NX-OS スタイル CLI の使用

この章の内容は、次のとおりです。

NX-OS スタイル CLI へのアクセス

（注） Cisco APIC リリース 1.0 からリリース 1.2 まで、デフォルト CLI は管理対象オブジェクト（MO）および管理情報モデルのプロパティから上で直接動作するコマンドの Bash シェルでした。Cisco APIC リリース 1.2 以降のデフォルト CLI は NX-OS スタイル CLI です。オブジェクト モデル CLI は、最初の CLI プロンプトで **bash** コマンドを入力することにより使用できます。

手順

ステップ 1 セキュア シェル（SSH）クライアントから、*username@ip-address* の APIC への SSH 接続を開きます。
初期設定時に設定した管理者のログイン名とアウトオブバンド管理 IP アドレスを使用します。たとえば、admin@192.168.10.1 などがこれに該当します。

ステップ 2 プロンプトが表示されたら、管理者パスワードを入力します。

次の作業

NX-OS スタイル CLI を入力する場合、最初のコマンド レベルは EXEC レベルになります。このレベルから、次のコンフィギュレーション モードに移行できます。

- NX-OS スタイル CLI で続行するには、EXEC モードのままにするか、**configure** と入力してグローバル コンフィギュレーション モードに移行できます。

  NX-OS スタイル CLI コマンドの詳細については、『*Cisco APIC NX-OS Style CLI Command Reference*』を参照してください。

- オブジェクト モデル CLI に移行するには、**bash** と入力します。

  オブジェクト モード CLI コマンドの詳細については、『*Cisco APIC Command-Line Interface User Guide, APIC Releases 1.0 and 1.1*』を参照してください。

APIC の NX-OS スタイル CLI の使用方法

CLI コマンド モードの使用方法

NX-OS スタイルの CLI は、ルートに EXEC モードを持つコマンド モードの階層にまとめられています。この中には、グローバルコンフィギュレーションモードで始まるコンフィギュレーション サブモードのツリーも含まれます。利用できるコマンドは、現在のモードによって異なります。任意のモードで使用可能なコマンドのリストを取得するには、システム プロンプトで疑問符（?）を入力します。

この表では、サブモードの例（DNS）とともに最もよく使用される 2 つのモード（EXEC およびグローバル設定）を挙げて説明します。表には、モードの開始方法と終了方法、および結果のシステムプロンプトを示しています。システムプロンプトから、現在実行しているモードを識別して、そのモードで使用できるコマンドを判断できます。

モード	アクセス方法	プロンプト	終了方法
EXEC	APIC のプロンプトから、execsh を入力します。	`apic#`	終了してログインプロンプトに戻るには、**exit** コマンドを使用します。
グローバル コンフィギュレーション	EXEC モードから、configure コマンドを入力します。	`apic(config)#`	コンフィギュレーション サブモードを終了して親モードに戻るには、**exit** コマンドを使用します。 コンフィギュレーション モードまたはサブモードを終了して EXEC モードに戻るには、**end** コマンドを使用します。
DNS の設定	グローバル コンフィギュレーション モードから dns コマンドを入力します。	`apic(config-dns)#`	

CLI のコマンド階層

コンフィギュレーション モードには、同じような機能を実行するコマンドが同じレベルに集められた、いくつかのサブモードがあります。たとえば、システム、設定、またはハードウェアに関する情報を表示するコマンドはすべて **show** コマンドとしてグループ化されています。また、スイッチを設定できるコマンドはすべて **configure** コマンドとしてグループ化されています。

EXEC モードでは使用できないコマンドを実行するには、階層の最上位となるサブモードから開始します。たとえば、DNS を設定するには、**configure** コマンドを使用してグローバル コンフィギュレーション モードに入り、次に **dns** コマンドを入力します。DNS 設定サブモードに入ると、次の例のように、使用可能なコマンドを照会できます。

```
apic1# configure
apic1(config)# dns
apic1(config-dns)# ?
 address   Configure the ip address for dns servers
 domain    Configure the domains for dns servers
 exit      Exit from current mode
 fabric    Show fabric related information
 no        Negate a command or set its defaults
 show      Show running system information
 use-vrf   Configure the management vrf for dns servers
 where     Show the current mode

apic1(config-dns)# end
apic1#
```

各サブモードを使用すると、プロンプトのより下の階層で作業できます。現在のモードの階層を表示するには、次の例のように **configure** コマンドを使用します。

```
apic1# where
exec
```

```
apic1# configure
apic1(config)# pod 1
apic1(config-pod)# ntp
apic1(config-ntp)# where
configure; pod 1; ntp
```

現在のレベルを終了し、前のレベルに戻るには、**exit** と入力します。直接 EXEC レベルに戻るには、**end** と入力します。

EXEC モード コマンド

CLI セッションを開始する場合、最初は EXEC モードから始めます。この EXEC モードから、コンフィギュレーション モードを開始できます。EXEC コマンドの大半は、現在の設定状態を表示する show コマンドのような 1 回限りのコマンドです。

コンフィギュレーション モード コマンド

コンフィギュレーション モードでは、既存の設定を変更できます。変更した設定を保存すると、スイッチの再起動後も変更内容が保存されます。コンフィギュレーション モードを開始すると、さまざまなプロトコル固有モードに入ることができます。コンフィギュレーション モードは、すべてのコンフィギュレーション コマンドの開始点です。

コマンドおよび構文の一覧表示

すべてのコマンドモードで、疑問符（?）を入力することにより、使用できるコマンドのリストを表示できます。

```
apic1(config-dns)# ?
 address   Configure the ip address for dns servers
 domain    Configure the domains for dns servers
 exit      Exit from current mode
 fabric    Show fabric related information
 no        Negate a command or set its defaults
 show      Show running system information
 use-vrf   Configure the management vrf for dns servers
 where     Show the current mode

apic1(config-dns)# end
apic1#
```

特定の文字シーケンスで始まるコマンドの一覧を表示するには、それらの文字を入力した後に疑問符（?）を入力します。疑問符の前にスペースを入れないでください。

```
apic1# sh?
 show       show running system information
 shutdown   shutdown controller

apic1#
```

コマンドの入力を完了するには、Tab キーを押します。

```
apic1# shu<TAB>
apic1# shutdown
```

キーワードまたは引数のリストを表示するには、キーワードまたは引数の代わりに疑問符を入力します。疑問符の前にスペースを 1 つ入れてください。この形式のヘルプをコマンド構文ヘルプ

と呼びます。入力したコマンド、キーワード、および引数に基づいて、使用できるキーワードまたは引数を表示するためです。

```
apic1(config-dns)# use-vrf ?
 inband-mgmt  Configure dns on inband
 oob-mgmt     Configure dns on out-of-band

apic1(config-dns)#
```

略語が明確であれば、コマンドを省略できます。この例では、**configure** コマンドが省略されています。

```
apic1# conf
apic1(config)#
```

「no」プレフィックスを使用して、取り消すかデフォルト値または条件に戻る

多くの設定コマンドでは、**no** キーワードをコマンドの前に付けて、設定を削除したり、設定をデフォルト値に戻したりすることができます。この例では、以前に設定されたDNSアドレスを設定から削除する方法を示しています。

```
apic1(config-dns)# address 192.0.20.123 preferred
apic1(config-dns)# show dns-address
 Address              Preferred
 -------------------- ---------
 192.0.20.123         yes

apic1(config-dns)# no address 192.0.20.123
apic1(config-dns)# show dns-address
 Address              Preferred
 -------------------- ---------
```

NX-OS スタイル CLI から Bash コマンドを実行する

bash シェルの単一のコマンドを実行するには、次に示す例のように **bash -c '***path/command***'** を入力します。

```
apic1# bash -c '/controller/sbin/acidiag avread'
```

NX-OS スタイル CLI のすべてのモードまたはサブモードから Bash コマンドを実行できます。

スペースや特殊文字を含むコンフィギュレーション テキストを入力する

設定フィールドがユーザ定義のテキストで構成されている場合、Bash での誤った解釈を避けるため、「$」などの特殊文字はエスケープ（「\$」）し、単語または文字列全体は単一引用符で囲む必要があります。

APIC の準備の例について

このマニュアルのいくつかの例の手順には、パラメータ名が含まれています。これらのパラメータ名は、便宜上理解しやすいように例として提供されるもので、それらを使用する必要はありません。

APIC によるスイッチ検出

APICは、ACIファブリックの一部であるすべてのスイッチに対する自動プロビジョニングおよび管理の中心となるポイントです。単一のデータセンターには、複数の ACI ファブリックを組み込むことができます。各データセンターは、自身のAPICクラスタとファブリックの一部であるCisco Nexus 9000 シリーズ スイッチを持つことができます。スイッチが単一の APIC クラスタによってのみ管理されるようにするには、各スイッチがファブリックを管理するその特定の APIC クラスタに登録される必要があります。

APICは、現在管理している任意のスイッチに直接接続されている新規スイッチを検出します。クラスタ内の各 APIC インスタンスは、直接接続されているリーフ スイッチのみを最初に検出します。リーフ スイッチが APIC で登録されると、APIC はリーフ スイッチに直接接続されているすべてのスパイン スイッチを検出します。各スパイン スイッチが登録されると、その APIC はそのスパインスイッチに接続されているすべてのリーフスイッチを検出します。このカスケード化された検出により、APIC は簡単なわずかな手順でファブリック トポロジ全体を検出することができます。

APIC クラスタによるスイッチ登録

（注） スイッチを登録する前に、ファブリック内のすべてのスイッチが物理的に接続され、適切な設定で起動されていることを確認します。シャーシの設置については、http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-installation-guides-list.htmlを参照してください。

スイッチが APIC で登録されると、そのスイッチは APIC で管理されるファブリック インベントリの一部となります。アプリケーション セントリック インフラストラクチャ ファブリック（ACI ファブリック）を使用すると、APICはインフラストラクチャ内のスイッチのプロビジョニング、管理、およびモニタリングのシングル ポイントとなります。

（注） インフラストラクチャのIPアドレス範囲は、インバンドおよびアウトオブバンドのネットワーク用の ACI ファブリックで使用する他の IP アドレスと重複してはなりません。

NX-OS スタイル CLI を使用した未登録スイッチの登録

（注） インフラストラクチャのIPアドレス範囲は、インバンドおよびアウトオブバンドのネットワーク用の ACI ファブリックで使用する他の IP アドレスと重複してはなりません。

手順

ステップ 1 次に示すようにしてコンフィギュレーション モードを開始します。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 次の例のように、スイッチを登録します。

（注） シリアル番号を取得するには、ノード自体に物理的に印刷されたノードのシリアル番号を見るか、または発見されたノードのシリアル番号のリストに対して **acidiag fnvread** コマンドを使用します。

例：

```
apic1(config)# system switch-id FGE173900ZD 101 leaf1
```

ステップ 3 残りのスイッチについて、前のステップを繰り返します。

APIC からのスイッチ検出の検証とスイッチ管理

スイッチが APIC で登録された後、APIC はファブリック トポロジ ディスカバリを自動的に実行し、ネットワーク全体のビューを取得し、ファブリック トポロジ内のすべてのスイッチを管理します。

各スイッチは、個々にアクセスせずに、APIC から設定、モニタ、およびアップグレードできます。

ネットワーク タイム プロトコルの設定

時刻同期と NTP

シスコアプリケーションセントリック インフラストラクチャ（ACI）ファブリックにおいて、時刻の同期は、モニタリング、運用、トラブルシューティングなどの多数のタスクが依存している

重要な機能です。クロック同期は、トラフィック フローの適切な分析にとって重要であり、複数のファブリック ノード間でデバッグとフォールトのタイムスタンプを関連付けるためにも重要です。

1 つ以上のデバイスでオフセットが生じると、多くの一般的な運用問題を適切に診断して解決する機能がブロックされる可能性があります。また、クロック同期によって、アプリケーションのヘルススコアが依存している ACI の内蔵アトミック カウンタ機能をフル活用できます。時刻同期が存在しない場合や不適切に設定されている場合でも、エラーやヘルススコアの低下が引き起こされるわけではありません。これらの機能を適切に使用できるように、ファブリックやアプリケーションを完全に展開する前に、時刻同期を設定する必要があります。デバイスのクロックを同期させる最も一般的な方法は、ネットワーク タイム プロトコル（NTP）を使用することです。

NTP を 設定する前に、どの管理 IP アドレス スキームを ACI ファブリックに配置するかを検討してください。すべての ACI ノードと Application Policy Infrastructure Controller（APIC）の管理を設定するために、インバンド管理とアウトオブバンド管理の 2 つのオプションがあります。ファブリックに対して選択した管理オプションに応じて、NTP の設定が異なります。時刻同期の展開に関するもう 1 つの考慮事項は、時刻源の場所です。プライベート内部時刻または外部パブリック時刻の使用を決定する際は、時刻源の信頼性について慎重に検討する必要があります。

インバンドおよびアウトオブバンドの管理 NTP

（注）

- 管理 EPG が NTP サーバ用に設定されていることを確認してください。設定されていない場合、このサーバはスイッチで設定されません。
- インバンド管理アクセスおよびアウトオブバンド管理アクセスについては、本書の「管理アクセスの追加」という項を参照してください。

- アウトオブバンド管理 NTP：ACI ファブリックをアウトオブバンド管理とともに展開する場合、ファブリックの各ノードは、スパイン、リーフ、および APIC クラスタの全メンバーを含めて、ACI ファブリックの外部から管理されます。この IP 到達可能性を活用することで、各ノードは一貫した時刻源として同じ NTP サーバに個々に照会することができます。NTP を設定するには、アウトオブバンド管理のエンドポイント グループを参照する日付時刻ポリシーを作成する必要があります。日付時刻ポリシーは 1 つのポッドに限定され、ACI ファブリック内のプロビジョニングされたすべてのポッドに展開する必要があります。現在は、ACI ファブリックあたり 1 つのポッドのみが許可されます。
- インバンド管理 NTP：ACI ファブリックをインバンド管理とともに展開する場合は、ACI のインバンド管理ネットワーク内から NTP サーバへの到達可能性を検討します。ACI ファブリック内で使用されるインバンド IP アドレッシングには、ファブリックの外部から到達できません。インバンド管理されているファブリックの外部の NTP サーバを使用するには、その通信を可能にするポリシーを作成します。インバンド管理ポリシーの設定に使用される手順は、アウトオブバンド管理ポリシーの確立に使用される手順と同じです。 違いは、ファブリックが NTP サーバに接続できるようにする方法です。

NTP over IPv6

NTP over IPv6 アドレスは、ホスト名とピア アドレスでサポートされます。gai.conf も、IPv4 アドレスのプロバイダーまたはピアの IPv6 アドレスが優先されるように設定できます。ユーザは、IP アドレス（インストールまたは優先順位よって IPv4、IPv6、または両方）を提供することによって解決できるホスト名を設定できます。

ユーザ アカウントの作成

NX-OS スタイル CLI を使用したローカル ユーザの設定

初期の設定スクリプトで、管理者アカウントが設定され、管理者はシステム起動時の唯一のユーザとなります。APIC は、きめ細かなロールベースのアクセス コントロール システムをサポートしており、そのシステムでは、権限が少ない管理者以外のユーザを含め、ユーザ アカウントをさまざまなロールで作成することができます。

外部認証サーバの AV ペア

Cisco 属性/値（AV）ペアを既存のユーザ レコードに追加して、ユーザ権限を APIC コントローラに伝播することができます。Cisco AV ペアは、APIC ユーザに対してロールベース アクセス コントロール（RBAC）のロールと権限を指定するために使用する単一の文字列です。オープンRADIUS サーバ（/etc/raddb/users）の設定例は次のとおりです。

```
aaa-network-admin Cleartext-Password := "<password>"
Cisco-avpair = "shell:domains = all/aaa/read-all(16001)"
```

NX-OS スタイル CLI を使用した欠落または不良 Cisco AV ペアを持つリモート ユーザのデフォルトの動作の変更

NX-OS スタイル CLI を使用して欠落または不良 Cisco AV ペアを持つリモート ユーザのデフォルトの動作を変更するには、次の手順を実行します。

手順

ステップ 1 NX-OS CLI で、コンフィギュレーション モードで開始します。

例：

```
apic1#
apic1# configure
```

ステップ 2 aaa ユーザ デフォルト ロールを設定します。

例：

```
apic1(config)# aaa user default-role
 assign-default-role  assign-default-role
 no-login             no-login
```

ステップ 3 aaa 認証ログイン メソッドを設定します。

例：

```
apic1(config)# aaa authentication
 login  Configure methods for login

apic1(config)# aaa authentication login
 console  Configure console methods
 default  Configure default methods
 domain   Configure domain methods

apic1(config)# aaa authentication login console
 <CR>

apic1(config)# aaa authentication login domain
 WORD      Login domain name
 fallback
```

AV ペアを割り当てるためのベスト プラクティス

ベストプラクティスとして、シスコは、bash シェルでユーザに割り当てられる AV ペアには 16000 ～ 23999 の範囲の一意の UNIX ユーザ ID を割り当てることを推奨します（SSH、Telnet または Serial/KVM のコンソールを使用）。Cisco AV ペアが UNIX ユーザ ID を提供しない状況が発生すると、そのユーザにはユーザ ID 23999 または範囲内の類似した番号が割り当てられます。これにより、そのユーザのホーム ディレクトリ、ファイル、およびプロセスに UNIX ID 23999 を持つリモート ユーザがアクセスできるようになってしまいます。

外部認証サーバの AV ペアの設定

属性/値（AV）のペア文字列のカッコ内の数字は、セキュア シェル（SSH）または Telnet を使用してログインしたユーザの UNIX ユーザ ID として使用されます。

手順

外部認証サーバの AV ペアを設定します。
Cisco AV ペアの定義は次のとおりです（シスコは、UNIX ユーザ ID が指定されているかどうかにかかわらず AV ペアをサポートします）。

例：

```
* shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2

        * shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(8101)

These are the boost regexes supported by APIC:
```

```
uid_regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})(\\(\\d+\\))$");
regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})$");
```

次に、例を示します。

```
shell:domains = coke/tenant-admin/read-all,pepsi//read-all(16001)
```

NX-OS スタイル CLI を使用したリモート ユーザの設定

ローカルユーザを設定する代わりに、APIC を一元化された企業クレデンシャルのデータセンターに向けることができます。APIC は、Lightweight Directory Access Protocol（LDAP）、Active Directory、RADIUS、および TACACS+ をサポートしています。

外部認証プロバイダーを通じて認証されたリモート ユーザを設定するには、次の前提条件を満たす必要があります。

- DNS 設定は、RADIUS サーバのホスト名ですでに名前解決されている必要があります。
- 管理サブネットを設定する必要があります。

NX-OS スタイル CLI によるリモート ユーザの設定

手順

ステップ 1 NX-OS CLI で、次に示すようにしてコンフィギュレーション モードを開始します。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 次の例では、RADIUS プロバイダーを作成します。

例：

```
apic1(config)# radius-server
 host     RADIUS server's DNS name or its IP address
 retries  Global RADIUS server retransmit count
 timeout  Global RADIUS server timeout period in seconds

apic1(config)# radius-server host 1.1.1.1
apic1(config-host)#
 descr     RADIUS server descr for authentication
 exit      Exit from current mode
 fabric    show fabric related information
 key       RADIUS server key for authentication
 no        Negate a command or set its defaults
 port      RADIUS server port for authentication
 protocol  RADIUS server protocol for authentication
 retries   RADIUS server retries for authentication
 show      Show running system information
 timeout   RADIUS server timeout for authentication
 where     show the current mode
```

```
apic1(config-host)# exit
```

ステップ 3 次の例では、TACACS+ プロバイダーを作成します。

例：

```
 apic1(config)# tacacs-server
 host     TACACS+ server's DNS name or its IP address
 retries  Global TACACS+ server retries period in seconds
 timeout  Global TACACS+ server timeout period in seconds

apic1(config)# tacacs-server host 1.1.1.1
apic1(config-host)# exit
```

ステップ 4 次の例では、LDAP プロバイダーを作成します。

例：

```
apic1(config)# ldap-server
 attribute  An LDAP endpoint attribute to be used as the CiscoAVPair
 basedn     The LDAP base DN for user lookup in the LDAP directory tree
 filter     LDAP search filter for the LDAP endpoint
 host       LDAP server DNS name or IP address
 retries    Global LDAP server retransmit count
 timeout    Global LDAP server timeout period in seconds

apic1(config)# ldap-server host 1.1.1.1
apic1(config-host)#
 enable-ssl            enabling an SSL connection with the LDAP provider
 exit                  Exit from current mode
 fabric                show fabric related information
 filter                Set the LDAP filter to be used in a user search
 key                   LDAP server key for authentication
 no                    Negate a command or set its defaults
 port                  LDAP server port for authentication
 retries               LDAP server retries for authentication
 show                  Show running system information
 ssl-validation-level  Set the LDAP Server SSL Certificate validation level
 timeout               LDAP server timeout for authentication
 where                 show the current mode

apic1(config-host)# exit
apic1(config)#
```

管理アクセスの追加

IPv4/IPv6 アドレスおよびインバンド ポリシー

インバンド管理アドレスは、ポリシーによってのみ（Postman REST API、NX-OS スタイル CLI、または GUI）APIC コントローラにプロビジョニングできます。また、インバンド管理アドレスは、各ノードに静的に設定する必要があります。

アウトオブバンド ポリシーの IPv4/IPv6 アドレス

アウトオブバンド管理アドレスは、ブートストラップ時に、またはポリシーを使用して（Postman REST API、NX-OS スタイル CLI、GUI）APIC コントローラにプロビジョニングできます。また、アウトオブバンド管理アドレスは、各ノードに静的にまたはクラスタ全体にアドレスの範囲（IPv4/IPv6）を指定することによって設定する必要があります。IP アドレスは、範囲からクラスタ内のノードにランダムに割り当てられます。

NX-OS スタイルの CLI を使用した管理アクセスの追加

APIC コントローラには、管理ネットワークに到達するルートが 2 つあります。1 つはインバンド管理インターフェイスを使用し、もう 1 つはアウトオブバンド管理インターフェイスを使用します。

- インバンド管理アクセス：APIC および ACI ファブリックへのインバンド管理接続を設定できます。APIC がリーフ スイッチと通信するときに APIC によって使用される VLAN を最初に設定し、次に VMM サーバがリーフ スイッチとの通信に使用する VLAN を設定します。
- アウトオブバンド管理アクセス：APIC および ACI ファブリックへのアウトオブバンド管理接続を設定できます。アウトオブバンドエンドポイント グループ（EPG）に関連付けられるアウトオブバンド契約を設定し、外部ネットワーク プロファイルにその契約を接続します。

（注） APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

APIC コントローラは、インバンド管理インターフェイスが設定されている場合は、アウトオブバンド管理インターフェイスを通してインバンド管理インターフェイスを常に選択します。アウトオブバンド管理インターフェイスは、インバンド管理インターフェイスが設定されていない場合、または宛先アドレスが APIC のアウトオブバンド管理サブネットと同じサブネットにある場合にのみ使用されます。この動作は、変更または再設定できません。

APIC 管理インターフェイスは IPv6 アドレスをサポートしないため、このインターフェイスを介して外部 IPv6 サーバに接続することはできません。

インバンドまたはアウトオブバンドの管理テナントで外部管理インスタンス プロファイルを設定しても、ファブリック全体の通信ポリシーで設定されているプロトコルには影響しません。外部管理インスタンスプロファイルで指定されているサブネットおよびコントラクトは、HTTP/HTTPS または SSH/Telnet には影響しません。

NX-OS CLI を使用した APIC コントローラ、スパイン、リーフ スイッチのインバンド管理アクセスを設定する

（注） インバンド管理アクセスでは、IPv4アドレスとIPv6アドレスがサポートされます。スタティック設定を使用した IPv6 設定がサポートされます（インバンドとアウトバンドの両方）。IPv4 および IPv6 のインバンドおよびアウトオブバンドのデュアル設定は、スタティック設定を使用する場合にのみサポートされます。詳細については、「*Configuring Static Management Access in Cisco APIC*」の KB 記事を参照してください。

手順

ステップ 1 次の例に示すように、APIC コントローラのインバンド管理インターフェイスの IP アドレスを 1 つ以上変更するには、作業をコンフィギュレーション モードから開始します。

例：

```
apic1# configure
apic1(config)# controller 1
apic1(config-controller)# interface inband-mgmt0
apic1(config-controller-if)# ip address 10.13.1.1/24 gateway 10.13.1.254
apic1(config-controller-if)# exit
```

（注） このモードは、スイッチのインバンド管理インターフェイスには表示されません。

ステップ 2 スイッチ コンフィギュレーション モードを開始することで、スパインおよびリーフ スイッチのインバンド管理インターフェイスを設定できます。次に示すように、スイッチの後にスイッチの ID を入力します。

例：

```
apic1(config)# switch 101
apic1(config-switch)# interface inband-mgmt0
apic1(config-switch-if)# ip address 10.13.1.101/24 gateway 10.13.1.254
```

（注） 上記の例では、スイッチ 101 はリーフまたはスパイン スイッチを設定できます。スイッチには2つのタイプ（スパインとリーフ）がありますが、管理構成の目的ではスイッチがスパインかリーフかは重要ではないため、両方に同じ設定を使用することができます。

例：

IP アドレス プールからの連続するアドレスを使用してスイッチの範囲を設定するには、**ip address-range** コマンドを使用できます。次の例では、広範囲の複数スイッチに対して、インバンド管理ポートの IP アドレスを同時に設定する方法を示します。

```
apic1(config)# switch 101-104
apic1(config-switch)# interface mgmt0
apic1(config-switch-if)# ip address-range 172.23.48.21/21 gateway 172.23.48.1
```

```
apic1(config-switch-if)# exit
apic1(config-switch)# exit
```

ステップ 3 外部のネットワークからインバンド管理ポートへの接続を確立するには、以下の設定ステップを実行します。

a) 外部インバンド接続に使用される VLAN の VLAN ドメインを作成します。

例：

（注） 次の例では、インバンド ネットワークへの接続に使用される管理ステーションは VLAN 11 上の Leaf 102、port 2 に接続され、サブネットは 179.10.1.0/24 です。

```
apic1(config)# vlan-domain external-inband
apic1(config-vlan)# vlan 11
apic1(config-vlan)# exit
```

b) 次の例に示すように、外部管理ステーションに接続されたポートを VLAN ドメインに追加し、インバンド接続用のポート上で VLAN を開始します。

例：

（注） アドレス 179.10.1.254/24 は、外部管理ステーションが使用するゲートウェイ アドレスであり、ゲートウェイ機能は ACI ファブリックによって提供されます。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# switchport trunk allowed vlan 11 inband-mgmt 179.10.1.254/24
```

以前の設定を使用することで、スパインおよびリーフ スイッチのインバンドポートに対して外部管理ステーションを接続できます。

APIC コントローラのインバンド ポートへ接続するには、次の例で説明する追加の設定により、コントローラ接続ポート上で VLAN を開始する必要があります。コントローラ 1 はリーフ 110 のイーサネット 1/1 のポートに接続され、VLAN 10 は APIC コントローラのインバンド接続に使用されます。

コントローラのインバンド VLAN を設定するには、次のように設定します。

```
apic1(config)# controller 1
apic1(config-controller)# interface inband-mgmt0
apic1(config-controller-if)# ip address x.x.x.x gateway x.x.x.y
apic1(config-controller-if)# vlan 10
apic1(config-controller-if)# inband-mgmt epg inb-default
```

APIC インバンド VLAN の VLAN ドメインを作成するには、次のように設定します。

```
apic1(config)# vlan-domain apic-inband
apic1(config-vlan)# vlan 10
apic1(config-vlan)# exit
```

コントローラに接続されているポートの VLAN を許可するには、次のように設定します。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/1
apic1(config-leaf-if)# vlan-domain member apic-inband
```

（注） 以前の設定を使用して、外部管理ステーションを、コントローラのインバンド ポートに接続することができます。インバンド VLAN（この例では VLAN 10）は、すべてのコントローラで同一となる必要があることに注意してください。

ステップ 4 APIC インバンド ポート上の特定のプロトコルに対して外部ネットワークからのアクセスを制御するには、次のように設定します。

例：

```
apic1(config)# tenant mgmt
apic1(config-tenant)# access-list inband-default
```

```
apic1(config-tenant-acl)# no match raw inband-default
apic1(config-tenant-acl)# match tcp dest 443
apic1(config-tenant-acl)# match tcp dest 22
```

前の例では、「no match raw inband-default」によって、デフォルトのアクセス リスト フィルタから allow all のエントリが削除されます。次の match tcp dest 443 および match tcp dest 22 は、インバンド ポート上にあるこれら TCP ポートへのアクセスのみを許可します。

次の作業

- APIC コントローラに再接続するには、新しい IP アドレスを使用する必要があります。
- 新しい IP アドレスがコントローラに割り当てられたら、コントローラの古い IP アドレスを削除する必要があります。

NX-OS CLI を使用した APIC コントローラ、スパイン、リーフ スイッチのアウトオブバンド管理アクセスの設定

（注） アウトオブバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。

手順

ステップ 1 次の例に示すように、APIC コントローラのアウトオブバンド管理インターフェイスの IP アドレスを 1 つ以上変更するにはコンフィギュレーション モードで開始します。

例：

```
apic1# configure
apic1(config)# controller 1
apic1(config-controller)# interface mgmt0
apic1(config-controller-if)# ip address 172.23.48.16/21 gateway 172.23.48.1
apic1(config-controller-if)# exit
apic1(config-controller)# exit
```

例：

次の例は、複数のコントローラを設定する際に IP アドレスの範囲を入力する方法を示しています。

（注） この例では、コントローラ 1 にはアドレス 172.23.48.16/21 が割り当てられ、コントローラ 2 には 172.23.48.17/21 が割り当てられ、コントローラ 3 には 172.23.48.18/21 が割り当てられます。

```
apic1(config)# controller 1-3
apic1(config-controller)# interface mgmt0
apic1(config-controller-if)# ip address-range 172.23.48.16/21 gateway 172.23.48.1
```

ステップ 2 スイッチ コンフィギュレーション モードにすることによって、スパインおよびリーフ スイッチのアウトオブバンド管理インターフェイスを設定できます。次に示すように、スイッチの後にスイッチの ID を入力します。

例：

```
apic1(config)# switch 101
apic1(config-switch)# interface mgmt0
apic1(config-switch-if)# ip address 172.23.48.101/21 gateway 172.23.48.1
```

例：

（注） 上記の例では、スイッチ101はリーフまたはスパインスイッチを設定できます。スイッチには2つのタイプ（スパインとリーフ）がありますが、管理構成の目的ではスイッチがスパインかリーフかは重要ではないため、両方に同じ設定を使用することができます。

例：

IP アドレス プールからの連続するアドレスを使用してスイッチの範囲を設定するには、**ip address-range** コマンドを使用できます。次の例では、4 つのスイッチの IP アドレスを同時に設定する方法を示します。

```
apic1(config)# switch 101-104
apic1(config-switch)# interface mgmt0
apic1(config-switch-if)# ip address-range 172.23.48.21/21 gateway 172.23.48.1
apic1(config-switch-if)# exit
apic1(config-switch)# exit
```

ステップ 3 外部のネットワークからアウトオブバンド管理ポートへの接続を確立するには、以下の設定ステップを実行します。

a) 特定の外部サブネットにアウトオブバンド管理インターフェイスのアクセス制御を提供します。

例：

（注） この例では、179.10.1.0/24 のネットワークを除き、他の外部ネットワークは APIC コントローラまたはリーフ/スパイン スイッチのアウトオブバンド管理インターフェイスに接続できません。System Management ポリシーは、mgmt と呼ばれる特別なテナント下に設定されます。

```
apic1(config)# tenant mgmt
apic1(config-tenant)# external-l3 epg default oob-mgmt
apic1(config-tenant-l3ext-epg)# match ip 179.10.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)#
```

b) アウトオブバンド管理ポート上の特定のプロトコルへの外部ネットワークからのアクセス制御を提供するには、次のように設定します。

例：

（注） この例では、「no match raw oob-default」によって、デフォルトのアクセス リストのフィルタ内の allow all のエントリが削除されます。次の match tcp dest 443 および match tcp dest 22 は、これらの指定されたポート上でのみ管理インターフェイスのアクセスを許可します。

```
apic1(config)# tenant mgmt
apic1(config-tenant)# access-list oob-default
apic1(config-tenant-acl)# no match raw oob-default
apic1(config-tenant-acl)# match tcp dest 443
apic1(config-tenant-acl)# match tcp dest 22
```

次の作業

- APIC コントローラに再接続するには、新しい IP アドレスを使用する必要があります。
- 新しい IP アドレスがコントローラに割り当てられたら、コントローラの古い IP アドレスを削除する必要があります。

既存の IP tables 機能をミラーリングする IPv6 の変更

すべての IPv6 は、ネットワーク アドレス変換（NAT）を除いて、既存の IP tables 機能をミラーリングします。

既存の IP tables

1. 以前は、IPv6 テーブルのすべてのルールが一度に 1 つずつ実行され、すべてのルールの追加または削除に対してシステム コールが行われていました。
2. 新しいポリシーが追加されるたびに、ルールが既存の IP tables ファイルに追加され、ファイルへの追加変更は行われませんでした。
3. 新しい送信元ポートがアウトオブバンドポリシーで設定されると、同じポート番号で送信元と宛先のルールを追加しました。

IP tables への変更

1. IP tables が作成されると、はじめにハッシュ マップに書き込まれ、次に中間ファイル IP tables-new に書き込まれてこれが復元されます。保存すると、新しい IP tables ファイルが /etc/sysconfig/ フォルダに作成されます。これら両方のファイルは同じ場所にあります。すべてのルールにシステム コールを行う代わりに、ファイルを復元および保存している時にのみシステム コールを行う必要があります。
2. ルールを追加する代わりに新しいポリシーがファイルに追加されると、hashmaps にデフォルトポリシーをロードし、新しいポリシーを確認し、hashmaps に追加することによって、IP テーブルがゼロから作成されます。その後、中間ファイル（/etc/sysconfig/iptables-new）に書き込まれて保存されます。
3. アウトオブバンド ポリシーのルールの送信元ポートだけを設定することはできません。宛先ポートまたは送信元ポートいずれかを宛先ポートとともにルールに追加できます。
4. 新しいポリシーが追加されると、新しいルールが IP tables ファイルに追加されます。このルールは、IP tables デフォルト ルールのアクセス フローを変更します。

   ```
   -A INPUT -s <OOB Address Ipv4/Ipv6> -j apic-default
   ```

5. 新しいルールが追加された場合、これは IP tables-new ファイルに存在して IP tables ファイルには存在せず、IP tables-new ファイルにエラーがあることを意味します。復元が正常な場合に限り、ファイルが保存され、新しいルールを IP tables ファイルで確認できます。

（注）

- IPv4 のみ有効な場合、IPv6 ポリシーを設定しないでください。
- IPv6 のみ有効な場合、IPv4 ポリシーを設定しないでください。
- IPv4 と IPv6 の両方が有効な場合にポリシーが追加されると、両方のバージョンに設定されます。したがって、IPv4 サブネットを追加すると IP tables に追加され、同様に IPv6 サブネットは IPv6 tables に追加されます。

VLAN ドメインの設定

NX-OS スタイル CLI を使用した VLAN ドメインの設定

ACI ファブリックは、4K VLAN のグループに分割することができ、ファブリック全体にわたる多数のレイヤ 2（L2）ドメインを複数のテナントから使用できます。

VLAN ドメインはノードおよびポートのグループ上で設定できる一連の VLAN を表します。VLAN ドメインは、ノード、ポート、VLAN などの共通ファブリック リソースを、互いに競合したり個別に管理する必要なく複数のテナントで共有することができます。テナントは 1 つ以上の VLAN ドメインにアクセスできます。

これらの VLAN ドメインは、スタティックまたはダイナミックに設定できます。スタティック VLAN ドメインは、スタティック VLAN プールをサポートしますが、ダイナミック VLAN ドメインは、スタティックとダイナミックの両方の VLAN プールをサポートできます。スタティック VLAN プールの VLAN は、ユーザによって管理され、ベア メタル ホストへの接続などのアプリケーションに使用されます。ダイナミック VLAN プールの VLAN は、ユーザの介入なしに APIC によって割り当てられ、管理されます。VMM などのアプリケーションに使用されます。VLAN ドメインおよびドメイン内の VLAN プールのデフォルト タイプはスタティックです。

テナントが L2/L3 構成にファブリック リソースを使用開始する前に次の手順を実行する必要があります。この手順で NX-OS CLI を使用する方法の例についての詳細ステップは、NX-OS スタイル CLI を使用したテナント、VRF、およびブリッジ ドメインの作成, （26 ページ）を参照してください。

手順

ステップ 1 VLAN ドメインを作成し、各 VLAN ドメインの VLAN を割り当てます。

例：

```
apic1# configure
apic1(config)# vlan-domain dom1
apic1(config-vlan)# vlan 5-100
apic1(config-vlan)# exit
apic1(config)# vlan-domain dom2 dynamic
apic1(config-vlan)# vlan 101-200
apic1(config-vlan)# vlan 301-400 dynamic
```

```
apic1(config-vlan)# exit
apic1(config)# vlan-domain dom3
apic1(config-vlan)# vlan 401-500
```

ステップ 2 リーフ スイッチのポートの VLAN ドメイン メンバーシップを設定します。

例：

```
apic1(config)# leaf 101,102
apic1(config-leaf)# interface ethernet 1/10-20
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# vlan-domain member dom2
apic1(config-leaf-if)#exit
apic1(config-leaf)# interface ethernet 1/21
apic1(config-leaf-if)# vlan-domain member dom3
apic1(config-leaf-if)#exit
```

ステップ 3 L3 ポートまたはサブインターフェイス経由の外部 L3 接続に L3 ポートとして使用するように一部のポートを変換します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/21
apic1(config-leaf-if)# no switchport
In this example, sub-interface encapsulations on ethernet1/21 come from vlans allowed in
dom3.
```

ステップ 4 設定を確認します。

関連トピック

NX-OS スタイル CLI を使用したテナント、VRF、およびブリッジ ドメインの作成, （26 ページ）

VMM ドメインの設定

NX-OS スタイル CLI を使用した VMM ドメインの設定

仮想マシン ネットワーキング ポリシーの設定

APIC は、サードパーティの VM マネージャ（VMM）（VMware vCenter および SCVMM など）と統合し、ACI の利点を仮想化されたインフラストラクチャに拡張します。APIC によって、VMM システム内の ACI ポリシーをその管理者が使用できるようになります。

ここでは、VMware vCenter および vShield を使用する VMM 統合の例を示します。シスコ ACI と VMM 統合の異なるモードに関する詳細については、『ACI Virtualization Guide』を参照してください。

VM マネージャについて

（注） vCenter との統合のために必要な APIC の設定に関する情報を次に示します。VMware コンポーネントの設定手順については、VMware のマニュアルを参照してください。

次は、VM マネージャの用語の詳細情報です。

- VM コントローラは、VMware vCenter や VMware vShield などの、外部仮想マシン管理エンティティです。APIC は、コントローラと通信し、仮想ワークロードに適用されるネットワーク ポリシーを公開します。VM コントローラの管理者は、APIC 管理者に VM コントローラの認証クレデンシャルを提供します。同じタイプの複数のコントローラが同じクレデンシャルを使用できます。
- 仮想マシンのモビリティ ドメイン（vCenter のモビリティ ドメイン）は、同様のネットワーキング ポリシー要件を持つ VM コントローラのグループです。この必須コンテナは、VLAN プールなどのためのポリシー、サーバ/ネットワーク MTU ポリシー、またはサーバ/ネットワーク アクセス LACP ポリシーとともに 1 つ以上の VM コントローラを保持します。エンドポイント グループが vCenter ドメインに関連付けられると、ネットワーク ポリシーが vCenter ドメイン内のすべての VM コントローラにプッシュされます。
- VLAN ドメインの詳細については、NX-OS スタイル CLI を使用した VLAN ドメインの設定, （19 ページ）を参照してください。
- 導入する VMware VCenter では、VLAN モードまたは VXLAN モードで動作する必要があります。VMM ドメインは VLAN プールに関連付け、vShield は vCenter に関連付ける必要があります。

VMM ドメイン プロファイルを作成するための前提条件

VMM ドメイン プロファイルを設定するには、次の前提条件を満たす必要があります。

- すべてのファブリック ノードが検出され、設定されている。
- インバンド（inb）またはアウトオブバンド（oob）管理が APIC 上で設定されている。
- Virtual Machine Manager（VMM）がインストールされ、設定されて、inb/oob 経由で到達可能である。
- VMM の管理者とルートのクレデンシャルがある（vCenter など）。

（注） vCenter の管理者とルートのクレデンシャルを使用しない場合は、必要な最小アクセス許可を持つカスタム ユーザ アカウントを作成できます。必要なユーザ権限のリストについては、最小 VMware vCenter 権限を持つカスタム ユーザ アカウント，（22 ページ）を参照してください。

- IP アドレスではなくホスト名で VMM を参照する予定がある場合は、APIC の DNS ポリシーを設定する必要があります。
- VMware vShield のドメイン プロファイルを作成している場合は、DHCP サーバとリレー ポリシーを設定する必要があります。

最小 VMware vCenter 権限を持つカスタム ユーザ アカウント

Cisco APIC から vCenter を設定するには、vCenter で次の最小権限セットが許可されるクレデンシャルである必要があります。

- アラーム
- データセンター
- フォルダ
- 分散スイッチ
- dvPortgroup
- ネットワーク
- VM
- ホスト

VMM ドメイン プロファイルの作成

ここでは、NX-OS CLI を使用して VMM ドメイン プロファイルを作成する方法と vCenter ドメインまたは vCenter および vShield ドメインの例を示します。

NX-OS スタイル CLI を使用した vCenter ドメイン プロファイルの作成

はじめる前に

ここでは、NX-OS スタイル CLI を使用して vCenter ドメイン プロファイルを作成する方法を説明します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：
```
apic1# configure
apic1(config)#
```

ステップ 2 VLAN ドメインを設定します。

例：
```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

ステップ 3 この VLAN ドメインにインターフェイスを追加します。これらは VMware ハイパーバイザのアップリンク ポートに接続されるインターフェイスです。

例：
```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 4 VMware ドメインを作成して VLAN ドメイン メンバーシップを追加します。

例：
```
apic1(config)# vmware-domain vmmdom1
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

ステップ 5 DVS にドメイン タイプを設定します。

例：
```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

ステップ 6 ドメインのコントローラを設定します。

例：
```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

（注） パスワードを設定する際には、Bash シェルが間違えて解釈することを避けるために、「$」または「!」などの特殊文字の前にバックスラッシュを付ける必要があります（「\$」）。エスケープのバックスラッシュは、パスワードを設定するときにだけ必要です。実際のパスワードにはバックスラッシュは表示されません。

ステップ 7 設定を確認します。

例：
```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
    configure-dvs
      exit
    exit
```

NX-OS スタイル CLI を使用した vCenter および vShield ドメイン プロファイルの作成

はじめる前に

ここでは、NX-OS CLI を使用して vCenter および vShield ドメイン プロファイルを作成する方法を説明します。

手順

ステップ 1 NX-OS CLI で、次のようにコンフィギュレーション モードに入ります。

例：
```
apic1# configure
apic1(config)# exit
```

ステップ 2 VLAN ドメインを次のように設定します。

例：
```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

ステップ 3 この VLAN ドメインにインターフェイスを追加します。これらは次のように VMware ハイパーバイザのアップリンク ポートに接続されるインターフェイスです。

例：
```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)#
```

ステップ 4 次のように、VMware ドメインを作成して VLAN ドメイン メンバーシップを追加します。

例：

```
apic1(config)# vmware-domain vmmdom1
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

ステップ 5 次のように DVS にドメイン タイプを設定します。

例：

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

ステップ 6 次のようにドメインの vCenter コントローラを設定します。

例：

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator password “password”
apic1(config-vmware-vc)#
```

ステップ 7 次のように、この vCenter にアタッチされた VShield コントローラを設定し、この VShield の vxlan プールおよびマルチキャスト アドレス プールを設定します。

例：

```
apic1(config-vmware-vc)# vshield 123.4.5.6
apic1(config-vmware-vc-vs)# username administrator password "password"
apic1(config-vmware-vc-vs)# vxlan pool 10000-12000
apic1(config-vmware-vc-vs)# vxlan multicast-pool 224.3.4.5-224.5.6.7
apic1(config-vmware-vc-vs)# exit
apic1(config-vmware-vc)#
```

ステップ 8 設定を確認します。

例：

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
      vshield 123.4.5.6
        username administrator password *****
        vxlan pool 10000-12000
        vxlan multicast-pool 224.3.4.5-224.5.6.7
        exit
      exit
    configure-dvs
      exit
    exit
```

テナント、VRF、およびブリッジ ドメインの作成

NX-OS スタイル CLI を使用したテナント、VRF、およびブリッジ ドメインの作成

ここでは、テナント、VRF およびブリッジ ドメインを作成する方法を説明します。

（注） テナントの設定を作成する前に、**vlan-domain** コマンドを使用して VLAN ドメインを作成し、ポートを割り当てる必要があります。

手順

ステップ 1 次のように、VLAN ドメイン（一連のポートで許可される一連の VLAN を含む）を作成し、VLAN の入力を割り当てます。

例：
次の例（exampleCorp）では、VLAN 50 ～ 500 が割り当てられることに注意してください。

```
apic1# configure
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 50-500
apic1(config-vlan)# exit
```

ステップ 2 VLAN が割り当てられたら、これらの VLAN を使用できるリーフ（スイッチ）およびインターフェイスを指定します。次に、「vlan-domain member」と入力し、その後に作成したドメインの名前を入力します。

例：
次の例では、これらの VLAN（50 ～ 500）は、インターフェイス イーサネット 1/2 ～ 4（1/2、1/3、1/4 を含む 3 つのポート）上の leaf 101 で有効になっています。これは、このインターフェイスを使用すると、VLAN を使用できるあらゆるアプリケーションにこのポートの VLAN 50 ～ 500 を使用できることを意味します。

```
apic1(config-vlan)# leaf 101
apic1(config-vlan)# interface ethernet 1/2-4
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 次の例に示すように、グローバル コンフィギュレーション モードでテナントを作成します。

例：

```
apic1(config)# tenant exampleCorp
```

ステップ 4 次の例に示すように、テナント コンフィギュレーション モードでプライベート ネットワーク（VRF とも呼ばれます）を作成します。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# vrf context exampleCorp_v1
apic1(config-tenant-vrf)# exit
```

ステップ 5 次の例に示すように、テナントの下にブリッジ ドメイン（BD）を作成します。

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
```

（注） この場合、VRF は「exampleCorp_v1」です。

ステップ 6 次の例に示すように、BD の IP アドレス（IP および ipv6）を割り当てます。

例：

```
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24
apic1(config-tenant-interface)# ipv6 address 2001:1:1::1/64
apic1(config-tenant-interface)# exit
```

次の作業

次の項では、アプリケーションプロファイルを追加し、アプリケーションエンドポイント グループ（EPG）を作成し、EPG をブリッジ ドメインに関連付ける方法について説明します。

関連トピック

NX-OS スタイル CLI を使用した VLAN ドメインの設定, （19 ページ）

NX-OS スタイル CLI を使用したアプリケーション プロファイルおよび EPG の作成

はじめる前に

アプリケーションプロファイル、アプリケーションエンドポイント グループ（EPG）を作成する前に、VLAN ドメイン、テナント、VRF、および BD を作成する必要があります（前の項で説明しています）。

手順

ステップ 1 次の例に示すように、アプリケーション プロファイルを作成します（exampleCorp_web1）。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# application exampleCorp_web1
```

ステップ 2 次の例に示すように、アプリケーションの下に EPG を作成します（exampleCorp_webepg1）。

例：

```
apic1(config-tenant-app)# epg exampleCorp_webepg1
```

ステップ 3 次に示すように、ブリッジ ドメインに EPG を関連付けます。

例：

```
apic1(config-tenant-app-epg)# bridge-domain member exampleCorp_b1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

（注） 各 EPG は BD に属します。EPG は、同じテナント（または）共通のテナントからの BD に属することができます。チェーンを見ると、最下端は EPG、その上は BD です。BD は VRF に属し、VRF はテナントに属します。

次の作業

これらの例では、テナントのアプリケーション EPG を設定する方法について説明しました。次の項では、EPG にポート上の VLAN をマッピングする方法を説明します。

NX-OS スタイル CLI を使用したポートの VLAN の EPG へのマッピング

このステップでは、リーフ スイッチのポートの VLAN をオープンまたは有効にしてアプリケーション EPG に関連付ける方法について説明します。このステップの前提条件は、インターフェイスが、この VLAN を含む VLAN ドメイン（vlan-domain）のメンバであることです。VLAN ドメインの作成については、NX-OS スタイル CLI を使用した VLAN ドメインの設定, （19 ページ）で説明しています。

手順

ステップ 1 リーフ スイッチの ID を入力して、リーフ コンフィギュレーション モードに入ります。

例：

```
apic1(config)# leaf 101
```

（注） 複数のリーフ スイッチで同じ設定を適用するには、「-」または「,」で区切られた ID を使用できます（leaf 101-103 など）。

ステップ 2 前の「interface ethernet 1/2」の例を使用して、次に示すようにモードに入ります。

例：

```
apic1(config-leaf)# interface ethernet 1/2
```

ステップ 3 コマンド「switchport trunk allowed vlan」の後に VLAN を入力してから、テナント、アプリケーション、EPG を入力します（次のようにそれぞれの前の例を使用して示します）。

例：

```
apic1(config-leaf-if)#switchport trunk allowed vlan 50 tenant exampleCorp application
exampleCorp_web1 epg exampleCorp_webepg1
```

アプリケーション ポリシーの展開

Three-Tier アプリケーションの展開

アプリケーション プロファイルでは、APIC がその後ネットワークおよびデータ センターのインフラストラクチャで自動的にレンダリングするアプリケーション要件をモデル化することができます。アプリケーション プロファイルでは、管理者がインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソース プールにアプローチすることができます。アプリケーション プロファイルは、互いに論理的に関連する EPG を保持するコンテナです。EPG は同じアプリケーション プロファイル内のもう一方の EPG および他のアプリケーション プロファイル内の EPG と通信できます。

契約は、エンドポイント グループ間（EPG 間）の通信をイネーブルにするポリシーです。これらのポリシーは、アプリケーション層間の通信を指定するルールです。契約が EPG に付属していない場合、EPG 間の通信はデフォルトでディセーブルになります。EPG 内の通信は常に許可されているので、EPG 内の通信には契約は必要ありません。

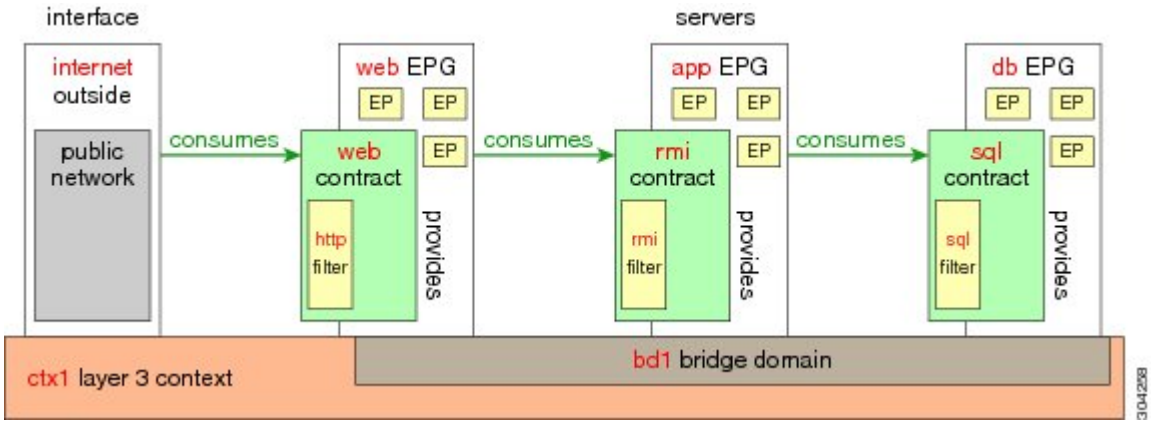
アクセス リスト（「フィルタ」とも呼ばれます）は、アクセス リストを含む契約により許可または拒否されるデータ プロトコルを指定します。契約には、複数のサブジェクトを含めることができます。サブジェクトは、単方向または双方向アクセス リストの作成に使用できます。単方向アクセス リストは、コンシューマからプロバイダー方向（IN）またはプロバイダーからコンシューマ方向（OUT）のどちらかに対して使用されます。双方向アクセス リストは、両方の方向で使用されます。これは、再帰的ではありません。

アプリケーション ポリシーを展開するには、必要なアプリケーション プロファイル、アクセス リスト（フィルタ）、および契約を作成する必要があります。通常、APIC ファブリックは、テナント ネットワーク内の Three-Tier アプリケーションをホストします。この例では、アプリケーションは 3 台のサーバ（Web サーバ、アプリケーション サーバ、およびデータベース サーバ）を使用して実行されます。Three-Tier アプリケーションの例については、次の図を参照してください。

Web サーバには HTTP アクセス リストがあり、アプリケーション サーバには Remote Method Invocation（RMI）アクセス リストがあり、データベース サーバには Structured Query Language

（SQL）アクセス リストがあります。アプリケーション サーバは、SQL 契約を消費してデータベース サーバと通信します。Web サーバは、RMI 契約を消費して、アプリケーション サーバと通信します。トラフィックはWebサーバから入り、アプリケーションサーバと通信します。アプリケーションサーバはその後、データベースサーバと通信し、トラフィックは外部に通信することもできます。

図 *1*：*Three-Tier* アプリケーションの図



HTTP のアクセス リストを作成するパラメータ

この例での http 用のアクセス リスト（フィルタ）を作成するパラメータは次のとおりです。

パラメータ名	HTTP のアクセス リスト（フィルタ）
名前	http
エントリの数	2
エントリ名	Dport-80 Dport-443
Ethertype	IP
プロトコル	tcp tcp
宛先ポート	http https

RMI および SQL のアクセス リストを作成するパラメータ

この例での RMI および SQL 用のフィルタを作成するパラメータは次のとおりです。

パラメータ名	RMI のフィルタ	SQL のフィルタ
名前	rmi	sql
エントリの数	1	1
エントリ名	Dport-1099	Dport-1521
Ethertype	IP	IP
プロトコル	tcp	tcp
宛先ポート	1099	1521

アプリケーション プロファイル データベースの例

この例のアプリケーション プロファイル データベースは次のとおりです。

EPG	提供される契約	消費される契約
Web	Web	rmi
app	rmi	sql
db	sql	--

NX-OS スタイル CLI を使用したアプリケーション ポリシーの展開

EPG が使用するポートは、VM マネージャ（VMM）ドメインまたは EPG に関連付けられた物理ドメインのいずれか 1 つに属している必要があります。

手順

ステップ 1 NX-OS CLI を使用してコンフィギュレーション モードにするには、次を入力します。

例：

```
apic1#configure
apic1(config)#
```

ステップ 2 テナントのアプリケーション ネットワーク プロファイルを作成します。
次の例のアプリケーション ネットワーク プロファイルは OnlineStore です。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# application OnlineStore
apic1(config-tenant-app)#
```

ステップ 3 テナントのこのアプリケーション ネットワーク プロファイルに関するアプリケーション web、db、および app EPG を作成します。

例：

```
apic1(config-tenant-app)# epg web
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# epg db
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# epg app
apic1(config-tenant-app-epg)# exit
```

ステップ 4 テナント モードに戻り、これらの EPG 間のさまざまなトラフィック タイプのアクセス リスト（フィルタ）を作成します。

例：

```
apic1(config-tenant-app)# exit
```

ステップ 5 http および https トラフィック用のアクセス リスト（フィルタ）を作成します。

例：

```
apic1(config-tenant)# access-list http
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# match tcp dest 443
apic1(config-tenant-acl)# exit
```

ステップ 6 Remote Method Invocation（RMI）トラフィック用のアクセス リスト（フィルタ）を作成します。

例：

```
apic1(config-tenant)# access-list rmi
apic1(config-tenant-acl)# match tcp dest 1099
apic1(config-tenant-acl)# exit
```

ステップ 7 SQL/database トラフィック用のアクセス リスト（フィルタ）を作成します。

例：

```
apic1(config-tenant)# access-list sql
apic1(config-tenant-acl)# match tcp dest 1521
apic1(config-tenant)# exit
```

ステップ 8 契約を作成し、EPG間のRMIトラフィック用のアクセスグループ（フィルタ）を割り当てます。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# contract rmi
apic1(config-tenant-contract)# subject rmi
apic1(config-tenant-contract-subj)# access-group rmi both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
```

ステップ 9 契約を作成し、EPG間のWebトラフィック用のアクセス グループ（フィルタ）を割り当てます。

例：

```
apic1(config-tenant)# contract web
apic1(config-tenant-contract)# subject web
apic1(config-tenant-contract-subj)# access-group http both
apic1(config-tenant-contract-subj)# exit
```

ステップ 10 契約を作成し、EPG間のSQLトラフィック用のアクセス グループ（フィルタ）を割り当てます。

例：

```
apic1(config-tenant)# contract sql
apic1(config-tenant-contract)# subject sql
apic1(config-tenant-contract-subj)# access-group sql both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
```

ステップ 11 web EPG にブリッジ ドメインと契約をアタッチします。

例：

```
apic1(config-tenant)# application OnlineStore
apic1(config-tenant-app)# epg web
apic1(config-tenant-app-epg)# bridge-domain member exampleCorp_b1
apic1(config-tenant-app-epg)# contract consumer rmi
apic1(config-tenant-app-epg)# contract provider web
apic1(config-tenant-app-epg)# exit
```

ステップ 12 db EPG にブリッジ ドメインと契約をアタッチします。

例：

```
apic1(config-tenant-app)# epg db
apic1(config-tenant-app-epg)# bridge-domain member exampleCorp_b1
apic1(config-tenant-app-epg)# contract provider sql
apic1(config-tenant-app-epg)# exit
```

ステップ 13 アプリケーション EPG にブリッジ ドメインと契約をアタッチします。

例：

```
apic1(config-tenant-app)# epg app
apic1(config-tenant-app-epg)# bridge-domain member exampleCorp_b1
```

ステップ 14 アプリケーション EPG にプロバイダー契約を関連付けます。

例：

```
apic1(config-tenant-app-epg)# contract provider rm1
```

```
apic1(config-tenant-app-epg)# contract consumer sql
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

ステップ 15 EPG app、db、および web にポートと VLAN を関連付けます。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# interface ethernet 1/2-4
apic1(config-leaf-if)# vlan-domain member exampleCorp
apic1(config-leaf)# exit
apic1(config)# leaf 103
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# switchport
access  trunk  vlan
apic1(config-leaf-if)#  switchport trunk allowed vlan 100 tenant exampleCorp application
OnlineStore epg app
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)#  switchport trunk allowed vlan 101 tenant exampleCorp application
OnlineStore epg db
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/4
apic1(config-leaf-if)#  switchport trunk allowed vlan 102 tenant exampleCorp application
OnlineStore epg web
apic1(config-leaf-if)# exit
```

テナントの外部 L3 接続の設定

ACI ファブリックの MP-BGP ルート リフレクタの設定

ACI ファブリック内のルートを配布するために、MP-BGP プロセスを最初に実行し、スパイン スイッチを BGP ルート リフレクタとして設定する必要があります。

次に、MP-BGP ルート リフレクタの設定例を示します。

（注） この例では、BGP ファブリック ASN は 100 です。スパイン スイッチ 104 と 105 が MP-BGP ルート リフレクタとして選択されます。

```
apic1(config)# pod 1
apic1(config-pod)# bgp fabric
apic1(config-pod-bgp)# asn 100
apic1(config-pod-bgp)# route-reflector spine 104,105
```

NX-OS CLI を使用したテナントの OSPF 外部ルーテッド ネットワークの作成

外部ルーテッド ネットワーク接続の設定には、次のステップがあります。

1 テナントの下に VRF を作成します。

2 外部ルーテッド ネットワークに接続された境界リーフ スイッチの VRF の L3 ネットワーキング構成を設定します。この設定には、インターフェイス、ルーティング プロトコル（BGP、OSPF、EIGRP）、プロトコル パラメータ、ルートマップが含まれています。

3 テナントの下に外部 L3 EPG を作成してポリシーを設定し、これらの EPG を境界リーフ スイッチに導入します。ACI ファブリック内で同じポリシーを共有する VRF の外部ルーテッド サブネットが、1 つの「外部 L3 EPG」または 1 つの「プレフィクス EPG」を形成します。

設定は、2 つのモードで実現されます。

- テナント モード：VRF の作成および外部 L3 EPG 設定
- リーフ モード：L3 ネットワーキング構成と外部 L3 EPG の導入

次の手順は、テナントの OSPF 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、テナントを選択してからテナント用の VRF を作成する必要があります。

（注） この項の例では、テナント「exampleCorp」の「OnlineStore」アプリケーションの「web」epg に外部ルーテッド接続を提供する方法について説明します。

手順

ステップ 1 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 5-1000
apic1(config-vlan)# exit
```

ステップ 2 テナント VRF を設定し、VRF のポリシーの適用を有効にします。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# vrf context
 exampleCorp_v1
apic1(config-tenant-vrf)# contract enforce
apic1(config-tenant-vrf)# exit
```

ステップ 3 テナント BD を設定し、ゲートウェイ IP を「public」としてマークします。エントリ「scope public」は、このゲートウェイ アドレスを外部 L3 ネットワークのルーティング プロトコルによるアドバタイズに使用できるようにします。

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
```

```
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24 scope public
apic1(config-tenant-interface)# exit
```

ステップ 4 リーフの VRF を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant exampleCorp vrf exampleCorp_v1
```

ステップ 5 OSPF エリアを設定し、ルート マップを追加します。

例：

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.1 route-map map100 out
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
```

ステップ 6 VRF をインターフェイス（この例ではサブインターフェイス）に割り当て、OSPF エリアを有効にします。

例：

（注） サブインターフェイスの構成では、メイン インターフェイス（この例では、ethernet 1/11）は、「no switchport」によって L3 ポートに変換し、サブインターフェイスが使用するカプセル化 VLAN を含む vlan ドメイン（この例では dom_exampleCorp）を割り当てる必要があります。サブインターフェイス ethernet1/11.500 で、500 はカプセル化 VLAN です。

```
apic1(config-leaf)# interface ethernet 1/11
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/11.500
apic1(config-leaf-if)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-if)# ip address 157.10.1.1/24
apic1(config-leaf-if)# ip router ospf default area 0.0.0.1
```

ステップ 7 外部 L3 EPG ポリシーを設定します。これは、外部サブネットを特定し、epg 「web」と接続する契約を消費するために一致させるサブネットが含まれます。

例：

```
apic1(config)# tenant t100
apic1(config-tenant)# external-l3 epg  l3epg100
apic1(config-tenant-l3ext-epg)# vrf member v100
apic1(config-tenant-l3ext-epg)# match ip 145.10.1.0/24
apic1(config-tenant-l3ext-epg)# contract consumer web
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)#exit
```

ステップ 8 リーフ スイッチの外部 L3 EPG を導入します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t100 vrf v100
apic1(config-leaf-vrf)# external-l3 epg l3epg100
```

サーバまたはサービス ポリシーの設定

DHCP リレー ポリシーの設定

DHCP リレー ポリシーは、DHCP クライアントとサーバが異なるサブネット上にある場合に使用できます。クライアントが配置された vShield ドメイン プロファイルとともに ESX ハイパーバイザ上にある場合は、DHCP リレー ポリシー設定を使用することが必須です。

vShield コントローラが Virtual Extensible Local Area Network（VXLAN）を展開すると、ハイパーバイザホストはカーネル（vmkN、仮想トンネルエンドポイント（VTEP））インターフェイスを作成します。これらのインターフェイスは、DHCP を使用するインフラストラクチャ テナントで IP アドレスを必要とします。したがって、APIC が DHCP サーバとして動作しこれらの IP アドレスを提供できるように、DHCP リレー ポリシーを設定する必要があります。

ACI fabricは、DHCP リレーとして動作するときに、DHCP オプション 82（DHCP Relay Agent Information Option）を、クライアントの代わりに中継する DHCP 要求に挿入します。応答（DHCP オファー）がオプション 82 なしで DHCP サーバから返された場合、その応答はファブリックによってサイレントにドロップされます。したがって、ACI fabricが DHCP リレーとして動作するときは、ACI fabricに接続されたノードを計算するために IP アドレスを提供している DHCP サーバはオプション 82 をサポートする必要があります。

NX-OS スタイル CLI を使用した APIC インフラストラクチャの DHCP サーバ ポリシーの設定

- アプリケーション EPG で使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインとのそのような関連付けが確立されていないと、APIC は EPG の展開を続行しますが、エラーを生成します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

はじめる前に

DHCP サーバ アドレスに到達するためにレイヤ 2 またはレイヤ 3 接続が設定されていることを確認します。

手順

APIC インフラストラクチャ トラフィックの DHCP サーバ ポリシー設定を設定します。

例：

```
apic1(config)# tenant infra
apic1(config-tenant)# template dhcp relay policy DhcpRelayP
apic1(config-tenant-template-dhcp-relay)# ip address 10.0.0.1 tenant infra application access epg
default
apic1(config-tenant-template-dhcp-relay)# exit
apic1(config-tenant)# interface bridge-domain default
apic1(config-tenant-interface)# dhcp relay policy tenant DhcpRelayP
apic1(config-tenant-interface)# exit
```

DNS サービス ポリシーの設定

DNS ポリシーは、ホスト名で外部サーバ（AAA、RADIUS、vCenter、サービスなど）に接続するために必要です。DNS サービス ポリシーは共有ポリシーであるため、このサービスを使用するすべてのテナントと VRF を特定の DNS プロファイル ラベルで設定する必要があります。ACI ファブリックの DNS ポリシーを設定するには、次のタスクを完了する必要があります。

- 管理 EPG が DNS ポリシー用に設定されていることを確認してください。設定されていない場合、このポリシーはスイッチで有効になりません。
- DNS プロバイダーと DNS ドメインに関する情報が含まれる DNS プロファイル（デフォルト）を作成します。
- DNS プロファイル（デフォルトまたは別の DNS プロファイル）の名前を必要なテナントで DNS ラベルに関連付けます。

テナントごと、VRF ごとの DNS プロファイル設定を設定することができます。適切な DNS ラベルを使用して、追加の DNS プロファイルを作成して、特定のテナントの特定の VRF に適用できます。たとえば、名前が acme の DNS プロファイルを作成する場合、テナント設定で acme の DNS ラベルを適切な [Networking] > [VRF] ポリシー設定に追加できます。

インバンド DNS サービス ポリシーによる外部宛先の設定

次のように、サービスに対して外部宛先を設定します。

ソース	インバンド管理	アウトオブバンド管理	外部サーバの場所
APIC	IP アドレスまたは完全修飾ドメイン名（FQDN）	IP アドレスまたは FQDN	Anywhere

ソース	インバンド管理	アウトオブバンド管理	外部サーバの場所
リーフ スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	Anywhere
スパイン スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	リーフ スイッチに直接接続されます

次に示すのは、外部サーバのリストです。

- Call Home SMTP サーバ
- Syslog サーバ
- SNMP トラップの宛先
- 統計情報のエクスポートの宛先
- エクスポートの設定の宛先
- Techsupport のエクスポートの宛先
- コア エクスポートの宛先

推奨されるガイドラインは次のとおりです。

- 外部サーバは、リーフ アクセス ポートに接続する必要があります。
- 管理ポートの追加の配線を避けるために、リーフ スイッチにはインバンド接続を使用します。

- スパイン スイッチにはアウトオブバンド管理接続を使用します。スパイン スイッチとリーフ スイッチが外部サーバの同じセットに到達できるように、スパイン スイッチのこのアウトオブバンドネットワークをインバンド管理の仮想ルーティングおよび転送（VRF）機能があるリーフ ポートの 1 つに接続します。
- 外部サーバには IP アドレスを使用します。

DNS プロファイルの IPv4 または IPv6 の優先順位のポリシー

DNS プロファイルは、IPv4 と IPv6 のバージョン優先順位の選択をサポートします。ユーザ インターフェイスを使用して、優先順位を有効にすることができます。IPv4 がデフォルトです。

次の例は、Postman REST API を使用したポリシーベースの設定を示します。

```
<?xml version="1.0" encoding="UTF-8”?>
<!— api/node/mo/uni/fabric/dnsp-default.xml —>
<dnsProfile dn="uni/fabric/dnsp-default" IPVerPreference="IPv6" childAction="" descr="" >
</dnsProfile>
```

gai.conf の設定は、宛先アドレス選択を制御します。ファイルには、ラベル テーブル、優先順位テーブル、IPv4 範囲テーブルが含まれます。IPv4 または IPv6 をもう一方よりも優先付けする変更は、優先順位テーブルのエントリに含める必要があります。Linux システムで多数のフレーバーに使用されている標準ファイルの内容例を下に示します。ファイルの precedence ラベルの一行でデフォルト設定を上書きします。

次の例は、IPv4 を IPv6 よりも優先させるための gai.conf です。

```
# Generated by APIC
label ::1/128       0
label ::/0          1
label 2002::/16     2
label ::/96         3
label ::ffff:0:0/96 4
precedence  ::1/128       50
precedence ::/0           40
precedence 2002::/16      30
precedence ::/96          20
# For APICs prefering IPv4 connections, change the value to 100.
precedence ::ffff:0:0/96  10
```

デュアル スタック IPv4 および IPv6 DNS サーバ

DNS サーバには、A レコード（IPv4）または AAAA レコード（IPv6）のプライマリ DNS レコードがあります。A および AAAA レコードは、ドメイン名を特定の IP アドレス（IPv4 または IPv6）と関連付けます。

ACI ファブリックは、IPv4 で実行する信頼できるパブリック DNS サーバを使用するように設定できます。これらのサーバは、A レコード（IPv4）または AAAA レコード（IPv6）で解決および応答できます。

純粋な IPv6 環境では、システム管理者は IPv6 DNS サーバを使用する必要があります。IPv6 DNS サーバは、/etc/resolv.conf に追加することによって有効化されます。

より一般的な環境では、デュアルスタック IPv4 および IPv6 DNS サーバを使用します。デュアルスタックの場合、IPv4 と IPv6 の両方が /etc/resolv.conf にリストされます。ただし、デュアルスタック環境で、単純に IPv6 DNS サーバをリストに追加すると、DNS 解決の大きな遅延を引き起

こす可能性があります。これは、デフォルトでIPv6プロトコルが優先されるため、IPv4 DNSサーバに接続できないためです（/etc/resolv.conf で最初にリストされている場合）。この解決法は、IPv4 DNS サーバの前に IPv6 DNS サーバをリストすることです。また、IPv4 と IPv6 両方のルックアップで同一ソケットを使用できるようにするために、「options single-request-reopen」を追加します。

IPv6 DNS サーバが最初にリストされているデュアルスタック IPv4 および IPv6 DNS サーバの resolv.conf の例を次に示します。「single-request-reopen」オプションにも注意してください。

```
options single-request-reopen
nameserver 2001:4860:4680::8888
nameserver 2001:4860:4680::8844
nameserver 8.8.8.8
nameserver 8.8.4.4
```

デュアル スタック IPv4 および IPv6 環境

ACI ファブリックの管理ネットワークが IPv4 と IPv6 の両方をサポートする場合、Linux システム アプリケーション（glibc）では、getaddrinfo() が IPv6 を最初に返すため、IPv6 ネットワークをデフォルトで使用します。

ただし、特定の条件下ではIPv4アドレスがIPv6アドレスよりも推奨されることがあります。Linux IPv6 スタックには、IPv6 にマッピングされた IPv4 アドレス（::ffff/96）を使用して、IPv6 アドレスとしてマッピングされたIPv4アドレスを有効にする機能があります。これは、IPv6 対応アプリケーションが IPv4 と IPv6 両方を受け入れまたは接続するためにシングル ソケットのみ使用できるようにします。これは /etc/gai.conf の getaddrinfo() の glibc IPv6 選択項目によって制御されます。

/etc/hosts を使用する場合は glibc が複数のアドレスを返すようにするために、/etc/hosts ファイルに「multi on」を追加する必要があります。追加しないと、最初に一致したものだけを返す場合があります。

アプリケーションが IPv4 と IPv6 の両方が存在するかどうかを認識していない場合、異なるアドレス ファミリを使用するフォールバック試行が実行されないことがあります。このようなアプリケーションでは、フォールバックの実装が必要な場合があります。

NX-OS スタイル CLI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定

手順

ステップ 1 NX-OS CLI で、次に示すようにしてコンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 DNS サーバ ポリシーを設定します。

例：

```
apic1(config)# dns
apic1(config-dns)# address 172.21.157.5 preferred
apic1(config-dns)# address 172.21.157.6
apic1(config-dns)# domain company.local default
apic1(config-dns)# use-vrf oob-default
```

ステップ 3 DNS プロファイルを使用する任意の VRF 上で DNS プロファイルのラベルを設定します。

例：

```
apic1(config)# tenant mgmt
apic1(config-tenant)# vrf context oob
apic1(config-tenant-vrf)# dns label default
```

NX-OS スタイル CLI を使用した DNS プロファイルがファブリック コントローラ スイッチに設定および適用されていることの確認

手順

ステップ 1 デフォルトの DNS プロファイルの設定を確認します。

例：

```
apic1# show running-config dns

# Command: show running-config dns
# Time: Sat Oct  3 00:23:52 2015
  dns
    address 172.21.157.5 preferred
    address 172.21.157.6
    domain company.local default
    use-vrf oob-default
    exit
```

ステップ 2 DNS ラベルの設定を確認します。

例：

```
apic1# show running-config tenant mgmt vrf context oob

# Command: show running-config tenant mgmt vrf context oob
# Time: Sat Oct  3 00:24:36 2015
  tenant mgmt
    vrf context oob
      dns label default
      exit
    exit
```

ステップ 3 適用された設定がファブリック コントローラで動作していることを確認します。

例：

```
apic1# cat /etc/resolv.conf
```

```
# Generated by IFC

nameserver 172.21.157.5
nameserver 172.21.157.6
```