

Cisco Application Policy Infrastructure Controller 3.0 with VMware Integration – Network Admin v1

最終更新日:2017 年 9 月 22 日

このデモンストレーションについて

この事前設定済みデモンストレーションの内容は次のとおりです。

- [要件](#)
- [このシスコソリューションについて](#)
- [トポロジ](#)
- [はじめに](#)
- [シナリオ 1: APIC システムの概要および操作](#)
- [シナリオ 2: アプリケーションの導入](#)
- [シナリオ 3: Python スクリプトを使用した L4-L7 サービス グラフの作成](#)
- [シナリオ 4: NX-OS スタイルの CLI の使用](#)

『VMware Administration Demo Guide (VMware 管理デモ ガイド)』を確認するには、デモンストレーションを実行しているデータセンターの下記のリンクをクリックしてください。

- [米国東部 \(RTP\)](#)
- [米国西部 \(SJC\)](#)
- [EMEAR \(LON\)](#)
- [APJ \(SNG\)](#)
- [GC \(CHI\)](#)

制限

このデモンストレーションでは、物理的なファブリックではなく、ファブリックをシミュレーションしたものを使用しているため、Cisco APIC 3.0 の特定の機能は扱いません。

- すべての設定は、APIC シミュレータのレポート後に失われます。
- シミュレーションされたファブリックに接続されているデバイス間で送受信されるトラフィックはありません。
- 画面の更新には想定よりも若干時間がかかる場合があります。

カスタマイゼーション

デモンストレーションで検出されたファブリックを使用する代わりに、ファブリックの検出機能をデモンストレーションするには、まず APIC シミュレータをリセット ([付録 A](#) を参照) し、次に、[付録 B](#) を参照してファブリックを検出します。

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. デモンストレーションの要件

必須	オプション
<ul style="list-style-type: none"> ラップトップ 	<ul style="list-style-type: none"> Cisco AnyConnect

このシスコ ソリューションについて

Cisco Application Policy Infrastructure Controller (Cisco APIC™) では、**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 (Cisco ACI™)** ファブリックの自動化と管理を一元的に行うことができます。Cisco APIC は、すべてのファブリック情報へのアクセスを一元化し、アプリケーション ライフサイクルを最適化して拡張性とパフォーマンスを向上させ、物理リソースと仮想リソースに対して柔軟なアプリケーション プロビジョニングをサポートします。

詳細については、www.cisco.com/go/apic [英語] を参照してください。

VMware Admin

Cisco ACI vCenter Plugin は、仮想化管理者がネットワーキング チームに依存せずに共有インフラストラクチャのネットワーク接続を定義できるようにするユーザ インターフェイスです。仮想化管理者は、このプラグインを使用して、vSphere Web クライアント内から ACI ファブリックを管理できます。これにより、VMware vSphere Web クライアントで一括管理が可能になり、VMware vCenter と ACI ファブリックの両方を設定できます。

Cisco ACI vCenter Plugin は「詳細な」ネットワーキングの設定には対応していません。仮想化管理者に関連する要素のみが公開されます。

VMware Admin スクリプトは、vCenter ACI Plugin を介して実行される管理タスクを示します。

Network Admin

APIC GUI は、APIC へのブラウザベースのグラフィカル インターフェイスで、REST API メッセージを交換することによって APIC エンジンと内部的に通信します。

Network Admin スクリプトは、ブラウザ インターフェイスで実行されるタスク、および Python スクリプトと NX-OS インターフェイスを介した設定を示します。

トポロジ

デモンストレーションには、ソリューションのスクリプト シナリオと機能を説明するために、あらかじめユーザとコンポーネントが設定されています。デモンストレーション用コンポーネントへのアクセスに必要なすべての情報は、アクティブなデモンストレーションの [トポロジ (Topology)] メニューおよび [サーバ (Servers)] メニューにあります。



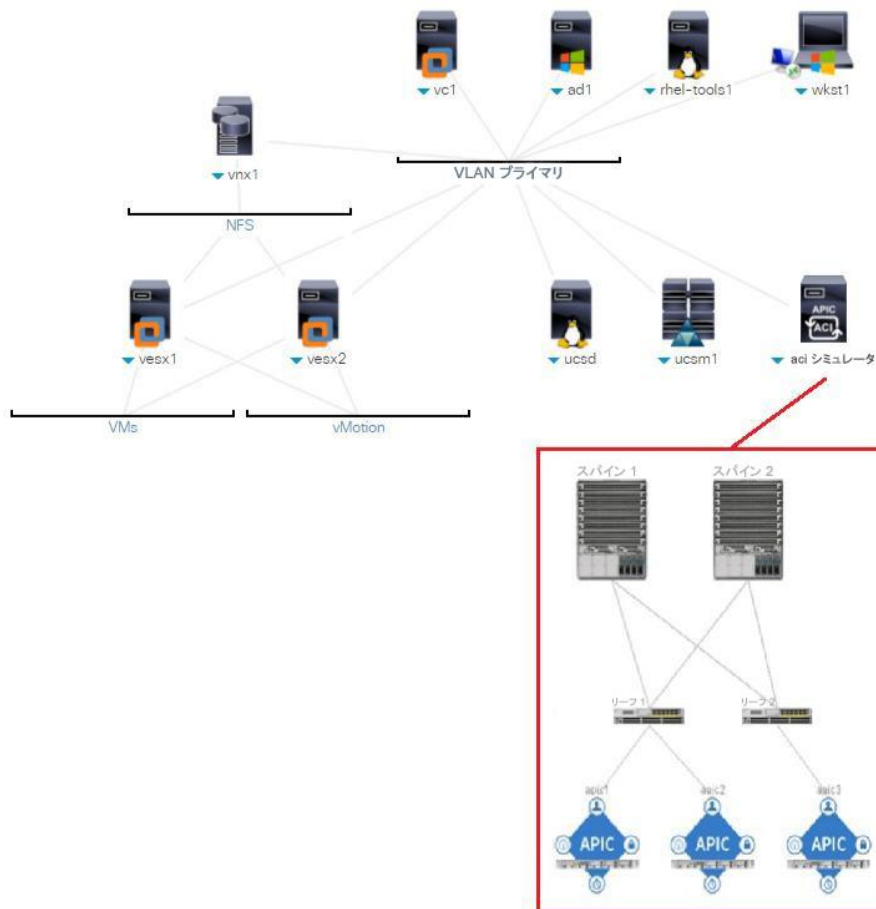
- [トポロジ (Topology)] メニュー: トポロジにあるサーバをクリックすると、使用可能なサーバ オプションがポップアップ ウィンドウに表示されます。
- [サーバ (Servers)] メニュー: サーバ名の横にある  または  をクリックすると、利用可能なサーバ オプションとクレデンシャルが表示されます。

図 1 に、次の仮想マシンで構成された、デモンストレーションの仮想トポロジを示します。

- Active Directory 2012 R2
- VMware Virtual Center Server 6.5 アプライアンス
- APIC シミュレータ バージョン 3.0(1k) : スパイン 1 およびスパイン 2、リーフ 1 およびリーフ 2、APIC1、APIC2、および APIC3 で構成されています。
- VMware ESXi 6.5.0
- EMC VNXe ストレージ アプライアンス
- Cisco Unified Computing System Platform Emulator 3.1 (2e)
- Cisco UCS Director 6.5.0.0
- Linux ツール リポジトリ (RHEL 7)
- Windows 10 ワークステーション

図 1. デモンストレーションのトポロジ



はじめに

デモンストレーションの前に

実際の対象者の前でプレゼンテーションを行う前に、このプロセスを少なくとも 1 回は実施しておくことを強く推奨します。そうすることで、ドキュメントとデモンストレーションの構成に慣れることができます。


環境を元の設定にリセットするには、または APIC シミュレータをリセット ([付録 A](#) を参照) してから [付録 B](#) を参照してファブリックを検出するには、このガイドに従って新しいセッションをスケジュールする必要が生じる場合があります。

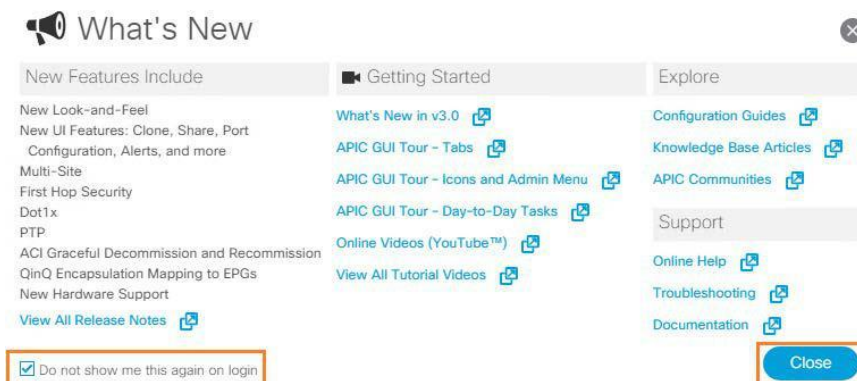
プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dcloud.cisco.com にアクセスして、最寄りのロケーションを選択し、Cisco.com アカウントでログインします。
2. セッションを予約します。[\[手順を見る\]](#)
3. ルータを dCloud で初めて使用する場合は、ルータを登録し、設定します。[\[手順を見る\]](#)
4. 接続をテストします。[\[手順を見る\]](#)
5. [マイダッシュボード(My Dashboard)] > [マイセッション(My Sessions)] でセッションのステータスが [アクティブ(Active)] であることを確認します。

注: セッションがアクティブになるまでに 20 分ほどかかることがあります。

6. [表示 (View)] をクリックしてアクティブなセッションを開きます。
7. 次のいずれかの方法でデモンストレーション環境に接続します。
 - **Cisco AnyConnect VPN** [\[手順を見る\]](#) および **ラップトップ上のローカル RDP クライアント** [\[手順を見る\]](#) (ワークステーション 1: 198.18.133.36、ユーザ名: DCLLOUD\demouser、パスワード: C1sco12345)
 - **Cisco dCloud Remote Desktop** クライアント [\[手順を見る\]](#)
8. ファブリックの検出はデモの設定時に自動的に開始されます。[APIC ログイン (APIC Login)] アイコン  をダブルクリックし、ログインします (**admin/C1sco12345**)。[新着情報 (What's New)] ポップアップを確認し、[今後ログオン時にこのメッセージを表示しない (Do not show me this again at logon)] を選択し、[閉じる (Close)] をクリックします。



9. 上部のメニューの [ファブリック(Fabric)] を選択します。
10. 上部のサブメニュー バーの [インベントリ(Inventory)] をクリックします。
11. 左側のメニューで、[ファブリック メンバーシップ (Fabric Membership)] をクリックし、4 つのデバイスが表示されていることを確認します(IP アドレスは異なる場合があります)。TEP-1-101 しか表示されない場合は、[付録 B](#) を参照してファブリックを検出します。

The screenshot shows the Cisco APIC interface with the 'Fabric Membership' page selected. The left sidebar shows the 'Inventory' menu with 'Fabric Membership' highlighted. The main content area displays a table with the following data:

Serial Number	Pod ID	Node ID	Node Name	Rack Name	Model	Role	IP	Supported Model	SSL Certificate	Status
TEP-1-101	1	101	Leaf1		NSK-C9396PX	leaf	10.0.64.64/32	True	yes	Active
TEP-1-102	1	102	Leaf2		NSK-C9396PX	leaf	10.0.64.67/32	True	yes	Active
TEP-1-103	1	103	Spine1		NSK-C9508	spine	10.0.64.66/32	True	yes	Active
TEP-1-104	1	104	Spine2		NSK-C9508	spine	10.0.64.65/32	True	yes	Active

注: ファブリックの検出には 15 分ほどかかることがあります。15 分経過する前にログインすると、すべてのデバイスが検出されないことがあります。次のエラー メッセージが表示される場合があります。

The screenshot shows the Cisco APIC 'System Health' page. A critical error message is displayed in a red box:

Critical
The cluster contains less than 3 in-service controllers. Please backup the cluster and do not make use of the fabric in this state for production.

The 'System Health' section shows a score of 'No stats data to display...'. The 'Fault Counts By' section shows the following data:

	2	1	1	0
SYSTEM WIDE	2	1	1	0
Access	0	0	0	0
External	0	0	0	0
Framework	0	0	0	0

シナリオ 1. APIC システムの概要および操作


このシナリオでは、APIC システム ヘルス ダッシュボードの概要と、根本的な問題を特定するためにヘルス スコアまでドリル ダウンする方法について説明します。

手順

システム ヘルス ダッシュボード

1. デモンストレーション ワークステーションから、**Application Policy Infrastructure Controller** を開きます(まだ開いていない場合)。



それには、[APIC ログイン (APIC Login)] アイコン  をクリックし、ログインします (**admin/C1sco12345**)。

2. メニュー バーの [システム (System)] をクリックして、[システム ヘルス ダッシュボード (System Health Dashboard)] を表示します。

- グローバル管理権限を持った状態でログインしているため、ビューにはすべてのシステム コンポーネントが含まれていることを説明します。
- 一括管理ビューを表示します。このビューは、一元化されたアプリケーションレベルの可視性、および物理環境と仮想環境全体にわたるリアルタイムのアプリケーション ヘルス モニタリングを備えています。
- ヘルス スコアを表示して、APIC でモニタリングされる以下を含むコンポーネントのヘルス スコアがどのように表示されるかを説明します。
 - ファブリック ヘルス
 - 仮想環境と物理環境への接続
- システム全体および特定のコンポーネントのヘルス スコアが左ペインに表示されることを示します。
- 右ペインには、エラーのあるエリア別に障害数が表示されることを示します。

システム ヘルス ダッシュボード:
グラフィカル表示による ACI ファブリックの経時的な状態

障害カウンタ: レベルおよびメイン別の障害数

障害カウンタ: レベルおよびタイプ別の障害数

オブジェクトヘルス: コンポーネント別のシステムヘルスに関する概要情報。詳細情報にドリルダウンすることも可能

Name	POD ID	Type	Health Score
Leaf1	1	leaf	99
Leaf2	1	leaf	99
Spine1	1	spine	99
Spine2	1	spine	99

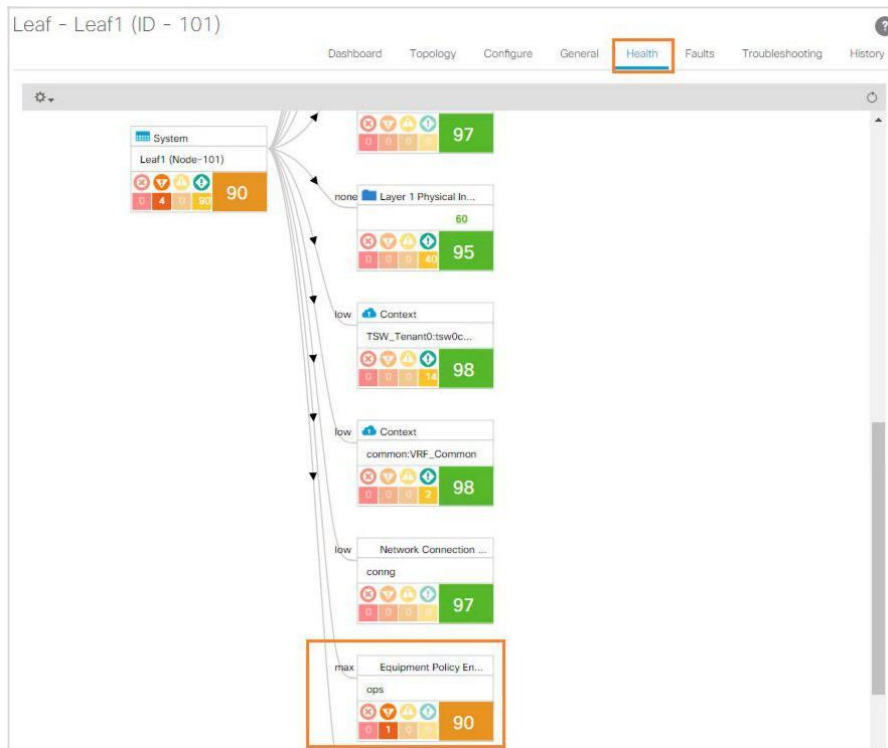
Name	Health Score
TSW_Tenant0	98

Domain	Count	Count	Count	Count
SYSTEM WIDE	3	29	7	512
Access	0	14	0	9
External	0	4	0	0
Framework	0	0	0	0
Infra	3			
Management	0			
Security	0			
Tenant	0	0	5	0

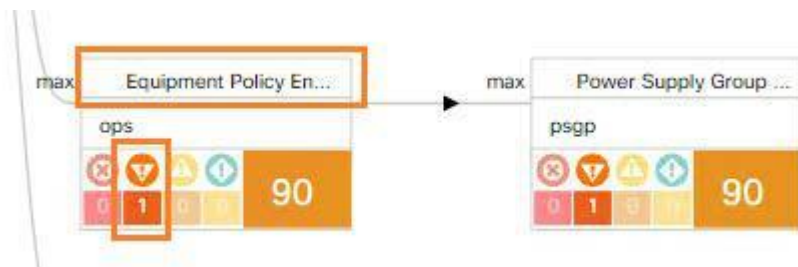
Type	Count	Count	Count
Communicati...	0	14	0
Config	0		
Environmental	0		
Operational	3		

ID	Name	IP	Admin State	Operational State	Health State
1	apic1	10.0.0.1	In Service	Available	Fully Fit
2	apic2	10.0.0.2	In Service	Available	Fully Fit
3	apic3	10.0.0.3	In Service	Available	Fully Fit

- ヘルス スコアが 90 の [リーフ 1(Leaf1)] をダブルクリックします。
- [リーフ 1(Leaf1)] ウィンドウで、[ヘルス(Health)] タブをクリックし、ヘルス スコアが 90 以下の [機器ポリシー エンティティ (Equipment Policy Entity)] 要素が表示されるまで下にスクロールします。



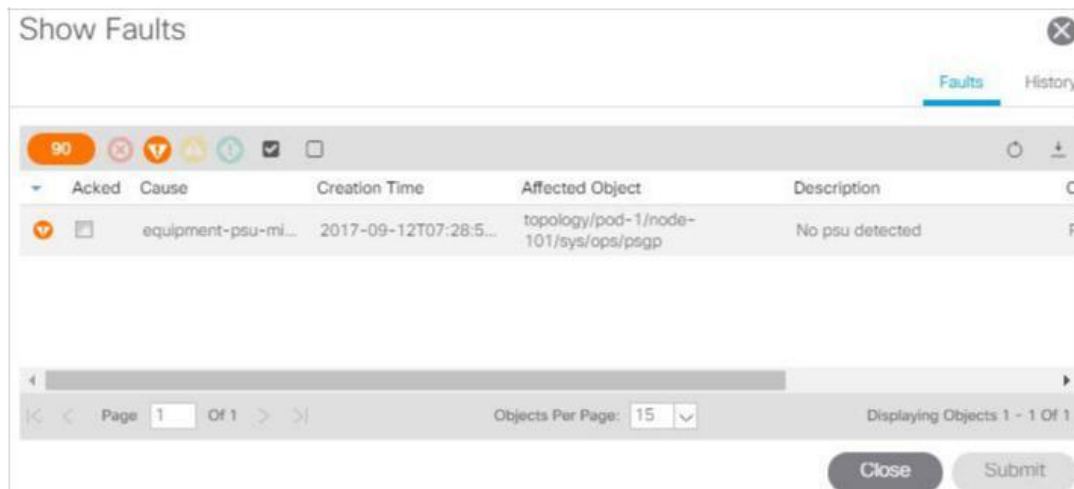
- 障害をクリックして [機器ポリシー (Equipment Policy)] を展開し、障害が示されている電源装置を表示します。



- [電源装置グループ (Power Supply Group)] を右クリックし、表示されたメニューで [障害を表示 (Show Faults)] をクリックします。



- 表示された表で障害の詳細を確認します。



- [障害を表示 (Show Faults)] ウィンドウを閉じます。

可視性およびトラブルシューティング

- [操作 (Operations)] をクリックし、[トラブルシューティング ウィザード ビュー (Troubleshooting Wizard View)] を表示します。



- [セッション名 (Session Name)] フィールドに **tsw_session1** と入力します。
- [セッション タイプ (Session Type)] は [エンドポイント間 (Endpoint to Endpoint)] のままにします。
- [説明 (Description)] フィールドに、**Troubleshooting Session 1** と入力します。
- [送信元 (Source)] フィールドに送信元 IP アドレスとして **10.193.101.14** と入力し、[検索 (Search)] をクリックします。結果をクリックします。
- [宛先 (Destination)] フィールドに宛先 IP アドレスとして **10.193.102.17** と入力し、[検索 (Search)] をクリックします。結果をクリックします。

7. [時間帯(Time Window)] セクションで、ドロップダウンを使用してセッションの時間(分)を選択するか、[時間帯(Time Window)] ドロップダウンで [固定時刻を使用(Use fixed time)] チェックボックスをオンにし、[開始時刻:(From:)] と [終了時刻:(To:)] の時刻を選択して [開始(Start)] ボタンをクリックします。


APIC はライブでトラブルシューティングを開始し、送信元と宛先を基に論理トポロジを構築します。




トラブルシューティング セッション

以前に入力した送信元と宛先の情報に基づいた論理トポロジが表示されます。

1. トポロジ固有の障害を表示するには、そのトポロジの黄色のアイコンをクリックします。



2. すべての障害を表示するには、作業ウィンドウの左上にある [リスト(List)] アイコン  をクリックします。

Severity	Affected Object	Code	Cause	Creation Time	Last Transition	Lifecycle	Description
	uni/trn-TSW_Tenant0/BD-tswOctx0BD1	F112425	threshold-cr...	Tue Sep 12 2017...	Tue Sep 12 2017...	Raised	TCA: ingress drop packets rate(i2IngrPktsAg... value 110 raised above threshold
	uni/trn-TSW_Tenant0/BD-tswOctx0BD1	F110473	threshold-cr...	Tue Sep 12 2017...	Tue Sep 12 2017...	Raised	TCA: ingress drop bytes rate(i2IngrBytesA... value 110069 raised above
	topology/pod-1/node-102/sys/ctx-[vlan-2162688]/bd-[vlan-16482194]/vlan-[vlan-2000]	F112128	threshold-cr...	Tue Sep 12 2017...	Tue Sep 12 2017...	Raised	TCA: ingress drop packets rate(i2IngrPkts5m... value 13 raised above threshold 10


3. [障害(Faults)] ウィンドウを閉じます。

ドロップ/統計情報

このセクションでは、論理トポロジ上のパケット ドロップを確認します。

1. サイドメニューの [ドロップ/統計情報(Drop/Stats)] をクリックします。
2. 論理トポロジを確認します。これは、前の [トポロジ(Topology)] ウィンドウの表示と同様です。



3. 下矢印  が表示されている黄色のアイコンをクリックし、そのデバイスまたはノードの統計情報を表示します。

Statistics - Leaf1

Drop Stats | Contract Drops | Traffic Stats

Show stats with zero values

Time	Affected Object	Stats	Value
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/ctx-[vxlan-2162688]/bd-[vxlan-16580486]/vlan-[vlan-2002]	ingress drop packets periodic	6358
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/ctx-[vxlan-2162688]/bd-[vxlan-16482194]/vlan-[vlan-2000]	ingress drop packets periodic	6507
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Ingress Error Drop Packets pe...	6012
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Ingress Load Balancer Drop P...	5256
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Ingress Buffer Drop Packets p...	5599
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Ingress Forwarding Drop Pac...	5954
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Egress Error Drop Packets pe...	5445
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Egress Buffer Drop Packets p...	6403
2017/09/12 08:50:00 - 2017/09/12 08:...	topology/pod-1/node-101/sys/phys-[eth1/50]	Egress AFD WRED Packets p...	5702

Page 1 Of 12 | Objects Per Page: 25 | Displaying Objects 1 - 25 Of 280

コントラクト

コントラクトは EPG(エンドポイントグループ)間に適用されます。下の図に双方向コントラクトを示します。

The screenshot shows the 'Contracts' section in the Cisco dCloud interface. Two panels are visible:

- S Source Endpoint → Destination Endpoint:**

Filter ID	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	557677...
Filter ID: implicit					BD Allow (TSW_Tenant0/tswoctst06D1)		
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	576763...
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	644444...
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	576763...
- D Destination Endpoint → Source Endpoint:**


Filter ID	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	568936...
Filter ID: implicit					BD Allow (TSW_Tenant0/tswoctst06D0)		
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	575498...
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	640862...
Filter ID: tswoctst2_Filter (new)	ip:tcp	http	http		permit	node-101	575498...

1. サイドメニューで [コントラクト(Contracts)] をクリックします。
2. [送信元エンドポイント → 宛先エンドポイント (Source Endpoint -> Destination Endpoint)] ボックスにコントラクトが表示されます。ノード ID によるフィルタとヒット数も示されます。
3. [宛先エンドポイント → 送信元エンドポイント (Destination Endpoint -> Source Endpoint)] ボックスには同じ情報が逆の方向で表示されます。

トレースルート

このセクションでは、方向とプロトコルを基に、ファブリック認識型トレースルートをマルチパスで実行します。

注: このデモンストレーション環境外の Cisco ACI ファブリックでは、送信元から宛先まで、つまりリーフ 1 から宛先ホストまでが緑色のトレースルートとして表示されます (その逆も同様です)。APIC シミュレータはスパインからのトレースルートのみを表示します。


1. サイドメニューで [トレースルート(Traceroute)] をクリックします。
2. [プロトコル (Protocol)] ドロップダウンから [icmp] を選択し、[再生 (Play)] ボタン  をクリックしてトレースルートを開始し、ポップアップで [OK] をクリックします。

The screenshot shows the 'Traceroute' section in the Cisco dCloud interface. The 'Traceroute' panel is active, showing a network topology with Spine and Leaf nodes. The 'Protocol' dropdown is set to 'icmp'. The 'Source Endpoint' and 'Destination Endpoint' are visible. The network path is highlighted with green bars, indicating successful hops.

3. 問題がないため、送信元から宛先までの緑色のパスが表示されます。

アトミック カウンタ

アトミック カウンタは送信元と宛先間のパケット数とバイト数をカウントします。ファブリックを通過したパケットのみがカウントされます。ローカルにスイッチされるパケットはカウントされません。

1. サイドメニューの [アトミック カウンタ(Atomic Counter)] をクリックします。
2. [再生 (Play)]  をクリックしてカウンタを開始します。下の図は [進行中のカウンタ(Ongoing Counters)] を示しています。[OK] をクリックします。
3. カウンタ テーブルが生成されるまで約 2 分待ちます。

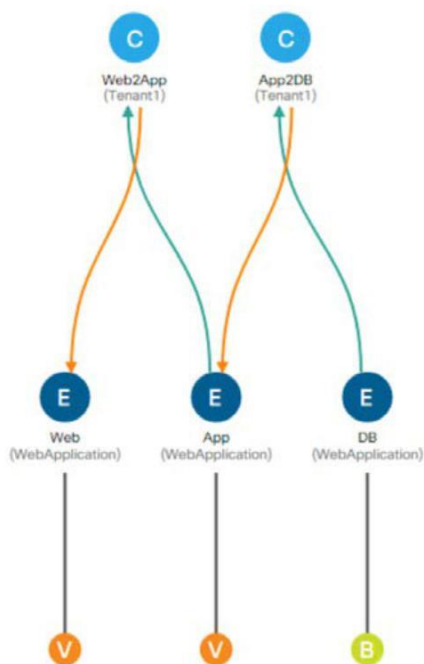
Source Endpoint ↔ Destination Endpoint							
Source Endpoint → Destination Endpoint							
Current				Cumulative			
Tx	Rx	Drop	Excess	Tx	Rx	Drop	Excess
240	240	0	0	240	240	0	0
Destination Endpoint → Source Endpoint							
Current				Cumulative			
Tx	Rx	Drop	Excess	Tx	Rx	Drop	Excess
240	240	0	0	240	240	0	0

4. データを確認し、[停止 (Stop)]  をクリックします。

シナリオ 2. アプリケーションの導入

このシナリオでは、テナントとブリッジドメインを作成してからアプリケーションを導入します。アプリケーションには 3 つの階層、すなわち Web、アプリケーション、DB があります。このシナリオでは、各層の EPG と、各層が相互に通信できるようにするコントラクトを作成します。最後の手順では、アプリケーションにネットワーキング機能を提供するために以前作成した EPG に、物理ドメインと VMM ドメインを追加してから vPC を作成します。

注: ユーザ インターフェイスの基本モードは、Cisco APIC Release 3.0(1) よりも後のリリースでは廃止されています。



手順

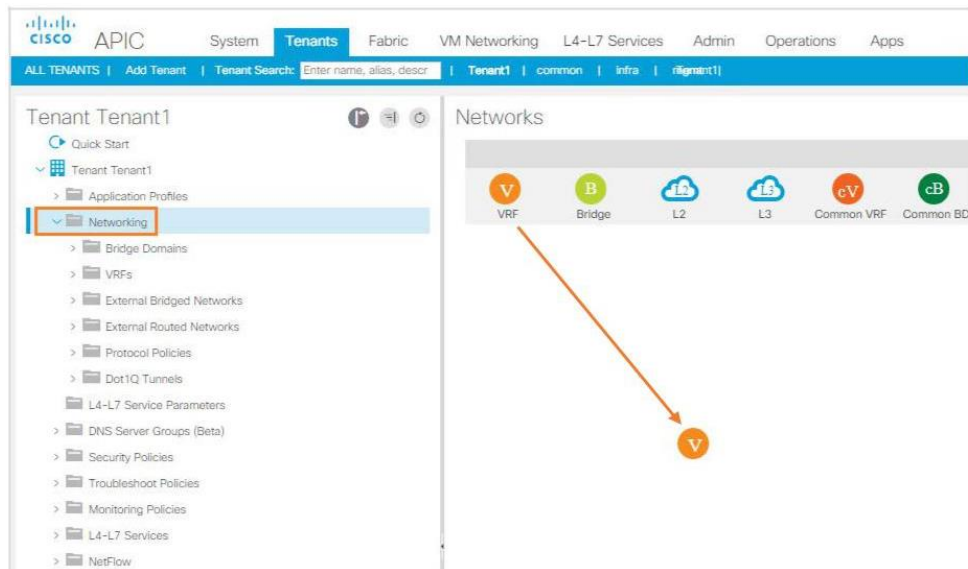
テナントおよびブリッジドメインの作成

このセクションでは、テナント、VRF、およびブリッジドメインを作成します。

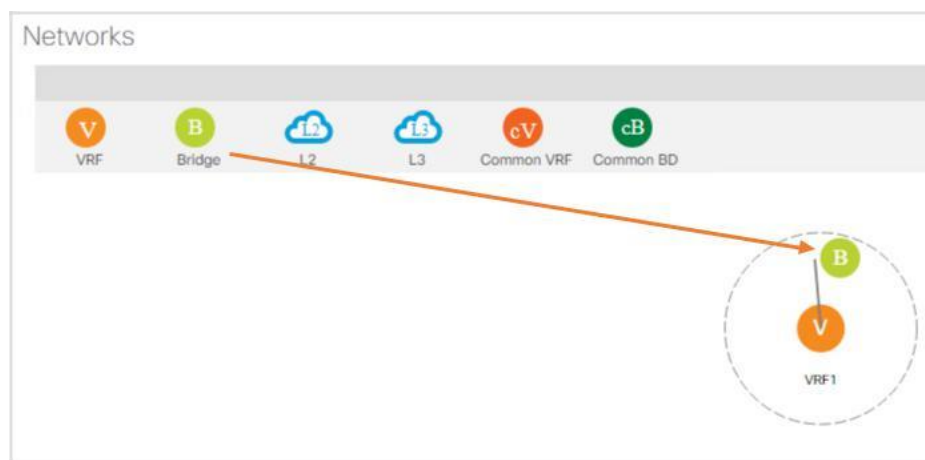
1. APIC ウィンドウのトップ メニューで、[テナント(Tenants)] > [テナントの追加(Add Tenant)] をクリックします。



2. [テナントの作成(Create Tenant)] ダイアログボックスで、[名前(Name)] フィールドに **Tenant1** と入力し、[送信(Submit)] をクリックします。
3. 表示された [Tenant1] ウィンドウで、サイド メニューの [ネットワーキング(Networking)] をクリックします。
4. [ネットワーク(Networks)] 作業ウィンドウで、[VRF] アイコンを [ネットワーク(Networks)] ウィンドウにドラッグします。



5. [VRF の作成(Create VRF)] ウィンドウで、[名前(Name)] フィールドに **VRF1** と入力し、[送信(Submit)] をクリックします。
6. [ブリッジ(Bridge)] アイコンを [ネットワーク(Networks)] ウィンドウにドラッグし、アイコンが VRF の周囲に表示される灰色の円に接続されていること、および 2 つのアイコン間に線が表示されていることを確認します。



7. 表示された [ブリッジドメインの作成(Create Bridge Domain)] ウィンドウで、次の手順を実行します。
 - a. [名前(Name)] フィールドに **BD1** と入力します。
 - b. [転送(Forwarding)] ドロップダウンから [最適化(Optimize)] を選択します。
 - c. [L3 設定(L3 Configurations)] タブをクリックします。

Create Bridge Domain
Specify Bridge Domain for the VRF

Main **L3 Configurations** Advanced/Troubleshooting

Name:

Alias:

Description: optional

Type: fc **regular**

Forwarding:

End Point Retention Policy:

IGMP Snoop Policy:

d. [+] 記号をクリックしてサブネットを追加します。

Create Bridge Domain
Specify Bridge Domain for the VRF

Main **L3 Configurations** Advanced/Troubleshooting

Unicast Routing: Enabled

ARP Flooding: Enabled

Config BD MAC Address:

MAC Address:

Subnets:

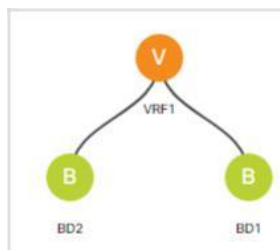
Gateway Address	Scope	Primary IP Address	Subnet Control
+			

e. [ゲートウェイ IP (Gateway IP)] フィールドに **10.1.1.1/24** と入力し、[OK] をクリックします。

f. [OK] を再度クリックします。

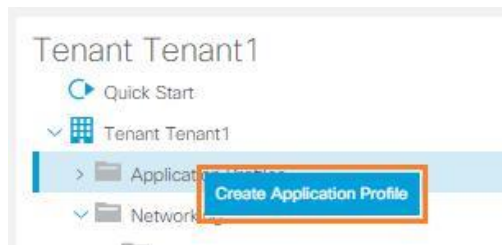
8. [ブリッジ (Bridge)] アイコンをメイン ウィンドウにドラッグし、VRF1 に接続される 2 つ目のブリッジドメインを作成します。

9. [名前 (Name)] フィールドに BD2 と入力し、[OK] をクリックします。



アプリケーション プロファイルの作成

1. [テナント Tenant1 (Tenant Tenant1)] フォルダ リストで、[アプリケーション プロファイル (Application Profiles)] を右クリックし、[アプリケーション プロファイルの作成 (Create Application Profile)] を選択します。



2. [アプリケーション プロファイルの作成(Create Application Profile)] ダイアログボックスで、次の手順を実行します。
 - a. [名前(Name)] フィールドに **WebApplication** と入力します。
 - b. [送信(Submit)] をクリックしてアプリケーション プロファイルを作成します。


注:[アプリケーション プロファイル(Application Profile)] ウィンドウには、[EPG の作成(Create EPGs)]、[コントラクトの作成(Create Contracts)]、[VMMドメインの作成(Create VMM Domains)]、[物理ドメインの作成(Create Physical Domain)] の4つのセクションがあります。これらのすべての要素を作成するまでは、ウィンドウの下部にある [送信(Submit)] をクリックしないでください。

EPG の作成

このセクションでは、アプリケーションの階層ごとに1つ、合計で3つの EPG(AppEPG、WebEPG、DBEPG)を作成します。

1. サイド ウィンドウで [テナント Tenant1(Tenant Tenant1)] > [アプリケーション プロファイル(Application Profiles)] を展開し、[WebApplication] をクリックして [アプリケーション プロファイル(Application Profile)] ウィンドウを表示します。




2. [EPG] アイコン  を [アプリケーション プロファイル(Application Profile)] ウィンドウにドラッグします。
3. [アプリケーション EPG の作成(Create Application EPG)] ダイアログボックスで、次の手順を実行します。
 - g. [名前(Name)] フィールドに **Web** と入力します。
 - h. [ブリッジドメイン(Bridge Domain)] ドロップダウンから [Tenant1/BD1] を選択します。
 - i. [OK] をクリックして、EPG を作成します。
4. 手順 2 と 3 を繰り返して、さらに 2 つの EPG (**APP** および **DB**) を作成します。DB EPG の場合は、[ブリッジドメイン(Bridge Domain)] で [Tenant1/BD2] を選択します。

コントラクトの作成

このセクションでは、2つのコントラクトを作成します。

- 最初のコントラクトである App2DB は、App 階層が DB 階層から情報を受信できるようにします。このコントラクトでは、App 階層がコンシューマ、DB 階層がプロバイダーです。
- 2つ目のコントラクトである Web2App コントラクトは、Web 階層が App 階層から情報を受信できるようにします。このコントラクトでは、Web 階層がコンシューマ、App 階層がプロバイダーです。



1. マウスを放さずに、[コントラクト(Contract)] アイコン  を [アプリケーション プロファイル(Application Profile)] ウィンドウにドラッグし、まず [DB EPG] 上に重ね合わせてから、[App EPG] に重ね合わせます。

注:[コントラクト(Contract)] アイコンが表示されない場合は、[APIC] ウィンドウを拡大してください。



2. コントラクト アイコンのドラッグ アンド ドロップが正常に行われた場合は、[コントラクトの作成 (Create Contract)] ダイアログボックスでコンシューマ EPG とプロバイダー EPG が事前を選択されています。選択されていない場合は、次の手順を実行します。
 - a. [コンシューマ EPG/外部ネットワーク (Consumer EPG / External Network)] ドロップダウンから [Tenant1/WebApplication/epg-App] を選択します。
 - b. [プロバイダー EPG/内部ネットワーク (Provider EPG / Internal Network)] ドロップダウンから [Tenant1/WebApplication/epg-DB] を選択します。
 - c. [コントラクト名 (Contract Name)] フィールドに **App2DB** と入力します。
 - d. [フィルタなし(すべてのトラフィックを許可) (No Filter (Allow All Traffic))] チェックボックスをオフにします。
 - e. [+] 記号をクリックしてフィルタ エントリを追加します。次のように更新してから [更新 (Update)] をクリックします。
 - [名前 (Name)]: **sql**
 - [エイリアス (Alias)]: **sql**
 - [EtherType]: **IP**
 - [IP プロトコル (IP Protocol)]: **tcp**
 - [宛て先ポート/範囲 (Destination Port / Range)] – [開始 (From)], [終了 (To)]: **481**

Config Contract With L4-L7 Service Graph

STEP 1 > Contract

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: Provider EPG / Internal Network:

Contract Information

Contract: Create A New Contract Choose An Existing Contract

Contract Name:

No Filter (Allow All Traffic):

Filter Entries:

Name	Alias	EtherType	ARP Flag	IP Protocol	Match Only	Stateful Fragments	Source Port / Range	Destination Port / Range	TCP Session Rules		
							From	To	From	To	
sql	sql	IP	Unspecif	tcp	<input type="checkbox"/>	<input type="checkbox"/>	481	481	481	481	Established

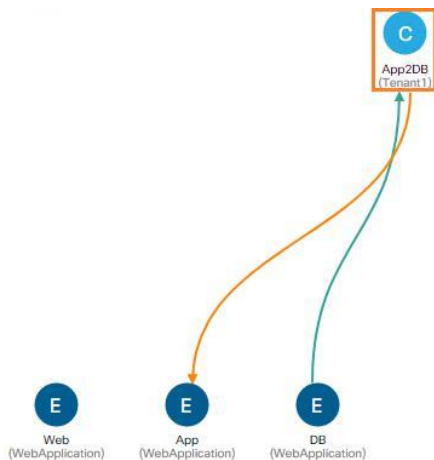
Update Cancel

Export Contract:

Previous Cancel OK

f. [OK] をクリックします。

- [アプリケーション プロファイル (Application Profile)] ウィンドウを確認します。このウィンドウには、App EPG と DB EPG の間に存在するコントラクトが表示されています。



- 2つ目の [コントラクト (Contract)] アイコンを [アプリケーション プロファイル (Application Profile)] ウィンドウにドラッグします。今回は、[App] 上に重ね合わせてから、[Web EPG] に重ね合わせます。
- [コントラクトの作成 (Create Contract)] ダイアログボックスで次の手順を実行します。
 - 事前に選択されていない場合は、[コンシューマ EPG/外部ネットワーク (Consumer EPG / External Network)] ドロップダウンから [Tenant1/WebApplication/epg-Web] を選択します。
 - 事前に選択されていない場合は、[プロバイダー EPG/内部ネットワーク (Provider EPG / Internal Network)] ドロップダウンから [Tenant1/WebApplication/epg-App] を選択します。
 - [コントラクト名 (Contract Name)] フィールドに **Web2App** と入力します。

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: Tenant1/WebApplication/epg-We Provider EPG / External Network: Tenant1/WebApplication/epg-Aps

Contract Information

Contract: Create A New Contract Choose An Existing Contract

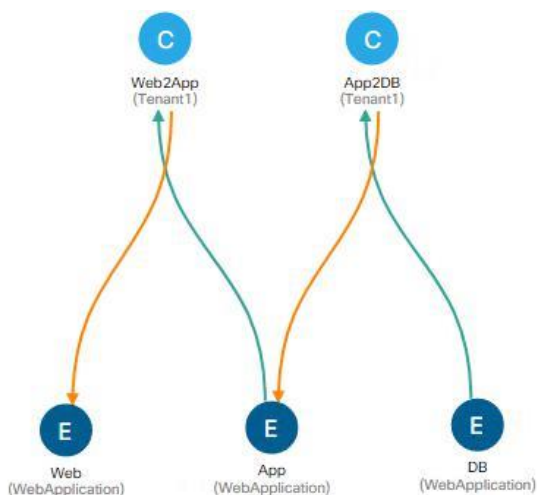
Contract Name: AppCtrct

No Filter (Allow All Traffic):

Export Contract:

d. [OK] をクリックします。

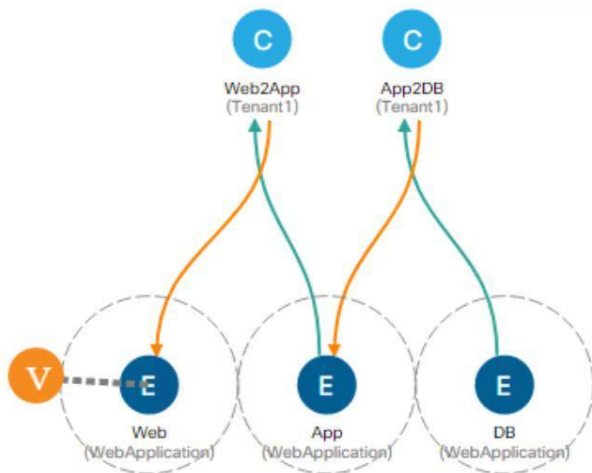
6. [アプリケーション プロファイル (Application Profile)] ウィンドウを確認します。このウィンドウには、3 つの EPG の間に存在する 2 つのコントラクトが表示されています。必要に応じて、アイコン間の関係がはっきり表示されるまで、ウィンドウ内でアイコンを移動させます。



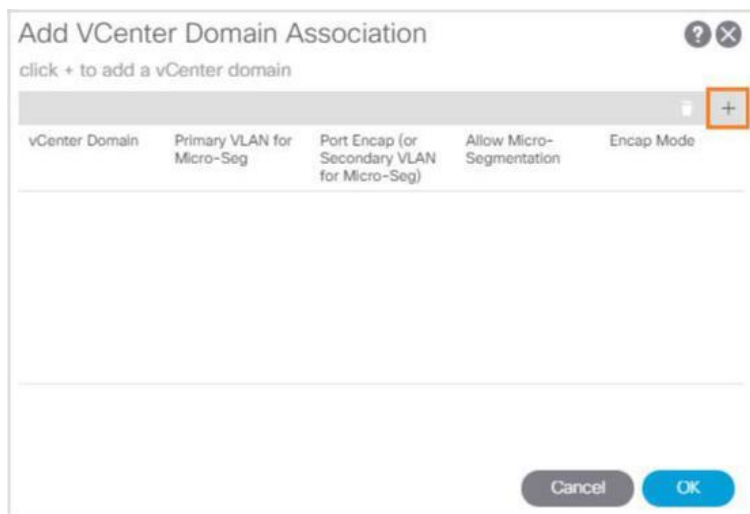
VMM ドメインの追加

このセクションでは、仮想ドメインを App EPG と Web EPG に追加します。

1. [VMware] アイコン  を [アプリケーション プロファイル (Application Profile)] ウィンドウにドラッグし、点線が [Web EPG] アイコンにつながるまで移動します。



- 表示されたダイアログボックスで、[+] 記号をクリックして vCenter ドメインを追加します。



- 表示されたダイアログボックスで、[ドメイン (Domains)] ドロップダウンから [My-vCenter] を選択し、[OK] をクリックします。



- [OK] をクリックします。
- 2 つ目の [VMware] アイコンをメイン ウィンドウにドラッグし、点線が [AppEPG] アイコンにつながるまで移動します。
- 手順 3 と 4 を繰り返して、2 つ目の VMM のパラメータを設定します。

物理ドメインの追加

このセクションでは、物理ドメインを DB EPG に追加します。



- [BareMetal] アイコン **Baremetal** をメイン ウィンドウにドラッグし、点線が [DB EPG] アイコンにつながるまで移動します。
- [+] 記号をクリックして、物理ドメインを EPG に追加します。

3. 表示されたウィンドウで、物理ドメインのパラメータを設定し、[更新 (Update)] をクリックします。

- [VLAN ドメイン (VLAN Domain)]: **phys**
- [パス (Path)]: **Pod-1/Node-101/eth1/20**
- [パス カプセル化 (Path Encap)]: **VLAN 100**

Assign Interfaces To EPG
click + to add interfaces

VLAN VSAN

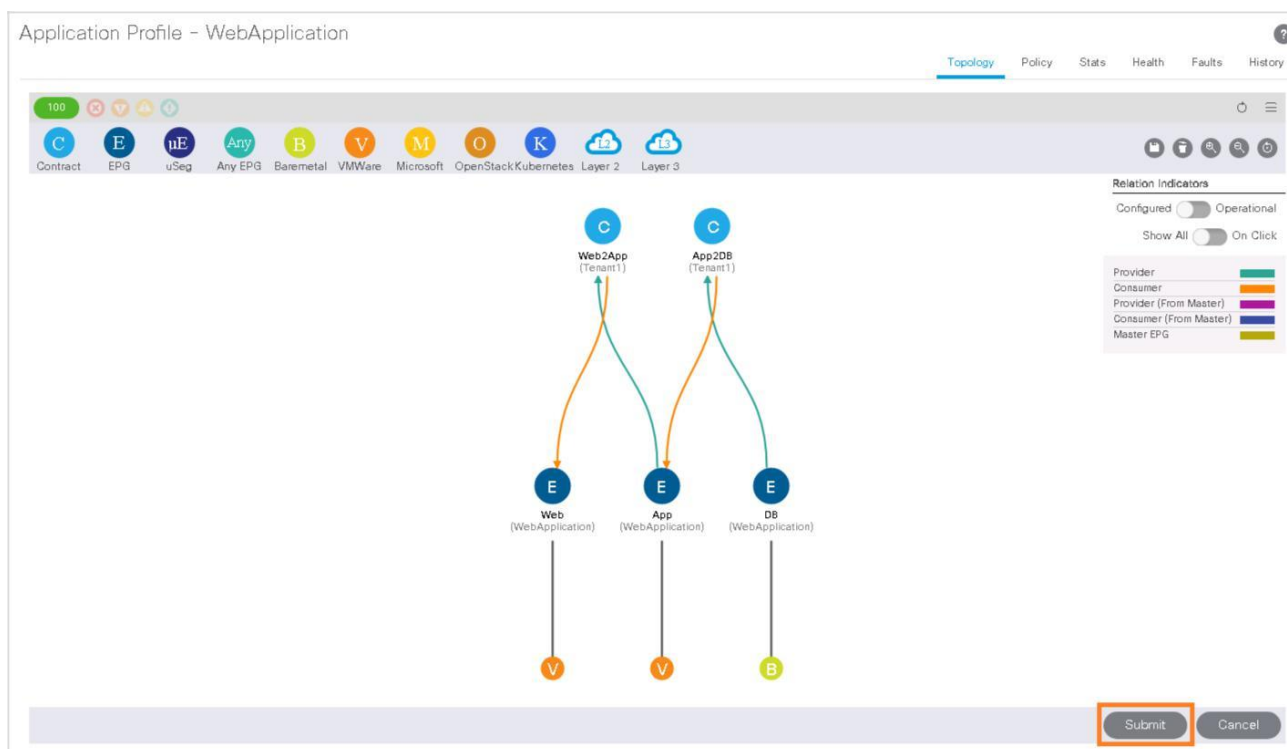
VLAN Domain	Path	Path Encap	Encap Mode
phys	Pod-1/Node-101/eth1/20	vlan-100	Trunk

Update Cancel

Cancel OK

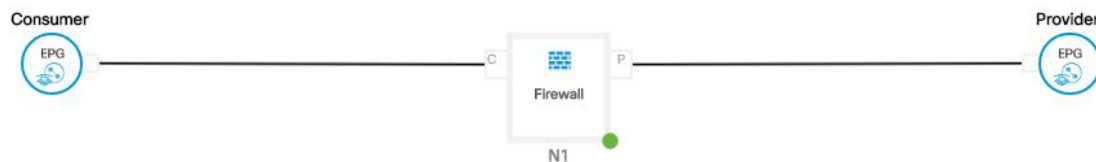
4. [OK] をクリックします。

5. [送信 (Submit)] をクリックしてアプリケーション プロファイルの作成を終了します。



シナリオ 3. Python スクリプトを使用した L4-L7 サービス グラフの作成

このシナリオでは、事前設定済みの Python スクリプトを使用して導入を行います。スクリプトでは、ノースバウンド API を利用して、**単一ノードのグラフを 1 つ持つテナントを APIC 内に 1 つ作成します。**




Python スクリプトは、次の機能を実行します。

- テナントの作成
- デバイス パッケージのインポート
- L4-L7 デバイスの作成
 - 具象デバイスの作成
 - 論理インターフェイスの作成
- サービス グラフの作成
- コントラクトへのサービス グラフの追加

手順

Python スクリプトの実行

1. [Cisco ASDM-IDM ランチャ(Cisco ASDM-IDM Launcher)] アイコン  をダブルクリックして、ASA のホームページを開きます。
2. ログインし(**admin/Cisco12345**)、セキュリティの警告が表示されたら [続行(Continue)] をクリックします。[OK] をクリックして、[ログイン履歴(Login History)] が利用できないことを確認します。



- ASDM ウィンドウを最小化します。



- vSphere アイコン  を使用してデスクトップから **vSphere Web クライアント** を起動し、[Windows セッションの認証を使用する (Use Windows session authentication)]

チェックボックスがオンになっていることを確認します。[ログイン(Login)] をクリックします。


- デモンストレーション ワークステーションから、[Application Policy Infrastructure Controller] ウィンドウを開きます。

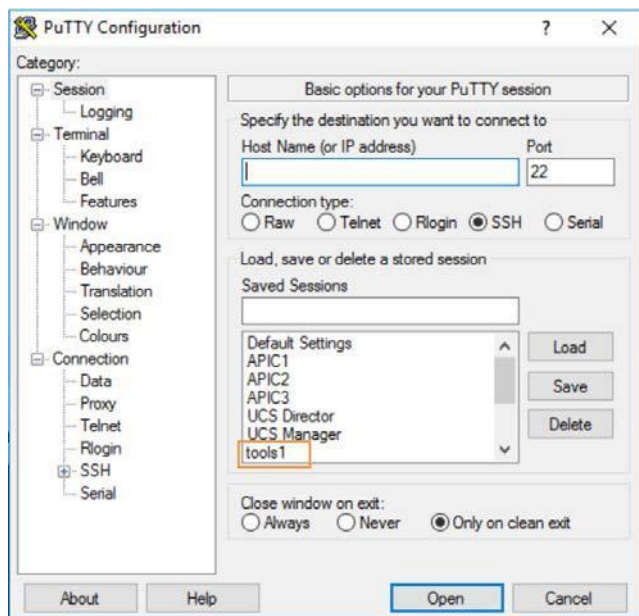


- APIC が開いていない場合は、[APIC ログイン(APIC Login)] アイコン  をクリックして、**Application Policy Infrastructure Controller** を起動します。ポップアップが表示されたら、[いいえ(No)] をクリックします。
- ログインします(使用するクレデンシャル: **admin/C1sco12345**)。

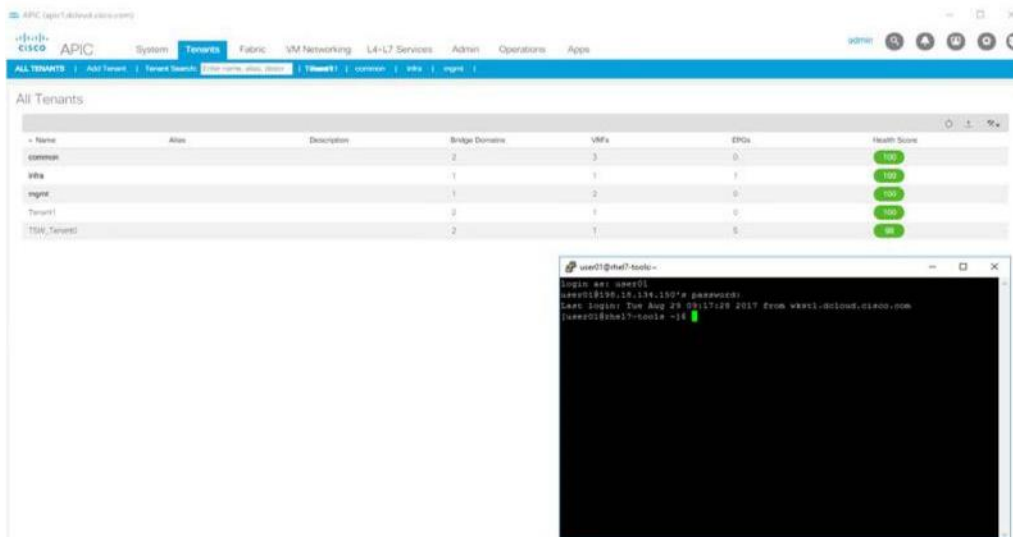
- トップ メニューの [テナント(Tenants)] をクリックします。

- サブメニューで [すべてのテナント(ALL TENANTS)] をクリックします。

- ワークステーションのタスクバーで、[PuTTY] のショートカット  をクリックしてアプリケーションを開き、[tools1] をダブルクリックして保存されたセッションをロードします。



- PuTTY にログインし(**user01/user01**)、PuTTY ウィンドウと APIC ウィンドウの両方が表示されるように配置します。



10. コマンドラインから `./request.py Scripts/Build_All.cfg` と入力し、Enter を押します。

注: Python スクリプトが各 XML スクリプトをコールするときに XML コードを表示するには、上記のコマンドの代わりに `./xml_request.py Scripts/Build_All.cfg` を使用してください。

```

user01@rhel7-tools:~$ ./xml_request.py Scripts/Build_All.cfg
Hit return to process Scripts/Tenant.xml or press 's' and return to skip this script.

+++++++ REQUEST (Scripts/Tenant.xml) ++++++++
<polUni>
  <fvTenant dn="uni/tn-Sales" name="Sales">
    <fvCtx name="Salesctx1"/>
    <!-- bridge domain -->
    <fvBD name="SalesBDWeb">
      <fvRsCtx tnFvCtxName="Salesctx1" />
      <fvSubnet ip="10.10.10.220/24">
      </fvSubnet>
    </fvBD>
    <!-- bridge domain -->
    <fvBD name="SalesBDApp">
      <fvRsCtx tnFvCtxName="Salesctx1" />
      <fvSubnet ip="192.168.10.220/24">
      </fvSubnet>
    </fvBD>
    <!-- bridge domain -->
    <fvBD name="SalesBDDB">
      <fvRsCtx tnFvCtxName="Salesctx1" />
      <fvSubnet ip="20.20.20.220/24">
      </fvSubnet>
    </fvBD>
  </fvTenant>
</polUni>

----- REQUEST (Scripts/Tenant.xml) -----
200

To verify the creation of the tenant, go to Tenants and select Sales. A few bridge domains and a private network was created in this tenant and can be verified under this tenant's Networking section.
Hit return to process Scripts/asa-device-pkg-1.2.9.18.zip or press 's' to skip this script.

```

これは、Build_All.cfg スクリプトの XML 出力の一部の例です。

`Build_All.cfg` スクリプトは、一連の XML スクリプトを使用して、必要な設定手順を実行します。このスクリプトは、各 XML スクリプトの間で一時的に停止するため、ユーザは Enter を押してスクリプトを実行するか、または `s` と入力してスクリプトをスキップし、ウィザードを使用してオブジェクトを設定することができます。スクリプト実行中に、スクリプトの実行内容についての簡単な説明が表示されます。また、APIC ウィンドウはリアルタイムで更新されます。スクリプトが正常に完了すると、成功を示すコード 200 が画面に表示されます。

```

user01@rhel7-tools:~
[user01@rhel7-tools ~]$ ./request.py Scripts/Build_All.cfg
Hit return to process Scripts/Tenant.xml or press 's' and return to skip this script.
200

This script creates a new tenant name Sales, along with the Private Network and Bridge Domain.

To verify the creation of the tenant, go to Tenants and select Sales. A few bridge domains and a private network was created in this tenant and can be verified under this tenant's Networking section.

Hit return to process Scripts/asa-device-pkg-1.2.9.18.zip or press 's' to skip this script.

```


11. テナントを作成します。

- APIC の [すべてのテナント(All Tenants)] ウィンドウで、テナントリストを確認します。シナリオ 1 をすでに実行している場合は、テナントリストが若干異なることがあります。

All Tenants

Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
common			2	3	0	100
infra			1	1	1	100
mgmt			1	2	0	100
Tenant1			2	1	0	100
TSW_Tenant0			2	1	5	98

注: TSW_Tenant0 テナントが存在しない場合は、ファブリックが検出されていません。手順を進める前に、付録 B を参照して **ファブリックの検出** を実行してください。

- PutTY ウィンドウに戻り、「スクリプト/Tenant.xml を処理する場合は Return を押し、このスクリプトをスキップする場合は「s」を入力して Return を押します(Hit return to process Scripts/Tenant.xml or press 's' and return to skip this script)」プロンプトで **Enter** を押します。
- Sales** テナントが作成され、APIC のテナントリストに表示されます。必要に応じて、[更新(Refresh)]  をクリックして、テナントリストに表示させます(「サーバ側のエラー(Server Side Error)」メッセージが生成された場合は、数秒待ってからもう一度更新してください)。

All Tenants

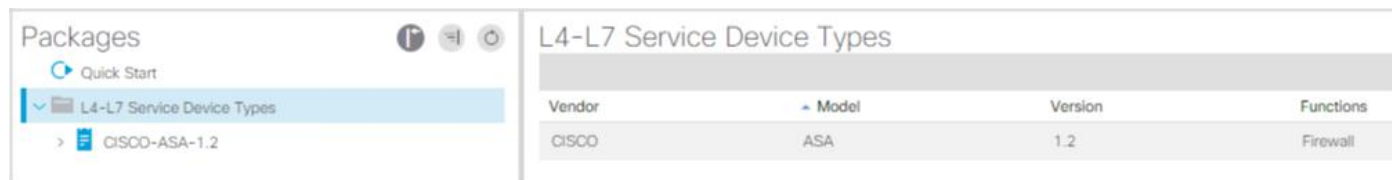
Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
common			2	3	0	100
infra			1	1	1	100
mgmt			1	2	0	100
Sales			3	1	0	100
Tenant1			2	1	0	100
TSW_Tenant0			2	1	5	98

- APIC テナントリストで [Sales] をダブルクリックします。
- [テナント Sales(Tenant Sales)] > [ネットワークング(Networking)] > [ブリッジドメイン(Bridge Domains)] デイレクトリを展開し、**SalesBDDb**、**SalesBDApp**、**SalesBDWeb** の各ブリッジドメインが作成されていることを示します。

[テナント Sales(Tenant Sales)] > [ネットワーキング(Networking)] > [VRFs] フォルダを展開し、プライベート ネットワークの **Salesctx1** が作成されたことを示します。

12. 次の手順に従って、**デバイス パッケージ**をインポートします。

- a. APIC のトップ メニューから、[L4-L7 サービス(L4-L7 Services)] を選択します。
- b. トップのサブメニューで [パッケージ(Packages)] を選択します。
- c. [L4-L7 サービス デバイス タイプ(L4-L7 Services Device Types)] フォルダを展開し、パッケージがないことを示します。
- d. PuTTY ウィンドウに戻り、「スクリプト/asa-device-pkg-1.2.4.8.zip を処理する場合は Return を押し、このスクリプトをスキップする場合は「s」を入力して Return を押します(Hit return to process Scripts/asa-device-pkg-1.2.4.8.zip or press 's' and return to skip this script)」プロンプトで **Enter** を押します。
- e. **CISCO-ASA-1.2** デバイス パッケージが作成されると、**L4-L7 Services Devices** ディレクトリに表示されます。

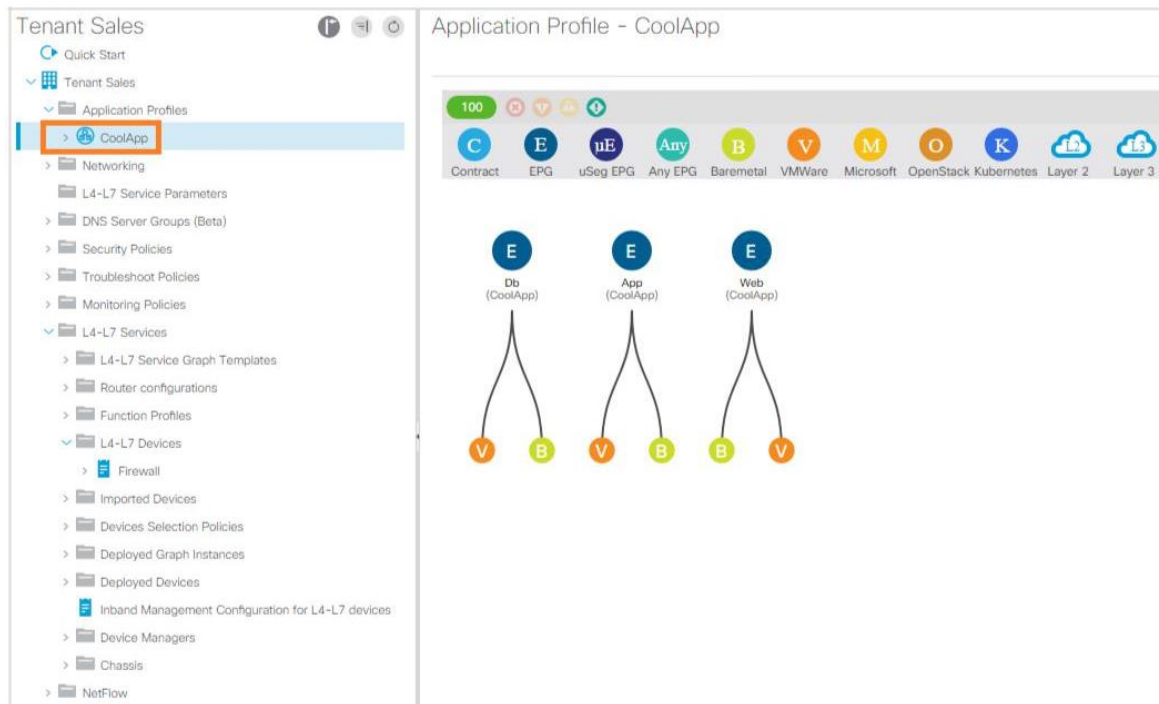


13. 次の手順に従って、**デバイス クラスタ**を作成します。

- a. APIC ウィンドウのトップ メニューから [テナント(Tenants)] を選択します。
- b. トップのサブメニューで [Sales] を選択します。[Sales] がサブメニューに表示されない場合は、テナント リストでダブルクリックします。
- c. [L4-L7 サービス(L4-L7 Services)] > [L4-L7 デバイス(L4-L7 Device)] フォルダを展開し、デバイス クラスタがないことを示します。
- d. PuTTY ウィンドウに戻り、「スクリプト/CreateDevice.xml を処理する場合は Return を押し、このスクリプトをスキップする場合は「s」を入力して Return を押します(Hit return to process Scripts/CreateDevice.xml or press 's' and return to skip this script)」プロンプトで **Enter** を押します。
- e. **ファイアウォール** デバイス クラスタが作成されたことを確認します。

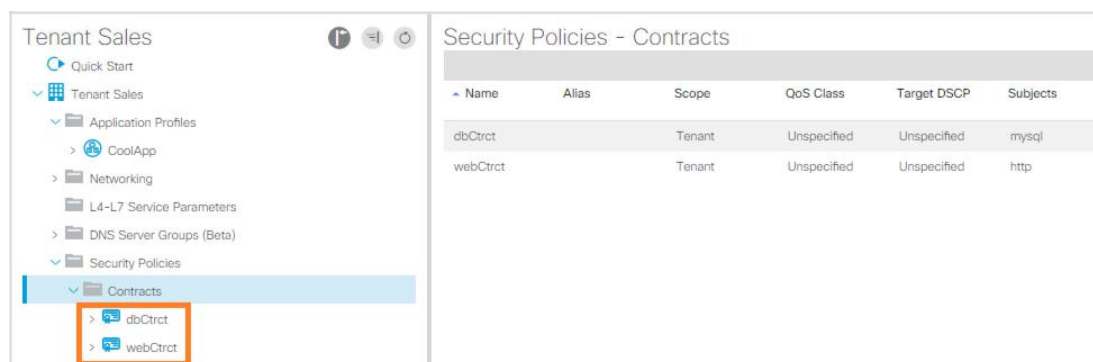
14. 次の手順に従って、**アプリケーション プロファイル**を作成します。

- a. **Tenant Sales** ディレクトリのまま、[アプリケーション プロファイル(Application Profiles)] を展開します。このフォルダは空です。
- b. PuTTY ウィンドウに戻り、「スクリプト/CreateAppProfile.xml を処理する場合は Return を押し、このスクリプトをスキップする場合は「s」を入力して Return を押します(Hit return to Process Scripts/CreateAppProfile.xml or press 's' and return to skip this script)」プロンプトで **Enter** を押します。
- c. **CoolApp** のアプリケーション プロファイルが作成されると、このディレクトリにドロップされます。[CoolApp] > [アプリケーション EPG(Application EPGs)] を展開し、EPG ([EPG App]、[EPG Db]、[EPG Web])を表示します。[CoolApp] をクリックし、トポロジを確認します。



15. 次の手順に従って、**dbCtrct** コントラクトと **webCtrct** コントラクトを作成します。

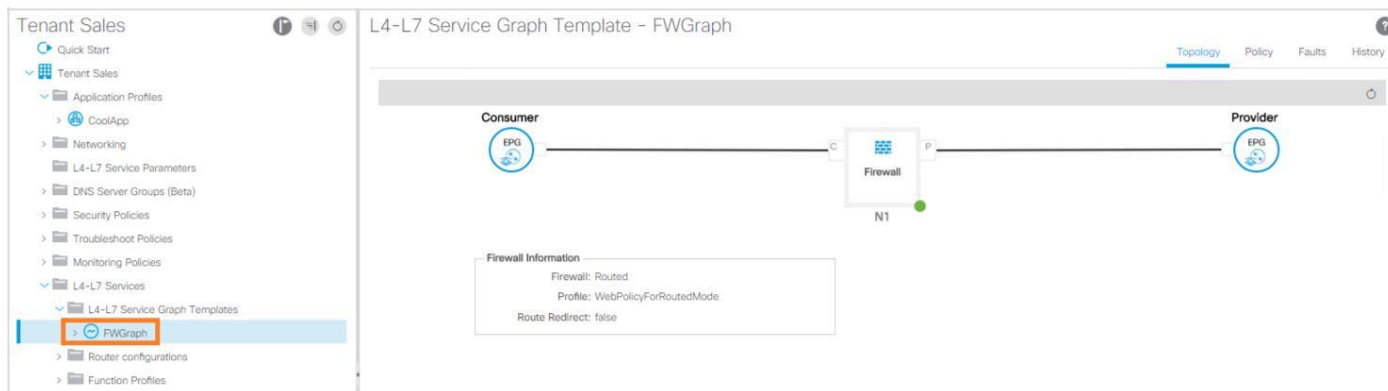
- a. [テナント Sales (Tenant Sales)] > [セキュリティ ポリシー (Security Policies)] > [コントラクト (Contracts)] を展開します。
- b. PuTTY ウィンドウに戻り、「スクリプト/CreateContract.xml を処理する場合は Return を押し、このスクリプトをスキップする場合は「s」を入力して Return を押します (Hit return to Process Scripts/CreateContract.xml or press 's' and return to skip this script)」プロンプトで **Enter** を押します。
- c. コントラクトが [コントラクト (Contracts)] に作成されます。画面を更新しないと、新しいコントラクトがトポロジに表示されない場合があります。



16. 次の手順に従って、**Webgraph** サービス グラフを作成します。

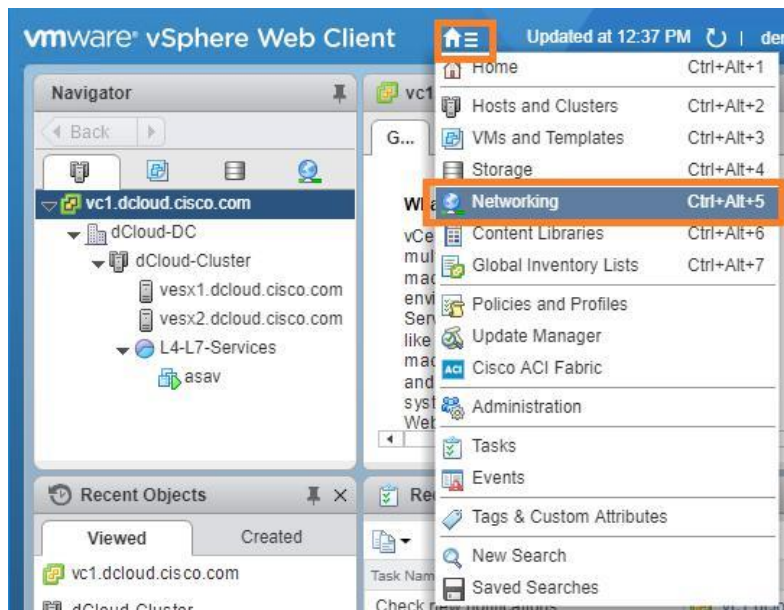
- a. **Tenant Sales** ディレクトリのまま、[L4-L7 サービス (L4-L7 Services)] > [L4-L7 サービス グラフ テンプレート (L4-L7 Service Graph Templates)] を展開します。このフォルダは空です。
- b. PuTTY ウィンドウに戻り、「スクリプト/CreateGraph.xml を処理する場合は Return を押し、このスクリプトをスキップするには「s」を入力して Return を押します (Hit return to process Scripts/CreateGraph.xml or press 's' and return to skip this script)」プロンプトで **Enter** を押します。

- c. [サービス グラフ(Service Graphs)] フォルダに、[機能ノード - N1(Function Node - N1)] サブディレクトリとともに **FWGraph** が作成されます。このスクリプトは、ポート プロファイルと接続もプッシュします。
- d. [機能ノード - N1(Function Node - N1)] を展開すると、作成されたオブジェクトが表示されます。
- e. [FWGraph] をクリックし、トポロジを確認します。

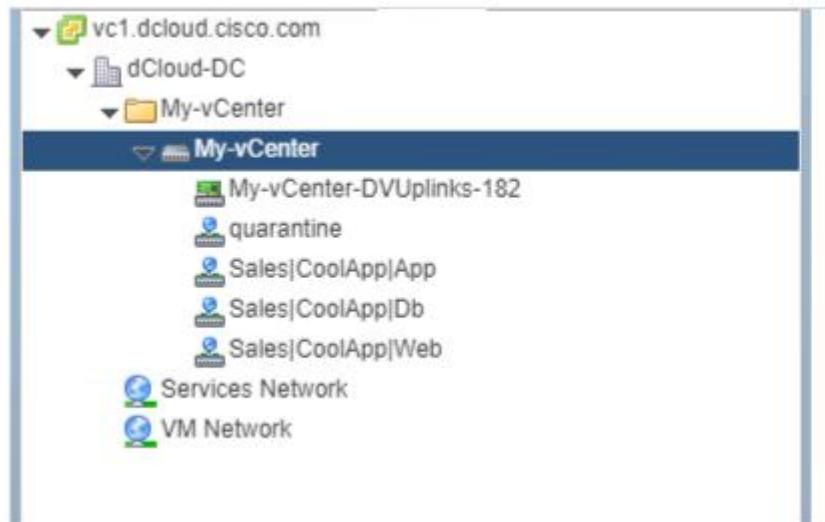


17. vSphere Web クライアントのウィンドウ内でクリックします。

18. [ネットワーキング(Networking)] ビューがまだロードされていない場合は、このビューを開きます。



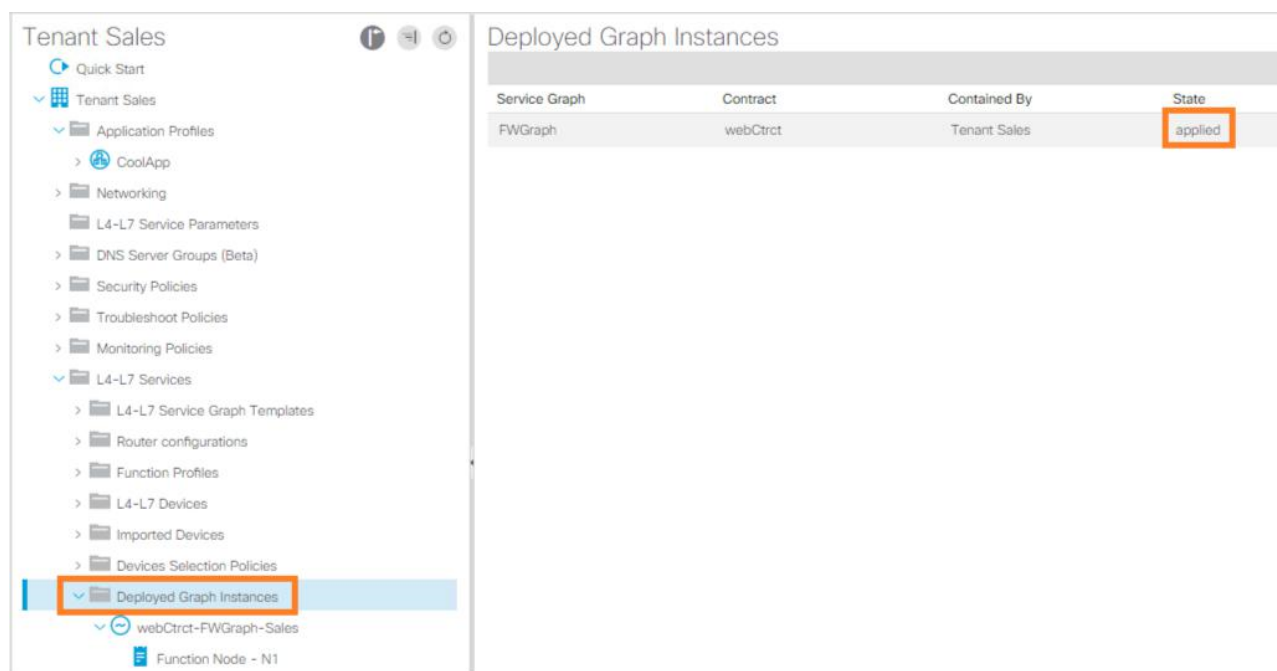
19. [vc1.dcloud.cisco.com] > [dCloud-DC] > [My-vCenter] > [My-vCenter] を展開し、[CoolApp] サービス プロファイルと EPG が vSphere に作成されていることを確認します。



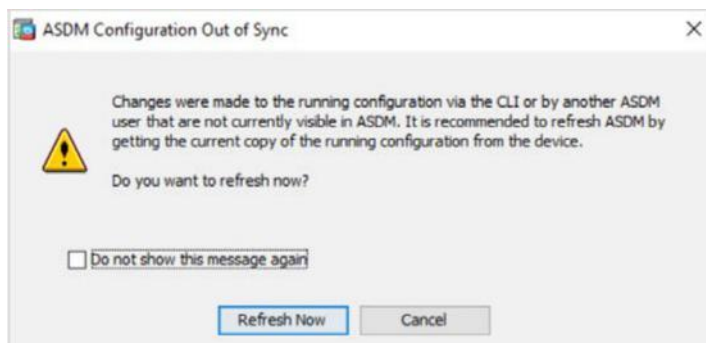
20. 次の手順に従って、**Sales** テナントに**サービス グラフ**を追加します。

- a. APIC ウィンドウに戻ります。[テナント(Tenants)] > [Sales] のまま、[L4-L7 サービス(L4-L7 Services)] > [導入されたグラフ インスタンス(Deployed Graph Instances)] を展開します。このフォルダは空です。
- b. PuTTY ウィンドウに戻り、「スクリプト/**AttachGraphToContract.xml**」を処理する場合は `Return` を押し、このスクリプトをスキップする場合は「s」を入力して `Return` を押します(Hit return to process Scripts/**AttachGraphToContract.xml** or press 's' and return to skip this script)プロンプトで **Enter** を押します。
- c. スクリプトが終了するまで数秒かかります。関連付けを示す **webCtrct-FWGraph-Sales** が **Deployed Service Graph** ディレクトリにドロップされます。

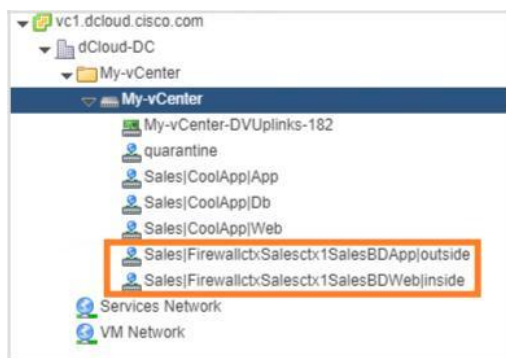
21. [L4-L7 サービス(L4-L7 Services)] > [導入されたグラフ インスタンス(Deployed Graph Instances)] フォルダをクリックします。コントラクトが [適用済み(applied)] の状態で一覧表示されます。



22. ASDM からポップアップが生成され、設定が同期していないことが示されます。[今すぐ更新 (Refresh Now)] をクリックしないでください。



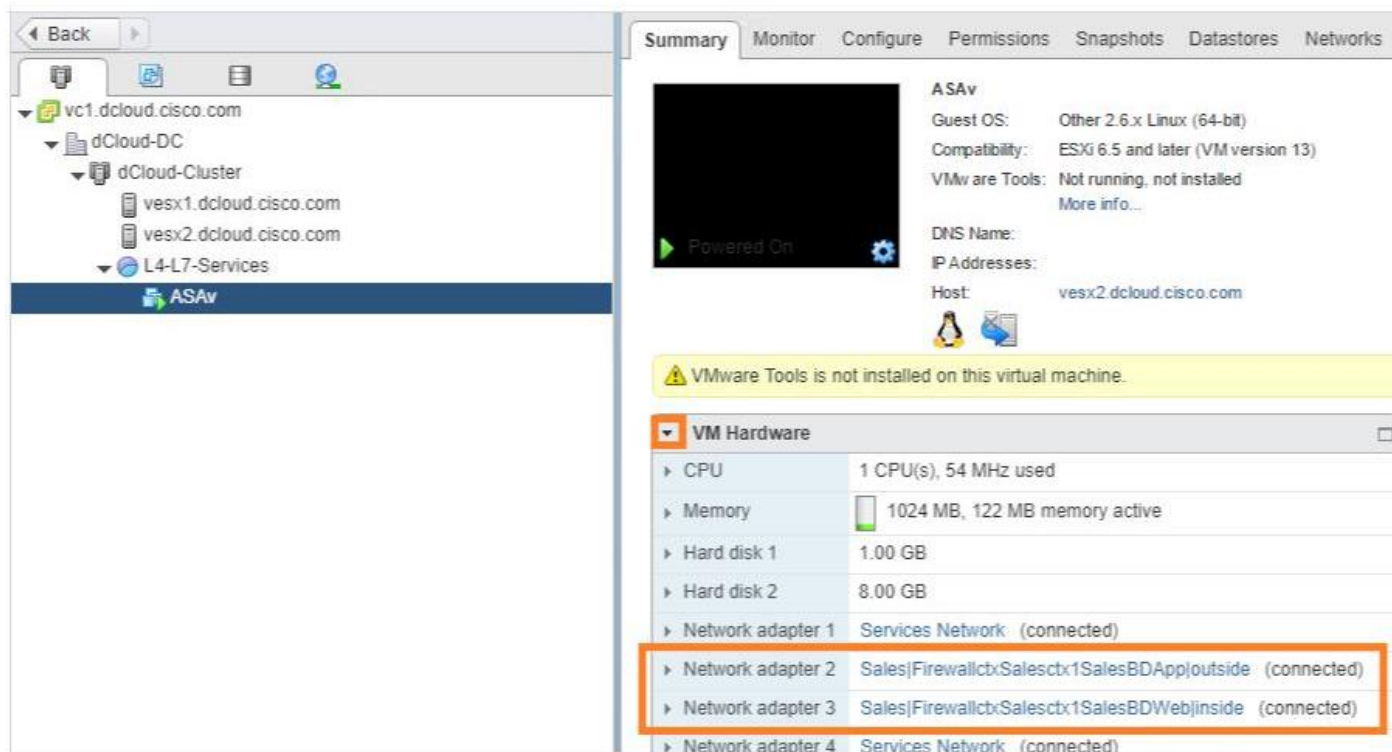
23. vSphere Web クライアントに戻ります。このクライアントには新しいポート プロファイルが作成されています。



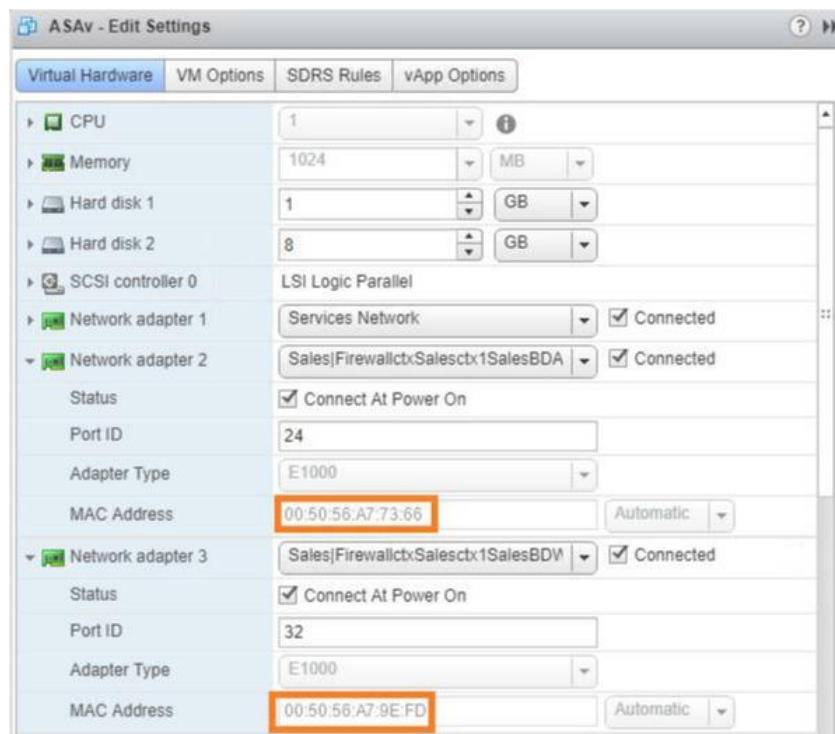
24. vSphere Web クライアント ウィンドウの下部にある [最近のタスク (Recent Tasks)] ペインで、新しいポート プロファイルを仮想マシン ASAv に追加するタスクを確認します。

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time
Add Distributed Port Groups	My-vCenter	✓ Completed	VSPHERE.LOCAL\...	2 ms	9/12/2017 12:42:13 ...	9/12/2017 12:42:13 ...
Add Distributed Port Groups	My-vCenter	✓ Completed	VSPHERE.LOCAL\...	12 ms	9/12/2017 12:42:13 ...	9/12/2017 12:42:13 ...

25. vSphere のロケーション バーで、[ホストとクラスター (Hosts and Clusters)] をクリックします。
26. [ASAv] をクリックし、[サマリー (Summary)] タブをクリックし、[仮想マシン ハードウェア (VM Hardware)] を展開して、仮想マシンハードウェア設定を表示します。



27. 仮想マシン **ASAv** を右クリックし、ポップアップ表示されたメニューから [設定の編集 (Edit Settings)] を選択します。
28. [ネットワークアダプタ 2 (Network adapter 2)] および [ネットワークアダプタ 3 (Network adapter 3)] をクリックして、MAC アドレスを表示します。



29. **APIC** ウィンドウに戻ります。[テナント Sales(Tenant Sales)] > [L4-L7 サービス(L4-L7 Services)] > [導入されたグラフ インスタンス (Deployed Graph Instances)] 内で、[webCtrct-FWGraph-Sales] をクリックし、導入されたサービス グラフのトポロジを確認します。
30. [webCtrct-FWGraph-Sales] を展開し、[機能ノード - N1 (Function Node - N1)] をクリックして、ASA に対する設定を確認します。

The screenshot shows the configuration for 'Function Node - N1'. The 'Cluster Interfaces' table is as follows:

Name	Concrete Interfaces	Encap
inside	Firewall_Device_1([GigabitEthernet0/1])	unknown
outside	Firewall_Device_1([GigabitEthernet0/0])	unknown

The 'Function Connectors' table is as follows:

Name	Encap	Class ID
consumer	vlan-1001	49157
provider	vlan-1337	16387

The 'Folders And Parameters' section shows the following parameters:

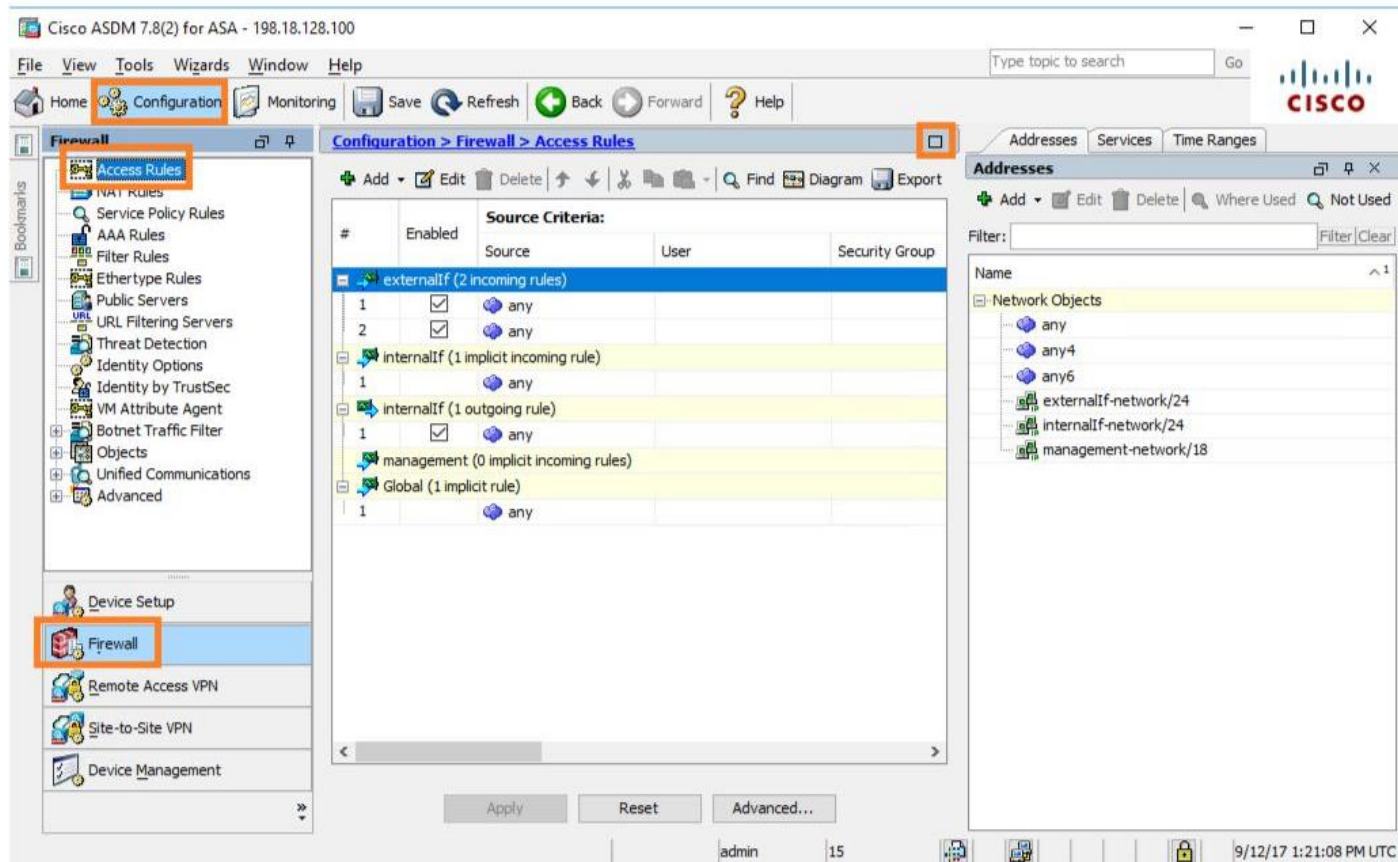
Meta Folder/Param Key	Name	Value	Override name/value To
Device Config	Device		
Access List	access-list-inbound		epg
Access List	access-list-outbound		epg
Interface Related Configuration	externalIf		epg
Interface Related Configuration	internalIf		epg

31. ASDM ウィンドウを最大化し、**ASDM** のポップアップで [今すぐ更新 (Refresh Now)] をクリックして、表示を更新します。

Interface	IP Address/Mask	Line	Link	Kbps
externalIf	20.20.20.50/24	↑ up	↑ up	0
internalIf	30.30.30.50/24	↑ up	↑ up	0
management	198.18.128.100/18	↑ up	↑ up	2

Select an interface to view input and output Kbps

32. ASDM 内で、[設定 (Configuration)] > [ファイアウォール (Firewall)] > [アクセス ルール (Access Rules)] に移動し、インバウンドのアクセス リスト設定とアウトバウンドのアクセス リスト設定が、ASA に作成されているアクセス ルールと一致していることを確認します。 [アクセス ルール (Access Rules)] ペインを最大化して、ルール設定を確認します。



33. APIC ウィンドウに戻り、MAC アドレスと正しいポート プロファイルが表示されていることを確認します。

- a. トップ メニューで、[仮想マシン ネットワーキング (VM Networking)] > [インベントリ (Inventory)] をクリックします。
- b. [VMware] > [My-vCenter] > [コントローラ (Controllers)] > [dCloud-DC] > [ハイパーバイザ (Hypervisors)] > [vesx1.dcloud.cisco.com] > [仮想マシン (Virtual Machines)] を展開し、[vesx2.dcloud.cisco.com] > [仮想マシン (Virtual Machines)] を展開します (ASAv はいずれかのホストにあります)。
- c. [ASAv] をクリックしてパラメータを表示します。新たに追加されたポート プロファイルが、追加された [ポートグループ (Portgroup)] フィールドに表示されていることを確認します。

Inventory

- Quick Start
- Kubernetes
- Microsoft
- OpenStack
- VMware
 - My-vCenter
 - Controllers
 - dCloud-DC
 - Hypervisors
 - vesx1.dcloud.cisco.com
 - Virtual Machines
 - base-template
 - vmnic0
 - vmnic1
 - vmnic2
 - vmnic3
 - vmnic4
 - vesx2.dcloud.cisco.com
 - Virtual Machines
 - ASAv
 - vmnic0

Virtual Machine - ASAv

General Stats Faults History

Properties

Name: ASAv
Status: Powered On

| Virtual Interfaces: | Name | IP | MAC | State | Portgroup |
|---------------------|--------------------|-----|-------------------|-------|--|
| | Network adapter 1 | --- | 00:50:56:A7:BE:9D | Up | |
| | Network adapter 10 | --- | 00:50:56:A7:18:A5 | Up | |
| | Network adapter 2 | --- | 00:50:56:A7:73:66 | Up | Sales FirewallctxSalesctx1SalesBDApp outside |
| | Network adapter 3 | --- | 00:50:56:A7:9E:FD | Up | Sales FirewallctxSalesctx1SalesBDWeb inside |
| | Network adapter 4 | --- | 00:50:56:A7:19:F5 | Up | |
| | Network adapter 5 | --- | 00:50:56:A7:DB:33 | Up | |
| | Network adapter 6 | --- | 00:50:56:A7:4A:84 | Up | |
| | Network adapter 7 | --- | 00:50:56:A7:B3:18 | Up | |
| | Network adapter 8 | --- | 00:50:56:A7:2A:D6 | Up | |
| | Network adapter 9 | --- | 00:50:56:A7:B2:3E | Up | |

Custom Attributes:

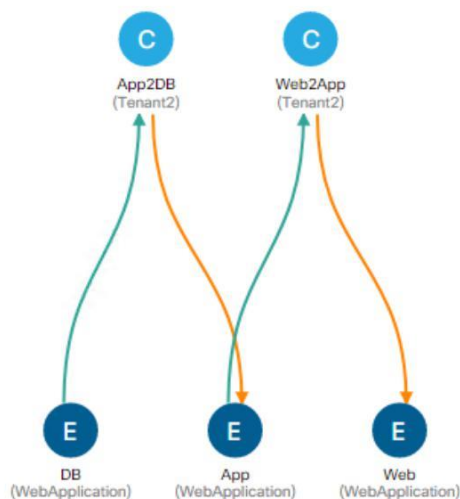
| Name | Value |
|---|-------|
| No items have been found.
Select Actions to create a new item. | |

シナリオ 4. NX-OS スタイルの CLI の使用


APIC CLI は NX-OS の CLI と同様になっています。NX-OS CLI には、APIC がいくつかの ACI モデル構造を自動的に作成できるようにする情報が組み込まれています。また、設定における一貫性を確保するための検証機能も備わっています。この機能によって障害の減少や防止が図れます。

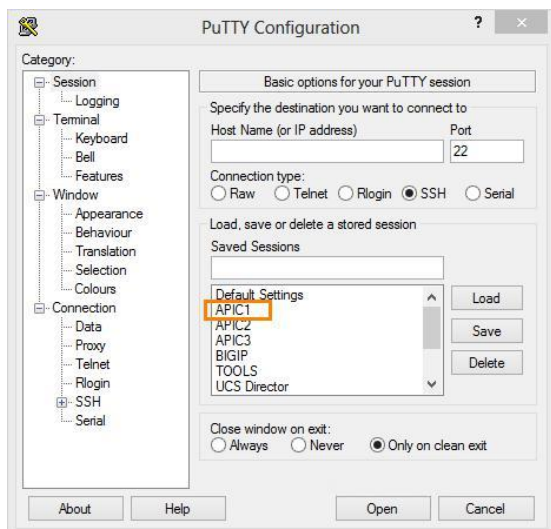
このシナリオでは、NX-OS スタイルの CLI を使用して、Cisco APIC に 3 階層アプリケーションを設定します。

注:このシナリオでは、NX-OS と同様に **Tab** キーと **↑** キーでコマンド補完機能と履歴機能が実行されます。



手順

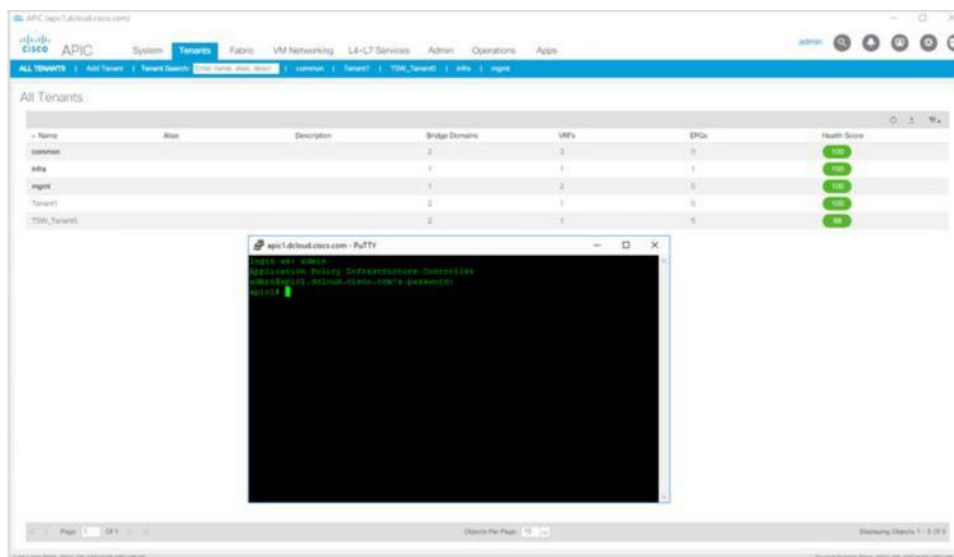
1. [wkst1] のタスクバーから、[PuTTY] ウィンドウ  を開きます。PuTTY ウィンドウが前のシナリオから開かれたままの場合は、タスクバーで PuTTY のショートカットを右クリックし、表示されたメニューから [PuTTY] を選択します。[PuTTY 設定 (PuTTY Configuration)] ウィンドウで [APIC1] をダブルクリックし、セキュリティ警告が表示されたらすべて [はい (Yes)] をクリックします。



2. PuTTY ウィンドウで、APIC にログインします (**admin/C1sco12345**)。パスワードの入力時、文字は表示されません。
3. **APIC** ウィンドウに戻り、または APIC ウィンドウを開き、APIC にログインします (**admin/C1sco12345**)。



4. コンソール ウィンドウと APIC ウィンドウの両方が表示されるようにウィンドウを配置します。APIC ウィンドウで、[テナント (Tenants)] > [すべてのテナント (ALL TENANTS)] をクリックし、テナント リストを表示します。



5. コンソール ウィンドウで次のコマンドを実行します。

```
conf
tenant Tenant2
```


6. APIC ウィンドウのテナント リストで、新しく作成された [Tenant2] をダブルクリックし、すべてのフォルダを展開します。オブジェクトは CLI で作成された際、APIC フォルダにドロップされます。
7. [テナント Tenant2 (Tenant Tenant2)] > [ネットワーキング (Networking)] > [ブリッジドメイン (Bridge Domains)] を展開します。このフォルダは空です。
8. PuTTY ウィンドウに戻り、次のコマンドを実行して、ブリッジドメインを作成します。ブリッジドメインが作成されることを APIC ウィンドウで確認します。

```
bridge-domain bd1
exit
bridge-domain bd2
exit
```

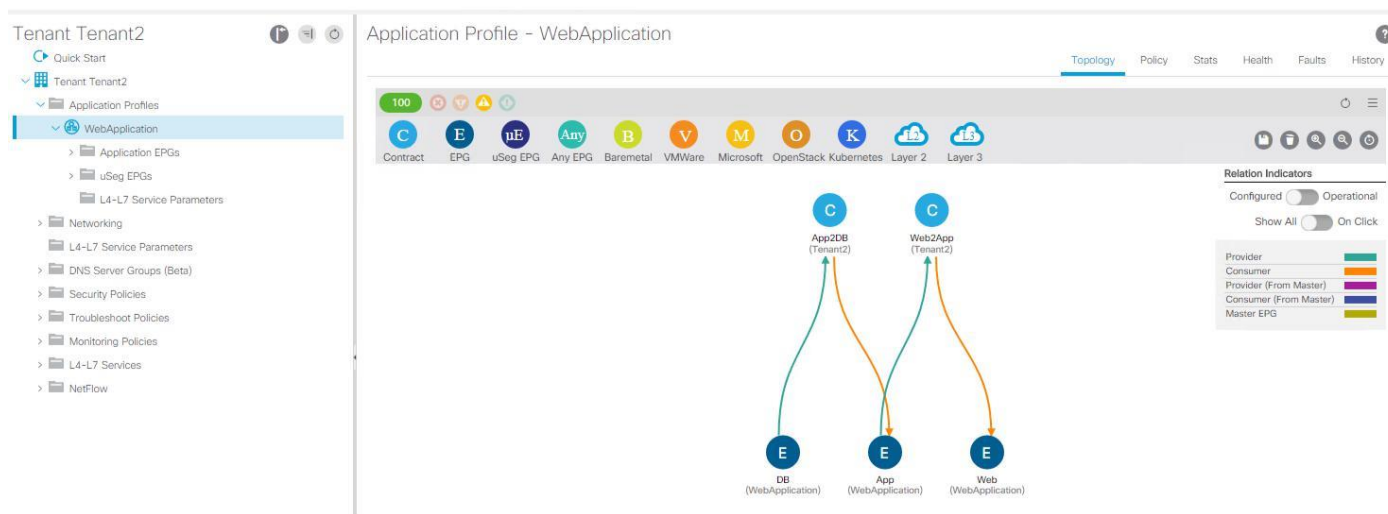
9. **APIC** ウィンドウに戻り、[テナント Tenant2(Tenant Tenant2)] > [セキュリティ ポリシー (Security Policies)] > [コントラクト (Contracts)] を展開し、[テナント Tenant2(Tenant Tenant2)] > [アプリケーション ポリシー (Application Policies)] を展開します。
10. コンソール ウィンドウで次のコマンドを実行します。後続の手順で EPG が作成されるまで、コントラクトは作業ウィンドウに表示されません。

```
contract App2DB
exit
contract Web2App
exit
application WebApplication
```

11. APIC ウィンドウで、[テナント Tenant2(Tenant Tenant2)] > [アプリケーション プロファイル (Application Profiles)] > [WebApplication] をクリックします。EPG とコントラクトが

作成されると、[アプリケーション プロファイル (Application Profile)] ウィンドウに表示されます。[更新 (Refresh)] ボタン  をクリックして、新しいオブジェクトを表示します。

```
epg Web
contract consumer
Web2App exit
epg App
contract consumer App2DB
contract provider
Web2App exit
epg DB
contract provider
App2DB end
```




オプション: APIC 3.0 VMware Admin スクリプトを実行する前に

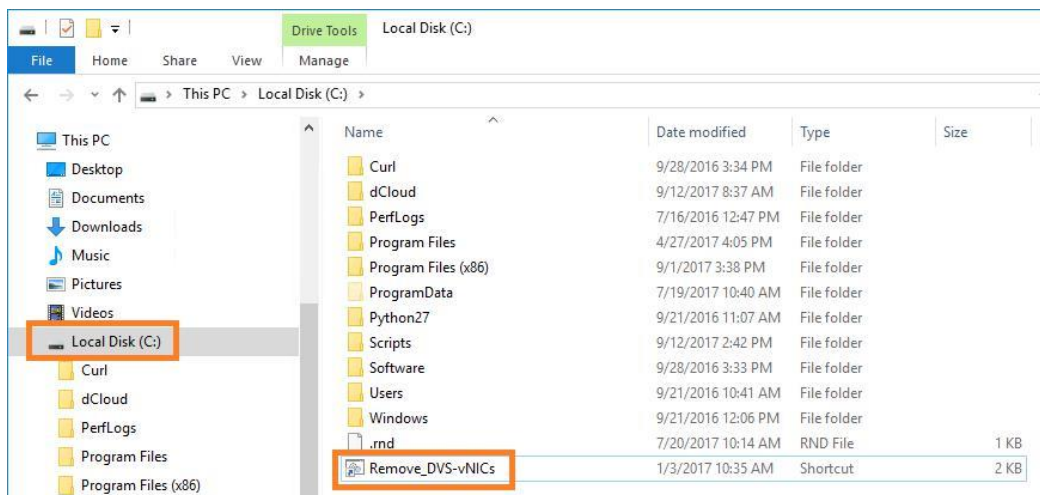
このデモの 2 つ目のスクリプト (*Cisco Application Policy Infrastructure Controller 2.1 with VMware – VMware Admin*) に進むには、まず次の手順を実行して、Sales テナントからファイアウォール デバイスを削除してください。


APIC オブジェクトの削除(オプション)

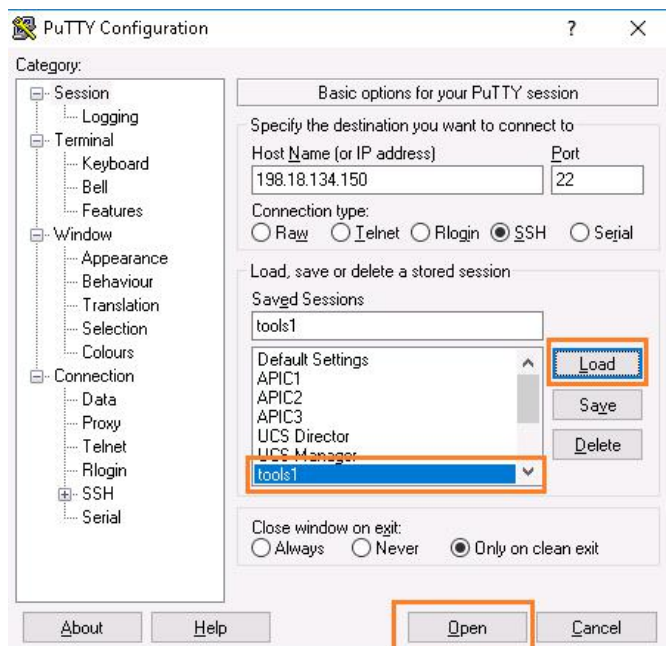
1. 次の手順に従って、ASA VM からポート プロファイルを削除します。

a. デモンストレーション ワークステーションのタスクバーから Windows エクスプローラを起動します。 

- b. Cドライブに移動し、[Remove_DVS_vNICs] をダブルクリックして、スクリプトを実行します。



2. 削除スクリプトが実行され、シェル ウィンドウに結果が表示されます。スクリプトが完了すると、シェル ウィンドウが閉じます。
3. ツール Linux サーバに接続し、クリーンアップ スクリプトを実行します。
 - a. デモンストレーション ワークステーションから、[PuTTY] () を起動します。
 - b. [PuTTY 設定 (PuTTY Configuration)] ウィンドウで、以下の操作を行います。
 - i. [保存済みセッション (Saved Sessions)] 領域で、[tools1] をダブルクリックします。
 - ii. ログインします (使用するクレデンシャルは、ユーザー名: **user01**、パスワード: **user01**)。



4. PuTTY コマンド ウィンドウのコマンド プロンプトで `./request.py Scripts/Remove_All.cfg` と入力し、Enter を押します。

注:この Python スクリプトは、複数の XML スクリプトを実行して、オブジェクトを削除します。**APIC** ウィンドウを表示し、[テナント(Tenants)] > [Sales] を開きます。各フォルダを展開して、削除されるオブジェクトを確認してください。

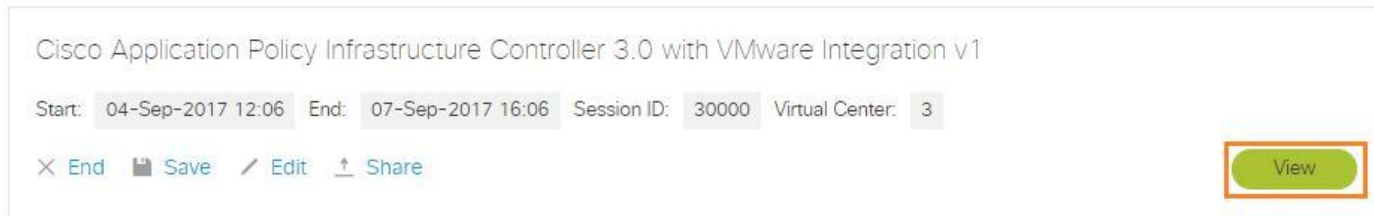
5. 各プロンプトで Enter を押して、スクリプトを実行します。
6. ASDM、vSphere、および APIC ウィンドウに戻り、Sales テナントに関連するすべてのオブジェクトが削除されていることを確認します。

付録 A. APIC シミュレータのリセット

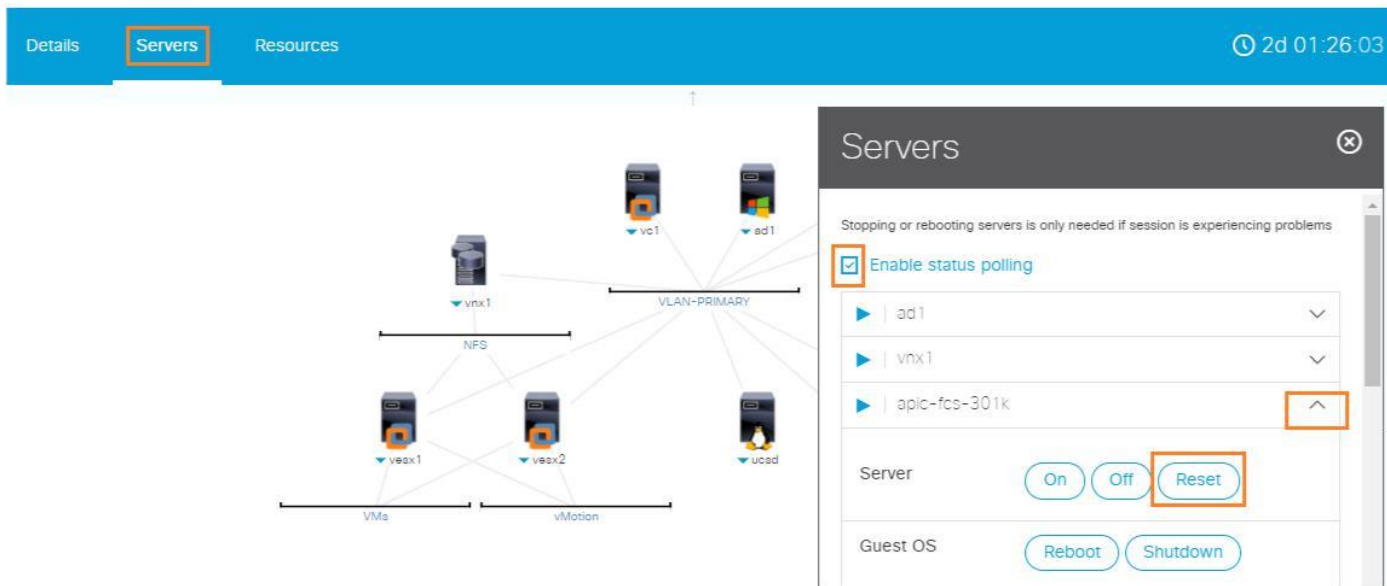
APIC ファブリック メンバーはデフォルトで検出されるため、APIC オブジェクトの作成からデモンストレーションを開始できます。

ファブリックの検出をデモンストレーションする場合は、次の手順に従って、ゲスト OS 制御を介して ACI シミュレータ (apic-fcs-301k) をリブートしてください。

1. Cisco dCloud で、[マイ ダッシュボード (My Dashboard)] をクリックし、目的のデモンストレーションに対する [表示 (View)] をクリックします。



2. メニュー バーから [サーバ (Servers)] を選択し、[ステータス ポーリングを有効にする (Enable Status Polling)] をオンにします。
3. **apic-fcs-301k** に対するメニューを展開し、[リセット (Reset)] を選択します。これにより、シミュレータのハード リブートが実行されます。この操作では、リブート後に設定は保持されないため、クリーン リブートは必要ありません。



注: ログインして、[付録 B](#) のファブリック検出方法の 1 つを使用してファブリックを再構築できるようになるまでに 5 分ほどかかります。


付録 B. デモの修正

場合により、セッション中に問題が発生することがあります。「Fix My Demo (デモの修正)」スクリプトを使用すると、一般的な問題を解決できます。下の手順により、次の問題を手動で解決できます。

- 設定を UCS Manager に適用する
- ACI ファブリックを検出し、デモ設定を ACI シミュレータに適用する
- VMware vCenter および ESXi ホストに適用されるライセンスを更新する
- UCS Director をリブートする

注: ACI ファブリックの検出が完了するまでに 15 分ほどかかる場合があります。APIC3 は、すべてのデバイスの検出後に検出されます。APIC GUI の [インベントリ (Inventory)] ペインで [トポロジ (Topology)] を選択することにより、進捗状況をモニタリングできます。検出の実行中、[シナリオ 1](#) を完了できます。このシナリオが終了すると、検出された要素を表示する [APIC トポロジ (APIC Topology)] ウィンドウが表示されます。

手順

1. デモンストレーション ワークステーションから、[デモの修正 (Fix My Demo)] アイコン  をクリックします。
2. 目的のタスクを選択します。タスクが完全に完了するまで、コマンド ウィンドウは閉じないでください。

Administrator: Fix My dCloud Session

```
Fix My dCloud Session
1. Apply Demo Configuration to UCS Manager
2. Apply APIC with VMware Demo Configuration to the ACI Simulator
3. Update VMware Licensing
4. Reboot UCS Director
```

Choose what you would like to do: _

©2018 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2018年3月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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