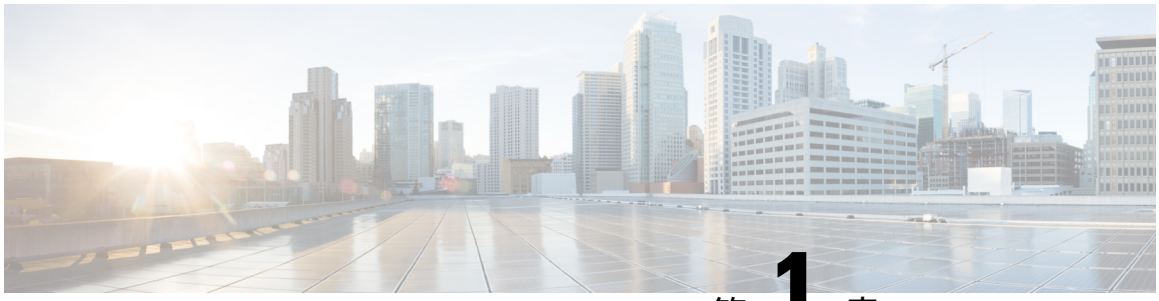
APIC 統合向け Cisco ASA クイック スタート ガイド 1.3(11)

初版：2018 年 9 月 10 日

最終更新：2018 年 9 月 12 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/



第 1 章

はじめに

概要

Cisco Application Policy Infrastructure Controller（APIC）は、Cisco Application Centric Infrastructure（ACI）のセントラル 機能を制御するシングルポイントです。APIC では、アプリケーション間の Cisco Adaptive Security Appliance（ASA）ノースバウンドなどのサービス挿入を自動化でき、エンドポイント グループ（EPG） とも呼ばれます。APIC は、ネットワークとサービスを設定するためにノースバウンド Application Programming Interfaces（API）を使用します。管理対象オブジェクトを使用して設定を作成、削除、変更するのに、これらの API を使用します。

サービス デバイスを設定しモニタするため、APIC にはデバイス パッケージと呼ばれるデバイスで実行されているソフトウェアが必要です。デバイス パッケージはサービス デバイスのクラスを管理し、デバイスに関する情報を APIC に送信するため、APIC はデバイスの動作を認識できます。デバイス パッケージを使用することで、ASA など、サービス デバイスにネットワーク サービス機能を挿入し設定できます。

このドキュメントでは、ASA と ACI の連携方法と、ASA の機能を利用するための APIC の設定法について説明します。

（注） 現在の ASA バージョンでサポートされない設定を作成しようとすると、次のようなエラーが APIC で表示されることがあります。

```
*Major script error: Configuration error: …. ERROR: % Invalid input detected at '^'
marker.
```

サポートされる機能については、ASA バージョンのマニュアルを参照してください。

サービス機能の挿入

サービス機能がアプリケーション間のサービス グラフに挿入されると、これらのアプリケーションからのトラフィックはAPICで分類され、オーバーレイ ネットワークのタグを使用して識別されます。サービス機能はタグを使用して、トラフィックにポリシーを適用します。APICとのASA統合の場合、サービス機能はルーテッドまたはトランスペアレント ファイアウォール動作を使用してトラフィックを転送します。

使用可能な APIC 製品

リリース1.2（7.8）以降、ACIのCisco ASAデバイス パッケージ ソフトウェアには2つのバージョンがあります。

- ACIのCisco ASAデバイス パッケージ ソフトウェア。このバージョンでは、次のようにAPICからASAの多くの重要機能を設定できます（ただし、次に限定されません）。
  - インターフェイス
  - Routing
  - Access-list（アクセス リスト）
  - NAT
  - TrustSec
  - アプリケーション インスペクション
  - NetFlow
  - ハイ アベイラビリティ
  - サイト間VPN
- ACIのCisco ASAデバイス パッケージ ファブリック挿入ソフトウェア。このバージョンには、元のバージョン機能の次のサブセットが含まれています。
  - インターフェイス
  - ダイナミック ルーティング
  - スタティック ルーティング

サポートされるバージョン

Cisco ASAデバイス パッケージのソフトウェアは、同梱されたAPIC ＭＰバージョンだけをサポートしています。

Cisco ASA デバイス パッケージ ソフトウェアのバージョン 1.3(x) は、APIC バージョン 3.1(x) 以降をサポートしています。したがって、1.3(x) は、クラウド オーケストレーター モードを 3.1(x) でサポートしていますが、古いバージョンではサポートしていません。

次の表は、サポートされるプラットフォームのそれぞれに対してサポートされている Cisco ASA ソフトウェアのバージョンを示しています。

プラットフォーム	ソフトウェア バージョン
ASA 5500-X（5512 ～ 5555）	ASA 8.4(x) 以降
ASA 5585-X（SSP 10 ～ SSP 60）	
Cisco Firepower 9300 セキュリティ アプライアンス	ASA 9.6(1) 以降
Cisco Firepower 41xx セキュリティ アプライアンス	
Cisco Firepower 21xx セキュリティ アプライアンス	ASA 9.8(1) 以降
Cisco ASAv	ASA 9.2(x) 以降 (Cisco ASA および APIC 互換性対応表)

Supported Features

次の表に、ASAv および ASA 5585-X でサポートされる機能を示します。BGP と OSPF をサポートするリリースについては、『Cisco ASA Device Package Software, Version 1.2(1) Release Notes』を参照してください。

機能	ASAv サポート	ASA 5500 X/5585 X サポート
アクセス リストおよびアクセス グループ	対応	対応
アプリケーション インスペクション	対応	対応
BGP	対応	対応
クラスタ	非対応	対応
接続制限	対応	対応
DNS クライアント	対応	対応
イーサ チャネル	非対応	対応

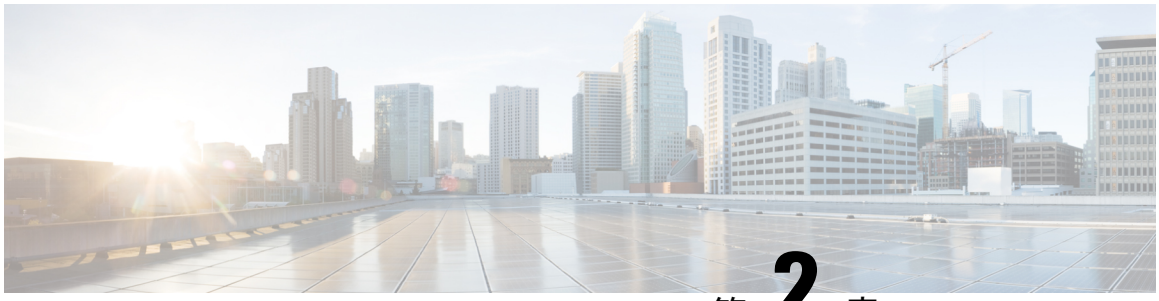
機能	ASAv サポート	ASA 5500 X/5585 X サポート
ハイ アベイラビリティ（アクティブ/アクティブ、アクティブ/スタンバイ）	アクティブ/スタンバイのみ	アクティブ/スタンバイのみ
インターフェイス コンフィギュレーション	対応	対応
インターフェイスの説明	対応	対応
IP 監査	対応	対応
IPv6	対応	対応
ロギング	対応	対応
毎日のメッセージ	対応	対応
マルチ コンテキスト	非対応	対応
NAT および Twice NAT	対応	対応
Netflow	対応	対応
ネットワーク、サービス オブジェクト、グループ	対応	対応
NTP	対応	対応
OSPF	対応	対応
プロトコルのタイムアウト	対応	対応
サービス ポリシー	対応	対応
AnyConnect Premium（共有）ライセンス	非対応	対応
サイト間 VPN	対応	対応
Smart Call Home の有効化	対応	対応
SNMPv3	対応	対応
スタティック ルーティング	対応	対応
TCP インターセプト（初期接続制限）	対応	対応
脅威の検出	対応	対応

機能	ASAv サポート	ASA 5500 X/5585 X サポート
TrustSec	対応	対応

関連資料

- Cisco ACI の基礎
- Cisco ACI セキュリティ ソリューション
- 『Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド』
- Cisco APIC の製品に関するサポート ページ
- Cisco ASA シリーズのロードマップ
- Cisco Firepower Management Center

関連資料



第 2 章

導入およびインストール

ASA の展開

ASA 5585-X を展開するには、インストール手順の Cisco ASA 5585-X クイック スタート ガイドを参照してください。

http://www.cisco.com/go/asa5585x-quick

ASAv を展開するには、インストール手順の Cisco Adaptive Security Virtual Appliance クイック スタート ガイドを参照してください。

http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/products-installation-guides-list.html

（注） ASAv の展開時に、管理インターフェイスの nameif プロパティの値を **management** として定義する必要があります。インターフェイス名を **management** 以外の値に定義した場合、デバイス クラスタは AuditRequested/AuditPending 状態で停止し、読み取り操作がタイムアウトしたことを示すエラーが表示されます。管理インターフェイスとデフォルト ゲートウェイの設定は ASAv から削除され、インターフェイスはシャット ダウンされます。

ASA デバイス パッケージのインストール

各サービス ノード タイプで、デバイス仕様とデバイス スクリプトの 2 つの部分を含むデバイス パッケージを指定する必要があります。同じタイプのサービス ノードは、単一のデバイス パッケージにバインドされます。

ASA デバイス パッケージでは、ASA を設定し、APIC を使用して ASA を登録できます。

始める前に

『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Overview」および「Prerequisites」の小の前提条件を確認します。

ステップ 1 ASA デバイス パッケージを http://www.cisco.com/go/asa-software にある .zip ファイルからダウンロードして、ローカル ドライブ上に保存します。このファイルは解凍しないでください。

ステップ 2 ASA デバイス パッケージをインストールします。『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Importing a Device Package」の章を参照してください。

ステップ 3 APIC に ASA を登録します。『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Configuring a Device Cluster」および「Configuring Connectivity to a Device Cluster」の章を参照してください。

1.2(x) から 1.3(x) への移行

ソフトウェア バージョン 1.2(x) から 1.3(x) に既存の Cisco ASA デバイス パッケージ導入を移行するには、次の手順を実行します。

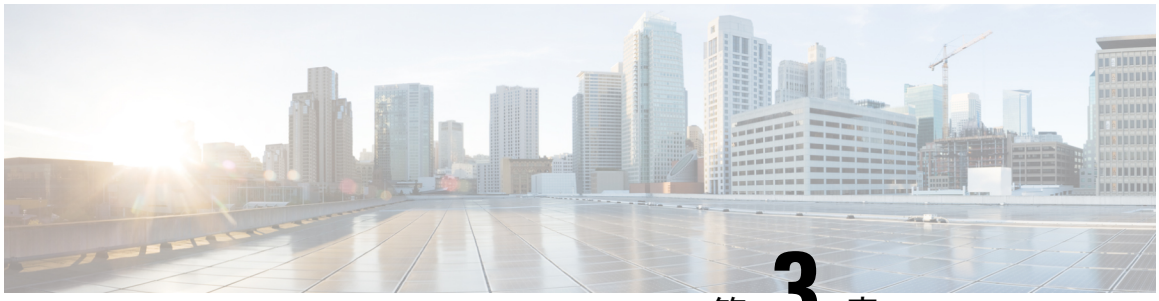
ステップ 1 ASA デバイス パッケージ ソフトウェア バージョン 1.3(x) を APIC にインストールします。

ステップ 2 既存の展開により、テナントから設定をダウンロードします。

ステップ 3 設定の top-level `<imdata>` タグを `<polUni>` に置き換えます。

ステップ 4 グローバルに設定の `mDev-CISCO-ASA-1.2` を `mDev-CISCO-ASA-1.3` に置き換えます。

ステップ 5 APIC 上で変更された設定をアップロードします。



第 3 章

設定

バックグラウンド

アプリケーションの一環として L4 L7 サービスの統合のため、ACI ファブリックを提供します。これは、APIC マネージド サービス グラフ、L4 L7 デバイス パッケージを必要とを使用して行います。インポートされたデバイス パッケージは、apic 内での設定パラメータを公開し、デバイス上に特定の設定を調整することができます。

L4 L7 サービス グラフをインストールするには、APIC に L4 L7 デバイスを登録機能プロファイルまたは L4 L7 サービス パラメータの一部として設定を追加し、サービス グラフに、これらの 2 つのリンクします。契約をこの L4 L7 サービス グラフを適用すると、APIC で表示ファブリックでは、デバイスインターフェイスをタギングおよびそれらを適切なコンシューマとプロバイダー Epg にステッチします。APIC では、自動方式で登録済みデバイスを特定の設定が適用されます。ACI ファブリックおよび L4 L7 デバイスに適用する設定をすべて、ACI ファブリックはインスペクションの特定のデバイスに契約で定義されたトラフィックを送信します。ACI では、1 つのサービス グラフの下に複数のサービスをチェーンすることもできます。

ASA への管理アクセスの設定

APIC が ASA を管理できるように ASA への管理アクセスを設定します。

- ASAv への管理アクセスを設定するには、それぞれのクイック スタート ガイドを参照してください。

  http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/products-installation-guides-list.html

• ASA 5585 X への管理アクセスを設定するには、このセクションの手順に従います。

ステップ 1 既存の設定を削除します。

```
ciscoasa(config)# clear configure all
```

ステップ 2 （任意）ファイアウォール モードをトランスペアレント ファイアウォール モードに設定します。

```
ciscoasa(config)# firewall transparent
```

ステップ 3 管理インターフェイスの IP アドレスとサブネット マスクを設定します。ASA は、APIC と同じサブネット上にある必要があります。

```
ciscoasa(config)# interface management {0/0 | 0/1}
ciscoasa(config-subif) # ip address ip_address subnet_mask
```

ステップ 4 インターフェイスの名前を "management" と指定します。

```
ciscoasa(config-subif)# nameif management
```

ステップ 5 インターフェイスを有効にします。

```
ciscoasa(config-subif) # no shutdown
```

ステップ 6 ASA HTTPS サーバを有効にします。

```
ciscoasa(config)# http server enable
```

ステップ 7 APIC で ASA へのアクセスをイネーブルにします。APIC クラスタの各 APIC に対してこの手順を繰り返します。

```
ciscoasa(config)# http apic_address 255.255.255.255 management
```

ステップ 8 ASA にアクセスする際に APIC が使用するユーザーを作成します。ユーザーは管理ユーザである必要はありません。任意のユーザを指定できます。

```
ciscoasa(config)# username username password password privilege 15
```

ステップ 9 APIC がローカル認証を使用して、HTTP コンソールにアクセスできる AAA 認証を作成します。

```
ciscoasa(config)# aaa authentication http console LOCAL
```

ステップ 10 秘密キーが存在することを確認します。存在しない場合、次のうち 1 つを生成します。

```
ciscoasa(config)# show crypto key mypubkey rsa
ciscoasa(config)# crypto key generate rsa
```

ステップ 11 Encryption-DES および Encryption-3DES-AES が有効になっていることを確認します。無効になっている場合は、新しいライセンスを生成します。

```
ciscoasa(config)# show version
```

ジャンボ フレーム サポートの設定

1500 バイトより大きいイーサネット パケットを使用するには、ジャンボ フレーム サポートを設定します

ステップ 1 ジャンボ フレームをイネーブルに設定します。

```
ciscoasa(config)# jumbo-frame reservation
```

ステップ 2 実行コンフィギュレーションを保存します。

```
ciscoasa(config)# write memory
```

ステップ 3 ASA をリブートします。

```
ciscoasa(config)# reload
```

マルチ コンテキスト モードの設定

マルチ コンテキスト モードを設定する場合、手順については、次の URL の『Cisco ASA Series General Operations CLI Configuration Guide』の「High Availability and Scalability」の章を参照してください。

システム モードでインターフェイスを設定し、それらをコンテキストに割り当て、各コンテキストでインターフェイスを設定する方法について説明しています。それらの手順はすべて、デバイス パッケージで実行します。

デバイス パッケージは、マルチ コンテキスト モードの各サービス グラフで使用されるインターフェイスの割り当ておよび設定を実行します。ただし、システム管理者は、マルチ コンテキスト ASA を APIC に登録する前に、それらをプロビジョニングする必要があります。

ステップ 1 必要なユーザ コンテキストを作成します。デバイス パッケージはコンテキストの作成または削除を行いません。

ステップ 2 コンテキストごとに、プロビジョニングをシングル コンテキスト ASA のプロビジョニングと同様にします。

1. 管理コンテキストから管理インターフェイスをそのコンテキストに割り当てます。次に例を示します。

```
context tenant
allocate-interface Management0/1
config-url disk0:/tenant1.cfg
```

2. ユーザー コンテキストで、**nameif** を使用して管理インターフェイスを **management** に設定し、静的 IP アドレスを指定します。次に例を示します。

```
interface management 0/1
nameif management
ip address 10.1.1.1 255.255.255.0
security-level 100
```

3. ユーザコンテキストで、管理インターフェイスへのHTTPSのアクセスをイネーブルにします。次に例を示します。

```
http server enable
http 0.0.0.0 0.0.0.0 management
```

4. ユーザー クレデンシャルを設定し、APIC がローカル認証を使用して、HTTP コンソールにアクセスできる AAA 認証を作成します。

```
username username password password privilege 15
aaa authentication http console LOCAL
```

5. 管理ルートを設定します。
6. 秘密キーが存在することを確認します。存在しない場合、次のうち 1 つを生成します。

```
show crypto key mypubkey rsa
crypto key generate rsa
```

ASA クラスタの設定

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての管理上の利便性を備える一方で、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。詳細については、『Cisco ASA Series General Operations CLI Configuration Guide』の「ASA Cluster」の章を参照してください。

デフォルトでは、APIC は ASA クラスタの設定にタッチしません。CLI、ASDM、または CSM を使用してアウトオブ バンドを設定するオプションがあります。

ASA デバイス パッケージのこのリリースは、APIC を使用した ASA クラスタの設定サポートが導入されています。この方法の利点は次のとおりです。

- 各 CDev 以外の LDev クラスタ パラメータを設定します。したがって、各ユニットで繰り返すのではなく、パラメータを 1 回入力するだけで済みます。これは、クラスタ ユニットの間でパラメータのミスマッチを防ぎます。ASA デバイス パッケージは、APIC から変更を行うときに、クラスタ ユニットから ASA クラスタ設定を設定または削除する順序で制御できます。
- ASA デバイス パッケージは、ユニット ラベル、優先度、管理 IP アドレス プールのように、一部のパラメータを自動で生成します。これにより、ユーザーによる設定タスクの数を最小限にして、ユーザーによるエラーを回避します。

（注） これを既存の ASA クラスタ セットアップとその設定を動作させるために使用することは推奨しません。

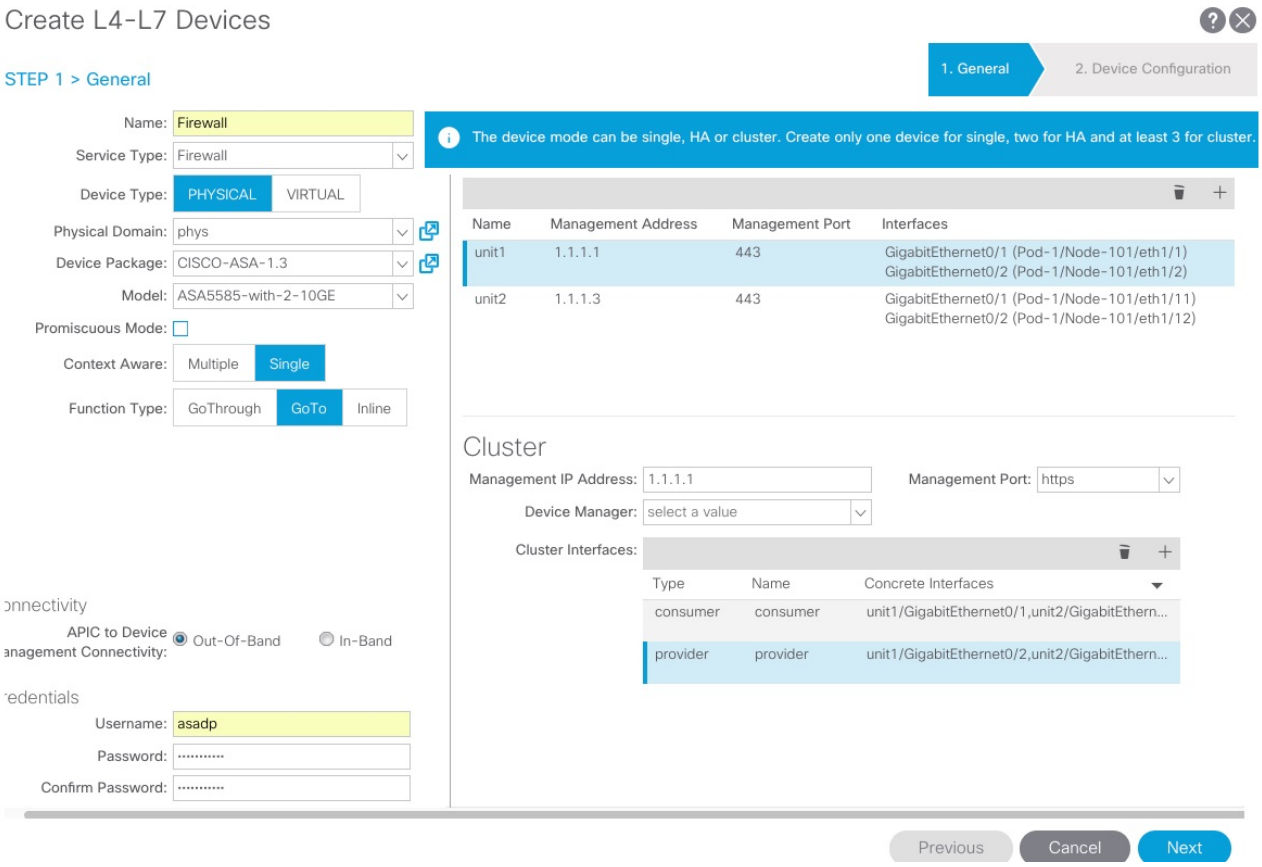
始める前に

- 物理 ASA ユニットを使用する必要があります。仮想 ASA では、クラスタリングはサポートされていません。
- 同じソフトウェア イメージ バージョンを実行している同じモデルと、同じモードで少なくとも 2 つの ASA ユニットが必要です。（トランスペアレントまたはルート。単一コンテキストモードのすべてまたは複数のコンテキストモードのすべて）混在させないでください。
- クラスタ制御リンクとして設計されている各 ASA から、少なくとも 1 つのハードウェア インターフェイスが必須です。
- ASA で、ASA クラスタを設定または削除するときに設定されたデータインターフェイスがないことを確認します。
- APIC で、クラスタ設定を作成または削除する前に、すべてのサービス グラフを削除する必要があります。

ステップ 1 APIC では、LDev（論理デバイス）で CDevs（具体的なデバイス）として、クラスタ内のすべての ASA ユニットを登録します。

（注） ASA クラスタが形成されたら APIC との接続を失うことがないように、ASA ユニットの管理 IP アドレスを連続させる必要があります。たとえば、2 つの ASA ユニットがあり最初の ASA に 1.1.1.1 の IP アドレスがある場合、2 番目の ASA が 1.1.1.3 となる必要があります。また、ASA クラスタが形成されるように 1.1.1.1 が ASA クラスタの仮想 IP アドレスになり、1.1.1.2 が最初の ASA のローカル IP アドレスになり、1.1.1.3 が 2 番目の ASA のローカル IP アドレスのままになります。

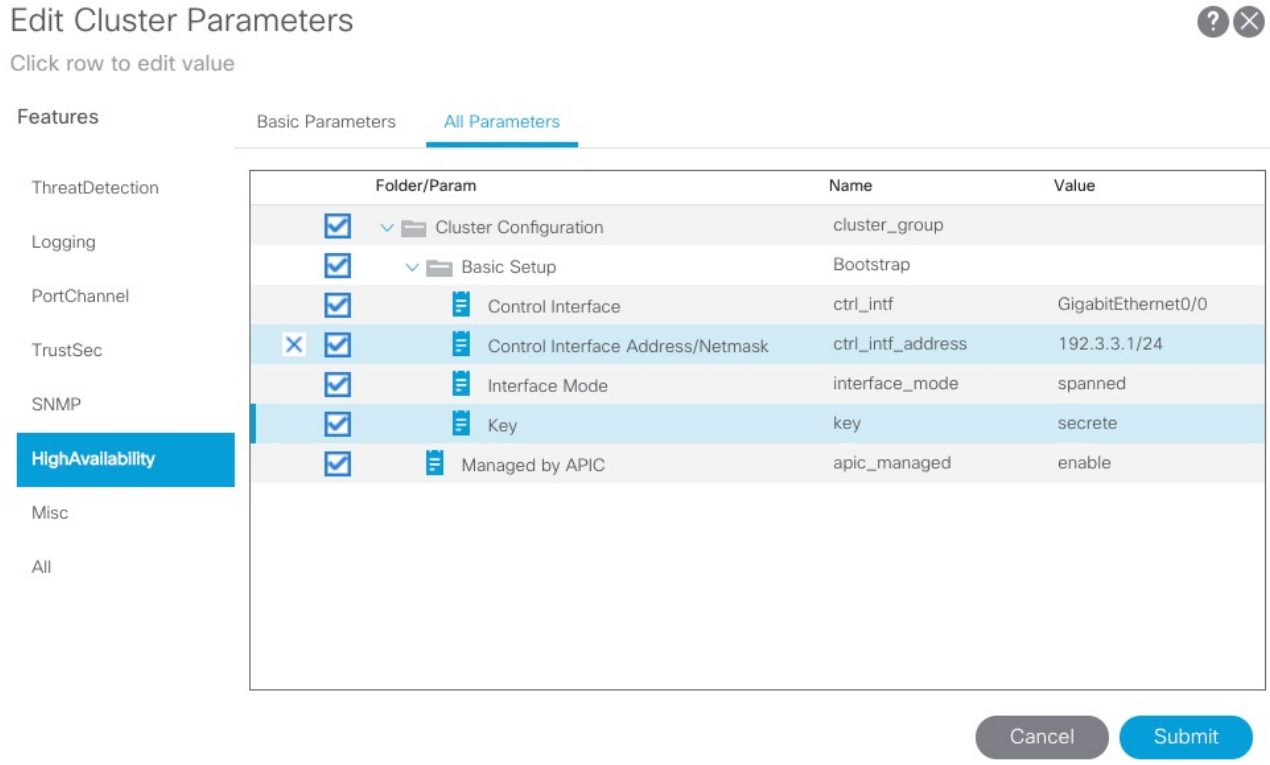
次に例を示します。



ステップ 2 LDev を設定します。

（注） ASA クラスタが形成されるまで 最大 2 分間待機します。クラスタ ユニットの管理 IP アドレスを正常に ping した後、設定を変更しないでください。

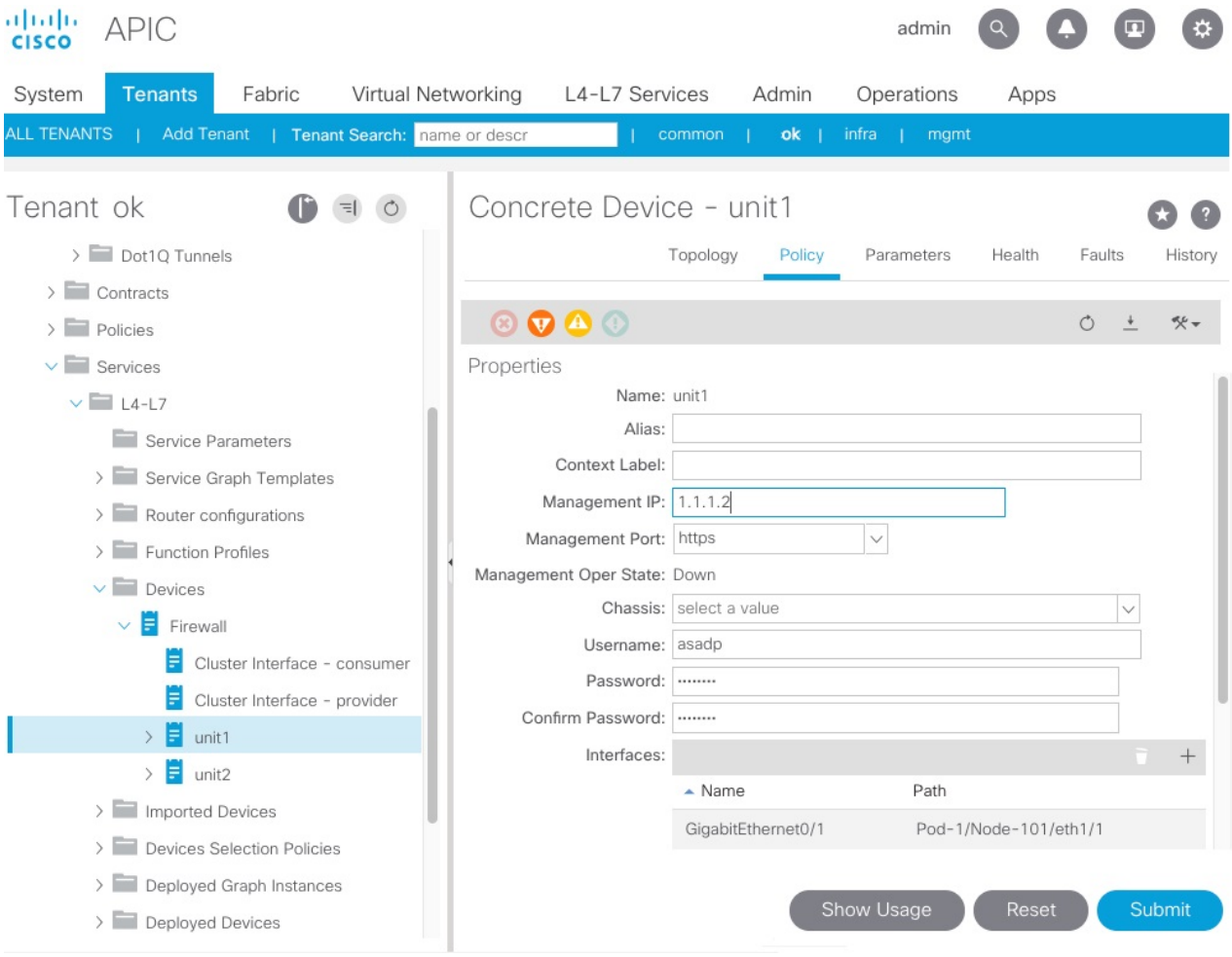
次に例を示します。



ステップ 3 LDev の管理 IP アドレスは、ASA クラスタの仮想 IP アドレスになります。クラスタが形成されると、マスタ ユニットはそのローカル IP アドレスとして別の IP アドレスを取得します。新しいローカル IP アドレスへのマスター ユニットを表す CDev の IP アドレスを変更します。そうしないと、ファールオーバー中などマスタ ユニットに変更がある場合、APIC はマスタの状態をモニタできません。

（注） ASA クラスタ設定を削除する場合は、元の値にマスタ ユニットの IP アドレスを復元するようしてください。

次に例を示します。



次のタスク

クラスタからASAユニットを追加または削除するには、クラスタ設定を削除し、APICのASAユニットを追加または削除し、クラスタを再度設定します。

APIC から ASA を設定する

ノースバウンド API を使用して、セキュリティ ポリシー（特にサービス グラフについて）を設定します。

APIC ノースバウンドの API の使用方法については、『Cisco APIC Management Information Model Reference（Cisco APIC 管理情報モデルのリファレンス）』を参照してください。

詳細については、『APIC documentation（APIC マニュアル）』を参照してください。