# cisco.



### APIC 連携、1.0.3 の Cisco Firepower Threat Defense クイック ス タート ガイド

**初版**:2018年4月17日 最終更新:2018年5月22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/ © 2018 Cisco Systems, Inc. All rights reserved.



# はじめに

- 概要 (1ページ)
- 前提条件 (3ページ)
- •関連資料 (5ページ)

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 Firepower Threat Defense(FTD)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、FTD アプライアンスなど、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。

FTD ファブリック挿入(FI)デバイスパッケージは、全デバイス設定の責任がセキュリティ とネットワーク管理者の間で共有されているハイブリッドモデル(ACI用語でサービスマネー ジャ)に基づいています。

- ・セキュリティ管理者:セキュリティゾーンの条件が未設定のまま、新しいサービスグラフにセキュリティポリシーを事前定義するためFMCを使用します。新しいポリシールールは適切なアクセス(プロトコルを許可)と、NGIPSおよびマルウェアのポリシー、URLフィルタリング、Threat Grid など高度な保護設定を定義します。
- ネットワーク管理者。サービスグラフをオーケストレーションし、ACIファブリックに FTD デバイスを挿入して、この事前定義されたセキュリティポリシーにダイレクトトラフィックを接続するため、APICを使用します。APICのL4~L7デバイスパラメータまたは機能のプロファイル内で、ネットワーク管理者は、事前定義されたFMCアクセスコントロールポリシーやルールの一致を含む、このガイドで定義されたパラメータを設定します。

APICがFMCのアクセスコントロールポリシールール名と一致する場合、ルールに新しく作成されたセキュリティゾーンを挿入するだけです。ルールが見つからない場合、APICはその名前で新しいルールを作成し、セキュリティゾーンを接続して、[拒否アクション]を設定します。これは、トラフィックが特定のサービスグラフに許可される前に、セキュリティ管理者が新しいルール基準と適切な保護設定を更新するように強制します。



このドキュメントでは、FTD と ACI の連携方法と、FTD 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。

- Firepower Management Center (FMC) で、REST API を有効化にします
- CCO から ACI デバイス パッケージ ソフトウェアの FTD をダウンロードします
- APIC に ACI デバイス パッケージの FTD をインポートします
- •FTD アプライアンスを登録します
- •FTD アプライアンスを使用するネットワーク サービス グラフを定義します

(注) このドキュメントで使用される例のスクリーン ショットでは、SampleTenant という名前の既存のテナントが示されています。このガイドの手順に従って提供されたテンプレートを使用する場合、実際のテナント名を使用します。

#### 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 FTD 統合の場合、サービス機能はルーテッド、トランスペアレント、またはインライン 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

初期のソフトウェア リリースには、ACI 用の Cisco FTD デバイス パッケージ ファブリック挿 入ソフトウェアが含まれています。

## 前提条件

- •FMC バージョン 6.2.3:FTD の REST API のサポートが含まれています。
- FTD バージョン 6.2.3.
- APIC バージョン 2.3(1f): そのデバイスマネージャがデバイスを登録するために使用します。FTDデバイスパッケージは、デバイスマネージャが FMC 設定のネットワーク部分を APIC によりインスタンス化することを許可するために使用されます。
- FTD アプライアンスを挿入し、ネットワークサービスが基本設定のブートストラップとして設定されており、FMC に登録されていることを確認します。たとえば、FTD の FMCのデバイス管理ページを参照してください。

Overview Analysis	Policies	Devices	Objects AMP		Deploy 🦺 Sys	stem Help 🔻 admin 🔻
Device Management	NAT	VPN QoS	Platform Settings	FlexConfig Certificates		
By Group 👻					🕥 Add 🗸	🔍 Device Name
Name				Model	License Type	Access Control Policy
4 🣁 Ungrouped (4)						
10.254.6.96 10.254.6.96 - Cisco Firepower Threat Defense for VMWare - v6.2.0 - routed			Cisco Firepower Threat Defense	Base, Threat, Malware	ACIAccPolicyRouted	

• REST API トークン生成の競合状態を避けるためには、ACI 上での使用専用の FMC 管理者 を作成します。次に例を示します。

Overview Analysis Policies Devices C	bjects AMP		and the second filler of the	Deploy	A System Help v
		Configuration Use	s Domains Integration	Updates Licenses •	Health • Monitoring •
Users User Roles External Authen	tication				
					O Create User
Username	Roles	Authentication Method	Password Lifetime		
aciadmin	Administrator	Internal	Unlimited		
admin	Administrator	Internal	Unlimited		0

- ・展開上の障害とサーバ間で時間差の両方を回避するには、同じNetwork Time Protocol (NTP) サーバを使用するように APIC と FMC を設定します。Firepower 41xx および 93xx シリー ズのアプライアンス上の FTD では、シャーシマネージャも設定するが必要があります。
  - APIC内で、[ファブリック]>[ファブリックポリシー]>[ポッドポリシー]>[ポリシー]
     [日付と時刻] に移動します。同じ NTPサーバを設定するには、作成日と時刻ポリシーのウィザードを使用します。

cisco	System	Tenants	Fabric	VM Networking	L4-L7 Services	Admin Operatio	ns 👂 i
		Inventory   Fa	bric Policies   Acc	ess Policies			
Policies	⊴ ⊙	Data and Time	Believ B	aliau dafault			
Quick Start		Date and Time	e Policy - P	olicy default			
Switch Policies		⊖±					
Module Policies		Description					
Interface Policies		Properties					
Pod Policies		Name:	detault				
Policies		Description.	optorial				
🔺 🚞 Date and Time							
🕨 🔯 Policy default		Administrative State:	disabled e	nabled			
🔯 default		Authorities Oblig					
SNMP		Authentication State:	disabled e	nabled			
Management Access		NTP Servers:					
ISIS Policy default		_			Minimum Pollin	Maximum Polling	
COOP Group Policy of	lefault		Host Name/IP Add	Iress Preferred	Interval	Interval	Management EPG
BGP Route Reflector	default		128.59.0.245	True	4	6	default (Out-of-Band)
Policy Groups							
Profiles							
Global Policies							
Monitoring Policies							
Troubleshoot Policies							
Geolocation Policies							
Tags							

•FMC で、[システム] > [設定] > [時間同期] に移動し、同じ NTPサーバを設定します。

Overview Analysis Policies D	evices Objects AMP			eter a la complete	a na setta series	del Parro ante a car	Deploy	A <sub>1</sub> Sy	stem Help 🔻	admin 🔻
		Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
									-	
Access List	Construction NTD	[a. 11.1.a]							ave	
Process	Serve Time via NTP	Enabled ¥								
Audit Log Certificate	Cable Chal	Manually in Loca	al Configura	tion						
Audit Log	Set My Clock	128,59,0,245								
Login Banner										
Change Reconciliation										
DNS Cache										
Dashboard										
Database										
External Database Access										
Email Notification										
Access Control Preferences										
HTTPS Certificate										
Information										
Intrusion Policy Preferences										
Language										
Management Interfaces										
Network Analysis Policy Preferences										
Remote Storage Device										
REST API Preferences										
SNMP										
UCAPL/CC Compliance										
Shell Timeout										
Time										
Time Synchronization										
VMware Tools										
Vulnerability Mapping										

• Firepower 41xx および 93xx シリーズ アプライアンスのシャーシ マネージャで、[プ ラットフォーム設定]>[NTP]>[時間同期] に移動し、同じNTPサーバを追加します。

Overview Interfaces L	ogical Devices S	ecurity Engine Plat	form Settings	System	Tool
► NTP	Time Synchroniza	tion Current Time			
SSH SNMP HTTPS AAA Syslog DNS FIPS and Common Criteria	Set Time Source Set Time Manua Date: Time:	Ily 02/06/2017 6   0 Get System Time	(mm/dd/yyyy)	nm)	
Access List	NTP Server Authe	ntication: Enable			
	<ul> <li>Use NTP Server</li> </ul>	•		A	dd
	NTP Server	Server Status	Acti	ons	
	ntp.esl.cisco.com	Synchronized	Ø (	1	

# (注)

現在の FMC または FTD バージョンでサポートされていない設定を作成する場合、APIC 上に 次と同様のエラーが表示される場合があります。「メジャースクリプトエラー:設定エラー: ERROR: % Invalid input detected at '^' marker."

# 関連資料

- Cisco Application Centric Infrastructure Fundamentals
- ・『Cisco APIC レイヤ4~レイヤ7サービス導入ガイド』
- Cisco Firepower Threat Defense NGFW
- Cisco Firepower Management Center



# インストールするもの

- FMC REST API が有効になっていることの確認 (7ページ)
- ・デバイス パッケージのインポート (8ページ)

# FMC REST API が有効になっていることの確認

APIC は REST API を使用して Firepower デバイスに接続します。デフォルトで、REST API は 有効になっています。APIC がセットアップされ Firepower デバイスを管理する前に、次の手順 を完了して FMC REST API が有効になっていることを確認します。

#### 始める前に

FMC ではバージョン 6.2.0 以降を実行している必要があります。



- (注) RESTAPIは、FMCソフトウェア;ですでにパッケージ化されており、ライセンスは必要ありません。
- ステップ1 管理者のクレデンシャルを使用して FMC にサインインします。
- ステップ2 [システム] > [設定] > [REST API 設定] に移動します。
- ステップ3 [REST API の有効化] チェック ボックスがまだ選択されていない場合、ボックスをオンにして [保存] をク リックします。

erview Analysis Policies De	vices Objects AMP		a construction and the					Deploy	Sys	tem Help v	admin
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools
											Saue
											0010
ccess List	a										
rocess	Enable REST API										
udit Log Certificate											
udit Log											
ogin Banner											
hange Reconciliation											
NS Cache											
ashboard											
atabase											
ternal Database Access											
nail Notification											
cess Control Preferences											
TPS Certificate											
formation											
rusion Policy Preferences											
nguage											
inagement Interfaces											
twork Analysis Policy Preferences											
mote Storage Device											
ST API Preferences											
MP											
APL/CC Compliance											
ell Timeout											
me											
me Synchronization											
fware Tools											
Inerability Mapping											

#### 次のタスク

REST API が有効になると、FMC は ACI デバイス パッケージの FTD をサポートする準備ができています。

APIC で使用する管理者以外のアカウントを作成します。

# デバイス パッケージのインポート

APIC は、サービス デバイスを設定およびモニタするためデバイス パッケージが必要です。 APIC が FTD アプライアンスの存在と FTD アプライアンスの機能を認識できるように、ACI デバイス パッケージの FTD を APIC にインポートします。

- **ステップ1** http://www.cisco.com/go/software からデバイスパッケージをダウンロードし、ローカルドライブ上に保存します。
  - (注) デバイス パッケージは .zip ファイルとしてダウンロードされます。このファイルは解凍しないで ください。
- ステップ2 プロバイダ管理者として APIC にサインインします。
- ステップ3 メニューバーで、[L4-L7 サービス] をクリックします。
- **ステップ4** サブメニュー バーで、[パッケージ] をクリックします。
- ステップ5 [ナビゲーション] ペインで、[L4-L7 サービス デバイス タイプ] をクリックします。
- ステップ6 [アクション] > [デバイス パッケージのインポート] を選択します。

ステップ7 [ファイル名] フィールドで、手順1 でダウンロードしたデバイス パッケージを指定し、[送信] をクリック します。

#### 次のタスク

[デバイス タイプ] ウィンドウを更新します。新しいデバイスがデバイス タイプのリスト内に 表示されます。

	Inventory   Packages						
Packages 😽 🖸	14-17 Servi	ice Device Type	20		;		
Cuick Start		loc Device Type			1		
L4-L7 Service Device Types	⊙±				ACTIONS -		
	Vendor	A Model	Version	Functions			
	CISCO	ASA	1.2	Firewall			
	CISCO	ASA_FI	1.2	Firewall			
	CISCO	FTD_FI	1.0	FTD			

(オプション)[ナビゲーション]ウィンドウで、[**デバイス タイプ**]を展開し、デバイス パッ ケージの機能のパラメータを表示します。



## 設定

- バックグラウンド(11ページ)
- •FTD アプライアンスの登録 (11ページ)
- サービス グラフの作成 (21ページ)
- ・サーサービス グラフ テンプレートの適用ビス グラフ テンプレートの適用 (22 ページ)
- Supported Functions  $(25 \sim \checkmark)$
- FTD 展開 (33 ページ)

# 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。

# FTD アプライアンスの登録

APICでFTDデバイスを登録する前に、APICデバイスマネージャとしてそのFMC管理ステー ションを追加します。このハイブリッドサービスグラフのモデルでは、APIC およびFMC は FTD 設定の完全な責任を共有します。FMC が EPG 間の通信を制御する脅威ポリシーとルール を定義する一方で、APICインターフェイス、IP アドレス、セキュリティゾーン、BVI、NGIPS インラインペアの設定をプロビジョニングします。デバイスマネージャとしてFMCを追加し て、サービスグラフで利用するために APIC で FTD アプライアンスを登録します。



(注) 1 個の FMC は、複数のサービス グラフにプロビジョニングされた複数の FTD デバイスに、デ バイス マネージャとして使用できます。

#### 始める前に

- •HTTPの通信を許可する APIC 通信ポリシーを設定します。
- ・仮想マシンマネージャまたは物理ドメインのいずれかを設定します。
- ・テナントを設定します。このセクションの手順では、既存のテナントが必要です。
- **ステップ1** APIC にサインインします。
- **ステップ2** メニューバーで、[テナント] をクリックします。
- ステップ3 [ナビゲーション]ペインで、[テナント] ブランチを展開し、[L4-L7 サービス] ブランチを展開して、[デ バイス マネージャ] をクリックします。
- ステップ4 [アクション]>[デバイス マネージャの作成] を選択します。
- **ステップ5** 次のオプションを完了します。

オプション	説明
デバイスマネージャ名	デバイスマネージャの名前。
デバイスマネージャタイプ	[CISCO-FTDmgr_FI-1.0] を選択します。
管理	[+]をクリックしてFMCを追加します。これはFTD アプライアンスを管理して、[ホスト] および [ポー ト] フィールドに入力します。[Update] をクリック します。
Username	FMC のユーザー名
Password	FMC のパスワード
Confirm Password	FMC のパスワード



- **ステップ6** [送信] をクリックして、デバイスマネージャを作成します。
- ステップ7 [ナビゲーション]ペインで、[テナント]ブランチを展開し、[L4-L7サービス]ブランチを展開して、[L4-L7 デバイス] をクリックします。

cisco APIC s	System Tenants	Fabric	VM Networking
ALL TENANTS   Add Tenant	Tenant Search: Ente	er name, alias, desc	r   common
Tenant			0 = 0
C Quick Start			
V 🔢 Tenant			
> Application Profiles			
> Networking			
L4-L7 Service Parameter	rs		
> Security Policies			
> Troubleshoot Policies			
> Monitoring Policies			
V L4-L7 Services			
> 🔚 L4-L7 Service Graph	Templates		
> Router configurations	;		
> E Function Profiles			
✓ 📰 L4-L7 Devices			

**ステップ8** [L4-L7 デバイスの作成] を右クリックして選択します。[L4-L7 デバイスの作成] ダイアログ ボックスが 表示され、[全般] ページが表示されます。

ステップ9 次の手順を実行します。

オプション	説明
名前	FTD アプライアンスの名前。
	<ul> <li>(注) FMC フィールドは 48 文字に制限され、FMC に 「<field value="">_<tenant name="">_<l4-l7 device<br="">Name&gt;」として保存されるため、この制限に対応 するためにテナント、デバイス名の長さを短くす ることをお勧めします。</l4-l7></tenant></field></li> </ul>
Service Type	<b>[ファイアウォール]</b> を選択します。
Device Type	[物理] または [仮想] を選択します。
デバイス パッケージ	アップロードしたデバイス パッケージを選択します。
モデル	FTD アプライアンスのモデルを選択します。

オプション	説明
コンテキスト認識	テナントにアプライアンスを割り当てます。
	(注) 複数は推奨されません。
	[単一]は、アプライアンスクラスタをこのプロバイダーネットワーク上でホストする特定のタイプの複数のテナント全体でアプライアンスクラスタを共有できないことを示しています。
	[複数]は、アプライアンスクラスタをこのプロバイダーネットワーク上でホストする特定のタイプの複数のテナント全体でアプライアンスクラスタを共有できることを示しています。たとえば、同じアプライアンスを共有する2つのホスティング会社が存在する可能性があります。テナントの割り当ては、パッケージがバインドされているエンドポイントグループ(EPG)に暗黙的に基づいています。クラスタを作成した場合、アプライアンス管理されるネットワークを判断する管理 EPG を指定する必要があります。
機能タイプ	[GoThrough] または [GoTo] を選択します。
	[GoThrough] アプライアンスは、トランスペアレントファイ アウォール (BVI を使用) または NGIPS モード (IPS 専用 ポートを使用) アプライアンスです。ネットワーク パケッ トは変更に応じてアプライアンスを通過し、エンドポイン トはそのアプライアンスを認識しません。[GoTo] アプライ アンスはルーテッド ファイアウォール モードであり、特定 のL3 宛先から L2 接続 EPG として動作します。
物理的なドメイン	物理 FTD アプライアンスについては、このアプライアンス クラスタを使用するグラフのネットワーク リリースを割り 当てる場合に使用するドメインを選択します。既存の物理 ドメインを選択するか、新規作成します。
	(注) これは、仮想FTDアプライアンスには必要はあり ません。
ビュー	単一ノードがデフォルト設定です。設定するデバイス1を 示します。
	<ul> <li>(注) 1.0.2 以降、HA ノードはサポートされています。</li> <li>[HAノード] が選択される場合、HAデバイスペアのデバイス1およびデバイス2 が設定のため表示されます。</li> </ul>

オプション	説明
	<ul> <li>(注) 1.0.3以降、クラスタリングがサポートされます。</li> <li>[クラスタ] が選択される場合、複数のデバイスを 独自の管理アドレスに追加できます。</li> </ul>
VMM ドメイン	仮想 FTD アプライアンスについては、Virtual Machine Manager (VMM) ドメイン (vCenter ドメイン)を選択します。既存 の VMM ドメインを選択するか、新規作成します。
	(注) これは、物理FTDアプライアンスには必要はあり ません。
Username	FMC のユーザー名
Password	FMC のパスワード
Confirm Password	FMC のパスワード

|--|

オプション	説明
管理 IP アドレス	アプライアンス クラスタ内の具体的なアプライア ンスの管理インターフェイスの IP アドレス。
Management Port	[HTTP] または [HTTPS] を選択します。
VM	仮想 FTD では、アプライアンスがホストされてい る仮想マシンの名前。
	(注) これは、物理 FTD アプライアンスには必要はありません。

ステップ11 デバイスインターフェイスでは、[+]をクリックして、具体的なアプライアンス上のインターフェイスである具体的なインターフェイスに情報を入力します。入力する情報は、具象インターフェイスがファブリックに接続され、具象インターフェイスが論理インターフェイスに接続される方法について指定します。[更新]をクリックしてインターフェイスを追加します。次のオプションを完了します。

オプション	説明
名前	[名前] フィールドは、具体的なアプライアンスのインターフェイスを 特定します。たとえば、GigabitEthernet0/1 または GigabitEthernet0/2 で す。
パス	物理アプライアンスは、具体的なインターフェイスがファブリックに 接続する方法を指定します。たとえば、具象インターフェイスがアタッ チされるリーフ ノード/スロット/ポートです。
vNIC	仮想アプライアンスでは、具体的なアプライアンスの対応するインター フェイスを識別するために vCenter 上で割り当てられたネットワーク アダプタ名。vCenter では通常、x=1、2、3の場合 vNIC が [ネットワー ク アダプタ x] にラベリングされます。
	<ul><li>(注) アプライアンス、インターフェイス MAC アドレスをチェックし、[MAC アドレス] フィールドを照合することで vCenter 上の対応するvNIC を識別できます。</li></ul>

ステップ12 [ビュー: HA ノード] が選択される場合、[デバイス 2] セクションの対応するオプションを入力します。 デバイス 1 および 2 は、HA フェールオーバーペアを形成します。

次に例を示します。

Device 1					
Management IP Address:	192.168.102.194		Management Port:	https	$\sim$
VM:	kevin-vcenter/vFTD622	~ <b>(2</b>			
Chassis:	select a value	$\sim$			
Device Interfaces:				Ì	+
	Name	VNIC	Path (Only For Route	Peering)	
	GigabitEthernet0/0	Network adapter 2			
	GigabitEthernet0/1	Network adapter 3			
Device 2					
Management IP Address:	192.168.102.195		Management Port:	https	$\sim$
VM:	kevin-vcenter/vFTDtfw	~ 🖉			
Chassis:	select a value	×			
Device Interfaces:				Ì	+
	Name	VNIC	Path (Only For Route	Peering)	
	GigabitEthernet0/0	Network adapter 2			
	GigabitEthernet0/1	Network adapter 3			

設定

[ビュー: クラスタ] が選択される場合:

General			Daviasa						
Managed:			Devices						
Name:	FTDRouted								
Service Type:	Firewall	$\sim$	Name Ma	anage	ement Addr	ess	Manag	gement Port	Interfaces
Device Type:	PHYSICAL VIRTUAL		FTDmaster 19	92.16	8.102.152		443		Port-channel1 ( Port-channel2 (
Physical Domain:	Shiva4100FTDPhy	~ 🖉	FTDslave 19	92.16	8.102.153		443		Port-channel1 (
View:	Single Node	IA Node							Port-channel2 (
	Oluster								
Device Package:	CISCO-FTD_FI-1.0	~ 🗗							
Model:	41xx-Series	~							
Promiscuous Mode: Context Aware: Function Type:	Multiple Single GoThrough GoTo		Cluster						
			Management IP Addre	ess:	192.168.10	2.195		Ma	anagement Port:
			Device Manag	ger:	common/FN	MC195	× (	ø	
			Cluster Interfaces:						
Connectivity				Typ	be	Name		Concrete Inte	rfaces
APIC to Device Management Connectivity:	Out-Of-Band In-Band			co	nsumer	outsid	de	FTDmaster/P	ort-channel1,FTD
Credentials				pro	ovider	inside	9	FTDmaster/P	ort-channel2,FTD
Username:	management-user								
Password:									
Confirm Password:									

ステップ13 [クラスタ] セクションで、次のオプションを入力します。

オプション	説明
管理IPアドレス	FMCのIPアドレス。
Management Port	FMC のポート番号。
Device Manager	デバイスマネージャを選択します。

ステップ14 クラスタインターフェイスでは、[+]をクリックして、クラスタ論理インターフェイスであるクラスタインターフェイスに情報を入力します。入力する情報は、論理インターフェイスがファブリックに接続され、論理インターフェイスがアプライアンスの具体的なインターフェイスに接続される方法について指定します。[更新]をクリックしてインターフェイスを追加します。次のオプションを完了します。

オプション	説明
タイプ	クラスタ論理インターフェイスの種類たとえば、 <b>[コンシュー</b> マ] または [プロバイダ]。

オプション	説明
名前	[名前] フィールドは、グラフのインターフェイスを特定しま す。たとえば、 <b>[外部]</b> または <b>[内部]</b> 。
具体的なインターフェイス	論理インターフェイスがアプライアンスの具体的なインター フェイスに接続する方法を指定します。

**ステップ15** クラスタのインターフェイスでは、HAデバイスペアの両方のメンバにインターフェイスを指定します。 次に例を示します。

Cluster					
Management IP Address:	192.168.102.	193		Management Port: https	
Device Manager:	common/FMC	165	~ 🕑		
Cluster Interfaces:				ì	i i
	Туре	ľ	lame	Concrete Interfaces	
	consumer	$\vee$ $\epsilon$	external	Device2/GigabitEthernet0/0	÷
			Lindata	Device1/GigabitEthernet0/0	
			Opdate	Device1/GigabitEthernet0/1	
				Device2/GigabitEthernet0/0	
				Device2/GigabitEthernet0/1	
Cluster					
Management IP Address:	192.168.102.	193		Management Port: https	
Device Manager:	common/FMC	165	~ 🗗		
Cluster Interfaces:				ì	ì ·
	Туре	Name	Concrete Interfaces		
	consumer	external	Device1/GigabitEthe	rnet0/0,Device2/GigabitEthernet0/0	
	provider	internal	Device1/GigabitEthe	rnet0/1,Device2/GigabitEthernet0/1	

- **ステップ16** [Next] をクリックします。
- **ステップ17** (任意) コンフィギュレーション パラメータを追加します。設定パラメータは具体的なアプライアンス を対象としており、初期化時にワンタイム設定中に使用されます初期化。

**ステップ18** [終了] をクリックししてアプライアンスを作成します。

#### 次のタスク

L4-L7 デバイスで FTD デバイスを選択するとき、APIC が適切に登録できる場合は「安定」状態を示している必要があります。FMC に到達不可能、または FMC 上の特定の IP アドレスで FTD が登録されている場合、エラーが表示されます。L4-L7 デバイスの障害を理解し解決する には、「トラブルシューティング」の章を参照してください。L4 - L7 設定を使用したサービ スグラフを作成する前に、FTD デバイスが「安定」状態であることを確認します。

## サービス グラフの作成

サービスグラフは、端末セット間の順序付けられた一連の機能ノードで、アプリケーションが 必要とする一連のネットワークサービス機能を識別します。グラフ内のサービス機能は、アプ リケーションの要件に基づいたサービスデバイスに自動的にプロビジョニングされます。

アプライアンスを登録した後は、そのアプライアンスおよびそのアプライアンスが提示したす べての機能を使用してサービス グラフを作成できます。サービス グラフは、共通テナントで 作成するか、テナント固有にすることができます。これは、プロバイダー管理者またはテナン ト内のテナント管理者によって実行されます。

サービス機能として FTD を挿入するには、サービス グラフ テンプレートを FTD 関数ノード を使用して作成する必要があります。

- ステップ1 APIC にサインインします。
- **ステップ2** 共通テナントまたは特定のテナントに移動します。
- ステップ3 [ナビゲーション]ペインで、[L4-L7サービス] ブランチを展開し、[L4-L7 サービス グラフ テンプレー ト] をクリックします。
- ステップ4 [アクション] > [L4 L7 サービス グラフ テンプレートの作成] を選択します。
  - (注) [L4-L7 サービス グラフ テンプレートの作成] ダイアログ ボックスが表示されます。左側のペインには、APIC が認識しているサービス デバイス、およびデバイスによって提供されるサービス機能が一覧表示されます。APIC は、以前インポートした ACI デバイス パッケージの FTD からこの情報を取得します。

Create L4-L7 Service Gr	aph Template 👋	() ×
Drag device clusters to cre	ate graph nodes.	10
Device Clusters	Graph Name: WebGraph	
0	+ - Graph Type:   Create A New One   Clone An Existing Or	1e
∃ svcType: FW		
🗱 SampleTenant/StrictFTD (Man	Aged) Consumer	
	Please drag a device from devices table and drop it here to create a	a service node.
	StrictFTD Information Firewall:  Routed Transparent	
	Profile: CISCO-FTD_FI-1.0/RoutedModeForF	e B
	SUBMIT	CANCEL

- **ステップ5** サービス グラフの名前を [グラフ名] フィールドに入力します。
- **ステップ6** 左ペインから右ペインに FTD サービス機能をドラッグ アンド ドロップして、その機能をサービス グラフに追加します。
- ステップ1 ノードの名前を変更します。
- **ステップ8** 展開に基づいて、ファイアウォールモードのタイプを[ルーテッド]または[トランスペアレント]から選択します。
- **ステップ9** サービスノードのプロファイルを選択します。デバイスパッケージに付属しているか、以前作成したデフォルトテンプレートで機能プロファイルを選択します。
- ステップ10 [送信] をクリックしてグラフをを作成します。 [サービス グラフ] ダイアログ ボックスは作成した新しいグラフを一覧表示します。

# サーサービス グラフ テンプレートの適用ビス グラフ テ ンプレートの適用

APIC は、サービス グラフに指定されているサービス機能要件に従ってサービスを自動的に設定します。APIC はまた、サービス グラフで指定されるサービス機能のニーズに応じてネット ワークを自動的に設定しますが、これによってサービスデバイスでの変更は要求されません。

APICでは、デバイスパッケージ内のアプライアンススクリプトにパラメータを渡します。ア プライアンススクリプトは、パラメータデータをアプライアンスにダウンロードされる設定 に変換します。これは、アプリケーションプロファイル、EPGが特定のテナントに存在して いると仮定し、作成したサービスグラフを関連付けます。

次の手順により、コントラクトとサービス グラフを関連付けます。

#### 始める前に

テナントを設定します。

EPG でアプリケーション プロファイルを設定します。

- ステップ1 APIC にサインインします。
- ステップ2 メニュー バーで、[テナント] をクリックします。
- ステップ3 [ナビゲーション]ペインで、テナントのフォルダツリーを展開します。
- **ステップ4** [L4-L7 サービス ]> [L4-L7 サービス グラフ テンプレート] ブランチを展開して、サービス グラフ テンプ レートを表示します。
- ステップ5 選択したサービスグラフテンプレートを右クリックし、表示されるポップアップメニューで[L4-L7サー ビス グラフ テンプレートの適用] をクリックします。
- ステップ6 [手順1コントラクト] ダイアログボックでス、コンシューマとプロバイダ EPG を選択します。

L4-L7 Service Graph Template - WebGraph
Apply L4-L7 Service Graph Template To EPGs
STEP 1 > Contract 1. Contract 2. Graph
Config A Contract Between EPGs
Provider EPG / External Network: SampleTenant/sap/epg-WebEPG 👻 🗗 🕤
Contract Information Contract:  Contract:  Contract:  Contract Name: WebCtrl
No Filter (Allow All Traffic):  PREVIOUS NEXT CANCEL

- **ステップ7**新しいコントラクトを作成するか、既存のコントラクト件名を選択します。新しいコントラクトの名前 を入力します。[Next] をクリックします。
- **ステップ8** [手順2グラフ] ダイアログ ボックスで、ブリッジ ドメイン (BD) とクラスタ インターフェイスを選択 します。[Next] をクリックします。

TER 2 > Craph	1 Contract 2 Graph 3 StrictETD Par	amete
EP 2 > Graph		GITTOLO
onfig A Service Graph		
evice Clusters	Graph Template: SampleTenant/WebGraph 🚽 🗗	
D +	Consumer Provide	r
	EPG EPG	
SampleTenant /StrictFTD (Managed Firewall)		)
	ADDEPG StrictFTD WebEPG	
	FTD	
	StrictFTD Information	
	Firewall: routed	
	Profile: RoutedModeForFTD	
	Consumer Connector	
	Type. I General Route Peering	
	BD: SampleTenant/AppBD -	
	Cluster Interface: external	
	Provider Connector	1
	Type:      General     Conte Peering	
	BD: SampleTenant/WebBD 🗸 🖓	
	The Bridge Domain that connects the two devices	
	Cluster Interface: internal 🗸	
		1
		_

ステップ9 [手順3パラメータ] ダイアログ ボックスで、[すべてのパラメータ] タブをクリックします。

	Stict i D Faranieters	L. C. upri	
ntig para ofile Name:	meters for the selected device		
outedMode	ForFTD <div 'd<="" id="vns:applyGraphTemplate2A:appl&lt;/th&gt;&lt;th&gt;yGraphNew:3:applyProfile_editIcon" style="" th=""><th>isplay: inline-block; width: 30</th></div>	isplay: inline-block; width: 30	
Features:	Required Parameters All Parameters		
Interferen	Folder/Param	Name Value	Write Domain
Intenaces	😑 🔺 🚭 Device Config	Device	
All	Access Policy	ACIAccPolicyRouted	
	Bridge Group Interface		
	🛨 🔲 🕨 📮 Inline Set		
	E 🕨 📮 Interface	externalInterface	
	E F D Interface	internalInterface	
	Security Zone	ExternalSZRT	
	Security Zone	InternaISZRT	
	😑 🔺 🚭 Function Config	Function	
	Access Policy Configuration	AccessPolicyFolder	
	Bridge Group Interface Config	uration	
	External Interface Configuration	on ExtConfig	
	Internal Interface Configuration	n IntConfig	

ステップ10 展開に基づいてパラメータを設定します。組み込みテンプレートに基づいて機能プロファイルを定義し、この手順で使用することができます。機能のサポートとFTD展開の次のセクションを参照してください。[終了]をクリックしてグラフにコントラクトをアタッチします。

#### 次のタスク

サービスグラフのインスタンスを作成したら、APICがFTDインターフェイスにプロビジョニ ングされた設定をFMCに正常にプッシュしていることを確認します。

また、エンドポイントがプロビジョニング済みのFTDを使用して相互に通信できることを確認します。

## **Supported Functions**

このセクションでは、ACI デバイス パッケージの FTD でサポートされている公開されている 機能について説明します。



アクセスポ	*Name	<name></name>		Name of the access policy.
リシー				<ul> <li>APICでは、ポリシーの 説明を GraphDeploymentSuffix およびその他の情報を 内部的に追加します。</li> <li>既存のFMCアクセス ポリシー名は、APICを 使用するのと一致する 必要があります。</li> </ul>
	*Access Rules	*Name	<name></name>	アクセスルールの名前。
				<ul> <li>APICでは、ルールのコ メントに、 GraphDeploymentSuffix およびその他の情報を 内部的に追加します。</li> <li>既存のFMCアクセス ルール名は、作成した サービスグラフセキュ リティゾーンを更新す る APIC の一致する必 要があります。</li> </ul>
		Source Interface	インターフェ	)]:
			イスオブ	
			シェクトのセ  キュリティ	
			ゾーンへの参 照	
		Destination Interface	インターフェ イス オブ ジェクトのセ キュリティ ゾーンへの参 照	)]:
		双方向	true   false	

		設定 true の場合、セキュリ ティの両方を適用するゾー ンでアクセスルール送信元 と宛先ゾーン。そうしない と、セキュリティゾーン は、個別に適用されている 送信元と宛先フィールドで す。
		/ 0

Security Zone       "Name <name>         Name of the security zone.       た、APIC他のオブジェクが参照できるようにする。         ルマンコンジンクトを。       APIC フォルダ名はオブシックトを。         APIC では、名前に、       GraphDeploymentSuffix P         的に追加します。たとえば、外部のセキュリティ       ジーンの名前を選択する         と、FMC にわかります       External <fnant< td="">         name=""&gt;&lt;<device< td="">         name=""&gt;       <device< td="">         Name of the security zone.       た、APIC他のオブジェク         が参照できるようにする。       APIC では、名前に、         GraphDeploymentSuffix P       的に追加します。たとえば、外部のセキュリティンジーンの名前を選択する         と、FMC にわかります       External <fnant< td="">         name=""&gt;&lt;<device< td="">         name=""&gt;&lt;<device< td="">         name=""&gt;(注)       Name フィール         くう名前のセキュリテ       ジーン         (注)       Name フィール         マンう名前のセキュリテ       ジーン         (注)       Name フィール          Shite f         されます FMC       ジャンクを使用す         めには、8 文字       フィールドの値</device<></device<></fnant<></device<></device<></fnant<></name>
が参照できるようにする め、セキュリティゾーン APIC フォルダ名はオブシ クトを。 APIC では、名前に、 GraphDeploymentSuffix が 的に追加します。たとえ ば、外部のセキュリティ ゾーンの名前を選択する と、FMC にわかります External_ <tenant name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device という名前のセキュリテ ゾーン (注) Name フィール <field value="">_ ゾーン (注) Name フィール <field value="">_ Name=""&gt;_ <device cata、合計で4 され、合計で4 され、合計で4 されます FMC CraphDeploymer 40 文字を使用す めには、8 文字 フィールドの値</device </field></field></device </device </device </tenant 
<ul> <li>め、セキュリティゾーン APIC フォルダ名はオブシ クトを。</li> <li>APIC では、名前に、 GraphDeploymentSuffix 炉 的に追加します。たとえ ば、外部のセキュリティ ゾーンの名前を選択する と、FMC にわかります External_<tenant name=""&gt;name=""&gt;という名前のセキュリテ ゾーン</tenant </li> <li>(注) Name フィール <field value=""> name=""&gt; 、The comparison of the comparison of th</field></li></ul>
APIC フォルダ名はオブミ クトを。 APIC では、名前に、 GraphDeploymentSuffix f 的に追加します。たとえ ば、外部のセキュリティ ゾーンの名前を選択する と、FMC にわかります External <tenant name=""&gt;<device name=""&gt;<device name=""&gt;<device name=""&gt;<device name=""&gt;<device name=""&gt;<device name=""&gt;<device この名前のセキュリテ ゾーン (注) Name フィール <field value=""> name=""&gt;、 (注) Name フィール <field value=""> name=""&gt;、 のDevice&gt;GraphDeploymer 40 文字を使用 めには、8 文字 フィールドの描</field></field></device </device </device </device </device </device </device </tenant 
APIC では、名前に、 GraphDeploymentSuffix が 的に追加します。たとえ ば、外部のセキュリティ ゾーンの名前を選択する と、FMC にわかります External_ <tenant name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device *Field value=""&gt; 'ゾーン' (注) Name フィール <field value="">_ name=""&gt;_<device *Field value=""&gt; name=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ chita ( *Field value=""&gt;_ name=""&gt;_ chita ( *Field value=""&gt;_ chita ( *Field value="") name=""&gt;_ chita ( *Field value="") name=""&gt;_ chita ( *Field value="") name=""&gt;_ chita ( *Field value="") name=""&gt;_ chita ( *Field value="") name=""&gt;_ chita ( *Field value="") name="") chita ( *Field value="") name="") chita ( *Field value="") name="") chita ( *Field value="") name="") chita ( *Field value="") name="") chita ( *Field value=") name="") chita ( *Field value=") name="") chita ( *Field value=") name="") chita ( *Field value=") name="") chita ( *Field value=") name="") chita ( *Field value=") name="") chita ( *Field value=") name=") chita ( *Field value=") name=") chita ( *Field value=") name=") chita ( *Field value=") chita ( *Field value=") name=") chita ( *Field value=") name=") chita ( *Field value=") name=") chita ( *Field value=") chita ( *Fie</device </field></device </device </device </device </device </device </device </tenant 
という名前のセキュリラ ゾーン (注) Nameフィール <field value="">_ name=""&gt;_<dev され、合計で4 されます FMC GraphDeploymer 40 文字を使用で めには、8 文字 フィールドの値</dev </field>
(注) Name フィール <field value=""> name=""&gt;_<dev され、合計で4 されます FMC GraphDeploymer 40 文字を使用で めには、8 文字 フィールドの値</dev </field>
ます。
*Type インライン ルーティング スイッチ セキュリティゾーンのタング プ。 一致しないセキュリティ
ソーンのタイプおよびイ ターフェイスのタイプは 可されません。これは、 開モードに基づくもので す。

インライン セット	*Name	<name></name>	Name of the inline set. また、 APIC フォルダ セットの名 前、インラインオブジェクト が参照できるようにしま す。 APIC では、名前に、 GraphDeploymentSuffix 内部 的に追加します。たとえ ば、外部のインラインセット名を選択する場合、FMC にわかりますインライン セットが External_ <tenant name=""&gt;_<device name=""&gt;_<device name=""&gt;_<device name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant color of the start という名前 (注) Name フィールドとして保存 <field value="">_<tenant name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant color of the start という名前 (注) Name フィールドとして保存 <field value="">_<tenant name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant name=""&gt;_<tenant color of the start color of the</tenant </tenant </tenant </tenant </tenant </tenant </tenant </field></tenant </tenant </tenant </tenant </field></tenant </tenant </tenant </tenant </device </device </device </tenant 
	*MTU	<integer></integer>	インラインセットの MTU プロパティ。
	*Snort Fail Open Busy	true   false	インラインセットのオープ ンビジーの失敗のプロパ ティを snort します。
	*Snort Fail Open Down	true   false	インラインセットのプロパ ティが失敗するオープンダ ウンを snort します。

インターフェ イス	*Name	<name></name>			インターフェイスオブジェ クトの APIC フォルダの名 前。	
	*Enabled	true   false			インターフェイスのプロパ ティを有効にします。	
	*MTU	<integer></integer>			MTU property of the interface.	
	*Logical Name	<name></name>			インターフェイスの論理名 (省略可能な限りインライン)。	
					APIC では、名前に、 GraphDeploymentSuffix 内部 的に追加します。たとえ ば、論理名の外部を選択す る場合、FMCにわかります 論理名の External_ <tenant name=""&gt;_<device name=""&gt;_ </device </tenant 	
					<ul> <li>(注) Name フィールドと</li> <li><field value="">_&lt;1</field></li> <li>name=""&gt;_<device li="" r<=""> <li>され、合計で48文</li> <li>されます FMC で</li> <li></li></device></li> <li>GraphDeploymentSuf</li> <li>40文字を使用でき</li> <li>めには、8文字を名</li> <li>フィールドの値を指</li> <li>ます。</li> </ul>	して保ィ Yenant hame="" 字に制序 〈Field〉。 fix には、 ます、た ()] 」限して。
	*Inline Set	Inline Set Object			APICインライン設定フォル ダオブジェクトへのリンク を参照します。	
	*Security Zone	セキュリティゾーンオブジェクト			セキュリティ ゾーンの APIC フォルダ オブジェク トへのリンクを参照しま す。	
	*IPv4	*static *address サブネットマ スクを使用し た IPv4 アド レス				

					ルーテッドインターフェイ スにのみ適用されます。値 は、サブネットマスクと IPv4アドレスです。たとえ ば、1.1.1.1/24というように なります。
□ブリッジグ ループ イン ターフェイス	*Name	<name></name>			ブリッジグループインター フェイスの APIC フォルダ の名前。
					APIC では、説明を GraphDeploymentSuffix およ びその他の情報を内部的に 追加します。
	* IPv4 アドレ スの設定	*static	*address	IPv4 address with subnet mask	透過インターフェイスにの み適用されます。値は、サ ブネットマスクと IPv4アド レスです。For example, 1.1.1.1/24
	*Bridge Group ID	<integer></integer>			)]:
	*Interfaces	)]:			APIC インターフェイス フォルダオブジェクトへの リンクを参照します。

IPv4 Static Route	*Network	<network></network>	このルートの外部ネット ワーク。A.B.C.D/prefix 形式 にする必要があります。For example, 192.168.1.0/24		
	*Gateway	<gateway></gateway>	外部ネットワークに到達す るために使用されるゲート ウェイの IPv4 アドレス。 For example, 192.168.1.1		
	メトリック	<integer></integer>	Distance metric for this route. 有効な範囲は1~255(両端 の値を含む)です。		
	isTunneled	true   false	)]:		
	<ul> <li>・ルーテッドモードのFTDのIPv4スタティックルートを設定する場合は、 設定、物理インターフェイスレベルでします。ただし、物理インターフェ イスがBVIインターフェイス (IRB 機能)に配置されます、BVIインター フェイスレベルでのIPv4スタティックルートを設定します。</li> <li>・透過モードのFTDのIPv4スタティックルートを設定する場合は、設定、 BVI設定に関係なく、物理インターフェイスレベルでします。</li> </ul>				

# FTD 展開

このセクションでは、さまざまな展開モードに必要な機能プロファイル設定の変更について説明します。3個すべてのモードで、適切なアクセスコントロールポリシーまたはルールの参照が必要です。

- •アクセスポリシー名が正確に設定されていることを確認します。
- アクセスポリシーの下のアクセスルールが、送信元と宛先のセキュリティゾーンのマッピングが正しいインターフェイスを指している状態で、正確に設定されていることを確認します。インターフェイスのセキュリティゾーンからアクセスルールソースおよび宛先ゾーンの両方に、双方向フラグが設定されていることを確認します。

#### トランスペアレント モード

デフォルトの機能プロファイル CISCO-FTD FI-1.0/TransparentModeForFTD を選択します。

 ・ブリッジドメインID([デバイス設定]>[□ブリッジグループインターフェイス]>[ブリッ ジグループID]>[値])が固有の番号であることを確認します。□ブリッジグループイン ターフェイスのIPアドレスを設定し、インターフェイスが正しく設定されていることを 確認します。

- ・セキュリティゾーン名(「デバイス設定]>[セキュリティゾーン]>[名前])が正しく設され、そのタイプがスイッチ済みに設定されていることを確認します。
- インターフェイスの論理名が固有であることを確認します([デバイス設定]>[インターフェイス(内部または外部))]>[論理名]>[値])。有効フラグが[true]に設定され、セキュリティゾーンが正しくマッピングされていることを確認します。

#### ルーテッド モード

デフォルトの機能プロファイル CISCO-FTD\_FI-1.0/RoutedModeForFTD を選択します。

- ・セキュリティゾーン名([デバイス設定]>[セキュリティゾーン]>[名前])が正しく設され、そのタイプがルーテッド済みに設定されていることを確認します。
- インターフェイスの論理名が固有であることを確認します([デバイス設定]>[インターフェイス(内部または外部))]>[論理名]>[値])。有効フラグが[true]に設定され、セキュリティゾーンが正しくマッピングされていることを確認します。インターフェイスIPアドレスを設定します。

#### インライン モード

デフォルトの機能プロファイル CISCO-FTD FI-1.0/InlineModeForFTD を選択し確認します。

- •インライン セット名([デバイス設定] > [インライン セット] > [名前])が正しく設定され ています。
- ・セキュリティゾーン名(「デバイス設定]>[セキュリティゾーン]>[名前])が正しく設され、そのタイプがルーテッド済みに設定されていることを確認します。
- インターフェイスの論理名が固有であることを確認します([デバイス設定]>[インターフェイス(内部または外部))]>[論理名]>[値])。有効フラグが[true]に設定されており、インラインセットとセキュリティゾーンが正しくマッピングされていることを確認します。



# **Troubleshoot**

・障害の修復 (35ページ)

# 障害の修復

このセクションでは、一般的な障害を含む基本的なトラブルシューティングの一部と、修復方 法について説明します。

### パラメータ設定

APIC のネットワーク サービス グラフ上で FTD サービス ノードの設定パラメータを誤ると、 次の障害のいずれかを返すことがあります。

#### 障害の形式

グラフ設定の結果「メジャー スクリプト エラー:設定エラー: <error>\* for <parameter-name> in context <context-name> on cluster <cluster-name> in tenant <tenant-name>

#### Fault メッセージ

グラフ設定の結果:テナント Sample Tenant のクラスタ Strict FTDv Cluster 上のコンテキスト Sample Tenant ctx1 で有効な「メジャースクリプトエラー;設定エラー:指定されたインター フェイス タプおよびセキュリティゾーン タイプが一致する必要があります」となります。

#### 修復

正しいタイプで新しいセキュリティゾーンを作成し、古いゾーンを削除します。作成した後、 FMCはセキュリティゾーンを変更できません。FMCの予想に基づき、サービスグラフの一致 しない設定パラメータを修正します。

#### Fault メッセージ

グラフの設定の結果:「メジャースクリプトエラー:設定エラー:名前 DefaultInlineSet の項目はすでに存在しています。別の名前を選択するか、または現在の項目を削除してください」

#### 修復

DefaultInlineSet の名前を持つインライン設定が FMC で設定されていないことを確認します。 すでに存在しているインライン設定はデバイスパッケージでは使用できません。デバイスパッ ケージは、ワークフローの影響を与えずに削除できるように新規インライン設定を作成する必 要があります。

#### Fault メッセージ

グラフの設定の結果:「メジャー スクリプトのエラー:設定エラー:インターフェイス名は 48 文字以上にすることはできません」

#### 修復

2個以上の区切り文字(「\_」)が含まれるテナント、デバイス、インターフェイス論理または インライン設定が48文字以上にならないことを確認します。

#### Fault メッセージ

グラフの設定の結果:「メジャースクリプトエラー:設定エラー:名前は48文字より短くす る必要があります」

#### 修復

2個以上の区切り文字(「\_」)が含まれるテナント、デバイス、インターフェイス セキュリ ティ ゾーン名が 48文字以上にならないことを確認します。

### アプライアンス設定

APICの誤った設定のアプライアンスログインと IP 情報はにより、次の障害のいずれかが発生 する可能性があります。

#### Fault メッセージ

グラフ設定の結果、\*重要なスクリプトエラーが発生しました:設定エラー:アプライアンス にログインできません。設定されているログイン情報が間違っています。\*というエラーが発 生します。

#### 修復

設定されている FMC ユーザー名とパスワードが正しいか確認してください。

#### Fault メッセージ

グラフ設定の結果、\*重要なスクリプトエラーが発生しました:設定エラー:要求されたデバイスがありません\*という障害が発生します。

#### 修復

設定されているデバイスが設定されている FMC に登録されていることを確認します。

#### Fault メッセージ

グラフの設定の結果、\*接続されたパーティが一定時間経過しても適切に応答しなかったか、 接続されているホストが応答に失敗したため接続の確立に失敗しました。\*というエラーが発 生します。

#### 修復

設定されている FMC IP アドレスが正しく、到達可能であることを確認します。

#### Fault メッセージ

グラフの設定の結果、\*重要なスクリプトのエラー:設定エラー:要求されたインターフェイス が見つかりません。\*というエラーが発生します。

#### 修復

デバイスクラスタが FMC に存在しており、デバイスに設定されている具体的なインターフェイスを確認します。

#### Fault メッセージ

グラフ設定の結果、\*重要なスクリプトエラーが発生しました:設定エラー:設定の変更をデバ イスに展開できません。考えられる理由は、別の展開が進行中か、APICとFMCの時間が同期 してない可能性があります。必ず同じNTPサービスに時間を同期し、タイムゾーンをセット アップしてから、サービスグラフを再度接続するようにしてください。\*というエラーが発生 します。

#### 修復

同じNTPサービスにACIとFMCが設定されており、その他の展開は同一のデバイスので進行 していないことを確認します。

#### Fault メッセージ

グラフの設定の結果、\* 重要なスクリプトのエラー: 設定エラー: デバイス設定がありません。 \* というエラーが発生します。

#### 修復

デバイス クラスタのデバイスが正しく設定されていることを確認します。また、デバイスマ ネージャが1つのみ FMC ホストの情報を使用して設定されていることを確認します。

#### Fault メッセージ

グラフの設定の結果、\*重要なスクリプトのエラー:設定エラー:デバイスのIPまたはポートの 設定がありません。\*というエラーが発生します。

#### 修復

登録済みのデバイス クラスタまたはアプライアンス IP アドレスとポートが正しく設定されて いることを確認します。

#### Fault メッセージ

グラフの設定の結果、\*重要なスクリプトエラー:設定エラー:デバイスのユーザ名またはパス ワードの設定がありません。\*

#### 修復

登録済みのデバイスクラスタのユーザ名とパスワードが正しく設定されていることを確認します。

#### Fault メッセージ

グラフの設定の結果、\*重要なスクリプトエラー:設定エラー:デバイスのユーザ名またはパス ワードの設定がありません。\*

#### 修復

登録済みのデバイスクラスタのユーザ名とパスワードが正しく設定されていることを確認しま す。

#### Fault メッセージ

グラフの設定の結果、\* 重要なスクリプト エラーが発生しました: 設定エラー: FMC フィール ドは48文字に制限し、<Field value="">\_<Tenant name="">\_<L4-L7 device="" name="">」.</L4-L7> </Tenant> </Field> として FMC に保存されます。2 つの区切り文字(「\_」)と組み合わせてある 現在のテナントとデバイス名が40文字以上であり、8文字の関数プロファイルフィールドで終 了しています。テナントまたはデバイス名の長さをこの制限に適合させて減らしてください。 \* というエラーが発生します。

#### 修復

テナントとデバイスの名前を組み合わせた結果が38文字以下ではないことを確認します。