアウォール用に各サイトのデータネットワークとゲートウェイルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイルータは、HSRP などの First Hop Redundancy Protocol (FHRP) を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化 (OTV) または同様のものを使用してサイト全体にわたって拡張されます。ローカルゲートウェイルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。
- トランスペアレントモードでは、クラスタが HSRP ルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして。隣接ルータで HSRP が使用される場合、HSRP IP アドレス宛てのトラフィックは HSRP MAC アドレスに送信されますが、リターントラフィックは特定のルータのインターフェイスの MAC アドレスから HSRP ペアで送信されます。したがって、MAC アドレステーブルは通常、HSRP IP アドレスの ARP テーブルエントリが期限切れになり、が ARP 要求を送信して応答を受信した場合にのみ更新されます。の ARP テーブルエントリはデフォルトで 14400 秒後に期限切れになりますが、MAC アドレステーブルエントリはデフォルトで 300 秒後に期限切れになるため、MAC アドレステーブルの期限切れトラフィックのドロップを回避するために静的 MAC アドレスエントリが必要です。
- スパンド EtherChannel を使用したルーテッドモードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが 1 つのサイトで到達不能になった場合、トラフィックが他のサイトのクラスタノードに正常に到達できるように

フィルタを削除する必要があります。ダイナミックルーティングは、サイト間クラスタが拡張セグメントのファースト ホップ ルータとして機能する場合はサポートされません。

### その他のガイドライン

- ユニットの既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは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となります。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。

# スタンドアロン論理デバイスの追加

スタンドアロン論理デバイスは単独またはハイ アベイラビリティ ユニットとして使用できます。ハイ アベイラビリティの使用率の詳細については、[ハイ アベイラビリティ ペアの追加 \(57 ページ\)](#) を参照してください。

## スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュールクラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

Firepower 4100/9300 シャーシからルーテッドまたはトランスペアレントファイアウォールモード ASA を展開できます。

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

### 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 シャーシにダウンロードします。



(注) Firepower 9300 の場合、異なるアプリケーションタイプ (ASA および FTD) をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。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ポートと同じではありません (FXOS では、MGMT、management0 のような名前が表示されます)。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス

## 手順

**ステップ1** セキュリティ サービス モードを開始します。

**scope ssa**

例 :

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

**ステップ2** アプリケーション インスタンスのイメージ バージョンを設定します。

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

**show app**

例 :

```
Firepower /ssa # show app
  Name          Version          Author          Supported Deploy Types CSP Type      Is
Default App
-----
  asa           9.9.1            cisco           Native          Application No
  asa           9.10.1           cisco           Native          Application Yes
  ftd           6.2.3            cisco           Native          Application Yes
  ftd           6.3.0            cisco           Native,Container Application Yes
```

b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

**scope slot slot\_ID**

*slot\_id* は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例 :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) アプリケーション インスタンスを作成します。

**enter app-instance asa device\_name**

*Device\_name* は、1 ~ 64 文字の範囲で指定できます。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。

例 :

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) ASA イメージバージョンを選択します。

**set startup-version version**



例 :

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) スロット モードを終了します。

**exit**

例 :

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 終了して ssa モードにします。

**exit**

例 :

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例 :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

**ステップ 3** 論理デバイスを作成します。

**enter logical-device** *device\_name* **asa** *slot\_id* **standalone**

以前に追加したアプリケーション インスタンスと同じ *device\_name* を使用します。

例 :

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

**ステップ 4** 管理インターフェイスとデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

**create external-port-link** *name* *interface\_id* **asa**

**set description** *description*

**exit**

- *name* : この名前は Firepower 4100/9300 シャーシ スーパーバイザによって使用されます。これは ASA の設定で使用するインターフェイス名ではありません。
- *description* : フレーズを引用符 (") で囲み、スペースを追加します。

管理インターフェイスは、シャーマン管理ポートとは異なります。ASA のデータ インターフェイスを後で有効にして設定します。これには、IP アドレスの設定も含まれます。

例 :

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

**ステップ 5** 管理ブートストラップ情報を設定します。

- a) ブートストラップ オブジェクトを作成します。

**create mgmt-bootstrap asa**

例 :

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

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

**create bootstrap-key FIREWALL\_MODE**

**set value {routed | transparent}**

**exit**

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

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

例 :

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

- c) admin とイネーブル パスワードを指定します。

**create bootstrap-key-secret PASSWORD**

**set value**

値の入力 : *password*

値の確認 : *password*

**exit**

例 :

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

例 :

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

- d) IPv4 管理インターフェイスの設定を行います。

**create ipv4 slot\_id default**

**set ip ip\_address mask network\_mask**

**set gateway gateway\_address**

**exit**

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) IPv6 管理インターフェイスを設定します。

**create ipv6 slot\_id default**

**set ip ip\_address prefix-length prefix**

**set gateway gateway\_address**

**exit**

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- f) 管理ブートストラップ モードを終了します。

**exit**

例 :

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

## ステップ 6 設定を保存します。

### commit-buffer

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

例 :

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
asa	asa1	2	Disabled	Not Installed		9.12.1
	Native		Not Applicable	None		
ftd	ftd1	1	Enabled	Online	6.4.0.49	6.4.0.49
	Container	Default-Small	Not Applicable	None		

## ステップ 7 セキュリティ ポリシーの設定を開始するには、『ASA 設定ガイド』を参照してください。

例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

## FMC のスタンドアロン FTD の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュールクラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用できます。

### 始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシにダウンロードします。



(注) Firepower 9300 の場合、異なるアプリケーションタイプ (ASA および FTD) をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーションインスタンスタイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。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ポートと同じではありません (FXOS では、MGMT、management0 のような名前が表示されます)。
- 後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。詳細については、[FTD コマンドリファレンス](#)の **configure network management-data-interface** コマンドを参照してください。
- また、少なくとも1つのデータタイプのインターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック (Web イベントなど) を運ぶ

firepower-eventing インターフェイスも作成できます。詳細については、「[インターフェイス タイプ](#)」を参照してください。

- 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、[コンテナインスタンスにリソースプロファイルを追加](#)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。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。詳細については、[セキュリティ モジュール/エンジンの最初期化](#)を参照してください。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - FMC 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス
  - Firepower Threat Defense ホスト名とドメイン名

## 手順

**ステップ 1** セキュリティ サービス モードを開始します。

**scope ssa**

例 :

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

**ステップ 2** 使用する Firepower Threat Defense バージョンのエンドユーザーライセンス契約書に同意します。この手順を実行する必要があるのは、該当するバージョンの EULA にまだ同意していない場合のみです。

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

**show app**

例 :

```

Firepower /ssa # show app
Name      Version      Author      Supported Deploy Types CSP Type      Is
Default App
-----
asa       9.9.1        cisco       Native        Application No
ftd       9.10.1       cisco       Native        Application Yes
ftd       6.2.3        cisco       Native        Application Yes
ftd       6.3.0        cisco       Native,Container Application Yes

```

- b) 範囲をイメージバージョンに設定します。

**scope app ftd application\_version**

例 :

```

Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #

```

- c) ライセンス契約に同意します。

**accept-license-agreement**

例 :

```

Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #

```

- d) 設定を保存します。

**commit-buffer**

例 :

```

Firepower /ssa/app* # commit-buffer

```

```
Firepower /ssa/app #
```

- e) 終了してセキュリティサービスモードを開始します。

**exit**

例：

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

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

- a) コンテナインスタンスの場合は、使用可能なリソースプロファイルを表示します。プロファイルを追加する場合は、[コンテナインスタンスにリソースプロファイルを追加](#)を参照してください。

**show resource-profile**

使用するプロファイル名を書き留めます。

例：

```
Firepower /ssa # show resource-profile
```

Profile Name	Core Count	RAM Size (MB)	App Name	App Version	Is In Use	Security Model	CPU Logical
			Default Profile	Profile	Profile	Description	
bronze	6		N/A	No	No	all	
			N/A	No	Custom	low end device	
silver 1	8		N/A	No	No	all	
			N/A	No	Custom	mid-level	

- b) セキュリティモジュール/エンジンスロットに範囲を設定します。

**scope slot slot\_ID**

*slot\_id* は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

- c) アプリケーションインスタンスを作成します。

**enter app-instance ftd device\_name**

*Device\_name* は、1～64文字の範囲で指定できます。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。

例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
```



```
Firepower /ssa/slot/app-instance* #
```

- d) コンテナ インスタンスの場合は、コンテナにアプリケーション インスタンス タイプを設定します。

**set deploy-type container**

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。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つのみインストールできます。

設定の保存後に、インスタンス タイプを変更することはできません。デフォルトタイプは **native** です。

例 :

```
Firepower /ssa/slot/app-instance* # set deploy-type container
```

- e) コンテナ インスタンスの場合は、リソース プロファイルを指定します。

**set resource-profile-name name**

このプロファイル名はすでに存在する必要があります。

後でさまざまなリソース プロファイルを割り当てると、インスタンスがリロードされ、この操作に約5分かかることがあります。確立されたハイアベイラビリティ ペアの場合に、異なるサイズのリソース プロファイルを割り当てるときは、すべてのメンバのサイズが同じであることをできるだけ早く確認してください。

例 :

```
Firepower /ssa/slot/app-instance* # set resource-profile-name bronze
```

- f) Firepower Threat Defense イメージバージョンを設定します。

**set startup-version version**

EULA に同意するときに上記の手順でメモしたバージョン番号を入力します。

例 :

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

- g) コンテナ インスタンスの場合は、TLS 暗号化アクセラレーションをイネーブルまたはディセーブルにします。

**enter hw-crypto**

**set admin-state {enabled | disabled}**

**exit**

この設定により、ハードウェアの TLS 暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。この機能はデフォルトでイネーブルになっています。セキュリティモジュールごとに最大 16 個のインスタンスについて TLS 暗号化アクセラレーションを有効にできます。この機能はネイティブインスタンスではサポートされていません。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。バージョン 2 とは、FXOS 2.7 以降で使用される TLS 暗号化アクセラレーションタイプを指しています。

例：

```
Firepower /ssa/slot/app-instance* # enter hw-crypto
Firepower /ssa/slot/app-instance/hw-crypto* # set admin-state enabled
Firepower /ssa/slot/app-instance/hw-crypto* # exit
Firepower /ssa/slot/app-instance* # commit-buffer
Firepower /ssa/slot/app-instance # show hw-crypto
Hardware Crypto:
  Admin State           Hardware Crypto Size      Hardware Crypto Version
  -----
  enabled                40%                        2
```

- h) スロット モードを終了します。

**exit**

例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- i) (任意) Firepower 4110 または 4120 の Radware DefensePro インスタンスを作成します。このためには、論理デバイスの作成前にアプリケーションインスタンスを作成する必要があります (Radware DefensePro はコンテナインスタンスでサポートされていません)。

**enter app-instance vdp devicename**

**exit**

Firepower Threat Defense アプリケーションインスタンスに一致するように *device\_name* を設定します。論理デバイスの設定を完了したら、続いて Firepower Threat Defense 論理デバイスを使用して、サービスチェーン内に Radware DefensePro デコレータを設定する必要があります。[スタンドアロンの論理デバイスでの Radware DefensePro の設定 \(97 ページ\)](#) を、手順 4 から参照してください。

例：

```
Firepower /ssa/slot* # enter app-instance vdp FTD1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- j) 終了して ssa モードにします。

**exit**

例 :

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例 :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

**ステップ 4** 論理デバイスを作成します。

**enter logical-device *device\_name* ftd *slot\_id* standalone**

以前に追加したアプリケーションインスタンスと同じ *device\_name* を使用します。

例 :

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

**ステップ 5** 管理インターフェイスとデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

**create external-port-link *name* *interface\_id* ftd**

**set description *description***

**exit**

- *name* : この名前は Firepower 4100/9300 シャーシスーパーバイザによって使用されます。これは Firepower Threat Defense の設定で使用するインターフェイス名ではありません。
- *description* : フレーズを引用符 (") で囲み、スペースを追加します。

管理インターフェイスは、シャーシ管理ポートとは異なります。後で、FMC でデータインターフェイスを有効にして設定します。これには IP アドレスの設定も含まれます。

コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナ インスタンスに割り当てることができます。

例 :

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
```

```

Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit

```

**ステップ 6** リンク状態の同期を有効にします。

#### set link state sync enabled

シャーシでは、Firepower Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firepower Threat Defense アプリケーションインターフェイスの管理状態は考慮されません。Firepower Threat Defense からの同期がない場合は、たとえば、Firepower Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Firepower Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、Firepower Threat Defense が処理できるようになる前に外部ルータが Firepower Threat Defense へのトラフィックの送信を開始することがあるためです。

この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。この機能は、管理やクラスタなどの非データインターフェイスには影響しません。

Firepower Threat Defense のリンク状態の同期を有効にすると、FXOS のインターフェイスの [サービス状態 (Service State)] が Firepower Threat Defense のこのインターフェイスの管理状態と同期されます。たとえば、Firepower Threat Defense でインターフェイスをシャットダウンすると、サービス状態は [無効 (Disabled)] と表示されます。Firepower Threat Defense アプリケーションをシャットダウンすると、すべてのインターフェイスが [無効 (Disabled)] と表示されます。ハードウェア バイパス インターフェイスの場合、Firepower Threat Defense でインターフェイスを管理上の目的でシャットダウンすると、サービス状態が [無効 (Disabled)] に設定されます。ただし、Firepower Threat Defense アプリケーションのシャットダウンや他のシャーシレベルのシャットダウン (電源オフなど) では、インターフェイスペアは有効な状態を維持します。

Firepower Threat Defense のリンク状態の同期を無効にすると、サービス状態は常に [有効 (Enabled)] と表示されます。

(注) この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する Firepower Threat Defense ではサポートされません。ASA ではサポートされていません。

インターフェイスの現在のサービス状態と最後のダウンの理由を表示するには、**show interface expand detail** コマンドを入力します。

例 :

```

Firepower /ssa/logical-device* # set link state sync enabled
Firepower /ssa/logical-device* # scope eth-uplink
Firepower /eth-uplink* # scope fabric a
Firepower /eth-uplink/fabric* # show interface expand detail
Interface:

```

```

Port Name: Ethernet1/2
User Label:
Port Type: Data
Admin State: Enabled
Oper State: Up
State Reason:
flow control policy: default
Auto negotiation: Yes
Admin Speed: 1 Gbps
Oper Speed: 1 Gbps
Admin Duplex: Full Duplex
Oper Duplex: Full Duplex
Ethernet Link Profile name: default
Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
Ulld Oper State: Admin Disabled
Inline Pair Admin State: Enabled
Inline Pair Peer Port Name:
Service State: Enabled
Last Service State Down Reason: None
Allowed Vlan: All
Network Control Policy: default
Current Task:
<...>

```

### ステップ7 管理ブートストラップパラメータを設定します。

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

- a) ブートストラップオブジェクトを作成します。

#### **create mgmt-bootstrap ftd**

例：

```

Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

- b) ネイティブインスタンスの場合、マネージャを FMC に設定します。

#### **enter bootstrap-key MANAGEMENT\_TYPE**

**set value FMC**

**exit**

ネイティブインスタンスは、マネージャとしての FDM もサポートしています。論理デバイスを展開した後にマネージャタイプを変更することはできません。

例：

```

Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key MANAGEMENT_TYPE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value FMC
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

- c) FMC を管理する IP アドレス、ホスト名、または NAT ID を指定します。

次のいずれかを設定します。

- **enter bootstrap-key FIREPOWER\_MANAGER\_IP**

```
set value IP_address
```

```
exit
```

- **enter bootstrap-key FQDN**

```
set value fmc_hostname
```

```
exit
```

- **enter bootstrap-key NAT\_ID**

```
set value nat_id
```

```
exit
```

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。FMC がデバイスの IP アドレスを指定し、デバイスが FMC 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。FMC 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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key
FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

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

- **create bootstrap-key FIREWALL\_MODE**

```
set value {routed | transparent}
```

```
exit
```

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

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

例：

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

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

- e) デバイスと FMC との間で共有するキーを指定します。このキーのパスフレーズは、1～37 文字の範囲で選択できます。Firepower Threat Defense を追加するときに、FMC に同じキーを入力します。

**create bootstrap-key-secret REGISTRATION\_KEY**

**set value**

値の入力 : *registration\_key*

値の確認 : *registration\_key*

**exit**

例 :

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

- f) 管理者のパスワードを指定します。このパスワードは、管理ユーザーの CLI アクセスに使用されます。

**create bootstrap-key-secret PASSWORD**

**set value**

値の入力 : *password*

値の確認 : *password*

**exit**

例 :

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

- g) 完全修飾ホスト名を指定します。

**create bootstrap-key FQDN**

**set value fqdn**

**exit**

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftdl.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) DNS サーバーのカンマ区切りリストを指定します。

**create bootstrap-key DNS\_SERVERS**

**set value** *dns\_servers*

**exit**

たとえば、FMCのホスト名を指定する場合、Firepower Threat DefenseはDNSを使用しません。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) 検索ドメインのカンマ区切りリストを指定します。

**create bootstrap-key SEARCH\_DOMAINS**

**set value** *search\_domains*

**exit**

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- j) (任意) コンテナインスタンスに対して、Firepower Threat Defense SSHセッションでエキスパートモードを許可します。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 Firepower Threat Defense シェルからアクセスできます。

**create bootstrap-key PERMIT\_EXPERT\_MODE**

**set value** {yes | no}

**exit**

- **yes** : SSHセッションからこのコンテナインスタンスに直接アクセスするユーザーが、エキスパートモードを開始できます。
- **no** : 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。



デフォルトでは、コンテナインスタンスの場合、エキスパートモードを使用できるのは FXOS CLI から Firepower Threat Defense CLI にアクセスするユーザーだけです。この制限は、インスタンス間の分離を増やす場合、コンテナ インスタンスのみに適用されます。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、Firepower Threat Defense CLI で **expert** コマンドを使用します。

例 :

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

- k) IPv4 管理インターフェイスの設定を行います。

```
create ipv4 slot_id firepower
set ip ip_address mask network_mask
set gateway gateway_address
exit
```

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- l) IPv6 管理インターフェイスを設定します。

```
create ipv6 slot_id firepower
set ip ip_address prefix-length prefix
set gateway gateway_address
exit
```

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- m) 管理ブートストラップ モードを終了します。

```
exit
```

例 :

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

**ステップ 8** 設定を保存します。

#### commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。

[Admin State (管理状態)] が [Enabled (有効)] で、[Oper State] が [Online] の場合、アプリケーションインスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup
Version Deploy Type Profile Name Cluster State Cluster Role
-----
asa          asa1          2          Disabled  Not Installed          9.12.1
Native
Not Applicable None
ftd          ftd1          1          Enabled   Online                6.4.0.49      6.4.0.49
Container   Default-Small Not Applicable None
```

**ステップ 9** Firepower Threat Defense を管理対象デバイスとして追加し、セキュリティポリシーの設定を開始するには、FMC コンフィギュレーションガイドを参照してください。

例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

## FDM のスタンドアロン FTD を追加します。

FDM はネイティブインスタンスで使用できます。コンテナインスタンスはサポートされていません。スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。

### 始める前に

- 論理デバイスに使用するアプリケーションイメージを [Cisco.com](https://www.cisco.com) からダウンロードして、そのイメージを Firepower 4100/9300 シャーシにダウンロードします。



(注) Firepower 9300 の場合、異なるアプリケーションタイプ (ASA および FTD) をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーションインスタンスタイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。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

FDM のスタンドアロン FTD を追加します。

ポートと同じではありません (FXOS では、MGMT、management0 のような名前が表示されます)。

- また、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - DNS サーバの IP アドレス
  - FTD ホスト名とドメイン名

## 手順

**ステップ 1** セキュリティ サービス モードを開始します。

**scope ssa**

例 :

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

**ステップ 2** 使用する Firepower Threat Defense バージョンのエンドユーザーライセンス契約書に同意します。この手順を実行する必要があるのは、該当するバージョンの EULA にまだ同意していない場合のみです。

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

**show app**

例 :

```
Firepower /ssa # show app
  Name          Version      Author      Supported Deploy Types CSP Type   Is
Default App
-----
  asa           9.9.1       cisco      Native      Application No
  asa           9.10.1      cisco      Native      Application Yes
  ftd           6.2.3       cisco      Native      Application Yes
  ftd           6.3.0       cisco      Native,Container Application Yes
```

b) 範囲をイメージバージョンに設定します。

**scope app ftd application\_version**

例 :

```
Firepower /ssa # scope app ftd 6.5.0
Firepower /ssa/app #
```

- c) ライセンス契約に同意します。

#### **accept-license-agreement**

例 :

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

- d) 設定を保存します。

#### **commit-buffer**

例 :

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

- e) 終了してセキュリティサービスモードを開始します。

#### **exit**

例 :

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

**ステップ 3** アプリケーションインスタンスのイメージバージョンを設定します。

- a) セキュリティ モジュール/エンジン スロットに範囲を設定します。

FDM のスタンドアロン FTD を追加します。

### scope slot *slot\_ID*

*slot\_id* は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

- b) アプリケーション インスタンスを作成します。

### enter app-instance ftd *device\_name*

*Device\_name* は、1 ~ 64 文字の範囲で指定できます。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。

例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

- c) Firepower Threat Defense イメージバージョンを設定します。

### set startup-version *version*

EULA に同意するときに上記の手順でメモしたバージョン番号を入力します。

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.5.0
```

- d) スロット モードを終了します。

### exit

例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- e) (任意) Firepower 4110 または 4120 の Radware DefensePro インスタンスを作成します。そのためには、論理デバイス作成の前にアプリケーションインスタンスを作成する必要があります。

### enter app-instance vdp *devicename*

### exit

Firepower Threat Defense アプリケーションインスタンスに一致するように *device\_name* を設定します。論理デバイスの設定を完了したら、続いて Firepower Threat Defense 論理デバイスを使用して、サービスチェーン内に Radware DefensePro デコレータを設定する必要があります。[スタンドアロンの論理デバイスでの Radware DefensePro の設定 \(97 ページ\)](#) を、手順 4 から参照してください。

例：

```
Firepower /ssa/slot* # enter app-instance vdp FTD1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 終了して ssa モードにします。

**exit**

例 :

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例 :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 6.5.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

**ステップ 4** 論理デバイスを作成します。

**enter logical-device *device\_name* ftd *slot\_id* standalone**

以前に追加したアプリケーションインスタンスと同じ *device\_name* を使用します。

例 :

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

**ステップ 5** 管理インターフェイスとデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

**create external-port-link *name* *interface\_id* ftd**

**set description *description***

**exit**

- *name* : この名前は Firepower 4100/9300 シャーシスーパーバイザによって使用されます。これは Firepower Threat Defense の設定で使用するインターフェイス名ではありません。
- *description* : フレーズを引用符 (") で囲み、スペースを追加します。

管理インターフェイスは、シャーシ管理ポートとは異なります。後で、FDM でデータインターフェイスを有効にして設定します。これには IP アドレスの設定も含まれます。

例 :

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
```

■ FDM のスタンドアロン FTD を追加します。

```
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

## ステップ 6 リンク状態の同期を有効にします。

### set link state sync enabled

シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーションインターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、デバイスが処理できるようになる前に外部ルータが FTD デバイスへのトラフィックの送信を開始することがあるためです。

この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。この機能は、管理やクラスタなどの非データインターフェイスには影響しません。

FTD のリンク状態の同期を有効にすると、FXOS のインターフェイスの [サービス状態 (Service State)] が FTD のこのインターフェイスの管理状態と同期されます。たとえば、FTD でインターフェイスをシャットダウンすると、サービス状態は [無効 (Disabled)] と表示されます。FTD アプリケーションをシャットダウンすると、すべてのインターフェイスが [無効 (Disabled)] と表示されます。ハードウェア バイパス インターフェイスの場合、FTD でインターフェイスを管理上の目的でシャットダウンすると、サービス状態が [無効 (Disabled)] に設定されます。ただし、FTD アプリケーションのシャットダウンや他のシャーシレベルのシャットダウン (電源オフなど) では、インターフェイスペアは有効な状態を維持します。

FTD のリンク状態の同期を無効にすると、サービス状態は常に [有効 (Enabled)] と表示されます。

(注) この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する FTD ではサポートされません。ASA ではサポートされていません。

インターフェイスの現在のサービス状態と最後のダウンの理由を表示するには、**show interface expand detail** コマンドを入力します。

例：

```
Firepower /ssa/logical-device* # set link state sync enabled
Firepower /ssa/logical-device* # scope eth-uplink
Firepower /eth-uplink* # scope fabric a
Firepower /eth-uplink/fabric* # show interface expand detail
Interface:
  Port Name: Ethernet1/2
```



```

User Label:
Port Type: Data
Admin State: Enabled
Oper State: Up
State Reason:
flow control policy: default
Auto negotiation: Yes
Admin Speed: 1 Gbps
Oper Speed: 1 Gbps
Admin Duplex: Full Duplex
Oper Duplex: Full Duplex
Ethernet Link Profile name: default
Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
Ulld Oper State: Admin Disabled
Inline Pair Admin State: Enabled
Inline Pair Peer Port Name:
Service State: Enabled
Last Service State Down Reason: None
Allowed Vlan: All
Network Control Policy: default
Current Task:
<...>

```

### ステップ7 管理ブートストラップパラメータを設定します。

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

- a) ブートストラップオブジェクトを作成します。

#### **create mgmt-bootstrap ftd**

例：

```

Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

- b) ネイティブインスタンスの場合、マネージャを FDM に設定します。

#### **enter bootstrap-key MANAGEMENT\_TYPE**

**set value LOCALLY\_MANAGED**

**exit**

ネイティブインスタンスは、マネージャとしての FMC もサポートしています。論理デバイスを展開した後にマネージャタイプを変更することはできません。

例：

```

Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key MANAGEMENT_TYPE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

- c) 管理者のパスワードを指定します。このパスワードは、管理ユーザーの CLI アクセスに使用されます。

#### **create bootstrap-key-secret PASSWORD**

■ FDM のスタンドアロン FTD を追加します。

**set value**

値の入力 : *password*

値の確認 : *password*

**exit**

例 :

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

- d) 完全修飾ホスト名を指定します。

**create bootstrap-key FQDN**

**set value** *fqdn*

**exit**

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftdl.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) DNS サーバーのカンマ区切りリストを指定します。

**create bootstrap-key DNS\_SERVERS**

**set value** *dns\_servers*

**exit**

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- f) 検索ドメインのカンマ区切りリストを指定します。

**create bootstrap-key SEARCH\_DOMAINS**

**set value** *search\_domains*

**exit**

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
```

```
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- g) IPv4 管理インターフェイスの設定を行います。

```
create ipv4 slot_id firepower
set ip ip_address mask network_mask
set gateway gateway_address
exit
```

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) IPv6 管理インターフェイスを設定します。

```
create ipv6 slot_id firepower
set ip ip_address prefix-length prefix
set gateway gateway_address
exit
```

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) 管理ブートストラップ モードを終了します。

```
exit
```

例 :

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

- ステップ 8** 設定を保存します。

```
commit-buffer
```

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。 **show app-instance** コマンドを使用して、展開のステータスを確認します。

FDM のスタンドアロン FTD を追加します。

[Admin State (管理状態)] が [Enabled (有効)] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
asa	asal	2	Disabled	Not Installed		9.12.1
	Native		Not Applicable	None		
ftd	ftdl	1	Enabled	Online	6.4.0.49	6.4.0.49
	Container	Default-Small	Not Applicable	None		

**ステップ 9** セキュリティポリシーの設定を始めるには、FDM のコンフィギュレーションガイドを参照してください。

例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.5.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd
Firepower /ssa/slot/app-instance* # set startup-version 6.5.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

## ハイアベイラビリティペアの追加

FTD または ASA ハイアベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイアベイラビリティのシャーシを準備するには、次の手順を参照してください。

### 始める前に

[ハイアベイラビリティの要件と前提条件（18 ページ）](#) を参照してください。

### 手順

- ステップ 1** 各論理デバイスに同一のインターフェイスを割り当てます。
- ステップ 2** フェールオーバーリンクとステートリンクに1つまたは2つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシの間でハイアベイラビリティトラフィックをやり取りします。統合されたフェールオーバーリンクとステートリンクには、10 GB のデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがある場合、別のフェールオーバーリンクとステートリンクを使用できます。ステートリンクが帯域幅の大半を必要とします。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。同じネットワークセグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

コンテナインスタンスの場合、フェールオーバーリンク用のデータ共有インターフェイスはサポートされていません。親インターフェイスまたは EtherChannel でサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバーリンクとして使用することをお勧めします。同じ親のすべてのサブインターフェイスをフェールオーバーリンクとして使用する必要があることに注意してください。あるサブインターフェイスをフェールオーバーリンクとして使用する一方で、他のサブインターフェイス（または親インターフェイス）を通常のデータインターフェイスとして使用することはできません。

- ステップ 3** 論理デバイスでハイアベイラビリティを有効にします。
- ステップ 4** ハイアベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

- (注) ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワークモジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できません。

## クラスタの追加

クラスタリングを利用すると、複数のデバイスをグループ化して1つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。複数のモジュールを含む Firepower 9300 は、1つのシャーシ内のすべてのモジュールをクラスタにグループ化する、シャーシ内クラスタリングをサポートします。複数のシャーシをまとめてグループ化する、シャーシ間クラスタリングも使用できます。シャーシ間クラスタリングは、Firepower 4100 シリーズなどの単一モジュールデバイスの唯一のオプションです。

## 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ーバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。

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

シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インター

フェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータ インターフェイスが機能します。シャーシ間クラスタリングでは、すべてのデータ インターフェイスでスパンド EtherChannel を使用します。



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

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

## プライマリユニットとセカンダリユニットの役割

クラスタのメンバの1つがプライマリユニットになります。プライマリユニットは自動的に決定されます。他のすべてのメンバはセカンダリ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標準出荷単位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、セカンダリ単位に複製されます。

## 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。

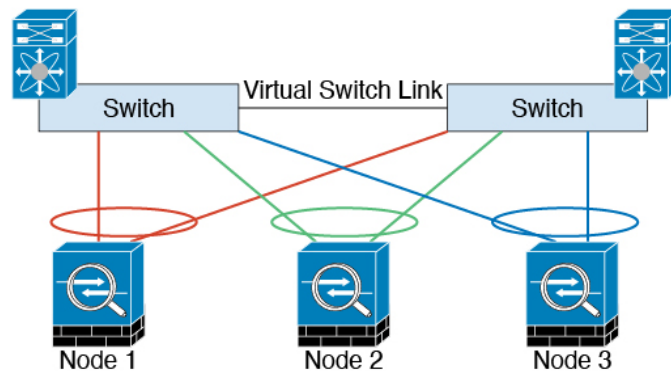
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。



(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、スタンド 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せん。クラスタを展開するときに、この IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ2スイッチングだけが許可されています。サイト間トラフィックには、オーバーレイ トランスポート 仮想化 (OTV) を使用することをお勧めします。

## 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。

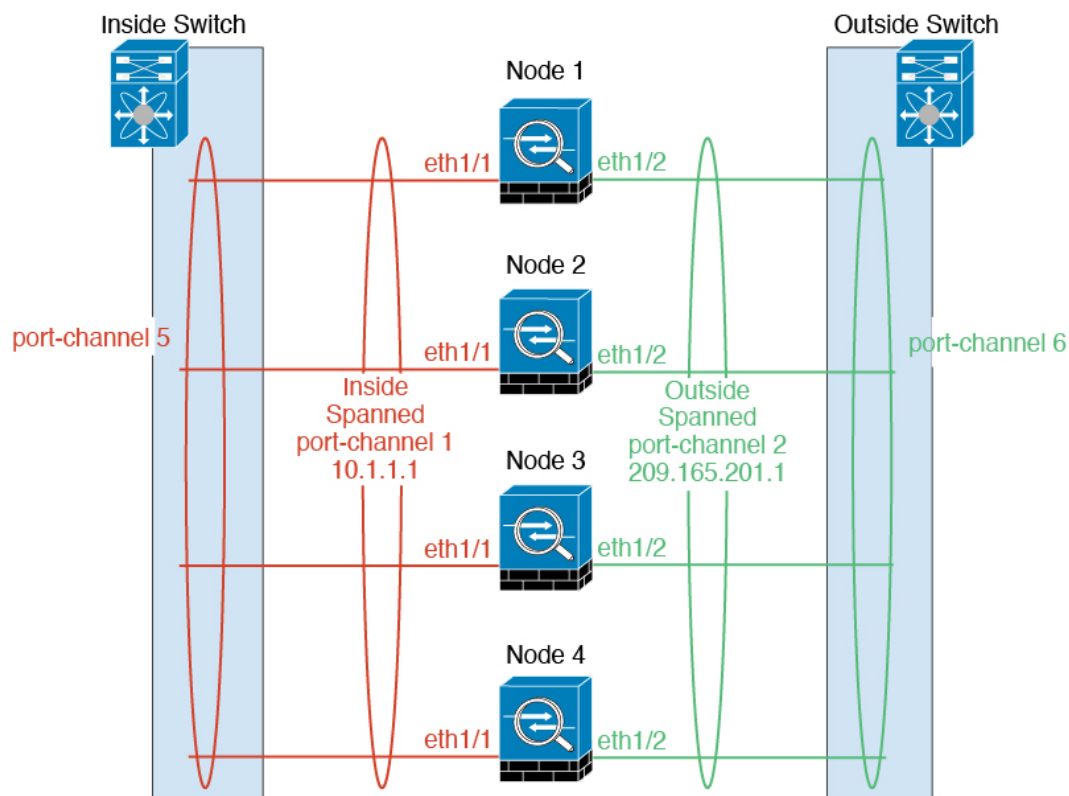
ASA の場合は、メインクラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の標準出荷単位に属します。アドレス範囲も設定して、現在の標準出荷単位を含む各単位がその範囲内のローカルアドレスを使用できるようにする必要があります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。標準出荷単位が変更されると、メインクラスタ IP アドレスは新しい標準出荷単位に移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の標準出荷単位に関連付けられています。個々のメンバーを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、標準出荷単位を含む各単位は、ローカル IP アドレスを使用してサーバに接続します。

Firepower Threat Defense では、同じネットワークの各単位に管理 IP アドレスを割り当てます。各単位を FMC に追加するときは、次の IP アドレスを使用します。

## スパンド EtherChannel

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



## サイト間クラスタリング

サイト間インストールの場合、次の推奨ガイドラインに従う限り、クラスタリングを利用できません。

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッドモードでサポートされます。

サイト ID は、LISP インスペクションを使用するフローモビリティ、データセンターのサイト間クラスタリングのパフォーマンスを向上し、ラウンドトリップ時間の遅延を減少させるためのディレクタ ローカリゼーション、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトにある接続のサイト冗長性を有効にするためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング : [クラスタリングの要件と前提条件 \(13 ページ\)](#)

- サイト間のガイドライン： [クラスタリング ガイドラインと制限事項](#) (21 ページ)
- サイト間での例： [サイト間クラスタリングの例](#) (123 ページ)

## ASA クラスタの追加

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

### ASA クラスタの作成

範囲をイメージバージョンに設定します。

クラスタは、Firepower 4100/9300 シャーシスーパー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。

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

#### 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](http://Cisco.com) からダウンロードして、そのイメージを Firepower 4100/9300 シャーシにアップロードします。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレスおよびネットワークマスク
  - ゲートウェイ IP アドレス

#### 手順

- ステップ 1** インターフェイスを設定します。
- ステップ 2** セキュリティ サービス モードを開始します。

**scope ssa**

例：

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

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

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

#### **show app**

例：

```
Firepower /ssa # show app
Name          Version      Author      Supported Deploy Types CSP Type      Is
Default App
-----
-----
asa           9.9.1        cisco       Native        Application No
asa           9.10.1       cisco       Native        Application Yes
ftd           6.2.3        cisco       Native        Application Yes
ftd           6.3.0        cisco       Native,Container Application Yes
```

b) 範囲をイメージバージョンに設定します。

#### **scope app asa application\_version**

例：

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

c) このバージョンをデフォルトとして設定します。

#### **set-default**

例：

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

d) 終了して ssa モードにします。

#### **exit**

例：

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

例：

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

**ステップ 4** クラスタを作成します。

**enter logical-device *device\_name* asa slots clustered**

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

例 :

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

**ステップ 5** クラスタ ブートストラップのパラメータを設定します。

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

a) クラスタ ブートストラップ オブジェクトを作成します。

**enter cluster-bootstrap**

例 :

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

b) シャーシ ID を設定します。

**set chassis-id *id***

クラスタの各シャーシは一意的 ID が必要です。

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

**set site-id *number*.**

サイト ID を削除するには、値を **0** に設定します。

例 :

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

d) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

**set key**

例：

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

共有秘密を入力するように求められます。

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

- e) クラスタ インターフェイス モードを設定します。

#### **set mode spanned-etherchannel**

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

例：

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

- f) セキュリティ モジュール設定でクラスタ グループ名を設定します。

#### **set service-type cluster\_name**

名前は1～38文字のASCII文字列であることが必要です。

例：

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

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

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

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

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

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

例：

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

- h) 管理 IP アドレス情報を設定します。

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

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

```
set ipv4 pool start_ip end_ip
```

```
set ipv6 pool start_ip end_ip
```

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュールスロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在の制御ユニットに属する仮想 IP アドレス（メインクラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

2. 管理インターフェイスのメインクラスタ IP アドレスを設定します。

```
set virtual ipv4 ip_address mask mask
```

```
set virtual ipv6 ip_address prefix-length prefix
```

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

3. ネットワーク ゲートウェイ アドレスを入力します。

```
set ipv4 gateway ip_address
```

```
set ipv6 gateway ip_address
```

例 :

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

- i) クラスタ ブートストラップ モードを終了します。

```
exit
```

例 :

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
```

```

Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #

```

## ステップ6 管理ブートストラップパラメータを設定します。

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

- a) 管理ブートストラップ オブジェクトを作成します。

**enter mgmt-bootstrap asa**

例：

```

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

```

- b) admin とイネーブル パスワードを指定します。

**create bootstrap-key-secret PASSWORD**

**set value**

値の入力：*password*

値の確認：*password*

**exit**

例：

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

例：

```

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

```

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

**create bootstrap-key FIREWALL\_MODE**

**set value {routed | transparent}**

**exit**

ルーテッドモードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペ



アレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。

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

例：

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

d) 管理ブートストラップモードを終了します。

**exit**

例：

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

**ステップ7** 設定を保存します。

#### **commit-buffer**

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

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
ftd	cluster1	1	Enabled	Online	7.3.0.49	7.3.0.49
	Native		In Cluster	Data Node		
ftd	cluster1	2	Enabled	Online	7.3.0.49	7.3.0.49
	Native		In Cluster	Control Node		
ftd	cluster1	3	Disabled	Not Available		7.3.0.49
	Native		Not Applicable	None		

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

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

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

## 例

シャーシ 1 :

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

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
  enter cluster-bootstrap
  set chassis-id 1
```

```
set ipv4 gateway 10.1.1.254
set ipv4 pool 10.1.1.11 10.1.1.27
set ipv6 gateway 2001:DB8::AA
set ipv6 pool 2001:DB8::11 2001:DB8::27
set key
Key: f@arscape
set mode spanned-etherchannel
set service-type cluster1
set virtual ipv4 10.1.1.1 mask 255.255.255.0
set virtual ipv6 2001:DB8::1 prefix-length 64
exit
exit
scope app asa 9.5.2.1
set-default
exit
commit-buffer
```

シヤーン2 :

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

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

## クラスタ メンバの追加

ASA クラスタメンバーを追加または置き換えます。



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

### 始める前に

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

### 手順

ステップ1 [OK] をクリックします。

**ステップ2** クラスタに別のシャーシを追加する場合は、[ASA クラスタの作成 \(63 ページ\)](#) の手順を繰り返しますが、一意の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、新しいシャーシに同じ設定を使用します。

## FTD 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、次のシャーシにほぼ同じ設定を入力します。

## FTD クラスタの作成

クラスタは、Firepower 4100/9300 シャーシスーパー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、[コンテナインスタンスにリソースプロファイルを追加](#)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。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。詳細については、[セキュリティ モジュール/エンジンの最初期化](#)を参照してください。

- 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
  - FMC 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス
  - FTD 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。

**ステップ 2** セキュリティ サービス モードを開始します。

### scope ssa

例 :

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

**ステップ 3** 使用する Firepower Threat Defense バージョンのエンドユーザーライセンス契約書に同意します。この手順を実行する必要があるのは、該当するバージョンの EULA にまだ同意していない場合のみです。

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

### show app

例 :

```
Firepower /ssa # show app
Name          Version      Author      Supported Deploy Types CSP Type  Is
Default App
-----
asa           9.9.1        cisco       Native      Application No
asa           9.10.1       cisco       Native      Application Yes
ftd           6.2.3        cisco       Native      Application Yes
ftd           6.3.0        cisco       Native,Container Application Yes
```

b) 範囲をイメージバージョンに設定します。

### scope app ftd application\_version

例 :

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

- c) ライセンス契約に同意します。

#### **accept-license-agreement**

例 :

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

- d) 設定を保存します。

#### **commit-buffer**

例 :

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

- e) 終了して ssa モードにします。

#### **exit**

例 :

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

例 :

```
Firepower /ssa # scope app ftd 6.3.0.21
```

```
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # exit
Firepower /ssa* #
```

**ステップ 4** アプリケーション インスタンス パラメータ（イメージバージョンを含む）を設定します。

- a) コンテナインスタンスの場合は、使用可能なリソースプロファイルを表示します。プロファイルを追加する場合は、[コンテナインスタンスにリソースプロファイルを追加](#)を参照してください。

#### **show resource-profile**

使用するプロファイル名を書き留めます。

例：

```
Firepower /ssa # show resource-profile
```

Profile Name	App Name	App Version	Is In Use	Security Model	CPU Logical
Core Count	RAM Size (MB)	Default Profile	Profile Type	Description	
bronze	N/A	N/A	No	all	
6	N/A	No	Custom	low end device	
silver 1	N/A	N/A	No	all	
8	N/A	No	Custom	mid-level	

- b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

#### **scope slot slot\_ID**

*slot\_id* は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

- c) アプリケーション インスタンスを作成します。

#### **enter app-instance ftd device\_name**

*Device\_name* は、1 ～ 64 文字の範囲で指定できます。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。

例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

- d) コンテナ インスタンスの場合は、コンテナにアプリケーション インスタンス タイプを設定します。

#### **set deploy-type container**



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。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つのみインストールできます。

設定の保存後に、インスタンスタイプを変更することはできません。デフォルトタイプは **native** です。

例：

```
Firepower /ssa/slot/app-instance* # set deploy-type container
```

- e) コンテナインスタンスの場合は、リソースプロファイルを指定します。

**set resource-profile-name** *name*

このプロファイル名はすでに存在している必要があります。

後でさまざまなリソースプロファイルを割り当てると、インスタンスがリロードされ、この操作に約5分かかることがあります。確立されたハイアベイラビリティペアまたはクラスタの場合に、異なるサイズのリソースプロファイルを割り当てるときは、すべてのメンバのサイズが同じであることをできるだけ早く確認してください。

例：

```
Firepower /ssa/slot/app-instance* # set resource-profile-name bronze
```

- f) イメージバージョンを設定します。

**set startup-version** *version*

この手順でメモしたバージョン番号を入力します。

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
```

- g) （任意）コンテナインスタンスの場合は、TLS 暗号化アクセラレーションをイネーブルまたはディセーブルにします。

**enter hw-crypto**

**set admin-state** {**enabled** | **disabled**}

**exit**

この設定により、ハードウェアの TLS 暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。この機能はデフォルトでイネーブルになっています。セキュリティモジュールごとに最大 16 個のインスタンスについて TLS 暗号化アクセラレーションを有効にできます。この機能はネイティブインスタンスではサポートされていません。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。バージョ

ン2 とは、FXOS 2.7 以降で使用される TLS 暗号アクセラレーションタイプを指しています。

例：

```
Firepower /ssa/slot/app-instance* # enter hw-crypto
Firepower /ssa/slot/app-instance/hw-crypto* # set admin-state enabled
Firepower /ssa/slot/app-instance/hw-crypto* # exit
Firepower /ssa/slot/app-instance* # commit-buffer
Firepower /ssa/slot/app-instance # show hw-crypto
Hardware Crypto:
  Admin State          Hardware Crypto Size    Hardware Crypto Version
-----
  enabled              40%                     2
```

h) スロットモードを終了します。

**exit**

例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

i) Firepower 9300 のコンテナインスタンスの場合は、これらの手順を繰り返して各セキュリティモジュールにコンテナインスタンスを作成します。

j) 終了して ssa モードにします。

**exit**

例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa # scope slot 2
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa # scope slot 3
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
```

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

**ステップ 5** クラスタを作成します。

**enter logical-device *device\_name* ftd slots clustered**

- *device\_name* : 以前に追加したアプリケーションインスタンスと同じ *device\_name* を使用します。
- スロット: シャーシモジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1,2,3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュールスロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

例 :

```
Firepower /ssa # enter logical-device FTD1 ftd 1,2,3 clustered
Firepower /ssa/logical-device* #
```

**ステップ 6** クラスタ ブートストラップのパラメータを設定します。

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

a) クラスタ ブートストラップ オブジェクトを作成します。

**enter cluster-bootstrap**

例 :

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

b) シャーシ ID を設定します。

**set chassis-id *id***

クラスタの各シャーシは一意的 ID が必要です。

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

**set site-id *number*.**

サイト ID を削除するには、値を **0** に設定します。

例 :

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

d) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

**set key**

例 :

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

共有秘密を入力するように求められます。

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

- e) クラスタ インターフェイス モードを設定します。

**set mode spanned-etherchannel**

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

例 :

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

- f) セキュリティ モジュール設定でクラスタ グループ名を設定します。

**set service-type cluster\_name**

名前は1～38文字のASCII文字列である必要があります。

例 :

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

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

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

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

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

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

例 :

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

```
10.10.0.0
```

- h) クラスタ ブートストラップ モードを終了します。

```
exit
```

例 :

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

### ステップ7 管理ブートストラップパラメータを設定します。

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

- a) 管理ブートストラップ オブジェクトを作成します。

```
enter mgmt-bootstrap ftd
```

例 :

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

- b) FMC を管理する IP アドレス、ホスト名または NAT ID を指定します。

次のいずれかを設定します。

- **enter bootstrap-key FIREPOWER\_MANAGER\_IP**

```
set value IP_address
```

```
exit
```

- **enter bootstrap-key FQDN**

```
set value fmc_hostname
```

```
exit
```

- **enter bootstrap-key NAT\_ID**

```
set value nat_id
```

```
exit
```

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。FMC がデバイスの IP アドレスを指定し、デバイスが FMC 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

側に一意的な 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。FMC 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。

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key NAT_ID
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value sc0rpius15
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

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

**create bootstrap-key FIREWALL\_MODE**

**set value {routed | transparent}**

**exit**

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

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

例 :

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

- d) デバイスと FMC との間で共有するキーを指定します。

**enter bootstrap-key-secret REGISTRATION\_KEY**

**set value**

値の入力 : *registration\_key*

値の確認 : *registration\_key*

**exit**

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。FMC を追加するときに、Firepower Threat Defense に同じキーを入力します。

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
```

```
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) CLI アクセスの Firepower Threat Defense 管理ユーザのパスワードを指定します。

**enter bootstrap-key-secret PASSWORD**

**set value**

値の入力 : *password*

値の確認 : *password*

**exit**

例 :

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

- f) 完全修飾ホスト名を指定します。

**enter bootstrap-key FQDN**

**set value fqdn**

**exit**

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

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftdcluster1.example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- g) DNS サーバーのカンマ区切りリストを指定します。

**enter bootstrap-key DNS\_SERVERS**

**set value dns\_servers**

**exit**

たとえば、FMC のホスト名を指定する場合、Firepower Threat Defense は DNS を使用しません。

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
```

```
10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) 検索ドメインのカンマ区切りリストを指定します。

```
enter bootstrap-key SEARCH_DOMAINS
```

```
set value search_domains
```

```
exit
```

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) (任意) コンテナインスタンスに対して、Firepower Threat Defense SSH セッションでエキスパートモードを許可します。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 Firepower Threat Defense シェルからアクセスできます。

```
create bootstrap-key PERMIT_EXPERT_MODE
```

```
set value {yes | no}
```

```
exit
```

- **yes** : SSH セッションからこのコンテナインスタンスに直接アクセスするユーザーが、エキスパートモードを開始できます。
- **no** : 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。

デフォルトでは、コンテナインスタンスの場合、エキスパートモードを使用できるのは FXOS CLI から Firepower Threat Defense CLI にアクセスするユーザーだけです。この制限は、インスタンス間の分離を増やす場合、コンテナインスタンスのみに適用されます。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、Firepower Threat Defense CLI で **expert** コマンドを使用します。

例 :

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

- j) クラスタ内の各セキュリティ モジュールの管理 IP アドレスを設定します。



- (注) Firepower 9300 の場合、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。

IPv4 管理インターフェイス オブジェクトを作成するには、次の手順を実行します。

1. 管理インターフェイス オブジェクトを作成します。  
**enter ipv4 slot\_id firepower**
2. ゲートウェイアドレスを設定します。  
**set gateway gateway\_address**
3. IP アドレスとマスクを設定します。  
**set ip ip\_address mask network\_mask**
4. 管理 IP モードを終了します。  
**exit**
5. シャーシの残りのモジュールに対して手順を繰り返します。

IPv6 管理インターフェイス オブジェクトを作成するには、次の手順を実行します。

1. 管理インターフェイス オブジェクトを作成します。  
**enter ipv6 slot\_id firepower**
2. ゲートウェイアドレスを設定します。  
**set gateway gateway\_address**
3. IP アドレスとプレフィックスを設定します。  
**set ip ip\_address prefix-length prefix**
4. 管理 IP モードを終了します。  
**exit**
5. シャーシの残りのモジュールに対して手順を繰り返します。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.35 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.36 mask
```

```

255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3211
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3212
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

k) 管理ブートストラップモードを終了します。

**exit**

例 :

```

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

```

例 :

```

Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: ziggy$tar dust
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: $pidersfrommars
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 1 firepower

```

```

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.32 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.33 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #

```

**ステップ 8** 設定を保存します。

#### commit-buffer

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

例：

```

Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance

```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Version	Deploy Type	Profile Name	Cluster State	Cluster Role		
ftd	cluster1	1	Enabled	Online	7.3.0.49	7.3.0.49
	Native		In Cluster	Data Node		
ftd	cluster1	2	Enabled	Online	7.3.0.49	7.3.0.49
	Native		In Cluster	Control Node		
ftd	cluster1	3	Disabled	Not Available		7.3.0.49
	Native		Not Applicable	None		

**ステップ 9** クラスタに別のシャーシを追加するには、この手順を繰り返しますが、固有の **chassis-id**、固有の管理 IP アドレス、および正しい **site-id** を設定する必要があります。そうでない場合は両方のシャーシで同じ設定を使用します。

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

**ステップ 10** 管理 IP アドレスを使用して、FMC 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、FMC 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。

FMC がデータユニットを自動的に検出します。

## ネイティブクラスタの例

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

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
  enter cluster-bootstrap
    set chassis-id 1
    set key cluster_key
    set mode spanned-etherchannel
    set service-type ftd-cluster
    exit
  enter mgmt-bootstrap ftd
    enter bootstrap-key FIREPOWER_MANAGER_IP
      set value 10.0.0.100
      exit
    enter bootstrap-key FIREWALL_MODE
      set value transparent
      exit
    enter bootstrap-key-secret REGISTRATION_KEY
```

```
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
      enter ipv4 1 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.31 mask 255.255.255.0
        exit
      enter ipv4 2 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.32 mask 255.255.255.0
        exit
      enter ipv4 3 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.33 mask 255.255.255.0
        exit
      exit
    exit
  scope app ftd 6.0.0.837
    accept-license-agreement
    set-default
    exit
  commit-buffer
```

シャーシ 2 :

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
      exit
      create member-port Ethernet1/2
      exit
    exit
  enter port-channel 2
    set port-type data
    enable
    create member-port Ethernet1/3
    exit
    create member-port Ethernet1/4
    exit
  exit
  enter port-channel 3
    set port-type firepower-eventing
    enable
    create member-port Ethernet1/5
    exit
    create member-port Ethernet1/6
    exit
```

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

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
    enter ipv4 1 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.31 mask 255.255.255.0
      exit
    enter ipv4 2 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.32 mask 255.255.255.0
      exit
    enter ipv4 3 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.33 mask 255.255.255.0
      exit
  exit
```

```
exit
scope app ftd 6.0.0.837
  set-default
  accept-license-agreement
  exit
commit-buffer
```

### マルチインスタンス クラスタリングの例

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
      exit
      create member-port Ethernet1/2
      exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
      exit
      create member-port Ethernet1/4
      exit
      exit
    enter interface Ethernet1/8
      set port-type mgmt
      enable
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
      exit
      enter subinterface 100
        set vlan 100
        set port-type cluster
      exit
    exit
  exit
commit-buffer

scope ssa
  scope slot 1
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
  scope slot 2
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
  enter app-instance ftd FTD1
    set deploy-type container
    set resource-profile-name medium
    set startup-version 6.6.0
```

```
    exit
  exit
  enter logical-device FTD1 ftd "1,2,3" clustered
  enter cluster-bootstrap
    set chassis-id 1
    set key cluster_key
    set mode spanned-etherchannel
    set service-type ftd-cluster
  exit
  enter mgmt-bootstrap ftd
  enter bootstrap-key FIREPOWER_MANAGER_IP
    set value 10.0.0.100
  exit
  enter bootstrap-key FIREWALL_MODE
    set value transparent
  exit
  enter bootstrap-key-secret REGISTRATION_KEY
    set value
      Value: alladinsane
  exit
  enter bootstrap-key-secret PASSWORD
    set value
      Value: widthofacircle
  exit
  enter bootstrap-key FQDN
    set value ftd.cisco.com
  exit
  enter bootstrap-key DNS_SERVERS
    set value 192.168.1.1
  exit
  enter bootstrap-key SEARCH_DOMAINS
    set value search.com
  exit
  enter ipv4 1 firepower
    set gateway 10.0.0.1
    set ip 10.0.0.31 mask 255.255.255.0
  exit
  enter ipv4 2 firepower
    set gateway 10.0.0.1
    set ip 10.0.0.32 mask 255.255.255.0
  exit
  enter ipv4 3 firepower
    set gateway 10.0.0.1
    set ip 10.0.0.33 mask 255.255.255.0
  exit
  enter bootstrap-key PERMIT_EXPERT_MODE
    set value yes
  exit
  exit
  scope app ftd 6.6.0
  accept-license-agreement
  exit
  commit-buffer
```

シャーシ 2 :

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



```
        create member-port Ethernet1/1
        exit
        create member-port Ethernet1/2
        exit
        exit
    enter port-channel 2
        set port-type data
        enable
        create member-port Ethernet1/3
        exit
        create member-port Ethernet1/4
        exit
        exit
    enter interface Ethernet1/8
        set port-type mgmt
        enable
        exit
    enter port-channel 48
        set port-type cluster
        enable
        enter member-port Ethernet2/3
            exit
            enter subinterface 100
                set vlan 100
                set port-type cluster
            exit
        exit
    exit
commit-buffer

scope ssa
    scope slot 1
        enter app-instance ftd FTD1
            set deploy-type container
            set resource-profile-name medium
            set startup-version 6.6.0
        exit
    exit
    scope slot 2
        enter app-instance ftd FTD1
            set deploy-type container
            set resource-profile-name medium
            set startup-version 6.6.0
        exit
    exit
    enter app-instance ftd FTD1
        set deploy-type container
        set resource-profile-name medium
        set startup-version 6.6.0
    exit
    exit
    enter logical-device FTD1 ftd "1,2,3" clustered
        enter cluster-bootstrap
            set chassis-id 2
            set key cluster_key
            set mode spanned-etherchannel
            set service-type ftd-cluster
        exit
        enter mgmt-bootstrap ftd
            enter bootstrap-key FIREPOWER_MANAGER_IP
                set value 10.0.0.100
            exit
            enter bootstrap-key FIREWALL_MODE
                set value transparent
```

```

exit
enter bootstrap-key-secret REGISTRATION_KEY
set value
Value: alladinsane
exit
enter bootstrap-key-secret PASSWORD
set value
Value: widthofacircle
exit
enter bootstrap-key FQDN
set value ftd.cisco.com
exit
enter bootstrap-key DNS_SERVERS
set value 192.168.1.1
exit
enter bootstrap-key SEARCH_DOMAINS
set value search.com
exit
enter ipv4 1 firepower
set gateway 10.0.0.1
set ip 10.0.0.31 mask 255.255.255.0
exit
enter ipv4 2 firepower
set gateway 10.0.0.1
set ip 10.0.0.32 mask 255.255.255.0
exit
enter ipv4 3 firepower
set gateway 10.0.0.1
set ip 10.0.0.33 mask 255.255.255.0
exit
enter bootstrap-key PERMIT_EXPERT_MODE
set value yes
exit
exit
scope app ftd 6.6.0
accept-license-agreement
exit
commit-buffer

```

## クラスタノードの追加

既存のクラスタ内の Firepower 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、FMC 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、FMC 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、FMC 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

別のシャーシをクラスタに追加するには、[FTD クラスタの作成 \(73 ページ\)](#) の手順を繰り返します (次の設定を固有のものとして設定する必要のある場合を除きます。そうでない場合には、両方のシャーシに同じ設定を使用します)。

- シャーシ ID (Chassis ID)
- 管理 IP アドレス

また、スタートアップバージョンをクラスタノードで現在実行中のバージョンに設定してください。

## Radware DefensePro の設定

Cisco Firepower 4100/9300 シャーシは、単一ブレードで複数のサービス (ファイアウォール、サードパーティの DDoS アプリケーションなど) をサポートできます。これらのアプリケーションとサービスは、リンクされて、サービス チェーンを形成します。

## Radware DefensePro について

現在サポートされているサービス チェーン コンフィギュレーションでは、サードパーティ製の Radware DefensePro 仮想プラットフォームを ASA ファイアウォールの手前、または Firepower Threat Defense の手前で実行するようにインストールできます。Radware DefensePro は、Firepower 4100/9300 シャーシに分散型サービス妨害 (DDoS) の検出と緩和機能を提供する KVM ベースの仮想プラットフォームです。Firepower 4100/9300 シャーシでサービスチェーンが有効になると、ネットワークからのトラフィックは主要な ASA または Firepower Threat Defense ファイアウォールに到達する前に DefensePro 仮想プラットフォームを通過する必要があります。



- (注)
- Radware DefensePro 仮想プラットフォームは、*Radware vDP* (仮想 DefensePro)、またはシンプルに *vDP* と呼ばれることがあります。
  - Radware DefensePro 仮想プラットフォームは、リンク デコレータと呼ばれることもあります。

## Radware DefensePro の前提条件

Radware DefensePro を Firepower 4100/9300 シャーシに導入する前に、**etc/UTC** タイムゾーンで NTP サーバを使用するように Firepower 4100/9300 シャーシを構成する必要があります。Firepower 4100/9300 シャーシの日付と時刻の設定の詳細については、[日時の設定](#)を参照してください。

## サービス チェーンのガイドライン

### モデル

- ASA : Radware DefensePro (vDP) プラットフォームは、次のモデルの ASA でサポートされています。
  - Firepower 9300
  - Firepower 4110
  - Firepower 4115
  - Firepower 4120
  - Firepower 4125
  - Firepower 4140
  - Firepower 4145
  - Firepower 4150
- FTD : Radware DefensePro プラットフォームは、次のモデルの Firepower Threat Defense でサポートされています。
  - Firepower 9300
  - Firepower 4110 : 論理デバイスと同時にデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。
  - Firepower 4112
  - Firepower 4115
  - Firepower 4120 : 論理デバイスと同時にデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。
  - Firepower 4125
  - Firepower 4140
  - Firepower 4145
  - Firepower 4150

### その他のガイドライン

- サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro (vDP) アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。

## スタンドアロンの論理デバイスでの Radware DefensePro の設定

スタンドアロン ASA または Firepower Threat Defense 論理デバイスの前にある単一のサービス チェーンに Radware DefensePro をインストールするには、次の手順に従います。

### 始める前に

- vDP イメージを Cisco.com からダウンロードして ([Cisco.com からのイメージのダウンロード](#)を参照)、そのイメージを Firepower 4100/9300 シャーシにダウンロードします ([Firepower 4100/9300 シャーシへの論理デバイスのソフトウェアイメージのダウンロード](#)を参照)。
- Radware DefensePro アプリケーションは、シャーシ内クラスタのスタンドアロン構成で導入できます。シャーシ内クラスタリングについては、[シャーシ内クラスタの Radware DefensePro の設定 \(100 ページ\)](#) を参照してください。

### 手順

- 
- ステップ 1** vDP で別の管理インターフェイスを使用する場合は、[物理インターフェイスの設定](#)に従ってインターフェイスを有効にし、そのタイプが `mgmt` になるように設定してください。あるいは、アプリケーション管理インターフェイスを共有できます。
- ステップ 2** スタンドアロン設定で ASA または Firepower Threat Defense 論理デバイスを作成します ([スタンドアロン ASA の追加 \(27 ページ\)](#) または [FMC のスタンドアロン FTD の追加 \(33 ページ\)](#) を参照)。Firepower 4110 または 4120 セキュリティアプライアンスにイメージをインストールする場合は、設定をコミットする前に、vDP を Firepower Threat Defense イメージとともにインストールする必要があることに注意してください。
- ステップ 3** セキュリティ サービス モードを開始します。
- ```
Firepower# scope ssa
```
- ステップ 4** Radware vDP インスタンスを作成します。
- ```
Firepower /ssa # scope slot slot_id
Firepower /ssa/slot # create app-instance vdp logical_device_identifier
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
```
- ステップ 5** 設定をコミットします。
- ```
commit-buffer
```

**ステップ 6** セキュリティ モジュールの vDP の設置とプロビジョニングを確認します。

Firepower /ssa # **show app-instance**

例 :

```
Firepower /ssa # show app-instance
App Name      Slot ID      Admin State  Oper State      Running Version  Startup Version  Cluster
State        Cluster Role
-----
ftd           1            Enabled      Online          6.2.1.62         6.2.1.62         Not
Applicable   None
vdp           1            Disabled     Installing      8.10.01.16-5     Not
Applicable   None
```

**ステップ 7** (オプション) サポートされている利用可能なリソース プロファイルを表示するには :

Firepower /ssa/app # **show resource-profile system**

例 :

```
Firepower /ssa # show resource-profile system
Profile Name      App Name      App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
-----
DEFAULT-4110-RESOURCE
      vdp           8.13.01.09-2 No          FPR4K-SM-12
      4            16384 Yes          System
DEFAULT-RESOURCE  vdp           8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      6            24576 Yes          System
VDP-10-CORES     vdp           8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      10           40960 No          System
VDP-2-CORES     vdp           8.13.01.09-2 No          all
      2            8192 No          System
VDP-4-CORES     vdp           8.13.01.09-2 No          all
      4            16384 No          System
VDP-8-CORES     vdp           8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      8            32768 No          System
```

**ステップ 8** (オプション) 前の手順の使用可能なプロファイルの1つを使用して、リソースプロファイルを設定します。

a) 範囲をスロット 1 にします :

Firepower /ssa\*# **scope slot 1**

b) DefensePro アプリケーション インスタンスを入力します。

Firepower /ssa/slot\* # **enter app-instance vdp**

c) リソース プロファイルを設定します。

Firepower /ssa/slot/app-instance\* # **set resource-profile-name resource\_profile\_name**

d) 設定をコミットします。

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

**ステップ 9** vDP アプリケーションがインストールされたら、論理デバイスにアクセスします。

```
Firepower /ssa # scope logical-device device_name
```

**ステップ 10** vDP に管理インターフェイスを割り当てます。論理デバイスのものと同じ物理インターフェイスを使用することも、別のインターフェイスを使用することもできます。

```
Firepower /ssa/logical-device # enter external-port-link name interface_id vdp
```

```
Firepower /ssa/logical-device/external-port-link* # exit
```

**ステップ 11** vDP の外部管理インターフェイス設定を設定します。

a) ブートストラップ オブジェクトを作成します。

```
Firepower /ssa/logical-device* # create mgmt-bootstrap vdp
```

b) 管理 IP アドレスを設定します。

```
Firepower /ssa/logical-device/mgmt-bootstrap* #create ipv4 slot_id default
```

c) ゲートウェイ アドレスを設定します。

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #set gateway gateway_address
```

d) IP アドレスとマスクを設定します。

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #set ip ip_address mask network_mask
```

e) 管理 IP 設定スコープを終了します。

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #exit
```

f) 管理ブートストラップ設定スコープを終了します。

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

**ステップ 12** ASA または Firepower Threat Defense フローの前に vDP を配置するデータインターフェイスを編集します。

```
Firepower /ssa/logical-device* # scope external-port-link name
```

**show external-port-link** コマンドを入力して、インターフェイス名を表示します。

**ステップ 13** 論理デバイスに vDP を追加します。

```
Firepower /ssa/logical-device/external-port-link* # set decorator vdp
```

vDP を使用するインターフェイスごとに手順を繰り返します。

(注) 更新された vDP インターフェイスを ASA で表示するには、vDP インターフェイスを追加または削除した後に ASA をリロードする必要があります。

**ステップ 14** 設定をコミットします。

```
commit-buffer
```

**ステップ 15** サードパーティのアプリケーションがインターフェイスに設定されていることを確認します。

```
Firepower /ssa/logical-device/external-port-link* # show detail
```

例 :

```
Firepower /ssa/logical-device/external-port-link # show detail

External-Port Link:
  Name: Ethernet11_ftd
  Port or Port Channel Name: Ethernet1/1
  App Name: ftd
  Description:
  Link Decorator: vdp
```

### 次のタスク

DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、[cisco.com](http://cisco.com) に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

## シャーシ内クラスタの Radware DefensePro の設定



(注) サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。

### 始める前に

- vDP イメージを [Cisco.com](http://Cisco.com) からダウンロードして ([Cisco.com からのイメージのダウンロード](#)を参照)、そのイメージを Firepower 4100/9300 シャーシにダウンロードします ([Firepower 4100/9300 シャーシへの論理デバイスのソフトウェア イメージのダウンロード](#)を参照)。

### 手順

- ステップ 1** vDP で別の管理インターフェイスを使用する場合は、[物理インターフェイスの設定](#)に従ってインターフェイスを有効にし、そのタイプが `mgmt` になるように設定してください。あるいは、アプリケーション管理インターフェイスを共有できます。
- ステップ 2** ASA シャーシ内クラスタ ([ASA クラスタの作成 \(63 ページ\)](#) を参照)、または Firepower Threat Defense シャーシ内クラスタ ([FTD クラスタの作成 \(73 ページ\)](#) を参照) を設定します。
- ステップ 3** 外部 (クライアント側) ポートを Radware DefensePro でデコレートします。  

```
enter external-port-link name interface_name { asa | ftd }
```

 セット `decorator vdp`



セット **description** ""

**exit**

**ステップ 4** 論理デバイスの外部管理ポートを割り当てます。

**enter external-port-link** { *mgmt\_asa* / *mgmt\_ftd* } *interface\_id* { *asa* / *ftd* }

セット **decorator** ""

セット **description** ""

**exit**

**ステップ 5** DefensePro の外部管理ポートを割り当てます。

**enter external-port-link** *mgmt\_vdp* *interface\_name* { *asa* / *ftd* }

セット **decorator** ""

セット **description** ""

**ステップ 6** (オプション) サポートされている利用可能なリソース プロファイルを表示するには :

**show resource-profile system**

例 :

```
Firepower /ssa # show resource-profile system
Profile Name      App Name  App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
-----
DEFAULT-4110-RESOURCE
      4          vdp          8.13.01.09-2 No          FPR4K-SM-12
      16384 Yes          System
DEFAULT-RESOURCE  vdp          8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      6          24576 Yes          System
VDP-10-CORES      vdp          8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      10         40960 No          System
VDP-2-CORES       vdp          8.13.01.09-2 No          all
      2          8192 No          System
VDP-4-CORES       vdp          8.13.01.09-2 No          all
      4          16384 No          System
VDP-8-CORES       vdp          8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      8          32768 No          System
```

**ステップ 7** (オプション) 前の手順の使用可能なプロファイルの1つを使用して、リソースプロファイルを設定します。

(注) この変更をコミットすると、FXOS シャーンが再起動します。

a) 範囲をスロット 1 にします :

Firepower /ssa\*# **scope slot 1**

- b) DefensePro アプリケーション インスタンスを入力します。

```
Firepower /ssa/slot* # enter app-instance vdp
```

- c) リソース プロファイルを設定します。

```
Firepower /ssa/slot/app-instance* # set resource-profile-name resource_profile_name
```

- d) 設定をコミットします。

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

- ステップ 8** クラスタ ポート チャンネルを設定します。

```
enter external-port-link port-channel48 Port-channel48 { asa | ftd }
```

```
セット decorator ""
```

```
セット description ""
```

```
exit
```

- ステップ 9** DefensePro の 3 つのすべてのインスタンスの管理ブートストラップを設定します。

```
enter mgmt-bootstrap vdp
```

```
enter ipv4 slot_id default
```

```
set gateway gateway_address
```

```
set ip ip_address mask network_mask
```

```
exit
```

例 :

```
enter mgmt-bootstrap vdp
  enter ipv4 1 default
    set gateway 172.16.0.1
    set ip 172.16.4.219 mask 255.255.0.0
  exit
```

```
enter ipv4 2 default
  set gateway 172.16.0.1
  set ip 172.16.4.220 mask 255.255.0.0
exit
```

```
enter ipv4 3 default
  set gateway 172.16.0.1
  set ip 172.16.4.221 mask 255.255.0.0
exit
```

- ステップ 10** 管理ブートストラップ設定範囲を終了します。

```
exit
```

- ステップ 11** 制御ブレードで DefensePro アプリケーションインスタンスを入力します。

```
connect module slot console
```

```
connect vdp
```

ステップ 12 制御ブレードで、管理 IP を設定します。

**device clustering management-channel ip**

ステップ 13 前のステップで確認した IP を使用して、制御 IP を設定します。

**device clustering master set management-channel ip**

ステップ 14 クラスタを有効化します。

**device clustering state set enable**

ステップ 15 アプリケーション コンソールを終了して FXOS モジュール CLI に戻ります。

**Ctrl ]**

ステップ 16 ステップ 10、12、13、14 を繰り返してステップ 11 で確認した制御ブレードの IP アドレスを設定し、各ブレードアプリケーションインスタンスに対してクラスタを有効化します。

ステップ 17 設定をコミットします。

**commit-buffer**

(注) この手順を完了したら、DefensePro インスタンスがクラスタに設定されているかどうかを確認する必要があります。

ステップ 18 DefensePro アプリケーションのすべてがクラスタに参加していることを確認します。

**device cluster show**

ステップ 19 以下のいずれかの方法で、「primary」と「secondary」の DefensePro インスタンスがどれであるかを確認します。

a) DefensePro インスタンスの範囲を指定し、DefensePro のアプリケーション属性のみを表示します。

**scope ssa**

**scope slot slot\_number**

**scope app-instance vdp**

**show app-attri**

b) スロットの範囲を指定し、DefensePro インスタンスの詳細を表示します。このアプローチでは、スロット上の論理デバイスと vDP 両方のアプリケーションインスタンス情報が表示されます。

**scope ssa**

**scope slot\_number**

**show app-instance** 詳細を展開

---

DefensePro アプリケーションがオンラインでもクラスタ化されていない場合は、CLI に次のように表示されます。

```
App Attribute:
  App Attribute Key: cluster-role
  Value: unknown
```

この「unknown」値が表示された場合は、vDP クラスタを作成するために、DefensePro アプリケーションを入力して制御ブレードの IP アドレスを設定する必要があります。

DefensePro アプリケーションがオンラインでクラスタ化されている場合は、CLI に次のように表示されます。

```
App Attribute:
  App Attribute Key: cluster-role
  Value: primary/secondary
```

## 例

```
scope ssa
  enter logical-device ld asa "1,2,3" clustered
  enter cluster-bootstrap
  set chassis-id 1
  set ipv4 gateway 172.16.0.1
  set ipv4 pool 172.16.4.216 172.16.4.218
  set ipv6 gateway 2010::2
  set ipv6 pool 2010::21 2010::26
  set key secret
  set mode spanned-etherchannel
  set name cisco
  set virtual ipv4 172.16.4.222 mask 255.255.0.0
  set virtual ipv6 2010::134 prefix-length 64
  exit
  enter external-port-link Ethernet1-2 Ethernet1/2 asa
  set decorator vdp
  set description ""
  exit
  enter external-port-link Ethernet1-3_asa Ethernet1/3 asa
  set decorator ""
  set description ""
  exit
  enter external-port-link mgmt_asa Ethernet1/1 asa
  set decorator ""
  set description ""
  exit
  enter external-port-link mgmt_vdp Ethernet1/1 vdp
  set decorator ""
  set description ""
  exit
  enter external-port-link port-channel48 Port-channel48 asa
  set decorator ""
  set description ""
  exit
  enter mgmt-bootstrap vdp
  enter ipv4 1 default
  set gateway 172.16.0.1
  set ip 172.16.4.219 mask 255.255.0.0
  exit

  enter ipv4 2 default
  set gateway 172.16.0.1
  set ip 172.16.4.220 mask 255.255.0.0
  exit
```

```
        enter ipv4 3 default
            set gateway 172.16.0.1
            set ip 172.16.4.221 mask 255.255.0.0
        exit
    exit
commit-buffer
scope ssa
    scope slot 1
    scope app-instance vdp
    show app-attri
    App Attribute:
    App Attribute Key: cluster-role
    Value: unknown
```

### 次のタスク

DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、[cisco.com](http://cisco.com) に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

## UDP/TCP ポートのオープンと vDP Web サービスの有効化

Radware APSolute Vision Manager インターフェイスは、さまざまな UDP/TCP ポートを使用して Radware vDP のアプリケーションと通信します。vDP のアプリケーションが APSolute Vision Manager と通信するために、これらのポートがアクセス可能でありファイアウォールによってブロックされないことを確認します。オープンする特定のポートの詳細については、APSolute Vision ユーザ ガイドの次の表を参照してください。

- **Ports for APSolute Vision Server-WBM Communication and Operating System**
- **Communication Ports for APSolute Vision Server with Radware Devices**

Radware APSolute Vision で FXOS シャーシ内に配置される Virtual DefensePro アプリケーションを管理するために、FXOS CLI を使用して vDP Web サービスを有効にする必要があります。

### 手順

---

**ステップ 1** FXOS CLI から、vDP のアプリケーション インスタンスに接続します。

```
connect module slot console
```

```
connect vdp
```

**ステップ 2** vDP Web サービスを有効化します。

```
manage secure-web status set enable
```

**ステップ 3** vDP アプリケーションのコンソールを終了して FXOS モジュール CLI に戻ります。

```
Ctrl ]
```

---

## TLS 暗号化アクセラレーションの設定

次のトピックでは TLS 暗号化アクセラレーション を紹介します。また、FMC を使用して、この機能を有効にする方法やステータスを表示する方法について説明します。

次の表は、Firepower Threat Defense および FXOS バージョンと必要な TLS 暗号のマッピングです。



(注) FXOS 2.6.1 を FXOS 2.7.x 以降にアップグレードした場合、FTD 6.4 は TLS 暗号化と互換性がないため、FTD 6.4 では暗号化が自動的に有効になりません。

| FTD    | FXOS   | Crypto                          |
|--------|--------|---------------------------------|
| 6.4    | 2.6    | 1つのコンテナインスタンスのみのサポート (フェーズ 1)   |
| 6.4    | 2.7 以降 | NA                              |
| 6.5 以降 | 2.7 以降 | 最大 16 のコンテナインスタンスのサポート (フェーズ 2) |

### About TLS 暗号化アクセラレーション

Firepower 4100/9300 は Transport Layer Security 暗号化アクセラレーションをサポートしています。これは、Transport Layer Security/Secure Sockets Layer (TLS/SSL) の暗号化と復号化をハードウェアで実行するもので、これにより次の高速化を実現します。

- TLS/SSL 暗号化および復号化
- VPN (TLS/SSL および IPsec を含む)

TLS 暗号化アクセラレーションはネイティブインスタンスで自動的に有効になり、無効にすることはできません。TLS 暗号化アクセラレーションはセキュリティエンジン/モジュールごとに最大 16 FTD コンテナインスタンスで有効にすることもできます。

### TLS 暗号化アクセラレーションに関するガイドラインと制限事項

Firepower Threat Defense で TLS 暗号化アクセラレーション が有効になっている場合は、次の点に留意してください。

#### エンジン障害インスペクション

インスペクションエンジンが接続を維持するように設定されていて、インスペクションエンジンが予期せず失敗した場合は、エンジンが再起動されるまで TLS/SSL トラフィックはドロップされます。

この動作は Firepower Threat Defense コマンド `configure snort preserve-connection {enable | disable}` によって制御されます。

### HTTP のみのパフォーマンス

トラフィックを復号しない FTD コンテナインスタンスで TLS 暗号化アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。TLS/SSL トラフィックを復号する FTD コンテナインスタンスで TLS 暗号化アクセラレーションのみ有効にすることをお勧めします。

### Federal Information Processing Standards (FIPS)

TLS 暗号化アクセラレーションと連邦情報処理標準 (FIPS) が両方とも有効になっている場合は、次のオプションの接続が失敗します。

- サイズが 2048 バイト未満の RSA キー
- Rivest 暗号 4 (RC4)
- 単一データ暗号化標準規格 (単一 DES)
- Merkle-Damgard 5 (MD5)
- SSL v3

セキュリティ認定準拠モードで動作するように FMC と Firepower Threat Defense を設定すると、FIPS が有効になります。このモードで動作しているときに接続を許可するには、FTD コンテナインスタンスで TLS 暗号化アクセラレーションを無効にするか、よりセキュアなオプションを採用するように Web ブラウザを設定します。

詳細については、次を参照してください。

- [コモンクライテリア](#)。

### 高可用性 (HA) とクラスタリング

高可用性 (HA) またはクラスタ化された Firepower Threat Defense がある場合は、Firepower Threat Defense ごとに TLS 暗号化アクセラレーションを有効にする必要があります。1 つのデバイスの TLS 暗号化アクセラレーション構成は、HA ペアまたはクラスタの他のデバイスとは共有されません。

### TLS ハートビート

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security (TLS) および Datagram Transport Layer Security (DTLS) プロトコルに対して、TLS ハートビートエクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている FMC によって管理されている Firepower Threat Defense が、TLS ハートビートエクステンションを使用するパケットを検出した場合、

Firepower Threat Defense は SSL ポリシーの [復号不可のアクション (Undecryptable Actions)] で [復号化エラー (Decryption Errors)] の FMC 設定で指定されたアクションを実行します。

- ブロック (Block)
- リセットしてブロック (Block with reset)

アプリケーションが TLS ハートビートを使用しているかどうかを確認するには、『*Firepower Management Center 構成ガイド*』の TLS/SSL トラブルシューティングルールの章を参照してください。

TLS 暗号化アクセラレーションが FTD コンテナインスタンスで無効になっている場合は、FMC のネットワーク分析ポリシー (NAP) の [最大ハートビート長 (Max Heartbeat Length)] を設定すると、TLS ハートビートの処理方法を決定できます。

TLS ハートビートの詳細については、『*Firepower Management Center 構成ガイド*』の TLS/SSL トラブルシューティングルールの章を参照してください。

### TLS/SSL オーバーサブスクリプション

TLS/SSL オーバーサブスクリプションとは、Firepower Threat Defense が TLS/SSL トラフィックにより過負荷になっている状態です。Firepower Threat Defense で TLS/SSL オーバーサブスクリプションが発生する可能性があります。TLS 暗号化アクセラレーションをサポートする Firepower Threat Defense でのみ処理方法を設定できます。

TLS 暗号化アクセラレーションが有効になっている FMC によって管理される Firepower Threat Defense がオーバーサブスクライブされた場合、Firepower Threat Defense によって受信されるパケットの扱いは、SSL ポリシーの [復号不可のアクション (Undecryptable Actions)] にある [ハンドシェイクエラー (Handshake Errors)] の設定に従います。

- デフォルトアクションを継承する (Inherit default action)
- Do not decrypt
- ブロック (Block)
- リセットしてブロック (Block with reset)

SSL ポリシーの [復号化不可のアクション (Undecryptable Actions)] の [ハンドシェイクエラー (Handshake Errors)] の設定が [復号しない (Do Not decrypt)] で、関連付けられたアクセスコントロールポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

大量のオーバーサブスクリプションが発生している場合は、次のオプションがあります。

- TLS/SSL の処理能力が高い Firepower Threat Defense にアップグレードします。
- SSL ポリシーを変更して、復号の優先順位が高くないトラフィック用に [Do Not Decrypt] ルールを追加します。

TLS オーバーサブスクリプションの詳細については、『*Firepower Management Center 構成ガイド*』の TLS/SSL トラブルシューティングルールの章を参照してください。



パッシブおよびインラインタップの設定はサポートされていません。

TLS 暗号化アクセラレーションが有効になっている場合、TLS/SSL トラフィックはパッシブまたはインラインタップ設定のインターフェイスでは復号できません。

## コンテナインスタンスの TLS 暗号化アクセラレーションの有効化

FMC のスタンドアロン FTD の追加 (33 ページ) で説明されているように、論理インスタンスを展開すると、TLS 暗号化アクセラレーションが自動的に有効になります。

TLS 暗号化アクセラレーションすべてのネイティブインスタンスで有効になり、無効にすることはできません。

## TLS 暗号化アクセラレーションのステータスの表示

このトピックでは、TLS 暗号化アクセラレーションが有効になっているかどうかを確認する方法について説明します。

FMC で次の作業を実行します。

### 手順

**ステップ 1** FMC にログインします。

**ステップ 2** [デバイス (Devices)] > [デバイス管理 (Device Management)] をクリックします。

**ステップ 3** をクリックして、管理対象デバイスを編集します。

**ステップ 4** [デバイス (Device)] ページをクリックします。TLS 暗号化アクセラレーションステータスが [全般 (General)] セクションに表示されます。

## 論理デバイスの管理

論理デバイスを削除したり、ASA をトランスペアレントモードに変換したり、インターフェイスコンフィギュレーションを変更したり、その他のタスクを既存の論理デバイスで実行することができます。

## アプリケーションのコンソールへの接続

アプリケーションのコンソールに接続するには、次の手順を使用します。

### 手順

**ステップ 1** コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

**connect module slot\_number { console | telnet }**

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot\_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

**ステップ 2** アプリケーションのコンソールに接続します。デバイスの適切なコマンドを入力します。

**connect asa name**

**connect ftd name**

**connect vdp name**

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

**ステップ 3** アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA : **Ctrl-a, d** と入力します。
- FTD : 「**exit**」 と入力します。
- vDP : **Ctrl-], .** と入力

**ステップ 4** FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

**Telnet セッションを終了します。**

a) **Ctrl-],.** と入力

---

### 例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパーバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

## 論理デバイスの削除

### 手順

---

**ステップ 1** セキュリティ サービス モードを開始します。

```
Firepower# scope ssa
```

**ステップ 2** シャーシ上の論理デバイスの詳細を表示します。

```
Firepower /ssa # show logical-device
```

**ステップ 3** 削除する論理デバイスごとに、次のコマンドを入力します。

```
Firepower /ssa # delete logical-device device_name
```

**ステップ 4** 論理デバイスにインストールされているアプリケーションの詳細を表示します。

```
Firepower /ssa # show app-instance
```

**ステップ 5** 削除するアプリケーションごとに、次のコマンドを入力します。

- a) Firepower /ssa # **scope slot slot\_number**
- b) Firepower /ssa/slot # **delete app-instance application\_name**
- c) Firepower /ssa/slot # **exit**

**ステップ 6** 設定を確定します。

#### **commit-buffer**

トランザクションをシステム設定にコミットします。

#### 例

```
Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
-----
Name          Description Slot ID    Mode          Operational State      Template Name
-----
FTD           1,2,3      Clustered    Ok              ftd
Firepower /ssa # delete logical-device ftd
Firepower /ssa* # show app-instance
Application Name      Slot ID    Admin State    Operational State      Running Version
Startup Version Cluster Oper State
-----
ftd                   1 Disabled      Stopping            6.0.0.837
6.0.0.837             Not Applicable
ftd                   2 Disabled      Offline             6.0.0.837
6.0.0.837             Not Applicable
ftd                   3 Disabled      Not Available
6.0.0.837             Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

## 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、Firepower Chassis Manager [論理デバイス (Logical Devices) ] ページで、**show cluster info** コマンドを使用してアプリケーション内のクラスタステータスを確認します。

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

FMCを使用したFTDでは、FMC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、ASA で **cluster group name** を入力してから **enable** を入力します。クラスタリングを再度有効にするには、FTD 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：FXOS CLI で、次の例を参照してください。

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

再度有効にするには、次の手順を実行します。

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

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

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

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

電源を投入するには、次の手順を実行します。

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

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

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

### 完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

FMC を使用した FTD 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 FMC 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 : FXOS CLI で、次の例を参照してください。

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

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

## 論理デバイスに関連付けられていないアプリケーションインスタンスの削除

論理デバイスを削除すると、その論理デバイスのアプリケーション設定も削除するかどうか尋ねられます。アプリケーション設定を削除しない場合、そのアプリケーションインスタンスが削除されるまで、別のアプリケーションを使用して論理デバイスを作成することはできません。セキュリティモジュール/エンジンが論理デバイスとすでに関連付けられていない場合は、アプリケーションインスタンスを削除するために以下の手順を使用できます。

### 手順

---

**ステップ 1** セキュリティ サービス モードを開始します。

```
Firepower# scope ssa
```

**ステップ 2** インストール済みアプリケーションの詳細を表示します。

```
Firepower /ssa # show app-instance
```

**ステップ 3** 削除するアプリケーションごとに、次のコマンドを入力します。

- a) Firepower /ssa # **scope slot slot\_number**
- b) Firepower /ssa/slot # **delete app-instance application\_name**
- c) Firepower /ssa/slot # **exit**

**ステップ 4** 設定を確認します。

```
commit-buffer
```

トランザクションをシステム設定にコミットします。

### 例

```
Firepower# scope ssa
Firepower /ssa* # show app-instance
Application Name      Slot ID      Admin State      Operational State      Running Version
Startup Version Cluster Oper State
-----
ftd                    1 Disabled      Stopping          6.0.0.837
6.0.0.837             Not Applicable
ftd                    2 Disabled      Offline           6.0.0.837
6.0.0.837             Not Applicable
ftd                    3 Disabled      Not Available
6.0.0.837             Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

## FTD 論理デバイスのインターフェイスの変更

Firepower Threat Defense 論理デバイスでは、インターフェイスの割り当てや割り当て解除を行うことができます。その後、FMC または FDM でインターフェイス設定を同期できます。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、Firepower Threat Defense の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバなど、Firepower Threat Defense の設定における多くの場所で直接参照されている可能性があります。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与

えず、かつ FMC または FDM での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

FMC の場合：インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。

FDM の場合：古いインターフェイスを削除する前に、あるインターフェイスから別のインターフェイスに設定を移行できます。

### 始める前に

- **物理インターフェイスの設定**および**EtherChannel (ポート チャンネル) の追加**に従ってインターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには (たとえば、デフォルトですべてのインターフェイスがクラスタに割り当てられます)、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でデバイスに EtherChannel を割り当てることができます。
- クラスタリングやハイアベイラビリティのため、FMC または FDM で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にデータ/スタンバイユニットでインターフェイスを変更してから、制御/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼさないことに注意してください。

### 手順

**ステップ 1** セキュリティ サービス モードを開始します。

```
Firepower# scope ssa
```

**ステップ 2** 論理デバイスを編集します。

```
Firepower /ssa # scope logical-device device_name
```

**ステップ 3** 論理デバイスに新しいインターフェイスを割り当てます。

```
Firepower /ssa/logical-device* # create external-port-link name interface_id ftd
```

まだインターフェイスを削除しないでください。

**ステップ 4** 設定を確定します。

```
commit-buffer
```

トランザクションをシステム設定にコミットします。

**ステップ 5** FMC でインターフェイスを同期します。

a) FMC にログインします。



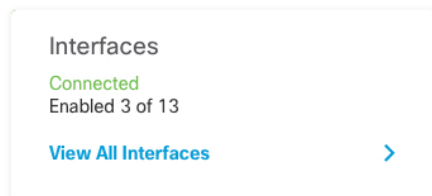
- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firepower Threat Defense デバイスをクリックします。[インターフェイス (Interfaces)] タブがデフォルトで選択されます。
- c) [インターフェイス (Interfaces)] タブの左上にある [デバイスの同期 (Sync Device)] ボタンをクリックします。
- d) 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス (Interfaces)] ページに表示されます。[クリックして詳細を表示 (Click to know more)] リンクをクリックしてインターフェイスの変更内容を表示します。
- e) インターフェイスを削除する場合は、古いインターフェイスから新しいインターフェイスにインターフェイス設定を手動で転送します。

インターフェイスはまだ削除していないため、既存の設定を参照できます。古いインターフェイスを削除して検証を再実行した後も、さらに設定を修正する機会があります。検証を実行すると、古いインターフェイスがまだ使用されているすべての場所が表示されます。

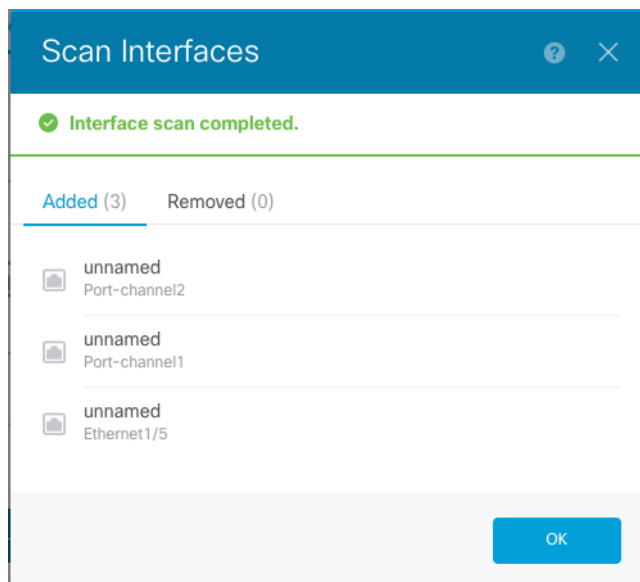
- f) [変更の検証 (Validate Changes)] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。  
エラーがある場合は、ポリシーを変更して検証に戻る必要があります。
- g) [Save (保存)] をクリックします。
- h) デバイスを選択して [展開 (Deploy)] をクリックし、割り当てられたデバイスにポリシーを展開します。変更はポリシーを導入するまで有効になりません。

#### ステップ 6 FDM でインターフェイスを同期して移行します。

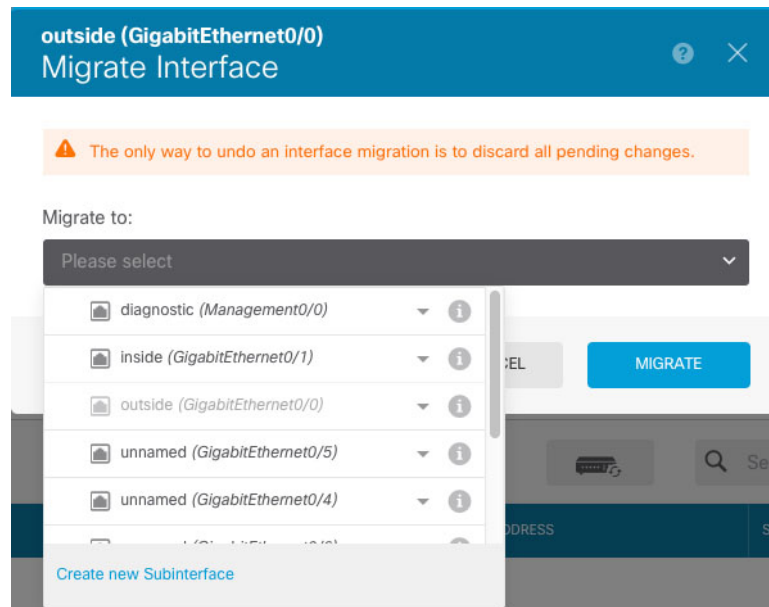
- a) FDM にログインします。
- b) [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにある [すべてのインターフェイスを表示 (View All Interfaces)] リンクをクリックします。



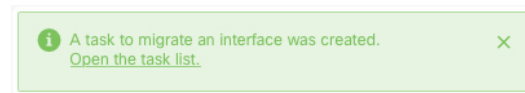
- c) [インターフェイス (Interfaces)] アイコンをクリックします。
- d) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



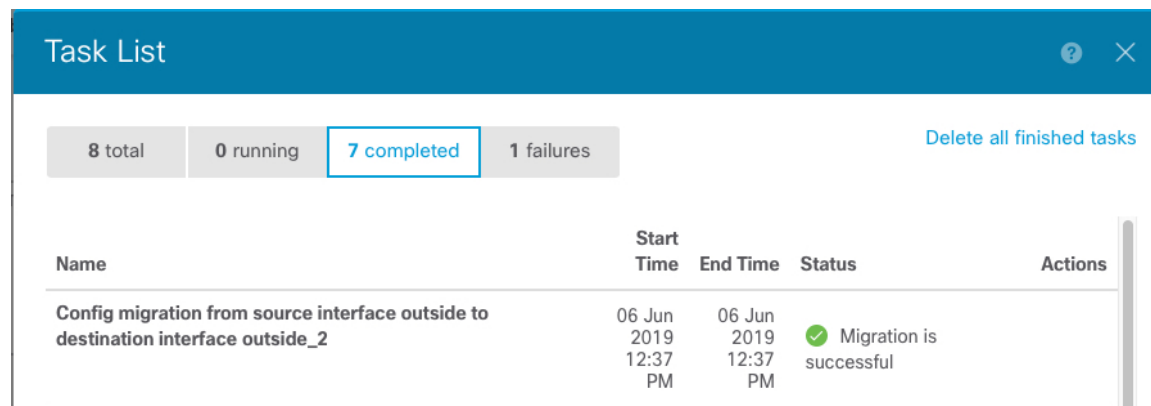
- e) 新しいインターフェイスに名前、IP アドレスなどを設定します。  
削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、古いインターフェイスをダミーの名前と IP アドレスで再設定する必要があります。
- f) 古いインターフェイスを新しいインターフェイスに置き換えるには、古いインターフェイスの [置換 (Replace) ] アイコンをクリックします。  
**[置換 (Replace) ] アイコン**  
このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに置き換えられます。
- g) [交換用インターフェイス (Replacement Interface) ] : ドロップダウン リストから新しいインターフェイスを選択します。



- h) [インターフェイス (Interfaces) ] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。



- i) [タスクリスト (Task List) ] を調べて、移行が成功したことを確認します。



**ステップ 7** FXOS で、論理デバイスからインターフェイスの割り当てを解除します。

Firepower /ssa/logical-device # **delete external-port-link name**

**show external-port-link** コマンドを入力して、インターフェイス名を表示します。

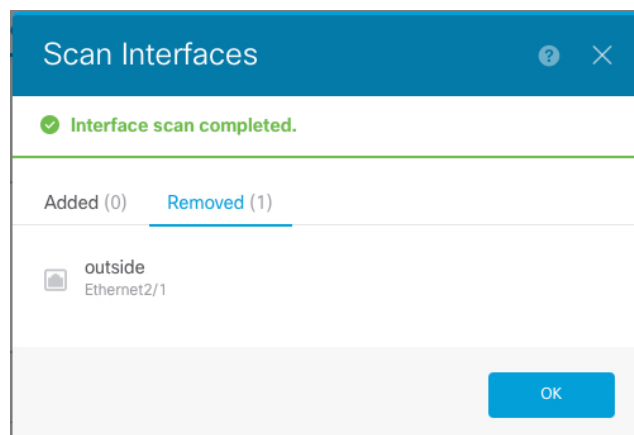
**ステップ 8** 設定を確定します。

**commit-buffer**

トランザクションをシステム設定にコミットします。

ステップ9 FMC または FDM でインターフェイスを再度同期します。

図 6: FDM によるインターフェイスのスキャン



## ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、ASA の設定に与える影響は最小限です。ただし、FXOS で割り当てられたインターフェイスを削除する場合（ネットワーク モジュールの削除、EtherChannel の削除、割り当てられたインターフェイスの EtherChannel への再割り当てなど）、そのインターフェイスがセキュリティポリシーで使用されると、削除は ASA の設定に影響を与えます。この場合、ASA 設定では元のコマンドが保持されるため、必要な調整を行うことができます。ASA OS の古いインターフェイス設定は手動で削除できます。



(注) 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。

### 始める前に

- [物理インターフェイスの設定](#)および[EtherChannel \(ポートチャネル\) の追加](#)に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトですべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でデバイスに EtherChannel を割り当てることができます。

- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にデータ/スタンバイユニットでインターフェイスを変更してから、制御/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

## 手順

**ステップ 1** セキュリティ サービス モードを開始します。

```
Firepower# scope ssa
```

**ステップ 2** 論理デバイスを編集します。

```
Firepower /ssa # scope logical-device device_name
```

**ステップ 3** 論理デバイスからインターフェイスの割り当てを解除します。

```
Firepower /ssa/logical-device # delete external-port-link name
```

**show external-port-link** コマンドを入力して、インターフェイス名を表示します。

管理インターフェイスの場合、新しい管理インターフェイスを追加する前に、現在のインターフェイスを削除し、**commit-buffer** コマンドを使用して変更をコミットします。

**ステップ 4** 論理デバイスに新しいインターフェイスを割り当てます。

```
Firepower /ssa/logical-device* # create external-port-link name interface_id asa
```

**ステップ 5** 設定を確定します。

```
commit-buffer
```

トランザクションをシステム設定にコミットします。

## 論理デバイスのモニタリング

### • show app

使用可能なイメージを表示します。

```
Firepower# scope ssa
Firepower /ssa # show app
```

| Name        | Version | Author | Supported        | Deploy | Types | CSP | Type        | Is  |
|-------------|---------|--------|------------------|--------|-------|-----|-------------|-----|
| Default App |         |        |                  |        |       |     |             |     |
| asa         | 9.10.1  | cisco  | Native           |        |       |     | Application | Yes |
| ftd         | 6.3.0   | cisco  | Native,Container |        |       |     | Application | Yes |
| ftd         | 6.2.3   | cisco  | Native           |        |       |     | Application | Yes |

```
vdp      8.13.01.09-2  radware  Vm      Application Yes
```

### • show app-instance

アプリケーション インスタンスのステータスと情報を表示します。

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name  Identifier Slot ID  Admin State Oper State  Running Version Startup
Version Deploy Type Profile Name Cluster State  Cluster Role
-----
ftd      LD1      1      Enabled  Online    6.4.0.10353
6.4.0.10353 Container Default-Small Not Applicable None
ftd      LD2      1      Enabled  Online    6.4.0.10353
6.4.0.10353 Container Default-Small Not Applicable None
ftd      LD3      1      Enabled  Online    6.4.0.10353
6.4.0.10353 Container Default-Small Not Applicable None
ftd      LD4      1      Enabled  Online    6.4.0.10353
6.4.0.1056 Container Default-Small Not Applicable None
```

### • show logical-device

論理デバイスの詳細を表示します。

```
Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
  Name      Description Slot ID  Mode      Oper State  Template
Name
-----
  asa1      1      Standalone Ok      asa
```

### • show resource-profile system

vDP のリソース プロファイルを表示します。

```
Firepower# scope ssa
Firepower /ssa # show resource-profile system
Profile Name  App Name  App Version  Is In Use  Security Model  CPU Logical
Core Count RAM Size (MB)  Default Profile Profile Type Description
-----
DEFAULT-4110-RESOURCE
  4      16384 Yes      System      FPR4K-SM-12
DEFAULT-RESOURCE
  6      24576 Yes      System      FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
VDP-10-CORES
  10     40960 No      System      FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
VDP-2-CORES
  2      8192 No      System      all
VDP-4-CORES
  2      8192 No      System      all
```

```

4          16384 No          System
VDP-8-CORES vdp          8.13.01.09-2 No          FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

```

```

8          32768 No          System

```

- **show resource-profile user-defined**

コンテナ インスタンスのリソース プロファイル割り当てを表示します。

```

Firepower# scope ssa
Firepower /ssa # show resource-profile user-defined
Profile Name          Is In Use  CPU Logical Core Count Description
-----
bronze                No        6          low end device
gold                  No        14         highest
silver                No        8          mid-level

```

- **show resource detail**

アプリケーション インスタンスのリソース割り当てを表示します。

```

Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
  Allocated Core NR: 10
  Allocated RAM (MB): 32413
  Allocated Data Disk (MB): 49152
  Allocated Binary Disk (MB): 3907
  Allocated Secondary Disk (MB): 0

```

## サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

### サイト固有のMACアドレスを使用したスパンドEtherChannelルーテッドモードの例

次の例では、各サイトのゲートウェイ ルータと内部ネットワーク間に配置された（イースト ウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタ メンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部両方のネットワークに対しスパンドEtherChannelを使用してローカルスイッチに接続します。各EtherChannelは、クラスタ内のすべてのシャーシにスパンされます。

データ VLAN は、オーバーレイ トランスポート 仮想化 (OTV)（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックがDCIを通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロック

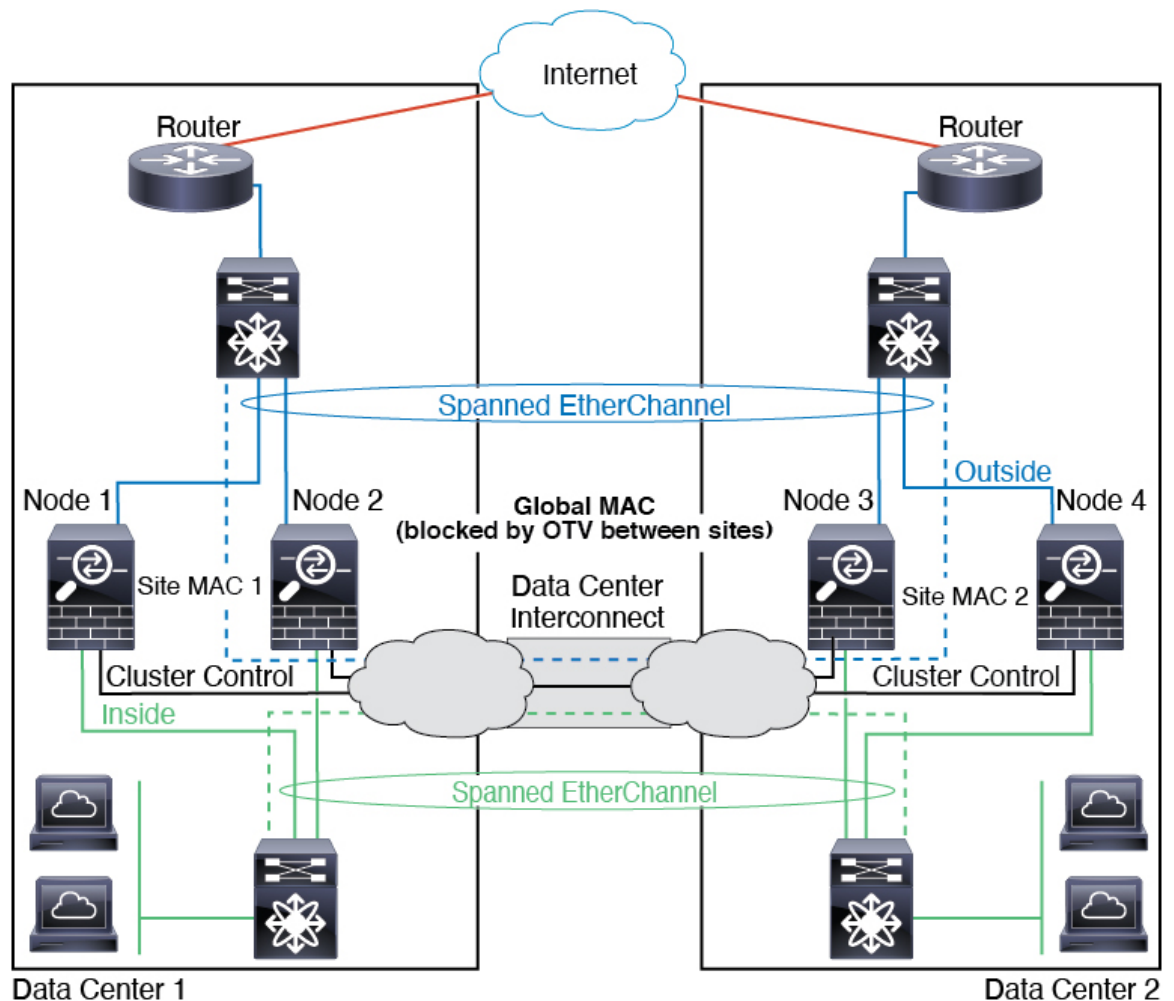
するフィルタを追加する必要があります。1つのサイトのクラスタノードが到達不能になった場合、トラフィックが他のサイトのクラスタノードに送信されるようにフィルタを削除する必要があります。Vaclを使用して、グローバルのMACアドレスのフィルタリングする必要があります。必ず ARP インスペクションを無効にしてください。

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

この場合のシナリオは次のとおりです。

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





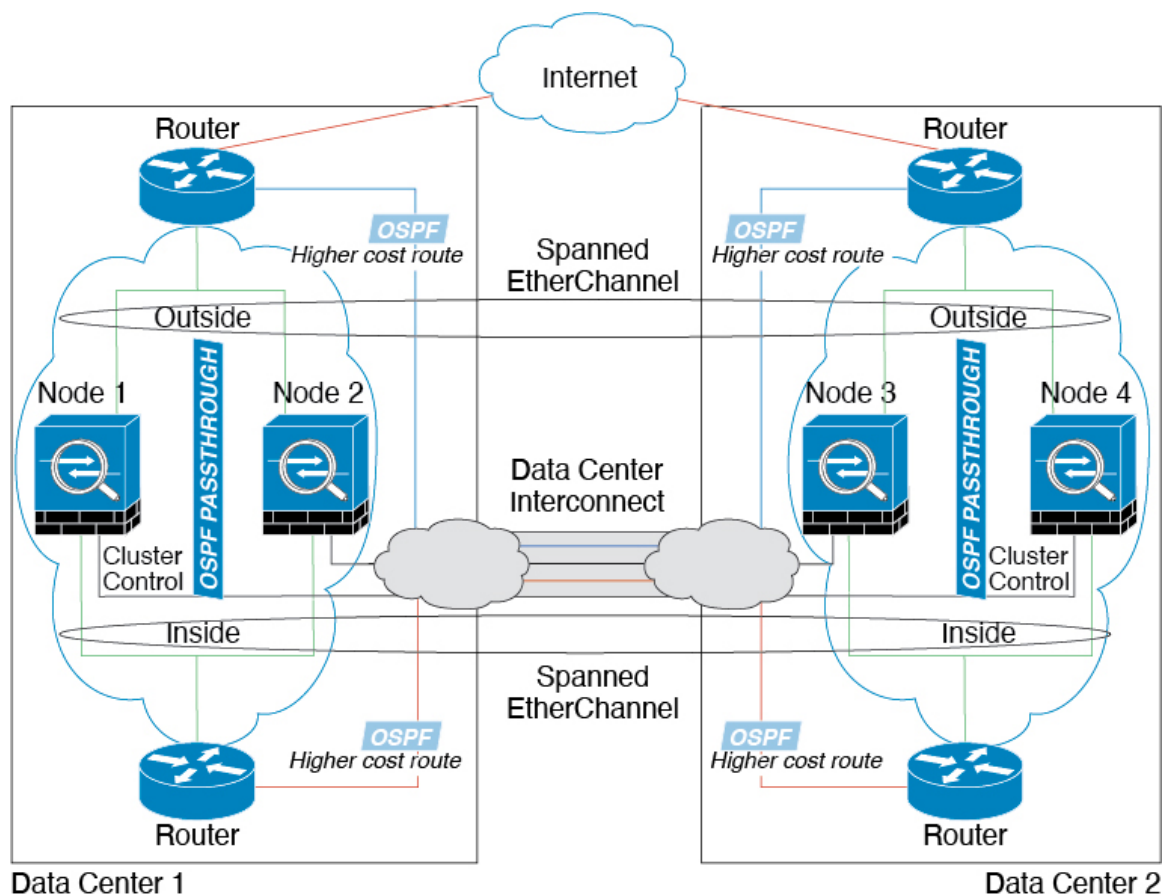
## スパンド EtherChannel トランスペアレントモード ノースサウス サイト間の例

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

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

各サイトのスイッチの実装には、次のものを含めることができます。

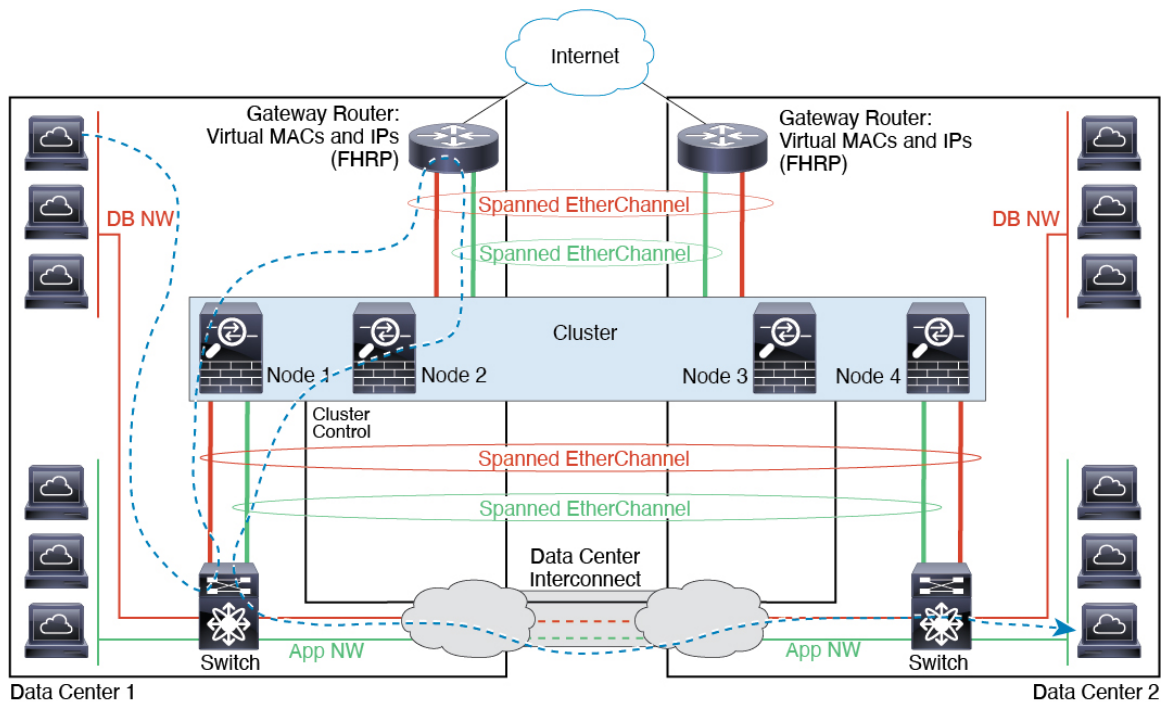
- サイト間 VSS、vPC、StackWise、StackWise Virtual：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、冗長スイッチトラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCI が余分なトラフィックを処理できる場合、必要に応じて、各ノードを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS、vPC、StackWise、StackWise Virtual：スイッチの冗長性を高めるには、各サイトに 2 つの異なる冗長スイッチペアをインストールできます。この場合、クラスタノードは、両方のローカルスイッチだけに接続されたデータセンター 1 のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター 2 のシャーシではスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル冗長スイッチは、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。



## スバンド EtherChannel トランスペアレントモード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスバンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャシーにスパンされます。

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



## 論理デバイスの履歴

| 機能名                                                       | プラットフォームリリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower Threat Defense 動作リンク状態と物理リンク状態の同期               | 2.9.1        | <p>シャーシでは、Firepower Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firepower Threat Defense アプリケーションインターフェイスの管理状態は考慮されません。Firepower Threat Defense からの同期がない場合は、たとえば、Firepower Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Firepower Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、Firepower Threat Defense が処理できるようになる前に外部ルータが Firepower Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。</p> <p>(注) この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する Firepower Threat Defense ではサポートされません。ASA ではサポートされていません。</p> <p>新規/変更された Firepower Chassis Manager 画面 : [Logical Devices] &gt; [Enable Link State]</p> <p>新規/変更された FXOS コマンド : <b>set link-state-sync enabled、show interface expand detail</b></p> |
| コンテナインスタンス向けのFMCを使用したFirepower Threat Defense設定のバックアップと復元 | 2.9.1        | <p>Firepower Threat Defense コンテナインスタンスで FMC バックアップ/復元ツールを使用できるようになりました。</p> <p>新規/変更された FMC 画面 : [システム (System)] &gt; [ツール (Tools)] &gt; [バックアップ/復元 (Backup/Restore)] &gt; [管理対象デバイスのバックアップ (Managed Device Backup)]</p> <p>新規/変更された Firepower Threat Defense CLI コマンド : <b>restore</b></p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p> <p>(注) Firepower 6.7 が必要です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| 機能名                                   | プラットフォームリリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| マルチインスタンスクラスタ                         | 2.8.1        | <p>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。</p> <p>新規/変更されたコマンド：<b>set port-type cluster</b></p> <p>(注) Firepower 6.6 以降が必要です。</p>                                                                                                                                                               |
| FDM での Firepower Threat Defense のサポート | 2.7.1        | <p>ネイティブ Firepower Threat Defense インスタンスを表示し、FDM 管理を指定できるようになりました。コンテナインスタンスはサポートされていません。</p> <p>新規/変更されたコマンド：<b>enter bootstrap-key MANAGEMENT_TYPE、set value LOCALLY_MANAGED</b></p> <p>(注) Firepower Threat Defense 6.5 以降が必要です。</p>                                                                                                                                                                                                                                                                                                                                                                                |
| 複数のコンテナインスタンスの TLS 暗号化アクセラレーション       | 2.7.1        | <p>Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス (最大 16 個) で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに 1 つのコンテナインスタンスに対してのみ TLS 暗号化アクセラレーションを有効にすることができました。</p> <p>新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、<b>enter hw-crypto</b> 次に <b>set admin-state enabled FXOS</b> コマンドを使用します。</p> <p>新しい FXOS CLI コマンド：<b>enter hw-crypto、set admin-state</b></p> <p>削除された FXOS CLI コマンド：<b>show hwCrypto、config hwCrypto</b></p> <p>削除された Firepower Threat Defense CLI コマンド：<b>show crypto accelerator status</b></p> <p>(注) Firepower Threat Defense 6.5 以降が必要です。</p> |
| Firepower 4115、4125、および 4145          | 2.6.1        | <p>Firepower 4115、4125、および 4145 が導入されました。</p> <p>(注) ASA 9.12(1) が必要です。Firepower 6.4.0 には FXOS 2.6.1.157 が必要です。</p> <p>変更されたコマンドはありません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| 機能名                                                                                               | プラットフォームリリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower 9300 SM-40、SM-48、および SM-56 のサポート                                                        | 2.6.1        | <p>3つのセキュリティ モジュール、SM-40、SM-48、および SM-56 が導入されました。</p> <p>(注) SM-40 および SM-48 には ASA 9.12(1) が必要です。SM-56 には、ASA 9.12(2) および FXOS 2.6.1.157 が必要です。</p> <p>すべてのモジュールには、Firepower Threat Defense 6.4 および FXOS 2.6.1.157 が必要です。</p> <p>変更されたコマンドはありません。</p>                                                                                                                                                                                                                                                                                     |
| ASA および Firepower Threat Defense を同じ Firepower 9300 の別のモジュールでサポート                                 | 2.6.1        | <p>ASA および Firepower Threat Defense 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。</p> <p>(注) ASA 9.12(1) が必要です。Firepower 6.4.0 には FXOS 2.6.1.157 が必要です。</p> <p>変更されたコマンドはありません。</p>                                                                                                                                                                                                                                                                                                                                                             |
| Firepower Threat Defense ブートストラップ設定については、Firepower Chassis Manager で FMC の NAT ID を設定できるようになりました。 | 2.6.1        | <p>Firepower Chassis Manager で FMC NAT ID を設定できるようになりました。以前は、FXOS CLI または Firepower Threat Defense CLI 内でのみ NAT ID を設定できました。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。FMC がデバイスの IP アドレスを指定し、デバイスが FMC 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 を指定する必要があります。FMC 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。</p> <p>新しい/変更された画面：</p> <p><b>[Logical Devices] &gt; [Add Device] &gt; [Settings] &gt; [Firepower Management Center NAT ID]</b> フィールド</p> |
| モジュール/セキュリティ エンジンのいずれかの Firepower Threat Defense コンテナインスタンスでの SSL ハードウェア アクセラレーションのサポート           | 2.6.1        | <p>これで、モジュール/セキュリティ エンジンのいずれかのコンテナ インスタンスに対して SSL ハードウェア アクセラレーションを有効にすることができるようになりました。他のコンテナ インスタンスに対して SSL ハードウェア アクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。詳細については、『FMC Configuration Guide』を参照してください。</p> <p>新規/変更されたコマンド：<b>config hwCrypto enable、show hwCrypto</b></p>                                                                                                                                                                                                                                                            |

| 機能名                                   | プラットフォームリリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower Threat Defense のマルチインスタンス機能 | 2.4.1        | <p>単一のセキュリティエンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナインスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーションインスタンスを展開するだけでした。ネイティブインスタンスも引き続きサポートされています。Firepower 9300 の場合、一部のモジュールでネイティブインスタンスを使用し、他のモジュールではコンテナインスタンスを使用することができます。</p> <p>柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。コンテナインスタンスを展開する場合、割り当てられた CPU コアの数を指定する必要があります。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。このリソース管理を使用すると、各インスタンスのパフォーマンス機能をカスタマイズできます。</p> <p>2 つの個別のシャーシでコンテナインスタンスを使用してハイアベイラビリティを使用することができます。たとえば、10 個のインスタンスを持つシャーシを 2 つ使用する場合は、10 個のハイアベイラビリティペアを作成できます。クラスタリングはサポートされません。</p> <p>(注) マルチインスタンス機能は、実装は異なりますが、ASA マルチコンテキストモードに似ています。マルチコンテキストモードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナインスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェアアップデート、および Firepower Threat Defense のフル機能のサポートが可能で、マルチコンテキストモードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。Firepower Threat Defense ではマルチコンテキストモードは使用できません。</p> <p>(注) Firepower Threat Defense バージョン 6.3 以降が必要です。</p> <p>新規/変更された FXOS コマンド : <b>connect Firepower Threat Defense name</b>、<b>connect module telnet</b>、<b>create bootstrap-key PERMIT_EXPERT_MODE</b>、<b>createresource-profile</b>、<b>create subinterface</b>、<b>scope auto-macpool</b>、<b>set cpu-core-count</b>、<b>set deploy-type</b>、<b>set port-type data-sharing</b>、<b>set prefix</b>、<b>set resource-profile-name</b>、<b>set vlan</b>、<b>scope app-instance Firepower Threat Defense name</b>、<b>show cgroups container</b>、<b>show interface</b>、<b>show mac-address</b>、<b>show subinterface</b>、<b>show tech-support module app-instance</b>、<b>show version</b></p> <p>新規/変更された FMC 画面 :</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [編集 (Edit)] アイコン &gt; [インターフェイス (Interfaces)] タブ</p> |

| 機能名                                                                              | プラットフォームリリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASA 論理デバイスのトランスペアレントモード展開のサポート                                                   | 2.4.1        | <p>ASAを展開するときに、トランスペアレントまたはルーテッドモードを指定できるようになりました。</p> <p>新規/変更されたコマンド：<b>enter bootstrap-key FIREWALL_MODE</b>、<b>set value routed</b>、<b>set value transparent</b></p>                                                                                                                                                                                                                                                              |
| クラスタ制御リンクのカスタマイズ可能な IP アドレス                                                      | 2.4.1        | <p>クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID (127.2.chassis_id.slot_id) に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック (127.0.0.0/8) およびマルチキャスト (224.0.0.0/4) アドレスを除き、FXOS にクラスタ制御リンクのカスタム/16 サブネットを作成できるようになりました。</p> <p>新規/変更されたコマンド：<b>set cluster-control-link network</b></p>                          |
| Firepower Threat Defense ブートストラップ設定については、FXOS CLI で FMC の NAT ID を設定できるようになりました。 | 2.4.1        | <p>FXOS CLI で FMC NAT ID を設定できるようになりました。以前は、Firepower Threat Defense CLI 内でのみ NAT ID を設定できました。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。FMC がデバイスの IP アドレスを指定し、デバイスが FMC 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。FMC 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。</p> <p>新規/変更されたコマンド：<b>enter bootstrap-key NAT_ID</b></p> |
| ASA のサイト間クラスタリングの改善                                                              | 2.1(1)       | <p>ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。</p> <p><b>set site-id</b> コマンドが変更されました</p>                                                                                                                        |
| Firepower 9300 上の 6 個の Firepower Threat Defense モジュールのシャーシ間クラスタリング               | 2.1.1        | <p>Firepower 9300 で Firepower Threat Defense のシャーシ間クラスタリングを有効化できます。最大 6 つのモジュールを搭載することができます。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て、最大 6 つのモジュールを組み合わせたことができます。</p>                                                                                                                                                                                                                                                   |



| 機能名                                                           | プラットフォームリリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower 4100 での Firepower Threat Defense クラスタリングのサポート       | 2.1.1        | Firepower Threat Defense クラスタで最大 6 個のシャーシをクラスタ化できます。                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ASA クラスタでの 16 個の Firepower 4100 シャーシのサポート                     | 2.0(1)       | ASA クラスタで最大 16 個のシャーシをクラスタ化できます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Firepower 4100 での ASA クラスタリングのサポート                            | 1.1.4        | ASA クラスタで最大 6 個のシャーシをクラスタ化できます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Firepower 9300 の Firepower Threat Defense でのシャーシ内クラスタリング サポート | 1.1.4        | Firepower 9300 が Firepower Threat Defense アプリケーションでシャーシ内クラスタリングをサポートするようになりました。<br>次のコマンドが導入されました。 <b>enter mgmt-bootstrap Firepower Threat Defense、enter bootstrap-key FIREPOWER_MANAGER_IP、enter bootstrap-key FIREWALL_MODE、enter bootstrap-key-secret REGISTRATION_KEY、enter bootstrap-key-secret PASSWORD、enter bootstrap-key FQDN、enter bootstrap-key DNS_SERVERS、enter bootstrap-key SEARCH_DOMAINS、enter ipv4 firepower、enter ipv6 firepower、set value、set gateway、set ip、accept-license-agreement</b> |
| Firepower 9300 上の 16 個の ASA モジュールのシャーシ間クラスタリング                | 1.1.3        | ASA のシャーシ間クラスタリングが実現されました。最大 16 のモジュールを搭載することができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。                                                                                                                                                                                                                                                                                                                                                                         |
| Firepower 9300 上の ASA のシャーシ内クラスタリング                           | 1.1.1        | Firepower 9300 シャーシ内のすべての ASA セキュリティ モジュールをクラスタ化できるようになりました。<br><b>enter cluster-bootstrap、enter logical-device clustered、set chassis-id、set ipv4 gateway、set ipv4 pool、set ipv6 gateway、set ipv6 pool、set key、set mode spanned-etherchannel、set port-type cluster、set service-type、set virtual ipv4、set virtual ipv6</b> コマンドを導入しました                                                                                                                                                                          |



## 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。