Cisco APIC リリース 6.0(x) セキュリティ設定ガイド

初版：2022 年 7 月 11 日

最終更新：2023 年 1 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

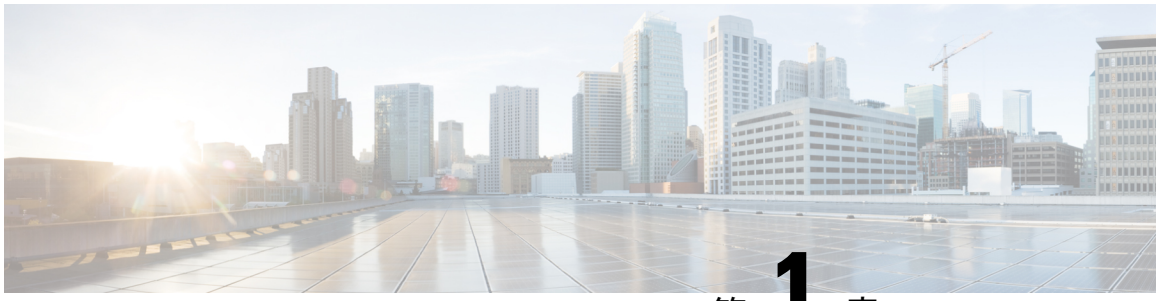
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

目 次



第 1 章

新規および変更情報

この章は、次の項で構成されています。

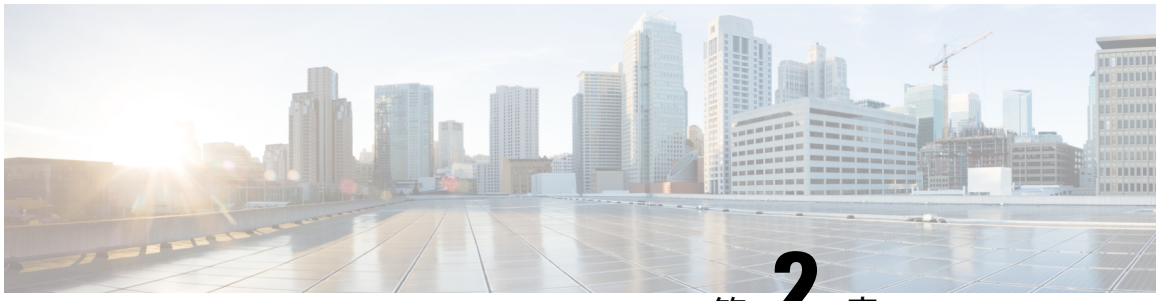
新規および変更情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC* リリース *6.0(1)* の新機能と動作変更

機能または変更	説明	参照先
SAML または OAuth2 のユーザーグループ マップルールのサポート	SAML および OAuth 2 のユーザーグループ マップルールを作成して、外部サーバーによる認証をサポートできます。	GUI を使用してローカル ドメインを作成する （66 ページ）
AAA GUI の変更	**[管理（Admin）]** > **[AAA]** のパスの APIC GUI が変更されました。**[認証（Authentication）]**、**[セキュリティ（Security）]**、および **[ユーザ（Users）]** の作業ペインが拡張され、機能が向上し、使いやすくなりました。	Cisco APIC GUI の機能強化 （5 ページ） （注） GUI の更新の結果、多くの手順のナビゲーション パスが変更されました。パスは、関連する手順に基づいて更新されています。

新規および変更情報



第 2 章

概要

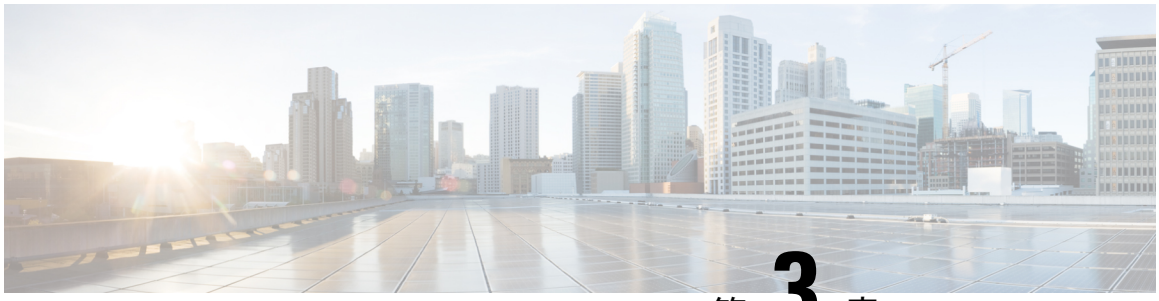
この章の内容は、次のとおりです。

概要

Cisco ACI がサポートするセキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザーの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

コア ファブリック サービスに関する詳細は、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/basic_config/b_APIC_Basic_Config_Guide_2_x/b_APIC_Basic_Config_Guide_2_x_chapter_011.html を参照してください。

概要



第 3 章

アクセス、認証およびアカウンティング

概要

ユーザ アクセス、認可およびアカウンティング

Application Policy Infrastructure Controller（APIC）ポリシーは、Cisco Application Centric Infrastructure（ACI）ファブリックの認証、認可、およびアカウンティング（AAA）機能を管理します。ユーザ権限、ロール、およびドメインとアクセス権限の継承を組み合わせることにより、管理者は細分化された方法で管理対象オブジェクト レベルで AAA 機能を設定することができます。これらの設定は、REST API、CLI、または GUI を使用して実行できます。

（注） ログイン ドメイン名に 32 文字を超えることはできないという既知の制限があります。また、ログイン ドメイン名とユーザ名を合わせた文字数は 64 文字を超えることはできません。

Cisco APIC GUI の機能強化

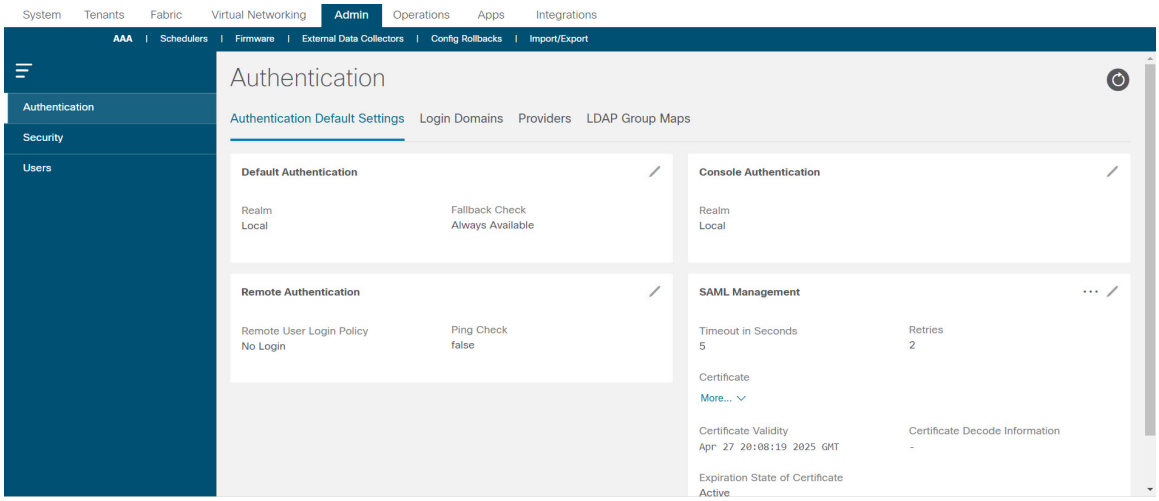
Cisco APIC リリース 6.0(1) から、**[管理（Admin）]** > **[AAA]** のパスの APIC GUI が変更されました。**[認証（Authentication）]**、**[セキュリティ（Security）]**、および **[ユーザ（Users）]** の作業ペインが拡張され、機能が向上し、使いやすくなりました。

GUI の機能拡張

[認証（Authentication）]の [作業（Work）] ペインには、次の 4 つのタブがあります。

- [認証のデフォルト設定（Authentication Default Settings）] : 4 つのダッシュレット、つまり、デフォルト認証、リモート認証、コンソール認証、SAML 管理が含まれています。これらの構成のいずれかを変更する必要がある場合は、[編集（Edit）] アイコンをクリックします。

- [ログイン ドメイン（Login Domains）]：構成済みのログイン ドメインのリストを表示します。
- [プロバイダー（Providers）]：構成されたプロバイダーのリストを表示します。
- [LDAP グループ（LDAP Groups）]：[LDAP グループ マップ（LDAP Group Maps）] と [LDAP グループ マップ ルール（LDAP Group Map Rules）] の 2 つのサブタブが含まれています。各サブタブには、それぞれグループ マップとグループ マップ ルールのリストが表示されます。



リリース 6.0(1) より前では、認証/認可プロトコル（TACACS、SAML など）は個別にタブとして表示され、これらのプロトコルのプロバイダーを作成するには、それぞれの個別のタブに移動する必要がありました。これで、[プロバイダー（Providers）] タブの **[アクション（Actions）]** ボタンを使用して、必要なレルムを選択して、認証/承認プロトコルのプロバイダーを直接作成できます。手順については、プロバイダーを作成する （61 ページ）を参照してください。

[セキュリティ（Security）] の [作業（Work）] ペインには、次のタブがあります。

- [セキュリティのデフォルト設定（Security Default Settings）]：デフォルトのセキュリティ設定を表示します。表示された詳細を変更するには、「編集（Edit）」アイコン をクリックします。
- [セキュリティ ドメイン（Security Domains）]：構成済みのセキュリティ ドメインのリストを表示します。
- [役割（Roles）]：構成された役割のリストを表示します。
- [RBAC ルール（RBAC Rules）]：2 つのサブタブ、[RBAC ルール（RBAC Rules）] と、[ノード ルール（Node Rules）] が含まれています。各サブタブには、それぞれ RBAC ルールとノード ルールのリストが表示されます。
- [認証局（Certificate Authorities）]：構成済みの認証局のリストを表示します。
- [キー リング（Key Rings）]：構成されたキー リングのリストを表示します。

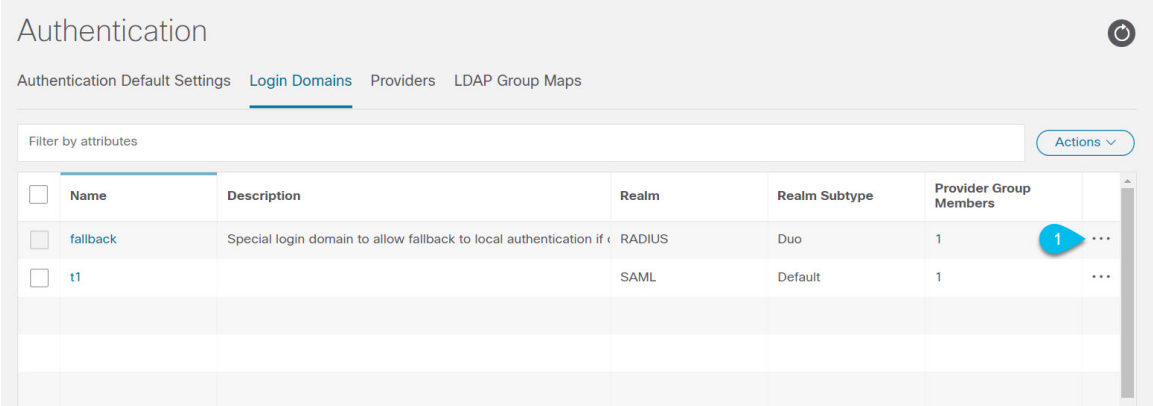
- [JWT キー（JWT Keys）]：構成された JWT キーのリストを表示します。
- [ユーザ アクティビティ（User Activity）]： セッションが記録するものと、ユーザが情報を記録するものの、2 つのサブタブが含まれています。

[ユーザ（Users）] の [作業（Work）] ペインには、次のタブがあります。

- [ローカル（Local）]：ローカルユーザのリストを表示します。[アクション（Actions）]アイコン ··· をクリックすると、以下のアクションを実行できます。
  - SSH 承認の追加
  - ユーザ ドメインの追加
  - X.509 証明書の追加
  - パスワードの変更
  - パスワード履歴のクリア
- [リモート（Remote）]：リモート ユーザのリストを表示します。

ペイン/画面全体に適用される顕著な変更の一部は次のとおりです。

- 要素を作成する： さまざまなタブが表示されているメインの [作業（Work）] ペインで、**[アクション（Actions）]** ボタンを使用して関連する要素を作成します。たとえば、[ログイン ドメイン（Login Domains）] タブを表示している場合は、**[アクション（Actions）]** > **[ログイン ドメインの作成（Create Login Domain）]** を選択して、ログイン ドメインを作成します。
- 要素の詳細情報を表示するには：要素（ログイン ドメイン、プロバイダー、ユーザ、ロールなど）をクリックすると、要素の詳細を含む新しいペインが右側に表示されます。要素のさらに詳しい情報が必要な場合は、[詳細（Details）]アイコン をクリックして、要素に関する詳細情報を含む完全に新しい画面を表示します。
- 要素を編集するには：選択した要素（ログイン ドメイン、プロバイダー、ユーザ、ロールなど）の詳細を表示する画面で、[編集（Edit）]アイコン をクリックして、表示されているパラメータを変更/更新します。
- 要素のイベント分析を表示するには：要素の詳細を表示する画面で、**[イベント分析（Event Analytics）]** タブをクリックして、障害、イベント、および監査ログを表示します。デバッグやトラブルシューティングで使用できます。
- 要素（ログイン ドメイン、ユーザ、ロールなど）のオブジェクト ストアの詳細を表示するには：**[アクション（Action）]** ボタン > **[オブジェクト ストア ブラウザで開く（Open in Object Store Browser）]** をクリックします。オブジェクト ストア内の要素のリストを含む新しい画面が表示されます。または、要素の行にある [アクション（Actions）] ··· アイコンをクリックし、**[オブジェクト ストア ブラウザで開く（Open in Object Store Browser）]** を選択することもできます。選択した要素のオブジェクト ストア画面が表示されます。



（注） [RBAC] タブと [プロバイダー（Providers）] タブでは、**[アクション（Actions）]** ボタンをクリックしてオブジェクト ストアの詳細にアクセスすることはできません。

マルチテナントのサポート

コア Application Policy Infrastructure Controller（APIC）の内部データ アクセス コントロール システムにより、マルチテナント分離が提供され、テナント間での個人情報の漏洩が防止されます。読み取り/書き込みの制約により、テナントによる他のテナントの設定、統計情報、障害、またはイベント データの参照が防止されます。管理者によって読み取り権限が割り当てられない限り、テナントはファブリックの設定、ポリシー、統計情報、障害、またはイベントの読み取りが制限されます。

ユーザ アクセス：ロール、権限、セキュリティ ドメイン

APIC では、ロールベース アクセス コントロール (RBAC) を介してユーザのロールに従ってアクセスが提供されます。Cisco Application Centric Infrastructure (ACI) ファブリック ユーザは、次に関連付けられています。

- 事前定義またはカスタム ロール。ユーザに割り当てられた 1 つ以上の権限のセットです。
- 権限のセット。ユーザがアクセスできる管理対象オブジェクト（MO）を決定します。
- ロールごとの権限タイプ：アクセスなし、読み取り専用、または読み取り/書き込み
- ユーザがアクセスできる管理情報ツリー (MIT) の一部を識別する 1 つ以上のセキュリティ ドメイン タグ

ロールと権限

権限はシステム内の特定の機能に対するアクセス権を制御します。ACI ファブリックは、管理対象オブジェクト（MO）レベルでアクセス権限を管理します。すべてのオブジェクトは、読み取り可能な権限のリストと、書き込み可能な権限のリストを保持しています。特定の機能に

対応するすべてのオブジェクトには、その機能の読み取りまたは書き込みリストの権限が付与されます。オブジェクトは追加の機能に対応する場合があるため、そのリストには複数の権限が含まれている場合があります。権限を含むロールがユーザに割り当てられると、そのユーザには、読み取りリストが読み取りアクセスを指定する関連オブジェクトへの読み取りアクセス権が付与され、書き込みリストが書き込みアクセスを指定するオブジェクトへの書き込みアクセス権が付与されます。

たとえば、「fabric-equipment」は、物理ファブリック内の機器に対応するすべてのオブジェクトへのアクセスを制御する権限です。物理ファブリック内の機器に対応するオブジェクト（「eqptBoard」など）には、特権リストに「fabric-equipment」が含まれます。「eqptBoard」オブジェクトは、「fabric-equipment」権限の読み取り専用アクセスを許可します。「fabric-admin」などの権限「fabric-equipment」が割り当てられているユーザには、「eqptBoard」オブジェクトへの読み取り専用アクセスなど、これらの機器オブジェクトへのアクセス権が付与されます。

（注） 一部のロールには他のロールが含まれています。たとえば、テナント管理者、ファブリック管理者、アクセス管理者などの「-admin」ロールは、同じベース名を持つロールのグループです。たとえば、「access-admin」は「access-connectivity」、「access-equipment」、「access-protocol」、および「access-qos」のグループです。同様に、tenant-adminは「テナント」ベースのロールのグループで、fabric-adminは「ファブリック」ベースのロールのグループです。

「admin」ロールにはすべての権限が含まれます。

ロールと権限の詳細については、『APIC ロールと権限マトリクス』を参照してください。

セキュリティ ドメイン

セキュリティ ドメインは、ACI MIT オブジェクト階層の特定のサブツリーに関連付けられたタグです。たとえば、デフォルトのテナント「common」にはドメインタグ `common` が付いています。同様に、特殊なドメインタグ `all` の場合、MIT オブジェクトツリー全体が含まれます。管理者は、MIT オブジェクト階層にカスタム ドメイン タグを割り当てることができます。たとえば、管理者は「solar」という名前のテナントにドメインタグ「solar」を割り当てることができます。MIT 内では、特定のオブジェクトだけがセキュリティ ドメインとしてタグ付けできます。たとえば、テナントはセキュリティ ドメインとしてタグ付けすることができますが、テナント内のオブジェクトはできません。

（注） セキュリティドメインのパスワード強度パラメータは、**[Custom Conditions]** を作成するか、または提供されている **[Any Three Conditions]** を選択して設定できます。

ユーザを作成してロールを割り当てても、アクセス権は有効になりません。1 つ以上のセキュリティ ドメインにそのユーザを割り当てることも必要です。デフォルトでは、ACI ファブリックには事前作成された次の 2 つの特殊なドメインが含まれています。

- `All`：MIT 全体へのアクセスを許可

- `Infra`：ファブリックアクセスポリシーなどの、ファブリックインフラストラクチャのオブジェクトおよびサブツリーへのアクセスを許可

（注） ユーザのクレデンシャルが許可しない管理対象オブジェクトの読み取り操作の場合、「DN/Class Unauthorized to read」ではなく「DN/Class Not Found」というエラーが返されます。ユーザのクレデンシャルが許可しない管理対象オブジェクトへの書き込み操作の場合、「HTTP 401 Unauthorized」というエラーが返されます。GUI では、ユーザのクレデンシャルが許可しないアクションの場合、表示されないか、またはグレー表示されます。

事前に定義された一連の管理対象オブジェクト クラスをドメインに関連付けることができます。これらのクラスがオーバーラップすることはできません。ドメインの関連付けをサポートするクラスの例：

- レイヤ 2 およびレイヤ 3 のネットワークで管理されたオブジェクト
- ネットワーク プロファイル (物理、レイヤ 2、レイヤ 3、管理など)
- Quality of Service（QoS）ポリシー

ドメインに関連付けることができるオブジェクトが作成されると、ユーザは、ユーザのアクセス権の範囲内でオブジェクトにドメインを割り当てる必要があります。ドメインの割り当てはいつでも変更できます。

仮想マシン管理 (VMM) ドメインがセキュリティ ドメインとしてタグ付けされている場合、セキュリティ ドメイン内のユーザは、対応するタグ付き VMM ドメインにアクセスできます。たとえば、solar という名前のテナントに sun というセキュリティ ドメインのタグが付いており、VMM ドメインにも sun というセキュリティ ドメインのタグが付いている場合、solar テナント内のユーザは各自のアクセス権限に従って VMM ドメインにアクセスできます。

連続してログインに失敗した後のユーザーのロックアウト

4.2(4) リリース以降、ユーザーが設定された回数のログイン試行に失敗すると、ユーザーがログインできないようにすることができます。特定の期間内にユーザーが何回ログインに失敗可能かを指定できます。ユーザーが何度もログインに失敗すると、そのユーザーは指定された期間ログインできなくなります。

この機能は、Cisco Application Centric Infrastructure（ACI）データベースにあるローカル ユーザーと、RADIUS、LDAP、TACACS+、DUO プロキシ、SAML、RSA などの外部認証サーバーで認証されたリモート ユーザーの両方の失敗したログイン試行をカウントします。1 つの外部認証サーバー タイプを使用して連続して認証に失敗したためにロックアウトされたリモート ユーザーは、すべての外部認証サーバー タイプからロックアウトされます。たとえば、RADIUS サーバーを使用してログインに失敗した後にロックアウトされたユーザーは、LDAP サーバーを使用しているときにもロックアウトされます。AAA サーバーが到達不能またはダウンしたために失敗した認証、または不正な SSH キーが原因で失敗した認証は、ユーザーのロックアウトにはカウントされません。この機能は、間違ったパスワードの入力のみを考慮します。

クラスタ内の 1 つの Cisco Application Policy Infrastructure Controller（APIC）ノードからロックアウトされたユーザーは、リーフ スイッチとスパイン スイッチを含む、クラスタ内のすべてのノードからロックアウトされます。Cisco ACI データベースに存在しないローカル ユーザーは、この機能によりロックアウトできません。

（注） CLI を使用してこの機能を設定できません。

アクセス権のワークフローの依存関係

Cisco Application Centric Infrastructure (ACI) RBAC のルールによって、ファブリック全体へのアクセスを有効にするか、一部へのアクセスに制限します。たとえば、ベア メタル サーバ アクセス用のリーフ スイッチを設定するには、ログインしている管理者が `infra` ドメインに対する権限を持っている必要があります。デフォルトでは、テナント管理者は `infra` ドメインに対する権限を持っていません。この場合、リーフ スイッチに接続されているベア メタル サーバの使用を計画しているテナント管理者は、そのために必要なすべての手順を実行することはできません。テナント管理者は、`infra` ドメインに対する権限を持っているファブリック管理者と連携する必要があります。ファブリック管理者は、テナント管理者が ACI リーフ スイッチに接続されたベア メタル サーバを使用するアプリケーション ポリシーを導入するために使用するスイッチ設定ポリシーをセットアップします。

AAA RBAC の役割および権限

Application Policy Infrastructure Controller（APIC）は、次の AAA ロールと権限を提供します。

（注） Cisco APIC リリース 5.0(1) では、関連する多くのレガシー権限が統合されているため、権限の数は以前のリリースから削減されています。以前の権限から現在の権限へのマッピングを レガシー権限の再マッピング に示します。

（注） Cisco APIC で定義された各ロールについて、APIC のロールと権限のマトリックスには、書き込み可能な管理オブジェクトクラスと読み取り可能な管理オブジェクトクラスが表示されます。

- 表 2 : ロールの権限：管理 （12 ページ）
- 表 3 : ロールの権限：aaa （12 ページ）
- 表 4 : ロールの権限：access-admin （12 ページ）
- 表 5 : ロールの権限：fabric-admin （13 ページ）
- 表 6 : ロールの権限：nw-svc-admin （13 ページ）

表 *2:* ロールの権限：管理

ロール：管理	
特権	**説明**
admin	すべてのファブリックの機能へのフルアクセスを提供します。管理者権限は、その他のすべての権限を組み合わせたものとみなされます。

表 *3:* ロールの権限：*aaa*

ロール：aaa	
特権	**説明**
aaa	ポリシーの認証、許可、アカウンティング、インポート/エクスポートの設定に使用されます。

表 *4:* ロールの権限：*access-admin*

Role: access-admin	
特権	**説明**
access-connectivity	インフラでのレイヤ 1 ～ 3 の構成、テナントの L3Out でのスタティックルート構成、管理インフラポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーでレイヤ 1 ～ 3 のプロトコル構成に使用されます。

Role: access-admin	
特権	説明
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。

表 *5 :* ロールの権限：*fabric-admin*

ロール：fabric-admin	
特権	説明
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ 1 ～ 3 の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1 ～ 3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN およびヘルススコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイント トラッキングポリシーに使用されます。

表 *6 :* ロールの権限：*nw-svc-admin*

ロール：nw-svc-admin	
特権	説明
nw-svc-policy	レイヤ 4 ～ レイヤ 7 ネットワークサービス オーケストレーションの管理に使用されます。

表 *7 :* ロールの権限：*nw-svc-params*

ロール： nw-svc-params	
特権	説明
nw-svc-params	レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。

表 *8 :* ロールの権限：*ops*

Role: ops	
特権	**説明**
ops	設定されているポリシーの表示に使用されます（ポリシーのトラブルシューティングなど）。 （注） **Ops** ロールは、新しいモニタリング ポリシーおよびトラブルシューティング ポリシーの作成には使用できません。これらのポリシーは、Cisco APIC の他のすべての構成と同様に、**admin** 権限を使用して作成する必要があります。

表 *9 :* ロールの権限：*port-mgmt*

ロール：**port-mgmt**	
特権	**説明**
port-mgmt	ノードをセキュリティドメインに割り当てるために使用されます。また、ノードルールを持つセキュリティドメインのユーザーは、`port-mgmt` のロールを持つドメイン `all` に割り当てる必要があります。

表 *10 :* ロールの権限：*tenant-admin*

Role: tenant-admin	
特権	**説明**
aaa	ポリシーの認証、許可、アカウンティング、インポート/エクスポートの設定に使用されます。
access-connectivity	インフラでのレイヤ 1 ～ 3 の構成、テナントの L3Out でのスタティックルート構成、管理インフラポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーでレイヤ 1 ～ 3 のプロトコル構成に使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。

Role: tenant-admin	
特権	説明
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ 1 ～ 3 の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1 ～ 3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN およびヘルススコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイントトラッキングポリシーに使用されます。
nw-svc-policy	レイヤ 4 ～ レイヤ 7 ネットワークサービス オーケストレーションの管理に使用されます。
ops	設定されているポリシーの表示に使用されます（ポリシーのトラブルシューティングなど）。 （注） **Ops** ロールは、新しいモニタリング ポリシーおよびトラブルシューティング ポリシーの作成には使用できません。これらのポリシーは、Cisco APIC の他のすべての構成と同様に、**admin** 権限を使用して作成する必要があります。
tenant-connectivity	ブリッジドメイン、サブネット、および VRF などの レイヤ 1 ～ 3 の接続変更に使用されます。これには、リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシー、テナントのインバンドおよびアウトオブバンド管理接続構成。アトミックカウンタやヘルススコアなどのデバッグ/モニタリングポリシーなどがあります。
tenant-epg	エンドポイント グループの削除/作成など、テナント構成の管理に使用されます。
tenant-ext-connectivity	ファームウェアポリシーの書き込みアクセスに使用されます。これには、テナント L2Out および L3Out 構成の管理、traceroute、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバポリシーがあります。

Role: tenant-admin	
特権	説明
tenant-ext-protocol	BGP、OSPF、PIM、IGMP などのテナント外部レイヤ 1 ～ 3 プロトコルの管理、およびトレースルート、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバポリシーに使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。
tenant-network-profile	ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ 1 ～ 3 プロトコルの構成、テナント トレースルートポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。
vmm-policy	認証や接続など、仮想マシンネットワークのポリシーを管理するために使用されます。

表 *11 :* ロールの権限：*tenant-ext-admin*

Role: tenant-ext-admin	
特権	説明
tenant-connectivity	ブリッジドメイン、サブネット、および VRF などの レイヤ 1 ～ 3 の接続変更に使用されます。これには、リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシー、テナントのインバンドおよびアウトオブバンド管理接続構成。アトミックカウンタやヘルススコアなどのデバッグ/モニタリングポリシーなどがあります。
tenant-epg	エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。
tenant-ext-connectivity	ファームウェアポリシーの書き込みアクセスに使用されます。これには、テナント L2Out および L3Out 構成の管理、traceroute、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバポリシーがあります。

Role: tenant-ext-admin	
特権	説明
tenant-ext-protocol	BGP、OSPF、PIM、IGMP などのテナント外部レイヤ 1 ～ 3 プロトコルの管理、およびトレースルート、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバポリシーに使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。
tenant-network-profile	ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ 1 ～ 3 プロトコルの構成、テナント トレースルートポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。
vmm-policy	認証や接続など、仮想マシンネットワークのポリシーを管理するために使用されます。

表 *12 :* ロールの権限： *vmm-admin*

Role: vmm-admin	
特権	説明
vmm-policy	認証や接続など、仮想マシンネットワークのポリシーを管理するために使用されます。

カスタム ロール

カスタム ロールを作成し、ロールに権限を割り当てることができます。インターフェイスは、すべての管理対象オブジェクト クラスに 1 つ以上の権限を内部的に割り当てます。XML モデルで、権限はアクセス属性に割り当てられています。権限のビット数は、コンパイル時に割り当てられ、クラスのインスタンスまたはオブジェクトごとではなく、クラスごとに適用されます。

45 権限ビットだけでなく、「aaa」権限ビットはすべての AAA サブシステムの設定と読み取り操作に適用されます。次の表は、サポートされている権限の組み合わせの一覧を提供します。表の行は Cisco Application Centric Infrastructure（ACI）モジュールを表し、列は特定のモジュールの機能を表します。セルの「○」の値は、モジュールがアクセス可能な機能と、機能にアクセスするための権限ビットが存在することを示します。空のセルは、権限ビットでアクセスで

きないモジュールの特定の機能を示します。権限ビットについての詳細は、各ビットの機能について参照してください。

	Connectivity	QoS	セキュリティ	アプリケーション	Fault	Stats	Provider	サービス プロファイル	サービス チェーン
VMM	はい		はい		はい	はい	はい		
ファブリック	はい	はい	はい	はい	はい	はい	はい		
External	はい	はい	はい		はい	はい			はい
テナント	はい	はい	はい	EPG、NP	はい	はい			はい
Infra	はい	はい	はい	はい	はい	はい			はい
操作					はい	はい			
ストレージ	はい	はい	はい	はい	はい	はい			
ネットワーク サービス	はい	はい	はい	はい	はい	はい		はい	

複数のセキュリティ ドメイン間で物理リソースを選択的に公開する

ファブリック全体の管理者は、RBAC規則を使用して、異なるセキュリティドメインにあるため他の方法ではアクセス不可能なユーザに対し、物理リソースを選択的に公開します。

たとえば、ソーラーというテナントのユーザが仮想マシン管理（VMM）ドメインへのアクセスを必要とする場合、ファブリック全体の管理者によって、これを許可するRBAC規則を作成することができます。RBAC 規則は、次の 2 つの部分から構成されます。アクセス対象オブジェクトを検索する識別名（DN）と、オブジェクトにアクセスするユーザを含むセキュリティドメインの名前です。したがって、この例では、ソーラーというセキュリティドメイン内の指定ユーザがログインすると、このルールにより、VMMドメインおよびツリーの内の子オブジェクトすべてへのアクセスが許可されます。VMM ドメインへのアクセスを複数のセキュリティドメイン内のユーザに許可するには、ファブリック全体の管理者は、セキュリティドメインそれぞれについて、VMM ドメインの DN とセキュリティ ドメインを含む RBAC 規則を作成します。

（注） 管理情報ツリー内の異なる部分に存在するユーザに対し、RBAC規則によりオブジェクトを公開することは可能ですが、CLIの使用によってツリーの構造を横断することでそのようなオブジェクトに移動することはできません。ただし、RBAC規則に含まれるオブジェクトのDNをユーザが把握していれば、ユーザはMO検索コマンドにより、CLIを使用してそれを見つけることができます。

複数のセキュリティ ドメイン間でのサービス共有を有効にする

ファブリック全体の管理者は、RBAC規則を使用して、テナント間の共有サービスを可能にするトランステナントEPG通信をプロビジョニングします。

APIC ローカル ユーザ

管理者は、外部AAAサーバを使用しないことを選択し、APIC自体でユーザを設定することができます。これらのユーザは、APIC ローカル ユーザと呼ばれます。

ユーザがパスワードを設定する時点で、APICによって以下の基準が検証されます。

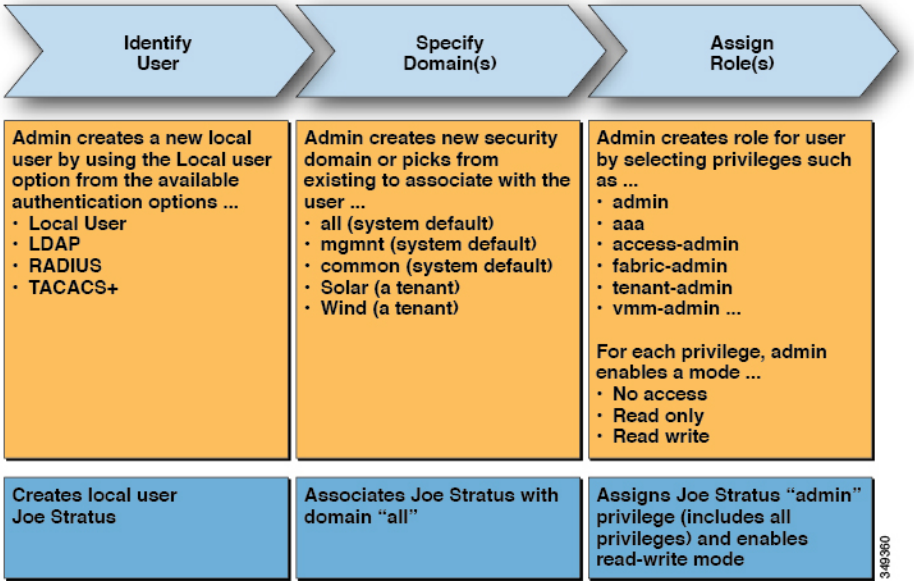
- パスワードの最小長は8文字です。
- パスワードの最大長は64文字です。
- 連続して繰り返される文字は3文字未満です。
- 小文字、大文字、数字、記号の文字種のうち少なくとも3種類の文字が含まれている必要があります。
- 簡単に推測できるパスワードは使用しません。
- ユーザ名やユーザ名を逆にしたものは使用できません。
- cisco、isco、またはこれらの文字列の並べ替えを変化させたものや、それらの文字の大文字化の変更により取得される変形語であってはなりません。

Cisco ACIでは、パスワードの保存にSHA256一方向ハッシュを使用した暗号化ライブラリが使用されます。保管中のハッシュされたパスワードは、暗号化されたファイルシステムに保存されます。暗号化されたファイルシステムのキーは、Trusted Platform Module（TPM）を使用して保護されます。

またAPICにより、管理者は、外部で管理されている認証Lightweight Directory Access Protocol（LDAP）、RADIUS、TACACS+、またはSAMLサーバで設定されたユーザにアクセス権を付与できます。ユーザは、異なる認証システムに属し、APICに同時にログインできます。

次の図は、ACIファブリック全体へのフルアクセス権があるローカルAPIC認証データベース内の管理ユーザを設定するプロセスがどのように動作するかを示します。

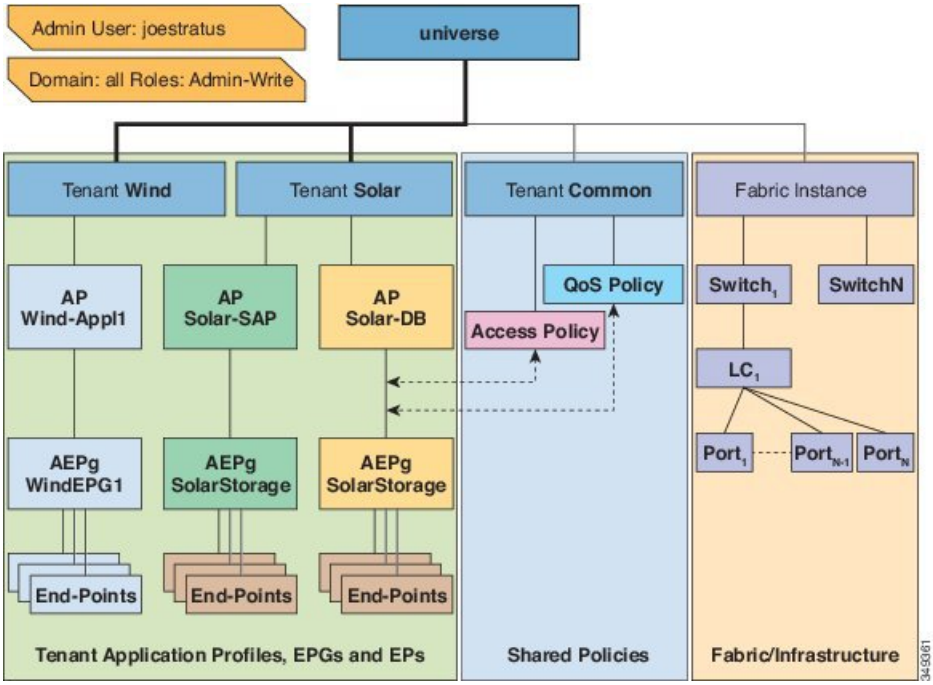
図 *1: APIC* ローカル ユーザの設定プロセス



（注） セキュリティ ドメイン「all」は、管理情報ツリー（MIT）全体を表します。このドメインには、システム内のすべてのポリシーとAPICよって管理されるすべてのノードが含まれます。テナント ドメインには、テナントのすべてのユーザおよび管理対象オブジェクトが含まれます。テナント管理者には、「all」ドメインへのアクセス権を付与しないでください。

次の図は、管理ユーザ Joe Stratus が持つシステムへのアクセス権を示します。

図 *2*:「*all*」ドメインへ管理ユーザを設定した結果



読み取り/書き込み「管理者」権限を持つユーザ Joe Stratus は、ドメイン「all」に割り当てられ、システム全体へのフル アクセス権が与えられます。

ローカル ユーザー向け OTP ベース 2 要素認証

ファブリック管理者ユーザーは、ローカルユーザーのワンタイムパスワード（OTP）機能を有効にできます。ワンタイムパスワードは30秒ごとに変更され、セキュリティが強化されます。OTP を有効にすると、Cisco Application Policy Infrastructure Controller（APIC）は、base32 OTP キーである、ランダムな人間が判読できる 16 バイナリオクテットを生成します。この OTP キーは、二要素認証に使用されるユーザーの OTP を生成するために使用されます。

Cisco APIC は、二要素認証で使用する次のセキュリティ プラットフォームをサポートしています。

- Duo Mobile App を使用した Duo Security
- Google、Google Authenticator アプリ（Android および Apple iOS スマートフォンのみ）

（注） 対応しているアプリストアから、表示されたアプリをダウンロードする必要があります。

これらのセキュリティ プラットフォームは、ユーザー ID のリポジトリとして機能しません。これらのプラットフォームは、組織の既存の認証（オンプレミスまたはクラウドベース）に加えて、二要素認証を提供します。二要素認証は、ユーザーが組織のプライマリ認証ソースで認証を完了すると発生します。

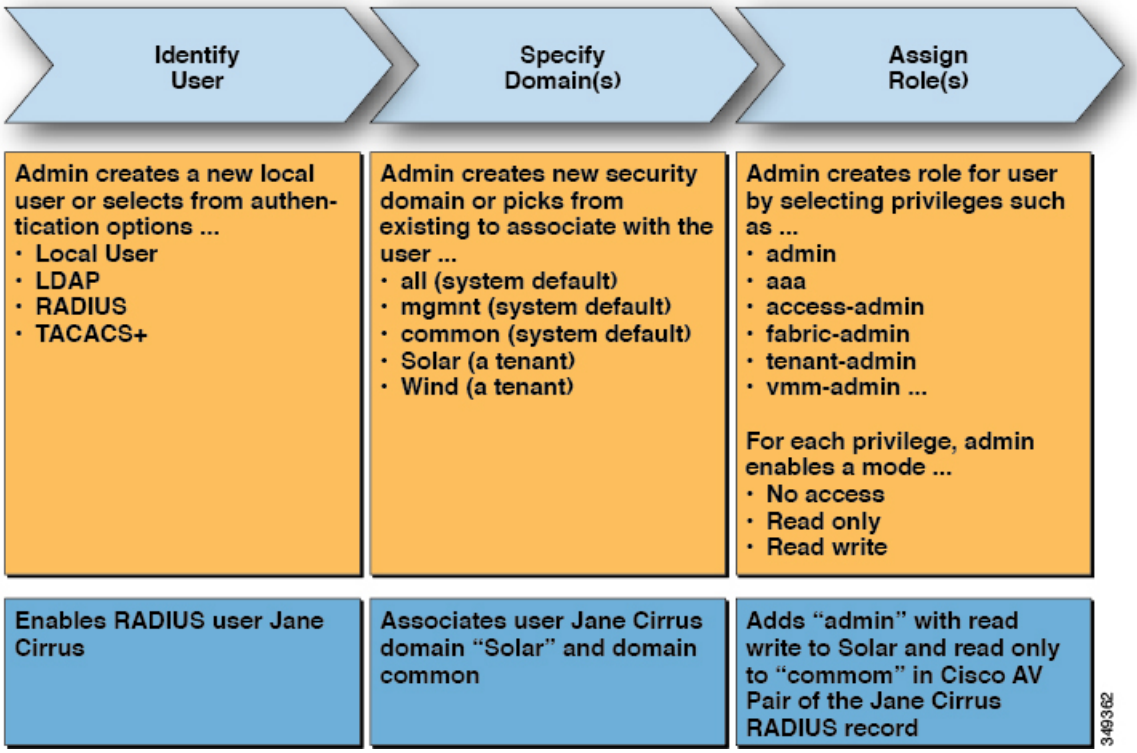
プラットフォームは、プライマリ認証ソースで認証を完了した後、3 種類の二要素認証方法をサポートします。

- スマートフォンで適切なモバイルアプリを使用したモバイルでのプッシュ通知。
- 登録済みの電話または携帯電話での通話。
- 適切なモバイルアプリで生成されるパスコード。

外部管理されている認証サーバのユーザ

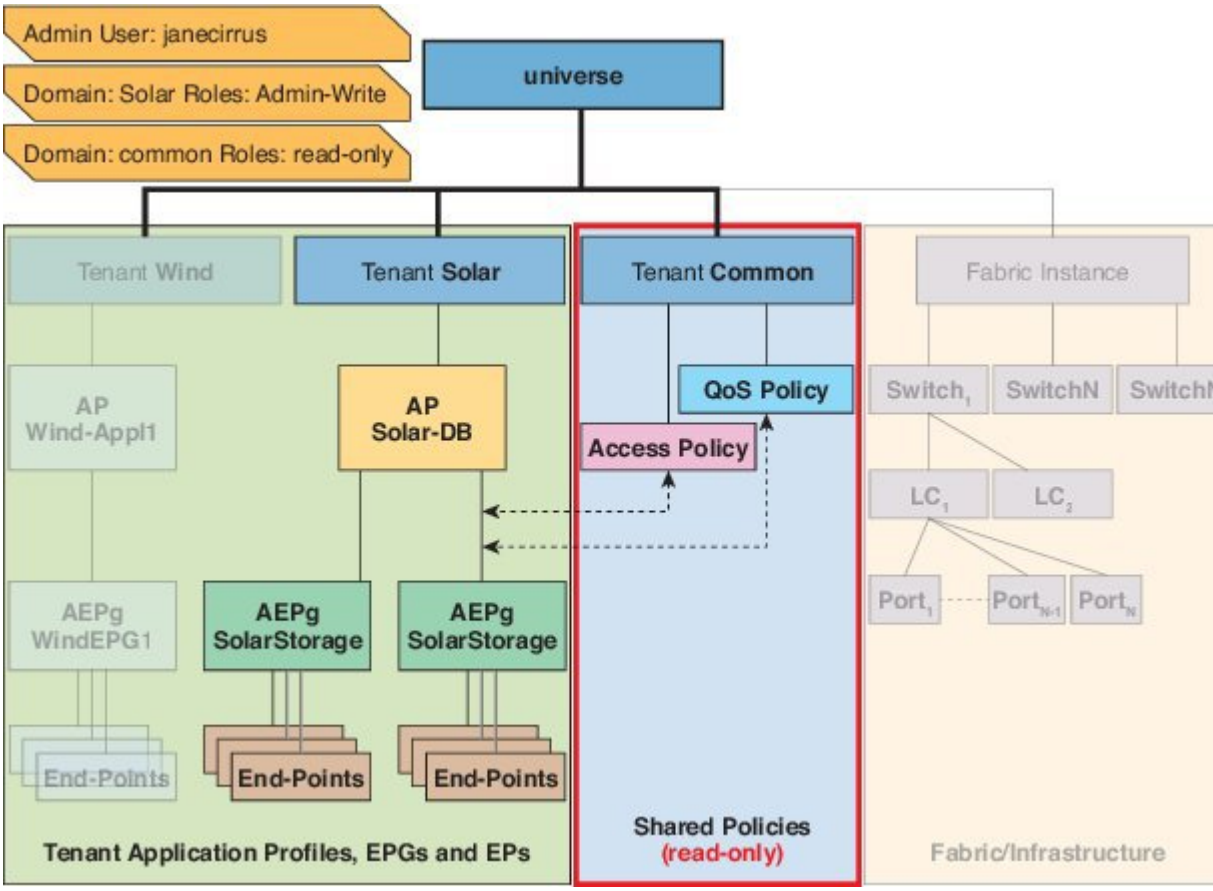
次の図は、テナント Solar へのフル アクセス権がある外部 RADIUS サーバ内の管理ユーザを設定するプロセスがどのように動作するかを示します。

図 *3*: 外部認証サーバでのユーザ設定のプロセス



次の図は、管理ユーザ Jane Cirrus が持つシステムへのアクセス権を示します。

図 *4 :* テナント ***Solar*** へ管理ユーザを設定した結果



この例では、Solar テナントの管理者には、Solar テナントに含まれるすべてのオブジェクトへのフル アクセス権と、テナント Common への読み取り専用アクセス権があります。テナント管理者 Jane Cirrus には、テナント Solar へのフル アクセス権があり、テナント Solar で新しいユーザを作成する機能などがあります。テナント ユーザは、自身が所有し制御する ACI ファブリックの設定パラメータを変更できます。また、エンドポイント、エンドポイント グループ（EPG）およびアプリケーション プロファイルなどの適用されるエンティティ（管理対象オブジェクト）の統計情報の読み取り、障害およびイベントのモニタもできます。

上記の例では、ユーザ Jane Cirrus は外部 RADIUS 認証サーバで設定されました。外部認証サーバで AV ペアを設定するには、既存のユーザ レコードに Cisco AV ペアを追加します。Cisco AV ペアは、APIC 上のユーザに対するロールベース アクセス コントロール（RBAC）のロールと権限を指定します。次に RADIUS サーバは、ユーザ権限を APIC コントローラに伝播します。

上記の例のオープン RADIUS サーバ（/etc/raddb/users）の設定は次のとおりです。

```
janecirrus Cleartext-Password := "<password>"
Cisco-avpair = "shell:domains = solar/admin/,common//read-all(16001)"
```

この例には、次の要素が含まれています。

- `janecirrus` はテナント管理者です。

- solar はテナントです。
- admin は書き込み権限があるロールです。
- common は、テナント共通サブツリーで、すべてのユーザがそのサブツリーへの読み取り専用アクセス権を持っています。
- read-all は、読み取り権限があるロールです。

Cisco AV ペアの形式

Cisco APIC は、管理者が外部認証サーバで Cisco AV ペアを設定し、1 個の AV ペアの文字列のみを検索することを要求しています。これを行うには、管理者は既存のユーザ レコードに Cisco AV ペアを追加します。Cisco AV ペアは、ユーザの RBAC ロールおよび権限に必要な APIC を指定します。

AV ペア文字列を機能させるため、次の形式にする必要があります。

```
shell:domains =
ACI_Security_Domain_1/ACI_Write_Role_1|ACI_Write_Role_2|ACI_Write_Role_3/ACI_Read_Role_1|ACI_Read_Role_2,
ACI_Security_Domain_2/ACI_Write_Role_1|ACI_Write_Role_2|ACI_Write_Role_3/ACI_Read_Role_1|ACI_Read_Role_2,
ACI_Security_Domain_3/ACI_Write_Role_1|ACI_Write_Role_2|ACI_Write_Role_3/ACI_Read_Role_1|ACI_Read_Role_2
```

- **shell:domains=**：ACI が正常に文字列を読み取るために必要です。シェル文字列を常にプリペンドする必要があります。
- **ACI_Security_Domain_1//admin**：管理者にこのセキュリティ ドメインのテナントへの読み取り専用アクセス権を付与します。
- **ACI_Security_Domain_2/admin**：管理者にこのセキュリティ ドメインのテナントへの書き込みアクセス権を付与します。
- **ACI_Security_Domain_3/read-all**：このセキュリティ ドメインのテナントへの読み取り/書き込みすべてのアクセス権を付与します。

（注） /により区別される文字列のセキュリティ ドメイン、書き込み、読み取りセクション同じセキュリティ ドメイン内の | により区別される複数の書き込みまたは読み取り権限

（注） Cisco APIC リリース 2.1 より、AV ペアに UNIX ID が指定されていない場合、APIC は UNIX の固有ユーザー ID を内部的に割り当てます。

APIC は、次の正規表現をサポートしています。

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

例：

- 例 1：writeRole のみを持つ単一のログイン ドメインを含む Cisco AV ペア

```
shell:domains=ACI_Security_Domain_1/Write_Role_1|Write_Role_2/
```

- 例 2：readRole のみを持つ単一のログイン ドメインを含む Cisco AV ペア

```
shell:domains=Security_Domain_1//Read_Role_1|Read_Role_2
```

（注） 文字「/」はログイン ドメインごとに writeRole と readRole の間を区切る記号で、使用するロールの種類が 1 つのみである場合も必要です。

Cisco AV ペアの文字列は、大文字と小文字が区別されます。エラーが表示されなくても、使用する大文字と小文字がドメイン名またはロールに一致していない場合は、予期しない権限が付与されることがあります。

AV ペア GUI の設定

セキュリティ ドメインは、 **[Admin]** > **[AAA]** > **[Security Management]** > **[Security Domains]** の ACI GUI で定義されており、**[テナント]** > **[Tenant_Name]** > **[ポリシー]** のテナントに割り当てられています。

セキュリティ ドメインには読み取りまたは書き込み権限のいずれかが必須です。これらの権限は、**[APIC]** > **[Admin]** > **[Security Management]** > **[Roles]** で定義されています。権限が書き込みセクションに入力される場合、ACI_Security_Domain_1/admin/admin/admin を使用する必要がないため、自動的に同じレベルの読み取り権限を付与します。

リモート ユーザー ロールの変更

ユーザー権限を「動的」に変更可能で、ユーザーがロール変更の要求を行うことが可能になり、ローカルまたはリモートで保存されている情報に基づいて、要求ロールが許可または拒否されます。

ロール変更は Cisco ACS サーバー経由でのみサポートされており、明示的な「要求」に基づくロールの割り当てによって実行できます。

ACI ファブリックは、Radius、TACACS +、LDAP プロトコルを使用して外部認証をサポートします。上記の両方の方法で、リモート認証サーバにロール変更機能をサポートするコンポーネントが含まれていると仮定します。

Cisco Secure ACS サーバーは、TACACS+ プロトコルのリモート認証、認証、およびアカウンティングの機能を提供します。

デフォルト デバイス管理または**デフォルト ネットワーク アクセス サービス**のどちらかにルールが一致する必要があります。

認証で、別のルール設定が設定されています。

- **AVPairOps**：tacacs + ユーザー名および AVPair 値と一致します（cisco-av-pair*newrole）。ルールに一致すると、ACI_OPS シェル プロファイルが返されます

- **NoAVPair**：tacacs + ユーザー名のみ一致し、一致で ACI_ADMIN シェル プロファイルを返します
- **opsuser**：プロトコルのみ一致し、ACI_OPS シェル プロファイルを返します

GUI を使用したリモート ユーザー ロールの変更

始める前に

ロールは、最初に AVPair と一致するように Cisco ASC サーバーで設定し、その一致に基づいてシェル認証プロファイルとして選択する必要があります。

ステップ 1 ASC 認証ポリシーを作成します。**[Access Policies]** > **[Access Services]** > **[Default Device Admin Identity]** に移動し、次の手順を実行します。

（注） シェル プロファイルが CiscoAVPair を使用して設定され、ユーザの認証に使用されます。

a) [TACACS+:AVPair equals cisco-av-pair*] に条件を追加し、[OK] をクリックします。

（注） デフォルトでは、ユーザは **cisco-av-pair** ロールを使用して認証されます。

b) [TACACS+:AVPair equals cisco-av-pair*readall] に条件を追加し、[OK] をクリックします。

（注） APIC でキーワード **readall** を使用して、ロールを **default** ロールから **readall** ロールに変更します（シェル プロファイルで read-all が設定されます）。

ステップ 2 APIC GUI にログインし、[welcome, <ログイン名>] ドロップダウン リストをクリックして、[Change Remote User Role] を選択します。

ステップ 3 [Change Remote User Role] ダイアログボックスで、[User Name]、[Password]、[New Role] の各フィールドに情報を入力し、[Submit] をクリックします。

GUI が更新され、新しいロールが適用されます。

（注） 親ロールに戻るには、もう一度 [Change Remote User Role] ダイアログボックスを開き、[User Name] と [Password] に情報を入力しますが、[New Role] フィールドは空欄のままにしておきます。

REST API を使用したリモート ユーザ ロールの変更

始める前に

ロールは、最初に AVPair と一致するように Cisco ASC サーバーで設定し、その一致に基づいてシェル認証プロファイルとして選択する必要があります。

ユーザーは、ユーザー名 **apicadmin** とパスワードでログインします。

ステップ 1 新しいロールに変更します。

例：

```
<!--   api/requestNewRole/json   -->
<aaaChangeRole>
<attributes userName="apic#tacacs” apicadmin="pwd Ins3965!” role=“newrole"/>
```

ステップ 2 元のロールに戻ります。

例：

```
<!--   api/requestNewRole/json   -->
<aaaChangeRole>
<attributes userName="apic#tacacs” apicadmin="pwd Ins3965!” role=“"/>
```

署名ベースのトランザクションについて

Cisco ACI ファブリックの APIC コントローラは、ユーザを認証するためにさまざまな方法を提供します。

主要な認証方式ではユーザ名とパスワードが使用され、APIC REST API は APIC に対するその後のアクセスに使用できる認証トークンを返します。これは、HTTPS が使用不可であるか有効でない状況では安全でないと見なされます。

提供されている別の認証形式では、トランザクションごとに計算される署名が活用されます。その署名の計算には秘密キーが使用され、そのキーは安全な場所に保管して秘密にしておく必要があります。APIC がトークン以外の署名が付いた要求を受信すると、APIC は X.509 証明書を活用して署名を確認します。署名ベースの認証では、APICに対するすべてのトランザクションに新しく計算された署名が必要です。これは、ユーザがトランザクションごとに手動で行うタスクではありません。理想的には、この機能は APIC と通信するスクリプトまたはアプリケーションで使用する必要があります。この方法では、攻撃者がユーザクレデンシャルを偽装またはなりすますためには RSA/DSA キーを解読する必要があるため、最も安全です。

（注） また、リプレイ攻撃を防ぐためには HTTPS を使用する必要があります。

認証に X.509 証明書ベースの署名を使用する前に、次の必須タスクが完了していることを確認します。

1. OpenSSL または同様のツールを使用して X.509 証明書と秘密キーを作成します。
2. APIC のローカル ユーザを作成します（ローカル ユーザがすでに利用可能である場合、このタスクはオプションです）。
3. APIC のローカル ユーザに X.509 証明書を追加します。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- ローカル ユーザはサポートされます。リモート AAA ユーザはサポートされません。

- APIC GUI は証明書認証方式をサポートしません。
- WebSocket と eventchannel は X.509 要求では動作しません。
- サードパーティにより署名された証明書はサポートされません。自己署名証明書を使用します。

アカウンティング

ACI ファブリック アカウンティングは、障害およびイベントと同じメカニズムで処理される以下の 2 つの管理対象オブジェクト（MO）によって処理されます。

- `aaaSessionLR` MO は、APIC およびスイッチでのユーザ アカウントのログイン/ログアウト セッション、およびトークン更新を追跡します。ACI ファブリック セッション アラート機能は、次のような情報を保存します。
  - ユーザ名
  - セッションを開始した IP アドレス
  - タイプ（telnet、https、REST など）
  - セッションの時間と長さ
  - トークン更新：ユーザ アカウントのログイン イベントは、ユーザ アカウントが ACI ファブリックの権利を行使するために必要な、有効なアクティブ トークンを生成します。

（注） トークンはログインに関係なく期限切れになります。ユーザはログアウトできますが、トークンは含まれているタイマー値の期間に従って期限切れになります。

- `aaaModLR` MO は、ユーザがオブジェクトに対して行う変更、およびいつ変更が発生したかを追跡します。
- AAA サーバが ping 可能でない場合は、使用不可としてマークされ、エラーが表示されます。

`aaaSessionLR` と `aaaModLR` の両方のイベント ログが、APIC シャードに保存されます。データがプリセットされているストレージ割り当てサイズを超えると、先入れ先出し方式でレコードを上書きします。

（注） APIC クラスタ ノードを破壊するディスク クラッシュや出火などの破壊的なイベントが発生した場合、イベント ログは失われ、イベント ログはクラスタ全体で複製されません。

aaaModLR MO と aaaSessionLR MO は、クラスまたは識別名（DN）でクエリできます。クラスのクエリは、ファブリック全体のすべてのログ レコードを提供します。ファブリック全体の aaaModLR レコードはすべて、GUI の **[Fabric]** > **[Inventory]** > **[POD]** > **[History]** > **[Audit Log]** セクションから入手できます。APIC GUI の **[History]** > **[Audit Log]** オプションを使用すると、GUI に示された特定のオブジェクトのイベント ログを表示できます。

標準の syslog、callhome、REST クエリ、および CLI エクスポート メカニズムは、aaaModLR MO と aaaSessionLR MO のクエリ データで完全にサポートされます。このデータをエクスポートするデフォルト ポリシーはありません。

APIC には、一連のオブジェクトまたはシステム全体のデータの集約を報告する、事前設定されたクエリはありません。ファブリック管理者は、aaaModLR および aaaSessionLR のクエリ データを定期的に syslog サーバにエクスポートするエクスポート ポリシーを設定できます。エクスポートされたデータを定期的にアーカイブし、システムの一部またはシステム ログ全体のカスタム レポートを生成するために使用できます。

共有サービスとしての外部ネットワークへのルーテッド接続の課金と統計情報

Cisco Application Policy Infrastructure Controller（APIC）は、共有サービスとして外部ネットワークへのルーテッド接続用に設定されたポートからバイト カウントおよびパケット カウント課金統計情報を収集するように設定できます。外部ネットワークは、Cisco Application Centric Infrastructure（ACI）内の外部 L3Out エンドポイント グループ（l3extInstP 管理対象オブジェクト）として表されます。任意のテナントの任意の EPG は、外部ネットワークへのルーテッド接続のために外部 L3Out EPG を共有できます。課金統計情報は、共有サービスとして外部 L3Out EPG を使用するテナントの各 EPG について収集できます。外部 L3Out EPG がプロビジョニングされているリーフスイッチは、課金統計情報を集約先である Cisco APIC に転送します。アカウンティング ポリシーは、これらの課金統計情報を定期的にサーバにエクスポートするように設定できます。

設定

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。

GUI を使用したローカルユーザーの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。

- 必要に応じて、ユーザがアクセスするセキュリティ ドメインが定義されていること。たとえば、新しいユーザ アカウントがテナントへのアクセスに制限される場合、テナント ドメインはそれに応じてタグ付けされます。
- 以下を行うことができる APIC ユーザーアカウントを使用できること。
  - ターゲット セキュリティ ドメインでのローカル ユーザ アカウントの作成。ターゲット ドメインが `all` である場合、新しいローカル ユーザの作成に使用するログイン アカウントは、`all` にアクセスできるファブリック全体の管理者である必要があります。ターゲット ドメインがテナントである場合、新しいローカル ユーザの作成に使用するログイン アカウントは、ターゲット テナント ドメインに対する完全な読み取り/書き込みアクセス権を持つテナント管理者である必要があります。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

ステップ 2 [Navigation] ペインで、[Users] をクリックします。

作業ペインで、[**ローカル（Local）**] タブが表示されていることを確認します。

ステップ 3 **作業**ペインで、[**アクション（Actions）**] をクリックして、[**ローカルユーザーの作成（Create Local User）**] を選択します。

ステップ 4 [**ユーザー名（Username）**] フィールドにユーザー名を入力します。

ログイン ID は、次のガイドラインを満たしている必要があります。

- APIC 内で一意である必要があります。
- 先頭は英字にする必要があります。
- 1 ー 32 文字を使用できます。
- 英数字、アンダースコア、ハイフンを使用してください。

ユーザーアカウントの作成後は、ユーザー名を変更できません。ユーザアカウントを削除し、新しいユーザ アカウントを作成する必要があります。

ステップ 5 [Password] フィールドにパスワードを入力します。[**確認パスワード（Confirm Password）**] フィールドに同じパスワードを入力します。

ステップ 6 （オプション）ユーザー名の [**説明（Description）**] を入力します。

ステップ 7 [**アカウントのステータス（Account Status）**] オプションを使用して、ユーザーアカウントを有効化または無効化できます。オプションは、アクティブ、非アクティブ、ブロックです。

ステップ 8 （オプション）ユーザー名に対し、[**姓（Last Name）**]、[**名（First Name）**]、[**電子メールアドレス（Email Address）**]、[**電話番号（Phone Number）**] を入力します。

ステップ 9 セキュリティドメインを追加するには、[**セキュリティドメインの追加（Add Security Domain）**] をクリックします。表示される [**セキュリティドメインの追加（Add Security Domain）**] ウィンドウで、次の詳細を入力します。

a) [**セキュリティドメインの選択（Select Security Domain）**] をクリックし、ドロップダウンリストからセキュリティドメインを選択します。

b) ロールをユーザー名に関連付けるには、[**ロールの選択（Select Role**）] をクリックし、ドロップダウンリストからロールを選択します。
c) ドロップダウンリストから [**権限タイプ（Privilege Type**）] を選択し、チェックマークをクリックして、選択したロールに権限を関連付けます。
d) **[追加（Add）]** をクリックします。

ステップ 10 [**有効期限設定のステータス（Expiration Set Status**）] オプションを有効にするには、[有効（Enabled）] のチェックボックスをオンにします。

チェックボックスを選択すると、日付と時刻を入力する必要がある場所にテキスト ボックスが表示されます。この日時を過ぎると、ユーザー名は非アクティブになります。

ステップ 11 [**パスワードの更新が必要（Password Update Required**）] オプションを有効にするには、[有効（Enabled）] のチェックボックスをオンにします。

チェックボックスを選択すると、ユーザは最初のログインに成功した後、パスワードを更新することが求められます。

ステップ 12 [**OTP**] オプションを有効にするには、[有効（Enabled）] のチェックボックスをオンにします。

チェックボックスを選択すると、ユーザの OTP キーと QR コードが生成されます。

ユーザの作成後、*[ユーザー名（User_name）]* > [詳細（Details）] アイコンをクリックして、ユーザの詳細画面を表示します。表示された OTP キーをクリックすると、QR コードが表示されます。

ステップ 13 [**ユーザー証明書属性（User Cert Attribute field**）] フィールドに、認証証明書からのユーザー ID を入力します。これは、証明書ベースの認証の場合です。

ステップ 14 [X509 証明書（X509 Certificate）] フィールドで、[**X509 証明書を追加（Add X509 Certifcate**）] をクリックして、名前と証明書の文字列を追加します。

X509 証明書の生成については、X.509 証明書と秘密キーの生成 （34 ページ）の手順を参照してください。

ステップ 15 [SSH 認証（SSH Authorization）] フィールドで、[**SSH 認証の追加（Add SSH Authorization**）] をクリックして、名前と認証データを追加します。

SSH 認証データを生成するには、ローカル マシンで UNIX コマンドの **ssh-keygen** を実行します。

ステップ 16 [保存（Save）] をクリックします。

GUI を使用した SSH 公開キー認証の設定

始める前に

- ターゲット セキュリティ ドメインでローカル ユーザ アカウントを作成します。ターゲット ドメインが `all` である場合、新しいローカル ユーザの作成に使用するログイン アカウントは、`all` にアクセスできるファブリック全体の管理者である必要があります。ターゲット ドメインがテナントである場合、新しいローカル ユーザの作成に使用するログイン ア

カウントは、ターゲット テナント ドメインに対する完全な読み取り/書き込みアクセス権を持つテナント管理者である必要があります。

- UNIX コマンド **ssh-keygen** を使用して公開キーを生成します。

  デフォルトのログイン ドメインは **local** に設定する必要があります。

ステップ 1 メニューバーで、**[管理者（Admin）]** > **[ユーザー（Users）]** を選択し、**[ローカル（Local）]** タブが表示されていることを確認します。

ステップ 2 **作業**ペインで、事前に作成したユーザーの名前をクリックします。

ユーザーに関する情報を含むウィンドウが右側に表示されます。

ステップ 3 **[詳細（Details）]** アイコンをクリックすると、新しい画面に  およびユーザーの詳細が表示されます。

下方向にスクロールして SSH 認証の詳細を確認します。

ステップ 4 [**編集（Edit**）] アイコンをクリックすると、  、および [**ローカル ユーザーの編集（Edit Local User**）] 画面が表示されます。必要に応じて、SSH の詳細を変更できます。

（注） リモートロケーションにダウンロードするための SSH 秘密キーファイルを作成するには、メニューバーで、**[ファイル名（Firmware）]** > **[タスクのダウンロード（Download Tasks）]** を展開します。

ステップ 5 **[保存（Save）]** をクリックします。

NX-OS スタイル CLI を使用したローカル ユーザの設定

手順の概要

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。
2. 新しいユーザを次に示すように作成します。

手順の詳細

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 新しいユーザを次に示すように作成します。

例：

```
apic1(config)# username
 WORD       User name (Max Size 28)
```

```
 admin
 cli-user
 jigarshah
 test1
 testUser

apic1(config)# username test
apic1(config-username)#
 account-status      Set The status of the locally-authenticated user account.
 certificate         Create AAA user certificate in X.509 format.
 clear-pwd-history   Clears the password history of a locally-authenticated user
 domain              Create the AAA domain to which the user belongs.
 email               Set The email address of the locally-authenticated user.
 exit                Exit from current mode
 expiration          If expires enabled, Set expiration date of locally-authenticated user account.

 expires             Enable expiry for locally-authenticated user account
 fabric              show fabric related information
 first-name          Set the first name of the locally-authenticated user.
 last-name           Set The last name of the locally-authenticated user.
 no                  Negate a command or set its defaults
 password            Set The system user password.
 phone               Set The phone number of the locally-authenticated user.
 pwd-lifetime        Set The lifetime of the locally-authenticated user password.
 pwd-strength-check  Enforces the strength of the user password
 show                Show running system information
 ssh-key             Update ssh key for the user for ssh authentication
 where               show the current mode

apic1(config-username)# exit
```

REST API を使用したローカル ユーザの設定

手順の概要

1. ローカル ユーザを作成します。

手順の詳細

ローカル ユーザを作成します。

例：

```
URL: https://apic-ip-address/api/node/mo/uni/userext.xml
POST CONTENT:
    <aaaUser name="operations" phone="" pwd="<strong_password>" >
        <aaaUserDomain childAction="" descr="" name="all" rn="userdomain-all" status="">
        <aaaUserRole childAction="" descr="" name="Ops" privType="writePriv"/>
        </aaaUserDomain>
    </aaaUser>
```

X.509 証明書と秘密キーの生成

ステップ 1 OpenSSL コマンドを入力して、X.509 証明書と秘密キーを生成します。

例：

```
$ openssl req -new -newkey rsa:1024 -days 36500 -nodes -x509 -keyout userabc.key -out userabc.crt
-subj '/CN=User ABC/O=Cisco Systems/C=US'
```

（注）
- X.509 証明書が生成されると、APIC のユーザプロファイルに追加され、署名の確認に使用されます。秘密キーは、署名を生成するためにクライアントによって使用されます。
- 証明書には公開キーは含まれていますが、秘密キーは含まれていません。公開キーは、計算された署名を確認するために APIC によって使用される主要な情報です。秘密キーが APIC に保存されることはありません。このキーを秘密にしておく必要があります。

ステップ 2 OpenSSL を使用して証明書のフィールドを表示します。

例：

```
$ openssl x509 -text -in userabc.crt
        Certificate:
            Data:
                Version: 3 (0x2)
                Serial Number:
                    c4:27:6c:4d:69:7c:d2:b6
                Signature Algorithm: sha1WithRSAEncryption
                Issuer: CN=User ABC, O=Cisco Systems, C=US
                Validity
                    Not Before: Jan 12 16:36:14 2015 GMT
                    Not After : Dec 19 16:36:14 2114 GMT
                Subject: CN=User ABC, O=Cisco Systems, C=US
                Subject Public Key Info:
                    Public Key Algorithm: rsaEncryption
                    RSA Public Key: (1024 bit)
                        Modulus (1024 bit):
                            00:92:35:12:cd:2b:78:ef:9d:ca:0e:11:77:77:3a:
                            99:d3:25:42:94:b5:3e:8a:32:55:ce:e9:21:2a:ff:
                            e0:e4:22:58:6d:40:98:b1:0d:42:21:db:cd:44:26:
                            50:77:e5:fa:b6:10:57:d1:ec:95:e9:86:d7:3c:99:
                            ce:c4:7f:61:1d:3c:9e:ae:d8:88:be:80:a0:4a:90:
                            d2:22:e9:1b:25:27:cd:7d:f3:a5:8f:cf:16:a8:e1:
                            3a:3f:68:0b:9c:7c:cb:70:b9:c7:3f:e8:db:85:d8:
                            98:f6:e3:70:4e:47:e2:59:03:49:01:83:8e:50:4a:
                            5f:bc:35:d2:b1:07:be:ec:e1
                        Exponent: 65537 (0x10001)
                X509v3 extensions:
                    X509v3 Subject Key Identifier:
                        0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34
                    X509v3 Authority Key Identifier:
                        keyid:0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34
                        DirName:/CN=User ABC/O=Cisco Systems/C=US
                        serial:C4:27:6C:4D:69:7C:D2:B6

                    X509v3 Basic Constraints:
                        CA:TRUE
            Signature Algorithm: sha1WithRSAEncryption
                8f:c4:9f:84:06:30:59:0c:d2:8a:09:96:a2:69:3d:cf:ef:79:
                91:ea:cd:ae:80:16:df:16:31:3b:69:89:f7:5a:24:1f:fd:9f:
```

```
                d1:d9:b2:02:41:01:b9:e9:8d:da:a8:4c:1e:e5:9b:3e:1d:65:
                84:ff:e8:ad:55:3e:90:a0:a2:fb:3e:3e:ef:c2:11:3d:1b:e6:
                f4:5e:d2:92:e8:24:61:43:59:ec:ea:d2:bb:c9:9a:7a:04:91:
                8e:91:bb:9d:33:d4:28:b5:13:ce:dc:fe:c3:e5:33:97:5d:37:
                cc:5f:ad:af:5a:aa:f4:a3:a8:50:66:7d:f4:fb:78:72:9d:56:
                91:2c
        [snip]
```

REST API を使用したローカル ユーザの作成とユーザ証明書の追加

ローカル ユーザを作成し、ユーザ証明書を追加します。

例：

```
method: POST
        url: http://apic/api/node/mo/uni/userext/user-userabc.json
        payload:
        {
            "aaaUser": {
                "attributes": {
                    "name": "userabc",
                    "firstName": "Adam",
                    "lastName": "BC",
                    "phone": "408-525-4766",
                    "email": "userabc@cisco.com",
                },
                "children": [{
                    "aaaUserCert": {
                        "attributes": {
                            "name": "userabc.crt",
                          "data": "-----BEGIN CERTIFICATE-----\nMIICjjCCAfegAwIBAgIJAMQnbE <snipped
 content> ==\n-----END CERTIFICATE-----",
                        },
                        "children": []
                    },
                    "aaaUserDomain": {
                        "attributes": {
                            "name": "all",
                        },
                        "children": [{
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "aaa",
                                    "privType": "writePriv",
                                },
                                "children": []
                            }
                        }, {
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "access-admin",
                                    "privType": "writePriv",
                                },
                                "children": []
                            }
                        }, {
                            "aaaUserRole": {
                                "attributes": {
                                    "name": "admin",
```

```
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "fabric-admin",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "nw-svc-admin",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "ops",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "read-all",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "tenant-admin",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "tenant-ext-admin",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }, {
                "aaaUserRole": {
                    "attributes": {
                        "name": "vmm-admin",
                        "privType": "writePriv",
                    },
                    "children": []
                }
            }]
        }
    }]
}
```

```
        }
```

Python SDK を使用したローカル ユーザの作成

ローカル ユーザを作成します。

例：

```
#!/usr/bin/env python
from cobra.model.pol import Uni as PolUni
from cobra.model.aaa import UserEp as AaaUserEp
from cobra.model.aaa import User as AaaUser
from cobra.model.aaa import UserCert as AaaUserCert
from cobra.model.aaa import UserDomain as AaaUserDomain
from cobra.model.aaa import UserRole as AaaUserRole
from cobra.mit.access import MoDirectory
from cobra.mit.session import LoginSession
from cobra.internal.codec.jsoncodec import toJSONStr

APIC = 'http://10.10.10.1'
username = 'admin'
password = 'p@$$w0rd'

session = LoginSession(APIC, username, password)
modir = MoDirectory(session)
modir.login()

def readFile(fileName=None, mode="r"):
   if fileName is None:
      return ""
   fileData = ""
   with open(fileName, mode) as aFile:
      fileData = aFile.read()
   return fileData

# Use a dictionary to define the domain and a list of tuples to define
# our aaaUserRoles (roleName, privType)
# This can further be abstracted by doing a query to get the valid
# roles, that is what the GUI does

userRoles = {'all': [
               ('aaa', 'writePriv'),
               ('access-admin', 'writePriv'),
               ('admin', 'writePriv'),
               ('fabric-admin', 'writePriv'),
               ('nw-svc-admin', 'writePriv'),
               ('ops', 'writePriv'),
               ('read-all', 'writePriv'),
               ('tenant-admin', 'writePriv'),
               ('tenant-ext-admin', 'writePriv'),
               ('vmm-admin', 'writePriv'),
           ],
}

uni = PolUni('') # '' is the Dn string for topRoot
aaaUserEp = AaaUserEp(uni)
aaaUser = AaaUser(aaaUserEp, 'userabc', firstName='Adam',
```

```
                    email='userabc@cisco.com')

aaaUser.lastName = 'BC'
aaaUser.phone = '555-111-2222'
aaaUserCert = AaaUserCert(aaaUser, 'userabc.crt')
aaaUserCert.data = readFile("/tmp/userabc.crt")
# Now add each aaaUserRole to the aaaUserDomains which are added to the
# aaaUserCert
for domain,roles in userRoles.items():
   aaaUserDomain = AaaUserDomain(aaaUser, domain)
   for roleName, privType in roles:
       aaaUserRole = AaaUserRole(aaaUserDomain, roleName,
                                 privType=privType)
print toJSONStr(aaaUser, prettyPrint=True)

cr = ConfigRequest()
cr.addMo(aaaUser)
modir.commit(cr)
# End of Script to create a user
```

秘密キーを使用した署名の計算

始める前に

次の情報が用意されている必要があります。

- HTTP メソッド：GET、POST、DELETE
- 要求される REST API URI（クエリ オプションを含む）
- POST 要求の場合、APIC に送信される実際のペイロード
- ユーザの X.509 証明書の生成に使用される秘密キー
- APIC のユーザ X.509 証明書の宛先名

ステップ 1 HTTP メソッド、REST API URI、およびペイロードをこの順序で連結し、ファイルに保存します。

OpenSSL で署名を計算するには、この連結データをファイルに保存する必要があります。この例では、ファイル名 payload.txt を使用します。秘密キーは userabc.key というファイルにあることに注意してください。

例：

GET の例：

```
GET http://10.10.10.1/api/class/fvTenant.json?rsp-subtree=children
```

POST の例：

```
POST http://10.10.10.1/api/mo/tn-test.json{"fvTenant": {"attributes": {"status": "deleted", "name":
 "test"}}}
```

ステップ 2 payload.txt ファイルに正しい情報が含まれていることを確認します。

たとえば、前の手順で示したような取得例を使用します。

```
GET http://10.10.10.1/api/class/fvTenant.json?rsp-subtree=children
```

payload.txt ファイルには、次の情報のみ含める必要があります。

```
GET/api/class/fvTenant.json?rsp-subtree=children
```

ステップ 3 payload ファイルを作成するときに新しい行を間違って作成していないことを確認します。

例：

```
# cat -e payload.txt
```

次と同じように出力の最後に **$** 記号があるか確認します。

```
GET/api/class/fvTenant.json?rsp=subtree=children$
```

ある場合、Payload.ファイルを作成したときに新しい行が作成されたことを意味します。payload ファイルの生成時に新しい行が作成されることを防ぐには、次のようなコマンドを使用します。

```
echo -n "GET/api/class/fvTenant.json?rsp-subtree=children" >payload.txt
```

ステップ 4 OpenSSL を使用して、秘密キーとペイロード ファイルを使用して署名を計算します。

例：

```
openssl dgst -sha256 -sign userabc.key payload.txt > payload_sig.bin
```

生成されたファイルには、複数行に印字された署名があります。

ステップ 5 base64 形式に署名を変換します。

例：

```
openssl base64 -A -in payload_sig.bin -out payload_sig.base64
```

ステップ 6 Bash を使用して、署名から改行文字を取り除きます。

例：

```
$ tr -d '\n' < payload_sig.base64
P+OTqK0CeAZjl7+Gute2R1Ww8OGgtzE0wsLlx8fIXXl4V79Zl7
Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f7q
IcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=
```

（注） これは、この特定の要求に関して APIC に送信される署名です。その他の要求では、独自の署名を計算する必要があります。

ステップ 7 署名を文字列内に配置し、APIC が署名をペイロードと照合して確認できるようにします。

この完全な署名が、要求のヘッダー内のクッキーとして APIC に送信されます。

例：

```
APIC-Request-Signature=P+OTqK0CeAZjl7+Gute2R1Ww8OGgtzE0wsLlx8f
IXXl4V79Zl7Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f
7qIcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=;
APIC-Certificate-Algorithm=v1.0; APIC-Certificate-Fingerprint=fingerprint;
APIC-Certificate-DN=uni/userext/user-userabc/usercert-userabc.crt
```

（注） ここで使用される DN が、次のステップの x509 証明書を含むユーザ認定オブジェクトの DN に一致する必要があります。

ステップ 8 署名を使用して APIC と通信するには、Python SDK の CertSession クラスを使用します。

次のスクリプトは、ACI Python SDK の CertSession クラスを使用して、署名を使用して APIC に要求する方法の例です。

例：

```
#!/usr/bin/env python
# It is assumed the user has the X.509 certificate already added to
# their local user configuration on the APIC
from cobra.mit.session import CertSession
from cobra.mit.access import MoDirectory

def readFile(fileName=None, mode="r"):
    if fileName is None:
        return ""
    fileData = ""
    with open(fileName, mode) as aFile:
        fileData = aFile.read()
    return fileData

pkey = readFile("/tmp/userabc.key")
csession = CertSession("https://ApicIPOrHostname/",
                       "uni/userext/user-userabc/usercert-userabc", pkey)

modir = MoDirectory(csession)
resp = modir.lookupByDn('uni/fabric')
pring resp.dn
# End of script
```

（注） 前のステップで使用した DN が、このステップの x509 証明書を含むユーザ認定オブジェクトの DN に一致する必要があります。

GUI を使用してログイン試行の連続失敗後のユーザー ロックアウトを設定する

ユーザーが設定された回数のログイン試行に失敗した後、そのユーザーをログインできないようにすることができます。特定の期間内にユーザーが何回ログインに失敗可能かを指定できます。ユーザーが何度もログインに失敗すると、そのユーザーは指定された期間ログインできなくなります。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

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

ステップ 3 [**作業（Work）**] ペインで、[**セキュリティのデフォルト設定（Security Default Settings）**] タブが表示されていることを確認します。

ステップ 4 [鉛筆（pencil）] アイコンをクリックして、次のフィールドを編集します。

a) **ログインに複数回失敗した後でユーザーをロックアウトする**には、**[有効化（Enable）]** を選択します。

b) **[ユーザーがロックアウトされるまでの試行失敗回数（Number of failed attempts before user is locked out）]** に、目的の値を入力します。

有効な範囲は 1 ～ 15 です。デフォルトは 5 分です。

c) **[連続して試行が失敗した期間 (m)（Time period in which consecutive attempts were failed (m)）]** に、Cisco Application Policy Infrastructure Controller（APIC）が失敗した試行をカウントする時間間隔の値を分単位で入力します。

範囲は 1 ～ 720 時間です。デフォルトは 5 分です。

d) **[ロックアウトの持続時間 (m)（Duration of lockout (m)）]** には、ユーザーが何度もログインに失敗したことを理由ににロックアウトされる時間を分単位で入力します。

ステップ 5 [送信（Submit）] をクリックします。

OTP ベース認証向けローカルユーザーの設定

次の手順では、Cisco APIC GUI を使用してローカル ユーザーの OTP ベースの 2 要素認証を構成します。この手順では、ファブリック管理者を想定しています。

始める前に

OTP ベースの 2 要素認証を有効にするローカル ユーザーをすでに作成している必要があります。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで **[ユーザー（Users）]** を選択します。

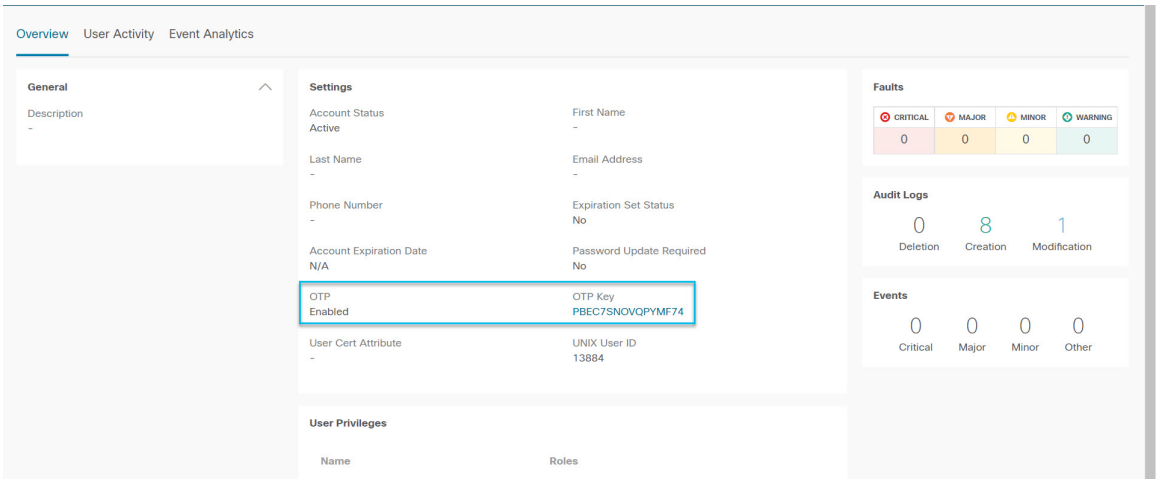
ステップ 3 **作業**ペインで、OTP ベース二要素認証を有効にするユーザーをクリックします。

ユーザーに関する詳細が記載されたウィンドウが右側に表示されます。詳細（  ）アイコンをクリックし、表示される新しい画面（ユーザの詳細を含む）で、[編集（Edit）] アイコンをクリックします。

ステップ 4 下にスクロールし、[詳細設定（Advanced Settings）] で、OTP の **[有効（Enable）]** ボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

OTP の詳細を取得するには、**[ユーザ（User）]** > **[ローカル（Local）]** タブで、*User_name* > [詳細（Details）] アイコンをクリックして、ユーザの詳細画面を表示します。表示された OTP キーをクリックすると、QR コードが表示されます。ユーザ詳細画面は以下のとおりです。



次のタスク

OTP を有効にしたユーザーは、OTP 認証の構成を完了する必要があります。「GUI を使用してユーザーによる OTP ベース 2 要素認証の設定を完了する （42 ページ）」を参照してください。

GUI を使用してユーザーによる OTP ベース 2 要素認証の設定を完了する

次の手順では、Cisco APIC GUI を使用した OTP ベースの 2 要素認証の設定を完了します。この手順は、ファブリック管理者が OTP ベースの 2 要素認証を有効にしたユーザーであることを前提としています。

始める前に

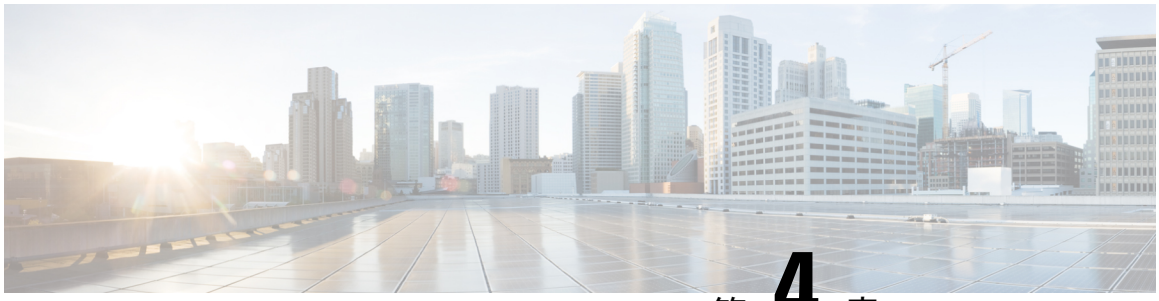
ファブリック管理者は、アカウントに対して OTP ベースの 2 要素認証を有効にしている必要があります。

ステップ 1 Android または Apple iOS スマートフォンで、適切な 2 要素認証アプリをダウンロードします。

ステップ 2 ファブリック管理者から、または Cisco APIC GUI にログインして、QR コードまたは OTP キーを取得します。

GUI にログインすると、資格情報を入力すると、QR コードと OTP キーが表示されます。

ステップ 3 スマートフォンを使用して QR コードをスキャンし、2 要素認証アプリの指示に従うか、Cisco APIC GUI で OTP キーを入力します。



第 4 章

セキュリティ ドメインとノード ルールを使用したアクセスの制限

ドメイン別にアクセスを制限する

制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、両方のグループのユーザーに同じ特権が割り当てられている場合、あるユーザー グループがテナント B などの別のセキュリティ ドメインのユーザー グループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、テナント A の制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで設定されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティ ドメインも制限されていない限り、テナント B は、テナント A で設定されたポリシー、プロファイル、またはユーザーを表示できます。ユーザーが適切な権限を持つシステム作成の設定に対して、ユーザーは常に読み取り専用で閲覧可能であることに注意してください。制限付きセキュリティドメインのユーザーには、そのドメイン内で幅広いレベルの特権を与えることができます。ユーザーが別のテナントの物理環境に不注意で影響を与える心配はありません。

ノードをドメインに割り当てる

ファブリック管理者は、RBAC ノード ルールを使用して、リーフ スイッチなどの物理ノードをセキュリティ ドメインに割り当てることができます。このノード割り当てにより、そのセキュリティ ドメイン内のユーザーは、ノード ルールの一部として割り当てられたノードにアクセスして操作を実行できます。セキュリティドメイン内のノード管理権限を持つユーザーの

みが、そのドメインに割り当てられたノードを設定できます。ユーザーは、セキュリティ ドメインの外部のノードにアクセスできず、他のセキュリティ ドメインのユーザーは、セキュリティ ドメインに割り当てられたノードにアクセスできません。セキュリティ ドメインに割り当てられたノードで構成を作成または変更するには、そのドメインのユーザもドメイン `all` に割り当てられていて、`port-mgmt` ロール（デフォルトで `custom-port-privilege` 権限を含むロール）か、または `custom-port-privilege` 権限を含むカスタム ロールを持っている必要があります。

（注） 割り当てられたノードのポートを管理するローカル ユーザを構成するときは、ドメイン `all` のユーザにロールを付与し、ノードが割り当てられているセキュリティ ドメインには `admin` ロールを付与する必要があります。どちらの役割も、**[ロール権限タイプ（Role Privilege Type）]** が `[書き込み（Write）]` として設定されている必要があります。

セキュリティ ドメインおよびノード ルールのガイドラインと制限事項

セキュリティドメインとノードルールを構成する際は、次の注意事項と制限事項に従ってください。このセクションで、「制限付きノードユーザー」とは、ノードが割り当てられている制限付きセキュリティ ドメイン内のユーザーのことです。

- Cisco Application Policy Infrastructure Controller（APIC）より前のリリースから 5.0 リリースにアップグレードする場合は、より詳細な以前の権限を使用するルール、ポリシー、ロールを再構成する必要があります。
- Cisco APIC 5.0 リリースからそれより前のリリースにダウングレードする場合は、デフォルトのロールを手動で編集して保持する必要があります。Cisco APIC 5.0 リリースで変更されたロールは保持されます。
- RBAC ノード ルールを使用してスパイン スイッチを割り当てることはできません。
- RBAC ノードルールを作成するときは、ノードを複数のセキュリティドメインに割り当てないでください。
- 制限付きノードユーザーは、ポリシーのみを構成できます。管理者ユーザーは、ノードの構成とトラブルシューティングを実行する必要があります。
- 制限付きノードユーザは、デフォルトのシステム作成の管理対象オブジェクトにアクセスできます。
- 制限付きノードユーザーは、障害ダッシュボードでファブリックレベルの障害数を表示できます。
- 制限付きノードユーザーは、AAA サーバー、NTP サーバー、DNS サーバーなどからのノードレベルの障害を表示できます。

- 管理者または非制限ドメインユーザーが関係ポリシーを制限ノードユーザーによって作成されたアクセス ポリシーに関連付ける場合、そのポリシーは制限ノード ユーザーに表示されます。
- CLI を使用して制限付きノード ユーザを構成することはできません。
- デフォルトでは、`port-mgmt` ロールには、事前定義されたアクセスポリシー管理オブジェクトを含む `custom-port-privilege` 権限があります。カスタム権限を設定する （47 ページ）の手順を使用して、さらに管理対象オブジェクトを追加できます。

セキュリティ ドメインの作成

この手順を使用して、セキュリティ ドメインを作成します。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[作業（Work）]** ペインで、**[セキュリティ ドメイン（Security Domains）]** タブ > **[アクション（Actions）]** > **[セキュリティ ドメインの作成（Create Security Domain）]** を選択します。

ステップ 4 **[セキュリティ ドメインの作成（Create Security Domain）]**ダイアログボックスで、次の操作を実行します。

a) **[名前（Name）]** フィールドで、セキュリティ ドメインの名前を入力します。

b) [**説明（Description）**] を入力します。

c) セキュリティドメインを**制限付き RBAC ドメイン**として設定するには、[有効（Enabled）] チェックボックスをオンにします。

セキュリティドメインが制限付きドメインとして構成されている場合、このドメインに割り当てられているユーザーは、他のセキュリティドメインで構成されたポリシー、プロファイル、ユーザーを表示できません。

d) [保存（Save）] をクリックします。

ノードにアクセス権を割り当てるノードルールを作成する

この手順を使用して、リーフ スイッチなどの物理ノードをセキュリティ ドメインに割り当てる RBAC ノード ルールを設定します。

始める前に

ノードが割り当てられるセキュリティ ドメインを作成します。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[作業（Work）]** ペインで、**[RBAC ルール（RBAC Rules）]** タブ > **[ノード ルール（Node Rules）]** サブタブ > **[アクション（Actions）]** > **[RBAC ノード ルールの作成（Create RBAC Node Rule）]** を選択します。

画面が表示されます。

ステップ 4 表示される **[ノードの RBAC ルールの作成（Create RBAC Rule for Node）]** 画面で、次の詳細を入力します。

a) [**ノード ID の選択（Select Node ID**）] をクリックして、ドロップダウンリストからノードを選択します。

b) **[ポートの RBAC ルール（RBAC Rule for Port ）]** を割り当てるには、**[ポートの RBAC ルールの追加（Add RBAC Rule for Port）]** をクリックして名前を入力し、**[ドメインの選択（Select Domain）]** をクリックしてドメインをルールに関連付けます。ドメインを選択したら、チェックマークをクリックします。

[ポートの RBAC ルールの追加（Add RBAC Rule for Port）] をクリックして、選択したポートに複数の RBAC ルールを割り当てることができます。

c) **[保存（Save）]** をクリックします。

次のタスク

セキュリティドメインに割り当てられたノードを管理するユーザーを割り当てます。

カスタムの役割と権限

カスタム権限を持つカスタム ロールの作成

この手順を使用して、ロールを作成し、一連の権限を選択します。

始める前に

カスタム ロールで使用できる権限を判断するには、AAA RBAC の役割および権限 （11 ページ）にリストされている事前定義されたロールと権限のセットを参照してください。事前定義された特権で公開されていない管理対象オブジェクト（MO）への読み取りまたは書き込みアクセスが必要な場合は、カスタム権限を設定する （47 ページ） で説明されているように、カスタム権限を設定できます。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[作業 (Work)]** ペインで、**[ロール（Roles）]** を選択します。

ステップ 4 **[作業 (Work)]** ペインで、[アクション（Actions）] アイコン ドロップダウン リストをクリックし、**[ロールの作成（Create Role）]** を選択します。

ステップ 5 [**ロールの作成（Create Role**）] 画面で、次の操作を実行します。

a) **[名前（Name）]** フィールドに、ロールの名前を入力します。

b) [**説明（Description**）] フィールドに、説明を入力します。

c) [**権限の追加（Add Privileges**）] をクリックします。表示されている [**権限の選択（Select Privileges**）] ウィンドウで、必要なチェックボックスを選択して、ロールに対する 1 つまたは複数の権限を選択します。

d) [権限の選択（Select Privileges）] ウィンドウで、[**選択（Select**）] をクリックします。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

`custom-privilege-1` などのカスタム権限を選択した場合は、カスタム権限を設定する （47 ページ） の手順に従って、このカスタム権限で公開される管理対象オブジェクト (MO) を選択します。

カスタム権限を設定する

この手順を使用してカスタム権限を設定し、事前定義された権限で公開されていない 1 つ以上の管理対象オブジェクト（MO）への読み取りまたは読み取り/書き込みアクセス権を提供します。

管理対象オブジェクト クラスについては、『Cisco APIC 管理情報モデル リファレンス』で説明されています。MO クラスごとに、そのクラスの読み取りまたは読み取り/書き込み権限を持つ事前定義されたロールがリファレンスに記載されています。

事前定義された権限ごとに、Cisco APIC のロールと権限のマトリクスを使用して、MO クラスのリストと読み取り/書き込み権限を表示できます。

MO クラスへの読み取りまたは書き込みアクセス権限を持つカスタム権限を設定するには、APIC REST API を使用する必要があります。API を使用する場合は、『*Cisco APIC REST API* 設定ガイド』を参照してください。

以下の形式で APIC REST API POST を作成して送信し、クラス `aaa:RbacClassPriv` のオブジェクトを作成します。

例：

```
POST https://<APIC-IP>/api/node/mo/uni/rbacdb/rbacclpriv-<moClassName>.json

{
    "aaaRbacClassPriv":
    {
        "attributes":
```

```
        {
            "name": "<moClasssName>",
            "wPriv": "<privilege>",
            "rPriv": "<privilege>"
        }
    }
}
```

URI の *moClassName* 値に、アクセスを設定するオブジェクト クラスの名前を含めます。

ペイロードで、次の属性を指定します。

- `name`：アクセスを設定するオブジェクト クラスの名前。
- `wPriv`：クラスのオブジェクトへの書き込みアクセスを含むカスタム権限の名前。
- `rPriv`：クラスのオブジェクトへの読み取りアクセスを含むカスタム権限の名前。

カスタム権限に読み取りおよび書き込みアクセスを割り当てるには、`wPriv` と `rPriv` の両方にカスタム権限の名前を入力します。

例

この例は、クラス `fabric:Pod` のオブジェクトへの読み取りアクセスと書き込みアクセスの両方を使用して、カスタム権限 `custom-privilege-1` を設定する方法を示しています。

```
POST https://apic-aci.cisco.com/api/node/mo/uni/rbacdb/rbacclpriv-fabricPod.json

{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "fabricPod",
            "wPriv": "custom-privilege-1",
            "rPriv": "custom-privilege-1"
        }
    }
}
```

次のタスク

カスタム権限を持つカスタム ロールの作成 （46 ページ） で説明されている手順を使用して、カスタム権限をカスタム ロールに追加します。

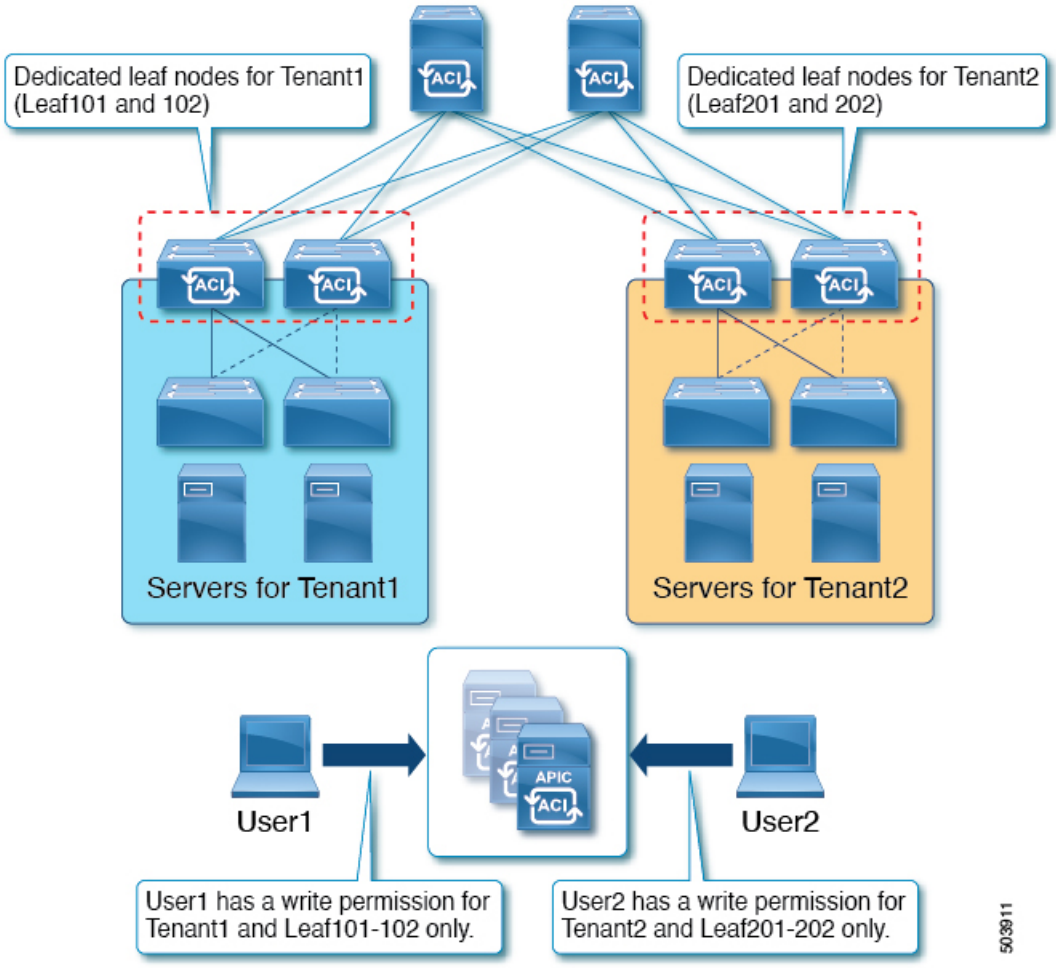
RBAC ノード ルールの設定の使用例

このセクションでは、このドキュメントで説明されている構成オプションが混在するユースケースについて説明します。各オプションの詳細については、このドキュメントの他の部分を参照してください。ユースケースは、次のシナリオに基づいています。

Cisco Application Centric Infrastructure (ACI) ファブリックに複数のテナントと複数のリーフノードがあるとします。マルチテナンシーの場合、ユーザーが特定のテナントと特定のリーフノードのセットのみを管理できるようにする必要があります。次に例を示します。

- User1 は Tenant1、リーフノード 101 と 102 のみを管理できます。
- User2 は Tenant2、リーフノード 201 および 202 のみを管理できます。

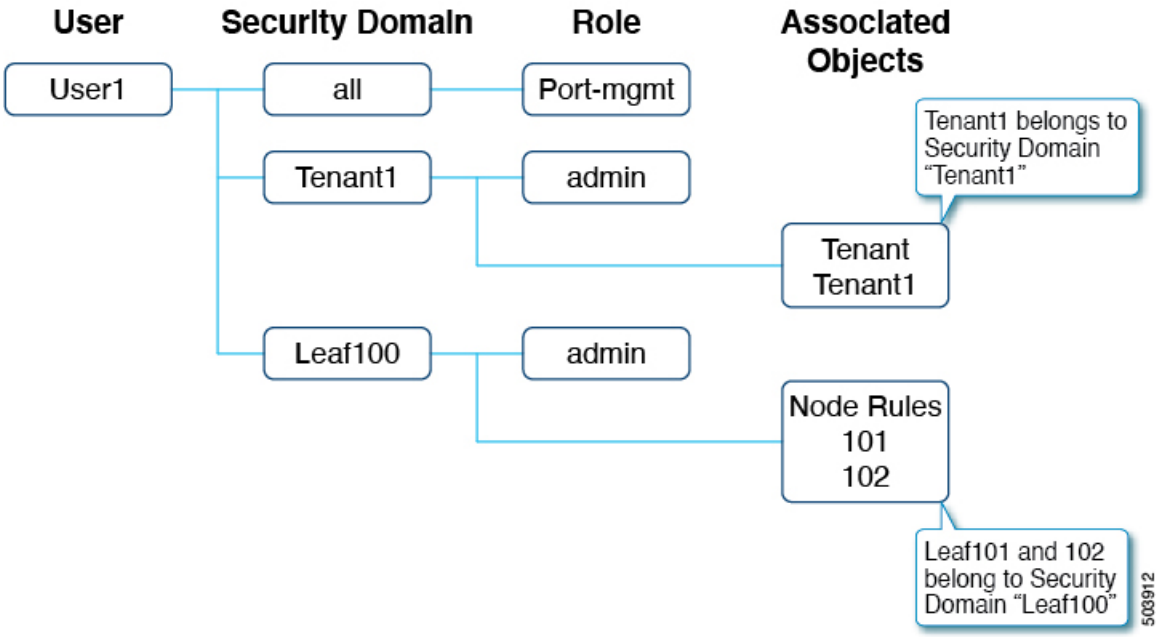
次の図では要件を説明しています。



これは、セキュリティドメインと RBAC ノードルールを使用して実現できます。高レベルでは、構成手順は次の通りです。

1. セキュリティドメインの作成
2. RBAC ノードルールの作成
3. ユーザーの作成

次の図は、この例の User1 の構成間の関係を示しています。



User1 には 3 つのセキュリティドメインがあります。

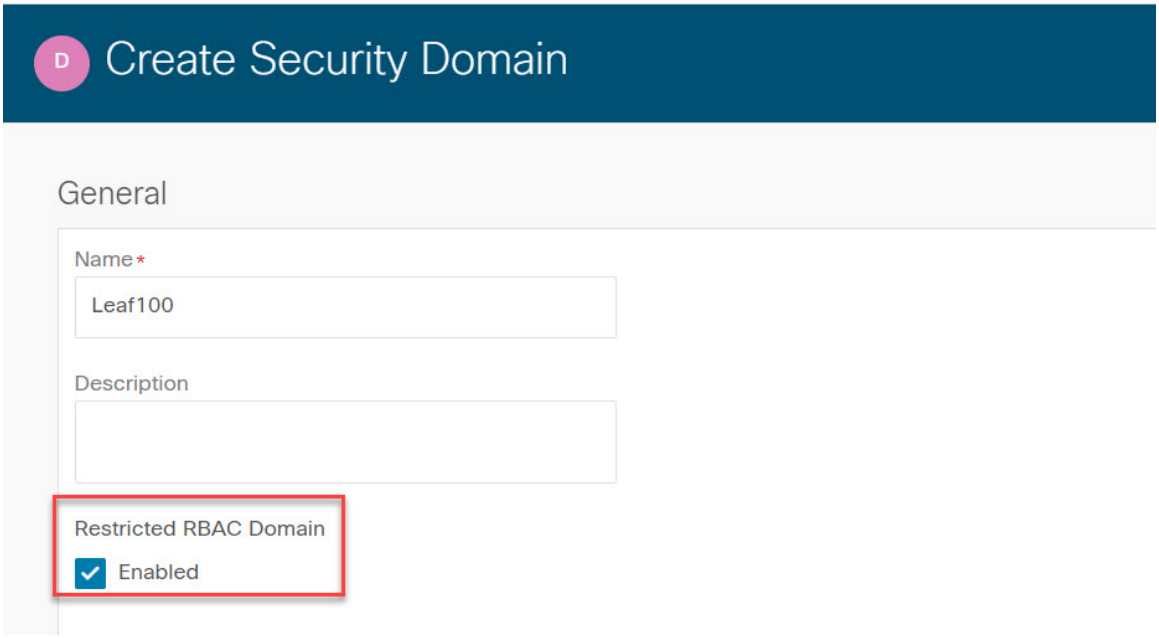
- すべての `port-mgmt` ロール：User1 が割り当てられたリーフノードでポート関連の構成を管理できるようにします。デフォルトでは、`port-mgmt` ロールには `custom-port-privilege` 権限があります。`custom-port-privilege` 権限を含むお客様ロールを使用することもできます。
- `admin` ロールを持つ Tenant1：User1 が Tenant1 を管理できるようにします。
- `admin` ロールを持つ Leaf100：User1 が Leaf101 と 102 を管理できるようにします。

以降の項では、より詳細に構成手順について説明します。

手順 1：セキュリティドメインの作成

最初の手順は、セキュリティドメイン Tenant1 と Leaf100 を作成することです。これらのセキュリティドメインを組み合わせることができますが、この例では個別のセキュリティドメインを使用しています。

ドメインを作成するには、GUI で **[管理（Admin）]>>[AAA]>>[セキュリティ（Security）]>>[セキュリティドメイン（Security Domains）]>>[アクション（Actions）]>>[セキュリティ ドメインの作成（Create Security Domain）]**に移動します。

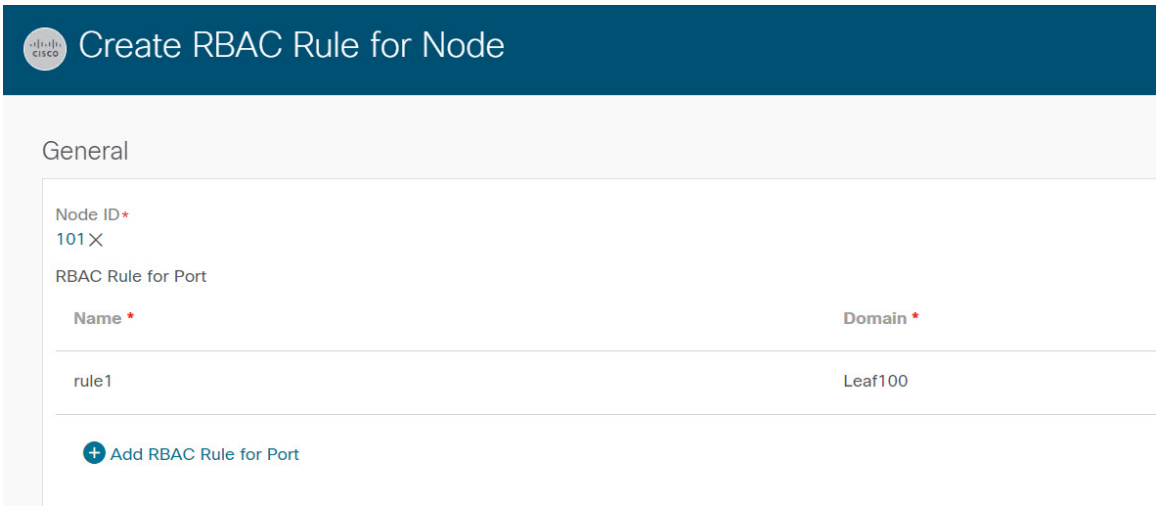


この例では、セキュリティドメイン Leaf100 の **[制限付き RBAC ドメイン（Restricted RBAC Domain）]** が有効になっています。そのため、User1 はインターフェイス ポリシー グループ、VLAN プール、および異なるセキュリティ ドメインの他のユーザによって作成された他のアクセスポリシーを表示できません。例外は、デフォルトのインターフェイスポリシーです。**[制限付き RBAC ドメイン（Restricted RBAC Domain）]** の構成に関係なく、デフォルトのインターフェイス ポリシーはリーフ RBAC ユーザに表示されます。つまり、**[制限付き RBAC ドメイン（Restricted RBAC Domain）]** が有効になっている場合、ユーザはデフォルト ポリシーの構成を変更できません。

テナント RBAC の場合、テナントはセキュリティドメインに関連付けられている必要があります。この例では、Tenant1 をセキュリティドメイン「Tenant1」に関連付けます。ドメインを作成するには、GUI で **[テナント（Tenant）]** > **[ポリシー（Policy）]** > **[セキュリティドメイン（Security Domains）]** に移動します。

手順 2: RBAC ノードルールを作成する

次の手順では、RBAC ノードルールを作成して、Leaf101 と Leaf102 をセキュリティドメイン Leaf100 に追加します。RBAC ノード ルールを作成するには、GUI で **[管理（Admin）]**> > **[AAA]**> > > **[セキュリティ（Security）]**> > **[RBAC ルール（RBAC Rules）]**> > **[ノード ルール（Node Rules）]**> > **[アクション（Actions）]**> > **[RBAC ノード ルールの作成（Create RBAC Node Rule）]**に移動します。



手順 3：ユーザーを作成する

最後の手順は、ユーザー User1 を作成することです。ユーザを作成するには、GUI で **[管理（Admin）]>>[AAA]>>[ユーザ（Users）]>>[アクション（Actions）]>>[ローカル ユーザの作成（Create Local User）]** に移動します。

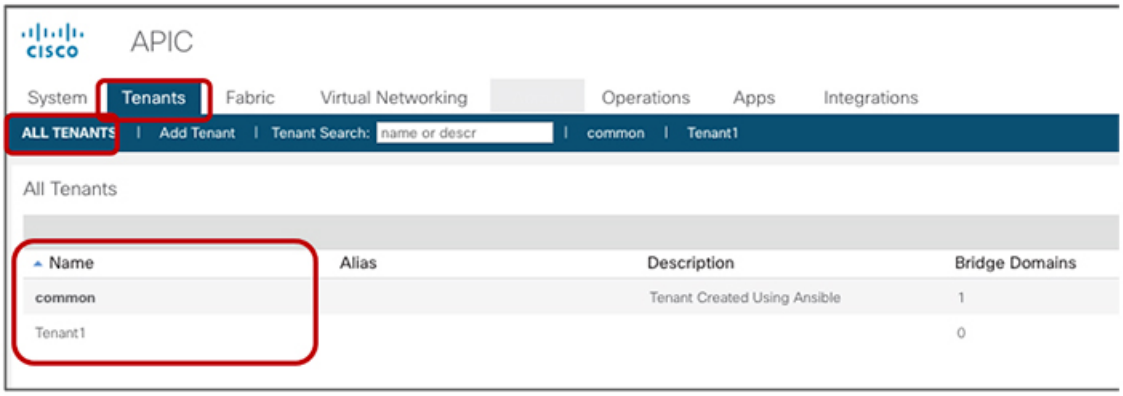
セキュリティと**ロール**の構成手順で、次のセキュリティドメインとロールを選択します。

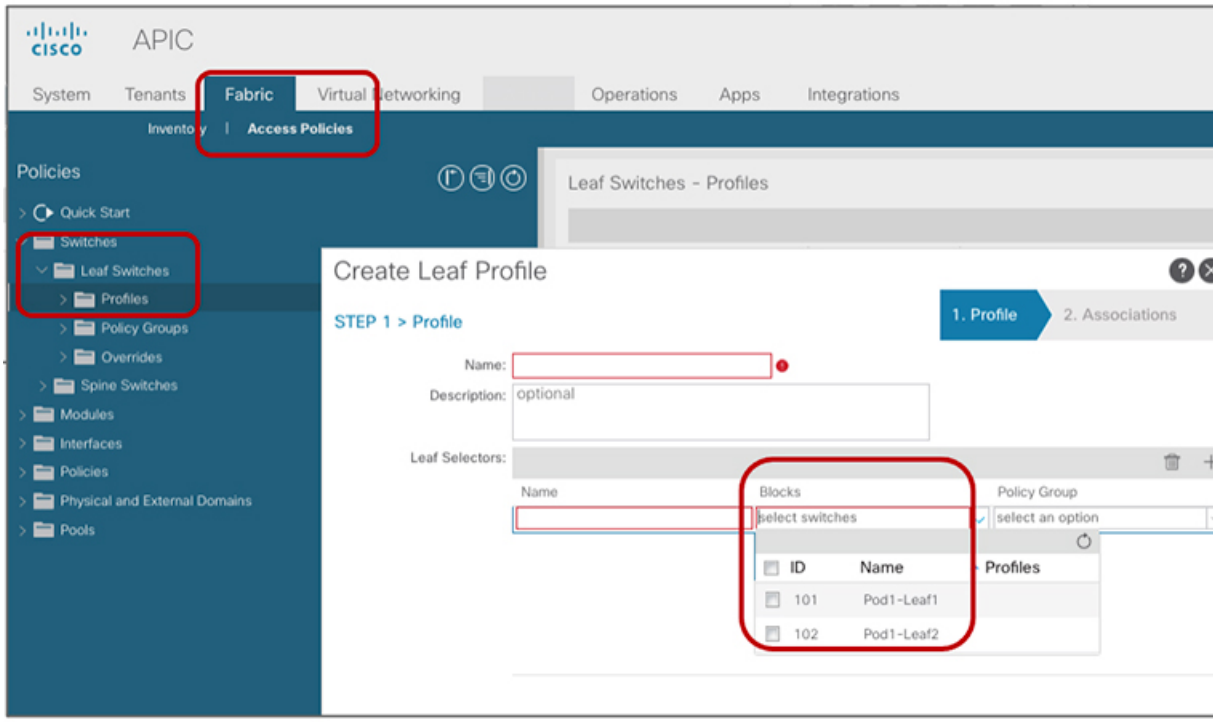
- all：書き込み権限を持つロール `port-mgmt`
- Leaf100：書き込み権限を持つロール `admin`
- Tenant1：書き込み権限を持つロール `admin`

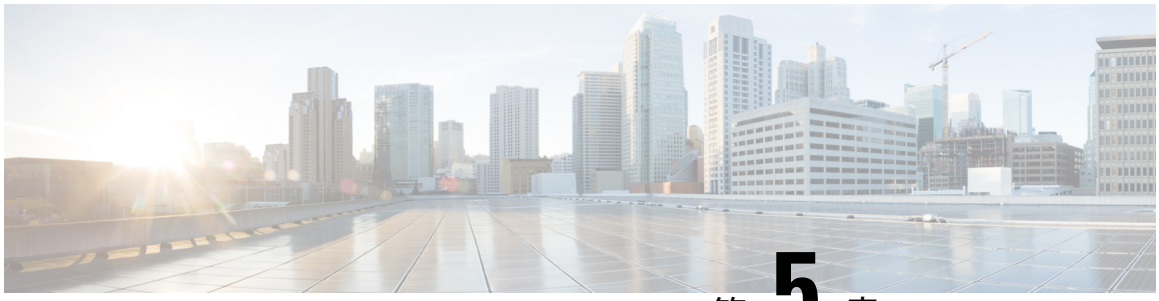
RBAC ノードルールの確認

User1 は Tenant1、Leaf 101 および 102 のみを管理できます。次に例を示します。

- User1 は、書き込み権限を持つ Tenant1 と読み出し権限を持つ共通テナント以外の他のテナントを参照することはできません。
- User1 は、**リーフセレクタ**で Leaf101 および 102 以外の他のリーフノードを表示できません。


APIC
System
Tenants
Fabric
Virtual Networking
Operations
Apps
Integrations
ALL TENANTS
Add Tenant
Tenant Search:
name or descr
common
Tenant1
All Tenants
Name
Alias
Description
Bridge Domains
common
Tenant Created Using Ansible
1
Tenant1
0


APIC
System
Tenants
Fabric
Virtual Networking
Operations
Apps
Integrations
Inventory
Access Policies
Policies
Quick Start
Switches
Leaf Switches
Profiles
Policy Groups
Overrides
Spine Switches
Modules
Interfaces
Policies
Physical and External Domains
Pools
Leaf Switches - Profiles
Create Leaf Profile
STEP 1 > Profile
1. Profile
2. Associations
Name:
Description:
optional
Leaf Selectors:
Name
Blocks
Policy Group
select switches
select an option
ID
Name
Profiles
101
Pod1-Leaf1
102
Pod1-Leaf2



第 5 章

RADIUS、TACACS+、LDAP、RSA、SAML、OAuth 2、DUO

この章は、次の項で構成されています。

概要

この記事では、RADIUS、TACACS+、LDAP、RSA、DUO、SAML、OAuth 2 ユーザーが APIC にアクセスできるようにする方法について、順を追って説明します。読者が *Cisco* プリケーション セントリック インフラストラクチャの基礎マニュアル、特にユーザー アクセス権、認証、アカウンティングの章を十分に利害していると仮定しています。

Cisco APIC リリース 6.0(1) から、**[管理（Admin）]** > **[AAA]** のパスの APIC GUI が変更されました。詳細については、Cisco APIC GUI の機能強化 （5 ページ）を参照してください。

（注） クラスタ内の 1 つを除くすべての APIC が失われるなどの障害シナリオの場合、APIC はリモート認証を無効にします。このシナリオでは、ローカル管理者アカウントのみがファブリック デバイスにログインできます。

（注） セキュリティ上の理由により、AAA 認証に shell:domains=all/read-all/ を使用するリモートユーザは、ファブリック内のリーフ スイッチおよびスパイン スイッチにアクセスすることはできません。このことは、4.0(1h) までのすべてのバージョンに当てはまります。

APIC Bash シェルのユーザ ID

APIC での Linux シェル用のユーザ ID は、ローカル ユーザ用に APIC 内で生成されます。認証クレデンシャルが外部サーバで管理されているユーザは、Linux シェル用のユーザ ID を cisco-av-pair で指定できます。上記の cisco-av-pair の（16001）を省略することは、リモートユーザがデフォルトの Linux ユーザ ID 23999 を取得すれば可能です。Linux ユーザ ID がバッシュ セッション中に使用され、標準の Linux 権限が適用されます。また、ユーザが作成するすべての管理対象オブジェクトは、そのユーザの Linux ユーザ ID によって作成されたとマークされます。

次に、APIC Bash シェルに表示されるユーザ ID の例を示します。

```
admin@ifav17-ifc1:~> touch myfile
admin@ifav17-ifc1:~> ls -l myfile
-rw-rw-r-- 1 admin admin 0 Apr 13 21:43 myfile
admin@ifav17-ifc1:~> ls -ln myfile
-rw-rw-r-- 1 15374 15374 0 Apr 13 21:43 myfile
admin@ifav17-ifc1:~> id
uid=15374(admin) gid=15374(admin) groups=15374(admin)
```

外部認証サーバの AV ペア

Cisco APIC では、管理者が外部認証サーバで Cisco AV ペアを設定する必要があります。Cisco AV ペアは、ユーザの RBAC ロールおよび権限に必要な APIC を指定します。Cisco AV ペアの形式は、RADIUS、LDAP、または TACACS+ のものと同じです。

外部認証サーバで Cisco AV ペアを設定するには、管理者が既存のユーザ レコードに Cisco AV ペアを追加します。Cisco AV ペアの形式は次のとおりです。

```
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(16003)
```

Cisco APIC リリース 2.1 より、AV ペアで UNIX ID が指定されていない場合は、APIC が固有の UNIX ユーザー ID を内部的に割り当てます。

（注） APIC の Cisco AV ペアの形式は互換性があり、他の Cisco AV ペアの形式と共存できます。APIC はすべての AV ペアから最初に一致した AV ペアを選択します。

リリース 3.1(x) 以降、AV Pair shell:domains=all//admin を使用すると、ユーザに読み取り専用権限を割り当て、スイッチにアクセスしてコマンドを実行できます。

APIC は、次の正規表現をサポートしています。

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

例：

- 例 1：writeRoles のみを持つ単一のセキュリティ ドメインを含む Cisco AV ペア：

```
shell:domains=domainA/writeRole1|writeRole2/
```

- 例 2：readRoles のみを持つ単一のセキュリティ ドメインを含む Cisco AV ペア：

```
shell:domains=domainA//readRole1|readRole2
```

（注） 「/」文字は、セキュリティ ドメインごとの writeRoles と readRoles の間の区切り文字であり、1 つのタイプのロールのみを使用する場合でも必要です。

Cisco AV ペアの文字列は、大文字と小文字が区別されます。エラーが表示されなくても、使用する大文字と小文字がドメイン名またはロールに一致していない場合は、予期しない権限が付与されることがあります。

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)"
```

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、

Cisco 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。

リモート認証サーバがその av ペアを cisco 応答 UNIX ID を明示的に指定していないことを確認するには、(リモート ユーザ アカウントを使用) は、管理者として、APIC とログインへの SSH セッションを開きます。ログインすると、次のコマンド (置換」ユーザ id「ログに記録するユーザ名と) を実行します。

```
admin@apic1:remoteuser-userid> cd /mit/uni/userext/remoteuser-userid
admin@apic1:remoteuser-userid> cat summary
```

Cisco AV ペアの文字列は、大文字と小文字が区別されます。エラーが表示されなくても、使用する大文字と小文字がドメイン名またはロールに一致していない場合は、予期しない権限が付与されることがあります。

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。

手順の概要

1. 外部認証サーバの AV ペアを設定します。

手順の詳細

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)
```

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。

（注） APIC が少数側である（クラスタから切断されている）場合、ACI は分散システムであり、ユーザ情報が APICS に分散されるため、リモート ログインは失敗する可能性があります。ただし、ローカル ログインは APIC に対してローカルであるため、この場合も機能します。

3.1 (1) のリリース以降、**サーバ モニタリング** は RADIUS、TACACS +、LDAP、および RSA を介して設定され、個別の AAA サーバがアクティブかを判断できます。サーバ モニタリング機能は、サーバがアクティブかどうか確認するためそれぞれのプロトコルのログインを使用します。たとえば、LDAP サーバは ldap 1ログインを使用し、Radius サーバはサーバがアクティブか判断するサーバ モニタリング機能を持つ radius のログインを使用します。

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 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。

Cisco AV ペアが欠落しているか不良であるリモート ユーザのデフォルトの動作の変更

ステップ 1 メニュー バーで、**[管理（Admin）] > [認証（Authentication）] > [AAA] > [ポリシー（Policy）]** タブを選択します。

ステップ 2 **[リモート ユーザー ログイン ポリシー（Remote user login policy）]** ドロップダウン リストから、**[デフォルト ロールの割り当て（Assign Default Role）]** を選択します。

デフォルト値は [No Login] です。[Assign Default Role] オプションは、Cisco AV ペアが欠落しているか不良であるユーザに最小限の読み取り専用権限を割り当てます。不正な AV ペアは、解析ルール適用時に問題があった AV ペアです。

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

Cisco APIC では、管理者が外部認証サーバで Cisco AV ペアを設定する必要があります。これを行うには、管理者は既存のユーザ レコードに Cisco AV ペアを追加します。Cisco AV ペアは、ユーザの RBAC ロールおよび権限に必要な APIC を指定します。Cisco AV ペアの形式は、RADIUS、LDAP、または TACACS+ のものと同じです。AV ペアの形式には Cisco UNIX ユーザ ID が含まれるものと含まれないものがあります。すべてのリモート ユーザが同じロールを持ち、相互ファイル アクセスが許可される場合はどちらの形式でも問題ありません。UNIX ユーザ ID を指定しないと、APIC システムによって ID 23999 が適用され、AV ペア ユーザに対して複数のロールまたは読み取り権限が指定されます。これは、グループ設定で設定された権限より高いかまたは低い権限がユーザに付与される原因になることがあります。このトピックでは、許可されない動作を変更する方法について説明します。

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。

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
```

プロバイダーを作成する

この手順に従って、認証/承認プロトコルのプロバイダーを作成します。

始める前に

認証/承認プロトコルのプロバイダーを作成する前の関連する前提条件については、関連するプロトコルのセクションで説明します。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。

ステップ 3 作業ペインで、[**プロバイダー（Providers**）] を選択します。

ステップ 4 [**アクション（Actions**）] > [**プロバイダーの作成（Create Provider**）] をクリックします。

ステップ 5 表示された **[プロバイダーの作成（Create Provider）]** 画面で、**[ホスト名/IP アドレス（Hostname/ IP Address）]**、**[説明（Description）]** を入力し、ドロップダウンリストから **[レルム（Realm）]** を選択します。**[レルム（Realm）]** で使用できるオプションは次のとおりです。

- RADIUS
- TACACS+
- LDAP
- SAML
- RSA
- OAuth 2

プロバイダーを構成するためのオプションは動的であり、選択した**レルム**に応じて変化します。各**レルム**で使用できるオプションについては、以降の手順で詳しく説明します。

ステップ 6 （任意） RADIUS にのみ適用可能：レルム サブタイプを選択します。**[レルム サブタイプ（Realm Subtype）]** を選択します。オプションは、**[デフォルト（Default）]** または **[デュオ（Duo）]** です。次に、以下を指定します。

- RADIUS サーバーのパスワード：確認のためにもう一度パスワードを入力してください。

- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイント グループを選択します。
- RADIUS のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 1812 です。
- 認証プロトコルのオプションは、**[PAP]**、**[CHAP]**、**[MS-CHAP]** です。このオプションは、**[デフォルト（Default）]** を **[レルム サブタイプ（Realm Subtype）]** として選択した場合にのみ、表示されます。
- RADIUS サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です（レルム サブタイプ：デフォルトの場合）。デフォルトは 30 秒です（レルム サブタイプ：Duo）。
- RADIUS エンドポイントに接続する際の再試行回数。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザ名とパスワードを入力します。

この手順は、RADIUS プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 7 （オプションの手順で TACACS+ にのみ適用）次を指定します。

- TACACS+ サーバーのパスワード：確認のためにもう一度パスワードを入力してください。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイントグループを選択します。
- TACACS+ のサービス ポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 49 です。
- 認証プロトコルのオプションは、PAP、CHAP、MS-CHAP です。
- TACACS+ サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- TACACS+ エンドポイントに接続する際の再試行回数。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

この手順は、TACACS+ プロバイダーの設定用です。これで、手順 12 に進むことができます。

ステップ 8 （オプションの手順でLDAPにのみ適用）レルム サブタイプを選択します。オプションは、**[デフォルト（Default）]** または **[デュオ（Duo）]** です。次に、以下を指定します。

- LDAP ディレクトリのルート識別名（DN）。
- LDAP ベース DN：APIC がリモートユーザーアカウントを検索する LDAP サーバー内のコンテナ名とパスです。これはパスワードが検証される場所です。フィルタを使用して、APIC が *Cisco AVPair* に使用するために要求している属性を見つけます。
- LDAP サーバーのパスワード。確認のためにもう一度パスワードを入力してください。
- LDAP のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 389 です。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイントグループを選択します。

- LDAP サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 30 秒です。
- LDAP エンドポイントに接続する際の再試行回数。
- **[有効（Enable）]** チェック ボックスをオンにして、SSL を有効にします。
- SSL 証明書の検証レベル。次のオプションがあります。
  - 許容（Permissive）：DUO LDAP SSL 証明書の問題の診断に役立つデバッグノブ。
  - 厳格（Strict）：実稼働環境で使用するレベル。
- LDAP 属性。
- 認証方式。次のオプションがあります。
  - LDAPバインド
  - パスワード比較
- フィルタ タイプフィルタは、検索要求のエントリの識別に使用される条件を定義する、主要なエレメントです。例：（cn=*）。これは、1 つ以上の *cn* 値を含むエントリを意味します。次のオプションがあります。
  - デフォルト
  - Microsoft Active Directory
  - カスタム（Custom）
- LDAP フィルタこのフィールドは、選択したフィルタ タイプに基づいて自動入力されます（カスタム オプションの [フィルタ タイプ（Filter Type）] を選択した場合を除く）。デフォルトを選択した場合、フィルタは `cn=Suserid` です。 Microsoft Active Directory を選択した場合、フィルタは `sAMAccountName=Suserid` です。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

この手順は、LDAP プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 9 （オプションの手順で RSA にのみ適用）次を指定します。

- RSA サーバーのパスワード：確認のためにもう一度パスワードを入力してください。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイントグループを選択します。
- RSA のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 1812 です。
- RSA サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- RSA エンドポイントに接続する際の再試行回数。

- 定期的なサーバー監視を有効にするには、[**有効（Enabled**）] チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

この手順は、RSA プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 10 （オプションの手順で SAML にのみ適用）以下を指定します。

- ID プロバイダー（IdP）オプションは、ADFS、OKTA、PING IDENTITY です。
- IDP が提供するメタデータ URL。

  ADFS の場合、IdP メタデータ URL は *https://<FQDN of ADFS>/FederationMetadata/2007-06/FederationMetadata.xml* という形式になります。OKTA の場合、IdP メタデータの URL を取得するには、Okta サーバーから対応する SAML アプリケーションの [サインオン（Sign On）] セクションで、アイデンティティ プロバイダーメタデータ URL のリンクをコピーします。

  Ping ID については、Ping ID サーバーの構成セクション（SAML アプリケーションの下）メタデータ URL リンクをコピーします。
- SAML ベースのサービスのエンティティ ID。
- IdP がプライベート CA によって署名されている場合は、[**認証局の選択（Select Certificate Authority**）] をクリックして認証局を選択します。
- GUI リダイレクトバナー。これは URL またはメッセージが可能です。この情報は、認証のためにユーザーが ID プロバイダーのログインページにリダイレクトされる前に表示されます。
- SAML サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- ドロップダウンリストから [署名アルゴリズム（Signature Algorithm）] を選択します。
- [**有効（Enabled**）] チェックボックスをオンにして、暗号化された SAML アサーション、SAML 応答の署名アサーション、SAML 署名要求、SAML 応答メッセージの署名のすべてまたは一部を有効にできます。

この手順は、SAML プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 11 （オプションの手順で OAuth 2 にのみ適用）以下を指定します。

- クライアント ID：IdP 上の APIC アプリケーションのクライアント識別子。
- APIC アプリケーションのクライアント シークレット。確認のため、もう一度クライアント シークレットを入力します。
- ユーザー名要求。トークンのユーザー名属性。例：メール、サブ。
- 範囲。OAuth 2 範囲のリスト。例：「openid プロファイル」。ユーザー グループ情報を受信するには、IdP プロバイダーで構成された対応するスコープを追加します。例：「openid プロファイル グループ」。
- OIDC プロトコルの **[有効化（Enable）]** または **[無効化（Disable）]** を選択します。
- **[有効化（Enabled）]** チェックボックスをオンにして、トークンの署名を検証します。

- JWKS エンドポイント。トークンを検証するための JSON Web キーセット（JWKS）。このフィールドは、トークン署名の検証を有効にしている場合にのみ表示されます。
- 認証エンドポイント。IdP エンドポイント認証 URL。IdP サーバーから認可エンドポイントを取得します。このフィールドは、OIDC プロトコルが無効な場合にのみ表示されます。
- トークンエンドポイント。IdP エンドポイントトークンの URL。IdP サーバーからトークン エンドポイントを取得します。このフィールドは、OIDC プロトコルが無効な場合にのみ表示されます。
- 発行元 URL IdP サーバーから発行者の URL を取得します。このフィールドは、OIDC プロトコルが有効な場合にのみ表示されます。
- IdP がプライベート CA によって署名されている場合は、[**認証局の選択（Select Certificate Authority）**] をクリックして、認証局を選択します。
- [**到達可能 EPG の選択（Select Reachability EPG**）] をクリックして、エンドポイントグループを選択します。
- OAuth 2 サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- GUI リダイレクトバナー。これは URL またはメッセージが可能です。この情報は、認証のためにユーザーが ID プロバイダーのログインページにリダイレクトされる前に表示されます。

この手順は、OAuth 2 プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 12 **[保存（Save）]** をクリックします。

ログイン ドメイン

ログイン ドメインは、ユーザの認証ドメインを定義します。ログイン ドメインは、ローカル、LDAP、RADIUS、TACACS+、DUO、SAML、RSA、または OAuth 2 認証メカニズムを設定できます。REST、CLI、または GUI からシステムにアクセスすると、APIC によりユーザは正しい認証ドメインを選択できます。

たとえば、REST シナリオでは、完全なログイン ユーザ名が次のように表示されるようにユーザ名の頭に文字列が付きます。

```
apic:<domain>\<username>
```

システムに GUI からアクセスする場合は、APIC により選択するユーザのドメインのドロップダウン リストが提供されます。`apic: domain` が指定されない場合は、デフォルトの認証ドメイン サーバがユーザ名の検索に使用されます。

ACI バージョン 1.0(2x) 以降、APIC のログイン ドメイン フォールバックのデフォルトはローカルになっています。デフォルト認証とコンソール認証方法がどちらも非ローカルの方法に設定されており、両方の非ローカル方法がローカル認証に自動的にフォールバックしない場合でも、APIC にはローカル認証を使用してアクセスすることができます。

APIC フォールバック ローカル認証にアクセスするには、次の文字列を使用します。

- GUI からは、*apic:fallback\\username* を使用します。
- REST API からは、*apic#fallback\\username* を使用します。

（注） フォールバック ログイン ドメインは変更しないでください。変更すると、システムからロックアウトされる可能性があります。

GUI を使用してローカル ドメインを作成する

SAML および OAuth 2 の外部サーバーによる認証は、標準の CiscoAVPair ベースの認証に加え、ユーザーグループのマップルール情報に基づいて行われるようになりました。

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- ログインドメイン名、レルム、リモートサーバープロバイダーは、ユーザーに対して認証ドメインを定義できます。

ステップ 1 メニュー バーで、**[管理（Admin）] > [AAA]** の順に選択します。
ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。
ステップ 3 作業ペインで、[**ログインドメイン（Login Domains**）] タブを選択します。
ステップ 4 [**アクション（Actions**）] ボタン > [**ログインドメインの作成（Create Login Domain**）] の順に選択します。
ステップ 5 [**ログインドメインの作成（Create Login Domain**）] 画面の [**一般（General**）] ペインで、次を指定します。

- ユーザーが構成したドメイン名。
- ログインドメインの説明。
- ファブリックデバイスにアクセスするエンティティ（個人またはデバイス）の ID を確認するためのレルムです。[**レルム（Realm**）] ドロップダウンリストにあるオプションは、以下で説明されています。

1. 認証用 RADIUS プロトコルをサポートするリモートサーバーグループに対する RADIUS プロバイダーグループ。
2. 認証に TACACS+ プロトコルをサポートするリモートサーバーグループの TACACS+ プロバイダーグループ。
3. 認証用 LDAP プロトコルをサポートするリモートサーバーのグループに対する LDAP プロバイダーグループ。
4. 認証用 RSA プロトコルをサポートするリモートサーバーのグループに対する RSA プロバイダーグループ。

5. 認証用の SAML プロトコルをサポートする SAML プロバイダー リモートサーバー。
6. 認証用 OAuth 2 プロトコルをサポートする OAuth 2 プロバイダー リモートサーバー

（注） LDAP、RADIUS、TACACS+ がデフォルトのセキュリティメソッドとして指定されており、このダイアログで指定された関連するプロバイダー グループがユーザ ログイン中に使用できない場合、特にそうするように構成されていない限り、Cisco APIC サーバーではフォールバック ローカル認証は実行されません。

Cisco APIC が ID プロバイダーに到達するためにプロキシサーバーを必要とする場合は、対応するプロキシ アドレスを構成します。プロキシ設定の構成は、**[システム（System）]**> > **[システム設定（System Setting）]**> > **[プロキシ ポリシー（Proxy Policy）]**の下にあります。**[プロキシ ポリシー（ Proxy Policy）]** ペインで、必要な URL を **[HTTP URL]** または **[HTTPS URL]** フィールドに入力します。

ステップ 6 表示されたオプションの詳細を入力します。表示されるオプションは動的で、選択した**レルム**に基づいています。

選択した**レルム**が RADIUS または LDAP の場合、次のオプションが表示されます。

- **レルムサブタイプ**として [**デフォルト（Default）**] または [**デュオ（Duo）**] を選択します。
- **[設定（Settings）]** ペインで、**[RADIUS (または LDAP) プロバイダーの追加（ Add RADIUS (or LDAP) Provider）]** をクリックしてプロバイダーを選択または作成します（上記の **[デフォルト（Default）]** オプションを選択した場合）。[**デュオ（Duo）**] オプションを選択した場合は、[**RADIUS (または LDAP) プロバイダーの追加（Add RADIUS (or LDAP) Provider**）] をクリックしてプロバイダーを選択または作成します。

選択した**レルム**が TACACS+ または RSA の場合、次のオプションが表示されます。

- [**設定（Settings**）] ペインで、[**RSA（または TACACS+） プロバイダーの追加（Add RSA（or TACACS+）Provider**）] をクリックして、プロバイダーを選択または作成します。

選択した**レルム**が SAML または OAuth 2 の場合、次のオプションが表示されます。

- [**設定（Settings**）] ペインで、[**SAML (または OAuth 2) プロバイダーの選択（Select SAML (or OAuth 2) Provider**）] をクリックして、プロバイダーを選択または作成します。
- [**SAML (または OAuth 2) 認証の選択（SAML (or OAuth 2) Authorization Choice**）] には、**CiscoAVPair** または **GroupMap** のいずれかを選択します。
  - **CiscoAVPair** を選択した場合、外部認証サーバーで設定された CiscoAVpair の値/文字列に基づいて承認されます。外部 IDP から CiscoAVPair の値を受信すると、それに応じて Cisco APIC ではリモートユーザに権限を割り当てます。
  - **GroupMap** を選択した場合、外部認証サーバーで構成されたグループ情報に基づいて承認されます。Cisco APIC では、外部 IDP からユーザーグループ情報を受信すると、 Cisco APIC に構成されたユーザーグループ名と照合し、それに応じてリモート ユーザ権限を割り当てます。

GroupMap を使用した承認には、次の 2 つの追加パラメータが必要です。

- [**グループ属性（Group Attribute**）] を入力します。ここで入力するグループ属性は、外部認証サーバーのグループ属性と一致している必要があります。SAML の場合、グループ属性は、SAML IdP サーバーによって送信される応答のグループ アサーションの名前と一致する必要があります。OAuth2 の場合、グループ属性は、OAuth2 サーバーによって送信される JWT（JSON Web トークン）のグループ要求と一致する必要があります。

  `Example: memberOf (used in Active directory), Groups or groups (used in ping ID/Okta)`

  また、OAuth2 の場合、IDP からグループ情報を適切に受信するには、対応するスコープが OAuth2 プロバイダー構成で構成されていることを確認してください。例：`openid profile groups`

- **[ユーザー グループ マップ ルール（User Group Map Rule）]** を、**[ユーザー グループ マップ ルールの追加（ Add User Group Map Rule）]** をクリックして、追加します。

  [**ユーザーグループ マップルールの作成（Create User Group Map Rule**）] 画面で、次の詳細を入力します。

  1. [**名前（Name**）] フィールドにユーザーグループ マップルールの名前を入力します。
  2. **[説明（Description）]** フィールドに、説明を入力します。
  3. [**グループ名（Group Name**）] フィールドに、ユーザーが属するユーザーグループの名前を入力します。

     ここで入力したユーザーグループが、外部サーバーのユーザーグループと一致していることを確認してください。これは、外部サーバーから受信した認証情報を検証するために Cisco APIC によって使用されます。権限は、ユーザーが属するユーザーグループに基づいて設定されます。
  4. **[ユーザー権限（User Privilegles）]** を設定するには、**[ユーザー権限の追加（Add User Privileges）]**をクリックします。
  5. セキュリティ ドメインを追加するには、**[セキュリティ ドメインの選択（Select Security Domain）]** をクリックして、表示されたリストからセキュリティ ドメインを選択します。
  6. **[ロールの選択（Select Role）]** をクリックしてロールを選択し、権限タイプ（読み取りまたは書き込み）を関連付け、チェックマークをクリックして、権限をロールに関連付けます。

     さらにロールを追加するには、**[ロールの追加（Add Role）]** をクリックし、権限を関連付けます。
  7. **[ユーザ権限の追加（Add User Privileges）]** ウィンドウで、**[追加（Add）]** をクリックします。
  8. **[ユーザーグループ マップ ルールの追加（Add User Group Map Rule）]** ウィンドウで、**[適用（Apply）]** をクリックします。

ステップ 7 [**ログインドメインの作成（Create Login Domain 画面**）] で、 [**保存（Save**）] をクリックします。

RADIUS 認証

Remote Authentication Dial-In User Service（RADIUS）は、ネットワーク サービスに接続し使用するユーザー向けに、一元化された認証、認可、およびアカウンティング(AAA)管理を提供するネットワーキング プロトコルです。

RADIUS サーバーでユーザーを設定するには、APIC 管理者は `cisco-av-pair` 属性を使用して必要な属性（`shell:domains`）を設定する必要があります。デフォルトのユーザ ロールは、network-operator です。

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。これらのオプションが `cisco-av-pair` 属性で指定されていない場合は、MD5 および DES がデフォルトの認証プロトコルとなります。

たとえば、SNMPv3 認証とプライバシー プロトコルの属性は次のように指定できます。

```
snmpv3:auth=SHA priv=AES-128
```

同様に、ドメインのリストは次のとおりです。

```
shell:domains="domainA domainB …"
```

RADIUS アクセス用の APIC の設定

始める前に

- ACI ファブリックが設置され、Application Policy Infrastructure Controller (APIC) がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- RADIUS サーバのホスト名または IP アドレス、ポート、認証プロトコル、およびキーを使用できること。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、RADIUS プロバイダーを作成します。

RADIUS プロバイダーの設定については、プロバイダーを作成する （61 ページ）を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

ナビゲーションウィンドウで、[**システム（System）**] > [**システム設定（System Settings）**] > [**APIC 接続設定（APIC Connectivity Preferences）**] の順に選択します。作業ペインで、[**インバンド（inband）**] または [**アウトオブバンド（ooband）**] のいずれかを選択します。

ステップ 2 RADIUS の**ログインドメイン**を作成します。

手順については、GUI を使用してローカル ドメインを作成する （66 ページ）を参照してください。

次のタスク

これで、APIC RADIUS 設定手順は完了です。次に、RADIUS サーバを設定します。

REST API を使用して APIC 内の RADIUS を設定する

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaRadiusProvider authPort="1812" authProtocol="pap" descr="myradius"
    monitorServer="disabled"
    name="server.radius.local" key="mykey"
    retries="1" timeout="5"/>
```

REST API を使用して RADIUS のログイン ドメインを設定するには：

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaUserEp  descr="" dn="uni/userext"  name=""  pwdStrengthCheck="yes" rn=""
status="modified">
    <aaaLoginDomain descr="" name="RadDom" rn="logindomain-RadDom" status="created">
        <aaaDomainAuth name="" providerGroup="RadDom" realm="radius" rn="domainauth"
status="created"/>
    </aaaLoginDomain>
   <aaaRadiusEp descr="" name="" retries="1" rn="radiusext" status="modified" timeout="5">

       <aaaRadiusProviderGroup descr=""  name="RadDom"  rn="radiusprovidergroup-RadDom"
  status="created">
           <aaaProviderRef descr="acs" name="radius1.server.com" order="1"
               rn="providerref-radius.server.com" status="created" />
           <aaaProviderRef descr="acs" name="radius2.server.com" order="2"
               rn="providerref-radius2.server.com" status="created" />
        </aaaRadiusProviderGroup>
    </aaaRadiusEp>
</aaaUserEp>
```

TACACS+ 認証

Terminal Access Controller Access Control device Plus（TACACS+）は、シスコのシステムでサポートされている、もう 1 つのリモート AAA プロトコルです。TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Cisco Application Policy Infrastructure Controller（APIC）は、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバー間のデータ送信に TCP を使用しているため、コネクション型プロトコルで確実に転送されます。
- スイッチと AAA サーバー間でプロトコルペイロード全体が暗号化されるため、高いデータ機密性が確保されます。RADIUS ではパスワードしか暗号化されません。
- 構文と設定が RADIUS と異なる av-pairs を使用しますが、Cisco APIC は `shell:domains` をサポートします。

次の XML の例では、IP アドレス 10.193.208.9 の TACACS+ プロバイダーと連携するように Cisco Application Centric Infrastructure（ACI）ファブリックを設定しています。

```
<aaaTacacsPlusProvider name="10.193.208.9"
           key="test123"
           authProtocol="pap"/>
```

（注） この例では IPv4 アドレスを使用していますが、IPv6 アドレスも使用できます。

TACACS+: を使用するときには、次の制約事項および使用上のガイドラインが適用されます。

- TACACS サーバおよび TACAC ポートは、ping で到達可能である必要があります。
- 優先順位が最も高い TACACS サーバーが、最初にプライマリ サーバーと見なされます。

TACACS+ アクセス用の APIC の設定

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- TACACS+ サーバのホスト名または IP アドレス、ポート、およびキーを使用できること。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの設定については、プロバイダーを作成する （61 ページ） を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

ナビゲーションウィンドウで、[**システム（System）**] > [**システム設定（System Settings）**] > [**APIC 接続設定（APIC Connectivity Preferences）**] の順に選択します。作業ペインで、[**インバンド（inband）**] または [**アウトオブバンド（ooband）**] のいずれかを選択します。

ステップ 2 TACACS+ の [Login Domain] を作成します。

手順については、GUI を使用してローカル ドメインを作成する （66 ページ）を参照してください。

次のタスク

これで、APIC TACACS+ 設定手順は完了です。次に、RAIDUS サーバも使用する場合は、RADIUS 用の APIC の設定も行います。TACACS+ サーバのみを使用する場合は、次の ACS サーバ設定に関するトピックに進みます。

REST API を使用して APIC の TACACS を設定する

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaTacacsPlusProvider name="server.tacacs.local"
    authProtocol="pap"
    monitorServer="enabled" monitoringUser="user1" monitoringPassword="mypwd"
    port="49" retries="1" key="mykey" timeout="15" />
```

REST API を使用して TACACS のログイン ドメインを設定するには:

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaUserEp  descr="" dn="uni/userext"  name=""  pwdStrengthCheck="yes" rn=""
status="modified">
    <aaaLoginDomain  descr=""  name="Tacacs" nameAlias=""  rn="logindomain-Tacacs"
status="created,modified">
        <aaaDomainAuth  descr="" name="" nameAlias=""  providerGroup="Tacacs"
            realm="tacacs" rn="domainauth" status="created,modified"/>
    </aaaLoginDomain>
    <aaaTacacsPlusEp  descr="" name="" nameAlias=""  retries="1" rn="tacacsext"
status="created,modified" timeout="5">
        <aaaTacacsPlusProviderGroup  descr="" name="Tacacs" nameAlias=""
            rn="tacacsplusprovidergroup-Tacacs" status="created,modified">
          <aaaProviderRef descr="testing" name="tacacs.server.com" nameAlias="" order="1"

              rn="providerref-tacacs.server.com"  status="created,modified" />
            <aaaProviderRef descr="testing" name="tacacs2.server.com" nameAlias=""
order="2"
              rn="providerref-tacacs2.server.com"  status="created,modified" />
        </aaaTacacsPlusProviderGroup>
    </aaaTacacsPlusEp>
</aaaUserEp>
```

APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の設定

始める前に

- Cisco Secure Access Control Server (ACS) バージョン 5.5 がインストールされ、オンラインになっていること。

（注） ここでは手順の説明に ACS v5.5 が使用されています。ACS の他のバージョンでもこのタスクを実行できる可能性がありますが、GUI の手順はバージョンによって異なる場合があります。

- Cisco Application Policy Infrastructure Controller (Cisco APIC) の RADIUS キーまたは TACACS+ キーを使用できること (両方を設定する場合は両方のキー) 。
- APIC が設置されオンラインになっており、APIC クラスタが形成されて正常に動作していること。

• RADIUS または TACACS+ のポート、認証プロトコル、およびキーを使用できること。

ステップ 1 APIC をクライアントとして設定するには、ACS サーバにログインします。

a) **[Network Resources]** > **[Network Devices Groups]** > **[Network Devices and AAA Clients]** に移動します。

b) クライアント名、APIC インバンド IP アドレスを指定し、TACACS + または RADIUS（または両方）の認証オプションを選択します。

（注） RADIUS または TACACS+ のみの認証が必要な場合は、必要なオプションのみを選択します。

c) 共有秘密 (キー) や認証オプションに適したポートなど、認証の詳細を指定します。

（注） **[共有秘密（Shared Secret）]** は **[プロバイダ（Provider）]** キーと一致する必要があります。

ステップ 2 ID グループを作成します。

a) **[Users and Identity Stores]** > **[Internal Groups]** オプションに移動します。

b) 必要に応じて、**[Name]** と **[Parent Group]** を指定します。

ステップ 3 ユーザを ID グループにマッピングします。

a) **[Navigation]** ペインで、**[Users and Identity Stores]** > **[Internal Identity Stores]** > **[Users]** オプションをクリックします。

b) 必要に応じて、ユーザの **[Name]** と **[Identity Group]** を指定します。

ステップ 4 ポリシー要素を作成します。

a) **[Policy Elements]** オプションに移動します。

b) RADIUS の場合、[Authorization and Permissions] > [Network Access] > [Authorization Profiles **Name]** を指定します。TACACS+ の場合、必要に応じて、[Authorization and Permissions] > [Device Administration] > [Shell Profile **Name]** を指定します。

c) RADIUS の場合、必要に応じて、**[Attribute]** には「`cisco-av-pair`」、**[Type]** には「string」、**[Value]** には「**`shell:domains = <domain>/<role>/,<domain>// role`**」と指定します。TACACS+ の場合、必要に応じて、**[Attribute]** には「`cisco-av-pair`」、**[Requirement]** には「Mandatory」、**[Value]** には「**`shell:domains = <domain>/<role>/,<domain>// role`**」と指定します。

[値（Value）] フィールドの構文は、書き込み権限を付与するかどうかを決定します。

- 読み取り/書き込み権限の場合、構文は `shell:domains = <domain>/<role>/` です。
- 読み取り専用権限の場合、構文は `shell:domains = <domain>// <role>` です。

たとえば、*cisco-av-pair* の値が `shell:domains = solar/admin/,common// read-all` である場合、`solar` はセキュリティ ドメイン、`admin` は `solar` というセキュリティ ドメインに対する書き込み権限をこのユーザに付与するロールであり、`common` はテナント共通であり `read-all` はテナント共通のすべてに対する読み取り権限をこのユーザに付与するロールです。

ステップ 5 サービス選択ルールを作成します。

a) RADIUS の場合、サービス選択ルールを作成して ID グループをポリシー要素に関連付けるには、**[Access Policies]** > **[Default Device Network Access Identity]** > **[Authorization]** に移動し、ルールの [Name]、

[Status]、および [Conditions] を指定し、必要に応じて「`Internal Users:UserIdentityGroup in ALL Groups:<identity group name>`」を追加します。

b) TACACS+ の場合、サービス選択ルールを作成して ID グループをシェル プロファイルに関連付けるには、**[Access Policies]** > **[Default Device Admin Identity]** > **[Authorization]** に移動します。ルールの [Name] と [Conditions] を指定し、必要に応じて [Shell Profile] を選択します。

次のタスク

新しく作成した RADIUS および TACACS + ユーザを使用して APIC にログインします。割り当てられた RBAC のロールと権限に従って、ユーザが正しい APIC セキュリティ ドメインにアクセスできることを確認します。ユーザは、明示的に許可されていない項目にアクセスできてはなりません。読み取り/書き込みアクセス権が、そのユーザに設定されたものと一致している必要があります。

LDAP/Active Directory の認証

RADIUS および TACACS+ と同様、LDAP により、ネットワーク要素はユーザを認証し、特定のアクションの実行を許可するために使用できる AAA クレデンシャルを取得できます。追加された認証局の設定は管理者によって実行でき、LDAPS（SSL 経由の LDAP）の信頼性をイネーブルにし、中間者攻撃を防ぐことができます。

次に示す XML の例では、ACI ファブリックが IP アドレス 10.30.12.128 の LDAP プロバイダーを使用するように設定しています。

（注） この例では IPv4 アドレスを使用していますが、IPv6 アドレスも使用できます。

```
<aaaLdapProvider name="10.30.12.128"
          rootdn="CN=Manager,DC=ifc,DC=com"
          basedn="DC=ifc,DC=com"
          SSLValidationLevel="strict"
          attribute="CiscoAVPair"
          enableSSL="yes"
     key="myldappwd"
          filter="cn=$userid"
          port="636" />
```

（注） LDAP 設定のベスト プラクティスは、属性文字列として **CiscoAVPair** を使用することです。顧客がオブジェクト ID 1.3.6.1.4.1.9.22.1 を使用して問題が発生した場合、その他のオブジェクト ID 1.3.6.1.4.1.9.2742.1-5 が LDAPサーバにも使用できます。

Cisco AVPair を設定する代わりに、APIC で LDAP グループ マップを作成するオプションがあります。

LDAP の設定

LDAP 設定には 2 つのオプションがあります。Cisco AVPair を設定したり、APIC 内で LDAP グループマップを設定したりできます。このセクションには、両方の設定オプションの手順が含まれています。

Cisco AVPair を使用した APIC アクセス用の Windows Server 2012 LDAP の設定

始める前に

- 最初に LDAP サーバを設定し、次に Cisco Application Policy Infrastructure Controller（Cisco APIC）を LDAP アクセス用に設定する。
- Microsoft Windows Server 2012 がインストールされ、オンラインになっていること。
- Microsoft Windows Server 2012 サーバ マネージャの ADSI Edit ツールがインストールされていること。ADSI Edit をインストールするには、Windows Server 2012 サーバ マネージャのヘルプに記載されている手順に従ってください。
- `CiscoAVPair` の属性の指定：Common Name = **`CiscoAVPair`**, LDAP Display Name = **`CiscoAVPair`**, Unique X500 Object ID = 1.3.6.1.4.1.9.22.1, Description = **`CiscoAVPair`**, Syntax = **`Case Sensitive String`**。

（注） LDAP 設定のベスト プラクティスは、属性文字列として **`CiscoAVPair`** を使用することです。顧客がオブジェクト ID 1.3.6.1.4.1.9.22.1 を使用して問題が発生した場合、その他のオブジェクト ID 1.3.6.1.4.1.9.2742.1-5 が LDAPサーバにも使用できます。

- 以下を行うことができる Microsoft Windows Server 2012 ユーザ アカウントを使用できること。
  - ADSI Edit を実行して `CiscoAVPair` 属性を Active Directory（AD）スキーマに追加します。
  - `CiscoAVPair` 属性パラメータに対するアクセス許可を持つように Active Directory LDAP ユーザーを設定します。
- ポート 636 は、SSll/TLS と LDAP の連携設定に必要です。

ステップ 1 ドメイン管理者として Active Directory（AD）サーバにログインします。

ステップ 2 AD スキーマに `CiscoAVPair` 属性を追加します。

a) **[Start]** > **[Run]** に移動し、「**`mmc`**」と入力し、Enter を押します。
Microsoft Management Console（MMC）が開きます。

b) **[File]** > **[Add/Remove Sanp-in]** > **[Add]** に移動します。
c) [Add Standalonee Snap-in] ダイアログボックスで、[Active Directory Schema] を選択し、[Add] をクリックします。
MMC コンソールが開きます。
d) **[属性]** フォルダを右クリックし、**[属性の作成]** オプションを選択します。
[Create New Attribute] ダイアログボックスが開きます。
e) **[共通名]** に「**CiscoAVPair**」、**[LDAP 表示名]** に「**CiscoAVPair**」、[Unique X500 Object ID] に「**1.3.6.1.4.1.9.22.1**」と入力し、**[構文]**で「**Case Sensitive String**」を選択します。
f) [OK] をクリックして、属性を保存します。

ステップ 3 [User Properties] クラスを [CiscoAVPair] 属性が含まれるように更新します。

a) MMC コンソールで、[Classes] フォルダを展開し、[user] クラスを右クリックし、[Properties] を選択します。
[user Properties] ダイアログボックスが開きます。
b) **[属性]** タブをクリックし、**[追加]** をクリックして **[スキーマのオブジェクトを選択する]** ウィンドウを開きます。
c) [Select a schema object:] リストで、「**CiscoAVPair**」を選択し、[Apply] をクリックします。
d) MMC コンソールで、[Active Directory Schema] を右クリックし、[Reload the Schema] を選択します。

ステップ 4 **CiscoAVPair** 属性のアクセス許可を設定します。

LDAP には **CiscoAVPair** 属性が含まれているため、LDAP ユーザーに Cisco APIC RBAC ロールを割り当てることにより Cisco APIC アクセス許可を付与する必要があります。

a) [ADSI Edit] ダイアログ ボックスで、Cisco APIC にアクセスする必要があるユーザを見つけます。
b) ユーザ名を右クリックし、[Properties] を選択します。
[<user> Properties] ダイアログボックスが開きます。
c) **[属性エディタ]** タブをクリックし、「*CiscoAVPair*」属性を選択し、*[値]* に「 **shell:domains = <domain>/<role>/,<domain>// role**」と入力します。

たとえば、*CiscoAVPair* の値が `shell:domains = solar/admin/,common// read-all(16001)` である場合、`solar` はセキュリティ ドメイン、`admin` は `solar` というセキュリティ ドメインに対する書き込み権限をこのユーザーに付与するロールであり、`common` は Cisco Application Centric Infrastructure（Cisco ACI）テナント共通であり `read-all(16001)` は Cisco ACI テナント共通のすべてに対する読み取り権限をこのユーザーに付与するロールです。

d) [OK] をクリックして変更を保存し、[<user> Properties] ダイアログボックスを閉じます。

LDAP サーバは Cisco APIC にアクセスするように設定されます。

次のタスク

Cisco APIC を LDAP アクセス用に設定します。

LDAP アクセス用の APIC の設定

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックがインストールされていて、Application Policy Infrastructure コントローラがオンラインになっており、APIC クラスタが形成されていて正常に動作していること。
- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、LDAP プロバイダーを設定します。

LDAP プロバイダーの設定については、プロバイダーを作成する （61 ページ）を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

ナビゲーションウィンドウで、[**システム（System）**] > [**システム設定（System Settings）**] > [**APIC 接続設定（APIC Connectivity Preferences）**] の順に選択します。作業ペインで、[**インバンド（inband）**] または [**アウトオブバンド（ooband）**] のいずれかを選択します。

ステップ 2 LDAP の **ログイン ドメイン** を作成します。

手順については、GUI を使用してローカル ドメインを作成する （66 ページ）を参照してください。

次のタスク

これで、APIC LDAP 設定手順は完了です。次に、APIC LDAP ログイン アクセスをテストします。

Cisco APIC での LDAP グループ マップ ルールの設定

Cisco APIC での LDAP グループ マップの設定には、作成の最初の LDAP グループ マップ ルールが必要です。このセクションでは、LDAP グループ マップ ルールを作成する方法について説明します。

始める前に

LDAPサーバが設定されているグループのマッピングを実行しています。

ステップ 1 メニュー バーで、**[管理（Admin）] > [AAA]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。

ステップ 3 作業ペインで、[**LADP グループマップ（LDAP Group Maps**）] > [**LDAP グループマップルール（LDAP Group Map Rules**）] を選択します。

ステップ 4 **[アクション（Actions）]** ボタン > **[LDAP グループ マップ ルールの作成（Create LDAP Group Map Rule）]** をクリックします。

ステップ 5 表示されている [**LDAP グループマップルールの作成（Create LDAP Group Map Rule**）] 画面で、タイプ、グループマップルール名、説明（オプション）、グループ DN を指定します。

ステップ 6 [セキュリティドメイン（Security Domains）] ペインで、[**セキュリティドメインの追加（Add Security Domain**）] をクリックします。[セキュリティドメイン（Security Domains）] ポップアップウィンドウで、次の詳細を入力します。

a) [**セキュリティドメインの選択（Select Security Domain**）] をクリックし、セキュリティドメインを選択します。

b) [**ロールの追加（Add Role**）] をクリックしてロールを追加し、ドロップダウンリストから権限を選択します。チェックマークをクリックして、選択した権限をロールに割り当てます。この手順を繰り返して、複数のロールをセキュリティドメインに追加します。

c) [セキュリティドメイン（Security Domains）] ウィンドウで **[追加（Add**）] をクリックします。

ステップ 7 [LDAP グループマップルールの作成（Create LDAP Group Map Rule）] 画面で **[保存（Save**）] をクリックします。

次のタスク

LDAP グループ マップ ルールを指定した後に、LDAP グループ マップを作成します。

Cisco APIC での LDAP グループ マップの設定

このセクションでは、LDAP グループ マップを作成する方法について説明します。

始める前に

- 実行中の LDAPサーバは、グループ マッピングで設定されます。

ステップ 1 メニュー バーで、**[管理（Admin**）] > **[AAA]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。

ステップ 3 作業ペインで、[**LADP グループマップ（LDAP Group Maps**）] > [**LDAP グループマップ（LDAP Group Map**）] の順に選択します。

ステップ 4 [**アクション（Actions**）]>[**LDAP グループマップの作成（Create LDAP Group Map**）] の順に選択します。

ステップ 5 表示されている [**LDAP グループマップの作成（Create LDAP Group Map**）] 画面で、[**LDAP グループマップルールの追加（Add LDAP Group Map Rule**）] をクリックして、[タイプ（Type）]、[グループマップ名（Group Map Name）]、[説明（オプション）（Description）]、[グループマップルール（LDAP Group Map Rule）] を指定します。

LDAP グループマップルールが使用できない場合は、[**LDAP グループマップルールの作成（Create LDAP Group Map Rule**）] をクリックします。LDAP グループ マップ ルール作成のための詳細な手順については、*LDAP* グループ マップ ルールの構成の手順を参照してください。

ステップ 6 [保存（Save）] をクリックします。

DUO による多要素認証

Cisco APIC は、Duo セキュリティによる多要素認証をサポートしています。Duo セキュリティ自体は、ユーザー ID のリポジトリとして機能しません。オンプレミスまたはクラウドベースの組織の既存の認証に加えて、2 要素（2F）認証を提供します。Duo による 2 要素認証は、ユーザーが組織のプライマリ認証ソースでの認証を完了すると発生します。

プライマリ認証ソースで認証を完了した後、Duo は 3 種類の 2F 認証方法をサポートします。

- スマートフォンの Duo モバイル アプリを使用したモバイルでの通知プッシュ。
- 登録済みの電話または携帯電話での通話。
- Duo モバイル アプリで生成されるパスコード。

ユーザーは、次のサーバーを使用して認証されます。

- Duo プロキシ RADIUS サーバーは、Cisco APIC の多要素認証を使用して、RADIUS PAP プライマリ認証方式を使用して分散クライアント/サーバー システムを認証します。
- Duo プロキシ LDAP サーバーは、Cisco APIC の多要素認証を使用して、Cisco AVPair または Group Maps 認証方法を使用してリモート サーバーを認証します。

DUO RADIUS プロバイダーまたは DUO LDAP プロバイダーの作成については、プロバイダーを作成する （61 ページ） の手順を参照してください。

REST API を使用して DUO プロキシを設定する

```
The URL for all XML data :
POST  https://{{apichost}}/api/node/mo/.xml
```

以下は、プロキシ RADIUS およびプロキシ LDAP サーバーを使用した Duo の設定例です。

RADIUS の設定

- DUO RADIUS プロバイダーを追加します。

```
<aaaRadiusProvider authPort="1812" authProtocol="pap" descr="duoradius"
       dn="uni/userext/duoext/radiusprovider-duoproxy.host.com"
       monitorServer="disabled" monitoringUser=""
       name="duoproxy.host.com"  key="mypasswd"
       retries="1" status="created" timeout="30"/>
```

- DUO RADIUS プロキシ プロバイダーを使用してログイン ドメインを追加します。

```
<aaaUserEp  descr="" dn="uni/userext"  name="" pwdStrengthCheck="yes" rn=""
status="modified">
    <aaaLoginDomain descr="" name="DuoRadDom" rn="logindomain-DuoRadDom"
status="created">
        <aaaDomainAuth descr="" name="" providerGroup="DuoRadDom" realm="radius"
realmSubType="duo" rn="domainauth" status="created"/>
```

```
    </aaaLoginDomain>
    <aaaDuoEp descr="" name="" retries="1" rn="duoext" status="modified" timeout="40">

        <aaaDuoProviderGroup name="DuoRadDom" providerType="radius"
secFacAuthMethods="auto,push"
             rn="duoprovidergroup-DuoRadDom" status="created">
            <aaaProviderRef descr="duoradproxy" name="duoproxy.host.com" order="1"
               rn="providerref-duoproxy.host.com" status="created" />
        </aaaDuoProviderGroup>
    </aaaDuoEp>
</aaaUserEp>
```

LDAP 設定

- 属性 `Cisco AVPair` を持つ DUO LDAP プロキシ プロバイダーを追加します。

```
<aaaLdapProvider name="duoproxy.host.com"
    SSLValidationLevel="strict"
    attribute="CiscoAvPair"
    basedn="CN=Users,DC=host,DC=com"
    dn="uni/userext/duoext/ldapprovider-duoproxy.host.com" enableSSL="no"
filter="cn=$userid"
    monitorServer="disabled"
    port="389" retries="1"
    rootdn="CN=admin,CN=Users,DC=host,DC=com"
    timeout="60"
    key="12345"/>
```

- 属性 `memberOf` を持つ DUO LDAP プロキシ プロバイダーを追加します。

```
<aaaLdapProvider name="duoproxy.host.com"
    SSLValidationLevel="strict"
    attribute="memberOf"
    basedn="CN=Users,DC=host,DC=com"
    dn="uni/userext/duoext/ldapprovider-duoproxy.host.com" enableSSL="no"
filter="cn=$userid"
    monitorServer="disabled"
    port="389" retries="1"
    rootdn="CN=admin,CN=Users,DC=host,DC=com"
    timeout="60"
    key="12345"/>
```

- LDAP GroupMap ルールを追加します。

```
<aaaLdapGroupMapRule name="DuoEmpRule"
dn="uni/userext/duoext/ldapgroupmaprule-DuoEmpRule"
       groupdn="CN=Employee,CN=Users,DC=host,DC=com" status="created">
       <aaaUserDomain name="all" rn="userdomain-all" status="created,modified">
         <aaaUserRole name="fabric-admin" privType="writePriv" rn="role-fabric-admin"
 status="created,modified"/>
       </aaaUserDomain>
</aaaLdapGroupMapRule>
```

- LDAP GroupMap ルールを追加します。

```
<aaaLdapGroupMap name="DuoEmpGroupMap"
dn="uni/userext/duoext/ldapgroupmap-DuoEmpGroupMap"  status="created">
    <aaaLdapGroupMapRuleRef name="DuoEmpRule" rn="ldapgroupmapruleref-DuoEmpRule"
status="created"/>
</aaaLdapGroupMap>
```

- GroupMap を使用して DUO LDAP ログイン ドメインを追加します。

```
<polUni>
   <aaaUserEp dn="uni/userext" name="" pwdStrengthCheck="yes" rn="" status="modified">
```

```
        <aaaDuoEp attribute="memberOf" basedn="" filter="sAMAccountName=$userid"
            name="" retries="1" rn="duoext" status="modified" timeout="30">
            <aaaDuoProviderGroup name="DuoLdapDom" authChoice="LdapGroupMap"
providerType="ldap"
                 rn="duoprovidergroup-DuoLdapDom" ldapGroupMapRef="DuoEmpGroupMap"
secFacAuthMethods="auto,push" status="modified">
                <aaaProviderRef name="duoproxy.host.com" order="1"
                    rn="providerref-duoproxy.host.com" status="modified"/>
            </aaaDuoProviderGroup>
        </aaaDuoEp>
        <aaaLoginDomain name="DuoLdapDom" rn="logindomain-DuoLdapDom"
status="modified">
            <aaaDomainAuth name="" providerGroup="DuoLdapDom" realm="ldap"
realmSubType="duo" rn="domainauth" status="modified"/>
        </aaaLoginDomain>
    </aaaUserEp>
</polUni>
```

GUI のログイン ドメインを取得する

ログイン ドメインの GET URL:

```
GET https://apic.host.com/api/aaaListDomains.json
```

```
{   "totalCount": "5",
    "imdata": [{
            "name": "DuoRadDom",
            "type": "DUO",
            "secAuths": "auto,push"
        }, {
            "name": "DuoLdapDom",
            "type": "DUO",
            "secAuths": "auto,push"
        }, {
            "name": "RadDom",
            "type": "OTHER"
        }, {
            "name": "LdapDom",
            "type": "OTHER"
        }, {
            "name": "DefaultAuth",
            "guiBanner": "",
            "type": "OTHER"
        }
    ] }
```

RSA Secure ID 認証

RSA認証は、使用できる組み合わせで固定キーを使用して、パスワードを作成するさまざまな方法でトークンを提供します。これは、ハードウェア トークンとソフトウェア トークンの両方をサポートします。

GUI を使用して、RSA アクセス用の APIC の設定

始める前に

- ACI ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- RSA サーバのホスト名または IP アドレス、ポート、認証プロトコル、およびキーを使用できること。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、RSA プロバイダを作成します。

RSA プロバイダーの構成については、「プロバイダーを作成する （61 ページ）」を参照してください。

ステップ 2 RSA の **[ログイン ドメイン（Login Domain）]** を作成します。

詳細な手順については、「GUI を使用してローカル ドメインを作成する （66 ページ）」 を参照してください。

次のタスク

これで、APIC RSA 設定手順は完了です。次に、RSA サーバを設定します。

SAML 認証

SAML は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のシスコのコラボレーション アプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。これは、サービス プロバイダーによってユーザーの認証に使用される認証プロトコルです。SAML により、ID プロバイダー（IdP）とサービス プロバイダーの間で、セキュリティ認証情報を交換できます。

SAML SSO は SAML 2.0 プロトコルを使用して、シスコのコラボレーション ソリューションのドメイン間と製品間で、シングル サインオンを実現しています。SAML 2.0 は、Cisco アプリケーション全体で SSO を有効にし、Cisco アプリケーションと IdP 間でフェデレーションを有効にします。SAML 2.0 では、高度なセキュリティ レベルを維持しながら、シスコの管理ユーザが安全なウェブ ドメインにアクセスして、IdP とサービス プロバイダーの間でユーザ認証と承認データを交換できます。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通の資格情報や関連情報を使用します。

SAML SSO の管理者権限は、シスコのコラボレーション アプリケーションでローカルに設定されたロールベース アクセス コントロール（RBAC）に基づき認証されます。

SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

（注） サービス プロバイダーが認証にかかわることはありません。SAML 2.0 では、サービス プロバイダーではなく、IdP に認証を委任します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。クライアントはサービス プロバイダーにアサーションを示します。CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザー名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。SAML SSO を使用することで、IdP とサービス プロバイダーの間で信頼の輪を作成できます。サービス プロバイダーは IdP 信頼して、ユーザを認証します。
- 認証情報を保護し、安全に保ちます。暗号化機能により、IdP、サービス プロバイダー、ユーザの間で認証情報を保護します。SAML SSO では、IdP とサービス プロバイダー間で転送される認証メッセージを外部ユーザから保護することもできます。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

SAML の基本要素

- クライアント（ユーザのクライアント）：これは、認証用にブラウザインスタンスを活用できる、ブラウザベースのクライアントまたはクライアントです。システム管理者のブラウザはその一例です。
- サービス プロバイダー：これは、クライアントがアクセスを試みるアプリケーションまたはサービスです。
- ID プロバイダー（IdP）サーバ：これは、ユーザ資格情報を認証し、SAML アサーションを発行するエンティティです。
- Lightweight Directory Access Protocol（LDAP）ユーザ：これらのユーザは、Microsoft Active Directory や OpenLDAP などの LDAP ディレクトリと統合されます。非 LDAP ユーザは、Unified Communications サーバ上にローカルに存在します。
- SAML アサーション：これは、ユーザ認証のために、IdP からサービス プロバイダーに転送されるセキュリティ情報で構成されます。アサーションは、ユーザ名や権限などのサブ

ジェクトに関する信頼されたステートメントを含む、XML ドキュメントです。通常では、信頼性を確保するために、SAML アサーションはデジタル署名されます。

- SAML 要求：これは、Unified Communications アプリケーションにより生成される認証要求です。LDAP ユーザを認証するために、Unified Communications アプリケーションは認証要求を IdP に委任します。
- 信頼の輪（CoT）：これは、共同で 1 つの IdP に対して共有と認証を行うさまざまなサービス プロバイダーで構成されます。
- メタデータ：これは、IdP と同様に ACI アプリケーションによって生成された、XML ファイルです。SAML メタデータの交換により、IdP とサービス プロバイダーの間に信頼関係が確立します。
- Assertion Consumer Service（ACS）URL：この URL は、アサーションをポストする場所を IdP に指示します。ACS URL は、最終的な SAML 応答を特定の URL にポストすることを IdP に指示します。

（注） 認証が必要なすべてのインスコープ サービスでは、SSO のメカニズムとして SAML 2.0 を使用します。

サポートされている IdPs および SAML コンポーネント

サポートされる IdP

ID プロバイダー（IdP）は、ユーザ、システム、サービスの ID 情報を作成、維持、管理する認証モジュールです。また、分散ネットワーク内のその他のアプリケーションやサービス プロバイダーに対して認証も行います。

SAML SSO で、IdPs はユーザーのロールまたは各 Cisco コラボレーション アプリケーションのログイン オプションに基づいて、認証オプションを提供します。IdP は、ユーザ資格情報を保管、検証し、ユーザがサービス プロバイダーの保護リソースにアクセスできる SAML 応答を生成します。

（注） IdP サービスを十分理解している必要があります。現在インストールされていて、操作可能であることを確認してください。

APIC の SAML SSO 機能は、次の IdP でテストされています。

- https://technet.microsoft.com/en-us/library/cc772128(WS.10).aspx
- Okta シングル サインオン： https://www.okta.com/products/single-sign-on/
- PingFederate： https://documentation.pingidentity.com/pingfederate/pf90/index.shtml#gettingStartedGuide/concept/gettingStarted.html

SAML のコンポーネント

SAML SSO ソリューションは、特定のアサーション、プロトコル、バインディング、プロファイルの組み合わせに基づきます。さまざまなアサーションは、プロトコルやバインディングを使用しているアプリケーション間やサイト間で交換され、これらのアサーションによりサイト間でユーザを認証します。SAML のコンポーネントは次のとおりです。

- SAML アサーション：これは、IdP からサービス プロバイダーに転送される情報の構造と内容を定義します。セキュリティ情報のパケットで構成され、さまざまなレベルのアクセス コントロール決定にサービス プロバイダの用途があることを示す文書が含まれます。SAML SSO は次の種類の文書を提供します。
  - 認証ステートメント：これらのステートメントは、IdP とブラウザの間で特定の時間に行う認証の方法について、サービス プロバイダーにアサートします。
  - 属性ステートメント：これらのステートメントは、ユーザに関連付ける特定の属性（名前と値のペア）についてアサートします。属性アサーションには、ユーザに関する具体的な情報が含まれます。サービスプロバイダーは、属性を使用してアクセス制御の決定を行います。
- SAML プロトコル：SAML プロトコルは、SAML がアサーションをどのように要求し、取得するかを定義します。このプロトコルは、特定の SAML エレメントまたはアサーションで構成されている、SAML 要求と応答エレメントに対応します。SAML 2.0 には次のプロトコルがあります。
  - アサーション クエリと要求のプロトコル
  - 認証要求のプロトコル
- SAML バインディング：SAML バインディングは、SOAP 交換のような、標準メッセージング形式または通信プロトコルとの SAML アサーションまたはプロトコル メッセージ（またはその両方）の交換のマッピングを指定します。ACI は次の SAML 2.0 バインディングをサポートしています。
  - HTTP Redirect（GET）バインディング
  - HTTP POST バインディング
- SAML プロファイル：SAML プロファイルでは、明確に定義された使用事例をサポートするために、SAML アサーション、プロトコル、およびバインディングの組み合わせについて詳細に説明しています。

NTP の設定

SAML SSO で、Network Time Protocol（NTP）では APIC および IdP 間のクロック同期が可能です。SAML は時間的な制約のあるプロトコルであり、IdP は SAML アサーションが有効であることを時間ベースで判断します。IdP および APIC クロックが同期されていない場合、アサーションが無効になり SAML SSO 機能が停止します。IdP および APIC の間で許可される最大時差は 3 秒です。

（注） SAML SSO を動作させるには、NTP 設定を正しくインストールする必要があり、IdP と APIC アプリケーション間の時間差が 3 秒を超えていないことを確認する必要があります。IdP および APIC クロックが同期されていない場合、ユーザーは IdP で認証に成功した後でも APIC のログイン ページにリダイレクトされます。

DNS の設定

Domain Name System（DNS）により、ホスト名とネットワーク サービスをネットワーク（複数可）内の IP アドレスにマッピングできるようになります。ネットワーク内に配置された DNS サーバは、ネットワーク サービスをホスト名にマッピングし、次にホスト名を IP アドレスにマッピングするデータベースを備えています。ネットワーク上のデバイスは、DNS サーバに照会して、ネットワークにある他のデバイスの IP アドレスを受信できます。そのため、ネットワーク デバイス間の通信が容易になります。

まとめると、APIC および Idp は互いの完全修飾ドメイン名を IP アドレスに対して解消でき、クライアントによって解消される必要があります。

Certificate Authority：認証局

シスコは、次のいずれかの種類の認証局（CA）により署名されるサーバ証明書を使用することを推奨します。

- **パブリック CA**：サードパーティ企業が、サーバーの識別情報を確認し、信頼できる証明書を発行します。
- **プライベート CA**：自身でローカルの CA を作成および管理し、信頼できる証明書を発行します。

署名プロセスは製品ごとに異なり、サーバのバージョン間でも異なる場合があります。各サーバのすべてのバージョンに関する詳細な手順については、このマニュアルの範囲外になります。CA により署名された証明書を取得する方法の詳細な手順については、該当するサーバのマニュアルを参照してください。

パブリック CA により署名されたサーバ証明書を取得する場合、パブリック CA は、クライアント コンピュータの信頼ストアで、ルート証明書をあらかじめ提示しておくようにします。この場合、クライアント コンピュータでルート証明書をインポートする必要はありません。プライベート CA など、CA により署名される証明書が信頼ストアにまだ存在しない場合は、ルート証明書をインポートしてください。SAML SSO では、CN または SAN での正しいドメインが記載された CA 署名付き証明書が、IdP およびサービス プロバイダーに必要になります。正しい CA 証明書が検証されない場合、ブラウザはポップ アップ警告を出します。

APIC の信頼ストアに IdP のルート証明書が含まれていない場合は、新しい証明機関を作成する必要があります。APIC で SAML プロバイダを設定する際は、この認証機関を後で使用する必要があります。

SAML アクセス用の APIC の設定

（注） SAML ベースの認証と CLI/REST の APIC GUI でのみです。また、リーフ スイッチと背表紙には適用されません。APIC CLI では、SAML 設定を行うことはできません。

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- SAML サーバ ホスト名または IP アドレスと、IdP メタデータの URL を使用できます。
- APIC 管理エンドポイント グループを使用できること。
- 次の設定を行います。
  - 時刻同期と NTP：https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/basic_config/b_APIC_Basic_Config_Guide_3_x/b_APIC_Basic_Config_Guide_3_x_chapter_011.html#concept_9CE11B84AD78486AA7D83A7DE1CE2A77。
  - 拡張 GUI 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：https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/basic_config/b_APIC_Basic_Config_Guide_3_x/b_APIC_Basic_Config_Guide_3_x_chapter_011.html#task_750E077676704BFBB5B0FE74628D821E。
  - GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定：https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/basic_config/b_APIC_Basic_Config_Guide_3_x/b_APIC_Basic_Config_Guide_3_x_chapter_011.html#task_F037F1B75FF74ED1BCA4F3C75A16C0FA。

ステップ 1 APIC で、SAML プロバイダーを作成します。

プロバイダーを作成するには、「プロバイダーを作成する （61 ページ）」を参照してください。

ステップ 2 SAML の**ログイン ドメイン**を作成します。

詳細な手順については、「GUI を使用してローカル ドメインを作成する （66 ページ）」 を参照してください。

REST API を使用して APIC で SAML を設定する

REST API を使用して SAML を構成するには、以下に示すように、最初に SAML プロバイダーを作成します。

```
<aaaSamlProvider name="cisco729224.okta.com"
dn="uni/userext/samlext/samlprovider-cisco729224.okta.com"
  entityId="http://www.okta.com/exk7j6qjvxgk8hwy0696"
  guiBannerMessage=""
  idP="okta"
  metadataUrl="https://cisco729224.okta.com/app/exk7j6qjvxgk8hwy0696/sso/saml/metadata"
monitorServer="disabled" retries="1" timeout="5"
  tp="oktacert"
  wantAssertionsEncrypted="no" wantAssertionsSigned="yes" wantRequestsSigned="yes"
wantResponseSigned="yes"
sigAlg="SIG_RSA_SHA256"
status="created,modified" />
```

次に、ログイン ドメインを作成します。認証には、CiscoAVPair またはグループ マップのいずれかを使用できます。

```
Authentication using CiscoAVPair
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TestSAML" name="TestSAML"
status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TestSAML/domainauth" providerGroup="TestSAML"
 realm="saml" realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaSamlEp rn="samlext" status="modified">
<aaaSamlProviderGroup dn="uni/userext/samlext/samlprovidergroup-TestSAML" name="TestSAML"
 authChoice="CiscoAVPair" status="created,modified">
<aaaProviderRef
dn="uni/userext/samlext/samlprovidergroup-TestSAML/providerref-cisco729224.okta.com"
name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaSamlProviderGroup>
</aaaSamlEp>
</aaaUserEp>

Authentication using Group Map
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TestSAML" name="TestSAML"
status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TestSAML/domainauth" providerGroup="TestSAML"
 realm="saml" realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaSamlEp rn="samlext" status="modified">
<aaaSamlProviderGroup dn="uni/userext/samlext/samlprovidergroup-TestSAML" name="TestSAML"
 authChoice="LdapGroupMap" groupAttribute="memberOf" status="created,modified">
<aaaUserGroupMapRule name="AdminRule" userGroup="CN=Domain
Admins,CN=Users,DC=insaaadev,DC=net" status="created,modified">
<aaaUserDomain name="all" rn="userdomain-all" status="created,modified">
<aaaUserRole name="fabric-admin" privType="writePriv" rn="role-fabric-admin"
status="created,modified"/>
</aaaUserDomain>
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="access-admin" privType="writePriv" rn="role-access-admin"
status="created,modified"/>
<aaaUserRole name="nw-svc-policy" privType="writePriv" rn="role-nw-svc-policy"
status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>

<aaaUserGroupMapRule name="EmpRule" userGroup="CN=Employee,CN=Users,DC=insaaadev,DC=net"
 status="created,modified">
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="ops" privType="writePriv" rn="role-ops" status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>
```

```
<aaaProviderRef
dn="uni/userext/samlext/samlprovidergroup-TestSAML/providerref-cisco729224.okta.com"
name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaSamlProviderGroup>
</aaaSamlEp>
</aaaUserEp>
```

Okta で SAML アプリケーションの設定

Okta で SAML を設定するには、管理者特権を持つユーザーとして Okta 組織にログインします。

（注） Okta 組織をお持ちでない場合、空の Okta を作成できます。

https://www.okta.com/start-with-okta/

ステップ 1 Okta で、青色の **[管理者]** ボタンをクリックします。

ステップ 2 **[アプリケーションの追加]** ショートカットをクリックします。

ステップ 3 緑色の **[新しいアプリケーションの作成]** ボタンをクリックし、次の操作を行います。

a) **[新しいアプリケーションの作成]** ダイアログ ボックスで、**[SAML 2.0]** オプションを選択し、緑色の **[作成]** ボタンをクリックします。

b) **[全般設定]** ボックスで、**[例 SAML アプリケーション]** を、 **[アプリケーション名]** フィールドに入力し、緑色の **[次へ]** ボタンをクリックします。

c) **[SAML の設定]** セクション A **[SAML 設定]** フィールドで、**[シングル サインオン URL]**、**[受信者 URL]**、**[対象者の制限]** フィールドに SAML URL を貼り付けます。

このフィールドは次の形式にする必要があります。

- https://<APIC_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC_hostname>
- 要求可能な SSO URL を使用して APIC のクラスタを設定します。
  - https://<APIC1_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC1_hostname>
  - https://<APIC2_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC2_hostname>
  - https://<APIC3_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC3_hostname>
- 名前 ID 形式：Transient
- 応答：署名済み
- アサーション署名: 署名

- アサーション暗号化: 暗号化されていません。
- SAML シングル ログアウト: Disabled
- authnContextClassRef: PasswordProtectedTransport
- SAML 発行者 ID: http://www.okta.com/$ {org.externalKey}

d) **[Attribute Statements]** セクションで、**[FirstName]**、**[LastName]**、**[Email]**、**[CiscoAvpair]** フィールドに情報を追加して、**[次へ]** をクリックします。

（注） **CiscoAvpair** と呼ばれるカスタム属性は **[プロファイル エディタ]** で Okta ユーザーを作成する必要があります。CiscoAvpair の詳細は、外部認証サーバの AV ペア （56 ページ） を参照してください。

e) **[フィードバック]** ボックスで、**[私は内部アプリケーションを追加する Okta 顧客です]** および **[これは私が作成した内部アプリケーションです]** を選択して、**[終了]** をクリックします。

ステップ 4 新しく作成した **[例 SAML アプリケーション]** アプリケーションの **[サインオン]** が表示されます。このページを保存し、別のタブまたはブラウザウィンドウで開きます。SAML 設定の **[ID プロバイダー メタデータ]** をコピーするには、後でこのページに戻ります。

（注） メタデータのリンクをコピーするには、**[ID プロバイダー メタデータ]** リンクを右クリックして **[コピー]** を選択します。

AD FS で Relying Party Trust の設定

AD FS 管理コンソールで信頼当事者証明を追加します。

ステップ 1 証明書利用者信頼を追加します。

a) AD FS サーバの AD FS 管理コンソールにログインし、**ADFS** > **Trust Relationships** > **Relying Party Trusts** の順に移動して、 [Add Relying Party Trust] を右クリックしてから [Start] をクリックします。

b) APIC 内で、対応するログイン ドメイン設定で利用できる [Download SAML Metadata] オプションを使用して生成されたメタデータ ファイルをインポートすることによって、 [Enter data about the relying party manually] または [Import data about relying party from a file (skip the steps d, e, f and g)] を選択します。

c) [Display Name] に信頼当事者証明の任意の表示名を入力し、[Next] をクリックします。

d) AD FS プロファイルを選択し、[Next] をクリックします。

e) もう一度 [Next] をクリックします。

f) [Enable support for the SAML 2.0 Web SSO Protocol] を選択し、**信頼当事者 SAML2.0 SSO サービス の URL** として *https://<APIC_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name>* と入力し、[Next] をクリックします。

g) **信頼当事者証明の識別子**として *https://<APIC_hostname>/api/aaaLoginSSO.json* 入力します。

h) [I do not want to configure multi-factor authentication settings for this relying party trust at this time] を選択し、[Next] をクリックします。

i) [Permit all users to access this relying party] を選択し、[Next] をクリックします。

j) [Open the Edit Claim Rules dialog for this relying party trust when the wizard closes] を選択し、[Close] をクリックします。

ステップ 2 次の**クレーム** ルールを追加します。

a) LDAP 属性をクレームとして送信します。

- [Edit Claim Rules] ウィンドウで、[Add Rule] をクリックします。
- [Claim Rule Template] で [Send LDAP attributes as Claims] を選択し、[Next] をクリックします。
- [Rule_Name] を入力し、[Attribute Store] として [Active Directory] を選択します。
- CiscoAvpair を格納するための予約済みユーザ属性を選択します（たとえば、[LDAP attribute type] として [Department] を選択し、それを [Outgoing Claim Manually Type] の [CiscoAvpair] にマッピングします）。
- [LDAP Attribute] で [E-Mail-Addresses] を選択し、それを [Outgoing Claim Type] の [E-mail Address] にマッピングして、[Finish] をクリックします。

b) 着信要求を変換します。

- [Edit Claim Rules] ウィンドウで再度 [Add Rule] をクリックし、[Transform an Incoming Claim as Claim Rule Template] を選択して、[Next] をクリックします。
- [Incoming claim type] として [E-Mail Address] を選択 します。
- [Outgoing claim type] として [Name ID] を選択します。
- [Outgoing name ID format] として [Transient Identifier] を選択します。

ステップ 3 APICのクラスタを追加するには、複数の**信頼当事者証明**をセットアップするか、または1つの**信頼当事者証明**をセットアップしてから複数の**信頼当事者識別子** および **SAML アサーション コンシューマ エンドポイント** をそれに追加することができます。

a) 上記で作成した同じ信頼当事者証明を持つクラスタ内に、他の APIC を追加する。

1. **ADFS Management Console** > **ADFS** > **Trust Relationships** > **Relying Party Trusts** と移動して、**CiscoAPIC** > **Properties** の順に右クリックします。
2. [Identifiers] タブをクリックし、クラスタ内に他の APIC を次のとおりに追加します：*https://<APIC2_hostname>/api/aaaLoginSSO.json*、*https://<APIC3_hostname>/api/aaaLoginSSO.json*
3. [Endpoints] タブをクリックし、[Add SAML] をクリックすることによって他の 2 つの APIC を追加します。[Add SAML Post Binding] 、[Index] を 1 として、信頼されている URL に *https://<APIC2_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name>* のように入力します。そして、[Add SAML Post Binding] に *https://<APIC3_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name* のように入力します。

ステップ 4 メッセージとアサーションは、ADFS サーバ内の powershell から ADFS で署名する必要があります。ADFS サーバーでメッセージおよびアサーションを署名するには：

a) Windows Powershell を開き（管理者として実行する必要があります）、次のコマンドを実行します。
b) Set AdfsRelyingPartyTrust TargetName **RelyingpartytrustnameOfCiscoAPIC** - SamlResponseSignature **MessageAndAssertion** 。

OAuth 2 / OIDC 認証

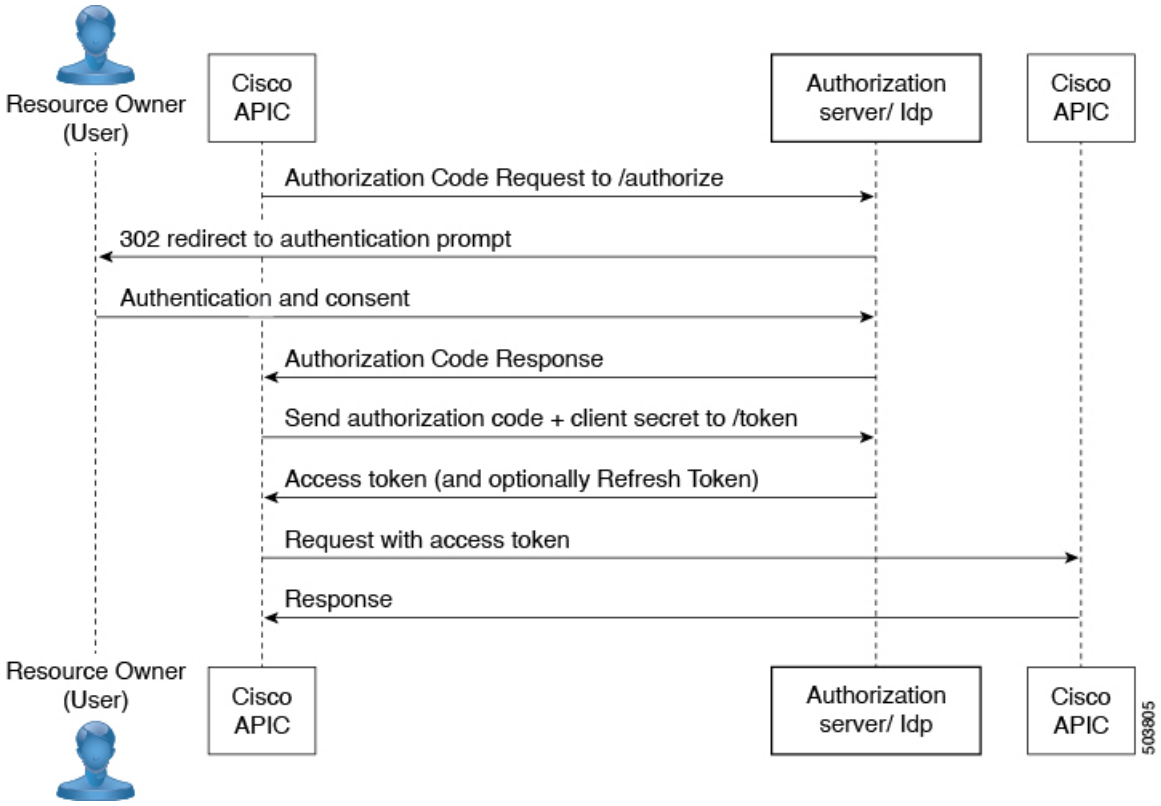
Open Authorization (OAuth) 2.0 は、オープン標準の認証プロトコルです。OAuth 2.0 を使用すると、ID プロバイダー (IdP) によって信頼または承認されたアプリケーション（サービスプロバイダー、すなわち SP）にアクセスできます。OAuth 2.0 は、承認トークンを使用して、コンシューマー アプリケーションに ID と承認請求を提供します。

OAuth 2.0 の詳細については、*RFC 6749* を参照してください。

OAuth 2.0 は、サービスプロバイダー アプリケーションから REST API を使用するさまざまなクライアントタイプをサポートするように設計されています。これには、企業内の Web サービスにアクセスするブラウザアプリケーションと、顧客のモバイルデバイスで実行されるアプリケーションの両方が含まれます。OAuthプロトコルでは、認証トークンを取得するための複数のメカニズムを定義し、さまざまなメカニズムがクライアントタイプの制約を認識します。単純な OAuth の例は、「https://service.example.com」などの Web サイトにログインしようとすると、ソーシャルメディアプラットフォームのログインまたは電子メールログインを使用して自分自身を識別するように求められる場合があります。これらの ID プロバイダーにログインしている場合は、何度もログインする必要はありません。いずれかのオプションを選択するとすぐに、「https://service.example.com」にログインすることが（OAuth を使用して）許可されます。

Cisco ACI での OAuth 2.0 認証

ACI で使用される OAuth のタイプは、承認付与フローです。この方法では、Cisco APIC は最初に認証されたユーザーによる承認付与を要求し、APIC は次に承認付与を使用して、承認情報を持つアクセス トークンを取得します。フローを次の図に示します。



OAuth の要素

- リソース所有者（ユーザー）— データ所有者
- Web アプリケーション — APIC（または Cloud APIC ）
- 承認サーバー（AS）または ID プロバイダー（IdP）サーバー - ユーザーを認証および承認します。
- リソース サーバー — APIC

（注） 承認サーバーが ID トークンとアクセス トークンの両方を提供する場合、ID トークンは、ユーザー名と CiscoAvpair クレームのアクセス トークンよりも優先されます。ID トークンで CiscoAvpair が利用できない場合、ユーザー名と CiscoAvpair の両方の要求がアクセス トークンから取得されます（利用可能な場合）。APIC は、両方のトークンからのユーザー名と CiscoAvpair クレームを結合しません。つまり、ID トークンからのユーザー名とアクセス トークンからの CiscoAvpair は考慮しません。また、その逆も考慮しません。どのトークンにも CiscoAvpair 要求がない場合、ID トークンからのユーザー名が取得され、設定されている場合はデフォルトの認証が試行されます。

Cisco APIC で OAuth を設定する

この手順を使用して、Cisco APIC で OAuth を設定します。

前提条件

Okta（またはその他の認証サーバー）で次のアクションを実行します。

- APIC 用の OAuth アプリケーションを作成します。クライアント ID とシークレットを書き留めます。
- APIC へのアクセスを許可する許可ポリシーが設定されていることを確認します。
- ACI で使用される承認エンドポイントとトークン エンドポイントに注意してください。
- APIC を使用するアプリケーションにユーザーを割り当てます。
- *CiscoAvpair* が、ACI での認証のためにユーザーに対して正しく設定されていることを確認します。
- トークン URL の証明書チェーンを保存します。

ID プロバイダーでの OAuth 2.0 アプリケーションの設定の詳細については、関連するドキュメントを参照してください。

OAuth 2 アクセス用の APIC の設定

この手順を使用して、OAuth 2 プロバイダーを作成し、ログインドメインを関連付けます。

ステップ 1 APIC で、OAuth 2 プロバイダーを作成します。

OAuth 2 プロバイダーの構成については、「プロバイダーを作成する （61 ページ）」 を参照してください。

ステップ 2 OAuth 2 の [**ログイン ドメイン（Login Domain）**] を作成します。

詳細な手順については、「GUI を使用してローカル ドメインを作成する （66 ページ）」 を参照してください。

認証局を作成する

トークン URL に使用される証明書チェーンを使用して認証局を作成するには、この手順を使用します。

ステップ 1 メニュー バーで、**[管理（Admin）] > [AAA]** の順に選択します。

ステップ 2 ナビゲーション ウィンドウで、[**セキュリティ（Security）**] を選択します。

ステップ 3 作業ペインで、[**認証局（Certificate Authorities）**] を選択します。

ステップ 4 [アクション（**Actions**）] > [認証局の作成（**Create Certificate Authority**）] をクリックします。

ステップ 5 名前、説明、および**証明書チェーン**を入力します。

以下の手順で**証明書チェーン**を取得してください。

a) Okta/承認サーバーからトークン URL を選択します。
b) ブラウザ ウィンドウで、トークン URL を入力します。
c) 右クリックして、**[詳細情報（More Information）]** を選択します。
d) 表示されたポップアップ ウィンドウから、**[新しい証明書（New Certificate）]** ボタンをクリックします。
e) 証明書画面が表示されます。**PEM（チェーン）** 証明書をダウンロードします。
f) 適切なプログラムを選択してファイルを開きます。
g) 表示された証明書のチェーンから必要な証明書を選択します。

（注） 最大 8 つの認証局を作成できます。

ステップ 6 **[保存（Save）]** をクリックします。

OAuth を使用したユーザー ログイン

OAuth 用に作成されたログイン ドメインを使用して APIC にログインしようとすると、認可サーバーのログインページにリダイレクトされます（まだ認証されていない場合）。ユーザーが認証されると、Web ブラウザを介して認可サーバーから APIC に認可コードが送信されます。APIC は、APIC アプリケーションのクライアント ID とシークレットを使用して、IdP からのアクセス トークンとこのコードを交換します。アクセス トークンには、*CiscoAvpair* のユーザー名と認証の詳細があります。その後、APIC にログインします。APIC では、ログインしているユーザーがそれに応じて示されます。

REST API を使用して APIC で OAuth を設定する

この手順を使用して、REST API を使用し APIC で OAuth を設定します。

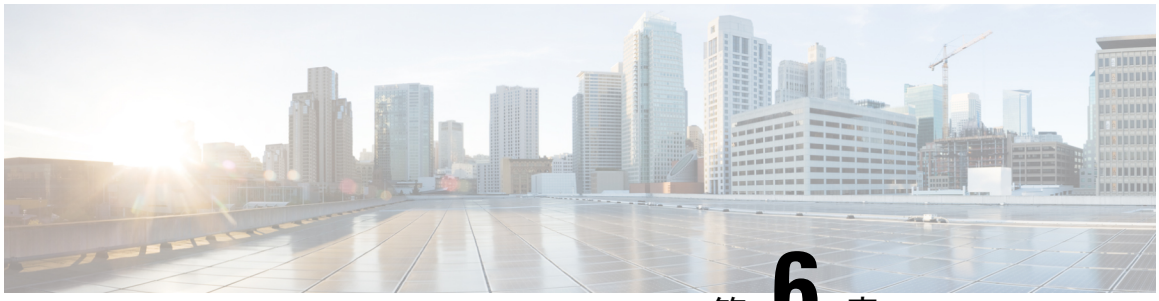
ステップ 1 OAuth プロバイダーを作成します。

```
<aaaOauthProvider name="cisco729224.okta.com"
dn="uni/userext/oauthext/oauthprovider-cisco729224.okta.com"
status="created,modified"
timeout="5"
key="vCnIq1EGCTPfqMU"
oidcEnabled="no"
verifyEnabled="yes"
baseUrl="https://cisco729224.okta.com/oauth2/default"
clientId="0oa9g25h1cE7yZZ0t696"
usernameAttribute="EmailId"
scope="openid groups"
tp="oktacert"/>
```

ステップ 2 OAuth ログイン ドメインを作成します。認証には、CiscoAVPair またはグループ マップのいずれかを使用できます。

```
Authentication using CiscoAVPair
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TOAUTH" name="TOAUTH" status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TOAUTH/domainauth" providerGroup="TOAUTH" realm="oauth"
 realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaOauthEp rn="oauthext" status="modified">
<aaaOauthProviderGroup dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH" name="TOAUTH"
authChoice="CiscoAVPair" status="created,modified">
<aaaProviderRef dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH/providerref-cisco729224.okta.com"
 name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaOauthProviderGroup>
</aaaOauthEp>
</aaaUserEp>
```

```
Authentication using Group Map
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TOAUTH" name="TOAUTH" status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TOAUTH/domainauth" providerGroup="TOAUTH" realm="oauth"
 realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaOauthEp rn="oauthext" status="modified">
<aaaOauthProviderGroup dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH" name="TOAUTH"
authChoice="LdapGroupMap" groupAttribute="memberOf" status="created,modified">
<aaaUserGroupMapRule name="AdminRule" userGroup="Domain Admins" status="created,modified">
<aaaUserDomain name="all" rn="userdomain-all" status="created,modified">
<aaaUserRole name="fabric-admin" privType="writePriv" rn="role-fabric-admin"
status="created,modified"/>
</aaaUserDomain>
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="access-admin" privType="writePriv" rn="role-access-admin"
status="created,modified"/>
<aaaUserRole name="nw-svc-policy" privType="writePriv" rn="role-nw-svc-policy"
status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>
<aaaUserGroupMapRule name="EmpRule" userGroup="Employee" status="created,modified">
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="ops" privType="writePriv" rn="role-ops" status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>
<aaaProviderRef dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH/providerref-cisco729224.okta.com"
 name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaOauthProviderGroup>
</aaaOauthEp>
</aaaUserEp>
```



第 6 章

802.1X

この章は、次の項で構成されています。

802.1X の概要

802.1X では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

RADIUS 分散クライアント/ サーバ システムを使用すると、不正アクセスからネットワークを保護できます。Cisco ACI 実装では、RADIUS クライアントは ToR で稼働し、すべてのユーザー認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウンティング要求を送信します。

ホスト サポート

802.1 X 機能は、次のモードでポート上のトラフィックを制限できます。

- **単一ホスト モード**：802.1Xポートで1台のエンドポイントデバイスのみからのトラフィックが許可されます。エンドポイント デバイスが認証されると、APIC はポートを許可状態にします。エンドポイント デバイスがログオフすると、OS はポートを無許可状態に戻します。802.1X のセキュリティ違反とは、認証に成功して許可された単一の MAC アドレスとは異なる MAC アドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティ アソシエーション（SA）違反（他の MAC アドレスからの EAPOL フレーム）が検出されたインターフェイスはディセーブルにされます。シングル ホスト モードは、ホストツースイッチ型トポロジで 1 台のホストが APIC のレイヤ 2 ポート（イーサネット アクセス ポート）またはレイヤ 3 ポート（ルーテッド ポート）に接続されている場合にだけ適用できます。
- **複数のホスト モード**：ポートごとに複数のホストを使用できますが、最初の 1 つだけが認証されます。最初のホストの許可に成功すると、ポートは許可ステートに移行します。ポートが許可ステートになると、後続のホストがネットワーク アクセスの許可を受ける必要はありません。再認証に失敗したり、または EAPOL ログオフ メッセージを受信して、ポートが無許可ステートになった場合には、接続しているすべてのクライアントはネットワーク アクセスを拒否されます。マルチ ホスト モードでは、SA 違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。このモードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます
- **マルチ認証モード**：複数のホストとすべてのホストを個別に認証を使用できます。

（注） 各ホストには、同じ EPG/VLAN 情報を必須です。

- **マルチ ドメイン モード**：別のデータおよび音声ドメイン。IP 電話で使用します。

認証モード

ACI 802.1 x は次の認証モードをサポートしています。

- **EAP**：オーセンティケータは EAP-Request/Identity フレームをサプリカントに送信して識別情報を要求します（通常、オーセンティケータは1つまたは複数の識別情報の要求のあとに、最初の Identity/Request フレームを送信します）。サプリカントはフレームを受信すると、EAP-Response/Identity フレームで応答します。
- **MAB**：フォールバック認証モードとして MAC 認証バイパス（MAB）がサポートされています。MAB により、エンドポイントの MAC アドレスを使用してポートベースのアクセス コントロールが有効になります。MAB が有効なポートは接続するデバイスの MAC アドレスに基づいて、動的に有効または無効にできます。MAB の前に、エンドポイントの ID が不明であり、すべてのトラフィックがブロックされます。スイッチでは、単一のパケットを検査して送信元 MAC アドレスを学習および認証します。MAB が成功するとエンドポイントの ID が判明し、エンドポイントからのすべてのトラフィックが許可されます。スイッチは送信元 MAC アドレス フィルタリングを実行し、MAB の認証されたエンドポイントのみがトラフィックの送信を許可されます。

注意事項と制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- Cisco ACI が 802.1X 認証をサポートするのは、物理ポート上だけです。
- Cisco ACI は、ポート チャネルまたはサブインターフェイスでは 802.1X 認証をサポートしません。
- Cisco ACI は、ポート チャネルのメンバ ポートでは 802.1X 認証をサポートしますが、ポート チャネル自体ではサポートしません。
- 802.1X 設定を含むメンバ ポートと含まないメンバ ポートはポート チャネルで共存できます。ただし、チャネリングと 802.1X が連携して動作するためには、すべてのメンバ ポートで 802.1X 設定を同一にする必要があります
- 802.1X 認証を有効にした場合、サプリカントが認証されてから、イーサネット インターフェイス上のレイヤ 2 またはレイヤ 3 のすべての機能が有効になります。
- 802.1X は、EX または FX タイプのリーフ シャーシでのみサポートされています。
- 802.1X は、ファブリック アクセス ポートでのみサポートされています。802.1X は、ポート チャネルまたは仮想ポート チャネルではサポートされていません。
- IPv6 は、dot1x クライアント 3.2(1) リリースではサポートされていません。
- 特に特定のインターフェイス設定（ホストモードおよび認証タイプ）がそのリリースでサポートされていない場合に以前のリリースにダウングレードすると、dot1x 認証タイプはデフォルトでなしになります。ホストモードは希望に応じて単一のホストか複数のホストのどちらかに手動で再設定する必要があります。これで、ユーザーがそのリリースでのみサポートされているモード/認証タイプを設定し、サポートされていないシナリオで実行していないことを確認します。
- マルチ認証では、1 音声クライアントと複数のデータ クライアント（すべて同じデータ vlan/epg に属する）をサポートします。
- 802.1X ノード認証ポリシーでの障害 epg/vlan は必須設定です。
- 1 音声および 1 データ クライアント以上のマルチドメインは、ポートをセキュリティ無効の状態にします。
- 次のプラットフォームでは 802.1X はサポートされていません。
  - N9K-C9396PX
  - N9K-M12PQ
  - N9K-C93128TX
  - N9K-M12PQ

コンフィギュレーションの概要

APIC で有効になっている場合にのみ、802.1X および RADIUS プロセスが開始されます。内部的にこれは、radius エンティティの作成時に 802.1X Inst MO が作成され radius プロセスが作成されたときに、dot1x プロセスが開始されることを意味します。そのインターフェイスに接続しているユーザーを認証するため、Dot1x ベースの認証が各インターフェイスで有効になっている必要があります。そうでない場合、動作が変更されません。

RADIUS サーバの設定は、dot1x 設定とは別に行われます。RADIUS の設定は、RADIUS サーバのリストとそれらに到達する方法を定義します。Dot1x 設定には、認証に使用する RADIUS グループ（またはデフォルト グループ）への参照が含まれています。

正常に認証を行うには 802.1X と RADIUS の両方を設定する必要があります。設定の順序は重要ではありませんが、RADIUS 設定がない場合は、802.1X 認証は正常に行われません。

APIC GUI を使用した 802.1X ポート認証の設定

始める前に

RADIUS プロバイダのポリシーを設定します。

ステップ 1 メニュー バーで、**[Fabric]** > **[External Access Policies]** > **[Policies]** > **[Interface]** > **[802.1X Port Authentication]** をクリックし、次の操作を行います。

a) [802.1X Port Authentication] を右クリックして、[Create 802.1X Port Authentication Policy] を開きます。

b) [Name] フィールドにポリシーの名前を入力します。

c) **[ホスト モード]** フィールドで、ポリシー モードを選択します。使用可能なモードを次に示します。

- **[マルチ認証]**：複数のホストおよびすべてのホストを個別に認証できます。

  （注） 各ホストには、同じ EPG/VLAN 情報が必須です。

- **[マルチ ドメイン]**：別のデータおよび音声ドメインです。IP 電話で使用します。
- **[マルチホスト]**：ポートごとに複数のホストを使用できますが、最初の1つだけが認証されます。
- **[単一ホスト]**：ポートごとに 1 個のホストのみ許可します。

d) デバイスが 802.1X をサポートしていない場合は、[MAC Auth] フィールドで [EAP_FALLBACK_MAB] を選択し、[Submit] をクリックします。

ステップ 2 **802.1X ポート認証ポリシー**をファブリック アクセス グループに関連付けるには、**[Fabric]** > **[External Access Policies]** > **[Interfaces]** > **[Leaf Interfaces]** > **[Policy Groups]** > **[Leaf Access Port]** に移動し、次の操作を行います。

a) **[リーフ アクセス ポート]** を右クリックして、**[リーフ アクセス ポート ポリシー グループの作成]** を開きます。

b) [Name] フィールドにポリシーの名前を入力します。
c) [802.1X Port Authentication Policy] フィールドで、以前に作成したポリシーを選択し、[Submit] をクリックします。

APIC GUI を使用した 802.1X ノード認証の設定

始める前に

RADIUS プロバイダのポリシーを設定します。

ステップ 1 メニュー バーで、**[Fabric]** > **[External Access Policies]** > **[Policies]** > **[Switch]** > **[802.1X Node Authentication]** をクリックし、次の操作を行います。
a) [802.1X Node Authentication] を右クリックして、[Create 802.1X Node Authentication Policy] を開きます。
b) [Name] フィールドにポリシーの名前を入力します。
c) **[EPG 認証の失敗]** フィールドで、認証が失敗した場合に展開するテナント、アプリケーションプロファイル、EPG を選択します。
d) **[VLAN 認証の失敗]** で、認証が失敗した場合に展開する VLAN を選択します。

ステップ 2 **802.1X ノード認証ポリシー**をリーフ スイッチ ポリシー グループに関連付けるには、**[Fabric]** > **[External AccessPolicies]** > **[Switches]** > **[Leaf Switches]** > **[Policy Groups]** に移動し、次の操作を行います。
a) **[ポリシー グループ]** を右クリックして、**[アクセス スイッチ ポリシー グループの作成]** を開きます。
b) [Name] フィールドにポリシーの名前を入力します。
c) [802.1X Node Authentication Policy] フィールドで、以前に作成したポリシーを選択し、[Submit] をクリックします。

ステップ 3 **802.1X ノード認証ポリシー**をリーフインターフェイス プロファイルに関連付けるには、**[Fabric]** > **[External AccessPolicies]** > **[Interfaces]** > **[Leaf Interfaces]** > **[Profiles]** に移動し、次の操作を行います。
a) **[プロファイル]** を右クリックして、**[リーフ インターフェイス プロファイルの作成]** を開きます。
b) [Name] フィールドにポリシーの名前を入力します。
c) **[インターフェイス セレクタ]** 表を展開し、**[アクセス ポート セレクタの作成]** ダイアログ ボックスを開き、**[名前]** および **[インターフェイス ID]** 情報を入力します。
d) **[インターフェイス ポリシー グループ]** フィールドで、以前に作成されたポリシーを選択し、**[OK]** および **[送信]** をクリックします。

NX-OS スタイル CLI を使用した 802.1X ポート認証の設定

ステップ 1 ポリシー グループを設定します。

例：

```
apic1# configure
apic1(config)#
apic1(config)# template policy-group mypol
apic1(config-pol-grp-if)# switchport port-authentication mydot1x
apic1(config-port-authentication)# host-mode multi-host
apic1(config-port-authentication)# no shutdown
apic1(config-port-authentication)# exit
apic1(config-pol-grp-if)# exit
```

ステップ 2 リーフ インターフェイス ポリシーを設定します。

例：

```
apic1(config)#
apic1(config)#leaf-interface-profile myprofile
apic1(config-leaf-if-profile)#leaf-interface-group mygroup
apic1(config-leaf-if-group)# interface ethernet 1/10-12
apic1(config-leaf-if-group)# policy-group mypol
apic1(config-leaf-if-group)# exit
apic1(config-leaf-if-profile)# exit
```

ステップ 3 リーフ プロファイルを設定します。

例：

```
apic1(config)#
apic1(config)# leaf-profile myleafprofile
apic1(config-leaf-profile)# leaf-group myleafgrp
apic1(config-leaf-group)# leaf 101
apic1(config-leaf-group)# exit
```

ステップ 4 リーフ スイッチ プロファイルにインターフェイス ポリシーを適用します。

例：

```
apic1(config-leaf-profile)# leaf-interface-profile myprofile
apic1(config-leaf-group)# exit
```

NX-OS スタイル CLI を使用した 802.1X ノード認証の設定

ステップ 1 Radius 認証グループを設定します。

例：

```
apic1# configure
apic1(config)#
apic1(config)# aaa group server radius myradiusgrp
apic1(config-radius)#server 192.168.0.100 priority 1
apic1(config-radius)#exit
```

ステップ 2 ノード レベル ポート認証ポリシーを設定します。

例：

```
apic1(config)# policy-map type port-authentication mydot1x
```

```
apic1(config-pmap-port-authentication)#radius-provider-group myradiusgrp
apic1(config-pmap-port-authentication)#fail-auth-vlan 2001
apic1(config-pmap-port-authentication)#fail-auth-epg tenant tn1 application ap1 epg epg256
apic1(config)# exit
```

ステップ 3 ポリシー グループを設定し、グループ内でポート認証ポリシーを指定します。

例：

```
apic1(config)#template leaf-policy-group lpg2
apic1(config-leaf-policy-group)# port-authentication mydot1x
apic1(config-leaf-policy-group)#exit
```

ステップ 4 リーフ スイッチ プロファイルを設定します。

例：

```
apic1(config)# leaf-profile mylp2
apic1(config-leaf-profile)#leaf-group mylg2
apic1(config-leaf-group)#  leaf-policy-group lpg2
apic1(config-leaf-group)#exit
```

REST API を使用した 802.1X ポート認証の設定

802.1X ポート認証ポリシーを作成します。

例：

```
<polUni>
<infraInfra>
  <l2PortAuthPol adminSt="enabled" annotation="" descr="" dn="uni/infra/portauthpol-test21"
hostMode="multi-auth" name="test21" nameAlias="" ownerKey="" ownerTag="">
    <l2PortAuthCfgPol annotation="" macAuth="bypass" maxReauthReq="2" maxReq="2"   reAuthPeriod="3600"
 serverTimeout="30" suppTimeout="30" txPeriod="30"/>
  </l2PortAuthPol>
</infraInfra>
</polUni>

Modify:
<polUni>
<infraInfra>
  <l2PortAuthPol adminSt="enabled" annotation="" descr="" dn="uni/infra/portauthpol-test21"
hostMode="multi-domain" name="test21" nameAlias="" ownerKey="" ownerTag="" >
    <l2PortAuthCfgPol annotation="" macAuth="eap" maxReauthReq="2" maxReq="2"   reAuthPeriod="3600"
 serverTimeout="30" suppTimeout="30" txPeriod="30"/>
  </l2PortAuthPol>
</infraInfra>
</polUni>

Delete:
<polUni>
<infraInfra>
  <l2PortAuthPol adminSt="enabled" annotation="" descr="" dn="uni/infra/portauthpol-test21"
hostMode="multi-host" name="test21" nameAlias="" ownerKey="" ownerTag="" status="deleted">
    <l2PortAuthCfgPol annotation="" macAuth="bypass" maxReauthReq="2" maxReq="2"   reAuthPeriod="3600"
 serverTimeout="30" suppTimeout="30" txPeriod="30" status="deleted"/>
  </l2PortAuthPol>
```

```
</infraInfra>
</polUni>
```

REST API を使用した 802.1X ノード認証の設定

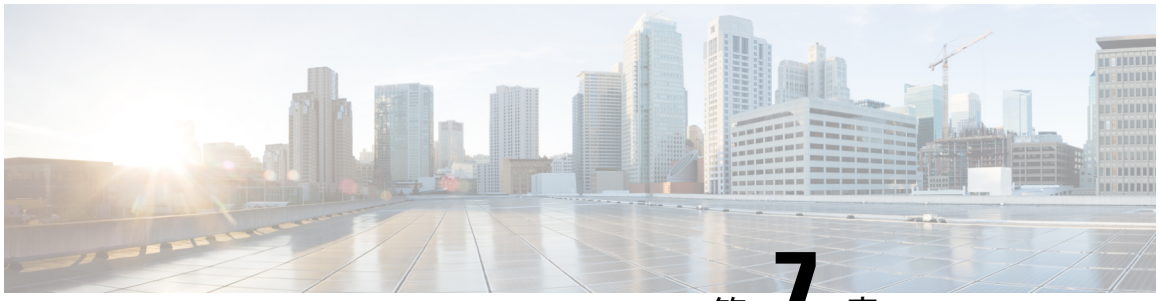
802.1X ノード認証ポリシーを設定します。

例：

```
<polUni>
<infraInfra>
  <l2NodeAuthPol annotation="" descr="" dn="uni/infra/nodeauthpol-802-node-2"
failAuthEpg="tn-t2,ap-ap,epg-epg1" failAuthVlan="vlan-2078" name="802-node-2" nameAlias="" ownerKey=""
 ownerTag="">
<l2RsAaaRadiusProviderGroup annotation="" tDn="uni/userext/radiusext/radiusprovidergroup-radius-grp"/>
</l2NodeAuthPol>
</infraInfra>
</polUni>

Modify:
<polUni>
<infraInfra>
  <l2NodeAuthPol annotation="" descr="" dn="uni/infra/nodeauthpol-802-node-2"
failAuthEpg="tn-t2,ap-ap,epg-epg1" failAuthVlan="vlan-2066" name="802-node-2" nameAlias="" ownerKey=""
 ownerTag="" status="deleted">
<l2RsAaaRadiusProviderGroup annotation="" tDn="uni/userext/radiusext/radiusprovidergroup-radius-grp"/>
</l2NodeAuthPol>
</infraInfra>
</polUni>

Delete:
<polUni>
<infraInfra>
  <l2NodeAuthPol annotation="" descr="" dn="uni/infra/nodeauthpol-802-node-2"
failAuthEpg="tn-t2,ap-ap,epg-epg1" failAuthVlan="vlan-2078" name="802-node-2" nameAlias="" ownerKey=""
 ownerTag="" status="deleted">
<l2RsAaaRadiusProviderGroup annotation="" tDn="uni/userext/radiusext/radiusprovidergroup-radius-grp"
 status="deleted"/>
</l2NodeAuthPol>
</infraInfra>
</polUni>
```



第 7 章

ポート セキュリティ

この章は、次の項で構成されています。

ポート セキュリティと ACI について

ポート セキュリティ機能は、ポートごとに取得される MAC アドレスの数を制限することによって、不明な MAC アドレスでフラッディングしないように ACI ファブリックを保護します。ポート セキュリティ機能のサポートは、物理ポート、ポート チャネル、および仮想ポート チャネルで使用できます。

ポート セキュリティに関するガイドラインと制約事項

次のようなガイドラインと制約事項があります。

- ポート セキュリティは、ポートごとに使用できます。
- ポートセキュリティは、物理ポート、ポートチャネル、および仮想ポートチャネル（vPC）でサポートされています。
- スタティック MAC アドレスとダイナミック MAC アドレスがサポートされています。
- セキュアなポートからセキュアでないポートへと、セキュアでないポートからセキュアなポートへの MAC アドレスの移動がサポートされています。
- MAC アドレスの制限は、MAC アドレスにのみ適用され、MAC と IP によるアドレスには実行されません。

- ポート セキュリティは、ファブリック エクステンダ（FEX）ではサポートされていません。

ポート レベルでのポート セキュリティ

APICでは、ユーザがスイッチポートのポートセキュリティを設定できます。ポート上でMACが制限の最大設定値を超過すると、超過したMACアドレスからすべてのトラフィックが転送されます。次の属性がサポートされます。

- **ポート セキュリティのタイムアウト** ：現在サポートされているタイムアウト値値は、60 ~ 3600 秒の範囲でサポートされています。
- **違反行為**：違反行為は保護モードで使用できます。保護モードでは、MACの取得が無効になるため、MACアドレスはCAMテーブルに追加されません。Macラーニングが設定されているタイムアウト値の後に再度有効になります。
- **最大エンドポイント** ：現在のサポートされている最大のエンドポイント設定値は、0 ～ 12000 の範囲でサポートされています。最大エンドポイント値が 0 の場合、そのポートではポート セキュリティ ポリシーが無効になります。

APIC GUI を使用したポート セキュリティの設定

ステップ 1 メニュー バーで [ファブリック アクセス ポリシー（**Fabric** > **Access Policies**）] をクリックし、[ナビゲーション（**Navigation**）] ペインで [ポリシー インターフェイス ポート セキュリティ（**Policies** > **Interface** > **Port Security**）] を展開します。

ステップ 2 **[ポート セキュリティ]** 右クリックして、**[ポート セキュリティ ポリシーの作成]** をクリックします。

ステップ 3 **[ポート セキュリティ ポリシーの作成]** ダイアログ ボックスで、次の操作を実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) **[ポート セキュリティのタイムアウト]** フィールドに、インターフェイスの MAC ラーニングを再度有効にする前に、タイムアウトの値を選択します。
c) **[最大エンドポイント]** フィールドに、インターフェイスで学習可能なエンドポイントの最大数の希望値を選択します。
d) **[違反アクション]** フィールドで、使用可能なオプションは **[保護]** です。[Submit] をクリックします。ポート セキュリティ ポリシーが作成されます。

ステップ 4 （注） リーフスイッチのインターフェイスを設定するときに、使用可能なポートセキュリティポリシーのリストからポート セキュリティ ポリシーを選択することができます。

[ナビゲーション] ペインで、**[ファブリック]**>**[インベントリ]**>**[トポロジ]** をクリックし、目的のリーフ スイッチに移動します。インターフェイスを設定する適切なポートを選択し、ポートセキュリティポリシードロップダウン リストから関連付けに必要なポート セキュリティ ポリシーを選択します。

これで、ポート上のポート セキュリティの設定を完了します。

REST API を使用して、ポート セキュリティの設定

ポート セキュリティを設定します。

例：

```
<polUni>
 <infraInfra>

   <l2PortSecurityPol name="testL2PortSecurityPol" maximum="10" violation=”protect” timeout=“300"/>


    <infraNodeP name="test">
        <infraLeafS name="test" type="range">
            <infraNodeBlk name="test" from_="101" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-test"/>
    </infraNodeP>

            <infraAccPortP name="test">
        <infraHPortS name="pselc" type="range">
           <infraPortBlk name="blk"
                                 fromCard="1" toCard="1" fromPort="20" toPort="22">
                 </infraPortBlk>
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-testPortG" />
         </infraHPortS>
            </infraAccPortP>

            <infraFuncP>
            <infraAccPortGrp name="testPortG">
                <infraRsL2PortSecurityPol tnL2PortSecurityPolName="testL2PortSecurityPol"/>
                <infraRsAttEntP tDn="uni/infra/attentp-test" />
            </infraAccPortGrp>
            </infraFuncP>

    <infraAttEntityP name="test">
        <infraRsDomP tDn="uni/phys-mininet"/>
    </infraAttEntityP>
 </infraInfra>
</polUni>
```

CLI を使用したポート セキュリティの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例：	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
	`apic1# configure`	
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	設定するリーフを指定します。
ステップ 3	**interface** *type-or-range* 例： `apic1(config-leaf)# interface eth 1/2-4`	設定するインターフェイスまたはインターフェイスの範囲を指定します。
ステップ 4	[**no**] **switchport port-security maximum** *number-of-addresses* 例： `apic1(config-leaf-if)# switchport port-security maximum 1`	インターフェイスのセキュア MAC アドレスの最大数を設定します。範囲は 0 ～ 12000 アドレスです。デフォルトは 1 アドレスです。
ステップ 5	[**no**] **switchport port-security violation protect** 例： `apic1(config-leaf-if)# switchport port-security violation protect`	セキュリティ違反が検出された場合に実行するアクションを設定します。**protect** アクションは、十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、不明な送信元アドレスのパケットをドロップします。
ステップ 6	[**no**] **switchport port-security timeout** 例： `apic1(config-leaf-if)# switchport port-security timeout 300`	インターフェイスのタイムアウト値を設定します。範囲は 60 ～ 3600 です。デフォルトは 60 秒です。

例

次に、イーサネットインターフェイスでポートセキュリティを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface eth 1/2
apic1(config-leaf-if)# switchport port-security maximum 10
apic1(config-leaf-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

次に、ポート チャネルでポート セキュリティを設定する例を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po2
apic1(config-leaf-if)# switchport port-security maximum 10
apic1(config-leaf-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

次に、仮想ポートチャネル（VPC）でポートセキュリティを設定する例を示します。

```
apic1# configure
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config-vpc)# exit
apic1(config)# template port-channel po4
apic1(config-if)# exit
apic1(config)# leaf 101-102
apic1(config-leaf)# interface eth 1/11-12
apic1(config-leaf-if)# channel-group po4 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc po4
apic1(config-vpc-if)# switchport port-security maximum 10
apic1(config-vpc-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

ポート セキュリティおよびラーニング動作

非 vPC ポートまたはポート チャネルでは、新しいエンドポイントに対して学習イベントが発生し、新しい学習が許可されているか確認する検証が行われます。対応するインターフェイスに設定されていない、または無効なポート セキュリティ ポリシーが存在する場合、エンドポイントラーニング動作はサポートされているものから変更されません。ポリシーが有効になっており制限に到達している場合、現在のサポートされているアクションは次の通りです。

- エンドポイントを学習し、ドロップ アクションのハードウェアにインストールします。
- サイレントに学習を破棄します。

制限に到達していない場合、エンドポイントが学習され、この新しいエンドポイントが発生したため制限に達しているかどうか確認する検証が行われます。制限に到達しており、学習の無効化アクションが設定されている場合、インターフェイス上のハードウェアでラーニングが無効になります（物理インターフェイスまたはポートチャネルまたはvPC）。制限に到達しており、学習の無効化アクションが設定されていない場合、エンドポイントはドロップアクションでハードウェアにインストールされます。このようなエンドポイントは、他のエンドポイントのように通常期限切れです。

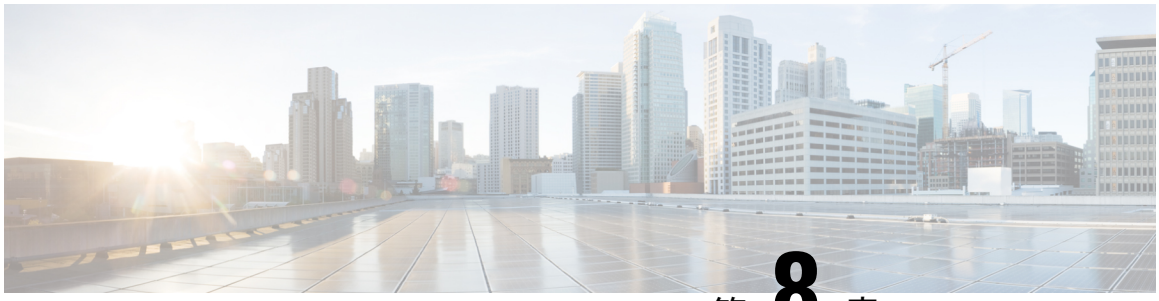
初めて制限に達したとき、ポート セキュリティ ポリシー オブジェクトの動作状態がそれを反映して更新されます。スタティック ルールは、ユーザーに警告ができるように、障害の発生と定義されます。制限に到達すると、Syslog も発生します。

vPCの場合、MAC 制限に到達するとピア リーフ スイッチにも通知されるため、ラーニングがピアで無効になる可能性があります。vPC ピアはいつでも再起動でき、vPC レッグが動作不能になるか再起動できるため、この状態はピアと調和して vPC ピアはこの状態に同期されません。同期しない場合は、1 個のレッグでラーニングが有効になり、他のレッグで無効になる状況が発生する可能性があります。

デフォルトでは、制限に到達してラーニングが無効になると、60 秒のデフォルト タイムアウト値の後、自動的に再度有効になります。

保護モード

保護モードはセキュリティ違反を発生している以上に増やさないようにします。MAC の制限がポートで設定されている最大値を超えると、超過したMACアドレスからすべてのトラフィックはドロップされ、さらにラーニングが無効になります。



第 8 章

ファーストホップ セキュリティ

この章は、次の項で構成されています。

ファースト ホップ セキュリティについて

ファーストホップセキュリティ（FHS）機能では、レイヤ2リンク上でより優れたIPv4とIPv6のリンク セキュリティおよび管理が可能になります。サービス プロバイダ環境で、これらの機能は重複アドレス検出（DAD）とアドレス解像度（AR）などのアドレス割り当てや派生操作が、より緊密に制御可能です。

次のサポートされている FHS 機能はプロトコルをセキュアにして、ファブリック リーフ スイッチにセキュアなエンドポイント データベースを構築するのに役立ち、MIM 攻撃や IP の盗難などのセキュリティ盗難を軽減するために使用されます。

- ARP 検査：ネットワーク管理者は、無効なMACアドレスからIPアドレスへのバインディングがある ARP パケットを代行受信、記録、およびドロップすることができます。
- ND 検査：レイヤ 2 ネイバー テーブルでステートレス自動設定アドレスのバインディングを学習し、保護します。
- DHCP 検査：信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- RA ガード：ネットワーク管理者は、不要または不正なルータ アドバタイズメント（RA）ガード メッセージをブロックまたは拒否できます。
- IPv4 および IPv6 ソース ガード—不明なソースからのデータ トラフィックをすべてブロックします。

- 信頼制御：信頼できる送信元はその企業の管理制御下にあるデバイスです。これらのデバイスには、ファブリック内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

FHS 機能は、次のセキュリティ対策を提供します。

- **ロールの適用**：信頼できない主催者が、そのロールの有効範囲を超えるメッセージを送信することを防ぎます。
- **バインディングの適用**：アドレスの盗難を防止します。
- **DoS 攻撃の軽減対策**：悪意あるエンドポイントを防ぎ、データベースが操作サービスを提供することを停止するポイントにエンドポイント データベースを成長させます。
- **プロキシ サービス**：アドレス解決の効率を高めるため一部のプロキシ サービスを提供します。

FHS機能は、テナントブリッジドメイン（BD）ごとに有効になっています。ブリッジドメインとして、単一または複数のリーフ スイッチで展開可能で、FHS 脅威の制御と軽減のメカニズムは単一のスイッチと複数のスイッチのシナリオにも対応できます。

ACI FHS の導入

ほとんどの FHS 機能はツーステップ傾向で設定されています。最初に機能の動作を説明するポリシーを定義し、次にこのポリシーを「ドメイン」に適用します（テナント ブリッジ ドメインまたはテナント エンドポイント グループになる）。異なる動作を定義する別のポリシーは、さまざまな交差ドメインに適用できます。特定のポリシーを使用する決定は、ポリシーを適用するもっとも明確なドメインで行われます。

ポリシーのオプションは、[Tenant_*name*]>[Networking]>[Protocol Policies]>[First Hop Security] タブの下にある Cisco APIC GUI から定義できます。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- リリース 3.1 (1) より、仮想エンドポイント（AV のみ）で FHS はサポートされています。
- FHS は、VLAN と VXLAN の両方のカプセル化でサポートされています。
- **[ダウン]** 状態の FHS バインディング表データベースでセキュリティ保護されたエンドポイント エントリは、タイムアウトから **18 時間** 後に消去されます。エントリが学習する前面パネル ポートがリンク ダウンする場合、エントリは **[ダウン]** 状態に移動します。この **18 時間** ウィンドウの中で、エンドポイントが別のロケーションに移動し別のポートで確認される場合、エンドポイントが他のポートから到達可能な限り移行され、エントリはグレースフルに **[ダウン]** 状態から **[REACHABLE/STALE]** に移行します。

- IP 発信元ガードが有効な時、IP 送信元アドレスとして Ipv6 リンク ローカル アドレスを使用して供給される Ipv6 トラフィックは、IP 送信元ガード施行を受けません（例：送信元 MAC の施行 <=> IP 調査機能によりセキュリティ保護された送信元 IP バインディング）。バインディング チェック障害に関係なく、デフォルトでこのトラフィックが許可されます。
- L3Out インターフェイスでは、FHS はサポートされていません。
- TOR に基づいて N9K-M12PQ では FHS はサポートされていません。
- ACI マルチサイトの FHS はサイトのローカル機能であるため、APIC クラスタからサイトでのみ有効にできます。また、ACI マルチサイトの FHS は、BD や EPG がサイト ローカルであり、サイト上でストレッチしない場合にのみ動作します。ストレッチ BD または EPG の FHS セキュリティを有効にすることはできません。
- レイヤ 2 専用ブリッジ ドメインでは、FHS はサポートされていません。
- FHS の有効化機能ではトラフィックが 50 秒間中断することがあります。これは、BD 内の EP がフラッシュされ、BD 内の EP ラーニングが 50 秒間無効になるためです。

APIC GUI を使用して FHS の設定

始める前に

- テナントとブリッジ ドメインが設定されています。

ステップ 1 メニューバーで、**[テナント]** > **[Tenant_name]** をクリックします。**[ナビゲーション]** ペインで、**[ポリシー]** > **[プロトコル]** > **[最初のホップ セキュリティ]** をクリックします。**[最初のホップ セキュリティ]** を右クリックして **[機能ポリシーの作成]** を開き、次の操作の実行します。

a) **[名前]** フィールドにホップ セキュリティ セキュリティ ポリシーの名前を入力します。

b) **[IP 検査]**、**[送信元ガード]**、**[ルータ アドバタイズメント]** フィールドが有効になっていることを確認し、**[提出]** をクリックします。

ステップ 2 **[ナビゲーション]** ペインで、**[最初のホップ セキュリティ]** を展開し、**[制御ポリシーの信頼]** を右クリックして**[信頼制御ポリシーの作成]** を開いて次のアクションを実行します。

a) **[名前]** フィールドに信頼制御ポリシーの名前を入力します。

b) ポリシーで許可する機能を選択し、**[提出]** をクリックします。

ステップ 3 （オプション）EPG に信頼制御ポリシーを適用するには、[Navigation] ペインで、**[Application Profiles]** > **[ApplicationProfile_*name*]** > **[Application EPGs]** を展開し、**[Application EPG_*name*]** をクリックして、次の操作を行います。

a) **[作業]** ペインで、**[全般]** タブをクリックします。

b) **[FHS 信頼制御ポリシー]** の下矢印をクリックして、以前作成したポリシーを選択し、**[提出]** をクリックします。

ステップ 4 **[ナビゲーション]** ペインで、**[ブリッジ ドメイン]** > **[ブリッジ ドメイン名]** を展開して、**[アドバンスト/トラブルシューティング]** タブをクリックして、次のアクションを実行します。

a) **[ホップの最初のセキュリティ ポリシー]** フィールドで、作成したポリシーを選択し、**[提出]** をクリックします。これで FHS 設定を完了します。

NX-OS CLI を使用した FHS の設定

始める前に

- テナントとブリッジ ドメインが設定されています。

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 FHS ポリシーを設定します。

例：

```
apic1(config)# tenant coke
apic1(config-tenant)# first-hop-security
apic1(config-tenant-fhs)# security-policy pol1
apic1(config-tenant-fhs-secpol)#
apic1(config-tenant-fhs-secpol)# ip-inspection-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# source-guard-admin-status enabled-both
apic1(config-tenant-fhs-secpol)# router-advertisement-guard-admin-status enabled
apic1(config-tenant-fhs-secpol)# router-advertisement-guard
apic1(config-tenant-fhs-raguard)#
apic1(config-tenant-fhs-raguard)# managed-config-check
apic1(config-tenant-fhs-raguard)# managed-config-flag
apic1(config-tenant-fhs-raguard)# other-config-check
apic1(config-tenant-fhs-raguard)# other-config-flag
apic1(config-tenant-fhs-raguard)# maximum-router-preference low
apic1(config-tenant-fhs-raguard)# minimum-hop-limit 10
apic1(config-tenant-fhs-raguard)# maximum-hop-limit 100
apic1(config-tenant-fhs-raguard)# exit
apic1(config-tenant-fhs-secpol)# exit
apic1(config-tenant-fhs)# trust-control tcpol1
pic1(config-tenant-fhs-trustctrl)# arp
apic1(config-tenant-fhs-trustctrl)# dhcpv4-server
apic1(config-tenant-fhs-trustctrl)# dhcpv6-server
apic1(config-tenant-fhs-trustctrl)# ipv6-router
apic1(config-tenant-fhs-trustctrl)#  router-advertisement
apic1(config-tenant-fhs-trustctrl)# neighbor-discovery
apic1(config-tenant-fhs-trustctrl)# exit
apic1(config-tenant-fhs)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# first-hop-security security-policy pol1
apic1(config-tenant-bd)# exit
```

```
apic1(config-tenant)# application ap1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# first-hop-security trust-control tcpol1
```

ステップ 3 FHS の設定例を示します。

例：

```
leaf4# show fhs bt all

Legend:
    TR       : trusted-access                        UNRES : unresolved              Age    : Age
since creation
    UNTR     : untrusted-access                     UNDTR : undetermined-trust      CRTNG : creating

    UNKNW    : unknown                               TENTV : tentative               INV    : invalid

    NDP      : Neighbor Discovery Protocol          STA   : static-authenticated    REACH : reachable

    INCMP    : incomplete                           VERFY : verify                  INTF  : Interface

    TimeLeft : Remaining time since last refresh    LM    : lla-mac-match           DHCP  :
dhcp-assigned

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID              BD-Vlan             BD-Name
15630220             3                   t0:bd200

-------------------------------------------------------------------------------------------------------------
| Origin | IP              | MAC               | INTF   | EPG(sclass)(mode) | Trust-lvl | State |
Age      | TimeLeft |
-------------------------------------------------------------------------------------------------------------
| ARP    | 192.0.200.12    | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)  | LM,TR     | STALE |
00:04:49 | 18:08:13 |
| ARP    | 172.29.205.232  | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)  | LM,TR     | STALE |
00:03:55 | 18:08:21 |
| ARP    | 192.0.200.21    | D0:72:DC:A0:3D:4F | eth1/1 | epg300(49154)(V)  | LM,TR     | REACH |
00:03:36 | 00:00:02 |
| LOCAL  | 192.0.200.1     | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       | REACH |
04:49:41 | N/A      |
| LOCAL  | fe80::200       | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       | REACH |
04:49:40 | N/A      |
| LOCAL  | 2001:0:0:200::1 | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       | REACH |
04:49:39 | N/A      |
-------------------------------------------------------------------------------------------------------------
```

信頼レベルは次のとおりです。

- **TR**：信頼されています。エンドポイントが、信頼設定が有効になっている EPG から学習されたときに表示されます。
- **UNTR**：信頼できません。エンドポイントが、信頼設定が有効になっていない EPG から学習されたときに表示されます。
- **UNDTR**：未定。DHCP サーバー ブリッジ ドメイン（BD）がリモート リーフにあり、DHCP クライアントがローカル リーフにある DHCP リレー トポロジの場合に表示されます。この状況では、ローカル リーフは、DHCP サーバー BD が信頼 DHCP を有効にしているかどうかを認識しません。

ステップ 4 さまざまなタイプと理由の例とともに違反を表示します。

例：

```
leaf4# show fhs violations all

Violation-Type:
    POL  : policy      THR : address-theft-remote
    ROLE : role        TH  : address-theft
    INT  : internal

Violation-Reason:
    IP-MAC-TH   : ip-mac-theft                    OCFG_CHK  : ra-other-cfg-check-fail     ANC-COL
    : anchor-collision
    PRF-LVL-CHK : ra-rtr-pref-level-check-fail    INT-ERR   : internal-error              TRUST-CHK
   : trust-check-fail
    SRV-ROL-CHK : srv-role-check-fail            ST-EP-COL : static-ep-collision         LCL-EP-COL
  : local-ep-collision
    MAC-TH      : mac-theft                       EP-LIM    : ep-limit-reached            MCFG-CHK
    : ra-managed-cfg-check-fail
   HOP-LMT-CHK : ra-hoplimit-check-fail         MOV-COL   : competing-move-collision    RTR-ROL-CHK
 : rtr-role-check-fail
    IP-TH       : ip-theft

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            3                   t0:bd200
-------------------------------------------------------------------------------------------------------
| Type | Last-Reason | Proto | IP           | MAC               | Port    | EPG(sclass)(mode) |
Count |
-------------------------------------------------------------------------------------------------------
| THR  | IP-TH       | ARP   | 192.0.200.21 | D0:72:DC:A0:3D:4F | tunnel5 | epg300(49154)(V)  | 21
    |
-------------------------------------------------------------------------------------------------------
Table Count: 1
```

ステップ 5 FHS 設定の表示:

例：

```
swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security binding-table

Pod/Node  Type    Family  IP Address            MAC Address        Interface     Level
State
--------  ------  ------  --------------------  -----------------  ------------  ---------------
-----
1/102     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
 able
1/102     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
 able
1/102     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
 able
1/101     arp     ipv4    192.0.200.23          D0:72:DC:A0:02:61  eth1/2        lla-mac-match
stale
                                                                                 ,untrusted-
                                                                                 access
1/101     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan3         static-
reach
                                                                                 authenticated
```

```
 able
1/101     nd      ipv6    fe80::d272:dcff:fea0  D0:72:DC:A0:02:61  eth1/2        lla-mac-match
reach
                           :261                                                  ,untrusted-
 able                                                                            access
1/101     nd      ipv6    2001:0:0:200::20      D0:72:DC:A0:02:61  eth1/2        lla-mac-match
stale                                                                            ,untrusted-
                                                                                 access
1/101     nd      ipv6    2001::200:d272:dcff:  D0:72:DC:A0:02:61  eth1/2        lla-mac-match
stale
                           fea0:261                                              ,untrusted-
                                                                                 access
1/101     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan3         static-
reach                                                                            authenticated
 able
1/101     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan3         static-
reach                                                                            authenticated
 able
1/103     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan4         static-
reach                                                                            authenticated
 able
1/103     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan4         static-
reach                                                                            authenticated
 able
1/103     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan4         static-
reach                                                                            authenticated
 able
1/104     arp     ipv4    192.0.200.10          F8:72:EA:AD:C4:7C  eth1/1        lla-mac-match
stale                                                                            ,trusted-access
1/104     arp     ipv4    172.29.207.222        D0:72:DC:A0:3D:4C  eth1/1        lla-mac-match
stale                                                                            ,trusted-access
1/104     local   ipv4    192.0.200.1           00:22:BD:F8:19:FF  vlan4         static-
reach                                                                            authenticated
 able
1/104     nd      ipv6    fe80::fa72:eaff:fead  F8:72:EA:AD:C4:7C  eth1/1        lla-mac-match
stale
                           :c47c                                                 ,trusted-access
1/104     nd      ipv6    2001:0:0:200::10      F8:72:EA:AD:C4:7C  eth1/1        lla-mac-match
stale                                                                            ,trusted-access
1/104     local   ipv6    fe80::200             00:22:BD:F8:19:FF  vlan4         static-
reach                                                                            authenticated
 able
1/104     local   ipv6    2001:0:0:200::1       00:22:BD:F8:19:FF  vlan4         static-
reach                                                                            authenticated
 able


Pod/Node  Type    IP Address            Creation TS                    Last Refresh TS
    Lease Period
--------  ------  --------------------  -----------------------------  -----------------------------
  ------------
```

```
1/102     local   192.0.200.1           2017-07-20T04:22:38.000+00:00  2017-07-20T04:22:38.000+00:00
1/102     local   fe80::200             2017-07-20T04:22:56.000+00:00  2017-07-20T04:22:56.000+00:00
1/102     local   2001:0:0:200::1       2017-07-20T04:22:57.000+00:00  2017-07-20T04:22:57.000+00:00
1/101     arp     192.0.200.23          2017-07-27T10:55:20.000+00:00  2017-07-27T16:07:24.000+00:00
1/101     local   192.0.200.1           2017-07-27T10:48:09.000+00:00  2017-07-27T10:48:09.000+00:00
1/101     nd      fe80::d272:dcff:fea0  2017-07-27T10:52:16.000+00:00  2017-07-27T16:04:29.000+00:00

                    :261
1/101     nd      2001:0:0:200::20      2017-07-27T10:57:32.000+00:00  2017-07-27T16:07:24.000+00:00
1/101     nd      2001::200:d272:dcff:  2017-07-27T11:21:45.000+00:00  2017-07-27T16:07:24.000+00:00

                    fea0:261
1/101     local   fe80::200             2017-07-27T10:48:10.000+00:00  2017-07-27T10:48:10.000+00:00
1/101     local   2001:0:0:200::1       2017-07-27T10:48:11.000+00:00  2017-07-27T10:48:11.000+00:00
1/103     local   192.0.200.1           2017-07-26T22:03:56.000+00:00  2017-07-26T22:03:56.000+00:00
1/103     local   fe80::200             2017-07-26T22:03:57.000+00:00  2017-07-26T22:03:57.000+00:00
1/103     local   2001:0:0:200::1       2017-07-26T22:03:58.000+00:00  2017-07-26T22:03:58.000+00:00
1/104     arp     192.0.200.10          2017-07-27T11:21:13.000+00:00  2017-07-27T16:05:48.000+00:00
1/104     arp     172.29.207.222        2017-07-27T11:54:48.000+00:00  2017-07-27T16:06:38.000+00:00
1/104     local   192.0.200.1           2017-07-27T10:49:13.000+00:00  2017-07-27T10:49:13.000+00:00
1/104     nd      fe80::fa72:eaff:fead  2017-07-27T11:21:13.000+00:00  2017-07-27T16:06:43.000+00:00

                    :c47c
1/104     nd      2001:0:0:200::10      2017-07-27T11:21:13.000+00:00  2017-07-27T16:06:19.000+00:00
1/104     local   fe80::200             2017-07-27T10:49:14.000+00:00  2017-07-27T10:49:14.000+00:00
1/104     local   2001:0:0:200::1       2017-07-27T10:49:15.000+00:00  2017-07-27T10:49:15.000+00:00


swtb23-ifc1#

swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics arp
Pod/Node          : 1/101
Request Received : 4
Request Switched : 2
Request Dropped  : 2
Reply Received   : 257
Reply Switched   : 257
Reply Dropped    : 0

Pod/Node          : 1/104
Request Received : 6
Request Switched : 6
Request Dropped  : 0
Reply Received   : 954
Reply Switched   : 954
Reply Dropped    : 0


swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics dhcpv4
Pod/Node                    : 1/102
Discovery Received          : 5
Discovery Switched          : 5
Discovery Dropped           : 0
Offer Received              : 0
Offer Switched              : 0
Offer Dropped               : 0
Request Received            : 0
Request Switched            : 0
Request Dropped             : 0
Ack Received                : 0
Ack Switched                : 0
Ack Dropped                 : 0
Nack Received               : 0
Nack Switched               : 0
```

```
Nack Dropped                : 0
Decline Received            : 0
Decline Switched            : 0
Decline Dropped             : 0
Release Received            : 0
Release Switched            : 0
Release Dropped             : 0
Information Received        : 0
Information Switched        : 0
Information Dropped         : 0
Lease Query Received        : 0
Lease Query Switched        : 0
Lease Query Dropped         : 0
Lease Active Received       : 0
Lease Active Switched       : 0
Lease Active Dropped        : 0
Lease Unassignment Received : 0
Lease Unassignment Switched : 0
Lease Unassignment Dropped  : 0
Lease Unknown Received      : 0
Lease Unknown Switched      : 0
Lease Unknown Dropped       : 0

swtb23-ifc1# show tenant t0 bridge-domain bd200 first-hop-security statistics neighbor-discovery
Pod/Node                        : 1/101
Neighbor Solicitation Received  : 125
Neighbor Solicitation Switched  : 121
Neighbor Solicitation Dropped   : 4
Neighbor Advertisement Received : 519
Neighbor Advertisement Switched : 519
Neighbor Advertisement Drop     : 0
Router Solicitation Received    : 4
Router Solicitation Switched    : 4
Router Solicitation Dropped     : 0
Router Adv Received             : 0
Router Adv Switched             : 0
Router Adv Dropped              : 0
Redirect Received               : 0
Redirect Switched               : 0
Redirect Dropped                : 0

Pod/Node                        : 1/104
Neighbor Solicitation Received  : 123
Neighbor Solicitation Switched  : 47
Neighbor Solicitation Dropped   : 76
Neighbor Advertisement Received : 252
Neighbor Advertisement Switched : 228
Neighbor Advertisement Drop     : 24
Router Solicitation Received    : 0
Router Solicitation Switched    : 0
Router Solicitation Dropped     : 0
Router Adv Received             : 53
Router Adv Switched             : 6
Router Adv Dropped              : 47
Redirect Received               : 0
Redirect Switched               : 0
Redirect Dropped                : 0
```

FHS スイッチ iBASH コマンド

ステップ 1 BD の FHS 機能設定と、EPG の信頼コントロール ポリシー設定を表示する show コマンド：

例：

```
leaf4# show fhs features all

BD-VNID             BD-Vlan             BD-Name
15630220            4                   t0:bd200
    Feature Policy:
        Feature      Family    Protocol    Operational-State    Options
        ipinspect    IPV4      ARP         UP                   stalelifetime: 180s
        ipinspect    IPV4      DHCP        UP                   -
        ipinspect    IPV4      LOCAL       UP                   -
        ipinspect    IPV4      STATIC      UP                   -
        ipinspect    IPV6      ND          UP                   stalelifetime: 180s
        ipinspect    IPV6      DHCP        UP                   -
        ipinspect    IPV6      LOCAL       UP                   -
        ipinspect    IPV6      STATIC      UP                   -
        raguard      IPV6      -           UP                   ManagedCfgFlag: on
                                                                OtherCfgFlag: on
                                                                maxHopLimit: 15
                                                                minHopLimit: 3
                                                                routerPref: medium
    ------------------------------------------------------------------------------------
    Trust Policy:
    Epg-id              Epg-type            Epg-name
    49154               Ckt-Vlan            epg300
        Trust-Attribute    Operational-State
        PROTO-ARP          UP
        PROTO-ND           UP
        DHCPV4-SERVER      UP
        DHCPV6-SERVER      UP
        ROUTER             UP
```

ステップ 2 FHS のセキュリティ保護されたエンドポイントのデータベースを表示する show コマンド：

例：

```
leaf1# show fhs bt
all       data      dhcpv4    local     static
arp       detailed  dhcpv6    nd        summary

leaf1# show fhs bt all

Legend:
    DHCP     : dhcp-assigned                      TR    : trusted-access         UNRES : unresolved

    Age      : Age since creation                  CRTNG : creating               TENTV : tentative

    VERFY    : verify                               UNDTR : undetermined-trust      INV   : invalid

    NDP      : Neighbor Discovery Protocol         STA   : static-authenticated    REACH : reachable

    LM       : lla-mac-match                       UNKNW : unknown                INTF  : Interface

    TimeLeft : Remaining time since last refresh    INCMP : incomplete              UNTR  :
untrusted-access
```

```
EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            3                   t0:bd200

-------------------------------------------------------------------------------------------------------------------
| Origin | IP                        | MAC               | INTF   | EPG(sclass)(mode) | Trust-lvl |
 State | Age      | TimeLeft |
-------------------------------------------------------------------------------------------------------------------
| ARP    | 192.0.200.23              | D0:72:DC:A0:02:61 | eth1/2 | epg200(32770)(V)  | LM,UNTR   |
 STALE | 00:07:47 | 00:01:33 |
| LOCAL  | 192.0.200.1               | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       |
 REACH | 00:14:58 | N/A      |
| NDP    | fe80::d272:dcff:fea0:261  | D0:72:DC:A0:02:61 | eth1/2 | epg200(32770)(V)  | LM,UNTR   |
 STALE | 00:10:51 | 00:00:47 |
| NDP    | 2001:0:0:200::20          | D0:72:DC:A0:02:61 | eth1/2 | epg200(32770)(V)  | LM,UNTR   |
 STALE | 00:05:35 | 00:00:42 |
| LOCAL  | fe80::200                 | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       |
 REACH | 00:14:58 | N/A      |
| LOCAL  | 2001:0:0:200::1           | 00:22:BD:F8:19:FF | vlan3  | LOCAL(16387)(I)   | STA       |
 REACH | 00:14:57 | N/A      |
-------------------------------------------------------------------------------------------------------------------


leaf1# show fhs bt summary all

--------------------------------------------------------------------------------
                          FHS Binding Table Summary
--------------------------------------------------------------------------------
BD-Vlan: 3        BD-Name: t0:bd200
    Total number of ARP entries       : 1
    Total number of DHCPv4 entries    : 0
    Total number of ND entries        : 2
    Total number of DHCPv6 entries    : 0
    Total number of Data entries      : 0
    Total number of Static entries    : 0
    Total number of Local entries     : 3
    Total number of entries           : 6
--------------------------------------------------------------------------------
Total entries across all BDs matching given filters
    Total number of ARP entries       : 1
    Total number of DHCPv4 entries    : 0
    Total number of ND entries        : 2
    Total number of DHCPv6 entries    : 0
    Total number of Data entries      : 0
    Total number of Static entries    : 0
    Total number of Local entries     : 3
    Total number of entries           : 6
--------------------------------------------------------------------------------
```

ステップ 3 FHS エンドポイントの違反を表示する show コマンド：

例：

```
leaf1# show fhs violations all

Violation-Type:
    POL  : policy      THR : address-theft-remote
    ROLE : role        TH  : address-theft
    INT  : internal

Violation-Reason:
    IP-MAC-TH   : ip-mac-theft                  OCFG_CHK  : ra-other-cfg-check-fail     ANC-COL
```

```
    : anchor-collision
    PRF-LVL-CHK : ra-rtr-pref-level-check-fail    INT-ERR   : internal-error              TRUST-CHK
   : trust-check-fail
    SRV-ROL-CHK : srv-role-check-fail            ST-EP-COL : static-ep-collision         LCL-EP-COL
  : local-ep-collision
    MAC-TH      : mac-theft                       EP-LIM    : ep-limit-reached            MCFG-CHK
    : ra-managed-cfg-check-fail
   HOP-LMT-CHK : ra-hoplimit-check-fail         MOV-COL   : competing-move-collision    RTR-ROL-CHK
 : rtr-role-check-fail
    IP-TH       : ip-theft

Trust-Level:
    TR   : trusted-access    UNTR : untrusted-access        UNDTR : undetermined-trust
    INV  : invalid           STA  : static-authenticated    LM    : lla-mac-match
    DHCP : dhcp-assigned

EPG-Mode:
    U : unknown    M : mac    V : vlan    I : ip

BD-VNID             BD-Vlan             BD-Name
15630220            4                   t0:bd200
-------------------------------------------------------------------------------------------------------------------
| Type | Last-Reason | Proto | IP                          | MAC               | Port    |
EPG(sclass)(mode) | Trust-lvl | Count |
-------------------------------------------------------------------------------------------------------------------
| TH   | IP-TH       | ND    | 2001:0:0:200::20          | D0:72:DC:A0:3D:4F | eth1/1 |
epg300(49154)(V)  | LM,UNTR   | 2     |
| POL  | HOP-LMT-CHK | RD    | fe80::fa72:eaff:fead:c47c | F8:72:EA:AD:C4:7C | eth1/1 |
epg300(49154)(V)  | LM,TR     | 2     |
-------------------------------------------------------------------------------------------------------------------
Table Count: 2
```

ステップ 4 FHS コントロール パケット転送カウンタを表示する show コマンド：

例：

```
leaf1# show fhs counters
all     arp     dhcpv4  dhcpv6  nd
leaf4# show fhs counters all

BD-VNID             BD-Vlan             BD-Name
15630220            4                   t0:bd200
 ---------------------------------------------------------------------------------------
| Counter Type           |            Received |            Switched |             Dropped |
|---------------------------------------------------------------------------------------|
| Arp Request            |                   6 |                   6 |                   0 |
| Arp Reply              |                  94 |                  94 |                   0 |
---------------------------------------------------------------------------------------
| Dhcpv4 Ack             |                   0 |                   0 |                   0 |
| Dhcpv4 Decline         |                   0 |                   0 |                   0 |
| Dhcpv4 Discover        |                   0 |                   0 |                   0 |
| Dhcpv4 Inform          |                   0 |                   0 |                   0 |
| Dhcpv4 Leaseactive     |                   0 |                   0 |                   0 |
| Dhcpv4 Leasequery      |                   0 |                   0 |                   0 |
| Dhcpv4 Leaseunassigned |                   0 |                   0 |                   0 |
| Dhcpv4 Leaseunknown    |                   0 |                   0 |                   0 |
| Dhcpv4 Nack            |                   0 |                   0 |                   0 |
| Dhcpv4 Offer           |                   0 |                   0 |                   0 |
| Dhcpv4 Release         |                   0 |                   0 |                   0 |
| Dhcpv4 Request         |                   0 |                   0 |                   0 |
---------------------------------------------------------------------------------------
| Dhcpv6 Advertise       |                   0 |                   0 |                   0 |
| Dhcpv6 Confirm         |                   0 |                   0 |                   0 |
| Dhcpv6 Decline         |                   0 |                   0 |                   0 |
```

```
| Dhcpv6 Informationreq  |                  0 |                  0 |                  0 |
| Dhcpv6 Rebind          |                  0 |                  0 |                  0 |
| Dhcpv6 Reconfigure     |                  0 |                  0 |                  0 |
| Dhcpv6 Relayforw       |                  0 |                  0 |                  0 |
| Dhcpv6 Relayreply      |                  0 |                  0 |                  0 |
| Dhcpv6 Release         |                  0 |                  0 |                  0 |
| Dhcpv6 Renew           |                  0 |                  0 |                  0 |
| Dhcpv6 Reply           |                  0 |                  0 |                  0 |
| Dhcpv6 Request         |                  0 |                  0 |                  0 |
| Dhcpv6 Solicit         |                  0 |                  0 |                  0 |
-------------------------------------------------------------------------------------
| Nd Na                  |                 18 |                 18 |                  0 |
| Nd Ns                  |                 26 |                 22 |                  4 |
| Nd Ra                  |                 11 |                  6 |                  5 |
| Nd Redirect            |                  0 |                  0 |                  0 |
| Nd Rs                  |                  0 |                  0 |                  0 |
-------------------------------------------------------------------------------------
```

ステップ 5 NxOS メモリから FHS のセキュリティ保護されたエンドポイントのデータベースを表示します。

例：

```
leaf1# vsh -c 'show system internal fhs bt'

Binding Table has 7 entries, 4 dynamic

Codes:
L - Local         S - Static        ND - Neighbor Discovery   ARP - Address Resolution Protocol
DH4 - IPv4 DHCP   DH6 - IPv6 DHCP   PKT - Other Packet        API - API created

Preflevel flags (prlvl):
0001: MAC and LLA match     0002: Orig trunk            0004: Orig access
0008: Orig trusted trunk    0010: Orig trusted access   0020: DHCP assigned
0040: Cga authenticated     0080: Cert authenticated    0100: Statically assigned

EPG types:
V - Vlan Based EPG      M - MAC Based EPG       I - IP Based EPG

-------------------------------------------------------------------------------------------------------------------------------
| Code | Network Layer Address                    | Link Layer Address | Interface      | Vlan |
Epg                | prlvl | Age        | State      | Time left       |
-------------------------------------------------------------------------------------------------------------------------------
| ARP  | 172.29.207.222                           | d0:72:dc:a0:3d:4c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 29 s       | STALE      | 157 s           |
| L    | 192.0.200.1                              | 00:22:bd:f8:19:ff  | Vlan4          |    4 |
0x400004003 (I)    | 0100  | 55 mn      | REACHABLE  |                 |
| ARP  | 192.0.200.10                             | f8:72:ea:ad:c4:7c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 156 s      | STALE      | 30 s            |
| L    | 2001:0:0:200::1                          | 00:22:bd:f8:19:ff  | Vlan4          |    4 |
0x400004003 (I)    | 0100  | 55 mn      | REACHABLE  |                 |
| ND   | 2001:0:0:200::10                         | f8:72:ea:ad:c4:7c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 143 s      | STALE      | 47 s            |
| L    | fe80::200                                | 00:22:bd:f8:19:ff  | Vlan4          |    4 |
0x400004003 (I)    | 0100  | 55 mn      | REACHABLE  |                 |
| ND   | fe80::fa72:eaff:fead:c47c                | f8:72:ea:ad:c4:7c  | Eth1/1         |    4 |
0x40000c002 (V)    | 0011  | 176 s      | STALE      | 11 s            |
-------------------------------------------------------------------------------------------------------------------------------
```

ステップ 6 NX-OS FHS プロセス内蔵メモリから FHS 機能の設定を表示します。

例：

```
leaf4# vsh -c 'show system internal fhs pol'
```

```
Target           Type  Policy           Feature       Target-Range Sub-Feature
epg 0x40000c002  EPG   epg 0x40000c002  Trustctrl      vlan 4      Device-Roles: DHCPv4-Server,
DHCPv6-Server, Router
                                                                   Protocols: ARP ND
vlan 4           VLAN  vlan 4           IP inspect     vlan all    Protocols: ARP, DHCPv4, ND,
DHCPv6,
vlan 4           VLAN  vlan 4           RA guard       vlan all    Min-HL:3, Max-HL:15,
M-Config-flag:Enable,On
                                                                   O-Config-flag:Enable,On,
Router-Pref:medium
```

ステップ 7 NX-OS 共有データベースから FHS のセキュリティ保護されたエンドポイントのデータベースを表示します。

例：

```
leaf1# vsh -c 'show system internal fhs sdb bt'

Preflevel flags (preflvl):
0001: MAC and LLA match     0002: Orig trunk            0004: Orig access
0008: Orig trusted trunk    0010: Orig trusted access   0020: DHCP assigned
0040: Cga authenticated     0080: Cert authenticated    0100: Statically assigned

Origin      Zone ID     L3 Address                              MAC Address         VLAN ID  EPG
ID              If-name         Preflvl  State
----------  ----------  --------------------------------------  ------------------  -------
------------------  --------------  -------  ---------
ARP         0x4         172.29.207.222                          d0:72:dc:a0:3d:4c   4
0x40000c002         Eth1/1          0011     STALE
L           0x4         192.0.200.1                             00:22:bd:f8:19:ff   4
0x400004003         Vlan4           0100     REACHABLE
ARP         0x4         192.0.200.10                            f8:72:ea:ad:c4:7c   4
0x40000c002         Eth1/1          0011     REACHABLE
L           0x4         2001:0:0:200::1                         00:22:bd:f8:19:ff   4
0x400004003         Vlan4           0100     REACHABLE
ND          0x4         2001:0:0:200::10                        f8:72:ea:ad:c4:7c   4
0x40000c002         Eth1/1          0011     STALE
L           0x80000004  fe80::200                               00:22:bd:f8:19:ff   4
0x400004003         Vlan4           0100     REACHABLE
ND          0x80000004  fe80::fa72:eaff:fead:c47c                f8:72:ea:ad:c4:7c   4
0x40000c002         Eth1/1          0011     STALE
```

ステップ 8 NxOS 共有データベースから FHS 機能の設定を表示します。

例：

```
leaf1# vsh -c 'show system internal fhs sdb pol'
Policies:

IP inspect      Vlan 4                    Protocols:ARP DHCPv4 ND DHCPv6
RA guard        Vlan 4                    Min-HL:3 Max-HL:15 M-Config-Flag:enable,on
O-Config-Flag:enable,on Router-Pref:medium
Trustctrl       Epg 0x40000c002           Vlan:4
                                          Device-Roles:DHCPv4-Server DHCPv6-Server Router
                                          Protocols:ARP ND
```

ステップ 9 セキュリティ保護されたデータベース エンドポイント エントリを消去する show コマンド：

例：

```
leaf1# vsh -c 'clear system internal fhs bt ipv4 172.29.207.222'
```

REST API を使用して apic 内で FHS の設定

始める前に

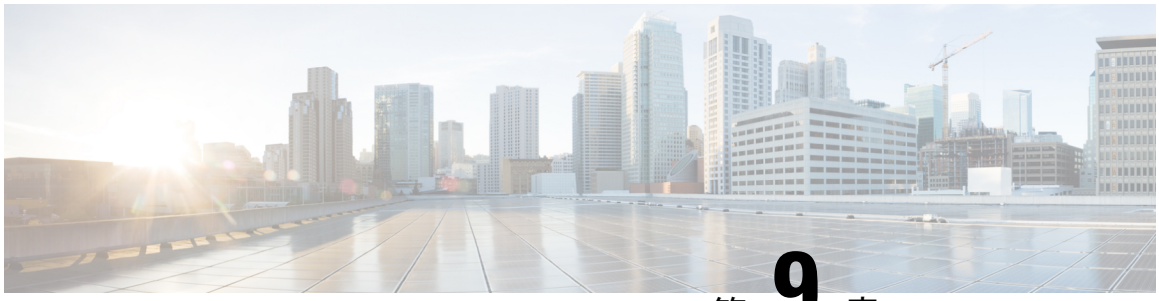
- テナントおよびブリッジ ドメインは設定しておく必要があります。

FHS と信頼制御ポリシーを設定します。

例：

```
<polUni>
    <fvTenant name="Coke">
        <fhsBDPol name="bdpol5" ipInspectAdminSt="enabled-ipv6" srcGuardAdminSt="enabled-both"
raGuardAdminSt="enabled" status="">
            <fhsRaGuardPol name="raguard5" managedConfigCheck="true" managedConfigFlag="true"
otherConfigCheck="true" otherConfigFlag="true" maxRouterPref="medium" minHopLimit="3" maxHopLimit="15"
 status=""/>
        </fhsBDPol>
        <fvBD name="bd3">
            <fvRsBDToFhs tnFhsBDPolName="bdpol5" status=""/>
        </fvBD>
    </fvTenant>
</polUni>

<polUni>
<fvTenant name="Coke">
        <fhsTrustCtrlPol name="trustctrl5" hasDhcpv4Server="true" hasDhcpv6Server="true"
hasIpv6Router="true" trustRa="true" trustArp="true" trustNd="true" />
        <fvAp name="wwwCokecom3">
           <fvAEPg name="test966">
           <fvRsTrustCtrl tnFhsTrustCtrlPolName="trustctrl5" status=""/>
        </fvAEPg>
        </fvAp>
</fvTenant>
</polUni>
```



第 9 章

プロトコル認証

この章は、次の項で構成されています。

COOP

概要

マッピング情報（ロケーションおよび ID）をスパイン プロキシに伝達するために、Council of Oracles Protocol（COOP）を使用します。リーフ スイッチは、Zero Message Queue（ZMQ）を使用して、エンドポイント アドレス情報をスパイン スイッチ「Oracle」に転送します。スパイン ノードで実行している COOP によって、すべてのスパイン ノードが一貫性のあるエンドポイント アドレスとロケーション情報のコピーを維持することができ、さらに、ロケーション マッピング データベースに対するエンドポイント ID の分散ハッシュ テーブル（DHT）レポジトリを維持することができます。

COOP データ パス通信は、セキュアな接続を介した転送を優先します。COOP は悪意のあるトラフィック インジェクションから COOP メッセージを保護するために MD5 オプションの活用が強化されます。APIC コントローラおよびスイッチは、COOP プロトコル認証をサポートします。

COOP プロトコルは 2 つの ZMQ 認証モードをサポートするために強化されています：ストリクトおよび互換性。

- ストリクト モード：COOP では MD5 認証済みの ZMQ 接続のみを許可します。
- 互換性モード；COOP ではメッセージの転送に MD5 認証接続と非認証 ZMQ 接続の両方を許可します。

Cisco APIC で COOP を使用する

Cisco Application Centric Infrastructure（ACI）ファブリック上で COOP ゼロ メッセージ キュー（ZMQ）認証サポートを行うため、Application Policy Infrastructure Controller（APIC）では MD5 パスワードおよび COOP セキュア モードをサポートします。

COOP ZMQ 認証タイプの設定：新しい管理対象オブジェクトの `coop: AuthP` は、データ管理エンジン（DME）データベース（DME）/COOP に追加されます。属性タイプのデフォルト値は「互換性」ですが、ユーザーには「厳密」タイプ設定を行うオプションがあります。

COOP ZMQ 認証 MD5 パスワード：APIC では管理対象オブジェクト（`fabric:SecurityToken`）提供し、MD5 パスワードに使用する属性が含まれます。「トークン」と呼ばれるこの管理対象オブジェクト内の属性は、1 時間ごとに変更される文字列です。COOP は、DME から通知を受け取り、ZMQ 認証のパスワードを更新します。この属性トークンの値は表示されません。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- ACI ファブリックのアップグレード中は、すべてのスイッチがアップグレードされるまで、COOP 厳格モードが許可されません。この保護は、早期に厳格なモードを有効にすることでトリガされる可能性がある、予期しない COOP 接続の拒否を防ぎます。

APIC GUI を使用した COOP 認証の設定

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順に選択します。

ステップ 2 **[ナビゲーション]** ペインで **[COOP グループ]** をクリックします。

ステップ 3 **[作業]** ペインの **[タイプ]** フィールドにある **[ポリシー プロパティ]** 領域で、**[互換性のあるタイプ]** および **[ストリクト タイプ]** オプションから希望のタイプを選択します。

ステップ 4 [Submit] をクリックします。
これにより、COOP 認証ポリシー設定を完了します。

Cisco NX OS スタイル CLI を使用した COOP 認証の設定

ストリクト モード オプションを使用して、COOP 認証ポリシーを設定します。

例：

```
apic1# configure
apic1(config)# coop-fabric
apic1(config-coop-fabric)# authentication type ?
compatible  Compatible type
```

```
strict      Strict type
apic101-apic1(config-coop-fabric)# authentication type strict
```

REST API を使用した COOP 認証の設定

COOP 認証ポリシーを設定します。

例では、ストリクト モードが選択されます。

例：

```
https://172.23.53.xx/api/node/mo/uni/fabric/pol-default.xml

<coopPol type="strict">
</coopPol>
```

EIGRP

概要

EIGRP は、リンクステート プロトコルの機能にディスタンス ベクトル プロトコルの利点を組み合わせたプロトコルです。EIGRP は、定期的に Hello メッセージを送信してネイバーを探索します。EIGRP は、新規ネイバーを検出すると、すべてのローカル EIGRP ルートおよびルート メトリックに対する 1 回限りの更新を送信します。受信側の EIGRP ルータは、受信したメトリックと、その新規ネイバーにローカルで割り当てられたリンクのコストに基づいて、ルート ディスタンスを計算します。この最初の全面的なルート テーブルの更新後は、ルート変更の影響を受けるネイバーにのみ、差分更新が EIGRP により送信されます。この処理により、コンバージェンスにかかる時間が短縮され、EIGRP が使用する帯域幅が最小限になります。

Cisco APIC では、EIGRP 認証でルートマップのキーチェーンのインフラストラクチャが MD5 認証に使用されます。2 つの EIGRP ピア間で認証を設定するには 2 つのパラメータが必要になります。パラメータは次のとおりです。

- モード
- Keychain

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- MD5 認証のみサポートされます。キーチェーンは、RPM で設定されているキーチェーン名です。

- 2 つの EIGRP ピア間で認証の不一致がある場合は、ネイバーシップのフラッピングが発生します。フラッピングの理由は **show eigrp internal event-history syslog** で確認できます。

APIC GUI を使用した EIGRP 認証の設定

ステップ 1 メニュー バーで、**[Tenant]*[tenant-name]*** を選択します。

ステップ 2 [Navigation] ペインで、**[Policies]** > **[Protocol]** > **[EIGRP]** を展開します。

ステップ 3 [EIGRP] を展開し、[EIGRP KeyChains] を右クリックして [Create Keychain Policy] を開き、次の操作を行います。

a) [Name] フィールドにポリシーの名前を入力します。
b) [KeyID] フィールドに、キー ID 番号を入力します。
c) [Preshared key] フィールドに、事前共有キーの情報を入力します。
d) オプション。[Start Time] フィールドと [End Time] フィールドに、時間を入力します。

ステップ 4 [Navigation] ペインで、[EIGRP Interface] を右クリックし、次の操作を行います。

a) [Authentication] フィールドで、ボックスをクリックして有効にします。
b) [Key Chain Policy] フィールドで、ドロップダウン リストから作成したポリシーを選択し、[Submit] をクリックします。

NX-OS CLI を使用した EIGRP 認証の設定

ステップ 1 テナントで、キーチェーン ポリシーとキーポリシーを設定します。

例：

```
tenant T1
keychain-policy KeyChainPol
key-policy 2
```

ステップ 2 オプション。開始時刻を設定します。

例：

```
startime 2018-11-01T08:39:27.000+00:00
exit
```

ステップ 3 APIC からリーフ設定を開始します。インターフェイスでの認証を有効にし、キーチェーン ポリシーを設定します。

例：

```
IFC1(config-leaf)# show run
# Command: show running-config leaf 104
# Time: Thu Nov 8 12:05:45 2018
leaf 104
interface ethernet 1/2.45
```

```
vrf member tenant T1 vrf V1 l3out L3Out
ip router eigrp authentication keychain-policy KeyChainPol
ip router eigrp authentication enable
!
ipv6 router eigrp authentication keychain-policy KeyChainPol
ipv6 router eigrp authentication enable
exit
```

ステップ 4 EIGRP の設定を確認するには、次の手順を実行します。

例：

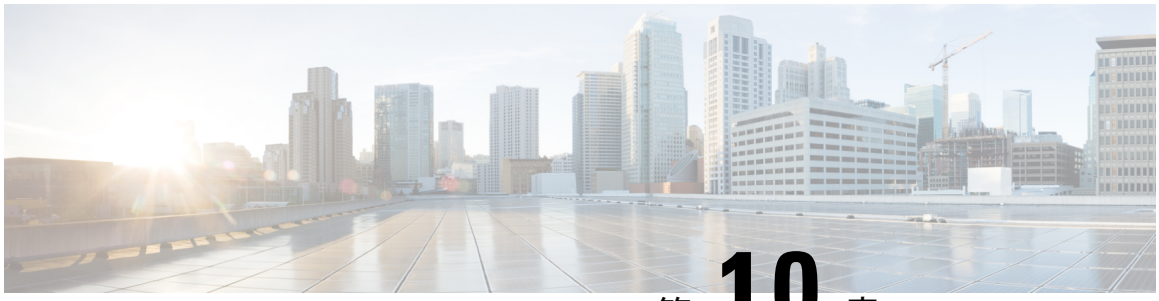
```
fav-blr4-ls-leaf4# show ip eigrp interfaces eth1/2.17
EIGRP interfaces for process 1 VRF T1:V1
Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
eth1/2.17 0 0/0 0 0/0 50 0
Hello interval is 5 sec
Holdtime interval is 15 sec
Next xmit serial: 0
Un/reliable mcasts: 0/3 Un/reliable ucasts: 6/4
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 1
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Classic/wide metric peers: 0/0
Authentication mode is md5, key-chain is T1:KeyChainPol
ifav-blr4-ls-leaf4#
```

ステップ 5 スイッチでトラブルシューティングを行う場合は、次の CLI を使用できます。EIGRP 認証は、IPv4 と IPv6 の両方のアドレス ファミリでサポートされています。

例：

```
(none)# show ip eigrp interface vrf all
EIGRP interfaces for process 100 VRF pepsi
Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
eth1/1 1 0/0 207 0/0 828 0
Hello interval is 10 sec
Holdtime interval is 15 sec
Next xmit serial: 0
Un/reliable mcasts: 0/7 Un/reliable ucasts: 21/18
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 4 Out-of-sequence rcvd: 2
Classic/wide metric peers: 0/1
Authentication mode is md5, key-chain is eigrp-auth

(none)# show ipv6 eigrp interface vrf pepsi
IPv6-EIGRP interfaces for process 100 VRF pepsi
Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
eth1/1 0 0/0 0 0/0 0 0
Hello interval is 10 sec
Holdtime interval is 15 sec
Next xmit serial: 0
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Classic/wide metric peers: 0/0
Authentication mode is md5, key-chain is eigrp-auth
```



第 10 章

コントロール プレーンのトラフィック

コントロール プレーン ポリシングについて

コントロール プレーン ポリシング（CoPP）はコントロールプレーンを保護し、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプロセッサに到達可能な各プロトコルに対して、パラメータの仕様でポリサーを使用したレート制限が可能になります。ポリシングは、ルータまたはレイヤ 3 スイッチの IP アドレスのいずれかを宛先とするすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイスインターフェイスに転送されるサービス妨害（DoS）攻撃です。

Cisco Application Centric Infrastructure（ACI）リーフおよびスパインスイッチ NX-OS は、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があり、通常は Cisco ACI リーフおよびスパインスイッチ CPU または CPU 自体のスーパーバイザモジュールに宛てられた大量のトラフィックが含まれます。

Cisco ACI リーフおよびスパインスイッチ スイッチのスーパーバイザモジュールは、管理対象のトラフィックを次の 2 つの機能コンポーネント（プレーン）に分類します。

- **データ プレーン**：すべてのデータトラフィックを処理します。NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。データ プレーンで処理されるのはこれらのパケットです。
- **コントロールプレーン**：ルーティングプロトコルのすべての制御トラフィックを処理します。ボーダー ゲートウェイ プロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティングプロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロール プレーン パケットと呼ばれます。

Cisco ACI リーフスイッチおよびスパインスイッチのスーパーバイザモジュールにはコントロールプレーンがあり、ネットワークの操作に重要です。スーパーバイザモジュールの動作が途絶したり、スーパーバイザモジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえば、スーパーバイザに過剰なトラフィックが加わると、スーパーバイザモジュールが過負荷になり、Cisco ACI ファブリック全体のパフォーマンスが低下する可能性があります。別の例としては、Cisco ACI リーフスイッチおよびスパインスイッチのスーパーバイザモジュールに対する DoS 攻撃は、コントロールプレーンに対して非常に高速に IP トラフィックストリームを生成することがあります。これにより、コントロールプレーンでは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

次に、DoS 攻撃の例を示します。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーション トラフィックの低下など）
- ルート プロセッサまたはスイッチ プロセッサの高い CPU 使用率
- ルーティング プロトコルのアップデートまたはキープアライブの消失によるルート フラップ
- メモリやバッファなどのプロセッサ リソースの枯渇
- 着信パケットの無差別のドロップ

（注） Cisco ACI リーフスイッチとスパインスイッチは、デフォルトで、デフォルト設定の CoPP によって保護されます。この機能では、顧客のニーズに基づいてノードのグループにパラメータを調整できます。

コントロール プレーン保護

コントロールプレーンを保護するため、Cisco ACI リーフスイッチおよびスパインスイッチで実行されている Cisco NX-OS はコントロールプレーンのさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

コントロール プレーンのパケット タイプ:

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

- **受信パケット**：ルーターの宛先アドレスを持つパケット。宛先アドレスには、レイヤ2アドレス（ルータ MAC アドレスなど）やレイヤ3アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータアップデートとキープアライブ メッセージも含まれます。ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャスト パケットも、このカテゴリに入ります。
- **例外パケット**：スーパーバイザモジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザモジュールが送信側に到達不能パケットを返します。他には、IP オプションがセットされたパケットもあります。
- **リダイレクトパケット**：スーパーバイザモジュールにリダイレクトされるパケット。ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングやダイナミック アドレス解決プロトコル（ARP）インスペクションなどの機能は、パケットをスーパーバイザ モジュールにリダイレクトします。
- **収集パケット**：宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザモジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットは、コントロールプレーンへの悪意ある攻撃に利用され、Cisco ACI ファブリックに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットを Cisco ACI リーフスイッチおよびスパインスイッチのスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類：

効果的に保護するために、Cisco ACI リーフスイッチおよびスパインスイッチ NX-OS は、スーパーバイザモジュールに到達するパケットを分類して、パケットタイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコルパケットには厳格度を緩和し、IP オプションがセットされているためにスーパーバイザモジュールに送信されるパケットには厳格度を強化することが考えられます。

利用可能なプロトコル：

プロトコル	説明
グリーニング	このプロトコルでは、ブリッジドメインがプロキシモードの場合、リーフスイッチが受信した不明なユニキャストトラフィックはハードウェアプロキシ（スパインスイッチ）に送信されます。スパインスイッチは、パケットの eth-type を特別な eth-type (0xfff2) に変更します。これらのパケットがファブリックポートを介してリーフスイッチに到達すると、パケットはグリーニングの下に分類されます。パケットはリーフスイッチの CPU に送信され、リーフスイッチの CPU は接続された外部デバイスに対して ARP 要求を生成します。

プロトコル	説明
ToR グリーニング	ToR グリーニングは、エンドポイントが移動するか、リンクフラップのためにクリアされたときにアクティブになり、送信元リーフスイッチのリモート IP アドレスのエンドポイントエントリは更新されません。パケットは、接続先リーフスイッチの TEP アドレスを使用して送信元リーフスイッチから出力されます。接続先リーフスイッチでは、ローカル IP アドレスエントリが欠落しているため、パケットはリーフスイッチ CPU に送信され、それらの IP アドレスに対する ARP 要求が生成されます。これらのパケットは、ToR グリーニングに分類されます。

レート制御メカニズム：

パケットの分類が終わると、Cisco ACI リーフおよびスパインスイッチ NX-OS デバイスにはスーパーバイザモジュールに到達するパケットのレートを制御するメカニズムがあります。

ポリシングには、次のパラメータを設定できます。

- **認定情報レート（CIR）**：1秒あたりのパケット数（PPS）で指定される、必要な帯域幅。
- **認定バースト（BC）**：パケット数で指定され、特定の時間枠内に CIR を超えるが、スケジューリングに影響を与えないトラフィックバーストのサイズ。

デフォルトのポリシング ポリシー：

Cisco ACI リーフスイッチおよびスパインスイッチが最初に起動するとき、異なるプロトコル用に事前定義された CoPP パラメータは、シスコで行ったテストに基づいています。

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 最初にデフォルト CoPP ポリシーを使用し、後で、データセンターおよびアプリケーションの要件に基づいて CoPP ポリシーを変更することをお勧めします。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能に加えて、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。
- CoPP を継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。いずれの場合も、状況を分析し、CoPP ポリシーを変更する必要を評価します。

- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco ACI リーフ/スパインへのリモート アクセスが禁止され、コンソール接続が必要となる場合があります。
- CoPP プレフィルタ エントリを誤って設定しないでください。CoPP プレフィルタ エントリは、マルチポッド設定、リモート リーフ スイッチ、および Cisco ACI マルチサイト展開への接続に影響を与える可能性があります。
- APIC UI を使用して、CoPP パラメータを調整することができます。
- プロトコルごとの各インターフェイスはリーフ スイッチでのみサポートされています。
- プロトコルごとの各インターフェイスで FEX ポートはサポートされていません。
- プロトコルごとの各インターフェイスでサポートされているプロトコルは、ARP、ICMP、CDP、LLDP、LACP、BGP、STP、BFD、および OSPF です。
- プロトコルごとの各インターフェイスの最大の TCAM エントリは 256 です。しきい値を超過すると、障害が発生します。

APIC GUI を使用した CoPP の設定

ステップ 1 メニュー バーで、**[ファブリック]** > **[外部アクセス ポリシー]** をクリックします。

ステップ 2 **[ナビゲーション]** ペインで、**[ポリシー]** > **[スイッチ]** > **[CoPP リーフ]** を展開して、**[リーフ レベルで適用される CoPP のプロファイルの作成]** ダイアログ ボックスを右クリックし、**[リーフ レベルで適用される CoPP のプロファイルの作成]** ダイアログ ボックスの次のアクションを実行します。

a) **[名前]** フィールドでポリシー名を追加します。

b) **[プロファイルのタイプ]** フィールドで、プロファイル タイプを選択します。

（注） 各プロトコルを個別に設定する場合、**[CoPP にカスタム値がある]** を選択します。プロファイル タイプを選択しない場合、デフォルト値が適用されます。

c) **[送信]** をクリックしてポリシーを作成します。

ステップ 3 **[ナビゲーション]** ペインで、**[スイッチ]** > **[リーフ スイッチ]** > **[ポリシー グループ]** を展開し、**[アクセス スイッチ ポリシー グループの作成]** ダイアログ ボックスを右クリックして、**[アクセス スイッチ ポリシー グループの作成]** ダイアログ ボックスの次のアクションを実行します。

a) **[名前]** フィールドでポリシー名を追加します。

b) **[COPP リーフ ポリシー]** フィールドで、以前に作成されたポリシーを選択します。

c) [Submit] をクリックします。

ステップ 4 **[ナビゲーション]** ペインで、**[スイッチ]** > **[リーフ スイッチ]** > **[プロファイル]** を展開して、**[リーフ プロファイルの作成]** ダイアログ ボックスを右クリックして、**[リーフ プロファイルの作成]** ダイアログ ボックスの次のアクションを実行します。

a) **[名前]** フィールドで、プロファイル名を追加します。

b) **[リーフ セレクタ]** 表を展開して、**[名前]** と **[ブロック]** フィールドにリーフ情報を追加して、以前作成した **[ポリシー グループ]** を選択します。
c) **[次へ]** および **[終了]** をクリックして、CoPP 設定を実行します。

Cisco NX-OS CLI を使用した CoPP の設定

ステップ 1 CoPP リーフ プロファイルを設定します。

例：

```
# configure copp Leaf Profile
apic1(config)# policy-map type control-plane-leaf leafProfile
apic1(config-pmap-copp-leaf)# profile-type custom
apic1(config-pmap-copp-leaf)# set arpRate 786
# create a policy group to be applied on leaves
apic1(config)# template leaf-policy-group coppForLeaves
apic1(config-leaf-policy-group)# copp-aggr leafProfile
apic1(config-leaf-policy-group)# exit
# apply the leaves policy group on leaves
apic1(config)# leaf-profile applyCopp
apic1(config-leaf-profile)# leaf-group applyCopp
apic1(config-leaf-group)# leaf 101-102
apic1(config-leaf-group)# leaf-policy-group coppForLeaves
```

ステップ 2 CoPP スパイン プロファイルを設定します。

例：

```
# configure copp Spine Profile
apic1(config)# policy-map type control-plane-spine spineProfile
apic1(config-pmap-copp-spine)# profile-type custom
apic1(config-pmap-copp-spine)# set arpRate 786
# create a policy group to be applied on spines
apic1(config)# template leaf-policy-group coppForSpines
apic1(config-spine-policy-group)# copp-aggr spineProfile
apic1(config-spine-policy-group)# exit
# apply the spine policy group on spines
apic1(config)# spine-profile applyCopp
apic1(config-spine-profile)# spine-group applyCopp
apic1(config-spine-group)# spine 201-202
apic1(config-spine-group)# spine-policy-group coppForSpines
```

REST API を使用した CoPP の設定

ステップ 1 CoPP リーフ プロファイルを設定します。

例：

```
<!-- api/node/mo/uni/.xml -->
<infraInfra>
  <coppLeafProfile type="custom" name="mycustom">                    <!-- define copp leaf profile
```

```
-->
    <coppLeafGen1CustomValues bgpBurst="150" bgpRate="300"/>
  </coppLeafProfile>
  <infraNodeP name="leafCopp">
    <infraLeafS name="leafs" type="range">
      <infraNodeBlk name="leaf1" from_="101" to_="101"/>
      <infraNodeBlk name="leaf3" from_="103" to_="103"/>
      <infraRsAccNodePGrp tDn="uni/infra/funcprof/accnodepgrp-myLeafCopp"/>
    </infraLeafS>
  </infraNodeP>
  <infraFuncP>
    <infraAccNodePGrp name="myLeafCopp">
      <infraRsLeafCoppProfile tnCoppLeafProfileName="mycustom"/>   <!-- bind copp leaf policy to
leaf </infraAccNodePGrp>                                                    profile -->
  </infraFuncP>
</infraInfra>
```

ステップ 2 CoPP スパイン プロファイルを設定します。

例：

```
<!-- api/node/mo/uni/.xml -->
<infraInfra>
  <coppSpineProfile type="custom" name="mycustomSpine">             <!-- define copp leaf profile
-->
    <coppSpineGen1CustomValues bgpBurst="150" bgpRate="300"/>
  </coppSpineProfile>
  <infraSpineP name="spineCopp">
    <infraSpineS name="spines" type="range">
      <infraNodeBlk name="spine1" from_="104" to_="104"/>
      <infraRsSpineAccNodePGrp tDn="uni/infra/funcprof/spaccnodepgrp-mySpineCopp"/>
    </infraSpineS>
  </infraSpineP>
  <infraFuncP>
    <infraSpineAccNodePGrp name="mySpineCopp">
      <infraRsSpineCoppProfile tnCoppSpineProfileName="mycustomSpine"/> <!-- bind copp spine policy
 to
    </infraSpineAccNodePGrp>                                                spine profile -->
  </infraFuncP>
</infraInfra>
```

GUI を使用した CoPP 統計情報の表示

CoPP の調整を適切に行うには、指定のモードの指定のプロトコルでドロップ/許可されたパケット数を知る必要があります。次の手順を使用して、GUI で情報を表示できます。

メニュー バーで、**[ファブリック]** > **[インベントリ]** > **[ポッド]*[番号]*** > **[ノード]*[名前]*** > **[コントロール プレーンの統計情報]** > **[デフォルト]** の順にクリックして、クラスのリストから選択し、統計情報の表示形式を設定します。

CoPP によって許可またはドロップされたパケット数に関する統計情報を収集することができます。

APIC GUI を使用したプロトコル CoPP ポリシーごとの各インターフェイスの設定

ステップ 1 メニュー バーで、**[ファブリック]** > **[外部アクセス ポリシー]** をクリックします。

ステップ 2 **[ナビゲーション]** ペインで、**[ポリシー]** > **[インターフェイス]** > **[CoPP インターフェイス]** を展開して、**[プロトコル CoPP ポリシーごとの各インターフェイスの作成]** ダイアログ ボックスを右クリックして、**[プロトコル CoPP ポリシーごとの各インターフェイスの作成]** ダイアログ ボックスの次のアクションを実行します。

a) **[名前]** フィールドでポリシー名を追加します。

b) **[CoPP ポリシー プロトコル]** 表を展開し、プロトコル名、タイプ、レート、バースト情報を入力します。**[更新]** と **[送信]** をクリックします。

ステップ 3 **[ナビゲーション]** ペインで、**[インターフェイス]** > **[リーフ インターフェイス]** > **[ポリシー グループ]** > **[リーフ アクセス ポート ポリシー グループの作成]** を展開して、**[リーフ アクセス ポート ポリシー グループの作成]** ダイアログ ボックスを右クリックして、**[リーフ アクセス ポート ポリシー グループの作成]** ダイアログ ボックスの次のアクションを実行します。

a) **[名前]** フィールドでポリシー名を追加します。

b) **[COPP リーフ ポリシー]** フィールドで、以前に作成されたポリシーを選択します。

c) [Submit] をクリックします。

ステップ 4 **[ナビゲーション]** ペインで、**[インターフェイス]** > **[リーフ インターフェイス]** > **[プロファイル]** > **[リーフ プロファイル]** を展開して、**[リーフ インターフェイス プロファイルの作成]** ダイアログ ボックスを右クリックして、**[リーフ インターフェイス プロファイルの作成]** ダイアログ ボックスの次のアクションを実行します。

a) **[名前]** フィールドで、プロファイル名を追加します。

b) **[インターフェイス セレクタ]** 表を展開し、**[名前]** および **[インターフェイス ID]** フィールドにインターフェイス情報を追加して、以前作成した **[インターフェイス ポリシー グループ]** を選択します。

c) **[Ok]** および **[送信]** をクリックして、プロトコル CoPP ごとの各インターフェイス設定を完了します。

NX-OS スタイル CLI を使用するプロトコル CoPP ポリシーごとのインターフェイスごとの設定

ステップ 1 CoPP クラス マップおよびポリシー マップを定義します。

例：

```
(config)# policy-map type control-plane-if <name>
        (config-pmap-copp)# protocol bgp bps <value>
        (config-pmap-copp)# protocol ospf bps <value>
```

ステップ 2 リーフのインターフェイスに設定を適用します。

例：

```
(config)# leaf 101
        (config-leaf)# int eth 1/10
        (config-leaf-if)# service-policy type control-plane-if output<name>
```

REST API を使用するプロトコルごとのインターフェイスあたりの CoPP の設定

プロトコルごとにインターフェイスあたりの CoPP を設定します。

例：

```
<polUni>
    <infraInfra>
    <infraNodeP name="default">
        <infraLeafS name="default" type="range">
            <infraNodeBlk name="default" to_="101" from_="101"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-default"/>
    </infraNodeP>
    <infraAccPortP name="default">
        <infraHPortS name="regularPorts" type="range">
            <infraPortBlk name="blk1" toPort="7" fromPort="1" toCard="1" fromCard="1"/>
                <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-copp"/>
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccPortGrp name="copp">
            <infraRsCoppIfPol tnCoppIfPolName="pc"/>
        </infraAccPortGrp>
    </infraFuncP>

    <coppIfPol name = "pc" >
        <coppProtoClassP name = "test" matchProto="lldp,arp" rate="505" burst = "201"/>
        <coppProtoClassP name = "test1" matchProto="bgp" rate="500" burst = "200" />
    </coppIfPol>
</infraInfra>
</polUni>
```

CoPP プレフィルタについて

DDoS 攻撃に対する保護のため、CoPP プレフィルタ プロファイルはスパインとリーフ スイッチで使用され、指定されたソースと TCP ポートに基づく認証サービスへのアクセスをフィルタします。CoPP プレフィルタ プロファイルがスイッチに展開されるとき、デフォルトでコントロール プレーン トラフィックは拒否されます。CoPP プレフィルタ プロファイルで指定されたトラフィックのみが許可されます。

サポートされるプラットフォーム

このセクションでは、CoPP プレフィルター機能のサポートされているプラットフォームを示します。

リーフ スイッチがサポートされています。

- N9K-C93108TC-EX
- N9K-C93108TC-FX
- N9K-C93108YC-FX
- N9K-C93180LC-EX
- N9K-C93180YC-EX
- N9K-C9348GC-FXP

スパイン スイッチがサポートされています。

- N9K-C92300YC
- N9K-C92304QC
- N9K-C9232C
- N9K-C9236C
- N9K-C9272Q
- N9K-C9364C
- N9K C9508 FM 2
- N9K-C9516-FM-E2

制限事項

- イーサネット タイプ IPv4 または IPv6 パケットだけは、出力 TCAM で一致ことができます。ARP ND パケットが一致しません。
- 合計 128 (ワイドキー) エントリの許可リストに含めることができます。ただし、一部のエントリは、社外秘予約されています。

GUI を使用した CoPP プレフィルタ、ポリシー グループ、プロファイルの設定

Cisco APIC GUI を使用した CoPP プレフィルタの設定

このセクションでは、リーフ レベルとスパイン レベルは、Cisco APIC GUI を使用して、CoPP プレフィルタを設定する方法について説明します。

始める前に

APIC GUI へのアクセス

ステップ 1 **[Fabric]** > **[External Access Policies]**をクリックします。

ステップ 2 [Navigation] ペインで、**[Policies]** > **[Switch]** をクリックします。
[Navigation] ペインに [CoPP Pre-Filter for Leaf] および [CoPP Pre-Filter for Spine] ノードが表示されます。

ステップ 3 [Navigation] ペインで、次のオプションから選択します。

- [CoPP Pre-Filter for Leaf] – リーフ スイッチの CoPP プレフィルタを作成する場合は、[CoPP Pre-Filter for Leaf] を右クリックして、[Create Profiles for CoPP Pre-Filter To Be Applied At The Leaf Level] を選択します。
- [CoPP Pre-Filter for Spine] – スパイン スイッチの CoPP プレフィルタを作成する場合は、[CoPP Pre-Filter for Spine] を右クリックして、[Create Profiles for CoPP Pre-Filter To Be Applied At The Spine Level] を選択します。

それぞれの CoPP プレフィルターのダイアログが表示されます。

ステップ 4 ダイアログのフィールドに適切な値を入力します。

（注） ダイアログ ボックスのフィールドの詳細については、ヘルプ アイコンをクリックすると Cisco APIC ヘルプ ファイルが表示されます。

ステップ 5 完了したら、[送信（Submit）] をクリックします。

次のタスク

ポリシー グループを設定します。

GUI を使用したリーフ ポリシー グループの設定

このセクションでは、ポリシー グループを作成する方法について説明します。

始める前に

Cisco APIC GUI にアクセスします。

ステップ 1 **[Fabric]** > **[External Access Policies]**をクリックします。

ステップ 2 [**ナビゲーション**] ペインで、**[スイッチ]** > **[リーフ スイッチ]** をクリックします。
[ポリシー グループ] ノードが **[ナビゲーション]** ウィンドウに表示されます。

ステップ 3 [**ナビゲーション**] ペインの **[ポリシー グループ]** で、リーフ ポリシー グループを作成するには、**[ポリシー グループ]** を右クリックして、**[アクセス スイッチ ポリシー グループの作成]** をクリックします。

それぞれのポリシー グループ ダイアログが表示されます。

ステップ 4 ポリシー グループ ダイアログから、**[名前]** フィールドに名前を入力して、適用するポリシー タイプのドロップダウン矢印をクリックします。選択したポリシー タイプに設定されているポリシーがドロップダウン リストに表示されます。

（注） ダイアログ ボックスのフィールドの詳細については、ヘルプ アイコンをクリックすると Cisco APIC ヘルプ ファイルが表示されます。

ステップ 5 完了したら、[送信（Submit）] をクリックします。

次のタスク

プロファイルを設定します。

GUI を使用したリーフ プロファイルの設定

このセクションでは、プロファイルを作成する方法について説明します。

始める前に

設定されているポリシー グループが必要です。

ステップ 1 **[Fabric]** > **[External Access Policies]**をクリックします 。

ステップ 2 [**ナビゲーション**] ペインで、**[スイッチ]** > **[リーフ スイッチ]** > **[プロファイル]** をクリックします。
[リーフ プロファイル] ノードが **[ナビゲーション]** ウィンドウに表示されます。

ステップ 3 [**ナビゲーション**]ペインの**[プロファイル]**で、リーフ スイッチのプロファイルを作成するには、**[プロファイル]** を右クリックして **[リーフ プロファイルの作成]** を選択します。
個別にプロファイル ダイアログが表示されます。

ステップ 4 プロファイル ダイアログから **[名前]** フィールドに名前を入力し、**[+]** をクリックしてセレクタ情報を入力します。完了したら、[Update] をクリックします。

[更新] をクリックした後、プロファイル ダイアログに戻ります。

ステップ 5 **[次へ]** をクリックして、インターフェイス セレクタ プロファイル情報を入力します。

（注） ダイアログ ボックスのフィールドの詳細については、ヘルプ アイコンをクリックすると Cisco APIC ヘルプ ファイルが表示されます。

ステップ 6 完了したら、**[終了]** をクリックします。

CLI を使用した CoPP プレフィルタの設定

CLI を使用したリーフ スイッチの CoPP プレフィルタの設定

このセクションでは、CoPP プレフィルタ ポリシーとポリシー グループを設定し、CLI を使用してスイッチ ポリシー グループとスイッチ プロファイルを関連付ける方法を説明します。

ステップ 1 Switch# **configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 Switch(config)# **template control-plane-policing-prefilter-leaf** <*name*>

リーフ スイッチの CoPP プレフィルタ プロファイルを作成します。

ステップ 3 Switch (config-control-plane-policing-prefilter-leaf)# **permit proto** { **tcp** | **udp** | **eigrp** | **unspecified** | **icmp** | **icmpv6** | **egp** | **igp** | **l2tp** | **ospf** | **pim** }

指定された IP プロトコルを許可します。

ステップ 4 Switch (config-control-plane-policing-prefilter-leaf)#**exit**

グローバル コンフィギュレーション モードを開始します。

ステップ 5 Switch(config)# **template leaf-policy-group** <*name*>

CoPP プレフィルタ ポリシー グループ リーフ スイッチを作成します。

ステップ 6 Switch(config-leaf-policy-group)# **control-plane-policing-prefilter** <*name*>

CoPP プレフィルタ ポリシーとリーフ ポリシー グループを関連付けます。

ステップ 7 Switch(config-leaf-policy-group)# **exit** <*name*>

グローバル コンフィギュレーション モードを開始します。

ステップ 8 Switch(config)# **leaf-profile** <*name*>

リーフ プロファイルを作成します。

ステップ 9 Switch(config-leaf-profile)# **leaf-group** <*name*>

リーフ プロファイルとリーフ グループを関連付けます。

ステップ 10 Switch(config-leaf-group)# **leaf-policy-group** <*name*>

リーフ グループとリーフ ポリシー グループを関連付けます。

CLI を使用したスパイン スイッチの CoPP プレフィルタの設定

このセクションでは、CoPP プレフィルタ ポリシーとポリシー グループを設定し、CLI を使用してスイッチ ポリシー グループとスイッチ プロファイルを関連付ける方法を説明します。

ステップ 1 Switch# **configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 Switch(config)# **template control-plane-policing-prefilter-spine** <*name*>

スパイン スイッチの CoPP プレフィルタ プロファイルを作成します。

ステップ 3 Switch (config-control-plane-policing-prefilter-spine)# **permit proto** { **tcp** | **udp** | **eigrp** | **unspecified** | **icmp** | **icmpv6** | **egp** | **igp** | **l2tp** | **ospf** | **pim** }

指定された IP プロトコルを許可します。

ステップ 4 Switch (config-control-plane-policing-prefilter-spine)#**exit**

グローバル コンフィギュレーション モードを開始します。

ステップ 5 Switch(config)# **template spine-policy-group** <*name*>

CoPP プレフィルタ ポリシー グループ スパイン スイッチを作成します。

ステップ 6 Switch(config-spine-policy-group)# **control-plane-policing-prefilter** <*name*>

CoPP プレフィルタ ポリシーとスパイン ポリシー グループを関連付けます。

ステップ 7 Switch(config-spine-policy-group)# **exit** <*name*>

グローバル コンフィギュレーション モードを開始します。

ステップ 8 Switch(config)# **spine-profile** <*name*>

スパイン プロファイルを作成します。

ステップ 9 Switch(config-spine-profile)# **spine-group** <*name*>

スパイン プロファイルとスパイン グループを関連付けます。

ステップ 10 Switch(config-spine-group)# **spine-policy-group** <*name*>

スパイン グループとスパイン ポリシー グループを関連付けます。

REST API を使用した CoPP プレフィルタの設定

REST API を使用したリーフ スイッチの CoPP プレフィルタ ポリシーの設定

このセクションでは、REST API を使用してリーフ スイッチの CoPP プレフィルタ ポリシーを設定する方法について説明します。

ステップ 1 許可リストのエントリとともに CoPP プレフィルタのスイッチ ポリシーを作成します。

```
<iaclLeafProfile descr="" dn="uni/infra/iaclspinep-spine_icmp" name="COPP_PreFilter_BGP_Config "
ownerKey="" ownerTag="">
<iaclEntry dstAddr="0.0.0.0/0" dstPortFrom="179" dstPortTo="179" ipProto="tcp" name="bgp" nameAlias=""
 srcAddr="0.0.0.0/0" srcPortFrom="179" srcPortTo="179"/>
</iaclLeafProfile>
```

ステップ 2 CoPP プレフィルタ ポリシーでスイッチ ポリシー グループを作成します。

```
<infraAccNodePGrp descr="" dn="uni/infra/funcprof/accnodepgrp-COPP_PreFilter_BGP_Config "
name="COPP_PreFilter_BGP_Config" nameAlias="" ownerKey="" ownerTag="">
<infraRsIaclLeafProfile tnIaclLeafProfileName="COPP_PreFilter_BGP_Config"/>
</infraAccNodePGrp>
```

ステップ 3 スイッチ プロファイルにスイッチ ポリシー グループを関連付けます。

```
<infraNodeP descr="" dn="uni/infra/nprof-leafP-103" name="leafP-103" nameAlias="" ownerKey=""
ownerTag="">
<infraLeafS descr="" name="103_Sel" nameAlias="" ownerKey="" ownerTag="" type="range">
<infraRsAccNodePGrp tDn="uni/infra/funcprof/accnodepgrp-COPP_PreFilter_BGP_Config"/>
<infraNodeBlk descr="" from_="103" name="nblk1" nameAlias="" to_="103"/>
</infraLeafS>
</infraNodeP>
```

REST API を使用したスパインの CoPP プレフィルタ ポリシーの設定

このセクションでは、REST API を使用してスパイン スイッチの CoPP プレフィルタ ポリシーを設定する方法について説明します。

ステップ 1 許可リストのエントリとともに CoPP プレフィルタのスイッチ ポリシーを作成します。

```
<iaclSpineProfile descr="" dn="uni/infra/iaclspinep-spine_icmp" name="COPP_PreFilter_OSPF_Config"
ownerKey="" ownerTag="">
<iaclEntry dstAddr="0.0.0.0/0" dstPortFrom="unspecified" dstPortTo="unspecified" ipProto="ospfigp"
 name="" nameAlias="" srcAddr="0.0.0.0/0" srcPortFrom="unspecified" srcPortTo="unspecified"/>
</iaclSpineProfile>
```

ステップ 2 CoPP プレフィルタ ポリシーでスイッチ ポリシー グループを作成します。

```
<infraSpineAccNodePGrp descr="" dn="uni/infra/funcprof/spaccnodepgrp-COPP_PreFilter_OSPF_Config"
name="COPP_PreFilter_OSPF_Config" nameAlias="" ownerKey="" ownerTag="">
```

```
<infraRsIaclSpineProfile tnIaclSpineProfileName="COPP_PreFilter_OSPF_Config"/>
</infraSpineAccNodePGrp>
```

ステップ 3 スイッチ プロファイルにスイッチ ポリシー グループを関連付けます。

```
<infraSpineP descr="" dn="uni/infra/spprof-204" name="204" nameAlias="" ownerKey="" ownerTag="">
<infraSpineS descr="" name="204" nameAlias="" ownerKey="" ownerTag="" type="range">
<infraRsSpineAccNodePGrp tDn="uni/infra/funcprof/spaccnodepgrp-COPP_PreFilter_OSPF_Config"/>
<infraNodeBlk descr="" from_="204" name="nodeblock1" nameAlias="" to_="204"/>
</infraSpineS>
<infraRsSpAccPortP tDn="uni/infra/spaccportprof-204"/>
</infraSpineP>
```

次のタスク

第 11 章

ファブリック セキュリティ

この章は、次の項で構成されています。

連邦情報処理標準（FIPS）について

連邦情報処理標準（FIPS）発行 140-2、暗号化モジュールのセキュリティ要件では、暗号化モジュールの米国政府要件が詳述されています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

FIPS の注意事項と制約事項

FIPS には、次の注意事項および制約事項が適用されます。

- FIPS が有効になっている場合、FIPS はCisco Application Policy Infrastructure Controller（APIC）全体に適用されます。
- FIPS が有効の場合は、Cisco APIC を FIPS がサポートされていないリリースにダウングレードする前に、FIPS を無効にする必要があります。
- パスワードは最小限 8 文字の長さで作成してください。
- Telnet をディセーブルにします。SSH のみを使用してログインします。
- SSH サーバーの RSA1 キー ペアすべてを削除してください。

- セキュア シェル（SSH） および SNMP がサポートされます。
- SNMP v1 および v2 をディセーブルにしてください。SNMPv3 に対して設定された、スイッチ上の既存ユーザ- アカウントのいずれについても、認証およびプライバシー用 AES3 は SHA でのみ設定されていなければなりません。
- 2.3(1) 以降のリリースでは、FIPS はスイッチレベルで構成できます。
- 3.1(1) 以降のリリースでは、FIP が有効になっている場合、NTP は FIPS モードで動作します。FIPS モードでは、NTP は HMAC-SHA1 による認証ありと認証なしをサポートしています。
- 5.2(3) 以前のリリースでは、Cisco APIC で FIPS を有効にした後、デュアルスーパーバイザスパインスイッチを 2 回再読み込みして FIPS を有効にします。
- 5.2(4) 以降のリリースでは、Cisco APIC で FIPS を有効にした後、デュアルスーパーバイザスパインスイッチを再読み込みしてから電源を入れ直し、FIPS を有効にします。
- 5.2(3) 以前のリリースでは、FIPS が有効になっているデュアルスーパーバイザ スパインスイッチで、すべてのスーパーバイザを交換した場合、FIPS を有効にするためにスパインスイッチを 2 回再読み込みする必要があります。
- 5.2(4) 以降のリリースでは、FIPS が有効になっているデュアルスーパーバイザ スパインスイッチで、すべてのスーパーバイザを交換した場合、スパインスイッチを再読み込みしてから、FIPS を有効にするために電源を再投入する必要があります。
- 5.2(3) 以前のリリースでは、RADIUS および TACACS+ リモート認証方式を無効にします。FIPS モードでは、ローカルおよび LDAP 認証方法のみがサポートされています。
- 5.2(4) 以降のリリースでは、RADIUS、TACACS+、RSA、DUO、OAuth2、および SAML リモート認証方式を無効にします。FIPS モードでは、ローカルおよび LDAP 認証方法のみがサポートされています。

GUI を使用した Cisco APIC の FIPS の設定

FIPS が有効になっている場合、Cisco Application Policy Infrastructure Controller(APIC) 全体に適用されます。

ステップ 1 メニュー バーで、**[システム（System）]** > **[システム設定（System Settings）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ファブリック セキュリティ（Fabric Security）]** を選択します。

ステップ 3 **[作業]** ペインの **[プロパティ]** 領域で、目的の FIPSモードを選択します。

FIPSモードのオプションは、**[無効化]** と **[有効化]** です。デフォルト値は **[無効（Disable）]** です。

（注） 設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。

NX-OS Style CLI を使用した Cisco APIC 向けの FIPS を設定する

FIPS を有効にすると、Cisco Application Policy Infrastructure Controller(APIC) 全体に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 **例**： `apic1# configure`	
ステップ 2	FIPS を有効にします。 **例**： `apic1(config)# fips mode enable`	設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。 **no fips mode enable** コマンドにより FIPS が無効になります。

REST API を使用した Cisco APIC の FIPS の設定

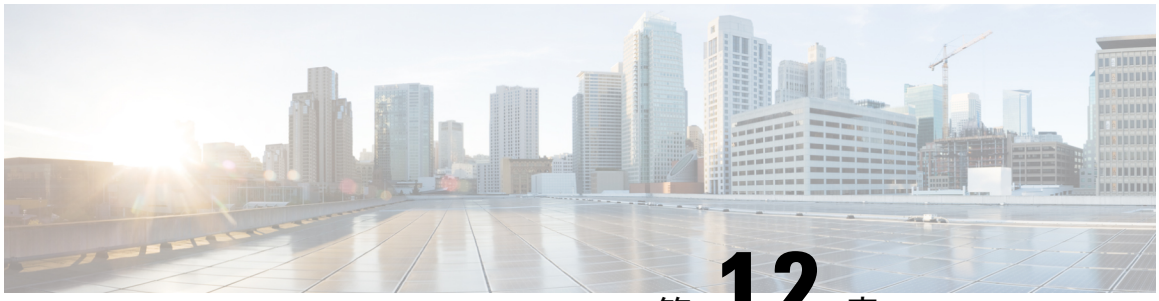
FIPS を有効にすると、Cisco APIC 全体に適用されます。

すべてのテナントの FIPS を設定します。

例：

```
https://apic1.cisco.com/api/node/mo/uni/userext.xml
<aaaFabricSec fipsMode="enable" />
```

（注） 設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。



第 12 章

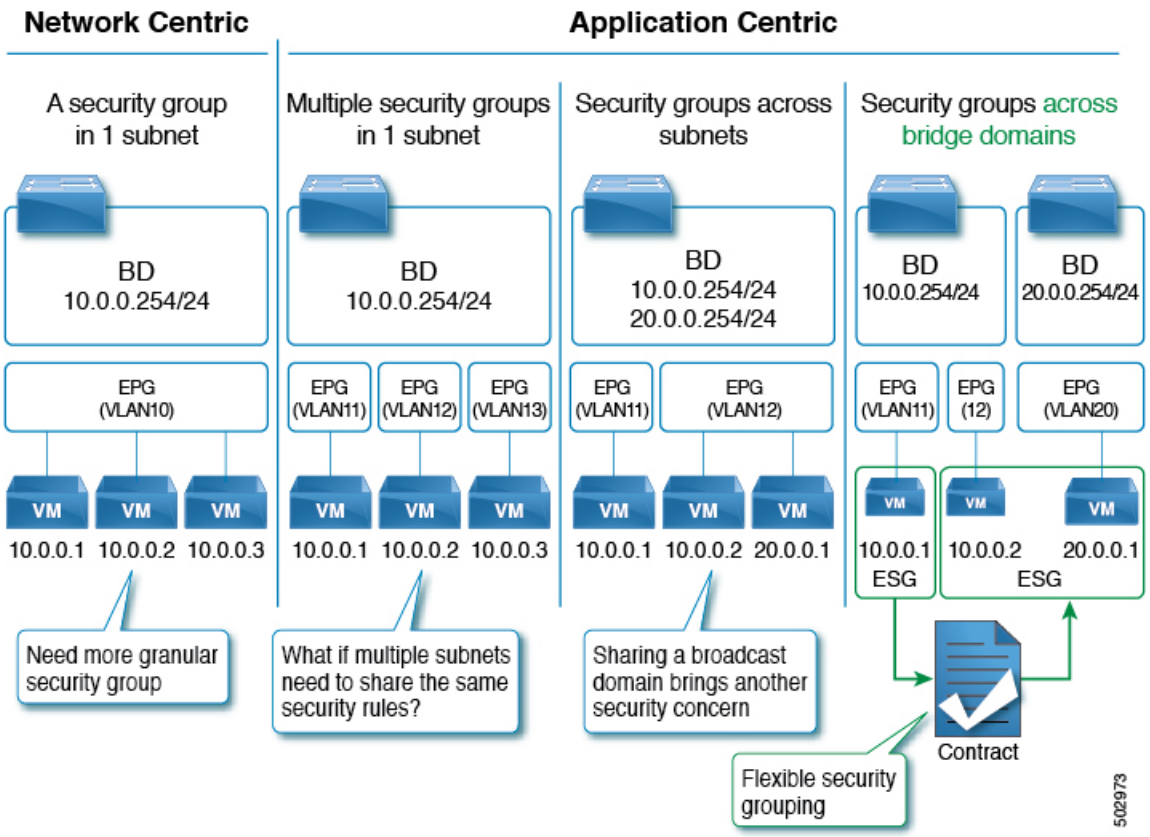
エンドポイント セキュリティ グループ

この章の内容は、次のとおりです。

エンドポイント セキュリティ グループについて

エンドポイントセキュリティ グループ（ESG）は、Cisco Application Centric Infrastructure（ACI）のネットワーク セキュリティ コンポーネントです。エンドポイントグループ（EPG）では Cisco ACI のネットワーク セキュリティを提供してきましたが、EPG は単一のブリッジドメインに関連付けられ、ブリッジドメイン内のセキュリティ ゾーンを定義するために使用する必要があります。これは、EPG が転送とセキュリティ セグメンテーションの両方を同時に定義するためです。ブリッジドメインと EPG の間の直接的な関係により、EPG が複数のブリッジドメインにまたがる可能性は制限されています。EPG のこの制限は、新しい ESG 構造を使用することで解決できます。

図 *5 : Cisco ACI* では、複数のセグメンテーション オプションを提供します



EPG を表すアプリケーション エンドポイントグループ（fvAEPg）オブジェクトは、レイヤ 2 ブロードキャストドメインを表すブリッジドメイン オブジェクト (fvBD) と直接関係があります。これは、上の図の最初の 3 列に示されています。

ESG は、物理または仮想ネットワークエンドポイントの収集を含む論理エンティティです。さらに、ESG はブリッジドメインではなく単一の VRF（仮想ルーティングおよび転送）インスタンスに関連付けられます。これにより、ブリッジドメインから独立したセキュリティ ゾーンの定義が可能になります（図 *1* の 4 番目の列は、この点を示しています）。EPG がブリッジドメインをセキュリティ ゾーンに分割するのと同様に、ESG は VRF インスタンスをセキュリティ ゾーンに分割します。

EPG ポリシーには、転送ロジックとセキュリティロジックの両方が組み込まれています。たとえば、EPG は、VLAN に基づくセキュリティゾーンだけでなく、リーフノードインターフェイスでの VLAN バインドも提供します。また EPG のコントラクトによってセキュリティを強化し、ブリッジドメイン サブネットを展開する必要があるリーフ ノードと、VRF ルート リーク（共有サービス）の場合にどのサブネットをどの VRF インスタンスにリークするかを決定するために使用されます。逆に、ESG はコントラクトによってセキュリティを強化するためにのみ使用され、転送ロジックは他のコンポーネントによって処理されます。ESG では、ブリッジドメイン サブネットの展開や VRF ルート リークなどのルーティング ロジックが VRF レベルに移動します。リーフノード インターフェイスの VLAN バインドは、引き続き EPG レベルで処理されます。

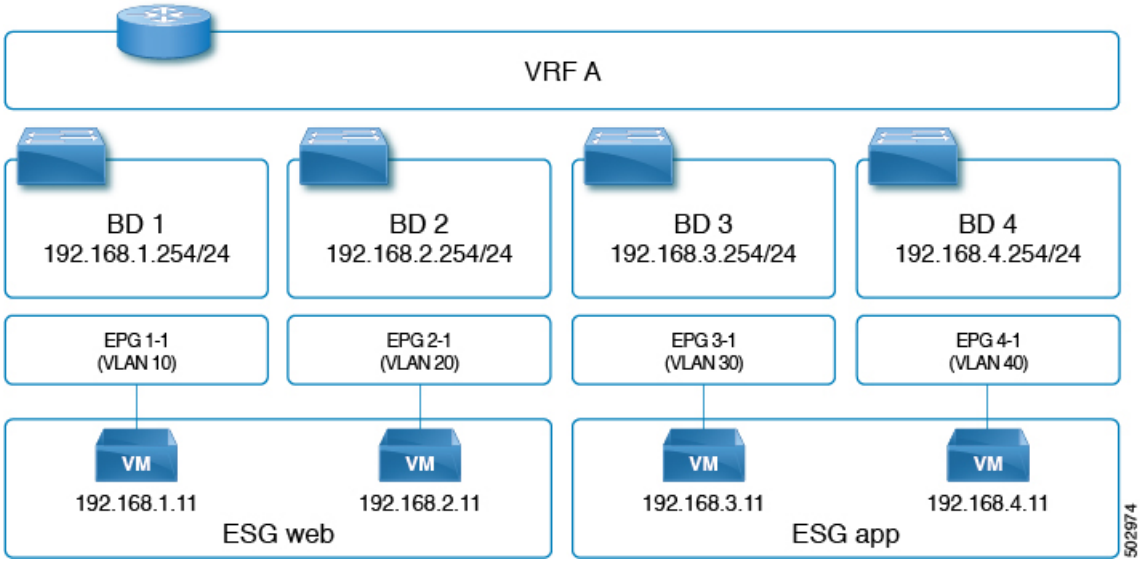
ESG はどのエンドポイントが ESG に属するかを定義する特定の一致基準を持つセキュリティ コンストラクトであり、コントラクトまたはポリシーを使用してセキュリティスタンスを定義します。一致基準は、関連付けられた VRF インスタンスのブリッジドメインにまたがる IPv4 または IPv6 アドレス、またはエンドポイント MAC アドレスに関連付けられたタグなどの属性に基づく ESG セレクタと呼ばれます。これらのセレクタおよびその他のサポートされているセレクタタイプの詳細については、「セレクターについて（158 ページ）」 を参照してください。

ESG でのコントラクトの使用は、EPG と同じです。同じ ESG に属するエンドポイントは、コントラクトを必要とせずに通信できます。異なる ESG に属するエンドポイント間の通信を有効にするには、ESG 間のコントラクトを構成する必要があります。Cisco ACI ファブリックの外部にあるデバイスと通信するには、L3Out 外部 EPG（`l3extInstP`）と ESG の間のコントラクトを構成する必要があります。ESG 間のコントラクトと組み合わせて、レイヤ 4 ～ レイヤ 7 サービスグラフを使用することもできます。ただし、EPG と ESG 間のコントラクトはサポートされていません。

ESG から ESG へのトラフィック フィルタリング

次の図では、4 つのブリッジ ドメインがそれぞれ 1 つの EPG に関連付けられています。管理者は EPG 設定を使用して、仮想マシンまたは物理サーバーからのトラフィックが、適切な VLAN に接続された適切なブリッジ ドメインに関連付けられていることを確認します。たとえば、EPG1-1 は VLAN 10 からのトラフィックの BD1 へのマッピングを定義し、EPG2-1 は VLAN 20 を BD2 にマッピングします。

図 *6 : ESG* を使用して、異なるサブネットのエンドポイントを集約できます



- VLAN 10 の 192.168.1.11 と VLAN 20 の 192.168.2.11 は、異なるサブネットと異なるブリッジ ドメインに属しています。
- 管理者は、192.168.1.11 と 192.168.2.11 を同じ ESG に属するものとして定義します。

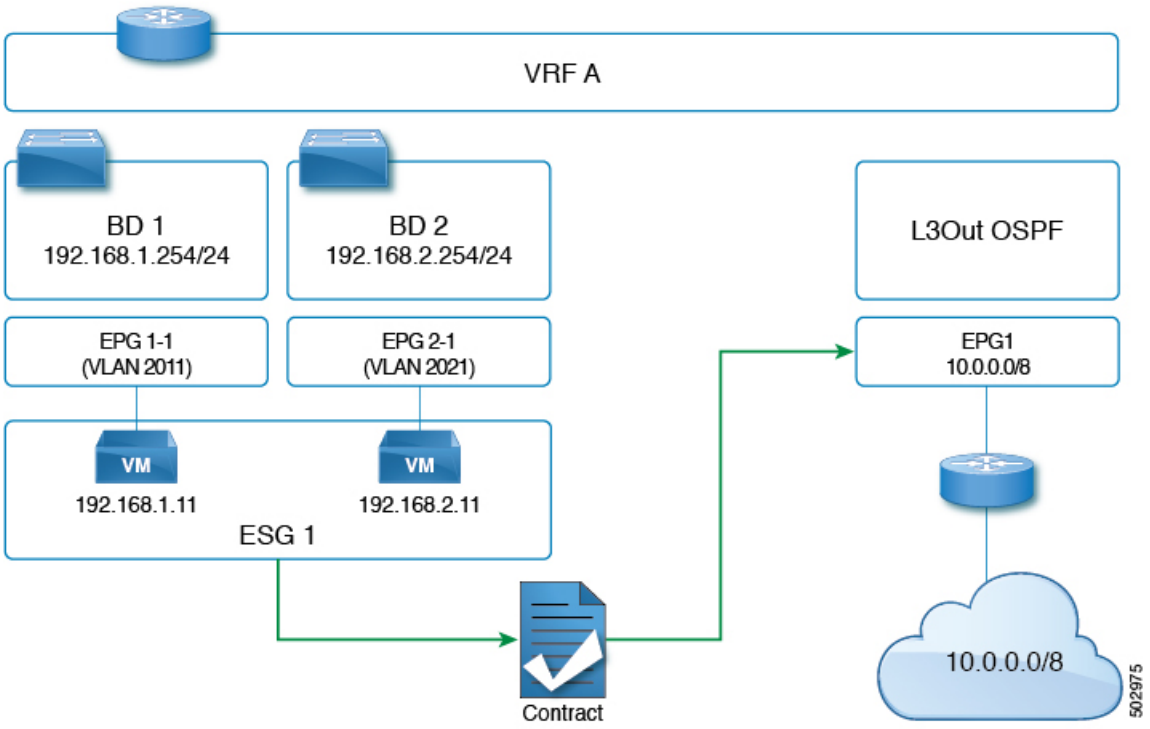
- 同様に、192.168.3.11 と 192.168.4.11 はそれぞれ BD3 と BD4（EPG3-1 と EPG4-1 経由）に関連付けられており、両方とも同じ ESG に属しています。
- 上記の設定により、192.168.1.11 は 192.168.2.11 と自由に通信できます。
- 同様に、192.168.3.11 は 192.168.4.11 と通信できます。ただし、192.168.1.11（または 192.168.2.11）は、契約なしでは 192.168.3.11 または 192.168.4.11 のいずれとも通信できません。

（注） EPG によって使用される契約は、ESG によって再利用できません。その逆も同様です。

外部から ESG へのトラフィック フィルタリング

外部から ESG への通信を許可する設定は、次の図に示すように、L3Out 外部 EPG（`l3extInstP`）と ESG 間の契約によって実行されます。L3Out の観点からは、ESG との契約と EPG との契約の間に違いはありません。

図 *7: ESG* から外部への接続は、*L3* 外部 *EPG* を使用して実装されます。



ESG の導入

このセクションでは、管理者が ESG を設定する場合に、Cisco APIC によってリーフノードをプログラムする方法をまとめます。

- 各 ESG は VRF に関連付けられており、ESG セレクタは VRF 内のどのエンドポイントが ESG に属するかを定義します。
- VRF（ESG が設定されている場所）は、入力または出力ポリシー適用モードで構成できます。
- Cisco ACI は、関連付けられた VRF が展開されているすべてのリーフノードで ESG 構成をインスタンス化します。
- ESG が構成されている場合、関連付けられた VRF 内のすべての BD サブネットは、その VRF が存在するすべてのリーフノード上で、スパインプロキシへの静的ルートとして存在します。
- ESG は常にオンデマンドの即時展開によって展開され、関連するコントラクトルールは、ESG セレクタに一致するエンドポイントが特定のリーフノードで学習された後にのみプログラムされます。
- ESG 間のコントラクトは、EPG の場合と同様に、リーフノード TCAM の policy-cam ルールとしてプログラムされます。
- ESG によって使用されるクラス ID は、グローバル pcTag です。コンテキストによっては、sclass と呼ばれます。
- EPG とは異なり、ESG 間のコントラクトはセキュリティルールのみを作成します。ESG は、サブネット展開やルートリークなどのネットワーク展開には使用されません。
- EPG、BD、および VRF コンストラクトは、ネットワーク フォワーディング コンストラクトに対して通常どおり構成する必要があります。ただし、セキュリティ定義は、EPG からアプリケーション中心のセキュリティを適用する ESG に移動されます。このようなシナリオでは、EPG の機能は VLAN をインターフェイスにバインドすることです。

（注） Cisco APIC は、EPG の場合と同様に、各 ESG を識別するため固有の番号を生成します。この番号は、pcTag またはクラス ID と呼ばれます。一部のコンテキストでは、sclass、S クラス、またはソースクラスと呼ばれます。

グローバル pcTag は、ESG（または EPG）が属する VRF に関係なく、ファブリック全体で固有の番号です。ESG には常にグローバル pcTag が割り当てられます。グローバル pcTag 番号の範囲は 16 ～ 16385 です。

ローカル pcTag は、VRF 範囲内で固有の番号です。つまり、Cisco APIC は同じ番号を生成して、異なる VRF 内の別の EPG を識別できます。ローカル pcTag 番号の範囲は 16386 ～ 65535 です。

1 から 15 までの pcTag 番号は、システム内部で使用するために予約されています。

セレクタ

セレクターについて

セレクタは、エンドポイントを ESG に分類するためのさまざまなマッチング基準を使用し、各 ESG の下に構成されます。VLAN を使用してエンドポイントを分類する EPG とは異なり、ESGはより柔軟な基準を使用してエンドポイントを分類できます。この概念は、マイクロセグメンテーション EPG（または useg EPG）に似ています。ただし、useg EPG は 1 つのブリッジドメインに関連付けられたままですが、ESGにはブリッジドメイン全体のエンドポイントを含めることができます。

サポートされている ESG セレクタは次のとおりです。

- **タグセレクタ**：MAC および IP アドレス、仮想マシン（VM）タグ、仮想マシン名（vm 名）、サブネットタグ、静的エンドポイントタグなどのさまざまな属性に割り当てられたポリシータグに基づいてエンドポイントをマッチングします。ESG タグセレクタは、ESG と同じテナントのポリシータグのみとマッチングできます。タグセレクタは Cisco APIC リリース 5.2(1) で導入されました。
- **EPG セレクタ**：特定の EPG 内のすべてのエンドポイントとマッチングし、ESG は EPG の下で構成されたすべてのコントラクトを継承します。このセレクタを使用すると、ユーザーはセキュリティ構成を EPG から ESG にシームレスに移行できます。ESG は、ESG と同じ VRF 内の EPG に対してのみ EPG セレクタを使用できます。EPG セレクタは、Cisco APIC リリース 5.2(1) で導入されました。
- **IP サブネットセレクタ**：ホストの IP アドレスまたは IP サブネットに基づいてエンドポイントをマッチングします。タグセレクタは、ポリシータグを介して同じ機能を提供します。IP サブネットセレクタは、Cisco APIC リリース 5.0(1) で導入されました。
- **サービス EPG セレクタ**：サービス EPG セレクタは、Cisco APIC リリース 5.2(4) で導入されました。

  サービス EPG は、デバイス選択ポリシーのコネクタに基づいて ACI が自動的に作成する EPG です。サービス グラフ リダイレクトに基づくほとんどの展開では、ACI がトラフィックをレイヤ 4 からレイヤ 7 デバイスにリダイレクトするため、レイヤ 4 からレイヤ 7 デバイスに直接送信されるトラフィックを許可または拒否するために特別なことを構成する必要はありません。レイヤ 4 からレイヤ 7 のデバイス IP アドレスにトラフィックを直接送信する必要がある場合は、サービス EPG へのトラフィックを許可または拒否する必要がある場合があります。サービス EPG セレクタを使用すると、サービス EPG をサービス ESG にマッピングできるため、管理者は、サービス グラフを介して展開されたレイヤ 4 からレイヤ 7 デバイスにトラフィックを送信できる ESG をより細かく制御できます。

タグ セレクターについて

タグセレクタはポリシータグを使用して、エンドポイントを特定の ESG に分類します。ポリシー タグは、「キー：所有者、値：ジョン」などのキーと値で構成されます。ポリシー タグ

は、ユーザが構成可能なさまざまなオブジェクトに割り当てることができ、Cisco Application Centric Infrastructure（ACI）機能はそれらのタグに基づいて動作します。ポリシータグを使用したセキュリティ分類は、複数のエンドポイントをセキュリティグループ(ESG)に追加するために簡単で直感的な操作ができます。ポリシータグと ESG タグセレクタを使用すると、各エンドポイントを個別に指定することなく、選択した複数のエンドポイントを ESG に分類できます。

ESG タグ セレクタは、ESG と同じテナントのポリシータグのみに一致します。この分離により、各テナントが独自のリソースを管理できるようになり、テナント間での意図しないポリシータグの一致が防止されます。ただし、ユーザ テナントがブリッジドメインまたは `Common` テナントからの VRF インスタンスを使用している場合、ユーザ テナントは構成を一部表示できない場合があることに注意してください。

構成は似ていますが、ポリシータグ（ユーザー定義可能な tagTag など）は、注釈（tagAnnotation）とは目的と使用方法が異なります。相違点の詳細については、*Cisco APIC System Management Configuration Guide*の「Alias, Annotations, and Tags」の章を参照してください。

ESG タグセレクタは、次のオブジェクトに割り当てられたポリシータグと一致します。

名前	説明	オブジェクト
BD サブネット	ブリッジドメインの下のサブネット	fvSubnet
IP エンドポイントタグ	エンドポイントのホスト IP アドレスのメタデータ	fvEpIpTag
MAC エンドポイントタグ	エンドポイントの MAC アドレスのメタデータ	fvEpMacTag
VMM MAC エンドポイントタグ	VMM 統合を介して派生したメタデータ	fvEpVmmMacTagDef
静的エンドポイント	静的エンドポイント	fvStCEp

（注） 仮想マシンを名前で選択する場合、仮想マシンが ESG に関連付けられる前に、VM が関連付けられている EPG の EPG セレクタを作成する必要があります。

次のセクションでは、サポートされているオブジェクトの各タイプのポリシータグの使用について説明します。

BD サブネットのポリシータグ

ブリッジドメインサブネットに割り当てられたポリシータグを照合することにより、タグセレクタはサブネット内のすべての IP エンドポイントを特定の ESG に分類できます。IP サブネットセレクタに似ていますが、ポリシータグとタグ セレクタを使用すると、特定の MAC アドレ

スなどのさまざまなタイプのパラメータに加えて、複数の IP サブネットをグループ化できます。

また、[**デフォルトの SVI ゲートウェイなし（No Default SVI Gateway**）] オプションを使用してより小さい BD サブネットを作成し、その小さいサブネットにポリシータグを割り当てることにより、BD サブネットのサブセットを一致させることができます。このオプションを使用すると、対応する SVI を展開せずにブリッジドメインの下にサブネットを構成できます。

BD サブネットのポリシータグに一致するタグセレクタを構成する場合は、次の注意事項を考慮してください。

- タグセレクタは、別のテナントの BD サブネットのポリシータグと一致させることはできません。たとえば、ESG がテナント「A」にあり、ブリッジドメインがテナント `Common` で構成されている場合、テナント「A」のタグ セレクタは、そのブリッジドメインのポリシータグと一致させることはできません。このようなケースでサブネットベースの分類が必要な場合は、代わりに IP サブネットセレクタを使用します。
- EPG サブネットの下のポリシータグは、ESG タグセレクタではサポートされていません。ESG では、EPG の下にサブネットを構成する必要はありません。ESG は、以前は EPG に結合されていたネットワークとセキュリティの構成を分離することにより、構成を簡素化することを目的としています。
- BD サブネットのポリシー タグに一致するタグ セレクタは、エンドポイントの IP アドレスのみを ESG に分類し、MAC アドレスは分類しません。このため、ここでは IP ベースのセレクタによるレイヤ 2 トラフィック制限が適用されます。詳細については、IP ベースセレクターによるレイヤー 2 トラフィック制限 （175 ページ）を参照してください。

IP エンドポイントタグのポリシータグ

エンドポイント（fvCEp、fvIp）を表すオブジェクトは、Cisco ACI スイッチのエンドポイント学習ステータスに基づいて動的に作成および削除されるため、そのようなオブジェクトにポリシー タグを直接割り当てることは実用的ではありません。そのため、エンドポイントの IP アドレスを表すために、新しいユーザによって構成可能なオブジェクトである IP エンドポイント タグが Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) で導入されました。IP エンドポイントタグ オブジェクトは、IP アドレスがエンドポイントとして学習される前でも作成し、維持できます。このオブジェクトを使用すると、いつでもエンドポイントの IP アドレスにポリシータグを割り当てることができます。

IP エンドポイントタグには VRF の範囲があり、特定の VRF で構成したホスト IP アドレスを表します。タグは、IP アドレスのメタデータまたは記述子です。IP エンドポイントタグを構成しても、エンドポイントまたは指定された IP アドレスは展開されません。エンドポイントが学習される前にエンドポイントとその IP アドレスを静的に展開する必要がある場合は、静的エンドポイントを構成します。

IP エンドポイントタグのポリシータグに一致するタグセレクタを構成するときは、次の注意事項を考慮してください。

- IP エンドポイントタグのポリシータグに一致するタグセレクタは、エンドポイントの IP アドレスのみを ESG に分類し、MAC アドレスは分類しません。このため、ここでは IP

ベースのセレクタによるレイヤ 2 トラフィック制限が適用されます。詳細については、IP ベース セレクターによるレイヤー 2 トラフィック制限 （175 ページ）を参照してください。

MAC エンドポイントタグのポリシータグ

エンドポイント（fvCEp、fvIp）を表すオブジェクトは、Cisco ACI スイッチのエンドポイント学習ステータスに基づいて動的に作成および削除されるため、そのようなオブジェクトにポリシー タグを直接割り当てることは実用的ではありません。そのため、エンドポイントの MAC アドレスを表すために、新しいユーザによって構成可能なオブジェクトである MAC エンドポイント タグが Cisco APIC リリース 5.2(1) で導入されました。MAC アドレスをエンドポイントとして学習する前でも、MAC エンドポイント タグオブジェクトを作成し、維持できます。このオブジェクトを使用して、いつでもエンドポイントの MAC アドレスにポリシータグを割り当てることができます。

MAC エンドポイント タグにはブリッジドメインの範囲があり、特定のブリッジドメインで構成した MAC アドレスを表します。MAC アドレスがブリッジドメイン全体で固有の場合は、ブリッジドメインの範囲を「任意」（「*」）として指定し、代わりにその範囲として VRF を提供できます。タグは、MACアドレスの単なるメタデータまたは記述子です。MACエンドポイントタグを構成しても、エンドポイントまたは指定された MAC アドレスは展開されません。エンドポイントが学習される前にエンドポイントとその MAC アドレスを静的に展開する必要がある場合は、静的エンドポイントを構成します。

VMM MAC エンドポイントタグのポリシータグ

Cisco APIC は VMM 統合を通じて学習した情報に基づいて、読み取り専用の VMM MAC エンドポイント ポリシー タグ（fvEpVmmMacTagDef）を自動的に入力します。Cisco APIC は VMM 統合を通じてエンドポイントに関する情報を取得し、その情報を各エンドポイントのポリシータグにマップします。手動で作成する MAC エンドポイント タグオブジェクトと同様に、VMM MAC エンドポイント タグオブジェクトは、対応するエンドポイントがデータプレーンでまだ学習されていない場合でも、ポリシータグを維持するための MAC アドレスの単なるメタデータまたは記述子です。ESG タグセレクタは、これらのポリシータグを使用して、エンドポイントを ESG に分類できます。

次の VMM 情報は、ESG タグセレクタによってサポートされます。

統合のタイプ	出典情報	翻訳されたポリシータグの形式
VMware vSphere 分散スイッチ（vDS）	VM 名	キー：`__vmm::vmname` 値：*VM name*
VMware vSphere 分散スイッチ（vDS）	vSphere タグ 「カテゴリ：タグ名」	キー：カテゴリ 値：タグ名

VMM MAC エンドポイントタグと VM の名前から変換されたポリシータグは、Cisco APIC の **[テナント（Tenant）] > [ポリシー（Polices）] > [エンドポイント タグ（Endpoint Tags）] > [エ**

ンドポイント MAC（Endpoint MAC）] の下に自動的に入力されます。これを有効にするには、VMM ドメインを EPG に関連付けるときに [**マイクロセグメンテーションを許可（Allow Micro-Segmentation**）] を有効にする必要があります。これらのタグは、手動で構成された MAC エンドポイントタグと区別するために、サフィックス「（VMM）」を付けて表示されます。VMware タグなど、VM の名前以外で翻訳されたポリシータグは、ESG タグセレクタで一致するまで VMM MAC エンドポイントタグで生成されません。また、対応する VMM ドメインで**タグコレクション**を有効にする必要があります。変換された各ポリシータグは、エンドポイントの MAC アドレスに割り当てられます。

MAC エンドポイント タグが、VMM MAC エンドポイント タグと同じブリッジドメインの同じ MAC アドレスで構成されている場合、MAC エンドポイント タグのポリシー タグのみが使用されます。この場合、VMM MAC エンドポイントタグからの変換されたポリシータグは無視されます。

静的エンドポイントのポリシータグ

EPG で構成された静的エンドポイントに割り当てられたポリシータグを照合することにより、タグセレクタは静的エンドポイントの MAC アドレスを特定の ESG に分類できます。静的エンドポイントのポリシータグサポートにより、静的エンドポイントと同じ MAC アドレスに MAC エンドポイントタグを構成する必要がなくなります。実際、これら 2 つの構成は互いに互換性がありません。まとめると、次のようになります。

- ポリシー タグが静的エンドポイントに割り当てられている場合、同じブリッジドメインで同じ MAC アドレスを持つ MAC エンドポイント タグを構成することはできません。
- MAC エンドポイント タグが MAC アドレスに割り当てられている場合、ポリシー タグを同じブリッジドメイン内の同じ MAC アドレスを持つ静的エンドポイントに割り当てることはできません。

静的エンドポイントタグは、**silent-host** タイプの静的エンドポイントに対してのみサポートされます。

EPG セレクターについて

EPG セレクタは、EPG 全体を ESG に一致させます。EPG セレクタを使用して複数の EPG を ESG に一致させることができますが、それは EPG が ESG と同じテナントおよび同じ VRF にある場合のみです。EPG セレクタは、ブリッジドメインにまたがる複数の VLAN を単一のセキュリティグループ（ESG）としてグループ化し、コントラクトの構成を簡素化するのに最適です。

EPG が EPG セレクタによって ESG に一致すると、EPG 内のすべてのエンドポイントが ESG に属し、すべてのセキュリティ構成が ESG によって処理されるようになりました。

EPG セレクタには次の特徴があります。

- EPG に基づく既存のコントラクトは、ESG によって継承されます。
- EPG は新しいコントラクトを消費または提供できません
- EPG 内分離は、ESG 内の ESG 内分離によって上書きされます。

• EPG の優先グループメンバーシップは、ESG によって上書きされます。

EPG が EPG セレクタを介して ESG に一致する場合、EPG と ESG の下での EPG 内/ESG の分離と優先グループメンバーシップの設定は同じである必要があります。一致後、ESG 設定は EPG 設定を上書きします。

EPG から ESG へのコントラクトの継承により、既存の EPG セキュリティ設計から新しい ESG セキュリティ設計へのシームレスな移行が可能になります。構成を簡素化して ESG の利点を十分に活用するために、移行を完了し、EPG から ESG への通信のために継承された EPG コントラクトを永続的な構成として保持しないことをお勧めします。ESG に EPG セレクタによって継承されたコントラクトがある場合、APIC は EPG から ESG への移行がまだ完了していないことを示す警告とリマインダとしてエラーを発生させます。EPGセレクタを使用した移行の詳細については、「ESG 移行計画」セクションを参照してください。

EPG が EPG セレクタによって ESG に一致すると、EPG のポリシー制御タグ（pcTag）が ESG の pcTag に置き換えられます。pcTag の置換操作により、EPG のエンドポイントで一時的なトラフィックの小規模の中断が発生する場合があります。これは、EPG で共有サービス（ルートリーク）を構成する場合など、他の機能で発生する他の pcTag 更新イベントと同じ影響があります。pcTag は ESG に固有ではなく、タグセレクタによって使用されるポリシータグ（tagTag）とは関係がないことに注意してください。pcTag は、データプレーンでコントラクトを適用するための EPG/ESG 識別子です。

IP サブネット セレクターの詳細

IP サブネット セレクターは、IP アドレスに基づいてエンドポイントを ESG に分類します。特定のエンドポイントに一致するようにホスト IP アドレスを設定するか、サブネット内の複数の IP アドレスに一致するようにサブネットを設定できます。

IP エンドポイント タグ セレクターは、エンドポイントの IP アドレスのみを ESG に分類し、MAC アドレスは分類しません。このため、ここでは IP ベースのセレクターによるレイヤー 2 トラフィック制限が適用されます。詳細については、「*IP* ベースのセレクターによるレイヤー *2* トラフィックの制限」を参照してください。

サービス EPG セレクターについて

リリース 5.2(4) より前のリリースでは、サービスグラフを通じて作成されたサービス EPG とのコントラクトを作成することはできません。この制限には、次のような特定の課題があります。

- [**直接接続（Direct Connect）**] オプションを使用して、サービス EPG からコンシューマーまたはプロバイダー EPG へのトラフィックの許可ルールを追加できます。ただし、コンシューマーやプロバイダー EPG ではない EPG は、vzAny コントラクトまたは優先グループをあわせて構成しなければ、サービス EPG と通信できません。
- vzAny にはサービス EPG が含まれているため、vzAny から vzAny へのコントラクトは、サービス EPG と VRF 内の他の EPG との間のトラフィックを許可できます。ただし、これは VRF 内の他のすべての EPG がサービス EPG と通信できることも意味しますが、VRF 内の特定の EPG のみを制限してサービス EPG と通信できるようにする必要がある場合もあります。

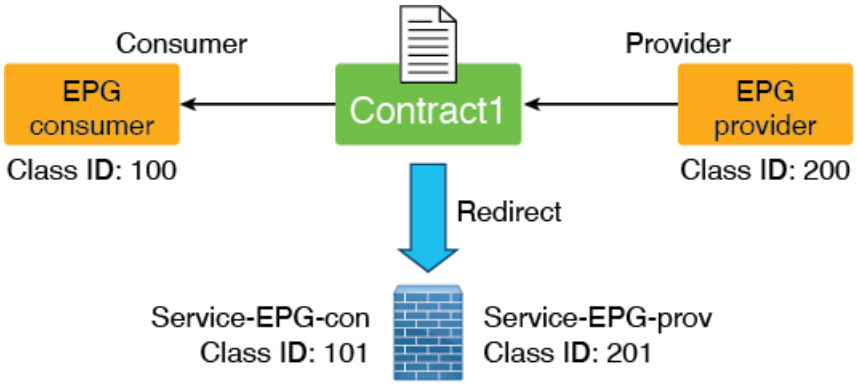
リリース 5.2(4) 以降のリリースでは、エンドポイントセキュリティ グループ (ESG) のサービス EPG セレクタが使用できるようになりました。この機能により、サービス EPG を ESG にマッピングし、その ESG とのコントラクトを作成できます。この機能を使用すると、vzAny-to-vzAny 許可コントラクトが構成されている場合でも、サービス ESG と他の ESG の間に拒否コントラクトを追加して、特定の ESG がサービス ESG と通信できるようにすることができます。

次のセクションでは、サービス EPG セレクタを使用する場合と使用しない場合の構成例と、サービス EPG セレクタの使用に関する追加情報について説明します。

- サービス EPG セレクタを使用しない構成例 （164 ページ）
- サービス EPG セレクタを使用した構成例 （168 ページ）
- ESG およびサービス EPG のサポートされている場所とサポートされていない場所 （170 ページ）
- サービス EPG セレクタの注意事項と制限事項 （174 ページ）

サービス EPG セレクタを使用しない構成例

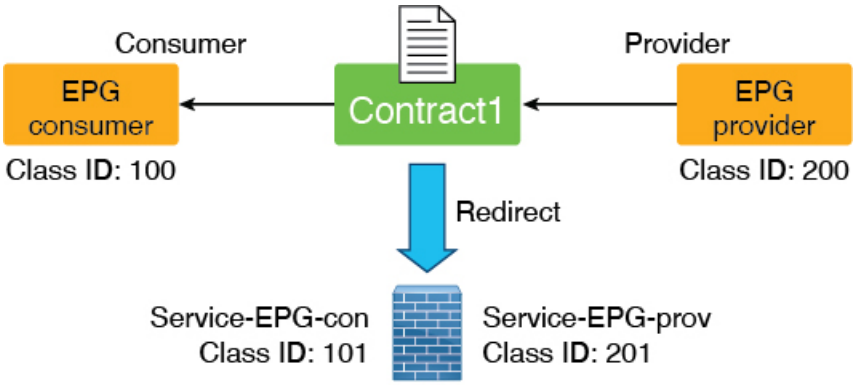
リリース 5.2(4) で導入されたサービス EPG セレクタ オプションを使用せずに必要な構成を有効にするには、[**直接接続（Direct Connect）**] オプションを使用できます。次の図は、[**直接接続（Direct Connect）**] オプションがデフォルト（無効）設定の構成例を示しています。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	100	Redirect
101	100	permit

504130

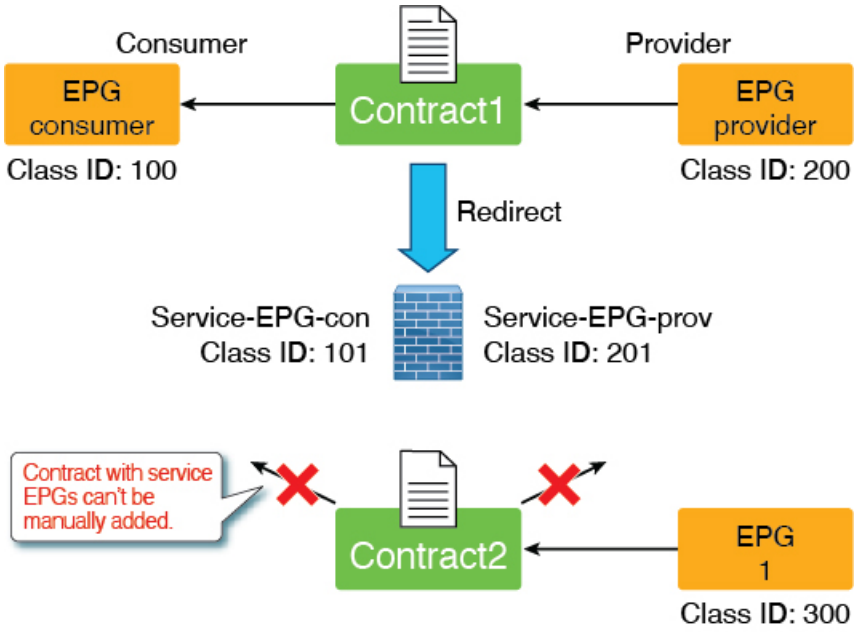
次の図は、[**直接接続（Direct Connect）**] オプションが有効になっている例を示しています。サービス EPG からコンシューマーまたはプロバイダー EPG へのトラフィックに許可ルールが追加されます。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	201	permit
200	100	Redirect
101	100	permit
100	101	permit

504131

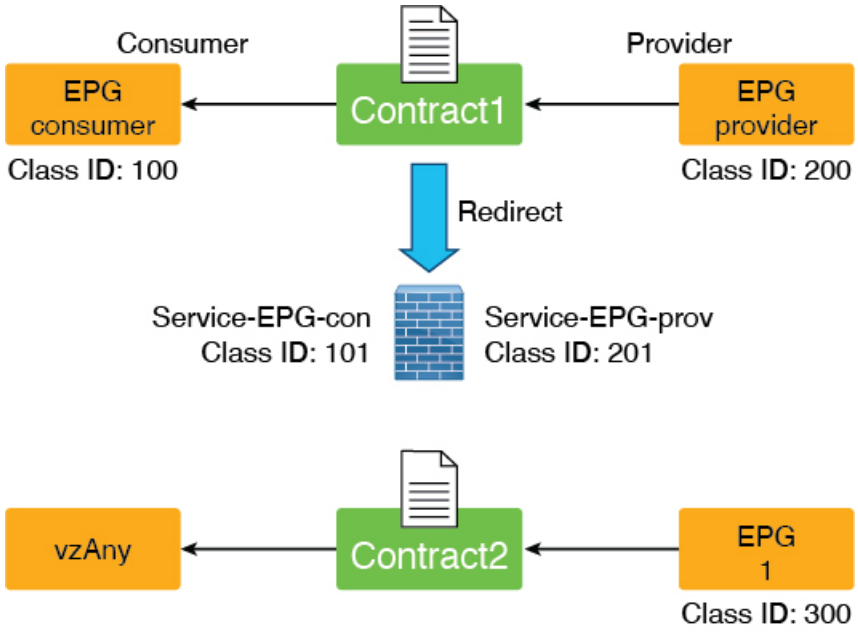
ただし、[**直接接続（Direct Connect**）] オプションが有効になっていても、コンシューマーまたはプロバイダー EPG ではない EPG にはサービス EPG の許可ルールがなく、コントラクトを手動で追加することはできません。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	201	permit
200	100	Redirect
101	100	permit
100	101	permit

504132

この制限を回避する方法の 1 つとして、次の図に示すように、サービス EPG が vzAny 構成の一部である vzAny コントラクトを構成する方法があります。

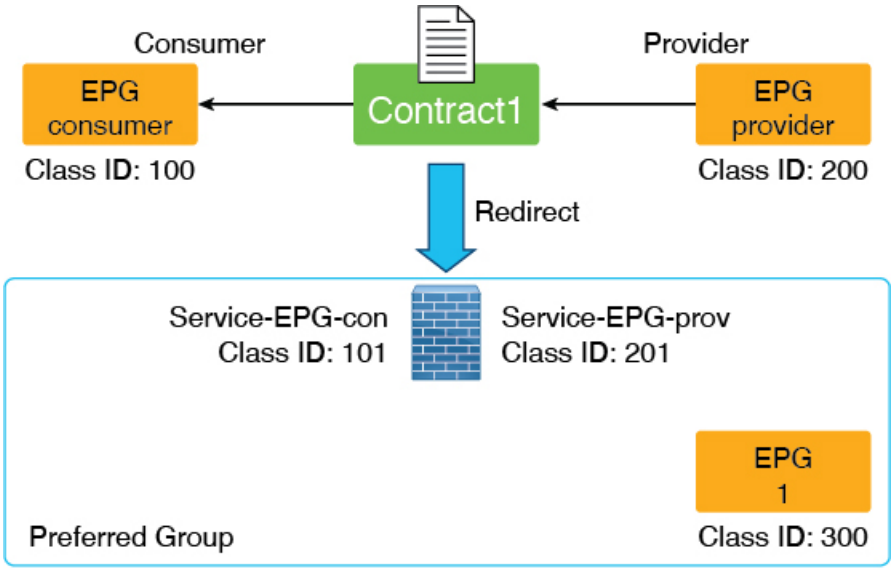


Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	100	Redirect
101	100	permit
0	300	permit
300	0	permit

504133

ただし、この回避策で考慮する事項として、EPG（前の例のクラス ID 300）も VRF 内の他の EPG と通信できることがあります。

2 番目に考えられる回避策は、次の図に示すように優先グループを構成することです。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	100	Redirect
101	100	permit
0	0	permit
0	100	deny
100	0	deny
0	200	deny
200	0	deny

504134

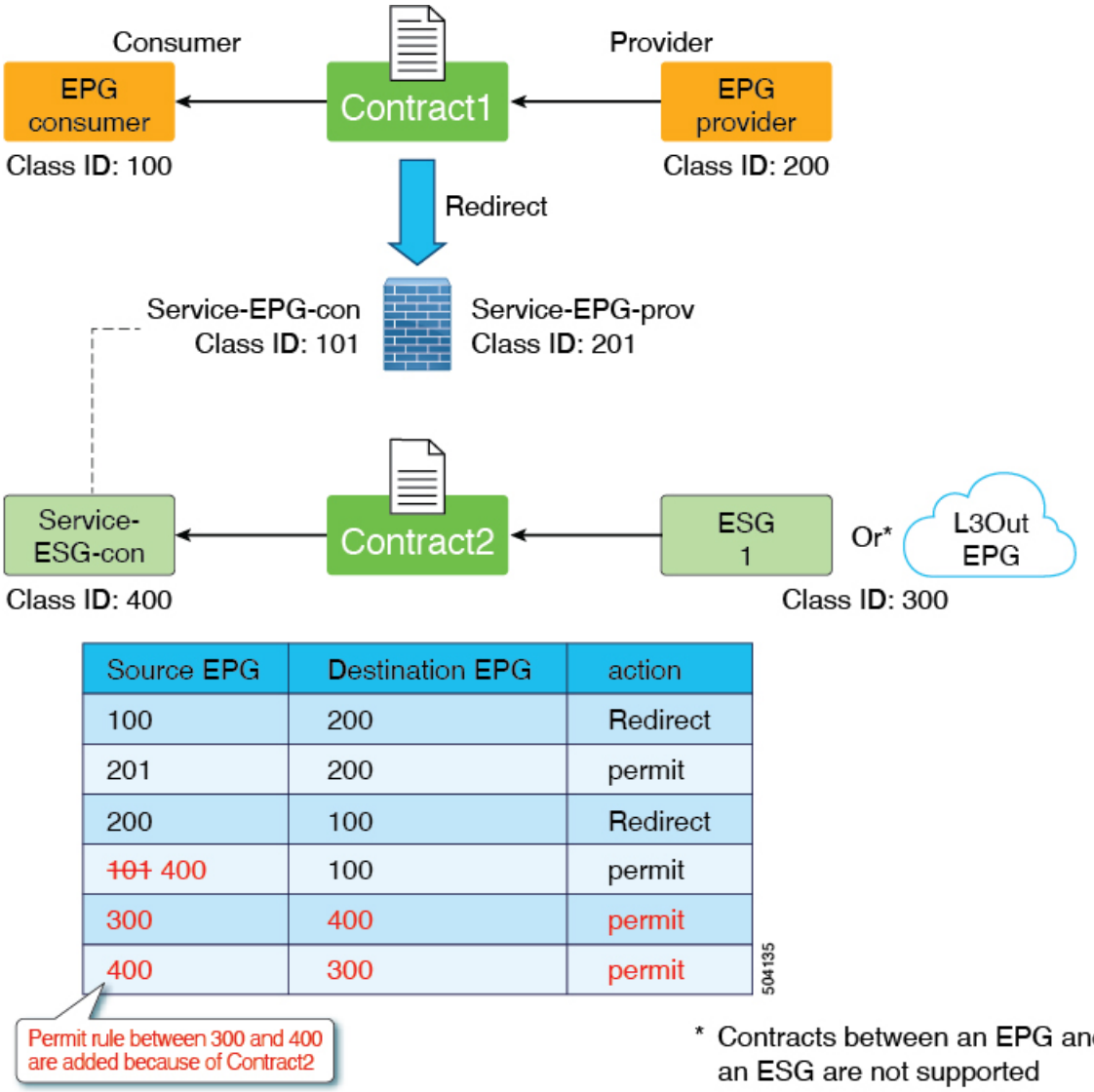
ただし、この 2 番目の回避策で考慮する事項として、優先グループ内の他の EPG がコントラクトなしで相互に通信できてしまうことがあります。また、より多くの TCAM リソースを消費する可能性もあります。

状況に対し、どちらの回避策も有効なソリューションではない場合、次のセクションで説明するように、リリース 5.2(4) 以降で利用可能なサービス EPG セレクタオプションを使用できます。

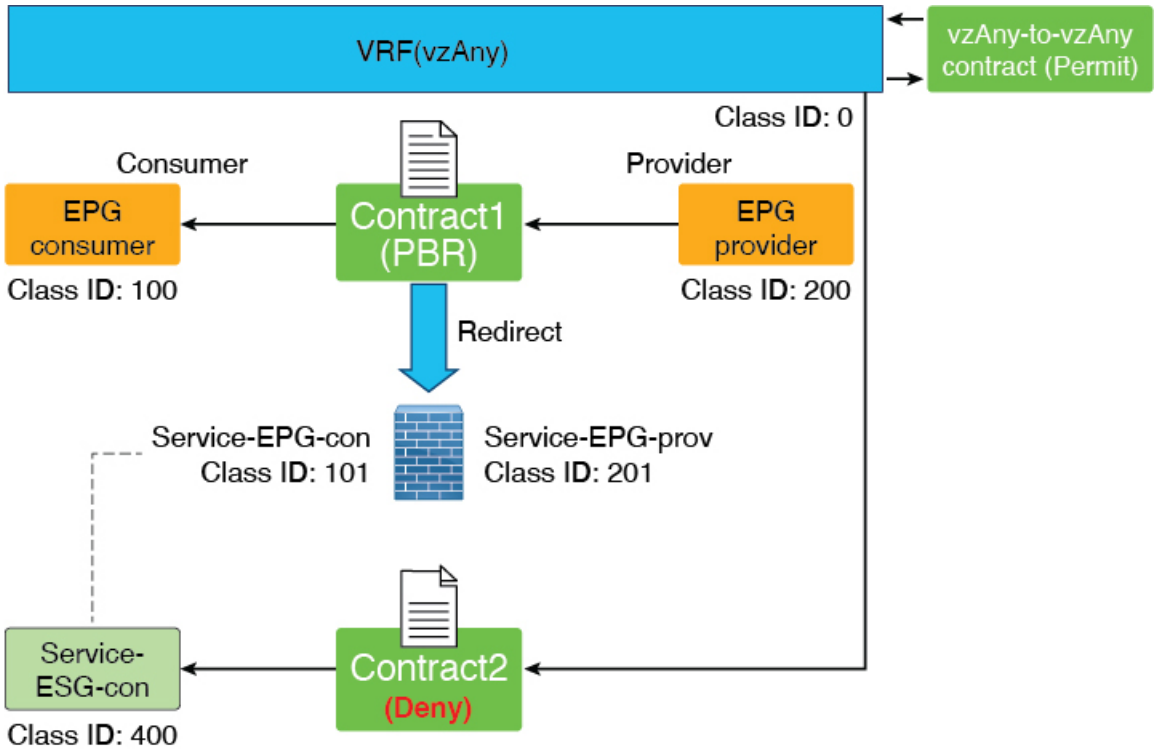
サービス EPG セレクタを使用した構成例

リリース 5.2(4) 以降で利用可能になったサービス EPG セレクタを使用すると、サービス EPG（`LifCtx`）を表すサービスデバイスコネクタを ESG にマッピングできます。これにより、ESG とのコントラクトを追加できます。さらに、サービス EPG セレクタを使用すると、サービス EPG に関連するゾーン分割ルールが継承されます。

サービス EPG セレクタを使用した構成例を次の図に示します。



サービス EPG セレクタ機能を使用するもう 1 つの方法は、vzAny-to-vzAny 許可コントラクトでサービスデバイスインターフェイスを除外することです。このシナリオでは、vzAny-to-vzAny を使用して VRF 内のすべてのトラフィックを許可しますが、次の図に示すように、サービスデバイス インターフェイスとの通信も禁止します。



Source EPG	Destination EPG	action
0	0	permit
100	200	Redirect
201	200	permit
200	100	Redirect
~~101~~ 400	100	permit
0	400	deny
400	0	deny

504136

Deny rules between 0 and 400 are added because of Contract2.

ESG およびサービス EPG のサポートされている場所とサポートされていない場所

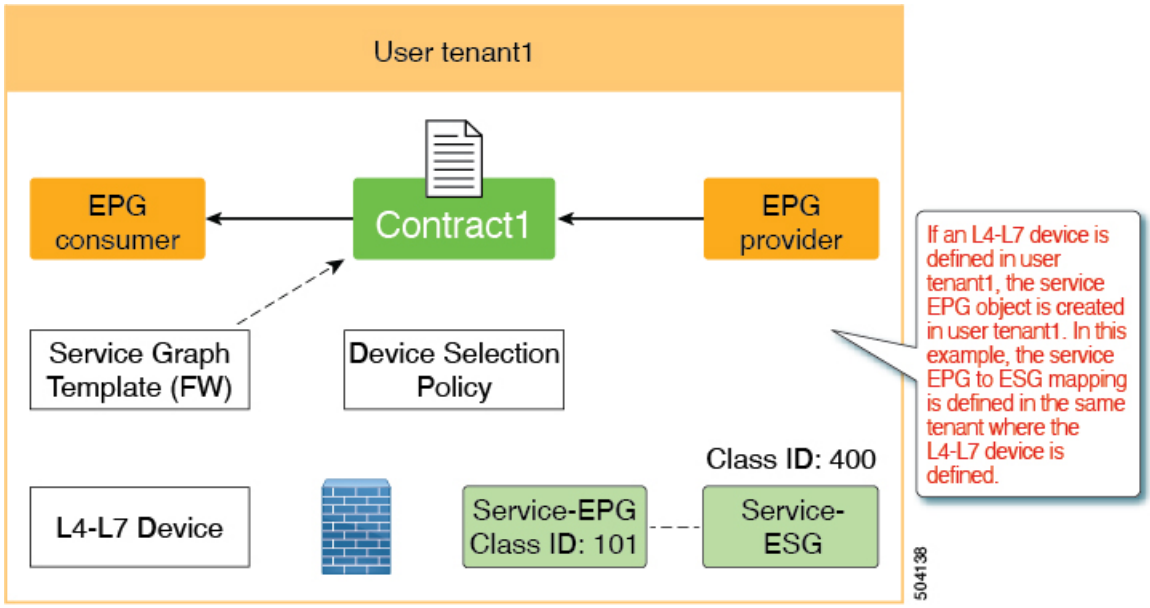
このセクションでは、ESG およびサービス EPG のサポートされているロケーションとサポートされていないロケーションに関する情報を提供します。

このセクションは、管理者が ESG からレイヤ 4 からレイヤ 7 デバイスに向けられたトラフィックを許可または拒否する必要がある設計にのみ関連します。レイヤ 4 からレイヤ 7 デバイスにリダイレクトされるトラフィックは、このカテゴリに属さず、このセクションで説明されてい

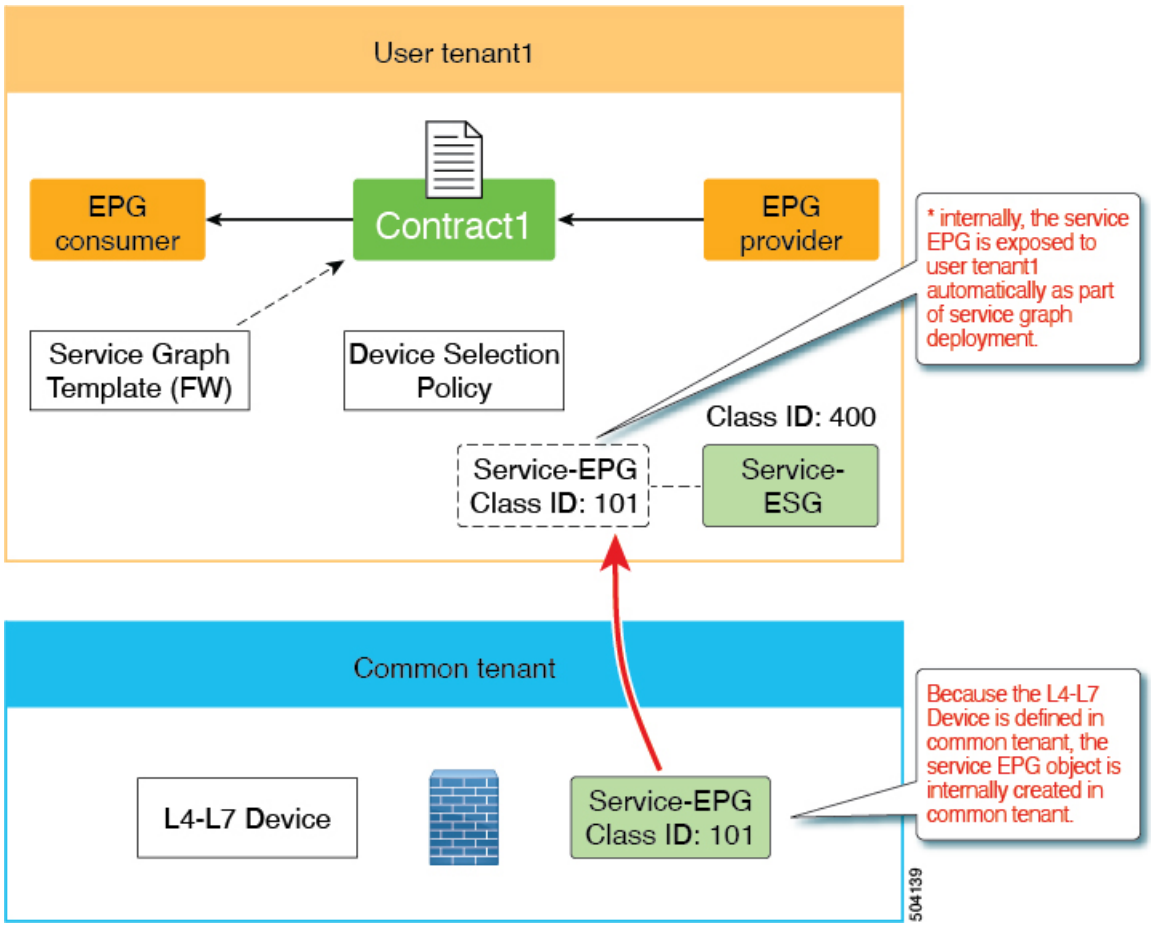
る制限の対象ではありません。これは、リダイレクトされたトラフィックの宛先 IP アドレスがエンドポイントであり、レイヤ 4 からレイヤ 7 のデバイス IP アドレスではないためです。

（注） サービス EPG は、レイヤ 4 ～ レイヤ 7 デバイスが定義されているテナントで内部的に作成されます。

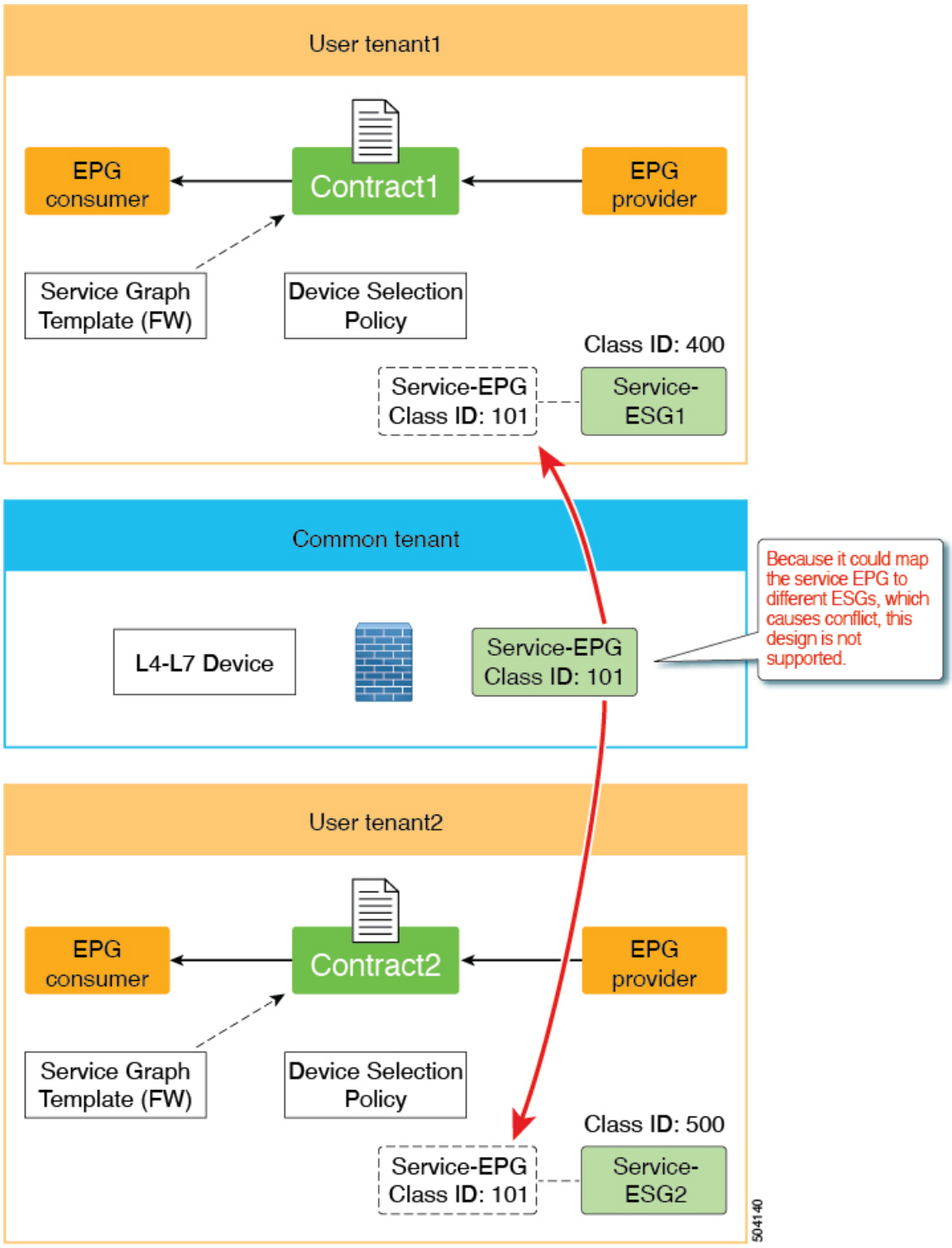
- **サポート**：レイヤ 4 ～ レイヤ 7 デバイスとサービス EPG から ESG へのマッピングは、同じテナントで定義されます。



- **サポート**：レイヤ 4 ～ レイヤ 7 デバイスは共通テナントにあり、サービス EPG から ESG へのマッピングはユーザーテナントで定義されます。下の図の例では、共通テナントのレイヤ 4 ～ レイヤ 7 デバイスが、サービスグラフが構成されているユーザーテナント `tenant1` にエクスポートされます。



- **サポート対象外**：レイヤ4～レイヤ7デバイスは共通のテナントにあり、複数のテナント間で共有されます。つまり、サービス EPG から ESG へのマッピングは複数のユーザーテナントで実行されます。

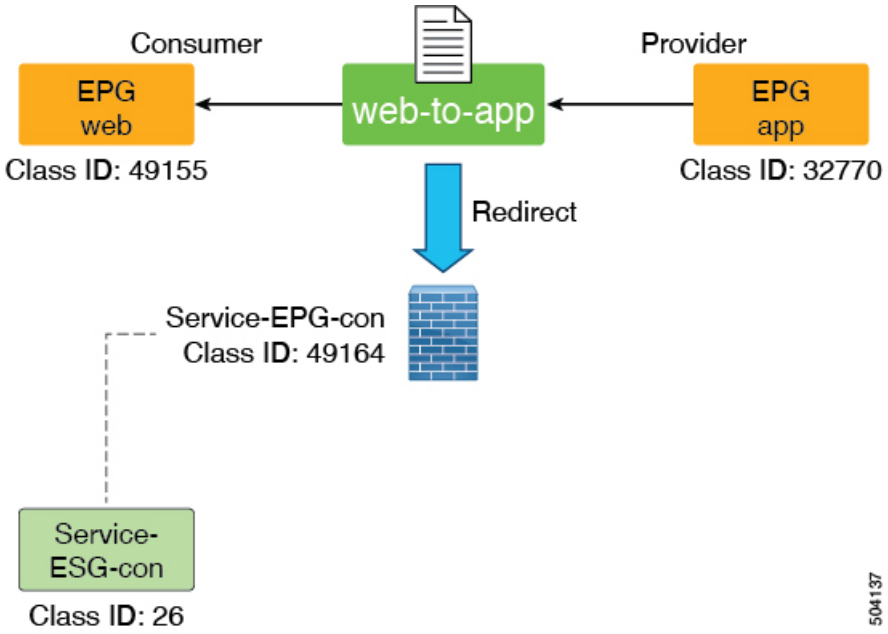

User tenant1
EPG consumer
Contract1
EPG provider
Service Graph Template (FW)
Device Selection Policy
Class ID: 400
Service-EPG Class ID: 101
Service-ESG1
Common tenant
L4-L7 Device
Service-EPG Class ID: 101
Because it could map the service EPG to different ESGs, which causes conflict, this design is not supported.
User tenant2
EPG consumer
Contract2
EPG provider
Service Graph Template (FW)
Device Selection Policy
Class ID: 500
Service-EPG Class ID: 101
Service-ESG2
504140

サービス EPG セレクタの注意事項と制限事項

次に、リリース 5.2(4) で導入されたサービス EPG セレクタ機能の注意事項と制限事項を示します。

- サービス EPG に関連するゾーン分割ルールは継承されますが、サービス EPG のクラス ID は、グローバルクラス ID を使用する ESG にマッピングされるため、グローバルクラス ID に変更されます。サービス EPG のクラス ID が変更されると、トラフィック損失が発生します。
- 同じブリッジドメインを使用する同じデバイス内のすべてのサービスデバイスコネクタ（`LifCTx`）は、同じ ESG にマッピングする必要があります。

  たとえば、次の図に示すように、PBR サービスグラフを使用してワンアームモードのファイアウォールを構成したとします。



  この例では、コンシューマーコネクタとプロバイダーコネクタは同じブリッジドメインにあり、同じサービス EPG を使用しています。この場合、両方のコネクタを同じ ESG にマップする必要があります。同じサービス EPG を使用するコネクタが同じ ESG にマッピングされていない場合、障害が発生し、サービスグラフの展開は失敗します。

  複数のサービスグラフの展開にサービスデバイスインターフェイスを再利用できることに注意してください。

- サービス EPG と ESG は同じ VRF にある必要があります。
- 現時点では、NDO は ESG をサポートしていないため、この機能は NDO ではサポートされていません。
- サポートは、ブリッジドメインの PBR 宛先を持つレイヤ 3 PBR でのみ使用できます。

- L3Out の PBR 宛先はサポートされていません（コントラクトは L3Out EPG により手動で構成できます）
- レイヤ 1/レイヤ 2 PBR はサポートされていません (レイヤ 1/レイヤ 2 デバイスインターフェイスはサーバーと直接通信することを想定していません)

IP ベース セレクターによるレイヤー 2 トラフィック制限

ESG ではさまざまな分類方法があるため、IP アドレスと MAC アドレスの分類の相違点を理解することが重要です。この相違点は、基本的にマイクロセグメント（uSeg）EPG 基準と同じです。

パケットがスイッチによってルーティングされる場合、転送ルックアップは IP アドレスに基づいて行われます。パケットがスイッチによってスイッチングされる場合、パケットに IP ヘッダーがある場合でも、転送ルックアップは MAC アドレスに基づいて行われます。同様に、パケットがスイッチによってルーティングされる場合、コントラクトルックアップは IP アドレスに基づいています。パケットがスイッチによって切り替わる場合、パケットに IP ヘッダーがある場合でも、コントラクトルックアップは MAC アドレスに基づいています。この動作は、以下のように ESG に基づくコントラクトの適用に影響します。

IP ベースのセレクタ（IP サブネットセレクタ、BD サブネットまたは IP エンドポイント タグオブジェクトのポリシータグに一致するタグセレクタなど）は、IP アドレスのみを分類します。このような分類は、スイッチングトラフィックには適用されません。一方、他のセレクタは MAC アドレスを分類し、そのような分類はスイッチングトラフィックとルーティングトラフィックの両方に有効です。これは、別の IP ベースのセレクタによってオーバーライドされない限り、MAC ベースのセレクタが MAC アドレスに関連付けられた IP アドレスにも適用されることを意味します。この動作は、次の 3 つのシナリオで示されています。

これらのシナリオでは、エンドポイント EP_A は EPG_A のメンバーであり、最初はどの ESG にも属していません。EP_A の MAC アドレスは MAC_A で、その IP アドレスは IP_A です。

```
Scenario 1:
    MAC_A is matched by a selector of ESG_1
    IP_A is _not_ matched by any ESG
  Result:
    Both MAC_A and IP_A are classified to ESG_1

Scenario 2:
    MAC_A is matched by a selector of ESG_1
    IP_A is matched by a selector of ESG_2
  Result:
    MAC_A is classified to ESG_1
    IP_A is classified to ESG_2

Scenario 3:
    MAC_A is _not_ matched by any ESG
    IP_A is matched by a selector of ESG_2
  Result:
    MAC_A is _not_ classified to any ESG, and still belongs to EPG_A.
    IP_A is classified to ESG_2
```

この動作により、トラフィックの送信元と宛先の IP アドレスが異なる ESG に属している場合でも、IP ベースのセレクタが使用されている場合、スイッチングトラフィック（レイヤ2 トラフィック）が ESG コントラクトをバイパスする可能性があります。IP ベースのセレクタでこの問題を回避するには、ACI のプロキシ ARP 機能を使用して、送信元と接続先の IP アドレスが同じサブネットにある場合でも、すべてのトラフィックが ACI スイッチでルーティングされたトラフィックとして処理されるようにする必要があります。この目的でプロキシ ARP を使用するには、次の 3 つのオプションがあります。

- ESG エンドポイントに VLAN からインターフェイスへのバインドを提供するすべての EPG で、プロキシ ARP とともに EPG 内分離を有効にします。
- ESG エンドポイントに VLAN からインターフェイスへのバインドを提供するすべての EPG で、共通のデフォルトコントラクトなどのすべて許可（permit-all）フィルタを使用して、EPG 内コントラクトを有効にします。EPG 内コントラクトにより、プロキシ ARP が自動的に有効になります。すべて許可する（permit-all） フィルタである理由は、どの ESG にも分類されていないエンドポイントが、同じ EPG 内で相互に通信できるようにするためです。ESG にまだ分類されていないエンドポイントのデフォルトの動作として、任意のフィルタを使用できます。
- VMM 統合が使用されている場合に、ESG エンドポイントに VLAN からインターフェイスへのバインドを提供する EPG に VMM ドメインを関連付ける際に、[**マイクロセグメンテーションを許可（Allow Micro-Segmentation**）] オプションを有効にします。このオプションは、プロキシ ARP を自動的に有効にします。

同じサブネット（または VLAN）内のエンドポイントが異なる ESG に分類されるレイヤ 2 トラフィックの場合、IP ベースのセレクタによるレイヤ2 トラフィックの制限に関係なく、プライベート VLAN 構成が必要になる場合があります。エンドポイントと ACI スイッチの間に非 ACI スイッチがある場合は、プライベート VLAN 構成が必要になる場合があります。これは、ACI スイッチが ESG に基づいてコントラクトを実施できるようになる前に、非 ACI スイッチがトラフィックをスイッチングする可能性があるためです。

セレクターの優先順位

セレクタータイプを選択するときは、トラフィックを切り替えるかルーティングするかを考慮してください。以下の表は、トラフィック タイプごとのセレクターの優先順位を示しています。

表 *13 :* スイッチング トラフィックの優先順位

優先順位	セレクタ
1	タグ セレクター（エンドポイント MAC タグ） タグ セレクター（静的エンドポイント）
2	タグ セレクター（エンドポイント VMM MAC タグ）
3	EPG セレクター

表 *14* : ルーティング トラフィックの優先順位

優先順位	セレクタ
1	タグ セレクター（エンドポイント IP タグ） IP サブネット セレクタ（ホスト IP）
2	タグ セレクター（BD サブネット） IP サブネット セレクター（サブネット）
3	タグ セレクター（エンドポイント MAC タグ） タグ セレクター（静的エンドポイント）
4	タグ セレクター（エンドポイント VMM MAC タグ）
5	EPG セレクター

オブジェクトが同じまたは異なるポリシー タグを介して複数のタグ セレクターで一致した場合、そのオブジェクトは最初に一致したタグ セレクターに関連付けられます。後続のタグ セレクターは無視されます。タグセレクターが以前にオブジェクトに一致していないときに、オブジェクトが複数のタグセレクターによって一致した場合、競合の一致が解決されるまでタグセレクターは有効になりません。障害は、複数のタグ セレクターによって一致する ESG およびオブジェクトの下で発生します。

コントラクト

コントラクトは、アクセスコントロールリスト（ACL）に相当する Cisco ACI です。ESG は、コントラクト規則に従う場合に限り、他の ESG と通信できます。管理者は契約を使用して、許可されているプロトコルとポートを含む ESG 間をパス可能なトラフィックの種類を選択します。ESG は、コントラクトのプロバイダー、コンシューマー、またはプロバイダーとコンシューマーの両方になることができ、複数のコントラクトを同時に使用できます。複数の ESG が優先グループに属する他の ESG と自由に通話できるように、ESG は優先グループに属することもできます。

サポートされているコントラクト関係：

1. ESG ⇔ ESG
2. ESG ⇔ L3Out EPG
3. ESG ⇔ インバンド EPG
4. ESG ⇔ vzAny

ESG と EPG（または uSeg EPG）の間のコントラクトはサポートされていません。ESG のエンドポイントが EPG の他のエンドポイントと通信する必要がある場合、他のエンドポイントを最初に ESG に移行する必要があります。 vzAny または優先グループは、移行中に代替として

使用できます。コントラクト継承、ESG内コントラクト、ESG内分離など、uSeg EPGでサポートされるその他のコントラクト関連機能もESGでサポートされます。例外は、ESGでサポートされていない禁止コントラクトです。

vzAny

ESG間の特定のコントラクトを使用する代わりに、vzAnyと呼ばれるConstructを使用してESG間のトラフィックを許可することもできます。

vzAnyは、特定のVRFインスタンス内のすべてのESGおよびEPGを表します。これには、VRFインスタンス内のL3Out外部EPG（`l3extInstP`）も含まれます。vzAny Constructは、そのVRFインスタンス内のすべてのEPGとESGを簡単に参照できるようにします。vzAny参照は、VRFインスタンス内のすべてのEPGおよびESGの単一のコントラクト構成を可能にすることで管理を容易にし、各EPGまたはESGに個別にではなく、この1つのグループにコントラクトを適用することにより、ハードウェアリソースの消費を最適化します。

図 *8 : vzAny* は、同じ *VRF* インスタンス内のすべての *EPG* と *ESG* を表す省略形です。

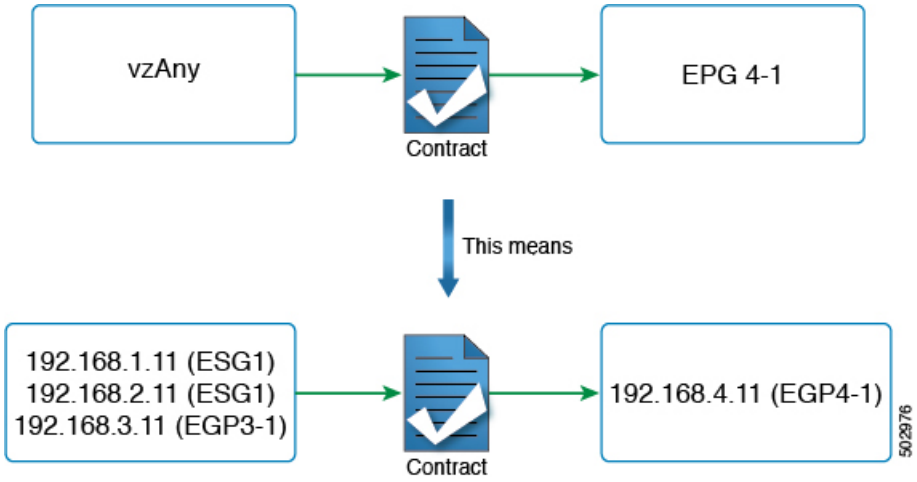


図4に例を示します。図2のトポロジで、管理者がvzAnyとEPG 4-1の間のコントラクトを構成した場合、エンドポイント192.168.1.11、192.168.2.11（ESG1）、および192.168.3.11（EPG3-1）は192.168.4.11（EPG4-1）と通信できます。

これは、ESG1とEPG3-1が同じセキュリティゾーンに属しており、192.168.11（または192.168.2.11）がコントラクトなしで192.168.3.11と通信できるという意味ではありません。必要な構成が、ESG、EPG、L3Out EPGなどに関係なく、VRFインスタンス内の任意の通信を許可することである場合、ユーザーは、VRFインスタンスで**ポリシーの適用**（非強制）を無効にする代わりに、すべてのトラフィックを許可するコントラクトを提供および消費するようにvzAnyを構成できます。

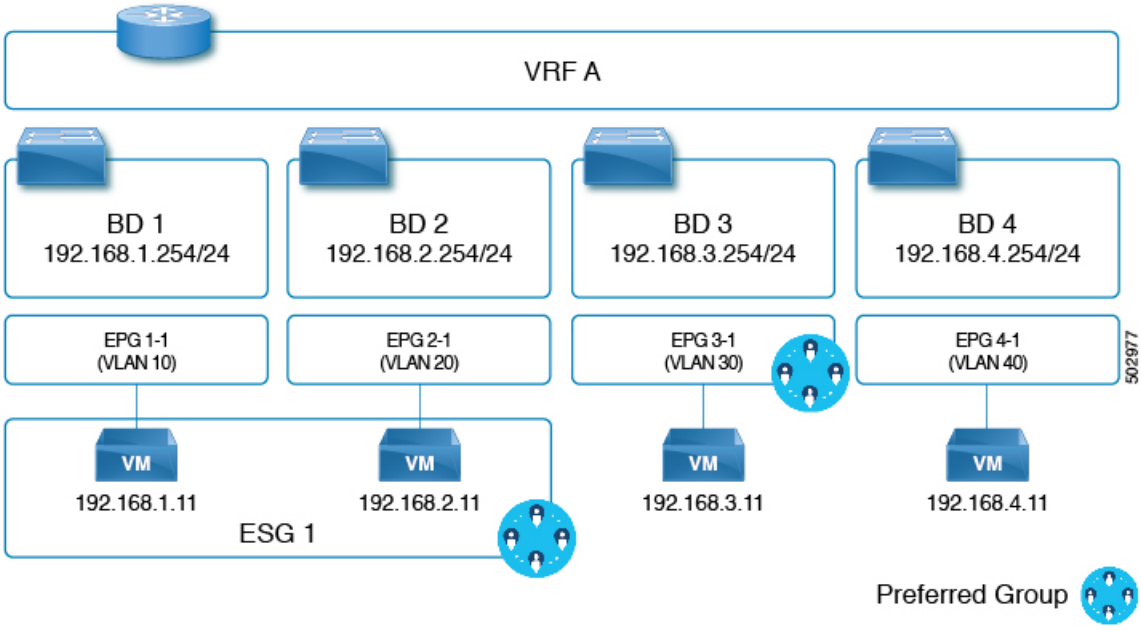
つまり、vzAny Constructによって、EPGと同様にESGがコントラクトを使用してVRFインスタンス内の誰とでも通信できるようにするために、コントラクトを提供および（または）消費するために使用できます。ESGとEPG間のコントラクトは許可されていませんが、vzAnyコントラクトを使用してESGとEPG間のトラフィックを許可できます。

優先グループ

優先グループは、ESG間で明示的な契約を使用したり、vzAny契約を使用したりする代わりに使用できます。ユーザーは、優先グループを設定して、VRF インスタンス内の ESG 間の通信を有効にすることもできます。優先グループ内のエンドポイントは、互いに自由に通信できます。

ユーザーは、優先グループを使用して、ESGからEPGへの通信を有効にすることもできます。これは、EPG ベース セキュリティ設定から ESG ベースのセキュリティ設定への移行に役立ちます。

図 *9*：同じ優先グループの *ESG1* および *EPG3-1* 部分の例。



上の図の例では、ESG1 と EPG3-1 が VRF A の優先グループの一部になるように設定されており、次の通信が許可されています。

1. ESG 1 と EPG 3-1 は、両方が優先グループに含まれているため、相互に通信できます。
2. ESG 1 と EPG 4-1 は、次の理由で相互に通信できません。
   - EPG 4-1 は優先グループに含まれません。
   - EPG と ESG 間の契約はサポートされていません。

優先グループの設定については、『Cisco APIC 基本設定ガイド』を参照してください。

ESG 共有サービス（ESG VRF ルート リーク）

エンドポイントが別の VRF によって共有されるサービスを必要とする場合、通信を行うために必要なことが 2 つあります。まず、ルーティングの到達可能性です。2 つ目はセキュリティ許可です。EPG では、これら 2 つは EPG サブネットや契約などの 1 セットの設定で密接に結合されています。ESG では、これら 2 つは 2 つの異なる設定で分離されています。

1. ESG 契約の設定とは独立した、VRF レベルでのルート リークの設定。
2. ESG 間の契約の設定。

これら 2 つの設定が完全に分離されているため、EPG で行う必要があるように、ESG の下にサブネットまたはサブネットのサブセットを設定する必要はありません。

次のセクションでは、ブリッジ ドメイン サブネットおよび外部ルーターから学習した外部プレフィックスのルート リークを設定する方法について説明します。ルート リークの設定が完了したら、2 つの ESG 間、または ESG と L3Out EPG 間の契約を設定して、通信を許可できます。グローバルなど、VRFより大きい範囲の契約を使用する必要があります。

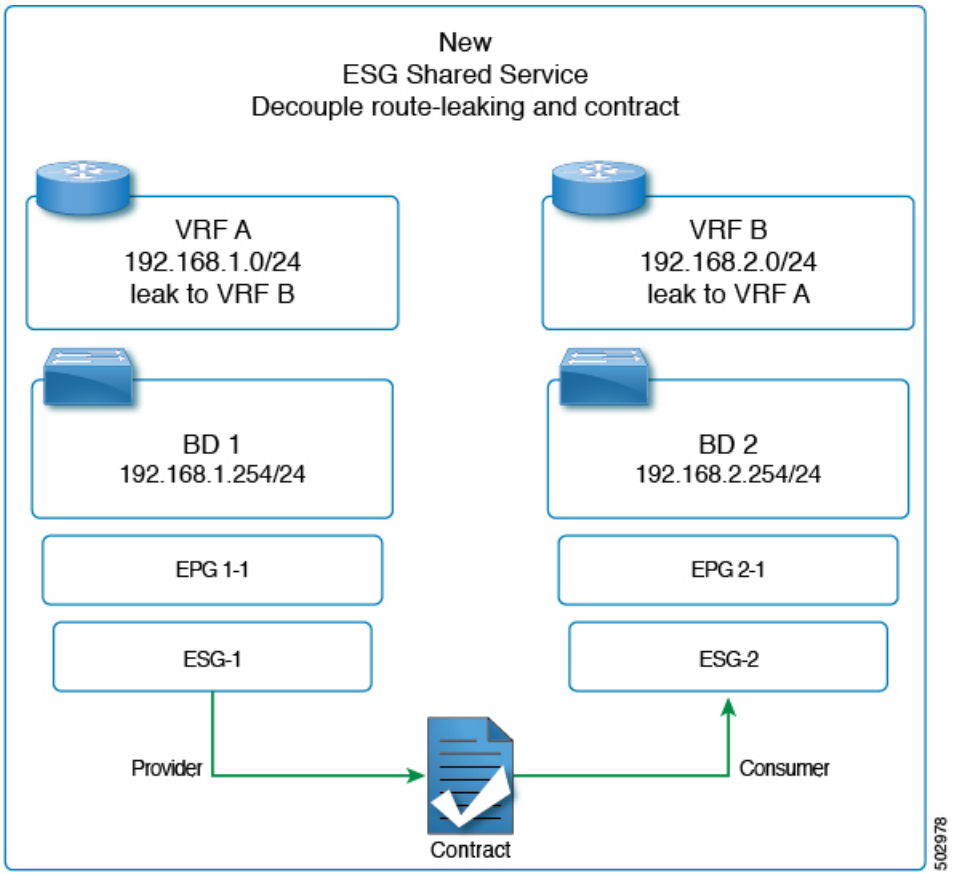
（注） VRF レベルでのルート リーク設定は、ESG でのみサポートされます。

内部ブリッジドメインサブネットのルートリーク

このセクションでは、ESG エンドポイントが属するブリッジドメインサブネットの VRF インスタンス間のルートリークを構成する方法について説明します。これは、ESG を使用しない場合に EPG レベルで実行されるのではなく、リークするサブネットと、VRF レベルで送信元 VRF インスタンスのターゲット VRF インスタンスを指定するだけで実行します。ルートリーク構成で入力するサブネットは、ブリッジドメインサブネットと一致するか、構成されたブリッジドメインサブネットのサブセットである必要があります。この構成でリークされるルートは、指定されたサブネットマスクを持つサブネットのみです。1 つの構成で複数のブリッジドメインサブネットをリークするサブネットの範囲を指定することはできません。

（注） VRF ルートリーク構成で構成するサブネットは、EPG で使用されるサブネットと一致させることもできます。これは、移行する場合に役立ちます。

図 *10 : ESG* によるルートリーク



上の図は、管理者が ESG1 と ESG2 の 2 つの ESG を構成した、2 つの VRF インスタンス（VRF A と VRF B）間の VRF リークの例を示しています。

（トラフィックを許可するための）ESG1 と ESG2 間のコントラクトに加えて、管理者はセクション「GUI を使用した内部ブリッジ ドメイン サブネットのルート リークの設定」で説明されているように、VRF インスタンスでルートリークを構成する必要があります。

ブリッジドメインサブネット範囲の構成 （[**外部でアドバタイズ（Advertised Externally）**]、[**VRF 間で共有（Shared between VRFs）**]）は、ESG の VRF レベルのルートリークでは必要ありません。リークされたブリッジドメインサブネットをターゲット VRF インスタンスの L3Out によってアドバタイズする必要がある場合は、VRF レベルのルートリーク構成で [**L3Out アドバタイズを許可（Allow L3Out Advertisement）**] を [**はい（True）**] に設定できます。 VRF レベルのルートリークで指定されたターゲット VRF インスタンスにサブネットをリークする場合、ブリッジドメインの下のサブネット範囲は無視され、VRF レベルのルートリークの構成が優先されることに注意してください。ブリッジドメインの下にあるこれらの範囲は、同じ VRF インスタンス内の L3Out からサブネットのアドバタイズ、EPG コントラクトによる従来の構成を介して別の VRF インスタンスへのルートリーク、またはその両方など、同時に他の構成でも引き続き優先されます。

外部プレフィックスのルートリーク

VRF の L3Out から別の VRF の ESG へのトラフィックを許可するためのルートリークの構成は、EPG の共有 L3Out と区別するために **ESG 共有 L3Out** と呼ばれます。

ESG 通信の L3Out から学習したルートをリークするには、管理者は VRF レベルで外部プレフィックスのルートリークを構成する必要があります。これは、IP プレフィックスリスト スタイルの構成を使用して行われます。ユーザーは、通常ルータの IP プレフィックスリストと同様に、「le」（以下）または「ge」（以上）を使用して、特定のプレフィックスを構成するか、プレフィックスの範囲を指定できます。ブリッジドメインサブネットとは異なり、外部ルートは動的に学習され、予測できないことが多いため、リークされたプレフィックスが実際のルート以下でなければならないという制限はありません。制限がないため、リークされた外部プレフィックスは、1 つの構成で複数のプレフィックスをリークする範囲を指定できます。設定では、ターゲット VRF も指定する必要があります。

設定の詳細については、『GUI を使用して外部プレフィックスのルートリークを構成する』を参照してください。

ESG 共有 L3Out 構成の場合、VRF でルートリークを構成し、L3Out EPG とのコントラクトを適用するとともに、どのプレフィックスがどの L3Out EPG に属するかを定義する必要があります。どのプレフィックスがどの L3Out EPG に属するかを指定するには、**外部 EPG の外部サブネット**および**共有セキュリティインポート サブネット**範囲を使用して L3Out サブネットを構成する必要があります。

レイヤ 4 ～ レイヤ 7 サービス

EPG で使用できるすべてのレイヤ 4 ～ レイヤ 7 サービス グラフ機能は、ESG でサポートされます。

（注） このメモは、高度なユーザー情報の実装の詳細です。ESG 間のコントラクトにサービス グラフが適用されている場合、Cisco Application Policy Infrastructure Controller (APIC) では、レイヤ 4 ～ レイヤ 7 サービスデバイスが適用される非表示サービス EPG を、 Cisco APIC が EPG 間のサービスグラフに行うのと同じように自動的に作成します。EPG 間のサービス グラフとは異なり、ESG の場合、隠しサービス EPG はグローバル pcTag を取得します。

Cisco APIC リリース 5.0(1) 以降のリリースでは、vzAny-to-vzAny コントラクトでレイヤ 4 ～ レイヤ 7 サービス展開用に作成されるすべての新しいサービス EPG は、グローバル pcTag を取得します。

レイヤ 4 ～ レイヤ 7 サービス展開の詳細については、『Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド』を参照してください。

運用ツール

キャパシティ ダッシュボード

[Capacity Dashboard] タブを使用して、重要なファブリック リソースのしきい値の概要を把握できます。これにより、承認されるスケーラビリティ制限にどの程度まで近づいているかを即座に確認できます。リーフ ノードごとの使用量も表示されるため、どのリーフ ノードがリソース制約に達しているかをすぐに確認できます。

1. [容量ダッシュボード（Capacity Dashboard）] トラブルシューティング ツールを起動するには、メニューバーで、**[操作（Operations）][容量ダッシュボード（Capacity Dashboard）]** の順に選択します。
2. **[容量ダッシュボード（Capacity Dashboard）]** ページで、ファブリック リソースの **[ファブリック容量（Fabric Capacity）]** を選択します。**[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** タイルと**[グローバル pcTag（Global pcTag）]** タイルまでスクロール ダウンして、使用可能なリソースを確認します。
3. **[容量ダッシュボード（Capacity Dashboard）]**ページで、リーフの使用状況として**[リーフ容量（Leaf Capacity）]** を選択します。エンドポイント セキュリティ グループのリソース使用量の詳細については、**[ESG]** タブを確認してください。

エンドポイント トラッカー

[**エンドポイントトラッカー（Endpoint Tracker**）] タブを使用して、ファブリックに適用されたエンドポイントの IP アドレスまたは MAC アドレスを入力すると、このエンドポイントのロケーション、エンドポイントが属するエンドポイントグループ、使用されている VLAN カプセル化、このエンドポイントで移行（フラップ）が発生しているかどうかをすばやく確認できます。

1. メニュー バーで、**[操作（Operations）]** > **[EP トラッカー（EP Tracker）]** の順にクリックして、エンドポイント トラッカーのトラブルシューティング ツールを起動します。
2. [End Point Search] フィールドに、エンドポイントの IP アドレスまたは MAC アドレスを入力し、[Search] をクリックします。
3. 表示された後にエンドポイントをクリックします。

エンドポイントトラッカー ツールでは、イベント中の IP アドレス、MAC アドレス、所有するエンドポイントグループ、アクション（適用または解除）、物理ノード、インターフェイス、および VLAN カプセル化とともに、各状態遷移の日時が表示されます。

エンドポイント トラッカー ツールは、fvCEp と呼ばれるオブジェクトを使用して、ESG および EPG について、ファブリックで学習されたエンドポイントを見つけます。ESG に属するエンドポイントは 2 つの fvCEp オブジェクトで表されます。1 つは VLAN バインドを提供する

EPG 用で、もう 1 つはセキュリティを提供する ESG 用です。したがって、エンドポイントトラッカーツールは、ESG エンドポイントに使用すると、2 つのエントリが表示されます（EPG 用と ESG 用）。

制限事項

Cisco APIC リリース 5.0(1) の時点で、次の制限が適用されます。

- ESG と EPG 間の契約はサポートされていません。
- ESG 機能は Cisco ACI マルチサイトと統合されていません。マルチポッド、マルチティア、リモート リーフなどの他のトポロジがサポートされています。
- サポートされている ESG セレクターは IP アドレスです。MAC アドレス、VM タグ、またはその他の基準はまだサポートされていません。
- ESG 契約は、セレクターとして IP を使用するルーティング トラフィックにのみ適用できます。
- タブー契約は ESG ではサポートされていません。
- ESG 間の VRF 間サービス グラフはサポートされていません。
- ESG は、次の機能のソースまたは宛先としてサポートされていません。
  - オンデマンド原子カウンター
  - オンデマンド遅延測定
  - SPAN
- BD/EPG のエンドポイントが ESG に分類されている場合、BD または EPG レベルで設定された次の機能はサポートされません。
  - エンドポイント到達可能性（BD/EPG 上の静的ルート）
  - エニーキャスト サービス
  - Microsoft NLB
  - First Hop Security (FHS)
  - ホスト ベース ルーティング/ホスト ルート アドバタイズメント
- ESG 展開では、EX 以降の世代のリーフ ノードのみがサポートされます。
- IP がセレクターとして使用されている場合に、レイヤ 2 トラフィック（つまり、ルーティングされていないトラフィック）が ESG セキュリティをバイパスしないようにするには、ESG エンドポイントに VLAN からインターフェイスへのバインディングを提供するすべての EPG で、共通のデフォルト契約などすべてを許可するルールを使用して EPG 契約を有効にします。EPG 内のすべてのエンドポイントが ESG に分類されている場合は、代わりに、EPG 内の契約ではなく、EPG でプロキシ ARP を使用して EPG 内の分離を有効にす

ることができます。EPG が VMM DVS 統合にのみ使用される場合は、上記の他の 2 つのオプションの代わりに、**[マイクロセグメンテーションを許可する（Allow Micro-Segmentation）]** オプションを有効にすることもできます。いずれの機能も、ESG エンドポイント間のすべての通信がレイヤ 3 ルーティングを通過するようにします。

（注） このメモでは、すべてを許可するルールを使用した EPG 内契約と、プロキシ ARP を使用した EPG 内の分離の違いについて説明します。両方の機能の主な目的は同じで、プロキシ ARP を使用して、ACI リーフ スイッチ上ですべてのトラフィックをルートするようにすることです。EPG間契約が使用される場合、プロキシ ARP は EPG に対して暗黙的に有効になることに注意してください。違いは、ESGに属していないが、EPGで学習されたエンドポイントが2つ以上ある場合です。すべてを許可するルールを使用したEPG内契約では、このようなエンドポイントは、すべてを許可するルールにより同じ EPG 内で引き続き自由に通信できます。ただし、プロキシ ARP を使用した EPG 内分離では、そのようなエンドポイントは同じEPGにある場合でも通信できなくなります。

- 契約を ESG に追加する場合、ラベル設定はサポートされていません。

ESG 以降戦略

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) 以降のリリースでは、EPG セレクタにより、エンドポイントセキュリティ グループ (ESG) が EPG からコントラクトを継承できるようになり、EPG から ESG への移行が簡素化されます。EPG セレクタによるコントラクトの継承により、エンドポイントは他のエンドポイントがまだ ESG に移行されていない場合でも、継承されたコントラクトを使用して他のエンドポイントとの通信を継続できるため、シームレスでフレキシブルな移行が可能になります。

以下の例では、次の図の EPG A1 の EPG から ESG への移行に焦点を当てます。EPG A1 からの現在の通信は、EPG B1、B2、および B3 とのコントラクト C1 を介して行われます。

図 *11 : EPG* から *ESG* への移行を開始する準備をする

最初の手順は、ESG（次の図の ESG A1）を作成し、EPG セレクタを使用して EPG A1 をそれに一致させることです。

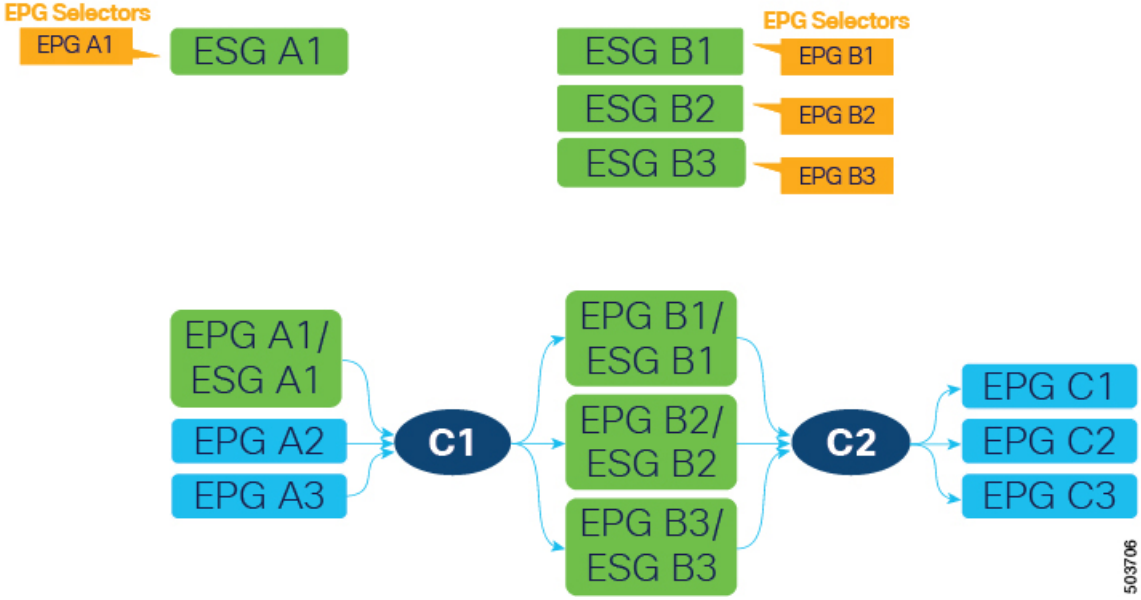
図 *12 : ESG* を作成し、最初の *EPG* を移行します

EPG A1 が ESG A1 に一致させた後、EPG A1 に属していたエンドポイントは ESG A1 に属し、EPG A1 によって提供されるコントラクト C1 は ESG A1 に継承されます。移行されたすべてのエンドポイントは、EPG がまだ ESG に移行されていなくても、EPG B1、B2、および B3 と引き続き通信できます。EPG セレクタによるコントラクトの継承がないと、Cisco Application Centric Infrastructure（ACI）は ESG と EPG 間のコントラクトが許可されないことに注意してください。ESG が EPG セレクタを介してコントラクトを継承する場合、EPG の元の pcTag は ESG の pcTag に置き換えられることに注意してください。この操作により、EPG のエンドポイントのトラフィックに一時的な小規模の中断が発生する場合があります。

この時点で、プロジェクトスケジュールに応じて、EPG A1 の移行を完了する代わりに、ESG A1 と他の ESG または L3Out 外部 EPG との間で新しいコントラクトを構成できます。ただし、すべてのセキュリティ構成は ESG によって管理される必要があるため、EPG A1 にこれ以上新しいコントラクトを追加することはできません。構成をシンプルに維持しやすくするために、できるだけ早く EPG から ESG への移行を完了することをお勧めします。EPG A1 がコントラクトの提供（または消費）を停止するまで、不完全な移行を通知する警告として障害 F3602 が発生します。

移行を続行するには、コントラクト C1 の反対側で EPG の ESG を作成します。この例では、EPG A1 がコントラクト C1 を提供しているため、それらの EPG（EPG B1、B2、および B3）がコントラクト C1 を消費しています。EPG セレクタを使用して、これらの EPG を新しい ESG（ESG B1、B2、および B3）に移行します。次の図の例では、各 EPG が ESG にマッピングされています。

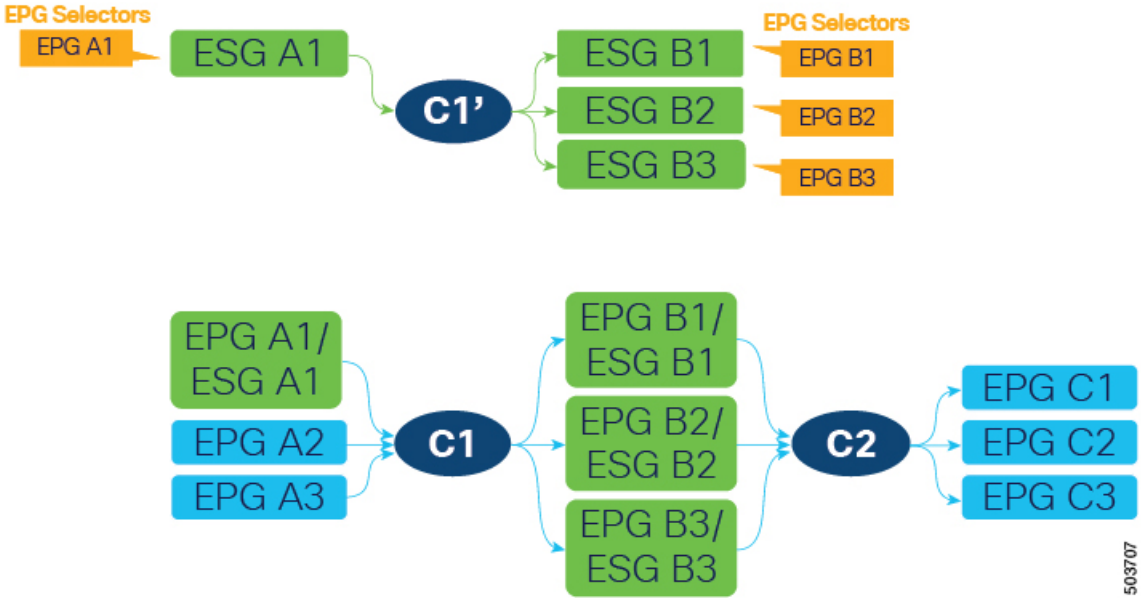
図 *13* : 追加の *ESG* の作成、*EPG* の移行



または、複数の EPG を 1 つの ESG に結合できます。たとえば、1 つの ESG を作成してから、同じ ESG 上の EPG B1 と B2 の両方に EPG セレクタを構成できます。

次に、コントラクト C1 と同じフィルタを使用して新しいコントラクト（次の図の C1'）を作成します。新しい ESG をプロバイダーおよびコンシューマーとして構成します。これは、EPG A1 からのコントラクト C1 の提供の停止を準備するため、EPG A1 の EPG から ESG への移行の最後の手順です。

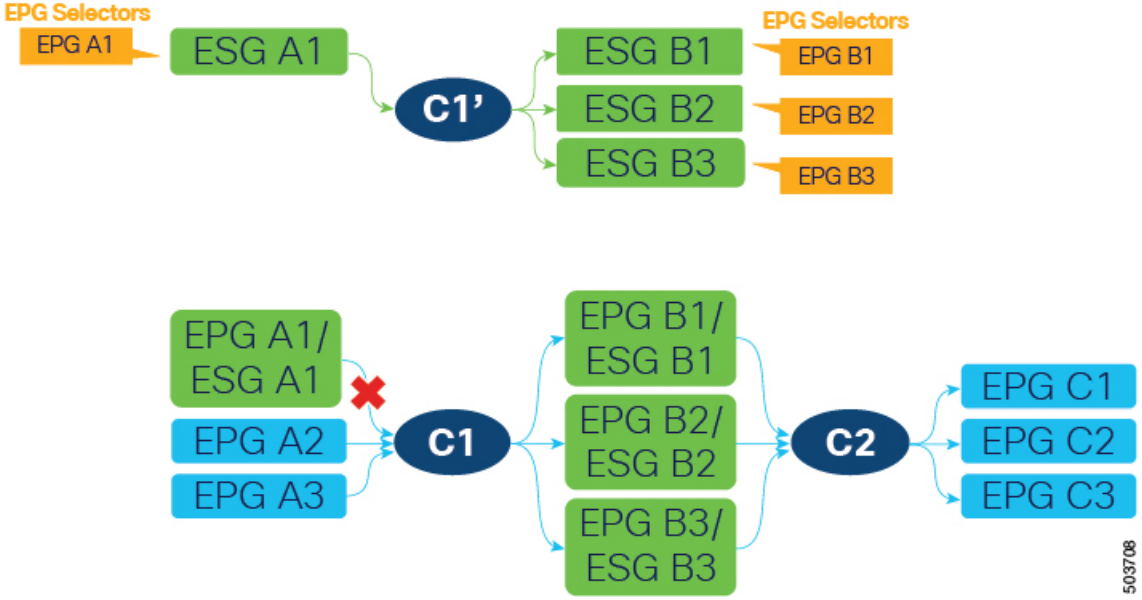
図 *14* : 新規契約を作成する



同じフィルタを持つコントラクトC1は、4つすべてのESG（A1、B1、B2、およびB3）によってすでに継承されているため、新しいコントラクト設定はハードウェアに新しいルールを展開せず、新しいコントラクトを作成することによって追加のポリシー TCAM が消費されることはありません。

ESG A1 には、ESG B1、B2、および B3 との C1 と同じ通信を許可するコントラクト C1' があります。この時点で、EPG A1 でのコントラクト C1 の提供を停止でき、次の図に示すように ESG A1 がすべてのセキュリティを処理できるようになります。

図 *15*：古いコントラクトのプロバイダーとしての *EPG* を削除する



B1、B2、および B3 は、コントラクト C1 はまだ ESG に移行されていない EPG A2 および A3 によっても提供されるため、コントラクト C1 の消費をまだ停止できないことに注意してください。EPG A2 および A3 が ESG に移行され、コントラクト C1' を提供した後、すべての EPG（A2、A3、B1、B2、および B3）は、トラフィックを中断することなくコントラクト C1 の使用を停止できます。

EPG から ESG への移行を完了するには、EPG レベルのコントラクト C2 およびその他のコントラクトについても同じ手順に従います。

エンドポイント セキュリティ グループを設定する

GUI を使用してエンドポイントセキュリティ グループを作成する

Cisco APIC リリース 5.2(1) 以降のリリースでは、ESG セレクタはポリシータグ、EPG、IP サブネットにすることができます。以前のリリースでは、IP サブネットのみがサポートされています。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]**を選択します。

ステップ 3 [**エンドポイントセキュリティ グループ（Endpoint Security Groups**）] を右クリックし、[**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] を選択します。

ステップ 4 [**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] ダイアログボックスの [**手順 1（STEP 1**） > **ID（Identity**）] ページで、次の情報を入力します。

a) **名前（Name**）：ESG の名前を入力します。

b) （任意） **説明（Description**）：ESG の説明を入力します。

c) **VRF**：ESG に関連付けられる VRF を入力します。

d) **ESG 管理状態**：ESG をシャットダウンするには、[**管理者によるシャットダウン（Admin Shut**）] を選択します。デフォルトでは、[**ESG 管理状態（ESG Admin State**）] は [**Admin Up**] の値です。このフィールドは、5.2(3) リリースから追加されました。

e) [次へ（Next）] をクリックします。

[**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] ダイアログボックスの [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページが開きます。

（注） 次の手順では、ポリシータグ、EPG、および IP サブネットに基づいてセレクタを作成できます。または、[**次へ（Next**）]をクリックして、セレクタとタグを設定する （190 ページ）で説明するようにセレクタを後で構成することもできます。

ステップ 5 [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページで、ポリシータグをエンドポイントセレクタとして使用する場合は、**タグセレクタ**バーの [+] 記号をクリックします。

[タグ セレクタの作成（Create a Tag Selector）] ダイアログ ボックスが開きます。「タグ セレクターを作成する （190 ページ）」の手順に従います。

ステップ 6 [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページで、EPG をエンドポイントセレクタとして指定する場合は、**EPG セレクタ**バーの [+] 記号をクリックします。

[EPG セレクタの作成（Create an EPG Selector）] ダイアログ ボックスが開きます。「EPG セレクタの作成 （191 ページ）」の手順に従います。

ステップ 7 [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページで、エンドポイントセレクタとして IP サブネットを指定する場合は、**IP サブネットセレクタ**バーの [+] 記号をクリックします。

[**IP サブネット セレクタの作成（Create an IP Subnet Selector**）] ダイアログ ボックスが開きます。「IP サブネット セレクターを作成する （192 ページ）」の手順に従います。

ステップ 8 [次へ（Next）] をクリックします。

[**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] ダイアログボックスの [**手順 3（STEP 3**）] > **[詳細（オプション）（Advanced (Optional)**）] ページが開きます。

ステップ 9 [手順 3（STEP 3）] > [詳細（オプション）（Advanced (Optional)）] ページで、次のオプションを構成できます。

a) （任意） ESG 内の通信をブロックするには、[**ESG 内分離（Intra ESG Isolation**）] フィールドで [**強制（Enforced**）] を選択します。デフォルトは [**非強制（Unenforced**）] です。

[**非強制（Unenforced**）] では、同じ ESG 内のすべてのエンドポイントが自由に通信できます。または、同じ ESG 内で特定のタイプの通信のみを許可する場合は、代わりに ESG 内コントラクトを使用できます。ESG 内のコントラクト構成については、「GUI を使用して契約をエンドポイント セキュリティ グループに適用する （195 ページ）」 を参照してください。

b) （任意） 設定済みグループメンバーとして ESG を含むには、[**設定済みグループメンバー（Preferred Group Member**）] フィールドで [**含める（Include**）] を選択します。デフォルトは [除外（Exclude）] です。

[**含める（Include**）] を選択する前に、優先グループが VRF レベルで有効になっていることを確認してください。

設定済みグループの詳細については、『*Cisco APIC* 基本構成ガイド』を参照してください。

c) （任意） 別の ESG からコントラクトを継承するには、**ESG コントラクトマスター**バーの [+] 記号をクリックし、コントラクトを継承する ESG を選択します。

ESG コントラクトマスターを選択した場合、作成している ESG は、選択した ESG のすべてのコントラクトを継承します。新しい ESG が既存の ESG と同じセキュリティ構成を持つようにする場合は、ESG コントラクトマスターを追加します。

ステップ 10 [Finish] をクリックします。

セレクタとタグを設定する

タグ セレクターを作成する

この手順を使用して、エンドポイント セキュリティ グループ (ESG) のタグ セレクターを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[タグ セレクター（Tag Selectors）]** を右クリックし、**[タグ セレクターの作成（Create a Tag Selector）]** を選択します。

ステップ 4 **[タグ セレクターの作成（Create an Tag Selector）]** ダイアログ ボックスに、次の情報を入力します。

a) **タグ キー**：タグ キーを入力するか、ドロップダウン リストから既存のタグ キーを選択します。

b) **値演算子**：ESG に含めるエンティティのタグ値を一致させるための条件を選択します。

選択できる演算子は次の通りです。

- **Contains**：タグ値を含むが、**[タグ値（Tag Value）]** と完全に一致しない可能性があるエンティティを選択します。
- **Equals**：タグ値が **[タグ値（Tag Value）]** と等しいエンティティを選択します。
- **Regex**：タグ値が **[タグ値（Tag Value）]** フィールドに入力された正規表現と一致するエンティティを選択します。

c) **タグ値**：値または正規表現を入力するか、ドロップダウン リストから既存の値を選択します。

正規表現を作成するときは、次のガイドラインを使用してください。

- 有効な文字は、a-z A-Z 0-9 _ . です。, : ^ $ [] () {} | + * -
- 次の文字は使用できません。/ \ ?
- [0-9]+ は任意の数に一致（\d+ と同等）
- a{0,1} は、a のゼロまたは 1 つに一致します（? と同等）
- [0-9]{3} は 3 桁の数字に完全に一致します
- dev(1)|(2) は dev1 または dev2 の値に一致します

d) **説明**：（オプション）オブジェクトの説明。

e) [送信（Submit）] をクリックします。

EPG セレクタの作成

この手順を使用して、エンドポイント セキュリティ グループ (ESG) の EPG セレクタを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[EPG セレクタ（EPG Selectors）]** を右クリックし、**[EPG セレクタの作成（Create an EPG Selector）]** を選択します。

ステップ 4 **[EPG セレクタの作成（Create an EPG Selector）]** ダイアログ ボックスに、次の情報を入力します。

a) **ESG VRF の EPG**：VRF に存在する EPG のリストから、ESG に含まれる EPG のチェックボックスをオンにします。

b) **説明**：（オプション）オブジェクトの説明。

c) [送信（Submit）] をクリックします。

IP サブネット セレクターを作成する

この手順を使用して、エンドポイント セキュリティ グループ（ESG）の IP サブネット セレクターを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[IP サブネット セレクター（IP Subnet Selectors）]** を右クリックし、**[IP サブネット セレクターの作成（Create an IP Subnet Selector）]** を選択します。

ステップ 4 **[IP サブネット セレクターの作成（Create an IP Subnet Selector）]** ダイアログ ボックスで、次の情報を入力します。

a) **IP サブネット**：**キー**：このフィールドは **IP** に設定されています。

b) **IP サブネット**：**演算子**：このフィールドは**等しい**に設定されています。セレクターは、指定されたサブネットに完全に一致する IP サブネットのみに一致します。

c) **IP サブネット**：値 : ESG に含まれるエンドポイントの IP サブネットを入力します。

特定の IP (/32、/128、またはサブネット マスクなし) または任意のマスク長のサブネット マッチを入力できます。

d) **説明**：（オプション）

e) [送信（Submit）] をクリックします。

サービス EPG セレクターを作成する

この手順を使用して、エンドポイント セキュリティ グループ（ESG）のサービス EPG セレクターを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[サービス EPG セレクター（Service EPG Selectors）]** を右クリックし、**[サービス EPG セレクターの作成（Create a Service EPG Selector）]** を選択します。

ステップ 4 **[サービス EPG セレクターの作成（Create a Service EPG Selector）]** ダイアログ ボックスに、次の情報を入力します。

a) **サービス EPG**：サービス EPG を ESG に含めるには、提供されているサービス デバイス コネクタのリストから選択します。

サービス EPG を表すサービス デバイス コネクタ（LifCtx）は、ESG にマッピングできます。表示されるサービス デバイス コネクタのリストは、次の場所にあるデバイス選択ポリシーで定義されたコネクタから取得されます。

Tenants > ***tenant_name*** > **Services** > **L4-L7** > **Device Selection Policies**

サービス デバイス コネクタは、次の形式で表示されます。

consumer または **provider**

TENANT_NAME/c-*CONTRACT_NAME*-g-*GRAPH_NAME*-n-*NODE_NAME*

次に例を示します。

コンシューマ

PBR/c-web-to-app-g-FW-Graph-n-N1

b) **説明**：（オプション）オブジェクトの説明。
c) [送信（Submit）] をクリックします。

エンドポイント MAC タグを作成する

この手順を使用して、ポリシー タグをエンドポイントの MAC アドレスに追加します。タグ セレクタは、このタグを使用して、エンドポイントの MAC アドレスをエンドポイント セキュリティ グループ (ESG) に関連付けることができます。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[アプリケーション EPG（Application EPGs）]** > ***[epg_name]*** を展開します。

ステップ 3 [作業（Work）] ペインで、**[操作（Operational）]** > **[クライアント エンドポイント（Client Endpoints）]** タブを選択します。

[クライアント エンドポイント（Client Endpoints）] には、関連付けられている IP アドレスとともに、利用可能な各エンドポイントの MAC アドレスを表示します。アドレスにすでにポリシー タグが割り当てられている場合、それらのポリシー タグは MAC または IP アドレスの **[ポリシー タグ（Policy Tags）]** 列に表示されます。

ステップ 4 目的の MAC アドレスの行を右クリックし、**[エンドポイント MAC タグの設定（Configure an Endpoint MAC Tag）]** を選択します。

MAC アドレスがテーブルに表示されない場合は、VMM 統合を通じてまだ学習または表示されていません。この場合、***[tenant_name]*** > **[ポリシー（Policies）]** > **[エンドポイント タグ（Endpoint Tags）]** を展開し、**[エンドポイント MAC（Endpoint MAC）]** を右クリックし、**[エンドポイント MAC タグの作成（Create an Endpoint MAC Tag）]** を選択します。

ステップ 5 **[エンドポイント MAC タグの作成（Create an Endpoint MAC Tag）]** ダイアログ ボックスに次の情報を入力します。

（注） **[クライアント エンドポイント（Client Endpoints）]** テーブルから MAC アドレスを選択した場合、MAC アドレスと BD フィールドはすでに入力されています。

a) **エンドポイント MAC アドレス**：タグを追加する MAC アドレスを入力します。

b) **BD 名**：既存のブリッジ ドメインを選択するか、新しいブリッジ ドメインを作成します。

***** を選択すると、エンドポイント MAC タグは、指定された VRF 内の任意の BD の MAC アドレスを表します。この場合、VRF も選択するよう求められます。

c) **注釈**：（オプション）**[+]** 記号をクリックし、注釈キーと値を追加し、[✓] 記号をクリックします。

複数の注釈を追加できます。

d) **ポリシー タグ**：**[+]** 記号をクリックし、ポリシー タグ キーと値を追加し、[✓] 記号をクリックします。

複数のポリシー タグを追加できます。

e) [送信（Submit）] をクリックします。

エンドポイント IP タグの作成

この手順を使用して、エンドポイント IP アドレスにポリシー タグを追加します。タグ セレクターは、このタグを使用して、エンドポイントの IP アドレスをエンドポイント セキュリティ グループ (ESG) に関連付けることができます。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[アプリケーション EPG（Application EPGs）]** > ***[epg_name]*** を展開します。

ステップ 3 [作業（Work）] ペインで、**[操作（Operational）]** > **[クライアント エンドポイント（Client Endpoints）]** タブを選択します。

[クライアント エンドポイント（Client Endpoints）] には、関連付けられている IP アドレスとともに、利用可能な各エンドポイントの MAC アドレスを表示します。アドレスにすでにポリシー タグが割り当てられている場合、それらのポリシー タグは MAC または IP アドレスの **[ポリシー タグ（Policy Tags）]** 列に表示されます。

ステップ 4 目的の IP アドレスの行を右クリックし、**[エンドポイント IP タグの設定（Configure an Endpoint IP Tag）]** を選択します。

IP アドレスがテーブルに表示されない場合、VMM 統合を通じてまだ学習または表示されていません。この場合、***[tenant_name]*** > **[ポリシー（Policies）]** > **[エンドポイント タグ（Endpoint Tags）]** を展開し、**[エンドポイント IP（Endpoint IP）]** を右クリックし、**[エンドポイント IP タグの作成（Create an Endpoint IP Tag）]** を選択します。

ステップ 5 **[エンドポイント IP タグの作成（Create an Endpoint IP Tag）]** ダイアログ ボックスに次の情報を入力します。

[クライアント エンドポイント（Client Endpoints）] テーブルからエンドポイントを選択した場合、IP アドレスと VRF フィールドはすでに入力されています。

a) **IP**：タグを追加する IP アドレスを入力します。
b) **注釈**：（オプション）**[+]** 記号をクリックし、注釈キーと値を追加し、[✓] 記号をクリックします。

複数の注釈を追加できます。

c) **VRF 名**：エンドポイントを含む VRF を選択または作成します。
d) **ポリシー タグ**：**[+]** 記号をクリックし、ポリシー タグ キーと値を追加し、[✓] 記号をクリックします。

複数のポリシー タグを追加できます。

e) [送信（Submit）] をクリックします。

GUI を使用して契約をエンドポイント セキュリティ グループに適用する

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** を選択します。

ステップ 3 **[契約（Contracts）]** を右クリックし、契約が展開される方法に応じてアクションを選択します。

次のオプションがあります。

- **提供されたコントラクトの追加**
- **消費される契約の追加**
- **消費されるコントラクト インターフェイスの追加**
- **ESG 内契約の追加**

（注） アプリケーション EPG によって消費または提供される契約は、ここでは ESG には使用できません。

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

a) **[契約名（Contract Name）]** を入力または選択します。
b) （任意） **[QOS ポリシー（QOS policy）]** を選択します。
c) （任意） **[ラベル（Label）]** を選択します。

ステップ 5 [送信（Submit）] をクリックします。

REST API を使用したエンドポイント セキュリティ グループの作成と契約の適用

手順：

```
<polUni>
  <fvTenant name="t0">
    <fvAp name="ap0">
      <!-- ESG with the name ESG1 and Preferred Group as Exclude -->
      <fvESg name="ESG1" prefGrMemb="exclude">
          <!-- The ESG is associated to VRFA -->
          <fvRsScope tnFvCtxName="VRFA" />

          <!-- provided and consumed contracts -->
          <fvRsProv tnVzBrCPName="provided_contract1" />
          <fvRsCons tnVzBrCPName="consumed_contract2" />

          <!-- Tag Selectors for the ESG -->
         <fvTagSelector matchKey="stage" valueOperator="equals" matchValue="production"/>

          <fvTagSelector matchKey="owner" valueOperator="contains" matchValue="teamA"/>
          <fvTagSelector matchKey="__vmm::vmname" valueOperator="regex"
matchValue="web_[0-9]+"/>

          <!-- EPG Selectors for the ESG -->
          <fvEPgSelector matchEpgDn="uni/tn-TK/ap-AP1/epg-EPG1-1"/>
          <fvEPgSelector matchEpgDn="uni/tn-TK/ap-AP1/epg-EPG1-2"/>

          <!-- IP Subnet Selectors for the ESG -->
          <fvEPSelector matchExpression="ip=='192.168.0.1/32'" />
          <fvEPSelector matchExpression="ip=='192.168.1.0/28'" />
          <fvEPSelector matchExpression="ip=='2001:23:45::0:0/64'" />
      </fvESg>
    </fvAp>
  </fvTenant>
</polUni>
```

REST API を使用してタグおよびセレクターを作成する

EPG セレクターを作成する

EPG セレクター オブジェクト（**fvEPgSelector**）は、特定の EPG の DN と一致します。

```
<polUni>
  <fvTenant name="ExampleCorp">
    <fvAp name="AP">
      <fvESg name="esg1">
        <fvEPgSelector matchEpgDn="uni/tn-ExampleCorp/ap-app/epg-epg1"/>
        <fvRsScope tnFvCtxName="dev"/>
      </fvESg>
    </fvAP>
  </fvTenant>
</polUni>
```

EPG セレクターは、ESG と同じテナントおよび VRF に属する EPG にのみ一致できます。

タグとタグ セレクターの作成

タグセレクタオブジェクト（**fvTagSelector**）は、次のオブジェクトの下で検出されたタグオブジェクト（**tagTag**）と一致します。

- **fvEpIpTag**
- **fvEpMacTag**
- **fvSubnet**
- **fvStCEp**

（注） タグ セレクター オブジェクトは、**fvEpVmmMacTagDef** 下のタグ オブジェクトにも一致します。ただし、このオブジェクトの下のポリシータグはVMM統合を通じて設定され、構成できません。

この例は、**tagTag** オブジェクトの位置と、タグを見つけて、一致する **fvTagSelector** オブジェクトを示しています。

```
<polUni>
  <fvTenant name="ExampleCorp">
    <fvEpTags>
      <fvEpIpTag ip="192.168.1.1" ctxName="example">
        <tagTag key="esg" value="Red"/>
       </fvEpIpTag>
    </fvEpTags>


    <fvAp name="AP">
      <fvESg name="esg1">
        <fvRsScope tnFvCtxName="example"/>
        <fvTagSelector matchKey="esg" matchValue="Red"/>
      </fvESg>
    </fvAp>
  </fvTenant>
</polUni>
```

タグを完全に一致させる代わりに、タグを部分的に一致させるか、または **valueOperator** の **fvTagSelector** プロパティを使用して正規表現を使用して一致させることができます。

- **valueOperator** プロパティがない場合、または「等しい」場合は、値が完全に一致する **tagTag** のみが認識されます。
- **valueOperator** プロパティが「含む」の場合、**tagTag** の値フィールドに **fvTagSelector** の **matchValue** フィールドが含まれていても、完全に一致していない場合に一致が認識されます。
- **valueOperator** プロパティが「regex」の場合、**tagTag** の値が **fvTagSelector** の **matchValue** フィールドに含まれる正規表現を満たす場合に一致が認識されます。

この例は、さまざまな一致条件を示しています。

```
<fvTagSelector matchKey="name" matchValue="Blue"/>
<fvTagSelector matchKey="name" matchValue="Blue" valueOperator = "equals"/>
<fvTagSelector matchKey="name" matchValue="prod" valueOperator = "contains"/>
<fvTagSelector matchKey="name" matchValue="prod[0-4]" valueOperator = "regex"/>
```

VMM エンドポイント用の特別なタグ セレクター

特別なキーを使用して、タグ セレクター オブジェクト（**fvTagSelector**）は VMM エンドポイントを名前で照合します。特殊な **matchKey** は「__vmm::vmname」で、**matchValue** は VM の名前です。

この例は、完全一致を使用して「vmName-Dev」という名前の VM に一致するタグ セレクターを示しています。

```
<polUni>
  <fvTenant name="ExampleCorp">
    <fvAp name="AP">
      <fvESg name="esg1">
        <fvTagSelector matchKey="type" matchValue="dev"/>
        <fvTagSelector matchKey="__vmm::vmname" matchValue="vmName-Dev"/>
        <fvRsScope tnFvCtxName="testctx0"/>
      </fvESg>
    </fvAp>
  </fvTenant>
</polUni>
```

エンドポイントセキュリティグループを使用してルートリークを設定する

GUIを使用した内部ブリッジドメインサブネットのルートリークの設定

この手順を使用して、内部ブリッジ ドメイン サブネットのルート リークを設定します。

始める前に

リークするテナント、VRF、ブリッジドメイン、サブネットを作成しておく必要があります。

ステップ 1 [Navigation] ペインで、[Tenant name] > [Networking] > [VRFs] > [Inter-VRF Leaked Routes for ESG] > [EPG/BD Subnets] に移動します。

ステップ 2 **[EPG/BD サブネット（EPG/BD Subnets）]** を右クリックし、**[EPG/BD サブネットをリークするようにに設定する（Configure EPG/BD Subnet to leak）]** を選択します。

ステップ 3 **[EPG/BD サブネットをリークするようにに設定する（Configure EPG/BD Subnet to leak）]** ダイアログ ボックスで、次の機能を実行します。

a) **IP**：リークするブリッジ ドメイン サブネットとそのマスクを入力します。
b) （任意） **説明**：EPG またはブリッジ ドメイン サブネットの説明を入力します。
c) （任意） **L3Out アドバタイズを許可する**：このサブネットを別の VRF の L3Out によってアドバタイズする必要がある場合は、**True** に設定します。

ステップ 4 **[テナントおよび VRF 宛先（Tenant and VRF destinations）]** フィールドで、右に移動し、**[+]** 記号をクリックします。

ステップ 5 **[テナントおよび VRF 宛先の作成（Create Tenant and VRF destination）]** ダイアログ ボックスで、次の機能を実行します。

a) **テナントおよび VRF**：テナントおよび VRF 名を入力または選択します。
b) （任意） **説明**：宛先の説明を入力します。
c) **L3Out アドバタイズメントを許可する**：ターゲット VRF ごとに許可を変更する必要がある場合は、**True** または **False** に設定します。デフォルトでは、このオプションは**継承**するように設定されており、ステップ 3 の **[L3Out アドバタイズを許可する（Allow L3Out Advertisement）]** と同じ設定を保持します。
d) [OK] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

REST API を使用した内部ブリッジ ドメイン サブネットのルート リークの設定

はじめる前に

漏洩する BD サブネット、または漏洩したサブネットを含む BD サブネットを設定しておく必要があります。

手順：

```
<polUni>
  <fvTenant name="t0">
    <fvCtx name="VRFA">
      <leakRoutes>
        <!--
            leak the BD subnet 192.168.1.0/24 with the Allow L3Out Advertisement
            False (i.e. scope private)
        -->
        <leakInternalSubnet ip="192.168.1.0/24" scope="private">
          <!--
              leak the BD subnet to Tenant t1 VRF VRFB with the
              Allow L3Out Advertisement configured in the parent
              scope (i.e. scope inherit)
          -->
          <leakTo ctxName="VRFB" tenantName="t1" scope="inherit" />
        </leakInternalSubnet>
      </leakRoutes>
    </fvCtx>
  </fvTenant>
</polUni>
```

GUI を使用して外部プレフィックスのルートリークを構成する

この手順を使用して、外部プレフィックスのルートリークを構成します。

始める前に

送信元 VRF で L3Out を構成しておく必要があり、外部プレフィックスが学習されます。

ステップ 1 ナビゲーションウィンドウで、[**テナント名（Tenant name**）]>[**ネットワーキング（Networking**）]>[**VRFs**] > [**ESG の VRF 間 リークルート（Inter- VRF Leaked Routes for ESG**）] > [**外部 プレフィックス（External Prefixes**）] の順に選択します。

ステップ 2 [**外部プレフィックス（External Prefixes**）] を右クリックし、[**リークされた外部プレフィックスの作成（Create Leaked External Prefix**）]を選択します。

ステップ 3 [**リークされた外部プレフィックスの作成（Create Leaked External Prefix**）] ダイアログボックスで、次の操作を実行します。

a) **IP**：リークされたプレフィックスを入力します。

b) （任意） **説明**：リークされた外部プレフィックスの説明を入力します。

c) （任意） **以上（プレフィックス）**：照合するプレフィックスの最小長を入力します。これは、通常のルータの IP プレフィックスリストの「ge」に相当します。

d) （任意） **以下（プレフィックス）**：照合するプレフィックスの最大長を入力します。これは、通常のルータの IP プレフィックスリストの「le」に相当します。

ステップ 4 **[テナントおよび VRF 宛先（Tenant and VRF destinations）]** フィールドで、右に移動し、**[+]** 記号をクリックします。

ステップ 5 **[テナントおよび VRF 宛先の作成（Create Tenant and VRF destination）]** ダイアログ ボックスで、次の機能を実行します。

a) **テナントおよび VRF**：テナントおよび VRF 名を入力または選択します。

b) （任意） **説明**：宛先の説明を入力します。

c) [OK] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

REST API を使用して外部プレフィックスのルート リークを設定する

はじめる前に

ソース VRF「VRFA」で L3Out を設定しておく必要があり、外部プレフィックスが学習されます。

手順：

```
<polUni>
  <fvTenant name="t0">
    <fvCtx name="VRFA">
      <leakRoutes>
        <!--
```

```
            leak the external prefixes in the range of
            10.20.0.0/17 and 10.20.0.0/30
          -->
          <leakExternalPrefix ip="10.20.0.0/16" ge="17" le="30">
            <!-- leak the external prefixes to Tenant t1 VRF VRFB -->
            <leakTo ctxName="VRFB" tenantName="t1" />
          </leakExternalPrefix>
        </leakRoutes>
      </fvCtx>
    </fvTenant>
</polUni>
```

エンドポイントセキュリティグループを使用したレイヤ 4 からレイヤ 7 を設定する

GUI を使用してエンドポイントセキュリティ グループへのレイヤ 4 ～ レイヤ 7 サービスを適用する

EPG を使用したサービス グラフの展開に提供されるすべての構成は、同様に ESG にも適用されます。必要な変更は、EPG にコントラクトを関連付ける代わりに ESG にコントラクトを関連付けることのみです。この手順を使用して、エンドポイントセキュリティ グループによって使用されるコントラクトに、非管理モードのレイヤ 4 ～ レイヤ 7 サービスデバイスのサービス グラフテンプレートを適用します。

始める前に

次を作成しておく必要があります。

- ESG
- サービス グラフ テンプレート

ステップ 1 メニュー バーで、**[テナント（Tenants）] > [すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [サービスグラフテンプレート（Service Graph Templates）]** の順に選択します。

ステップ 4 ナビゲーションウィンドウで、ESG に適用する **[サービスグラフテンプレート名（Service Graph Template Name）]** を右クリックし、**[L4 ～ L7 サービスグラフテンプレートを適用する（Apply L4-L7 Service Graph Template）]** を選択します。

Apply L4-L7 Service Graph Template To EPGs ダイアログボックスが表示されます。レイヤ 4 ～ レイヤ 7 サービスグラフテンプレートを、エンドポイントセキュリティ グループ間のコントラクトに関連付けます。

ステップ 5 適切な値を入力して、**[L4 ～ L7 サービスグラフテンプレートを ESG に適用する（Apply L4-L7 Service Graph Template To EPGs）手順 1（STEP 1）] > [コントラクト（Contract）]** ダイアログボックスのコントラクトを構成します。

a) エンドポイント グループタイプとして **[エンドポイントセキュリティ グループ（Endpoint Security Group）]** を選択します。

b) ESG 内コントラクトを構成している場合は、**[エンドポイント内コントラクトを構成する（Configure an Intra-Endpoint Contract）]** チェックボックスをオンにして、**[ESG/ネットワーク（ESG / Network）]** ドロップダウンリストから ESG を選択します。

c) ESG 内コントラクトではなく通常のコントラクトを使用している場合は、コンシューマーとプロバイダーの ESG とネットワークの組み合わせを選択します。

d) **[コントラクトタイプ（Contract Type）]** フィールドで適切なオプションボタンをクリックして、新しいコントラクトを作成するか既存のコントラクトを選択します。[Create A New Contract] を選択した場合、フィルタを設定するには、[No Filter (Allow All Traffic)] チェックボックスをオフにします。[+] をクリックしてフィルタ エントリを追加し、完了したら [Update] をクリックします。

ステップ 6 [次へ] をクリックします。

[STEP 2] > [Graph] ダイアログが表示されます。

ステップ 7 **[ご使用のデバイス情報（your device name Information）]** セクションで、赤いボックスで示されている必須フィールドでを構成します。

ステップ 8 **[Finish（完了）]** をクリックします。

これで、ESG が使用するコントラクトにサービスグラフテンプレートを適用できました。

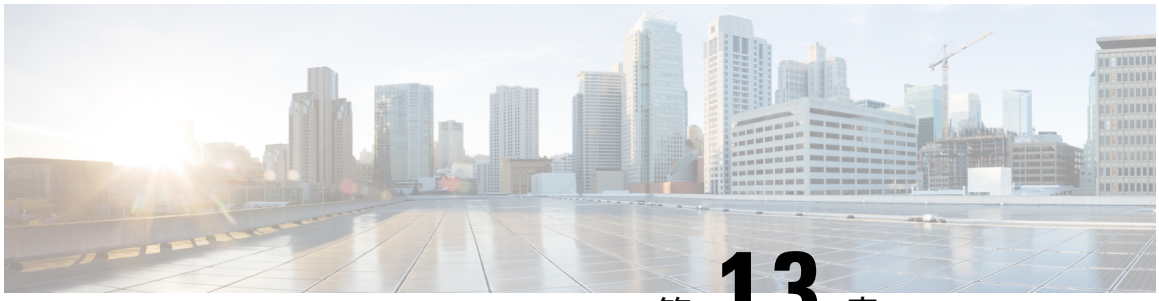
（注） vzAny を構成するには、上記の手順 5.c で、プロバイダーとして **AnyEPG** を選択し、コンシューマーとして関心のある ESG を選択するか、またはその逆を選択します。

サービス グラフを vzAny-to-vzAny コントラクト vzAny-vzAny に適用するには、エンドポイントグループタイプとして **[エンドポイントポリシーグループ（EPG）（Endpoint Policy Group (EPG)）]** を選択し、プロバイダーおよびコンシューマーとして **[AnyEPG]** を選択します。

REST API を使用したエンドポイント セキュリティ グループへのレイヤ 4 からレイヤ 7 サービスの適用

EPG を使用してサービス グラフを展開するために提供されるすべての REST API は、ESG にも等しく適用されます。ただし、契約は ESG に関連付けられている必要があります。

詳細については、レイヤ 4 からレイヤ 7 の REST API の例を参照してください。



第 13 章

セキュリティ ポリシー

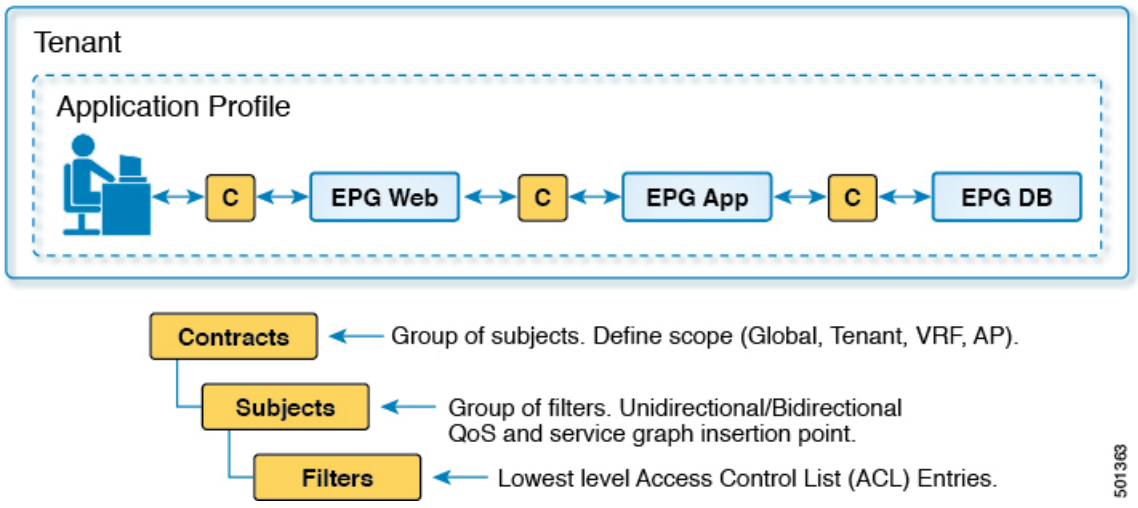
この章は、次の項で構成されています。

ACI ファブリック ネットワーク アクセス セキュリティ ポリシー モデル（契約）

ACI のファブリック セキュリティ ポリシー モデルはコントラクトに基づいています。このアプローチにより、従来のアクセス コントロール リスト（ACL）の制限に対応できます。コントラクトには、エンドポイント グループ間のトラフィックで適用されるセキュリティ ポリシーの仕様が含まれます。

次の図は、 契約のコンポーネントを示しています。

図 *16* : 契約のコンポーネント



EPG 通信にはコントラクトが必要です。EPG/EPG 通信はコントラクトなしでは許可されません。APICは、コントラクトや関連するEPGなどのポリシーモデル全体を各スイッチの具象モデルにレンダリングします。入力時に、ファブリックに入るパケットはすべて、必要なポリシーの詳細でマークされます。EPGの間を通過できるトラフィックの種類を選択するためにコントラクトが必要とされるので、コントラクトはセキュリティポリシーを適用します。コントラクトは、従来のネットワーク設定でのアクセス コントロール リスト（ACL）によって扱われるセキュリティ要件を満たす一方で、柔軟性が高く、管理が容易な、包括的なセキュリティ ポリシー ソリューションです。

アクセス コントロール リストの制限

従来のアクセス コントロール リスト（ACL）には、ACI ファブリック セキュリティ モデルが対応する多数の制限があります。従来の ACL は、ネットワーク トポロジと非常に強固に結合されています。それらは通常、ルータまたはスイッチの入力および出力インターフェイスごとに設定され、そのインターフェイス、およびそれらのインターフェイスを流れることが予期されるトラフィックに合わせてカスタマイズされます。このカスタマイズにより、それらは多くの場合インターフェイス間で再利用できません。もちろんこれはルータまたはスイッチ間にも当てはまります。

従来の ACL は、非常に複雑で曖昧です。なぜなら、そのリストには、許可された特定の IP アドレス、サブネット、およびプロトコルのリストと、明確に許可されていない多くのものが含まれているためです。この複雑さは、問題が生じるのを管理者が懸念して ACL ルールを削除するのを躊躇するため、維持が困難で、多くの場合は増大するだけということを意味します。複雑さは、それらが通常 WAN と企業間または WAN とデータセンター間の境界などのネットワーク内の特定の境界ポイントでのみ配置されていることを意味します。この場合、ACLのセキュリティのメリットは、エンタープライズ内またはデータセンターに含まれるトラフィック向けには生かされません。

別の問題として、1 つの ACL 内のエントリ数の大幅増加が考えられます。ユーザは多くの場合、一連の送信元が一連のプロトコルを使用して一連の宛先と通信するのを許可する ACL を作成します。最悪の場合、*N*の送信元が*K*のプロトコルを使用して*M*の宛先と対話する場合、ACLに*N***M***K*の行が存在する場合があります。ACLは、プロトコルごとに各宛先と通信する各送信元を一覧表示する必要があります。また、ACLが非常に大きくなる前に多くのデバイスやプロトコルを取得することはありません。

ACI ファブリック セキュリティ モデルは、これらの ACL の問題に処理します。ACI ファブリックセキュリティモデルは、管理者の意図を直接表します。管理者は、連絡先、フィルタ、およびラベルの管理対象オブジェクトを使用してエンドポイントのグループがどのように通信するかを指定します。これらの管理対象オブジェクトは、ネットワークのトポロジに関連していません。なぜなら、それらは特定のインターフェイスに適用されないためです。それらは、エンドポイントのこれらのグループの接続場所に関係なく、ネットワークが強要しなければならない簡易なルールです。このトポロジの独立性は、これらの管理対象オブジェクトが特定の境界ポイントとしてだけではなくデータセンター全体にわたって容易に配置して再利用できることを意味します。

ACI ファブリック セキュリティ モデルは、エンドポイントのグループ化コンストラクトを直接使用するため、サーバのグループが相互に通信できるようにするための概念はシンプルで

す。1 つのルールにより、任意の数の送信元が同様に任意の数の宛先と通信することを可能にできます。このような簡略化により、そのスケールと保守性が大幅に向上します。つまり、データセンター全体でより簡単に使用できることにもつながります。

セキュリティ ポリシー仕様を含むコントラクト

ACI セキュリティ モデルでは、コントラクトに EPG 間の通信を管理するポリシーが含まれます。コントラクトは通信内容を指定し、EPG は通信の送信元と宛先を指定します。コントラクトは次のように EPG をリンクします。

EPG 1 ---------- コントラクト ---------- EPG 2

コントラクトで許可されていれば、EPG 1 のエンドポイントは EPG 2 のエンドポイントと通信でき、またその逆も可能です。このポリシーの構造には非常に柔軟性があります。たとえば、EPG 1 と EPG 2 間には多くのコントラクトが存在でき、1 つのコントラクトを使用する EPG が 3 つ以上存在でき、コントラクトは複数の EPG のセットで再利用できます。

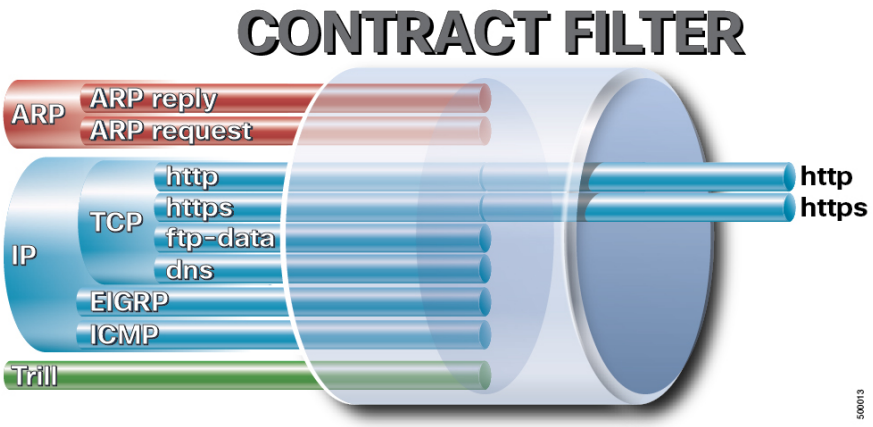
また EPG とコントラクトの関係には方向性があります。EPG はコントラクトを提供または消費できます。コントラクトを提供する EPG は通常、一連のクライアント デバイスにサービスを提供する一連のエンドポイントです。そのサービスによって使用されるプロトコルはコントラクトで定義されます。コントラクトを消費する EPG は通常、そのサービスのクライアントである一連のエンドポイントです。クライアント エンドポイント (コンシューマ) がサーバ エンドポイント (プロバイダー) に接続しようとすると、コントラクトはその接続が許可されるかどうかを確認します。特に指定のない限り、そのコントラクトは、サーバがクライアントへの接続を開始することを許可しません。ただし、EPG 間の別のコントラクトが、その方向の接続を簡単に許可する場合があります。

この提供/消費の関係は通常、EPG とコントラクト間を矢印を使って図で表されます。次に示す矢印の方向に注目してください。

EPG 1 <------- 消費 -------- コントラクト <------- 提供 -------- EPG 2

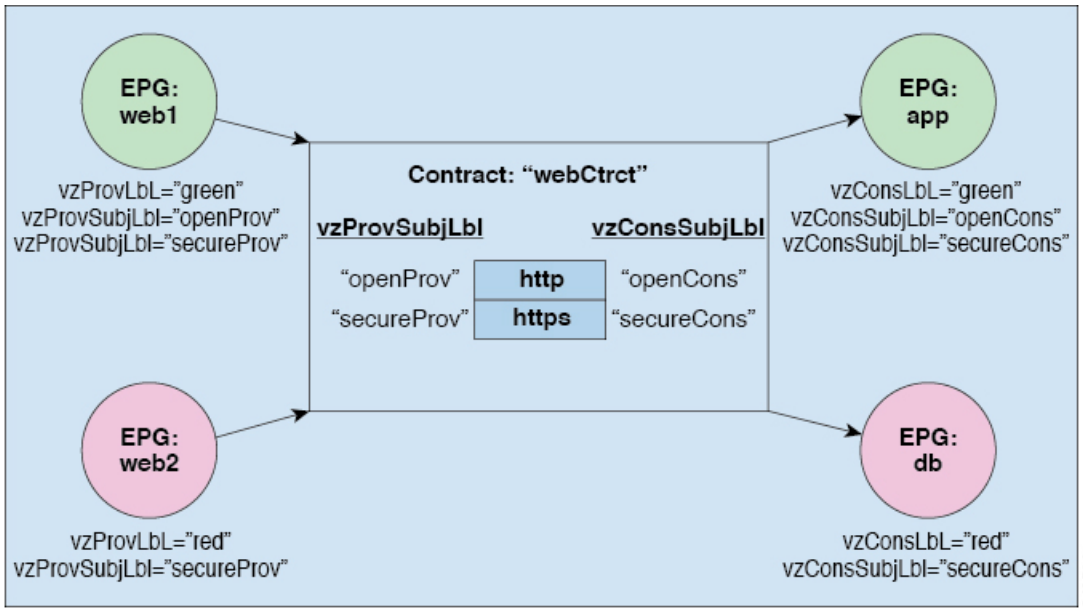
コントラクトは階層的に構築されます。1 つ以上のサブジェクトで構成され、各サブジェクトには 1 つ以上のフィルタが含まれ、各フィルタは 1 つ以上のプロトコルを定義できます。

図 *17*: コントラクト フィルタ



次の図は、コントラクトが EPG の通信をどのように管理するかを示します。

図 *18 : EPG/EPG* 通信を決定するコントラクト



たとえば、TCP ポート 80 とポート 8080 を指定する HTTP と呼ばれるフィルタと、TCP ポート 443 を指定する HTTPS と呼ばれる別のフィルタを定義できます。その後、2 セットの情報カテゴリを持つ webCtrct と呼ばれるコントラクトを作成できます。openProv と openCons are が HTTP フィルタが含まれる情報カテゴリです。secureProv と secureCons は HTTPS フィルタが含まれる情報カテゴリです。この webCtrct コントラクトは、Web サービスを提供する EPG とそのサービスを消費するエンドポイントを含む EPG 間のセキュアな Web トラフィックと非セキュアな Web トラフィックの両方を可能にするために使用できます。

これらの同じ構造は、仮想マシンのハイパーバイザを管理するポリシーにも適用されます。EPG が Virtual Machine Manager（VMM）のドメイン内に配置されると、APIC は EPG に関連付けられたすべてのポリシーを VMM ドメインに接続するインターフェイスを持つリーフ スイッチにダウンロードします。VMM ドメインの完全な説明については、『*Application Centric Infrastructure Fundamentals*』の「*Virtual Machine Manager Domains*」の章を参照してください。このポリシーが作成されると、APIC は EPG のエンドポイントへの接続を可能にするスイッチを指定する VMM ドメインにそれをプッシュ（あらかじめ入力）します。VMM ドメインは、EPG 内のエンドポイントが接続できるスイッチとポートのセットを定義します。エンドポイントがオンラインになると、適切な EPG に関連付けられます。パケットが送信されると、送信元 EPG および宛先 EPG がパケットから取得され、対応するコントラクトで定義されたポリシーでパケットが許可されたかどうかが確認されます。許可された場合は、パケットが転送されます。許可されない場合は、パケットはドロップされます。

コントラクトは 1 つ以上のサブジェクトで構成されます。各サブジェクトには 1 つ以上のフィルタが含まれます。各フィルタには 1 つ以上のエントリが含まれます。各エントリは、アクセス コントロール リスト (ACL) の 1 行に相当し、エンドポイント グループ内のエンドポイントが接続されているリーフ スイッチで適用されます。

詳細には、コントラクトは次の項目で構成されます。

- 名前：テナントによって消費されるすべてのコントラクト (common テナントまたはテナント自体で作成されたコントラクトを含む) にそれぞれ異なる名前が必要です。
- サブジェクト：特定のアプリケーションまたはサービス用のフィルタのグループ。
- フィルタ：レイヤ 2 ～ レイヤ 4 の属性 (イーサネット タイプ、プロトコル タイプ、TCP フラグ、ポートなど) に基づいてトラフィックを分類するために使用します。
- アクション：フィルタリングされたトラフィックで実行されるアクション。次のアクションがサポートされます。
  - トラフィックの許可 (通常のコントラクトのみ)
  - トラフィックのマーク (DSCP/CoS) (通常のコントラクトのみ)
  - トラフィックのリダイレクト (サービス グラフによる通常のコントラクトのみ)
  - トラフィックのコピー (サービス グラフまたは SPAN による通常のコントラクトのみ)
  - トラフィックのブロック（禁止コントラクトのみ）

    Cisco APIC リリース 3.2(x) および名前が EX または FX で終わるスイッチでは、標準コントラクトで代わりに件名 [拒否] アクションまたは [コントラクトまたは件名の除外] を使用して、指定のパターンを持つトラフィックをブロックできます。
  - トラフィックのログ（禁止コントラクトと通常のコントラクト）
- エイリアス：(任意) 変更可能なオブジェクト名。オブジェクト名は作成後に変更できませんが、エイリアスは変更できるプロパティです。

このように、コントラクトによって許可や拒否よりも複雑なアクションが可能になります。コントラクトは、所定のサブジェクトに一致するトラフィックをサービスにリダイレクトしたり、コピーしたり、その QoS レベルを変更したりできることを指定可能です。具象モデルでアクセス ポリシーをあらかじめ入力すると、APIC がオフラインまたはアクセスできない場合でも、エンドポイントは移動でき、新しいエンドポイントをオンラインにでき、通信を行うことができます。APIC は、ネットワークの単一の障害発生時点から除外されます。ACI ファブリックにパケットが入力されると同時に、セキュリティ ポリシーがスイッチで実行している具象モデルによって適用されます。

セキュリティ ポリシーの適用

トラフィックは前面パネルのインターフェイスからリーフ スイッチに入り、パケットは送信元 EPG の EPG でマーキングされます。リーフ スイッチはその後、テナント エリア内のパケットの宛先 IP アドレスでフォワーディング ルックアップを実行します。ヒットすると、次のシナリオのいずれかが発生する可能性があります。

1. ユニキャスト（/32）ヒットでは、宛先エンドポイントの EPG と宛先エンドポイントが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。

2. サブネット プレフィクス（/32 以外）のユニキャスト ヒットでは、宛先サブネット プレフィクスの EPG と宛先サブネット プレフィクスが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
3. マルチキャスト ヒットでは、ファブリック全体の VXLAN カプセル化とマルチキャスト グループの EPG で使用するローカル レシーバのローカル インターフェイスと外側の宛先 IP アドレスが提供されます。

（注） マルチキャストと外部ルータのサブネットは、入力リーフ スイッチでのヒットを常にもたらします。セキュリティ ポリシーの適用は、宛先 EPG が入力リーフ スイッチによって認識されるとすぐに発生します。

転送テーブルの誤りにより、パケットがスパイン スイッチの転送プロキシに送信されます。転送プロキシはその後、転送テーブル検索を実行します。これが誤りである場合、パケットはドロップされます。これがヒットの場合、パケットは宛先エンドポイントを含む出力リーフ スイッチに送信されます。出力リーフ スイッチが宛先の EPG を認識するため、セキュリティ ポリシーの適用が実行されます。出力リーフ スイッチは、パケット送信元の EPG を認識する必要があります。ファブリック ヘッダーは、入力リーフ スイッチから出力リーフ スイッチに EPG を伝送するため、このプロセスをイネーブルにします。スパイン スイッチは、転送プロキシ機能を実行するときに、パケット内の元の EPG を保存します。

出力リーフ スイッチでは、送信元 IP アドレス、送信元 VTEP、および送信元 EPG 情報は、学習によってローカルの転送テーブルに保存されます。ほとんどのフローが双方向であるため、応答パケットがフローの両側で転送テーブルに入力し、トラフィックが両方向で入力フィルタリングされます。

マルチキャストおよび EPG セキュリティ

マルチキャスト トラフィックでは、興味深い問題が起こります。ユニキャスト トラフィックでは、宛先 EPG はパケットの宛先の検査からはっきり知られています。ただし、マルチキャスト トラフィックでは、宛先は抽象的なエンティティ、マルチキャスト グループです。パケットの送信元はマルチキャスト アドレスではないため、送信元 EPG は以前のユニキャストの例と同様に決定されます。宛先グループの起源はマルチキャストが異なる場所です。

マルチキャスト グループが、ネットワーク トポロジから若干独立しているので、グループ バインディングへの (S, G) および (*, G) の静的設定は受け入れ可能です。マルチキャスト グループが転送テーブルにある場合、マルチキャスト グループに対応する EPG は、転送テーブルにも配置されます。

（注） このマニュアルでは、マルチキャスト グループとしてマルチキャスト ストリームを参照します。

リーフ スイッチは、マルチキャスト ストリームに対応するグループを常に宛先 EPG と見なし、送信元 EPG と見なすことはありません。前述のアクセス コントロール マトリクスでは、マルチキャスト EPG が送信元の場合は行の内容は無効です。トラフィックは、マルチキャスト ストリームの送信元またはマルチキャスト ストリームに加わりたい宛先からマルチキャストストリームに送信されます。マルチキャストストリームが転送テーブルにある必要があり、ストリーム内に階層型アドレッシングがないため、マルチキャストトラフィックは、入力ファブリックの端でアクセスが制御されます。その結果、IPv4 マルチキャストは入力フィルタリングとして常に適用されます。

マルチキャストストリームの受信側は、トラフィックを受信する前にマルチキャストストリームに最初に加わる必要があります。IGMP Join 要求を送信すると、マルチキャスト レシーバは実際に IGMP パケットの送信元になります。宛先はマルチキャスト グループとして定義され、宛先 EPG は転送テーブルから取得されます。ルータが IGMP Join 要求を受信する入力点で、アクセス制御が適用されます。Join 要求が拒否された場合、レシーバはその特定のマルチキャスト ストリームからトラフィックを受信しません。

マルチキャスト EPG へのポリシーの適用は、前述のようにコントラクトのルールに従ってリーフ スイッチにより入力時に発生します。また、EPG バインディングに対するマルチキャストグループは、APIC によって特定のテナント（VRF）を含むすべてのリーフ スイッチにプッシュされます。

タブー

セキュリティを確保する通常のプロセスも適用されますが、ACI ポリシーモデルは、どのようなセキュリティ プラクティスが採用されても完全性を確保するのに役立ちます。ACI ポリシーモデルのアプローチでは、すべての通信がこれらの条件に準拠する必要があります。

- 通信は、モデルの管理対象オブジェクトであるコントラクトに基づいてのみ許可されます。コントラクトがなければ、EPG 間通信はデフォルトでディセーブルになります。
- ハードウェアへのダイレクト アクセスはなく、すべてのインタラクションはポリシー モデルを通じて管理されます。

禁止コントラクトは特定のトラフィックを拒否するために使用できます。そうしないと、コントラクトによって許可されます。ドロップされるトラフィックは、パターンと一致しています（すべての EPG、特定の EPG、フィルタに一致するトラフィックなど）。禁止ルールは単方向で、コントラクトを提供する EPG に対して一致するトラフィックを拒否します。

Cisco APIC リリース 3.2(x) および名前が EX または FX で終わるスイッチでは、標準コントラクトで代わりに件名 [拒否] アクションまたは [コントラクトまたは件名の除外] を使用して、指定のパターンを持つトラフィックをブロックできます。

ACL コントラクトおよび拒否ログの有効化および表示

ACL 契約の許可および拒否ログについて

契約ルールのトラフィック フローをログ記録および監視するには、契約の許可ルールのため送信されることが許可されたパケットまたはフローのログを有効化および表示するか、契約の許可ルールのためドロップされたフローのログを有効化および表示できます。

- 禁止契約拒否ルール
- 契約の件名でアクションを拒否する
- 契約または件名の例外
- ACI ファブリックの ACL コントラクト許可は、EX または FX で終わる名前の Nexus 9000 シリーズ スイッチ、およびそれ以降のすべてのモデルでのみサポートされます。たとえば、N9K-C93180LC-EX や N9K-C9336C-FX のように指定してください。
- ACI ファブリックでのログの拒否は、すべてのプラットフォームでサポートされています。
- 管理契約のフィルタでログ directive を使用することはサポートされていません。ログ directive を設定すると、ゾーン分割ルールの展開エラーが発生します。

標準および禁止契約と件名についての詳細は、『*CiscoApplication Centric Infrastructure Fundamentals*』および『*Cisco APIC Basic Configuration Guide*』を参照してください。

ACL 許可および拒否ログ出力に含まれる EPG データ

Cisco APIC、リリース 3.2(1) まで、ACL 許可および拒否ログでは、記録されている契約に関連付けられた EPG を識別していませんでした。リリース 3.2(1) では、送信元 EPG と 送信先 EPG が ACI 許可および拒否ログの出力に追加されます。ACL 許可および拒否ログには、次の制限を持つ関連 EPG を含めます。

- ネットワーク内の EPG の配置によっては、ログの EPG データを使用できない場合があります。
- 設定の変更が発生するとき、ログデータが期限切れになっている可能性があります。安定した状態では、ログ データは正確です。

ログが次にフォーカスされているとき、許可および拒否ログの EPG データは最も正確になります。

- 入力 TOR で入力ポリシーがインストールされており、出力 TOR で出力ポリシーがインストールされている場合の EPG から EPG へのフロー。
- 境界リーフ TOR で 1 個のポリシーが適用され、非 BL TOR で他のポリシーが適用されている場合の EPG から L3Out へのフロー。

ログ出力の EPG は、共有サービス（共有 L3Outs を含む）で使用される uSeg Epg または Epg ではサポートされていません。

GUI を使用してACL 契約の許可とロギングの拒否を有効にする

次の手順では、GUI を使用してACL 契約の許可とロギングの拒否を有効にする方法を表示します。

（注） 許可ロギングを含むテナントは、EPG が関連する VRF を含むテナントです。これは必ずしも EPG と同じテナントや関連する契約である必要はありません。

ステップ 1 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、[Contracts] を展開し、 [Standard] を右クリックして [Create Contract] を選択します。

ステップ 3 [Create Contract] ダイアログボックスで、次の作業を実行します。

a) [Name] フィールドに、契約の名前を入力します。
b) [Scope] フィールドで、そのスコープ（[VRF]、[Tenant]、または [Global]）を選択します
c) オプション。契約に適用するターゲット DSCP または QoS クラスを設定します。
d) [+] アイコンをクリックして、[Subject] を展開します。

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

ステップ 5 件名の名前と詳細な説明を入力します。

ステップ 6 オプション。ターゲット DSCP のドロップダウン リストから、件名に適用する DSCP を選択します。

ステップ 7 契約を両方向でなくコンシューマからプロバイダの方向にのみ適用するのでない限り、[Apply Both Directions] はオンにしたままにしておきます。

ステップ 8 [Apply Both Directions] をチェックしてない場合 [Reverse Filter Ports] をチェックしたままにして、ルールがプロバイダから消費者に適用されるようにレイヤ 4 ソースと宛先ポートを交換します。

ステップ 9 [+] アイコンをクリックして、[Filters] を展開します。

ステップ 10 [Name] ドロップダウンリストで、たとえば、**arp**、**default**、**est**、**icmp** などオプションを選択するか、以前設定したフィルタを選択します。

ステップ 11 [Directives] ドロップダウン リストで、[log] をクリックします。

ステップ 12 （任意） この件名で実行するアクションを [Deny] に変更します（またはアクションをデフォルトの [Permit] のままにします。

Directive：ログ有効化により、この件名のアクションが [Permit] になっている場合、ACL は件名と契約により制御されているフローとパケットを追跡します。この件名のアクションが [Deny] の場合、ACL の拒否ログはフローとパケットを追跡します。

ステップ 13 （任意） 件名の優先順位を設定します。

ステップ 14 [Update] をクリックします。

ステップ 15 [OK] をクリックします。

ステップ 16 **[送信（Submit）]** をクリックします。
ロギングがこの契約に対して有効になります。

NX-OS CLI を使用した ACL 契約許可ロギングの有効化

次の例は、NX-OS CLI を使用して契約許可ロギングを有効にする方法を示しています。

ステップ 1 契約許可ルールにより送信できたパケットまたはフローのロギングを有効にするには、次のコマンドを使用します。

```
configure
tenant <tenantName>
contract <contractName> type <permit>
subject <subject Name>
access-group <access-list> <in/out/both> log
```

例：

次に例を示します。

```
apic1# configure
apic1(config)# tenant BDMode1
apic1(config-tenant)# contract Logicmp type permit
apic1(config-tenant-contract)# subject icmp
apic1(config-tenant-contract-subj)# access-group arp both log
```

ステップ 2 許可ロギングを無効にするには、**no** 形式の access-group コマンドを使用します。たとえば、`no access-group arp both log` コマンドを使用します。

REST API を使用した ACL 契約許可ロギングの有効化

次の例は、REST API を使用して許可および拒否ロギングを有効にする方法を示しています。この例では、ACL の許可を設定し、件名 Permit 設定し、設定されたアクションを拒否するには、契約のロギングを拒否します。

この設定では、次の例のように XML で post を送信します。

例：

```
<vzBrCP dn="uni/tn-Tenant64/brc-C64" name="C64" scope="context">
    <vzSubj consMatchT="AtleastOne" name="HTTPSsbj" provMatchT="AtleastOne" revFltPorts="yes"
rn="subj-HTTPSsbj">
          <vzRsSubjFiltAtt action="permit" directives="log" forceResolve="yes"
priorityOverride="default"
rn="rssubjFiltAtt-PerHTTPS" tDn="uni/tn-Tenant64/flt-PerHTTPS" tRn="flt-PerHTTPS"
tnVzFilterName="PerHTTPS"/>
    </vzSubj>
    <vzSubj consMatchT="AtleastOne" name="httpSbj" provMatchT="AtleastOne" revFltPorts="yes"
rn="subj-httpSbj">
```

```
        <vzRsSubjFiltAtt action="deny" directives="log" forceResolve="yes" priorityOverride="default"

rn="rssubjFiltAtt-httpFilter" tDn="uni/tn-Tenant64/flt-httpFilter" tRn="flt-httpFilter"
tnVzFilterName="httpFilter"/>
    </vzSubj>
    <vzSubj consMatchT="AtleastOne" name="subj64" provMatchT="AtleastOne" revFltPorts="yes"
rn="subj-subj64">
        <vzRsSubjFiltAtt action="permit" directives="log" forceResolve="yes" priorityOverride="default"

rn="rssubjFiltAtt-icmp" tDn="uni/tn-common/flt-icmp" tRn="flt-icmp" tnVzFilterName="icmp"/>
    </vzSubj>
</vzBrCP>
```

GUI を使用した禁止契約拒否ロギングの有効化

次の手順は、GUIを使用して禁止コントラクトの拒否ロギングを有効にする方法を示しています。

ステップ 1 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、[Contracts] を展開します。

ステップ 3 [Taboos] を右クリックし、[Create Taboo Contract] を選択します。

ステップ 4 [Create Taboo Contract] ダイアログ ボックスで、次の操作を実行して禁止契約を指定します。

a) [Name] フィールドに、契約の名前を入力します。

b) オプション。[Description] フィールドに、禁止契約の説明を入力します。

c) [+] アイコンをクリックして、[Subject] を展開します。

ステップ 5 [Create Taboo Contract Subject] ダイアログ ボックスで、次の操作を実行します。

a) [Specify Identity of Subject] 領域に、名前と説明（オプション）を入力します。

b) [+] アイコンをクリックして、[Filters] を展開します。

c) [Name] ドロップダウン リストから、**<tenant_name>/arp**、**<tenant_name>/default**、**<tenant_name>/est**、**<tenant_name>/icmp** などのデフォルト値のいずれかを選択し、以前作成したフィルタか [Create Filter] を選択します。

（注） [Specify Filter Identity] 領域で [Create Filter] を選択した場合、次の操作を実行して、ACL 拒否ルールの基準を指定します。

1. 名前とオプションの説明を入力します。
2. [Entries] を展開し、ルールの名前を入力して、拒否するトラフィックを定義する条件を選択します。
3. [Directives] ドロップダウンリストで [log] を選択します。
4. [Update] をクリックします。
5. [OK] をクリックします。

ステップ 6 **[送信（Submit）]** をクリックします。
ロギングがこの禁止契約に対して有効になります。

NX-OS CLI を使用した禁止契約拒否ロギングの有効化

次の例は、NX-OS CLI を使用して禁止契約拒否ロギングを有効にする方法を示しています。

ステップ 1 禁止契約拒否ルールのためにドロップされたパケットまたはフローのロギングを有効にするには、次のコマンドを使用します。

```
configure
tenant <tenantName>
contract <contractName> type <deny>
subject <subject Name>
access-group <access-list> <both> log
```

例：

次に例を示します。

```
apic1# configure
apic1(config)# tenant BDMode1
apic1(config-tenant)# contract dropFTP type deny
apic1(config-tenant-contract)# subject dropftp
apic1(config-tenant-contract-subj)# access-group ftp both log
```

ステップ 2 拒否ロギングを無効にするには、**no** 形式の access-group コマンドを使用します。たとえば、`no access-group https both log` コマンドを使用します。

REST API を使用した禁止契約拒否ロギングの有効化

次の例は、REST API を使用して禁止契約拒否ロギングを有効にする方法を示しています。

タブー契約を設定するロギングを拒否する、次の例のように XML で post を送信します。

例：

```
<vzTaboo dn="uni/tn-Tenant64/taboo-TCtrctPrefix" name="TCtrctPrefix" scope="context">
    <vzTSubj name="PrefSubj" rn="tsubj-PrefSubj"">
        <vzRsDenyRule directives="log" forceResolve="yes" rn="rsdenyRule-default" tCl="vzFilter"
tDn="uni/tn-common/flt-default" tRn="flt-default"/>
    </vzTSubj>
</vzTaboo>
```

GUI を使用した ACL 許可および拒否ログの表示

次の手順は、GUI を使用して、トラフィック フローの ACL 許可および拒否ログを（有効になっていれば）表示する方法を示しています。

ステップ 1 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 <tenant name>] をクリックします。

ステップ 3 **Tenants <tenant name> [Work]** ペインで、**[Operational]** タブをクリックします。

ステップ 4 [Operational] タブの下で、[Flows] タブをクリックします。
[Flows] タブの下で、いずれかのタブをクリックして、レイヤ 2 許可ログ（[L2 Permit]）、レイヤ 3 許可ログ（[L3 Permit]）、レイヤ 2 拒否ログ（[L2 Drop]）、またはレイヤ 3 拒否ログ（[L3 Drop]）のログ データを表示します。各タブで、トラフィックがフローしていれば、ACL ロギング データを表示できます。データ ポイントは、ログ タイプと ACL ルールに応じて異なります。たとえば、[L3 Permit] ログおよび [L3 Deny] ログには次のデータ ポイントが含まれます。

- VRF
- Alias
- 送信元 IP アドレス
- 宛先 IP アドレス
- プロトコル
- 送信元ポート
- 宛先ポート
- 送信元 MAC アドレス
- 宛先 MAC アドレス
- Node
- 送信元インターフェイス
- VRF Encap
- 送信元 EPG
- 宛先 EPG
- 送信元 PC タグ
- 宛先 PC タグ

（注） また、[Flows] タブの横の [Packets] タブを使用して、シグニチャ、送信元、および宛先が同じであるパケットのグループ（最大 10 個）の ACL ログにアクセスできます。送信されたりドロップされたりするパケットのタイプを確認できます。

REST API を使用した ACL 許可および拒否ログ

次の例は、REST API を使用して、トラフィック フローのレイヤ 2 拒否ログ データを表示する方法を示しています。次の MO を使用してクエリを送信することができます。

- acllogDropL2Flow
- acllogPermitL2Flow
- acllogDropL3Flow
- acllogPermitL3Flow
- acllogDropL2Pkt
- acllogPermitL2Pkt
- acllogDropL3Pkt
- acllogPermitL3Pkt

始める前に

ACL 契約許可および拒否ログのデータを表示する前に、許可または拒否ロギングを有効にする必要があります。

レイヤ 3 ドロップ ログ データを表示するには、REST API を使用して次のクエリを送信します。

```
GET https://apic-ip-address/api/class/acllogDropL3Flow
```

例：

次の例では、サンプル出力をいくつか示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <acllogPermitL3Flow childAction="" dn="topology/pod-1/node-101/ndbgs/acllog/tn-common/ctx-inb

/permitl3flow-spctag-333-dpctag-444-sepgname-unknown-depgname-unknown-sip-[100:c000:a00:700:b00:0:f00:0]


-dip-[19.0.2.10]-proto-udp-sport-17459-dport-8721-smac-00:00:15:00:00:28-dmac-00:00:12:00:00:25-sintf-

        [port-channel5]-vrfencap-VXLAN: 2097153" dstEpgName="unknown" dstIp="19.0.2.10"
dstMacAddr="00:00:12:00:00:25"
        dstPcTag="444" dstPort="8721" lcOwn="local" modTs="never" monPolDn="" protocol="udp"
srcEpgName="unknown"
       srcIntf="port-channel5" srcIp="100:c000:a00:700:b00:0:f00:0" srcMacAddr="00:00:15:00:00:28"
 srcPcTag="333"
        srcPort="17459" status="" vrfEncap="VXLAN: 2097153"/>
    <acllogPermitL3Flow childAction="" dn="topology/pod-1/node-102/ndbgs/acllog/tn-common/ctx-inb

/permitl3flow-spctag-333-dpctag-444-sepgname-unknown-depgname-unknown-sip-[100:c000:a00:700:b00:0:f00:0]-dip-


[19.0.2.10]-proto-udp-sport-17459-dport-8721-smac-00:00:15:00:00:28-dmac-00:00:12:00:00:25-sintf-
        [port-channel5]-vrfencap-VXLAN: 2097153" dstEpgName="unknown" dstIp="19.0.2.10"
dstMacAddr="00:00:12:00:00:25"
        dstPcTag="444" dstPort="8721" lcOwn="local" modTs="never" monPolDn="" protocol="udp"
```

```
srcEpgName="unknown"
       srcIntf="port-channel5" srcIp="100:c000:a00:700:b00:0:f00:0" srcMacAddr="00:00:15:00:00:28"
 srcPcTag="333"
        srcPort="17459" status="" vrfEncap="VXLAN: 2097153"/>
</imdata>
```

NX-OS CLI を使用した ACL 許可および拒否ログの表示

次の手順は、NX-OS スタイル CLI **show acllog** コマンドを使用して ACL ログの詳細を表示する方法を示しています。

レイヤ 3 コマンドの構文は、**show acllog {permit | deny} l3 {pkt | flow} tenant <tenant_name> vrf <vrf_name> srcip <source_ip> dstip <destination_ip> srcport <source_port> dstport <destination_port> protocol <protocol> srcintf <source_interface> start-time <startTime> end-time <endTime> detail** です。

レイヤ 2 コマンドの構文は、**show acllog {permit | deny} l2 {flow | pkt} tenant <tenant_name> vrf <VRF_name> srcintf <source_interface> vlan <VLAN_number> detail** です。

（注） **show acllog** コマンドの完全な構文は、第二世代 Cisco Nexus 9000 シリーズ スイッチ（N9K-C93180LC-EX など名前の最後に EX または FX がつく。もしくはそれ以降のシリーズ）および Cisco APIC リリース 3.2 以降でのみ使用できます。第一世代のスイッチ（名前の最後に EX または FX が付かない）または 3.2 以前の Cisco APIC リリースでは、使用可能な構文は上記の通りです。

Cisco APIC 3.2 以降では、追加のキーワードが **detail** keyword:**[dstEpgName <destination_EPG_name>| dstmac <destination_MAC_address> | dstpctag <destination_PCTag> | srcEpgName <source_EPG_name> | srcmac <source_MAC_address> | srcpctag <source_PCTag>]** とともにコマンドの両方のバージョンに追加されます。

ステップ 1 次の例では、**show acllog drop l3 flow tenant common vrf default detail** コマンドを使用して、共通テナントのレイヤ 3 拒否ログに関する詳細情報を表示する方法を示します。

例：

```
apic1# show acllog deny l3 flow tenant common vrf default detail
SrcPcTag  : 49153
DstPcTag  : 32773
SrcEPG    : uni/tn-TSW_Tenant0/ap-tsw0AP0/epg-tsw0ctx0BD0epg6
DstEPG    : uni/tn-TSW_Tenant0/ap-tsw0AP0/epg-tsw0ctx0BD0epg5
SrcIp     : 16.0.2.10
DstIp     : 19.0.2.10
Protocol  : udp
SrcPort   : 17459
DstPort   : 8721
SrcMAC    : 00:00:15:00:00:28
DstMAC    : 00:00:12:00:00:25
Node      : 101
```

```
SrcIntf   : port-channel5
VrfEncap  : VXLAN: 2097153
```

この例では第二世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

ステップ 2 次の例では、**show acllog deny l2 flow tenant common vrf tsw0connctx0 detail** コマンドを使用して、共通テナントのレイヤ 3 拒否ログに関する詳細情報を表示する方法を示します。

例：

```
apic1# show acllog deny l2 flow tenant common vrf tsw0connctx0 detail
SrcPcTag DstPcTag   SrcEPG           DstEPG          SrcMAC            DstMAC         Node   SrcIntf
   vlan
--------- --------- ----------------  --------------  ------------------  ------------------
-----   ---------  ------
 32773    49153   uni/tn-TSW       uni/tn-TSW  00:00:11:00:00:11  11:00:32:00:00:33   101     port-
     2
                _Tenant0/ap-     _Tenant0/ap-                                                channel8

                 tsw0AP0/epg-     tsw0AP0/epg-
                 tsw0ctx0BD0epg5  tsw0ctx0BD0epg6
```

この例では第二世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

ステップ 3 次の例では、**show acllog permit l3 pkt tenant <tenant name> vrf <vrf name> [detail]** コマンドを使用して、送信された一般的な VRF ACL レイヤ 3 許可パケットに関する詳細情報を表示する方法を示しています。

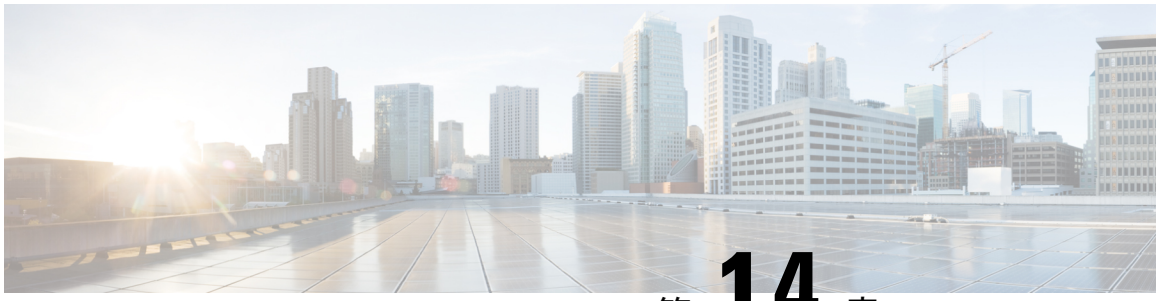
```
apic1# show acllog permit l3 pkt tenant common vrf default detail acllog permit l3 packets detail:
srcIp      : 10.2.0.19
dstIp      : 10.2.0.16
protocol   : udp
srcPort    : 13124
dstPort    : 4386
srcIntf    : port-channel5
vrfEncap   : VXLAN: 2097153
pktLen     : 112
srcMacAddr : 00:00:15:00:00:28
dstMacAddr : 00:00:12:00:00:25
timeStamp  : 2015-03-17T21:31:14.383+00:00
```

この例では第一世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

ステップ 4 次の例では、**show acllog permit l2 pkt tenant <tenant name> vrf <vrf name> srcintf <s interface>** コマンドを使用して、インターフェイス ポートチャネル 15 から送信されたデフォルトの VRF レイヤ 2 パケットに関する情報を表示する方法を示しています。

```
apic1# show acllog permit l2 pkt tenant common vrf default srcintf port-channel5
acllog permit L2 Packets
      Node          srcIntf       pktLen     timeStamp
 --------------  --------------  --------  --------------
                 port-channel5      1      2015-03-17T21:
                                           31:14.383+00:00
```

この例では第一世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。



第 14 章

データ プレーン ポリシング

この章は、次の項で構成されています。

データ プレーン ポリシングの概要

データ プレーン ポリシング（DPP）を使用して、Cisco Application Centric Infrastructure（ACI）ファブリック アクセス インターフェイスの帯域幅使用量を管理します。DPP ポリシーは出力トラフィック、入力トラフィック、またはその両方に適用できます。DPP は特定のインターフェイスのデータ レートを監視します。データ レートがユーザ設定値を超えると、ただちにパケットのマーキングまたはドロップが発生します。ポリシングではトラフィックがバッファリングされないため、伝搬遅延への影響はありません。トラフィックがデータ レートを超えた場合、Cisco ACI ファブリックは、パケットのドロップか、パケット内 QoS フィールドのマーキングのどちらかを実行できます。

3.2 リリースより前は、DPP ポリシーが EPG に適用されている場合、ポリサーの標準的な動作は EPG メンバーごとでしたが、レイヤ 2 およびレイヤ 3 の場合は同じポリサーがリーフ スイッチに割り当てられていました。この区別は、レイヤ 2/レイヤ 3 ケースの DPP ポリサーがすでにインターフェイスごとになっていると想定されたため行われました。そのため、異なるのインターフェイスは、別のポリサーを取得できると想定されました。EPG ごとの DPP ポリシーが導入されましたが、特定のリーフ スイッチに複数のメンバーが存在する可能性があることは明らかでした。したがって、ポリサーは、不要なドロップを避けるためにメンバーごとにすることが理にかなっていました。

3.2のリリース以降、明確なセマンティクスはデータ プレーン ポリサー ポリシー自体になり、同じように CLI に示されるように共有モード設定を導入する新しいフラグです。基本的に、データ プレーン ポリサーがレイヤ 2/レイヤ 3 または各 EPG に適用される場合、異なる暗黙の動作はありません。現在、ユーザーは動作の管理が可能です。共有モードが**[共有済み（shared）]**に設定されている場合、同じデータ プレーン ポリサーを参照するリーフ スイッチ上のすべてのエンティティが同じハードウェア ポリサーを共有します。共有モードが**[専用（dedicated）]**に設定されている場合、リーフ スイッチの各レイヤ 2 またはレイヤ 3 または EPG メンバーに異なるHWポリサーが割り当てられます。ポリサーは、制限する必要があるエンティティ専用です。

DPPポリシーは、シングルレート、デュアルレート、カラー対応のいずれかになります。シングルレートポリシーは、トラフィックの認定情報レート（CIR）を監視します。デュアルレート ポリサーは、CIR と最大情報レート（PIR）の両方を監視します。また、システムは、関連するバースト サイズもモニタします。指定したデータ レート パラメータに応じて、適合（グリーン）、超過（イエロー）、違反（レッド）の3つのカラー、つまり条件が、パケットごとにポリサーによって決定されます。

通常、DPPポリシーは、サーバやハイパーバイザなどの仮想または物理デバイスへの物理または仮想レイヤ2接続に適用されます。ルータについてはレイヤ3接続で適用されます。リーフ スイッチ アクセス ポートに適用される DPP ポリシーは、Cisco ACI ファブリックのファブリック アクセス（インフラ）部分で設定され、ファブリック管理者が設定する必要があります。境界リーフ スイッチ アクセス ポート（l3extOut または l2extOut）のインターフェイスに適用される DPP ポリシーは、Cisco ACI ファブリックのテナント（fvTenant）部分で設定され、テナント管理者が設定できます。

データ プレーン ポリサーを EPG に適用して、エンドポイントのグループから Cisco ACI ファブリックに入るトラフィックが、EPG のメンバー アクセス インターフェイスごとに制限されるようにすることもできます。これは、1 つ EPG のさまざまな Epg でアクセス リンクを共有する場所の monopolization を防ぐために役立ちます。

各状況に設定できるアクションは1つだけです。たとえば、DPP ポリシーを最大 200 ミリ秒のバーストで、256,000 bps のデータ レートに適合させることが可能です。この場合、システムは、このレートの範囲内のトラフィックに対して適合アクションを適用し、このレートを超えるトラフィックに対して違反アクションを適用します。カラー対応ポリシーは、トラフィックが以前にカラーによってすでにマーキングされているものと見なします。次に、このタイプのポリサーが実行するアクションの中で、その情報が使用されます。

トラフィック ストーム制御に関する詳細は、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』を参照してください。

注意事項と制約事項

下記はデータプレーンポリシングの構成に関する注意事項と制限事項です。

- データプレーンは、ACI ファブリック アクセス インターフェイス上の CPU および CPU バウンド パケットから送信されたパケットをポリシングしません。
- **専用ポリサー**共有モードは、レイヤ 2 インターフェイスではサポートされていません。

次に、EPG ポリシングの注意事項と制限事項を示します。

- 機能サポートは、EX または FX で終わるスイッチ モデルおよびそれ以降の後続モデルから開始されます（例：N9K-C93180YC-EX）。
- EPG レベル ポリサーでは、出力トラフィック ポリシングはサポートされていません。
- ポリサー モード packet-per-second はサポートされていません。
- ポリサー タイプ 2R3C はサポートされていません。
- EPG で **EPG 内分離**が適用されている場合、ポリサーはサポートされません。
- **調整**の統計情報およびに考慮事項には次が含まれます。
  - 許可/ドロップされたパケットを認識することは、移行に関する問題やリソースの多用を知るために重要です。
  - 統計情報は、統計情報のインフラストラクチャを使用してGUIで提供されます。統計は、Cisco ACI ファブリック内の統計と同様に REST API を介してエクスポートされます。
  - 統計情報は各 EPG メンバーで使用でき、データプレーン ポリサーポリシーが [**専用（dedicated**）] タイプの場合に便利です。その代わり、リーフスイッチ上で使用すると統計情報がすべてのポートの統計を反映します。
- フレームが FCoE でサポートされているデバイスを通過する場合など、特定のケースではこれらは no drop FCoE クラスに分類されます。FCoE デバイスでは、パケット長が許可されている 2,184 バイトよりも長い場合、パケットがドロップオフする可能性があります。

GUIを使用したレイヤ2インターフェイスのデータプレーンポリシングの構成

始める前に

データプレーン ポリシングポリシーを構成するテナント、VRF、外部ルーテッドネットワークはすでに作成されている必要があります。

レイヤ2データプレーン ポリシングポリシーを適用するには、ポリシーをポリシーグループに追加し、ポリシーグループをインターフェイス プロファイルにマッピングする必要があります。

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）]** > **[インターフェイス（Interface）]** > **[データ ピレーン ポリシング（Data Plane Policing**） を選択します

ステップ 3 [Data Plane Policing Policing] を右クリックし、 [Create a Data Plane Policing Policy] をクリックします。

ステップ 4 [Create a Data Plane Policing Policy] ダイアログボックスの [Name] フィールドに、ポリシーの名前を入力します。

ステップ 5 [**管理状態（Administrative State**）] は [**有効（enabled**）] を選択します。

ステップ 6 [**BGP ドメインポリサーモード（BGP Domain Policer Mode**）]では、[**ビットポリサー（Bit Policer**）]または[**パケットポリサー（Packet Policer**）**]**を選択します。

ステップ 7 **[タイプ（Type）]** では、**[1 レート 2 カラー（1 Rate 2 Color）]** または **[2 レート 3 カラー（2 Rate 3 Color）]** を選択します。

EX/FX で終わるスイッチモデル（例：N9K-C93180YC-EX）以降のモデルは、**2 レート 3 カラー**をサポートしていません。

ステップ 8 [**適合アクション（Conform Action**）] で、アクションを選択します。

この選択により、特定の条件に一致するトラフィックのアクションが定義されます。

- **ドロップ**：条件が満たされた場合、パケットをドロップします。
- **マーク**：条件が満たされた場合にパケットにマークを付けます。
- **送信**：条件が満たされた場合、パケットを送信します。

ステップ 9 [**適合アクション（Conform Action**）] で [**マーク（Mark**）] を選択した場合は、次のサブステップを実行します。

a) [**適合マーク CoS（Conform mark CoS**）] には、条件に適合したパケットのサービスクラスを入力します。

b) [**適合マーク dscp（Conform mark dscp**）] には、条件に適合したパケットの差別化サービスコードポイント（DSCP）を入力します。

ステップ 10 管理者は、[Conform] と [Violate] フィールドの CoS および DSCP 値を設定できます。

ステップ 11 [**タイプ（Type**）] で [**2 レート 3 カラー（2 Rate 3 Color**）] を選択した場合、[**超過アクション（Exceed Action**）] でアクションを選択します。

この選択によって、ある一定の条件を超えるトラフィックのアクションを定義します。

- **ドロップ**：条件が満たされた場合、パケットをドロップします。
- **マーク**：条件が満たされた場合にパケットにマークを付けます。
- **送信**：条件が満たされた場合、パケットを送信します。

ステップ 12 [**超過アクション（Exceed Action**）] で [**マーク（Mark**）] を選択した場合は、次のサブステップを実行します。

a) [**超過マーク CoS（Exceed mark CoS**）] には、条件を超えたパケットのサービスクラスを入力します。

b) [**超過マーク dscp（Exceed mark dscp**）] には、条件を超えたパケットの差別化サービスコード ポイント（DSCP）を入力します。

ステップ 13 [**違反アクション（Violate Action**）] で、アクションを選択します。

この選択によって、特定の条件に違反するトラフィックのアクションを定義します。

- **ドロップ**：条件が満たされた場合、パケットをドロップします。
- **マーク**：条件が満たされた場合にパケットにマークを付けます。
- **送信**：条件が満たされた場合、パケットを送信します。

ステップ 14 [**違反アクション（Violate Action**）] で [**マーク（Mark**）] を選択した場合は、次のサブステップを実行します。

a) [**違反マーク CoS（Violate mark CoS**）] には、条件に違反したパケットのサービスクラスを入力します。

b) [**違反マーク dscp（Violate mark dscp**）] には、条件に違反したパケットの差別化サービスコードポイント (DSCP) を入力します。

ステップ 15 [**共有モード（Sharing Mode**）] で、[**共有ポリサー（Shared Policer**）] を選択します。

[**共有ポリサー（Shared Policer**）] モード機能を使用すると、同じポリシングパラメータを複数のインターフェイスに同時に適用できます。[**専用ポリサー（Dedicated Policer**）] モードは、レイヤ 2 インターフェイスではサポートされていません。

ステップ 16 [**レート（Rate**）] には、パケットがシステムに許可されるレートを入力し、パケットごとの単位を選択します。

ステップ 17 [**バースト（Burst**）] には、バースト中にラインレートで許可されるパケット数を入力し、パケットごとの単位を選択します。

ステップ 18 [**タイプ（Type**）] で [**2 レート 3 カラー（2 Rate 3 Color**）] を選択した場合は、次のサブステップを実行します。

a) [**ピークレート（Peak Rate**）] には、データトラフィックに悪影響を与えるレートであるピーク情報レートを入力し、パケットあたりの単位を選択します。

b) [**超過バースト（Excessive Burst**）] には、すべてのトラフィックがピーク情報レートを超える前にトラフィックバーストが到達できるサイズを入力し、パケットあたりの単位を選択します。

ステップ 19 [送信（Submit）] をクリックします。

これでレイヤ 2 の DPP 構成は完了です。データプレーンポリシーを、レイヤ 2 インターフェイスにマッピングするインターフェイスポリシーグループにマッピングできるようになりました。

APIC GUI を使用したレイヤ 3 インターフェイスのデータ プレーン ポリシングを設定する

始める前に

データ プレーン ポリシング ポリシーを設定するテナント、VRF、外部ルーテッド ネットワークはすでに作成されています。

データ プレーン ポリシング ポリシーは、インターフェイス プロファイルにマッピングされたポリシー グループおよびポリシー グループに追加され、L3 DPP ポリシーを適用する必要があります。

ステップ 1 **[ナビゲーション]** ペインで、**[Tenant_name]** > **[ネットワー キング]** > **[外部ルーテッド ネットワーク]** > **[Network_name]** > **[論理ノード プロファイル]** > **[論理ノード生成]** > **[論理インターフェイス プロファイル]** をクリックして、次のアクションを実行します。

a) **[論理インターフェイス プロファイル]** を右クリックして、**[インターフェイス プロファイルの作成]** を選択します。

b) [Create Interface Profile] ダイアログボックスの [Name] フィールドに、プロファイルの名前を入力します。

c) [Ingress Data Plane Policing] の隣にある [Create Data Plane Policing Policy] を選択します。

d) [Name] フィールドにポリシーの名前を入力します。

e) [Administrative State] フィールドで、[enabled] をクリックします。

f) [Policer Mode] の隣にある [Bit Policer] または [Packet Policer] のどちらかのボタンを選択します。

g) [Type] の隣にある [1 Rate 2 Color] または [2 Rate 3 Color] のボタンを選択します。

EX/FX で終わるスイッチ モデル (例: N9K-C93180YC-EX) 以降のモデルは、2 レート 3 カラーをサポートしていません)。

a) 管理者は、[Conform] と [Violate] フィールドの CoS および DSCP 値を設定できます。

b) [Sharing Mode] フィールドで、ポリサー モードを選択します。

（注） 共有ポリサー モード機能を使用すると、同じポリシング パラメータを複数のインターフェイスに同時に適用できます。

c) [Burst]、[Excessive Burst]、[Rate] フィールドの隣にあるドロップダウン矢印を選択し、[1 Rate 2 Color] ポリシー タイプの各パケット レートを設定します。

（注） **[2 レート 3 色]** ポリシー タイプでは、**[ピーク レート]** フィールが追加されます。

d) [Submit] をクリックします。

ステップ 2 **[ルーテッド インターフェイス]** 表を展開して、**[パス]** フィールドでインターフェイスに移動し、ポリシーを適用して、次のアクションを実行します。

a) **[IPv4 または Ipv6 優先アドレス]** の隣にあるサブネット IP アドレスを入力します。

b) [OK] をクリックします。
c) **[SVI]** タブをクリックして展開し、**[パス]** フィールドでインターフェイスに移動し、ポリシーを適用します。
d) **[Encap]** の隣に VLAN 名を入力します。
e) **[IPv4 または Ipv6 優先アドレス]** の隣にあるサブネット IP アドレスを入力します。
f) [OK] をクリックします。
g) **[ルーティング サブインターフェイス]** タブを展開し、ルーテッド インターフェイスとして同じ設定手順を実行します。
h) [OK] をクリックします。これにより L3 の DPP 設定を完了します。

REST API を使用したデータ プレーン ポリシングの設定

リーフ スイッチに着信するレイヤ2トラフィックをポリシングするには、次の手順を実行します。

```
<!--  api/node/mo/uni/.xml  -->
<infraInfra>
<qosDppPol name="infradpp5" burst="2000" rate="2000" be="400" sharingMode="shared"/>
<!--
 List of nodes. Contains leaf selectors. Each leaf selector contains list of node blocks
-->
<infraNodeP name="leaf1">
<infraLeafS name="leaf1" type="range">
<infraNodeBlk name="leaf1" from_="101" to_="101"/>
</infraLeafS>
<infraRsAccPortP tDn="uni/infra/accportprof-portselector1"/>
</infraNodeP>
<!--
 PortP contains port selectors. Each port selector contains list of ports. It
       also has association to port group policies
-->
<infraAccPortP name="portselector1">
<infraHPortS name="pselc" type="range">
<infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="48" toPort="49"></infraPortBlk>
<infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-portSet2"/>
</infraHPortS>
</infraAccPortP>
<!--  FuncP contains access bundle group policies  -->
<infraFuncP>
<infraAccPortGrp name="portSet2">
<infraRsQosIngressDppIfPol tnQosDppPolName="infradpp5"/>
</infraAccPortGrp>
</infraFuncP>
</infraInfra>
```

リーフ スイッチから発信されるレイヤ2トラフィックをポリシングするには、次の手順を実行します。

```
<!--  api/node/mo/uni/.xml  -->
<infraInfra>
<qosDppPol name="infradpp2" burst="4000" rate="4000"/>
<!--
 List of nodes. Contains leaf selectors. Each leaf selector contains list of node blocks
-->
```

```
<infraNodeP name="leaf1">
<infraLeafS name="leaf1" type="range">
<infraNodeBlk name="leaf1" from_="101" to_="101"/>
</infraLeafS>
<infraRsAccPortP tDn="uni/infra/accportprof-portselector2"/>
</infraNodeP>
<!--
 PortP contains port selectors. Each port selector contains list of ports. It
       also has association to port group policies
-->
<infraAccPortP name="portselector2">
<infraHPortS name="pselc" type="range">
<infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="37" toPort="38"></infraPortBlk>
<infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-portSet2"/>
</infraHPortS>
</infraAccPortP>
<!--  FuncP contains access bundle group policies  -->
<infraFuncP>
<infraAccPortGrp name="portSet2">
<infraRsQosEgressDppIfPol tnQosDppPolName="infradpp2"/>
</infraAccPortGrp>
</infraFuncP>
</infraInfra>
```

リーフ スイッチに着信するレイヤ3トラフィックをポリシングするには、次の手順を実行します。

```
<!--  api/node/mo/uni/.xml  -->
<fvTenant name="dppTenant">
<qosDppPol name="gmeo" burst="2000" rate="2000"/>
<l3extOut name="Outside">
<l3extInstP name="extroute"/>
<l3extLNodeP name="borderLeaf">
<l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="10.0.0.1">
<ipRouteP ip="0.0.0.0">
<ipNexthopP nhAddr="192.168.62.2"/>
</ipRouteP>
</l3extRsNodeL3OutAtt>
<l3extLIfP name="portProfile">
<l3extRsPathL3OutAtt addr="192.168.40.1/30" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/40]"/>
<l3extRsPathL3OutAtt addr="192.168.41.1/30" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/41]"/>
<l3extRsIngressQosDppPol tnQosDppPolName="gmeo"/>
</l3extLIfP>
</l3extLNodeP>
</l3extOut>
</fvTenant>
```

リーフ スイッチから発信されるレイヤ3トラフィックをポリシングするには、次の手順を実行します。

```
<!--  api/node/mo/uni/.xml  -->
<fvTenant name="dppTenant">
<qosDppPol name="gmeo" burst="2000" rate="2000"/>
<l3extOut name="Outside">
<l3extInstP name="extroute"/>
<l3extLNodeP name="borderLeaf">
<l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="10.0.0.1">
<ipRouteP ip="0.0.0.0">
<ipNexthopP nhAddr="192.168.62.2"/>
</ipRouteP>
</l3extRsNodeL3OutAtt>
<l3extLIfP name="portProfile">
```

```
<l3extRsPathL3OutAtt addr="192.168.40.1/30" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/40]"/>
<l3extRsPathL3OutAtt addr="192.168.41.1/30" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/41]"/>
<l3extRsEgressQosDppPol tnQosDppPolName="gmeo"/>
</l3extLIfP>
</l3extLNodeP>
</l3extOut>
</fvTenant>
```

NX-OS スタイル CLI を使用したデータ プレーン ポリシングの設定

ステップ 1 1 つの EPG を伝送するようにレイヤ 2 ポートを設定します。

例：

```
apic1# conf t
apic1(config)# vlan-domain test
apic1(config-vlan)# vlan 1000-2000
apic1(config-vlan)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# vlan-domain member test
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# tenant test1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# application ap1
apic1(config-tenant-app)# epg e1
apic1(config-tenant-app-epg)# bridge-domain member bd1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# switchport trunk allowed vlan 1001 tenant test1 application ap1 epg e1
apic1(config-leaf-if)# switchport trunk allowed vlan 1501 tenant test1 application ap1 epg e1
# Now the port leaf 101 ethernet 1/10 carries two vlan mapped both to the same Tenant/Application/EPG
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

a) インターフェイスに適用するポリシー マップを作成します。

例：

```
apic1(config)# policy-map type data-plane qosTest
apic1(config-pmap-dpp)# set burst 2400 mega
apic1(config-pmap-dpp)# set cir 70 mega

apic1(config-pmap-dpp)# set sharing-mode shared
apic1(config-pmap-dpp)# exit
apic1(config)# leaf 101
```

```
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# service-policy type data-plane input qosTest
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# policy-map type data-plane qosTest2
apic1(config-pmap-dpp)# set cir 78 mega
apic1(config-pmap-dpp)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# service-policy type data-plane output qosTest2
apic1(config-leaf-if)# end
```

b) 設定されたポリシーを可視化します。

例：

```
apic1# show policy-map type data-plane infra
Type data-plane policy-maps
====================
Global Policy
policy-map type data-plane default
    set burst unspecified
    set conform-cos-transmit unspecified
    set conform-dscp-transmit unspecified
    set conform transmit
    set excessive-burst unspecified
    set exceed-cos-transmit unspecified
    set exceed-dscp-transmit unspecified
    set exceed drop
    set mode byte
    set pir 0
    set cir 78 mega
    set type 1R2C
    set violate-cos-transmit unspecified
    set violate-dscp-transmit unspecified
    set violate drop
Global Policy
policy-map type data-plane qosTest
    set burst 2400 mega
    set cir 78 mega
    set conform-cos-transmit unspecified
    set conform-dscp-transmit unspecified
    set conform transmit
    set excessive-burst unspecified
    set exceed-cos-transmit unspecified
    set exceed-dscp-transmit unspecified
    set exceed drop
    set mode byte
    set pir 0
    set type 1R2C
    set violate-cos-transmit unspecified
    set violate-dscp-transmit unspecified
    set violate drop
Global Policy
policy-map type data-plane qosTest2
    set burst unspecified
    set conform-cos-transmit unspecified
    set conform-dscp-transmit unspecified
    set conform transmit
    set excessive-burst unspecified
    set exceed-cos-transmit unspecified
    set exceed-dscp-transmit unspecified
    set exceed drop
    set mode byte
```

```
    set pir 0
    set cir 78 mega
    set type 1R2C
    set violate-cos-transmit unspecified
    set violate-dscp-transmit unspecified
    set violate drop
```

c) show running-config.

例：

```
apic1# show runn policy-map
# Command: show running-config policy-map
# Time: Fri Jan 29 19:26:18 2016
  policy-map type data-plane default
    exit
  policy-map type data-plane qosTest
    set burst 2400 mega
    set cir 78 mega
    no shutdown
    exit
  policy-map type data-plane qosTest2
    set cir 78 mega
    no shutdown
    exit
apic1# show runn leaf 101
# Command: show running-config leaf 101
# Time: Fri Jan 29 19:26:29 2016
  leaf 101
    interface ethernet 1/10
      vlan-domain member test
      switchport trunk allowed vlan 1501 tenant test1 application ap1 epg e1
      service-policy type data-plane input qosTest
      service-policy type data-plane output qosTest2
      exit
    exit
```

ステップ 2 レイヤ 3 ポートを設定する準備をします。

例：

```
apic1# conf t
apic1(config)# vlan-domain l3ports
apic1(config-vlan)# vlan 3000-3001
apic1(config-vlan)# exit
apic1(config)# tenant l3test1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant l3test1 vrf v1
apic1(config-leaf-vrf)# exit
# Configure a physical Layer 3 port
apic1(config-leaf)# interface ethernet 1/20
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vlan-domain member l3ports
apic1(config-leaf-if)# vrf member tenant l3test1 vrf v1
apic1(config-leaf-if)# ip address 56.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2000::1/64  preferred
apic1(config-leaf-if)# exit
# Configure base interface for L3 subinterfaces
apic1(config-leaf)# interface ethernet 1/21
apic1(config-leaf-if)# vlan-domain member l3ports
apic1(config-leaf-if)# no switchport
```

```
apic1(config-leaf-if)# exit
# Configure a Layer 3 subinterface
apic1(config-leaf)# interface ethernet 1/21.3001
apic1(config-leaf-if)# vrf member tenant l3test1 vrf v1
apic1(config-leaf-if)# ip address 60.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# exit
# Configure a Switched Vlan Interface
apic1(config-leaf)# interface vlan 3000
apic1(config-leaf-if)# vrf member tenant l3test1 vrf v1
apic1(config-leaf-if)# ip address 70.1.1.1/24
apic1(config-leaf-if)# ipv6 address 3000::1/64 preferred
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

a) レイヤ 3 の使用のためにテナントのポリサーを設定します。

例：

```
apic1(config)# tenant l3test1
apic1(config-tenant)# policy-map type data-plane iPol
apic1(config-tenant-pmap-dpp)# set cir 56 mega
apic1(config-tenant-pmap-dpp)# set burst 2000 kilo
apic1(config-tenant-pmap-dpp)# exit
apic1(config-tenant)# policy-map type data-plane ePol
apic1(config-tenant-pmap-dpp)# set burst 2000 kilo
apic1(config-tenant-pmap-dpp)# set cir 56 mega
apic1(config-tenant-pmap-dpp)# exit
apic1(config-tenant)# exit
```

b) レイヤ 3 インターフェイスにポリサーを適用する

例：

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/20
apic1(config-leaf-if)# service-policy type data-plane input iPol
apic1(config-leaf-if)# service-policy type data-plane output ePol
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/21.3001
apic1(config-leaf-if)# service-policy type data-plane input iPol
apic1(config-leaf-if)# service-policy type data-plane output ePol
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface vlan 3000
apic1(config-leaf-if)# service-policy type data-plane input iPol
apic1(config-leaf-if)# service-policy type data-plane output ePol
apic1(config-leaf-if)# end
```

c) レイヤ 3 インターフェイスで使用されるポリサーのコマンドを表示します。

例：

```
apic1# show tenant l3test1 policy-map type data-plane
Type data-plane policy-maps
====================
Policy in Tenant: l3test1
policy-map type data-plane ePol
    set burst 2000 kilo
    set conform-cos-transmit unspecified
    set conform-dscp-transmit unspecified
    set conform transmit
    set excessive-burst unspecified
    set exceed-cos-transmit unspecified
    set exceed-dscp-transmit unspecified
```

```
    set exceed drop
    set mode byte
    set pir 0
    set cir 56 mega
    set type 1R2C
    set violate-cos-transmit unspecified
    set violate-dscp-transmit unspecified
    set violate drop
Policy in Tenant: l3test1
policy-map type data-plane iPol
    set burst 2000 kilo
    set burst unspecified
    set conform-cos-transmit unspecified
    set conform-dscp-transmit unspecified
    set conform transmit
    set excessive-burst unspecified
    set exceed-cos-transmit unspecified
    set exceed-dscp-transmit unspecified
    set exceed drop
    set mode byte
    set pir 0
    set cir 56 mega
    set type 1R2C
    set violate-cos-transmit unspecified
    set violate-dscp-transmit unspecified
    set violate drop
```

d) レイヤ 3 に使用されるポリサーの show running-config です。

例：

```
apic1# show runn tenant l3test1
# Command: show running-config tenant l3test1
# Time: Fri Jan 29 19:48:20 2016
  tenant l3test1
    vrf context v1
      exit
    policy-map type data-plane ePol
      set burst 2000 kilo
      set cir 56 mega
      no shutdown
      exit
    policy-map type data-plane iPol
      set burst 2000 kilo
      set cir 56 mega
      no shutdown
      exit
    exit
apic1# show running-config leaf 102
# Command: show running-config leaf 102
# Time: Fri Jan 29 19:48:33 2016
  leaf 102
    vrf context tenant l3test1 vrf v1
      exit
    interface vlan 3000
      vrf member tenant l3test1 vrf v1
      ip address 70.1.1.1/24
      ipv6 address 3000::1/64 preferred
      bfd ip tenant mode
      bfd ipv6 tenant mode
      service-policy type data-plane input iPol
      service-policy type data-plane output ePol
      exit
    interface ethernet 1/20
      vlan-domain member l3ports
```

```
      no switchport
      vrf member tenant l3test1 vrf v1
      ip address 56.1.1.1/24
      ipv6 address 2000::1/64 preferred
      bfd ip tenant mode
      bfd ipv6 tenant mode
      service-policy type data-plane input iPol
      service-policy type data-plane output ePol
      exit
    interface ethernet 1/21
      vlan-domain member l3ports
      no switchport
      bfd ip tenant mode
      bfd ipv6 tenant mode
      exit
    interface ethernet 1/21.3001
      vrf member tenant l3test1 vrf v1
      ip address 60.1.1.1/24
      ipv6 address 2001::1/64 preferred
      bfd ip tenant mode
      bfd ipv6 tenant mode
      service-policy type data-plane input iPol
      service-policy type data-plane output ePol
    exit
    exit
apic1#
```

エンドポイントのグループ レベルでのデータ プレーン ポリシング

データ プレーン ポリシング（DPP）は、エンドポイント グループ（EPG）に適用できます。トラフィックのポリシングは、EPG が展開されているすべてのリーフ スイッチ上のすべての EPG メンバに適用されます。

3.2(1) より前のリリースでは、EPG メンバーごとに独自のポリサーがありました。3.2(1) 以降のリリースでは、動作はデータプレーンポリサーの共有モードプロパティ（CLI または GUI で構成されている場合）に依存します。それが [**専用（dedicated）**] に設定されている場合、状況は 3.2(1) リリース前と同様です。共有モードが [**共有済み（shared）**] に設定されている場合、同じデータプレーンポリサー ポリシーを使用している同じスライスのすべてのメンバーは、リーフスイッチのハードウェアポリサーを使用します。

たとえば、EPG には次のメンバがあります。

- リーフ 101、Eth1/1、vlan-300
- リーフ 101、Eth1/2、vlan-301
- リーフ 102、Eth1/2、vlan-500

この場合、各メンバーは他のメンバーとは独立して、ポリサーに従ってトラフィックを制限します。データプレーンポリサーで共有モードが [**共有済み（shared）**] に設定されている場合、

上記の同じスライス内のすべてのメンバーは、リーフスイッチで1つのポリサーのみを使用します。

データプレーンポリサーは、共有モードが [**専用（dedicated**）] に設定されている場合、リーフ 101 とリーフ 102 で独立して機能します。次に例を示します。

- ポリサー A（100Mbps ポリシング）は、EPG1（Leaf101 e1/1 vlan-300 、e1/2 vlan-301、およびリーフ 102 e1/2 vlan-500）に適用されます。
- リーフ 101：E1/1 vlan-300 および E1/2 vlan-301（インターフェイスごとに 100Mbps）を介したトラフィックに適用される EPG1 レベルでトラフィックをポリシングします。
- リーフ 102：E1/2 vlan-500（インターフェイスごとにまた 100Mbps）を介したトラフィックに適用される EPG1 レベルでトラフィックをポリシングします。

EPG1 の合計は最大 300Mbps です。

共有モードが [**共有済み（shared**）] に設定されている場合、インターフェイスが同じスライスにある場合、同じポリサーを使用して 100 Mbps が EPG 間で共有されます。次に例を示します。

- EPG1 および EPG2 に適用されるポリサー A（100Mbps ポリシング）。
- リーフ 101：EPG1 と EPG2 のトラフィックの合計をポリシングします。
- リーフ 102：EPG1 と EPG2 のトラフィックの合計をポリシングします。

インターフェイスが同じスライスにある場合、EPG1 と EPG2 の合計は最大 200 Mbps です。

以下は、EPG レベルでのデータ プレーン ポリシングの制限です。

- EPG ポリサー機能は、製品 ID に -EX、-FX、またはそれ以降のサフィックスが付いているスイッチモデルでサポートされます。
- 出力トラフィック ポリシングでは EPG レベル ポリサーはサポートされていません。
- ポリサー モード **Packet-per-second** はサポートされていません。
- ポリサー タイプ 2R3C はEPG ポリサーではサポートされていません。
- **intra-EPG isolation-enforced** が EPG に適用されている場合、ポリサーはサポートされません。
- スケール制限では、ノードごとに 128 EPG ポリサーがサポートできます。

CLI を使用したエンドポイント グループ レベルでのデータ プレーン ポリシングの設定

手順の概要

1. ポリサーの定義：

手順の詳細

ポリサーの定義：

例：

```
apic1# conf t
apic1(config)# vlan-domain test
apic1(config-vlan)# vlan 1000-2000
apic1(config-vlan)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# vlan-domain member test
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# tenant test1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
apic1(config)# policy-map type data-plane pol1
apic1(config-pmap-dpp)# set burst 2400 mega
apic1(config-pmap-dpp)# set cir 78 mega
apic1(config-pmap-dpp)# exit
apic1(config-tenant)# application ap1
apic1(config-tenant-app)# epg e1
apic1(config-tenant-app-epg)# bridge-domain member db1
apic1(config-tenant-app-epg)# service-policy type data-plane poll
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# switchport trunk allowed vlan 1001 tenant test1 application ap1 epg e1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

データ プレーン APIC GUI を使用してエンドポイント グループ レベルでのポリシングの設定

[Tenants] ペインで、**[Tenant_name]** > **[Policies]** > **[Protocol]** > **[Data Plane Policing]** をクリックします。[Data Plane Policing] を右クリックし、 [Create Data Plane Policing Policy] をクリックします。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Administrative State] フィールドで、[enabled] をクリックします。
c) [Policer Mode] の隣にある [Bit Policer] または [Packet Policer] のどちらかのボタンを選択します。
d) **[タイプ（Type）]** の隣で、**[1 Rate 2 Color]** のボタンを選択します。
e) [Conform Action] で 、[Drop]、 [Mark]、または [Transmit] を選択します 。
f) 管理者は、[Conform] と [Violate] フィールドの CoS および DSCP 値を設定できます。

g) [Burst]、[Excessive Burst]、[Rate] フィールドの隣にあるドロップダウン矢印をクリックして、次のいずれかを選択します。

- バイト/パケット
- キロ バイト/パケット
- メガ バイト/パケット
- ギガ バイト/パケット
- ミリ秒
- マイクロ秒

データ プレーンの Rest API を使用したエンドポイント グループ レベルでのポリシングの設定

リーフ スイッチに着信するトラフィックを規制します。

```
<!-- api/node/mo/.xml -->
<polUni>
  <fvTenant  name="t1">

    <qosDppPol name="gmeo" burst="2000" rate="2000"/>
    <fvAp name="ap1">
      <fvAEPg name="ep1">
        <fvRsDppPol tnQosDppPolName="gmeo"/>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

GUI のエンドポイント グループ レベルでデータ プレーン ポリサーの統計情報へのアクセス

EPG レベルの DPP は、EPG メンバ レベルのトラフィックを規制するために使用されます。その結果、統計情報はポリサーが存在するトラフィックをドロップすることを保証する整数です。統計情報は、EPG メンバ レベルで詳細に報告されます。

ステップ 1 **[テナント]** ペインで、**[Tenant_name]** > **[アプリケーション EPG]** > **[EPG メンバ]** > **[スタティック EPG メンバ]** をクリックします。

ステップ 2 ノードを選択します。

ステップ 3 **[統計情報の選択]** をクリックします。

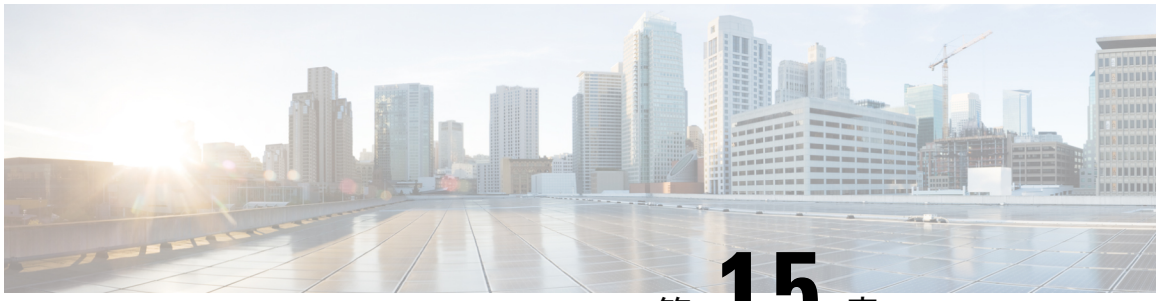
a) **[サンプリング間隔]** 時間単位を選択します。

b) **[利用可能]** ポリサー属性から、矢印を使用して属性を選択します。最大2種類の属性を選択できます。

c) [Submit] をクリックします。

次のタスク

DPP 統計情報がグラフィカル表示されます。



第 15 章

HTTPS アクセス

この章は、次の項で構成されています。

概要

この記事は、Cisco ACI を使用する際の HTTPS アクセスのカスタム証明書を設定する方法の例を示します。

カスタム証明書の設定のガイドライン

- Cisco Application Policy Infrastructure Controller（APIC）で証明書署名要求（CSR）を生成するために使用される秘密キーのエクスポートはサポートされていません。証明書の CSR を生成するために使用された秘密キーを共有することにより、「Subject Alternative Name（SAN）」フィールドのワイルドカード（「* cisco.com」など）を介して複数のサーバで同じ証明書を使用する場合は、秘密キーを Cisco Application Centric Infrastructure（ACI）ファブリックの外部に配置し、Cisco ACI ファブリックにインポートします。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco APIC は、送信された証明書が設定された CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。

- 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
- Cisco APIC で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
- 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキー リングを削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

- Cisco ACI マルチサイト、VCPlugin、VRA、および SCVMM は、証明書ベースの認証ではサポートされません。
- Cisco APIC クラスタごとに 1つのSSL証明書のみが許可されます。
- 以降のリリースからリリース 4.0(1) にダウングレードする前に、証明書ベースの認証を無効にする必要があります。
- 証明書ベースの認証セッションを終了するには、ログアウトして CAC カードを削除する必要があります。
- Cisco APIC に設定されたカスタム証明書は、リーフ スイッチとスパイン スイッチに展開されます。ファブリック ノードに接続するために使用される URL または DN が **[サブジェクト（Subject）]** または **[サブジェクト代替名（Subject Alternative Name）]** フィールド内にある場合、ファブリック ノードは証明書でカバーされます。
- Cisco APIC GUI は、最大サイズが 4k バイトの証明書を受け入れることができます。

SSL 暗号設定を変更する

SSL 暗号は、有効化、無効化、または完全に削除できます。必要な暗号設定に応じて、必要な正確な組み合わせを理解する必要があります。暗号が残らない方法で暗号を無効化および有効化することは設定ミスであり、NGINX の検証に失敗します。

NGINX は OpenSSL 暗号リスト形式を使用します。形式については、OpenSSL Web サイトにアクセスしてください。

Cisco APIC SSL 設定オプションを暗号リスト形式化にマッピングする

暗号を有効にすると、その暗号が NGINX 構成ファイルに書き込まれます。暗号を無効にすると、その暗号が NGINX 構成ファイルに前に感嘆符 (!) を付けて書き込まれます。たとえば、「EEDCH」を無効にすると、「!EEDCH」と書き込まれます。暗号を削除すると、その暗号が NGINX 構成ファイルに暗号がまったく書き込まれなくなります。

（注） OpenSSL 暗号リスト形式のドキュメントには次のように記載されています。「(!) が使用されている場合、暗号はリストから完全に削除されます。削除された暗号は、明示的に指定されていても、リストに再び表示されることはありません」これにより、暗号の「有効」状態に関係なく、「無効」に設定された暗号を参照する組み合わせ暗号が削除される可能性があります。

例：「EEDCH」を無効にし、「EECDH+aRSA+SHA384」を有効にします。これにより、次が NGINX 構成ファイルに書き込まれます：「!EEDCH:EECDH+aRSA+SHA384」。「!EEDCH」は、「EECDH+aRSA+SHA384」が追加されないようにします。これにより、暗号が使用されないことでNGINX検証に失敗するため、NGINXの更新（カスタムHTTPS証明書の適用など）が成功しなくなります。

Cisco APIC SSL 設定を変更する前の暗号リスト形式のテスト

Cisco Application Policy Infrastructure Controller（APIC）に暗号の変更を加える前に、`openssl ciphers -V 'cipher_list'` コマンドを使用して、計画した暗号の組み合わせの結果を検証し、暗号出力が目的の結果と一致することを確認します。

例：

```
apic# openssl ciphers -V 'EECDH+aRSA+SHA256:EECDH+aRSA+SHA384'
         0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(128)
 Mac=SHA256
         0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(256)
 Mac=SHA384
```

テストした暗号リストがエラーまたは「暗号が一致しません」という結果になった場合は、この設定を Cisco APIC に適用しないでください。これを行うと、Cisco APIC GUI にアクセスできなくなったり、カスタム証明書アプリケーションが壊れたりするなど、NGINX の問題が発生する可能性があります。

例：

```
apic# openssl ciphers -V '!EECDH:EECDH+aRSA+SHA256:EECDH+aRSA+SHA384'
Error in cipher list
132809172158128:error:1410D0B9:SSL routines:SSL_CTX_set_cipher_list:no cipher
match:ssl_lib.c:1383:
```

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。ダウンタイムは外部ユーザまたはシステムからの Cisco Application Policy Infrastructure Controller（APIC）APIC クラスタおよびスイッチへのアクセスには影響しますが、Cisco APIC とスイッチの接続には影響しませスイッチ上の NGINX プロセスも影響を受けますが、外部接続のみでファブリックのデータプレーンには影響ありません。Cisco APIC、設定、管理、トラ

ブルシューティングなどへのアクセスは影響を受けることになります。Cisco APIC および スイッチで実行されている NGINX Web サーバーは、この操作中に再起動されます。

始める前に

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

ステップ 1 メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。

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

ステップ 3 **作業**ペインで、**[認証局（Certificate Authorities）]** > **[アクション（Actions）]** > **[認証局の作成（Create Certificate Authority）]** の順に選択します。

ステップ 4 [**認証局の作成（Create Certificate Authority**）] 画面で、[**Name（名前**）] フィールドに、認証局の名前を入力します。

ステップ 5 （オプション）認証局の [**説明（Description**）] を入力します。

ステップ 6 **[証明書チェーン（Certificate Chain）]** フィールドで、Cisco APIC の証明書署名要求（CSR）に署名する認証局の中間証明書とルート証明書をコピーします。

証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

ステップ 7 [**保存（Save**）] をクリックします。

ステップ 8 **作業**ペインで、**[キーリング（Key Rings）]** > **[アクション（Actions）]** > **[キーリングの作成（Create Key Ring）]** の順に選択します。

キー リングを使用すると、秘密キー（外部デバイスからインポートされるか、APIC で内部的に生成される）、秘密キーによって生成される CSR、および CSR によって署名された証明書を管理できます。

ステップ 9 [Create Key Ring] ダイアログボックスで、[Name] フィールドに、名前を入力します。

ステップ 10 （オプション）キーリングの [**説明（Description**）] を入力します。

ステップ 11 [**認証局（Certificate Authority**）] フィールドで、[**認証局の選択（Select Certificate Authority**）] をクリックし、以前に作成した認証局を選択するか、[**認証局の作成（Create Certificate Authority**）] を選択します。

ステップ 12 [**秘密キー（Private Key**）] フィールドで必要なラジオボタンをクリックします。オプションは、[新しいキーの生成（Generate New Key）]、[既存のキーのインポート（Import Existing Key）] です。

ステップ 13 秘密キーを入力します。このオプションは、**秘密キー**の [既存のキーのインポート（Import Existing Key）] オプションを選択した場合にのみ表示されます。

キーリングから Cisco APIC を使用して CSR を生成する場合は、コンテンツを追加しないでください。

署名付き証明書と秘密キーを入力していない場合は、**[作業（Work）]**ペインの**[キー リング（Key Rings）]**領域で、作成されたキー リングの **[管理状態（Admin State）]** に **[開始（Started）]** と表示され、CSR が生成されるのを待ちます。手順 17 に進みます。

署名付き証明書と秘密キーの両方を入力した場合は、**[キーリング（Key Rings）]** 領域に、作成されたキー リングの **[管理状態（Admin State）]** が **[完了（Completed）]** と表示されます。手順 21 に進みます。

（注） キー リングは削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

ステップ 14 キー リングで Cisco APIC を使用して CSR を生成する場合は、**[証明書（Certificate）]** フィールドにコンテンツを追加しないでください。または、Cisco APIC 外の秘密キーおよび CSR を生成して前の手順で CA によって署名されたものがある場合は、署名された証明書の内容を追加します。

ステップ 15 [**モジュラス**（**Modulus**）] フィールドで、ドロップダウンリストから目的のキーの強さを選択します。このオプションは、**秘密キー**に [新しいキーの生成（Generate New Key）] オプションを選択した場合にのみ表示されます。

ステップ 16 [**保存**（**Save**）] ([**キーリングの作成**（**Create Key Ring**）] 画面) をクリックします。

ステップ 17 **作業**ペインで、**[キーリング（Key Rings）]** > ***[キーリング名]***を選択します（または、必要なキーリングの行をダブルクリックします）。

新しい画面に選択したキーリングが表示されます。

ステップ 18 **[証明書要求（Certificate Request）]** ペインで、**[証明書要求の作成（Create Certificate Request）]** をクリックします。

[証明書要求（Certificate Request）] ウィンドウが表示されます。

a) **[サブジェクト（Subject）]** フィールドに、CSR の共通名（CN）を入力します。

ワイルドカードを使用して Cisco APIC の完全修飾ドメイン名（FQDN）を入力できますが、最新の証明書では、通常、識別可能な証明書の名前を入力し、**[代替サブジェクト名（Alternate Subject Name）]** フィールドにすべての Cisco APIC の FQDN を入力することを推奨します（多くの最新のブラウザは SAN フィールドに FQDN を想定しているため、*SAN*（サブジェクト代替名）とも呼ばれます。

b) **[代替サブジェクト名（Alternate Subject Name）]** フィールドに、「DNS：apic1.example.com、DNS：apic2.example.com、DNS：apic3.example.com」や「DNS：* example.com」など、すべての Cisco APIC の FQDN を入力します。 。

c) **[地域（Locality）]** フィールドに、組織の市または町を入力します。

d) **[州（State）]** フィールドに、組織が所在する州を入力します。

e) **[国（Country）]** フィールドに、組織の所在地の国を表す 2 文字の ISO コードを入力します。

f) **[組織名（Organization Name）]** を入力し、**[組織単位名（ Organization Unit Name）]** に単位を入力します。

g) 組織の連絡担当者の **[電子メール（Email）]** アドレスを入力します。

h) **[パスワード（Password）]** に入力し、**[パスワードの確認（Confirm Password）]** フィールドにもう一度入力します。

i) [OK] をクリックします。

ステップ 19 [証明書要求の設定] ペインに、上で入力した情報が表示されます（手順 18）。

ステップ 20 **作業**ペインで、**[キーリング（Key Rings）]** > ***[キーリング名]***を選択します（または、必要なキーリングの行をダブルクリックします）。

新しい画面に選択したキーリングが表示されます。証明書の詳細が表示されます。

（注） CSR がキー リングで示されている認証局によって署名されていない場合、または証明書に MS-DOS 形式の行末が含まれている場合は、エラー メッセージが表示され、証明書は承認されません。MS-DOS 形式の行末を削除します。

キーが確認されて [Work] ペインの [Admin State] が [Completed] に変わり、HTTP ポリシーを使用できるようになります。

ステップ 21 メニュー バーで、**[Fabric]** > **[Fabric Policies]** の順に選択します。

ステップ 22 [Navigation] ペインで、**[Pod Policies]** > **[Policies]** > **[Management Access]** > **[default]** の順に選択します。

ステップ 23 **[作業（Work）]** ペインの **[管理者キーリング（Admin Key Ring）]** ドロップダウン リストで、目的のキー リングを選択します。

ステップ 24 （オプション）証明書ベースの認証では、[Client Certificate TP] ドロップダウン リストで、以前に作成したローカル ユーザ ポリシーを選択し、[Client Certificate Authentication state] の [Enabled] をクリックします。

ステップ 25 [Submit] をクリックします。
すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキー リングが HTTPS アクセスに関連付けられています。

次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キー リングを削除すると、Cisco APIC に内部的に保存されている秘密キーも削除されるため、新しいキー リングの削除または作成は行わないでください。

NX-OS CLI を使用した証明書ベースの認証の有効化

証明書ベースの認証を有効にするには、次の手順を実行します。

例：

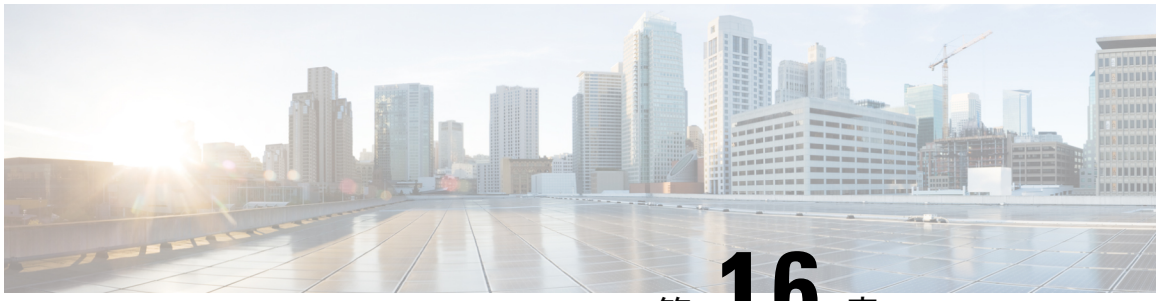
```
To enable CAC for https access:
  configure terminal
   comm-policy default
    https
     client-cert-ca <ca name>
     client-cert-state-enable
 To disable:
```

```
configure terminal
 comm-policy default
  https
   no client-cert-state-enable
   no client-cert-ca
```

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。



第 16 章

その他の ACI セキュリティ機能

この章は、次の項で構成されています。

その他のセキュリティ機能

現在 ACI でサポートされているその他のセキュリティ機能は次のリストのとおりです。それぞれの詳細については、他の構成ガイドで説明されています（https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html）。

- **コントラクト**の設定については、『*Cisco APIC Basic Configuration Guide, Release 3.x*（Cisco APIC 基本設定ガイド リリース 3.x）』および『*Operating Cisco Application Centric Infrastructure*（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の運用）』を参照してください。
- **EPG 通信ルール**については、ナレッジベースの記事『*Use vzAny to Automatically Apply Communication Rules to all EPGs in a VRF*（vzAny を使用して通信ルールを VRF 内のすべての EPG に自動的に適用する ）』を参照してください。
- **インバンドおよびアウトオブバンドの管理アクセス**については、ナレッジベースの記事『*Cisco APIC and Static Management Access*（Cisco APIC と静的管理アクセス）』および『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.2(3)*（Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド、リリース 2.2(3)）』を参照してください。
- **EPG 内での分離適用**については、『*Cisco ACI Virtualization Guide, Release 3.0(1)*（Cisco ACI 仮想化ガイド、リリース 3.0 (1)）』を参照してください。
- **トラフィック ストーム制御**については、『*Cisco APIC Layer 2 Networking Configuration Guide*（Cisco APIC レイヤ 2 ネットワーキング設定ガイド）』を参照してください。

インフラ VLAN トラフィックの制限

ファブリック内のハイパーバイザー間の分離を強化するために、インフラ VLAN トラフィックをインフラ セキュリティ エントリ ポリシーで指定されたネットワーク パスのみに制限できます。この機能を有効にすると、各リーフ スイッチは、コンピューティング ノードからのインフラ VLAN トラフィックを制限して、VXLAN トラフィックのみを許可します。また、スイッチは、リーフ ノードへのトラフィックを制限して、OpFlex、DHCP/ARP/ICMP、および iVXLAN/VXLAN トラフィックのみを許可します。APIC 管理トラフィックは、インフラ VLAN のフロント パネル ポートで許可されます。

この機能は、デフォルトで無効にされています。この機能を有効にするには、次の手順を実行します。

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** を選択します。

ステップ 2 ナビゲーション ペインで **[ファブリック幅設定（Fabric-Wide Settings）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、**[インフラ VLAN トラフィックの制限（Restrict Infra VLAN Traffic）]** のチェックボックスをオンにします。

ステップ 4 [送信（Submit）] をクリックします。

APIC で生成されたセッション ログ ファイルをオフにする

このセクションでは、APIC で生成されたログをオフにする方法について説明します。ファブリックに何らかの監視を設定している場合は、次のログ ファイルが表示されます。

```
Body of session record log example:
From-127.0.0.1-client-type-REST-Success
```

APIC で生成されたセッション ログ ファイルをオフにするには、次の手順を実行します。

ステップ 1 メニュー バーで、**[ADMIN] > [AAA]** を選択します。

ステップ 2 **[AAA]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[ユーザー管理 – セキュリティ（User Management – Security）]** ペインで、デフォルトの **[管理設定（Management Settings）]** ペインが選択されていることを確認します。

ステップ 4 **[セッション レコードに更新を含める（Include Refresh in Session Records）]** フィールドで、チェック ボックスをオフにして、生成されたセッション ログ ファイルを無効にします。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 **[変更の送信（Submit Changes）]** をクリックします。

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