

# Cisco Application Policy Infrastructure Controller 3.0 with VMware Integration – VMware 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 の操作およびトラブルシューティング](#)
- [シナリオ 2: VC Plugin を使用したアプリケーションの導入](#)
- [シナリオ 3: L4-L7 サービスの追加](#)
- [シナリオ 4: L3 外部接続の追加](#)

『Network Administration Demo Guide (ネットワーク管理デモ 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 \(CHI\)](#)

## 制限事項

### APIC シミュレータの制限事項

- vSphere 用の VC Plugin では、予期しない結果が発生する可能性があり、特にシナリオ 1 では、vSphere Web クライアントの再起動が繰り返し必要となることがあります。



この問題が発生した場合は、[はい(Yes)] をクリックして再起動を実行し、シナリオの手順に従って、VC Plugin、テナント、およびアプリケーション プロファイルを再度選択してください。現段階までの作業内容が保存されます。

その他のすべてのエラーは無視しても問題ありません。エラー ウィンドウを閉じて、手順を続行してください。

- 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 シミュレータのリ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"> <li>• ラップトップ</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco AnyConnect</li> </ul>

## 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](http://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、APIC GUI 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。



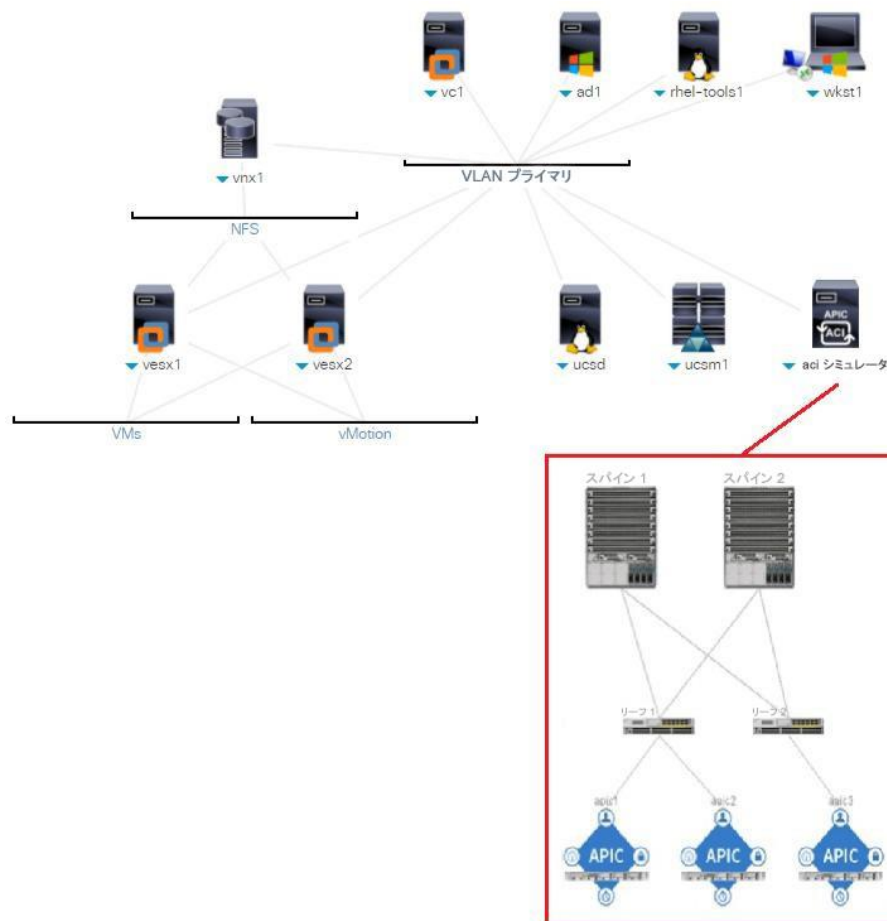
- [トポロジ (Topology)] メニュー: トポロジにあるサーバをクリックすると、使用可能なサーバ オプションがポップアップ ウィンドウに表示されます。
- [サーバ (Servers)] メニュー: サーバ名の横にある  または  をクリックすると、利用可能なサーバ オプションとクレデンシャルが表示されます。

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。

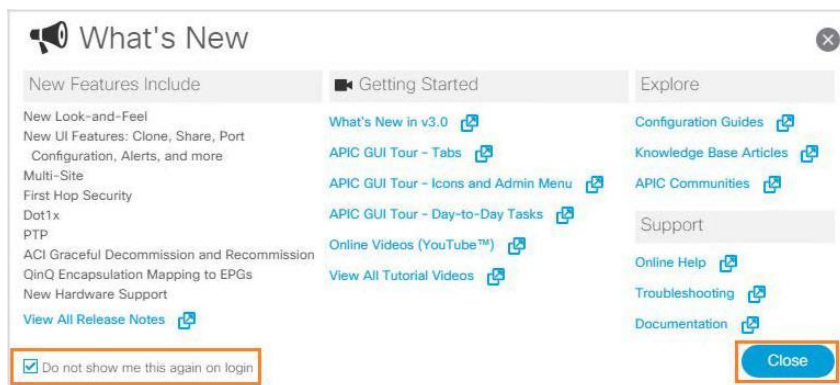
1. dcloud.cisco.com にアクセスして、最寄りのロケーションを選択し、Cisco.com アカウントでログインします。
2. セッションを予約します。[手順を見る](#)

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。

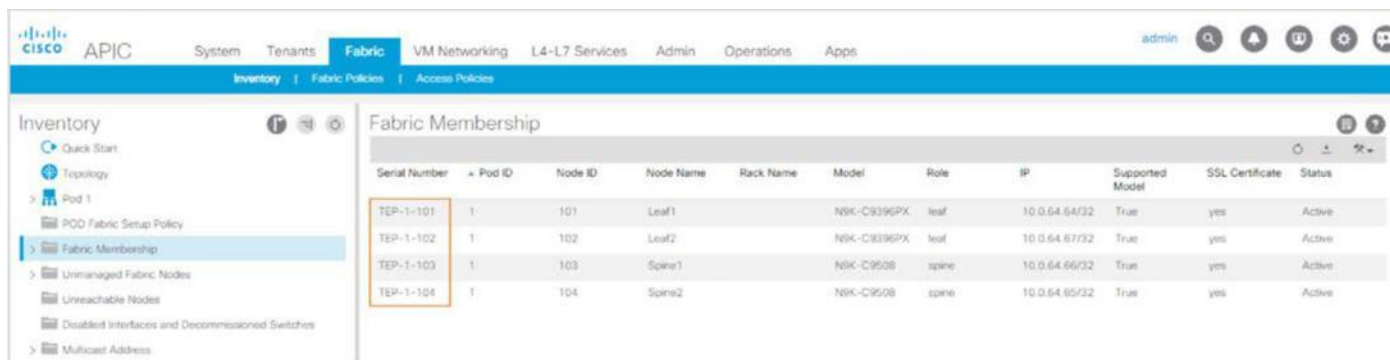
**注:** セッションがアクティブになるまでに 20 分ほどかかることがあります。

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: DCLLOUDdemouser、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。



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 APIC (Application Policy Infrastructure Controller) System Health page. The page title is "System Health" and it includes a "Zoom" section with buttons for "1H", "1D", "1M", "1Y", and "All". The main content area displays "No stats data to display...". On the right side, there is a "Fault Counts By" section with a table and two checkboxes: "Hide Acked Faults" and "Hide Delegated Faults". A critical error message is displayed in a red box, stating: "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 error message is highlighted with an orange border.

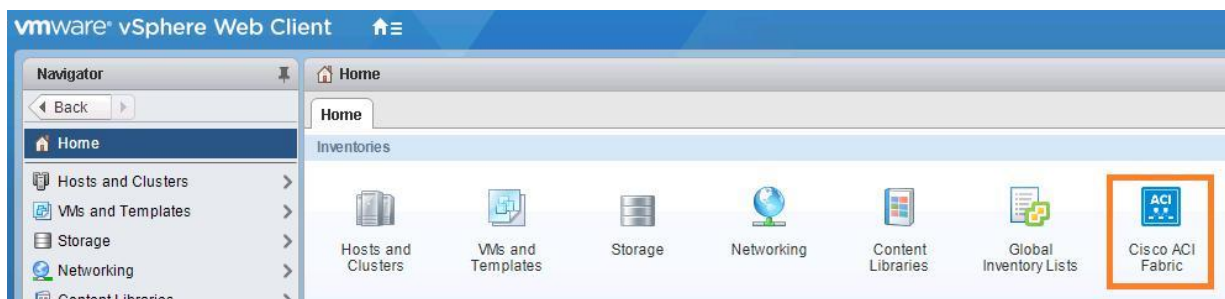
	2	1	1	0
SYSTEM WIDE	2	1	1	0
Access	0	0	0	0
External	0	0	0	0
Framework	0	0	0	0

## シナリオ 1. APIC の操作およびトラブルシューティング

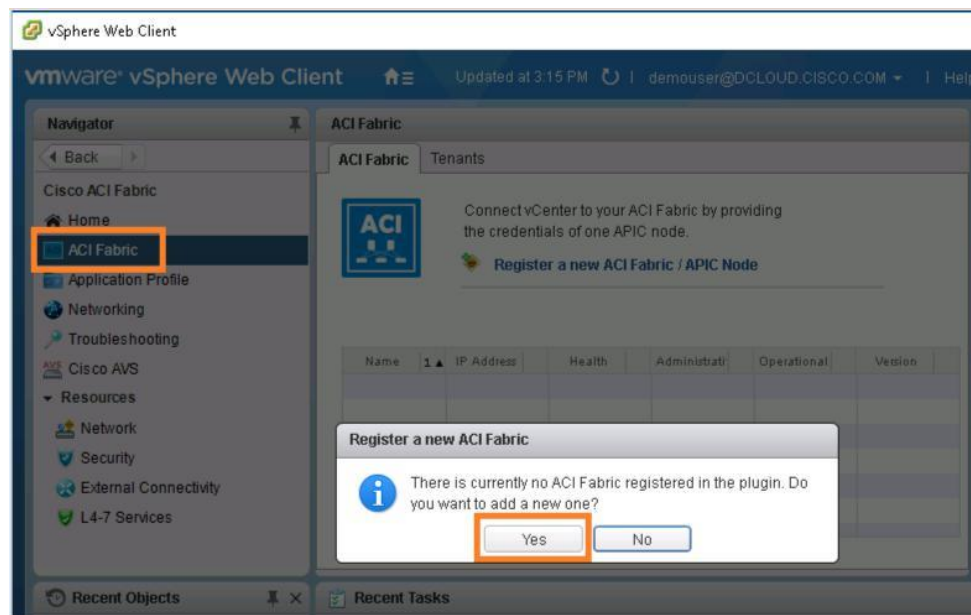
このシナリオでは、VMware vSphere vcPlugin を使用して、APIC 2.1 の操作およびトラブルシューティングを実行します。

### 手順

1. APIC をまだ開いていない場合は APIC にログインします (**admin/C1sco12345**)。
2. [テナント(Tenants)] をクリックします。
3. デスクトップで、**vSphere Web クライアント**のショートカット  をダブルクリックして、vSphere Web クライアントを開きます。  
[Windows ログイン クレデンシャルを使用する(Use Windows login credentials)] をクリックし、[ログイン(Login)] をクリックします。
4. [Cisco ACI ファブリック(Cisco ACI Fabric)] をクリックします(下のような vSphere ランディング ページが表示されない場合は、[ホーム(Home)] アイコン  をクリックし、ドロップダウン メニューから [Cisco ACI ファブリック(Cisco ACI Fabric)] を選択します)。



5. サイド メニューの [ACI ファブリック(ACI Fabric)] をクリックします。
6. [はい(Yes)] をクリックして、ACI ファブリックを登録します。



7. [新しい APIC ノードの登録 (Register a New APIC Node)] ダイアログボックスで、[パスワード (Password)] フィールドに **C1sco12345** と入力し、[OK] をクリックします。

8. 成功を通知するポップアップで [OK] をクリックします。また、関連付けられている APIC コントローラも登録されたことを確認します。
9. vCenter で 3 つのコントローラを含む APIC ノードが表示されていることを確認します。

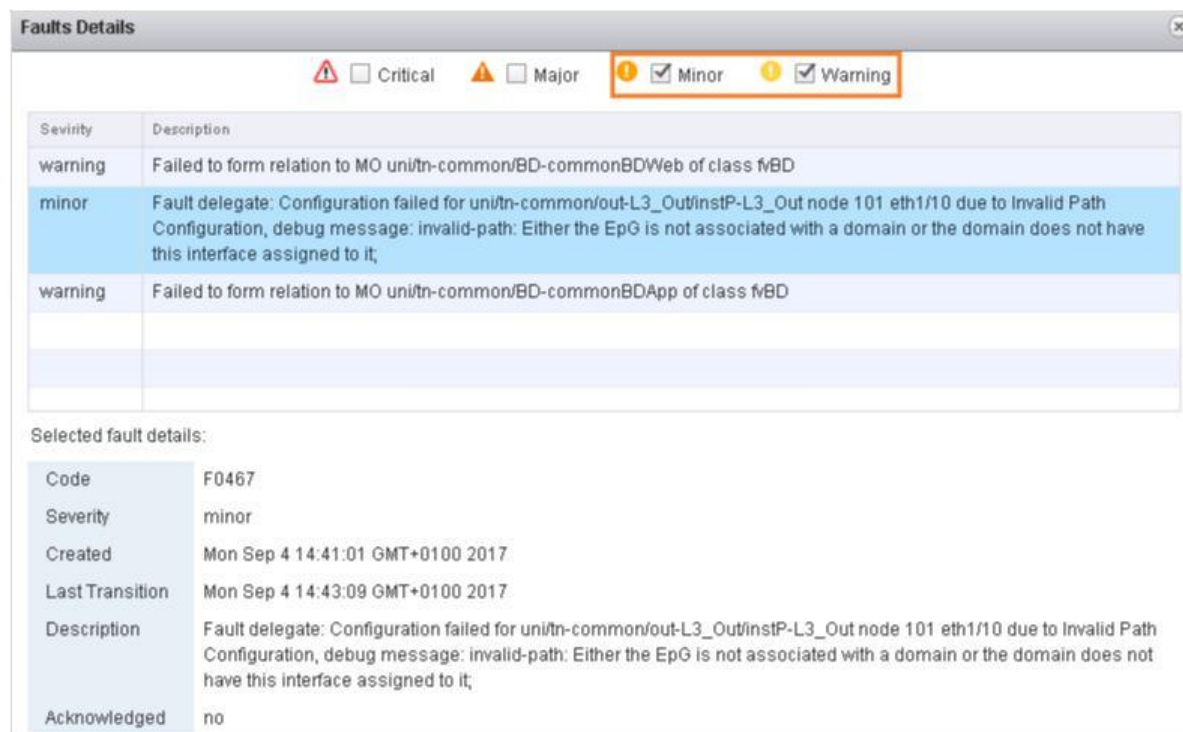
Name	IP Address	Health	Administrative State	Operational State	Version
apic1	198.18.133.200	Fully Fit	In Service	Available	3.0(1k)
apic2	198.18.133.201	Fully Fit	In Service	Available	3.0(1k)
apic3	198.18.133.202	Fully Fit	In Service	Available	3.0(1k)

10. [テナント (Tenants)] タブをクリックして、このファブリックに関連付けられているテナントを表示します。各テナントでは、関連する障害のリストが表示されます。
11. 色が付けられた重大度インジケータ (色付きの場合、その重大度の障害が存在することを示します) のいずれかをクリックすると、その詳細が表示されます。

Name	Health Score	Faults
common	100	1 (Warning), 2 (Info)
TSW_Tenant0	98	4 (Warning)



12. 障害の詳細を確認します。障害の重大度の選択を切り替えて、その他の障害を確認します。



**Faults Details**

Critical
  Major
  Minor
  Warning

Severity	Description
warning	Failed to form relation to MO uni/fn-common/BD-commonBDWeb of class fvBD
minor	Fault delegate: Configuration failed for uni/fn-common/out-L3_Out/instP-L3_Out node 101 eth1/10 due to Invalid Path Configuration, debug message: invalid-path: Either the EpG is not associated with a domain or the domain does not have this interface assigned to it;
warning	Failed to form relation to MO uni/fn-common/BD-commonBDApp of class fvBD

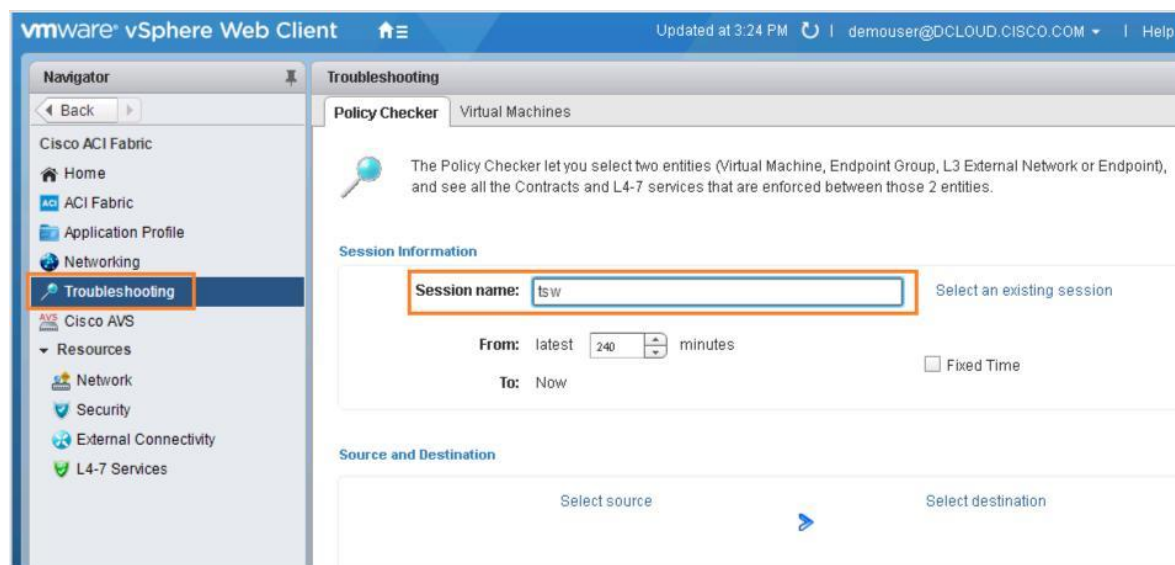
Selected fault details:

Code	F0467
Severity	minor
Created	Mon Sep 4 14:41:01 GMT+0100 2017
Last Transition	Mon Sep 4 14:43:09 GMT+0100 2017
Description	Fault delegate: Configuration failed for uni/fn-common/out-L3_Out/instP-L3_Out node 101 eth1/10 due to Invalid Path Configuration, debug message: invalid-path: Either the EpG is not associated with a domain or the domain does not have this interface assigned to it;
Acknowledged	no

13. [障害の詳細 (Faults Details)] ウィンドウを閉じます。

14. サイドメニューの [トラブルシューティング (Troubleshooting)] をクリックして、トラブルシューティング セッションを開始します。

15. [セッション名 (Session name)] フィールドに **tsw** と入力します。



vmware vSphere Web Client Updated at 3:24 PM demouser@DCLOUD.CISCO.COM Help

Navigator

- Cisco ACI Fabric
  - Home
  - ACI Fabric
  - Application Profile
  - Networking
  - Troubleshooting**
  - Cisco AVS
  - Resources
    - Network
    - Security
    - External Connectivity
    - L4-7 Services

Troubleshooting

Policy Checker Virtual Machines

The Policy Checker let you select two entities (Virtual Machine, Endpoint Group, L3 External Network or Endpoint), and see all the Contracts and L4-7 services that are enforced between those 2 entities.

Session Information

Session name:  Select an existing session

From: latest  minutes

To: Now  Fixed Time

Source and Destination

Select source  Select destination

16. [送信元の選択 (Select source)] をクリックします。

17. 表示されたメニューから [エンドポイントの選択 (Select Endpoint)] を選択します。

18. 表示された [エンドポイントの選択 (Select Endpoint)] ウィンドウで、IP アドレスが **10.193.101.14** のエンドポイントをクリックします。  
リスト上での位置は異なる場合があります。[OK] をクリックします。

Name	1 ▲	IP	Type
EndPoint 42:1D:BD:C4:00:00		10.193.101.22, 2222::65:16	Physical
EndPoint 42:9D:BC:C4:00:00		10.193.101.14, 2222::65:e	Physical
EndPoint 42:BD:BC:C4:00:00		10.193.101.16, 2222::65:10	Physical
EndPoint 42:DD:BC:C4:00:00		2222::65:12, 10.193.101.18	Physical
EndPoint 42:FD:BC:C4:00:00		2222::65:14, 10.193.101.20	Physical
EndPoint 43:0D:BD:C4:00:00		10.193.102.21, 2222::66:15	Physical
EndPoint 43:8D:BC:C4:00:00		10.193.102.13, 2222::66:d	Physical
EndPoint 43:AD:BC:C4:00:00		2222::66:f, 10.193.102.15	Physical
EndPoint 43:CD:BC:C4:00:00		2222::66:11, 10.193.102.17	Physical
EndPoint 43:ED:BC:C4:00:00		10.193.102.19, 2222::66:13	Physical

OK

Cancel

19. [宛先の選択 (Select destination)] をクリックします。

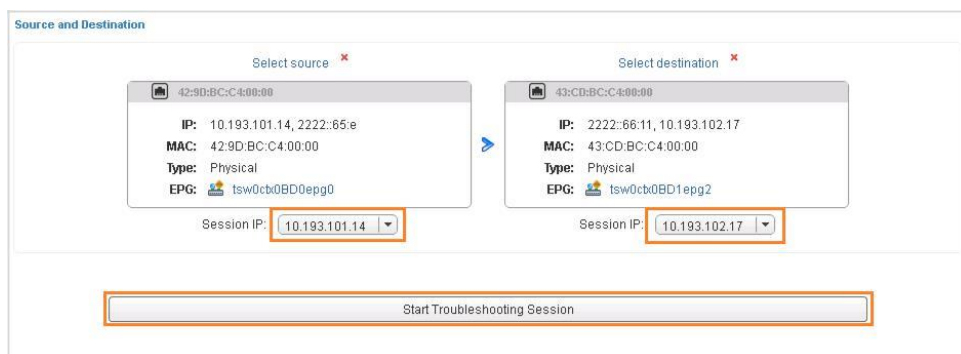
20. 表示されたメニューから [エンドポイントの選択 (Select Endpoint)] を選択します。



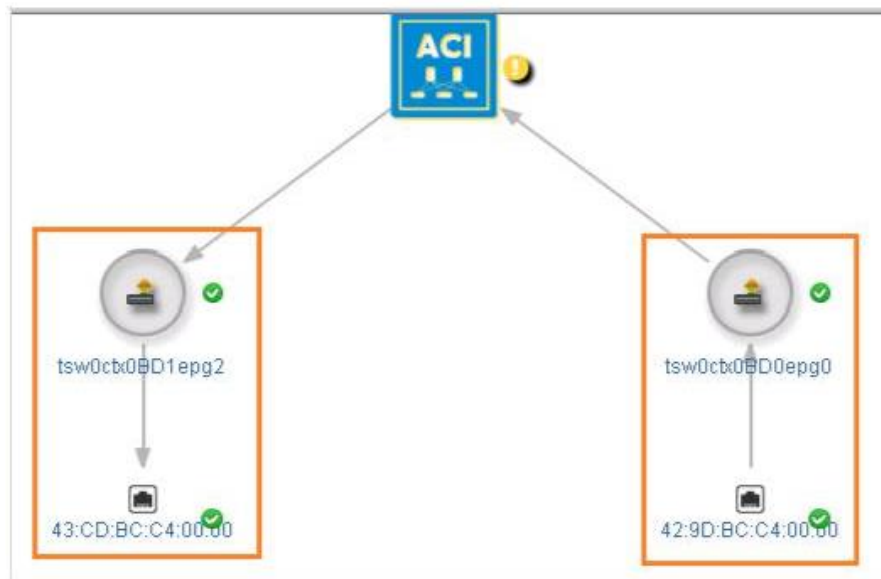
21. 表示された [エンドポイントの選択 (Select Endpoint)] ウィンドウで、IP アドレスが **10.193.102.17** のエンドポイントをクリックします。リスト上での位置は異なる場合があります。[OK] をクリックします。

Name	IP	Type
EndPoint 42:1D:BD:C4:00:00	10.193.101.22, 2222::65:16	Physical
EndPoint 42:9D:BC:C4:00:00	10.193.101.14, 2222::65:e	Physical
EndPoint 42:BD:BC:C4:00:00	10.193.101.16, 2222::65:10	Physical
EndPoint 42:DD:BC:C4:00:00	2222::65:12, 10.193.101.18	Physical
EndPoint 42:FD:BC:C4:00:00	2222::65:14, 10.193.101.20	Physical
EndPoint 43:0D:BD:C4:00:00	10.193.102.21, 2222::66:15	Physical
EndPoint 43:8D:BC:C4:00:00	10.193.102.13, 2222::66:d	Physical
EndPoint 43:AD:BC:C4:00:00	2222::66:f, 10.193.102.15	Physical
EndPoint 43:CD:BC:C4:00:00	2222::66:11, 10.193.102.17	Physical
EndPoint 43:ED:BC:C4:00:00	10.193.102.19, 2222::66:13	Physical

22. 各 [セッション IP (Session IP)] ドロップダウンを順番にクリックし、ドロップダウンでエンドポイントの IP アドレスを選択します。
23. [トラブルシューティング セッションの開始 (Start Troubleshooting Session)] バーをクリックします。



24. トラブルシューティング セッションが開始されるまで約 10 秒待ちます。
25. トラブルシューティング セッションのグラフィカル表示を確認します。MAC アドレスで送信元と宛先を識別して、各 EPG に接続されているノードを確認できます。



26. [ACI ファブリック(ACI Fabric)] アイコンの横にある [障害 (Fault)] アイコンをクリックして、記録された障害の表を表示します。

Severity	Affected	Description
warning	topology/pod-1/node-101/sys/cb-[vlan-2654208]/bd-[vlan-15892443]/lan-[vlan-2002]/fault-F110176	TCA: ingress drop bytes rate(l2IngrBytes5min:dropRate) value 13357 raised above threshold 10000
warning	topology/pod-1/node-101/sys/cb-[vlan-2654208]/bd-[vlan-15892443]/lan-[vlan-2002]/fault-F112128	TCA: ingress drop packets rate(l2IngrPkts5min:dropRate) value 10 raised above threshold 10
warning	topology/pod-1/node-102/sys/cb-[vlan-2654208]/bd-[vlan-15892443]/lan-[vlan-2002]/fault-F110176	TCA: ingress drop bytes rate(l2IngrBytes5min:dropRate) value 11671 raised above threshold 10000
warning	topology/pod-1/node-102/sys/cb-[vlan-2654208]/bd-[vlan-15892443]/lan-[vlan-2002]/fault-F110176	TCA: ingress drop packets rate(l2IngrPkts5min:dropRate) value 10 raised above threshold 10

27. 必要に応じて、障害の説明をいくつか確認します。

28. [障害 (Faults)] ウィンドウを閉じます。

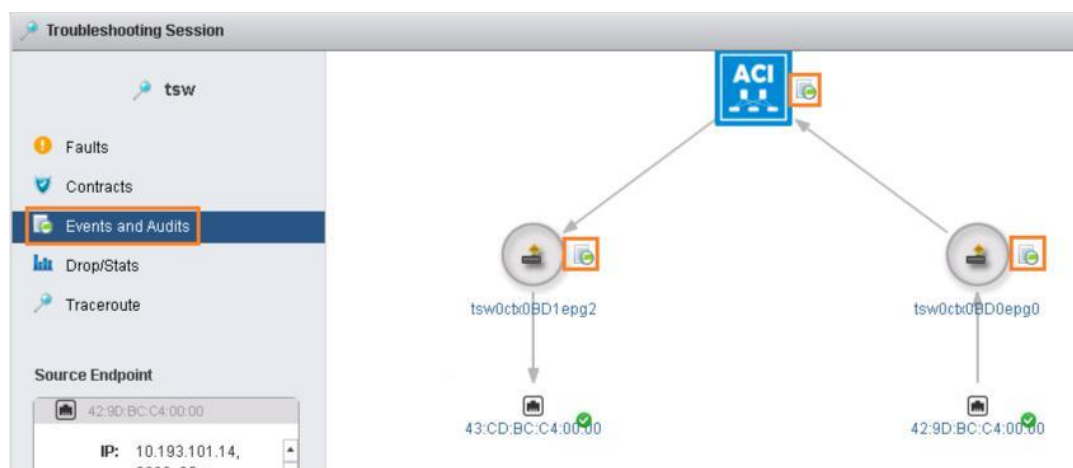
29. サイドメニューで [コントラクト(Contracts)] をクリックします。

30. コントラクト名をクリックします。

Name	Ethernet Type	Protocol	Source	Destination	Filter	Contract
http	ip	tcp	any	80	tsw0ctrc12_Filter	tsw0ctrc12

12. コントラクトの詳細を確認します。

31. 何も変更せずに [コントラクト設定の編集 (Edit Contract Settings)] ウィンドウを閉じます。
32. 左側のメニューで [イベントと監査 (Events and Audits)] をクリックし、ACI ファブリックまたはいずれかの EPG の横にある [イベント (Events)] アイコンをクリックします。



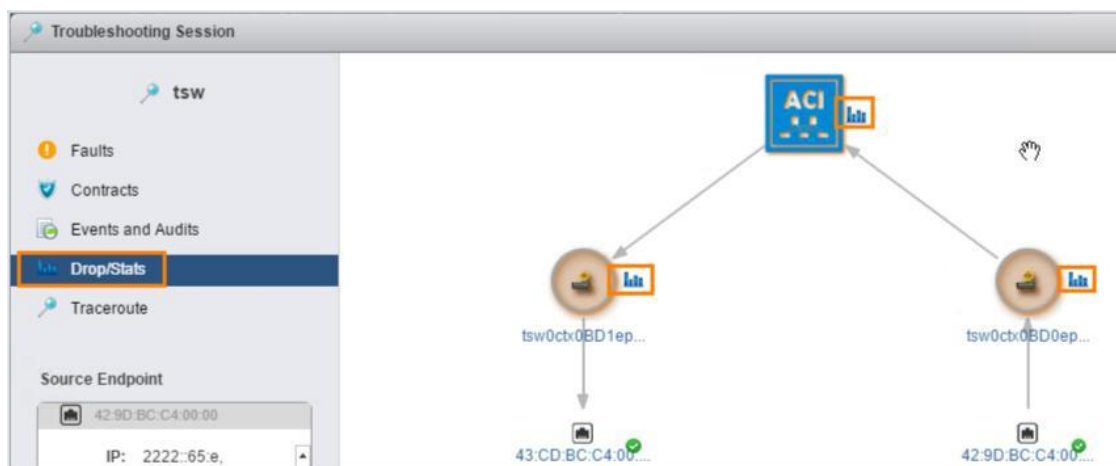
33. 表示されたウィンドウの [監査 (Audit)] タブで、その EPG またはファブリック上でユーザーが実行した操作を確認します。監査ログには、ログインとログアウト (aaa:SessionLR) や構成の変更 (aaa:ModLR) など、ユーザーが開始したイベント (監査可能となっている必要がある) のレコードがオブジェクトとして含まれています。

Time Stamp	User	Action	Affected Object	Description
Mon Sep 4 14:39:41 GMT+0100 2017	admin	creation	uni/tn-TSW_Tenant0/ap-tsw0AP0/epg-tsw0ctx0BD1epg2/rsdomAtt-[uni/phys-vpc]	RsDomAtt uni/phys-vpc created
Mon Sep 4 14:39:41 GMT+0100 2017	admin	creation	uni/tn-TSW_Tenant0/ap-tsw0AP0/epg-tsw0ctx0BD1epg2/rspathAtt-[topology/pod-1/paths-102/pathep-[eth1/17]]	RsPathAtt topology/pod-1/paths-102/pathep-[eth1/17] created

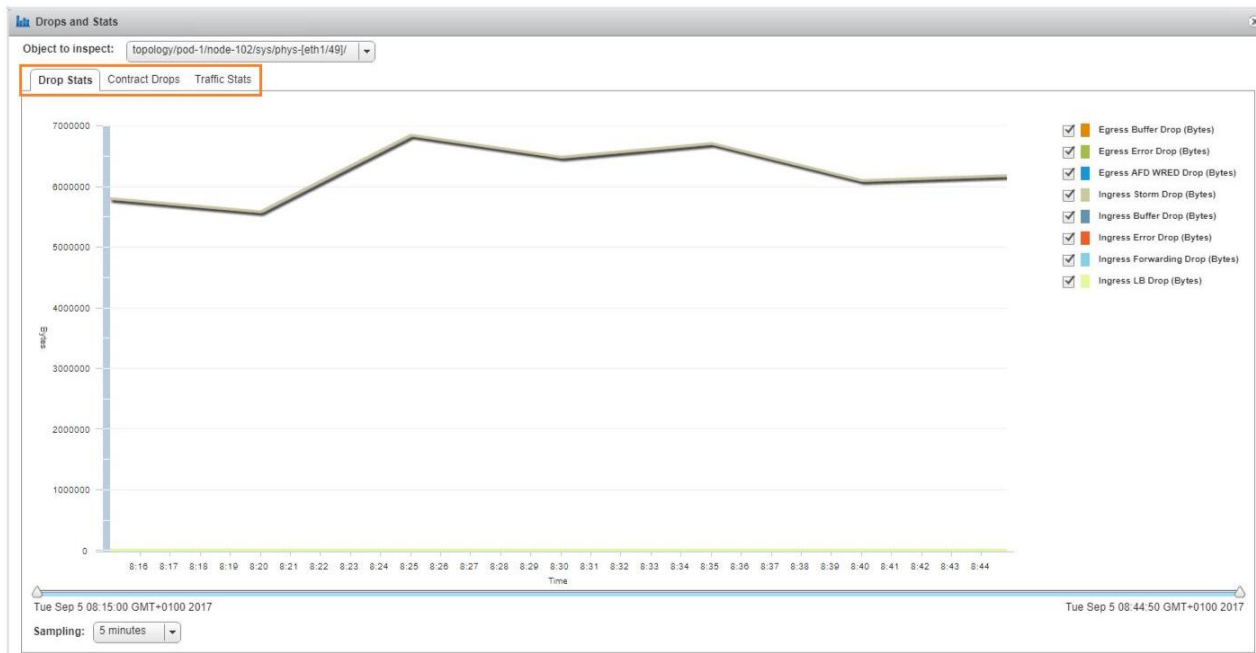
34. [イベント (Events)] タブをクリックします。このタブには、リンク状態遷移など、システムによって生成されたその他のイベント (event:Record) のレコードが表示されます。

Time Stamp	User	Action	Affected Object	Description
Mon Sep 4 14:41:01 GMT+0100 2017	internal	creation	topology/pod-1/node-101/sys/cbc-[vlan-2654208]/bd-[vlan-15892443]/vlan-[vlan-2002]	CktEp vlan-2002 created
Mon Sep 4 14:41:01 GMT+0100 2017	internal	creation	topology/pod-1/node-101/sys/cbc-[vlan-2654208]/bd-[vlan-15892443]/vlan-[vlan-2002]	CktEp vlan-2002 created
Mon Sep 4 14:41:01 GMT+0100 2017	internal	modification	topology/pod-1/node-101/sys/cbc-[vlan-2654208]/bd-[vlan-15892443]/vlan-[vlan-2002]	CktEp vlan-2002 modified
Mon Sep 4 14:40:58 GMT+0100 2017	internal	creation	topology/pod-1/lncnt-103/lnk-101-1-49-to-103-5-1	Fabric Link topology/pod-1/lncnt-103/lnk-101-1-49-to-103-5-1 created
Mon Sep 4 14:40:58 GMT+0100 2017	internal	state-transition	topology/pod-1/lncnt-103/lnk-101-1-49-to-103-5-1	Link State of Fabric Link is set to ok
Mon Sep 4 14:41:57 GMT+0100 2017	internal	creation	topology/pod-1/node-102/sys/cbc-[vlan-2654208]/bd-[vlan-15892443]/vlan-[vlan-2002]	CktEp vlan-2002 created

35. [監査とイベント (Audits and Events)] ウィンドウを閉じます。
36. サイドメニューの [ドロップ/統計情報 (Drop/Stats)] をクリックし、ACI ファブリックまたはいずれかの EPG の横にある [ドロップ/統計情報 (Drop/Stats)] アイコンをクリックします。

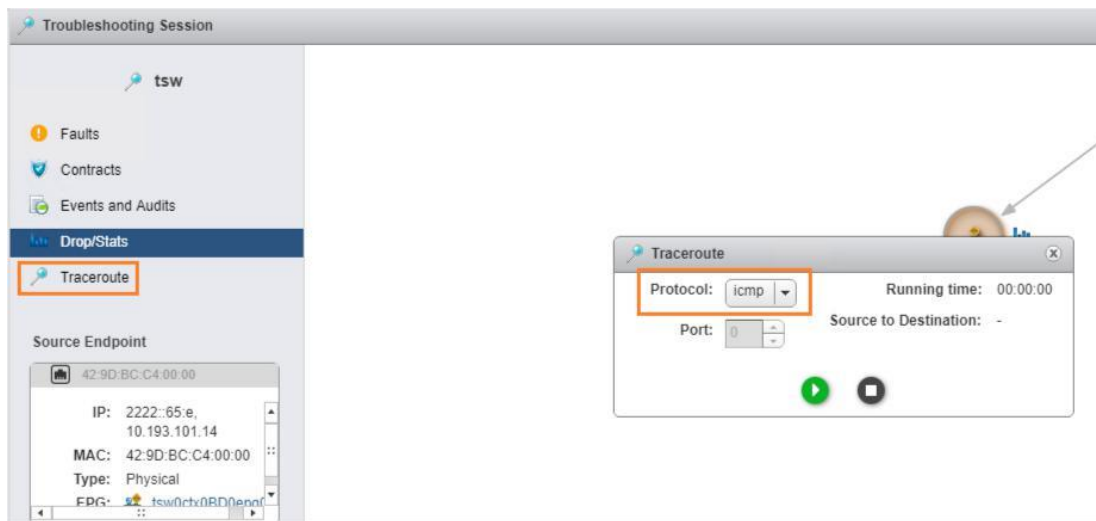


37. [ドロップと統計情報 (Drops and Stats)] ウィンドウの各タブをクリックして、[ドロップ統計情報 (Drop Stats)]、[コントラクトドロップ (Contract Drops)]、および [トラフィック統計情報 (Traffic Stats)] を確認します。



**注:** [コントラクトドロップ (Contract Drops)] ウィンドウは通常は空です。

38. 必要に応じて、[サンプリング (Sampling)] ドロップダウンで時間枠を変更します。ただし、各セッションのファブリックはセッションの開始時に作成されるため、セッションが作成される前のデータはありません。
39. [ドロップと統計情報 (Drops and Stats)] ウィンドウを閉じます。
40. サイドメニューで [トレースルート (Traceroute)] をクリックします。
41. ドロップダウンで [icmp] を選択し、[再生 (Play)] アイコンをクリックします。



42. 送信元 IP から宛先 IP にトラフィックが流れていることを示す [成功 (Success)] の通知が表示されるのを待ちます。



43. [トレースルート(Traceroute)] ウィンドウおよび [トラブルシューティングセッション(Troubleshooting Session)] ウィンドウを閉じます。



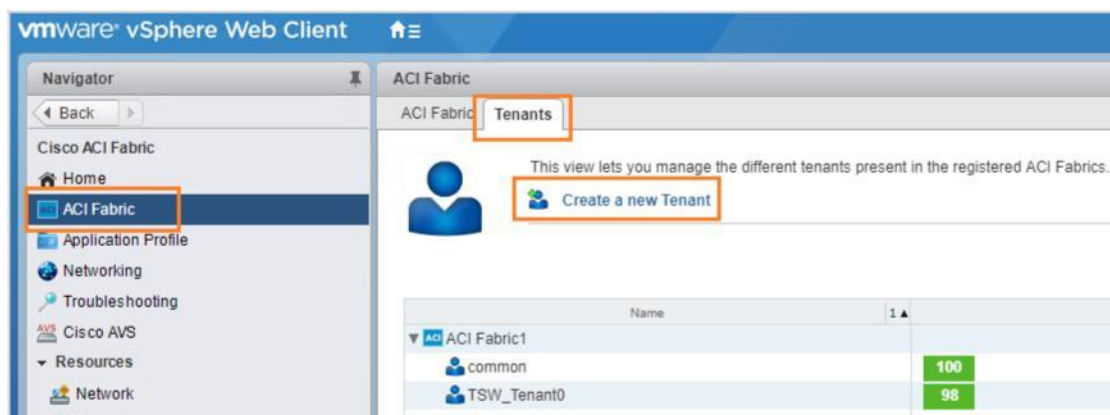
## シナリオ 2. VC Plugin を使用したアプリケーションの導入

このシナリオでは、VMware vSphere Web クライアントで vcPlugin を使用して、テナントを作成し、3 階層アプリケーションを導入します。

**重要:** このシナリオでは、デモンストレーション環境の性質上、エラー メッセージが生成される場合があります。これらのメッセージはすべて無視でき、デモンストレーション機能の妨げとなることはありません。[OK] をクリックするか、必要に応じて [はい(Yes)] をクリックして、vSphere をリロードしてください。

### 手順

1. **vSphere Web クライアント**をまだ開いていない場合は開いて、[ACI ファブリック (ACI Fabric)] をクリックします。
2. サイドメニューの [ACI ファブリック (ACI Fabric)] をクリックします。
3. [テナント (Tenants)] タブをクリックします。
4. [新しいテナントの作成 (Create a new Tenant)] をクリックします。



5. テナントの作成ウィンドウで、名前フィールドに **dCloud** と入力します。
6. 説明フィールドに **Created by VC Plug-in** と入力します。
7. [OK] をクリックします。

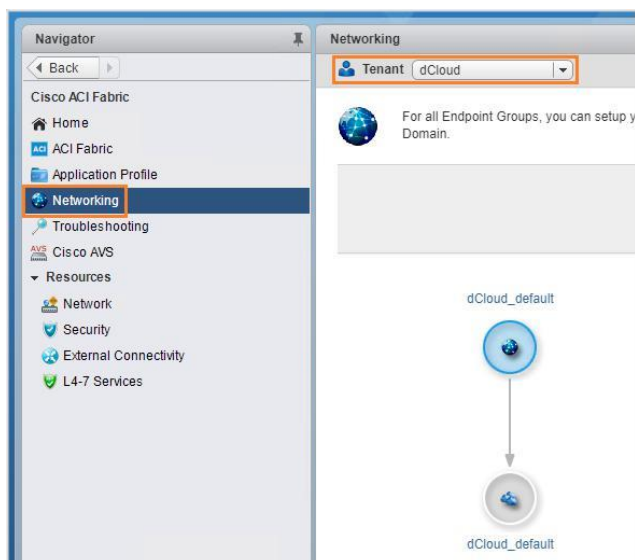


8. サイドメニューの [アプリケーション プロファイル (Application Profile)] をクリックします。

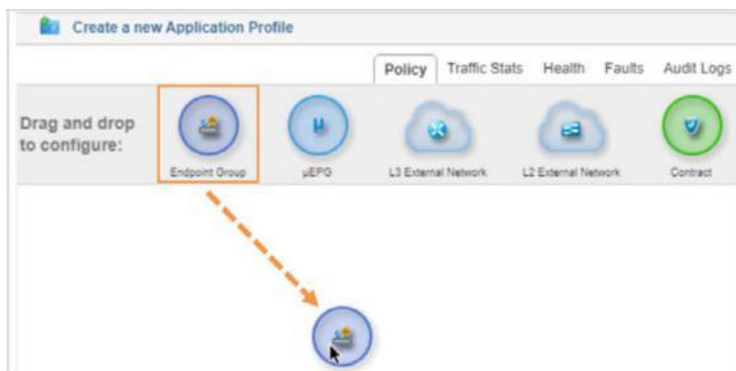
9. [テナント (Tenant)] ドロップダウンから [dCloud] を選択します。新しいアプリケーション プロファイル (Application Profile) がテナントとともに作成されていることがわかります (**dCloud\_default**)。このアプリケーション プロファイルは空です。EPG、コントラクト、L2 または L3 外部ネットワークは含まれていません。一緒に作成されるのは VRF とブリッジドメインだけです。



10. 側面パネルの [ネットワーキング (Networking)] をクリックし、VRF とブリッジドメインが新しいテナントとともに作成されたことを示します。



11. サイドメニューの [アプリケーション プロファイル (Application Profile)] を再度クリックし、次の手順に従って、アプリケーションの Web EPG を追加します。
- [エンドポイント グループ (Endpoint Group)] アイコンをクリックし、作業ウィンドウにドラッグします。



- 表示されたウィンドウで、[名前 (Name)] フィールドに **Web** と入力します。

- c. [編集 (Edit)] アイコンをクリックして、ブリッジドメインを指定します。

New Endpoint Group

Endpoint Group Information

Name:

Description:

Networking

Distributed Switch:  Allow micro-segmentation:

Bridge Domain:

Security

Intra EPG Isolation:

Application Profile:

OK Cancel

- d. [テナント dCloud (Tenant dCloud)] > [VRF dCloud\_default] を展開し、[ブリッジドメイン dCloud\_default (Bridge Domain dCloud\_default)] を選択します。[OK] をクリックします。

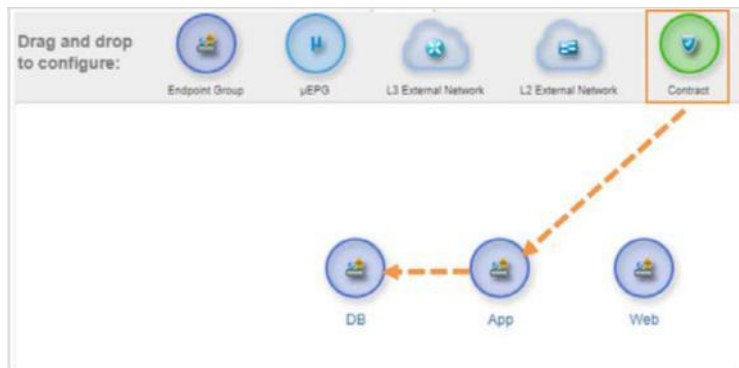


- e. [OK] を再度クリックして、Web EPG を作成します。

12. 手順 a. ~ e. を繰り返して、**App** EPG を作成します。
13. 手順 a. ~ e. を繰り返して、**DB** EPG を作成します。
14. 次の手順に従って、App 階層を DB 階層に接続する **ApptoDB** コントラクトを作成します。

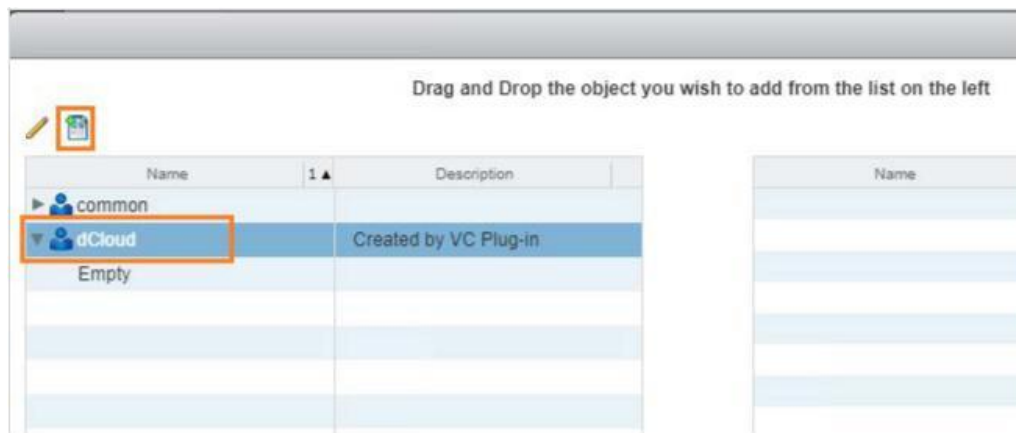
**注:** DB 階層はプロバイダーとなり、App 階層はこのコントラクトのコンシューマとなります。

- a. [コントラクト (Contract)] アイコンを作業ウィンドウにドラッグし、[App] EPG 上にドロップしてから、[DB] EPG にマウスオーバーします。

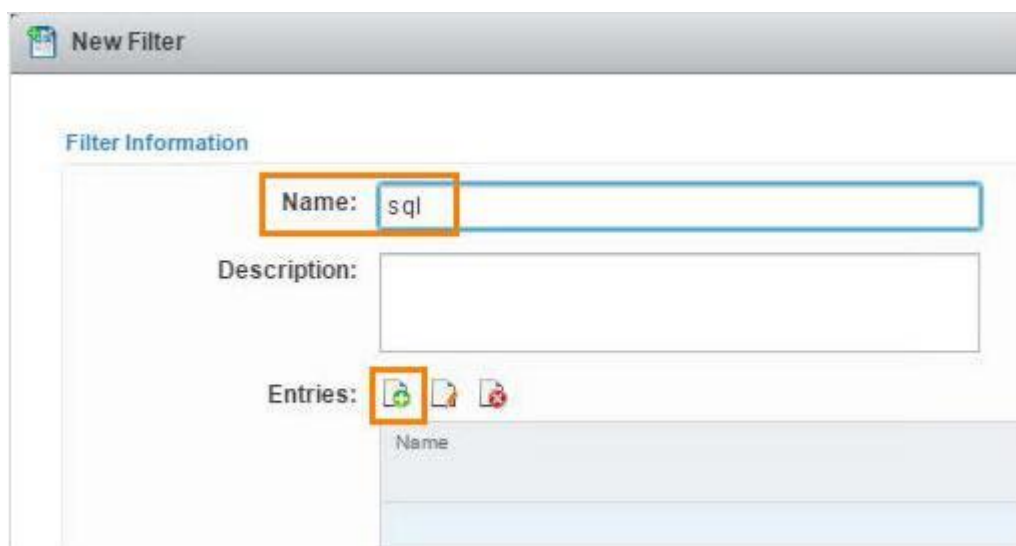


- b. 表示されたウィンドウで、[名前 (Name)] フィールドに **ApptoDB** と入力します。
- c. [+] をクリックして、フィルタを追加します。

- d. 表示されたウィンドウで、**dCloud** テナントを展開します。このテナントは空です。テナントをクリックします。
- e. [新しいフィルタの作成 (Create a new filter)] アイコンをクリックします。



- f. [名前(Name)] フィールドに **sql** と入力し、[エンtriesの追加 (Add Entry)] アイコンをクリックします。



- g. [名前(Name)] フィールドに **sql** と入力します。
- h. [ポート(Port)] フィールドに **1433** と入力します。
- i. 必要に応じ、[詳細モード(Advanced mode)] チェックボックスをオンにして、用意されているオプションを表示します。ただし、[OK] をクリックする前に、[詳細モード(Advanced mode)] チェックボックスをオフにしてください。
- j. [OK] をクリックします。

**New Entry**

Name:   Advanced mode

Protocol:

Port:   Any

- k. [OK] をクリックして、フィルタを追加します。
- l. **sql** フィルタが **dCloud** テナントに表示されます。このフィルタをクリックし、[利用可能なオブジェクト (Available objects)] 列から [追加するオブジェクト (Objects to add)] 列にドラッグします。
- m. [OK] をクリックします。

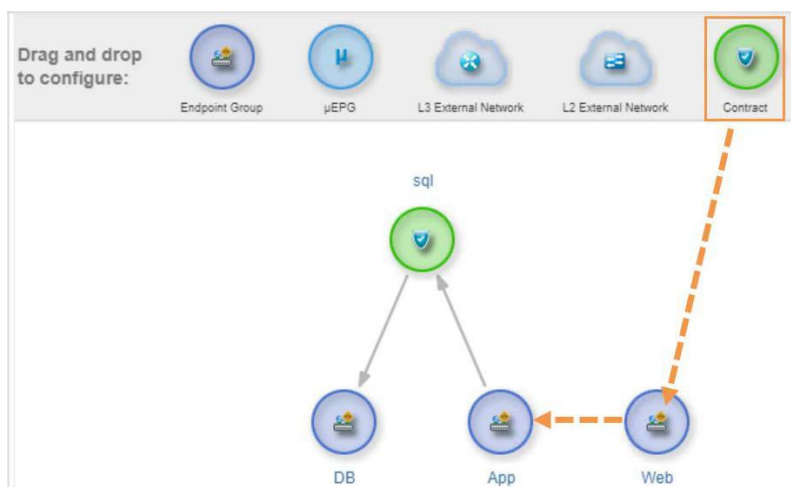


- n. [OK] をクリックして、**ApptoDB** コントラクトの作成を完了します。

15. 次の手順に従って、App 階層を Web 階層に接続する **WebtoApp** コントラクトを作成します。

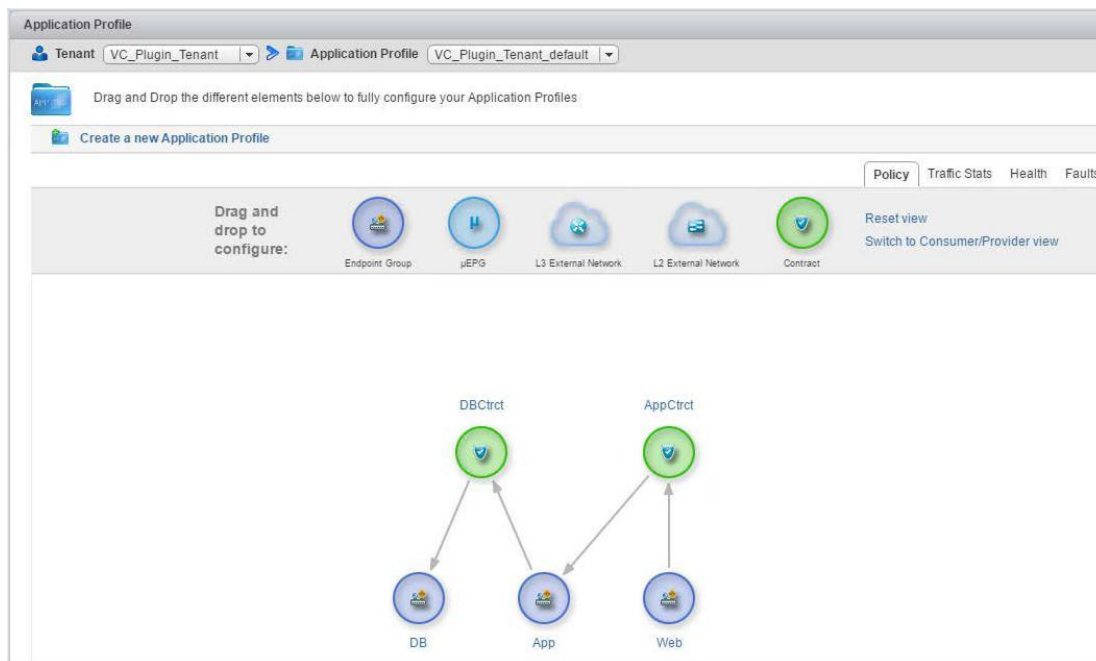
**注:** App 階層はプロバイダーとなり、Web 階層はこのコントラクトのコンシューマとなります。

- a. [コントラクト (Contract)] アイコンを作業ウィンドウにドラッグします。[Web] 階層上にドロップしてから、[App] 階層にマウスオーバーし、クリックします。



- b. 表示されたウィンドウで、[名前 (Name)] フィールドに **WebtoApp** と入力し、[OK] をクリックします。

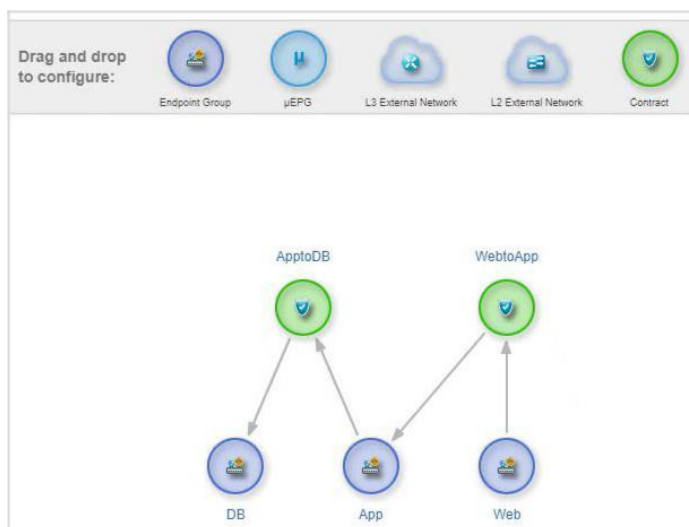
16. 作業ウィンドウでアプリケーショントポロジを確認します。矢印の方向は、各階層間のトラフィックの方向を示しています。



17. [コンシューマ/プロバイダービューに切り替える (Switch to Consumer/Provider view)] リンクをクリックして、トポロジのビューを変更します。



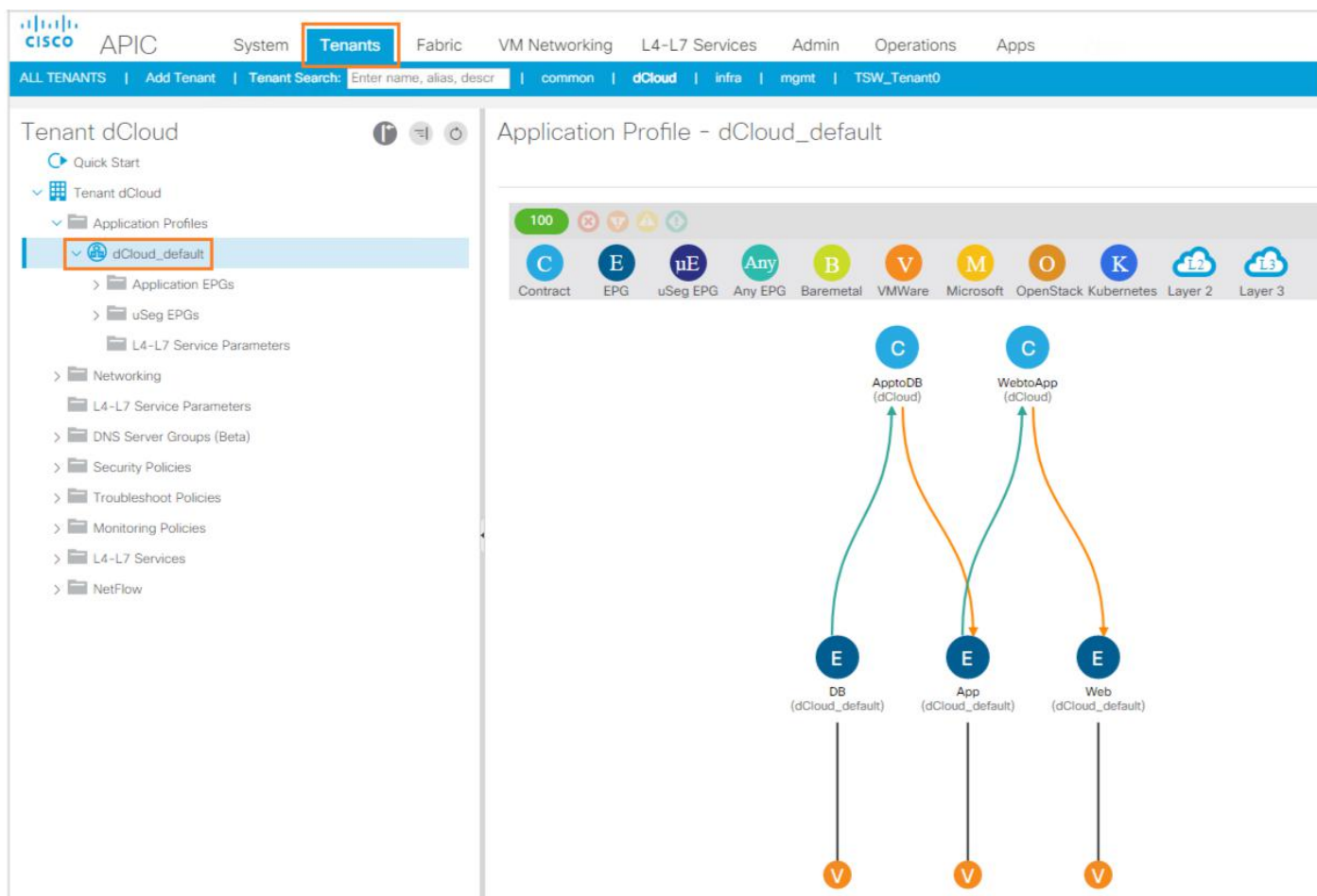
18. コンシューマ/プロバイダービューで、App 階層が **ApptoDB** のコンシューマであり、Web 階層が **WebtoApp** のコンシューマであることを確認します。必要に応じて、要素をドラッグ アンド ドロップします。



19. APIC ウィンドウに戻ります。または、APIC ウィンドウをまだ開いていない場合は開いてログインします (**admin/C1sco12345**)。
20. トップ メニューの [テナント(Tenants)] をクリックし、[dCloud] をダブルクリックします。

Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
common			2	3	0	100
dCloud		Created via VC Plug-in	1	1	6	100
infra			1	1	1	100
mgmt			1	2	0	100
TSW_Tenant0			2	1	5	98

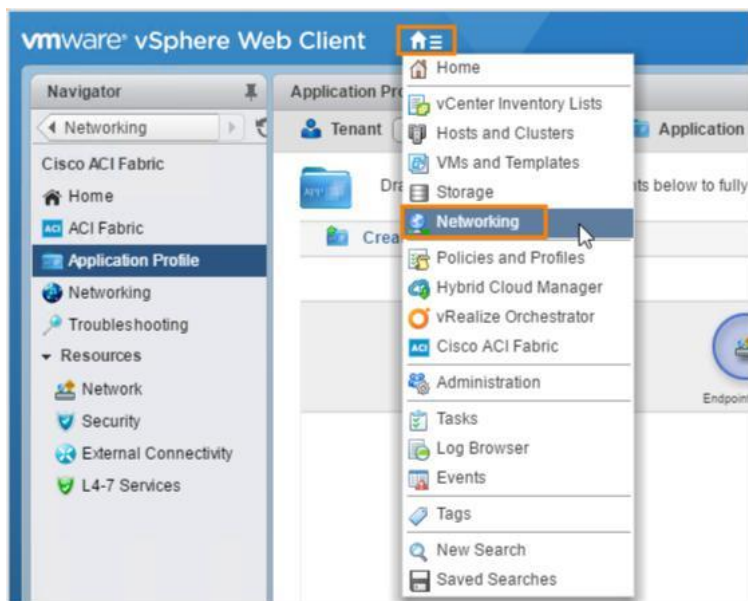
21. [テナント dCloud(Tenant dCloud)] > [アプリケーション プロファイル(Application Profiles)] を展開し、[dCloud\_default] をクリックして、新しく作成された 3 階層アプリケーションを APIC ウィンドウに表示します。



注: 必要に応じ、コントラクトをドラッグして、最もわかりやすい方法でトポロジを示してください。



22. [vSphere Web クライアント(vSphere Web Client)] タブに戻ります。
23. [ホーム(Home)] アイコンをクリックし、メニューから [ネットワーキング(Networking)] を選択します。



24. [vc1.dcloud.cisco.com] > [dCloud-DC] > [My-vCenter] > [My-vCenter] を展開し、新しく作成されたアプリケーション プロファイルの 3 つの階層に関連付けられた 3 つの新しいポートグループを表示します。

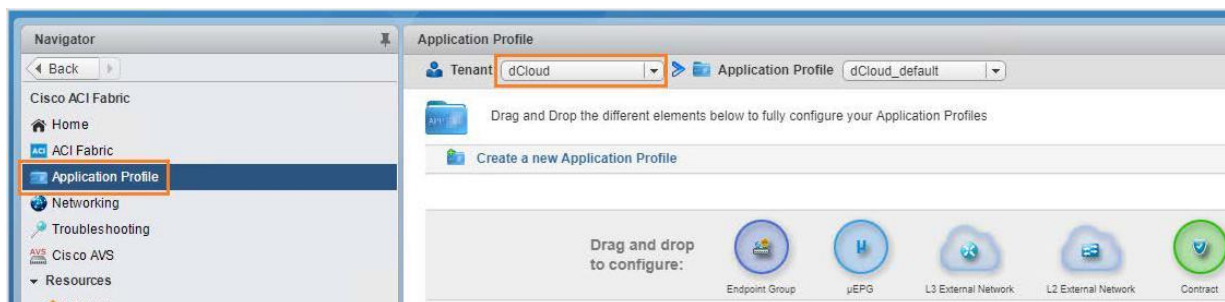


## シナリオ 3. L4-L7 サービスの追加

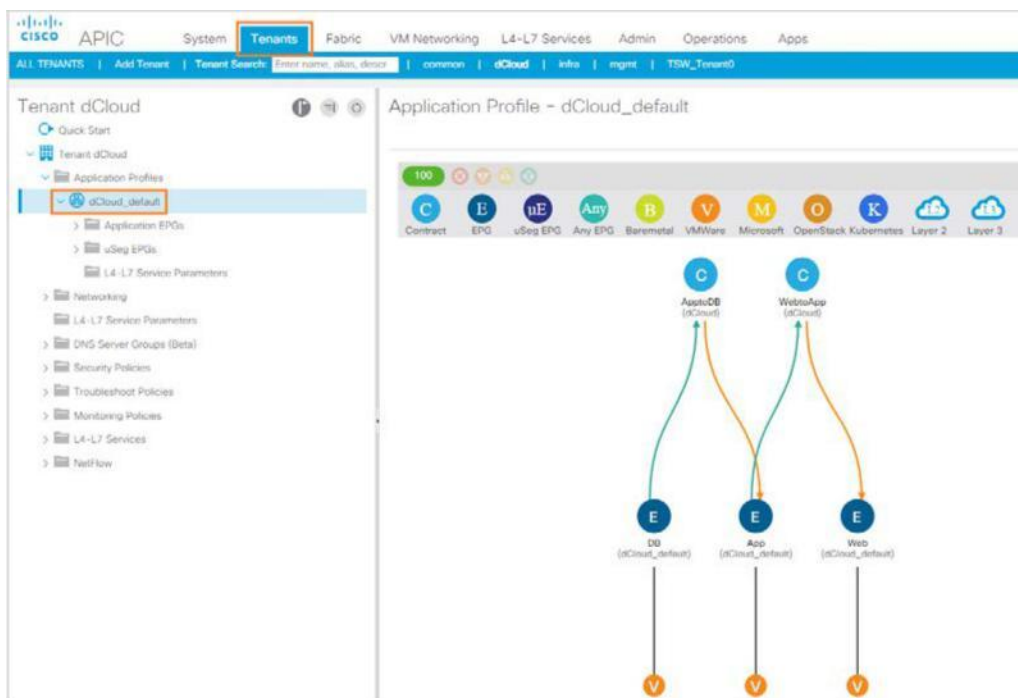
このシナリオでは、vCenter を使用して、common (共通) テナントに存在する L4-L7 サービスを前の手順で作成した dCloud テナントに追加します。

### 手順

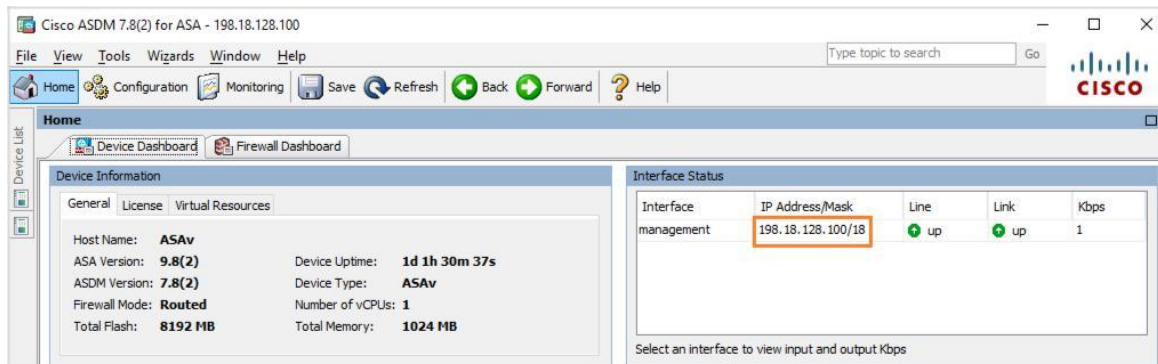
1. VMware vSphere Web クライアントで、[ホーム (Home)] ボタンをクリックします。または、アプリケーションがまだ実行されていない場合はログインします (**admin/C1sco12345**)。
2. [Cisco ACI ファブリック (Cisco ACI Fabric)] を選択します
3. 左側のメニューで [アプリケーション プロファイル (Application Profile)] をクリックします。[テナント (Tenant)] ドロップダウンに [dCloud] が表示されていることを確認します。



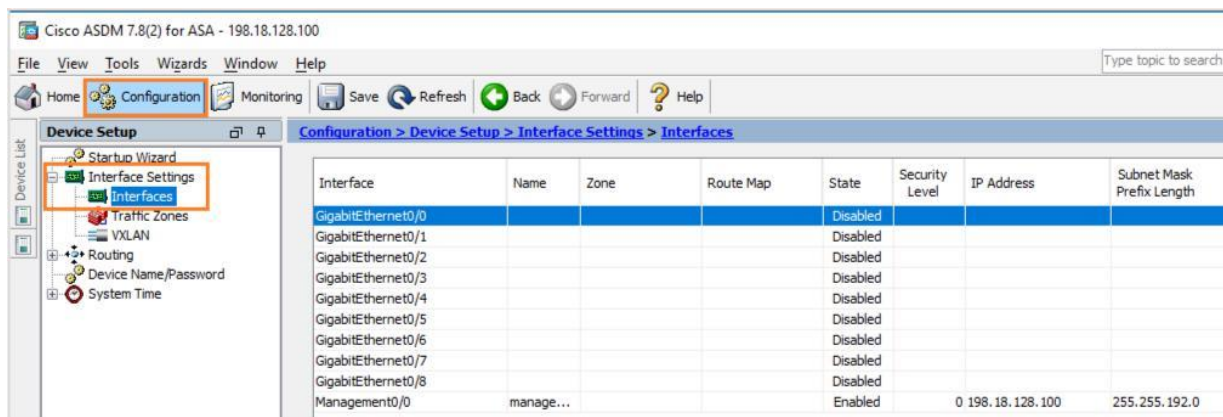
4. APIC をまだ開いていない場合はデスクトップ ショートカットを使用して APIC 3.0 にログインします (**admin/C1sco12345**)。
5. APIC ウィンドウで、[テナント (Tenants)] > [dCloud] > [アプリケーション プロファイル (Application Profiles)] をクリックし、[dCloud\_default] をクリックして、3 階層アプリケーションのトポロジを表示します。



6. デスクトップで **Cisco ASDM-IDM** のショートカットをダブルクリックします。ログインします (**admin/C1sco12345**)。Web サイトが信頼できないというメッセージが表示された場合は、[続行 (Continue)] を選択します。
7. **管理 IP** アドレスを確認します。



8. [設定 (Configuration)] をクリックします。
9. [インターフェイス設定 (Interface Settings)] > [インターフェイス (Interfaces)] をクリックして、基本デバイス上のインターフェイスは現在設定されているインターフェイスのみであることを確認します。



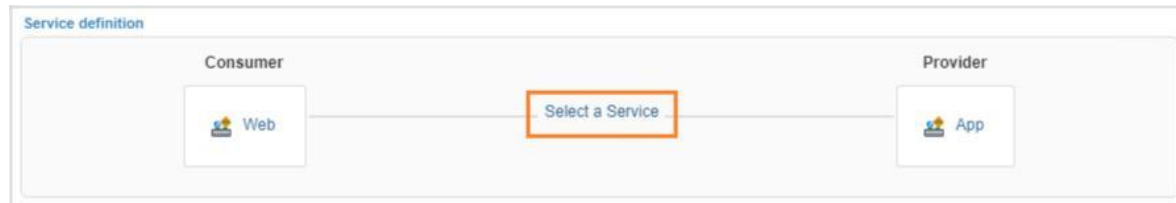
10. [vSphere Web クライアント (vSphere Web Client)] に戻ります。作業ウィンドウで、[WebtoApp] コントラクトを右クリックし、表示されたメニューで [設定の編集 (Edit Settings)] をクリックします。



11. [設定の編集(Edit Settings)] ウィンドウで、[L4-7 サービスを設定 (Configure L4-7 Service)] チェックボックスをオンにし、[次へ(L4-7 の設定) (Next (Configure L4-7))] をクリックします。

The screenshot shows the 'Edit Contract settings' window. It includes sections for 'Consumer / Provider', 'Contract Information', 'Traffic', and 'L4-7 Configuration'. In the 'L4-7 Configuration' section, the 'Configure L4-7 Service' checkbox is checked and highlighted with an orange box. At the bottom, the 'Next (Configure L4-7)' button is also highlighted with an orange box. Other elements include 'Consumers: Web', 'Providers: App', 'Name: WebtoApp', 'Description', 'Filters: default', 'Bidirectional: [checked]', and 'Tenant: ACI Fabric1, dCloud'.

12. [サービスの選択(Select a Service)] をクリックします。

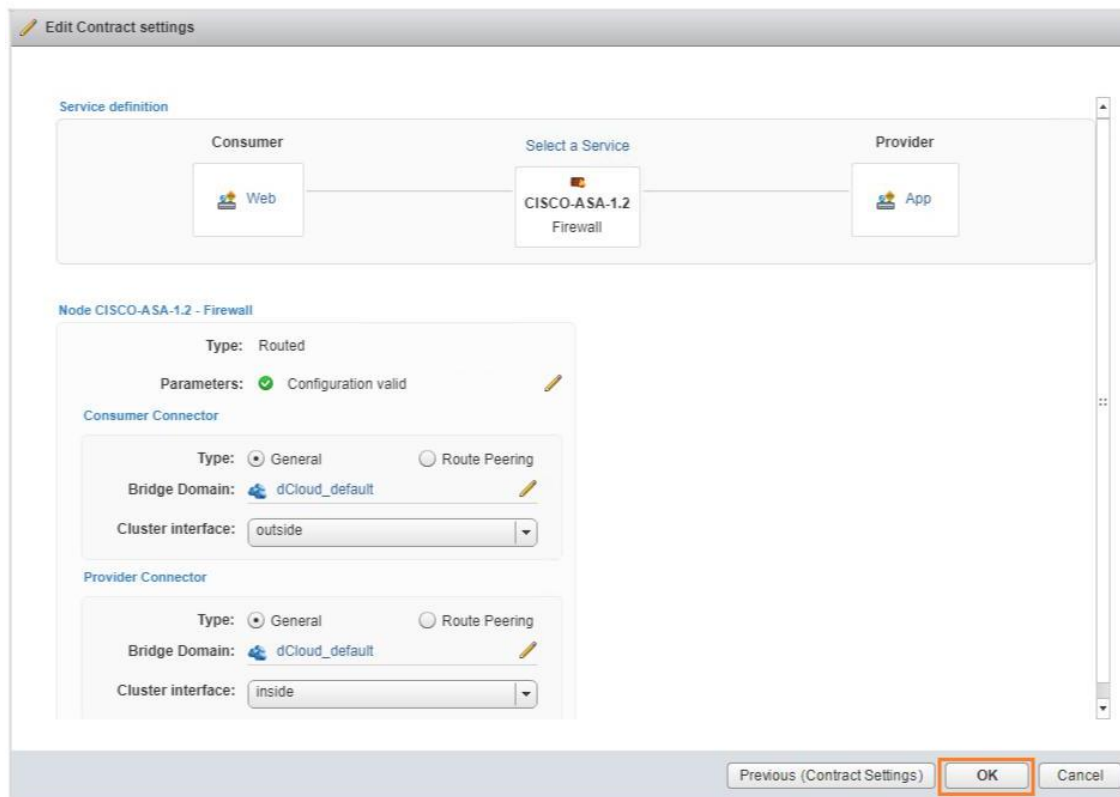


13. 表示されたウィンドウで、common テナントを展開し、[CISCO-ASA-1.2 ファイアウォール (CISCO-ASA-1.2 Firewall)] を選択します。

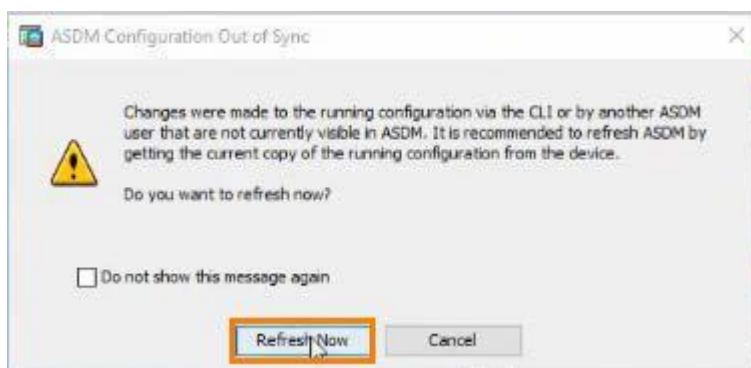
The screenshot shows the 'Select an object' window. It displays a table with columns for 'Template' and 'Services'. The table is expanded to show 'Tenant common' and 'Tenant dCloud'. The 'CISCO-ASA-1.2 Firewall' entry is highlighted with an orange box.

Template	Services
▼ Tenant common	
✓ L4-7 Device ASA_Srv_Graph	CISCO-ASA-1.2 Firewall
▶ Tenant dCloud	Created by VC Plug-in

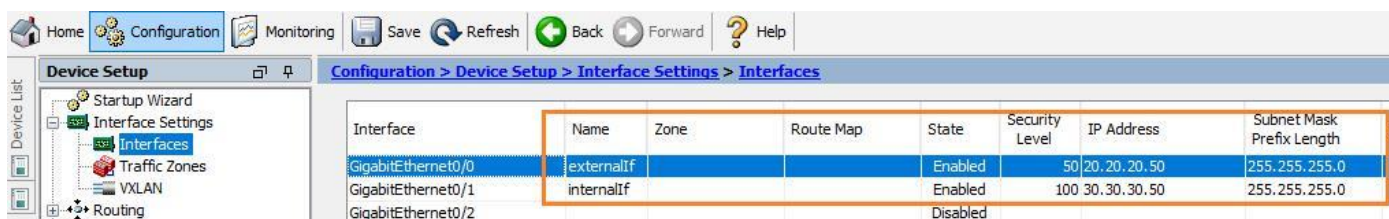
14. [OK] をクリックします。
15. 設定がロードされたら、何も変更せずに [OK] をクリックします。



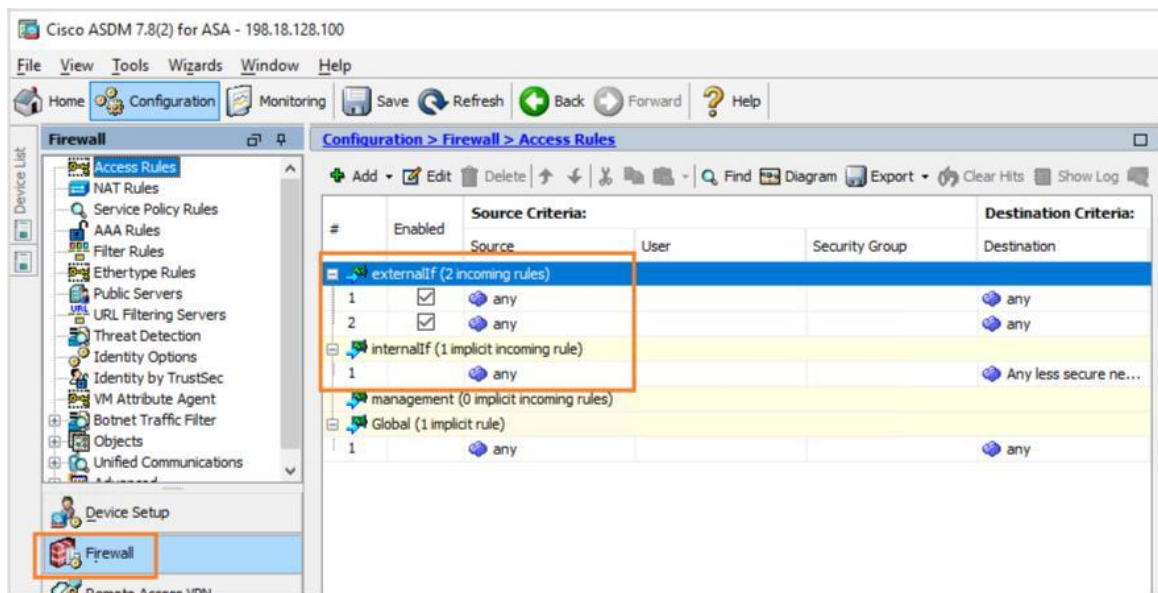
16. ASDM ウィンドウに戻ります。[設定が同期していません (Configuration Out Of Sync)] というダイアログボックスがポップアップ表示されます。
17. [今すぐ更新 (Refresh Now)] をクリックします。



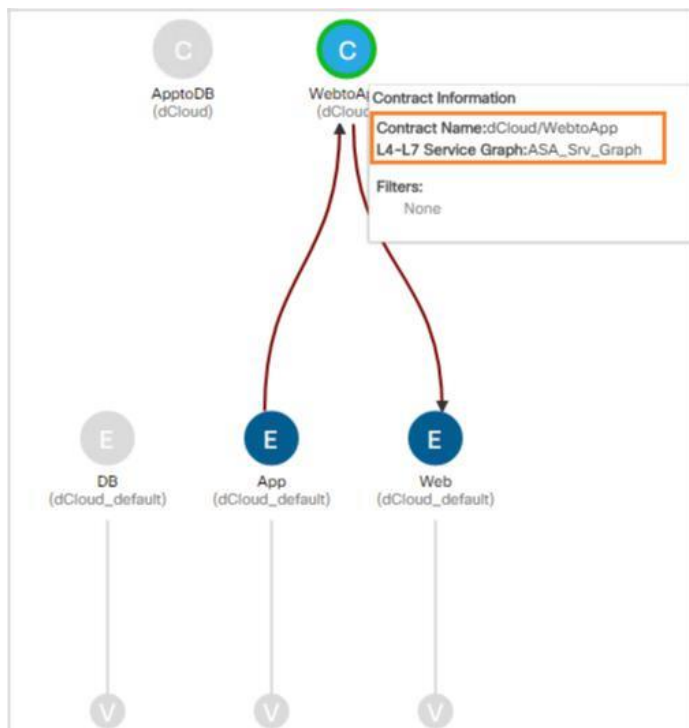
18. [インターフェイス ステータス (Interface Status)] ウィンドウに表示される内部 (internal) インターフェイスと外部 (external) インターフェイスを確認します。
19. [設定 (Configuration)] タブをクリックし、2 つの新しいインターフェイスがデバイスにも表示されることを確認します。



20. サイドメニューの [ファイアウォール (Firewall)] タブをクリックして、Cisco ASA 1.2 ファイアウォールで内部インターフェイスと外部インターフェイスを表示します。



21. APIC 3.0 ウィンドウに戻り、更新します。
22. [WebtoApp] コントラクトを 1 回クリックして、[ASA\_Srv\_Graph] がコントラクトに追加されたことを示します。

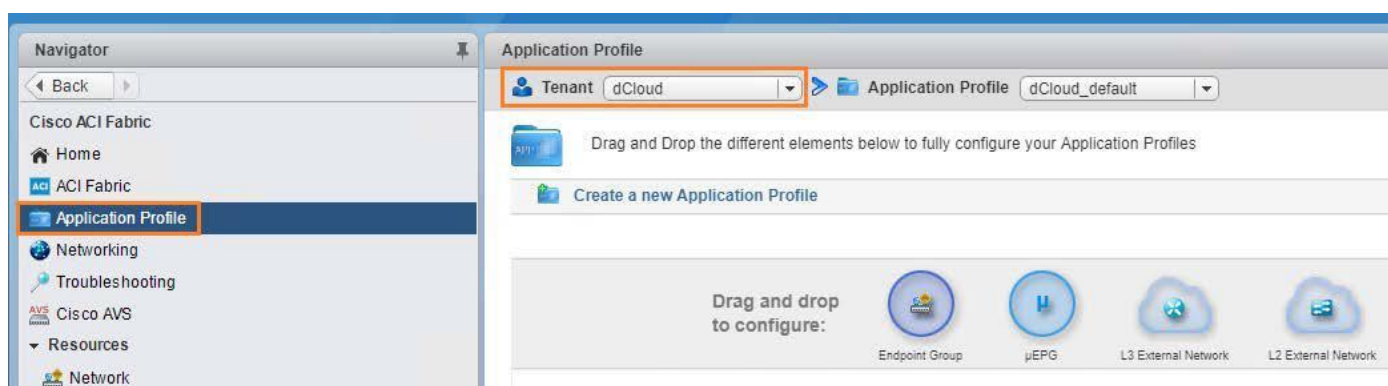


## シナリオ 4. L3 外部接続の追加

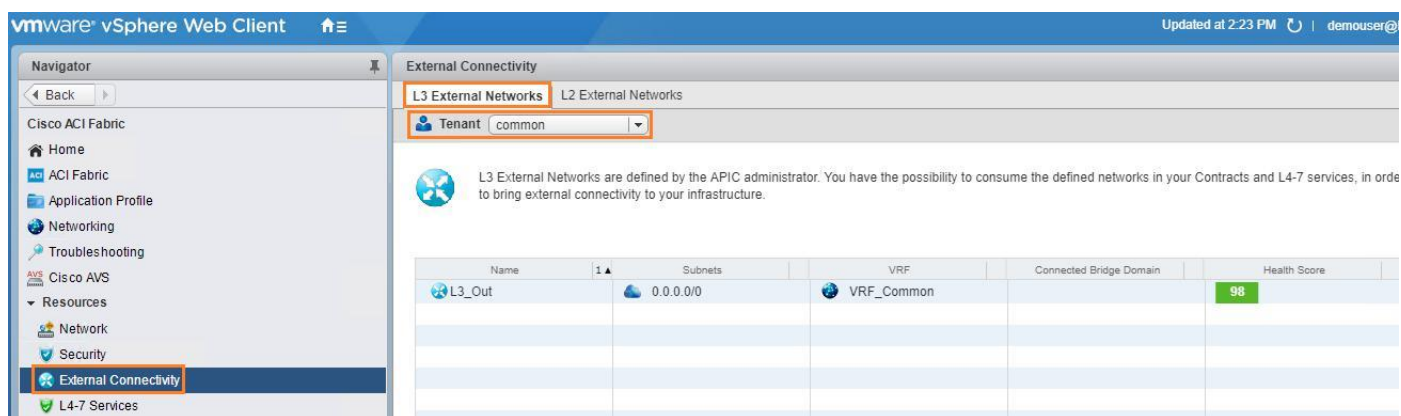
このシナリオでは、VMware vSphere Web Client を使用して L3 サービスを VC\_Plugin\_Tenant テナントに追加し、アプリケーションの Web EPG からインターネットに接続できるようにします。

### 手順

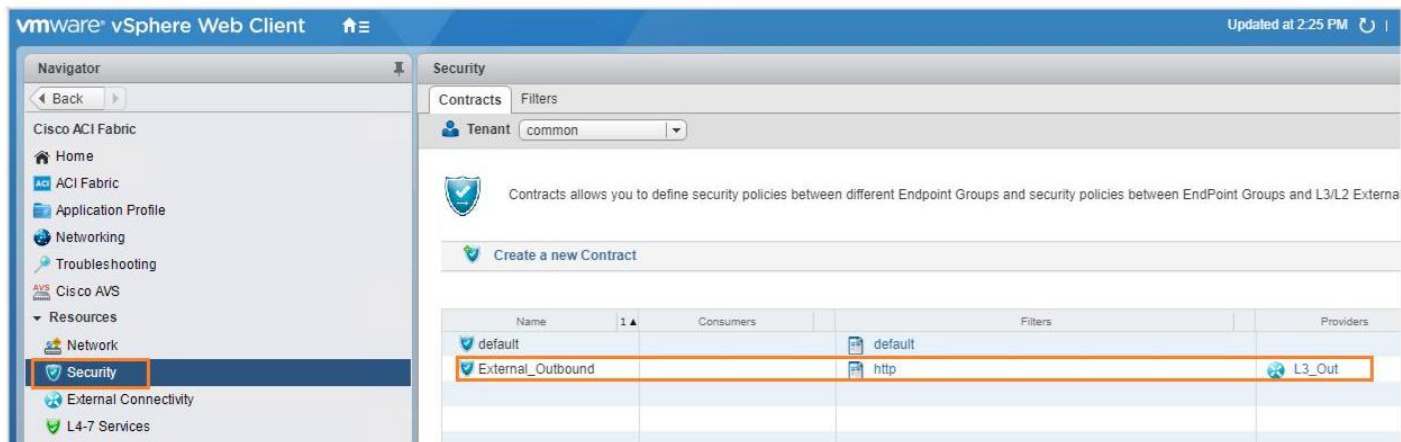
1. **VMware vSphere Web クライアント**をまだ開いていない場合は開いて ([Windows セッションの認証を使用する (Use Windows session credentials)])、[Cisco ACI ファブリック (Cisco ACI Fabric)] をクリックします。
2. 左側のメニューで [アプリケーション プロファイル (Application Profile)] をクリックします。[テナント (Tenant)] ドロップダウンに [dCloud] が表示されていることを確認します。



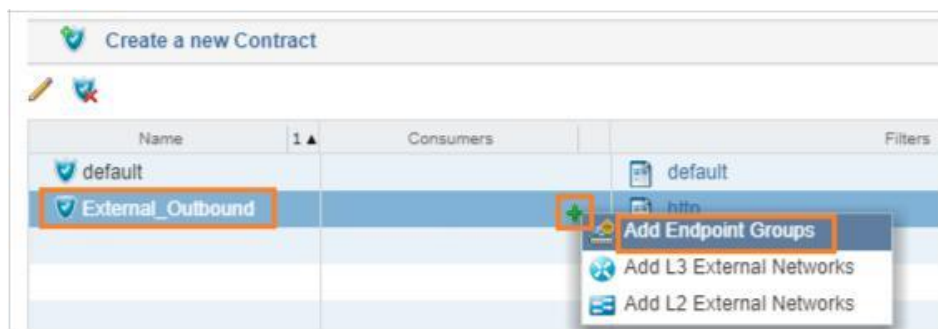
3. サイドメニューの [外部接続 (External Connectivity)] をクリックします。
4. [L3 外部ネットワーク (L3 External Networks)] タブで、[テナント (Tenant)] ドロップダウンから [common] を選択して、common テナントの L3 接続パラメータを表示します。



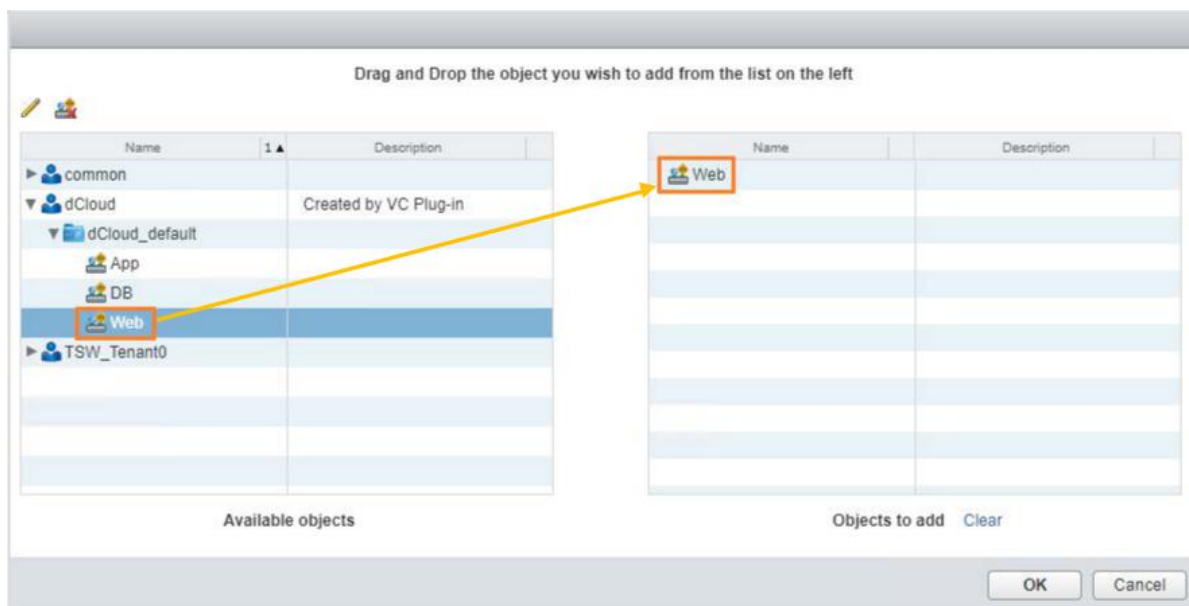
5. サイドメニューで、[セキュリティ (Security)] をクリックします。コントラクト タブで、[External\_Outbound] コントラクトが [common] テナントの [L3\_Out] を使用していることを確認します。



6. [External\_Outbound] コントラクトをクリックします。
7. [+] が有効になったらクリックし、表示されたメニューから [エンドポイント グループの追加 (Add Endpoint Groups)] を選択します。



8. [dCloud] > [dCloud\_default] を展開し、[Web] EPG を [利用可能なオブジェクト (Available objects)] リストから [追加するオブジェクト (Objects to add)] リストにドラッグします。





9. [OK] をクリックします。
10. [External\_Outbound] コントラクトが更新されて、[dCloud/Web] EPG がコンシューマとして表示されます。

Create a new Contract				
Name	1 ▲	Consumers	Filters	Providers
default			default	
External_Outbound		dCloud/Web	http	L3_Out

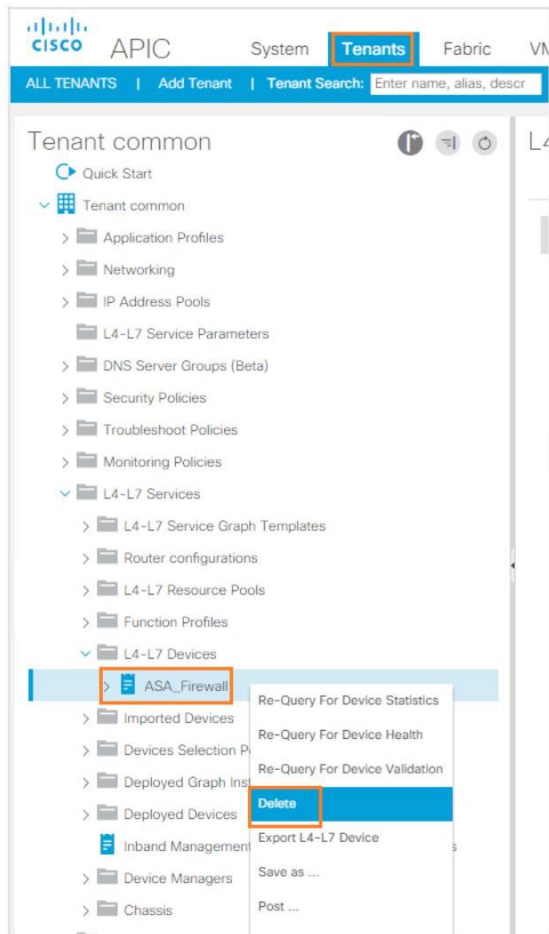
11. 左側のメニューで [アプリケーション プロファイル (Application Profile)] をクリックします。[テナント (Tenant)] ドロップダウンで [dCloud] が選択されていることを確認します。
12. トポロジに L3 接続が追加されていることがわかります。要素をドラッグして移動し、トポロジの表示が最適になるようにします。



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

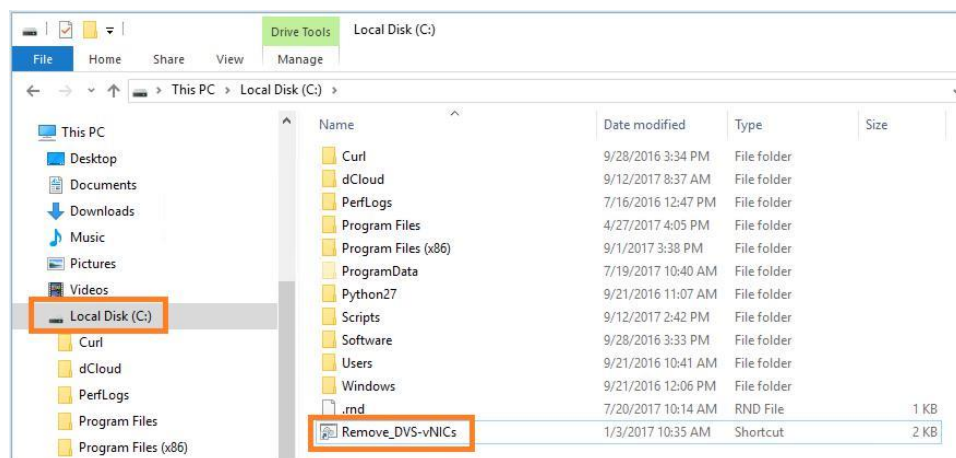
このデモの 2 つ目のスクリプト (*Cisco Application Policy Infrastructure Controller 3.0 with VMware – Network Admin*) に進むには、まず次の手順を実行して、common テナントから ASA ファイアウォール デバイスを削除してください。

1. APIC ウィンドウのトップ メニューで、[テナント (Tenants)] をクリックします。
2. [テナント common (Tenant common)] > [L4-L7 サービス (L4-L7 Services)] > [L4-L7 デバイス (L4-L7 Devices)] に移動し、[ASA\_Firewall] を右クリックします。
3. メニューから [削除 (Delete)] を選択します。



4. 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。

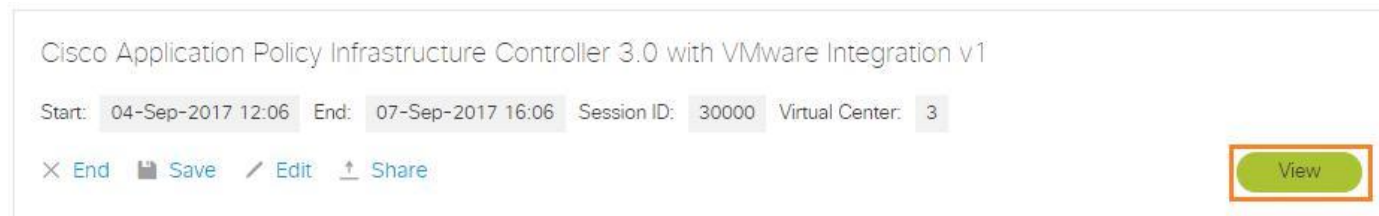


5. 削除スクリプトが実行され、シェル ウィンドウに結果が表示されます。スクリプトが完了すると、シェル ウィンドウが閉じます。

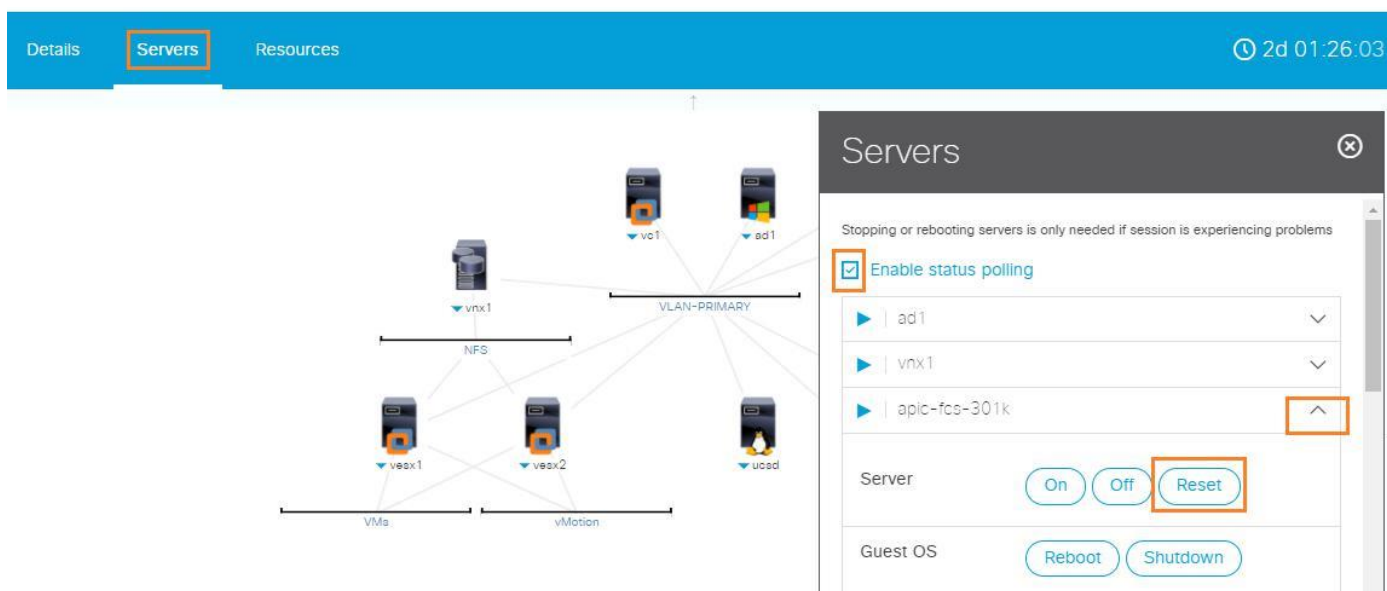
## 付録 A. APIC シミュレータのリセット

APIC ファブリック メンバーはデフォルトで作成されるため、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)をリポートしてください。

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 リポートが実行されます。この操作では、リポート後に設定は保持されないため、クリーン リポ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 **Fix My Demo** をクリックします。
2. 修正する項目を選択します。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