Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 2.11(1) コンフィギュレーション ガイド

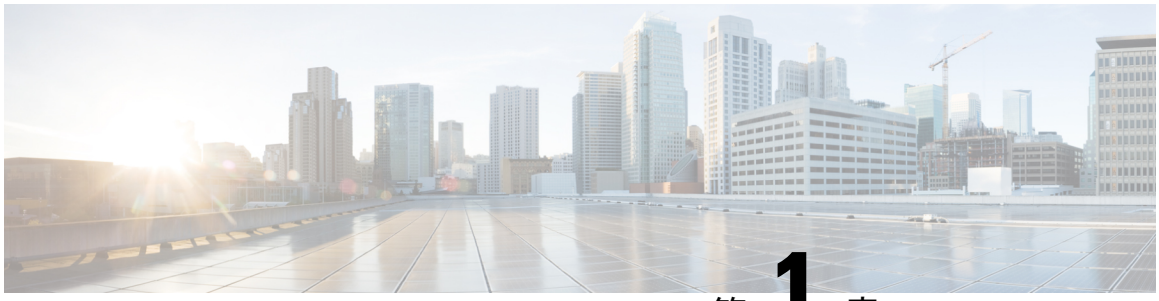
初版：2021 年 12 月 1 日

最終更新：2022 年 5 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

セキュリティ アプライアンスの概要

Firepower セキュリティ アプライアンスについて

Cisco Firepower 4100/9300 シャーシは、ネットワークおよびコンテンツ セキュリティ ソリューションの次世代プラットフォームです。Firepower 4100/9300 シャーシはシスコ アプリケーション セントリック インフラストラクチャ（ACI）セキュリティ ソリューションの一部であり、拡張性、一貫性のある制御、シンプルな管理を実現するために構築された、俊敏でオープン、かつセキュアなプラットフォームを提供します。

Firepower 4100/9300 シャーシ は次の機能を提供します。

- モジュラ シャーシベースのセキュリティ システム：高いパフォーマンス、柔軟な入出力設定、および拡張性を提供します。
- Firepower Chassis Manager：グラフィカルユーザインターフェイスによって、現在のシャーシ ステータスが効率良く視覚的に表示され、シャーシの機能は簡単に設定できます。
- Firepower eXtensible オペレーティングシステム（FXOS）CLI：機能の設定、シャーシステータスのモニタリング、および高度なトラブルシューティング機能へのアクセスを行うコマンドベースのインターフェイスを提供します。
- FXOS REST API：ユーザがシャーシをプログラムを使用して設定し、管理できます。

論理デバイスの動作方法：Firepower 4100/9300

Firepower 4100/9300 は、Firepower eXtensible Operating System（FXOS）という独自のオペレーティング システムをスーパバイザ上で実行します。オンボックスの Firepower Chassis Manager では、シンプルな GUI ベースの管理機能を利用できます。Firepower Chassis Manager を使用して、ハードウェア インターフェイスの設定、スマートライセンシング（ASA 用）、およびその他の基本的な操作パラメータをスーパバイザ上で設定します。

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および1つのオプションデコレータアプリケーションを実行し、サービスチェーンを形成できます。論理デバイスを導入すると、スーパバイザは選択されたアプリケーションイメージをダウンロードし、デフォルト設定を確立します。その後、アプリケーションのオペレーティングシステム内でセキュリティポリシーを設定できます。

論理デバイスは互いにサービスチェーンを形成できず、バックプレーンを介して相互に通信することはできません。別の論理デバイスに到達するために、すべてのトラフィックが1つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。コンテナインスタンスの場合、データインターフェイスを共有できます。この場合にのみ、複数の論理デバイスがバックプレーンを介して通信できます。

サポートされるアプリケーション

次のアプリケーション タイプを使用して、シャーシに論理デバイスを展開できます。

FTD

FTD は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、マルウェア防御などの次世代ファイアウォールサービスを提供します。

FTDは、次のいずれかのマネージャを使用して管理できます。

- FMC：別のサーバ上で実行されるフル機能のマルチデバイス マネージャ。
- FDM：デバイスに含まれるシンプルな単独のデバイスマネージャ。
- CDO：クラウドベースのマルチデバイスマネージャ。

ASA

ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたものです。次のいずれかのマネージャを使用して ASA を管理できます。

- ASDM：デバイスに含まれるシンプルな単独のデバイス マネージャ。
- CLI
- CDO：クラウドベースのマルチデバイスマネージャ。
- CSM：別のサーバー上のマルチデバイスマネージャ。

Radware DefensePro （デコレータ）

Radware DefensePro（vDP）をインストールし、デコレータアプリケーションとして ASA または FTD の目の前で実行することができます。vDP は、Firepower 4100/9300 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。ネットワークからのトラフィックは、ASA または FTD に到達する前に、まず vDP を通過する必要があります。

Firepower Chassis Manager の概要

FXOS は、プラットフォーム設定やインターフェイスの構成、デバイスのプロビジョニング、およびシステム ステータスのモニタリングを簡単にする Web インターフェイスを提供します。ユーザ インターフェイスの上部にあるナビゲーション バーを使用すると次の項目にアクセスできます。

- 概要：[概要（Overview）] ページでは、シャーシのステータスを簡単にモニタできます。詳細については、シャーシ ステータスのモニタリング （4 ページ）を参照してください。
- インターフェイス：[インターフェイス（Interfaces）] ページでは、シャーシにインストールされたインターフェイスのステータスを表示したり、インターフェイス プロパティを編集したり、インターフェイスを有効または無効にしたり、ポート チャネルを作成したりできます。詳細については、インターフェイス管理 （171 ページ）を参照してください。
- Logical Devices：[Logical Devices] ページから、論理デバイスを作成、編集、削除できます。既存の論理デバイスの現在のステータスを表示することもできます。詳細については、論理デバイス （211 ページ）を参照してください。
- セキュリティ モジュール/セキュリティ エンジン：[セキュリティ モジュール/セキュリティ エンジン（Security Modules/Security Engine）] ページから、セキュリティ モジュール/エンジンのステータスを表示し、電源の再投入、再初期化、確認応答、解放などのさまざまな機能を実行できます。詳細については、セキュリティ モジュール/エンジン管理 （317 ページ）を参照してください。
- プラットフォーム設定：[プラットフォーム設定（Platform Settings）] ページでは、日付と時刻、SSH、SNMP、HTTPS、AAA、syslog、DNS のシャーシ設定を行うことができます。詳細については、プラットフォーム設定 （115 ページ）を参照してください。
- システム設定：[システム（System）] メニューでは、次の設定を管理できます。
  - ライセンス：[ライセンス（Licensing）] ページでは、Smart Call Home 設定を行ったり、シャーシをライセンス認証局に登録したりできます。詳細については、ASA のライセンス管理 （19 ページ）を参照してください。
  - 更新：[更新（Updates）] ページでは、プラットフォーム バンドルやアプリケーションのイメージをシャーシにアップロードできます。詳細については、イメージ管理 （65 ページ）を参照してください。
  - ユーザ管理：[ユーザ管理（User Management）] ページでは、ユーザ設定を行ったり、Firepower 4100/9300 シャーシ のユーザ アカウントを定義したりできます。詳細については、ユーザ管理 （45 ページ）を参照してください。

シャーシ ステータスのモニタリング

[Overview] ページから、Firepower 4100/9300 シャーシのステータスを簡単にモニタできます。[概要（Overview）] ページには、次の要素が表示されます。

- [デバイス情報（Device Information）]：[概要（Overview）] ページの上部には、Firepower 4100/9300 シャーシについての次の情報が表示されます。
  - [シャーシ名（Chassis name）]：初期設定時にシャーシに割り当てられた名前を表示します。
  - [IP アドレス（IP address）]：初期設定時にシャーシに割り当てられた IP アドレスを表示します。
  - [Model]：Firepower 4100/9300 シャーシ のモデルを表示します。
  - [Version]：シャーシ上で実行されている FXOS のバージョンを示します。
  - [動作状態（Operational State）]：シャーシの動作可能ステータスを示します。
  - [シャーシの稼働時間（Chassis uptime）]：システムが最後に再起動されてからの経過時間を表示します。
  - [Shutdown] ボタン：Firepower 4100/9300 シャーシをグレースフル シャットダウンします（Firepower 4100/9300 シャーシの電源オフ （111 ページ）を参照）。

（注） [セキュリティモジュール/セキュリティエンジン（Security Modules/Security Engine）] ページから セキュリティ モジュール/エンジンの電源をオン/オフできます（セキュリティモジュール/エンジンの電源オン/オフ （321 ページ）を参照）。

  - [再起動（Reboot）] ボタン：Firepower 4100/9300 シャーシをグレースフル シャットダウンします（Firepower 4100/9300 シャーシ の再起動 （111 ページ）を参照）。
  - [Uptime Information] アイコン：アイコンにカーソルを合わせると、シャーシおよびインストールされているセキュリティ モジュール/エンジンの稼働時間を表示します。

- [Visual Status Display]：[Device Information] セクションの下にはシャーシが視覚的に表示されて、搭載されているコンポーネントとそれらの全般ステータスを示します。[Visual Status Display] に表示されるポートにカーソルを合わせると、インターフェイス名、速度、タイプ、管理状態、動作状態などの追加情報が表示されます。複数のセキュリティ モジュール搭載モデルでは、[Visual Status Display] に表示されるポートにカーソルを合わせると、デバイス名、テンプレート タイプ、管理状態、動作状態などの追加情報が表示されます。当該セキュリティ モジュールに論理デバイスがインストールされている場合は、管理 IP アドレス、ソフトウェア バージョン、論理デバイス モードも表示されます。

- Detailed Status Information：[Visual Status Display] の下に表示されるテーブルで、シャーシの詳細なステータス情報を含みます。ステータス情報は、[障害（Faults）]、[インターフェイス（Interfaces）]、[デバイス（Device）]、[ライセンス（License）]、および[インベントリ（Inventory）] の 5 つのセクションに分かれています。これらの各セクションの概要をテーブルの上に表示できます。さらに確認する情報の概要エリアをクリックするとそれぞれの詳細を表示できます。

  システムは、シャーシについての次の詳細ステータス情報を提供します。

  - [障害（Faults）]：システム内で生成された障害を一覧表示します。これらの障害は、[Critical]、[Major]、[Minor]、[Warning]、[Info] の重大度によってソートされます。一覧表示された障害ごとに重大度、障害の説明、原因、発生回数、最近発生した時刻を表示できます。また、障害が確認されているかどうかも確認できます。

    障害についての追加情報を表示したり、障害を確認するには、該当する障害をクリックします。複数の障害を確認するには、確認する各障害の横にあるチェックボックスを選択して、[Acknowledge] をクリックします。複数の障害の選択と選択解除をすばやく切り替えるには、[Select All Faults] ボタンと [Cancel Selected Faults] ボタンを使用できます。

（注） 障害の根本原因に対処すると、その障害は次のポーリング間隔中にリストから自動的にクリアされます。特定の障害に対処する場合、現在処理中であることが他のユーザにわかるように、その障害を確認済みにすることができます。

  - [Interfaces]：システムにインストールされているインターフェイスが表示されます。[All Interfaces] タブにインターフェイス名、動作状態、管理状態、受信したバイト数、送信したバイト数が表示されます。[**ハードウェア バイパス**] タブには、FTDアプリケーションのハードウェア バイパス機能でサポートされるインターフェイス ペアだけが表示されます。各ペアについて、動作状態が表示されます（disabled：このペアで ハードウェア バイパスは構成されていない、standby：ハードウェア バイパスは構成されているが、現在アクティブではない、bypass：ハードウェア バイパスでアクティブ）。

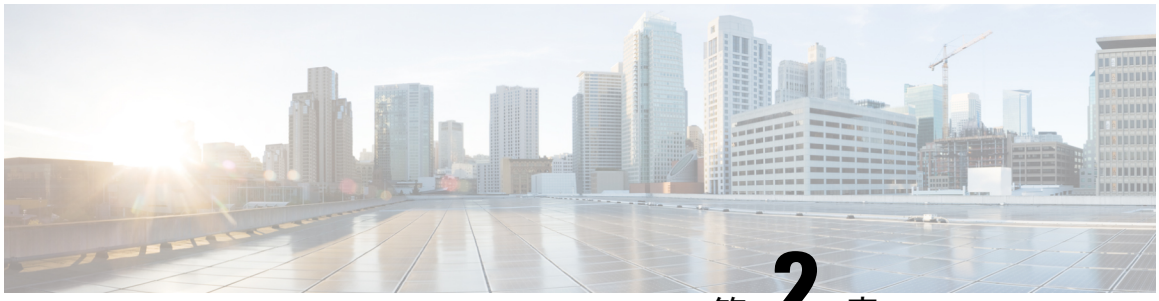
  - [デバイスおよびネットワークインスタンス（Devices & Network Instances）]：システムに設定されている論理デバイスを表示し、各論理デバイス（バー上でカーソルを合わせる）に次の詳細情報を提供します。デバイス名、ステータス、イメージバージョン、管理 IP アドレス、およびコア数。ページの下部では入力 VLAN グループエントリ使用率とスイッチ転送パスエントリ使用率も確認できます。

  - [ライセンス（License）]：（ASA 論理デバイスの場合）スマート ライセンスが有効化になっているかどうかを表示し、Firepower ライセンスの現在の登録ステータスおよびシャーシのライセンス認可情報を示します。

  - [Inventory]：シャーシに搭載されているコンポーネントをリスト表示し、それらのコンポーネントの関連情報（コンポーネント名、コアの数、設置場所、動作ステータ

ス、運用性、キャパシティ、電源、温度、シリアル番号、モデル番号、製品番号、ベンダー）を示します。

（注） 電源の冗長化が実装されている場合は、FXOSの電源の冗長化に関連する設定を変更しないでください。



第 2 章

使用する前に

タスク フロー

次に、Firepower 4100/9300 シャーシを設定する際に実行する必要がある基本的なタスクの手順を示します。

手順

ステップ 1 Firepower 4100/9300 シャーシ ハードウェアを設定します（『*Cisco Firepower Security Appliance Hardware Installation Guide*』を参照）。

ステップ 2 初期設定を完了します（初期設定 （8 ページ）を参照）。

ステップ 3 Firepower Chassis Manager にログインします（Firepower Chassis Manager のログイン/ログアウト （15 ページ）を参照）。

ステップ 4 日時を設定します（日時の設定 （115 ページ） を参照）。

ステップ 5 DNS サーバを設定します（DNS サーバの設定 （162 ページ）を参照）。

ステップ 6 製品ライセンスを登録します（ASA のライセンス管理 （19 ページ）を参照）。

ステップ 7 ユーザを設定します（ユーザ管理 （45 ページ）を参照）。

ステップ 8 必要に応じてソフトウェアの更新を実行します（イメージ管理 （65 ページ）を参照）。

ステップ 9 追加のプラットフォーム設定を実行します（プラットフォーム設定 （115 ページ）を参照）。

ステップ 10 インターフェイスを設定します（インターフェイス管理 （171 ページ）を参照）。

ステップ 11 論理デバイスを作成します（論理デバイス （211 ページ）を参照）。

初期設定

システムの設定と管理に Firepower Chassis Manager または FXOS CLI を使用するには、初めにいくつかの初期設定タスクを実行する必要があります。初期設定を実行するには、コンソールポートを介してアクセスする FXOS CLI を使用するか、管理ポートを介してアクセスする SSH、HTTPS、または REST API を使用します（この手順は、ロータッチ プロビジョニングとも呼ばれます）。

コンソール ポートを使用した初期設定

FXOS CLI を使用して Firepower 4100/9300 シャーシに初めてアクセスすると、システムの設定に使用できるセットアップ ウィザードが表示されます。

（注） 初期設定を繰り返すには、次のコマンドを使用して既存の設定をすべて消去する必要があります。

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Firepower 4100/9300 シャーシの単一の管理ポートには、1 つのみの IPv4 アドレス、ゲートウェイ、サブネット マスク、または 1 つのみの IPv6 アドレス、ゲートウェイ、ネットワーク プレフィックスを指定する必要があります。管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

始める前に

1. Firepower 4100/9300 シャーシの次の物理接続を確認します。
   - コンソール ポートがコンピュータ端末またはコンソール サーバに物理的に接続されている。
   - 1 Gbps イーサネット管理ポートが外部ハブ、スイッチ、またはルータに接続されている。

   詳細については、ハードウェア設置ガイドを参照してください。
2. コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。
   - 9600 ボー
   - 8 データ ビット
   - パリティなし
   - 1 ストップ ビット

3. セットアップ スクリプトで使用する次の情報を収集します。
   - 新しい管理者パスワード
   - 管理 IP アドレスおよびサブネット マスク
   - ゲートウェイ IP アドレス
   - HTTPS および SSH アクセスを許可するサブネット
   - ホスト名とドメイン名
   - DNS サーバの IP アドレス

手順

ステップ 1 シャーシの電源を入れます。

ステップ 2 ターミナル エミュレータを使用して、シリアル コンソール ポートに接続します。

Firepower 4100/9300 には、RS-232 - RJ-45 シリアルコンソールケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。次のシリアル パラメータを使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ステップ 3 プロンプトに従ってシステム設定を行います。

（注） 必要に応じて、初期設定時に随時デバッグメニューに移動し、セットアップ問題のデバッグ、設定の中止、およびシステムの再起動を行うことができます。デバッグ メニューに移動するには、Ctrl+C を押します。デバッグ メニューを終了するには、Ctrl+D を 2 回押します。Ctrl+D を 押す 1 回目と 2 回目の間に入力したものがある場合、2 回目の Ctrl + D を押した後に実行されます。

例：

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.
```

```
  You have chosen to setup a new Security Appliance.
        Continue? (yes/no): y

  Enforce strong password? (yes/no) [y]: n

  Enter the password for "admin": Farscape&32
  Confirm the password for "admin": Farscape&32
  Enter the system name:  firepower-9300

  Supervisor Mgmt IP address : 10.80.6.12

  Supervisor Mgmt IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 10.80.6.1

  The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

  Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

  SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  SSH Mgmt Access IPv4 netmask: 255.0.0.0

  Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

  Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

  HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

  Configure the DNS Server IP address? (yes/no) [n]: y

    DNS IP address : 10.164.47.13

  Configure the default domain name? (yes/no) [n]: y

    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
```

```
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

管理ポートを使用したロータッチ プロビジョニング

Firepower 4100/9300 シャーシ の起動時にスタートアップ コンフィギュレーションが見つからない場合、デバイスはロータッチプロビジョニング モードに入り、Dynamic Host Control Protocol（DHCP）サーバを検出して、その管理インターフェイスIPを使用して自身のブートストラップを実行します。その後、管理インターフェイスを介して接続して、SSH、HTTPS、またはFXOS REST API を使用してシステムを設定できます。

（注） 初期設定を繰り返すには、次のコマンドを使用して既存の設定をすべて消去する必要があります。

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Firepower 4100/9300 シャーシの単一の管理ポートには、1 つのみの IPv4 アドレス、ゲートウェイ、サブネット マスク、または 1 つのみの IPv6 アドレス、ゲートウェイ、ネットワーク プレフィックスを指定する必要があります。管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

始める前に

セットアップ スクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネット マスク
- ゲートウェイ IP アドレス
- HTTPS および SSH アクセスを許可するサブネット
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ 1 DHCP サーバを設定して、Firepower 4100/9300 シャーシ の管理ポートに IP アドレスを割り当てます。

Firepower 4100/9300 シャーシ からの DHCP クライアント要求には、次のものが含まれます。

- 管理インターフェイスの MAC アドレス。
- DHCP オプション 60（vendor-class-identifier）：「FPR9300」または「FPR4100」に設定します。
- DHCP オプション 61（dhcp-client-identifier）：Firepower 4100/9300 シャーシ のシリアル番号に設定します。このシリアル番号は、シャーシの引き出しタブで確認できます。

ステップ 2 Firepower 4100/9300 シャーシの電源を入れます。
シャーシの起動時にスタートアップ コンフィギュレーションが見つからない場合、デバイスはロータッチ プロビジョニング モードに入ります。

ステップ 3 HTTPS を使用してシステムを設定するには、次の手順を実行します。

a) サポートされているブラウザを使用して、アドレス バーに次の URL を入力します。

`https://<ip_address>/api`

ここで、<*ip_address*> は、DHCP サーバによって割り当てられた Firepower 4100/9300 シャーシ の管理ポートの IP アドレスです。

（注） サポートされるブラウザの詳細については、使用しているバージョンのリリース ノートを参照してください（http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.htm を参照）。

b) ユーザ名とパスワードの入力を求められたら、それぞれ **install** と <*chassis_serial_number*> を入力してログインします。

<*chassis_serial_number*> は、シャーシのタグを調べると確認できます。

c) プロンプトに従ってシステム設定を行います。

- 強力なパスワードの適用ポリシー（強力なパスワードのガイドラインについては、ユーザ アカウント （45 ページ） を参照）。
- admin アカウントのパスワード。
- システム名。
- スーパーバイザ管理の IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス。
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス。

- SSH アクセスが許可されているホスト/ネットワーク アドレスおよびネットマスク/プレフィックス。
- HTTPSアクセスが許可されるホスト/ネットワークアドレスとネットマスク/プレフィックス。
- DNS サーバの IPv4 または IPv6 アドレス。
- デフォルト ドメイン名。

d) **[送信（Submit）]** をクリックします。

ステップ 4 SSH を使用してシステムを設定するには、次の手順を実行します。

a) 次のコマンドを使用して、管理ポートに接続します。

ssh install@*<ip_address>*

ここで <*ip_address*> は、DHCP サーバによって割り当てられた Firepower 4100/9300 シャーシ の管理ポートの IP アドレスです。

b) パスワードの入力を求められたら、**Admin123** を入力してログインします。

c) プロンプトに従ってシステム設定を行います。

（注） 必要に応じて、初期設定時に随時デバッグメニューに移動し、セットアップ問題のデバッグ、設定の中止、およびシステムの再起動を行うことができます。デバッグ メニューに移動するには、Ctrl + C を押します。デバッグ メニューを終了するには、Ctrl + D を 2 回押します。Ctrl + D を 押す 1 回目と 2 回目の間に入力したものがある場合、2 回目の Ctrl + D を押した後に実行されます。

例：

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0
```

```
IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.


Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

  Default domain name : cisco.com

Following configurations will be applied:

  Switch Fabric=A
  System Name=firepower-9300
  Enforced Strong Password=no
  Supervisor Mgmt IP Address=10.89.5.14
  Supervisor Mgmt IP Netmask=255.255.255.192
  Default Gateway=10.89.5.1
  SSH Access Configured=yes
      SSH IP Address=10.0.0.0
      SSH IP Netmask=255.0.0.0
  HTTPS Access Configured=yes
      HTTPS IP Address=10.0.0.0
      HTTPS IP Netmask=255.0.0.0
  DNS Server=72.163.47.11
  Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):
 y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Initial Setup complete, Terminating sessions
.Connection to <ip_address> closed.
```

ステップ 5 FXOS REST API を使用してシステムを設定するには、次の手順を実行します。

REST API を使用してシステムを設定するには、次の例を使用します。詳細については、https://developer.cisco.com/site/ssp/firepower/を参照してください。

（注） dns、domain_name、https_net、https_mask、ssh_net、ssh_mask の各属性はオプションです。REST API 設定の場合、他のすべての属性は必須です。

```
IPv4 REST API example:
```

```
{
    "fxosBootstrap": {
        "dns": "1.1.1.1",
        "domain_name": "cisco.com",
        "mgmt_gw": "192.168.0.1",
        "mgmt_ip": "192.168.93.3",
        "mgmt_mask": "255.255.0.0",
        "password1": "admin123",
        "password2": "admin123",
        "strong_password": "yes",
        "system_name": "firepower-9300",
        "https_mask": "2",
        "https_net": "::",
        "ssh_mask": "0",
        "ssh_net": "::"
    }
}
```

IPV6 REST API example

```
{
    "fxosBootstrap": {
        "dns": "2001::3434:4343",
        "domain_name": "cisco.com",
        "https_mask": "2",
        "https_net": "::",
        "mgmt_gw": "2001::1",
        "mgmt_ip": "2001::2001",
        "mgmt_mask": "64",
        "password1": "admin123",
        "password2": "admin123",
        "ssh_mask": "0",
        "ssh_net": "::",
        "strong_password": "yes",
        "system_name": "firepower-9300"
    }
}
```

Firepower Chassis Manager のログイン/ログアウト

Firepower Chassis Manager を使用して Firepower 4100/9300 シャーシ を設定するには、その前に、有効なユーザー アカウントを使用してログオンする必要があります。ユーザ アカウントの詳細については、ユーザ管理 （45 ページ）を参照してください。

一定期間にわたって操作がない場合は、自動的にシステムからログアウトされます。デフォルトでは、10 分間にわたり操作を行わないと自動的にログアウトします。このタイムアウト設定を変更するには、セッション タイムアウトの設定 （56 ページ）を参照してください。 また、セッションがアクティブな場合でも、一定時間の経過後にユーザをシステムからログオフさせるように絶対タイムアウトを設定することもできます。絶対タイムアウトを設定するには、絶対セッション タイムアウトの設定 （57 ページ）を参照してください。

システムを変更した結果、Firepower Chassis Manager から自動的にログアウトされる場合の一覧については、セッション変更により Firepower Chassis Manager セッションが閉じる場合 （93 ページ）を参照してください。

（注） 指定した時間でユーザがシステムからロックアウトされる前に、ログイン試行の失敗を特定の数だけ許可するように Firepower Chassis Manager を任意で設定できます。詳細については、ログイン試行の最大回数の設定 （58 ページ）を参照してください。

手順

ステップ 1 Firepower Chassis Manager にログインするには、次の手順を実行します。

a) サポートされているブラウザを使用して、アドレス バーに次の URL を入力します。

`https://<chassis_mgmt_ip_address>`

ここで、*<chassis_mgmt_ip_address>* は、初期設定時に入力した Firepower 4100/9300 シャーシ の IP アドレスまたはホスト名です。

（注） サポートされるブラウザの詳細については、使用しているバージョンのリリース ノートを参照してください（http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.htn を参照）。

b) ユーザ名とパスワードを入力します。

c) [ログイン（Login）] をクリックします。

ログインすると Firepower Chassis Manager が開き、[概要（Overview）] ページが表示されます。

ステップ 2 Firepower Chassis Manager からログアウトするには、ナビゲーション バーに表示されている自分のユーザ名をポイントし、[ログアウト（Logout）] を選択します。
Firepower Chassis Manager からログアウトすると、ログイン画面に戻ります。

FXOS CLIへのアクセス

FXOS CLIには、コンソール ポートに繋いだ端末を使って接続します。コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

SSH と Telnet を使用しても FXOS CLI に接続できます。FXOS は最大 8 つの SSH 接続を同時にサポートできます。SSH で接続するには、Firepower 4100/9300 シャーシ のホスト名または IP アドレスが必要になります。

次のシンタックスの例のいずれかを使用して、SSH、Telnet、または Putty でログインします。

（注） SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

```
ssh ucs-example\\jsmith@192.0.20.11
ssh ucs-example\\jsmith@2001::1
```

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

Linux 端末からは以下の Telnet を使用します。

（注） デフォルトでは、Telnet はディセーブルになっています。Telnet を有効化する手順については、Telnet の設定 （123 ページ）を参照してください。

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

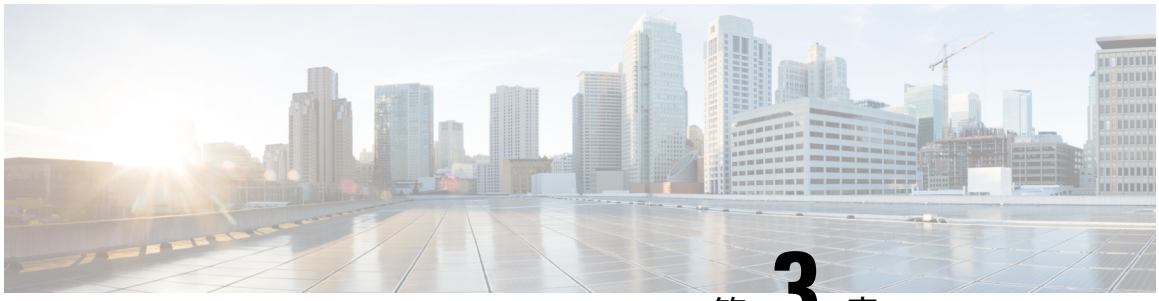
```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty クライアントから：

- **ucs-***auth-domain**username* でログインします。

```
Login as: ucs-example\jsmith
```

（注） デフォルトの認証がローカルに設定されており、コンソール認証がLDAPに設定されている場合は、**ucs-local\admin**（adminはローカル アカウントの名前）を使用してPuttyクライアントからファブリック インターコネクトにログインできます。



第 3 章

ASA のライセンス管理

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザがアクセスできるものを制御できます。スマート ライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

（注） このセクションは、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。FTD 論理デバイスのライセンスの詳細については、『FMC Configuration Guide』を参照してください。

スマート ソフトウェア ライセンスについて

ここでは、スマート ソフトウェア ライセンスの仕組みについて説明します。

（注） このセクションは、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。FTD 論理デバイスのライセンスの詳細については、『FMC Configuration Guide』を参照してください。

ASA のススマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ上の ASA アプリケーションの場合、スマート ソフトウェア ライセンス設定は Firepower 4100/9300 シャーシ スーパバイザとアプリケーションの間で分割されます。

- Firepower 4100/9300 シャーシ：ライセンス認証局との通信を行うためのパラメータを含めて、スーパバイザにすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。

（注） シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマート ライセンス方式を有効にする必要があります。

- ASA アプリケーション：アプリケーションのすべてのライセンスの権限付与を設定します。

（注） Cisco Transport Gateway は、Firepower 4100/9300 セキュリティアプライアンスではサポートされていません。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、オプションで追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社ごとにアカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびデバイスの管理をより簡単に行うことができます。

オフライン管理

デバイスにインターネット アクセスがなく、License Authority に登録できない場合は、オフライン ライセンスを設定できます。

永久ライセンスの予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、License Authority への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様にライセンスを購入し、ASA のライセンス キーをインストールします。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用します。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。

すべての機能、すなわちモデルの正しい最大スループットを備えた標準ティアおよびキャリアライセンスを有効にするライセンスを取得できます。ライセンスはFirepower4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

サテライト サーバ

デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト サーバをインストールできます。サテライト（衛星）は、Smart Software Manager 機能のサブセットを提供し、これによりすべてのローカル デバイスに重要なライセンス サービスが提供可能になります。ライセンス使用を同期するために、定期的にサテライトだけが License Authority と同期する必要があります。スケジュールに沿って同期するか、または手動で同期できます。

サテライトアプリケーションをダウンロードして導入したら、インターネットを使用してCisco SSM にデータを送信しなくても、以下の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、スマート アカウント マネージャ サテライトにある『Smart Software Manager satellite installation and configuration guide』を参照してください。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのデバイスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシのみがデバイスとして登録され、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3 つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

評価ライセンス

Firepower 4100/9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシ レベル評価モード：Firepower 4100/9300 シャーシによる Licensing Authority への登録の前に、評価モードで 90 日間（合計使用期間）動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシが Licensing Authority に登録をした後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを取得することはできません。永続ライセンスのみでこの権限がサポートされます。

Smart Software Manager 通信

このセクションでは、デバイスが Smart Software Manager と通信する方法について説明します。

デバイス登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各シャーシを導入するとき、または既存のシャーシを登録するときにこのトークン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

導入した後、または既存のシャーシでこれらのパラメータを手動で設定した後、そのシャーシを起動するとシスコのライセンス認証局に登録されます。シャーシがトークンで登録されるとき、ライセンス認証局はシャーシとそのライセンス認証局との間で通信を行うために ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

ライセンス認証局との定期通信

デバイスはライセンス認証局と 30 日おきに通信します。Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、すぐに変更されるようにすることができます。または、スケジュールどおりにデバイスが通信するのを待ちます。

必要に応じて、HTTP プロキシを設定できます。

Firepower 4100/9300 シャーシでは、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネットアクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

（注） デバイスが 1 年間ライセンス認証局と通信できない場合、デバイスは未登録状態になりますが、以前に有効にされた強力な暗号化機能は失われません。

コンプライアンス逸脱状態

次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 使用超過：デバイスが利用できないライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、Firepower 4100/9300 シャーシで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反の場合、特別なライセンスが必要な機能への設定変更はできなくなりますが、その他の動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。

Smart Call Home インフラストラクチャ

デフォルトで、Smart Call Home のプロファイルは、ライセンス認証局の URL を指定する FXOS 設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの設定可能なオプションは、ライセンス機関の宛先アドレス URL のみであることに注意してください。Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

（注） Cisco Transport Gateway は、Firepower 4100/9300 セキュリティアプライアンスではサポートされていません。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、Firepower 4100/9300 シャーシ と Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリのストリーミングにより、対象データを ASA から選択して、構造化形式でリモート管理ステーションに送信するメカニズムが提供されるため、次のことが実現します。

- ネットワーク内の製品の有効性を向上させるために利用可能な未使用の機能が通知されます。
- 製品に付随する追加のテクニカル サポート サービスとモニタリングについて通知されます。
- シスコ製品の改善に役立ちます。

Cisco Smart Software Manager に Firepower 4100/9300 を登録するときは、Cisco Success Network を有効にします。Firepower 4100/9300 シャーシ の License Authority への登録 （37 ページ）を参照してください。

次の条件がすべて満たされている場合にのみ、Cisco Success Network に登録できます。

- スマート ソフトウェア ライセンスが登録されている
- スマートライセンスのサテライトモードが無効になっている
- パーマネントライセンスが無効になっている

Cisco Success Network に登録すると、シャーシは常にセキュアな接続を確立して維持します。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

[System] > **[Licensing]** > **[Cisco Success Network]** ページで Cisco Success Network の登録ステータスを表示できます。また、登録ステータスを変更することもできます。Cisco Success Network の登録の変更 （38 ページ） を参照してください。

Cisco Success Network テレメトリ データ

Cisco Success Network により、シャーシの設定と動作状態に関する情報を 24 時間ごとに Cisco Success Network クラウドにストリーミングすることができます。収集およびモニタ対象のデータには、次の情報が含まれます。

- **登録済みデバイス情報**：Firepower 4100/9300 シャーシ のモデル名、製品 ID、シリアル番号、UUID、システム稼働時間、およびスマートライセンス情報。登録済みデバイス データ （25 ページ）を参照してください。

- **ソフトウェア情報**：Firepower 4100/9300 シャーシで実行されているソフトウェアのタイプとバージョン番号。ソフトウェア バージョン データ （26 ページ）を参照してください。
- **ASA デバイス情報**：Firepower 4100/9300 の セキュリティ モジュール/エンジン で稼動している ASA デバイスに関する情報。Firepower 4100 シリーズ の場合は、単一の ASA デバイスに関する情報のみが対象になることに注意してください。ASA デバイス情報には、各デバイス、デバイスモデル、シリアル番号、およびソフトウェアバージョンに使用されるスマートライセンスが含まれます。ASA デバイスデータ （26 ページ）を参照してください。
  - **パフォーマンス情報**：ASA デバイスのシステム稼働時間、CPU 使用率、メモリ使用率、ディスク容量の使用率、および帯域幅の使用状況に関する情報。パフォーマンス データ （27 ページ）を参照してください。
  - **使用状況**：機能ステータス、クラスタ、フェールオーバー、およびログイン情報。
    - **機能ステータス**：設定済みまたはデフォルトで有効になっている ASA 機能のリスト。
    - **クラスタ情報**：ASA デバイスがクラスタモードの場合は、クラスタ情報が表示されます。ASA デバイスがクラスタモードではない場合、この情報は表示されません。クラスタ情報には、ASA デバイスのクラスタグループ名、クラスタインターフェイスモード、ユニット名、および状態が含まれます。同じクラスタ内の他のピア ASA デバイスの場合、クラスタ情報には名前、状態、およびシリアル番号が含まれます。
    - **フェールオーバー情報**：ASA がフェールオーバーモードの場合、フェールオーバー情報が表示されます。ASA がフェールオーバーモードではない場合、この情報は表示されません。フェールオーバー情報には、ASA のロールと状態、およびピア ASA デバイスのロール、状態、およびシリアル番号が含まれます。
    - **ログイン履歴**：ASA デバイスで最後にログインに成功したユーザのログイン頻度、ログイン時間、および日付スタンプ。ただし、ログイン履歴にはユーザのログイン名、ログイン情報、その他の個人情報は含まれません。

  詳細については、使用状況データ （28 ページ）を参照してください。

登録済みデバイス データ

Cisco Success Network に Firepower 4100/9300 シャーシ を登録したら、シャーシに関するテレメトリデータの Cisco Cloud へのストリーミングを選択します。収集およびモニタ対象のデータを次の表に示します。

表 *1*：登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス モデル	Cisco Firepower FP9300 セキュリティ アプライアンス

データ ポイント	値の例
シリアル番号	GMX1135L01K
スマートライセンス PIID	752107e9-e473-4916-8566-e26d0c4a5bd9
スマートライセンスの仮想アカウント名	FXOS-general
システムの動作期間	32115
UDI 製品 ID	FPR-C9300-AC

ソフトウェア バージョン データ

Cisco Success Network には、タイプやソフトウェアバージョンといったソフトウェア情報が収集されます。収集およびモニタ対象のソフトウェア情報を次の表に示します。

表 *2:* ソフトウェア バージョンのテレメトリ データ

データ ポイント	値の例
タイプ	package_version
バージョン	2.7(1.52)

ASA デバイスデータ

Cisco Success Network には、 Firepower 4100/9300 の セキュリティ モジュール/エンジン で稼動している ASA デバイスに関する情報が収集されます。収集およびモニタ対象の ASA デバイス情報を次の表に示します。

表 *3: ASA* デバイステレメトリデータ

データ ポイント	値の例
ASA デバイス PID	FPR9K-SM-36
ASA デバイスモデル	Cisco Adaptive Security Appliance
ASA デバイスのシリアル番号	XDQ311841WA
展開タイプ（ネイティブまたはコンテナ）	Native
セキュリティ コンテキスト モード（シングルまたはマルチ）	シングル

ASA のソフトウェアバージョン	{
	type: "asa_version",
	ersion: "9.13.1.5"
	}

データ ポイント	値の例

デバイスマネージャのバージョン	{
	type: "device_mgr_version",
	version: "7.10.1"
	}

使用中の有効なスマートライセンス	{
	"type": "Strong encryption",
	"tag":
	"regid.2016-05.com.cisco.ASA-GEN-STRONG-ENCRYPTION,
	5.7_982308k4-74w2-5f38-64na-707q99g10cce",
	"count": 1
	}

パフォーマンス データ

Cisco Success Network には、ASA デバイス固有のパフォーマンス情報が収集されます。この情報には、システム稼働時間、CPU使用率、メモリ使用率、ディスク容量の使用率、および帯域幅の使用状況が含まれます。

- **CPU 使用率**：過去 5 分間の CPU 使用率情報
- **メモリ使用率**：システムの空きメモリ、使用メモリ、および合計メモリ
- **ディスク使用率**：ディスクの空き容量、使用済み容量、および合計容量の情報
- **システムの稼働時間**：システムの稼働時間情報
- **帯域幅の使用状況**：システム帯域幅の使用状況（nameif が設定されたすべてのインターフェイスから集約）

  これは、システムの稼働時間以降に受信および送信された1秒あたりのパケット（またはバイト）の統計情報を示します。

収集およびモニタ対象の情報を次の表に示します。

表 *4:* パフォーマンス テレメトリデータ

データ ポイント	値の例

過去 5 分間のシステム CPU 使用率	{
	“fiveSecondsPercentage”:0.2000000,
	“oneMinutePercentage”: 0,
	“fiveMinutesPercentage”: 0
	
	}

システム メモリ使用率	{
	“freeMemoryInBytes”:225854966384,
	“usedMemoryInBytes”: 17798281616,
	“totalMemoryInBytes”:243653248000
	
	}

データ ポイント	値の例

システムのディスク使用率	{
	"freeGB": 21.237285,
	"usedGB": 0.238805,
	"totalGB": 21.476090
	
	}

システムの動作期間	99700000

システム帯域幅の使用状況	{
	"receivedPktsPerSec": 3,
	"receivedBytesPerSec": 212,
	"transmittedPktsPerSec": 3,
	"transmittedBytesPerSec": 399
	}

使用状況データ

Cisco Success Network には、シャーシの セキュリティ モジュール/エンジン で稼動している ASAデバイスの機能ステータス、クラスタ、フェールオーバー、およびログイン情報が収集されます。ASA デバイス使用率に関して収集およびモニタされる情報を次の表に示します。

表 *5:* テレメトリデータの使用率

データ ポイント	値の例

機能ステータス	[{
	"name": "cluster",
	"status": "enabled"
	},
	{
	"name": "webvpn",
	"status": "enabled"
	},
	{
	"name": "logging-buffered",
	"status": "debugging"
	}]

クラスタ情報	{
	"clusterGroupName": "asa-cluster",
	"interfaceMode": "spanned",
	"unitName": "unit-3-3",
	"unitState": "SLAVE",
	"otherMembers": {
	"items": [
	{
	"memberName": "unit-2-1",
	"memberState": "MASTER",
	
	"memberSerialNum": "DAK391674E"
	}
	]
	}
	
	}

データ ポイント	値の例

フェールオーバー情報	{
	myRole: “Primary”,
	peerRole: “Secondary”,
	myState: “active”,
	peerState: “standby”,
	peerSerialNum:
	“DAK39162B”
	}

ログイン履歴	{
	"loginTimes": "1 times in last 1 days",
	"lastSuccessfulLogin": "12:25:36 PDT Mar 11
	2019"
	}

テレメトリ ファイルの例

Firepower 4100/9300 シャーシ テレメトリが有効でオンライン状態にあるすべての ASA デバイスから受信されたデータは、シャーシ固有の情報やその他のフィールドと集約されてから Cisco Cloud に送信されます。テレメトリデータを持つアプリケーションがない場合でも、テレメトリはシャーシ情報とともに Cisco Cloud に送信されます。

以下は、Cisco Success Network テレメトリファイルの例です。このファイルには、Cisco Cloud に送信された Firepower 9300 の 2 台の ASA デバイスの情報が保存されています。

```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json",
    "msgID": "2227"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1560868270055,
    "FXOS": {
      "FXOSdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "HNY4475P01K",
       "smartLicenseProductInstanceIdentifier": "413509m0-f952-5822-7492-r62c0a5h4gf4",

        "smartLicenseVirtualAccountName": "FXOS-general",
        "systemUptime": 32115,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "2.7(1.52)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
          "CPUUsage": {
```

```
  "fiveMinutesPercentage": 0,
  "fiveSecondsPercentage": 0,
  "oneMinutePercentage": 0
},
"bandwidthUsage": {
  "receivedBytesPerSec": 1,
  "receivedPktsPerSec": 0,
  "transmittedBytesPerSec": 1,
  "transmittedPktsPerSec": 0
},
"deviceInfo": {
  "deploymentType": "Native",
  "deviceModel": "Cisco Adaptive Security Appliance",
  "securityContextMode": "Single",
  "serialNumber": "ADG2158508T",
  "systemUptime": 31084,
  "udiProductIdentifier": "FPR9K-SM-24"
},
"diskUsage": {
  "freeGB": 19.781810760498047,
  "totalGB": 20.0009765625,
  "usedGB": 0.21916580200195312
},
"featureStatus": {
  "items": [
    {
      "name": "aaa-proxy-limit",
      "status": "enabled"
    },
    {
      "name": "firewall_user_authentication",
      "status": "enabled"
    },
    {
      "name": "IKEv2 fragmentation",
      "status": "enabled"
    },
    {
      "name": "inspection-dns",
      "status": "enabled"
    },
    {
      "name": "inspection-esmtp",
      "status": "enabled"
    },
    {
      "name": "inspection-ftp",
      "status": "enabled"
    },
    {
      "name": "inspection-hs232",
      "status": "enabled"
    },
    {
      "name": "inspection-netbios",
      "status": "enabled"
    },
    {
      "name": "inspection-rsh",
      "status": "enabled"
    },
    {
      "name": "inspection-rtsp",
      "status": "enabled"
```

```
    },
    {
      "name": "inspection-sip",
      "status": "enabled"
    },
    {
      "name": "inspection-skinny",
      "status": "enabled"
    },
    {
      "name": "inspection-snmp",
      "status": "enabled"
    },
    {
      "name": "inspection-sqlnet",
      "status": "enabled"
    },
    {
      "name": "inspection-sunrpc",
      "status": "enabled"
    },
    {
      "name": "inspection-tftp",
      "status": "enabled"
    },
    {
      "name": "inspection-xdmcp",
      "status": "enabled"
    },
    {
      "name": "management-mode",
      "status": "normal"
    },
    {
      "name": "mobike",
      "status": "enabled"
    },
    {
      "name": "ntp",
      "status": "enabled"
    },
    {
      "name": "sctp-engine",
      "status": "enabled"
    },
    {
      "name": "smart-licensing",
      "status": "enabled"
    },
    {
      "name": "static-route",
      "status": "enabled"
    },
    {
      "name": "threat_detection_basic_threat",
      "status": "enabled"
    },
    {
      "name": "threat_detection_stat_access_list",
      "status": "enabled"
    }
  ]
},
"licenseActivated": {
```

```
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:18 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226031548496,
    "totalMemoryInBytes": 241583656960,
    "usedMemoryInBytes": 15552108464
  },
  "versions": {
    "items": [
      {
        "type": "asa_version",
        "version": "9.13(1)248"
      },
      {
        "type": "device_mgr_version",
        "version": "7.13(1)31"
      }
    ]
  }
},
{
  "CPUUsage": {
    "fiveMinutesPercentage": 0,
    "fiveSecondsPercentage": 0,
    "oneMinutePercentage": 0
  },
  "bandwidthUsage": {
    "receivedBytesPerSec": 1,
    "receivedPktsPerSec": 0,
    "transmittedBytesPerSec": 1,
    "transmittedPktsPerSec": 0
  },
  "deviceInfo": {
    "deploymentType": "Native",
    "deviceModel": "Cisco Adaptive Security Appliance",
    "securityContextMode": "Single",
    "serialNumber": "RFL21764S1D",
    "systemUptime": 31083,
    "udiProductIdentifier": "FPR9K-SM-24"
  },
  "diskUsage": {
    "freeGB": 19.781543731689453,
    "totalGB": 20.0009765625,
    "usedGB": 0.21943283081054688
  },
  "featureStatus": {
    "items": [
      {
        "name": "aaa-proxy-limit",
        "status": "enabled"
      },
      {
        "name": "call-home",
        "status": "enabled"
      },
      {
        "name": "crypto-ca-trustpoint-id-usage-ssl-ipsec",
        "status": "enabled"
      },
      {
```

```
  "name": "firewall_user_authentication",
  "status": "enabled"
},
{
  "name": "IKEv2 fragmentation",
  "status": "enabled"
},
{
  "name": "inspection-dns",
  "status": "enabled"
},
{
  "name": "inspection-esmtp",
  "status": "enabled"
},
{
  "name": "inspection-ftp",
  "status": "enabled"
},
{
  "name": "inspection-hs232",
  "status": "enabled"
},
{
  "name": "inspection-netbios",
  "status": "enabled"
},
{
  "name": "inspection-rsh",
  "status": "enabled"
},
{
  "name": "inspection-rtsp",
  "status": "enabled"
},
{
  "name": "inspection-sip",
  "status": "enabled"
},
{
  "name": "inspection-skinny",
  "status": "enabled"
},
{
  "name": "inspection-snmp",
  "status": "enabled"
},
{
  "name": "inspection-sqlnet",
  "status": "enabled"
},
{
  "name": "inspection-sunrpc",
  "status": "enabled"
},
{
  "name": "inspection-tftp",
  "status": "enabled"
},
{
  "name": "inspection-xdmcp",
  "status": "enabled"
},
{
```

```
            "name": "management-mode",
            "status": "normal"
          },
          {
            "name": "mobike",
            "status": "enabled"
          },
          {
            "name": "ntp",
            "status": "enabled"
          },
          {
            "name": "sctp-engine",
            "status": "enabled"
          },
          {
            "name": "smart-licensing",
            "status": "enabled"
          },
          {
            "name": "static-route",
            "status": "enabled"
          },
          {
            "name": "threat_detection_basic_threat",
            "status": "enabled"
          },
          {
            "name": "threat_detection_stat_access_list",
            "status": "enabled"
          }
        ]
      },
      "licenseActivated": {
        "items": []
      },
      "loginHistory": {
        "lastSuccessfulLogin": "05:53:16 UTC Jun 18 2019",
        "loginTimes": "1 times in last 1 days"
      },
      "memoryUsage": {
        "freeMemoryInBytes": 226028740080,
        "totalMemoryInBytes": 241581195264,
        "usedMemoryInBytes": 15552455184
      },
      "versions": {
        "items": [
          {
            "type": "asa_version",
            "version": "9.13(1)248"
          },
          {
            "type": "device_mgr_version",
            "version": "7.13(1)31"
          }
        ]
      }
    }
  ]
 }
}
```

スマート ソフトウェア ライセンスの前提条件

- この章は、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。FTD 論理デバイスのライセンスの詳細については、『FMC Configuration Guide』を参照してください。
- Cisco Smart Software Manager でマスター アカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- Cisco Commerce Workspace から 1 つ以上のライセンスを購入します。ホーム ページの [製品とソリューションを検索（Find Products and Solutions）] フィールドで、該当するプラットフォームを検索します。一部のライセンスは無料ですが、スマート ソフトウェア ライセンス アカウントにそれらを追加する必要があります。
- シャーシがライセンス機関と通信できるように、シャーシからのインターネット アクセスまたは HTTP プロキシ アクセスを確保します。
- シャーシがライセンス機関の名前を解決できるように、DNS サーバを設定します。
- シャーシのための時間を設定します。
- ASA ライセンス資格を設定する前に、Firepower 4100/9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

スマート ソフトウェア ライセンスのガイドライン

フェイルオーバー クラスタリングのための ASA ガイドライン

各 Firepower 4100/9300 シャーシは、License Authority またはサテライト サーバに登録される必要があります。セカンダリ ユニットに追加費用はかかりません。 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。

スマート ソフトウェア ライセンスのデフォルト

Firepower 4100/9300 シャーシ のデフォルト設定には、ライセンス認証局の URL を指定する「SLProfile」という Smart Call Home のプロファイルが含まれています。

通常スマート ソフトウェア ライセンシングの設定

Cisco License Authority と通信するため、必要に応じて HTTP プロキシを設定できます。License Authority に登録するには、スマート ソフトウェア ライセンス アカウントから取得した Firepower 4100/9300 シャーシ の登録トークン ID を入力する必要があります。

手順

ステップ 1 （任意）HTTP プロキシの設定 （36 ページ）。
ステップ 2 （任意）Call Home URL の削除 （37 ページ）
ステップ 3 Firepower 4100/9300 シャーシ の License Authority への登録 （37 ページ）。

（任意）HTTP プロキシの設定

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

手順

ステップ 1 **[システム（System）]** > **[ライセンス（Licensing）]** > **[Call Home]** を選択します。

[Call Home] ページには、License Authority の宛先アドレス URL を設定するフィールド、および HTTP プロキシを設定するフィールドが表示されます。

（注） Cisco TAC からの指示がない限り、ライセンス認証局の URL を変更しないでください。

ステップ 2 [サーバの有効化（Server Enable）] ドロップダウン リストから、[オン（on）] を選択します。
ステップ 3 [サーバ URL（Server URL）] フィールドと [サーバ ポート（Server Port）] フィールドにプロキシ IP アドレスとポートを入力します。たとえば、HTTPS サーバのポート 443 を入力します。
ステップ 4 [保存（Save）] をクリックします。

（任意）Call Home URL の削除

以前に設定された Call Home URL を削除するには、次の手順を実行します。

手順

ステップ 1 **[システム（System）]** > **[ライセンス（Licensing）]** > **[Call Home]** を選択します。

ステップ 2 [Call home Configuration] 領域で、[Delete] を選択します。

Firepower 4100/9300 シャーシ の License Authority への登録

Firepower 4100/9300 シャーシ を登録すると、ライセンス認証局によって Firepower 4100/9300 シャーシ とライセンス認証局との間の通信に使用される ID 証明書が発行されます。また、Firepower 4100/9300 シャーシが該当する仮想アカウントに割り当てられます。通常、この手順は 1 回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、Firepower 4100/9300 シャーシ の再登録が必要になります。

手順

ステップ 1 Smart Software Manager または Smart Software Manager Satellite で、このFirepower 4100/9300 シャーシの追加先となるバーチャル アカウントの登録トークンを要求してコピーします。

スマート ソフトウェア マネージャ サテライトを使用して登録トークンを要求する方法について詳しくは、『Cisco Smart Software Manager Satellite User Guide』（https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html）を参照してください。

ステップ 2 Firepower Chassis Manager で、**[システム（System）]** > **[ライセンス（Licensing）]** > **[スマート ライセンス（Smart License）]** の順に選択します。

ステップ 3 [Enter Product Instance Registration Token] フィールドに登録トークンを入力します。

ステップ 4 （任意）Cisco Success Network 機能を無効にするには、**Enable Cisco Success Network** チェックボックスをオフにします。

詳細については、Cisco Success Network （24 ページ）を参照してください。

ステップ 5 [登録（Register）] をクリックします。

Firepower 4100/9300 シャーシがライセンス認証局への登録を試行します。

デバイスの登録を解除するには、[登録解除（Unregister）] をクリックします。

Firepower 4100/9300 シャーシ の登録を解除すると、アカウントからデバイスが削除されます。さらに、デバイス上のすべてのライセンス資格と証明書が削除されます。登録を解除すること

で、ライセンスを新しい Firepower 4100/9300 シャーシ に利用することもできます。または、Smart Software Manager からデバイスを削除することもできます。

Cisco Success Network の登録の変更

Cisco Smart Software Manager に Firepower 4100/9300 を登録するときは、Cisco Success Network を有効にします。その後、次の手順を使用して、登録ステータスを表示または変更します。

（注） Cisco Success Network は評価モードでは機能しません。

手順

ステップ 1 **[System]** > **[Licensing]** > **[Cisco Success Network]** を選択します。

ステップ 2 [Cisco Success Network Preferences] の下で、シスコから提供される情報に目を通してから、[Click here] をクリックして、シスコに送信されるサンプルデータを確認します。

ステップ 3 [Enable Cisco Success Network] をどうするかを選択し、[Save] をクリックします。

Firepower 4100/9300 シャーシのスマート ライセンス サテライト サーバの設定

スマート ライセンス サテライト サーバを使用するように Firepower 4100/9300 シャーシを設定するには、次の手順に従います。

始める前に

- スマート ソフトウェア ライセンスの前提条件 （35 ページ）に記載のすべての前提条件を満たす必要があります。
- Smart Software Satellite Server を展開して設定します。

  スマート ライセンス サテライト OVA ファイルを Cisco.com からダウンロードし、VMwareESXi サーバにインストールおよび設定します。詳細については、『Smart Software Manager satellite Install Guide』を参照してください。
- 内部 DNS サーバによって Smart Software Satellite Server の FQDN が解決できることを確認します。
- サテライト トラストポイントがすでに存在しているかどうかを確認します。

scope security

show trustpoint

FXOS バージョン 2.4(1) 以降では、トラストポイントはデフォルトで追加されることに注意してください。トラストポイントが存在しない場合は、次の手順を使用して手動で追加する必要があります。

1. http://www.cisco.com/security/pki/certs/clrca.cer に移動し、SSL 証明書の本文全体（"-----BEGIN CERTIFICATE-----" から "-----END CERTIFICATE-----" まで）を、設定中にアクセスできる場所にコピーします。
2. セキュリティ モードを開始します。

   scope security
3. トラスト ポイントを作成して名前を付けます。

   create trustpoint *trustpoint_name*
4. トラスト ポイントの証明書情報を指定します。証明書は、Base64 エンコード X.509（CER）フォーマットである必要があることに注意してください。

   set certchain *certchain*

   certchain 変数には、ステップ 1 でコピーした証明書のテキストを貼り付けます。

   コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パスを定義するトラストポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、**ENDOFBUF** と入力して終了します。
5. 設定をコミットします。

   commit-buffer

手順

ステップ 1 **[System]** > **[Licensing]** > **[Call Home]** を選択します。

ステップ 2 [Call Home Configuration] 領域で、[Address] フィールド内のデフォルト URL を、Smart Software Satellite Server の URL に置き換えます。これを行うには、この手順の前提条件で収集した情報を使用します。次の形式を使用します。 **https://***[FQDN of Satellite server]***/Transportgateway/services/DeviceRequestHandler**

ステップ 3 Firepower 4100/9300 シャーシ の License Authority への登録 （37 ページ）。スマート ライセンス マネージャ サテライトの登録トークンを要求し、コピーする必要があることに注意してください。

パーマネント ライセンス予約の設定

Firepower 4100/9300 シャーシにパーマネント ライセンスを割り当てることができます。このユニバーサル予約では、デバイスで無制限の数の使用権を使用できるようになります。

（注） Smart Software Manager で使用できるように、開始前にパーマネント ライセンスを購入する必要があります。すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

パーマネント ライセンスのインストール

以下の手順は、Firepower 4100/9300 シャーシにパーマネント（永続）ライセンスを割り当てる方法を示しています。

手順

ステップ 1 **System** > **Licensing** > **Permanent License** を選択します。

ステップ 2 **Generate** をクリックして、予約要求コードを生成します。予約要求コードをクリップボードにコピーします。

ステップ 3 Cisco Smart Software Manager ポータルの Smart Software Manager インベントリ画面に移動して、**Licenses** タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

Licenses タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 **License Reservation** をクリックして、生成された予約リクエスト コードをボックスにペーストします。

ステップ 5 **Reserve License** をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

License Reservation ボタンが表示されない場合、お使いのアカウントにはパーマネント ライセンスの予約が許可されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 6 Firepower Chassis Managerで、生成された承認コードを **Authorization Code** テキスト ボックスに入力します。

ステップ 7 **Install** をクリックします。

Firepower 4100/9300 シャーシが PLR で完全にライセンス付与されたら、[Permanenet License] ページにライセンス ステータスが表示され、パーマネント ライセンスを返却するためのオプションが示されます。

ステップ 8 ASA 論理デバイスで機能のライセンス資格を有効にします。ライセンス資格を有効にするには、ASA ライセンスの章を参照してください。

（任意）パーマネント ライセンスの返却

パーマネント ライセンスが不要になった場合、この手順で Smart Software Manager に正式に返却する必要があります。すべてのステップに従わないと、ライセンスが使用状態のままになり、別の場所で使用できません。

手順

ステップ 1 **System** > **Licensing** > **Permanent License** を選択します。

ステップ 2 **Return** をクリックして、戻りコードを生成します。戻りコードをクリップボードにコピーします。

ただちに Firepower 4100/9300 シャーシ のライセンスがなくなり、評価状態に移行します。

ステップ 3 Smart Software Manager インベントリ画面に移動して、**Product Instances** タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

ステップ 4 ユニバーサル デバイス識別子（UDI）を使用して Firepower 4100/9300 シャーシを検索します。

ステップ 5 **Actions** > **Remove** の順に選択して、生成された戻りコードをボックスに貼り付けます。

ステップ 6 **Remove Product Instance** をクリックします。

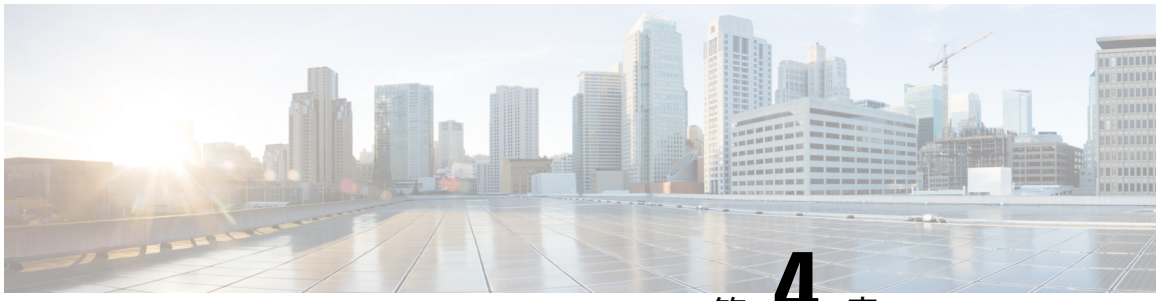
パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

ステップ 7 システムをリブートします。Firepower 4100/9300 シャーシの再起動の方法については、Firepower 4100/9300 シャーシ の再起動 （111 ページ）を参照してください。

スマート ソフトウェア ライセンスの履歴

機能名	プラットフォームリリース	説明
Cisco Success Network	2.7.1	Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、Firepower 4100/9300 シャーシと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリのストリーミングにより、対象データを ASA から選択して、構造化形式でリモート管理ステーションに送信するメカニズムが提供されるため、次のことが実現します。 • ネットワーク内の製品の有効性を向上させるために利用可能な未使用の機能が通知されます。 • 製品に付随する追加のテクニカルサポートサービスとモニタリングについて通知されます。 • シスコ製品の改善に役立ちます。 Cisco Success Network に登録すると、シャーシは常にセキュアな接続を確立して維持します。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。 次のコマンドを導入しました。 **scope telemetry {enable | disable}** 次の画面が導入されました。 **[システム（System）] > [ライセンス（Licensing）] > [Cisco Success Network]**

機能名	プラットフォームリリース	説明
Firepower 4100/9300 シャーシ向けシスコ スマート ソフトウェア ライセンシング	1.1(1)	スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを管理することができます。スマートライセンスは特定のシリアル番号に結び付けられていません。各ユニットのライセンスキーを管理する必要なく、デバイスを簡単に導入または削除できます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。スマート ソフトウェア ライセンスの設定は、Firepower 4100/9300 シャーシ スーパバイザとセキュリティモジュール間で分割されます。 次の画面が導入されました。 **[システム（System）] > [ライセンス（Licensing）] > [Call Home]** **[システム（System）] > [ライセンス（Licensing）] > [スマートライセンス（Smart License）]**



第 4 章

ユーザ管理

ユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。最大 48 のローカル ユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

管理者アカウント

管理者アカウントはデフォルト ユーザ アカウントであり、変更や削除はできません。このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。管理者アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。管理者アカウントを非アクティブに設定することはできません。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザアカウントは、シャーシを通じて直接認証され、管理者権限または AAA 権限があれば誰でも有効化または無効化できます。ローカル ユーザ アカウントを無効にすると、ユーザはログインできません。データベースは無効化されたローカル ユーザ アカウントの設定の詳細を削除しません。無効なローカルユーザアカウントを再度有効にすると、アカウントは既存の設定で再びアクティブになりますが、アカウントのパスワードは再設定する必要があります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントとは、LDAP、RADIUS、または TACACS+ を通じて認証されたユーザアカウントのことです。すべてのリモートユーザーには、デフォルトで、最初に**読み取り専用**ロールが割り当てられます。

ユーザがローカル ユーザ アカウントとリモート ユーザ アカウントを同時に保持する場合、ローカル ユーザ アカウントで定義されたロールがリモート ユーザ アカウントに保持された値を上書きします。

フォールバック認証方式では、ローカルデータベースを使用します。このフォールバック方式は設定できません。

リモート認証のガイドラインの詳細や、リモート認証プロバイダーの設定および削除方法については、次のトピックを参照してください。

- リモート認証のガイドライン （48 ページ）
- LDAP プロバイダーの設定 （150 ページ）
- RADIUS プロバイダーの設定 （154 ページ）
- TACACS+ プロバイダーの設定 （157 ページ）

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。有効期限の時間になると、ユーザ アカウントは無効になります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。

ユーザ名に関するガイドライン

ユーザ名は、Firepower Chassis Manager および FXOS CLI のログイン ID としても使用されます。ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。

- 任意の英字
- 任意の数字
- _（アンダースコア）
- -（ダッシュ）
- .（ドット）

- ログイン ID は一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字から始めることはできません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

パスワードに関するガイドライン

ローカル認証された各ユーザ アカウントにパスワードが必要です。admin または AAA 権限を持つユーザについては、ユーザ パスワードのパスワード強度チェックを実行するようにシステムを設定できます。パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。ローカル認証されたユーザのパスワード強度チェックを有効にすると、FXOS は次の要件を満たしていないパスワードを拒否します。

- 少なくとも 8 文字を含み、最大 127 文字であること

（注） コモン クライテリア要件に準拠するために、オプションでシステムの最小文字数 15 文字の長さのパスワードを設定できます。詳細については、最小パスワード長チェックの設定（59 ページ）を参照してください。

- アルファベットの大文字を少なくとも 1 文字含む。
- アルファベットの小文字を少なくとも 1 文字含む。
- 英数字以外の文字（特殊文字）を少なくとも 1 文字含む。
- スペースを含まない。

- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- passwordABC や password321 などの 3 つの連続した数字や文字をどのような順序であっても含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、辞書に記載されている標準的な単語に基づくパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。

（注） この制限は、パスワードの強度チェックが有効になっているかどうかにかかわらず適用されます。

- ローカル ユーザ アカウントおよび admin アカウントの場合は空白にしない。

リモート認証のガイドライン

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Firepower 4100/9300 シャーシがそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Firepower 4100/9300 シャーシ にローカルに存在するか、またはリモート認証サーバに存在することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションを、Firepower Chassis Manager または FXOS CLI から表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Firepower 4100/9300 シャーシで作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を FXOS で使用される名前と一致させることが必要です。ロール ポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

リモート認証プロバイダーのユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Firepower Chassis Manager または FXOS CLI へのログインに使用する各リモート認証プロバイダーに Firepower 4100/9300 シャーシ 用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

ユーザがログインすると、FXOS は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

次の表は、FXOS でサポートしているリモート認証プロバイダーのユーザ属性要件を比較したものです。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	オプション	次のいずれかを実行するように選択できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します 次の項で、サンプル OID を示します。
RADIUS	オプション	次のいずれかを実行するように選択できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用します。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成します。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

ユーザの役割

システムには、次のユーザ ロールが用意されています。

管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトのadminアカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

読み取り専用

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

操作

NTPの設定、Smart LicensingのためのSmart Call Homeの設定、システム ログ（syslogサーバとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

AAA アドミニストレータ

ユーザ、ロール、およびAAA設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

ローカル認証されたユーザのパスワード プロファイル

パスワードのプロファイルには、ローカル認証されたユーザすべてのパスワード履歴やパスワード変更間隔プロパティが含まれます。ローカル認証されたユーザのそれぞれに異なるパスワード プロファイルを指定することはできません。

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。このプロパティが設定されている場合、Firepowerシャーシは、ローカル認証されたユーザがこれまでに使用した最大15個のパスワードを保存します。パスワードは最近のものから時系列の逆順で格納され、履歴カウントがしきい値に達した場合に、最も古いパスワードだけを再利用可能にします。

あるパスワードが再利用可能になる前に、ユーザはパスワード履歴カウントで設定された数のパスワードを作成して使用する必要があります。たとえば、パスワード履歴カウントを8に設定した場合、ローカル認証されたユーザは9番目のパスワードが期限切れになった後まで、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は0に設定されます。この値は、履歴のカウントをディセーブルにし、ユーザはいつでも前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザについてパスワード履歴カウントをクリアし、以前のパスワードの再利用をイネーブルにできます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更回数を制限することができます。次の表で、パスワード変更間隔の2つの設定オプションについて説明します。

間隔の設定	説明	例
パスワード変更禁止	このオプションを設定すると、ローカル認証されたユーザは、パスワードを変更してから指定された時間内はパスワードを変更できなくなります。 1 ～ 745 時間の変更禁止間隔を指定できます。デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが48時間の間パスワードを変更できないようにする場合、次のように設定します。 • [間隔中の変更（Change During Interval）] を無効にする • [変更禁止間隔（No Change Interval）] を 48 に設定する
変更間隔内のパスワード変更許可	このオプションは、ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。デフォルトでは、ローカル認証されたユーザに対して、48時間間隔内で最大2回のパスワード変更が許可されます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に最大 1 回そのパスワードを変更できるようにするには、次のように設定します。 • [間隔中の変更（Change During Interval）] を有効にする • [変更カウント（Change Count）] を 1 に設定する • [変更間隔（Change Interval）] を 24 に設定する

ユーザ設定の設定

手順

ステップ 1 **[システム（System）]** > **[ユーザ管理（User Management）]** を選択します。

ステップ 2 [設定（Settings）] タブをクリックします。

ステップ 3 次のフィールドに必要な情報を入力します。

（注） デフォルトの認証とコンソール認証の両方が同じリモート認証プロトコル（RADIUS、TACACS+、または LDAP）を使用するように設定されている場合、そのサーバの設定の特定の側面を変更することは（たとえば、サーバの削除や、割り当ての順序の変更）、これらのユーザ設定を更新することなしではできません。

名前	説明
[Default Authentication] フィールド	リモート ログイン中にユーザが認証されるデフォルトの方法。次のいずれかになります。 • [ローカル（Local）]：ユーザーアカウントはシャーシでローカルに定義する必要があります。 • [Radius]：ユーザーアカウントは、シャーシに指定された RADIUS サーバーで定義する必要があります。 • [TACACS]：ユーザーアカウントは、シャーシに指定された TACACS+ サーバーで定義する必要があります。 • [LDAP]：ユーザーアカウントは、シャーシに指定された LDAP/MS-AD サーバーで定義する必要があります。 • [なし（None）]：ユーザーアカウントがシャーシに対してローカルである場合、ユーザーがリモートでログインするときにパスワードは必要ありません。 （注） [Radius]、[TACACS]、および [LDAP] のすべての設定は、[Platform Settings] で設定する必要があります。詳細については、「プラットフォームの設定」の章の「AAA について （147 ページ）」を参照してください。

名前	説明
[Console Authentication] フィールド	コンソール ポート経由で FXOS CLI に接続するときにユーザが認証される方法。次のいずれかになります。 • [ローカル（Local）]：ユーザーアカウントはシャーシでローカルに定義する必要があります。 • [Radius]：ユーザーアカウントは、シャーシに指定された RADIUS サーバーで定義する必要があります。 • [TACACS]：ユーザーアカウントは、シャーシに指定された TACACS+ サーバーで定義する必要があります。 • [LDAP]：ユーザーアカウントは、シャーシに指定された LDAP/MS-AD サーバーで定義する必要があります。 • [なし（None）]：ユーザーアカウントがシャーシに対してローカルである場合、ユーザーがコンソールポートを使用して FXOS CLI に接続するときにはパスワードは不要です。
リモート ユーザの設定	
リモート ユーザのロール ポリシー	ユーザがログインを試みたときに、リモート認証プロバイダーが認証情報を含むユーザ ロールを提供しない場合の動作を制御します。 • [デフォルト ロールの割り当て（Assign Default Role）]：ユーザは、読み取り専用ユーザ ロールでログインできます。 • [ログイン禁止（No-Login）]：ユーザ名とパスワードが正しい場合でも、ユーザはシステムにログインできません。
ローカル ユーザ設定	
[パスワード強度チェック（Password Strength Check）] チェックボックス	オンにすると、すべてのローカルユーザパスワードは、強力なパスワードのガイドラインに準拠しなければならなくなります（パスワードに関するガイドライン （47 ページ）を参照）。デフォルトでは、強力なパスワードチェックが有効になっています。

名前	説明
[History Count] フィールド	以前に使用したパスワードが再使用可能になるまでにユーザが作成する必要がある、一意のパスワードの数。履歴カウントは、最も新しいパスワードを先頭に時系列とは逆の順番で表示され、履歴カウントのしきい値に到達すると、最も古いパスワードのみが使用可能になります。 この値は、0 ～ 15 から自由に設定できます。 [History Count] フィールドを 0 に設定して履歴カウントをディセーブルにすると、ユーザは以前のパスワードをいつでも再使用できます。
[Change During Interval] フィールド	ローカル認証されたユーザがパスワードを変更できるタイミングを制御します。ここに表示される値は次のとおりです。 • [Enable]：ローカル認証されたユーザは、[Change Interval] および [Change Count] の設定に基づいてパスワードを変更できます。 • [Disable]：ローカル認証されたユーザは、[No Change Interval] に指定された期間はパスワードを変更できません。
[Change Interval] フィールド	[Change Count] フィールドで指定したパスワード変更回数が適用される時間数。 この値は、1 ～ 745 時間から自由に設定できます。 たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。
[Change Count] フィールド	ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数。 この値は、0 ～ 10 から自由に設定できます。
[No Change Interval] フィールド	ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数。 この値は、1 ～ 745 時間の範囲で自由に設定できます。 この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合は無視されます。
[Passphrase Expiration Days] フィールド	有効期限を 1 ~ 9999 日の間で設定します。デフォルトでは、有効期限は無効になっています。

名前	説明
[Passphrase Expiration Warning Period] フィールド	ログイン時にパスワードの有効期限をユーザに警告するのは、有効期限の何日前かを 0 ~ 9999 の間で設定します。デフォルトは、14 日です。
[Expiration Grace Period] フィールド	有効期限の何日後までにユーザがパスワードを変更する必要があるかを 0 ~ 9999 の間で設定します。デフォルトは 3 日です。
[Password Reuse Interval] フィールド	パスワードの再利用が可能になるまでの日数を 1 ~ 365 の間で設定します。デフォルトは 15 日です。[History Count] と [Password Reuse Interval] の両方を有効にする場合は、両方の要件を満たしている必要があります。たとえば、履歴カウントを 3 に設定し、再利用間隔を 10 日に設定すると、パスワードを変更できるのは 10 日間経過した後で、パスワードを 3 回変更した場合に限られます。

ステップ 4 [保存（Save）] をクリックします。

セッション タイムアウトの設定

FXOS CLI を使用することにより、ユーザ アクティビティなしで経過可能な時間を指定できます。この時間が経過した後、Firepower 4100/9300 シャーシはユーザセッションを閉じます。コンソール セッションと、HTTPS、SSH、および Telnet セッションとで、異なる設定を行うことができます。

タイムアウトとして 3600 秒（60 分）以下の値を設定できます。デフォルト値は 600 秒です。この設定を無効にするには、セッション タイムアウト値を 0 に設定します。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 デフォルト認証セキュリティ モードを開始します。

Firepower-chassis /security # **scope default-auth**

ステップ 3 HTTPS、SSH、および Telnet セッションのアイドル タイムアウトを設定します。

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

ステップ 4 （任意）コンソール セッションのアイドル タイムアウトを設定します。

Firepower-chassis /security/default-auth # **set con-session-timeout** *seconds*

ステップ 5 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/default-auth # **commit-buffer**

ステップ 6 （任意）セッションおよび絶対セッション タイムアウトの設定を表示します。

Firepower-chassis /security/default-auth # **show detail**

例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

絶対セッション タイムアウトの設定

Firepower 4100/9300 シャーシには絶対セッション タイムアウト設定があり、セッションの使用状況に関係なく、絶対セッション タイムアウト期間が経過するとユーザ セッションは閉じられます。この絶対タイムアウト機能は、シリアル コンソール、SSH、HTTPS を含むすべての形式のアクセスに対してグローバルに適用されます。

絶対タイムアウト値のデフォルトは 3600 秒（60 分）であり、FXOS CLI を使用して変更できます。この設定を無効にするには、絶対セッション タイムアウト値を 0 に設定します。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 デフォルト認証セキュリティ モードを開始します。

Firepower-chassis /security # **scope default-auth**

ステップ 3 絶対セッション タイムアウトを設定します。

Firepower-chassis /security/default-auth # **set absolute-session-timeout** *seconds*

ステップ 4 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/default-auth # **commit-buffer**

ステップ 5 （任意）セッションおよび絶対セッション タイムアウトの設定を表示します。

Firepower-chassis /security/default-auth # **show detail**

例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

ログイン試行の最大回数の設定

ロックアウト前にユーザに許可されるログイン試行の最大回数を指定します。この回数を超えると、指定した時間だけ Firepower 4100/9300 シャーシからロックアウトされることになります。ユーザは、設定した最大回数を超えてログインを試行すると、システムからロックされます。ユーザがロックアウトされたことを示す通知は表示されません。これが起きると、ユーザは次にログインを試行できるようになるまで、指定された時間だけ待機する必要があります。

ログイン試行の最大数を設定するには、次の手順を実行します。

（注）
- どのタイプのユーザ アカウントであっても（管理者を含む）、ログイン試行の最大数を超えてログインを試行すると、システムからロックアウトされます。
- 失敗できるログイン試行のデフォルトの最大回数は0です。ユーザがログイン試行の最大数を超えたときにシステムからロックアウトされるデフォルトの時間は、30 分（1800 秒）です。

このオプションは、システムのコモンクライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定準拠 （75 ページ）を参照してください。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 失敗できるログイン試行の最高回数を設定します。

set max-login-attempts *num_attempts*

num_attempts の値は、0 ～ 10 の範囲内の任意の整数です。

ステップ 3 ログイン試行の最高回数に達した後、ユーザがシステムからロック アウトされる時間（秒単位）を指定します。

set user-account-unlock-time

unlock_time

ステップ 4 設定をコミットします。

commit-buffer

最小パスワード長チェックの設定

最小パスワード長チェックを有効にした場合は、指定した最小文字を使用するパスワードを作成する必要があります。たとえば、*min_length* オプションを 15 に設定した場合、パスワードは 15 文字以上を使用して作成する必要があります。このオプションは、システムのコモン クライテリア認定への準拠のための数の 1 つです。詳細については、「セキュリティ認定準拠」を参照してください。

最小パスワード長チェックを設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 パスワードの最小の長さを指定します。

set min-password-length *min_length*

ステップ 3 設定をコミットします。

commit-buffer

ローカル ユーザ アカウントの作成

手順

ステップ 1 [System] > [User Management] > を選択します。

ステップ 2 [Local Users] タブをクリックします。

ステップ 3 [ユーザの追加（Add User）] をクリックして [ユーザの追加（Add User）] ダイアログボックスを開きます。

ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

名前	説明
[User Name] フィールド	このアカウントにログインするときに使用されるアカウント名。この名前は、固有であり、ユーザ アカウント名のガイドラインと制限を満たしている必要があります（ユーザ名に関するガイドライン （46 ページ）を参照）。 ユーザを保存した後は、ログイン ID を変更できません。ユーザアカウントを削除し、新しいユーザアカウントを作成する必要があります。
[First Name] フィールド	ユーザの名。このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。このフィールドには、32 文字までの値を入力できます。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone Number] フィールド	ユーザの電話番号。
[Password] フィールド	このアカウントに関連付けられているパスワード。パスワード強度チェックを有効にした場合は、ユーザ パスワードを強固なものにする必要があります。FXOS は強度チェック要件を満たしていないパスワードを拒否します（パスワードに関するガイドライン （47 ページ）を参照）。 （注） パスワードには次の記号を含めることはできません。$（ドル記号）、?（疑問符）、=（等号）。この制限は、パスワードの強度チェックが有効になっているかどうかにかかわらず適用されます。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Status] フィールド	ステータスが [アクティブ（Active）] に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Firepower Chassis Manager と FXOS CLI にログインできます。

名前	説明
[User Role] リスト	ユーザ アカウントに割り当てる権限を表すロール（ユーザの役割 （50 ページ）を参照）。 すべてのユーザはデフォルトでは読み取り専用ロールが割り当てられます。このロールは選択解除できません。複数のロールを割り当てるには、**Ctrl** を押したまま、目的のロールをクリックします。 （注） ユーザロールを削除すると、そのユーザの現在のセッション ID が取り消されます。つまり、すべてのユーザ'のアクティブセッション（CLI と Web の両方）がただちに終了します。
[Account Expires] チェックボックス	オンにすると、このアカウントは期限切れになり、[Expiration Date] フィールドに指定した日付以降に使用できなくなります。 （注） ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。
[Expiry Date] フィールド	アカウントが期限切れになる日付。日付の形式は yyyy-mm-dd です。 このフィールドの終端にあるカレンダー アイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 5 [Add] をクリックします。

ローカル ユーザ アカウントの削除

手順

ステップ 1 [System] > [User Management] > を選択します。
ステップ 2 [Local Users] タブをクリックします。
ステップ 3 削除するユーザ アカウントの行で、[削除（Delete）] をクリックします。
ステップ 4 [確認（Confirm）] ダイアログボックスで、[はい（Yes）] をクリックします。

ローカルユーザアカウントのアクティブ化または非アクティブ化

ローカルユーザアカウントをアクティブ化または非アクティブ化できるのは、admin権限またはAAA権限を持つユーザのみです。

手順

ステップ1 [System] > [User Management] > を選択します。

ステップ2 [Local Users] タブをクリックします。

ステップ3 アクティブ化または非アクティブ化するユーザ アカウントの行で、[編集（Edit）]（鉛筆アイコン）をクリックします。

ステップ4 [ユーザの編集（Edit User）] ダイアログボックスで、次のいずれかの手順を実行します。

- ユーザ アカウントをアクティブ化するには、[Account Status] フィールドの [Active] オプションボタンをクリックします。ユーザアカウントを再アクティブ化する際、アカウントのパスワードをリセットする必要があるので注意してください。
- ユーザ アカウントを非アクティブ化するには、[Account Status] フィールドの [Inactive] オプション ボタンをクリックします。

admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。

ステップ5 [保存（Save）] をクリックします。

ステップ6 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/local-user # **commit-buffer**

ローカル認証されたユーザのパスワード履歴のクリア

手順

ステップ1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ2 指定したユーザ アカウントに対してローカル ユーザ セキュリティ モードを開始します。

Firepower-chassis /security # **scope local-user** *user-name*

ステップ3 指定したユーザ アカウントのパスワード履歴をクリアします。

Firepower-chassis /security/local-user # **clear password-history**

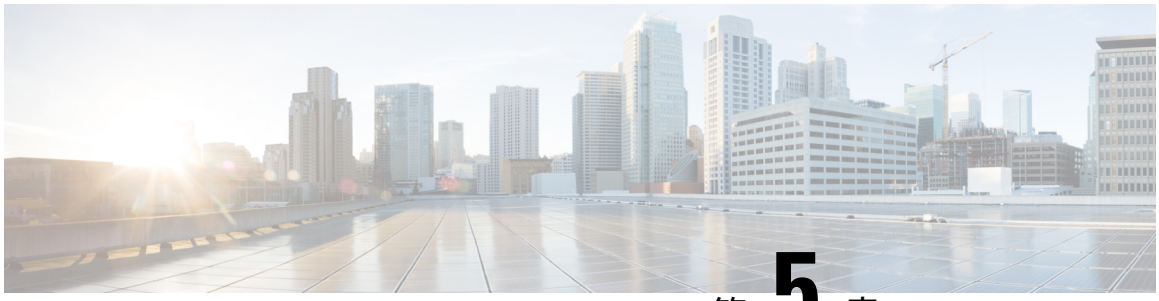
ステップ 4 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/local-user # **commit-buffer**

例

次に、パスワード履歴を消去し、トランザクションを確定する例を示します。

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```



第 5 章

イメージ管理

イメージ管理について

Firepower 4100/9300 シャーシ では 2 つの基本タイプのイメージを使用します。

（注） すべてのイメージにデジタル署名が行われ、セキュア ブートによって検証されます。どのような場合も、イメージを変更しないでください。変更すると、検証エラーになります。

- プラットフォームバンドル：プラットフォームバンドルは、Supervisor および セキュリティ モジュール/エンジン で動作する、複数の独立したイメージの集まりです。プラットフォーム バンドルは、FXOS のソフトウェア パッケージです。
- アプリケーション：アプリケーションイメージは、Firepower 4100/9300 シャーシのセキュリティ モジュール/エンジンに導入するソフトウェア イメージです。アプリケーション イメージは、Cisco Secure Package ファイル（CSP）として提供されます。これは、論理デバイス作成時にセキュリティ モジュール/エンジンに展開されるまで（または以降の論理デバイス作成に備えて）スーパーバイザに保存されます。同じアプリケーション イメージ タイプの複数の異なるバージョンをスーパバイザに保存できます。

（注） プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

（注） デバイスに ASA アプリケーションをインストールする場合は、既存のアプリケーション FTD のイメージを削除できます。その逆も同様です。すべての FTD イメージを削除しようとすると、少なくとも 1 つのイメージの削除が拒否され、「`Invalid operation as no default FTD/ASA APP will be left. Please select a new default FTD app`」というエラーメッセージが表示されます。すべての FTD イメージを削除するには、デフォルトイメージだけを残して、その他のイメージを削除し、最後にデフォルトイメージを削除する必要があります。

Cisco.com からのイメージのダウンロード

FXOS およびアプリケーションイメージをシャーシにアップロードできるように Cisco.com からダウンロードします。

始める前に

Cisco.com アカウントが必要です。

手順

ステップ 1 Web ブラウザを使用して、http://www.cisco.com/go/firepower9300-software または http://www.cisco.com/go/firepower4100-software にアクセスします。
Firepower 4100/9300 シャーシのソフトウェア ダウンロード ページがブラウザに表示されます。

ステップ 2 該当するソフトウェア イメージを見つけて、ローカル コンピュータにダウンロードします。

セキュリティアプライアンスへのイメージのアップロード

FXOS およびアプリケーションイメージをシャーシにアップロードできます。

始める前に

アップロードするイメージがローカル コンピュータで使用可能であることを確認してください。

手順

ステップ 1 **[システム（System）] > [更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能なFXOSプラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 2 [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。

ステップ 3 [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。

ステップ 4 [Upload] をクリックします。
選択したイメージがFirepower 4100/9300 シャーシにアップロードされます。イメージのアップロード中、完了したアップロードの割合を示す進行状況バーが表示されます。

ステップ 5 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

イメージの整合性の確認

イメージの整合性は、新しいイメージがFirepower 4100/9300 シャーシに追加されると自動的に確認されます。必要な場合に、手動でイメージの整合性を確認するには、次の手順を実行できます。

手順

ステップ 1 **[システム（System）] > [更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能なFXOSプラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 2 確認するイメージの [確認（Verify）]（チェックマーク アイコン）をクリックします。

システムはイメージの整合性を確認し、[イメージの整合性（Image Integrity）] フィールドにステータスを表示します。

FXOS プラットフォーム バンドルのアップグレード

始める前に

プラットフォーム バンドルのソフトウェア 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（66 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにアップロードします（セキュリティアプライアンスへのイメージのアップロード（66 ページ）を参照）。

（注） アップグレード プロセスには通常 20 ～ 30 分かかります。

スタンドアロン論理デバイスを実行中の Firepower 9300 または 4100 シリーズ セキュリティ アプライアンスをアップグレードしている場合、または シャーシ内クラスタを実行中の Firepower 9300 セキュリティアプライアンスをアップグレードしている場合、アップグレード中にはトラフィックがデバイスを通過しません。

シャーシ間クラスタに属する Firepower 9300 または 4100 シリーズ セキュリティ アプライアンスをアップグレードしている場合、アップグレード中には、アップグレード対象のデバイスをトラフィックが通過しません。ただし、クラスタ内の他のデバイスではトラフィックは通過し続けます。

手順

ステップ 1 **[システム（System）]** > **[更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 2 アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 3 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

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

FTP、HTTP/HTTPS、SCP、SFTP、または TFTP を使用して、論理デバイスのソフトウェアイメージを Firepower 4100/9300 シャーシ にコピーできます。

始める前に

コンフィギュレーション ファイルのインポートに必要な次の情報を収集します。

- イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル
- ソフトウェア イメージ ファイルの完全修飾名

（注） FXOS 2.8.1 以降のバージョンでは、ファームウェアおよびアプリケーションイメージのダウンロード用に HTTP/HTTPS プロトコルがサポートされています。

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-chassis # **scope ssa**

ステップ 2 アプリケーション ソフトウェア モードに入ります。

Firepower-chassis /ssa # **scope app-software**

ステップ 3 論理デバイスのソフトウェア イメージをダウンロードします。

Firepower-chassis /ssa/app-software # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*
- **http**://*username@hostname*/*path*
- **https**://*username@hostname*/*path*
- **scp**://*username@hostname*/*path*
- **sftp**://*username@hostname*/*path*
- **tftp**://*hostname*:*port-num*/*path*

ステップ 4 ダウンロード プロセスをモニタする場合：

Firepower-chassis /ssa/app-software # **show download-task**

ステップ 5 ダウンロード アプリケーションを表示するには、次のコマンドを使用します。

Firepower-chassis /ssa/app-software # **up**

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

ステップ 6 特定のアプリケーションの詳細情報を表示するには、次のコマンドを使用します。

Firepower-chassis /ssa # **scope app** *application_type image_version*

Firepower-chassis /ssa/app # **show expand**

例

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server              Userid          State

   ------------------------------ ---------- ------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
    Name: asa
    Version: 9.4.1.65
    Description: N/A
    Author:
    Deploy Type: Native
    CSP Type: Application
    Is Default App: Yes

    App Attribute Key for the Application:
        App Attribute Key Description
        ----------------- -----------
        cluster-role      This is the role of the blade in the cluster
        mgmt-ip           This is the IP for the management interface
        mgmt-url          This is the management URL for this application
```

```
    Net Mgmt Bootstrap Key for the Application:
        Bootstrap Key Key Data Type Is the Key Secret Description
        ------------ ------------- ----------------- -----------
        PASSWORD      String        Yes               The admin user password.

    Port Requirement for the Application:
        Port Type: Data
        Max Ports: 120
        Min Ports: 1

        Port Type: Mgmt
        Max Ports: 1
        Min Ports: 1

        Mgmt Port Sub Type for the Application:
            Management Sub Type
            -------------------
            Default

        Port Type: Cluster
        Max Ports: 1
        Min Ports: 0
Firepower-chassis /ssa/app #
```

論理デバイスのイメージ バージョンの更新

この手順を使用して、新しいバージョンに ASA アプリケーションイメージをアップグレードするか、FTD アプリケーションイメージをディザスタ リカバリ シナリオで使用される新しいスタートアップバージョンに設定します。

Firepower Chassis Manager または FXOS CLI を使用して FTD 論理デバイスでスタートアップバージョンを変更しても、アプリケーションはすぐに新しいバージョンにアップグレードされません。論理デバイス スタートアップ バージョンは、FTD がディザスタ リカバリ シナリオで再インストールされるバージョンです。FTD 論理デバイスの初期作成後には、FTD 論理デバイスを、Firepower Chassis Manager または FXOS CLI を使用してアップグレードすることはありません。FTD 論理デバイスをアップグレードするには、FMC を使用する必要があります。詳細については、次のサイトにあるシステムリリースノートを参照してください。
http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html

さらに、FTD 論理デバイスへの更新は、Firepower Chassis Manager の **[論理デバイス（Logical Devices）]** > **[編集（Edit）]** ページおよび **[システム（System）]** > **[更新（Updates）]** ページには反映されないことに注意してください。これらのページで、表示されるバージョンは、FTD 論理デバイスを作成するために使用されたソフトウェア バージョン（CSP イメージ）を示します。

（注） FTDのスタートアップバージョンを設定すると、アプリケーションのスタートアップバージョンが更新されます。したがって、アプリケーションを手動で再インストールするか、ブレードを再初期化して、選択したバージョンを適用する必要があります。この手順は、FTD ソフトウェアのアップグレードまたはダウングレードとは異なり、完全な再インストール（再イメージ化）です。そのため、アプリケーションが削除され、既存の設定が失われます。

ASA 論理デバイスでスタートアップ バージョンを変更すると、ASA はこのバージョンにアップグレードされ、すべての設定が復元されます。設定に応じて ASA スタートアップ バージョンを変更するには、次のワークフローを使用します。

（注） ASA のスタートアップバージョンを設定すると、アプリケーションが自動的に再起動されます。この手順は、ASA ソフトウェアのアップグレードまたはダウングレードと同様です（既存の設定は保持されます）。

ASA ハイ アベイラビリティ：

1. スタンバイ ユニットで論理デバイス イメージ バージョンを変更します。
2. スタンバイ ユニットをアクティブにします。
3. 他のユニットでアプリケーション バージョンを変更します。

ASA シャーシ間クラスタ：

1. データユニットでスタートアップバージョンを変更します。
2. データユニットを制御ユニットにします。
3. 元の制御ユニット（ここではデータユニット）でスタートアップバージョンを変更します。

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 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（66 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにアップロードします（セキュリティアプライアンスへのイメージのアップロード（66 ページ）を参照）。

プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。

ステップ 2 更新する論理デバイスの [Update Version] をクリックして、[Update Image Version] ダイアログボックスを開きます。

ステップ 3 [New Version] では、ソフトウェア バージョンを選択します。

ステップ 4 [OK] をクリックします。

ファームウェア アップグレード

Firepower 4100/9300 シャーシでファームウェアをアップグレードする方法については、『*Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド*』を参照してください。

バージョン 2.0.1 以下への手動ダウングレード

セキュリティモジュールに CIMC イメージを手動でダウングレードするには、次の CLI 手順に従います。

（注） この手順は、バージョン 2.1.1 以降からバージョン 2.0.1 以前にダウングレードする際に使用します。

始める前に

ダウングレード対象のアプリケーションイメージが Firepower 4100/9300 シャーシにダウンロードされていることを確認します（「Cisco.com からのイメージのダウンロード （66 ページ）」および「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 （69 ページ）」を参照）。

手順

ステップ 1 CIMC イメージをダウングレードする前に、イメージバージョンの比較を無効にします。

デフォルトのプラットフォーム イメージ バージョンを消去するには、次の例の手順に従います。

例：

```
firepower# scope org
firepower /org # scope fw-platform-pack default
firepower /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility
issue.
firepower /org/fw-platform-pack* # commit-buffer
firepower /org/fw-platform-pack #
```

ステップ 2 モジュールイメージをダウングレードします。

CIMC イメージを変更するには、次の例の手順に従います。

例：

```
firepower# scope server 1/1
firepower /chassis/server # scope cimc
firepower /chassis/server/cimc # update firmware <version_num>
firepower /chassis/server/cimc* # activate firmware <version_num>
firepower /chassis/server/cimc* # commit-buffer
firepower /chassis/server/cimc #
```

他のモジュールを更新するには、必要に応じてこの手順を繰り返します。

ステップ 3 新しいファームウェアバンドルをインストールします。

ダウングレードイメージをインストールするには、次の例の手順に従います。

例：

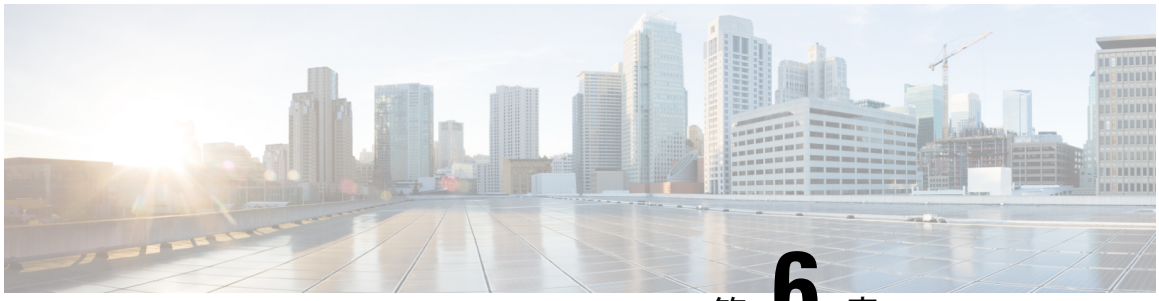
```
firepower# scope firmware
firepower /firmware # scope auto-install
firepower /firmware/auto-install # install platform platform-vers <version_num>
The currently installed FXOS platform software package is <version_num>

WARNING: If you proceed with the upgrade, the system will reboot.

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
Do you want to proceed? (yes/no):
```

次のタスク

`firmware/auto-install` モードで **show fsm status expand** コマンドを使用すると、インストールプロセスをモニタできます。



第 6 章

セキュリティ認定準拠

セキュリティ認定準拠

米国連邦政府機関は、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower 4100/9300 シャーシ は、これらのセキュリティ認証基準のいくつかに準拠しています。

これらの基準に準拠する機能を有効にするステップについては、次のトピックを参照してください。

- FIPS モードの有効化
- コモン クライテリア モードの有効化
- IPSec セキュア チャネルの設定 （77 ページ）
- トラストポイントのスタティック CRL の設定 （83 ページ）
- 証明書失効リストのチェックについて （84 ページ）
- CRL 定期ダウンロードの設定 （89 ページ）
- NTP を使用した日付と時刻の設定 （117 ページ）
- LDAP キー リング証明書の設定 （91 ページ）
- IP アクセスリストの設定 （165 ページ）
- 最小パスワード長チェックの設定

- ログイン試行の最大回数の設定 （58 ページ）

（注） これらのトピックは Firepower 4100/9300 シャーシ における認定準拠の有効化についてのみ説明していることに注意してください。Firepower 4100/9300 シャーシ で認定準拠を有効にしても、接続された論理デバイスにまでそのコンプライアンスは自動的には伝搬されません。

SSH ホスト キーの生成

FXOS リリース 2.0.1 より以前は、デバイスの初期設定時に作成した既存の SSH ホスト キーが 1024 ビットにハードコードされていました。FIPS およびコモン クライテリア認定に準拠するには、この古いホスト キーを破棄して新しいホスト キーを生成する必要があります。詳細については、「FIPS モードの有効化」または「コモン クライテリア モードの有効化」を参照してください。

古い SSH ホスト キーを破壊し、新しい証明書準拠キーを生成するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、サービス モードに入ります。

scope system

scope services

ステップ 2 SSH ホスト キーを削除します。

delete ssh-server host-key

ステップ 3 設定を確定します。

commit-buffer

ステップ 4 SSH ホスト キーのサイズを 2048 ビットに設定します。

set ssh-server host-key rsa 2048

ステップ 5 設定をコミットします。

commit-buffer

ステップ 6 新しい SSH ホスト キーを作成します。

create ssh-server host-key

commit-buffer

ステップ 7 新しいホスト キーのサイズを確認します。

show ssh-server host-key

ホスト キー サイズ：2048

IPSec セキュア チャネルの設定

IPSec は Internet Engineering Task Force（IETF）で開発されたオープン規格のフレームワークです。IP ネットワークを介した、認証された信頼性の高いセキュアな通信を実現します。IPSec セキュリティサービスは、次の機能を提供します。

- コネクションレス型の完全性：受信トラフィックが変更されていないことを保証します。
- データ発信元の認証：トラフィックが正当な当事者によって送信されることを保証します。
- 機密性（暗号化）：ユーザーのトラフィックが許可されていない当事者によって調査されないことを保証します。
- アクセス制御：リソースの不正使用を防止します。

（注） IPSec 接続は FXOS からのみ開始できます。FXOS は着信 IPSec 接続要求を受け入れません。

IPsec トンネルとは、FXOS がピア間に確立する SA のセットのことです。SA とは、機密データに適用するプロトコルとアルゴリズムを指定するものであり、ピアが使用するキー関連情報も指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

Chassis Manager の IPSec には次の 2 つのモードがあります。

トランスポート モード
IP ヘッダー、IPSec ヘッダー、TCP ヘッダー、データ

トンネル モード
新しい IP ヘッダー、IPSec ヘッダー、元の IP ヘッダー、TCP ヘッダー、データ

IPSec の動作は、次の 5 つの主要なステップに分けられます。

1. トラフィックの選択：IPSec ポリシーに一致する対象トラフィックが IKE プロセスを開始します。たとえば、送信元/宛先ホスト IP またはサブネットを使用してトラフィックを選択できます。また、admin コマンドを使用して IKE プロセスをトリガーすることもできます。
2. IKE フェーズ 1：IPSec ピアを認証し、セキュアなチャネルをセットアップして IKE 交換を有効にします。

3. IKE フェーズ 2：SA をネゴシエートして IPSec トンネルをセットアップします。SA は、セキュリティアソシエーション（Security Association）の略であり、データトラフィックを保護するために使用されるセキュリティサービスを記述する IPSec エンドポイント間の関係です。
4. データの転送：データパケットは、SA に保存されているパラメータとキーを使用して、暗号化され、IPSec ヘッダーにカプセル化されます。
5. IPSec トンネルの終了：IPSec SA は、削除またはタイムアウトによって終了します。

Firepower 4100/9300 シャーシ上で IPSec を設定して、エンドツーエンドのデータ暗号化や、パブリック ネットワーク内を移動するデータ パケットに対する認証サービスを提供できます。このオプションは、システムのコモンクライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定準拠 （75 ページ）を参照してください。

（注）
- FIPS モードで IPSec セキュア チャネルを使用している場合は、IPSec ピアで RFC 7427 をサポートしている必要があります。
- IKE 接続と SA 接続の間で一致する暗号キー強度の適用を設定する場合は、次のようにします（次の手順で sa-strength-enforcement を yes に設定します）。

SA の適用を有効にする場合	IKE によりネゴシエートされたキー サイズが、ESP によりネゴシエートされたキー サイズより小さい場合、接続は失敗します。 IKE によりネゴシエートされたキー サイズが、ESP によりネゴシエートされたキー サイズより大きいか等しい場合、SA 適用検査にパスして、接続は成功します。
SA の適用を無効にした場合	SA 適用検査にパスし、接続は成功します。

IPSec セキュア チャネルを設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 キー リングを作成します。

enter keyring ssp

! create certreq subject-name *subject-name* **ip** *ip*

ステップ 3 関連する証明書要求情報を入力します。

enter certreq

ステップ 4 国を設定します。

set country *country*

ステップ 5 DNS を設定します。

set dns *dns*

ステップ 6 電子メールを設定します。

set e-mail 電子メール

ステップ 7 IP 情報を設定します。

set ip *ip-address*

set ipv6 *ipv6*

ステップ 8 ローカリティを設定します。

set locality *locality*

ステップ 9 組織名を設定します。

set org-name *org-name*

ステップ 10 組織ユニット名を設定します。

set org-unit-name *org-unit-name*

ステップ 11 パスワードを設定します。

! set password

ステップ 12 状態を設定します。

set state *state*

ステップ 13 certreq のサブジェクト名を設定します。

set subject-name *subject-name*

ステップ 14 終了します。

exit

ステップ 15 モジュラスを設定します。

set modulus *modulus*

ステップ 16 証明書要求の再生成を設定します。

set regenerate *{ yes | no }*

ステップ 17 トラストポイントを設定します。

set trustpoint interca

ステップ 18 終了します。

exit

ステップ 19 新しく作成されたトラストポイントを入力します。

enter trustpoint interca

ステップ 20 証明書署名要求を作成します。

set certchain

例：

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMAsG
A1UECwwEU1RCVTELMAkGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWC3NzcEBzc3Au
bmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690Vl8/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FlRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QIiGYSctlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMOdWbdeMG3EihxEEOUPD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVl/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZlO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhzYxVZ10DHKIzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpBQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJCggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/fluJ+s/VJSVZWK4tAWvR7wl
QngCKRJW6FYpzeyNBctiJ07wO+Wt4e3KhIjJDYvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBjN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
```

```
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
```

ステップ **21** 証明書署名要求を表示します。

show certreq

例：

```
Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
□□□
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQwwCgYDVQQH
DANTSkMxDjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3t0laoxPbfE
p/lTKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClK/tsIxsPkV0
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPlX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAlBgkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
```

```
rjANBgkqhkiG9w0BAQsFAAOCAQEARtRBoInxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZl03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMl9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----
```

ステップ 22 IPSec モードに入ります。

scope ipsec

ステップ 23 ログ冗長レベルを設定します。

set log-level *log_level*

ステップ 24 IPSec 接続を作成し、入力します。

enter connection *connection_name*

ステップ 25 IPSec モードをトンネリングまたは伝送のために設定します。

set mode *tunnel_or_transport*

ステップ 26 ローカル IP アドレスを設定します。

set local-addr *ip_address*

ステップ 27 リモート IP アドレスを設定します。

set remote-addr *ip_address*

ステップ 28 トンネル モードを使用している場合、リモート サブネットを設定します。

set remote-subnet *ip/mask*

ステップ 29 （任意）リモート ID を設定します。

set remote-ike-ident *remote_identity_name*

ステップ 30 キーリング名を設定します。

set keyring-name *name*

ステップ 31 （任意）キーリング パスワードを設定します。

set keyring-passwd *passphrase*

ステップ 32 （任意）IKE-SA の有効期間を分単位で設定します。

set ike-rekey-time *minutes*

minutes 値には、60 ～ 1440 の範囲内の任意の整数を設定できます。

ステップ 33 （任意）子の SA の有効期間を分単位（30 ～ 480 分）で設定します。

set esp-rekey-time *minutes*

minutes 値には、30 ～ 480 の範囲内の任意の整数を設定できます。

ステップ 34 （任意）初期接続中に実行する再送信シーケンスの番号を設定します。

set keyringtries *retry_number*

retry_number 値には、1 ～ 5 の範囲の任意の整数を指定できます。

ステップ 35 （任意）証明書失効リスト検査を、有効または無効にします。

set revoke-policy *{ relaxed | strict }*

ステップ 36 接続を有効にします。

set admin-state enable

ステップ 37 接続をリロードします。

reload-conns

システムはすべての接続を停止し、リロードします。すべての接続の再確立が試行されます。

ステップ 38 （任意）既存のトラストポイント名を IPsec に追加します。

create authority *trustpoint_name*

ステップ 39 IKE 接続と SA 接続との間の、対応する暗号キー強度の適用を設定します。

set sa-strength-enforcement *yes_or_no*

トラストポイントのスタティック CRL の設定

失効した証明書は、証明書失効リスト（CRL）で保持されます。クライアントアプリケーションは、CRL を使用してサーバの認証を確認します。サーバ アプリケーションは CRL を使用して、信頼されなくなったクライアントアプリケーションからのアクセス要求を許可または拒否します。

証明書失効リスト（CRL）情報を使用して、Firepower 4100/9300 シャーシがピア証明書を検証するように設定できます。このオプションは、システムのコモン クライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定準拠 （75 ページ）を参照してください。

CRL 情報を使用してピア証明書を検証するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 トラストポイント モードに入ります。

scope trustpoint *trustname*

ステップ 3 取り消しモードに入ります。

scope revoke

ステップ 4 CRL ファイルをダウンロードします。

import crl *protocol*://*user_id@CA_or_CRL_issuer_IP*/tmp/*DoDCA1CRL1.crl*

（注） DER 形式の静的 CRL は FXOS ではサポートされていません。次のコマンドを使用して、DER 形式の CRL ファイルを PEM 形式に変換する必要があります。

```
openssl crl -in filename.crl -inform DER -outform PEM -out crl.pem
```

ステップ 5 （任意）CRL 情報のインポート プロセスのステータスを表示します。

show import-task detail

ステップ 6 CRL 専用の、証明書取り消し方法を設定します。

set certrevokemethod {crl}

証明書失効リストのチェックについて

証明書失効リスト（CRL）チェック モードを、IPSec およびセキュアな LDAP 接続で厳格または緩和に設定できます。

FXOS は、動的な CRL 情報を示すダイナミック（非スタティック）CRL 情報を、X.509 証明書の CDP 情報から収集します。システム管理によってスタティック CRL 情報を手動でダウンロードします。この情報は、FXOS システムのローカルな CRL 情報を示します。FXOS では、ダイナミック CRL 情報は証明書チェーン内で現在処理中の証明書に対してのみ処理されます。スタティック CRL は、ピアの証明書チェーン全体に適用されます。

セキュアな LDAP および IPSec 接続の証明書失効のチェックを有効または無効にするステップについては、IPSec セキュア チャネルの設定 （77 ページ）およびLDAP プロバイダーの作成（151 ページ）を参照してください。

（注）
- 証明書失効のチェック モードが厳格に設定されている場合、スタティック CRL はピア証明書チェーンのレベルが 1 以上のときにのみ適用されます（たとえば、ピア証明書チェーンにルート CA 証明書およびルート CA によって署名されたピア証明書のみが含まれているとき）。
- IPSec に対してスタティック CRL を設定している場合、[Authority Key Identifier (authkey)] フィールドはインポートされた CRL ファイルに存在している必要があります。そうでない場合、IPSec はそれを無効と見なします。
- スタティック CRL は、同じ発行元からのダイナミック CRL より優先されます。FXOS でピア証明書を検証するときに、同じ発行者の有効な（決定済みの）スタティック CRL があれば、ピア証明書の CDP は無視されます。
- 次のシナリオでは、デフォルトで厳格な CRL チェックが有効になっています。
  - 新しく作成したセキュアな LDAP プロバイダー接続、IPSec 接続、またはクライアント証明書エントリ
  - 新しく展開した FXOS シャーシマネージャ（FXOS 2.3.1.x 以降の初期開始バージョンで展開）

次の表は、証明書失効リストのチェックの設定と証明書の検証に応じた接続の結果を示しています。

表 *6:* 厳格（ローカル スタティック *CRL* なし）に設定した証明書失効のチェック モード

ローカル スタティック CRL なし	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンで CDP が 1 つ欠落している	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に成功

ローカル スタティック CRL なし	LDAP 接続	IPSec 接続
有効な署名付きピア証明書チェーンの 1 つの CDP CRL が空です	接続に失敗（syslog メッセージあり）	接続に成功
ピア証明書チェーンの CDP がダウンロードできません	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に成功
証明書に CDP はありますが、CDP サーバがダウンしています	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に成功

表 *7:* 厳格（ローカル スタティック *CRL* あり）に設定した証明書失効のチェック モード

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンで CDP が 1 つ欠落している（証明書チェーン レベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です（証明書チェーンのレベルは 1）	接続に成功	接続に成功

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンの CDP をダウンロードできません（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP がありますが、CDP サーバがダウンしています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗（syslog メッセージあり）	CDP と組み合わせて使用すると、接続に成功します CDP がなければ、接続に失敗し、syslog メッセージが表示されます

表 *8*：緩和（ローカル スタティック *CRL* なし）に設定した証明書失効のチェック モード

ローカル スタティック CRL なし	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーン内の CDP のチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンで CDP が 1 つ欠落している	接続に成功	接続に成功

ローカル スタティック CRL なし	LDAP 接続	IPSec 接続
ピア証明書チェーンの 1 つの CDP CRL が空です	接続に成功	接続に成功
ピア証明書チェーンの CDP がダウンロードできません	接続に成功	接続に成功
証明書に CDP はありますが、CDP サーバがダウンしています	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります	接続に成功	接続に成功

表 *9:* 緩和（ローカル スタティック *CRL* あり）に設定した証明書失効のチェック モード

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーン内の CDP のチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンで CDP が 1 つ欠落している（証明書チェーン レベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの CDP をダウンロードできません（証明書チェーンのレベルは 1）	接続に成功	接続に成功

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
証明書に CDP がありますが、CDP サーバがダウンしています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗（syslog メッセージあり）	CDP と組み合わせて使用すると、接続に成功します CDP がなければ、接続に失敗し、syslog メッセージが表示されます

CRL 定期ダウンロードの設定

システムを、CRL を定期的にダウンロードして、証明書の検証に新しい CRL を 1 ～ 24 時間ごとに使用するように設定できます。

この機能とともに、次のプロトコルとインターフェイスを使用できます。

- FTP
- SCP
- SFTP
- TFTP
- USB

（注）
- SCEP および OCSP はサポートされません。
- CRL ごとに設定できるのは 1 つの定期ダウンロードのみです。
- トラストポイントごとにサポートされるのは 1 つの CRL です。

（注） 期間は 1 時間間隔でのみ設定できます。

CRL 定期ダウンロードを設定するには、次の手順を実行します。

始める前に

Firepower 4100/9300 シャーシが、ピア証明書を（CRL）情報を使用して検証するように設定されていることを確認します。詳細については、トラストポイントのスタティック CRL の設定（83 ページ）を参照してください。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 トラストポイント モードに入ります。

scope trustpoint

ステップ 3 取り消しモードに入ります。

scope revoke

ステップ 4 取り消し設定を編集します。

sh config

ステップ 5 優先設定を設定します。

例：

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

ステップ 6 設定ファイルを終了します。

exit

ステップ 7 （任意）新しい CRL をダウンロードして、新しい設定をテストします。

例：

```
Firepower-chassis /security/trustpoint/revoke # sh import-task

Import task:
```

```
File Name Protocol Server          □□□     Userid       □□
--------- -------- --------------- ---------- ------------- -----
rootCA.crl Scp     182.23.33.113   0          MyName       □Downloading□
```

LDAP キー リング証明書の設定

Firepower 4100/9300 シャーシ上で TLS 接続をサポートする、セキュアな LDAP クライアント キー リング証明書を設定できます。このオプションは、システムのコモン クライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、セキュリティ認定準拠（75 ページ）を参照してください。

（注） コモン クライテリア モードを有効にする場合は、SSL が有効になっている必要があります。さらにキー リング証明書を作成するために、サーバ DNS 情報を使用する必要があります。

SSL を LDAP サーバ エントリに対して有効にすると、接続の形成時にキー リング情報が参照されて確認されます。

LDAP サーバ情報は、セキュア LDAP 接続（SSL 使用可能）用の、CC モードの DNS 情報である必要があります。

セキュア LDAP クライアントのキー リング証明書を設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 LDAP モードに入ります。

scope ldap

ステップ 3 LDAP サーバ モードに入ります。

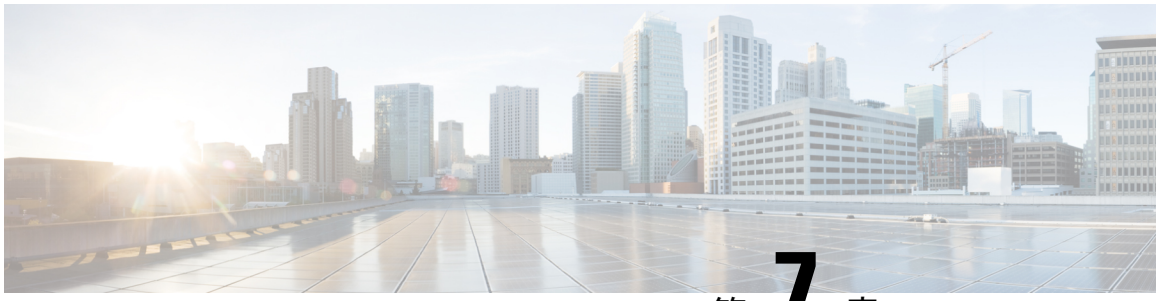
enter server *{server_ip|server_dns}*

ステップ 4 LDAP キー リングを設定します。

set keyring *keyring_name*

ステップ 5 設定をコミットします。

commit-buffer



第 7 章

システム管理

セッション変更により Firepower Chassis Manager セッションが閉じる場合

次のようにシステムを変更すると、自動的に Firepower Chassis Manager からログアウトする可能性があります。

- 10 分を超えてシステム時刻を変更した場合。
- Firepower Chassis Manager または FXOS CLI を使用してシステムを再起動またはシャットダウンした場合。
- Firepower 4100/9300 シャーシ 上の FXOS のバージョンをアップグレードした場合。
- FIPS またはコモン クライテリア モードを有効または無効にした場合。

（注） 上記の変更に加えて、一定期間にわたって操作がない場合は自動的にシステムからログアウトします。デフォルトでは、10 分間にわたり操作を行わないと自動的にログアウトします。このタイムアウト設定を変更するには、セッション タイムアウトの設定 （56 ページ）を参照してください。 また、セッションがアクティブな場合でも、一定時間の経過後にユーザをシステムからログオフさせるように絶対タイムアウトを設定することもできます。絶対タイムアウトを設定するには、絶対セッション タイムアウトの設定 （57 ページ）を参照してください。

管理 IP アドレスの変更

始める前に

FXOS CLI から Firepower 4100/9300 シャーシの管理 IP アドレスを変更できます。

（注） 管理 IP アドレスを変更した後、新しいアドレスを使用して Firepower Chassis Manager または FXOS CLI への接続を再確立する必要があります。

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセス （16 ページ）を参照）。

ステップ 2 IPv4 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。

Firepower-chassis# **scope fabric-interconnect a**

b) 現在の管理 IP アドレスを表示するには、次のコマンドを入力します。

Firepower-chassis /fabric-interconnect # **show**

c) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。

Firepower-chassis /fabric-interconnect # **set out-of-band ip** *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

d) トランザクションをシステム設定にコミットします。

Firepower-chassis /fabric-interconnect* # **commit-buffer**

ステップ 3 IPv6 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。

Firepower-chassis# **scope fabric-interconnect a**

b) 管理 IPv6 設定のスコープを設定します。

Firepower-chassis /fabric-interconnect # **scope ipv6-config**

c) 現在の管理 IPv6 アドレスを表示するには、次のコマンドを入力します。

Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band ipv6** *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

（注） シャーシの IPv6 管理アドレスとしてサポートされるのは、IPv6 グローバル ユニキャスト アドレスのみです。

e) トランザクションをシステム設定にコミットします。

Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

例

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
    64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask
255.255.255.0 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                            Prefix     IPv6 Gateway
    ----------------------------------- ---------- ------------
    2001::8998                              64         2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

アプリケーション管理 IP の変更

FXOS CLI から Firepower 4100/9300 シャーシに接続されたアプリケーションの管理 IP アドレスは変更できます。そのためには、まず FXOS プラットフォーム レベルで IP 情報を変更し、次にアプリケーション レベルで IP 情報を変更する必要があります。

（注） アプリケーション管理 IP を変更すると、サービスの中断が発生します。

手順

ステップ 1 FXOS CLI に接続します。（FXOS CLIへのアクセス （16 ページ） を参照）。

ステップ 2 範囲を論理デバイスにします。

scope ssa

scope logical-device *logical_device_name*

ステップ 3 範囲を管理ブートストラップにし、新しい管理ブートストラップ パラメータを設定します。導入間で違いがあることに注意してください。

ASA 論理デバイスのスタンドアロンの設定の場合。

a) 論理デバイスのブートストラップに入ります。
scope mgmt-bootstrap *asa*

b) スロットを IP モードにします。
scope *ipv4_or_6 slot_number* default

c) （IPv4 のみ）新しい IP アドレスを設定します。
set ip *ipv4_address* **mask** *network_mask*

d) （IPv6 のみ）新しい IP アドレスを設定します。
set ip *ipv6_address* **prefix-length** *prefix_length_number*

e) ゲートウェイ アドレスを設定します。
set gateway *gateway_ip_address*

f) 設定をコミットします。
commit-buffer

ASA 論理デバイスのクラスタ設定の場合。

a) クラスタ管理ブートストラップに入ります。
scope cluster-bootstrap *asa*

b) （IPv4 のみ）新しい仮想 IP を設定します。

set virtual ipv4 *ip_address* **mask** *network_mask*

c) （IPv6 のみ）新しい仮想 IP を設定します。

set virtual ipv6 *ipv6_address* **prefix-length** *prefix_length_number*

d) 新しい IP プールを設定します。

set ip pool *start_ip end_ip*

e) ゲートウェイ アドレスを設定します。

set gateway *gateway_ip_address*

f) 設定をコミットします。

commit-buffer

FTD のスタンドアロン設定およびクラスタ設定の場合。

a) 論理デバイスのブートストラップに入ります。
scope mgmt-bootstrap *ftd*

b) スロットを IP モードにします。

scope *ipv4_or_6 slot_number* firepower

c) （IPv4 のみ）新しい IP アドレスを設定します。

set ip *ipv4_address* **mask** *network_mask*

d) （IPv6 のみ）新しい IP アドレスを設定します。

set ip *ipv6_address* **prefix-length** *prefix_length_number*

e) ゲートウェイ アドレスを設定します。

set gateway *gateway_ip_address*

f) 設定をコミットします。

commit-buffer

（注） クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに新しい IP アドレスを設定する必要があります。シャーシ間クラスタまたは HA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

ステップ 4 アプリケーションごとに管理ブートストラップ情報をクリアします。

a) 範囲を ssa モードにします。

scope ssa

b) 範囲をスロットにします。

scope slot *slot_number*

c) 範囲をアプリケーション インスタンスにします。

scope app-instance *asa_or_ftd*

d) 管理ブートストラップ情報をクリアします。

clear-mgmt-bootstrap

e) 設定を確定します。

commit-buffer

ステップ 5 アプリケーションを無効にします。

disable

commit-buffer

（注） クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに管理ブートストラップ情報をクリアし、無効にする必要があります。シャーシ間クラスタまたはHA設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

ステップ 6 アプリケーションがオフラインで、スロットが再度オンラインになったときに、アプリケーションを再度有効にします。

a) 範囲を ssa モードに戻します。

scope ssa

b) 範囲をスロットにします。

scope slot *slot_number*

c) 範囲をアプリケーション インスタンスにします。

scope app-instance *asa_or_ftd*

d) アプリケーションを有効にします。

enable

e) 設定を確定します。

commit-buffer

（注） クラスタ設定の場合、これらのステップを繰り返して、Firepower 4100/9300 シャーシに接続されている各アプリケーションを再度有効にします。シャーシ間クラスタまたはHA設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

Firepower 4100/9300 シャーシ名の変更

Firepower 4100/9300 シャーシに使用する名前を FXOS CLI から変更することができます。

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセス （16 ページ）を参照）。

ステップ 2 システム モードに入ります。

Firepower-chassis-A# **scope system**

ステップ 3 現在の名前を表示します。

Firepower-chassis-A /system # **show**

ステップ 4 新しい名前を構成します。

Firepower-chassis-A /system # **set name** *device_name*

ステップ 5 トランザクションをシステム設定にコミットします。

Firepower-chassis-A /fabric-interconnect* # **commit-buffer**

例

次の例では、デバイス名を変更します。

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- --------------------
    New-name   Stand Alone 192.168.100.10    ::
New-name-A /system #
```

トラスト ID 証明書のインストール

初期設定後に、自己署名 SSL 証明書が Firepower 4100/9300 シャーシ Web アプリケーションで使用するために生成されます。その証明書は自己署名であるため、クライアントブラウザが自動的に信頼することはありません。新しいクライアントブラウザで Firepower 4100/9300 シャーシ Web インターフェイスに初めてアクセスするときに、ブラウザは SSL 警告をスローして、ユーザが Firepower 4100/9300 シャーシ にアクセスする前に証明書を受け入れることを要求します。FXOS CLI を使用して証明書署名要求（CSR）を生成し、Firepower 4100/9300 シャーシで使用する結果の ID 証明書をインストールするには、以下の手順を使用できます。この ID 証明書により、クライアント ブラウザは接続を信頼し、警告なしで Web インターフェイスを起動できるようになります。

手順

ステップ 1 FXOS CLI に接続します。（FXOS CLIへのアクセス （16 ページ） を参照）。

ステップ 2 セキュリティ モジュールを入力します。

scope security

ステップ 3 キーリングを作成します。

create keyring *keyring_name*

ステップ 4 秘密キーのモジュラス サイズを設定します。

set modulus *size*

ステップ 5 設定をコミットします。

commit-buffer

ステップ 6 CSR フィールドを設定します。証明書は、基本オプション（subject-name など）を指定して生成できます。さらに任意で、ロケールや組織などの情報を証明書に組み込むことができる詳細オプションを指定できます。CSR フィールドを設定する場合、システムにより証明書パスワードの入力が求められることに注意してください。

create certreq subject-name *subject_name*

password

set country *country*

set state *state*

set locality *locality*

set org-name *organization_name*

set org-unit-name *organization_unit_name*

set subject-name *subject_name*

ステップ 7 設定をコミットします。

commit-buffer

ステップ 8 認証局に提供する CSR をエクスポートします。認証局は CSR を使用して ID 証明書を作成します。

a) 完全な CSR を表示します。

show certreq

b) 「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までの出力をコピーします。

例：

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx
ETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
```

```
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUgk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVDcL+tATu5xFE3LA310ck6GjlNv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvDl1n70JCegHdCWtP75SaNyaBEPkO0365rTckbw==
-----END CERTIFICATE REQUEST-----
```

ステップ 9 certreq モードを終了します。

exit

ステップ 10 キーリング モードを終了します。

exit

ステップ 11 認証局の登録プロセスに従って認証局に CSR の出力を提供します。要求が成功すると、認証局はこの CA の秘密キーを使用してデジタル署名された ID 証明書が返されます。

ステップ 12 （注） FXOS にインポートするすべての ID 証明書は、Base64 形式でなければなりません。認証局から受信した ID 証明書チェーンの形式が多様である場合は、まずそれを OpenSSL などの SSL ツールを使用して変換する必要があります。

ID 証明書チェーンを保持する新規トラストポイントを作成します。

create trustpoint *trustpoint_name*

ステップ 13 画面の指示に従って、手順 11 で認証局から受信した ID 証明書チェーンを入力します。

（注） 中間証明書を使用する認証局の場合は、ルートと中間証明書とを結合させる必要があります。テキスト ファイルで、ルート証明書を一番上にペーストし、それに続いてチェーン内の各中間証明書をペーストします。この場合、すべての BEGIN CERTIFICATE フラグと END CERTIFICATE フラグを含めます。この全体のテキスト ブロックを、トラストポイントにコピー アンド ペーストします。

set certchain

例：

```
firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOp3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
```

```
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsv1gCxsQVOw0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

ステップ 14 設定をコミットします。

commit-buffer

ステップ 15 トラストポイント モードを終了します。

exit

ステップ 16 キーリング モードに入ります。

scope keyring *keyring_name*

ステップ 17 ステップ 13 で作成されたトラストポイントを、CSR に作成されたキーリングに関連付けます。

set trustpoint *trustpoint_name*

ステップ 18 サーバの署名付き ID 証明書をインポートします。

set cert

ステップ 19 認証局により提供された ID 証明書の内容をペーストします。

例：

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
```

```
>-----END CERTIFICATE-----
>ENDOFBUF
```

ステップ 20 キーリング モードを終了します。

exit

ステップ 21 セキュリティ モードを終了します。

exit

ステップ 22 システム モードに入ります。

scope system

ステップ 23 サービス モードに入ります。

scope services

ステップ 24 新しい証明書を使用するように FXOS Web サービスを設定します。

set https keyring *keyring_name*

ステップ 25 設定をコミットします。

commit-buffer

ステップ 26 HTTPS サーバに関連付けられているキーリングを表示します。これにはこの手順の手順 3 で作成したキーリングの名前が反映されることになります。画面出力にデフォルトのキーリング名が表示される場合には、HTTPS サーバはまだ、新しい証明書を使用するように更新されていません。

show https

例：

```
fp4120 /system/services # show https
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: firepower_cert
    Cipher suite mode: Medium Strength
    Cipher suite:
ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

ステップ 27 インポートされた証明書の内容を表示し、**Certificate Status**値が**Valid**と表示されることを確認します。

scope security

show keyring *keyring_name* **detail**

例：

```
fp4120 /security #  scope security
fp4120 /security #  show keyring firepower_cert detail
Keyring firepower_cert:
    RSA key modulus: Mod2048
    Trustpoint CA: firepower_chain
```

```
    Certificate status: Valid
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
        Validity
            Not Before: Apr 28 13:09:54 2016 GMT
            Not After : Apr 28 13:09:54 2018 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
                    0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
                    a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
                    50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
                    fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
                    d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
                    87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
                    07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
                    47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
                    cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
                    5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
                    d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
                    1d:85
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Subject Alternative Name:
                    DNS:fp4120.test.local
                X509v3 Subject Key Identifier:
                    FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
                X509v3 Authority Key Identifier:
                    keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
                X509v3 CRL Distribution Points:
                    Full Name:
                      URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
                       CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,


DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
                Authority Information Access:
                    CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
                      CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                      DC=local?cACertificate?base?objectClass=certificationAuthority
                1.3.6.1.4.1.311.20.2:
                    ...W.e.b.S.e.r.v.e.r
                X509v3 Key Usage: critical
                    Digital Signature, Key Encipherment
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
         e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
         02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
```

```
        2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

次のタスク

新しい信頼できる証明書が存在していることを確認するには、Web ブラウザのアドレス バーに *https://<FQDN_or_IP>/* と入力して、Firepower Chassis Manager に移動します。

（注） ブラウザはさらに、アドレス バーの入力内容に照らして証明書のサブジェクト名を確認します。証明書が完全修飾ドメイン名に対して発行されている場合、ブラウザでもそのようにアクセスする必要があります。IP アドレスを使用してアクセスすると、信頼できる証明書が使用されているとしても、別の SSL エラー（共通名が無効）がスローされます。

証明書の更新の自動インポート

Cisco 証明書サーバーが別のルート CA を利用するようにアイデンティティ証明書を変更すると、ASA デバイスを実行している 4100 または 9300 のスマートライセンスの接続が切断されます。ライセンス接続はアプリケーションの Lina ではなくスーパーバイザによって処理される

ため、スマートライセンス機能は失敗します。FXOS ベースのデバイスの場合、FXOS ソフトウェアにアップグレードしなくても、自動インポート機能を使用して問題を解決できます。

デフォルトでは、自動インポート機能はディセーブルです。次の手順を使用して、FXOS CLI を使用して自動インポート機能を有効にすることができます。

始める前に

DNS サーバーは、Cisco 証明書サーバーに到達するように設定する必要があります。
http://www.cisco.com/security/pki/trs/ios_core.p7b

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 セキュリティ モジュールを入力します。

scope security

ステップ 3 自動インポート機能を有効にします。

enter tp-auto-import

例：

```
FXOS# scope security
FXOS /security # enter tp-auto-import
 FXOS /security #
```

ステップ 4 設定をコミットします。

commit-buffer

ステップ 5 自動インポートステータスの検証

show detail

例：

自動インポートの成功：

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

自動インポートの失敗：

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Failure
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

ステップ 6 tp-auto-import 機能を設定します。import-time-hour を設定します。

set import-time-hour *hour* **import-time-min** *minutes*

例：

```
FXOS /security/tp-auto-import # set
  import-time-hour  Trustpoints auto import hour time
FXOS /security/tp-auto-import # set import-time-hour
  0-23  Import Time Hour
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min
  0-59  Import Time Min
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
<CR>
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
FXOS /security/tp-auto-import* # commit-buffer
FXOS /security/tp-auto-import #
```

（注） 自動インポートのソース URL は固定されており、インポート時間の詳細を 1 日あたりの分に変更する必要があります。インポートは、スケジュールされた時刻に毎日行われます。時間と分が設定されていない場合、証明書のインポートはその有効化時に 1 回だけ行われます。証明書は、/opt/certstore パスの下のボックスにバンドルとしてダウンロードされ、セキュアログインオプションを介してのみアクセスできます。バンドル（ios_core.p7b）とともに、個々の証明書（AutoTP1 から AutoTPn）が自動的に抽出されます。

ステップ 7 自動インポート設定が完了したら、show detail コマンドを入力します。

show detail

例：

```
FXOS  /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 07:20
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
```

（注） インポートできる証明書の最大数は 30 です。Cisco 証明書サーバーへの接続に問題がある場合、各インポートは 6 回繰り返され、show コマンドで最後のインポートステータスが更新されます。

ステップ 8 （オプション）自動インポート機能を無効にするには、delete auto-import コマンドを入力します。

delete tp-auto-import

例：

```
FXOS /security #
FXOS /security # delete tp-auto-import
FXOS /security* # commit-buffer
FXOS /security # show detail
security mode:
    Password Strength Check: No
    Minimum Password Length: 8
    Is configuration export key set: No
    Current Task:
FXOS /security # scope tp-auto-import
Error: Managed object does not exist
```

```
FXOS /security #
FXOS /security # enter tp-auto-import
FXOS /security/tp-auto-import* # show detail
FXOS /security/tp-auto-import* #
```

（注） 自動インポート機能を無効にすると、インポートされた証明書は、ビルドの変更がなくなるまで持続します。自動インポート機能を無効にしてからビルドをダウングレード/アップグレードすると、証明書が削除されます。

ログイン前バナー

ログイン前バナーでは、ユーザがFirepower Chassis Managerにログインするとシステムにバナーテキストが表示されます。ユーザ名とパスワードのシステムプロンプトの前に、メッセージの画面で [OK] をクリックする必要があります。ログイン前バナーを設定しないと、システムはユーザ名とパスワードのプロンプトにすぐに進みます。

ユーザがFXOS CLIにログインすると、設定されている場合はシステムがパスワードのプロンプトの前にログイン バナー テキストを表示します。

ログイン前バナーの作成

手順

ステップ1 FXOS CLIに接続します（FXOS CLIへのアクセス （16 ページ）を参照）。

ステップ2 セキュリティ モードを開始します。

Firepower-chassis# **scope security**

ステップ3 バナー セキュリティ モードに入ります。

Firepower-chassis /security # **scope banner**

ステップ4 次のコマンドを入力して、ログイン前バナーを作成します。

Firepower-chassis /security/banner # **create pre-login-banner**

ステップ5 Firepower Chassis ManagerまたはFXOS CLIへのログイン前のユーザにFXOSが表示するメッセージを指定します。

Firepower-chassis /security/banner/pre-login-banner* # **set message**

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

ステップ6 プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準のASCII文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は192文字です。行の区切りで Enter キーを押します。

入力内容の次の行に **ENDOFBUF** と入力し、**Enter** キーを押して終了します。

[メッセージの設定（set message）] ダイアログをキャンセルするには、**Ctrl**+**C** キーを押します。

ステップ 7 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

例

次の例は、ログイン前バナーを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

ログイン前バナーの変更

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセス （16 ページ）を参照）。

ステップ 2 セキュリティ モードを開始します。

Firepower-chassis# **scope security**

ステップ 3 バナー セキュリティ モードに入ります。

Firepower-chassis /security # **scope banner**

ステップ 4 ログイン前バナーのバナー セキュリティ モードに入ります。

Firepower-chassis /security/banner # **scope pre-login-banner**

ステップ 5 Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。

Firepower-chassis /security/banner/pre-login-banner # **set message**

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

ステップ 6 プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準の ASCII 文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は 192 文字です。行の区切りで Enter キーを押します。

入力内容の次の行に **ENDOFBUF** と入力し、**Enter** キーを押して終了します。

[メッセージの設定（set message）] ダイアログをキャンセルするには、**Ctrl**+**C** キーを押します。

ステップ 7 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

例

次に、ログイン前バナーを変更する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

ログイン前バナーの削除

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセス （16 ページ）を参照）。

ステップ 2 セキュリティ モードを開始します。

Firepower-chassis# **scope security**

ステップ 3 バナー セキュリティ モードに入ります。

Firepower-chassis /security # **scope banner**

ステップ 4 システムからログイン前バナーを削除します。

Firepower-chassis /security/banner # **delete pre-login-banner**

ステップ 5 トランザクションをシステム設定にコミットします。

Firepower-chassis /security/banner* # **commit-buffer**

例

次に、ログイン前バナーを削除する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

Firepower 4100/9300 シャーシ の再起動

手順

ステップ 1 [概要（Overview）] を選択して、[概要（Overview）] ページを開きます。

ステップ 2 [概要（Overview）] ページの右上隅の [シャーシ稼働時間（Chassis Uptime）] の横にある [リブート（Reboot）] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、Firepower 4100/9300 シャーシを電源オフにすることを確認します。
システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的にFirepower4100/9300 シャーシの電源をオフにして再始動する前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。このプロセスには約 15 ～ 20 分かかります。

Firepower 4100/9300 シャーシの電源オフ

手順

ステップ 1 [Overview] を選択して、[Overview] ページを開きます。

ステップ 2 [概要（Overview）]ページの右上隅の [シャーシ稼働時間（Chassis Uptime）] の横にある [シャットダウン（Shutdown）] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、Firepower 4100/9300 シャーシを電源オフにすることを確認します。
システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにする前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。

工場出荷時のデフォルト設定の復元

FXOS CLI を使用して Firepower 4100/9300 シャーシを工場出荷時のデフォルト設定に戻すことができます。

（注） このプロセスによって、論理デバイス設定を含むすべてのユーザ設定がシャーシから消去されます。この手順が完了したら、システムを再設定する必要があります（初期設定（8 ページ） を参照してください）。

手順

ステップ 1 （任意） **erase configuration** コマンドはシャーシからスマート ライセンス設定を削除しません。スマート ライセンス設定も削除する場合は、次の手順を実行します。

scope license

deregister

Firepower 4100/9300 シャーシの登録を解除すると、アカウントからデバイスが削除されます。さらに、デバイス上のすべてのライセンス資格と証明書が削除されます。

ステップ 2 ローカル管理シェルに接続します。

connect local-mgmt

ステップ 3 Firepower 4100/9300 シャーシからすべてのユーザ設定を消去し、最初の工場出荷時のデフォルト設定にシャーシを復元するには、次のコマンドを入力します。

erase configuration

すべてのユーザ設定を消去するかどうかを確認するように求められます。

ステップ 4 設定の消去を確認するには、コマンド プロンプトに **yes** と入力します。
すべてのユーザ設定が Firepower 4100/9300 シャーシから消去された後、システムがリブートします。

システム コンポーネントの安全な消去

FXOS CLI を使用して、アプライアンスのコンポーネントを安全に消去することができます。

「工場出荷時のデフォルト設定の復元 （112 ページ）」で説明されているように、**erase configuration** コマンドを実行すると、シャーシのすべてのユーザ設定情報が削除され、工場出荷時のデフォルト設定に戻ります。

secure erase コマンドにより、指定したアプライアンス コンポーネントが安全に消去されます。つまり、単にデータが削除されるだけでなく、物理ストレージが「ワイプ」（完全に消去）されます。これは、ハードウェア ストレージ コンポーネントが残存データやスタブを保持しない状態で、アプライアンスを転送または返却する際に重要です。

（注） 完全消去中にデバイスが再起動します。これは、SSH接続が終了したことを意味します。したがって、シリアルコンソールポート接続を介して完全消去を実行することをお勧めします。

手順

ステップ 1 ローカル管理シェルに接続します。

connect local-mgmt

ステップ 2 指定したアプライアンス コンポーネントを安全に消去するには、次の **erase configuration** コマンドのいずれかを入力します。

a) **erase configuration chassis**

すべてのデータとイメージが失われ、回復できないことを警告するメッセージが表示され、続行するかどうかの確認が求められます。**y** を入力すると、シャーシ全体が安全に消去されます。セキュリティモジュールが最初に消去され、その後にスーパーバイザが消去されます。

デバイス上のすべてのデータとソフトウェアが消去されるため、デバイスリカバリはROMモニタ（ROMMON）からのみ実行できます。

b) **erase configuration security_module** *module_id*

モジュール上のすべてのデータとイメージが失われ、回復できないことを警告するメッセージが表示され、続行するかどうかの確認が求められます。**y**を入力すると、モジュールが消去されます。

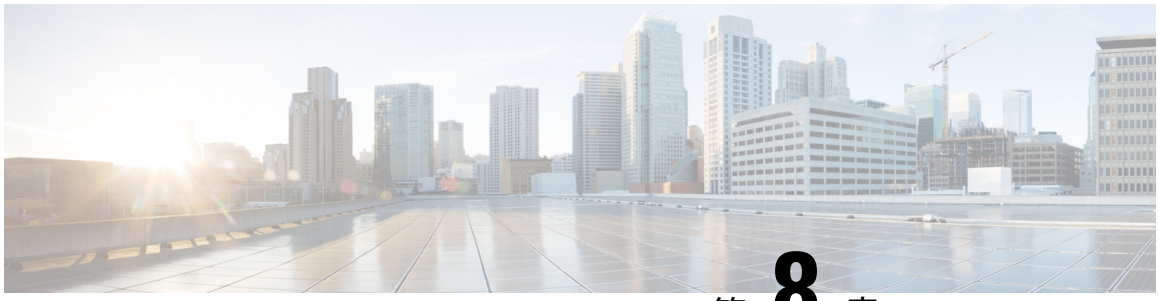
（注） **decommission-secure** コマンドの実行結果は、基本的にこのコマンドを実行した場合と同じです。

セキュリティモジュールが消去されると、確認応答されるまでダウンした状態になります（デコミッションされたモジュールと同様）。

c) **erase configuration supervisor**

すべてのデータとイメージが失われ、回復できないことを警告するメッセージが表示され、続行するかどうかの確認が求められます。**y** を入力すると、スーパーバイザが安全に消去されます。

スーパーバイザ上のすべてのデータとソフトウェアが消去されるため、デバイスリカバリは ROM モニタ（ROMMON）からのみ実行できます。



第 8 章

プラットフォーム設定

日時の設定

日付と時刻を手動で設定したり、現在のシステム時刻を表示するには、下記で説明する [NTP] ページの システムのネットワーク タイム プロトコル（NTP）を設定します。

NTP の設定は、Firepower 4100/9300 シャーシとシャーシにインストールされている論理デバイス間で自動的に同期されます。

（注） Firepower 4100/9300 シャーシ に FTD を導入すると、スマートライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように Firepower 4100/9300 シャーシ で NTP を設定する必要があります。Firepower 4100/9300 シャーシ と FMC の両方で同じ NTP サーバーを使用する必要がありますが、FMC は Firepower 4100/9300 シャーシ の NTP サーバーとして使用できないので注意してください。

NTP を使用すると、[Current Time] タブの全体的な同期ステータスを表示できます。または、[Time Synchronization] タブの [NTP Server] テーブルの [Server Status] フィールドを見ると、設定済みの各 NTP サーバの同期ステータスを表示できます。システムが特定 NTP サーバと同期できない場合、[サーバのステータス（Server Status）] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

設定された日付と時刻の表示

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [Current Time] タブをクリックします。

システムは、デバイスに設定された日付、時刻、タイム ゾーンを表示します。

NTP を使用している場合、[現在時刻（Current Time）] タブに総合的な同期ステータスを表示することもできます。設定済みの各 NTP サーバの同期ステータスは、[時刻同期（Time Synchronization）] タブにある **NTP サーバ** テーブルの [サーバ ステータス（Server Status）] フィールドを見て確認できます。システムが特定 NTP サーバと同期できない場合、[サーバのステータス（Server Status）] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

タイム ゾーンの設定

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [Current Time] タブをクリックします。

ステップ 3 シャーシの適切なタイムゾーンを [タイムゾーン（Time Zone）] ドロップダウンリストから選択します。

NTP を使用した日付と時刻の設定

NTP を使用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。 最大 4 台の NTP サーバを設定できます。

（注）
- FXOS では、NTP バージョン 3 を使用します。
- 外部 NTP サーバのストラタム値が 13 以上の場合、アプリケーションインスタンスは FXOS シャーシ上の NTP サーバと同期できません。NTP クライアントが NTP サーバと同期するたびに、ストラタム値が 1 ずつ増加します。

  独自の NTP サーバをセットアップしている場合は、サーバ上の /etc/ntp.conf ファイルでそのストラタム値を確認できます。NTP サーバのストラタム値が 13 以上の場合は、ntp.conf ファイルのストラタム値を変更してサーバを再起動するか、別の NTP サーバ（たとえば、pool.ntp.org）を使用することができます。

始める前に

NTP サーバのホスト名を使用する場合は、DNS サーバを設定する必要があります。DNS サーバの設定 （162 ページ）を参照してください。

手順

ステップ 1 **[Platform Settings]** > **[NTP]** を選択します。

[Time Synchronization] タブがデフォルトで選択されています。

ステップ 2 [Set Time Source] で、[Use NTP Server] をクリックします。

ステップ 3 （任意） NTP サーバで認証が必要な場合は、[NTP Server Authentication: Enable] チェックボックスをオンにします。

認証キー ID と値が必要な場合は、[Yes] をクリックします。

NTP サーバ認証では SHA1 のみがサポートされます。

ステップ 4 [Add] をクリックして、IP アドレスまたはホスト名で最大 4 つの NTP サーバを識別します。

ステップ 5 （任意） NTP サーバの [Authentication Key] ID と [Authentication Value] を入力します。

NTP サーバからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーバ バージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp. keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの両方に対して、メッセージ ダイジェストの計算時に使用するキー値を通知するために使用します。

ステップ 6 **[保存（Save）]** をクリックします。

各サーバの同期ステータスは、**NTP サーバ** テーブルの [Server Status] フィールドを見て確認できます。システムが特定NTPサーバと同期できない場合、[サーバのステータス（Server Status）] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

（注） システム時刻の変更に10分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

NTP サーバの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [時刻同期（Time Synchronization）] タブをクリックします。

ステップ 3 削除する各 NTP サーバに対して、**NTP サーバ** テーブルでそのサーバの [削除（Delete）] アイコンをクリックします。

ステップ 4 [Save] をクリックします。

日付と時刻の手動での設定

ここでは、シャーシで日付と時刻を手動で設定する方法ついて説明します。シャーシの日時を手動で設定した後、インストールされている論理デバイスに変更が反映されるまでに時間がかかる場合があることに注意してください。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [Time Synchronization] タブをクリックします。

ステップ 3 [時刻源の設定（Set Time Source）] で、[時刻を手動で設定（Set Time Manually）] をクリックします。

ステップ 4 [日付（Date）] ドロップダウンリストをクリックしてカレンダーを表示し、そのカレンダーで使用可能なコントロールを使用して日付を設定します。

ステップ 5 時、分、および AM/PM のそれぞれのドロップダウン リストを使用して時間を指定します。

ヒント [システム時刻を取得（Get System Time）] をクリックすると、Firepower Chassis Manager への接続に使用するシステムの設定に一致する日付と時刻を設定できます。

ステップ 6 [保存（Save）] をクリックします。

指定した日付と時刻がシャーシに設定されます。

（注） システム時刻の変更に10分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

Configuring SSH

次の手順では、シャーシへの SSH アクセスを有効または無効にする方法、FXOS シャーシを SSH クライアントとして有効にする方法、さらに SSH で使用する暗号化、キー交換、およびメッセージ認証用のさまざまなアルゴリズムを SSH サーバーと SSH クライアントに設定する方法について説明します。

SSH はデフォルトでイネーブルになります。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [SSH] > [SSH サーバ（SSH Server）]** の順に選択します。

ステップ 2 シャーシへの SSH アクセスを有効にするには、[SSHの有効化（Enable SSH）] チェックボックスをオンにします。SSH アクセスをディセーブルにするには、[Enable SSH] チェックボックスをオフにします。

ステップ 3 サーバの [暗号化アルゴリズム（Encryption Algorithm）] として、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

（注）
- 次の暗号化アルゴリズムは、コモン クライテリア モードではサポートされていません。
  - 3des-cbc
  - chacha20-poly1305@openssh.com
- chacha20-poly1305@openssh.com は FIPS ではサポートされていません。FXOS シャーシで FIPS モードが有効になっている場合、chacha20-poly1305@openssh.com を暗号化アルゴリズムとして使用することはできません。
- 次の暗号化アルゴリズムは、デフォルトでは有効になっていません。

```
aes128-cbc
aes192-cbc
aes265-cbc
```

ステップ 4 サーバの [Key Exchange Algorithm] として、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認

証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

（注）
- 次のキー交換アルゴリズムは、コモン クライテリア モードではサポートされていません。
  - diffie-hellman-group14-sha256
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- FIPS モードでは、次のキー交換アルゴリズムはサポートされていません。
  - curve25519-sha256
  - curve25519-sha256@libssh.org

ステップ 5 サーバの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 6 サーバの [ホスト キー（Host Key）] について、RSA キー ペアのモジュラス サイズを入力します。

モジュラス値（ビット単位）は、1024 ～ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

ステップ 7 サーバの [キー再生成のボリューム制限（Volume Rekey Limit）] に、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 8 サーバの [キー再生成の時間制限（Time Rekey Limit）] では、FXOS がセッションを切断する前に SSH セッションがアイドル状態を続けられる長さを分単位で設定します。

ステップ 9 [Save]をクリックします。

ステップ 10 [SSH クライアント（SSH Client）] タブをクリックして、FXOS シャーシの SSH クライアントをカスタマイズします。

ステップ 11 [厳密なホスト キー検査（Strict Host Keycheck）] について、[有効（enable）]、[無効（disable）]、または [プロンプト（prompt）] を選択して、SSH ホスト キー チェックを制御します。

- [enable]：FXOS が認識するホスト ファイルにそのホスト キーがまだ存在しない場合、接続は拒否されます。 FXOS CLI でシステム スコープまたはサービス スコープの **enter ssh-host** コマンドを使用して、手動でホストを追加する必要があります。
- [プロンプト（prompt）]：シャーシにまだ保存されていないホストキーを許可または拒否するように求められます。
- **disable**：（デフォルト）シャーシは過去に保存されたことがないホストキーを自動的に許可します。

ステップ 12 クライアントの [暗号化アルゴリズム（Encryption Algorithm）] として、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

（注）
- 次の暗号化アルゴリズムは、コモン クライテリア モードではサポートされていません。
  - 3des-cbc
  - chacha20-poly1305@openssh.com

  FXOS シャーシでコモン クライテリア モードが有効な場合、暗号化アルゴリズムとして 3des-cbc を使用することはできません。
- chacha20-poly1305@openssh.com は FIPS ではサポートされていません。FXOS シャーシで FIPS モードが有効になっている場合、chacha20-poly1305@openssh.com を暗号化アルゴリズムとして使用することはできません。
- 次の暗号化アルゴリズムは、デフォルトでは有効になっていません。

```
aes128-cbc
aes192-cbc
aes265-cbc
```

ステップ 13 クライアントの [キー交換アルゴリズム（Key Exchange Algorithm）] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

（注）
- 次のキー交換アルゴリズムは、コモンクライテリアモードではサポートされていません。
  - diffie-hellman-group14-sha256
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- FIPS モードでは、次のキー交換アルゴリズムはサポートされていません。
  - curve25519-sha256
  - curve25519-sha256@libssh.org

ステップ 14 クライアントの [Mac アルゴリズム（Mac Algorithm）] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 15 クライアントの [キー再生成のボリューム制限（Volume Rekey Limit）] について、FXOS がセッションを切断する前にその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 16 クライアントの [キー再生成の時間制限（Time Rekey Limit）] について、FXOS がセッションを切断する前に SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 17 [Save] をクリックします。

TLS の設定

Transport Layer Security（TLS）プロトコルは、互いに通信する 2 つのアプリケーションの間でプライバシーとデータの整合性を確保します。FXOS シャーシと外部デバイスとの通信で許容する最小 TLS バージョンは、FXOS CLI を使用して設定できます。新しいバージョンの TLS では通信のセキュリティを強化できる一方、古いバージョンの TLS では古いアプリケーションとの後方互換性を維持できます。

たとえば、FXOS シャーシで設定されている最小 TLS バージョンが v1.1 の場合、クライアントブラウザが v1.0 だけを実行するように設定されていると、クライアントは HTTPS を使用して FXOS Chassis Manager との接続を開くことができません。したがって、ピアアプリケーションと LDAP サーバを適切に設定する必要があります。

次の手順で、FXOS シャーシと外部デバイス間の通信で許容する最小 TSL バージョンを設定、表示する方法を説明します。

（注）
- FXOS 2.3(1) リリースの時点では、FXOS シャーシのデフォルト最小 TLS バージョンは v1.1 です。

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

ステップ 2 システムで使用できる TLS バージョンのオプションを表示します。

Firepower-chassis /system # **set services tls-ver**

例：

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver
    v1_0  v1.0
    v1_1  v1.1
    v1_2  v1.2
```

ステップ 3 最小 TLS バージョンを設定します。

Firepower-chassis /system # **set services tls-ver** *version*

例：

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver v1_2
```

ステップ 4 設定をコミットします。

Firepower-chassis /system # **commit-buffer**

ステップ 5 システムで設定されている最小 TLS バージョンを表示します。

Firepower-chassis /system # **scope services**

Firepower-chassis /system/services # **show**

例：

```
Firepower-chassis /system/services # show
Name: ssh
    Admin State: Enabled
    Port: 22
Kex Algo: Diffie Hellman Group1 Sha1,Diffie Hellman Group14 Sha1
Mac Algo: Hmac Sha1,Hmac Sha1 96,Hmac Sha2 512,Hmac Sha2 256
Encrypt Algo: 3des Cbc,Aes256 Cbc,Aes128 Cbc,Aes192 Cbc,Aes256 Ctr,Aes128 Ctr,Ae
s192 Ctr
Auth Algo: Rsa
    Host Key Size: 2048
Volume: None Time: None
Name: telnet
    Admin State: Disabled
    Port: 23
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: default
    Cipher suite mode: Medium Strength
    Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIU
M:+EXP:+eNULL
    Https authentication type: Cert Auth
    Crl mode: Relaxed
TLS:
    TLS version: v1.2
```

Telnet の設定

次の手順では、シャーシへの Telnet アクセスを有効化または無効化にする方法について説明します。デフォルトでは、Telnet は無効化になっています。

（注） 現在、Telnet は CLI を使用してのみ設定できます。

手順

ステップ 1 システム モードに入ります。

Firepower-chassis # **scope system**

ステップ 2 システム サービス モードを開始します。

Firepower-chassis /system # **scope services**

ステップ 3 シャーシへの Telnet アクセスを設定するには、次のいずれかを実行します。

- シャーシへの Telnet アクセスを許可するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **enable telnet-server**

- シャーシへの Telnet アクセスを禁止するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **disable telnet-server**

ステップ 4 トランザクションをシステム設定にコミットします。

Firepower /system/services # **commit-buffer**

例

次に、Telnet を有効にし、トランザクションを確定する例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

SNMP の設定

シャーシに Simple Network Management Protocol（SNMP）を設定するには、[SNMP] ページを使用します。詳細については、次のトピックを参照してください。

SNMP の概要

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMPマネージャ：SNMPを使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに報告するシャーシ内のソフトウェアコンポーネント。シャーシには、エージェントと一連のMIBが含まれています。SNMPエージェントを有効にし、マネージャとエー

ジェント間のリレーションシップを作成するには、Firepower Chassis Manager または FXOS CLI で SNMP を有効にし、設定します。

- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。SNMP は次のように定義されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

（注） SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。これらのバージョンで唯一の認証形式として機能するコミュニティストリングも含まれます。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

シャーシは、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、シャーシはトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。シャーシが PDU を受信しない場合、インフォーム要求を再送できます。

ただし、インフォームは SNMPv2c でのみ使用可能ですが、安全ではないと考えられているため、推奨されません。

（注） SNMP を使用するインターフェイスの ifindex の順序は、FXOS の再起動後も変更されません。ただし、FXOS ディスク使用率 OID のインデックス番号は、FXOS を再起動すると変更されます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限レベルは、メッセージが開示されないよう保護または認証の必要があるかどうかを決定します。サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているかによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 *10 : SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	水準器	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング（Community string）	なし	コミュニティ ストリングの照合を使用して認証します。

モデル	水準器	認証	暗号化	結果
v2c	noAuthNoPriv	コミュニティ ストリング（Community string）	なし	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	[ユーザ名（Username）]	なし	ユーザ名の照合を使用して認証します。 （注） 設定することはできますが、FXOS では SNMP バージョン 3 で noAuthNoPriv を使用することはできません。
v3	authNoPriv	HMAC-SHA	なし	HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュアアクセスを実現します。SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。SNMPv3 ユーザベース セキュリティ モデル（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

SNMP サポート

シャーシは、SNMP に次のサポートを提供します。

MIB のサポート

シャーシは、MIB への読み取り専用アクセスをサポートします。

利用可能な特定の MIB の詳細とその入手場所については、『Cisco FXOS MIB Reference Guide』を参照してください。

SNMPv3 ユーザの認証プロトコル

シャーシは、SNMPv3 ユーザーの HMAC-SHA-96（SHA）認証プロトコルをサポートします。

SNMPv3 ユーザの AES プライバシー プロトコル

シャーシは、SNMPv3 メッセージ暗号化用プライバシープロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。

プライバシーパスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 の設定を有効にして、SNMPv3 ユーザー用のプライバシーパスワードを含めると、シャーシはそのプライバシーパスワードを使用して 128 ビット AES キーを生成します。AES priv パスワードは、8 文字以上にします。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

SNMP の有効化および SNMP プロパティの設定

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

ステップ 2 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[管理状態（Admin State）] チェックボックス	SNMP を有効にするかまたは無効にするか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスを有効にします。
[ポート（Port）] フィールド	シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。

名前	説明
[Community/Username] フィールド	（任意）SNMP v1 および v2 のポーリングに使用するコミュニティストリング。 SNMP コミュニティ名を指定すると、SNMP リモートマネージャからのポーリング要求に対して SNMP バージョン 1 および 2c も自動的に有効になります。このフィールドは SNMP v3 には適用されません。 SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。コミュニティ ストリングは、これらのバージョンで唯一の認証形式として機能します。 1 ～ 32 文字の英数字文字列を入力します。@（アットマーク）、&（アンパサンド）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは **public** です。 [Community/Username] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [Set: Yes] を読み取ります。[Community/Username] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [Set: No] を読み取ります。 （注） CLI コマンド **set snmp community** を使用して既存のコミュニティ ストリングを削除することで、SNMP リモートマネージャからのポーリング要求に対して SNMP バージョン 1 および 2c を無効にすることができます。
[System Administrator Name] フィールド	SNMP の実装担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location]フィールド	SNMP エージェント（サーバ）が動作するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

次の手順では、SNMP トラップを作成する方法について説明します。

（注） 最大 8 つの SNMP トラップを定義できます。

手順

ステップ 1 **[Platform Settings]** > **[SNMP]** を選択します。

ステップ 2 [SNMP Traps] 領域で、[Add] をクリックします。

ステップ 3 [SNMP トラップの追加（Add SNMP Trap）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[Community/Username] フィールド	トラップの宛先へのアクセスを許可するために必要な SNMPv1/v2c コミュニティストリングまたは SNMPv3 ユーザ名を入力します。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[Port] フィールド	シャーシがトラップのために SNMP ホストと通信するポート。 1 ～ 65535 の整数を入力します。
[Version] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **V1** • **[V2]** • **V3** （注） SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。これらのバージョンで唯一の認証形式として機能するコミュニティストリングも含まれます。

名前	説明
[Type] フィールド	送信するトラップのタイプを指定します。 • **[Traps]** • [Informs]（[Version] が**V2**の場合にのみ有効）
[v3 Privilege] フィールド	バージョンで**V3**を選択した場合は、トラップに関連付ける権限を指定します。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし これを選択することはできますが、FXOS は SNMPv3 でこのセキュリティレベルをサポートしていないことに注意してください。 • [Priv]：認証あり、暗号化あり

ステップ 4 [OK] をクリックして、[Add SNMP Trap] ダイアログボックスを閉じます。

ステップ 5 [保存（Save）] をクリックします。

SNMP トラップの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

ステップ 2 [SNMP Traps] 領域で、削除するトラップに対応するテーブルの行の [Delete] アイコンをクリックします。

SNMPv3 ユーザの作成

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

ステップ 2 [SNMP Users] 領域で、[Add] をクリックします。

ステップ 3 [SNMP ユーザの追加（Add SNMP User）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	SNMPv3 ユーザに割り当てられているユーザ名。 32 文字まで入力します。名前の先頭は文字である必要があります。有効な文字は、文字、数字、_（アンダースコア）です。（ピリオド）、@（アットマーク）、-（ハイフン）も指定できます。
[Auth Type] フィールド	許可タイプ：**SHA**。
[AES-128 の使用（Use AES-128）] チェックボックス	オンにすると、このユーザにAES-128暗号化が使用されます。 （注） SNMPv3 はDES をサポートしていません。[AES-128] ボックスをオフのままにすると、プライバシーの暗号化は行われず、設定されたプライバシーパスワードは無効になります。
[パスワード（Password）] フィールド	このユーザのパスワード。 FXOS では、次の要件を満たさないパスワードは拒否されます。 • 8 ～ 80 文字を含む。 • 含められるのは、文字、数字、および次の文字のみです。 ~`!@#%^&*()_-+{}[]\:;'"<,>./ • 次の記号を含まない。$（ドル記号）、?（疑問符）、「=」（等号）。 • 5 つ以上の異なる文字を含める必要があります。 • 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は4つ、「ZYXW」は3つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約 4 ～ 6 回発生）、簡素化チェックに失敗します。 （注） 連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&!21 はパスワード チェックに失敗しますが、abcd&!25 は失敗しません。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[プライバシー パスワード（Privacy Password）] フィールド	このユーザのプライバシー パスワード。 FXOS では、次の要件を満たさないパスワードは拒否されます。 • 8 ～ 80 文字を含む。 • 含められるのは、文字、数字、および次の文字のみです。 ~`!@#%^&*()_-+{}[]\\:;"'<,>./ • 次の記号を含まない。$（ドル記号）、?（疑問符）、「=」（等号）。 • 5 つ以上の異なる文字を含める必要があります。 • 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は4つ、「ZYXW」は3つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約 4 ～ 6 回発生）、簡素化チェックに失敗します。 （注） 連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&!21 はパスワード チェックに失敗しますが、abcd&!25 は失敗しません。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 4 [OK] をクリックして [Add SNMP User] ダイアログボックスを閉じます。

ステップ 5 [保存（Save）] をクリックします。

SNMPv3 ユーザの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

ステップ 2 [SNMP Users] 領域で、削除するユーザに対応するテーブルの行の [Delete] アイコンをクリックします。

HTTPS の設定

ここでは、Firepower 4100/9300 シャーシ で HTTPS を設定する方法を説明します。

（注） Firepower Chassis Manager または FXOS CLI を使用して HTTPS ポートを変更できます。他の HTTPS の設定はすべて、FXOS CLI を使用してのみ設定できます。

証明書、キー リング、トラスト ポイント

HTTPS は、公開キー インフラストラクチャ（PKI）を使用してクライアントのブラウザと Firepower 4100/9300 シャーシ などの 2 つのデバイス間でセキュアな通信を確立します。

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。通常、長いキーは短いキーよりもより安全です。FXOS では最初に 2048 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキーリング証明書を手動で再生成する必要があります。

証明書

セキュアな通信を準備するには、まず2つのデバイスがそれぞれのデジタル証明書を交換します。証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。暗号化された通信をサポートするために、デバイスは独自のキーペアと独自の自己署名証明書を生成できます。リモートユーザが自己署名証明書を提示するデバイスに接続する場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。デフォルトでは、FXOSにはデフォルトのキーリングからの公開キーを含む組み込みの自己署名証明書が含まれます。

トラスト ポイント

FXOSに強力な認証を提供するために、デバイスのIDを証明する信頼できるソース（つまり、トラストポイント）からサードパーティ証明書を取得し、インストールできます。サードパー

ティ証明書は、発行元トラスト ポイント（ルート認証局（CA）、中間 CA、またはルート CA につながるトラスト チェーンの一部となるトラスト アンカーのいずれか）によって署名されます。新しい証明書を取得するには、FXOS で証明書要求を生成し、トラスト ポイントに要求を送信する必要があります。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

キー リングの作成

FXOS は、デフォルト キー リングを含め、最大 8 個のキー リングをサポートします。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 キー リングを作成し、名前を付けます。

Firepower-chassis # **create keyring** *keyring-name*

ステップ 3 SSL キーのビット長を設定します。

Firepower-chassis # **set modulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}

ステップ 4 トランザクションをコミットします。

Firepower-chassis # **commit-buffer**

例

次の例は、1024 ビットのキー サイズのキー リングを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

次のタスク

このキー リングの証明書要求を作成します。

デフォルト キー リングの再生成

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

（注） デフォルトのキーリングは、FXOS 上の FCM によってのみ使用されます。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 デフォルト キー リングでキー リング セキュリティ モードに入ります。

Firepower-chassis /security # **scope keyring default**

ステップ 3 デフォルト キー リングを再生成します。

Firepower-chassis /security/keyring # **set regenerate yes**

ステップ 4 トランザクションをコミットします。

Firepower-chassis # **commit-buffer**

例

次に、デフォルト キー リングを再生成する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

キー リングの証明書要求の作成

基本オプション付きのキー リングの証明書要求の作成

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 キー リングのコンフィギュレーション モードに入ります。

Firepower-chassis /security # **scope keyring** *keyring-name*

ステップ 3 指定された IPv4 または IPv6 アドレス、またはファブリック インターコネクトの名前を使用して証明書要求を作成します。証明書要求のパスワードを入力するように求められます。

Firepower-chassis /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] | **subject-name** *name*}

ステップ 4 トランザクションをコミットします。

Firepower-chassis /security/keyring/certreq # **commit-buffer**

ステップ 5 コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。

Firepower-chassis /security/keyring # **show certreq**

例

次の例では、基本オプション付きのキー リングについて IPv4 アドレスで証明書要求を作成して表示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name
sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #
```

次のタスク

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キーリングの証明書を取得するため、証明書要求を含むファイルをトラストアンカーまたは認証局に送信します。
- トラスト ポイントを作成し、トラスト アンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

詳細オプション付きのキー リングの証明書要求の作成

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 キー リングのコンフィギュレーション モードに入ります。

Firepower-chassis /security # **scope keyring** *keyring-name*

ステップ 3 証明書要求を作成します。

Firepower-chassis /security/keyring # **create certreq**

ステップ 4 会社が存在している国の国コードを指定します。

Firepower-chassis /security/keyring/certreq* # **set country** *country name*

ステップ 5 要求に関連付けられたドメイン ネーム サーバ（DNS）アドレスを指定します。

Firepower-chassis /security/keyring/certreq* # **set dns** *DNS Name*

ステップ 6 証明書要求に関連付けられた電子メール アドレスを指定します。

Firepower-chassis /security/keyring/certreq* # **set e-mail** *E-mail name*

ステップ 7 Firepower 4100/9300 シャーシの IP アドレスを指定します。

Firepower-chassis /security/keyring/certreq* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }

ステップ 8 証明書を要求している会社の本社が存在する市または町を指定します。

Firepower-chassis /security/keyring/certreq* # **set locality** *locality name (eg, city)*

ステップ 9 証明書を要求している組織を指定します。

Firepower-chassis /security/keyring/certreq* # **set org-name** *organization name*

ステップ 10 組織ユニットを指定します。

Firepower-chassis /security/keyring/certreq* # **set org-unit-name** *organizational unit name*

ステップ 11 証明書要求に関するオプションのパスワードを指定します。

Firepower-chassis /security/keyring/certreq* # **set password** *certificate request password*

ステップ 12 証明書を要求している会社の本社が存在する州または行政区分を指定します。

Firepower-chassis /security/keyring/certreq* # **set state** *state, province or county*

ステップ 13 Firepower 4100/9300 シャーシ の完全修飾ドメイン名を指定します。

Firepower-chassis /security/keyring/certreq* # **set subject-name** *certificate request name*

ステップ 14 トランザクションをコミットします。

Firepower-chassis /security/keyring/certreq # **commit-buffer**

ステップ 15 コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。

Firepower-chassis /security/keyring # **show certreq**

例

（注） 2.7 より前のリリースでは、「set dns」または「set subject-name」で FQDN を使用せずにバッファをコミットすることはお勧めできません。FQDN ではない DNS またはサブジェクト名を使用して認証要件を作成しようとすると、エラーがスローされます。

次の例では、詳細オプション付きのキー リングについてIPv4アドレスで証明書要求を作成して表示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* #  set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
```

```
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #
```

次のタスク

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キーリングの証明書を取得するため、証明書要求を含むファイルをトラストアンカーまたは認証局に送信します。
- トラスト ポイントを作成し、トラスト アンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

トラスト ポイントの作成

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 トラストポイントを作成します。

Firepower-chassis /security # **create trustpoint** *name*

ステップ 3 このトラスト ポイントの証明書情報を指定します。

Firepower-chassis /security/trustpoint # **set certchain** [*certchain*]

コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パスを定義するトラスト ポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、**ENDOFBUF** と入力して終了します。

重要　　証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ステップ 4 トランザクションをコミットします。

Firepower-chassis /security/trustpoint # **commit-buffer**

例

次の例は、トラスト ポイントを作成し、トラスト ポイントに証明書を提供します。

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

次のタスク

トラスト アンカーまたは認証局からキー リング証明書を取得し、キー リングにインポートします。

キー リングへの証明書のインポート

始める前に

- キー リング証明書の証明書チェーンを含むトラスト ポイントを設定します。
- トラスト アンカーまたは認証局からキー リング証明書を取得します。

（注） HTTPS ですでに設定されているキーリングの証明書を変更する場合は、新しい証明書を有効にするためにHTTPSを再起動する必要があります。詳細については、HTTPS の再起動 （145 ページ） を参照してください。

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 証明書を受け取るキー リングでコンフィギュレーション モードに入ります。

Firepower-chassis /security # **scope keyring** *keyring-name*

ステップ 3 キー リング証明書の取得元のトラスト アンカーまたは認証局に対しトラスト ポイントを指定します。

Firepower-chassis /security/keyring # **set trustpoint** *name*

ステップ 4 キー リング証明書を入力してアップロードするためのダイアログを起動します。

Firepower-chassis /security/keyring # **set cert**

プロンプトで、トラストアンカーまたは認証局から受け取った証明書のテキストを貼り付けます。証明書の後の行に **ENDOFBUF** と入力して、証明書の入力を完了します。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ステップ 5 トランザクションをコミットします。

Firepower-chassis /security/keyring # **commit-buffer**

例

次に、トラストポイントを指定し、証明書をキー リングにインポートする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

次のタスク

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

注意 HTTPS で使用するポートとキーリングの変更を含め、HTTPS の設定を完了した後、トランザクションを保存またはコミットするとすぐに、現在のすべての HTTP および HTTPS セッションは警告なく閉じられます。

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

ステップ 2 システム サービス モードを開始します。

Firepower-chassis /system # **scope services**

ステップ 3 HTTPS サービスを有効にします。

Firepower-chassis /system/services # **enable https**

ステップ 4 （任意） HTTPS 接続で使用されるポートを指定します。

Firepower-chassis /system/services # **set https port** *port-num*

ステップ 5 （任意） HTTPS に対して作成したキー リングの名前を指定します。

Firepower-chassis /system/services # **set https keyring** *keyring-name*

ステップ 6 （任意） ドメインで使用される暗号スイート セキュリティのレベルを指定します。

Firepower-chassis /system/services # **set https cipher-suite-mode** *cipher-suite-mode*

cipher-suite-mode には、以下のいずれかのキーワードを指定できます。

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom**：ユーザ定義の暗号スイート仕様の文字列を指定できます。

ステップ 7 （任意） **cipher-suite-mode** が **custom** に設定されている場合は、ドメインに対してカスタム レベルの暗号スイート セキュリティを指定します。

Firepower-chassis /system/services # **set https cipher-suite** *cipher-suite-spec-string*

cipher-suite-spec-string は最大 256 文字で構成できます。これは OpenSSL 暗号スイート仕様に準拠する必要があります。次を除き、スペースや特殊文字は使用できません。！（感嘆符）、+（プラス記号）、-（ハイフン）、および :（コロン）。詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite を参照してください。

たとえば、FXOS がデフォルトとして使用する中強度仕様の文字列は次のようになります。
ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

（注） **cipher-suite-mode** は **custom** 以外に設定されている場合、このオプションは無視されます。

ステップ 8 トランザクションをシステム設定にコミットします。

Firepower-chassis /system/services # **commit-buffer**

例

次の例では、HTTPS をイネーブルにし、ポート番号を 443 に設定し、キーリング名を kring7984 に設定し、暗号スイートのセキュリティ レベルを [high] に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

HTTPS ポートの変更

HTTPS サービスは、デフォルトでポート 443 で有効化になります。HTTPS をディセーブルにすることはできませんが、HTTPS 接続に使用するポートは変更できます。

手順

ステップ 1 [Platform Settings] > [HTTPS] > を選択します。

ステップ 2 HTTPS 接続に使用するポートを [Port] フィールドに入力します。1 ～ 65535 の範囲内の整数を指定します。このサービスは、デフォルトではポート 443 で有効になっています。

ステップ 3 [Save] をクリックします。

シャーシが指定した HTTPS ポートで設定されます。

HTTPS ポートを変更した後に、現在のすべての HTTPS セッションが閉じられます。ユーザは、次のように新しいポートを使用して再度 Firepower Chassis Manager にログインする必要があります。

https://*<chassis_mgmt_ip_address>*:*<chassis_mgmt_port>*

<*chassis_mgmt_ip_address*> は、初期設定時に入力したシャーシの IP アドレスまたはホスト名で、<*chassis_mgmt_port*> は設定が完了した HTTPS ポートです。

HTTPS の再起動

HTTPS ですでに設定されているキーリングの証明書を変更する場合は、新しい証明書を有効にするためにHTTPSを再起動する必要があります。更新されたキーリングでHTTPSを再設定するには、次の手順を使用します。

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

ステップ 2 システム サービス モードを開始します。

Firepower-chassis /system # **scope services**

ステップ 3 HTTPS キーリングをデフォルト値に戻します。

Firepower-chassis /system/services # **set https keyring default**

ステップ 4 トランザクションをシステム設定にコミットします。

Firepower-chassis /system/services # **commit-buffer**

ステップ 5 5 秒間待機します。

ステップ 6 作成したキーリングで HTTPS を設定します。

Firepower-chassis /system/services # **set https keyring** *keyring-name*

ステップ 7 トランザクションをシステム設定にコミットします。

Firepower-chassis /system/services # **commit-buffer**

キーリングの削除

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 名前付きのキー リングを削除します。

Firepower-chassis /security # **delete keyring** *name*

ステップ 3 トランザクションをコミットします。

Firepower-chassis /security # **commit-buffer**

例

次の例では、キー リングを削除します。

```
Firepower-chassis# scope security
Firepower-chassis /security # delete keyring key10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

トラスト ポイントの削除

始める前に

トラスト ポイントがキー リングによって使用されていないことを確認してください。

手順

ステップ 1 セキュリティ モードに入ります。

Firepower-chassis# **scope security**

ステップ 2 指定したトラスト ポイントを削除します。

Firepower-chassis /security # **delete trustpoint** *name*

ステップ 3 トランザクションをコミットします。

Firepower-chassis /security # **commit-buffer**

例

次に、トラスト ポイントを削除する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # delete trustpoint tPoint10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

HTTPS の無効化

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

ステップ 2 システム サービス モードを開始します。

Firepower-chassis /system # **scope services**

ステップ 3 HTTPS サービスを無効にします。

Firepower-chassis /system/services # **disable https**

ステップ 4 トランザクションをシステム設定にコミットします。

Firepower-chassis /system/services # **commit-buffer**

例

次に、HTTPS を無効にし、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # disable https
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

AAA の設定

ここでは、認証、許可、およびアカウンティングについて説明します。詳細については、次のトピックを参照してください。

AAA について

認証、許可、およびアカウンティング（AAA）は、ネットワークリソースへのアクセス制御、ポリシーの強化、使用状況の評価、およびサービスの課金に必要な情報提供を行う一連のサービスです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実装します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

認証

認証はユーザを識別する方法です。通常、ユーザが有効なユーザ名と有効なパスワードを入力すると、アクセスが許可されます。AAA サーバは、ユーザが入力したログイン情報とデータベースに保存されているユーザのログイン情報を比較します。ログイン情報が一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

シャーシへの管理接続を認証するように Firepower 4100/9300 シャーシ を設定できます。これには、次のセッションが含まれます。

- HTTPS
- SSH
- シリアル コンソール

認可

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザは認証後にさまざまなタイプのアクセスやアクティビティを許可される可能性があります。

アカウンティング

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証は、単独で使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

サポートされている認証タイプ

FXOS は次の認証タイプをサポートします。

- [Remote]：次のネットワーク AAA サービスがサポートされています。
  - LDAP
  - RADIUS
  - TACACS+
- [ローカル（Local）]：シャーシは、ユーザープロファイルを取り込むことができるローカルデータベースを維持します。 AAA サーバの代わりに、このローカルデータベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

ユーザ ロール

FXOS は、ユーザロール割り当ての形式でローカルおよびリモート認証をサポートします。割り当てることができるロールは次のとおりです。

- [Admin]：システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。
- [AAA Administrator]：ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
- [Operations]：NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ（syslog サーバとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
- [Read-Only]：システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

ローカル ユーザとロールの割り当ての詳細については、「ユーザ管理 （45 ページ）」を参照してください。

AAA の設定

Firepower 4100/9300 アプライアンスで認証、許可、アカウンティング（AAA）を設定するための基本的な手順の概要を紹介します。

1. ユーザ認証の目的タイプを設定します。
   - [Local]：ユーザ定義とローカル認証は ユーザ管理 （45 ページ） の一部です。
   - [Remote]：リモート AAA サーバ アクセスの設定は、[Platform Settings] の一部です。具体的には次のとおりです。
     - LDAP プロバイダーの設定 （150 ページ）
     - RADIUS プロバイダーの設定 （154 ページ）
     - TACACS+ プロバイダーの設定 （157 ページ）

（注） リモート AAA サーバーを使用する場合は、シャーシでリモート AAA サーバーアクセスを設定する前に、リモートサーバーで AAA サービスを有効にして設定する必要があります。

2. デフォルトの認証方式を指定します。これも ユーザ管理 （45 ページ） の一部です。

（注） デフォルトの認証とコンソール認証の両方が同じリモート認証プロトコル（RADIUS、TACACS+、または LDAP）を使用するように設定されている場合、そのサーバの設定の特定の側面を変更することは（たとえば、サーバの削除や、割り当ての順序の変更）、これらのユーザ設定を更新することなしではできません。

LDAP プロバイダーの設定

LDAP プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、FXOS でその設定が使用され、デフォルト設定は無視されます。

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで FXOS にバインドするユーザアカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [LDAP] タブをクリックします。

ステップ 3 [プロパティ（Properties）] 領域で、次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力します。デフォルト値は 30 秒です。このプロパティは必須です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザレコードで、この属性と一致する値を検索します。 LDAP プロバイダーのプロパティを設定する場合は `shell:roles="admin,aaa"` 属性値が必要であることに注意してください。

名前	説明
[Base DN] フィールド	リモート ユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から *cn=$userid* の長さを引いた長さに設定することができます。$userid により、LDAP 認証を使用してシャーシにアクセスしようとするリモートユーザーが識別されます。 このプロパティは、LDAP プロバイダーに必要です。このタブでベース DN を指定しない場合、定義する LDAP プロバイダーごとに 1 つずつ指定する必要があります。
[Filter] フィールド	LDAP サーバで使用するフィルタ属性を入力します（*cn = $userid*、*sAMAccountName = $userid* など）。LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。フィルタには *$userid* が含まれている必要があります。 このプロパティは必須です。このタブでフィルタを指定しない場合は、定義する LDAP プロバイダーごとにフィルタを指定する必要があります。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

次の手順に従い、LDAP プロバイダー（このアプライアンスに LDAP ベースの AAA サービスを提供する特定のリモートサーバー）を定義および設定します。

（注） FXOS では、最大 16 の LDAP プロバイダーをサポートします。

始める前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで FXOS にバインドするユーザアカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [AAA]** を選択します。

ステップ 2 [LDAP] タブをクリックします。

ステップ 3 追加する LDAP プロバイダーごとに、次の手順を実行します。

a) [LDAP プロバイダー（LDAP Providers）] 領域で、[追加（Add）] をクリックします。

b) [LDAP プロバイダーの追加（Add LDAP Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Hostname/FQDN (または IP アドレス)] フィールド	LDAP サーバのホスト名および IP アドレス。SSL がイネーブルの場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名（CN）と正確に一致している必要があります。
[Order] フィールド	FXOS でこのプロバイダーをユーザの認証に使用する順序。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を FXOS で自動的に割り当てるには、**lowest-available** または **0**（ゼロ）を入力します。
[Bind DN] フィールド	ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 255 文字（ASCII）です。
[Base DN] フィールド	リモートユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字 + CN=$userid の長さに設定することができます。$userid により、LDAP 認証を使用して Firepower Chassis Manager または FXOS CLI にアクセスしようとするリモート ユーザが識別されます。 デフォルトのベース DN が [LDAP] タブで設定されていない場合は、この値が必要です。
[Port] フィールド	Firepower Chassis Manager または FXOS CLI が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。

名前	説明
[Enable SSL] チェックボックス	このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。このチェックボックスをオフにすると、認証情報はクリアテキストで送信されます。 LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。 （注） STARTTLS 操作では、LDAP プロバイダーの CA 証明書が FXOS 証明書チェーンにインストールされている必要があります。
[Filter] フィールド	LDAP サーバで使用するフィルタ属性を入力します（*cn = $userid*、*sAMAccountName = $userid* など）。LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。フィルタには *$userid* が含まれている必要があります。 デフォルトのフィルタが [LDAP] タブで設定されていない場合は、この値が必要です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 デフォルトの属性が [LDAP] タブで設定されていない場合は、この値が必要です。
[Key] フィールド	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Key] フィールド	確認のための LDAP データベースパスワードの再入力。
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [LDAP] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 30 秒です。

名前	説明
[Vendor] フィールド	この選択により、LDAP プロバイダーやサーバの詳細を提供するベンダーが識別されます。 • LDAP プロバイダーが Microsoft Active Directory の場合は、[MS AD] を選択します。 • LDAP プロバイダーが Microsoft Active Directory でない場合は、[Open LDAP] を選択します。 デフォルトは [Open LDAP] です。

c) [OK] をクリックして [LDAP プロバイダーの追加（Add LDAP Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 （任意）証明書失効リスト検査を有効にします。

Firepower-chassis /security/ldap/server # **set revoke-policy** *{strict | relaxed}*

（注） この設定は、SSL 接続が使用可能である場合にのみ有効です。

LDAP プロバイダーの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [LDAP] タブをクリックします。

ステップ 3 [LDAP プロバイダー（LDAP Providers）] 領域で、削除する LDAP プロバイダーに対応するテーブルの行にある [削除（Delete）] アイコンをクリックします。

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、FXOS でその設定が使用され、このデフォルト設定は無視されます。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 [プロパティ（Properties）] 領域で、次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	RADIUS データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力します。デフォルト値は 5 秒です。 このプロパティは必須です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

次の手順に従い、RADIUS プロバイダー（このアプライアンスに RADIUS ベースの AAA サービスを提供する特定のリモートサーバー）を定義および設定します。

（注） FXOS では、最大 16 の RADIUS プロバイダーをサポートします。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 追加する RADIUS プロバイダーごとに、次の手順を実行します。

a) [RADIUS プロバイダー（RADIUS Providers）] 領域で、[追加（Add）] をクリックします。

b) [RADIUS プロバイダーの追加（Add RADIUS Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Hostname/FQDN (または IP アドレス)] フィールド	RADIUS サーバのホスト名または IP アドレス。

名前	説明
[Order] フィールド	FXOS でこのプロバイダーをユーザの認証に使用する順序。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を FXOS で自動的に割り当てるには、**lowest-available** または **0**（ゼロ）を入力します。
[Key] フィールド	データベースの SSL 暗号キー。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Authorization Port] フィールド	Firepower Chassis Manager または FXOS CLI が RADIUS データベースと通信するために使用されるポート。有効な範囲は 1 ～ 65535 です。標準ポート番号は 1700 です。
[Timeout] フィールド	RADIUS データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [RADIUS] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 5 秒です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。 必要に応じて、0 ～ 5 の整数を入力します。値を指定しない場合、Firepower Chassis Manager は [RADIUS] タブに指定した値を使用します。

c) [OK] をクリックして [RADIUS プロバイダーの追加（Add RADIUS Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

RADIUS プロバイダーの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 [RADIUS プロバイダー（RADIUS Providers）] 領域で、削除する RADIUS プロバイダーに対応するテーブルの行にある [削除（Delete）] アイコンをクリックします。

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定になります。個々のプロバイダーの設定にいずれかのプロパティの設定が含まれている場合、FXOS でその設定が使用され、このデフォルト設定は無視されます。

（注） FXOS シャーシは、Terminal Access Controller Access-Control System Plus（TACACS+）プロトコルのコマンドアカウンティングをサポートしていません。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 [プロパティ（Properties）] 領域で、次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	TACACS+ データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力します。デフォルト値は 5 秒です。 このプロパティは必須です。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

次の手順に従い、TACACS+ プロバイダー（このアプライアンスに TACACS+ ベースの AAA サービスを提供する特定のリモートサーバー）を定義および設定します。

（注） FXOS では、最大 16 の TACACS+ プロバイダーをサポートします。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 追加する TACACS+ プロバイダーごとに、次の手順を実行します。

a) [TACACS プロバイダー（TACACS Providers）] 領域で、[追加（Add）] をクリックします。

b) [TACACS プロバイダーの追加（Add TACACS Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Hostname/FQDN (または IP アドレス)] フィールド	TACACS+ サーバのホスト名または IP アドレス。
[Order] フィールド	FXOS でこのプロバイダーをユーザの認証に使用する順序。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を FXOS で自動的に割り当てるには、**`lowest-available`** または **`0`**（ゼロ）を入力します。
[Key] フィールド	データベースの SSL 暗号キー。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Port] フィールド	Firepower Chassis Manager または FXOS CLI が TACACS+ サーバと通信するために使用するポート。 1 ～ 65535 の整数を入力します。デフォルト ポートは 49 です。
[Timeout] フィールド	TACACS+ データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [TACACS+] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 5 秒です。

c) [OK] をクリックして [TACACS プロバイダーの追加（Add TACACS Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

TACACS+ プロバイダーの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [AAA]** を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 [TACACS プロバイダー（TACACS Providers）] 領域で、削除する TACACS+ プロバイダーに対応するテーブルの行にある [削除（Delete）] アイコンをクリックします。

Syslog の設定

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。syslogサービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログ用の保護された長期ストレージを提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

手順

ステップ 1 [Platform Settings] > [Syslog] > を選択します。

ステップ 2 ローカル宛先を設定します。

a) [Local Destinations] タブをクリックします。

b) [ローカル宛先（Local Destinations）] タブで、次のフィールドに入力します。

名前	説明
[コンソール（Console）] セクション	
[管理状態（Administrative State）] フィールド	シャーシがコンソールに syslog メッセージを表示するかどうかを指定します。 ログに追加するとともに、コンソールに syslog メッセージを表示する場合は、[有効化（Enable）] チェックボックスをオンにします。[有効化（Enable）] チェックボックスをオフにすると、syslogメッセージはログに追加されますが、コンソールに表示されません。

名前	説明
[レベル（Level）] フィールド	[コンソール（Console）] > [管理状態（Admin State）] で [有効化（Enable）] チェックボックスをオンにした場合は、コンソールに表示する最低のメッセージ レベルを選択します。シャーシのコンソールにはそのレベル以上のメッセージが表示されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]**
[モニタ（Monitor）] セクション	
[管理状態（Administrative State）] フィールド	シャーシがモニタに syslog メッセージを表示するかどうかを指定します。 syslog メッセージをログに追加するとともに、モニタに表示する場合は、[有効化（Enable）] チェックボックスをオンにします。[有効化（Enable）] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、モニタに表示されません。
[レベル（Level）] ドロップダウン リスト	[モニタ（Monitor）] > [管理状態（Admin State）] で [有効化（Enable）] チェックボックスをオンにした場合は、モニタに表示する最低のメッセージ レベルを選択します。モニタにはそのレベル以上のメッセージが表示されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**

c) [Save] をクリックします。

ステップ 3 リモート宛先を設定します。

a) [リモート宛先（Remote Destinations）] タブをクリックします。

b) [リモート接続先（Remote Destinations）] 領域で、シャーシによって生成されたメッセージを保存できる最大 3 個の外部ログの次のフィールドに入力します。

syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギングデータを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

名前	説明
[Admin State] フィールド	リモート ログ ファイルに syslog メッセージを保存する場合は、[有効（Enable）]チェックボックスをオンにします。
[レベル（Level）] ドロップダウン リスト	システムに保存するメッセージの最低レベルを選択します。そのレベル以上のメッセージがリモート ファイルに保存されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**
[ホスト名/IP アドレス（Hostname/IP Address）] フィールド	リモート ログ ファイルが存在するホスト名または IP アドレス。 （注） IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

名前	説明
[ファシリティ（Facility）] ドロップダウン リスト	ファイル メッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。次のいずれかになります。 • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **local7**

c) [Save] をクリックします。

ステップ 4 ローカル送信元を設定します。

a) [Local Sources] タブをクリックします。

b) [ローカル送信元（Local Sources）] タブで、次のフィールドに入力します。

名前	説明
[障害管理状態（Faults Admin State）] フィールド	システム障害ロギングを有効化するかどうか。[有効化（Enable）]チェックボックスをオンにすると、シャーシはすべてのシステム障害をログに記録します。
[監査管理状態（Audits Admin State）] フィールド	監査ロギングを有効化するかどうか。[有効化（Enable）] チェックボックスをオンにすると、シャーシはすべての監査ログイベントをログに記録します。
[イベント管理状態（Events Admin State）] フィールド	システム イベント ロギングを有効化するかどうか。[有効化（Enable）]チェックボックスをオンにすると、シャーシはすべてのシステムイベントをログに記録します。

c) [保存（Save）] をクリックします。

DNS サーバの設定

システムでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバを指定する必要があります。たとえば、DNS サーバーを設定していない場合は、シャーシに関する設定を行うときに、www.cisco.com などの名前を使用できません。サーバの IP アドレスを使用する必要があり

ます。これには、IPv4 または IPv6 アドレスのいずれかを使用できます。最大 4 台の DNS サーバを設定できます。

（注） 複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。ローカル管理コマンドが DNS サーバの検索を必要とする場合、3 台の DNS サーバのみをランダムに検索します。

手順

ステップ 1 [Platform Settings] > [DNS] > を選択します。

ステップ 2 [Enable DNS Server] チェックボックスをオンにします。

ステップ 3 追加する DNS サーバ（最大 4 台）ごとに、それぞれの IP アドレスを [DNS Server） フィールドに入力し、[Add] をクリックします。

ステップ 4 [Save] をクリックします。

FIPS モードの有効化

Firepower 4100/9300 シャーシで FIPS モードを有効にするには、次の手順を実行します。

手順

ステップ 1 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。

ステップ 2 **Platform Settings** を選択して、[Platform Settings] ウィンドウを開きます。

ステップ 3 **FIPS/CC mode** を選択して、[FIPS and Common Criteria] ウィンドウを開きます。

ステップ 4 FIPS の **Enable** チェックボックスをオンにします。

ステップ 5 **Save** をクリックして、設定を保存します。

ステップ 6 プロンプトに従ってシステムをリブートします。

FIPS モードが有効になっている場合は、許可されるキーサイズとアルゴリズムが制限されます。MIO は、CiscoSSL と FIPS オブジェクトモジュール（FOM）を使用して暗号化を行います。これにより、ASA 独自の暗号化ライブラリの実装および HW アクセラレーションと比較して、FIPS の検証が容易になります。

次のタスク

FXOS リリース 2.0.1 より以前は、デバイスの最初の設定時に作成した SSH ホスト キーが 1024 ビットにハード コードされていました。FIPS およびコモンクライテリア認定要件に準拠する

には、この古いホストキーを破棄し、「SSH ホスト キーの生成」で詳細を説明する手順を使用して新しいホストキーを生成する必要があります。これらの追加手順を実行しないと、FIPS モードを有効にしてデバイスをリブートした後に、SSH を使用してスーパバイザに接続できなくなります。FXOS 2.0.1 以降を使用して初期設定を行った場合は、新しいホスト キーを生成する必要はありません。

コモン クライテリア モードの有効化

Firepower 4100/9300 シャーシ上でコモン クライテリア モードを有効にするには、次の手順を実行します。

手順

ステップ 1 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。
ステップ 2 **Platform Settings** を選択して、[Platform Settings] ウィンドウを開きます。
ステップ 3 **FIPS/CC mode** を選択して、[FIPS and Common Criteria] ウィンドウを開きます。
ステップ 4 コモン クライテリアの **Enable** チェックボックスをオンにします。
ステップ 5 **Save** をクリックして、設定を保存します。
ステップ 6 プロンプトに従ってシステムをリブートします。

コモンクライテリア（CC）はコンピュータセキュリティ向け国際基準です。CCは、証明書、監査、ロギング、パスワード、TLS、SSH などに重点を置いています。基本的に FIPS 準拠を前提としています。FIPS と同様に、シスコは、NIST 認定ラボベンダーと契約してテストと NIAP への提出を行っています。

CC モードを有効にすると、サポートする必要があるアルゴリズム、暗号スイート、および機能のリストが制限されます。MIO は、Network Device Collaborative Protection Profile（NDcPP）に対して評価されます。CiscoSSL は、ほとんどがCC コンプライアンスガイドに記載されている要件の一部のみを適用できます。

次のタスク

FXOS リリース 2.0.1 より以前は、デバイスの最初の設定時に作成した SSH ホスト キーが 1024 ビットにハード コードされていました。FIPS およびコモンクライテリア認定要件に準拠するには、この古いホストキーを破棄し、「SSH ホスト キーの生成」で詳細を説明する手順を使用して新しいホストキーを生成する必要があります。これらの追加手順を実行しないと、コモン クライテリア モードを有効にしてデバイスをリブートした後に、SSH を使用してスーパバイザに接続できなくなります。FXOS 2.0.1 以降を使用して初期設定を行った場合は、新しいホスト キーを生成する必要はありません。

IP アクセスリストの設定

デフォルトでは、Firepower 4100/9300 シャーシはローカル Web サーバへのすべてのアクセスを拒否します。IP アクセスリストを、各 IP ブロックの許可されるサービスのリストを使用して設定する必要があります。

IP アクセスリストは、次のプロトコルをサポートします。

- HTTPS
- SNMP
- SSH

IP アドレス（v4 または v6）の各ブロックで、最大 100 個の異なるサブネットを各サービスに対して設定できます。サブネットを 0、プレフィックスを 0 と指定すると、サービスに無制限にアクセスできるようになります。

手順

ステップ 1 Firepower 4100/9300 シャーシ に管理者ユーザとしてログインします。

ステップ 2 **Platform Settings** を選択し、[プラットフォーム設定（Platform Settings）] ページを開きます。

ステップ 3 **Access List** を選択し、[アクセスリスト（Access List）] 領域を開きます。

ステップ 4 この領域で、[IPアクセスリスト（IP Access List）] にリストされている IPv4 および IPv6 アドレスを表示、追加、削除できます。

IPv4 ブロックを追加するには、有効な IPv4 IP アドレスとプレフィックスの長さ（0 ～ 32）を入力し、プロトコルを選択する必要があります。

IPv6 ブロックを追加するには、有効な IPv6 IP アドレスとプレフィックスの長さ（0 ～ 128）を入力し、プロトコルを選択する必要があります。

MAC プール プレフィックスの追加とコンテナ インスタンス インターフェイスの MAC アドレスの表示

FXOS 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の MAC アドレスを使用するように、コンテナ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。FXOS 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。

A2*xx.yyzz.zzzz*

xx.yy はユーザ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。

詳細については、「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（219 ページ）」を参照してください。

この手順では、MAC アドレスの表示方法と生成で使用されるプレフィックスのオプションの定義方法について説明します。

（注） 論理デバイスの展開後に MAC アドレスのプレフィックスを変更すると、トラフィックが中断される可能性があります。

手順

ステップ 1 **[Platform Settings]** > **[Mac Pool]** を選択します。

このページには、MAC アドレスを使用したコンテナ インスタンスやインターフェイスとともに生成された MAC アドレスが表示されます。

ステップ 2 （任意）MAC アドレスの生成時に使用される MAC アドレスのプレフィックスを追加します。

a) [プレフィックスの追加（Add Prefix）] をクリックします。

[Set the Prefix for the MAC Pool] ダイアログ ボックスが表示されます。

a) 1 ～ 65535 の 10 進数を入力します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、シャーシは 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シ ネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D.00***zz.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。

A2**F1.03***zz.zzzz*

b) [OK] をクリックします。

プレフィックスを使用して新しい MAC アドレスが生成され、割り当てられます。現在のプレフィックスと生成される 16 進数はテーブルの上に表示されます。

コンテナインスタンスにリソースプロファイルを追加

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

- コアの最小数は 6 です。

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

- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、セキュリティモジュール/シャーシモデルによって異なります。「コンテナインスタンスの要件と前提条件 （229 ページ）」を参照してください。

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

使用中のリソースプロファイルの設定を変更することはできません。そのリソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。確立されたハイ アベイラビリティ ペアまたはクラスタ内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

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

手順

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

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

ステップ 2 次のパラメータを設定します。

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

ステップ 3 [OK] をクリックします。

ネットワーク制御ポリシーの設定

他社製デバイスのディスカバリを許可するために、FXOS は、IEEE 802.1ab 規格で定義されているベンダーニュートラルなデバイス ディスカバリ プロトコルである *Link Layer Discovery Protocol*（*LLDP*）をサポートしています。LLDP を使用すると、ネットワークデバイスはネットワーデバイスに関する情報を、ネットワーク上の他のデバイスにアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信する単一方向のプロトコルです。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

To enable this functionality on your FXOS chassis, you can configure a network control policy, which specifies LLDP transmission and receiving behavior. ネットワーク制御ポリシーを作成した後、インターフェイスに割り当てる必要があります。固定ポート、EPM ポート、ポートチャネル、およびブレイクアウトポートなどの任意の前面インターフェイスでLLDP を有効にできます。

（注）
- LLDP is not configurable on dedicated management ports.
- ブレードに接続する内部バックプレーンポートではデフォルトでLLDPが有効になっています。無効にするオプションはありません。他のすべてのポートでは、LLDPはデフォルトで無効になっています。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [ネットワーク制御ポリシー（Network Control Policy）]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [ネットワーク制御ポリシー（Network Control Policy）] ダイアログボックスで、次のフィールドを編集します。

名前	説明
[Name] フィールド	ネットワーク制御ポリシーの一意の名前。
[LLDP受信（LLDP receive）] チェックボックス	FXOS が LLDP パケットを受信できるようにします。
[LLDP transmit] チェックボックス	FXOS が LLDP パケットを送信できるようにします。
[Description] フィールド	ネットワーク制御ポリシーの説明。

ステップ 4 **[保存（Save）]** をクリックします。After creating the Network Control Policy, you must assign it to an interface. ネットワーク制御ポリシーでインターフェイスを編集および設定する手順については、「物理インターフェイスの設定 （195 ページ）」を参照してください。

シャーシ URL の設定

管理 URL を指定して、FMC から直接、FTD インスタンスの Firepower Chassis Manager を簡単に開くことができます。シャーシ管理 URL を指定しない場合には、代わりにシャーシ名が使用されます。

FTD インスタンスを FMC に追加した後にシャーシ URL 設定を変更する場合は、**[Devices]** > **[Device Management]** > **[Device]** > **[System]** > **[Inventory]** ダイアログボックスで各ユニットのインベントリを更新します。

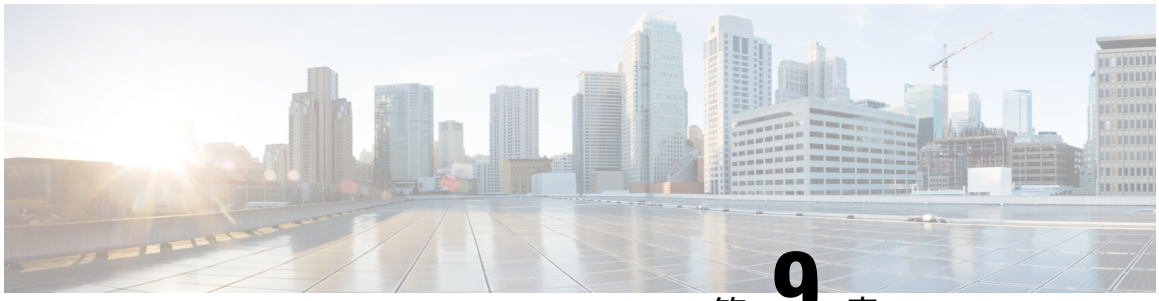
手順

ステップ 1 **[Platform Settings]** > **[Chassis URL]** を選択します。

ステップ 2 次のパラメータを設定します。

- [Chassis Name]：シャーシの名前を 1 ～ 60 文字で設定します。
- [シャーシURL（Chassis URL）]：Firepower Chassis Manager 内で FMC が FTD インスタンスに接続するために使用する URL を設定します。URL は https:// で始まる必要があります。シャーシ管理 URL を指定しない場合、代わりにシャーシ名が使用されます。

ステップ 3 [更新（Update）] をクリックします。



第 9 章

インターフェイス管理

インターフェイスについて

Firepower 4100/9300 シャーシ は、物理インターフェイス、コンテナ インスタンス用の VLAN サブインターフェイス、およびEtherChannel（ポート チャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager によって、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定にする必要があります。管理 IP アドレスの変更 （94 ページ）も参照してください。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

物理インターフェイス、コンテナインスタンスの VLAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス（FTDFMC 専用）で共有できます。 各コンテナ インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、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、パッシブインターフェイス、クラスタ、またはフェールオーバーリンクではサポートされません。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。アプリケーションと管理によっては、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。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： FMC デバイスを使用した FTD のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。詳細については、管理センター構成ガイドを参照してください。Eventing インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェ

イスを共有する他の倫理デバイスと通信することはできません。後で管理用のデータインターフェイスを設定する場合は、別のイベントインターフェイスを使用できません。

（注） 各アプリケーション インスタンスのインストール時に、仮想イーサネット インターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。マルチインスタンスクラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用でできるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。FDM および CDO はクラスタリングをサポートしていません。

（注） この章では、*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 （175 ページ）を参照してください。

スタンドアロン展開とクラスタ展開での FTD および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 *11* : インターフェイスタイプのサポート

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
FTD	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	対応	—	—
	スタンドアロン コンテナ インスタンス	対応	対応	対応	対応	対応	対応	—	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	—
	クラスタ コンテナ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	対応
ASA	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	—	対応	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	—	対応	—

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

Firepower 4100/9300 は、物理インターフェイス、コンテナインスタンスの VLAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

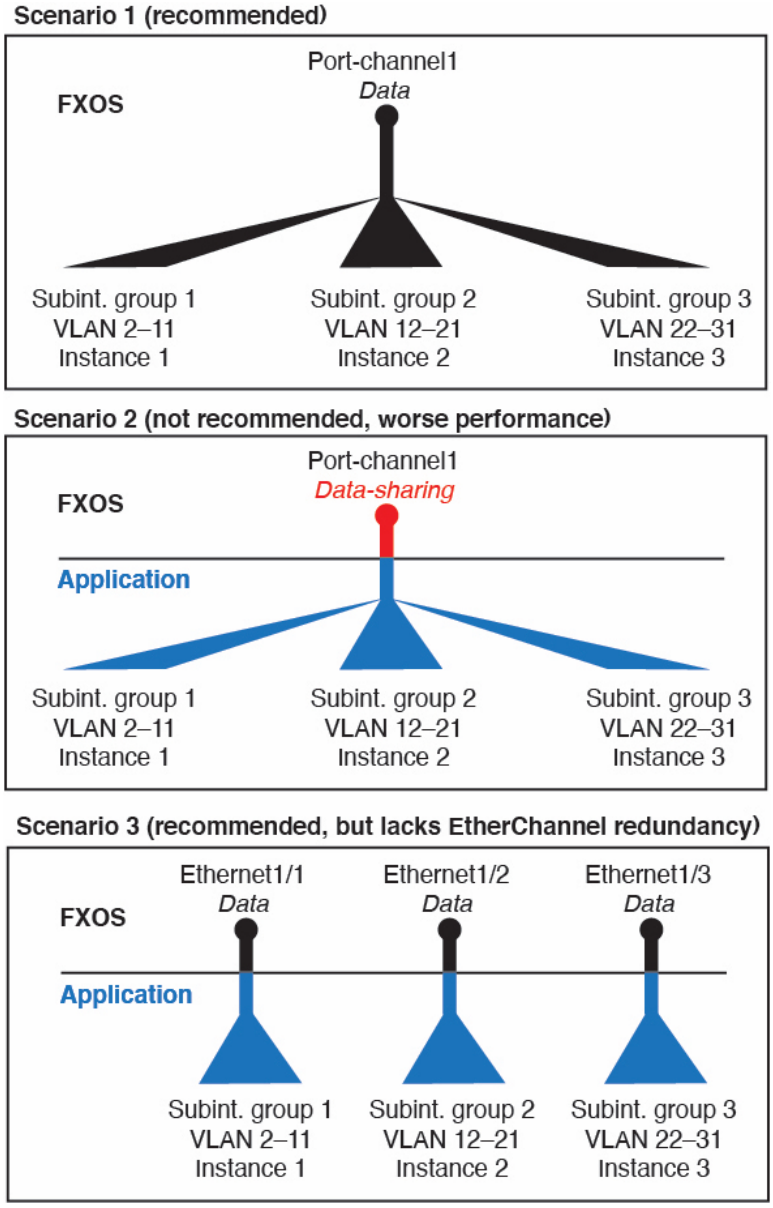
続くセクションでは、インターフェイスの FXOS とアプリケーション間の連携について説明します。

VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

スタンドアロンモードのコンテナインスタンスの場合のみ、FXOS で（FXOS サブインターフェイスのないインターフェイス上に）VLAN サブインターフェイスを作成することもできます。マルチインスタンスクラスタは、クラスタタイプのインターフェイスを除いて、FXOS のサブインターフェイスをサポートしません。アプリケーション定義のサブインターフェイスは、FXOS 制限の対象にはなりません。サブインターフェイスを作成するオペレーティング システムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイス グループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有しますが、これはお勧めしません。このシナリオを実現する 3 つの方法については、次の図を参照してください。

図 *1 : FXOS* の *VLAN* とコンテナインスタンスのアプリケーション



シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるため、シャーシとアプリケーションの間で不一致が発生することがあります。

アプリケーション内のインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたはEtherChannelは、アプリケーショ

ン内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

ハードウェア バイパス ペア

FTD では、Firepower 9300 および 4100 シリーズの特定のインターフェイス モジュールを使用することで、ハードウェア バイパス 機能を有効にできます。ハードウェア バイパス は、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

ハードウェア バイパス 機能は、FTD アプリケーション内で設定されます。これらのインターフェイスを ハードウェア バイパス ペアとして使用する必要はありません。これらは、ASA と FTD アプリケーションの両方について通常のインターフェイスとして使用できます。ハードウェア バイパス 対応のインターフェイスをブレークアウト ポート用に設定することはできないため注意してください。ハードウェア バイパス 機能を使用するには、ポートを EtherChannel として設定しないでください。そうでない場合は、これらのインターフェイスを通常のインターフェイス モードの EtherChannel メンバとして含めることができます。

ハードウェア バイパス がインラインペアで有効になっている場合、スイッチのバイパスが最初に試行されます。スイッチのエラーが原因でバイパス設定が失敗した場合は、物理バイパスが有効になります。

（注） ハードウェアバイパス（FTW）は、VDP/Radware などのサードパーティ製アプリケーションを使用したサービスチェイニングにインストールされた FTD ではサポートされません。

FTD は、以下のモデルの特定のネットワーク モジュールのインターフェイス ペアで ハードウェア バイパス をサポートします。

- Firepower 9300
- Firepower 4100 シリーズ

これらのモデルでサポートされている ハードウェア バイパス ネットワーク モジュールは以下のとおりです。

- Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR-NM-6X1SX-F）
- Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR-NM-6X10SR-F）
- Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR-NM-6X10LR-F）
- Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR-NM-2X40G-F）

- Firepower 8 ポート 1G Copper FTW ネットワーク モジュール シングルワイド（FPR-NM-8X1G-F）

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 および 2
- 3 および 4
- 5 および 6
- 7 および 8

ジャンボ フレーム サポート

Firepower 4100/9300 シャーシは、デフォルトで有効になっているジャンボ フレームをサポートします。Firepower 4100/9300 シャーシにインストールされた特定の論理デバイスのジャンボ フレーム サポートを有効にするには、論理デバイスのインターフェイスに適切な MTU の設定を構成する必要があります。

Firepower 4100/9300 シャーシのアプリケーションでサポートされている最大 MTU は、9184 です。

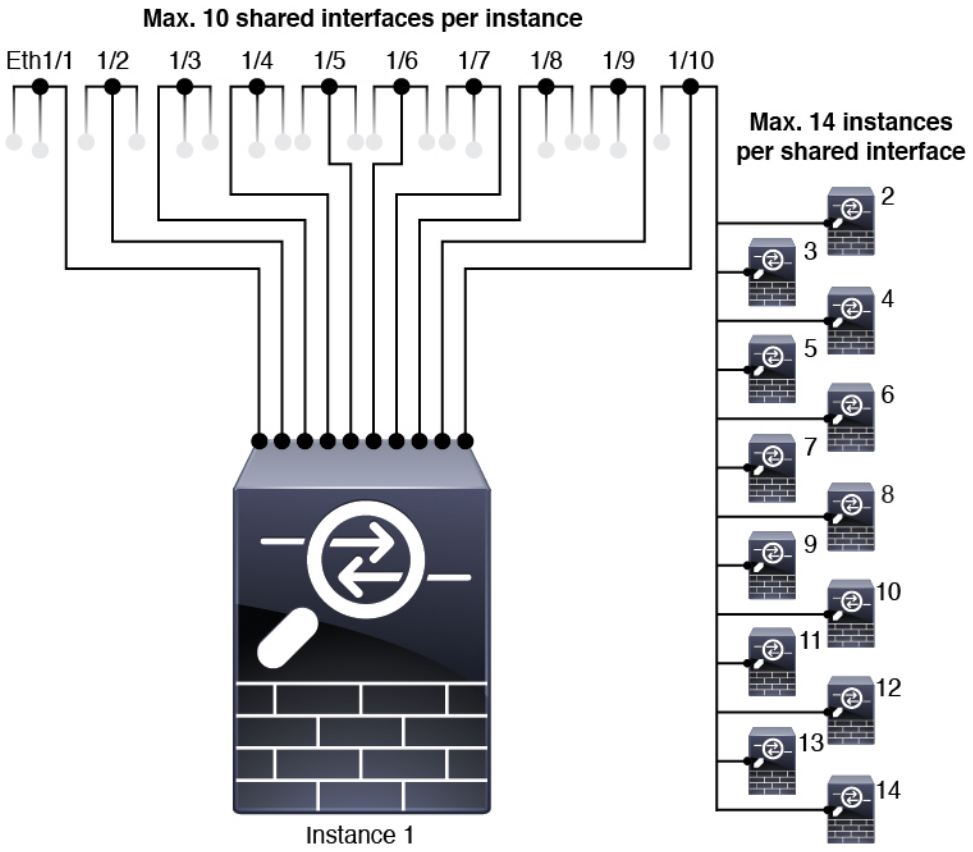
（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

共有インターフェイスの拡張性

コンテナ インスタンスは、data-sharing タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャーシは一意の MAC アドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャーシは VLAN サブインターフェイスの転送用に VLAN グループ テーブルも保持します。最大 500 個の VLAN サブインターフェイスを作成できます。

共有インターフェイスの割り当てに次の制限を参照してください。



共有インターフェイスのベスト プラクティス

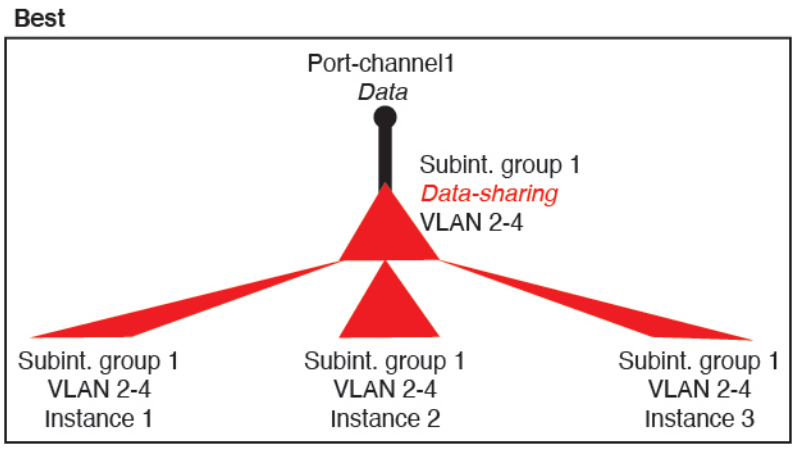
転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1 つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナ インスタンスで VLAN を分割できます。

インターフェイスを共有する場合は、拡張性の高いものから低いものの順に次の手順を実行します。

1. 最適：単一の親の下のサブインターフェイスを共有し、インスタンスグループと同じサブインターフェイスのセットを使用します。

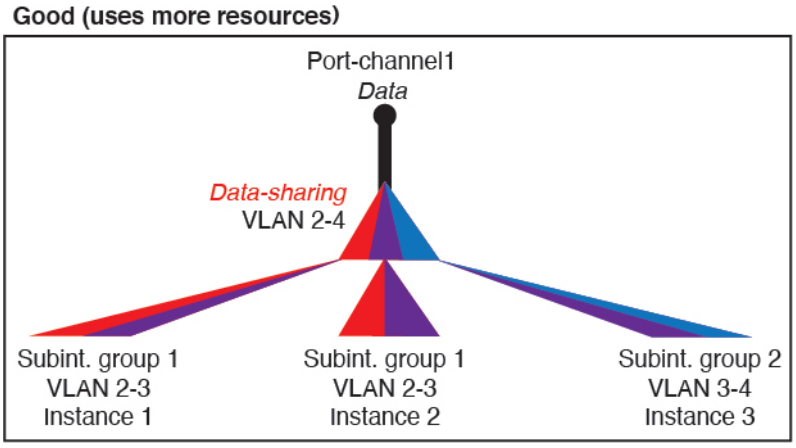
   たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、Port-Channel2、Port-Channel3、Port-Channel4 の代わりに、その EtherChannel のサブインターフェイス（Port-Channel1.2、3、4）を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループ テーブルの拡張性は転送テーブルよりも優れています。

図 *2:* 最適：単一の親のサブインターフェイスグループを共有



インスタンスグループと同じサブインターフェイスのセットを共有しない場合は、（VLAN グループよりも）より多くのリソースを設定で使用することになる可能性があります。たとえば、Port-Channel1.2 および 3 をインスタンス 1 および 2 と共有するとともに Port-Channel1.3 および 4 をインスタンス 3 と共有する（2 つの VLAN グループ）のではなく、Port-Channel1.2、3、および 4 をインスタンス 1、2、および 3 と共有（1 つの VLAN グループ）します。

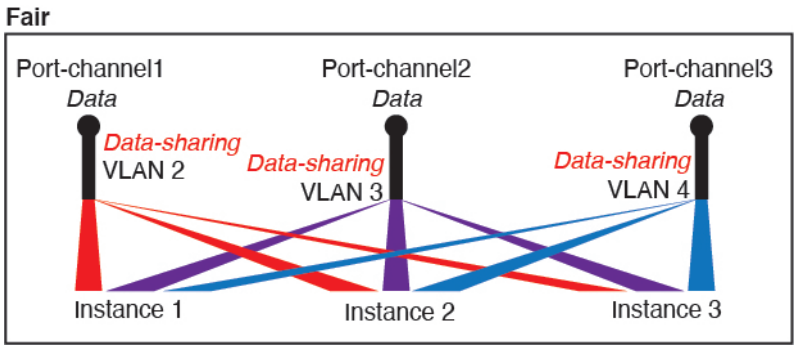
図 *3:* 良好：単一の親の複数のサブインターフェイスグループを共有



2. 普通：親の間でサブインターフェイスを共有します。

   たとえば、Port-Channel2、Port-Channel4、および Port-Channel4 ではなく、Port-Channel1.2、Port-Channel2.3、および Port-Channel3.4 を共有します。この使用方法は同じ親のサブインターフェイスのみを共有するよりも効率は劣りますが、VLAN グループを利用しています。

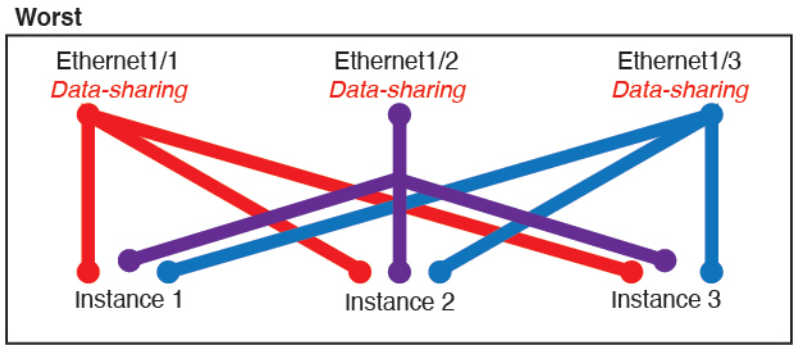
図 *4*：普通：個別の親のサブインターフェイスを共有



3. 最悪：個々の親インターフェイス（物理または EtherChannel）を共有します。

   この方法は、最も多くの転送テーブル エントリを使用します。

図 *5*：最悪：親インターフェイスを共有



共有インターフェイスの使用状況の例

インターフェイスの共有と拡張性の例について、以下の表を参照してください。以下のシナリオは、すべてのインスタンス間で共有されている管理用の 1 つの物理/EtherChannel インターフェイスと、ハイアベイラビリティで使用する専用のサブインターフェイスを含むもう 1 つの物理/EtherChannel インターフェイスを使用していることを前提としています。

- 表 12 : 3 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス （182 ページ）
- 表 13 : 3 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス （184 ページ）
- 表 14 : 1 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス （186 ページ）
- 表 15 : 1 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス （188 ページ）

3 つの SM-44 と firepower 9300

次の表は、物理インターフェイスまたはEtherchannelのみを使用している9300のSM-44セキュリティモジュールに適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 *12 : 3* つの *SM-44* を備えた *Firepower 9300* の物理/*EtherChannel* インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**0**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30： • 15 • 15	**0**	**2:** • インスタンス 1 • インスタンス 2	14%
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（各 1） • 11（各 1） • 11（各 1）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
33： • *11*（各 *1*） • *11*（各 *1*） • *12*（各 *1*）	***3***： • *1* • *1* • *1*	***34***： • インスタンス *1* - インスタンス *11* • インスタンス *12* - インスタンス *22* • インスタンス *23* - インスタンス *34*	*102 %* 許可しない
30： • 30（各 1）	**1**	**6**： • インスタンス 1 - インスタンス 6	25 %
30： • 10（各 5） • 10（各 5） • 10（各 5）	**3**： • 1 • 1 • 1	**6**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 4 • インスタンス 5 - インスタンス 6	23 %
30： • 30（各 6）	**2**	**5**： • インスタンス 1 - インスタンス 5	28%
30： • 12（各 6） • 18（各 6）	**4**： • 2 • 2	**5**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 5	26 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
24： • 6 • 6 • 6 • 6	**7**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	44 %
24： • 12（各 6） • 12（各 6）	**14**： • 7 • 7	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 2 - インスタンス 4	41%

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 9300 上の 3 つの SM-44 セキュリティ モジュールに適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 ***13 : 3*** つの ***SM-44*** を備えた ***Firepower 9300*** 上の ***1*** つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
168： • 168（4 ea.）	**0**	**42**： • インスタンス 1 - インスタンス 42	33%
224： • 224（16 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	27 %
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
33： • 11（各 1） • 11（各 1） • 11（各 1）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**6**： • 2 • 2 • 2	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70： • 70（5 ea.）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
165： • *55*（*5 ea.*） • *55*（*5 ea.*） • *55*（*5 ea.*）	***30***： • *10* • *10* • *10*	***33***： • インスタンス *1* - インスタンス *11* • インスタンス *12* - インスタンス *22* • インスタンス *23* - インスタンス *33*	*102 %* 許可しない

1 つの SM 44 を備えた Firepower 9300

次の表は、物理インターフェイスまたは Etherchannel のみを使用している 1 つの SM-44 を備えた Firepower 9300 に適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 *14 : 1* つの *SM-44* を備えた *Firepower 9300* の物理*/EtherChannel* インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**0**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30： • 15 • 15	**0**	**2:** • インスタンス 1 • インスタンス 2	14%
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
14： • 7（各 1） • 7（各 1）	**2:** • **1** • **1**	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
32： • 8 • 8 • 8 • 8	**1**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	21 %
32： • 16（各 8） • 16（各 8）	**2**	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	20 %
32： • 8 • 8 • 8 • 8	**2**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	25 %
32： • 16（各 8） • 16（各 8）	**4**： • 2 • 2	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	24 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
24： • 8 • 8 • 8	**8**	**3**： • インスタンス 1 • インスタンス 2 • インスタンス 3	37 %
10： • 10（各 2）	**10**	**5**： • インスタンス 1 - インスタンス 5	69%
10： • 6（各 2） • 4（各 2）	**20**： • 10 • 10	**5**： • インスタンス 1 - インスタンス 3 • インスタンス 4 - インスタンス 5	59%
14： • *12（2 ea.）*	***10***	***7***： • インスタンス *1* - インスタンス *7*	*109%* 許可しない

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 1 つの SM-44 を備えた Firepower 4150 に適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 *15 : 1* つの *SM-44* を備えた *Firepower 9300* 上の *1* つの親のサブインターフェイスとインスタンス

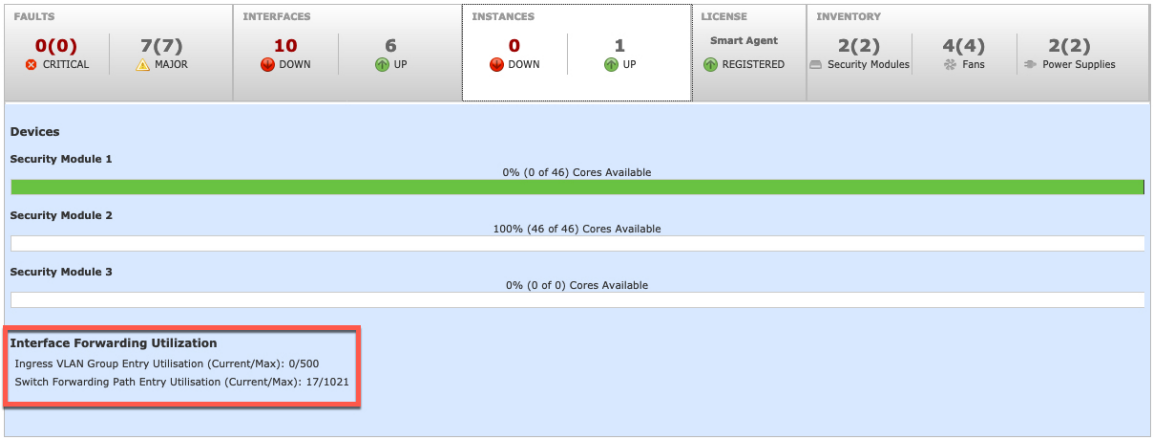
専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 112（各 8）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
224： • 224（16 ea.）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%
14： • 14（各 1）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（各 1） • 7（各 1）	**2:** • 1 • 1	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
112： • 112（各 8）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
112： • 56（各 8） • 56（各 8）	**2:** • 1 • 1	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
112： • 112（各 8）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %
112： • 56（各 8） • 56（各 8）	**4**： • 2 • 2	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
140： • 140（各 10）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %
140： • 70（各 10） • 70（各 10）	**20**： • 10 • 10	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %

共有インターフェイス リソースの表示

転送テーブルと VLAN グループの使用状況を表示するには、**[インスタンス（Instances）]>[インターフェイス転送の使用率（Interface Forwarding Utilization）]** エリアを参照し ます。次に例を示します。



FTD のインライン セット リンク ステート伝達サポート

インラインセットはワイヤ上のバンプのように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

FTD アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、FTD はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝

達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンク ステートが変化すると、シャーシはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、シャーシからリンク ステートの変更が伝達されるまで最大 4 秒かかります。障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

インターフェイスに関する注意事項と制約事項

VLAN サブインターフェイス

- 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（175ページ）を参照してください。
- サブインターフェイス（および親インターフェイス）はコンテナインスタンスにのみ割り当てることができます。

（注） コンテナ インスタンスに親インターフェイスを割り当てる場合、タグなし（非VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。 クラスタタイプのインターフェイスの場合、親インターフェイスを使用することはできません。

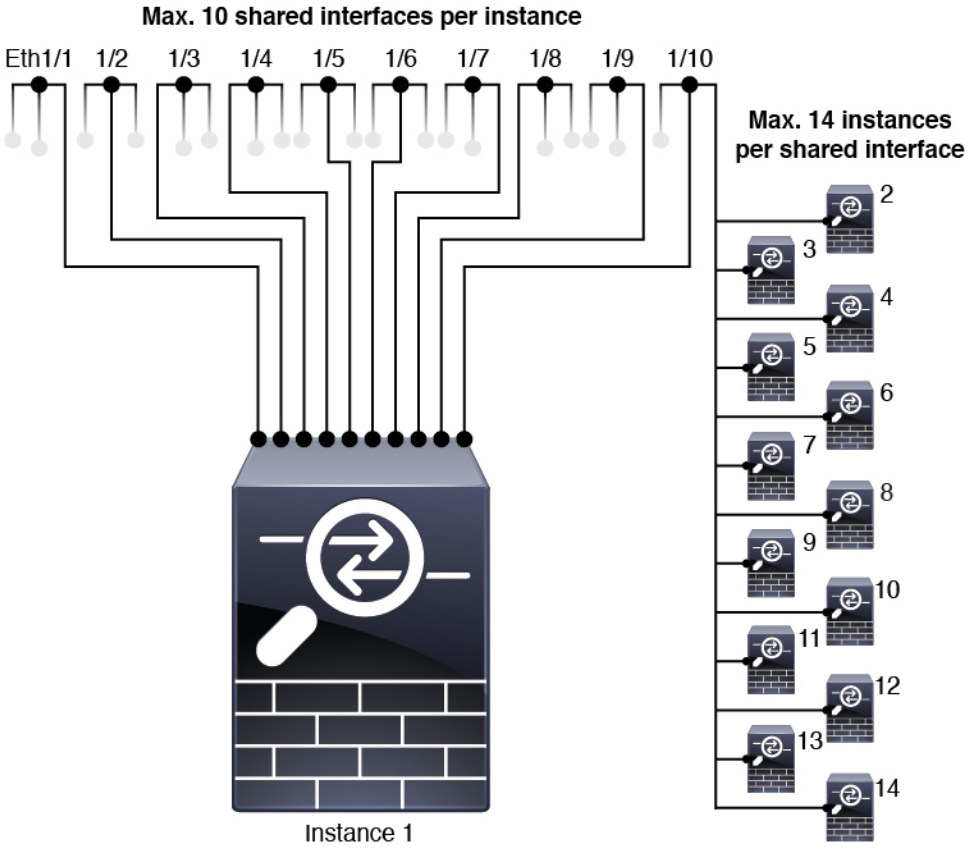
- サブインターフェイスはデータまたはデータ共有タイプのインターフェイス、およびクラスタタイプのインターフェイスでサポートされます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。
- マルチインスタンス クラスタリングの場合、データインターフェイス上の FXOS サブインターフェイスはサポートされません。ただし、クラスタ制御リンクではサブインターフェイスがサポートされているため、クラスタ制御リンクには専用の EtherChannel または EtherChannel のサブインターフェイスを使用できます。アプリケーション定義のサブインターフェイスは、データインターフェイスでサポートされていることに注意してください。
- 最大 500 個の VLAN ID を作成できます。
- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。

- FTDインラインセットに、またはパッシブインターフェイスとしてサブインターフェイスを使用することはできません。
- フェールオーバーリンクに対してサブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体のフェールオーバーリンクとしての使用が制限されます。一部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、一部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。

データ共有インターフェイス

- ネイティブインスタンスではデータ共有インターフェイスを使用することはできません。
- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance1 ～ Instance14 に Ethernet1/1 を割り当てることができます。

  インスタンスごとの最大共有インターフェイス数：10 たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。



- クラスタではデータ共有インターフェイスを使用することはできません。
- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。

- トランスペアレント ファイアウォール モード デバイスでデータ共有インターフェイスを使用することはできません。
- FTDインラインセットでまたはパッシブインターフェイスとしてデータ共有インターフェイスを使用することはできません。
- フェールオーバーリンクに対してデータ共有インターフェイスを使用することはできません。

次に対するインライン セット FTD

- 物理インターフェイス（通常かつブレイクアウト ポート）と Etherchannel のサポート。 サブインターフェイスはサポートされません。
- リンク ステートの伝達はサポートされます。

ハードウェア バイパス

- FTD をサポート。ASA の通常のインターフェイスとして使用できます。
- FTD はインライン セットでのみ ハードウェア バイパス をサポートします。
- ハードウェア バイパス 対応のインターフェイスをブレークアウト ポート用に設定することはできません。
- ハードウェア バイパス インターフェイスを EtherChannel に含めたり、ハードウェア バイパス 用に使用することはできません。EtherChannel で通常のインターフェイスとして使用できます。
- ハードウェア バイパス は高可用性ではサポートされません。

デフォルトの MAC アドレス

ネイティブインスタンス向け：

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MACアドレスを使用します。インターフェイスのメンバーシップは、MACアドレスには影響しません。

コンテナインスタンス向け：

- すべてのインターフェイスの MAC アドレスは MAC アドレス プールから取得されます。サブインターフェイスでは、MAC アドレスを手動で設定する場合、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。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 （219 ページ） を参照してください。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、EtherChannels を追加して、VLAN サブインターフェイスを追加し、、インターフェイス プロパティを編集して、ブレークアウト ポートを設定できます。

（注） FXOS でインターフェイスを削除した場合（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す。

インターフェイスの有効化または無効化

各インターフェイスの **[Admin State]** を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスはディセーブルになっています。VLAN サブインターフェイスの場合、管理状態は親インターフェイスから継承されます。

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

[インターフェイス（Interface）] ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。

ステップ 2 インターフェイスを有効にするには、[disabled **無効なスライダ**（ ）] をクリックします。これで、[enabled **有効なスライダ**（ ）] に変わります。

[はい（Yes）]をクリックして、変更を確定します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変化します。

ステップ 3 インターフェイスを無効にするには、有効な **有効なスライダ**（ ） をクリックして、無効な **無効なスライダ**（ ） に変更します。

[はい（Yes）]をクリックして、変更を確定します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

物理インターフェイスの設定

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

始める前に

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

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

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

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

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

ステップ 4 インターフェイスの [タイプ（Type）] を選択します。

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

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

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

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

ステップ 8 （任意） 以前に設定した**ネットワーク制御ポリシー**を選択します。

ステップ 9 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

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

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

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

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

非データ インターフェイスのみがアクティブ モードをサポートしています。

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

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

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

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

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

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

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

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

クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、ポートチャネル 48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスを追加できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。

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

ステップ 5 インターフェイスの [タイプ（Type）] を選択します。

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

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

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

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

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

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

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

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

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

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

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

ステップ 11 **[OK]** をクリックします。

コンテナ インスタンスの VLAN サブインターフェイスの追加

シャーシには最大 500 個のサブインターフェイスを追加できます。

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

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

本書では、*FXOS* VLAN サブインターフェイスについてのみ説明します。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。

手順

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

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

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

ステップ 3 インターフェイスの [タイプ（Type）] を選択します。

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

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

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

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

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

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

ステップ 6 1 ～ 4095 の間で [VLAN ID] を設定します。

ステップ 7 [OK] をクリックします。

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

ブレークアウト ケーブルの設定

Firepower 4100/9300 シャーシで使用するブレークアウト ケーブルを設定するには、次の手順に従います。ブレークアウト ケーブルを使用すると、1 つの 40 Gbps ポートの代わりに 4 つの 10 Gbps ポートを実装できます。

始める前に

ハードウェア バイパス 対応のインターフェイスをブレークアウト ポート用に設定することはできません。

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

[インターフェイス（Interface）] ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。

ブレークアウト ケーブルに対応できるインターフェイスが、現在そのように設定されていない場合は、そのインターフェイスの行に [ブレークアウト ポート（Breakout Port）] アイコンが表示されます。ブレークアウト ケーブルを使用するように設定されているインターフェイスの場合、個々のブレークアウト インターフェイスが別々にリストされます（例：イーサネット 2/1/1、2/1/2、2/1/3、2/1/4）。

ステップ 2 1 つの 40 Gbps インターフェイスを 4 つの 10 Gbps インターフェイスに変換するには、次の手順を実行します。

a) 変換するインターフェイスの [ブレークアウト ポート（Breakout Port）] アイコンをクリックします。

[ブレークアウト ポートの作成（Breakout Port Creation）] ダイアログボックスが開いて、続行の確認を求められ、シャーシのリブートについての警告が表示されます。

b) [はい（Yes）] をクリックして確定します。

シャーシが再起動し、指定したインターフェイスが 4 つの 10 Gbps インターフェイスに変換されます。

ステップ 3 4 つの 10 Gbps ブレークアウト インターフェイスを 1 つの 40 Gbps インターフェイスに再度変換するには、次の手順を実行します。

a) いずれかのブレークアウト インターフェイスの [削除（Delete）] をクリックします。

確認のダイアログボックスが開き、続行するかどうかの確認が求められるとともに、4 つのブレークアウト インターフェイスが削除され、シャーシが再起動すると警告されます。

b) [はい（Yes）] をクリックして確定します。

シャーシが再起動し、指定したインターフェイスが 1 つの 40 Gbps インターフェイスに変換されます。

モニタリング インターフェイス

Firepower Chassis Manager の [インターフェイス（Interfaces）] ページから、シャーシにインストールされているインターフェイスのステータスの表示、インターフェイスのプロパティの編集、インターフェイスの有効化または無効化、ポート チャネルの作成を行えます。

[インターフェイス（Interfaces）] ページは、2 つのセクションで構成されています。

- 上部のセクションには、シャーシにインストールされているインターフェイスの視覚的表現が表示されます。インターフェイスのいずれかにマウスのカーソルを合わせると、そのインターフェイスの詳細情報が表示されます。

  インターフェイスは、それぞれの現在のステータスを示すために色分けされています。

  - 緑色：そのインターフェイスはインストールされており、有効になっています。
  - ダーク グレイ：そのインターフェイスはインストールされていますが、無効になっています。
  - 赤色：インターフェイスの動作状態に問題があります。
  - 淡い灰色：インターフェイスがインストールされていません。

（注） ポート チャネルのポートとして機能するインターフェイスは、このリストに表示されません。

- 下部のセクションには、[All Interfaces] と [**ハードウェア バイパス**] の 2 つのタブが含まれています。**[All Interfaces]** タブ：インターフェイスごとに、インターフェイスを有効または無効にできます。[Edit] をクリックすると、インターフェイスのプロパティ（速度やインターフェイス タイプなど）を編集することもできます。**ハードウェア バイパス**については、ハードウェア バイパス ペア （177 ページ）を参照してください。

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

インターフェイスのトラブルシューティング

エラー：スイッチの転送パスに 1076 のエントリがあり、1024 の制限を超えています。インターフェイスを追加する場合は、論理デバイスに割り当てられている共有インターフェイスの数を減らすか、論理デバイス共有インターフェイスの数を減らすか、または共有されていないサブインターフェイスを使用します。サブインターフェイスを削除すると、このメッセージが表示されます。これは、残りの設定が [Switch Forwarding Path] テーブル内に収まるように最適化されなくなったためです。削除の使用例に関するトラブルシューティング情報については、FXOS

コンフィギュレーション ガイドを参照してください。'scope fabric-interconnect' の 'show detail' を使用して、現在の [Switch Forwarding Path Entry Count] を表示します。

論理デバイスから共有サブインターフェイスを削除しようとしたときにこのエラーが表示される場合は、新しい設定が共有サブインターフェイス向けのこのガイドラインに従っていないためです。同じ論理デバイスのグループと同じサブインターフェイスのセットを使用します。1つの論理デバイスから共有サブインターフェイスを削除すると、さらに多くの VLAN グループを作成できるため、転送テーブルの使用効率が低くなります。この状況に対処するには、CLI を使用して共有サブインターフェイスを同時に追加および削除し、同じ論理デバイスのグループに対して同じサブインターフェイスのセットを維持する必要があります。

詳細については、次のシナリオを参照してください。これらのシナリオは、次のインターフェイスと論理デバイスから始まります。

- 同じ親で設定された共有サブインターフェイス：Port-Channel1.100（VLAN 100）、Port-Channel1.200（VLAN 200）、Port-Channel1.300（VLAN 300）
- 論理デバイス グループ：LD1、LD2、LD3、LD4

シナリオ 1：**あるサブインターフェイスを 1 つの論理デバイスから削除するが、他の論理デバイスに割り当てられたままにする**

サブインターフェイスは削除しないでください。アプリケーション設定で無効にするだけにしてください。サブインターフェイスを削除する必要がある場合は、一般に共有インターフェイスの数を減らして、転送テーブルに収まるようにする必要があります。

シナリオ 2：**1 つの論理デバイスからセット内のすべてのサブインターフェイスを削除する**

CLI で論理デバイスからセット内のすべてのサブインターフェイスを削除した後、設定を保存して、削除が同時に実行されるようにします。

1. 参照用の VLAN グループを表示します。次の出力では、グループ 1 には、3 つの共有サブインターフェイスを表す VLAN 100、200、300 が含まれています。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status         INTF         Vlan Status
1    1         configured
                                          100  present
                                          200  present
                                          300  present
2048 512       configured
                                          0    present
2049 511       configured
                                          0    present
firepower(fxos)# exit
firepower#
```

2. 変更する論理デバイスに割り当てられている共有サブインターフェイスを表示します。

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # show external-port-link
```

```
External-Port Link:
    Name                           Port or Port Channel Name Port Type          App
 Name   Description
    ------------------------------ ------------------------- ------------------
---------- -----------
    Ethernet14_ftd                 Ethernet1/4               Mgmt               ftd
    PC1.100_ftd                    Port-channel1.100         Data Sharing       ftd
    PC1.200_ftd                    Port-channel1.200         Data Sharing       ftd
    PC1.300_ftd                    Port-channel1.300         Data Sharing       ftd
```

3. 論理デバイスからサブインターフェイスを削除した後、設定を保存します。

```
firepower /ssa/logical-device # delete external-port-link PC1.100_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.200_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

シナリオ 3：グループ内のすべての論理デバイスから 1 つのサブインターフェイスを削除する

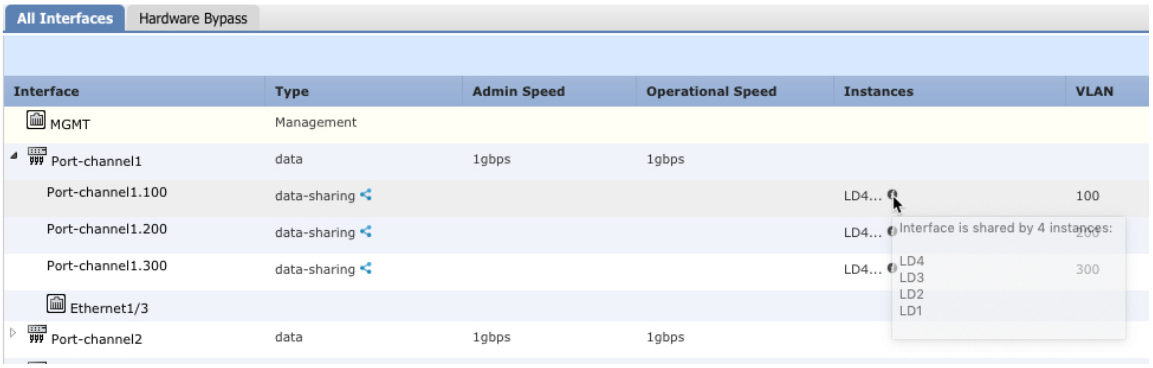
CLI でグループ内のすべての論理デバイスからサブインターフェイスを削除した後、設定を保存して、削除が同時に実行されるようにします。次に例を示します。

1. 参照用の VLAN グループを表示します。次の出力では、グループ 1 には、3 つの共有サブインターフェイスを表す VLAN 100、200、300 が含まれています。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status         INTF         Vlan Status
1    1         configured
                                          100  present
                                          200  present
                                          300  present
2048 512       configured
                                          0    present
2049 511       configured
                                          0    present
```

2. 各論理デバイスに割り当てられているインターフェイスを表示し、共通の共有サブインターフェイスに注目してください。同じ親インターフェイス上に存在する場合、それらは 1 つの VLAN グループに属し、**show ingress-vlan-groups** リストと一致しているはずです。Firepower Chassis Manager では、各共有サブインターフェイスにカーソルを合わせて、割り当てられているインスタンスを確認できます。

図 *6* : 共有インターフェイスごとのインスタンス



CLI では、割り当てられたインターフェイスを含むすべての論理デバイスの特性を表示できます。

```
firepower# scope ssa
firepower /ssa # show logical-device expand

Logical Device:
    Name: LD1
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:25

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]
```

```
    Name: LD2
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:28

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]

    Name: LD3
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
```

```
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:2B

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]

    Name: LD4
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:2E

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]
```

3. 各論理デバイスからサブインターフェイスを削除した後、設定を保存します。

```
firepower /ssa # scope logical device LD1
firepower /ssa/logical-device # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD2
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
```

```
firepower /ssa* # scope logical-device LD3
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD4
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

シナリオ 4：1 つまたは複数の論理デバイスにサブインターフェイスを追加する

CLI でグループ内のすべての論理デバイスにサブインターフェイスを追加し、その後、その追加が同時になるように設定を保存します。

1. 各論理デバイスにサブインターフェイスを追加してから、設定を保存します。

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD2
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD3
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD4
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # commit-buffer
firepower /ssa/logical-device/external-port-link #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

2. Port-Channel1.400 VLAN ID が VLAN グループ 1 に追加されたことを確認できます。

```
firepower /ssa/logical-device/external-port-link # connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status         INTF         Vlan Status
1    1         configured
                                          200  present
                                          100  present
                                          300  present
                                          400  present
2048 512       configured
                                          0    present
2049 511       configured
                                          0    present
firepower(fxos)# exit
```

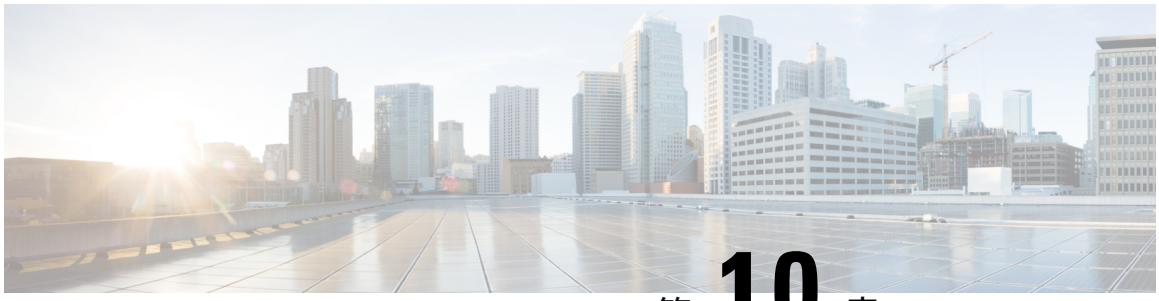
```
firepower /ssa/logical-device/external-port-link #
```

インターフェイスの履歴

機能名	プラットフォームリリース	機能情報
FTD 動作リンク状態と物理リンク状態の同期	2.9.1	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、 FTD が処理できるようになる前に外部ルータが FTD 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。 （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。 新規/変更された Firepower Chassis Manager 画面：[Logical Devices] > [Enable Link State] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail**
クラスタ タイプ インターフェイスでの VLAN サブインターフェイスのサポート（マルチインスタンス使用のみ）	2.8.1	マルチインスタンスクラスタで使用するために、クラスタタイプのインターフェイスで VLAN サブインターフェイスを作成できるようになりました。各クラスタには一意のクラスタ制御リンクが必要であるため、VLAN サブインターフェイスはこの要件を満たすための簡単な方法を提供します。または、クラスタごとに専用の EtherChannel を割り当てることもできます。複数のクラスタタイプのインターフェイスが許可されるようになりました。 新しい/変更された画面： **[インターフェイス（Interfaces）]**>**[すべてのインターフェイス（All Interfaces）]**>**[新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] > [タイプ（Type）] フィールド
500 Vlan のサポート（不測事態がない場合）	2.7.1	以前は、親インターフェイスの数とその他の導入の決定事項に応じて、250 から 500 の VLAN がサポートされていました。すべてのケースで 500 の VLAN を使用できるようになりました。

機能名	プラットフォームリリース	機能情報
コンテナ インスタンスで使用される VLAN サブインターフェイス	2.4.1	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。 （注） FTD バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces]** > **[All Interfaces]** > **[Add New]** ドロップダウン メニュー > **[Subinterface]** 新規/変更された FMC 画面： **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** アイコン > **[インターフェイス（Interfaces）]** タブ
コンテナ インスタンスのデータ共有インターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、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。 （注） FTD バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces]** > **[All Interfaces]** > **[Type]**
オン モードでのデータ EtherChannel のサポート	2.4.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 新規/変更された画面： **[Interfaces]** > **[All Interfaces]** > **[Edit Port Channel]** > **[Mode]**
FTD インライン セットでの EtherChannel のサポート	2.1(1)	FTD インライン セットで EtherChannel を使用できるようになりました。
FTD のインライン セット リンク ステート伝達サポート	2.0(1)	FTD アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、FTD はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。
ハードウェア バイパス ネットワーク モジュールのサポート FTD	2.0(1)	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新規/変更された FMC 画面： **[Devices]** > **[Device Management]** > **[Interfaces]** > **[Edit Physical Interface]**

機能名	プラットフォームリリース	機能情報
FTD の Firepower イベントタイプ インターフェイス	1.1.4	FTD で使用するために、Firepower イベントとしてインターフェイスを指定できます。このインターフェイスは、FTD デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。FMC 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。 新規/変更された Firepower Chassis Manager 画面： **[Interfaces]** > **[All Interfaces]** > **[Type]**



第 10 章

論理デバイス

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 FTD 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 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。

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 FTD でのみサポートされています。ASA または FDM を使用する FTD 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 FTD 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。FTD 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（178ページ）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 （198ページ）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（175ページ）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。

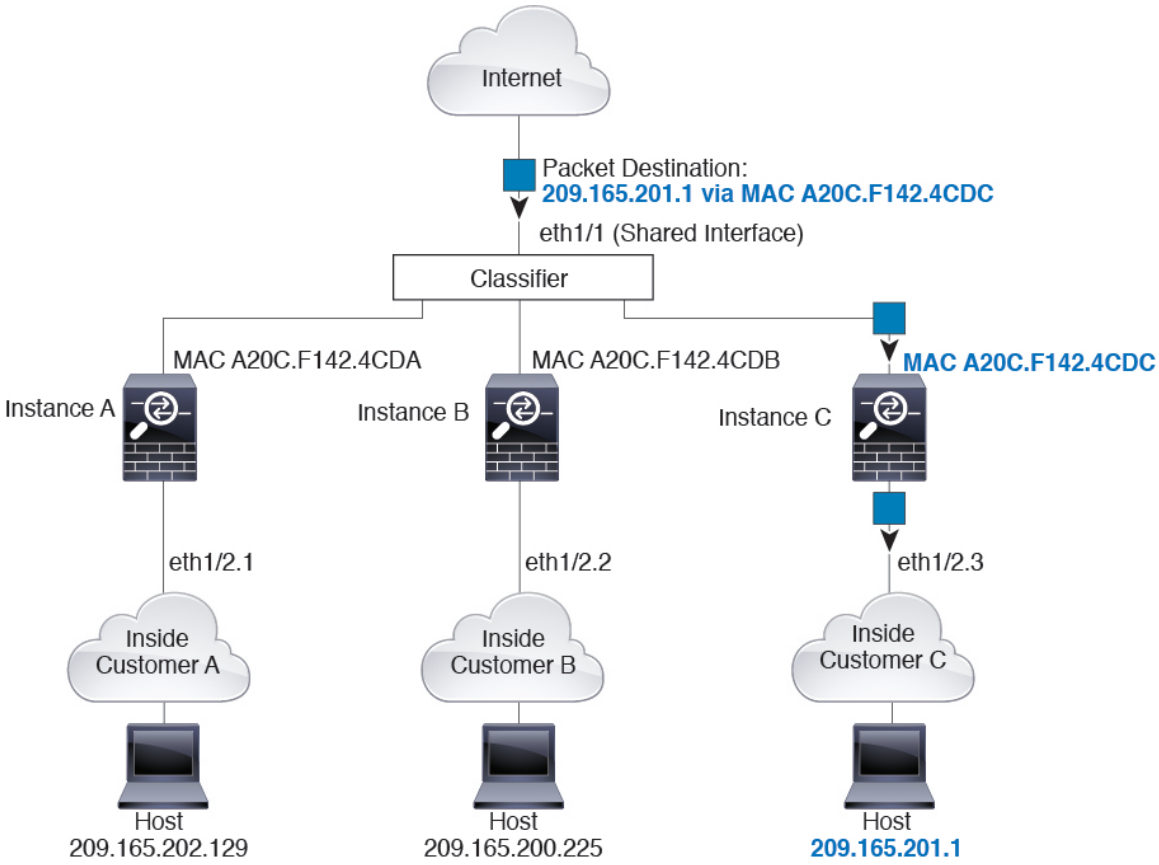
- 一意のインターフェイス：1つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループメンバー インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意のMACアドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意のMACアドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイスに割り当てられた固有の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

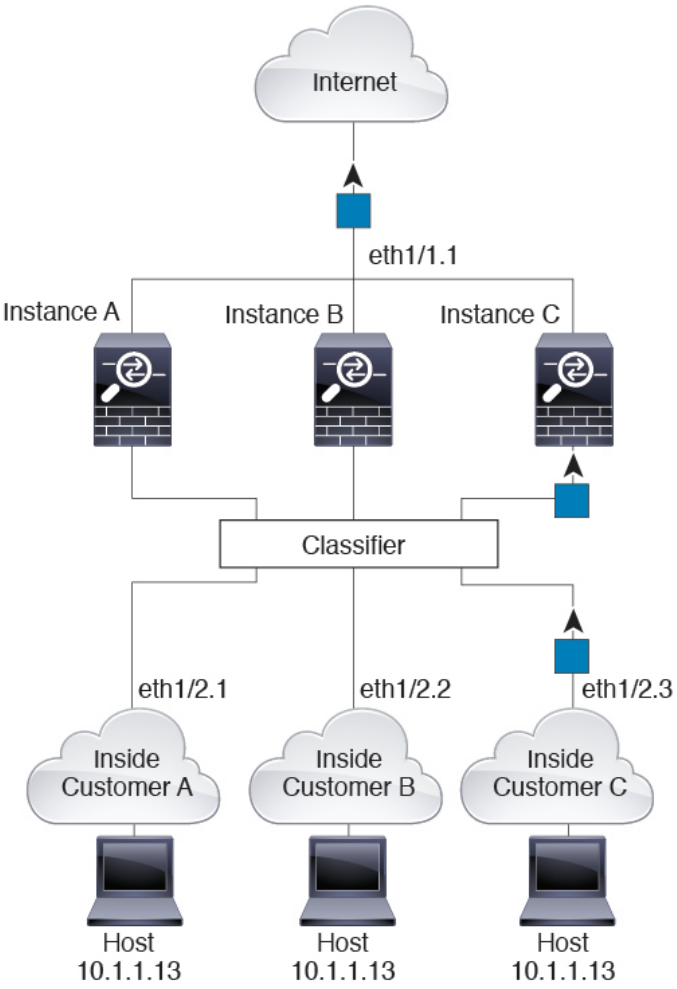
次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンスCにはルータがパケットを送信するMACアドレスが含まれているため、分類子はパケットをインスタンスCに割り当てます。

図 *7: MAC* アドレスを使用した共有インターフェイスのパケット分類



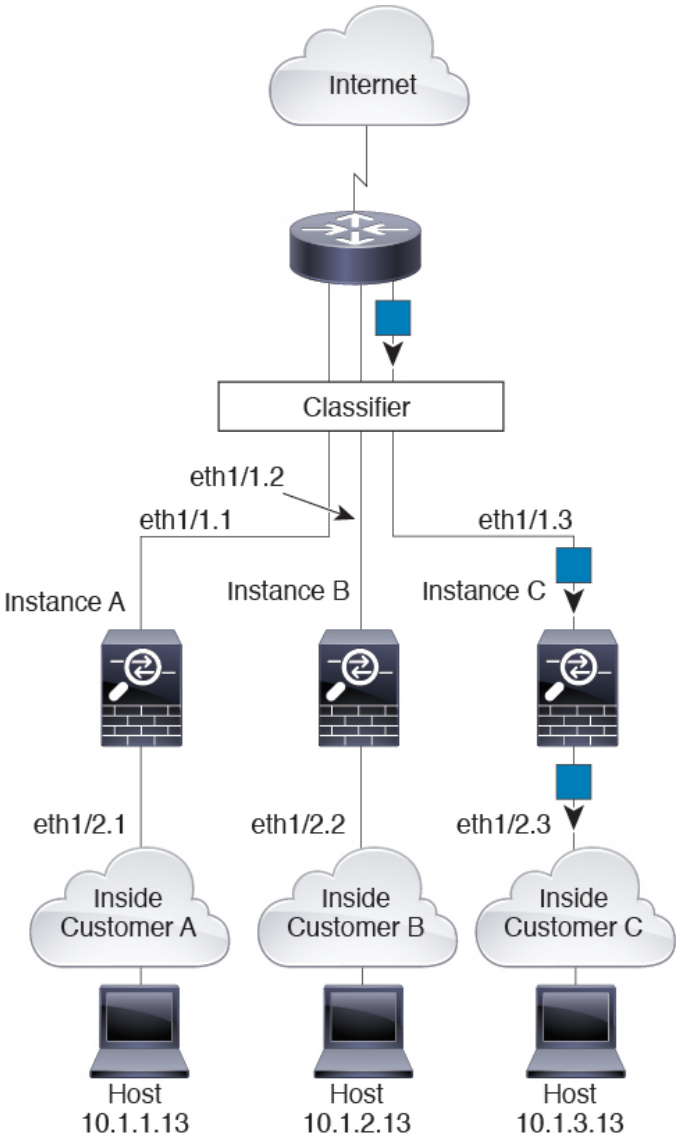
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *8* : 内部ネットワークからの着信トラフィック



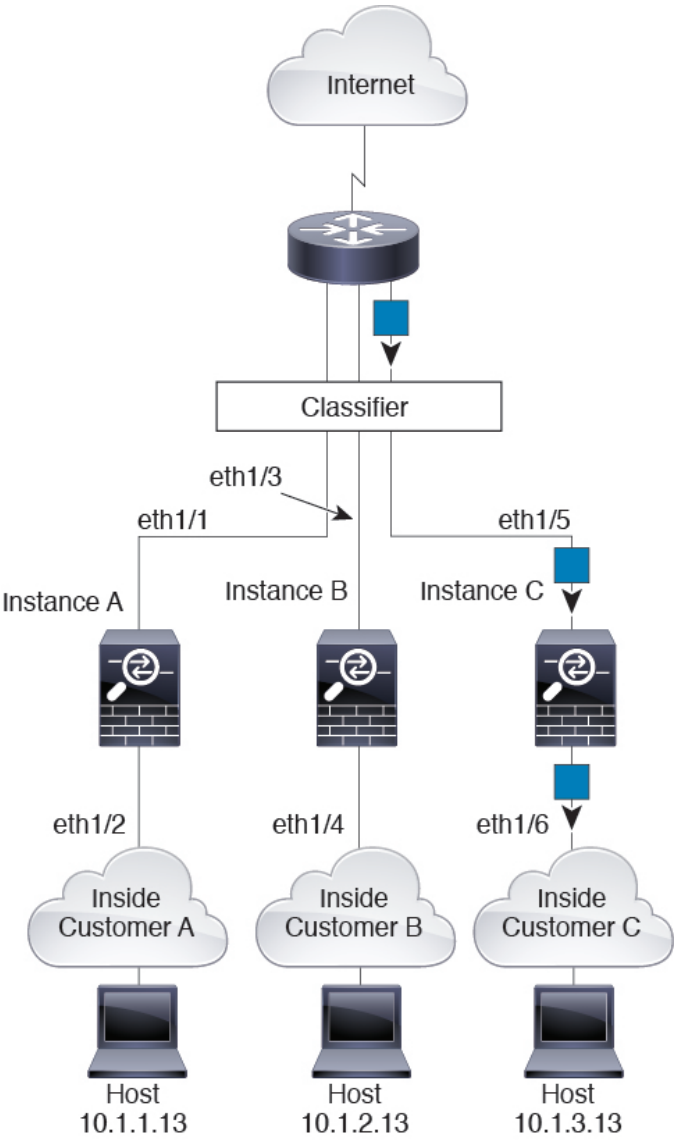
トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンス C に割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *9:* 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 *10* : 次に対するインライン セット *FTD*

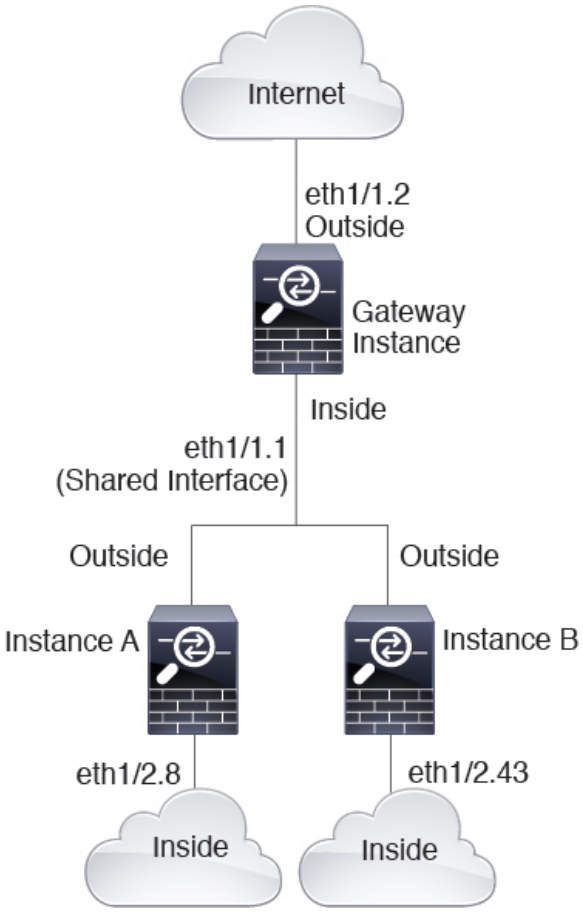


コンテナ インスタンスのカスケード

別のインスタンスの前にコンテナ インスタンスを直接配置することをカスケード コンテナ インスタンスと呼びます。1 つのインスタンスの外部インターフェイスは、別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 *11* : コンテナ インスタンスのカスケード

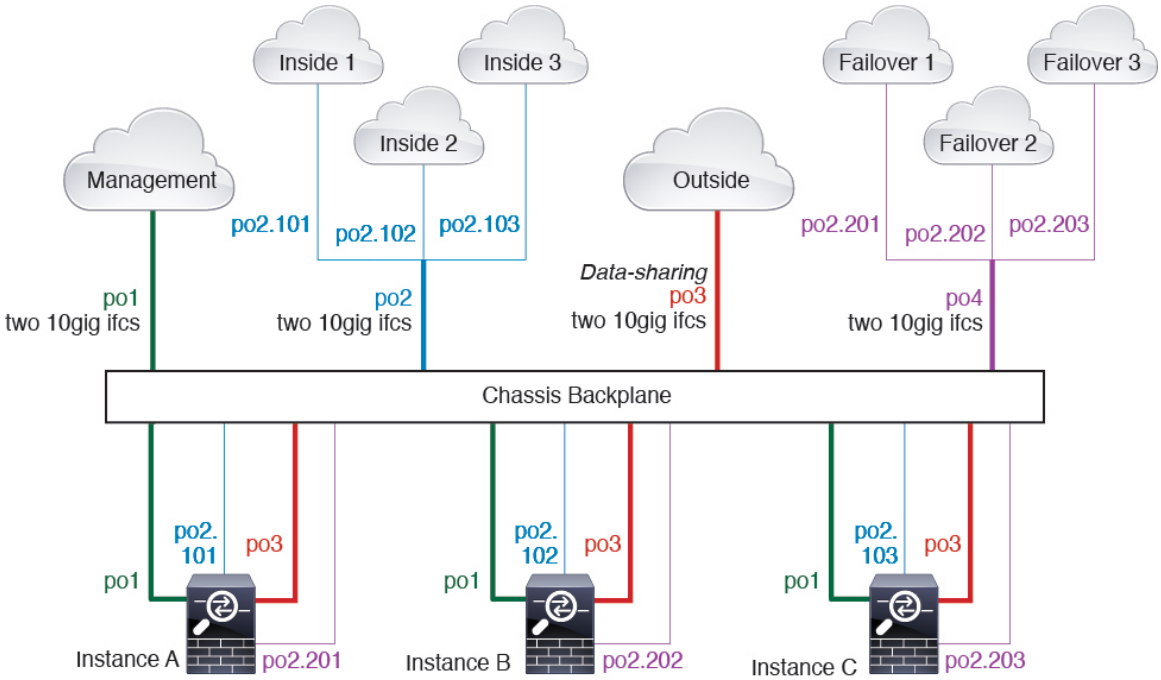


一般的な複数インスタンス展開

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の 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の 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

FXOS 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の MAC アドレスを使用するように、コンテナ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。

アプリケーション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、アプリケーション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。

FXOS 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。

A2*xx.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、シャーシは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シネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D.00***zz.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。

A2**F1.03***zz.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（229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（167ページ）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 つのシャーシがある場合、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（228ページ）」と「ハイアベイラビリティ ペアの追加（251 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 （223 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。

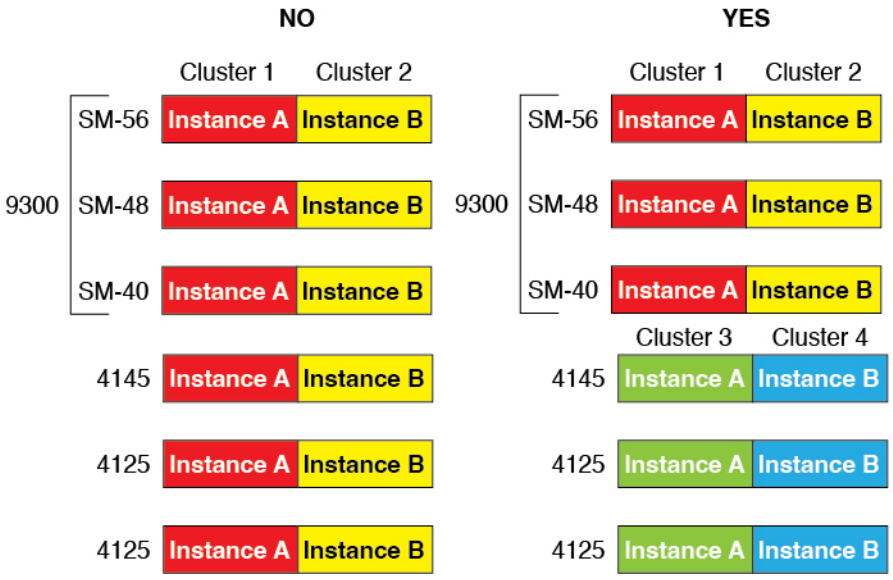
- セキュリティモジュール タイプ：Firepower 9300 に異なるタイプのモジュールをインストールできます。たとえば、SM-48 をモジュール 1、SM-40 をモジュール 2 、SM-56 をモジュール 3 としてインストールできます。
- ネイティブインスタンスとコンテナインスタンス：セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを 1 つのみインストールできます。一部のモジュールでネイティブイ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 FTD 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

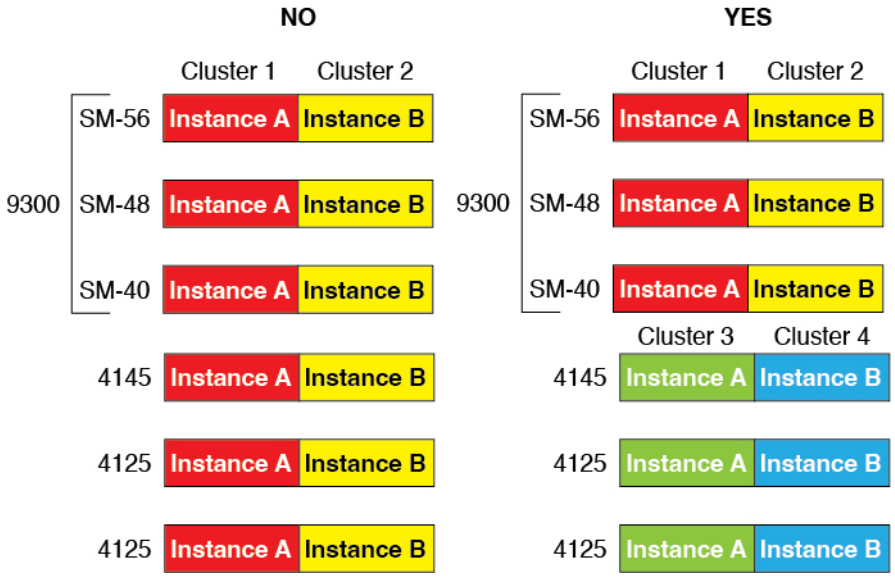
- Firepower 9300 上の ASA：最大 16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。シャーシ内、シャーシ間、およびサイト間クラスタリングでサポート。
- Firepower 4100 シリーズ 上の ASA：最大 16 個のシャーシ。シャーシ間、およびサイト間クラスタリングでサポート。
- FTDFirepower 9300 で FMC を使用：1 シャーシ内に最大 3 モジュール。 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：FTD 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 ソフトウェアを実行する必要があります。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュール タイプを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイスモジュールの追加や削除、または EtherChannel の設定などにより）クラスタリングを有効にした後

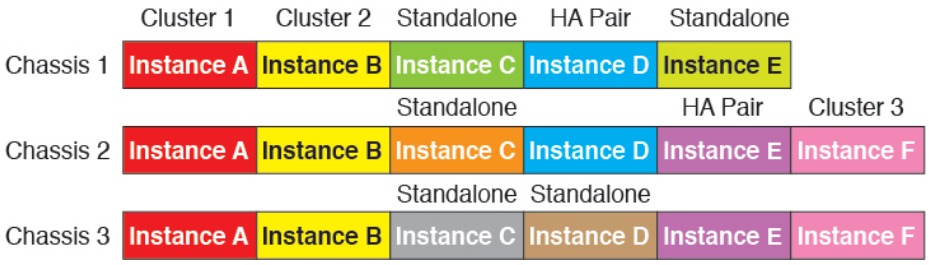
にFXOSでインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データノードから始めて、制御ノードで終わります）。

- 同じNTPサーバを使用する必要があります。FTDでは、FMCも同じNTPサーバーを使用する必要があります。時間を手動で設定しないでください。
- 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。FTD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

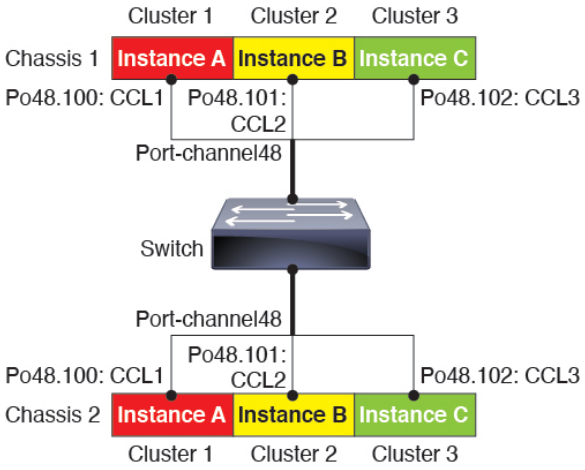
- セキュリティモジュール/エンジン間クラスタリングなし：特定のクラスタでは、セキュリティモジュール/エンジンごとに1つのコンテナインスタンスのみを使用できます。同じモジュール上で実行されている場合、同じクラスタに2つのコンテナインスタンスを追加することはできません。

- 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。

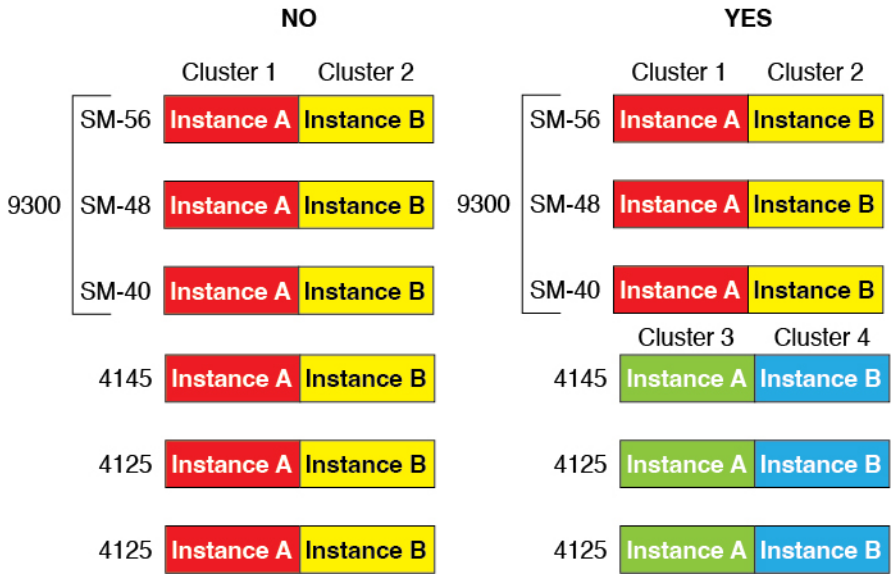


- Firepower 9300の3つすべてのモジュールはクラスタに属している必要があります。Firepower 9300の場合、クラスタには3つすべてのモジュールで1つのコンテナインスタンスが必要です。たとえば、モジュール1と2のインスタンスを使用してクラスタを作成し、モジュール3のネイティブインスタンスを使用することはできません。

- 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 *16 :* 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

FTD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 FTD に対してのみ使用できます。
- FTD 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。
- FTD 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 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 *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 の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリープロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

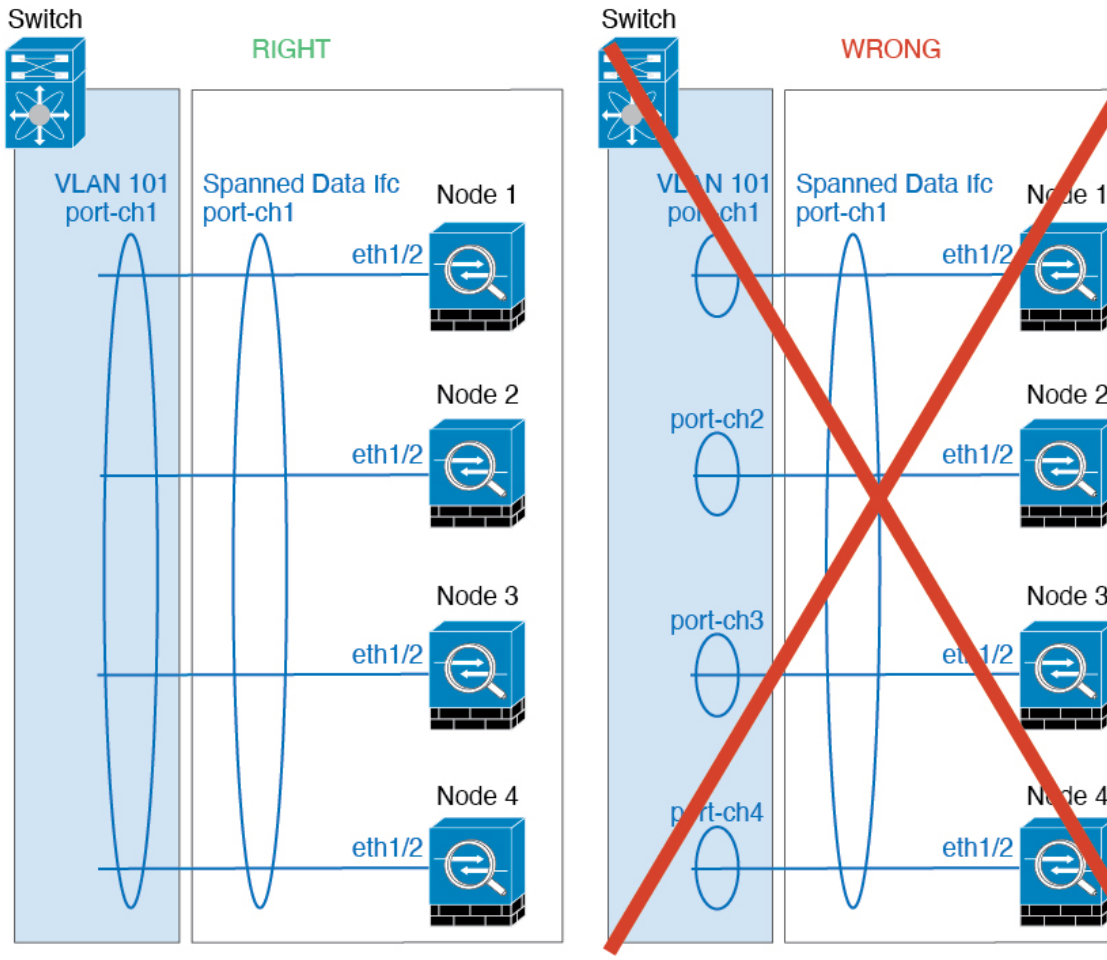
router(config)# **port-channel** *id* **hash-distribution fixed**

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

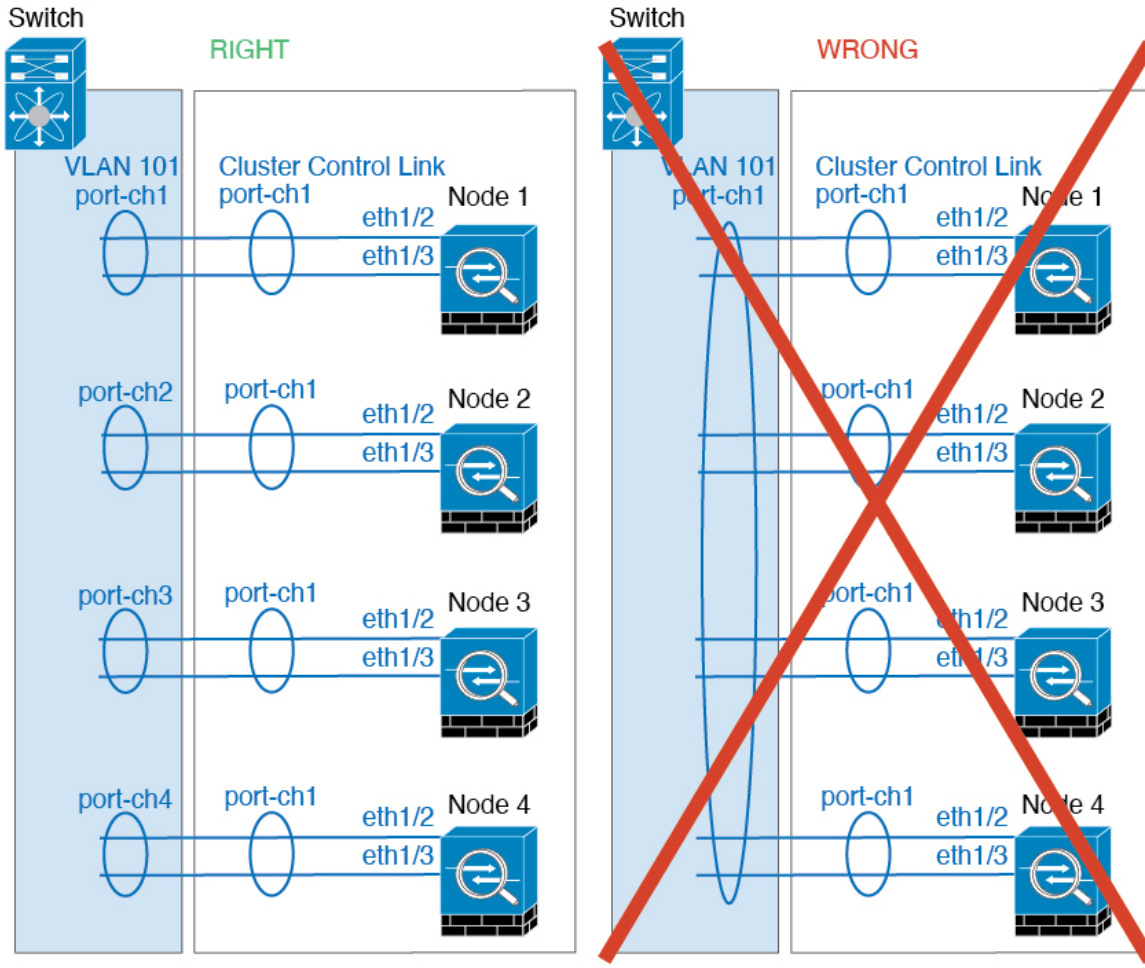
- Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサー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

シャーシ間クラスタリングの EtherChannel

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



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



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ロ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 ディレクタのロールは（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 メンバーがサイト 2 のメンバー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

- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC 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（251 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 にアップロードします。

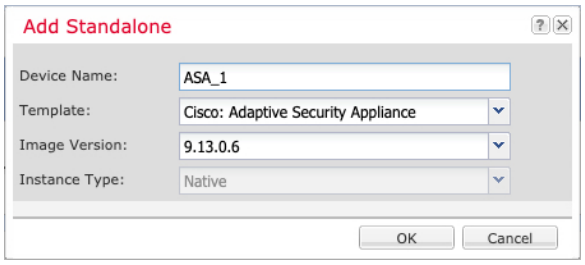
（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および FTD）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

- 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（また、[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示されます）。
- 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 [論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

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

b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。
c) [Image Version] を選択します。
d) [OK] をクリックします。

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

ステップ 3 [データ ポート（Data Ports）] 領域を展開し、デバイスに割り当てる各ポートをクリックします。

以前に [Interfaces] ページで有効にしたデータインターフェイスのみを割り当てることができます。後で、ASA でこれらの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。

ステップ 4 画面中央のデバイス アイコンをクリックします。

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

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。

a) （Firepower 9300 の場合）[セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。
b) [Management Interface] を選択します。

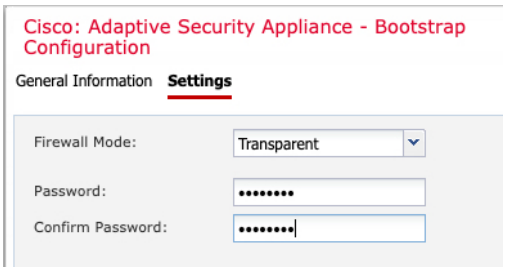
このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。
f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブをクリックします。



ステップ 7 [Firewall Mode] を [Routed] または [Transparent] に指定します。

ルーテッド モードでは、ASA は、ネットワークのルータ 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。

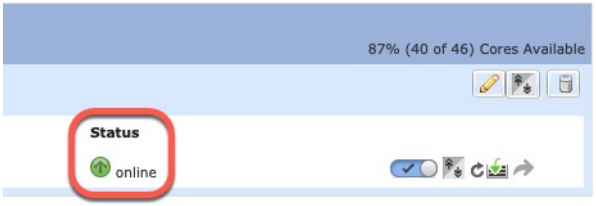
ステップ 8 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザ/パスワードおよびイネーブル パスワードは、パスワードの回復に役立ちます。FXOS アクセスが可能な場合、管理者ユーザ パスワード/イネーブル パスワードを忘れたときにリセットできます。

ステップ 9 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 10 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーション インスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 11 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。

FMC のスタンドアロン FTD を追加します。

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 にアップロードします。

（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（また、[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示されます）。
- 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 （172 ページ）」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 （167 ページ）に従ってリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティ モジュール/エンジン を再度初期化する必要があります。[セキュリティモジュール（Security Modules）] または [セキュリティエンジン（Security Engine）] を選択し、[再初期化（Reinitialize）] をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテ

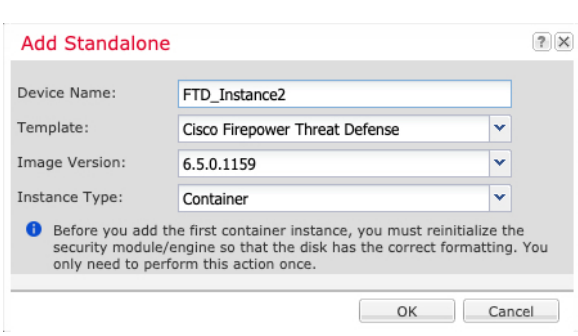
ナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。詳細については、セキュリティモジュール/エンジンの最初期化（321 ページ）を参照してください。

- 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
  - FTD ホスト名とドメイン名

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

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

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

c) [Image Version] を選択します。

d) [インスタンスタイプ（Instance Type）] : [コンテナ（Container）] または [ネイティブ（Native）] を選択します。

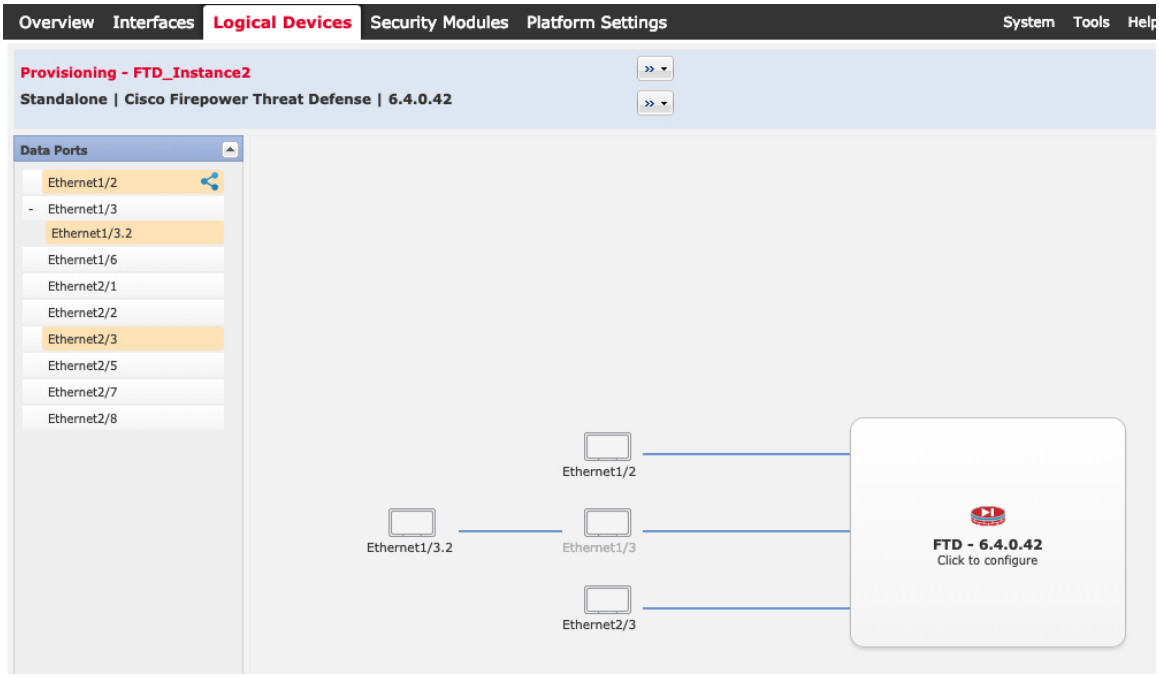
ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。コンテナ インスタンスでは、セキュリティ モジュール/エンジンのリ

ソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

e) [OK] をクリックします。

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

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



[Interfaces] ページでは、以前に有効にしたデータとデータ共有インターフェイスのみを割り当てることができます。後で FMC のこれらの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。

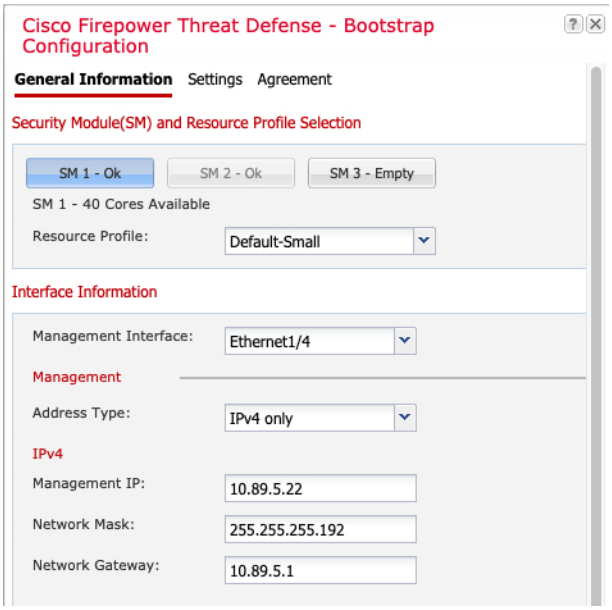
コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナ インスタンスに割り当てることができます。データ共有インターフェイスは [Sharing] アイコン（）で示されます。

ハードウェア バイパス 対応のポートは次のアイコンで表示されます：。特定のインターフェイス モジュールでは、インライン セット インターフェイスに対してのみハードウェア バイパス機能を有効にできます（FMC設定ガイドを参照）。ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェア バイパス ペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェア バイパス 機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

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

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。



a) （Firepower 9300 の場合）[セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。

b) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

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。

c) [Management Interface] を選択します。

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

d) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

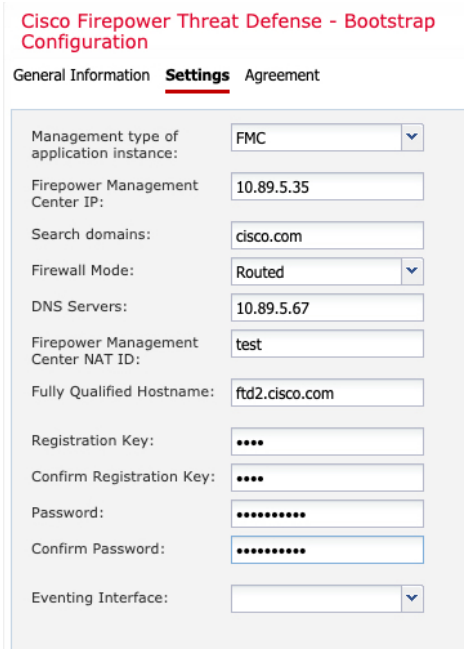
e) [Management IP] アドレスを設定します。

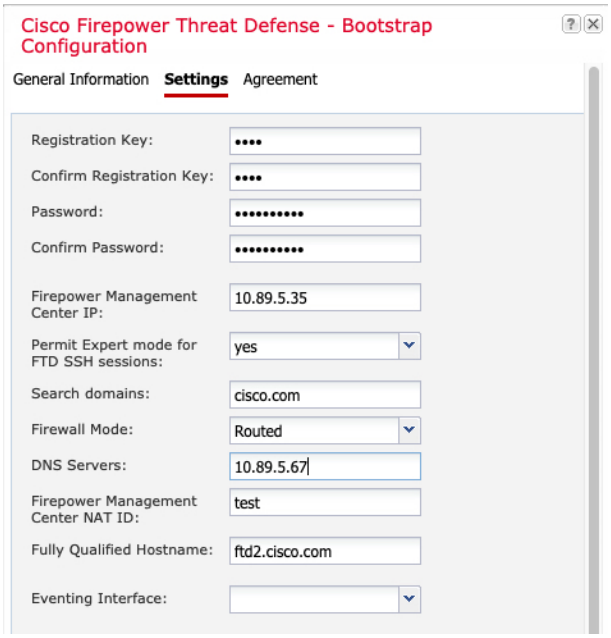
このインターフェイスに一意の IP アドレスを設定します。

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

g) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブで、次の項目を入力します。





a) ネイティブ インスタンスの場合は、[アプリケーションインスタンスの管理タイプ（Management type of application instance）] ドロップダウン リストで [FMC] を選択します。

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。

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

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

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

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

d) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。

e) [Firewall Mode] を [Transparen] または [Routed] に選択します。

ルーテッド モードでは、FTD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。

f) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、FMCのホスト名を指定する場合、FTDは DNS を使用します。

g) FTD の [Fully Qualified Hostname] を入力します。

h) 登録時に FMC とデバイス間で共有する [Registration Key] を入力します。

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

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

j) イベントの送信に使用する [イベンティングインターフェイス（Eventing Interface）] を選択します。指定しない場合は、管理インターフェイスが使用されます。

このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。

k) コンテナインスタンスの場合は、[ハードウェア暗号化（Hardware Crypto）] を [有効（Enabled）] または [無効（Disabled）] に設定します。

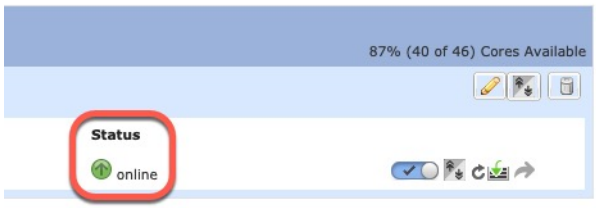
この設定により、ハードウェアの TLS 暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。この機能はデフォルトでイネーブルになっています。セキュリティモジュールごとに最大 16 個のインスタンスについて TLS 暗号化アクセラレーションを有効にできます。この機能は、ネイティブインスタンスでは常に有効になっています。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。

ステップ 7 [利用規約（Agreement）] タブで、エンドユーザ ライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 10 FTD 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。

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 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。

（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

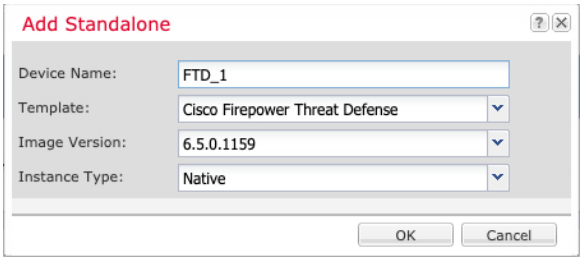
ポートと同じではありません（また、[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示されます）。

- 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 [論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

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

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

c) [Image Version] を選択します。

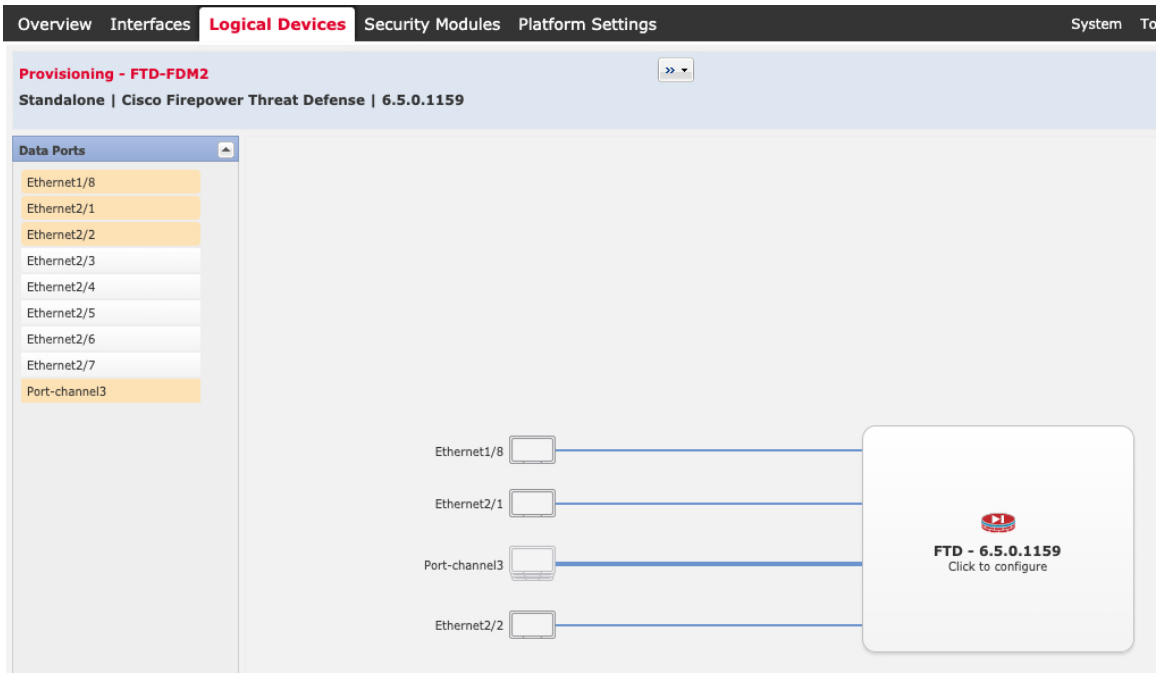
d) [Instance Type] で [Native] を選択します。

コンテナインスタンスは FDM ではサポートされていません。

e) [OK] をクリックします。

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

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。

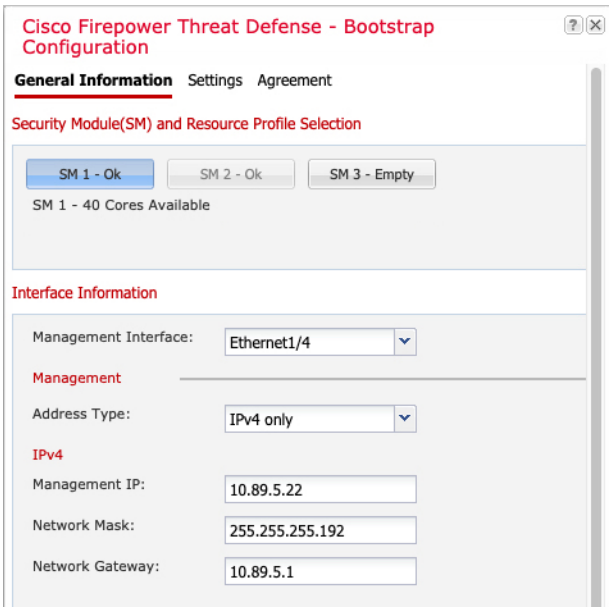


以前に[インターフェイス（Interfaces）]ページで有効にしたデータインターフェイスのみを割り当てることができます。後で FDM でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

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

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。



a) （Firepower 9300 の場合）[セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。

b) [Management Interface] を選択します。

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

c) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

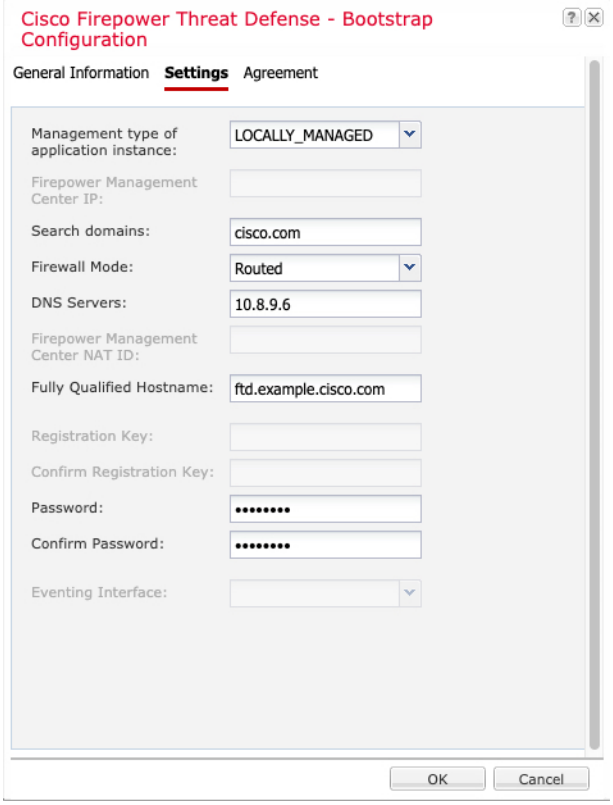
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

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

f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [Settings] タブで、次の手順を実行します。



a) [Management type of application instance] ドロップダウンリストで、[LOCALLY_MANAGED] を選択します。

ネイティブインスタンスは、マネージャとしての Firepower Management Center もサポートしています。論理デバイスの展開後にマネージャを変更すると、設定が消去され、デバイスが再初期化されます。

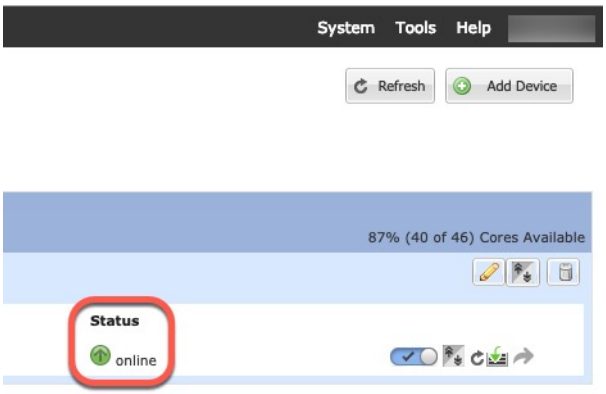
b) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。
c) [Firewall Mode] では [Routed] モードのみサポートされています。
d) [DNS Servers] をカンマ区切りのリストとして入力します。
e) FTD の [Fully Qualified Hostname] を入力します。
f) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

ステップ 7 [利用規約（Agreement）] タブで、エンドユーザライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 10 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。

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 （228 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す。

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。

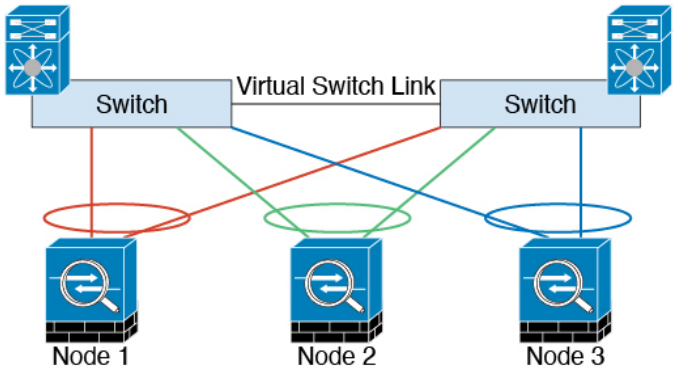
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

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）または仮想ポートチャネル（vPC）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 VSS または vPC 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、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

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

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

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。通常、同じ EtherChannel の異なる VLAN サブインターフェイスを使用するマルチインスタンス クラスタの場合は、VLAN の分離によって異なるクラスタに同じ IP アドレスを使用できます。クラスタを展開するときに、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。

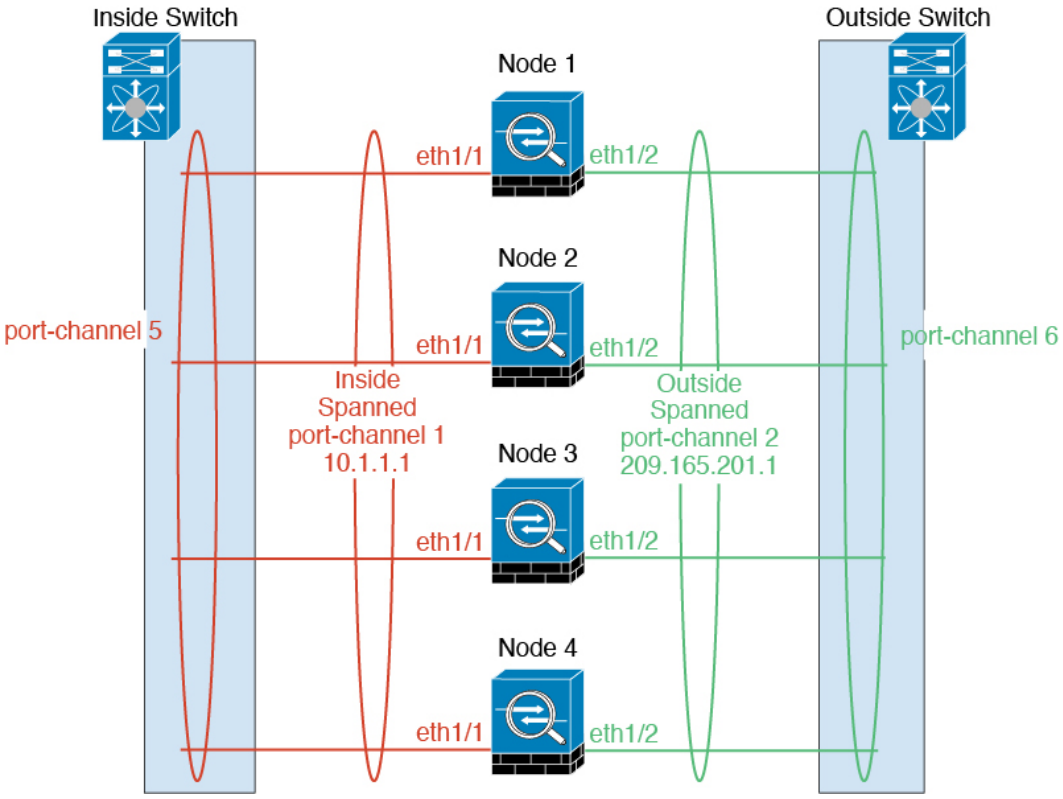
ASA の場合は、メイン クラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の標準出荷単位に属します。アドレス範囲も設定して、現在の標準出荷単位を含む各単位がその範囲内のローカル アドレスを使用できるようにする必要があります。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。標準出荷単位が変更されると、メインクラスタ IP アドレスは新しい標準出荷単位に移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメイン クラスタ 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。

FTD 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、チャネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジ グループ メンバのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。

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



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す。

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 （223 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 （231 ページ）
- サイト間での例：サイト間クラスタリングの例 （304 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、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

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、Firepower4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

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

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

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

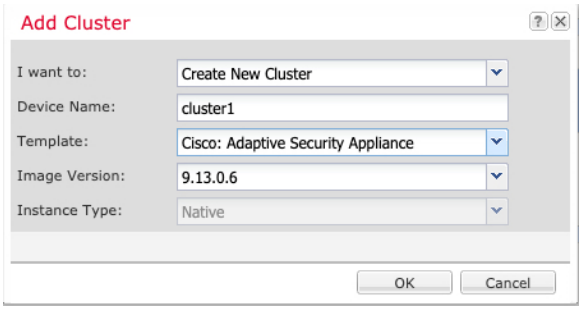
- ゲートウェイ IP アドレス

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 [論理デバイス（Logical Devices）] を選択します。

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



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

b) **デバイス名**を入力します。

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

c) [テンプレート（Template）] には、[Cisco 適応型セキュリティ アプライアンス（Cisco Adaptive Security Appliance）] を選択します。

d) [Image Version] を選択します。

e) [Instance Type] では、[Native] タイプのみがサポートされます。

f) [OK] をクリックします。

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

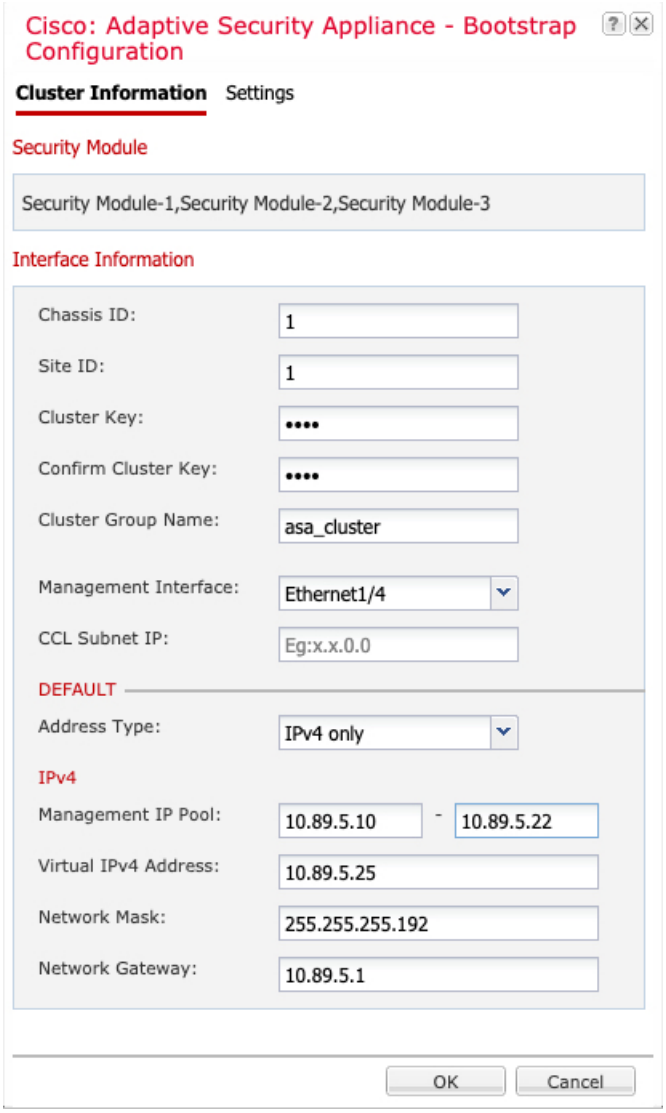
ステップ 4 このクラスタに割り当てるインターフェイスを選択します。

デフォルトでは、すべての有効なインターフェイスが割り当てられています。マルチクラスタタイプのインターフェイスを定義した場合は、すべての選択を解除し、1 つのみ選択します。

ステップ 5 画面中央のデバイス アイコンをクリックします。

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

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



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

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

b) サイト間クラスタリングの場合、[サイト ID（Site ID）] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。

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

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

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

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

e) [Management Interface] を選択します。

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

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

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

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

g) 管理インターフェイスの [アドレスタイプ（Address Type）] を選択します。

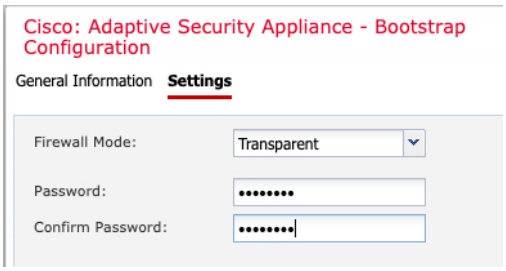
この情報は、ASA設定で管理インターフェイスを設定するために使用されます。次の情報を設定します。

- [管理IPプール（Management IP Pool）]：開始アドレスと終了アドレスをハイフンで区切って入力し、ローカル IP アドレスのプールを設定します。このうちの 1 つがインターフェイス用に各クラスタユニットに割り当てられます。

  最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。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。

- **ネットワークマスク**または**プレフィックス長**
- **ネットワークゲートウェイ**
- [仮想IPアドレス（Virtual IP address）]：現在の制御ユニットの管理 IP アドレスを設定します。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、プールに含まれていてはなりません。

ステップ 7 [Settings] ページで、以下を実行します。



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

ルーテッドモードでは、FTD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。

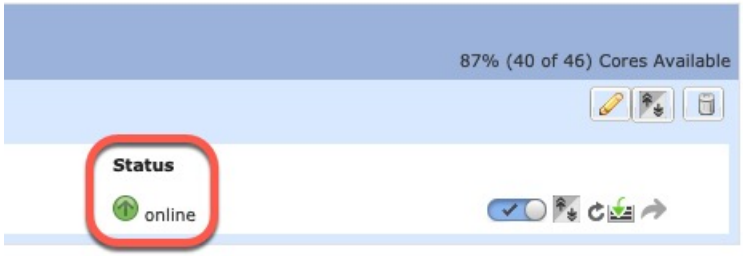
b) 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

事前設定されているASA管理者ユーザ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。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

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



ステップ 10 シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

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

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

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

d) **[OK]** をクリックします。

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

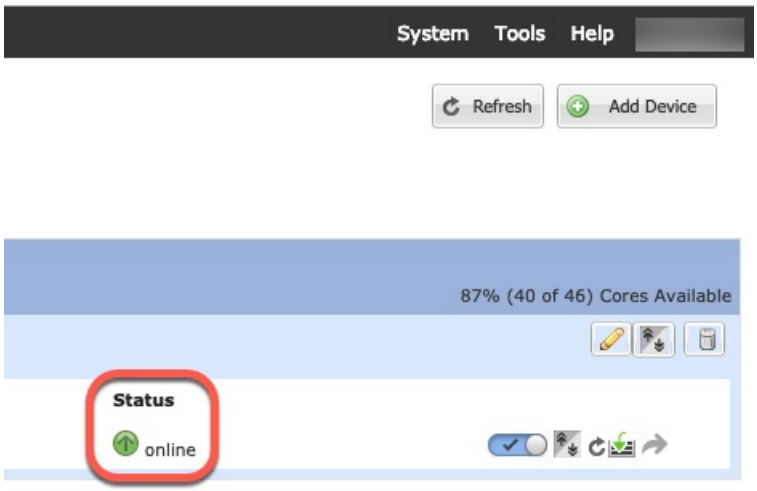
f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **サイト ID（Site ID）**：正しいサイト ID を入力します。
- **クラスタ キー（Cluster Key）**：（事前に入力されていない）同じクラスタ キーを入力します。

[OK] をクリックします。

g) [保存（Save）] をクリックします。

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



ステップ 11 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。

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

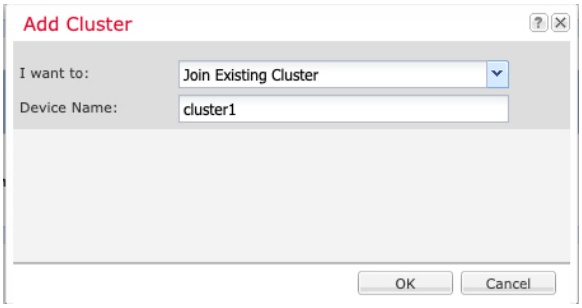
- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。
- マルチ コンテキスト モードでは、最初のクラスタ メンバの ASA アプリケーションでマルチ コンテキスト モードを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

ステップ 2 右上の [設定を表示（Show Configuration）] アイコン（  ）をクリックして、表示されるクラスタの設定をコピーします。

ステップ 3 新しいシャーシの Firepower Chassis Manager に接続して、**[追加（Add）]**>**[クラスタ（Cluster）]** をクリックします。



ステップ 4 **[I want to:]** > **[Join an Existing Cluster]**を選択します。

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

ステップ 6 [OK] をクリックします。

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

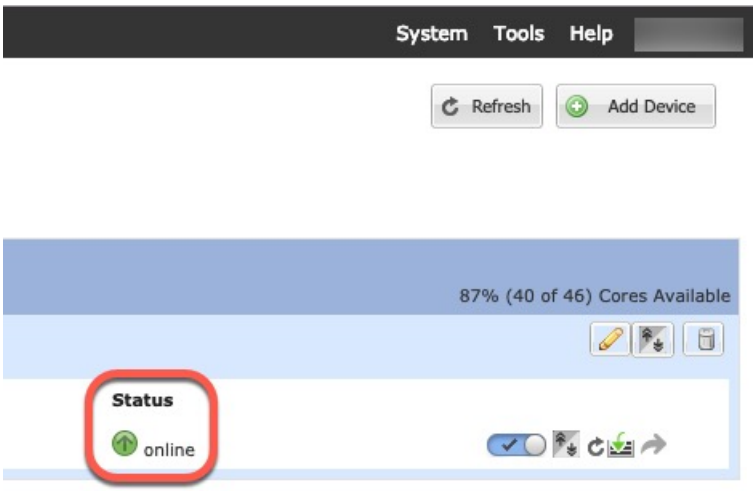
ステップ 8 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **サイト ID（Site ID）**：正しいサイト ID を入力します。
- **クラスタ キー（Cluster Key）**：（事前に入力されていない）同じクラスタ キーを入力します。

[OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

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



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、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

FTD クラスタの作成

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

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

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

始める前に

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

- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、コンテナインスタンスにリソースプロファイルを追加 （167ページ）に従ってリソースプロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティ モジュール/エンジン を再度初期化する必要があります。[Security Modules] または [Security Engine] を選択して、[再初期化（Reinitialize）]アイコン（⟳）をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。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 （321 ページ）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 [論理デバイス（Logical Devices）] を選択します。

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

図 *12 :* ネイティブクラスタ

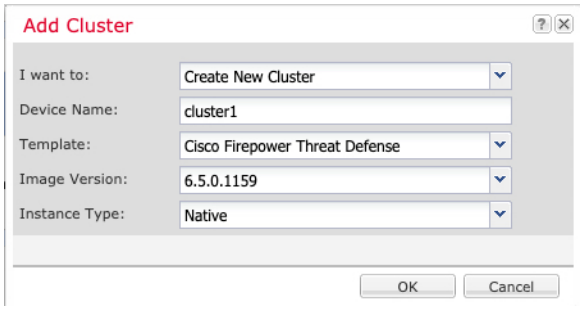
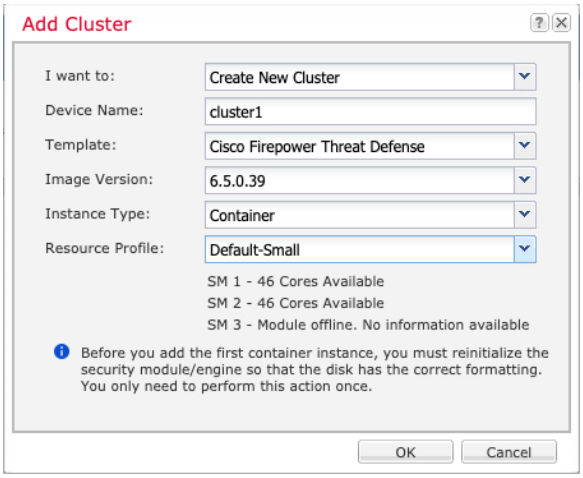
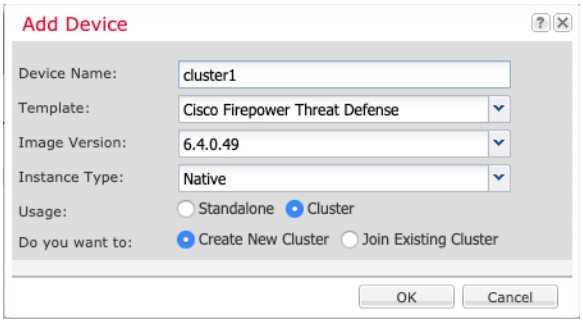


図 *13* : マルチインスタンスクラスタ





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

b) **デバイス名**を入力します。

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

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

d) [Image Version] を選択します。

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

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

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

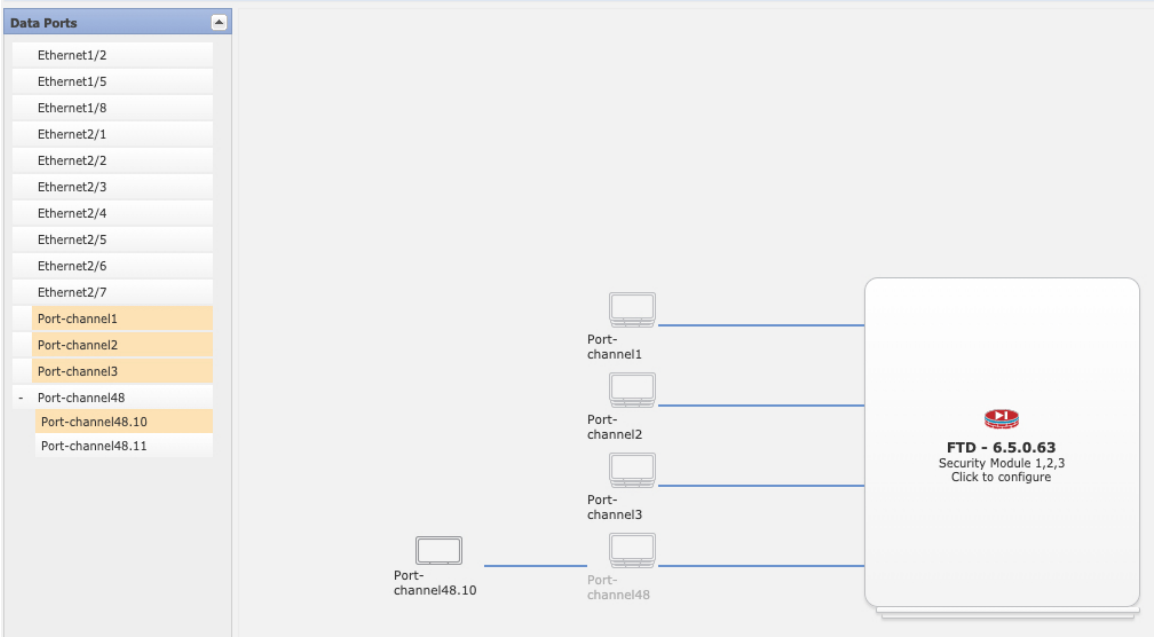
Firepower 9300 の場合、このプロファイルは各セキュリティモジュールの各インスタンスに適用されます。この手順の後半では、セキュリティモジュールごとに異なるプロファイルを設定できます。たとえば、異なるセキュリティモジュールのタイプを使用していて、

ローエンドのモデルでより多くのCPUを使用する場合に設定できます。クラスタを作成する前に、正しいプロファイルを選択することを推奨します。新しいプロファイルを作成する必要がある場合は、クラスタの作成をキャンセルし、コンテナインスタンスにリソースプロファイルを追加 （167 ページ） を使用して 1 つ追加します。

g) [OK] をクリックします。

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

ステップ 4 このクラスタに割り当てるインターフェイスを選択します。



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

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

ステップ 5 画面中央のデバイス アイコンをクリックします。

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

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

図 *14* : ネイティブクラスタ

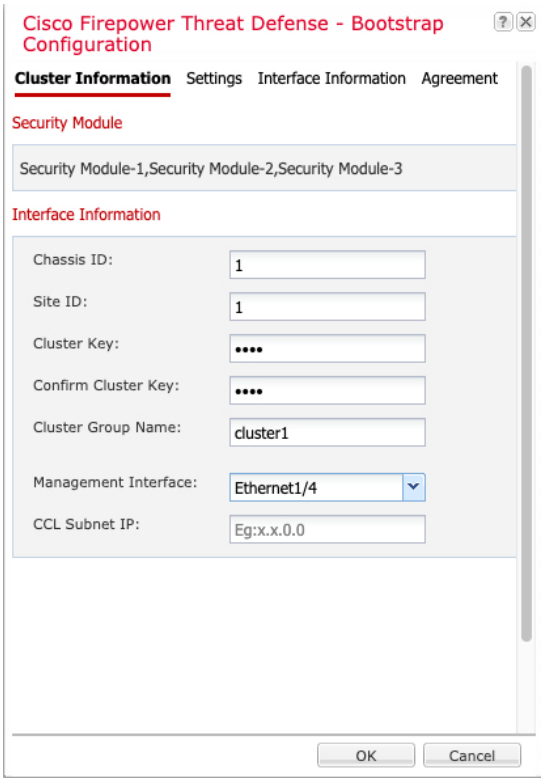
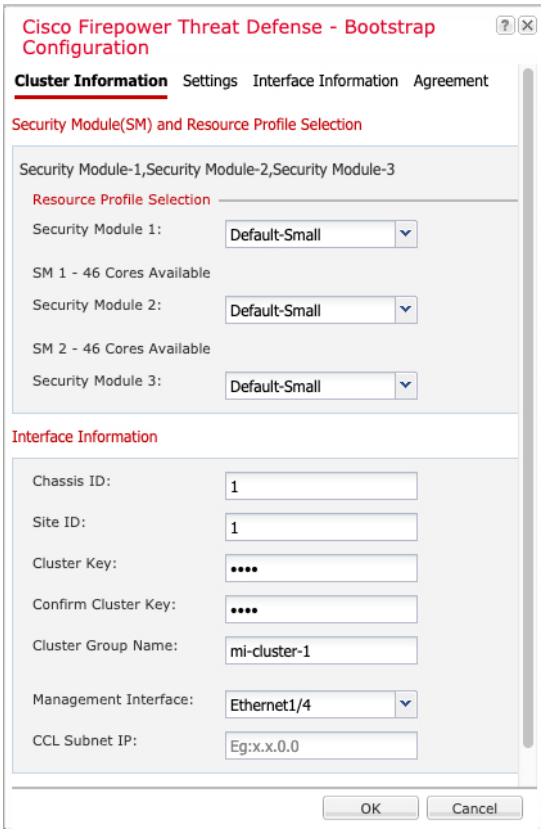


図 *15 :* マルチインスタンスクラスタ



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

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

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

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

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

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送され

るパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

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

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

f) [Management Interface] を選択します。

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

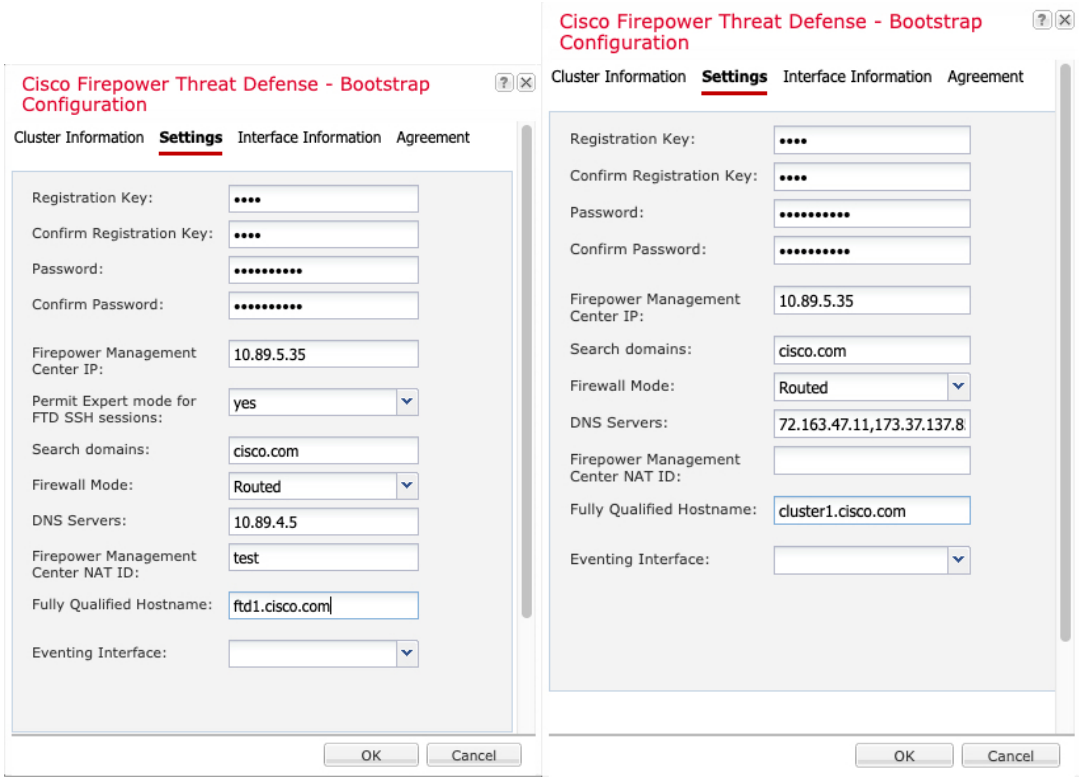
ハードウェア バイパス 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

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

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

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

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



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

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

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

c) [Firepower Management CenterのIP（Firepower Management Center IP）] フィールドに、管理側の FMC の IP アドレスを入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

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

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

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

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

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

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

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

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

たとえば、FMCのホスト名を指定する場合、FTDは DNS を使用します。

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

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。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。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。

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

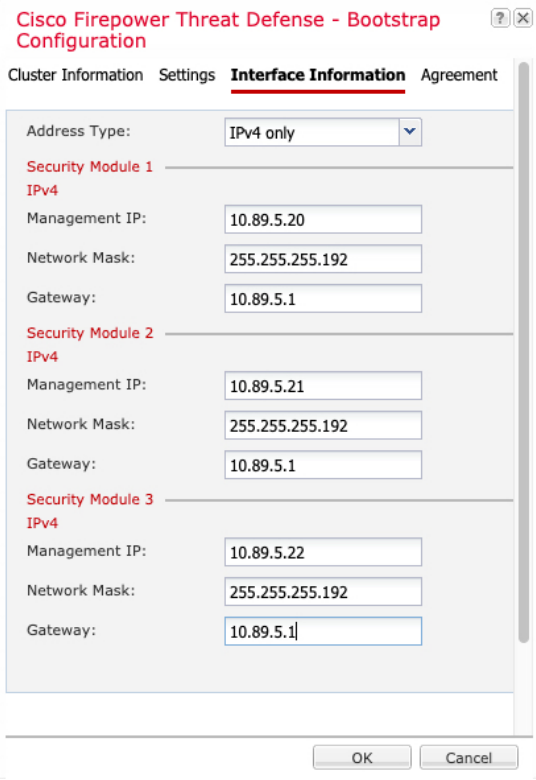
有効な文字は、a ー z の文字、0 ー 9 の数字、ドット（.）、ハイフン（-）です。最大文字数は 253 です。

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

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

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

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



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

モジュールごとに同じネットワーク上の一意の IP アドレスを指定します。

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

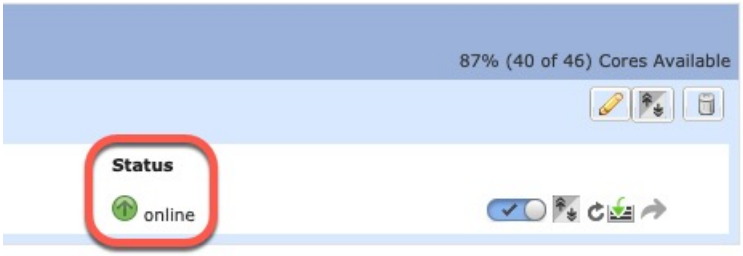
c) **ネットワーク ゲートウェイ** アドレスを入力します。

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

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

ステップ 11 [保存（Save）] をクリックします。

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



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

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

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

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

d) **[OK]** をクリックします。

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

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

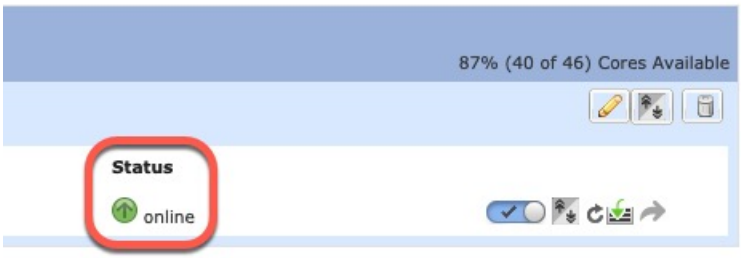
- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。ディレクタのローカリゼーション、サイト冗長性、クラスタフローモビリティなど、冗長性と安定性を向上させることを目的としたサイト間クラスタの追加のカスタマイズは、FMC FlexConfig 機能を使用した場合にのみ設定できます。
- [クラスタ キー（Cluster Key）]：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理 IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

g) [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバーの [論理デバイス（Logical Devices）] ペー

ジで、新しい論理デバイスのステータスを確認します。各クラスタメンバーの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 13 管理 IP アドレスを使用して、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。

クラスタノードの追加

既存のクラスタ内の FTD 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

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

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

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

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

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

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

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

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

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

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

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

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

ステップ 6 **[OK]** をクリックします。

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

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

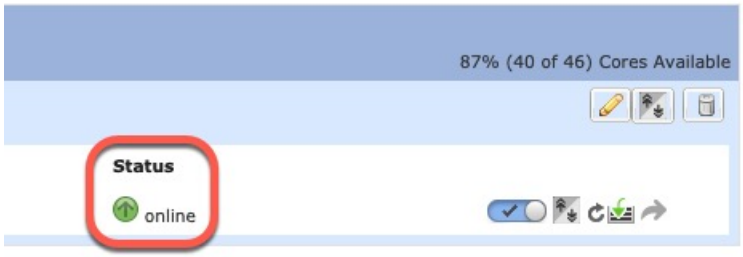
- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。この機能は、FMC FlexConfig 機能を使用した場合にのみ構成可能です。

- [クラスタ キー（Cluster Key）]：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理 IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

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



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 FTD 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 FTD 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（115 ページ）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 4115
  - Firepower 4120
  - Firepower 4125
  - Firepower 4140
  - Firepower 4145
  - Firepower 4150

（注） Radware DefensePro プラットフォームは、Firepower 4110 デバイスの ASA では現在サポートされていません。

- FTD：Radware DefensePro プラットフォームは、次のモデルの FTD 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

（注） すべての FTD プラットフォームでは、CLI を使用して Radware DefensePro を導入する必要があります。Firepower Chassis Manager は、この機能をサポートしていません。

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 FTD 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。

（注） vDP アプリケーションを設定し、この手順の最後で変更を確定すると、論理デバイス（ASA または FTD）が再起動します。

Firepower 4120 または 4140 セキュリティ アプライアンス上で ASA の前に Radware vDP をインストールする場合、FXOS CLI を使用してデコレータを展開する必要があります。Radware DefensePro を、Firepower 4100 デバイス上で ASA の前にあるサービス チェーンにインストールして設定する方法の詳細な CLI 手順については、『FXOS CLI Configuration Guide』を参照してください。

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 （66 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにアップロードします（セキュリティアプライアンスへのイメージのアップロード （66 ページ）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 （282 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 （195 ページ）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 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。

[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが表示されます。

ステップ 3 スタンドアロン ASA または FTD 論理デバイスを作成します（スタンドアロン ASA の追加 （237 ページ） または FMC のスタンドアロン FTD を追加します。 （240 ページ）を参照）。

ステップ 4 [デコレータ（Decorators）] 領域で、[vDP] を選択します。[Radware: Virtual DefensePro - 設定（Radware: Virtual DefensePro - Configuration）] ウィンドウが表示されます。[一般情報（General Information）] タブで、次のフィールドを設定します。

ステップ 5 Firepower 4100/9300 シャーシ に複数の vDP バージョンをアップロードしている場合は、[バージョン（Version）] ドロップダウンから使用するバージョンを選択します。

ステップ 6 リソース構成可能な Radware DefensePro アプリケーションがある場合は、[Resource Profile] ドロップダウンの下に、サポートされているリソースプロファイルのリストが表示されます。デバイスに割り当てるリソース プロファイルを選択してください。リソース プロファイルを選択しない場合、デフォルトの設定が使用されます。

ステップ 7 [Management Interface] ドロップダウンで、この手順のステップ 1 で作成した管理インターフェイスを選択します。

ステップ 8 デフォルトの [アドレス タイプ（Address Type）]（[IPv4 のみ（IPv4 only）]、[IPv6 のみ（IPv6 only）]、または [IPv4 および IPv6（IPv4 and IPv6）]）を選択します。

ステップ 9 前のステップで選択した [アドレス タイプ（Address Type）] に基づいて次のフィールドを設定します。

a) [管理 IP（Management IP）] フィールドには、ローカル IP アドレスを設定します。

b) IPv4 のみ（IPv4 only）：[ネットワーク マスク（Network Mask）] を入力します。

IPv6 のみ（IPv6 only）：[プレフィックス長（Prefix Length）] を入力します。

c) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 10 デバイスに割り当てる各データ ポートの横にあるチェックボックスをクリックします。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

FXOS は、指定したソフトウェア バージョンをダウンロードし、指定したセキュリティ モジュールにブートストラップ コンフィギュレーション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。

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 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

Radware DefensePro イメージをインストールして ASA または FTD シャーシ内クラスタの前にサービスチェーンを設定するには、次の手順に従います。

（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 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 （66 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにアップロードします（セキュリティアプライアンスへのイメージのアップロード （66 ページ）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（195 ページ）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 または FTD シャーシ内クラスタを設定します（ASA クラスタの作成（257 ページ） または FTD クラスタの作成（265 ページ） を参照）。

シャーシ内クラスタを設定する手順の最後で [保存（Save）] をクリックする前に、以下のステップに従ってクラスタに vDP デコレータを追加しておく必要があります。

ステップ 3 [デコレータ（Decorators）] 領域で、[vDP] を選択します。[Radware: Virtual DefensePro - 設定（Radware: Virtual DefensePro - Configuration）] ダイアログボックスが表示されます。[一般情報（General Information）] タブで、次のフィールドを設定します。

ステップ 4 Firepower 4100/9300 シャーシ に複数の vDP バージョンをアップロードした場合は、使用する vDP バージョンを [バージョン（Version）] ドロップダウンで選択します。

ステップ 5 リソース構成 Radware DefensePro アプリケーションがある場合は、[リソース プロファイル（Resource Profile）] ドロップダウンの下に、サポートされているリソース プロファイルのリストが表示されます。デバイスに割り当てるリソース プロファイルを選択してください。リソース プロファイルを選択しない場合、デフォルトの設定が使用されます。

ステップ 6 [Management Interface] ドロップダウンで管理インターフェイスを選択します。

ステップ 7 vDP デコレータに割り当てる各データ ポートの横にあるチェックボックスをクリックします。

ステップ 8 [インターフェイス情報（Interface Information）] タブをクリックします。

ステップ 9 使用する [アドレス タイプ（Address Type）]（[IPv4 のみ（IPv4 only）]、[IPv6 のみ（IPv6 only）]、または [IPv4 および IPv6（IPv4 and IPv6）]）を選択します。

ステップ 10 各セキュリティ モジュールで、次のフィールドを設定します。表示されるフィールドは、前のステップで選択した [アドレス タイプ（Address Type）] により異なります。

a) [管理 IP（Management IP）] フィールドには、ローカル IP アドレスを設定します。

b) IPv4 のみ（IPv4 only）：[ネットワーク マスク（Network Mask）] を入力します。

IPv6 のみ（IPv6 only）：[プレフィックス長（Prefix Length）] を入力します。

c) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

FXOS は、指定したソフトウェア バージョンをダウンロードし、指定したセキュリティ モジュールにブートストラップ コンフィギュレーション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。

ステップ 13 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。

ステップ 14 設定された論理デバイスのリストをスクロールして vDP のエントリを表示します。[Management IP] 列に示されている属性を確認します。

- [CLUSTER-ROLE] 要素の DefensePro インスタンスが「*unknown*」と表示される場合は、vDP クラスタの作成を完了するために、DefensePro アプリケーションを入力して制御ユニットの IP アドレスを設定する必要があります。
- [CLUSTER-ROLE] 要素の DefensePro インスタンスが「*primary*」または「*secondary*」と表示される場合は、アプリケーションはオンラインで、クラスタ化されています。

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 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、FTD および FXOS バージョンと必要な TSL 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 暗号アクセラレーションに関するガイドラインと制限事項

FTD 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 FTD 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 FTD 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 FTD がある場合は、 FTD 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 FTD 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、FTD は SSL ポリシー

の [復号化不可のアクション（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、FTD 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。FTD 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が、TLS 暗号化アクセラレーション をサポートする FTD 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FTDがオーバーサブスクライブされた場合、FTD によって受信されるパケットの扱いは、SSL ポリシーの [復号化不可のアクション（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 FTD 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 を追加します。 （240 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 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。

FTD リンク状態の同期を有効にします。

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、 FTD が処理できるようになる前に外部ルータが FTD 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。

手順

ステップ1 [論理デバイス（Logical Devices）] を選択し、FTD論理デバイスに対してドロップダウンリストから[リンク状態の有効化（Enable Link State）] を選択します。

この機能を無効にするには、[リンク状態の無効化（Disable Link State）] を選選択します。

ステップ2 インターフェイスの現在の状態と最後のダウンの理由を表示します。

show interface expand detail

例：

```
Firepower # 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
    Udld 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:
<...>
```

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 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。

[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。

ステップ 2 削除する論理デバイスの [削除（Delete）] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、この論理デバイスを削除することを確認します。

ステップ 4 [はい（Yes）] をクリックして、このアプリケーション設定を削除することを確認します。

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。

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：Firepower Chassis Manager の [論理デバイス（Logical Devices）] ページで **有効なスライダ**（  ）をクリックします。**無効なスライダ**（  ）を使用して後で再度有効にすることができます。

- セキュリティ モジュール/エンジン のシャットダウン：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。

- 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。

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

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が尋ねられます。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 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。

[論理デバイス（Logical Devices）] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。論理デバイスのリストの下に、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 インスタンスのリストが表示されます。

ステップ 2 削除するアプリケーション インスタンスの [削除（Delete）] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、このアプリケーション インスタンスを削除することを確認します。

FTD 論理デバイスのインターフェイスの変更

FTD 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、または管理インターフェイスの置き換え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、FTD 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、FTD 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 （195 ページ）およびEtherChannel（ポート チャネル）の追加 （196 ページ）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。
- 管理インターフェイスまたはイベントインターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。FTD デバイスの再起動（管理インターフェイスの変更により再起動）後、FMC または FDM で設定を同期すると、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- 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。

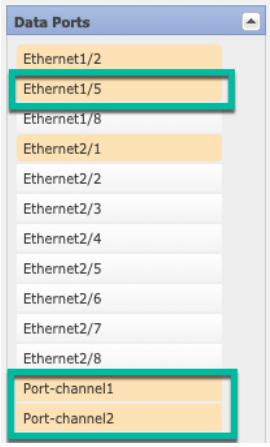
手順

ステップ 1 Firepower Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 右上にある [編集（Edit）] アイコンをクリックして、その論理デバイスを編集します。

ステップ 3 [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。

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 次のように、管理インターフェイスまたはイベントインターフェイスを置き換えます。

これらのタイプのインターフェイスでは、変更を保存するとデバイスがリブートします。

a) ページ中央のデバイス アイコンをクリックします。
b) [一般（General）] または [クラスタ情報（Cluster Information）] タブで、ドロップダウン リストから新しい [管理インターフェイス（Management Interface）] を選択します。
c) [設定（Settings）] タブで、ドロップダウン リストから新しい [イベント インターフェース（Eventing Interface）] を選択します。
d) [OK] をクリックします。

管理インターフェイスの IP アドレスを変更した場合は、FMC でデバイスの IP アドレスを変更する必要もあります。**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス/クラスタ（Device/Cluster）]** と移動します。[Management] 領域で、ブートストラップ設定アドレスと一致するように IP アドレスを設定します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 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、FTD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。

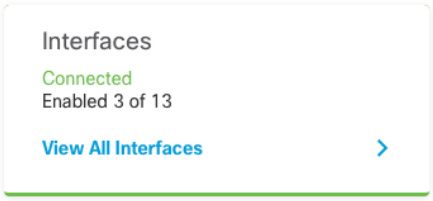
g) **[Save（保存）]** をクリックします。

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 7 FDM でインターフェイスを同期して移行します。

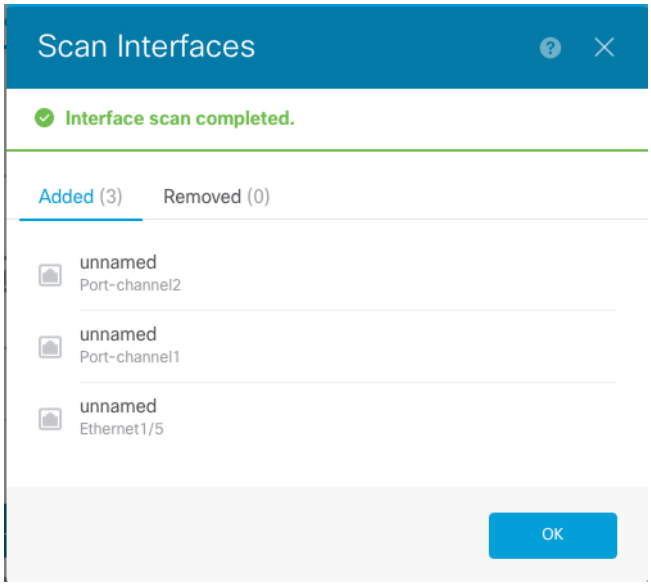
a) FDM にログインします。

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。

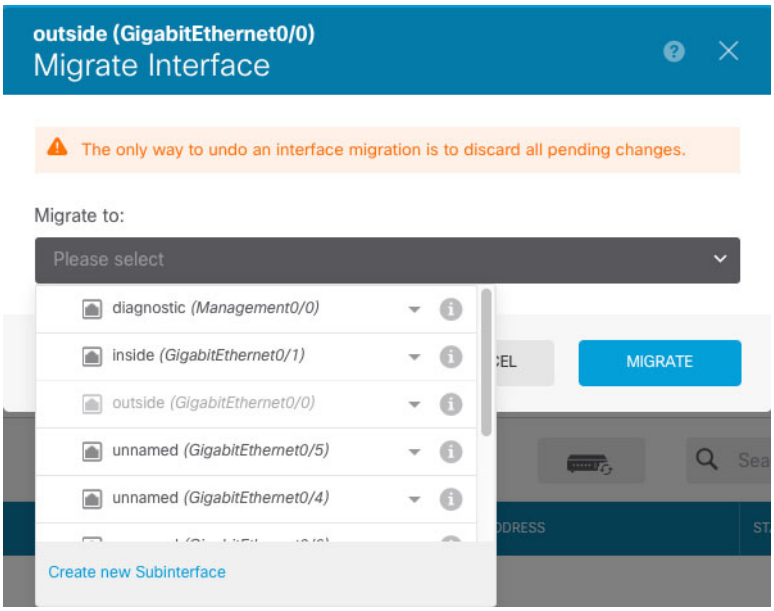
削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、古いインターフェイスをダミーの名前と IP アドレスで再設定する必要があります。

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。

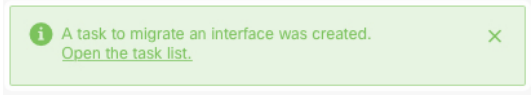
[置換（Replace）] アイコン

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。

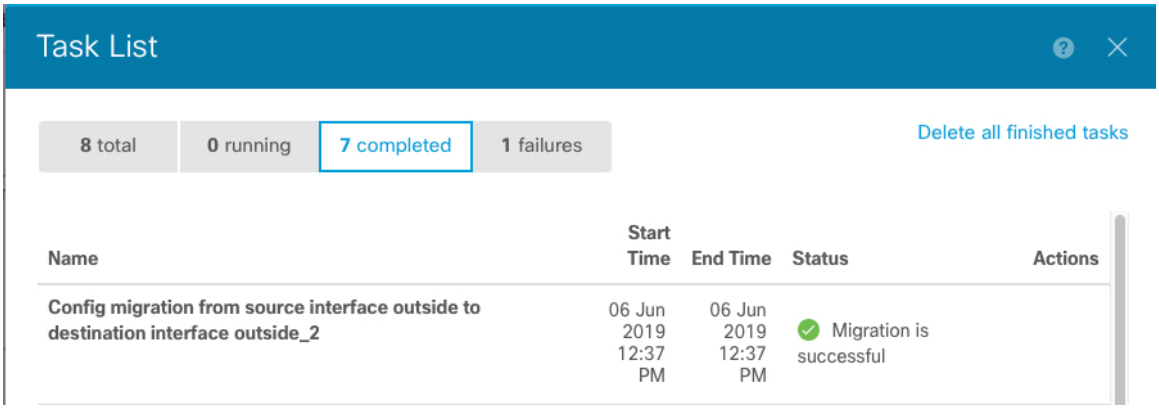
g) [交換用インターフェイス（Replacement Interface）]：ドロップダウン リストから新しいインターフェイスを選択します。



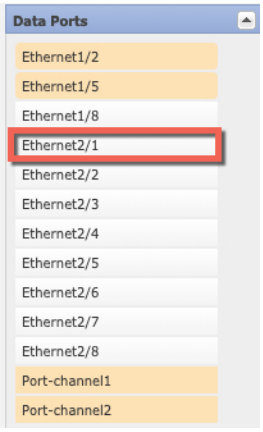
h) [インターフェイス（Interfaces）] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。



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。



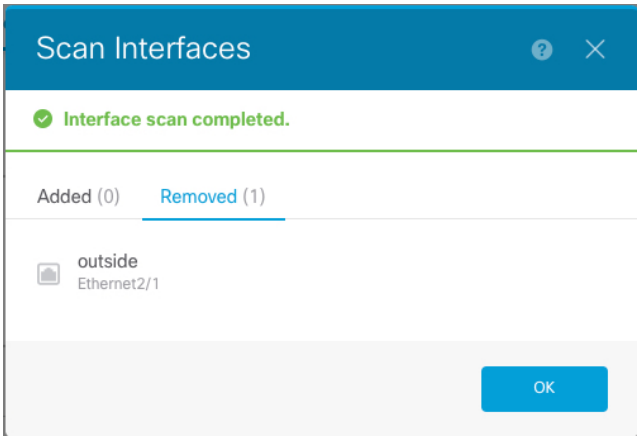
ステップ 8 Firepower Chassis Manager でデータインターフェイスの割り当てを解除するには、[データ ポート（Data Ports）] 領域でそのインターフェイスの選択を解除します。



ステップ 9 [Save] をクリックします。

ステップ 10 FMC または FDM でインターフェイスを再度同期します。

図 *16 : 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 （195 ページ）およびEtherChannel（ポート チャネル）の追加 （196 ページ）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。
- 管理インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つあるEtherChannelを作成し、現在の管理インターフェイスをそのEtherChannelに置き換える必要があります。ASAがリロードし（管理インターフェイスを変更するとリロードします）、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- 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 Firepower Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 右上にある [編集（Edit）] アイコンをクリックして、その論理デバイスを編集します。

ステップ 3 データ インターフェイスの割り当てを解除するには、[データ ポート（Data Ports）] 領域でそのインターフェイスの選択を解除します。

ステップ 4 [データ ポート（Data Ports）] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。

ステップ 5 次のように、管理インターフェイスを置き換えます。

このタイプのインターフェイスでは、変更を保存するとデバイスがリロードします。

a) ページ中央のデバイス アイコンをクリックします。

b) [一般/クラスタ情報（General/Cluster Information）] タブで、ドロップダウン リストから新しい [管理インターフェイス（Management Interface）] を選択します。

c) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

論理デバイスのブートストラップ設定の変更または回復

論理デバイスのブートストラップ設定は、変更することができます。変更した後、直ちに新しい設定を使用してアプリケーションを再起動することも、変更を保存しておいて後で新しい設定を使用してアプリケーション インスタンスを再起動することもできます。

手順

ステップ 1 Firepower Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 右上にある [編集（Edit）] アイコンをクリックして、その論理デバイスを編集します。

ステップ 3 ページ中央のデバイス アイコンをクリックします。

ステップ 4 必要に応じて論理デバイスの設定を変更します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Restart Now] をクリックすると、変更を保存してアプリケーション インスタンスを再起動でるようになります。アプリケーション インスタンスを再起動せずに変更を保存するには、[Restart Later] をクリックします。

（注） [Restart Later] を選択した場合、アプリケーション インスタンスを再起動する準備が整ってから、[Logical Devices] ページで [Restart Instance] をクリックしてアプリケーション インスタンスを再起動できます。

[論理デバイス（Logical Devices）] ページ

Firepower Chassis Manager の [Logical Devices] ページを使用して、論理デバイスを作成、編集、削除します。[Logical Devices] ページには、各 Firepower 4100/9300 シャーシ セキュリティ モジュール/エンジンにインストールされている論理デバイスの情報エリアが含まれています。

各論理デバイス エリアのヘッダーには次の情報が含まれています。

- 論理デバイスの一意の名前。
- 論理デバイスのモード（スタンドアロンまたはクラスタ）。
- [Status]：論理デバイスの状態を示します。
  - [ok]：論理デバイスの設定は完了しています。
  - [設定未完了（incomplete-configuration）]：論理デバイス設定は未完了です。

各論理デバイス エリアには次の情報が含まれます。

- [Application]：セキュリティ モジュールで実行しているアプリケーションを示します。
- [Version]：セキュリティ モジュールで実行しているアプリケーションのソフトウェア バージョン番号を示します。

（注） FTD の論理デバイスへの更新は FMC を使用して行います。Firepower Chassis Manager の **[論理デバイス（Logical Devices）]** > **[編集（Edit）]** および **[システム（System）]** > **[更新（Updates）]** ページには反映されません。これらのページで、表示されるバージョンは、FTD論理デバイスを作成するために使用されたソフトウェア バージョン（CSP イメージ）を示します。

- [Resource profile]：論理デバイス/アプリケーション インスタンスに割り当てられたリソース プロファイルを表示します。
- [Management IP]：論理デバイス管理 IP として割り当てられているローカル IP アドレスを示します。
- [Gateway]：アプリケーション インスタンスに割り当てられているネットワーク ゲートウェイ アドレスを示します。
- [Management Port]：アプリケーション インスタンスに割り当てられている管理ポートを示します。
- [Status]：アプリケーション インスタンスの状態を示します。
  - [オンライン（Online）]：アプリケーションは実行中であり、動作しています。
  - [オフライン（Offline）]：アプリケーションは停止され、使用できません。
  - [インストール（Installing）]：アプリケーションのインストールを実行しています。
  - [未インストール（Not Installed）]：アプリケーションがインストールされていません。
  - [インストール失敗（Install Failed）]：アプリケーションのインストールに失敗しました。
  - [起動中（Starting）]：アプリケーションを起動しています。
  - [起動失敗（Start Failed）]：アプリケーションの起動に失敗しました。
  - [開始（Started）]：アプリケーションは正常に開始し、アプリケーション エージェントのハートビートを待機しています。
  - [停止中（Stopping）]：アプリケーションは停止処理中です。
  - [停止失敗（Stop Failed）]：アプリケーションをオフラインにできませんでした。

- [Not Responding]：アプリケーションは応答不能です。
- [Updating]：アプリケーション ソフトウェアの更新が進行中です。
- [Update Failed]：アプリケーション ソフトウェアの更新に失敗しました。
- [Update Succeeded]：アプリケーション ソフトウェアの更新に成功しました。
- [Unsupported]：このインストール済みアプリケーションはサポートされていません。

セキュリティ モジュールが存在しないか障害状態の場合は、その情報がステータス フィールドに表示されます。情報アイコンにカーソルを合わせると、障害に関する詳細情報が表示されます。セキュリティ モジュールの障害について詳しくは、FXOS セキュリティ モジュール/セキュリティ エンジンについて （317 ページ）を参照してください。

- **[Expanded Information]** 領域：現在実行中のアプリケーション インスタンスの追加属性を示します。

（注） アプリケーションのブートストラップ設定を変更した後、直ちにアプリケーション インスタンスを起動しなければ、[Attributes] フィールドには現在実行中のアプリケーションに関する情報が表示され、アプリケーションを再起動するまで変更は反映されません。

- [Ports]：アプリケーション インスタンスに割り当てられたインターフェイスの名前とタイプを示します。
- [Cluster Operation Status]：アプリケーション インスタンスに割り当てられている管理 URL を示します。
- [Management IP/Firepower Management IP]：アプリケーション インスタンスに割り当てられている管理 IP アドレスを示します。
- [クラスタロール（Cluster Role）]：アプリケーション インスタンスのクラスタロール（制御またはデータ）を示します。
- [Cluster IP]：アプリケーション インスタンスに割り当てられている IP アドレスを示します。
- [HA Role]：アプリケーション インスタンス、アクティブまたはスタンバイのハイ アベイラビリティ ロールを示します。
- [Management URL]：アプリケーション インスタンスに割り当てられている管理アプリケーションの URL を示します。
- [UUID]：アプリケーション インスタンスの汎用一意識別子を示します。

Firepower Chassis Manager の [Logical Devices] ページから、論理デバイスに対して次の機能を実行できます。

- [Refresh]：[Logical Devices] ページに表示されている情報が更新されます。
- [Add Device]：論理デバイスを作成できます。
- [Edit]：既存の論理デバイスを編集できます。
- **[Set Version]**：論理デバイス上のソフトウェアをアップグレードまたはダウングレードできます。
- [Delete]：論理デバイスが削除されます。
- [Show Configuration]：ダイアログボックスが開き、論理デバイスまたはクラスタの構成情報が JSON 形式で表示されます。クラスタに含める追加デバイスを作成する際は、この構成情報をコピーして使用できます。
- [Enable/Disable]：アプリケーション インスタンスが有効化/無効化されます。
- [Upgrade/Downgrade]：アプリケーション インスタンスをアップグレード/ダウングレードできます。
- [Restart Instance]：アプリケーション インスタンスを再起動できます。デバイスのブートストラップ情報を変更した後、アプリケーションインスタンスをまだ再起動していない場合、[Restart Instance] をクリックすることで、既存の管理ブートストラップ情報をクリアし、新しいブートストラップ情報を使用してアプリケーションインスタンスを再起動できます。
- [Reinstall instance]：アプリケーションインスタンスを再インストールできます。
- [デバイスマネージャに移動（Go To Device Manager）]：アプリケーション インスタンスに定義されている FMC または ASDM へのリンクを提示します。
- [リンク状態の有効化/無効化（Enable/Disable Link State）]：FTD リンク状態の同期を有効または無効にします。詳細については、FTD リンク状態の同期を有効にします。 （288 ページ）を参照してください。

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 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

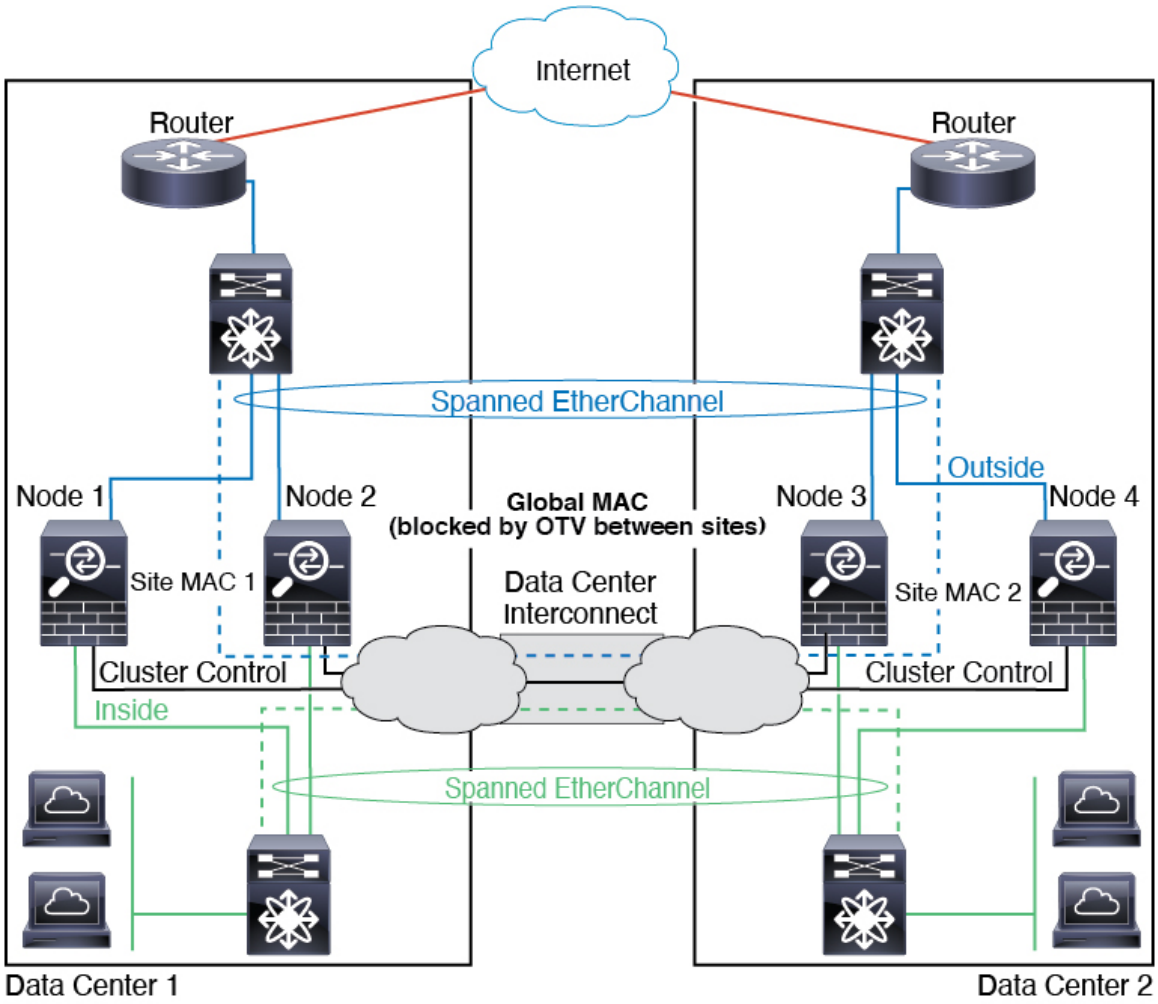
を使用してローカルスイッチに接続します。各EtherChannelは、クラスタ内のすべてのシャーシにスパンされます。

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。



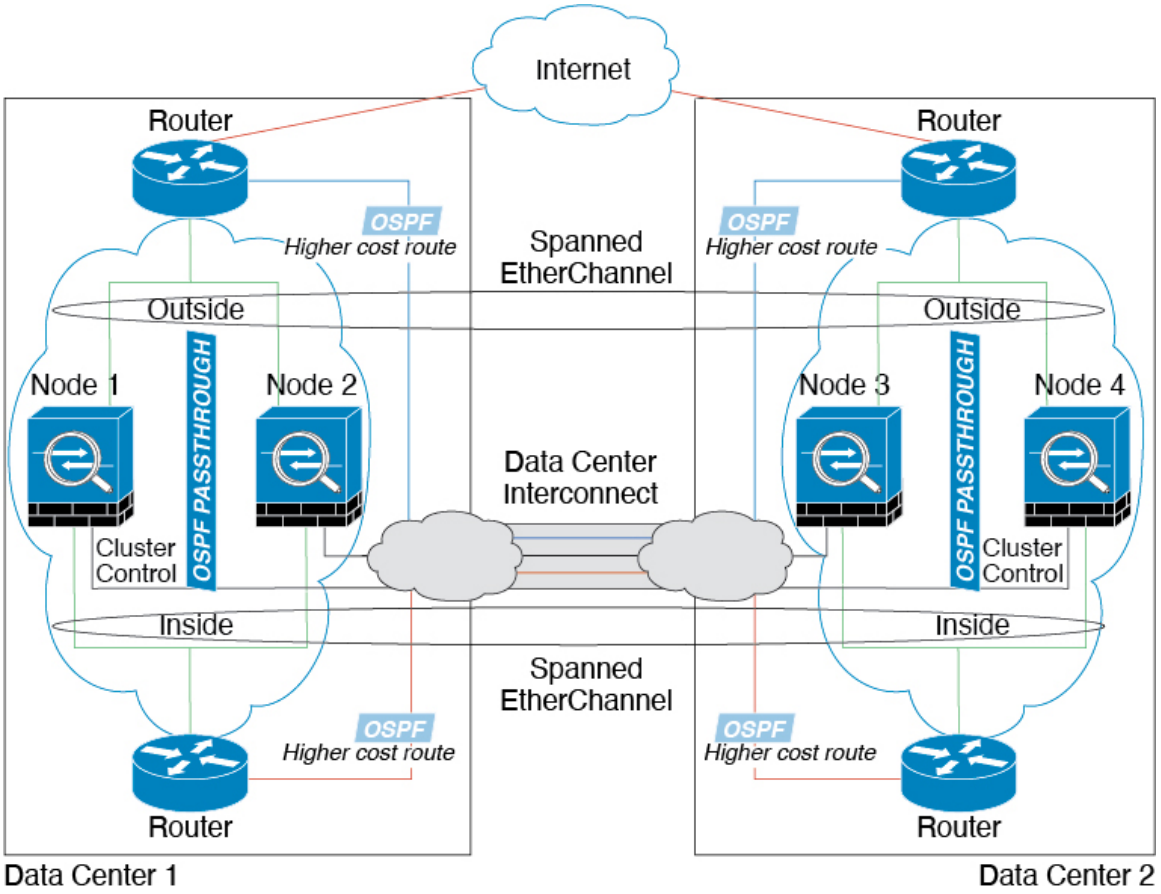
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

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。

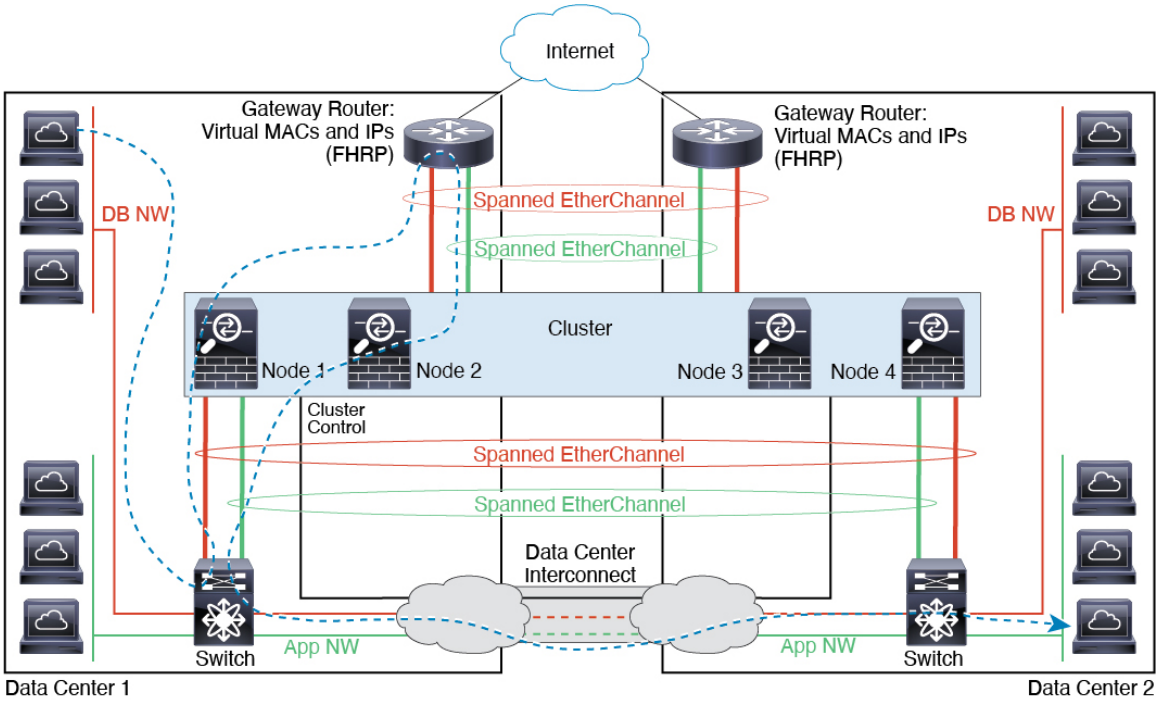
- サイト間 VSS/vPC：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、VSS/vPC トラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCI が余分なトラフィックを処理できる場合、必要に応じて、各ノードを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS/vPC：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 VSS/vPC 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 VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。



スパンド 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、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
FTD 動作リンク状態と物理リンク状態の同期	2.9.1	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、 FTD が処理できるようになる前に外部ルータが FTD 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。 （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。 新規/変更された Firepower Chassis Manager 画面：[Logical Devices] > [Enable Link State] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail**
コンテナインスタンス向けの FMC を使用した FTD 設定のバックアップと復元	2.9.1	FTD 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。 新規/変更された FMC 画面：[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）] 新規/変更された FTD CLI コマンド：**restore** サポートされるプラットフォーム：Firepower 4100/9300 （注） Firepower 6.7 が必要です。

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	コンテナインスタンスを使用してクラスタを作成できるようになりました。Firepower 9300 では、クラスタ内の各モジュールに 1 つのコンテナインスタンスを含める必要があります。セキュリティエンジン/モジュールごとに複数のコンテナインスタンスをクラスタに追加することはできません。クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。 新規/変更された画面： • **[論理デバイス（Logical Devices）] > [クラスタの追加（Add Cluster）]** • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] > [タイプ（Type）] フィールド （注） Firepower 6.6 以降が必要です。
FDM での FTD のサポート	2.7.1	ネイティブ FTD 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。 新規/変更された Firepower Chassis Manager 画面： **[Logical Devices] > [Add Device] > [Settings] > [Management type of application instance]** （注） FTD 6.5 以降が必要です。
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	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。 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、**enter hw-crypto** 次に **set admin-state enabled** FXOS コマンドを使用します。 新規/変更された Firepower Chassis Manager 画面： **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）] > [設定（Settings）] >** の [ハードウェア暗号化（Hardware Crypto）] ドロップダウンメニュー （注） FTD 6.5 以降が必要です。

機能名	プラットフォームリリース	機能情報
Firepower 4115、4125、および 4145	2.6.1	Firepower 4115、4125、および 4145 が導入されました。 （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。 変更された画面はありません。
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	2.6.1	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。 （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。 すべてのモジュールには、FTD 6.4 および FXOS 2.6.1.157 が必要です。 変更された画面はありません。
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	2.6.1	ASA および FTD 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。 （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。 変更された画面はありません。
FTD 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	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 FTD 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。 新しい/変更された画面： **[Logical Devices]** > **[Add Device]** > **[Settings]** > **[Firepower Management Center NAT ID]** フィールド

機能名	プラットフォームリリース	機能情報
モジュール/セキュリティ エンジンのいずれかの FTD 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	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。 新規/変更されたコマンド：**config hwCrypto enable**、**show hwCrypto** 変更された画面はありません。

機能名	プラットフォームリリース	機能情報
FTD のマルチインスタンス機能	2.4.1	

機能名	プラットフォームリリース	機能情報
		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FTD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できるだけでした。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。 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。 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。 （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 FTD 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。FTD ではマルチコンテキストモードは使用できません。 （注） FTD バージョン 6.3 以降が必要です。 新規/変更された Firepower Chassis Manager 画面： **[概要（Overview）] > [デバイス（Devices）]** **[インターフェイス（Interfaces）]>[すべてのインターフェイス（All Interfaces）]>[新規追加（Add New）]** ドロップダウン メニュー > [サブインターフェイス（Subinterface）] **[Interfaces] > [All Interfaces] > [Type]** **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）]** **[プラットフォームの設定（Platform Settings）] > [Macプール（Mac Pool）]** **[プラットフォームの設定（Platform Settings）] > [リソースのプロファイル**

機能名	プラットフォームリリース	機能情報
		（**Resource Profiles**）**]** 新規/変更された FMC 画面： **[Devices]** > **[Device Management]** > **[Edit]** アイコン > [Interfaces] タブ
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	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。 新規/変更された Firepower Chassis Manager 画面： **[Logical Devices]** > **[Add Device]** > **[Settings]** 新規/変更されたオプション：[Firewall Mode] ドロップダウン リスト
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	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。 新規/変更された画面： **[Logical Devices]** > **[Add Device]** > **[Cluster Information]** > **[CCL Subnet IP]** フィールド
FTD 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	FXOS CLIで FMC NAT ID を設定できるようになりました。以前は、FTD 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。 新規/変更されたコマンド： **enter bootstrap-key NAT_ID**
ASA のサイト間クラスタリングの改善	2.1(1)	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。 次の画面が変更されました。**[Logical Devices]** > **[Configuration]**

機能名	プラットフォームリリース	機能情報
Firepower 9300 上の 6 個の FTD モジュールのシャーシ間クラスタリング	2.1.1	Firepower 9300 で FTD 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ることができます。 次の画面が変更されました。**[Logical Devices]** > **[Configuration]**
Firepower 4100 での FTD クラスタリングのサポート	2.1.1	FTD 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 FTD でのシャーシ内クラスタリング サポート	1.1.4	Firepower 9300 が FTD 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。 次の画面が変更されました。**[Logical Devices]** > **[Configuration]**
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。 次の画面が変更されました。**[Logical Devices]** > **[Configuration]**
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。 次の画面が導入されました。**[Logical Devices]** > **[Configuration]**

第 11 章

セキュリティ モジュール/エンジン管理

FXOS セキュリティ モジュール/セキュリティ エンジンについて

Firepower Chassis Manager の [Security Modules/Security Engine] ページから、セキュリティ モジュール/エンジンのステータスを表示したり、セキュリティ モジュール/エンジンに対してさまざまな機能を実行したりできます。

[Security Modules/Security Engine] ページに次の情報が表示されます。

- [Hardware State]：セキュリティ モジュール/エンジンのハードウェアの状態を表示します。
  - [Up]：セキュリティ モジュール/エンジン は正常に起動しています。セキュリティ モジュール/エンジン に関連付けられている論理デバイスがない場合でも、ハードウェア障害は表示されません。
  - [Booting Up]：セキュリティ モジュール/エンジンに電源投入中です。
  - [Restart]：セキュリティ モジュール/エンジン は再起動中です。
  - [Down]：セキュリティモジュール/エンジンに電源が投入されていないか、ハードウェア障害によってセキュリティ モジュール/エンジンが正常に起動できません。

- [Mismatch]：セキュリティ モジュールが使用停止となっているか、新しいセキュリティモジュールがスロットにインストールされていませんでした。確認応答機能を使用して、セキュリティモジュールを機能している状態に戻します。
- [Empty]：スロットにセキュリティ モジュールは取り付けられていません。

- [Service State]：セキュリティ モジュール/エンジンのソフトウェアの状態を表示します。
  - [使用不可（Not-available）]：セキュリティ モジュールはシャーシのスロットから取り外されています。セキュリティモジュールを再度取り付けて、通常の動作状態に戻します。
  - [Online]：セキュリティモジュール/エンジンはインストールされており、通常の動作モードになっています。
  - [Not Responding]：セキュリティ モジュール/エンジンは応答不能です。
  - [Token Mismatch]：以前に設定したもの以外のセキュリティ モジュールがシャーシ スロットにインストールされていることを示します。これは、ソフトウェアのインストール エラーが原因である可能性もあります。再初期化機能を使用して、セキュリティ モジュールを機能している状態に戻します。
  - [Online]：セキュリティモジュール/エンジンは障害状態にあります。障害状態の原因についての詳細情報を得るには、システム障害リストを確認してください。障害の情報アイコンにカーソルを合わせて、詳細情報を表示することもできます。

  セキュリティ モジュールの障害
  - [Failsafe Mode]：セキュリティ モジュールは、フェイルセーフ モードになっています。このモードでは、アプリケーションの起動がブロックされます。セキュリティモジュールに接続すると、トラブルシューティングを行ったり、フェイルセーフモードを無効にしたりできます。アプリケーション インスタンスを削除することもできます。
  - [HDD Error]：セキュリティ モジュールで、ディスク ドライブ エラーが発生しました。ディスクドライブが存在することを確認してください。エラーが解消されない場合は、障害のあるディスク ドライブを交換します。
  - [Filesystem Error]：セキュリティ モジュール上のディスク パーティションに互換性がありません。セキュリティ モジュールを再起動することで回復できる場合があります。それでも障害が解消されない場合は、外部デバイスにデータをバックアップしてからスロットを再初期化してください。
  - [Format Failure]：セキュリティモジュールのディスク ドライブを自動的にフォーマットできませんでした。セキュリティモジュールを再初期化して再フォーマットしてください。

- [Power]：セキュリティ モジュール/エンジンの電源ステータスを表示します。

- [オン（On）]：[電源オフ/オン（Power off/on）] 機能を使用して、セキュリティ モジュール/エンジンの電源ステータスを切り替えます。
- [オフ（Off）]：[電源オフ/オン（Power off/on）] 機能を使用して、セキュリティ モジュール/エンジンの電源ステータスを切り替えます。

- [アプリケーション（Application）]：セキュリティモジュール/エンジンにインストールされている論理デバイスのタイプを表示します。

Firepower Chassis Manager の [セキュリティモジュール/セキュリティエンジン（Security Modules/Security Engine）] ページから、セキュリティ モジュール/エンジンに対して次の機能を実行できます。

- [デコミッション（Decommission）]（セキュリティモジュールのみ）：セキュリティモジュールを使用停止にすると、セキュリティモジュールはメンテナンスモードに設定されます。また、特定の障害状態を修正するために、セキュリティモジュールをデコミッションしてから確認応答することもできます。セキュリティモジュールの使用停止（320 ページ）を参照してください。
- [確認応答（Acknowledge）]：新たにインストールされたセキュリティモジュールをオンラインにします。セキュリティモジュール/エンジンの確認応答（320 ページ）を参照してください。
- [電源の再投入（Power Cycle）]：セキュリティ モジュール/エンジンを再起動します。セキュリティモジュール/エンジンの電源オン/オフ（321 ページ）を参照してください。
- [再初期化（Reinitialize）]：セキュリティモジュール/エンジンのハードディスクを再フォーマットし、導入済みのすべてのアプリケーションや設定をセキュリティ モジュール/エンジンから削除し、システムを再起動します。論理デバイスがセキュリティ モジュール/エンジンに設定されている場合は、再初期化が完了すると、FXOS はアプリケーション ソフトウェアをインストールし、論理デバイスを再度導入し、アプリケーションを自動的に起動します。セキュリティモジュール/エンジンの最初期化（321 ページ）を参照してください。

警告 セキュリティモジュール/エンジンのすべてのアプリケーション データが再初期化時に削除されます。セキュリティ モジュール/エンジンを再初期化する前に、すべてのアプリケーション データをバックアップしておいてください。

- [電源オフ/オン（Power off/on）]：セキュリティ モジュール/エンジンの電源状態を切り替えます。セキュリティモジュール/エンジンの電源オン/オフ（321 ページ）を参照してください。

セキュリティモジュールの使用停止

セキュリティ モジュールを使用停止にすると、セキュリティ モジュール オブジェクトが設定から削除され、そのセキュリティモジュールは管理対象外になります。セキュリティモジュール上で実行していた論理デバイスやソフトウェアは非アクティブになります。

セキュリティ モジュールの使用を一時的に中止する場合に、セキュリティ モジュールを使用停止にできます。

手順

ステップ 1 [Security Modules] を選択して、[Security Modules] ページを開きます。

ステップ 2 セキュリティモジュールを使用停止にするには、そのセキュリティモジュールの [Decommission] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、指定したセキュリティモジュールを使用停止または再稼働することを確認します。

セキュリティモジュール/エンジンの確認応答

新しいセキュリティモジュールがシャーシに取り付けられた後、または既存のモジュールが異なる製品ID（PID）を持つモジュールで交換された後、セキュリティモジュールを確認応答してからでなければ、そのモジュールを使用することはできません。

セキュリティ モジュールのステータスが [mismatch] または [token mismatch] として示されている場合、スロットに取り付けたセキュリティモジュールのデータが、そのスロットに以前インストールされたデータと一致していないことを意味します。セキュリティモジュールに既存のデータがあり、新しいスロットでそのデータを使用する（つまり、そのセキュリティモジュールは不注意で誤ったスロットに取り付けられたのではない）場合は、論理デバイスを展開する前に、セキュリティ モジュールを再初期化する必要があります。

手順

ステップ 1 [セキュリティ モジュール/セキュリティ エンジン（Security Modules/Security Engine）] を選択して、[セキュリティ モジュール/セキュリティ エンジン（Security Modules/Security Engine）] ページを開きます。

ステップ 2 確認応答するセキュリティモジュール/エンジンの [確認応答（Acknowledge）] をクリックします。

ステップ 3 [Yes] をクリックして、指定したセキュリティ モジュール/エンジンに確認応答することを確認します。

セキュリティモジュール/エンジンの電源オン/オフ

セキュリティ モジュール/エンジンの電源の再投入を行うには、次の手順に従います。

手順

ステップ 1 [Security Modules/Security Engine] を選択して、[Security Modules/Security Engine] ページを開きます。

ステップ 2 リブートするセキュリティ モジュール/エンジンの [電源の再投入（Power Cycle）] をクリックします。

ステップ 3 次のいずれかを実行します。

- [安全な電源の再投入（Safe Power Cycle）] をクリックして、システムに、指定のセキュリティモジュール/エンジンの電源を再投入する前に、セキュリティモジュール/エンジンで実行しているアプリケーションがシャットダウンするのを最大で 5 分間待機させます。
- システムに、指定のセキュリティモジュール/エンジンの電源をすぐに再投入させるには、[ただちに電源再投入（Power Cycle Immediately）] をクリックします。

セキュリティ モジュール/エンジンの最初期化

セキュリティ モジュール/エンジン を再初期化すると、セキュリティ モジュール/エンジン のハードディスクがフォーマットされ、インストールされているすべてのアプリケーション インスタンス、設定、およびデータが削除されます。論理デバイスがセキュリティ モジュール/エンジンに設定されている場合、再初期化が完了すると、FXOSはアプリケーション ソフトウェアを再インストールし、論理デバイスを再導入して、アプリケーションを自動的に起動します。

⚠

注意 セキュリティモジュール/エンジンのすべてのアプリケーションデータが再初期化時に削除されます。Back up all application data before reinitializing a セキュリティ モジュール/エンジン.

手順

ステップ 1 [Security Modules/Security Engine] を選択して、[Security Modules/Security Engine] ページを開きます。

ステップ 2 再初期化するセキュリティ モジュール/エンジンの [再初期化（Reinitialize）] をクリックします。

ステップ 3 [はい（Yes）] をクリックして、指定したセキュリティ モジュール/エンジンを再初期化することを確認します。

セキュリティ モジュール/エンジンが再起動し、そのセキュリティ モジュールのすべてのデータが削除されます。このプロセスには数分かかることがあります。

ネットワークモジュールの確認応答

新しいネットワークモジュールがシャーシに取り付けられた後、または既存のモジュールが異なる製品 ID（PID）を持つモジュールで交換された後、ネットワークモジュールを確認応答してからでなければ、そのモジュールを使用することはできません。

手順

ステップ 1 `scope fabric-interconnect` モードを開始します。

```
scope fabric-interconnect
```

ステップ 2 新しいモジュールをインストールした後、またはモジュールを同じタイプではない（つまり、異なる PID を持つ）別のネットワークモジュールと交換した後、**acknowledge** コマンドを入力します。

```
acknowledge
```

例：

```
FPR1 /fabric-interconnect # acknowledge
  fault  Fault
  slot   Card Config Slot Id  <======
```

ステップ 3 挿入されたスロットを確認するには、**acknowledge slot** を入力します。

```
acknowledge slot
```

例：

```
FPR1 /fabric-interconnect # acknowledg slot 2
  0-4294967295  Slot Id
```

ステップ 4 設定をコミットします。

```
commit-buffer
```

ネットワーク モジュールのオフラインまたはオンラインの切り替え

CLI コマンドを使ってネットワーク モジュールをオフラインにしたりオンラインに戻したりするには、次の手順を実行します。この方法は、モジュールのオンライン挿入や削除（OIR）を実行する場合などに使用されます。

（注）

- ネットワーク モジュールを取り外して交換する場合は、お使いのデバイスに該当するインストール ガイドの中で、メンテナンスとアップグレードの章にある指示に従ってください。https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.htmlを参照してください。
- 8 ポート1G 銅線 FTW ネットワークモジュール（FPR-8X1G-F FTW）でネットワークモジュールのオンライン挿入および取り外し（OIR）を実行する場合は、この手順を使用してカードをオンラインにするまで、ネットワークモジュールの LED が消灯していることを確認してください。LED は最初にオレンジ色で点滅します。ネットワークモジュールが検出されてアプリケーションがオンラインになると緑色に変わります。

（注） FTW ネットワークモジュールを取り外してからスロットに対して確認応答すると、ネットワーク モジュール ポートはFTD の論理デバイスから削除されます。この場合、ネットワークモジュールを再挿入する前に、FMC を使用してハードウェアのバイパスインラインセット構成を削除する必要があります。ネットワークモジュールを挿入し直すと、次のことを行う必要があります：

- Firepower Chassis Manager または FXOS コマンドライン インターフェイス（CLI）を使用して、ネットワーク モジュール ポートを管理用オンライン状態として設定します。
- FTD 論理デバイスにネットワーク モジュール ポートを追加し、FMC を使用してポートを再設定します。

スロットに対して確認応答せずにネットワークモジュールを取り外すと、インラインセット構成は保持され、FMC ではポートがダウン状態と表示されます。ネットワークモジュールを再挿入すると、以前の設定が復元されます。

ハードウェアバイパスのインラインセットの詳細については、「ハードウェア バイパス ペア （177 ページ）」を参照してください

手順

ステップ 1 次のコマンドを使用して `/fabric-interconnect` モードに入った後、オフラインにする対象のモジュールの `/card` モードに入ります。

```
scope fabric-interconnect a
scope card ID
```

ステップ 2 **show detail** コマンドを使用すると、このカードに関する、現在のステータスなどの情報を表示することができます。

ステップ 3 モジュールをオフラインにするには、次のコマンドを入力します。

```
set adminstate offline
```

ステップ 4 **commit-buffer** コマンドを入力して、設定の変更内容を保存します。

再度 **show detail** コマンドを使用すると、モジュールがオフラインであることを確認できます。

ステップ 5 ネットワーク モジュールをオンラインに戻すには、次のコマンドを入力します。

```
set adminstate online
commit-buffer
```

例

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
    Id: 2
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DE
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
FP9300-A /fabric-interconnect/card # set adminstate offline
FP9300-A /fabric-interconnect/card* # commit-buffer
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
    Id: 2
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Offline
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DE
    Perf: N/A
    Admin State: Offline
    Power State: Off
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
FP9300-A /fabric-interconnect/card #
```

ブレードのヘルスモニタリング

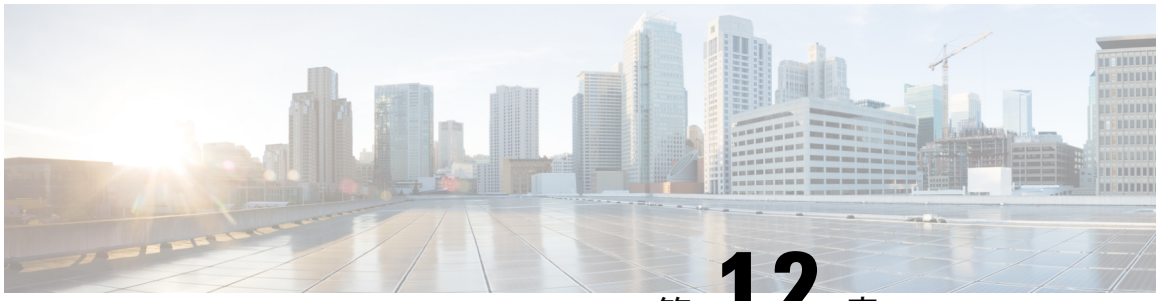
指定した回数の予期しないアプリケーションの再起動がブレードで検出されると、セキュリティモジュールまたはエンジンでフェールセーフが実行されます。これにより、冗長なHAまたはクラスタデプロイメントでさらなる副作用を引き起こす可能性のある無限のブートループ状態を防止します。

ブレードプラットフォームは定期的にヘルスチェックを実行し、MIOに報告します。ブレードが障害状態の場合、障害とエラーのメッセージが通知されます。

障害とエラーメッセージ

ブレードに問題がある場合は、プラットフォームの [概要（Overview）] ページで障害とエラーメッセージを表示できます。

- [概要（Overview）] ページ：セキュリティモジュールに障害シンボルが表示され、動作状態は [障害（Fault）] となります。
- [セキュリティモジュール（Security Module）] ページ：ブレードのサービス状態は、[障害（Fault）] として表示されます。「i」アイコンにカーソルを合わせると、エラーメッセージが表示されます。
- [論理デバイス（Logical Devices）] ページ：論理デバイスが使用可能で、セキュリティモジュールに障害が発生した場合、カーソルを合わせると「i」アイコンにエラーメッセージが表示されます。



第 12 章

コンフィギュレーションのインポート/エクスポート

コンフィギュレーションのインポート/エクスポートについて

Firepower 4100/9300 シャーシの論理デバイスとプラットフォームのコンフィギュレーション設定を含むXMLファイルをリモートサーバまたはローカルコンピュータにエクスポートするコンフィギュレーションのエクスポート機能を使用できます。そのコンフィギュレーションファイルを後でインポートしてFirepower 4100/9300 シャーシに迅速にコンフィギュレーション設定を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。

ガイドラインと制限

- FXOS 2.6.1から、暗号キーを設定できるようになりました。コンフィギュレーションをエクスポートする前に、暗号キーを設定する必要があります。エクスポートしたコンフィギュレーションをインポートするときには、システムに同じ暗号キーを設定する必要があります。エクスポート時に使用したものと一致しなくなるように暗号キーを変更した場合、インポート操作は失敗します。エクスポートした各コンフィギュレーションに使用した暗号キーを必ず記録しておいてください。
- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。

- 用途別のコンフィギュレーション設定は、コンフィギュレーションファイルに含まれていません。用途別の設定やコンフィギュレーションを管理するには、アプリケーションが提供するコンフィギュレーション バックアップ ツールを使用する必要があります。
- Firepower 4100/9300 シャーシへのコンフィギュレーションのインポート時、Firepower 4100/9300 シャーシのすべての既存のコンフィギュレーション（論理デバイスを含む）は削除され、インポートファイルに含まれるコンフィギュレーションに完全に置き換えられます。
- RMA シナリオを除き、コンフィギュレーション ファイルのエクスポート元と同じFirepower 4100/9300 シャーシだけにコンフィギュレーション ファイルをインポートすることをお勧めします。
- インポート先の Firepower 4100/9300 シャーシのプラットフォーム ソフトウェア バージョンは、エクスポートしたときと同じバージョンになるはずです。異なる場合は、インポート操作の成功は保証されません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。
- インポート先のFirepower 4100/9300 シャーシでは、エクスポートしたときと同じスロットに同じネットワークモジュールがインストールされている必要があります。
- インポート先のFirepower 4100/9300 シャーシでは、インポートするエクスポートファイルに定義されているすべての論理デバイスに、正しいソフトウェアアプリケーションイメージがインストールされている必要があります。
- インポートするコンフィギュレーションファイルに、そのアプリケーションにエンドユーザライセンス契約書（EULA）がある論理デバイスが含まれていると、コンフィギュレーションをインポートする前に、そのアプリケーションの EULA が Firepower 4100/9300 シャーシで受け入れられている必要があります。受け入れられていない場合、操作は失敗します。
- 既存のバックアップファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

（注） FXOS のインポート/エクスポートは FXOS の設定のみをバックアップするため、ロジックアプリを個別にバックアップする必要があります。FXOS の設定をインポートすると、論理デバイスが再起動され、工場出荷時のデフォルト設定でデバイスが再構築されます。

コンフィギュレーションのインポート/エクスポート用暗号キーの設定

コンフィギュレーションをエクスポートするときに、FXOS はパスワードやキーなどの機密データを暗号化します。

FXOS 2.6.1 から、暗号キーを設定できるようになりました。コンフィギュレーションをエクスポートする前に、暗号キーを設定する必要があります。エクスポートしたコンフィギュレーションをインポートするときには、システムに同じ暗号キーを設定する必要があります。エクスポート時に使用したものと一致しなくなるように暗号キーを変更した場合、インポート操作は失敗します。エクスポートした各コンフィギュレーションに使用した暗号キーを必ず記録しておいてください。

暗号キーは、[Export] ページまたは [Import] ページのいずれかで設定できます。ただし、一度設定すると、エクスポートとインポートの両方に同じキーが使用されます。

2.6.1 より前のリリースの FXOS からエクスポートしたコンフィギュレーションを FXOS 2.6.1 以降にインポートする場合、システムは暗号キーをチェックせずにインポートを許可します。

（注） インポート先のプラットフォームのソフトウェア バージョンが、エクスポート実行時と同じバージョンではない場合、インポート操作を正常に実行できる保証はありません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。

[バージョンの設定（Set Version）] オプションを使用するとともに、FTD 論理アプライアンスが新しいソフトウェアにアップグレードされるたびにバックアップ設定をエクスポートします。これにより、新しいスタートアップバージョンがアップグレードされたバージョンのソフトウェアリリースと一致するようになります。

手順

ステップ 1 **[System]** > **[Configuration]** > **[Export]** の順に選択します。

ステップ 2 [Encryption] で、機密データの暗号化/復号化に使用するキーを [Key] フィールドに入力します。暗号キーの長さは 4 ～ 40 文字である必要があります。

ステップ 3 [Save Key] をクリックします。

暗号キーが設定され、コンフィギュレーションのエクスポートおよびインポート時に機密データの暗号化/復号化に使用されます。[Key] フィールドの横に *Set: Yes* と表示され、暗号キーが設定されていることが示されます。

FXOS コンフィギュレーション ファイルのエクスポート

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。

始める前に

「コンフィギュレーションのインポート/エクスポートについて」を確認してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）] > [エクスポート（Export）]** の順に選択します。

ステップ 2 コンフィギュレーション ファイルをローカル コンピュータにエクスポートするには、[ローカルにエクスポート（Export Locally）] をクリックします。
コンフィギュレーションファイルが作成され、ブラウザによって、ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するようプロンプトが表示されます。

ステップ 3 コンフィギュレーション ファイルを設定済みのリモート サーバにエクスポートするには、使用するリモート構成の [エクスポート（Export）] をクリックします。
コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

ステップ 4 コンフィギュレーション ファイルを新しいリモート サーバにエクスポートするには、次の操作を行います。

a) [オンデマンドエクスポート（On-Demand Export）] の下で、[オンデマンド設定の追加（Add On-Demand Configuration）] をクリックします。
b) リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

   IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

d) デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。
e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
g) [場所（Location）] フィールドに、ファイル名を含む設定ファイルをエクスポートする場所のフル パスを入力します。
h) [OK] をクリックします。
   リモート構成はオンデマンド エクスポート テーブルに追加されます。
i) 使用するリモート構成の [エクスポート（Export）] をクリックします。
   コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

自動設定エクスポートのスケジューリング

スケジュールされたエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。エクスポートは、毎日、毎週、または2週間ごとに実行されるようにスケジュールできます。設定のエクスポートは、スケジュールされたエクスポート機能がいつ有効になるかに基づき、スケジュールに従って実行されます。そのため、たとえば週ごとのスケジュールされたエクスポートが水曜日の10:00pmに有効になる場合、システムは新しいエクスポートを水曜日の 10:00pm ごとに開始します。

エクスポート機能の使用に関する重要な情報については、「コンフィギュレーションのインポート/エクスポートについて」を参照してください。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）] > [エクスポート（Export）]** の順に選択します。

ステップ 2 [Schedule Export] をクリックします。
[スケジュールされたエクスポートの設定（Configure Scheduled Export）] ダイアログボックスが表示されます。

ステップ 3 リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。

ステップ 4 スケジュールされたエクスポートを有効にするには、[有効化（Enable）] チェックボックスをオンにします。

（注） このチェックボックスを使用して、スケジュールされたエクスポートを後から有効または無効にできます。ただし、スケジュールされたエクスポートを有効または無効にするには、もう一度パスワードを指定する必要があります。

ステップ 5 バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

ステップ 6 デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。

ステップ 7 リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

ステップ 8 リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

ステップ 9 [場所（Location）] フィールドに、ファイル名を含む設定ファイルをエクスポートする場所のフルパスを入力します。ファイル名を省略すると、エクスポート手順によって、ファイルに名前が割り当てられます。

ステップ 10 設定を自動的にエクスポートするスケジュールを選択します。これは、[毎日（Daily）]、[毎週（Weekly）]、または [隔週（BiWeekly）] のいずれかにできます。

ステップ 11 [OK] をクリックします。
スケジュールされたエクスポートが作成されます。スケジュールされたエクスポートを有効にすると、システムは、指定の場所に、選択したスケジュールに従ってコンフィギュレーションファイルを自動的にエクスポートします。

設定エクスポート リマインダの設定

設定エクスポートが特定の日数実行されていないときにシステムにエラーを生成させるには、エクスポートリマインダ機能を使用します。

デフォルトでは、エクスポートリマインダは 30 日間の頻度で有効になっています。

（注） リマインダの頻度が、スケジュールされたエクスポートポリシーの日数（毎日、毎週、または隔週）よりも短いと、エクスポートリマインダ障害メッセージ（「`Config backup may be outdated`」）が表示されます。たとえば、エクスポートスケジュールが毎週で、リマインダの頻度が 5 日間の場合、リマインダの間隔内に設定がエクスポートされないと、この障害メッセージが 5 日ごとに生成されます。

手順

ステップ 1 **[システム（System）]** > **[設定（Configuration）]** > **[エクスポート（Export）]** の順に選択します。

ステップ 2 設定エクスポート リマインダを有効にするには、[Reminder to trigger an export] の下のチェックボックスをオンにします。

ステップ 3 最後に設定エクスポートが実行されてからリマインダエラーを生成するまでシステムが待機する期間を、1 ～ 365 の範囲の日数で入力します。

ステップ 4 [Save Reminder] をクリックします。

コンフィギュレーション ファイルのインポート

設定のインポート機能を使用して、Firepower 4100/9300 シャーシからエクスポートした構成設定を適用できます。この機能を使用して、既知の良好な構成に戻したり、システム障害を解決したりできます。

始める前に

「コンフィギュレーションのインポート/エクスポートについて」を確認してください。

手順

ステップ 1 **[システム（System）] > [ツール（Tools）] > [インポート/エクスポート（Import/Export）]** を選択します。

ステップ 2 ローカルのコンフィギュレーション ファイルからインポートする場合は、次の操作を行います。

a) [ファイルの選択（Choose File）] をクリックし、インポートするコンフィギュレーション ファイルを選択します。

b) [インポート（Import）] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。

c) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

ステップ 3 設定済みのリモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

a) リモート インポート テーブルで、使用するリモート構成の [インポート（Import）] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。

b) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

ステップ 4 新しいリモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

a) [リモート インポート（Remote Import）] の下にある [リモート設定の追加（Add Remote Configuration）] をクリックします。

b) リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。

c) デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。

d) バックアップ ファイルが格納されている場所のホスト名または IP アドレスを入力します。サーバ、ストレージアレイ、ローカル ドライブ、またはFirepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

   IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

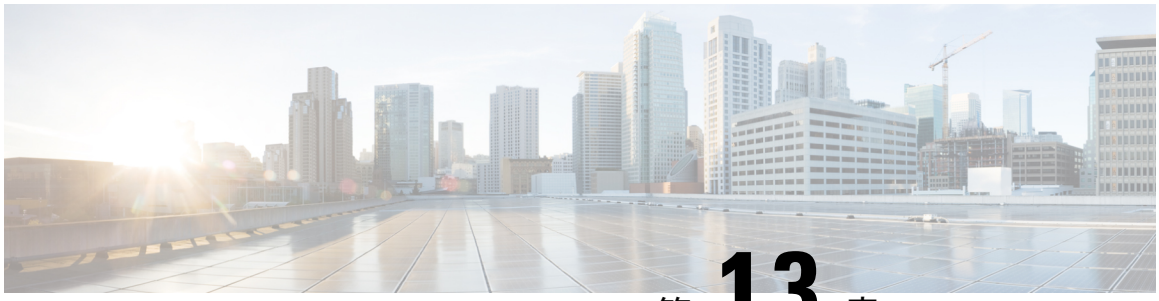
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

g) [ファイルパス（File Path）] フィールドに、コンフィギュレーション ファイルのフルパスをファイル名を含めて入力します。

h) [保存（Save）] をクリックします。
   リモート構成がリモート インポート テーブルに追加されます。

i) 使用するリモート構成の [インポート（Import）] をクリックします。
   操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。

j) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
   既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。



第 13 章

トラブルシューティング

パケット キャプチャ

パケット キャプチャ ツールは、接続と設定の問題のデバッグや、Firepower 4100/9300 シャーシを通過するトラフィック フローの理解に使用できる価値ある資産です。パケット キャプチャ ツールを使用すると、Firepower 4100/9300 シャーシの特定のインターフェイスを通過するトラフィックについてログを記録できます。

複数のパケット キャプチャ セッションを作成でき、各セッションで複数のインターフェイスのトラフィックをキャプチャできます。パケット キャプチャ セッションに含まれる各インターフェイス用に、個別のパケット キャプチャ（PCAP）ファイルが作成されます。

バックプレーン ポート マッピング

Firepower 4100/9300 シャーシでは、内部バックプレーン ポートに次のマッピング ポートを使用します。

セキュリティ モジュール	ポート マッピング	説明
セキュリティ モジュール 1/セキュリティ エンジン	Ethernet1/9	Internal-Data0/0
セキュリティ モジュール 1/セキュリティ エンジン	Ethernet1/10	Internal-Data0/1
セキュリティ モジュール 2	Ethernet1/11	Internal-Data0/0
セキュリティ モジュール 2	Ethernet1/12	Internal-Data0/1
セキュリティ モジュール 3	Ethernet1/13	Internal-Data0/0
セキュリティ モジュール 3	Ethernet1/14	Internal-Data0/1

パケット キャプチャの注意事項および制限事項

パケット キャプチャ ツールには、次の制限事項があります。

- キャプチャできるのは最大 100 Mbps までです。
- パケット キャプチャ セッションの使用に使用可能な十分な記憶域がなくても、パケット キャプチャセッションを作成できます。パケットキャプチャ セッションを開始する前に、使用可能な十分な記憶域があることを確認する必要があります。
- シングル幅の 4x100Gbps または 2x100Gbps ネットワークモジュール（それぞれ部品番号 FPR-NM-4X100G および FPR-NM-2X100G）でのパケット キャプチャ セッションの場合、モジュールの `adminstate` が `off` に設定されると、キャプチャセッションが自動的に無効になり、「Oper State Reason: Unknown Error」というメッセージが生成されます。モジュールの `adminstate` を再度 `on` に設定してから、キャプチャセッションを再起動する必要があります。

  他のすべてのネットワークモジュールでは、モジュールの `adminstate` が変更されてもパケット キャプチャ セッションが継続されます。
- 複数のアクティブなパケット キャプチャ セッションはサポートされません。
- 内部スイッチの入力の段階でのみキャプチャされます。
- 内部スイッチが認識できないパケット（セキュリティ グループ タグ、ネットワーク サービス ヘッダー パケットなど）にはフィルタの効果がありません。
- 1 つ以上の親で複数のサブインターフェイスを使用する場合でも、セッションごとに 1 つのサブインターフェイスのパケットのみをキャプチャできます。
- EtherChannel 全体または EtherChannel のサブインターフェイスのパケットをキャプチャできません。ただし、論理デバイスに割り当てられている EtherChannel の場合、EtherChannel のメンバ インターフェイスごとにパケットをキャプチャできます。 親インターフェイス

ではなくサブインターフェイスを割り当てる場合は、メンバインターフェイス上のパケットをキャプチャすることはできません。

- キャプチャ セッションがアクティブな間は、PCAP ファイルをコピーしたり、エクスポートできません。
- パケットキャプチャ セッションを削除すると、そのセッションに関連するすべてのパケット キャプチャ ファイルも削除されます。

パケット キャプチャ セッションの作成または編集

手順

ステップ 1 **[ツール（Tools）]** > **[パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 次のいずれかを実行します。

- パケット キャプチャ セッションを作成するには、[キャプチャ セッション（Capture Session）] ボタンをクリックします。
- 既存のパケット キャプチャ セッションを編集するには、そのセッションの [Edit] ボタンをクリックします。

ウィンドウの左側では、特定のアプリケーション インスタンスを選択し、そのインスタンスの表記を表示します。この表示は、パケットをキャプチャするインターフェイスを選択するために使用されます。ウィンドウの右側にパケットキャプチャ セッションを定義するためのフィールドが含まれています。

ステップ 3 ドロップダウン メニューから**インターフェイスを選択します**。

ステップ 4 トラフィックをキャプチャするインターフェイスをクリックします。選択したインターフェイスにチェック マークを表示します。

ステップ 5 サブインターフェイスの場合、[Subinterface selection] 列でサブインターフェイスを表示する親インターフェイスの左にあるアイコンをクリックします。列内のサブインターフェイスをクリックします。1 つ以上の親で複数のサブインターフェイスを使用する場合でも、キャプチャ セッションごとに 1 つのサブインターフェイスのパケットのみをキャプチャできます。

複数のサブインターフェイスの場合、アイコンのラベルは **Subinterfaces(n)** になり、単一のサブインターフェイスの場合、ラベルはサブインターフェイス ID になります。親インターフェイスをインスタンスにも割り当てる場合、親インターフェイスまたはサブインターフェイスのいずれかを選択できます。両方を選択することはできません。親が割り当てられていない場合は、グレー表示されます。Etherchannel のサブインターフェイスはサポートされていません。

ステップ 6 論理デバイスからバックプレーン ポート上で送信されるトラフィックをキャプチャするには、次の操作を行います。

a) アプリケーション インスタンスを示すボックスをクリックします。

[Capture On]、[Application Port]、および [Application Capture Direction] フィールドは、[Configure Packet Capture Session] ウィンドウの右側で利用可能になります。

b) トラフィックをキャプチャするバックプレーン ポートを選択するか、[Capture On] ドロップダウン リストから [All Backplane Ports] を選択します。

ステップ 7 [Session Name] フィールドにパケット キャプチャ セッションの名前を入力します。

ステップ 8 [Buffer Size] リストからあらかじめ定義された値の 1 つを選択するか、[Custom in MB] を選択してから目的のバッファ サイズを入力して、パケット キャプチャ セッションに使用するバッファ サイズを指定します。指定するバッファ サイズは 1 ～ 2048 MB にする必要があります。

ステップ 9 [Snap Length] フィールドに、キャプチャするパケットの長さを指定します。有効値は 64 ～ 9006 バイトです。デフォルトのスナップ長は 1518 バイトです。

ステップ 10 このパケット キャプチャ セッションを実行したときに、既存の PCAP ファイルを上書きするか、または PCAP ファイルにデータを追加するかを指定します。

ステップ 11 アプリケーションインスタンスと特定のインターフェイス間のトラフィックをキャプチャするには、次の操作を行います。

a) 論理デバイスを表すボックスをクリックします。

b) [Capture On] ドロップダウン リストから、アプリケーション タイプ（[asa] など）を選択します。

c) 受信または送信トラフィックをキャプチャする [Application Port] を選択します。

d) 論理デバイスから指定したインターフェイスに向かうトラフィックのみキャプチャするには、[Application Capture Direction] の横にある [Egress Packets] オプションをクリックします。

（注） [Egress Packets] を選択すると、トラフィックは選択したバックプレーンポートでのみキャプチャされます。選択した場合でも、物理ポートではトラフィックはキャプチャされません。

e) 指定したインターフェイスで送信または受信するトラフィックをキャプチャするには、[Application Capture Direction] の横にある [All Packets] オプションをクリックします。

ステップ 12 キャプチャしたトラフィックをフィルタリングするには、次の手順を実行します。

a) [キャプチャ フィルタ（Capture Filter）] フィールドの [フィルタの適用（Apply Filters）] オプションをクリックします。

フィルタを設定するための一連のフィールドが示されます。

b) フィルタを作成する必要がある場合、[フィルタの作成（Create Filter）] をクリックします。

[パケット フィルタの作成（Create Packet Filter）] ダイアログボックスが表示されます。詳細については、パケット キャプチャのためのフィルタの設定（339 ページ）を参照してください。

c) [適用（Apply）] ドロップダウン リストから、使用するフィルタを選択します。

d) [適用先（To）] ドロップダウン リストから、フィルタを適用するインターフェイスを選択します。
e) 追加のフィルタを適用するには、[別のフィルタの適用（Apply Another Filter）] をクリックしてから上記の追加のフィルタを適用するステップを繰り返します。

ステップ 13 次のいずれかを実行します。

- このパケット キャプチャ セッションを保存してすぐ実行するには、[保存して実行（Save and Run）] ボタンをクリックします。このオプションは、他のパケット キャプチャ セッションが現在実行されていない場合のみ使用できます。
- このパケットキャプチャセッションを後で実行できるように保存するには、[保存（Save）] ボタンをクリックします。

[キャプチャ セッション（Capture Session）] タブに作成された他のセッションとともにセッションが一覧表示されます。[保存して実行（Save and Run）] を選択した場合、パケットキャプチャセッションは、パケットをキャプチャします。セッションからPCAPファイルをダウンロードする前に、キャプチャを停止する必要があります。

パケット キャプチャのためのフィルタの設定

パケット キャプチャ セッションに含まれるトラフィックを制限するためにフィルタを作成できます。パケット キャプチャ セッションの作成中にどのインターフェイスが特定のフィルタを使用するかを選択できます。

（注） 現在実行中のパケット キャプチャ セッションに適用されているフィルタを変更または削除する場合、そのセッションを無効にしてから再度有効にするまでは実行されません。

手順

ステップ 1 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 次のいずれかを実行します。

- フィルタを作成するには、[フィルタの追加（Add Filter）] ボタンをクリックします。
- 既存のフィルタを編集するには、そのフィルタの [編集（Edit）] ボタンをクリックします。

[パケットフィルタの作成または編集（Create or Edit Packet Filter）] ダイアログボックスが表示されます。

ステップ 3 [フィルタ名（Filter Name）] フィールドにパケット キャプチャ フィルタの名前を入力します。

ステップ 4 特定のプロトコルをフィルタリングするには、[プロトコル（Protocol）] リストから選択するか、または [カスタム（Custom）] を選択して目的のプロトコルを入力します。カスタム プロトコルは 10 進形式（0 ～ 255）の IANA によって定義されたプロトコルである必要があります。

ステップ 5 特定の EtherType をフィルタリングするには、[EtherType] リストから選択するか、または [カスタム（Custom）] を選択して目的の EtherType を入力します。カスタム EhterType は 10 進形式の IANA によって定義された EtherType である必要があります（たとえば、IPv4＝2048、IPv6 = 34525、ARP = 2054、SGT = 35081）。

ステップ 6 内部 VLAN（ポートに入力する時の VLAN ID）または外部 VLAN（Firepower 4100/9300 シャーシによって追加された VLAN ID）に基づいてトラフィックをフィルタリングするには、指定されたフィールドに VLAN ID を入力します。

ステップ 7 特定の送信元または宛先のトラフィックをフィルタリングするには、IP アドレスとポートを入力するか、または特定の送信元または宛先フィールドに MAC アドレスを入力します。

（注） IPv4 または IPv6 アドレスを使用してフィルタリングできますが、同じパケット キャプチャ セッションでの両方によるフィルタリングはできません。

ステップ 8 [保存（Save）] をクリックしてフィルタを保存します。

[フィルタ リスト（Filter List）] タブに他の作成されたフィルタとともにフィルタがリスト表示されます。

パケット キャプチャ セッションの開始および停止

手順

ステップ 1 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 パケット キャプチャ セッションを開始するには、そのセッションの [セッションの有効化（Enable Session）] ボタンをクリックし、次に確認のために [はい（Yes）] をクリックします。

（注） 別のセッションの実行中は、パケット キャプチャ セッションを開始できません。

セッションに含まれるインターフェイスの PCAP ファイルがトラフィックの収集を開始します。セッションがセッション データを上書きするように設定されている場合、既存の PCAP

データは消去されます。そうでない場合、データは（もしあれば）既存のファイルに追加されます。

パケット キャプチャ セッションの実行中は、トラフィックをキャプチャするにつれて個々のPCAPファイルのファイルサイズが増加します。バッファのサイズ制限に達すると、システムがパケットの廃棄を開始し、廃棄カウント フィールドの値が増加します。

ステップ 3 パケット キャプチャ セッションを停止するには、そのセッションの [セッションの無効化（Disable Session）] ボタンをクリックし、次に確認のために [はい（Yes）] をクリックします。

セッションが無効になった後、PCAPファイルをダウンロードできます（パケットキャプチャファイルのダウンロード （341 ページ）を参照）。

パケット キャプチャ ファイルのダウンロード

セッションからローカル コンピュータにパケット キャプチャ（PCAP）ファイルをダウンロードできます。これでネットワーク パケット アナライザを使用して分析できるようになります。

手順

ステップ 1 **[ツール（Tools）] > [パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 パケット キャプチャ セッションから特定のインターフェイスの PCAP ファイルをダウンロードするには、そのインターフェイスに対応する [ダウンロード（Download）] ボタンをクリックします。

（注） パケット キャプチャ セッションの実行中は PCAP ファイルをダウンロードできません。

ブラウザによって、指定したPCAPファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するように求められます。

パケット キャプチャ セッションの削除

個々のパケットキャプチャセッションは、現在実行していなければ削除できます。非アクティブ パケット キャプチャ セッションは、いずれも削除できます。

手順

ステップ 1 **[ツール（Tools）]** > **[パケット キャプチャ（Packet Capture）]** の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャ セッションのリストが表示されます。パケット キャプチャ セッションが現在設定されていなければ、代わりにそのことを示すメッセージが表示されます。

ステップ 2 特定のパケット キャプチャ セッションを削除するには、そのセッションの対応する [削除（Delete）] ボタンをクリックします。

ステップ 3 すべての非アクティブ パケット キャプチャ セッションを削除するには、パケット キャプチャ セッションのリストの上にある [すべてのセッションの削除（Delete All Sessions）] ボタンをクリックします。

ネットワーク接続のテスト

始める前に

基本的なネットワーク接続をテストする目的で、ネットワーク上の別のデバイスのホスト名または IPv4 アドレスを使って ping を実行するには、**ping** コマンドを使用します。ネットワーク上の別のデバイスのホスト名または IPv6 アドレスを使って ping を実行するには、**ping6** コマンドを使用します。

ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv4 アドレスを使ってトレースするには、**traceroute** コマンドを使用します。ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv6 アドレスを使ってトレースするには、**traceroute6** コマンドを使用します。

- **ping** コマンドおよび **ping6** コマンドは、`local-mgmt` モードで使用可能です。
- **ping** コマンドは `module` モードでも使用できます。
- **traceroute** コマンドおよび **traceroute6** コマンドは、`local-mgmt` モードで使用可能です。
- **traceroute** コマンドは `module` モードでも使用できます。

手順

ステップ 1 次のコマンドのいずれか 1 つを入力することにより、`local-mgmt` モードまたは `module` モードに接続します。

- **connect local-mgmt**
- **connect module** *module-ID* {**console** | **telnet**}

例：

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

ステップ 2 基本的なネットワーク接続をテストする目的で、ネットワーク上の別のデバイスのホスト名またはIPv4 アドレスを使って ping を実行します。

ping {*hostname* | *IPv4_address*} ［**count** *number_packets* ］ | ［**deadline** *seconds* ］ | ［**interval** *seconds* ］ | ［**packet-size** *bytes* ］

例：

この例は、ネットワーク上の別のデバイスに対して ping 接続を 12 回実行する方法を示しています。

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

ステップ 3 ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv4 アドレスを使ってトレースします。

traceroute {*hostname* | *IPv4_address*}

例：

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1  198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

FP9300-A(local-mgmt)#
```

ステップ 4 （任意）`local-mgmt` モードを終了して最上位モードに戻るには、**exit** を入力します。

管理インターフェイスのステータスのトラブルシューティング

初期化時や設定時に、何らかの理由（Chassis Manager にアクセスできないなど）で管理インターフェイスが起動しないと思われる場合は、`local-mgmt` シェルで **show mgmt-port** コマンドを使用して、管理インターフェイスのステータスを確認します。

（注） `fxos` シェルで **show interface brief** コマンドを使用しないでください。現在、このコマンドでは、誤った情報が表示されます。

手順

ステップ 1 次のコマンドを入力することにより、`local-mgmt` モードに接続します。

- **connect local-mgmt**

例：

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

ステップ 2 **show mgmt-port** コマンドを使用して管理インターフェイスのステータスを確認します。

例：

```
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3210912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:705434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1648941394 (1.5 GiB)  TX bytes:138386379 (131.9 MiB)

firepower(local-mgmt)#
```

show mgmt-ip-debug コマンドを使用することもできますが、インターフェイス設定情報の広範なリストが生成されます。

ポート チャネル ステータスの確認

現在定義されているポート チャネルのステータスを判別するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力して `/eth-uplink/fabric` モードを開始します。

- **scope eth-uplink**
- **scope fabric** {**a** | **b**}

例：

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

ステップ 2 現在のポート チャネルとそれぞれの管理状態および動作状態のリストを表示するには、**show port-channel** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    --------------- ---------------- ------------------ -----
------ ---------------- ------------
    10              Port-channel10   Data               Enabl
ed     Failed           No operational members
    11              Port-channel11   Data               Enabl
ed     Failed           No operational members
    12              Port-channel12   Data               Disab
led    Admin Down       Administratively down
    48              Port-channel48   Cluster            Enabl
ed     Up

FP9300-A /eth-uplink/fabric #
```

ステップ 3 個々のポート チャネルとポートに関する情報を表示するには、次のコマンドを入力して `/port-channel` モードを開始します。

- **scope port-channel** *ID*

例：

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

    <--- remaining lines removed for brevity --->

FP9300-A(fxos)#
```

ステップ 4 指定したポート チャネルのステータス情報を表示するには、**show** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    ---------------- ---------------- ------------------ -----
------ ---------------- ------------
    10              Port-channel10   Data               Enabl
ed     Failed           No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

ステップ 5 ポート チャネルのメンバ ポートのステータス情報を表示するには、**show member-port** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
    Port Name       Membership         Oper State       State Reas
on
    --------------- ------------------ ---------------- ----------
--
    Ethernet2/3     Suspended          Failed           Suspended
    Ethernet2/4     Suspended          Failed           Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

ポートチャネルは、論理デバイスに割り当てられるまでは表示されないことに注意してください。ポートチャネルが論理デバイスから削除された場合や論理デバイスが削除された場合は、ポート チャネルが一時停止状態に戻ります。

ステップ 6 追加のポート チャネルおよび LACP 情報を表示するには、次のコマンドを入力することにより、 `/eth-uplink/fabric/port-channel` モードを終了して `fxos` モードに入ります。

- **top**
- **connect fxos**

例：

ステップ 7 現在のポート チャネルのサマリー情報を表示するには、**show port-channel summary** コマンドを入力します。

例：

```
FP9300-A(fxos)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
------------------------------------------------------------
------------------
```

```
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------
-------------------
10    Po10(SD)    Eth      LACP      Eth2/3(s)    Eth2/4(s)

11    Po11(SD)    Eth      LACP      Eth2/1(s)    Eth2/2(s)

12    Po12(SD)    Eth      LACP      Eth1/4(D)    Eth1/5(D)

48    Po48(SU)    Eth      LACP      Eth1/1(P)    Eth1/2(P)
```

`fxos` モードでは、さらに **show port-channel** コマンドおよび **show lacp** コマンドも使用できます。これらのコマンドを使用すると、容量、トラフィック、カウンタ、使用状況など、さまざまなポート チャネルおよび LACP 情報を表示することができます。

次のタスク

ポートチャネルの作成方法については、EtherChannel（ポートチャネル）の追加 （196 ページ）を参照してください。

ソフトウェア障害からの回復

始める前に

システムが正常にブートできないソフトウェア障害が発生した場合は、以下の手順を実行して、ソフトウェアの新規バージョンをブートできます。このプロセスを実行するには、キックスタートイメージをTFTPブートし、新規システムとマネージャイメージをダウンロードし、新規イメージを使用してブートする必要があります。

特定の FXOS バージョンのリカバリ イメージは、以下のいずれかのロケーションの Cisco.com から入手できます。

- Firepower 9300：https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263
- Firepower 4100 シリーズhttps://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263

リカバリ イメージには、3 つの異なるファイルが含まれます。たとえば、FXOS 2.1.1.64 の現在のリカバリ イメージを以下に示します。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

手順

ステップ 1 ROMMON にアクセスします。

a) コンソール ポートに接続します。

b) システムをリブートします.

システムはロードを開始し、そのプロセス中にカウントダウン タイマーを表示します。

c) カウントタウン中に **Esc** キーを押すと、ROMMON モードに入ります。

例：

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1  >
```

ステップ 2 キックスタート イメージを TFTP ブートします。

a) 管理 IP アドレス、管理ネットマスク、ゲートウェイ IP アドレスが正しく設定されていることを確認します。これらの値は、**set** コマンドを使用して表示できます。**ping** コマンドを使用すると、TFTP サーバへの接続をテストできます。

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

b) キックスタート イメージは、Firepower 4100/9300 シャーシからアクセス可能な TFTP ディレクトリにコピーします。

（注） キックスタートイメージのバージョン番号は、バンドルのバージョン番号に一致しません。FXOS バージョンとキックスタート イメージとの間の対応を示す情報は、Cisco.com のソフトウェア ダウンロード ページにあります。

c) ブート コマンドを使用して、ROMMON からイメージをブートします。

```
boot tftp://<IP address>/<path to image>
```

（注） さらに、Firepower 4100/9300 シャーシのフロントパネルにある USB スロットに挿入した FAT32 フォーマットの USB メディアデバイスを使用して、ROMMON からキックスタートをブートすることもできます。システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

システムは、イメージを受け取ってキックスタートイメージをロードすることを示す、一連の # を表示します。

例：

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
             ADDRESS: 10.0.0.2
             NETMASK: 255.255.255.0
             GATEWAY: 10.0.0.1
              SERVER: 192.168.1.2
               IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

        TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....................................................................

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

############################################################################
############################################################################
############################################################################

File reception completed.
```

ステップ 3 Firepower 4100/9300 シャーシに直前にロードしたキックスタートイメージと一致するリカバリ システムとマネージャ イメージをダウンロードします。

a) リカバリ システムとマネージャ イメージをダウンロードするには、管理IPアドレスとゲートウェイを設定する必要があります。これらのイメージは、USBを使用してダウンロードすることはできません。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

b) リカバリ システムとマネージャ イメージを、リモート サーバからブートフラッシュにコピーします。

switch(boot)# **copy** *URL* **bootflash:**

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*/*path*/*image_name*

例：

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) Firepower 4100/9300 シャーシにイメージが正常にコピーされたら、nuova-sim-mgmt-nsg.0.1.0.001.binからマネージャ イメージへのsymlinkを作成します。このリンクは、ロードするマネージャ イメージをロード メカニズムに指示します。symlink名は、ロードしようとしているイメージに関係なく、常にnuova-sim-mgmt-nsg.0.1.0.001.binとする必要があります。

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

例：

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
```

```
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

ステップ 4 直前にダウンロードしたシステム イメージをロードします。

```
switch(boot)# load bootflash:<system-image>
```

例：

```
switch(boot)# load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful
...
System is coming up ... Please wait ...


Cisco FPR Series Security Appliance
FP9300-A login:
```

ステップ 5 リカバリ イメージがロードされたら、以下のコマンドを入力して、システムが旧イメージをロードしないようにします。

（注） この手順は、リカバリ イメージのロードの直後に実行する必要があります。

```
FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility
issue.
FP9300-A /org/fw-platform-pack* # commit-buffer
```

ステップ 6 Firepower 4100/9300 シャーシで使用するプラットフォーム バンドル イメージをダウンロードしてインストールします。詳細については、イメージ管理（65ページ）を参照してください。

例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    fxos-k9.2.1.1.73.SPA
              Tftp     192.168.1.2           0                  Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
    Version: 2.1(1.73)
    Type: Platform Bundle
    State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

破損ファイル システムの回復

始める前に

スーパバイザのオンボード フラッシュが破損し、システムが正常に開始できなくなった場合は、次の手順を使用してシステムを回復できます。このプロセスを実行するには、キックスタート イメージを TFTP ブートし、フラッシュを再フォーマットし、新規システムとマネージャ イメージをダウンロードし、新規イメージを使用してブートする必要があります。

（注） この手順には、システム フラッシュの再フォーマットが含まれています。その結果、回復後にはシステムを完全に再設定する必要があります。

特定の FXOS バージョンのリカバリ イメージは、以下のいずれかのロケーションの Cisco.com から入手できます。

- Firepower 9300：https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263
- Firepower 4100 シリーズhttps://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263

リカバリ イメージには、3 つの異なるファイルが含まれます。たとえば、FXOS 2.1.1.64 の回復イメージを以下に示します。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

手順

ステップ 1 ROMMON にアクセスします。

a) コンソール ポートに接続します。

b) システムをリブートします.

システムはロードを開始し、そのプロセス中にカウントダウン タイマーを表示します。

c) カウントタウン中に **Esc** キーを押すと、ROMMON モードに入ります。

例：

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1  >
```

ステップ 2 キックスタート イメージを TFTP ブートします。

a) 管理 IP アドレス、管理ネットマスク、ゲートウェイ IP アドレスが正しく設定されていることを確認します。これらの値は、**set** コマンドを使用して表示できます。**ping** コマンドを使用すると、TFTP サーバへの接続をテストできます。

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

b) キックスタート イメージは、Firepower 4100/9300 シャーシからアクセス可能な TFTP ディレクトリにコピーします。

（注） キックスタートイメージのバージョン番号は、バンドルのバージョン番号に一致しません。FXOS バージョンとキックスタート イメージとの間の対応を示す情報は、Cisco.com のソフトウェア ダウンロード ページにあります。

c) ブート コマンドを使用して、ROMMON からイメージをブートします。

boot tftp://*<IP address>***/***<path to image>*

（注） さらに、Firepower 4100/9300 シャーシのフロント パネルにある USB スロットに挿入した USB メディア デバイスを使用して、ROMMON からキックスタートをブートすることもできます。システムの稼動中にUSBデバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

システムは、イメージを受け取ってキックスタートイメージをロードすることを示す、一連の # を表示します。

例：

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
             ADDRESS: 10.0.0.2
             NETMASK: 255.255.255.0
             GATEWAY: 10.0.0.1
              SERVER: 192.168.1.2
               IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

        TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....................................................................

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

############################################################################
############################################################################
############################################################################

File reception completed.
```

ステップ 3 キックスタートイメージをロードしたら、**init system** コマンドを使用してフラッシュを再フォーマットします。

init system コマンドを実行すると、システムにダウンロードされているすべてのソフトウェアイメージやシステムのすべての設定を含め、フラッシュの内容は消去されます。コマンドが完了するまで約 20 ～ 30 分かかります。

例：

```
switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
 your bootflash:.

Do you want to continue? (y/n)  [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting Sysdebug  partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
```

ステップ 4 リカバリ イメージを Firepower 4100/9300 シャーシへダウンロードします。

a) リカバリ イメージをダウンロードするには、管理 IP アドレスとゲートウェイを設定する必要があります。これらのイメージは、USB を使用してダウンロードすることはできません。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

b) リモート サーバからブートフラッシュに3つすべてのリカバリ イメージをコピーします。

switch(boot)# **copy** *URL* **bootflash:**

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*

- **sftp**://*username@hostname / path / image_name*
- **tftp**://*hostname / path / image_name*

例：

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA

  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) Firepower 4100/9300 シャーシにイメージが正常にコピーされたら、nuova-sim-mgmt-nsg.0.1.0.001.bin からマネージャ イメージへの symlink を作成します。このリンクは、ロードするマネージャ イメージをロード メカニズムに指示します。symlink 名は、ロードしようとしているイメージに関係なく、常に nuova-sim-mgmt-nsg.0.1.0.001.bin とする必要があります。

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

例：

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
```

```
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

ステップ 5 スイッチをリロードします。

```
switch(boot)# reload
```

例：

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.

!!  Rommon image verified successfully  !!


Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016  by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb

autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 >
```

ステップ 6 キックスタート イメージおよびシステム イメージからブートします。

```
rommon 1 > boot <kickstart-image> <system-image>
```

（注） システム イメージのロード中に、ライセンス マネージャのエラー メッセージが表示されることがあります。このようなメッセージは無視して構いません。

例：

```
rommon 1 > dir
Directory of: bootflash:\

  01/01/12  12:33a <DIR>          4,096  .
  01/01/12  12:33a <DIR>          4,096  ..
  01/01/12  12:16a <DIR>         16,384  lost+found
  01/01/12  12:27a           34,333,696  fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
```

```
  01/01/12  12:29a          330,646,465  fxos-k9-manager.4.1.1.69.SPA
  01/01/12  12:31a          250,643,172  fxos-k9-system.5.0.3.N2.4.11.69.SPA
  01/01/12  12:34a          330,646,465  nuova-sim-mgmt-nsg.0.1.0.001.bin
          4 File(s) 946,269,798 bytes
          3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA

  !!   Kickstart Image verified successfully   !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[    0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan  1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

           ---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.


  You have chosen to setup a new Security Appliance. Continue? (y/n):
```

ステップ 7 イメージのロードが完了すると、システムにより初期構成設定を入力するように求められます。詳細については、コンソール ポートを使用した初期設定 （8 ページ）を参照してください。

ステップ 8 Firepower 4100/9300 シャーシで使用するプラットフォーム バンドル イメージをダウンロードします。詳細については、イメージ管理 （65 ページ）を参照してください。

例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    fxos-k9.2.1.1.73.SPA
              Tftp     192.168.1.2           0                 Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
    Version: 2.1(1.73)
    Type: Platform Bundle
    State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

ステップ 9 以前の手順でダウンロードしたプラットフォーム バンドル イメージをインストールします。

（注） インストールプロセスには通常 15 ～ 20 分かかります。

a) auto-install モードにします。

Firepower-chassis /firmware # **scope auto-install**

b) FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.1(1.73)）。

c) システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

d) インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

e) アップグレード プロセスをモニタするには、次の手順を実行します。

- **scope firmware** を入力します。
- **scope auto-install** を入力します。
- **show fsm status expand** を入力します。

例：

```
TB10 /firmware/auto-install # show fsm status expand
    FSM Status:
        Affected Object: sys/fw-system/fsm
```

```
Current FSM: Deploy
Status: In Progress
Completion Time:
Progress (%): 98

FSM Stage:
Order  Stage Name                                 Status       Try
------ ---------------------------------------- ------------ ---
1      DeployWaitForDeploy                        Success      0
2      DeployResolveDistributableNames            Skip         0
3      DeployResolveDistributable                 Skip         0
4      DeployResolveImages                        Skip         0
5      DeployValidatePlatformPack                 Success      1
6      DeployDebundlePort                         Success      0
7      DeployPollDebundlePort                     Success      1
8      DeployActivateUCSM                         Success      0
9      DeployPollActivateOfUCSM                   Success      0
10     DeployActivateMgmtExt                      Skip         0
11     DeployPollActivateOfMgmtExt                Skip         0
12     DeployUpdateIOM                            Skip         0
13     DeployPollUpdateOfIOM                      Skip         0
14     DeployActivateIOM                          Skip         0
15     DeployPollActivateOfIOM                    Skip         0
16     DeployActivateRemoteFI                     Skip         0
17     DeployPollActivateOfRemoteFI               Skip         0
18     DeployWaitForUserAck                       Skip         0
19     DeployActivateLocalFI                      Success      0
20     DeployPollActivateOfLocalFI                In Progress  1
```

（注） ステージのステータスが「進行中」から「スキップ」または「成功」に変わるまで、次のステップに進まないでください。

ステップ 10 インストールしたプラットフォーム バンドル イメージがシステムの回復に使用するイメージに対応している場合は、将来的にシステムのロード時で使用できるようにキックスタート イメージおよびシステムイメージを手動で有効にする必要があります。回復イメージとして同じイメージを使用しているプラットフォーム バンドルをインストールする場合、自動アクティベーションは発生しません。

a) fabric-interconnect a のスコープを設定します。

```
FP9300-A# scope fabric-interconnect a
```

b) 実行中のカーネルバージョンと実行中のシステムバージョンを表示するには、**show version** コマンドを使用します。イメージをアクティブにするには、次の文字列を使用します。

```
FP9300-A /fabric-interconnect # show version
```

（注） Startup-Kern-Vers および Startup-Sys-Vers がすでに設定され、Running-Kern-Vers および Running-Sys-Vers と一致する場合は、イメージを有効にする必要はなく、手順 11 に進みます。

c) 次のコマンドを入力して、イメージをアクティブにします。

```
FP9300-A /fabric-interconnect # activate firmware
  kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

（注） サーバのステータスは「失敗したディスク（Disk Failed）」に変更される場合があります。このメッセージには注意を払う必要はなく、手順を続行できます。

d) スタートアップバージョンが正しく設定されていることを確認し、イメージのアクティブ化ステータスをモニタするには、**show version** コマンドを使用します。

重要 ステータスが「アクティブにしています（Activating）」から「実行可能（Ready）」に変わるまで、次のステップには進まないでください。

```
FP9300-A /fabric-interconnect # show version
```

例：

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers:
    Startup-Sys-Vers:
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
  5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers: 5.0(3)N2(4.11.69)
    Startup-Sys-Vers: 5.0(3)N2(4.11.69)
    Act-Kern-Status: Activating
    Act-Sys-Status: Activating
    Bootloader-Vers:

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers: 5.0(3)N2(4.11.69)
    Startup-Sys-Vers: 5.0(3)N2(4.11.69)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

ステップ 11 システムを再起動します。

例：

```
FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
```

```
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #
```

システムはFirepower 4100/9300 シャーシの電源を最終的にオフにしてから再起動する前に、各セキュリティ モジュール/エンジンの電源をオフにします。このプロセスには約 5 ～ 10 分かかります。

ステップ 12 システムのステータスをモニタします。サーバのステータスは「検出（Discovery）」から「構成（Config）」、最終的には「OK」へと変わります。

例：

```
FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Discovery             In Progress
1/2     Equipped                           Discovery             In Progress
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Config                Complete
1/2     Equipped                           Config                Complete
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Ok                    Complete
1/2     Equipped                           Ok                    Complete
1/3     Empty
```

総合的なステータスが「OK」になれば、システムは回復したことになります。引き続き、セキュリティ アプライアンス（ライセンス設定を含む）を再設定し、論理デバイスがあれば再作成する必要があります。詳細については、次を参照してください。

- Firepower 9300 のクイック スタート ガイド [英語]：http://www.cisco.com/go/firepower9300-quick
- Firepower 9300 のコンフィギュレーション ガイド [英語]：http://www.cisco.com/go/firepower9300-config
- Firepower 4100 シリーズのクイック スタート ガイド [英語]：http://www.cisco.com/go/firepower4100-quick
- Firepower 4100 シリーズのコンフィギュレーション ガイド [英語]：http://www.cisco.com/go/firepower4100-config

管理者パスワードが不明な場合における工場出荷時のデフォルト設定の復元

この手順により Firepower 4100/9300 シャーシシステムがデフォルト設定に戻ります。管理者パスワードも含まれます。管理者パスワードが不明な場合、次の手順を使用してデバイスの設定をリセットします。この手順では、インストールされている論理デバイスも消去されます。

（注） この手順では、Firepower 4100/9300 シャーシのコンソールにアクセスする必要があります。

手順

ステップ 1 付属のコンソールケーブルを使用して PC をコンソールポートに接続します。ターミナルエミュレータを回線速度 9600 ボー、データビット 8、パリティなし、ストップビット 1、フロー制御なしに設定して、コンソールに接続します。詳細については、『Cisco Firepower 9300 ハードウェア設置ガイド』を参照してください。

ステップ 2 デバイスの電源を入れます。次のようなプロンプトが表示されたら、ESC キーを押してブートを中断します。

例：

```
!!  Rommon image verified successfully  !!

Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015  by Cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: 00:00:00:00:00:00

find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
rommon 1 >
```

ステップ 3 キックスタートイメージとシステムイメージの名前をメモします。

例：

```
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

ステップ 4 キックスタートイメージをロードします。

[rommon 1] > [kickstart_image]**boot**

例：

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
 !! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
can't create lock file /var/lock/mtab~302: No such file or directory (use -n flag to
override)
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

ステップ 5 config ターミナルモードを開始します。

switch(boot) # **config terminal**

例：

```
switch(boot)#
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

ステップ 6 パスワードを再設定し、変更を確認します。

switch(boot) (config) # **admin-password erase**

（注） この手順を実行すると、すべての設定が消去され、システムがデフォルト設定に戻ります。

例：

```
switch(boot)(config)# admin-password erase
Your password and configuration will be erased!
Do you want to continue? (y/n)  [n] y
```

ステップ 7 config ターミナルモードを開始します。

switch(boot) (config) # **exit**

ステップ 8 この手順のステップ 3 でメモしたシステムイメージをロードし、初期設定 （8 ページ） タスクフローを使用してシステムを最初から設定します。

switch(boot) # **load** *system_image*

例：

```
switch(boot)# load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Uncompressing system image:
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

トラブルシューティング ログ ファイルの生成

必要に応じて、トラブルシューティングに利用するため、またはCisco TACへ送信するためのログ ファイルを生成できます。

手順

ステップ 1 **[Tools]** > **[Troubleshooting Logs]** を選択します。

ステップ 2 生成するログ ファイルのタイプをドロップダウン リストから選択します。

- [シャーシ（Chassis）]：シャーシハードウェアの問題やスーパーバイザやサービスマネージャを含むソフトウェアの問題のトラブルシューティングに使用するログファイルを生成します。
- [Module <#>]：セキュリティ モジュール/エンジン の問題のトラブルシューティングに使用するログ ファイルを生成します。

ステップ 3 [Generate Log] をクリックします。

ステップ 4 [Yes] をクリックして、ログ ファイルを生成することを確認します。

ログ ファイルが生成されます。このプロセスには、時間がかかる場合があります。ログ ファイルの生成中は、黄色のステータス メッセージが表示されます。ログ ファイルの生成をキャンセルするには、ステータス メッセージの [Abort Job] をクリックします。ログファイルが生成されると、ステータスメッセージが緑色に変わり、ジョブが正常に完了したことが示されます。

ステップ 5 生成されたログ ファイルをダウンロードするには、[Download Files] リスト内のログ ファイルに移動して、[Download] をクリックします。ログ ファイルは、techsupportフォルダに保存されます。

（注） 新しく生成されたファイルを [Download files] リストに表示するには、必要に応じて [Refresh] をクリックする必要があります。

ステップ 6 生成されたログ ファイルを削除するには、[Download Files] リスト内のログ ファイルに移動して、[Delete] をクリックします。

モジュールのコアダンプの有効化

モジュールでコアダンプを有効にすると、システムクラッシュが発生した場合のトラブルシューティングに役立つ可能性があり、必要に応じて Cisco TAC に送信できます。

手順

ステップ 1 目的のモジュールに接続します。次に例を示します。

Firepower# connect module 1 console

ステップ 2 （任意）次のコマンドを入力して、現在のコアダンプステータスを表示します。

Firepower-module1> show coredump detail

このコマンドの出力には、コアダンプ圧縮が有効かどうかといった、現在のコアダンプステータス情報が表示されます。

例：

```
Firepower-module1>show coredump detail
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

（注） このコマンドは、アプライアンスで ASA 論理デバイスを実行している場合にのみ使用でき、アプライアンスで FTD 論理デバイスを実行している場合には使用できません。

ステップ 3 **config coredump** コマンドを使用して、コアダンプを有効または無効にし、クラッシュ時のコアダンプ圧縮を有効または無効にします。

- クラッシュ時のコアダンプの作成を有効にするには、**config coredump enable** を使用します。
- クラッシュ時のコアダンプの作成を有効にするには、**config coredump disable** を使用します。
- コアダンプの圧縮を有効にするには、**config coredump compress enable** を使用します。
- コアダンプの圧縮を無効にするには、**config coredump compress disable** を使用します。

例：

```
Firepower-module1>config coredump enable
Coredump enabled successfully.
ASA coredump enabled, do 'config coredump disableAsa' to disable
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system
failure.  Are you sure? (y/n):
y
```

```
Firepower-module1>
```

（注） コアダンプファイルはディスク容量を消費します。容量が少なくなり、圧縮が有効になっていない場合は、コアダンプが有効になっていても、コアダンプファイルが保存されないことがあります。

シリアル番号の確認 Firepower 4100/9300 シャーシ

Firepower 4100/9300 シャーシ とそのシリアル番号の詳細を確認できます。Firepower 4100/9300 シャーシのシリアル番号は、論理デバイスのシリアル番号とは異なるので注意してください。

手順

ステップ 1 **[概要（Overview）] > [インベントリ（Inventory）] > [すべて（All）]** を選択します。

この表には、シャーシにインストールされているコンポーネントのリストと、それらのコンポーネントの関連情報が記載されています。

ステップ 2 [シリアル（serial）] 列のシャーシのシリアル番号を探します。

RAID 仮想ドライブの再構築

RAID（独立ディスクの冗長アレイ）とは、優れたパフォーマンスとフォールトトレランス機能を提供する複数の独立した物理ドライブのアレイ（グループ）です。ドライブ グループは、物理ドライブのグループです。これらのドライブは、仮想ドライブと呼ばれるパーティションで管理されます。

RAID ドライブ グループでは、単一ドライブのストレージ システムに比べてデータ ストレージの信頼性と耐障害性が高まります。ドライブの障害によるデータの損失は、失われたデータを残りのドライブから再構築することで防ぐことができます。RAID は、I/O パフォーマンスを向上させるとともに、ストレージサブシステムの信頼性を向上させます。

RAID ドライブのいずれかが故障するかオフラインになると、RAID 仮想ドライブは劣化状態と見なされます。以下の手順を使用して、RAID 仮想ドライブが劣化状態かどうかを確認し、必要に応じて、ローカルディスク設定保護ポリシーを一時的に no に設定して再構築してください。

（注） ローカルディスク設定保護ポリシーを no に設定すると、ディスク上のすべてのデータが破棄されます。

手順

ステップ 1 RAID ドライブのステータスを確認します。

1. シャーシ モードに入ります。

   scope chassis

2. サーバモードに入ります。

   scope server 1

3. RAID コントローラに入ります。

   scope raid-controller 1 sas

4. 仮想ドライブを表示します。

   show virtual-drive

   RAID仮想ドライブが劣化状態である場合は、動作状態が**Degraded**と表示されます。次に例を示します。

```
Virtual Drive:
    ID: 0
    Block Size: 512
    Blocks: 3123046400
    Size (MB): 1524925
    Operability: Degraded
Presence: Equipped
```

ステップ 2 RAIDドライブを再構築するために、ローカルディスク設定ポリシー保護をnoに設定します。この手順を完了するとディスク上のすべてのデータが破棄されることに注意してください。

1. 組織の範囲を入力します。

   scope org

2. ローカルディスク設定ポリシーの範囲を入力します。

   scope local-disk-config-policy ssp-default

3. 保護を no に設定します。

   set protect no

4. 設定をコミットします。

   commit-buffer

ステップ 3 RAID ドライブが再構築されるまで待ちます。RAID 再構築ステータスを確認します。

scope chassis 1

show server

RAID ドライブが正常に再構築されると、スロットの全体的なステータスが **Ok** と表示されます。次に例を示します。

例：

```
Server:
    Slot    Overall Status        Service Profile
    ------- --------------------- ---------------
          1 Ok                    ssp-sprof-1
```

ステップ 4 RAID ドライブが正常に再構築されたら、ローカルディスク設定ポリシー保護を yes に戻します。

1. 組織の範囲を入力します。

   scope org

2. ローカルディスク設定ポリシーの範囲を入力します。

   scope local-disk-config-policy ssp-default

3. 保護を no に設定します。

   set protect yes

4. 設定をコミットします。

   commit-buffer

SSD を使用している場合の問題の特定

デバイスに搭載されている SSD に関して、情報を収集し、考えられる問題を特定するには、以下の手順を使用します。SSDの問題の症状の例として、データ管理エンジン（DME）プロセスの起動に失敗することがあります。

（注） 新しい SSD を挿入すると、ブレード BIOS 検出後にインベントリに基本情報（タイプ、モデル、SN など）のみが入力されます。ローカルディスクデータは、SSP-OS アップグレードの完了時にのみ、インベントリに入力されます。SSP-OS のアップグレードの状態がまだ「更新中」の場合、インベントリにはローカルディスクのエントリが表示されず、SSD の接続に関する障害メッセージも表示されません。

以下の手順に示されているログファイルの出力が SSD に関する問題を示している場合は、TAC にお問い合わせください（https://www.cisco.com/c/en/us/buy/product-returns-replacements-rma.html を参照）。

手順

ステップ 1 FXOS コマンドシェルに接続します。

connect fxos

ステップ 2 nvram ログファイルを表示します。

show logging nvram

エラー出力の例：

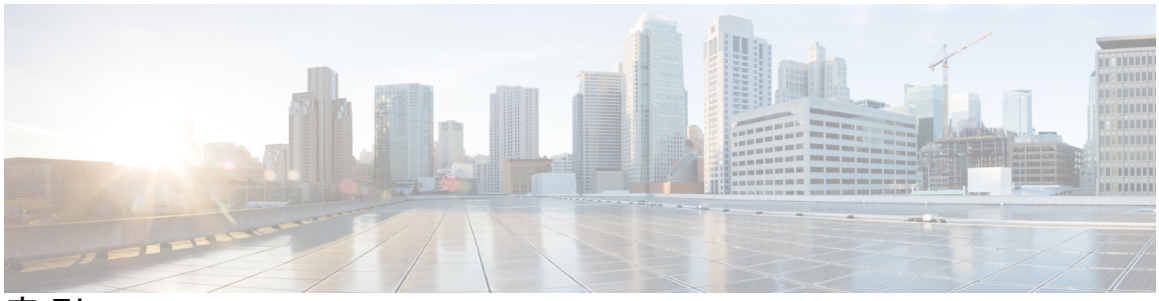
```
2020 Oct 22 13:03:26 MDCNGIPSAPL02 %$ VDC-1 %$ Oct 22 13:03:25 %KERN-2-SYSTEM_MSG:
[28175880.598580] EXT3-fs error (device sda4): ext3_get_inode_loc: unable to read inode
 block - inode=14, block=6
```

ステップ 3 ログファイルを表示します。

show logging logfile

エラー出力の例：

```
   2020 Oct 21 21:11:25  (none) kernel: [28118744.718445] EXT3-fs error (device sda4):
ext3_get_inode_loc: unable to read inode block - inode=14, block=6
```



索 引

き

く

こ

し

せ

そ

た

て

と

ね

は

ふ

ほ

ゆ

ら

ろ

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。