Cisco ACI with Microsoft Windows Azure Pack

この章の内容は、次のとおりです。

- Cisco ACI with Microsoft Windows Azure Pack について （1 ページ）
- Cisco ACI with Microsoft Windows Azure Pack の開始 （5 ページ）
- Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアップグレード （13 ページ）
- 管理者とテナント エクスペリエンスのユース ケース シナリオ （16 ページ）
- Cisco ACI with Microsoft Windows Azure Pack のトラブルシューティング （55 ページ）
- プログラマビリティのリファレンス （56 ページ）
- Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアンインストール （57 ページ）
- Cisco ACI および Microsoft Windows Azure Pack コンポーネントでの Cisco APIC およびスイッチ ソフトウェアのダウングレード （61 ページ）

Cisco ACI with Microsoft Windows Azure Pack について

Cisco Application Centric Infrastructure（ACI）と Microsoft Windows Azure Pack の統合によって、テナントにセルフサービス エクスペリエンスが提供されます。

ACI によってプラットフォームのネットワーク管理機能が拡張されます。Microsoft Windows Azure Pack は、既存の Microsoft System Center Virtual Machine Manager（SCVMM）インストールの最上位に構築されます。Cisco ACI はこれらの各レイヤに統合ポイントを備えています。そのため、SCVMM 環境で実行した作業を活用でき、Microsoft Windows Azure Pack のインストールで使用することができます。

- Cisco ACI with Microsoft Windows Azure Pack（Microsoft Windows Azure Pack for Windows Server）は、次の機能を含む Microsoft Azure テクノロジーのコレクションです。
  - テナント用の管理ポータル
  - 管理者用の管理ポータル
  - サービス管理 API

- Cisco ACI with Microsoft System Center Virtual Machine Manager：Cisco ACI with Microsoft System Center Virtual Machine Manager（SCVMM）を設定する方法の詳細については、「Cisco ACI with Microsoft SCVMM ソリューションの概要」を参照してください。

（注） Windows Azure パックで直接サーバ リターン (DSR) を設定することはできません。DSR を設定する場合は、Cisco APIC で行う必要があります。詳細については、『*Cisco APIC レイヤ 4 ～レイヤ 7 サービス導入ガイド*』の「直接サーバ リターンの設定」の章を参照してください。

Cisco ACI with Microsoft Windows Azure Pack ソリューションの概要

Cisco Application Centric Infrastructure（ACI）と Microsoft Windows Azure Pack の統合によって、テナントにセルフサービス エクスペリエンスが提供されます。Windows Azure Pack の ACI リソース プロバイダーによって Application Policy Infrastructure Controller（APIC）が動作し、ネットワーク管理機能がもたらされます。ネットワークは、System Center Virtual Machine Manager（SCVMM）で作成され、それぞれのテナントのために Windows Azure Pack で使用可能になります。ACI の F5 のレイヤ 4 ～レイヤ 7 機能、Citrix ロード バランサ、およびステートレスのファイアウォールがテナントに提供されます。詳細については、ロード バランシングの概要（29 ページ）を参照してください。

Windows Server 向けの Windows Azure Pack は、Microsoft の顧客が使用可能な Microsoft Azure テクノロジーのコレクションで、データセンターへのインストールに追加コストはかかりません。Windows Server 2012 R2 および System Center 2012 R2 で動作し、Windows Azure テクノロジーを使用することで、Windows Azure エクスペリエンスとともに、豊富なセルフサービス、マルチテナント クラウド、一貫性の提供を実現します。

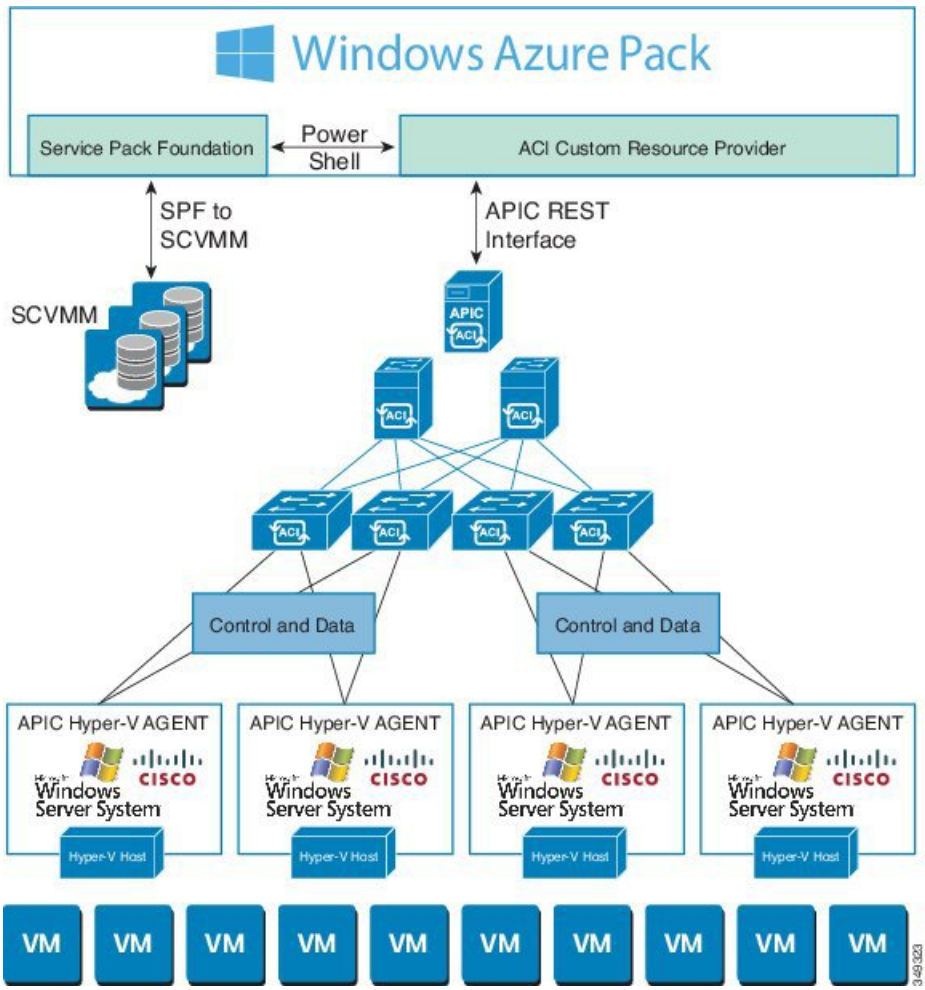
Windows Azure Pack には次の機能があります。

- テナントの管理ポータル：ネットワーク、ブリッジ ドメイン、VM、ファイアウォール、ロードバランサ、外部接続、共有サービスなどのサービスをプロビジョニング、監視、および管理するためのカスタマイズ可能なセルフサービス ポータル。ユーザ ポータルの GUI を参照してください。
- 管理者の管理ポータル：リソース クラウド、ユーザ アカウント、テナントのオファー、クォータ、価格設定、Web サイトのクラウド、仮想マシンのクラウド、およびサービス バスのクラウドを設定し管理する管理者のためのポータル。
- サービス管理 API：カスタム ポータルや課金システムなどのさまざまな統合シナリオの実現に役立つ REST API。

詳細については、管理者とテナント エクスペリエンスのユース ケース シナリオ（16 ページ）を参照してください。

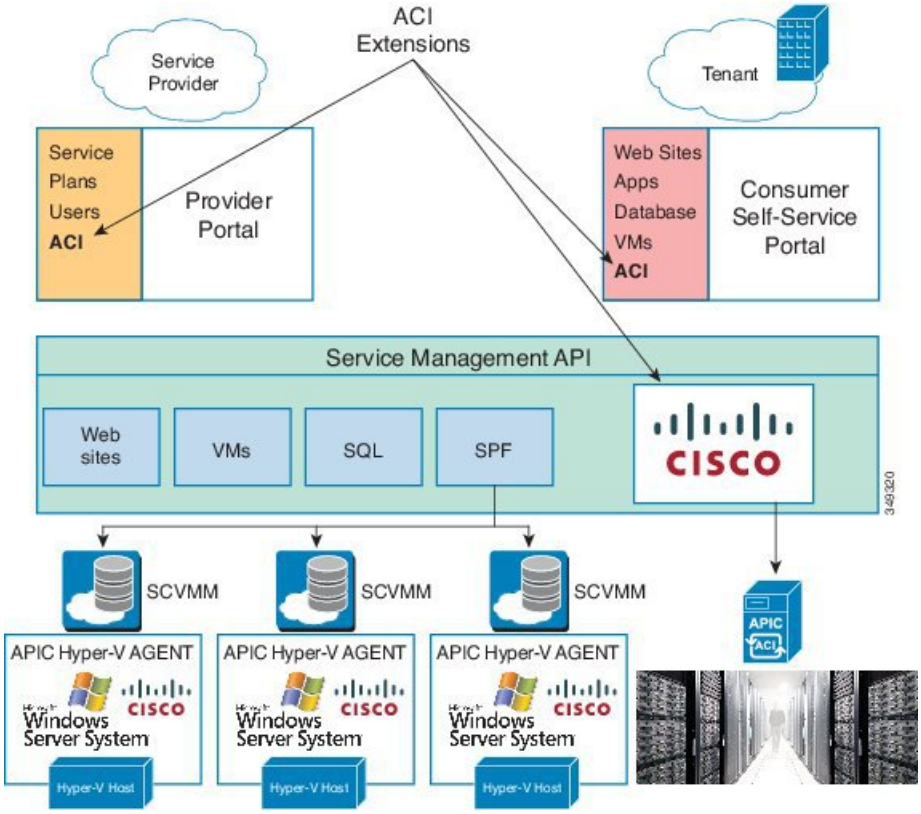
物理トポロジと論理トポロジ

図 *1 : ACI* ファブリックを使用した標準的な *Windows Azure Pack* 導入トポロジ



前の図は、Cisco Application Centric Infrastructure（ACI）ファブリックを使用した標準的な Windows Azure Pack 導入の代表的なトポロジを示しています。Windows Azure Pack と Application Policy Infrastructure Controller（APIC）間の接続は管理ネットワークを経由します。テナントインターフェイスは、GUI または REST API のどちらかを介して Windows Azure Pack のみを対象とします。テナントからは APIC に直接アクセスすることはできません。

図 *2 : ACI* リソース プロバイダー フレームワークにおける *ACI*



Microsoft Windows Azure Pack での ACI 構造のマッピングについて

ここでは、Microsoft Windows Azure Pack での Cisco Application Centric Infrastructure（ACI）のマッピングの表を示します。

表 *1 : ACI* および *Windows Azure Pack* の構造のマッピング

Windows Azure Pack	ACI
サブスクリプション	テナント
ネットワーク	EPG
ファイアウォール ルール	テナント内の契約
共有サービス	テナント間の契約
SCVMM クラウド	VM ドメイン

Cisco ACI with Microsoft Windows Azure Pack の開始

ここでは、Cisco ACI with Microsoft Windows Azure Pack を使い始める方法について説明します。

Cisco をインストールする前に ACI 、Microsoft Windows Azure Pack をダウンロードして、Cisco が入っているフォルダを解凍 ACI Cisco APIC リリースの Microsoft 統合ファイルに一致するとします。

1. Cisco's Application Policy Infrastructure Controller (APIC) website に移動します。
2. **All Downloads for this Product** > **APIC Software** を選択します。
3. リリースのバージョンと、それに適合する zip 圧縮フォルダを選択します。
4. [Download] をクリックします。
5. Zip 圧縮のフォルダに解凍します。

（注） Cisco ACI with Microsoft Windows Azure Pack は ASCII 文字のみをサポートします。非 ASCII 文字はサポートしていません。

Windows のシステム ロケールとして **English** が設定されていることを確認します。それ以外の場合、CiscoACI with Windows Azure Pack はインストールされません。また、インストールの後にシステム ロケールを英語以外に変更した場合、Cisco APIC および Cisco ACI ファブリックとの通信の際に、統合コンポーネントがエラーを生じる場合があります。

Cisco ACI with Microsoft Windows Azure Pack を開始するための前提条件

開始する前に、コンピューティング環境が以下の前提条件を満たしていることを確認します。

- Cisco Application Centric Infrastructure（ACI）with Microsoft System Center Virtual Machine Manager（SCVMM）の設定が完了していることを確認します。

  詳細については、Cisco ACI with Microsoft SCVMM の開始を参照してください。

- Microsoft Windows Azure Pack の更新ロールアップ 5、6、7、9、10 または 11 がインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- Windows Server 2016 がインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- Hyper-V ホストがインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- クラウドが SCVMM で設定されていることを確認します。

Microsoft のマニュアルを参照してください。

- VM クラウドが Windows Azure Pack で設定されていることを確認します。

  Microsoft のマニュアルを参照してください。

- インフラストラクチャ VLAN が有効な「default」 AEP が存在することを確認します。
- 「default」および「vpcDefault」ブリッジ ドメイン と、対応する「default」および「vpcDefault」EPG がテナントに共通して存在することを確認します。
- APIC Windows Azure Pack リソースおよびホスト エージェント用の Cisco MSI ファイルがあることを確認します。

  詳細については、Cisco ACI with Microsoft SCVMM の開始を参照してください。

（注） 症状：プランを作成または更新するときに、エラー メッセージが表示されて失敗することがあります。

条件：FQDN を使用せずに Microsoft の Windows Azure Pack を設定している場合に、次のエラー メッセージが表示されます。

```
Cannot validate the new quota settings because one of the underlying services failed to
respond. Details: An error has occurred.
```

回避策：VM クラウドを設定するときは、SCVMM サーバに FQDN を使用するよう通知する Microsoft の Windows Azure Pack UI の指示に従います。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのインストール、設定および確認

ここでは、Cisco ACI with Microsoft Windows Azure Pack コンポーネントをインストール、設定および確認する方法を説明します。

コンポーネント	タスク
ACI Azure Pack のリソース プロバイダーのインストール	ACI Azure Pack リソース プロバイダーのインストール （7 ページ）を参照してください。
OpflexAgent 証明書のインストール	OpflexAgent 証明書のインストール （7 ページ）を参照してください。
ACI Azure Pack のリソース プロバイダー サイトの設定	ACI Azure Pack のリソース プロバイダー サイトの設定 （10 ページ）を参照してください。
ACI Azure Pack の管理者サイト拡張のインストール	ACI Azure Pack の管理者サイト拡張のインストール （11 ページ）を参照してください。

コンポーネント	タスク
ACI Azure Pack のテナント サイト拡張のインストール	ACI Azure Pack のテナント サイト拡張のインストール （11 ページ）を参照してください。
ACI の設定	ACI のセットアップ （11 ページ）を参照してください。
Windows Azure Pack のリソース プロバイダーの確認	Windows Azure Pack のリソース プロバイダーの確認 （12 ページ）を参照してください。

ACI Azure Pack リソース プロバイダーのインストール

ここでは、Windows Azure Pack サーバに ACI Azure Pack リソース プロバイダーをインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack 環境に VM クラウドを提供する Microsoft Service Provider Foundation サーバにログインします。ACI Azure Pack - Resource Provider Site.msi ファイルを見つけてコピーします。

ステップ 2 ACI Azure Pack - Resource Provider Site.msi ファイルをダブルクリックします。

ステップ 3 [Setup] ダイアログボックスで以下の操作を実行し、ACI Azure Pack - リソース プロバイダーをインストールします。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。
b) [Install] をクリックします。
c) [Install] をクリックします。
d) [Finish] をクリックします。

OpflexAgent 証明書のインストール

ここでは、OpflexAgent 証明書をインストールする方法について説明します。

手順

ステップ 1 管理者クレデンシャルで Windows Azure Pack サーバにログインします。

ステップ 2 次のいずれかの方法を使用します。

- 大規模な展開の場合、グループ ポリシーを使用した証明書の展開について、Microsoft ドキュメントを参照してください。

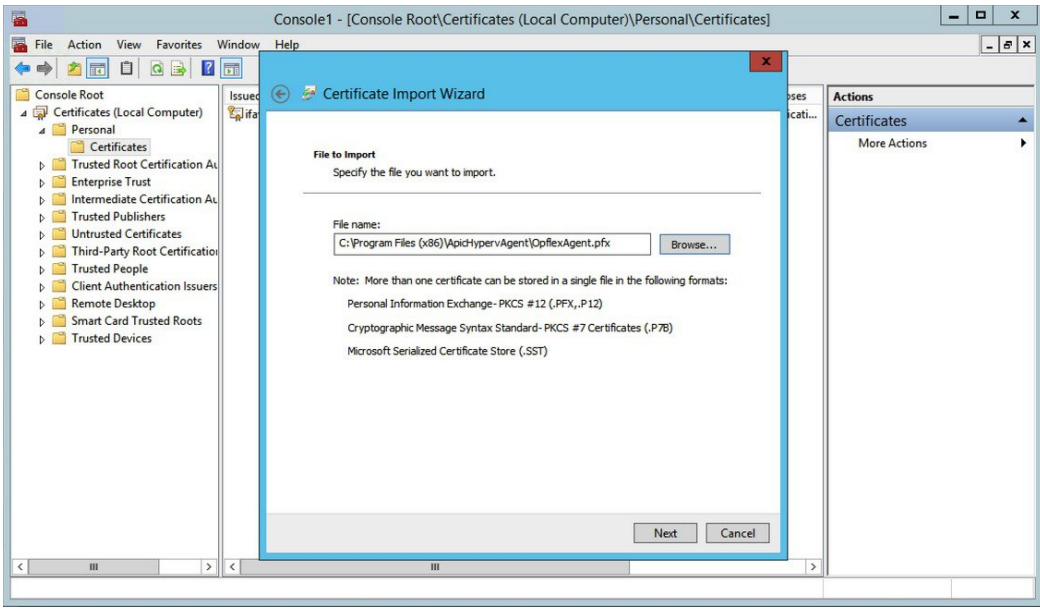
  https://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx。

- 小規模な展開の場合は、次の手順に従います。

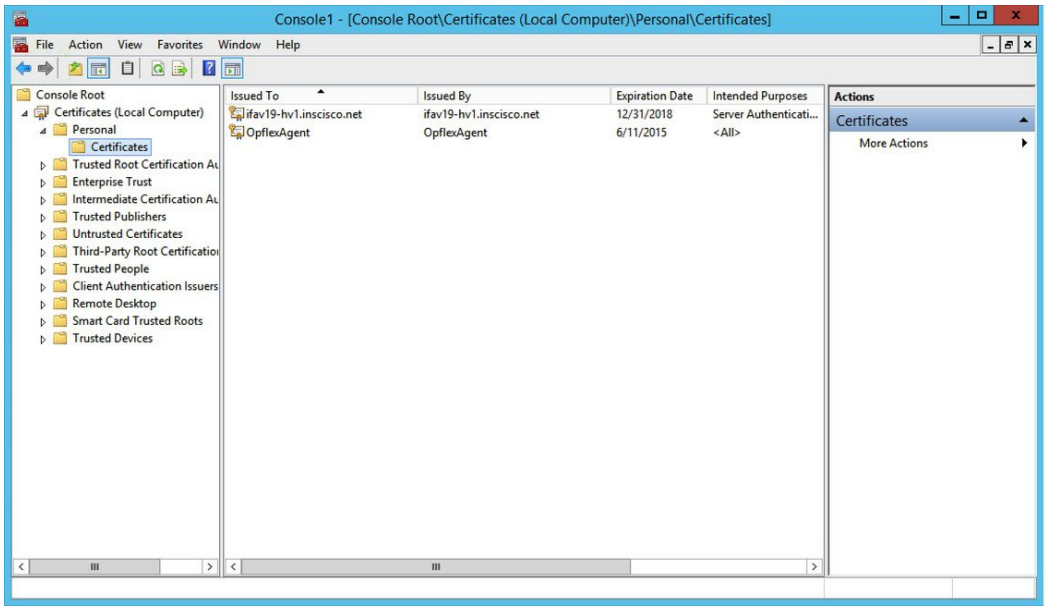
  ローカル システムに OpFlex セキュリティ証明書を追加する必要があります。ACI Windows Azure Pack のリソース プロバイダーは、SCVMM サーバ上にある（**C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx**）、Cisco ACI SCVMM インストール プロセスからの同じセキュリティ証明書ファイルを使用します。このファイルを Windows Azure Pack のリソース プロバイダー サーバにコピーします。ACI Windows Azure Pack のリソース プロバイダー サーバで次の手順を実行しない場合、APIC ACI Windows Azure Pack のリソース プロバイダーは Application Policy Infrastructure Controller（APIC）と通信できません。

  ACI Windows Azure Pack のリソース プロバイダーの Windows Server 2012 ローカル マシンの証明書リポジトリに、OpFlex セキュリティ証明書をインストールします。各 ACI Windows Azure Pack のリソース プロバイダー サーバで次の手順を実行して、この証明書をインストールします。

  1. **[Start]** > **[Run]** を選択します。
  2. **mmc** と入力し、**[OK]** をクリックします。
  3. [Console Root] ウィンドウのメニュー バーで、[Add/Remove Snap-in] を選択します。
  4. [Available Snap-ins] フィールドで [Certificates] を選択して [Add] をクリックします。
  5. [Certificates snap-in] ダイアログボックスで [Computer Account] オプション ボタンを選択し、[Next] をクリックします。
  6. [Select Computer] ダイアログボックスで [Local Computer] オプション ボタンを選択し、[Finish] をクリックします。
  7. [OK] をクリックして、[MMC Console] メイン ウィンドウに戻ります。
  8. [MMC Console] ウィンドウで [Certificates (local computer)] をダブルクリックして、ビューを展開します。
  9. [Personal] の下で [Certificates] を右クリックして、**[All Tasks]** > **[Import]** の順に選択します。
  10. [Certificates Import Wizard] ダイアログボックスで、次の操作を実行します。
      1. [Next] をクリックします。
      2. **Opflex Agent** ファイルを参照して [Next] をクリックします。



11. MSI のインストール時に提供された証明書のパスワードを入力します。
12. [Mark this key as exportable.This will allow you to back up or transport your keys at a later time] オプション ボタンを選択する必要があります。
13. [Include all extended properties] オプション ボタンを選択します。
14. [Place all certificates in the following store] オプション ボタンを選択し、[Personal] を見つけて [Next] をクリックします。
15. [Finish] をクリックします。
16. [OK] をクリックします。



ACI Azure Pack のリソース プロバイダー サイトの設定

ここでは、Windows Azure Pack サーバで ACI Azure Pack のリソース プロバイダー IIS サイトを設定する方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、[Internet Information Services Manager Application] を開きます。

ステップ 2 **[Application Pools]** > **[Cisco-ACI]** に移動します。

ステップ 3 [Actions] タブで [Advanced Settings] をクリックします。

a) ID フィールドを見つけて、スクロール バーの左側の省略記号をクリックします。

b) カスタム アカウントを選択し、Service Provider Foundation 管理者のアカウント名とパスワードからなるクレデンシャルを入力します。Service Provider Foundation 管理者のユーザ アカウントには、Administrator、SPF_Admin のグループ メンバーシップが必要です。このユーザ アカウントが必要なのは、リソース プロバイダーが接続された SCVMM サーバを問い合わせるためです。また、ユーザ クレデンシャルには、ローカル マシンのレジストリへの書き込み権限、リソース プロバイダーのロギング用に次のディレクトリへの読み取り/書き込みアクセス権が必要です。

C:\Windows\System32\config\systemprofile\AppData\Local

c) [OK] をクリックして、アプリケーション プール ID を終了します。

ステップ 4 [OK] をクリックして、拡張設定を終了します。

ACI Azure Pack の管理者サイト拡張のインストール

ここでは、Windows Azure Pack サーバに ACI Azure Pack の管理者サイト拡張をインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、**ACI Azure Pack - Admin Site Extension.msi** ファイルを見つけます。

ステップ 2 **ACI Azure Pack - Admin Site Extension.msi** ファイルをダブルクリックします。

ステップ 3 [Setup] ダイアログボックスで、次の操作を実行して ACI Azure Pack の管理者サイト拡張をインストールします。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。
b) [Install] をクリックします。
c) [Finish] をクリックします。

ACI Azure Pack のテナント サイト拡張のインストール

ここでは、Windows Azure Pack サーバに ACI Azure Pack のテナント サイト拡張をインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、**ACI Azure Pack - Tenant Site Extension.msi** ファイルを見つけます。

ステップ 2 **ACI Azure Pack - Tenant Site Extension.msi** ファイルをダブルクリックします。

ステップ 3 [Setup] ダイアログボックスで、次の操作を実行して ACI Azure Pack のテナント サイト拡張をインストールします。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。
b) [Install] をクリックします。
c) [Finish] をクリックします。

ACI のセットアップ

ここでは、ACI の設定方法について説明します。

手順

ステップ 1 サービス管理ポータルにログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

[ACI] がない場合、[Refresh] をクリックします。

ステップ 3 QuickStart アイコンをクリックします。

ステップ 4 [QuickStart] ペインで、次の操作を順序どおりに実行します。

a) [Register your ACI REST endpoint] をクリックします。
b) [ENDPOINT URL] フィールドに、リソース プロバイダー アドレスである Cisco-ACI ポート（http://*resource_provider_address*:50030）を入力します。
c) [USERSNAME] フィールドに、ユーザ名（ドメイン管理者）を入力します。
d) [PASSWORD] フィールドに、パスワード（ドメイン管理者のパスワード）を入力します。

ステップ 5 **[ACI]** > **[Setup]** タブを選択し、次の操作を実行します。

a) [APIC ADDRESS] フィールドに、APIC IP アドレスを入力します。
b) [CERTIFICATE NAME] フィールドに OpflexAgent と入力します。

Windows Azure Pack のリソース プロバイダーの確認

ここでは、Windows Azure Pack のリソースプロバイダーを確認する方法について説明します。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [aci] ペインで QuickStart Cloud アイコンを選択します。

[Register your ACI REST Endpoint] リンクがグレー表示になっていることを確認します。

ステップ 4 [aci] ペインで [SETUP] を選択します。

APIC アドレスに有効な apic アドレスがあり、証明書名が OpflexAgent であることを確認します。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアップグレード

前提条件：

ACI に統合する Microsoft サーバは、ACI を 2.0(1) リリースにアップグレードする前に、KB2919355 と KB3000850 の更新ロールアップで更新する必要があります。KB2919355 更新ロールアップには、2929781 のパッチが含まれており、新しい TLS 暗号スイートを追加し、Windows 8.1 および Windows サーバ 2012 R2 で暗号スイートの優先順位を変更します。

次の Microsoft サーバにパッチを適用する必要があります:

- Microsoft Windows Azure パック リソース プロバイダ サーバ
- Microsoft Windows Azure パック テナント サイト サーバ
- Microsoft Windows Azure パック管理サイト サーバ
- Microsoft System Center のサービス プロバイダの基盤/オーケストレーション サーバ
- Microsoft System Center 2012 R2 サーバ
- Microsoft HyperV 2012 R2 サーバ

各 Cisco ACI with Windows Azure Pack 統合の `.msi` ファイルをアップグレードするには、更新プログラム ロールアップごとにリストされる Windows Azure Pack コンポーネントをアップグレードするための Microsoft の全般的なガイドラインに従います。全般的なガイドラインは次のとおりです。

- システムが現在稼働中（顧客のトラフィックを処理中）の場合は、Azure サーバのダウンタイムをスケジュールします。Windows Azure Pack は現在ローリング アップグレードをサポートしていません。
- 顧客のトラフィックを停止するか、適切と思われるサイトにリダイレクトします。
- コンピュータのバックアップを作成します。

（注） 仮想マシン（VM）を使用している場合は、現在の状態のスナップショットを撮ります。

VM を使用していない場合は、Windows Azure Pack コンポーネントがインストールされている各マシンの `inetpub` ディレクトリの各 `MgmtSvc-*` フォルダのバックアップを作成します。

証明書、ホスト ヘッダーなどのポートの変更に関連するファイルと情報を収集します。

アップグレードが完了し確認したら、VM スナップショットの管理に関する Hyper-V のベストプラクティス（https://technet.microsoft.com/en-us/library/dd560637(v=ws.10).aspx）に従います。

ACI Windows Azure Pack ワークフローのアップグレード

ここでは、ACI Windows Azure Pack のワークフローをアップグレードする方法を説明します。

手順

ステップ 1 APIC コントローラとスイッチ ソフトウェアをアップグレードします。

『*Cisco APIC Firmware Management Guide*』を参照してください。

ステップ 2 ACI Windows Azure Pack をアップグレードします。

1.1(2x) 以前のリリースからアップグレードする場合：

a) APIC Windows Azure Pack のリソース プロバイダーをアンインストールする必要があります。「APIC Windows Azure Pack のリソース プロバイダーのアンインストール （58 ページ）」を参照してください。

b) Cisco ACI with Microsoft Windows Azure Pack コンポーネントのインストール、設定および確認 （6 ページ）の手順に従います。

c) ステップ 6 に進み、SCVMM で APIC SCVMM エージェントをアップグレードするか、高可用性 SCVMM で APIC SCVMM エージェントをアップグレードします。

リリース 1.1(2x) 以降からアップグレードする場合：

a) ステップ 3 に進みます。

ステップ 3 ACI Windows Azure Pack のリソース プロバイダーをアップグレードします。

詳細については、ACI Windows Azure Pack リソース プロバイダーのアップグレード （15 ページ）を参照してください。

ステップ 4 ACI Azure Pack の管理者サイト拡張をアップグレードします。

詳細については、ACI Azure Pack 管理者サイト拡張のアップグレード （15 ページ）を参照してください。

ステップ 5 ACI Azure Pack のテナント サイト拡張をアップグレードします。

詳細については、ACI Azure Pack テナント サイト拡張のアップグレード （16 ページ）を参照してください。

ステップ 6 SCVMM で APIC SCVMM エージェントをアップグレードするか、高可用性 SCVMM で APIC SCVMM エージェントをアップグレードします。

詳細については、SCVMM での APIC SCVMM エージェントのアップグレードを参照してください。

詳細については、可用性の高い SCVMM 上の APIC SCVMM エージェントのアップグレードを参照してください。

ステップ 7 APIC Hyper-V エージェントをアップグレードします。

詳細については、APIC Hyper-V エージェントのアップグレードを参照してください。

ACI Windows Azure Pack リソース プロバイダーのアップグレード

ここでは、ACI Windows Azure Pack のリソース プロバイダーをアップグレードする方法を説明します。

手順

ACI Windows Azure Pack のリソース プロバイダーをアップグレードします。

リリース 1.1(2x) 以降からアップグレードする場合：

a) ACI Azure Pack リソース プロバイダーのインストール （7 ページ）の手順に従ってください。

   MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

b) ACI Azure Pack のリソース プロバイダー サイトの設定 （10 ページ）の手順に従ってください。

1.1(2x) 以前のリリースからアップグレードする場合：

a) APIC Windows Azure Pack のリソース プロバイダーのアンインストール （58 ページ）の手順に従ってください。
b) ACI Azure Pack リソース プロバイダーのインストール （7 ページ）の手順に従ってください。

   MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

c) ACI Azure Pack のリソース プロバイダー サイトの設定 （10 ページ）の手順に従ってください。

ACI Azure Pack 管理者サイト拡張のアップグレード

ここでは、ACI Azure Pack の管理者サイト拡張をアップグレードする方法を説明します。

手順

ACI Azure Pack の管理者サイト拡張をアップグレードします。

a) ACI Azure Pack の管理者サイト拡張のインストール （11 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

ACI Azure Pack テナント サイト拡張のアップグレード

ここでは、ACI Azure Pack のテナント サイト拡張をアップグレードする方法を説明します。

手順

ACI Azure Pack のテナント サイト拡張をアップグレードします。

a) ACI Azure Pack のテナント サイト拡張のインストール （11 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

管理者とテナント エクスペリエンスのユース ケース シナリオ

ここでは、管理者とテナントエクスペリエンスのユース ケース シナリオについて説明します。

（注） 共有サービス コンシューマは、プロバイダーよりも異なる VRF では、ルート漏出、Vrf 間では、通信を有効にするには自動的に発生します。

Use case	共有プラン	VPC プラン	ユーザ	タスク
プランの作成 これにより、管理者は独自の制限値を使用してプランを作成できます。	○	○	Admin	1.プラン タイプについて （21 ページ）を参照してください。
			Admin	2.プランの作成 （23 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
テナントの作成 これにより、管理者はテナントを作成できます。	○	○	Admin	テナントの作成 （24 ページ）を参照してください。
共有プランでのネットワークの作成と検証 これにより、テナントは共有プランのネットワークを作成し検証できます。	○	なし	テナント	1.共有プランでのネットワークの作成 （40 ページ）を参照してください。
			テナント	2.APIC の Microsoft Windows Azure Pack で作成されたネットワークの確認 （40 ページ）を参照してください。
VPC プランでのネットワークの構築 これにより、テナントは VPC プランでネットワークを作成できます。	なし	○	テナント	VPC プランでのネットワークの構築 （42 ページ）を参照してください。
VPC プランのブリッジ ドメインの作成、ネットワークの作成、およびブリッジ ドメインの関連付け 仮想プライベート クラウド（VPC）プランのみに適用されます。これにより、テナントはネットワークに対する独自の IP アドレス空間を取得できます。	なし	○	テナント	1.VPC プランでのブリッジ ドメインの作成 （40 ページ）を参照してください。
			テナント	2.VPC プランでのネットワークの作成およびブリッジ ドメインへの関連付け （41 ページ）を参照してください。
同一サブスクリプション内のファイアウォールの作成 これにより、テナントは同一サブスクリプション内にファイアウォールを作成できます。	○	○	テナント	同一サブスクリプション内のファイアウォールの作成 （41 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
テナントによる共有サービス提供の許可 これにより、テナントはネットワークを作成し、作成したネットワークにコンピューティング サービス（サーバ）を接続し、他のテナントにこれらのサービスへの接続を提供できます。管理者は、プランで明示的にこの機能を有効にする必要があります。	○	○	Admin	1.テナントによる共有サービス提供の許可 （25 ページ）を参照してください。
			テナント	2.共有サービスの提供 （44 ページ）を参照してください。
			テナント	3.アクセス コントロール リストの追加 （46 ページ）またはアクセス コントロール リストの削除 （46 ページ）を参照してください。
			Admin	4.テナントによる共有サービス消費の許可 （26 ページ）を参照してください。
			テナント	5.消費される共有サービスの設定 （44 ページ）を参照してください。
			Admin	6.共有サービス プロバイダーとコンシューマの表示 （27 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
NAT を消費するためにテナントを許可するファイアウォールと ADC ロード バランサ サービス	なし	○	Admin	1.NAT ファイアウォールおよび ADC ロードバランサ サービスを消費するテナントを許可する （26 ページ）を参照してください。
			テナント	2.VM ネットワークに NAT ファイアウォール レイヤ 4 ～ レイヤ 7 サービスを追加する （50 ページ）を参照してください。
			テナント	3.NAT ファイアウォール ポート転送ルールを VM ネットワークに追加する （51 ページ）を参照してください。
			テナント	4.プライベート ADC ロードバランサ レイヤ 4 ～ レイヤ 7 サービスを伴う NAT ファイアウォールを VM ネットワークに追加する （51 ページ）を参照してください。
			テナント	5.パブリック ADC ロードバランサ レイヤ 4 ～ レイヤ 7 サービスを VM ネットワークに追加する （53 ページ）を参照してください。
			テナント	6.VM ネットワークに ADC ロードバランサの設定を追加する （54 ページ）を参照してください。
共有サービスの管理 これにより、管理者は新しいテナントの共有サービスを廃止し、共有サービスからのテナントアクセスを取り消すことができます。	○	○	Admin	新しいテナントからの共有サービスの廃止 （28 ページ）を参照してください。 共有サービスからのテナントの取り消し （28 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
VM の作成とネットワークへの接続	○	○	テナント	VM の作成とネットワークへの接続 （43 ページ）を参照してください。
ロード バランサの作成	○	○	Admin	1.ロード バランシングの概要 （29 ページ）を参照してください。
			Admin	2.APIC でのデバイス パッケージのインポート （29 ページ）を参照してください。
			Admin	3.XML POST を使用した APIC でのロード バランサ デバイスの設定 （30 ページ）を参照してください。
			Admin	4.プランに合わせたロード バランサの作成 （36 ページ）を参照してください。
			テナント	5.ロード バランサの設定 （45 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
外部接続の作成 これにより、テナントネットワークでファブリックの外部宛てに送信されるトラフィックを開始し、外部からのトラフィックを引き付けることができます。	○	○	APIC 管理者	1.L3 外部接続について （37 ページ）を参照してください。
			APIC 管理者	2.Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （37 ページ）を参照してください。
			APIC 管理者	3.l3extinstP「default」で提供される契約の作成 （38 ページ）を参照してください。
			APIC 管理者	4.l3extinstP「vpcDefault」で提供される契約の作成 （39 ページ）を参照してください。
			テナント	5.外部接続用ネットワークの作成 （48 ページ）を参照してください。
			テナント	6.外部接続用のファイアウォールの作成 （48 ページ）を参照してください。
			APIC 管理者	7.APIC でのテナントの L3 外部接続の確認 （49 ページ）を参照してください。

管理タスク

プラン タイプについて

管理者は独自の価値観でプランを作成します。プラン タイプは次のとおりです。

	共有インフラストラクチャ	仮想プライベート クラウド
分離ネットワーク	○	○
ファイアウォール	○	○
プロバイダー DHCP	Yes	あり *
共有ロード バランサ	Yes	あり *

	共有インフラストラクチャ	仮想プライベート クラウド
パブリック インターネット アクセス	○	○
テナント間共有サービス	○	○
独自のアドレス空間（プライベート アドレス空間）と DHCP サーバの保持	なし	○

*仮想プライベート クラウド（VPC）プランでは、プライベート アドレス空間に対するロードバランサと DHCP はサポートされません。いずれの機能もテナントには提供されますが、共有インフラストラクチャによって所有されます。

プラン オプションについて

このセクションでは、プラン オプションについて説明します。

- APIC テナント:APIC テナントの自動作成を無効にする
  - デフォルト: 選択されていません。

    選択されていない: Cisco ACI Azure Pack リソースプロバイダは自動的に APIC テナントを作成/削除します。APIC テナント名は、Windows Azure Pack テナントのサブスクリプション ID (GUID) になります。リソース プロバイダが必要なすべてのマッピングを処理するため、APIC 管理者による手動の介入は不要です。

    選択: Cisco ACI Azure Pack リソース プロバイダは、APIC テナントを自動的に作成/削除しません。APIC テナントは Windows Azure Pack サブスクリプション ID に明示的にマップする必要があります。このマッピングが APIC で確立されると、Azure Pack テナントは、ネットワーク、ファイアウォール、ロードバランサなどとの通常の操作を実行できます。

- APIC テナントの自動作成を無効にすることで有効になる機能
  - SCVMM と Windows Azure Pack VM のネットワーク名は、GUID ではなく APIC テナント名を使用します。これにより、SCVMM 管理者および Azure Pack テナントの可読性が向上します。VM ネットワークは GUID ではなくフレンドリーな名前を持つためです。

- プラン クォータ: Azure Pack プラン管理者は、Azure Pack テナントが作成できる EPG、BD、および VRF の数を制限するプランを作成できるようになりました。
  - APIC 管理者が APIC の下で作成した EPG、BD、および VRF は、Azure Pack プランの割り当て量にカウントされます。
    - 例 1: プラン管理者は、EPG の上限が 5 つの Azure Pack プランを作成します。Azure Pack テナントは 4 つの EPG を作成し、APIC 管理者は Azure Pack テナントの EPG

を作成します。Azure Packテナントは現在、プラン クォータに達しており、プラン クォータ以下になるまで EPG を作成することはできません。

- 例 2: プラン管理者は、EPG の上限が 5 つの Azure Pack プランを作成します。Azure Pack テナントは 5 つの EPG を作成します。APIC 管理者が Azure Pack テナントの EPG を作成します。Azure Packのテナントは現在、プラン クォータに達しており、プラン クォータ以下になるまで EPG を作成することはできません。
- これらのクォータは、Azure Pack テナントに適用されますが、APIC 管理者には適用されません。APIC 管理者は、テナントが自分のクォータを超えた場合でも Azure Pack テナントの EPG、BD、VRF を作成し続けることができます。

- すべてのプラン タイプ: EPG の公開
  - APIC 管理者が EPG を Windows Azure Pack テナントにプッシュできるようになりました。
  - APIC 管理者は、APIC に EPG を作成し、それをテナントプランに関連付けられた VMM ドメイン (SCVMM Cloud) に関連付けることで、Azure Pack テナント用の EPG を作成できるようになりました。
  - テナントの下の「デフォルト」のアプリケーションプロファイルは、Azure Packテナントの所有スペースとみなされます。これはAzure Packテナントが契約を結んで削除できることを意味します。
  - 他のすべてのアプリケーション プロファイルは、APIC 管理者が所有するスペースと見なされます。これらの EPG は、Azure Pack テナントが使用できるようになりますが、Azure Packテナントは、仮想マシンネットワーク アダプタとの関連付け以外で、EPG の変更、削除、または操作を行うことはできません。

プランの作成

これにより、管理者は独自の値でプランを作成できます。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 [Navigation] ペインで [PLANS] を選択します。

ステップ 3 [NEW] を選択します。

ステップ 4 [NEW] ペインで [CREATE PLAN] を選択します。

ステップ 5 [Let's Create a Hosting Plan] ダイアログボックスで、プラン（ブロンズ）の名前を入力し、矢印をクリックして次に進みます。

ステップ 6 [Select services for a Hosting Plan] ダイアログボックスで機能を選択します。[VIRTUAL MACHINE CLOUDS] および [NETWORKING (ACI)] チェックボックスをオンにし、矢印をクリックして次に進みます。

ステップ 7 [Select add-ons for the plan] ダイアログボックスで、チェックマークをクリックして次に進みます。

ステップ 8 [plans] ペインで、プラン（ブロンズ）が作成されるのを待って、（ブロンズ）プラン矢印を選択して設定します。

ステップ 9 プランのサービスの [Bronze] ペインで、[Virtual Machine Clouds] 矢印を選択します。

ステップ 10 [virtual machine clouds] ペインで、次の操作を実行します。

a) [VMM MANAGEMENT SERVER] フィールドで、VMM 管理サーバ（172.23.142.63）を選択します。
b) [VIRTUAL MACHINE CLOUD] フィールドで、クラウド名（Cloud01）を入力します。
c) 下にスクロールして、[Add templates] を選択します。
d) [Select templates to add to this plan] ダイアログボックスで、テンプレートのチェックボックスをオンにし、チェックマークをクリックして次に進みます。
e) [Custom Settings] まで下にスクロールして、SCVMM について [Disable built-in network extensions for tenants] チェックボックスをオンにします。
f) 下部で [SAVE] をクリックします。
g) 終了したら、[OK] をクリックします。

ステップ 11 サービス管理ポータルで、戻る矢印をクリックすると、[Bronze] ペインに戻ります。

ステップ 12 プランのサービスの [Bronze] ペインで、[Networking (ACI)] をクリックして、次の操作を実行します。

a) [PLAN TYPE] フィールドで、ドロップダウン リストからプラン タイプを選択します。
b) 仮想プライベートクラウドプランタイプでは、「テナントごとに許可される最大EPG」、「テナントごとに許可される最大 Bd」、「テナントごとに許可される最大 CTX」に 1 ～ 4000 の間の有効な値を入力します。

   共有インフラストラクチャ プラン タイプでは、「テナントごとに許可される最大 EPG」に 1 ～ 4000 の間の有効な値を入力します。

c) [SAVE] をクリックします。

ステップ 13 [OK] をクリックします。
プランが作成されました。

テナントの作成

これにより、管理者はテナントを作成できます。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで、[USER ACCOUNTS] を選択します。

ステップ 3 [NEW] を選択します。

ステップ 4 [NEW] ペインで下にスクロールし、[USER ACCOUNTS] を選択します。

ステップ 5 [NEW] ペインで、[QUICK CREATE] を選択し、以下の操作を実行します。

a) [ENTER EMAIL ADDRESS] フィールドに電子メール アドレス（tenant@domain.com）を入力します。
b) [ENTER PASSWORD] フィールドにパスワードを入力します。
c) [CONFIRM PASSWORD] フィールドに同じパスワードをもう一度入力します。
d) [CHOOSE PLAN] フィールドでプラン（BRONZE）を選択します。
e) [CREATE] をクリックします。
f) [OK] をクリックします。
テナントが作成されました。

ステップ 6 「APIC テナントの自動作成を無効にする」というプランに関連付けられている Windows Azure パック テナントの場合、Azure パック テナントのログイン情報とサブスクリプション ID をメモしておいてください。

a) APIC GUI にログインし、メニューバーで **TENANTS** > **Tenant Name** を選択します。このテナントは、Azure パック サブスクリプション マッピングをターゲットとする APIC テナントを対象にしています。
b) **Policy** タブを選択します。
c) [GUID] セクションで、+ アイコンをクリックして、新しい Azure パック サブスクリプション マッピングを追加します。
d) Azure パック テナントのサブスクリプション ID を持つ GUID と、Azure パックのログイン アカウントを持つアカウント名を入力します。
e) **Submit** をクリックして変更を保存します。

（注） APIC テナントがマッピングできるのは、ただ 1 つの Azure パック テナント サブスクリプション ID だけです。

テナントによる共有サービス提供の許可

このオプションにより、テナントはネットワークを作成し、コンピューティング サービス（サーバ）をこれらのネットワークに接続し、他のテナントにこれらのサービスへの接続を提供することができます。管理者は、プランで明示的にこの機能を有効にする必要があります。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 [Navigation] ペインで [PLANS] を選択します。

a) プランを選択します。
b) プランのサービスで、[Networking (ACI)] をクリックします。

ステップ 3 [networking (aci)] ペインで [allow tenants to provide shared services] チェックボックスをオンにして、[SAVE] をクリックします。

テナントによる共有サービス消費の許可

テナントが他のテナントで使用される共有サービスを作成できる場合であっても、管理者はテナント間で共有できるサービスを選択する必要があります。この手順では、Windows Azure Pack の管理者がプラン用に共有サービスを選択する方法を示します。

始める前に

- 管理者がテナントによる共有サービスの提供を許可していることを確認します。
- テナントが共有サービスを提供していることを確認します。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[PLANS]** を選択します。

ステップ 3 **[plans]** ペインで **[PLANS]** を選択します。

a) プラン (ゴールド) をクリックします。

ステップ 4 **[Gold]** ペインで **[Networking (ACI)]** を選択します。

ステップ 5 **[networking (aci)]** ペインで、アクセス権を与える共有サービスのチェックボックスをオンにします (DBSrv) 。

ステップ 6 **[SAVE]** をクリックします。

NAT ファイアウォールおよび ADC ロード バランサ サービスを消費するテナントを許可する

Cisco Application Centric Infrastructure（ACI）にはサービス グラフの概念があり、テナントがサービス ノードを挿入してファブリック内の 2 つのエンドポイント グループ（EPG）間でさまざまなレイヤ 4 ～レイヤ 7 機能を実行できます。

ACI と連携した Windows Azure Packには、共有スペース内に外部 NAT ファイアウォール IP および外部 ADC ロード バランサが存在している場合、仮想プライベート クラウド（VPC）でサービスを簡単かつシームレスにプロビジョニングおよび展開できる機能が含まれます。この機能の最も一般的な使用例は、EPG のさまざまなポート転送技術またはロード バランシングが外部 IP に対して行われる場合に、IP アドレスが外部からのアクセスを制限されているサービス プロバイダ モデルが使用できます。

テナント仮想ルーティングおよび転送（VPC）内にすべてのネットワークが含まれている場合や、ACI ファブリックを使用するすべてのテナントでアクセス可能な一連の L3Out を APIC 管理者が設定できる VRF モデルを分割する場合、Azure Pack 内のテナントがストリクト VPCモデルを利用きます。Azure Pack テナントがレイヤ 4 ～ レイヤ 7 サービス デバイスを消費し、テナント VRF 内から提供される提供されたサービスのパブリック アドレスを割り当て可能な、VRF ワークフローの分割に関する指示を提供します。

始める前に

- Application Policy Infrastructure Controller（APIC）管理者が、共通テナントの少なくともレイヤ 4 ～ レイヤ 7 リソース プールで設定されていることを確認します。「*Cisco APIC レイヤ 4 ～ レイヤ 7 サービス展開ガイド*」の「レイヤ 4 ～レイヤ 7 のリソース プールの設定」章を参照してください。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[PLANS]** を選択します。

ステップ 3 **[plans]** ペインで **[PLANS]** を選択します。

a) プラン (ゴールド) をクリックします。

ステップ 4 **[Gold]** ペインで **[Networking (ACI)]** を選択します。

ステップ 5 **[ネットワー キング（aci）]** ペインで、Azure Pack 消費の APIC 管理者によりプロビジョニングされたレイヤ 4 ～ レイヤ 7 サービス プールを選択します。

ステップ 6 [SAVE] をクリックします。

共有サービス プロバイダーとコンシューマの表示

これにより、管理者は共有サービス プロバイダーとコンシューマを表示できます。

始める前に

- 管理者がテナントによる共有サービスの提供を許可していることを確認します。
- テナントが共有サービスを提供していることを確認します。
- 管理者がプランで共有サービスを有効化していることを確認します。
- 消費される共有サービスがテナントに設定されていることを確認します。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [ACI] ペインで、[SHARED SERVICES] を選択して共有サービス プロバイダーを表示します。

ステップ 4 プロバイダーをクリックします。

ステップ 5 [INFO] をクリックして、この共有サービスを消費しているすべてのユーザを表示します。

共有サービスの管理

新しいテナントからの共有サービスの廃止

これにより、管理者は新しいテナントから共有サービスを廃止できます。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。
ステップ 2 [Navigation] ペインで [PLANS] を選択します。
ステップ 3 [plans] ペインで、プラン（ゴールド）を選択します。
ステップ 4 [gold] ペインで [Networking (ACI)] を選択します。
ステップ 5 [networking (aci)] ペインで、プランからサービスのマークを外して [SAVE] をクリックします。テナントから共有サービスを廃止しました。

共有サービスからのテナントの取り消し

これにより、管理者は共有サービスからテナントを取り消すことができます。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。
ステップ 2 [Navigation] ペインで [ACI] を選択します。
ステップ 3 [aci] ペインで、共有サービス（DBSrv）を選択します。
ステップ 4 [INFO] をクリックして、取り消すユーザがその共有サービスに存在することを確認します。
ステップ 5 [Navigation] ペインで [PLANS] を選択します。
ステップ 6 [plans] ペインで、プラン（ゴールド）を選択します。
ステップ 7 [gold] ペインで [Networking (ACI)] を選択します。
ステップ 8 [networking (aci)] ペインで、プランからサービスのマークを外して [SAVE] をクリックします。
ステップ 9 [Navigation] ペインで [ACI] を選択します。
ステップ 10 [aci] ペインで [SHARED SERVICES] を選択します。
ステップ 11 [aci] ペインで、共有サービス（DBSrv）を選択して [INFO] クリックします。
ステップ 12 [Revoke Consumers of DBSrv] ダイアログボックスで、取り消すユーザのチェックボックスをオンにします。
ステップ 13 チェックマークをクリックします。

ロード バランシングの概要

VLAN、Virtual Routing and Forwarding（VRF）スティッチングは従来のサービス挿入モデルによってサポートされ、Application Policy Infrastructure Controller（APIC）はポリシー制御の中心点として機能する一方でサービス挿入を自動化できます。APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。APICは、アプリケーション要件に従ってサービスを自動的に設定することもでき、それにより組織はサービス挿入を自動化し、従来のサービス挿入の複雑な技術の管理に伴う課題を排除できます。

詳しくは、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』を参照してください。

APIC GUI を使用してレイヤ 4 ～ 7 のサービスを導入するには、以下のタスクを実行する必要があります。

デバイス パッケージのインポート 管理者のみがデバイス パッケージをインポートできます。	APIC でのデバイス パッケージのインポート（29 ページ）を参照してください。
XML POST の設定と Application Policy Infrastructure Controller（APIC）へのポスト デバイス パッケージについては、Microsoft の Windows Azure Pack サービスに関する項を参照してください。 管理者のみが XML POST を設定して送信できます。	XML POST を使用した APIC でのロード バランサ デバイスの設定 （30 ページ）を参照してください。
プランに合わせたロード バランサの作成 Windows Azure Pack に対する VIP 範囲が設定されています。 管理者のみがプランに合わせたロード バランサを作成できます。	プランに合わせたロードバランサの作成 （36 ページ）を参照してください。
ロード バランサの設定 テナントのみがロード バランサを設定できます。	ロード バランサの設定 （45 ページ）を参照してください。

APIC でのデバイス パッケージのインポート

管理者のみがデバイス パッケージをインポートできます。管理者がデバイス パッケージを Application Policy Infrastructure Controller（APIC）にインポートすると、APIC はユーザが持っているデバイス、およびそのデバイスで何ができるかを知ることができます。

始める前に

デバイス パッケージがダウンロードされていることを確認します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **[L4-L7 SERVICES]** > **[PACKAGES]** の順に選択します。

ステップ 2 [navigation] ペインで、[Quick Start] を選択します。

ステップ 3 [Quick Start] ペインで、[Import a Device Package] を選択します。

ステップ 4 [Import Device Package] ダイアログボックスで、次の操作を実行します。

a) [BROWSE] をクリックして、F5 や Citrix デバイス パッケージなどのデバイス パッケージを探します。

b) [Submit] をクリックします。

XML POST を使用した APIC でのロード バランサ デバイスの設定

管理者のみが XML POST を設定して送信できます。

始める前に

- Application Policy Infrastructure Controller（APIC）でデバイス パッケージ ファイルをアップロードしておく必要があります。

  詳細については、「『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』」を参照してください。

- テナント共通には、「default」および「vpcDefault」という 2 つのブリッジ ドメインが必要です。ロードバランサを消費するテナントで使用されるサブネットが、これらのブリッジ ドメインに追加されていることを確認します。通常、Windows Azure Pack テナントに DHCP インフラストラクチャを設定する際に、これらのブリッジ ドメインとサブネットを作成します。

- 非 VPC プランでは、ロード バランサのバックエンド インターフェイスは、上で作成したテナント共通下のデフォルト EPG に配置する必要があります。VPC プランでは、EPG は「vpcDefault」です。

- ロード バランサの VIP インターフェイスは、外部にリンクする必要がある任意の EPG に配置する必要があります。

  ファブリック外部の L3 extOut 外部接続については、『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』を参照してください。

- （オプション）必要に応じて、VIP サブネットが L3 または L2 extOut にリンクされていることを確認してください。EPG あたり 1 つの VIP が割り当てられます。

手順

ステップ 1 次に、Citrix および F5 の XML POST の例を示します。

a) Citrix の XML POST の例：

例：

```
<polUni dn="uni">
    <fvTenant dn="uni/tn-common" name="common">

        <vnsLDevVip name="MyLB" devtype="VIRTUAL">

                                            <!-- Device Package -->
            <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScaler-1.0"/>

                                            <!-- VmmDomain -->
            <vnsRsALDevToDomP tDn="uni/vmmp-VMware/dom-mininet"/>

            <vnsCMgmt name="devMgmt" host="172.31.208.179" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="nsroot"/>

            <vnsDevFolder key="enableFeature" name="EnableFeature">
                    <vnsDevParam key="LB" name="lb_1" value="ENABLE"/>
                    <vnsDevParam key="CS" name="cs_1" value="ENABLE"/>
                    <vnsDevParam key="SSL" name="ssl_1" value="ENABLE"/>
            </vnsDevFolder>
            <vnsDevFolder key="enableMode" name="EnableMode_1">
                    <vnsDevParam key="USIP" name="usip_1" value="DISABLE"/>
                    <vnsDevParam key="USNIP" name="usnip_1" value="ENABLE"/>
            </vnsDevFolder>

            <vnsCDev name="ADC1" devCtxLbl="C1">
                <vnsCIf name="1_1"/>
                <vnsCIf name="mgmt"/>

                <vnsCMgmt name="devMgmt" host="172.31.208.179" port="80"/>
                <vnsCCred name="username" value="nsroot"/>
                <vnsCCredSecret name="password" value="nsroot"/>
            </vnsCDev>

            <vnsLIf name="C5">
              <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mIfLbl-outside"/>

                <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-ADC1/cIf-[1_1]"/>
            </vnsLIf>
            <vnsLIf name="C4">
              <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mIfLbl-inside"/>

                <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-ADC1/cIf-[1_1]"/>
            </vnsLIf>

        </vnsLDevVip>

        <vnsAbsGraph name ="MyLB">

            <!-- Node2 Provides SLB functionality -->
            <vnsAbsNode name = "Node2" funcType="GoTo" >

                <vnsRsDefaultScopeToTerm
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeProv-Output1/outtmnl"/>

                <vnsAbsFuncConn name = "C4">
                    <vnsRsMConnAtt
tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mFunc-LoadBalancing/mConn-external" />
                </vnsAbsFuncConn>
```

```
                <vnsAbsFuncConn name = "C5" attNotify="true">
                    <vnsRsMConnAtt
tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mFunc-LoadBalancing/mConn-internal" />
                </vnsAbsFuncConn>

                <vnsAbsDevCfg>
                    <vnsAbsFolder key="Network"
                                  name="network"
                                  scopedBy="epg">
                        <vnsAbsFolder key="nsip" name="snip1">
                         <vnsAbsParam key="ipaddress" name="ip1" value="5.5.5.251"/>

                            <vnsAbsParam key="netmask" name="netmask1"
value="255.255.255.0"/>
                            <vnsAbsParam key="hostroute" name="hostroute"
value="DISABLED"/>
                            <vnsAbsParam key="dynamicrouting" name="dynamicrouting"
 value="ENABLED"/>
                            <vnsAbsParam key="type" name="type" value="SNIP"/>
                        </vnsAbsFolder>
                    </vnsAbsFolder>

                </vnsAbsDevCfg>

                <vnsAbsFuncCfg>
                    <vnsAbsFolder key="internal_network"
                                  name="internal_network"
                                  scopedBy="epg">
                        <vnsAbsCfgRel name="internal_network_key"
                                      key="internal_network_key"
                                      targetName="network/snip1"/>
                    </vnsAbsFolder>
                </vnsAbsFuncCfg>

                <vnsRsNodeToMFunc
tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mFunc-LoadBalancing"/>
            </vnsAbsNode>

            <vnsAbsTermNodeCon name = "Input1">
                <vnsAbsTermConn name = "C1"/>
            </vnsAbsTermNodeCon>

            <vnsAbsTermNodeProv name = "Output1">
                <vnsAbsTermConn name = "C6"/>
            </vnsAbsTermNodeProv>

            <vnsAbsConnection name = "CON1" adjType="L2">
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeCon-Input1/AbsTConn" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Node2/AbsFConn-C4" />
            </vnsAbsConnection>

            <vnsAbsConnection name = "CON3" adjType="L2">
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Node2/AbsFConn-C5" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeProv-Output1/AbsTConn" />
            </vnsAbsConnection>

        </vnsAbsGraph>

    </fvTenant>
</polUni>
```

b) F5 の XML POST の例：

例：

```
<polUni dn="uni">
    <fvTenant name="common">

      <fvBD name="MyLB">
        <fvSubnet ip="6.6.6.254/24" />
        <fvRsCtx tnFvCtxName="default"/>
      </fvBD>

      <vnsLDevVip name="MyLB" devtype="VIRTUAL">
          <vnsRsMDevAtt tDn="uni/infra/mDev-F5-BIGIP-1.1.1"/>
          <vnsRsALDevToDomP tDn="uni/vmmp-VMware/dom-mininet"/>
          <vnsCMgmt name="devMgmt" host="172.31.210.88" port="443"/>
          <vnsCCred name="username" value="admin"/>
          <vnsCCredSecret name="password" value="admin"/>

          <vnsLIf name="internal">
              <vnsRsMetaIf tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mIfLbl-internal"/>
             <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-BIGIP-1/cIf-[1_1]"/>

          </vnsLIf>

          <vnsLIf name="external">
              <vnsRsMetaIf tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mIfLbl-external"/>
             <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-BIGIP-1/cIf-[1_2]"/>

          </vnsLIf>

      <vnsCDev name="BIGIP-1">
          <vnsCIf name="1_1"/>
          <vnsCIf name="1_2"/>

          <vnsCMgmt name="devMgmt" host="172.31.210.88" port="443"/>
          <vnsCCred name="username" value="admin"/>
          <vnsCCredSecret name="password" value="admin"/>

          <vnsDevFolder key="HostConfig" name="HostConfig">
            <vnsDevParam key="HostName" name="HostName"
value="example22-bigip1.ins.local"/>
            <vnsDevParam key="NTPServer" name="NTPServer" value="172.23.48.1"/>
        </vnsDevFolder>

      </vnsCDev>

    </vnsLDevVip>
    <vnsAbsGraph name = "MyLB">
    <vnsAbsTermNodeCon name = "Consumer">
        <vnsAbsTermConn name = "Consumer">
        </vnsAbsTermConn>
    </vnsAbsTermNodeCon>
      <!-- Node1 Provides Virtual-Server functionality -->
      <vnsAbsNode name = "Virtual-Server" funcType="GoTo">

        <vnsAbsFuncConn name = "internal" attNotify="yes">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mFunc-Virtual-Server/mConn-internal"
 />
        </vnsAbsFuncConn>
        <vnsAbsFuncConn name = "external">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mFunc-Virtual-Server/mConn-external"
```

```
/>
        </vnsAbsFuncConn>
        <vnsRsNodeToMFunc
            tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mFunc-Virtual-Server"/>
        <vnsAbsDevCfg>
          <vnsAbsFolder key="Network" name="webNetwork">

            <!-- Active Bigip SelfIP -->
            <vnsAbsFolder key="ExternalSelfIP" name="External1" devCtxLbl="ADC1">
              <vnsAbsParam key="SelfIPAddress" name="seflfipaddress"
                           value="6.6.6.251"/>
              <vnsAbsParam key="SelfIPNetmask" name="selfipnetmask"
                           value="255.255.255.0"/>
              <vnsAbsParam key="Floating" name="floating"
                           value="NO"/>
            </vnsAbsFolder>
            <vnsAbsFolder key="InternalSelfIP" name="Internal1" devCtxLbl="ADC1">
              <vnsAbsParam key="SelfIPAddress" name="seflfipaddress"
                           value="12.0.251.251"/>
              <vnsAbsParam key="SelfIPNetmask" name="selfipnetmask"
                           value="255.255.0.0"/>
              <vnsAbsParam key="Floating" name="floating"
                           value="NO"/>
            </vnsAbsFolder>
            <vnsAbsFolder key="Route" name="Route">
              <vnsAbsParam key="DestinationIPAddress" name="DestinationIPAddress"
                           value="0.0.0.0" />
              <vnsAbsParam key="DestinationNetmask" name="DestinationNetmask"
                           value="0.0.0.0"/>
              <vnsAbsParam key="NextHopIPAddress" name="NextHopIP"
                           value="6.6.6.254"/>
            </vnsAbsFolder>
          </vnsAbsFolder>
        </vnsAbsDevCfg>
        <vnsAbsFuncCfg>
          <vnsAbsFolder key="NetworkRelation" name="webNetwork">
            <vnsAbsCfgRel key="NetworkRel" name="webNetworkRel"
                          targetName="webNetwork"/>
          </vnsAbsFolder>
        </vnsAbsFuncCfg>
      </vnsAbsNode>
    <vnsAbsTermNodeProv name = "Provider">
         <vnsAbsTermConn name = "Provider" >
         </vnsAbsTermConn>
    </vnsAbsTermNodeProv>
    <vnsAbsConnection name = "CON3" adjType="L3">
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeCon-Consumer/AbsTConn" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Virtual-Server/AbsFConn-external" />
    </vnsAbsConnection>
    <vnsAbsConnection name = "CON1" adjType="L2">
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Virtual-Server/AbsFConn-internal" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeProv-Provider/AbsTConn" />
    </vnsAbsConnection>
    </vnsAbsGraph>
  </fvTenant>

</polUni>
```

ステップ 2 次に、Citrix および F5 の設定可能なパラメータを示します。

a) Citrix の設定可能なパラメータ：

パラメータ	サンプル値	説明
vnsLDevVip name	「MyLB」	この値はロード バランサの ID で、ロード バランサ選択のプラン セクションの、Windows Azure Pack の管理者ポータルに表示されます。これは、同じ代替値を持つ XML POST 全体でグローバルに変更できます。
vnsRsALDevToDomP tDn	「uni/vmmp-VMware/dom-mininet」	これは、ロードバランサ VM が置かれている VMM ドメインです。たとえば、仮想ロード バランサがある場合、vCenter VMM ドメイン、SCVMM、または物理ドメインに関連付けることができます。 （注） どのドメインを指定する場合でも、VLAN 範囲が関連付けられている必要があります。
vnsCMgmt name="devMgmt" host	「172.31.208.179」	これは、Cisco Application Centric Infrastructure（ACI）ファブリックに通信されるロード バランサの IP アドレスです。
vnsCCred name	「username」	ユーザ名。
vnsCCredSecret name	「password」	パスワード。
vnsAbsParam key	「ipaddress」	これは、ファブリックがこのデバイスを識別する IP アドレスです。
vnsAbsParam key="ipaddress" name="ip1" value	「5.5.5.251」	この IP アドレスは、ブリッジ ドメインの 1 つである必要があります。

b) F5 の設定可能なパラメータ：

パラメータ	サンプル値	説明
fvBD name	「MyLB」	この値はロード バランサの ID で、ロード バランサ選択のプラン セクションの、Windows Azure Pack の管理者ポータルに表示されます。これは、同じ代替値を持つ XML POST 全体でグローバルに変更できます。
vnsRsALDevToDomP tDn	「uni/vmmp-VMware/dom-mininet」	これは、有効な VLAN ENCAP ブロックを持つ任意の VMM ドメインです。 （注） この Windows Azure Pack のロード バランサ設定では、この VMM ドメインに LB 構成との関連性はほかにありません。これは、後方互換性のために使用されます。
vnsCMgmt name="devMgmt" host	「172.31.210.88」	これは、ACI ファブリックに通信されるロード バランサの IP アドレスです。
vnsCCred name	「username」	ユーザ名。
vnsCCredSecret name	「password」	パスワード。

ステップ 3 F5 または Citrix のいずれかのデバイス パッケージを POST します。

プランに合わせたロード バランサの作成

管理者のみがデバイス パッケージをインポートできます。

始める前に

- デバイス パッケージをインポートします。
- XML POST の設定と Application Policy Infrastructure Controller（APIC）へのポスト

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで [PLANS] を選択します。

ステップ 3 [plans] ペインで、ロード バランサを追加するプランを選択します（shareplan）。

ステップ 4 [shareplan] ペインで **[Networking (ACI)]** を選択します。

ステップ 5 [networking (aci)] ペインで、次の操作を実行して共有ロード バランサを追加します。

a) [shared load balancer] チェックボックスをオンにします。

b) [LB DEVICE ID IN APIC] フィールドで、ドロップダウン リストからロード バランサ（MyLB）を選択します。

c) [VIP RANGE] フィールドで、VIP 範囲（5.5.5.1 ～ 5.5.5.100）を指定します。

d) [SAVE] をクリックします。

（注） VIP 範囲が重複しない限り、異なるプラン間で共有される、単一のロードバランサを使用できます。

L3 外部接続について

レイヤ 3（L3）外部接続は、スタティック ルーティング、OSPF、EIGRP、BGP などの L3 ルーティング プロトコルによって、外部ネットワークに ACI ファブリックを接続する Cisco Application Centric Infrastructure（ACI）機能です。Microsoft Windows Azure Pack に L3 外部接続を設定することで、テナント ネットワークはファブリック外部への発信トラフィックを開始し、外部からのトラフィックを引き付けることができます。この機能の前提は、テナント仮想マシンの IP アドレスが、NAT を使用しないファブリック外部に表示され、ACI L3 外部接続に NAT が含まれないことです。

Windows Azure Pack 用に L3 外部接続を設定するための前提条件

Windows Azure Pack 用にレイヤ 3（L3）外部接続を設定するには、次の前提条件を満たす必要があります。

- Application Policy Infrastructure Controller（APIC）GUI にログインしていることを確認し、メニューバーで **[TENANT] > common]** の順に選択します。
  - 「default」という l3ExtOut を作成し、BD「default」を参照します。
  - l3ExtOut の下に名前が「defaultInstP」の l3extInstP を作成します。これは、共有サービスのテナントで使用されます。

  L3 外部接続設定については、*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。
- APIC GUI にログインしていることを確認し、メニューバーで **[TENANT] > common]** の順に選択します。

- 「vpcDefault」という l3ExtOut を作成し、BD「vpcDefault」を参照します。
- この l3ExtOut の下に名前が「vpcDefaultInstP」の l3extInstP を作成します。

  これは、VPC テナントで使用されます。

テナントの外部接続の設定については、*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。

Windows Azure Pack は、上で強調表示した命名規則以外の特別な要件なしで、共通 l3ExtOut 構成を利用します。

l3extinstP「default」で提供される契約の作成

ここでは、l3extinstP「default」で提供される契約の作成方法を説明します。

Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （37 ページ）を参照してください。

スコープが「グローバル」であることを確認します。この契約では、コンシューマからプロバイダーへのすべてのトラフィックを許可し、プロバイダーからコンシューマへ確立された TCP のみを許可します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Tenant Name]** > **[Security Policies]** > **[Contracts]** の順に展開します。

ステップ 3 [ACTION] をクリックし、ドロップダウン リストから [Create Contract] を選択します。

ステップ 4 [Create Contract] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに名前（L3_DefaultOut）を入力します。
b) [Scope] タブで、ドロップダウン リストから [Global] を選択します。
c) [Subjects] フィールドで、[+] アイコンをクリックします。
d) [Create Contract Subject] ダイアログボックスで、次の操作を実行します。
e) [Name] フィールドに、任意の名前を入力します。
f) [Apply Both direction] をオフにします。
g) **[Filter Chain For Consumer to Provider]** フィールドで **[+]**アイコンをクリックし、ドロップダウン リストから **[default/common]** を選択して、**[Update]** をクリックします。
h) **[Filter Chain For Provider to Consumer]** フィールドで [+] アイコンをクリックし、ドロップダウン リストから **[est/common]**を選択して、**[Update]** をクリックします。
i) **[OK]**をクリックして **[Create Contract Subject]**ダイアログボックスを閉じます。
j) [OK] をクリックして [Create Contract] ダイアログボックスを閉じます。

これで、l3extinstP「default」で提供される契約が作成されました。

l3extinstP「vpcDefault」で提供される契約の作成

ここでは、l3extinstP「vpcDefault」で提供される契約の作成方法を説明します。

Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （37 ページ）を参照してください。

スコープが「グローバル」であることを確認します。この契約では、コンシューマからプロバイダーへのすべてのトラフィックを許可し、プロバイダーからコンシューマへ確立された TCP のみを許可します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Tenant Name]** > **[Security Policies]** > **[Contracts]** の順に展開します。

ステップ 3 [ACTION] をクリックし、ドロップダウン リストから [Create Contract] を選択します。

ステップ 4 [Create Contract] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに名前（L3_VpcDefaultOut）を入力します。
b) [Scope] タブで、ドロップダウン リストから [Global] を選択します。
c) [Subjects] フィールドで、[+] アイコンをクリックします。
d) [Create Contract Subject] ダイアログボックスで、次の操作を実行します。
e) [Name] フィールドに、任意の名前を入力します。
f) [Apply Both direction] をオフにします。
g) **[Filter Chain For Consumer to Provider]** フィールドで **[+]**アイコンをクリックし、ドロップダウン リストから **[default/common]** を選択して、**[Update]** をクリックします。
h) **[Filter Chain For Provider to Consumer]** フィールドで [+] アイコンをクリックし、ドロップダウン リストから **[est/common]**を選択して、**[Update]** をクリックします。
i) **[OK]**をクリックして **[Create Contract Subject]**ダイアログボックスを閉じます。
j) [OK] をクリックして [Create Contract] ダイアログボックスを閉じます。

これで、l3extinstP「vpcDefault」で提供される契約が作成されました。

テナントのタスク

ここでは、テナントのタスクについて説明します。

（注） 共有サービスのコンシューマがプロバイダとは異なる VRF に属している場合には、通信を可能にするため、VRF 間のルート リーキングが自動的に生じます。

共有または仮想プライベート クラウド プランのエクスペリエンス

これは、共有または仮想プライベートクラウド（VPC）プランでのテナントのエクスペリエンスです。

共有プランでのネットワークの作成

これにより、管理者は共有プランのネットワークを作成できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **[ACI]** ペインで、**[NETWORKS]** を選択します。

ステップ 4 **[New]** をクリックします。

ステップ 5 **[NEW]** ペインで、**[NETWORKS]** を選択し、以下の操作を実行します。

a) **[NETWORK NAME]** フィールドに、ネットワークの名前 (S01) を入力します。

b) **[CREATE]** をクリックします。

c) **[REFRESH]** をクリックします。

APIC の *Microsoft Windows Azure Pack* で作成されたネットワークの確認

ここでは、APIC の Microsoft Windows Azure Pack で作成したネットワークを確認する方法を説明します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで [TENANTS] を選択します。

ステップ 2 **Navigation**ペインで、**Tenant 018b2f7d-9e80-43f0-abff-7559c026bad5** > **Application Profiles** > **default** > **Application EPGs** > **EPG Network01** の順に展開し、Microsoft Windows Azure Pack で作成したネットワークがAPIC で作成されたことを確認します。

VPC プランでのブリッジ ドメインの作成

仮想プライベートクラウド（VPC）プランのみに適用されます。これにより、テナントはネットワークに対する独自の IP アドレス空間を取得できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[BRIDGE DOMAIN] を選択します。

ステップ 5 [BRIDGE DOMAIN] フィールドにブリッジ ドメイン名（BD01）を入力します。

ステップ 6 現在のテナントが複数の Azure Pack プランをサブスクライブしている場合は [Subscription] を選択し、対象のブリッジ ドメインを作成します。

ステップ 7 オプション：[SUBNET'S GATEWAY] フィールドにサブネットのゲートウェイ（192.168.1.1/24）を入力します。

ステップ 8 **[コンテキスト]** フィールドで、すでにサブスクリプションの一部になっているコンテキストを選択するか、または **[新規作成]** を選択して、ブリッジ ドメインに新規コンテキストを作成します。

ステップ 9 [CREATE] をクリックします。

VPC プランでのネットワークの作成およびブリッジ ドメインへの関連付け

これにより、テナントは VPC プランでネットワークを作成し、ブリッジ ドメインに関連付けることができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで [NETWORK] を選択します。

ステップ 5 [NETWORK NAME] フィールドに、ネットワーク名（S01）を入力します。

ステップ 6 [BRIDGE NAME] フィールドに、ブリッジ名（BD01）を入力します。

ステップ 7 [CREATE] をクリックします。

ステップ 8 [aci] ペインで、[NETWORKS] を選択します。

ネットワークがブリッジ ドメインに関連付けられていることがわかります。

同一サブスクリプション内のファイアウォールの作成

これにより、テナントは同一サブスクリプション内にファイアウォールを作成できます。

始める前に

2 つのネットワークが作成されていることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 [Navigation] ペインで [ACI] を選択します。
ステップ 3 [New] をクリックします。
ステップ 4 [NEW] ペインで、[FIREWALL] を選択します。
ステップ 5 [FROM NETWORK] フィールドで、ドロップダウン リストから、ネットワーク名（WEB01）を選択します。
ステップ 6 [TO NETWORK] フィールドで、ドロップダウン リストから、もう 1 つのネットワーク名（WEB02）を選択します。
ステップ 7 [PROTOCOL] フィールドにプロトコル（tcp）を入力します。
ステップ 8 [PORT RANGE BEGIN] フィールドに開始ポート範囲（50）を入力します。
ステップ 9 [PORT RANGE END] フィールドに終了ポート範囲（150）を入力します。
ステップ 10 [CREATE] をクリックします。
同一サブスクリプション内にファイアウォールが追加されました。

VPC プランでのネットワークの構築

これにより、テナントは VPC プランでネットワークを作成できます。

手順

ステップ 1 サービス管理ポータル（テナント ポータル）にログインします。
ステップ 2 [Navigation] ペインで [ACI] を選択します。
ステップ 3 **[New]** をクリックします。
ステップ 4 [NEW] ペインで **[ACI]** > **[NETWORK]** の順に選択して、次の操作を実行します。
a) [NETWORK NAME] フィールドに、ネットワーク名（Network01）を入力します。
b) オプション 1：共有ブリッジ ドメインにネットワークを作成します。
- [BRIDGE DOMAIN] フィールドで、ドロップダウン リストからブリッジ ドメインを選択します。（デフォルト）。
- [CREATE] をクリックします。

このプロセスが完了するには、数分かかることがあります。

c) オプション 2：テナント ブリッジ ドメインにネットワークを作成します。
- [BRIDGE DOMAIN] フィールドで、ドロップダウン リストからブリッジ ドメイン（myBridgeDomain）を選択します。

d) オプション：スタティック IP アドレス プールを使用してネットワークを導入するには、次の操作を実行します。

- アドレス/マスクの形式でゲートウェイを入力します（192.168.1.1/24）。結果のスタティック IP アドレス プールはゲートウェイ サブネットの全範囲を使用します。
- DNS サーバを入力します。複数のサーバが必要な場合は、セミコロンを使用してリストを区切ります（192.168.1.2;192.168.1.3）。

（注） サブネットは、コンテキスト内の他のすべてのサブネットと照合して検証されます。ネットワークの作成では、重複が検出された場合はエラーが返されます。

- [CREATE] をクリックします。

このプロセスが完了するには、数分かかることがあります。

VM の作成とネットワークへの接続

これにより、テナントは VM を作成し、ネットワークに接続することができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、**[STANDALONE VIRTUAL MACHINE]** > **[FROM GALLERY]** の順に選択します。

ステップ 5 [Virtual Machine Configuration] ダイアログボックスで、設定（LinuxCentOS）を選択します。

ステップ 6 次に進む矢印をクリックします。

ステップ 7 [Portal Virtual Machine Settings] 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 VM 名（SVM01）を入力します。
b) [ADMINISTRATOR ACCOUNT] フィールドに root が表示されます。
c) [New Password] フィールドに新しいパスワードを入力します。
d) 確認のために [CONFIRM] フィールドにもう一度パスワードを入力します。
e) 次に進む矢印をクリックします。

ステップ 8 [Provide Virtual Machine Hardware Information] ダイアログボックスで、次の操作を実行します。

a) [NETWORK ADAPTER 1] フィールドのドロップダウン リストから、関連付けて計算するネットワーク アダプタ（6C6DB302-aObb-4d49-a22c-151f2fbad0e9|default|S01）を選択します。
b) チェックマークをクリックします。

ステップ 9 [Navigation] ペインで、[Virtual Machines] を選択して VM（SVM01）のステータスを確認します。

共有サービスの提供

これにより、テナントは共有サービスを提供することができます。

始める前に

管理者がテナントによる共有サービスの提供を許可していることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [ACI] ペインで [SHARED SERVICE] を選択します。

ステップ 4 [SHARED SERVICES] ダイアログボックスで、次の操作を実行します。

a) [ACTION] フィールドで、ドロップダウン リストから、[PROVIDE A SHARED SERVICE CONTRACT] を選択します。
b) [NETWORK] フィールドで、ドロップダウン リストから、ネットワーク（WEB01）を選択します。
c) [SERVICE NAME] フィールドに、サービス名（DBSrv）を入力します。
d) [DESCRIPTION] フィールドに、説明を入力します。
e) [PROTOCOL] フィールドにプロトコル（tcp）を入力します。
f) [PORT RANGE BEGIN] フィールドに、ポート範囲の開始（139）を入力します。
g) [PORT RANGE END] フィールドに、終了ポート範囲（139）を入力します。
h) チェックマークをクリックします。

消費される共有サービスの設定

これにより、テナントは消費される共有サービスを設定できます。

始める前に

- 管理者がテナントによる共有サービスの提供を許可していることを確認します。
- テナントが共有サービスを提供していることを確認します。
- 管理者がプランで共有サービスを有効化していることを確認します。
- 共有サービス コンシューマは、プロバイダーよりも異なる VRF では、ルート漏出、Vrf 間では、通信を有効にするには自動的に発生します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 ナビゲーション ウィンドウで、**[ACI]** > **[SHARED SERVICE]** の順に選択します。

ステップ 3 **[SHARED SERVICE]** ダイアログボックスで、次の操作を実行します。

a) **[Network]** フィールドで、ネットワーク (V1) を選択します。

b) **[Consumed Services]** フィールドで、サービスのチェックボックス (DBSrv) をオンにします。

c) チェックマークを付けます。

ステップ 4 **[aci]** ペインで **[SHARED SERVICES]** を選択して、プランのコンシューマをチェックします。

ロード バランサの設定

これにより、テナントはロード バランサを設定することができます。

始める前に

- 管理者がデバイス パッケージをインポートしたことを確認します。
- 管理者が XML POST を設定し、Application Policy Infrastructure Controller（APIC）にポストしたことを確認します。
- 管理者がプランにロード バランサを追加したことを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[LOAD BALANCER] を選択します。

ステップ 5 [NETWORK NAME] フィールドに、ネットワーク名（WEB01）を入力します。

ステップ 6 [PORT] フィールドにポート（80）を入力します。

ステップ 7 [PROTOCOL] フィールドにプロトコル（tcp）を入力します。

ステップ 8 [CREATE] をクリックします。

ステップ 9 [ACI] ペインで、[LOAD BALANCER] を選択し、ロード バランサのネットワーク、仮想サーバ、アプリケーション サーバ、ポート、およびプロトコルを確認します。

ブリッジ ドメインには次のサブネットを設定してください。

- SNIP のサブネット
- ホストのサブネット

- VIP のサブネット

VIP のサブネットが必要な場合は、L3 または L2 extOut にリンクする必要があります。

アクセス コントロール リストの追加

これにより、テナントは共有サービスにアクセス コントロール リスト（ACL）を追加することができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [aci] ペインで [SHARED SERVICES] を選択します。

ステップ 4 [aci] ペインで、ACL（DBSrv）をさらに追加する共有サービスを選択します。

ステップ 5 [+ACL] をクリックして ACL を追加します。

ステップ 6 [Add ACL for DBSrv] ダイアログボックスで、次の操作を実行します。

a) [PROTOCOL] フィールドにプロトコル（tcp）を入力します。
b) [PORT NUMBER BEGIN] フィールドに、開始ポート番号（301）を入力します。
c) [PORT NUMBER END] フィールドに、終了ポート番号（400）を入力します。
d) チェックマークをクリックします。

アクセス コントロール リストの削除

これにより、テナントは共有サービスからアクセス コントロール リスト（ACL）を削除することができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **[aci]** ペインで、次の操作を実行します。

a) **[SHARED SERVICES]** を選択します。
b) ACL を削除する共有サービス（DBSrv）を選択します。
c) **[Trash ACL]** をクリックして ACL を削除します。

ステップ 4 **[Delete ACL from DBSrv]** ダイアログボックスで、削除する ACL のチェック ボックスをオンにし、チェックマークをクリックします。

Windows Azure Pack で使用する APIC 上でのテナント L3 外部発信の準備

ここでは、Windows Azure Pack で使用するためにテナント L3 外部発信を APIC でどのように準備するかについて説明します。

手順

ステップ 1 APIC GUI にログインし、メニューバーで **[TENANTS]** > **[Tenant Name]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[External Routed Networks]** の順に展開し、[External Routed Networks] を右クリックして [Create Routed Outside] を選択します。

ステップ 3 [Create Route Outside] ダイアログボックスで、次の操作を実行します。

a) 名前（myRouteOut）を入力します。
b) VRF（3b4efb29-f66e-4c93-aed4-dc88ed4be8f2/CTX_01）を選択します。
c) ネットワーク設定の要件に従って現在のダイアログ ボックスを設定します。次の Web サイトには、ACI ファブリック レイヤ 3 Outside 接続の詳細が示されています。http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/basic-config/b_ACI_Config_Guide/b_ACI_Config_Guide_chapter_0110.html
d) [Next] をクリックします。
e) [Finish] をクリックします。

ステップ 4 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[External Routed Networks]** > **[Route Outside Name]** の順に展開し、[Logical Node Profiles] を右クリックして [Create Node Profile] を選択します。

ステップ 5 L3ExtOut のガイドに従って、ノード プロファイルの作成を実行します。次の Web サイトには、ACI ファブリック レイヤ 3 Outside 接続の詳細が示されています。 http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/basic-config/b_ACI_Config_Guide/b_ACI_Config_Guide_chapter_0110.html

ステップ 6 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[External Routed Networks]** > **[Route Outside Name]** の順に展開し、[Networks] を右クリックして [Create External Network] を選択します。

ステップ 7 [Create External Network] ダイアログボックスで、次の操作を実行します。

a) **<RouteOutsideName>InstP** の形式で名前を入力します。たとえば、[Route Outside Name] に **myRoutOut** と入力し、[my External Network Name] に **myRoutOutInstP** を入力します。
b) [Subnet] セクションで、[+] アイコンをクリックします。
c) ネットワーク設計ごとに、[Create Subnet] ダイアログボックスに外部サブネットの詳細を入力します。
d) [Subnet] ダイアログボックスで、[OK] をクリックして完了します。
e) [Create External Network] ダイアログボックスで、[Submit] をクリックします。

ステップ 8 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[Bridge Domains]** > **[Bridge Domain Name]** の順に展開し、[L3 Configurations] タブを選択して次の操作を実行します。

a) [Associated L3 Outs] の右側の + アイコンをクリックします。
b) ドロップダウンリストで、[L3 Out (3b4efb29-f66e-4c93-aed4-dc88ed4be8f2/myRouteOut)] を選択します。

c) [UPDATE] をクリックします。
d) [Bridge Domain - <Name>] ページで [Submit] をクリックします。

ステップ 9 オプション：ACI Integrated Windows Azure Pack の統合されたスタティック IP アドレス プール機能を使用しないテナント ネットワークの場合は、次の手順を実行します。

[Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[Bridge Domains]** > **[Bridge Domain Name]** の順に展開し、[L3 Configurations] タブを選択して次の操作を実行します。

a) [Subnets] の右側の + アイコンをクリックします。
b) [Create Subnet] ダイアログボックスで、次の操作を実行します。
   - アドレス/マスクの形式でゲートウェイ IP を入力します。
   - [Advertised Externally] チェックボックスをオンにします。
   - [Submit] をクリックします。

外部接続用ネットワークの作成

これにより、テナントは外部接続用のネットワークを作成することができます。

外部接続は ACI 共通 L3ExtOut またはユーザ定義の L3ExtOut のいずれかで確立できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 [Navigation] ペインで [ACI] を選択します。
ステップ 3 [New] をクリックします。
ステップ 4 [NEW] ペインで [NETWORK] を選択します。
ステップ 5 [NETWORK NAME] フィールドに、ネットワーク名（wapL3test）を入力します。
ステップ 6 オプション 1：ルート アドバタイズメントにブリッジ ドメインのサブネットを使用します。

[CREATE] をクリックします。

ステップ 7 オプション 2：ルート アドバタイズメントに EPG のサブネットを使用します。

アドレス/マスクの形式でゲートウェイを入力します（192.168.1.1/24）。

a) [CREATE] をクリックします。

外部接続用のファイアウォールの作成

これにより、テナントは外部接続用のファイアウォールを作成することができます。

外部接続は ACI 共通 L3ExtOut またはユーザ定義の L3ExtOut のいずれかで確立できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[FIREWALL] を選択します。

ステップ 5 オプション 1：ACI 共通の L3ExtOut *External:default を使用した共有 Windows Azure Pack プランまたは VPC Windows Azure Pack プランの場合は、次の手順を実行します。

a) [FROM NETWORK] フィールドで、ドロップダウン リストからネットワーク名（*External:default）を選択します。

オプション 2：ユーザ定義の外部ネットワークを使用した VPC Windows Azure Pack プランの場合は、次の手順を実行します。

a) [FROM NETWORK] フィールドで、ドロップダウン リストからネットワーク名（External:myRouteOut）を選択します。

ステップ 6 [TO NETWORK] フィールドで、ドロップダウン リストから別のネットワーク名（wapL3test）を選択します。

ステップ 7 [PROTOCOL] フィールドにプロトコル（tcp）を入力します。

ステップ 8 [PORT RANGE BEGIN] フィールドに、ポート範囲の開始（12345）を入力します。

ステップ 9 [PORT RANGE END] フィールドに、ポート範囲の終了（45678）を入力します。

ステップ 10 [CREATE] をクリックします。
外部接続用のファイアウォールが追加されました。

APIC でのテナントの L3 外部接続の確認

ここでは、APIC 上のテナントの L3 外部接続を確認する方法について説明します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで [TENANTS] を選択します。

ステップ 2 ナビゲーション ウィンドウで、**[Tenant b81b7a5b-7ab8-4d75-a217-fee3bb23f427]** > **[Application Profiles]** > **[Application EPG]** の順に展開し、外部接続用ネットワークの作成 （48 ページ）で作成したネットワークが存在することを確認します（wapL3test）。

ステップ 3 ナビゲーション ウィンドウで、**[EPG wapL3test]** > **[Contracts]** の順に展開し、契約名が L3+EPG 名+プロトコル+ポート範囲（L3wapL3testtcp1234545678）の形式で存在し、契約が EPG によって提供され、STATE が [formed] であることを確認します。

ステップ 4 オプション 1：*External:default で契約を作成した共有 L3 Out 導入では、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

オプション 2：テナント所有の L3 Out 導入では、メニュー バーで **[TENANTS]** > ***<your tenant-id>*** を選択します。

ステップ 5 ナビゲーション ウィンドウで、**[Security Policies]** > **[Imported Contracts]** の順に展開し、ステップ 3 で確認した契約が契約インターフェイスとしてインポートされていることを確認します。

ステップ 6 オプション 1：*External:default で契約を作成した共有 L3 Out 導入では、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

オプション 2：テナント所有の L3 Out 導入では、**[TENANTS]** > ***<your tenant-id>*** を選択します。

ステップ 7 [External Network Instance Profile -defaultInstP] ペインの [Consumed Contracts] フィールドで、ステップ 5 で確認した契約インターフェイスを探し、それが存在することおよび STATE が [formed] であることを確認します。

ステップ 8 メニュー バーで、**[TENANTS]** を選択します。

ステップ 9 ナビゲーション ウィンドウで、**[Tenant b81b7a5b-7ab8-4d75-a217-fee3bb23f427]** > **[Application Profiles]** > **[Application EPG]** > **[EPG wapL3test]** > **[Contracts]** の順に展開します。

ステップ 10 [Contracts] ペインの [Consumed Contracts] フィールドで、Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （37 ページ）で共有サービスのテナントまたは VPC のテナントのために定義したデフォルトの契約がこの EPG によって消費され、STATE が [formed] であることを確認します。

ステップ 11 オプション 2：ユーザ定義の外部ネットワークとゲートウェイを指定したテナント ネットワークを使用する VPC Windows Azure Pack プランの場合は、次の手順に従います。

[Navigation] ペインで、**[Tenant Name]** > **[Application Profiles]** > **[Application EPG]** > **[EPG *wapL3test*]** > **[Subnets]** > **[Subnet Address]** の順に選択し、[Scope] が [Advertised Externally] とマークされていることを確認します。

VM ネットワークに NAT ファイアウォール レイヤ 4 ～ レイヤ 7 サービスを追加する

これにより、適応型セキュリティ アプライアンス (ASA) ファイアウォールまたはファイアウォール コンテキストがプロビジョニングされ、外部 IP アドレス プールからネットワーク アドレス変換（NAT） IP がダイナミックに割り当てられ、ASA 上にダイナミックな PAT が構成されてアウトバウンド トラフィックが可能になり、サービス グラフの残りの部分のプロビジョニングが容易に行えるようになります。

始める前に

- Azure パック プランがレイヤ 4 ～ レイヤ 7 サービス プールにアクセスできるように構成されていることを確認します。
- ACI VM ネットワークがゲートウェイまたはサブネットを持つように作成されていることを確認します。
- レイヤ 4 ～ レイヤ 7 リソース プールのプライベート サブネットが APIC 管理者から提供されていない場合、サブネットとオーバーラップする状態で レイヤ 4 ～ レイヤ 7 サービ

スを追加しようとすると、エラーが発生し、設定はプッシュされません。この場合、VM ネットワークを削除して、別のサブネットとともに再度作成してください。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。
ステップ 3 **aci** ペインで、**NETWORKS** を選択し、さらにネットワーク設定を入力します。
ステップ 4 **Enable direct internet access using NAT** チェック ボックスをオンにします。
ステップ 5 **SAVE** をクリックします。

NAT ファイアウォール ポート転送ルールを VM ネットワークに追加する

これは、ネットワークアドレス変換（NAT）ファイアウォールを設定し、VMネットワーク内で NAT IP から内部 IP にトラフィックを転送します。

始める前に

- Cisco Application Centric Infrastructure（ACI）VM ネットワークが NAT に設定されていることを確認します。.

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。
ステップ 3 **[aci]** ペインで、**[ネットワーク]** を選択し、さらにネットワーク設定を入力します。
ステップ 4 **[ネットワーク]** ペインで、**[ルール]** を選択します。
ステップ 5 パネル下部の **[追加]** をクリックします。
ステップ 6 ポート転送ルールに必要な情報を入力します。

（注） 宛先 IP アドレスは、VM ネットワークのサブネット範囲内の IP アドレスである必要があります。

ステップ 7 **[保存]** チェックマークをチェックします。

プライベート ADC ロード バランサ レイヤ 4 ～ レイヤ 7 サービスを伴う NAT ファイアウォールを VM ネットワークに追加する

NAT ファイアウォールを展開することに加えて、この設定では内部ロード バランサが展開されます。このシナリオでは、ロード バランサの VIP は、レイヤ 4 ～ レイヤ 7 のプライベート IP アドレス サブネットから (テナント VRF ごとに) 動的に割り当てられます。この 2 ノード

サービス グラフの展開では、テナントが、トラフィックのロード バランシングのために、内部ロードバランサへトラフィックを転送するポート転送規則を作成していることを前提としています。

始める前に

- Azure パック プランがレイヤ 4 ～ レイヤ 7 サービス プールにアクセスするように設定されていることを確認します。
- ACI VM ネットワークが、ゲートウェイまたはサブネットを持つように作成されていることを確認します。
- レイヤ 4 ～ レイヤ 7 リソース プールのプライベート サブネットが APIC 管理者から提供されていない場合、サブネットとオーバーラップする状態で レイヤ 4 ～ レイヤ 7 サービスを追加しようとすると、エラーが発生し、設定はプッシュされません。このような場合には、VM ネットワークを削除し、代わりのサブネットを用意して再度作成してください。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。
ステップ 3 **aci** ペインで、**NETWORKS** を選択し、さらにネットワーク設定を入力します。
ステップ 4 **Enable direct internet access using NAT** チェック ボックスをクリックします。
ステップ 5 **Enable internal load balancer (internal)** チェック ボックスをクリックします。
ステップ 6 **SAVE** をクリックします。

VRF の追加の NAT ファイアウォールのパブリック IP アドレスを要求します。

NAT ルールを使用するため、追加のパブリック IP アドレスを割り当てるには、次の手順を使用します。NAT が有効になっているすべての EPG からこのパブリック IP アドレスを要求できます。したがって、VRF 内のすべての Epg の使用可能です。

NAT ルールは、各 EPG に保存されます。したがってことをお勧め NAT ルールのポイントの宛先 IP、EPG 内およびしない、VRF に別の場所にエンドポイントにのみ。

始める前に

NAT ファイアウォールの Cisco ACI VM ネットワークが設定されていることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **Aci**] ペインを選択します **ネットワーク** 、矢印をクリックしてさらにネットワーク構成を入力します。

ステップ 4 **ネットワーク**] ペインで、選択 **IP アドレス** 。

ステップ 5 下部のパネルでをクリックして **IP アドレスを要求** 。

ステップ 6 [OK] をクリックします。

L4 L7 リソース プールで使用可能なパブリック IP アドレスがある場合は、IP アドレスが割り当てられ、このテーブルに存在します。この IP アドレスもに存在するが、 **ルール**] タブの [着信の NAT ルールを設定します。

パブリック ADC ロード バランサ レイヤ 4 ～ レイヤ 7 サービスを VM ネットワークに追加する

これにより、ロード バランサが提供され、外部 IP アドレス プールから VIP が動的に割り当てられ、必要なルートとプロビジョニングがサービス グラフの残りの部分に追加されるので、導入が容易になります。

始める前に

- Azure パック プランがレイヤ 4 ～ レイヤ 7 サービス プールにアクセスするように設定されていることを確認します。
- ACI VM ネットワークが、ゲートウェイまたはサブネットを持つように作成されていることを確認します。
- レイヤ 4 ～ レイヤ 7 リソース プールのプライベート サブネットが APIC 管理者から提供されていない場合、サブネットとオーバーラップする状態で レイヤ 4 ～ レイヤ 7 サービスを追加しようとすると、エラーが発生し、設定はプッシュされません。このような場合には、VM ネットワークを削除し、代わりのサブネットで VM ネットワークを再度作成してください。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **aci** ペインで、 **NETWORKS** を追加し、矢印をクリックして残りのネットワーク設定を入力します。

ステップ 4 **Enable load balancer (public)** チェック ボックスをオンにします。

ステップ 5 (オプション) **Allow Outbound Connections** チェック ボックスをオンにします。

（注） このオプションを使用できるのは、この VM ネットワークで NAT が設定されていない場合だけです。

ステップ 6 **SAVE** をクリックします。

VM ネットワークに ADC ロード バランサの設定を追加する

これにより、パブリックかプライベートの ADC ロード バランサが設定されます。VM ネットワークに割り当てられた VIP 上でリッスンし、ロード バランシングの行われるトラフィックを、接続数の最も少ない実サーバに転送します。VM ネットワーク全体が負荷分散されることになります。VM または VNIC がオンラインになると、それらは自動的にロード バランサに追加されます。VM ネットワーク全体で負荷分散が行われるため、VM ネットワークのすべてのエンドポイントが同一であり、定義されているロードバランサのサービスを行えると想定されます。

始める前に

- ACI VM ネットワークが、パブリックまたはプライベートのロードバランシングに合わせて設定されていることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **aci** ペインで、 **NETWORKS** を追加し、矢印をクリックして残りのネットワーク設定を入力します。

ステップ 4 **NETWORKS** ペインで、**LOAD BALANCERS** を選択します。

ステップ 5 下部パネルの **ADD** をクリックします。

ステップ 6 ロード バランサに必要な情報を入力します (名称: HTTP、プロトコル: TCP、ポート: 80)。

ステップ 7 **SAVE** チェックマークをクリックします。

Cisco ACI with Microsoft Windows Azure Pack のトラブルシューティング

管理者としてのトラブルシューティング

手順

Windows Azure Pack の管理者は管理者ポータルで、テナントによって導入されたすべてのネットワークを表示できます。問題が発生した場合は、APIC GUI を使用して、次のオブジェクトのエラーを探します。

a) VMM ドメイン
b) Windows Azure Pack のテナント ネットワークに対応するテナントおよび EPG

テナントとしてトラブルシューティング

エラー メッセージがある場合、エラー メッセージとともにワークフローの説明および管理者に対するアクションを提供してください。

EPG の設定の問題のトラブルシューティング

エンドポイント グループ（EPG）のライフタイム中、EPG の VLAN ID が APIC で変更された場合、新しい設定を有効にするには、すべての仮想マシンで VLAN 設定を更新する必要があります。

手順

この操作を実行するには、SCVMM サーバで次の PowerShell コマンドを実行します。

例：

```
$VMs = Get-SCVirtualMachine
$VMs | Read-SCVirtualMachine
$NonCompliantAdapters=Get-SCVirtualNetworkAdapter -All | Where-Object
{$_.VirtualNetworkAdapterComplianceStatus -eq "NonCompliant"}
$NonCompliantAdapters | Repair-SCVirtualNetworkAdapter
```

プログラマビリティのリファレンス

ACI Windows Azure Pack の PowerShell コマンドレット

ここでは、Cisco Application Centric Infrastructure（ACI）Windows Azure Pack の PowerShell コマンドレット、ヘルプおよび例をリストする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、**[開始]** > **[実行]** > **[Windows PowerShell]** の順に選択します。

ステップ 2 次のコマンドを入力します。

例：

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator> cd C:\inetpub\Cisco-ACI\bin
PS C:\inetpub\Cisco-ACI\bin> Import-Module .\ACIWapPsCmdlets.dll
PS C:\inetpub\Cisco-ACI\bin> Add-Type -Path .\Newtonsoft.Json.dll
PS C:\inetpub\Cisco-ACI\bin> Get-Command -Module ACIWapPsCmdlets

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Add-ACIWAPEndpointGroup                            ACIWapPsCmdlets
Cmdlet          Get-ACIWAPAdminObjects                             ACIWapPsCmdlets
Cmdlet          Get-ACIWAPAllEndpointGroups                        ACIWapPsCmdlets
Cmdlet          Get-ACIWAPBDSubnets                                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPConsumersForSharedService                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPEndpointGroups                           ACIWapPsCmdlets
Cmdlet          Get-ACIWAPEndpoints                                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPLBConfiguration                          ACIWapPsCmdlets
Cmdlet          Get-ACIWAPOpflexInfo                               ACIWapPsCmdlets
Cmdlet          Get-ACIWAPPlans                                    ACIWapPsCmdlets
Cmdlet          Get-ACIWAPStatelessFirewall                        ACIWapPsCmdlets
Cmdlet          Get-ACIWAPSubscriptions                            ACIWapPsCmdlets
Cmdlet          Get-ACIWAPTenantCtx                                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPTenantPlan                               ACIWapPsCmdlets
Cmdlet          Get-ACIWAPTenantSharedService                      ACIWapPsCmdlets
Cmdlet          Get-ACIWAPVlanNamespace                            ACIWapPsCmdlets
Cmdlet          New-ApicOpflexCert                                 ACIWapPsCmdlets
Cmdlet          Read-ApicOpflexCert                                ACIWapPsCmdlets
Cmdlet          Remove-ACIWAPEndpointGroup                         ACIWapPsCmdlets
Cmdlet          Remove-ACIWAPPlan                                  ACIWapPsCmdlets
Cmdlet          Remove-ACIWAPTenantCtx                             ACIWapPsCmdlets
Cmdlet          Set-ACIWAPAdminLogin                               ACIWapPsCmdlets
Cmdlet          Set-ACIWAPBDSubnets                                ACIWapPsCmdlets
Cmdlet          Set-ACIWAPLBConfiguration                          ACIWapPsCmdlets
Cmdlet          Set-ACIWAPLogin                                    ACIWapPsCmdlets
Cmdlet          Set-ACIWAPOpflexOperation                          ACIWapPsCmdlets
Cmdlet          Set-ACIWAPPlan                                     ACIWapPsCmdlets
Cmdlet          Set-ACIWAPStatelessFirewall                        ACIWapPsCmdlets
Cmdlet          Set-ACIWAPTenantSharedService                      ACIWapPsCmdlets
```

```
Cmdlet          Set-ACIWAPUpdateShareServiceConsumption   ACIWapPsCmdlets
Cmdlet          Set-ACIWAPVlanNamespace                   ACIWapPsCmdlets
```

ステップ 3 ヘルプを生成します。

例：

```
commandname -?
```

ステップ 4 例を生成します。

例：

```
get-help commandname -examples
```

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアンインストール

ここでは、Cisco Application Centric Infrastructure（ACI）with Microsoft Windows Azure Pack コンポーネントをアンインストールする方法について説明します。

（注） アンインストールでは、VM や論理ネットワークのようなアーティファクトが削除されます。アンインストールは、VM やホストなどの他のリソースが、これらを使用していないときにのみ成功します。

コンポーネント	タスク
VM ネットワークからのすべての仮想マシンの切断	Microsoft のマニュアルを参照してください。
すべての Hyper-V からの VXLAN トンネル エンドポイント（VTEP）の論理スイッチの削除	Microsoft のマニュアルを参照してください。
System Center Virtual Machine Manager（SCVMM）からのクラウドの削除	Microsoft のマニュアルを参照してください。
ACI with Microsoft Windows Azure Service Pack 1.1(1j) リリースをアンインストールするために APIC Windows Azure Pack リソース プロバイダーをアンインストール	APIC Windows Azure Pack のリソース プロバイダーのアンインストール（58 ページ）を参照してください。

コンポーネント	タスク
このリリースの ACI with Microsoft Windows Azure Pack をアンインストールするために以下をアンインストール • ACI Azure Pack リソース プロバイダー • ACI Azure Pack 管理者サイト拡張 • ACI Azure Pack テナント サイト拡張	ACI Azure Pack リソース プロバイダーのアンインストール （58 ページ）を参照してください。 ACI Azure Pack 管理者サイト拡張のアンインストール （59 ページ）を参照してください。 ACI Azure Pack テナント サイト拡張のアンインストール （59 ページ）を参照してください。
APIC Hyper-V エージェントのアンインストール	APIC Hyper-V エージェントのアンインストール （60 ページ）を参照してください。

APIC Windows Azure Pack のリソース プロバイダーのアンインストール

ここでは、APIC Windows Azure Pack のリソース プロバイダーをアンインストールする方法について説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [APIC Windows Azure Pack Resource Provider] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから APIC Windows Azure Pack のリソース プロバイダーがアンインストールされます。

ステップ 4 APIC Windows Azure Pack のリソース プロバイダーがアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

b) [Programs and Features] ウィンドウで [APIC Windows Azure Pack Resource Provider] が表示されていないことを確認します。

ACI Azure Pack リソース プロバイダーのアンインストール

ここでは、ACI Azure Pack のリソース プロバイダーをアンインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ACI Azure Pack Resource Provider] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから ACI Azure Pack のリソース プロバイダーがアンインストールされます。

ステップ 4 ACI Azure Pack のリソース プロバイダーがアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。
b) [Programs and Features] ウィンドウで [ACI Azure Pack Resource Provider] が表示されていないことを確認します。

ACI Azure Pack 管理者サイト拡張のアンインストール

ここでは、ACI Azure Pack の管理者サイト拡張をアンインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ACI Azure Pack Admin Site Extension] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから ACI Azure Pack の管理者サイト拡張がアンインストールされます。

ステップ 4 ACI Azure Pack の管理者サイト拡張がアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[プログラムのアンインストール]** の順に選択します。
b) [プログラムと機能] ウィンドウで [ACI Azure Pack Admin Site Extension] が表示されていないことを確認します。

ACI Azure Pack テナント サイト拡張のアンインストール

ここでは、ACI Azure Pack のテナント サイト拡張をアンインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ACI Azure Pack Tenant Site Extension] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから ACI Azure Pack のテナント サイト拡張がアンインストールされます。

ステップ 4 ACI Azure Pack のテナント サイト拡張がアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。
b) [Programs and Features] ウィンドウで [ACI Azure Pack Tenant Site Extension] が表示されていないことを確認します。

APIC Hyper-V エージェントのアンインストール

ここでは、APIC Hyper-V エージェントをアンインストールする方法について説明します。

手順

ステップ 1 Hyper-V Server にログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [Cisco APIC HyperV Agent] を右クリックして、[Uninstall] を選択します。
これで、Hyper-V Server から APIC Hyper-V エージェントがアンインストールされます。

ステップ 4 APIC Hyper-V エージェントがアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。
b) [Programs and Features] ウィンドウで [Cisco APIC HyperV Agent] が表示されていないことを確認します。

ステップ 5 Hyper-V Server ごとにステップ 1 ～ -4 を繰り返します。

Cisco ACI および Microsoft Windows Azure Pack コンポーネントでの Cisco APIC およびスイッチ ソフトウェアのダウングレード

ここでは、Cisco ACI with Microsoft Windows Azure Pack コンポーネントで Cisco APIC とスイッチ ソフトウェアをダウングレードする方法について説明します。

（注） Cisco APIC 3.1 (1) 以降で作成し使用しているレイヤ 4 ～ レイヤ 7 のリソース プール設定は、古いビルドの Cisco APIC/Windows Azure Pack と互換性がありません。ステップ 1 ～ 3 は、Cisco APIC 3.1(1) 以降のバージョンをそれより前のバージョンにダウングレードする場合に適用されます。

手順

ステップ 1 Cisco APIC でレイヤ 4 ～ レイヤ 7 のリソース プールのリストを確認します。

Cisco APIC 3.1(1) 以降で作成したリソース プールのリストを控えておきます。これらのリソース プールでは、GUI に [Function Profiles] タブがあり、NX-OS スタイル CLI の設定に「version normalized」があります。

ステップ 2 Windows Azure Pack テナント ポータル：レイヤ 4 ～ レイヤ 7 クラウド オーケストレータ モードのリソース プール（Cisco APIC 3.1(1) 以降で作成したリソース プール）を使用して、仮想プライベート クラウドのある Cisco ACI VM ネットワークごとに、次の手順を実行します。

a) サービス管理ポータル (テナント ポータル) にログインします。
b) [Navigation] ペインで [ACI] を選択します。
c) [aci] ペインで [NETWORKS] を選択し、矢印をクリックして、さらにネットワーク設定を入力します。
d) [Enable direct internet access using NAT] チェックボックスがオンの場合はオフにします。
e) [Enable internal load balancer（internal）] チェックボックスがオンの場合はオフにします。
f) [Enable load balancer（public）] チェックボックスがオンの場合はオフにします。
g) [SAVE] をクリックします。

ステップ 3 Windows Azure Pack 管理者：プラン サービスとして ACI ネットワー キングを追加し、レイヤ 4 ～ レイヤ 7 クラウド オーケストレータ モードのリソース プールを使用している Windows Azure Pack プランごとに、次の手順を実行します。

a) サービス管理ポータル (管理者ポータル) にログインします。
b) [Navigation] ペインで [PLANS] を選択します。
c) [Plans] ペインで、[PLANS] を選択し、プラン（ゴールド）をクリックします。
d) [Gold] ペインで、[Networking（ACI）] を選択します。

e) [Networking] ペインで、次のいずれかの操作を実行します。

- Cisco APIC 管理者が Cisco APIC 3.0(x) またはそれ以前で Azure Pack を使用するためにプロビジョニングしたレイヤ 4 ～ レイヤ 7 リソース プールを選択します。
- [Choose one…] を選択して、Azure Pack テナント用の仮想プライベート クラウド NAT ファイアウォール サービスおよび ADC ロード バランサ サービスを無効にします。

f) [SAVE] をクリックします。

ステップ 4 Cisco ACI with Microsoft Windows Azure Pack コンポーネントをアンインストールします。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアンインストール （57 ページ）を参照してください。

ステップ 5 APIC コントローラとスイッチ ソフトウェアをダウングレードします。

『Cisco APIC ファームウェアの管理、インストール、アップグレード、およびダウングレード ガイド』を参照してください。

ステップ 6 ダウングレード バージョンの Cisco ACI with Microsoft Windows Azure Pack コンポーネントをインストールします。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのインストール、設定および確認（6 ページ）を参照してください。