Cisco ACI vCenter プラグイン

この章は、次の内容で構成されています。

Cisco ACI と VMware vSphere Web クライアントについて

Cisco ACI vCenter プラグインは、vSphere Web クライアント内から ACI ファブリックを管理することを可能にするユーザ インターフェイスです。

これにより、VMware vSphere Web クライアントから VMware vCenter と ACI ファブリックの両方を一括管理することが可能になります。

Cisco ACI vCenter プラグインを使えば、仮想化管理者は、同じインフラストラクチャを共有しながら、ネットワーキング チームから独立して、ネットワークの接続性を定義することが可能になります。

詳細なネットワークの構成は、Cisco ACI vCenter プラグインの対象ではありません。仮想化管理者と直接関連する要素だけが表示されます。

Cisco APIC リリース 6.0(3) 以降、VMM ドメインは VMware vSphere 8.0 をサポートしています。ただし、vSphere 8.0 は vCenter プラグインをサポートしていません。 vCenter プラグインを使用する必要がある場合は、vSphere 7.0 を使用してください。

Cisco ACI vCenter プラグインの概要

VMware vSphere Web クライアント用の Cisco Application Centric Infrastructure(ACI) vCenter プラグインは、GUI に Cisco ACI ファブリックと呼ばれる新しいビューを追加します。

Cisco Application Centric Infrastructure(ACI) vCenter プラグインは、ACI と vCenter との既存の統合は変更しませんが、EPG、uSeg EPG、契約、テナント、VRF、および VMware vSphere Web クライアントからのブリッジ ドメインを設定することができます。

Cisco Application Centric Infrastructure(ACI) vCenter プラグインはステートレスで、すべてを Application Policy Infrastructure Controller(APIC) から取得しますが、情報は一切保存しません。

Cisco ACI vCenter プラグインによって提供される機能の簡単な概要を次に示します:

詳細については、Cisco ACI vCenter プラグインの機能と制約事項 （9 ページ）を参照してください。

Cisco ACI vCenter プラグインでは、ACI ファブリックで次のオブジェクトの作成、読み取り、更新および削除 (CRUD) を行うことができます:

- テナント
- アプリケーション プロファイル
- EPG / uSeg EPG
- 契約
- VRF
- ブリッジ ドメイン

Cisco ACI vCenter プラグインは、L2 および L3 Out の使用に関する、より限定された操作も提供します。すべての高度な設定は、APIC でも前もって行っておく必要があります。

- 事前設定された L2 および L3 Out は、契約のプロバイダまたはコンシューマとして使用できます。
- 作成、編集、または削除は行えません。

Cisco ACI vCenter プラグインではまた、契約に既存のグラフ テンプレートを適用して、事前設定された L4 ～ L7 サービスを利用することもできます。

- グラフの既存のテンプレートを使用できませす。作成はできません。
- 機能プロファイルのうち、必須であるのに空のパラメータだけが表示され、設定できます。

Cisco ACI vCenter プラグインには、トラブルシューティングの機能もあります:

- エンドポイントからエンドポイントへのセッション(障害、監査、イベント、統計、契約、Traceroute)

Cisco ACI vCenter プラグインを開始する

Cisco ACI vCenter プラグイン ソフトウェアの要件

Cisco ACI vCenter プラグイン ソフトウェアの要件は次のとおりです:

プラットフォーム シリーズ	推奨リリース
vCenter	Cisco APIC は、VMware がサポートする Linux アプライアンスと Windows サーバの任意のバージョンをサポートします。詳細は、VMware のマニュアルを参照してください。
Application Policy Infrastructure Controller（APIC）	リリース 3.2(2) 以降

必要な APIC の設定

このセクションでは、必要な APIC 設定について説明します。

APIC と、プラグインがインストールされる vCenter の間には、少なくとも 1 つの VMM ドメインがすでに存在している必要があります。

詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

Cisco ACI vCenter プラグインのインストール

このセクションでは、Cisco Application Centric Infrastructure（ACI）vCenter プラグインのインストール方法について説明します。 VMware vCenter と Cisco Application Policy Infrastructure Controller（APIC）の間でHTTPS トラフィックが機能している必要があります。これは、VMware vCenter がプラグインを Cisco APIC から直接ダウンロードするためです。

VMware vCenter と Cisco APIC の間の HTTPS トラフィックを有効にできず、独自の Web サーバを使用して Cisco ACI vCenter プラグインの zip ファイルをホストする場合は、Cisco ACI vCenter プラグインの代替インストール （41 ページ） を参照してください。

VMware vCenter 5.5（更新 3e 以降）または vCenter 6.0（更新 2 以降）を使用している場合は、このセクションの手順に従ってください。vCenter 5.5 または 6.0 より前のリリースを使用している場合は、Cisco ACI vCenter プラグインの代替インストール （41 ページ） を参照してください。

プラグインをインストールするには、vCenter が Web サーバからプラグインをダウンロードする必要があります。次の手順では、Cisco APIC が Web サーバとして使用され、VMware vCenter が Cisco APIC からプラグインを直接ダウンロードします。

vCenter 5.5 更新 3e または vCenter 6.0 更新 2 より前のバージョンでは、vCenter は HTTPS 通信に TLSv1 を使用していましたが、現在は廃止されています。セキュリティ上の理由から、Cisco APIC は TLSv1.1 と TLSv1.2 のみをサポートしているため、vCenter は Cisco APIC からプラグインをダウンロードできません。プラグインは、TLSv1 を許可し、または HTTPS を使用しない独立した Web サーバに配置する必要があります。

（注） VMware vCenter 6.7 からログアウトしてから再度ログインすると、vCenter プラグイン アイコンが表示されない場合があります。その場合は、Cookie と履歴を消去するか、別のブラウザを使用してログインしてください。

始める前に

- すべての前提条件を満たしていることを確認します。

  詳細については、Cisco ACI vCenter プラグイン ソフトウェアの要件 （3 ページ）および必要な APIC の設定 （3 ページ）のセクションを参照してください。

- vCenter サーバと APIC の間で HTTPS トラフィックが許可されることを確認します。
- VMware vCenter 6.7 の Cisco ACI vCenter プラグインをインストールする場合は、PowerCLI バージョン 11.2.0 以降が必要です。

（注） インストール中に、コンソールに次のエラーが表示される場合があります。

エラー：無効なサーバ証明書。`Set-PowerCLIConfiguration` を使用して、`InvalidCertificationAction` オプションの値をプロンプトに設定し、`1` 回接続するか、このサーバに永続的な例外を追加します。

このエラーが表示されないようにするには、インストール前に次のコマンドを入力します。**`Set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Confirm:$false`**

手順

ステップ 1 次の URL にアクセスします:

例：

`https://`<*APIC*>**`/vcplugin`**

ステップ 2 Web ページの指示に従って作業を行います。

Cisco ACI vCenter プラグインを Cisco ACI ファブリックに接続する

このセクションでは、Cisco Application Centric Infrastructure ファブリックに Cisco ACI（ACI）vCenter プラグインを接続する方法について説明します。

（注）
- 登録は VMware vCenter 全体で行われ、それを実行するユーザーは考慮されません。これは、それを実行するログイン ユーザーだけでなく、VMware vCenter 全体の構成です。
- Role Based Access Control（RBAC）は、登録時に使用するクレデンシャルに基づくものです。登録に使用する Cisco Application Policy Infrastructure Controller（APIC）アカウントのパーミッションにより、Cisco ACI vCenterプラグインの構成制限を定義します。

次のいずれかの方法を使用して、プラグインを Cisco ACI ファブリックに接続できます。

資格情報を使用して Cisco ACI vCenter プラグインを Cisco ACI ファブリックに接続します。	詳細については、資格情報を使用して vCenter プラグインを Cisco ACI ファブリックに接続する （5 ページ） を参照してください。
既存の証明書を使用して、Cisco ACI vCenter プラグインを Cisco ACI ファブリックに接続します。	詳細については、既存の証明書を使用して vCenter プラグインを ACI ファブリックに接続する （6 ページ） を参照してください。
新しい証明書を作成して、Cisco ACI vCenter プラグインを Cisco ACI ファブリックに接続します。	詳細については、「新しい証明書の作成により、vCenter プラグインを ACI ファブリックに接続する （7 ページ）」を参照してください。

資格情報を使用して vCenter プラグインを Cisco ACI ファブリックに接続する

このセクションでは、資格情報を使用して Cisco Application Centric Infrastructure（ACI）vCenter プラグインを Cisco ACI ファブリックに接続する方法について説明します。

始める前に

Cisco ACI vCenter プラグインがインストールされていることを確認します。詳細については、Cisco ACI vCenter プラグインのインストール （3 ページ） を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[Cisco ACI ファブリック]** を選択します。

ステップ 3 **Getting Started** ペインで、**Connect vSphere to your ACI Fabric** を選択します。

ステップ 4 **[新しい ACI ファブリックの登録]** ダイアログ ボックスで **[はい]** をクリックして、新しい ACI ファブリックを登録します。

ステップ 5 **Register a new APIC Node** ダイアログボックスで、次の操作を実行します:

a) **IP/FQDN** フィールドに、IP アドレスまたは完全修飾ドメイン名(FQDN) を入力します。

b) **[証明書の使用（Use Certificate）]** フィールドで、Cisco Application Policy Infrastructure Controller（APIC）認証を使用するには、[証明書の使用] チェック ボックスをオンにしないでください。

c) **[ユーザー名]** フィールドにユーザー名を入力します（admin）。

d) [Password] フィールドにパスワードを入力します。

e) [OK] をクリックします。

ステップ 6 **[情報]** ダイアログ ボックスで、**[OK]** をクリックします。

Cisco APIC ノードが Cisco ACI ファブリックに正常に追加されました。

ステップ 7 **[ACI ファブリック]** ペインで、新しく登録された Cisco APIC でその他の Cisco APIC を検出したことが表示されますs。

Cisco ACI vCenter プラグインは、常に要求に単一の Cisco APIC を使用します。ただし、現在使用している Cisco APIC が使用できなくなった場合は Cisco APIC を切り替えます。

（注）
Cisco ACI vCenter プラグインを使用した Cisco ACI ファブリックの登録は、リモート ユーザーにはサポートされていません。

既存の証明書を使用して vCenter プラグインを ACI ファブリックに接続する

このセクションでは、既存の証明書を使用して、vCenter プラグインを ACI ファブリックに接続する方法について説明します。

始める前に

- 証明書はすでに管理者ユーザが使用できるよう APIC で設定されています。
- 証明書の名前と秘密キーを取得しています。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[Cisco ACI ファブリック]** を選択します。

ステップ 3 **Getting Started** ペインで、**Connect vSphere to your ACI Fabric** を選択します。

ステップ 4 **Register a new ACI Fabric** ダイアログボックスで **Yes** をクリックして、新しい ACI ファブリックを登録します。

ステップ 5 **Register a new APIC Node** ダイアログボックスで、次の操作を実行します:

a) **IP/FQDN** フィールドに、IP アドレスまたは完全修飾ドメイン名(FQDN) を入力します。

b) **Use Certificate** フィールドで **Use Certificate** チェック ボックスをオンにします。

ステップ 6 **Action** セクションで **Use an existing certificate** を選択します。

ステップ 7 **Name** フィールドに証明書名を入力します。

ステップ 8 **Private Key** セクションに、証明書の秘密キーをペーストします。

ステップ 9 **Check Certificate** をクリックします。

ステータスは [Connection Success] に切り替わります。

（注）
接続エラーが表示された場合には、証明書の名前と秘密キーが正しいか確認して、もう一度やり直してください。

ステップ 10 [OK] をクリックします。

ステップ 11 **Information** ダイアログボックスで、**OK** をクリックします。
APIC ノードは、ACI ファブリックに正常に追加されました。

ステップ 12 **ACI Fabric** ペインでは、新たに登録した APIC が、他の APIC を検出します。

Cisco ACI vCenter プラグインは常に、リクエストのため、単一の APIC を使用します。現在使用中の APIC が利用できなくなった場合には、Cisco ACI vCenter プラグインは APIC を切り替えます。

新しい証明書の作成により、vCenter プラグインを ACI ファブリックに接続する

このセクションでは、新しい証明書を作成することにより、vCenter プラグインを ACI ファブリックに接続する方法について説明します。

始める前に

- プラグインがインストールされていることを確認します。
- APIC 管理者のクレデンシャルに対するアクセス権があります。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[Cisco ACI ファブリック]** を選択します。

ステップ 3 **Getting Started** ペインで、**Connect vSphere to your ACI Fabric** を選択します。

ステップ 4 **Register a new ACI Fabric** ダイアログボックスで **Yes** をクリックして、新しい ACI ファブリックを登録します。

ステップ 5 **Register a new APIC Node** ダイアログボックスで、次の操作を実行します:

a) **IP/FQDN** フィールドに、IP アドレスまたは完全修飾ドメイン名(FQDN) を入力します。
b) **Use Certificate** フィールドで **Use Certificate** チェック ボックスをオンにします。

ステップ 6 **Action** フィールドで、**Generate a new certificate** を選択します。

ステップ 7 [Name] フィールドに新しい証明書の名前を入力します。

ステップ 8 **Generate certificate** ぼたんをクリックします。

ステップ 9 表示された証明書をコピーします。

コピーが必要なのは、-----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- までで、これらの行も含めます。

ステップ 10 この証明書を APIC 内の管理者ユーザに追加します。同じ証明書名を使用していることを確認してください。

a) APIC GUI に admin としてログインします。
b) メニュー バーで、**Admin** を選択します。
c) **Navigation** ペインで、**Security Management** > **Local Users** > **admin** を展開します。
d) **Work** ウィンドウの **User Certificate** セクションで、プラスのアイコンをクリックして証明書を追加します。
e) **Name** フィールドに証明書名を入力します。
f) **Data** フィールドに、手順 8 でコピーした証明書の内容をペーストします。
g) [Submit] をクリックします。

ステップ 11 vCenter プラグインで、**Check Certificate** をクリックします。

ステータスは [Connection Success] に変わります。

（注）
接続エラー メッセージが表示された場合には、証明書が APIC に正しく追加されていること、証明書名が同じであることを確認します。

ステップ 12 [OK] をクリックします。

ステップ 13 **Information dialog** ボックスで、**OK** をクリックします。
APIC ノードは、ACI ファブリックに正常に追加されます。

ステップ 14 **ACI Fabric** ペインでは、新たに登録した APIC が、他の APIC を検出します。

Cisco ACI vCenter プラグインは常に、リクエストのため、単一の APIC を使用します。現在使用中の APIC が利用できなくなった場合には、Cisco ACI vCenter プラグインは APIC を切り替えます。

Cisco ACI vCenter プラグインの機能と制約事項

このセクションでは、管理するすべてのオブジェクト タイプに対して、Cisco ACI vCenter プラグインで提供される可能な操作について説明します。また、意図的な設定制限が課されます。

オブジェクトに関する詳細情報については、「*Cisco Application Centric Infrastructure Fundamentals*」を参照してください。

テナント

Cisco ACI vCenter プラグインは、テナント オブジェクトで CRUD 操作を使用できます。次の属性はプラグインで公開されます。

- [Name]：テナントの名前。
- Description (Optional)：テナントの説明です。

テナントがプラグインで作成される場合、VRF に接続されている VRF *tenant_name*>_default とブリッジ ドメイン< *tenant_name* >_default は、内部で自動的に作成されます。アプリケーション プロファイル <*tenant_name*>_default は、内部で作成されます。

インフラストラクチャテナント（インフラ）および管理テナント（管理）は、プラグインで公開されていません。

（注） プラグインにACIファブリックを登録中、プラグインで表示されるテナントは使用されるアカウントに関連付けられている権限によって異なります。

Application Profiles

Cisco ACI vCenter プラグインは、アプリケーション プロファイル オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：アプリケーション プロファイルの名前。
- Description (Optional)：アプリケーションプロファイルの説明です。

エンドポイント グループ

Cisco ACI vCenter プラグインは、エンドポイント グループ オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：エンドポイント グループの名前。
- Description (Optional)：エンドポイント グループの説明です。
- ブリッジ ドメイン：このエンドポイントのグループに関連付けられているブリッジ ドメイン。

- EPG 内分離：これにより、EPG に接続されている仮想マシン間のすべてのトラフィックを拒否します。デフォルトでは、同じEPGのすべての仮想マシンは互いに通信できます。
- 分散型スイッチ：EPG が展開されている DVS/Cisco AV。これは、ACI の VMM ドメインの関連付けに対応しています。

  デフォルトでは、プラグインで作成されたすべての EPG は、プラグインが使用されている vCenter を指す VMM ドメインに関連付けられています。同じ vCenter を指す複数の VMM ドメインがある場合は、EPG を展開する DVS で選択された形式で少なくとも 1 つ選択する必要があります。

マイクロセグメンテーションの許可（Cisco AV ではなく DVS のみ)：これにより、「ベース EPG」を作成できます。この EPG に接続されているすべての仮想マシンは、uSeg EPG の「マイクロセグメンテーション」ルールを適用するための候補です。マイクロセグメントEPGルールは、「ベース EPG」に接続されている仮想マシンにのみ適用されます。

（注） すべて EPG は、分散型のスイッチが Cisco AV の場合ベース EPG として見なされます。

使用されるプラグインが「仮想」として表示される vCenter を指す VMM ドメインに、EPG がリンクされています。その他の EPG は「物理」として表示されます。

アクションの更新と削除は、vCenter（仮想）を指しているVMMドメインにリンクされているEPG にのみ許可されます。他の EPG（物理）は読み取り専用です。VMM ドメインに関係なく、更新は EPG がコントラクトの消費または提供を行うように許可されています。

uSeg EPG

Cisco ACI vCenter プラグインは、マイクロセグメント EPG オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：マイクロセグメント EPG の名前。
- Description (Optional)：マイクロセグメント EPG の説明です。
- ブリッジ ドメイン：このマイクロセグメント EPG に関連付けられているブリッジ ドメイン。
- EPG 内分離：これにより、EPG に接続されている仮想マシン間のすべてのトラフィックを拒否します。デフォルトでは、同じEPGのすべての仮想マシンは互いに通信できます。
- 分散型スイッチ：EPG が展開されている DVS/Cisco AV。これは、ACI の VMM ドメインの関連付けに対応しています。

  デフォルトでは、プラグインで作成されたすべての EPG は、プラグインが使用されている vCenter を指す VMM ドメインに関連付けられています。同じ vCenter を指す複数の VMM ドメインがある場合は、EPG を展開する DVS で選択された形式で少なくとも 1 つ選択する必要があります。

- Miroセグメンテーションの属性：このマイクロセグメントEPGに属数VMを決定するルールのリスト。ルールのオプションには、IP、MAC、VM名、OS、ホスト、VM id、VNic、ドメイン、データ センタ、カスタム属性を含みます。

（注） ドメイン属性（VMM ドメイン）では、ローカル vCenter に VMM ドメインを選択できます。対応する DVS/Cisco AV を選択してドメインを選択します。

カスタム属性のみ選択できます。これらはプラグインでは設定できません。これらは、VMware vSphere クライアントを設定する必要があります。カスタム ラベルを作成するには、VMware Web サイトのドキュメントを参照してください。

L2 および L3 の外部ネットワーク

レイヤ 2 およびレイヤ 3 の外部ネットワークは、ネットワーク管理者によって APIC で作成および設定される必要があります。これらは vCenter プラグインの読み取り専用です。

これらのオブジェクトで許可されるプラグイン操作のみ、コントラクトを消費または提供できます。

L3 外部ネットワークに表示されている情報は次のとおりです。

- Name：L3 外部ネットワークの名前
- Subnets：この L3 外部ネットワークで示される外部サブネット
- VRF：この L3 外部ネットワークに属する VRF
- 接続されたブリッジ ドメイン：このL3外部ネットワークに接続されているブリッジ ドメイン

L2 外部ネットワークに表示されている情報は次のとおりです。

- Name：L2 外部ネットワークの名前
- ブリッジ ドメイン：このブリッジ ドメインに関連付けられているブリッジ ドメイン
- VLAN ID：この L2 外部ネットワークに関連付けられている VLAN ID

VRF

Cisco ACI vCenter プラグインでは、VRF オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：VRF の名前。
- Description (Optional)：VRF の説明です。
- ポリシーの適用：コントラクトをこの VRF の EPG に適用する必要があるかどうかを決定します。

ブリッジ ドメイン

Cisco ACI vCenter プラグインでは、ブリッジ ドメインのオブジェクトに CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：ブリッジ ドメインの名前。
- Description (Optional)：ブリッジ ドメインの説明です。
- プライベート サブネット：このブリッジ ドメインのゲートウェイのリスト。

（注）
- 共有およびアドバタイズされるサブネットは読み取り専用です。これらは、プラグインで設定できることはできません。プライベート サブネットのみを追加または削除できます。
- ブリッジ ドメインはが APIC により L3/L2 アウトに接続されていますが、これは削除できません。

契約

Cisco ACI vCenter プラグインでは、コントラクトのオブジェクトに CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：コントラクトの名前。
- Description (Optional)：コントラクトの説明です。
- コンシューマ：コントラクト（EPG、uSeg Epg、L2/L3 外部ネットワーク）のコンシューマ
- プロバイダ：コントラクトのプロバイダ（EPG、uSeg Epg、L2/L3 外部ネットワーク）
- フィルタ：コントラクトに関連付けられているフィルタのリスト
- 両方向に適用：指定されたフィルタがコンシューマからプロバイダまたはプロバイダからコンシューマへのみ適用できることを示します。
- L4 L7 グラフテンプレート：既存のグラフテンプレートをコントラクトに関連付けることができます。L4 ～ L7 サービス セクションについては以下を参照してください。

（注）
- サブネットは表示されません。プラグインは、単一の件名を持つコントラクトのみ管理します。複数の件名を持つコントラクトが表示されますが、編集できません。
- コンシューマおよびコントラクトが同じテナント内にない場合は、コントラクトインターフェイスが自動的に作成されます（*_Tenant-name_contract-name* という名前）。

Filters

Cisco ACI vCenter プラグインでは、フィルタ オブジェクトの CRUD 操作が可能です。APIC からすべてのパラメータが公開されます。

L4 ～ L7 サービス

- L4 L7 サービスは、単一のプロバイダ契約にのみ追加できます。
- プラグインではグラフ テンプレートを作成できません（既存のグラフ テンプレートのみ消費）
  - グラフ テンプレートには次を含むように設定する必要があります。
    - デバイスとの関連付け
    - 機能プロファイルとの関連付け
  - 最大 2 個のノードを持つグラフ テンプレートのみをサポートします
- プラグインがフォルダ操作を許可していないため、機能プロファイルフォルダの名前つけと階層が有効である必要があります。
  - 機能プロファイルの空の必須パラメータが、プラグインで編集できます。
- グラフ コネクタが設定可能です。
  - APIC からすべてのパラメータが公開されます
  - 必要に応じて、リダイレクト ポリシーを消費のみ可能ですが作成はできません

トラブルシューティング

- エンドポイント間のトラブルシューティング セッションのみがサポートされます。
  - 既存のセッションを選択するか、新規を作成できます。
  - 物理トポロジ（スパイン/リーフ）は表示されません。
  - トポロジの表示はvNICが接続するホスト、VM、ｖNIC、EPGにフォーカスしているVM 中心型です。
- セッションで使用可能な情報：
  - 障害
  - コントラクト：表では 2 つの EPG 間のすべてのコントラクト/フィルタ/エントリを一覧にします（ヒット カウントは表示されません）
  - ドロップ/統計情報
  - 監査/イベント

- traceroute

- アトミック カウンタおよび SPAN は利用できません。
- より基本的なトラブルシューティング ツールは、エンドポイントではないオブジェクト（VM、EPG、L3 アウト）間で使用でき、選択された 2 つのオブジェクト間の設定されたコントラクトのみ表示します。
- VM および EPG への接続のビューが使用可能です。
  - 特定の VM については、VNIC を接続する EPG を表示することができます。
- L4 - L7 コネクタがトラブルシューティング セッションの送信元または宛先として使用される場合、トラブルシューティング ウィザードのコントラクト セクションで次のエラーが表示されることが予想されます。

  この機能には、EPG の一部である両方に対して送信元と宛先のエンドポイントが必要です。

  このエラーメッセージは、無視しても問題ありません。

Cisco AVS のインストールとアップグレード

Cisco ACI vCenter プラグインでは、vSphere Web クライアントから Cisco AV をインストール、アンインストール、アップグレード、ダウングレードできます。

- VCenter プラグインを ACI ファブリックに接続すると、Cisco APIC のすべての Cisco AVS ドメインの親を表示でき、Cisco AVS ドメインに関連付けられているデータ センタの一部またはすべてのホストの Cisco AVS をインストール、アンインストール、アップグレード、ダウングレードできます。
- Cisco.com からダウンロードされた Cisco AVS の新しいバージョンは、GUI を使用して vCenter にアップロードできます。これらのバージョンは、特定のドメイン内のホストにインストールできます。
- 特定の Cisco AV ドメインに接続されている場合は、すべてのホストを表示できます。インストールされている場合、ホストの OpFlex エージェントのステータスと Cisco AV の現在のバージョンを表示できます。

Cisco AVS をインストールまたはアップグレードするとき、Cisco AVS は ESXi ホストで次の手順を自動的に実行します。

1. ホストでメンテナンス モードを開始します。
2. ホストのデータ ストアに適した VIB ファイルをアップロードします。
3. Cisco AVS ソフトウェアをインストールまたは再インストールします。
4. ホストのデータ ストアから VIB ファイルを削除します。
5. ホストのメンテナンス モードを終了します。

（注）
- VCenter プラグインはホスト上の Cisco AV VIB をインストールまたはアンインストールのみします。Cisco AVS スイッチに対してホストを接続または切断する必要があります。
- ホストが HA/DRS クラスタの一部である場合、ホストがメンテナンス モードになっているとき、VM は自動的に移行されます。VM が自動的に移行できない場合、インストールまたはアップグレードを正常に行うため、ホストのすべての VM を移行するかオフにする必要があります。

詳細については、『Cisco AVS インストール ガイド』の次のセクションを参照してください。

- 「VMware vCenter プラグインを使用した Cisco AVS のインストール」
- 「VMware vCenter プラグインを使用した Cisco AVS のアップグレードまたはダウングレード」
- 「VMware vCenter プラグインを使用した Cisco AVS のアンインストール」

Cisco ACI vCenter プラグインのためのロールベース アクセス コントロール

Cisco APIC リリース 3.1 (1)から Cisco ACI vCenter プラグインは、 Cisco APIC のユーザ ロールとセキュリティ ドメインに基づいて、拡張されたロールベース アクセス コントロール (RBAC) をサポートしています。

Cisco ACI vCenter プラグインの UI には、Cisco APIC ユーザの読み取りと書き込み権限が反映されます。たとえば、ユーザが契約機能にアクセスしようとしても、契約に対する読み取り権限を持っていない場合、グレーの画面と、ユーザがアクセス権を持っていないことを示すメッセージが表示されます。書き込み権限を持っていないユーザには、無効なリンクまたはアクションが表示されます。

設定の読み取りと書き込みロール

次のテーブルでは、Cisco ACI vCenter プラグインの RBAC のさまざまな機能を有効または無効にするための読み取りと書き込みロールに関し、それぞれの権限を設定する方法について説明しています。

（注） ユーザに対し、セキュリティ ドメインを割り当てる際には、Cisco APICのロールを作成し、割り当てる必要があります。ユーザがアクセスするテナントについても、セキュリティ ドメインを追加する必要があります。

表 *1 : Cisco ACI vCenter* プラグインの *RBAC* 権限

ロール	ワークフロー	限定読み取りロール	書き込みロール
すべてのロールで必須の設定		vmm-connectivity および vmm-ep	
アプリケーションプロファイル	リスト	tenant-network-profile または tenant-epg	
	作成/削除		テナントネットワークプロファイル
EPG	List	tenant-epg、tenant-connectivity-l2、および tenant-connectivity-l3	
	作成/削除	tenant-connectivity-l2 および tenant-connectivity-l3	tenant-epg
VRF	List	tenant-connectivity-l2 および tenant-connectivity-l3	
	作成/削除		tenant-connectivity-l2 および tenant-connectivity-l3
ブリッジ ドメイン	BD の一覧	tenant-connectivity-l2 および tenant-connectivity-l3	
	BD の作成/削除		tenant-connectivity-l2 および tenant-connectivity-l3
	BD サブネットの一覧	tenant-connectivity-l2 および tenant-connectivity-l3	
	BD サブネットの作成/削除		tenant-connectivity-l2 および tenant-connectivity-l3

ロール	ワークフロー	限定読み取りロール	書き込みロール
契約	契約の一覧	tenant-security および tenant-epg	
	契約の作成/削除		tenant-security および tenant-epg
	フィルタの一覧	tenant-security および tenant-epg	
	フィルタの作成/削除	tenant-epg	tenant-security
L4L7	一覧	tenant-security、tenant-epg、および nw-svc-policy	
	作成/削除	tenant-epg	tenant-security および nw-svc-policy
トラブルシューティング	セッションの一覧	admin*	
	セッションの作成/削除		admin*
L2 Out	L2Out の一覧	tenant-ext-connectivity-l2	
	契約の作成	tenant-ext-connectivity-l2	tenant-security
L3 Out	L3Out の一覧	tenant-ext-connectivity-l3	
	契約の作成	tenant-ext-connectivity-l3	tenant-security

（注） 上記のテーブルでは、セキュリティ ドメインが「all」になっている場合、アスタリスク (*) が付いているロールを追加する必要があります。

Cisco APIC のユーザ ロールとセキュリティ ドメインの詳細については、『Cisco ACI Fundamentals』の「User Access: Roles, Privileges, and Security Domains」のセクションを参照してください。

Cisco ACI vCenter プラグインで推奨される RBAC 設定

aaaUser のために、APIC 上で権限を持つ 2 つのユーザ ロールを定義することを推奨します:

- vcplugin_read — aaaUser の読み取りアクセス許可を定義します。
- vcplugin_write — aaaUser の書き込みアクセス権を定義します。

Cisco ACI ファブリックは、Cisco APIC 上のローカル ユーザとしてのみ登録できます。デフォルトのログイン ドメインがローカルの場合は、admin または任意のローカル ユーザ名とパスワードでログインできます。

ただし、デフォルトのログイン ドメインがローカルではない場合でも、ユーザ名でローカル ドメインを指定することにより、やはりファブリックを定義することができます:

```
apic#local domain\username
```

ローカル ドメインとユーザ名を入力する場合には、Cisco APIC にローカル ドメイン名が存在する必要があります。

（注） どの RBAC 設定でも、aaaUser のセキュリティ ドメインを Cisco APIC と VMware vCenter の間の VMM ドメインに割り当てることが必要です。

（注） Cisco ACI vCenter プラグインは、このガイドの Cisco ACI vCenter プラグインのためのロールベース アクセス コントロール （15 ページ） の RBAC 権限のテーブルで記述されているアクセス許可に従うものであれば、どのユーザ ロールの組み合わせにでも適応することができます。

Cisco ACI vCenter プラグインを使用している場合の VMware vCenter のアップグレード

VMware vCenter をバージョン 6.0 からバージョン 6.5 にアップグレードしようとしており、Cisco ACI vCenter プラグインを使用している場合には、アップグレードに進む前に、追加の手順を実行する必要があります。

（注） VMware vCenter をアップグレードする前に vCenter プラグインをアンインストールし、アップグレード後に再インストールすることをお勧めします。

手順

vCenter で、`C:\ProgramData\cisco_aci_plugin\` フォルダを削除します。

フォルダを削除しないまま、アップグレード後にファブリックをもう一度登録しようとすると、「Error while saving setting in C:\ProgramData\cisco_aci_plugin*user_domain*.properties」というエラーメッセージが出ます。ここでの user は vSphere Web クライアントにログインしているユーザであり、domain は所属ドメインになります。

ファブリックを登録することはできますが、古い VMware vCenter で作成された設定を上書きする権限はありません。VMware vCenter を再起動した後、Cisco APIC 構成の変更を再度入力する必要があります。

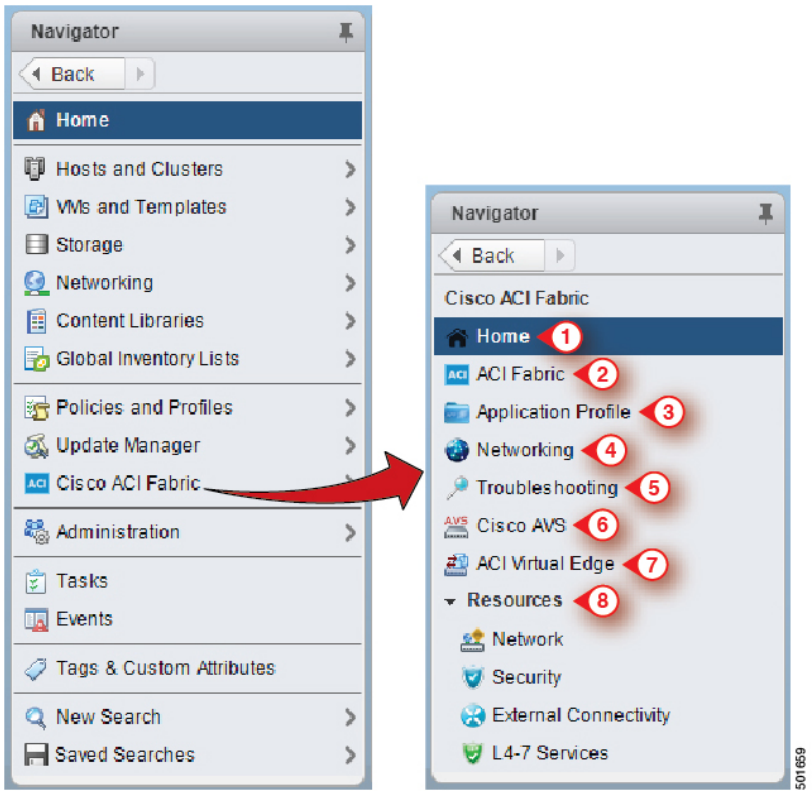
Cisco ACI vCenter プラグイン GUI

Cisco ACI vCenter プラグイン GUI アーキテクチャの概要

ここでは、Cisco ACI vCenter プラグインの GUI アーキテクチャの概要について説明します。

メイン メニュー

図 *1:* メイン メニュー



（注） Cisco APIC リリース 5.0（1）以降、Cisco Application Virtual Switch（AVS）はサポートされなくなりました。Cisco AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、Cisco AVS ドメインの障害が発生します。

1	**Home**—Cisco ACI vCenterプラグインホームページを表示し、**[Getting Started]** タブと**[About]**タブがあります。 **[Create a new Tenant]**、**[Create a new Application Profile]**、**[Create a new Endpoint Group]** などの基本的なタスクを実行できる**[Getting Started]**タブ、Cisco Application Centric Infrastructure (ACI) リンクをクリックして、ACI Web サイトを参照してください。 The **[About]** タブには、Cisco ACI vCenter プラグインの現在のバージョンが表示されます。
2	**ACI Fabric**—ACI ファブリックをプラグインに登録し、ファブリックのテナントを管理するために使用されます。
3	**Application Profile**—EPG、uSeg EPG、L2/L3Out、および契約のドラッグアンドドロップインターフェイスでアプリケーションプロファイルを管理するために使用します。アプリケーションの健全性、統計およびフォルトに関する可視性を提供します。
4	**Networking**—VRF およびブリッジドメインを管理するためのドラッグアンドドロップ インターフェース。
5	**Troubleshooting**—エンティティ、エンドポイントからエンドポイントへのトラブルシューティングセッションの間で定義されたコントラクトを表示し、仮想マシン(VM)をブラウズし、エンドポイント グループ (EPG) への接続を表示します。
6	**Cisco AVS**—Cisco AVS のインストール、アップグレード、またはアンインストール。 （注） Cisco APIC リリース 5.0(1) 以降、AVS はサポートされていません。
7	**Cisco ACI Virtual Edge**：Cisco ACI Virtual Edge（AVE）をインストールまたはアンインストールするか、Cisco AVS または VMware VDS から ACI Virtual Edge に移行します。 （注） Cisco APIC リリース 6.0(1) 以降、AVE はサポートされません。
8	**Resources**—プラグインによって管理されているすべてのオブジェクトの階層型ビューでブラウズすることができます。

（注） **[Application Profile]**、**[Networking]** および **[Resources]** のセクションをナビゲートしている間、各画面の上部にある選択バーでは、アクティブなテナントを選択できます。各セクションに表示されるコンテンツは、そのバーで選択されたテナントに固有です。

Cisco ACI vCenter プラグインの概要

このセクションでは、Cisco ACI vCenter プラグインの GUI 概要について説明します。

（注） すべての障害、統計、イベント、監査の時刻は、ブラウザのローカル タイム ゾーンに表示されます。Cisco APIC のタイム ゾーンがシステムのタイム ゾーンと一致していない場合、タイム スタンプは別のタイム ゾーンのものになる可能性があります。

ホーム

VMware vSphere Web クライアントの [Navigator] ペインで、[Home] を選択します。[Work] ペインには次のタブが表示されます。

- [Getting Started] タブ

  [Getting Started] ペインの下部では、次の操作を実行できます:

  - [Create a new Tenant] をクリックして、新しいテナントを作成します。
  - [Create a new Application Profile] をクリックして、新しいアプリケーション プロファイルを作成します。
  - [Create a new Endpoint Group] をクリックして、新しいエンドポイント グループを作成します。
  - Cisco Application Centric Infrastructure (ACI) リンクをクリックして、ACI の Web サイトを閲覧します。

- [About] タブ

  [About] ペインには、Cisco ACI vCenter プラグインのバージョンが表示されます。

ACI ファブリック

VMware vSphere Web クライアントの [Navigator] ペインで、[Cisco ACI Fabric] を選択します。[Work] ペインには次のタブが表示されます。

- [ACI Fabric] タブ

  [ACI Fabric] ペインでは、ペインでは、次の操作を実行できます:

  - [Register a new ACI Fabric / ACI Node] をクリックして、新しい ACI ファブリックまたは ACI ノードを登録します。
  - ファブリックの現在の Cisco APIC 状態に関する情報を表示します。

（注） プラグインは、Cisco APIC が利用不可であることを検出すると、接続の試行を中止して、ステータスを更新しなくなります。応答しない Cisco APIC に接続しようとしてタイムアウトまで待機するのを避けるには、次の操作を行います。[Reload] をクリックして、Cisco APIC の状態を更新します。これは、利用不可なものも含めて、それぞれの Cisco APIC への再接続を試みます。再び利用可能になっていた場合には、そのステータスは更新されます。

- [Tenants] タブ

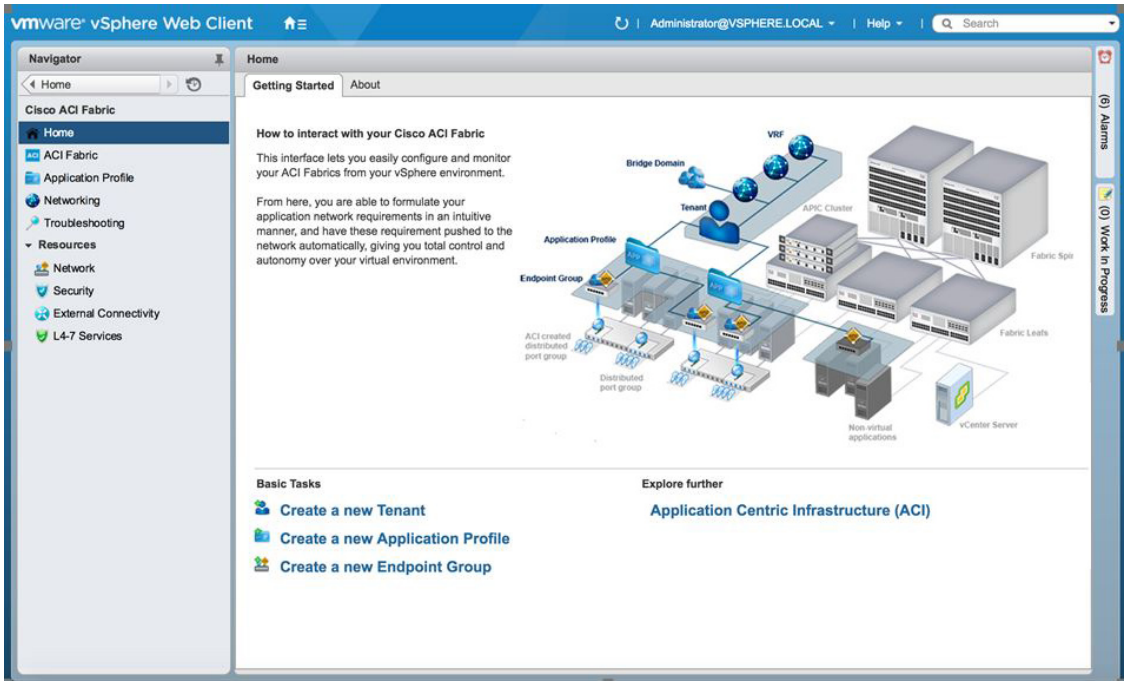
  [Tenants] ペインでは、次の操作を実行できます:

  - 登録済みの ACI ファブリックに存在する別のテナントを管理します。
  - [Create a new Tenant] をクリックして、新しいテナントを作成します。
  - 別のテナントを表示します。

    テーブルでテナントを選択して、[Delete Tenant <テナント名>] をクリックすれば、テナントを削除できます。

    テーブルでテナントを選択して、[<テナント名>] を右クリックし、[Edit settings] を選択すれば、テナントの説明を編集できます。

図 *2: ACI* ファブリック - ホーム



アプリケーション プロファイル

VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Application Profile]** を選択します。[Work] ペインでは、次の操作を実行できます。

- アクティブなテナントとアプリケーションプロファイルを選択します。
- [Create a new Application Profile] をクリックして、新しいアプリケーション プロファイルを作成します。
- [Drag and drop to configure] セクションで要素をドラッグ アンド ドロップすることにより、アプリケーション プロファイル全体を構成できます。要素は次のとおりです。
  - エンドポイント グループ
  - uSeg
  - L3 外部ネットワーク
  - L2 外部ネットワーク
  - コントラクト
- これらのタブを使用して、ポリシー、トラフィック統計、健全性、障害、監査ログとイベントを表示します。

  [Policy] タブでは、コンシューマとプロバイダ表示またはトラフィック表示に切り替えることができます。

ネットワーキング

VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Networking]** を選択します。[Work] ペインでは、次の操作を実行できます。

- ブリッジ ドメインが設定される分離 VRF を作成することにより、すべてのエンドポイント グループに対する自分独自のアドレッシングをセットアップします。エンドポイント グループは、1 つのブリッジ ドメインに関連付けられます。
- アクティブなテナントを選択します。
- [Drag and drop to configure] セクションで次の要素をドラッグ アンド ドロップします:
  - VRF
  - ブリッジ ドメイン

（注） 使用可能なレイヤ 3 およびレイヤ 2 エンドポイント グループは、ここに表示されますが、構成はできません。

トラブルシューティング

VMware vSphere Web クライアントの [Navigator ペインで、**[Cisco ACI Fabric]** > **[Troubleshooting]** を選択します。[Work] ペインには次のタブが表示されます。

- [Policy Checker] タブ

  [Policy Checker] タブでは、2 つのエンティティ (仮想マシン、エンドポイント グループ、レイヤ 3 の外部ネットワークまたはエンドポイント) を選択して、これら 2 つのエンティティ間で適用される、すべての契約およびレイヤ 4 ～ レイヤ 7 サービスを表示できます。

  2 つのエンドポイント間でトラブルシューティング セッションを開始することもできます。

  - [From]、[To] および [Fix Time] チェック ボックスでセッションのタイム フレームを選択します。
  - [Fix Time] チェック ボックスをオンにして、タイム フレームを設定することができます。
  - [Source Destination] セクションでは、送信元と宛先のエンドポイントを選択できます。[Start Troubleshooting session] をクリックすれば、新しいトラブルシューティング セッションを開始できます。
  - [Troubleshooting Session] では、障害、構成された契約、イベント、監査、およびトラフィック統計を検査することができます。
  - [Traceroute] をクリックすると、2 つのエンドポイント間でのトレース ルートを開始できます。
  - 要素の隣にあるアイコンをクリックすると、左ペインで選択した大項目に対応する詳細情報を取得できます。
  - エンドポイントごとに、対応する vNIC、VM、およびホスト、および vNIC が接続されている EPG を表すトポロジを取得できます。

- [Virtual Machines] タブ

  このビューでは、仮想マシンのネットワーク インターフェイス カードが、エンドポイントのグループに接続されているかどうかを可視化できます。

  - このリストは、[search] フィールドを使用して制限することができます。
  - VNIC が EPG に接続されている場合は、それぞれの VM を表示できます。
  - 関連付けられている EPG が正常かまたは何らかの問題を抱えているかを迅速に確認し、それが属しているテナントとアプリケーションプロファイルを表示できます。

リソース

- ネットワーク

VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[Network]** を選択します。[Work] ペインには次のタブが表示されます。

- [Endpoint Groups] タブ

  エンドポイント グループを作成してネットワークインフラストラクチャを設定します。各エンドポイント グループには対応する VMware 分散ポート グループがあり、仮想マシンを接続することができます。異なるエンドポイントグループをアプリケーション プロファイルに編成できます。

  - アクティブなテナントを選択します。
  - [Create a new Application Profile] をクリックして、新しいアプリケーション プロファイルを作成します。
  - テーブルでアプリケーションを選択してから [Create a new Endpoint Group] をクリックして、新しいエンドポイント グループを作成します。
  - テーブルを表示して、アクティブなテナントのアプリケーションプロファイルとエンドポイント グループを確認します。
  - 接続されているすべての VM を表示するには、エンドポイント グループを選択します。

- [VRFs] タブ

  すべてのエンドポイント グループで、ブリッジ ドメインで設定される分離 VRF を作成することにより、独自のアドレッシングをセットアップできます。エンドポイントグループは、1 つのブリッジ ドメインに関連付けられます。

  - アクティブなテナントを選択します。
  - [Create a new VRF] をクリックして、新しいVRFを作成します。
  - [Create a new Bridge Domain] をクリックして、新しいブリッジ ドメインを作成します。
  - VRG を確認するには、テーブルを表示します。

- **セキュリティ**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[Security]** を選択します。[Work] ペインには次のタブが表示されます。

  - [Contracts] タブ

    契約では、異なるエンドポイント グル - プの間、およびエンドポイント グループとレイヤ 3 およびレイヤ 2 外部ネットワーク間で、セキュリティ ポリシーを定義できます。

    - アクティブなテナントを選択します。
    - [Create a new Contract] をクリックして、新しい契約を作成します。

- 契約を確認するには、テーブルを表示します。

- [Filters] タブ

  フィルタは、(プロトコル、ポートなどに基づく) トラフィックの特定のタイプと一致するエンティティです。これらは、契約により、エンドポイントグループとレイヤ3外部ネットワーク間で承認されるサービスを定義するために用いられます。

  - アクティブなテナントを選択します。
  - [Create a new Filter] をクリックして、新しいフィルタを作成します。
  - フィルタを確認するには、テーブルを表示します。

- **外部接続**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[External Connectivity]** を選択します。[Work] ペインには次のタブが表示されます。

  - [L3 External Networks] タブ

    レイヤ 3 外部ネットワークは、Cisco APIC 管理者が定義します。定義されたネットワークは、自分のインフラストラクチャと外部を接続できるようにするために、自分の契約とレイヤ 4 ～ レイヤ 7 サービスで使用できます。

    - アクティブなテナントを選択します。
    - レイヤ 3 外部ネットワークを確認するには、テーブルを表示します。

  - [L2 External Networks] タブ

    レイヤ 2 外部ネットワークは、Cisco APIC 管理者が定義します。定義されたネットワークは、自分のインフラストラクチャと外部を接続できるようにするために、自分の契約とレイヤ 4 ～ レイヤ 7 サービスで使用できます。

    - アクティブなテナントを選択します。
    - レイヤ 2 外部ネットワークを確認するには、テーブルを表示します。

- **L4 ～ 7 サービス**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[External Connectivity]** を選択します。[Work] ペインには次のものが表示されます:

  - レイヤ4～レイヤ7サービスを使えば、エンドポイントグループと外部レイヤ3ネットワークの間に、事前プロビジョニングされたファイアウォールとロードバランサを追加できます。
  - アクティブなテナントを選択します。
  - 現在、テナント内に展開されているレイヤ4～7のグラフインスタンスを確認するには、テーブルを表示します。

GUI のヒント

このセクションでは、GUI のヒントについて説明します。

- テーブルやグラフに表示されている ACI オブジェクトを右クリックすると、関連したアクションが表示されます。
- vCenter プラグインのテーブル内に仮想マシン オブジェクトが表示されている時には、それをダブルクリックすると、vSphere Web クライアントの仮想マシンに移動することができます。

ACI オブジェクトの設定の実行

新しいテナントの作成

この項では、新しいテナントを作成する方法について説明します。

始める前に

ACI ファブリックが登録されていることを確認します。詳細については、資格情報を使用して vCenter プラグインを Cisco ACI ファブリックに接続する （5 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Work** ウィンドウで、**Cisco ACI Fabric** を選択します。

ステップ 3 **Navigator** ウィンドウで、**ACI Fabric** を選択します。

ステップ 4 **ACI Fabric** ペインで、**Tenants** タブを選択します。

ステップ 5 **Tenants** ペインで、**Create a new Tenant** をクリックします。

ステップ 6 **New Tenant** ダイアログボックスで、次の操作を実行します:

a) **Enter a name for the Tenant** フィールドに、テナントの名前を入力します。

b) (オプション) **Enter a description for the Tenant** フィールドに、テナントの説明を入力します。

c) **[OK]** をクリックします。

新しいアプリケーション プロファイルの作成

このセクションでは、新しいアプリケーションプロファイルを作成する方法について説明します。

始める前に

- テナントが作成済みであることを確認します。

  詳細については、新しいテナントの作成 （27 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Work** ウィンドウで、**Cisco ACI Fabric** を選択します。

ステップ 3 **Navigator** ウィンドウで、**Resources** > **Network** を選択します。

ステップ 4 **Network** ウインドウの、**Endpoint Groups** タブの下で、次の操作を実行します:

a) **Tenant** ドロップダウン リストから、テナント名を選択します。

b) **Create a new Application Profile** をクリックします。

ステップ 5 **New Application Profile** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、アプリケーション プロファイルの名前を入力します。

b) (オプション) **Description** フィールドで、アプリケーション プロファイルについての説明を入力します。

c) **[OK]** をクリックします。

ドラッグ アンド ドロップ方式を使用して EPG を作成する

このセクションでは、ドラッグ アンド ドロップ方式を用いてエンドポイント グループ (EPG) を作成する方法について説明します。

（注） Cisco APIC リリース 5.0（1）以降、Cisco Application Virtual Switch（AVS）はサポートされなくなりました。Cisco AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、Cisco AVS ドメインの障害が発生します。

始める前に

- テナントが作成済みであることを確認します。

  詳細については、新しいテナントの作成 （27 ページ）を参照してください。

- アプリケーションプロファイルが作成されたことを確認します。

  詳細については、新しいアプリケーション プロファイルの作成 （27 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** フィールドで、ドロップダウン リストからテナントを選択します。

b) **Application Profile** フィールドで、ドロップダウン リストからアプリケーション プロファイルを選択します。

c) **Drag and drop to configure** 要素エリアで、**Endpoint Group** をドラッグ アンド ドロップします。

ステップ 4 **New Endpoint Group** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、エンドポイント グループの名前を入力します。

b) (オプション) **Description** フィールドに、EPGの説明を入力します。

c) **Bridge Domain** フィールドで、一般的なテナントや EPG が作成されたテナントから、ブリッジ ドメインを選択します。デフォルトのブリッジ ドメインは、common/default です。ペンのアイコンをクリックして、別のブリッジ ドメインを選択します。

ステップ 5 **Distributed Switch** フィールドで、次の操作を実行します:

a) 少なくとも 1 つの分散スイッチのチェック ボックスをオンにして、EPG を、センタkした分散 スイッチに接続します。

b) マイクロセグメンテーションを許可するために、**Allow micro-segmentation** チェック ボックスをオンにします。

Allow micro-segmentation チェック ボックスは、分散スイッチが DVS である場合にのみ表示されます。分散スイッチが AVS である場合には、GUI は **Allow micro-segmentation** チェック ボックスを表示しません。分散スイッチが AVS である場合、すべての EPG が基本 EPG であると見なされます。

この方法で基本EPGを作成できます。このEPGに接続されているすべての仮想マシンは、uSeg EPG のマイクロセグメンテーション ルールを適用する候補者となります。マイクロセグメンテーション EPG ルールは、基本 EPG に接続されている仮想マシンにのみ適用されます。

c) EPG を分離する場合には、**Intra EPG isolation** チェック ボックスをオンにします。

これにより、このEPGに接続されている仮想マシン間のすべてのトラフィックを拒否することができます。このルールは、マイクロセグメンテーションEPGの下に表示されるマシンにも適用されます。デフォルトでは、同じEPGのすべての仮想マシンは互いに通信できます。

ステップ 6 **OK** をクリックして、新しい EPG を APIC にプッシュします。

新しい EPG がトポロジ内で作成されたのを確認できます。

ドラッグ アンド ドロップ方式を使用した新規 uSeg EPG の作成

このセクションでは、ドラッグ アンド ドロップ方式を使用して新しい uSeg を作成する方法について説明します。

始める前に

- テナントが作成されたことを確認します。

  詳細については、「新規テナントの作成」を参照してください。

- アプリケーションプロファイルが作成されたことを確認します。

  詳細については、新しいアプリケーション プロファイルの作成 （27 ページ）を参照してください。

- （DVS のみ）ベース EPG を作成し、マイクロセグメンテーションに参加する必要があるすべての VM をそのベース EPG に接続したことを確認します。詳細については、新しいエンドポイント グループの作成を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。

b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します。

c) **[設定するドラッグ アンド ドロップ]** 要素エリアで、トポロジに uSeg をドラッグ アンド ドロップします。

ステップ 4 **[新しいエンドポイント グループ]** ダイアログ ボックスで、次の操作を実行します。

a) **[名前]** フィールドに、EPG の名前を入力します。

b) **[説明]** フィールドに、EPG の説明を入力します。

ステップ 5 **[分散型スイッチ]** フィールドで、その uSeg EPG に関連付ける必要がある分散型スイッチを選択します。

（注）
DVS が 1 個のみ存在する場合、デフォルトで選択されるようにチェック ボックスが表示されません。

ステップ 6 **[ブリッジ ドメイン]** フィールドで、共通または uSeg EPG が作成されるテナントからブリッジ ドメインを選択します。デフォルトのブリッジ ドメインでは、共通/デフォルトです。**[ペン]** アイコンをクリックして、別のブリッジ ドメインを選択します。

ステップ 7 **[EPG 内分離]** チェック ボックスをチェックして、EPG を分離します。

ステップ 8 **[マイクロセグメンテーション]** セクションで、**[+]** アイコンをクリックします。

ステップ 9 **[新しいマイクロセグメンテーション グループ]** ダイアログ ボックスで、次の操作を実行します。

a) **[名前]** フィールドに、新規属性の名前を入力します。
b) （任意） **[説明]** フィールドに、新規属性の説明を入力します。
c) **[タイプ]** セクションで、フィルタ対象のタイプを選択します。
d) **[演算子]** セクションで、**[使用する演算子を含む]** を選択します。
e) 使用可能な場合、手動で値を入力する代わりに、**[参照]** ボタンをクリックして特定のオブジェクトを選択します。
f) **[OK]** をクリックすると、新しい属性が uSeg EPG に追加されます。

ステップ 10 USeg EPG に他の属性を追加するには、ステップ 7 および 8 を繰り返します。

ステップ 11 **[OK]** をクリックします。

ドラッグ アンド ドロップ方式を使用した 2 つの EPG 間のコントラクトの作成

このセクションでは、ドラッグ アンド ドロップ方式を使用して 2 つのエンドポイント グループ（EPG）間のコントラクトを作成する方法について説明します。

始める前に

- 2 つの EPG が作成されていることを確認します。

  詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （28 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Work** ウィンドウで、**Cisco ACI Fabric** を選択します。

ステップ 3 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 4 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。
b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します。

ステップ 5 **[設定するドラッグ アンド ドロップ方式]** 要素エリアで、送信元 EPG にコントラクトをドラッグ アンド ドロップします。

ステップ 6 宛先 EPG をクリックします。送信元 EPG から宛先 EPG に移動する矢印が表示されます。

ステップ 7 **New Contract** ダイアログボックスで、次の操作を実行します:

a) **[コンシューマ]** フィールドで、正しい EPG が表示されていることを確認します。
b) **[プロバイダ]** フィールドで、正しい EPG が表示されていることを確認します。
c) **[名前]** フィールドに、コントラクトの名前を入力します。
d) （オプション）**[説明]** フィールドにコントラクトの説明を入力します。
e) **[フィルタ]** フィールドで、**[+]** アイコンをクリックして、コントラクトをフィルタします。
f) **[新規]** ダイアログ ボックスで、左のリストから右のリストへ[コントラクト]に追加するすべてのフィルタをドラッグ アンド ドロップして**[OK]** をクリックします。
g) （オプション）**[L4 ～ L7 サービスの設定]** チェック ボックスをオンにして、レイヤ 4 ～ レイヤ 7 サービスを設定します。
h) **[OK]** を選択して、コントラクトを作成します。

ドラッグ アンド ドロップ方式を使用して既存の契約への EPG の追加

このセクションでは、ドラッグ アンド ドロップ方式を使用して、既存のコントラクトに EPG を追加する方法について説明します。

（注） Cisco APIC リリース 5.0（1）以降、Cisco Application Virtual Switch（AVS）はサポートされなくなりました。Cisco AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、Cisco AVS ドメインの障害が発生します。

始める前に

- コントラクトが作成されたことを確認します。
- EPG が作成されたことを確認します。

  詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （28 ページ）を参照してください。
- コントラクトが **[アプリケーション プロファイル]** ウィンドウで表示されていることを確認します。たとえば、アプリケーション プロファイルの別の EPG はコントラクトをすでに使用しています。このケースではない場合、「セキュリティ タブを使用して既存のコントラクトに EPG を追加する」の手順に従います。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。**[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。

b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します。

ステップ 4 **[設定するドラッグ アンド ドロップ]** 要素エリアで、コントラクトをドラッグ アンド ドロップして、次のいずれかを実行します。

- EPG がコントラクトを消費するには：

  1. **[コントラクト]** をコントラクトが消費する必要がある EPG にドラッグ アンド ドロップします。
  2. 関連するコントラクト（EPG からコントラクトに向かって矢印が表示されます）、EPG がコントラクトを消費するコントラクトをクリックします。

- EPG がコントラクトを提供するには：

  1. 提供する必要があるコントラクトに **[コントラクト]** をドラッグ アンド ドロップします。
  2. 関連するコントラクト（コントラクトから EPG に向かって矢印が表示されます）、EPG がコントラクトを提供する **[コントラクト]** をクリックします。

[Security] タブを使用して既存の契約に EPG を追加する

始める前に

- コントラクトが作成されたことを確認します。
- EPG が作成されたことを確認します。

  詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （28 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Navigator** ペインで、**Resources** > **Security** を選択します。

ステップ 3 **Tenant** ドロップダウン リストから、テナントを選択します。

ステップ 4 契約のリストから、EPG を追加する必要のある契約をクリックします。

ステップ 5 + アイコンを、**Consumers** または **Providers** カラムでクリックします (それぞれ EPG の使用または契約の提供を行います)。

ステップ 6 表示されたオプションで、**Add Endpoint Groups** を選択します。

ステップ 7 ダイアログボックスで、次の操作を実行します。

a) EPG があるテナントを展開します。
b) EPG がある **Application Profile** を展開します。
c) EPG を左側のリストから右側のリストにドラッグ アンド ドロップします。
d) **[OK]** をクリックします。

L3 外部ネットワークのセット アップ

このセクションでは、レイヤ 3 外部ネットワークに接続する方法について説明します。

（注） レイヤ 3 外部ネットワークのすべての設定を行うことはできません。Cisco Application Policy Infrastructure Controller（APIC）に存在するレイヤ 3 外部ネットワークのみ設定できます。

始める前に

- APIC のレイヤ 3（L3）外部ネットワークが設定されていることを確認します。詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイドを参照してください。
- EPG が作成されたことを確認します。詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （28 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。
b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します（アプリケーション）。
c) **[設定にドラッグ アンド ドロップ]** 要素エリアで、**[L3 外部ネットワーク]** トポロジにドラッグ アンド ドロップします。

ステップ 4 **[オブジェクトの選択]** ダイアログ ボックスで、テナント<*tenant_name*>（tenant1）を選択し、レイヤ 3 外部ネットワークを選択して、**[OK]** をクリックします。

ステップ 5 **[設定にドラッグ アンド ドロップ]** 要素エリアで、**[コントラクト]** を レイヤ 3 外部ネットワーク上にドラッグ アンド ドロップし、それから EPG (WEB) にドラッグして接続します。

ステップ 6 **New Contract** ダイアログボックスで、次の操作を実行します:

a) **[コンシューマ]** フィールドで、正しい レイヤ 3 外部ネットワーク（l3Ext）が表示されていることを確認します
b) **[プロバイダ]** フィールドで、正しい EPG (WEB) が表示されていることを確認します。
c) **Name** フィールドに、契約の名前 (L3ext-to-WEB) を入力します。
d) （任意） **Description** フィールドに、契約の説明を入力します。
e) **[フィルタ]** フィールドでは、**[+]** アイコンをクリックして、トラフィック フィルタを追加できます。
f) **[新規]** ダイアログ ボックスで、コントラクトに追加するすべてのフィルタを左側のリストから右側のリストにドラッグ アンド ドロップして、**[OK]** をクリックします。
g) （任意） **Configure L4-7 service** チェック ボックスをオンにして、Layer 4 to Layer 7 サービスを設定します。
h) **[OK]** を選択して、コントラクトを作成します。

コントラクトは、トポロジのレイヤ 3 の外部ネットワークに接続されます。

L2 外部ネットワークの設定

このセクションでは、レイヤ 2 (L2) 外部ネットワークに接続する方法について説明します。

（注） L2 外部ネットワークのすべての設定を行えるわけではありません。Cisco Application Policy Infrastructure Controller（APIC）に存在する L2 外部ネットワークのみ設定できます。

始める前に

- APIC で L2 外部ネットワークが設定されていることを確認します。詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイドを参照してください。
- EPG が存在することを確認します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。
ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。
ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します (tenant1)。
b) **Application Profile** ドロップダウン リストから、[Expenses] を選択します。
c) **Drag and drop to configure** エレメント エリアで、**L2 External Network** をトポロジにドラッグ アンド ドロップします。

d) **Drag and drop to configure** エレメント エリアで、**Contract** を L2 外部ネットワーク上にドラッグ アンド ドロップし、それから EPG (WEB) にドラッグして接続します。

ステップ 4 **New Contract** ダイアログボックスで、次の操作を実行します:

a) **Consumers** フィールドで、正しい L2 外部ネットワーク (L2ext) が表示されていることを確認します
b) **Providers** ィールドで、正しい EPG (WEB) が表示されていることを確認します。
c) **Name** フィールドに、契約の名前 (L2ext-to-WEB) を入力します。
d) **Description** フィールドに、契約の説明を入力します。
e) **[フィルタ]** フィールドでは、**[+]** アイコンをクリックして、トラフィック フィルタを追加できます。
f) **[新規]** ダイアログ ボックスで、コントラクトに追加するすべてのフィルタを左側のリストから右側のリストにドラッグ アンド ドロップして、**[OK]** をクリックします。
g) （任意） **Configure L4-7 service** チェック ボックスをオンにして、Layer 4 to Layer 7 サービスを設定します。
h) [OK] をクリックします。

契約はトポロジの L2 外部ネットワークに接続されます。

ドラッグ アンド ドロップ方式を使用した VRF の作成

このセクションでは、ドラッグ アンド ドロップ方式を使用して VRF を作成する方法について説明します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[作業]** ウィンドウで **[ネットワーキング]** を選択します。

ステップ 3 **Networking** ペインで、次の操作を実行します:

a) **[テナント]** ドロップダウン リストから、テナントを選択します。
b) **[設定するドラッグ アンド ドロップ]** 要素エリアで VRF をペインにドラッグ アンド ドロップします。

ステップ 4 **[新規 VRF]** ダイアログ ボックスで、次の操作を実行します:

a) **[名前]** フィールドに、VRF の名前を入力します。
b) (オプション)**[説明]** フィールドに、VRF の説明を入力します。
c) **[セキュリティ]** セクションで、**[**ポリシーの適用] チェック ボックスをオンにします。ポリシーの適用は、セキュリティ ルール（コントラクト）を適用する必要があるか、VRF 用かを決定します。
d) **[OK]** をクリックします。

ブリッジ ドメインの作成

この項では、ブリッジ ドメインを作成する方法について説明します。

始める前に

- VRF (プライベート ネットワーク) が存在することを確認します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Navigator** ウィンドウで **Networking** を選択します。

ステップ 3 **Networking** ペインで、次の操作を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します (tenant1)。

b) **Drag and drop to configure** エレメント エリアで、VRF の上にブリッジ ドメインをドラッグ アンド ドロップします。

ステップ 4 **New Bridge Domain** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、ブリッジ ドメインの名前を入力します (BD2) 。

b) （任意） **Description** フィールドに、論理スイッチの説明を入力します。

c) **Private Subnets** セクションにプライベート サブネット (2.2.2.2/24) を入力し、+ アイコンをクリックしてサブネットをブリッジ ドメインに追加します。

d) （任意） 手順 c と d を繰り返して、必要な数のサブネットをブリッジ ドメインに追加します。

e) [OK] をクリックします。

ブリッジ ドメインは、トポロジ内の VRF に接続します。

エンドポイントの間で新しいトラブルシューティングセッションを開始する

このセクションでは、エンドポイントの間で新しいトラブルシューティングセッションを開始する方法について説明します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Work** ウィンドウで、**Cisco ACI Fabric** を選択します。

ステップ 3 **Navigator** ウィンドウで、**Troubleshooting** を選択します。

ステップ 4 **Policy Checker** タブの **Session name** セクションに、新しいセッション名を入力します。

ステップ 5 **Source and Destination** セクションで、**Select source** をクリックします。

ステップ 6 表示されるメニューで、**Select Endpoint** をクリックします。

ステップ 7 新たに表示されるダイアログボックスで、送信元として使用するエンドポイントを選択して、**OK** をクリックします。

ステップ 8 **Source and Destination** セクションで、**Select destination** をクリックします。

ステップ 9 表示されるメニューで、**Select Endpoint** をクリックします。

ステップ 10 新たに表示されるダイアログボックスで、宛先として使用するエンドポイントを選択して、OK をクリックします

ステップ 11 **[トラブルシューティング セッションの開始]** をクリックします。

ステップ 12 **[トラブルシューティング]**ペインでは、障害、構成された契約、イベント、監査、およびトラフィック統計を検査することができます。

トポロジには、各エンドポイント、対応する vNIC、VM、ホスト、および vNIC が接続されている EPG の設定が表示されます。要素の隣にあるアイコンをクリックすると、左ペインで選択した大項目に対応する詳細情報を取得できます。

ステップ 13 **[ナビゲーション（Navigation）]** ウィンドウで、**[Traceroute]** をクリックして、2 つのエンドポイント間で traceroute を開始します。

エンドポイント間の既存のトラブルシューティングセッションの開始

このセクションでは、エンドポイント間の既存のトラブルシューティング セッションを開始する方法について説明します。

始める前に

手順

ステップ 1 VMware vSphere Web クライアントにでログインして、**[作業]** ペインで **[Cisco ACI ファブリック]** を選択します。

ステップ 2 **[ナビゲータ]** ペインで、**[トラブルシューティング]** を選択します。

ステップ 3 **[ポリシー チェッカー]** タブの **[セッション名]** セクションで、**[既存のセッションの選択]** をクリックします。

a) **[セクションの選択]** ダイアログ ボックスで、トラブルシューティング セッション を選択します。

b) [OK] をクリックします。

エンドポイント間のトラブルシューティングのみ実行できます。

ステップ 4 **[トラブルシューティング セッションの開始]** をクリックします。

ステップ 5 **[トラブルシューティング]**ペインでは、障害、構成された契約、イベント、監査、およびトラフィック統計を検査することができます。

トポロジには、各エンドポイント、対応する vNIC、VM、ホスト、および vNIC が接続されている EPG の設定が表示されます。要素の隣にあるアイコンをクリックすると、左ペインで選択した大項目に対応する詳細情報を取得できます。

ステップ 6 **[ナビゲーション（Navigation）]** ウィンドウで、**[Traceroute]** をクリックして、2 つのエンドポイント間で traceroute を開始します。

Cisco ACI vCenter プラグインのアンインストール

このセクションでは、VMware vCenter プラグインのアンインストール方法について説明します。

始める前に

- PowerCLI コンソールを利用可能にしておく必要があります。
- `ACIPlugin-Uninstall.ps1` スクリプトを利用可能にしておく必要があります。

  このスクリプトはプラグインアーカイブにあります。次のサイトからダウンロードすることもできます: `https://APIC_IP/vcplugin/ACIPlugin-Uninstall.ps1`.

手順

ステップ 1 PowerCLI コンソールを開きます。

ステップ 2 `ACIPlugin-Uninstall.ps1` スクリプトを実行します。

ステップ 3 要求されたら、**vCenter IP / FQDN** フィールドに、プラグインをアンインストールする vCenter の場所を入力します。

ステップ 4 表示されたダイアログボックスに、vCenter のルート権限のクレデンシャルを入力します。アンインストールが成功した場合、コンソールに次のメッセージが表示されます:

```
[x] Uninstalled ACI vCenter Plugin
```

Cisco ACI vCenter プラグインのアップグレード

このセクションでは、Cisco ACI vCenter プラグインをアップグレードする方法について説明します。

手順

Cisco ACI vCenter プラグインをアップグレードするには、インストールの手順に従う必要があります。

詳細については、「Cisco ACI vCenter プラグインのインストール （3 ページ）」を参照してください。

Cisco ACI vCenter プラグインのインストールのトラブルシューティング

このセクションでは、Cisco ACI vCenter プラグインのインストールのトラブルシューティングを行う方法について説明します。

VMware vSphere Web クライアント GUI で Cisco ACI vCenter プラグインが表示されない場合は、以下の操作を実行してください:

- vCenter と .zip ファイルをホストしている Web サーバの間で HTTPS/HTTP トラフィックが動作していることを確認して、.zip ファイルが vCenter からダウンロードできるようにします。
- HTTP Web サーバを使用している場合には、HTTP ダウンロードが有効であることを確認します。
- HTTPS を使用している場合には、使用するサムプリントが 正しいことを確認します。
- 次の URL に移動し、登録が行われたかどうかを確認します。

  https://<*VCENTER_IP*>/mob/?moid=ExtensionManager&doPath=extensionList%5b"com%2ecisco%2eaciPlugin"%5d

  Cisco ACI vCenter プラグインの詳細が表示されるはずです。

  そうならず、ページが空白の場合には、登録が成功しなかったことを示します。これは、登録スクリプトの実行中にエラーが発生したことを意味しています。これを解決するには、もう一度インストール手順を実行し、登録スクリプトでエラーが表示されるかどうかに注意する必要があります。
- vSphere Web クライアント ログを確認します。
  - Linux アプライアンス: `/var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log`
  - 5.5 Windows 2008: `C:\ProgramData\VMware\vSphere Web Client\serviceability\logs\vsphere_client_virgo.log`

- 6.0 Windows 2008:
  %ALLUSERSPROFILE%\VMWare\vCenterServer\logs\vsphere-client\logs\vsphere_client_virgo.log
- ログで「vcenter-plugin」または「com.cisco.aciPlugin」を検索すると、インストール/アップグレードについての関連情報を見つけられます。

正常なアップグレードの例:

```
[2016-05-31T19:32:56.780Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004 com.vmware.vise.vim.extension.VcExtensionManager
Downloading plugin package from https://172.23.137.72/vcenter-plugin-2.0.343.6.zip
(no proxy defined)
[2016-05-31T19:32:56.872Z] [INFO ] m-catalog-manager-pool-11128 70002693 100019
200004
com.vmware.vise.vim.cm.CmCatalogManager
Detected service providers (ms):206
[2016-05-31T19:32:56.872Z] [INFO ] m-catalog-manager-pool-11128 70002693 100019
200004
com.vmware.vise.vim.cm.CmCatalogManager
No new locales or service infos to download.
[2016-05-31T19:32:57.678Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004
com.vmware.vise.vim.extension.VcExtensionManager
Done downloading plugin package from https://172.23.137.72/vcenter-plugin-2.0.343.6.zip

[2016-05-31T19:32:58.438Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004
com.vmware.vise.vim.extension.VcExtensionManager
Done expanding plugin package to /etc/vmware/vsphere-client/vc-packages/vsphere-client-
serenity/com.cisco.aciPlugin-2.0.343.6
[2016-05-31T19:32:58.440Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004
com.vmware.vise.extensionfw.ExtensionManager
Undeploying plugin package 'com.cisco.aciPlugin:2.0.343.5'.
```

参考情報

Cisco ACI vCenter プラグインの代替インストール

ここでは、Cisco ACI vCenter プラグインのインストール方法について説明します。 vCenter と APIC 間で HTTPS トラフィックをイネーブルにできず、独自の Web サーバを使用して Cisco ACI vCenter プラグイン zip ファイルをホストする場合は、次の手順を実行します。

始める前に

- すべての前提条件が満たされていることを確認してください。

  詳細については、Cisco ACI vCenter プラグイン ソフトウェアの要件 （3 ページ）を参照してください。

  詳細については、必要な APIC の設定 （3 ページ）を参照してください。

- PowerCLI コンソールを用意してください。

詳細については、VMware のマニュアルを参照してください。

手順

ステップ 1 .zip ファイルを Web サーバーで使用可能にします。

a) Web サーバーが HTTPS でない場合。デフォルトでは、vCenter は HTTPS ソースからのダウンロードのみを許可します。HTTP を許可するには、vCenter の次の構成ファイルを開いて編集します。

- vCenter 5.5 Linux アプライアンス: **/var/lib/vmware/vsphere-client/webclient.properties**
- vCenter 6.0 Linux アプライアンス: **/etc/vmware/vsphere-client/webclient.properties**
- vCenter 5.5 Windows 2008: **%ALLUSERSPROFILE%\VMware\vSphere Web Client\webclient.properties**
- vCenter 6.0 Windows 2008: **C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\webclient.properties**

b) ファイルの最後に **allowHttp=true** を追加します。

c) Web サーバーが HTTPS でない場合は、「**/etc/init.d/vsphere-client restart**」コマンドを使用して vSphere Web Client サービスを再起動します。

ステップ 2 PowerCLI コンソールまたは Python を使用してスクリプトを実行します。

オプション	説明

PowerCLI コンソールを使用するには	**1.** PowerCLI コンソールを開きます。
	2. **ACIPlugin-Install.ps1** スクリプトを実行します。
	プロンプトが表示されたら、次の情報を入力します。
	• **vCenter IP / FQDN** フィールドに、プラグインをインストールする必要のある vCenter を入力します。
	• **Plugin .zip file URL** フィールドに、vCenter でプラグインをダウンロードできる URL を入力します。
	（注）
	.zip ファイルの名前を変更していないことを確認します。
	• HTTPを使用している場合は、[SHA1 Thumbprint] フィールドを空のままにします。HTTPS を使用している場合は、使用している Web サーバーの SHA1 サムプリントを次のいずれかの形式で入力します。
	• コロンで区切る場合：
	`xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx`
	• スペースで区切る場合：
	`xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx`

オプション	説明
	（注） Windows の一部のブラウザでは、証明書サムプリントが区切り文字のない単一の文字列（たとえば、xxxxxxxxxxxxxxxxx）として表示されることがあります。この場合はインストールスクリプトで正しく処理されません。Web サーバの SHA1 サムプリントで、必ずいずれかの正しい形式を使用してください。そうしないと、Cisco ACI vCenter プラグインが見かけ上障害を起こします。 **3.** ダイアログボックスで、vCenter のルート権限の資格情報を入力します。

Python を使用するには	（注）
	Python 2.7.9 以降を使用し、Python 環境に pyvmomi パッケージをインストールする必要があります。
	Pythonスクリプトを実行します: **`python deployPlugin.py`**
	プロンプトが表示されたら、次の情報を入力します。
	• **[vCenter IP]** フィールドに、プラグインをインストールする必要のある vCenter を入力します。
	• **[vCenter Username & Password]** フィールドに、vCenter のルート権限の資格情報を入力します。
	• **Plugin .zip file URL** フィールドに、vCenter でプラグインをダウンロードできる URL を入力します。
	.zip ファイルの名前を変更していないことを確認します。
	• **[Https server thumbprint]** フィールドで、HTTP を使用している場合は、これを空のままにします。それ以外の場合は、使用する Web サーバーの SHA1 サムプリントを入力します。フィールドはコロンで区切られています。次に例を示します。
	`D7:9F:07:61:10:B3:92:93:E3:49:AC:89:84:5B:03:80:C1:9E:2F:8B`
	（注）
	情報を事前に入力できる **`deploy.cfg`** ファイルもあります。そのファイルを引数としてスクリプトを実行できます。次に例を示します。
	`$ python deployPlugin.py deploy.cfg`

ステップ 3 登録が完了したら、vSphere Web Client にログインします。

（注）
vCenter が Web サーバーからプラグインをダウンロードして展開するため、最初のログインに時間がかかることがあります。

VMware vSphere Web Client がロードされると、**Navigator** ペインに **Cisco ACI Fabric** が表示されます。これにより、ACI ファブリックを管理できます。

（注）
プラグインを登録した後、初めて Web クライアントを起動すると、Web クライアントのリロードを要求するエラー メッセージが表示されることがあります。**[Reload]** をクリックしてページを更新すると、エラー メッセージは表示されません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。