

Cisco 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基本、リリース 5.3(x)

最終更新：2025 年 5 月 16 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/

© 2021– 2023 Cisco Systems, Inc. All rights reserved.



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: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners.

Trademarks

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



目 次

はじめに：

Trademarks iii

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

Cisco Application Centric Infrastructure 5

Cisco Application Centric Infrastructure について 5

Cisco Application Policy Infrastructure Controller について 5

Cisco アプリケーション セントリック インフラストラクチャ ファブリック 6

ファブリックの動作方法を決定する 8

第 3 章

ACI ポリシー モデル 11

ACI ポリシー モデルの概要 11

ポリシー モデルの主な特性 12

論理構造 12

Cisco ACI ポリシー管理情報モデル 13

テナント 15

VRF 16

アプリケーション プロファイル 17

エンドポイント グループ 18

IP ベース EPG 21

マイクロセグメンテーション 21

EPG 内エンドポイント分離 22

ブリッジ ドメインとサブネット 23

ブリッジ ドメイン オプション 26
接続可能エンティティ プロファイル 29
VLAN と EPG 30
アクセス ポリシーによる VLAN から EPG への自動割り当て 30
インターフェイス上のネイティブ 802.1p およびタグ付き EPG 31
ポート単位の VLAN 34
vPC に展開された EPG の VLAN ガイドライン 36
カプセル化によるすべてのプロトコルおよびプロキシ ARP のカプセル化のフラッディングを設定する 37
コントラクト 42
EPG 通信を制御するラベル、フィルタ、エイリアス、および情報カテゴリ 44
コントラクトまたはコントラクトの件名の例外の設定 46
タブー 47
コントラクト継承について 48
契約優先グループについて 49
契約のパフォーマンスの最適化 51
vzAny とは 53
コピー サービスについて 54
外部ネットワーク 55
管理対象オブジェクトの関係とポリシー解決 56
デフォルト ポリシー 57
トランス テナント EPG 通信 59
タグ 60
APIC クォータ管理の構成について 61

第 4 章 ファブリック プロビジョニング 63
ファブリック プロビジョニング 64
スタートアップ検出と構成 64
ファブリック インベントリ 66
プロビジョニング 68
多層アーキテクチャ 68

APIC クラスタの管理 69
クラスタ管理の注意事項 69
Cold Standby について (Cisco APIC クラスタ用) 71
メンテナンス モード 71
ストレッチ ACI ファブリックの設計の概要 73
ストレッチ ACI ファブリック関連ドキュメント 74
ファブリック ポリシーの概要 74
ファブリック ポリシーの構成 75
アクセスポリシーの概要 76
アクセス ポリシーの構成 78
Cisco ACI の仮想ポート チャネル 79
ポートチャネルと仮想ポートチャネル アクセス 81
FEX 仮想ポート チャネル 81
ファイバチャネルおよび FCoE 83
Cisco ACI ファブリックでの Fibre Channel over Ethernet トラフィックのサポート 83
ファイバ チャネル接続の概要 85
802.1Q トンネル 89
ACI 802.1 q トンネルについて 89
ダイナミック ブレイクアウト ポート 91
ブレークアウト ポートの設定 91
ポート プロファイルの設定 92
ポート プロファイルの設定のまとめ 98
ファブリック ポートの障害検出のためのポート トラッキング ポリシー 105
Epg の Q-で-Q カプセル化のマッピング 106
レイヤ 2 マルチキャスト 107
Cisco APIC および IGMP スヌーピングについて 107
ACI ファブリックに IGMP スヌーピングを実装するには 108
仮想化のサポート 110
APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーブ機能 110
APIC IGMP スヌーピング ファンクション キーと IGMPv3 110
Cisco APIC および IGMP スヌーピング クエリア関数 111

ファブリック セキュア モード 112
FAST リンク フェールオーバー ポリシーの構成 112
ポート セキュリティと ACI について 113
ポート セキュリティおよびラーニング動作 113
保護モード 114
ポート レベルでのポート セキュリティ 114
ポート セキュリティに関するガイドラインと制約事項 114
ファースト ホップ セキュリティについて 115
MACsec について 116
データ プレーン ポリシング 117
スケジューラ 118
ファームウェア アップグレード 119
設定ゾーン 122
位置情報 124

第 5 章 ACI ファブリック内での転送 125
ACI ファブリック内の転送について 125
ACI ファブリックは現代のデータ センター トラフィック フローを最適化する 126
ACI で VXLAN 127
サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID 129
ポリシー ID と適用 131
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） 132
アクセス コントロール リストの制限 133
セキュリティ ポリシー仕様を含むコントラクト 134
セキュリティ ポリシーの適用 137
マルチキャストおよび EPG セキュリティ 138
マルチキャスト ツリー トポロジ 138
トラフィック ストーム制御について 140
ストーム制御の注意事項と制約事項 140
ファブリック ロード バランシング 143
エンドポイントの保持 146

IP エンドポイントの学習動作 148
プロキシ ARP について 149
ループ検出 156
Mis-cabling プロトコルのモード 157
MCP 厳格モードのガイドラインおよび制約事項 159
不正なエンドポイントの検出 159
不正なエンドポイントの制御ポリシーについて 159
不正/ COOP 例外リストについて 160
TCP MSS調整について 160

第 6 章 ネットワーキングと管理接続 163
DHCPリレー 163
DNS 166
インバンドおよびアウトオブバンド管理アクセス 166
インバンド管理アクセス 167
アウトオブバンド管理アクセス 168
IPv6 のサポート 170
グローバル ユニキャスト アドレス 171
リンクローカル アドレス 171
スタティック ルート 172
ネイバー探索 173
重複アドレス検出 174
ステートレス アドレス自動設定（SLAAC）および DHCPv6 174
テナント内のルーティング 175
ルート リフレクタの設定 175
共通パーベイシブ ゲートウェイ 176
WAN およびその他の外部ネットワーク 177
ルータ ピアリングおよびルート配布 177
ネットワーク ドメイン 178
外部ネットワークへのブリッジおよびルーテッド接続 178
外部ネットワークへのブリッジ接続用レイヤ 2 Out 179

外部ルータへのブリッジド インターフェイス 179
外部ネットワークへのルーテッド接続のためのレイヤ 3 Out 180
静的ルート プリファレンス 182
ルートのインポートとエクスポート、ルート集約、ルート コミュニティの一致 182
共有サービス契約の使用 186
共有レイヤ 3 Out 188
双方向フォワーディング検出 192
ACI IP SLA 194
テナント ルーテッド マルチキャスト 195
ファブリック インターフェイスについて 196
IPv4/IPv6 テナント ルート マルチキャストの有効化 197
レイヤ 3 IPv4/IPv6 マルチキャストの設定のガイドライン、制約事項、および予想される動作 198
Cisco ACI GOLF 202
ルート ターゲット フィルタリング 203
DCIG への BGP EVPN タイプ 2 のホスト ルートの配信 204
マルチポッド 205
複数ポッドのプロビジョニング 207
マルチポッド QoS および DSCP 変換ポリシー 209
エニーキャストサービスについて 209
リモート リーフ スイッチ 210
ACI ファブリックのリモート リーフ スイッチについて 210
リモート リーフ スイッチの制約事項と制限事項 217
QoS 222
L3Out QoS 222
入力および出力トラフィックのサービスクラス（CoS）プレゼンテーション 222
マルチポッド QoS および DSCP 変換ポリシー 223
QoS マーキングの入力から出力への変換 224
HSRP 224
HSRP について 224
Cisco APIC と HSRP について 226
注意事項と制約事項 226

HSRP のバージョン 228

第 7 章 ACI トランジット ルーティング、ルート ピアリング、および EIGRP サポート 229

ACI 中継ルーティング 229

トランジット ルーティングの使用例 230

ACI ファブリック ルート ピアリング 234

ルートの再配布 234

プロトコルによるルート ピアリング 236

トランジット ルート制御 241

デフォルト ポリシー動作 243

EIGRP プロトコルのサポート 244

L3extOut の構成 246

EIGRP インターフェイス プロファイル 247

第 8 章 ユーザ アクセス、認証およびアカウンティング 249

ユーザ アクセス、認可およびアカウンティング 249

マルチテナントのサポート 250

ユーザ アクセス：ロール、権限、セキュリティ ドメイン 250

アカウンティング 252

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 254

カスタム RBAC 規則 254

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 254

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 255

APIC ローカル ユーザ 255

外部管理されている認証サーバのユーザ 257

Cisco AV ペアの形式 260

RADIUS 認証 261

TACACS+ 認証 262

LDAP/Active Directory の認証 262

APIC Bash シェルのユーザ ID 263

ログイン ドメイン 263

SAML 認証 264

第 9 章 **Virtual Machine Manager のドメイン 267**

Cisco ACI の VM ネットワーキングによる Virtual Machine Manager のサポート 267

VMM ドメイン ポリシー モデル 269

Virtual Machine Manager ドメインの主要コンポーネント 269

Virtual Machine Manager のドメイン 270

VMM ドメイン VLAN プールの関連付け 271

VMM ドメイン EPG の関連付け 272

トランク ポート グループ 274

EPG ポリシーの解決および展開の緊急度 275

VMM ドメインを削除するためのガイドライン 277

第 10 章 **レイヤ 4 ～ レイヤ 7 のサービスの挿入 279**

レイヤ 4 ～ レイヤ 7 のサービスの挿入 279

レイヤ 4 ～ レイヤ 7 のポリシー モデル 280

サービス グラフについて 280

ポリシーベースのリダイレクトについて 282

対称ポリシー ベースのリダイレクトについて 284

自動サービス挿入 285

デバイス パッケージについて 285

デバイス クラスタについて 288

デバイス マネージャとシャーシ マネージャについて 290

具象デバイスについて 293

機能ノードについて 294

機能ノード コネクタについて 294

端末ノードについて 295

権限について 295

サービスの自動化と構成管理 295

サービス リソースのプーリング 296

第 11 章 管理ツール 297

管理ツール 297
管理 GUI について 297
CLI について 298
ユーザ ログインのメニュー オプション 298
GUI および CLI バナーのカスタマイズ 299
REST API 299
REST API について 299
API インスペクタ 301
Visore 管理対象オブジェクト ビューア 301
管理情報モデルのリファレンス 302
MIT 内のオブジェクトの検索 303
ツリーレベルのクエリ 305
オブジェクトレベル クエリ 305
オブジェクトレベル クエリ 306
管理対象オブジェクトのプロパティ 307
REST インターフェイスによるオブジェクト データへのアクセス 308
エクスポート/インポートの構成 309
データベースのシェーディング 309
設定ファイルの暗号化 310
設定のエクスポート 311
インポートの構成 312
テクニカル サポート、統計、コア 314
Puppet を使用したプログラマビリティ 314
Puppet について 314
Cisco ciscoacipuppet パペット モジュール 315
ACI に関する Puppet ガイドラインと制限事項 315

第 12 章 モニタリング 317

障害、エラー、イベント、監査ログ 317

障害 318
ログ レコード オブジェクト 320
ログ レコード オブジェクトについて 320
GUI を使用したログ レコード オブジェクトの表示 321
Errors 322
統計プロパティ、階層、しきい値およびモニタリング 323
統計データについて 324
モニタリング ポリシーの構成 325
Tetration Analytics 329
Cisco Tetration Analytics エージェントのインストールについて 329
NetFlow 329
NetFlow について 329
NetFlow に関するサポートおよび制限事項 330

第 13 章 トラブルシューティング 333
トラブルシューティング 333
ACL 契約の許可および拒否ログについて 334
ARP、ICMP Ping および Traceroute 335
アトミック カウンタ 336
デジタル オプティカル モニタリング（DOM）について 337
ヘルススコア 338
システムおよびポッドの正常性スコア 338
テナントの正常性スコア 341
MO 正常性スコア 341
正常性スコアの集約と影響 343
SPAN の概要 344
SNMP について 345
Syslog について 345
トラブルシューティング ウィザードについて 346
Cisco Nexus 9000 スイッチの安全な消去について 347

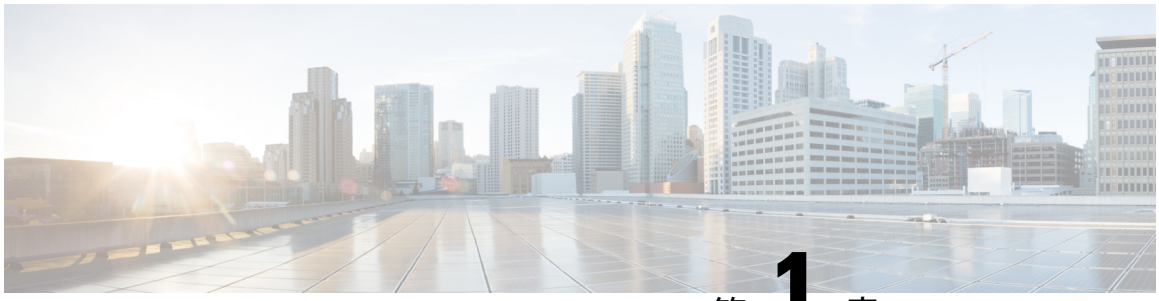
付録 A： ラベルの一致 349
ラベルの一致 349

付録 B： コントラクト範囲の例 351
コントラクト範囲の例 351

付録 C： セキュアプロパティ 355
セキュアプロパティ 355

付録 D： 構成ゾーンでサポートされるポリシー 359
構成ゾーンでサポートされるポリシー 359

付録 E： ACI 用語 363
ACI 用語 363



第 1 章

新機能および変更された機能に関する情報

この章は、次の内容で構成されています。

- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの主な変更点の概要を示したものです。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 *6.1(1)* の新機能および変更された動作

機能または変更	説明	参照先
該当なし	このドキュメントには、以前のリリースからの変更はありません。	なし

表 *2 : Cisco APIC* リリース *6.0(4)* の新機能と変更された動作

機能または変更	説明	参照先
該当なし	このドキュメントには、以前のリリースからの変更はありません。	なし

表 *3 : Cisco APIC* リリース *6.0(3)* の新機能および変更された機能に関する情報

特長	説明	参照先
TCP MSS の調整	伝送制御プロトコル（TCP）の最大セグメント サイズ（MSS）を調整して、パケットのフラグメンテーションやドロップを回避できます。	TCP MSS調整について （160 ページ）

新機能および変更された機能に関する情報

特長	説明	参照先
ブリッジ ドメインと L3Out の不正エンドポイント例外リストのサポート	グローバルな不正/COOP 例外リストを作成できます。このリストは、MACアドレスが見つかったブリッジ ドメイン上の全ての不正エンドポイントコントロールからMACアドレスを除外します。そして、L3Out の 不正 /COOP 例外リストを作成できます。ブリッジドメインまたは L3Out のすべてのMACアドレスを除外することもできます。これにより、すべてのMACアドレスに対して例外を作成する場合に例外リストを簡単に作成できます。各アドレスを個別に入力する必要はありません。	不正/ COOP 例外リストについて （160 ページ）

表 *4 : Cisco APIC* リリース *6.0(2)* の新機能と変更された動作

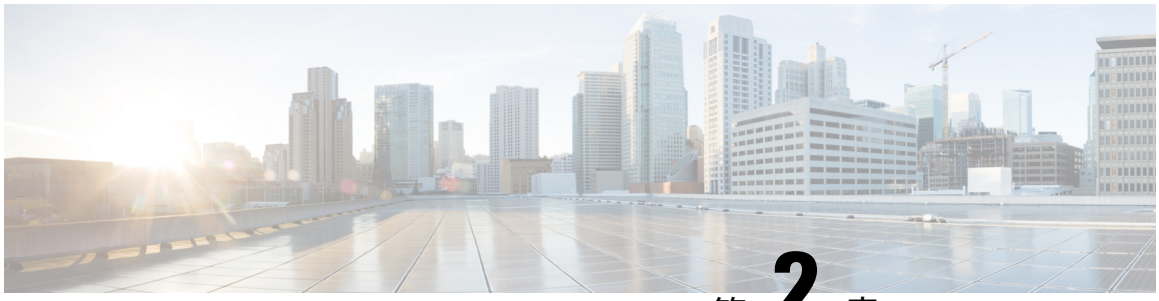
機能または変更	説明	参照先
該当なし	このドキュメントには、以前のリリースからの変更はありません。	なし

新機能および変更された機能に関する情報

表 *5 : Cisco APIC* リリース *6.0(1)* の新機能および変更された機能に関する情報

特長	説明	参照先
Cisco Nexus 9000 スイッチの安全な消去	Cisco Nexus 9000 スイッチは、永続的なストレージを利用して、システム ソフトウェア イメージ、スイッチ構成、ソフトウェア ログ、および動作履歴を維持します。これらの各エリアには、ネットワーク アーキテクチャや設計の詳細など、ユーザ固有の情報と、潜在的な攻撃者からの目標ベクトルが含まれている可能性があります。安全な消去機能を使用すると、この情報を包括的に消去できます。これは、返品許可（RMA）を使用してスイッチを返品するとき、スイッチをアップグレードまたは交換するとき、または寿命に達したシステムを廃止するときに実行できます。	Cisco Nexus 9000 スイッチの安全な消去について （347 ページ）

新機能および変更された機能に関する情報



第 2 章

Cisco Application Centric Infrastructure

この章は、次の内容で構成されています。

- Cisco Application Centric Infrastructure について （5 ページ）
- Cisco Application Policy Infrastructure Controller について （5 ページ）
- Cisco アプリケーション セントリック インフラストラクチャ ファブリック （6 ページ）
- ファブリックの動作方法を決定する （8 ページ）

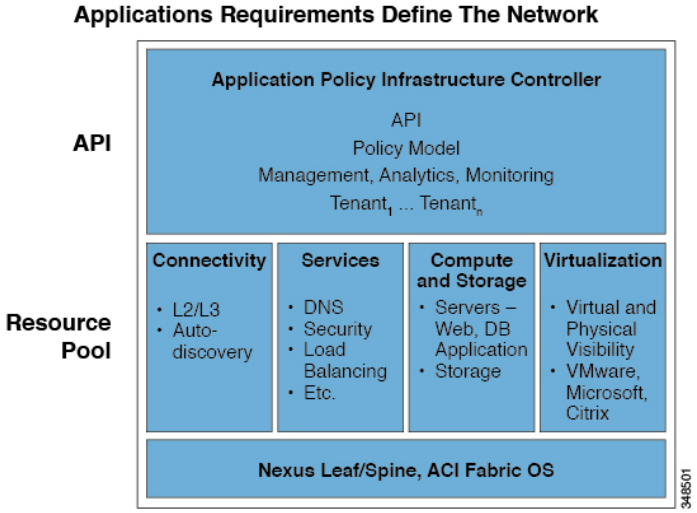
Cisco Application Centric Infrastructure について

Cisco Application Centric Infrastructure（ACI）では、アプリケーションの要件によってネットワークを定義できます。このアーキテクチャにより、アプリケーションの導入ライフサイクル全体がシンプルになって最適化され、短時間で完了します。

Cisco Application Policy Infrastructure Controller について

Cisco Application Policy Infrastructure Controller（APIC）API により、アプリケーションはネットワーク、コンピューティング、およびストレージ機能を含む、安全な共有の高パフォーマンス リソース プールと直接接続することができます。次の図は、APIC の概要について説明します。

図 *1 : APIC* の概要

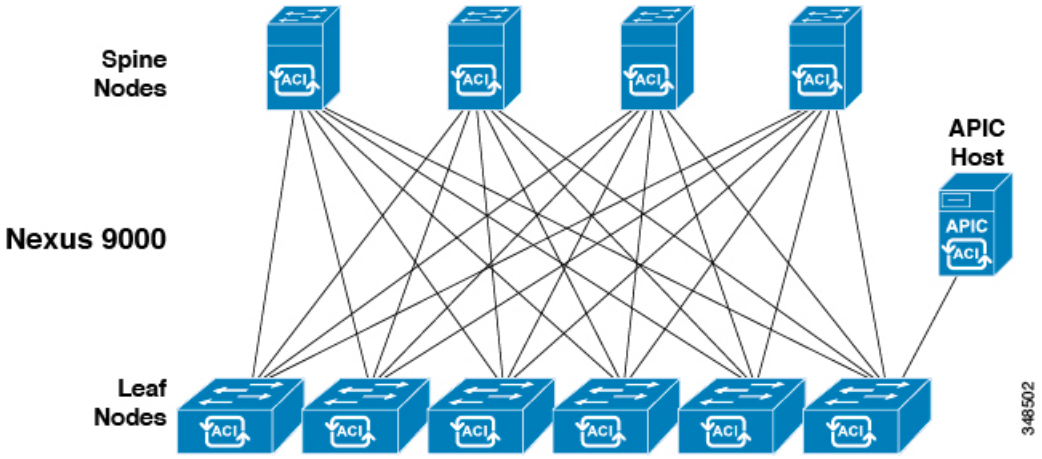


APIC は、拡張性のある ACI のマルチテナント ファブリックを管理します。APIC は、ファブリックの自動化と管理、ポリシープログラミング、アプリケーション展開、およびヘルスモニタリングの統合ポイントを提供します。複製同期されたクラスタ化コントローラとして実装される APIC により、パフォーマンスが最適化され、アプリケーションがあらゆる場所でサポートされ、物理および仮想インフラストラクチャの統合操作が提供されます。APICにより、ネットワーク管理者はアプリケーションの最適なネットワークを容易に定義できます。データセンターのオペレータは、アプリケーションがどのようにネットワーク リソースを消費するかを確認でき、アプリケーションとインフラストラクチャの問題を簡単に切り分けて解決できます。また、リソースの使用パターンをモニタおよびプロファイリングできます。

Cisco アプリケーション セントリック インフラストラクチャ ファブリック

Cisco アプリケーション セントリック インフラストラクチャ ファブリック（ACI）のファブリックには、APIC がリーフ/スパイン ACI のファブリック モードで稼働する Cisco Nexus 9000 シリーズ スイッチが含まれます。これらのスイッチは、各リーフノードをそれぞれのスパインノードに接続することで、「ファットツリー」ネットワークを形成します。他のすべてのデバイスは、リーフノードに接続されます。APIC は、ACI ファブリックを管理します。APIC に対する推奨される最小構成は、3 つの複製されたホストのクラスタです。APIC ファブリック管理機能は、ファブリックのデータ パスでは動作しません。次の図は、リーフ/スパイン ACI ファブリックの概要を示します。

図 *2 : ACI* ファブリックの概要

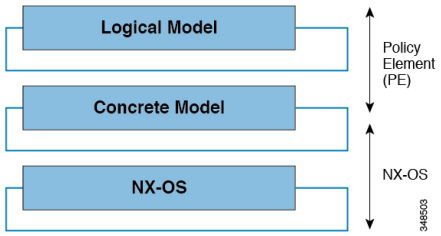


ACI ファブリックは、高帯域幅リンク（40 Gbps および 100 Gbps）全体で一貫した低遅延転送を提供します。同じリーフスイッチ上で送信元と接続先を持つトラフィックはローカルで処理され、他のトラフィックはすべて入力リーフから出力リーフへスパイン スイッチを経由して伝送されます。このアーキテクチャは、物理的な観点から 2 つのホップのように見えますが、ファブリックは単一のレイヤ 3 スイッチとして動作するため、実際には単一のレイヤ 3 ホップとなります。

ACI ファブリック オブジェクト指向のオペレーティング システム（OS）は、Cisco Nexus 9000 シリーズの各ノードで動作します。これにより、システムの構成可能な各要素のオブジェクトのプログラミングが可能になります。

ACI ファブリック OS は、ポリシーを APIC から物理インフラストラクチャで動作する具象モデルにレンダリングします。具象モデルはコンパイルされたソフトウェアに類似していて、スイッチのオペレーティング システムが実行できるモデルの形式です。次の図は、論理モデルと具象モデルおよびスイッチ OS との関係を示します。

図 *3 :* 具象モデルにレンダリングされる論理モデル



すべてのスイッチ ノードには、具象モデルの完全なコピーが含まれます。管理者が APIC で構成を表すポリシーを作成すると、APIC は論理モデルを更新します。次に APIC は、十分に精緻化されたポリシーを作成する中間ステップを実行し、そのポリシーは、具象モデルが更新されるすべてのスイッチ ノードにプッシュされます。

（注） Cisco Nexus 9000 シリーズ スイッチは唯一具象モデルを実行できます。各スイッチには、具象モデルのコピーがあります。APICがオフラインになると、ファブリックは動作し続けますが、ファブリック ポリシーへの変更はできません。

APIC は、ファブリックの有効化、スイッチ ファームウェア管理、ネットワークポリシー構成およびインスタンス化を行います。APICはファブリックに対する一元化されたポリシーとネットワーク管理エンジンとして機能する一方で、転送トポロジを含むデータ パスから完全に削除されます。したがって、ファブリックは APIC との通信が失われてもトラフィックを転送できます。

Cisco Nexus 9000 シリーズ スイッチでは、モジュラ型および固定型の 1、10、40、および 100 ギガビット イーサネット スイッチ構成が提供され、現在の Cisco Nexus スイッチでは Cisco NX-OS スタンドアロン モードとして動作し互換性と一貫性が実現され、ACI モードでは APIC のアプリケーション ポリシーに基づくサービスおよびインフラストラクチャの自動化機能を最大限に活用できます。

ファブリックの動作方法を決定する

ACI ファブリックにより、お客様はクラウド導入に対しスケーラブルで高パフォーマンスのネットワーク、コンピューティングおよびストレージ リソースを自動化し、調整することができます。ACI ファブリックがどのように動作するかを定義するキープレーヤーには次が含まれます。

- IT プランナー、ネットワークエンジニア、およびセキュリティ エンジニア
- APIC API 経由でシステムにアクセスする開発者
- アプリケーションおよびネットワーク管理者

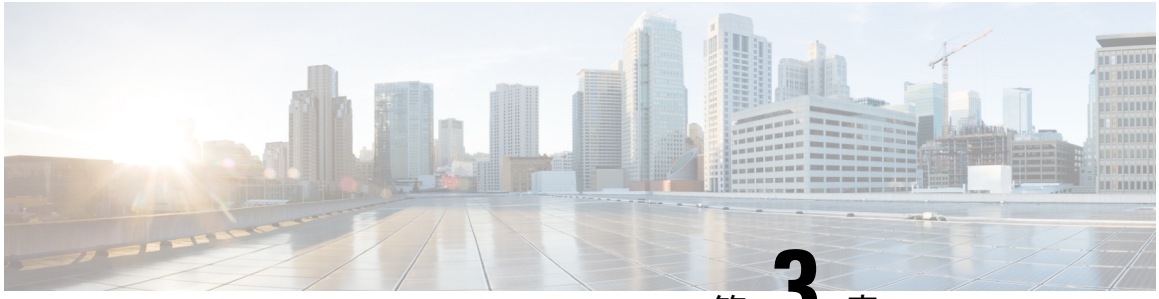
Representational State Transfer（REST）アーキテクチャは、クラウドコンピューティングをサポートする重要な開発手法です。ACI API は、REST ベースです。ワールド ワイド ウェブは、REST アーキテクチャ スタイルに適合するシステムの最大実装を表します。

クラウドコンピューティングは、規模とアプローチの点で従来のコンピューティングとは異なります。従来の環境には、大幅な運用コストを消費する関連するスキル セットとともにソフトウェアおよび保守の要件が含まれます。クラウドアプリケーションは、急激に低下している費用曲線に沿って展開される大規模なインフラストラクチャによってサポートされるシステム設計を使用します。このインフラストラクチャ タイプでは、システム管理者、開発チームおよびネットワーク技術者が協力してより価値のある貢献を行います。

従来の設定では、コンピューティング リソースおよびエンドポイントへのネットワーク アクセスは、仮想LAN（VLAN）またはロードバランサやファイアウォールなどのしっかりと定義されたネットワーク サービス経由でトラフィックを強制するマルチプロトコル ラベル スイッチング（MPLS）などの厳格なオーバーレイを通じて管理されます。APICは、プログラマビリティと中央管理を目的として設計されています。ネットワークを抽象化することで、ACI ファ

ブリック上でオペレータはネットワークのリソースを静的方式の代わりに動的にプロビジョニングできます。その結果、導入までの時間（製品化までの時間）が月単位または週単位から分単位に短縮できます。仮想または物理スイッチ、アダプタ、ポリシー、およびその他のハードウェアおよびソフトウェア コンポーネントの構成変更は、API コールにより数分で行うことができます。

従来の方式からクラウドコンピューティング方式への変換では、データセンターからの柔軟でスケーラブルなサービスへの要求が増大します。これらの変更には、この変換を有効にするためにスキルの高いスペシャリストの大規模プールが要求されます。APIC は、プログラマビリティと中央管理を目的として設計されています。APIC の主な機能は、REST と呼ばれる Web API です。APIC REST API は JavaScript オブジェクトの表記（JSON）または Extensible Markup Language（XML）のマニュアルを含む HTTP または HTTPS メッセージを受け入れて返します。現在、多くの Web デベロッパーが RESTful 方式を使用しています。ネットワーク全体で Web API を採用することで、企業はサービスを容易に開発し他の内部または外部のプロバイダーと組み合わせることができます。このプロセスにより、ネットワークは提供時に静的なリソースの複雑な組み合わせからサービスの動的な交換に変換されます。



第 3 章

ACI ポリシー モデル

この章は、次の内容で構成されています。

- ACI ポリシー モデルの概要 （11 ページ）
- ポリシー モデルの主な特性 （12 ページ）
- 論理構造 （12 ページ）
- Cisco ACI ポリシー管理情報モデル （13 ページ）
- テナント （15 ページ）
- VRF （16 ページ）
- アプリケーション プロファイル （17 ページ）
- エンドポイント グループ （18 ページ）
- ブリッジ ドメインとサブネット （23 ページ）
- 接続可能エンティティ プロファイル （29 ページ）
- VLAN と EPG （30 ページ）
- コントラクト （42 ページ）
- 外部ネットワーク （55 ページ）
- 管理対象オブジェクトの関係とポリシー解決 （56 ページ）
- デフォルト ポリシー （57 ページ）
- トランス テナント EPG 通信 （59 ページ）
- タグ （60 ページ）
- APIC クォータ管理の構成について （61 ページ）

ACI ポリシー モデルの概要

ACI ポリシー モデルにより、アプリケーション要件のポリシーの指定を有効化します。APIC は、ファブリック インフラストラクチャにポリシーを自動的にレンダリングします。ユーザまたはプロセスがファブリック内のオブジェクトへの管理上の変更を開始すると、APIC は最初にポリシー モデルにその変更を適用します。このポリシー モデルの変更により、実際の管理対象エンドポイントへの変更がトリガーされます。この方法を、モデル方式フレームワークといいます。

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

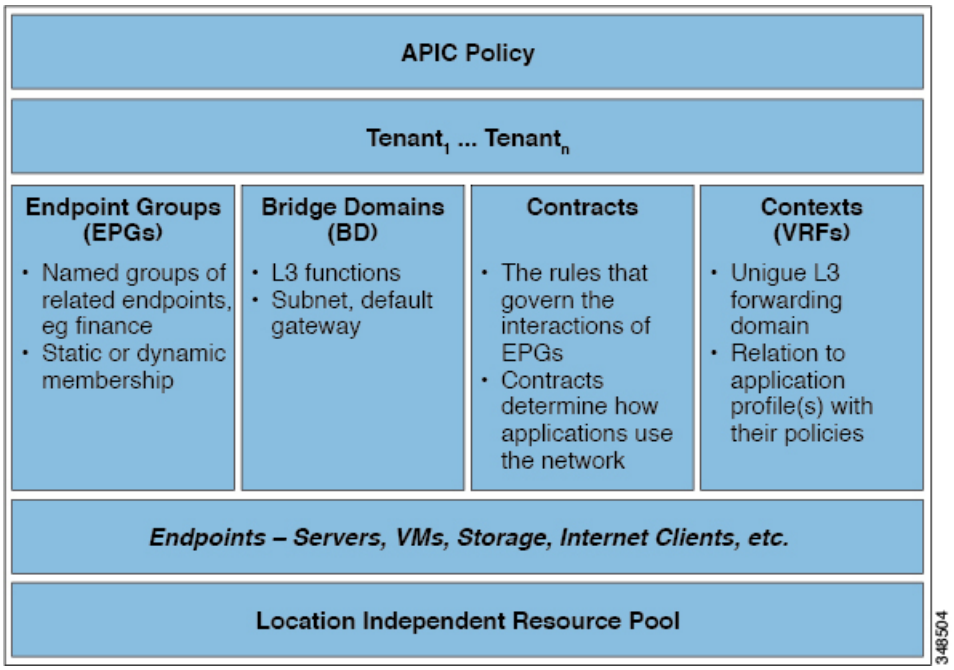
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはファブリック、サービス、システム動作、およびネットワークに接続された仮想および物理デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な構成は、使用可能なリソースに関連するポリシーを適用することで具体的な構成にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、APIC ポリシー モデルの変更の副作用として明示的に構成されます。具象エンティティは、（仮想マシンまたはVLANなど）物理的にすることができますが、そうする必要はありません。
- システムは、新しいデバイスを含めるようにポリシーモデルが更新されるまで、新たに接続されたデバイスとの通信を禁止します。
- ネットワーク管理者は、論理的および物理的なシステムリソースを直接構成しませんが、システム動作のさまざまな面を制御する（ハードウェアに依存しない）論理的な構成とAPIC ポリシーを定義します。

モデル内の管理対象オブジェクトを操作することで、エンジニアは独立した個々のコンポーネントの構成を管理することから開放されます。これらの特性により、自動化と柔軟なワークロードのプロビジョニングが可能になり、インフラストラクチャ内のワークロードをどこでも検索できるようになります。ネットワーク接続されたサービスは簡単に展開でき、APIC により自動化フレームワークが提供され、それらのネットワーク接続されたサービスのライフサイクルを管理できます。

論理構造

ポリシーモデルは、インフラストラクチャ、認証、セキュリティ、サービス、アプリケーション、診断など、ファブリック全体を管理します。ポリシーモデルの論理構造は、ファブリックの機能のニーズをファブリックがどのように満たすかを定義します。次の図は、ACIポリシーモデルの論理構造の概要を示します。

図 *4 : ACI* ポリシー モデルの論理構造の概要



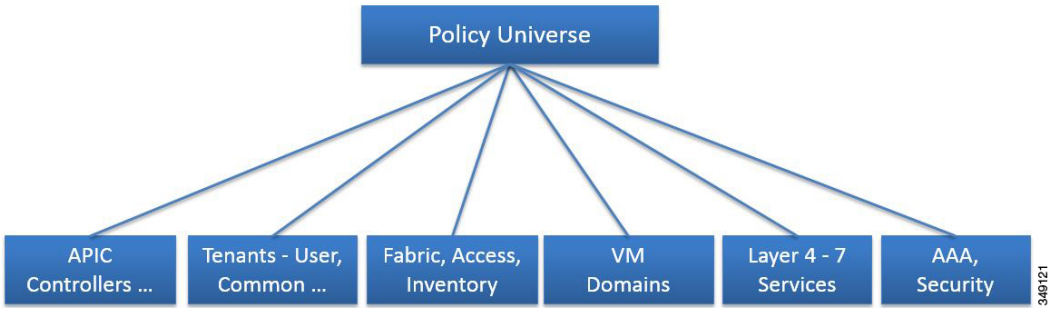
ファブリック全体またはテナントの管理者は、アプリケーションまたは共有リソースの要件を含む事前定義されたポリシーを作成します。これらのポリシーは、アプリケーション、ネットワーク接続サービス、セキュリティ ポリシー、およびテナント サブネットのプロビジョニングを自動化し、管理者をインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソース プールにアプローチするポジションにします。アプリケーションは、ネットワーキングの動作を誘導する必要があり、その逆ではありません。

Cisco ACI ポリシー管理情報モデル

ファブリックは、階層型管理情報ツリー（MIT）で表示できる管理情報モデル（MIM）に記録される物理および論理コンポーネントから構成されます。情報モデルは、APIC で実行するプロセスによって保存され管理されます。OSI 共通管理情報プロトコル（CMIP）および他の X.500 バリアントと同様に、APIC によって、MIT の階層構造内のオブジェクトの場所に応じて継承できるオブジェクトのプロパティとして管理可能な特性を示すことにより、管理対象リソースの制御が可能になります。

ツリーの各ノードは、管理対象オブジェクト（MO）またはオブジェクトのグループを表します。MO はファブリック リソースの抽象化です。MO は、スイッチ、アダプターなどの具象オブジェクト、またはアプリケーション プロファイル、エンドポイント グループ、または障害などの論理オブジェクトを表すことができます。次の図は、MIT の概要について説明します。

図 *5 : Cisco ACI* ポリシー管理情報モデルの概要



階層構造は、最上位（ルート）でポリシー ユニバースから始まり、親と子ノードが含まれます。ツリー内の各ノードはMOで、ファブリック内の各オブジェクトには、オブジェクトを説明しツリー内の場所を検索する一意な識別名（DN）があります。

次の管理対象オブジェクトには、システムの動作を管理するポリシーが含まれます。

- APIC コントローラは、マルチテナント ファブリックの管理、ポリシー プログラミング、アプリケーション展開、およびヘルスモニタリングを提供する複製同期されたクラスタ化コントローラを構成します。
- テナントはポリシーのコンテナで、管理者はドメインベースのアクセス制御を実行できます。システムにより、次の 4 種類のテナントが提供されます。
  - ユーザ テナントは、ユーザのニーズに応じて管理者によって定義されます。アプリケーション、データベース、Web サーバ、ネットワークアタッチド ストレージ、仮想マシンなどのリソースの動作を管理するポリシーが含まれます。
  - 共通テナントは、システムによって提供されますが、ファブリックの管理者が構成できます。ファイアウォール、ロードバランサ、レイヤ4～レイヤ7サービス、侵入検知アプライアンスなど、すべてのテナントにアクセス可能なリソースの動作を管理するポリシーが含まれます。
  - インフラストラクチャテナントは、システムによって提供されますが、ファブリックの管理者が構成できます。ファブリック VXLAN オーバーレイなどのインフラストラクチャ リソースの動作を管理するポリシーが含まれます。また、ファブリック プロバイダーはリソースを1つ以上のユーザテナントに選択的に展開できます。インフラストラクチャ テナント ポリシーは、ファブリックの管理者が構成できます。
  - 管理テナントは、システムによって提供されますが、ファブリックの管理者が構成できます。ファブリック ノードのインバンドおよびアウトオブバンドの構成に使用するファブリック管理機能の動作を管理するポリシーが含まれます。管理テナントには、スイッチの管理ポートを介したアクセスを提供するファブリック データ パスの外部にある APIC/fabric 内部通信用のプライベートなアウトオブバウンド アドレス空間が含まれます。管理テナントにより、仮想マシン コントローラとの通信の検出と自動化が可能になります。
- アクセスポリシーは、ストレージ、コンピューティング、レイヤ2およびレイヤ3（ブリッジおよびルーテッド）接続、仮想マシン ハイパーバイザ、レイヤ 4 ～ レイヤ 7 のデバイ

スなどのリソースへの接続を提供するスイッチ アクセス ポートの動作を管理します。テナントが Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control Protocol（LACP）、またはスパニングツリーなどのデフォルトのリンクで提供される構成以外のインターフェイス構成を必要とする場合、管理者はアクセスポリシーを構成して、リーフスイッチのアクセス ポートでそのような構成を有効にする必要があります。

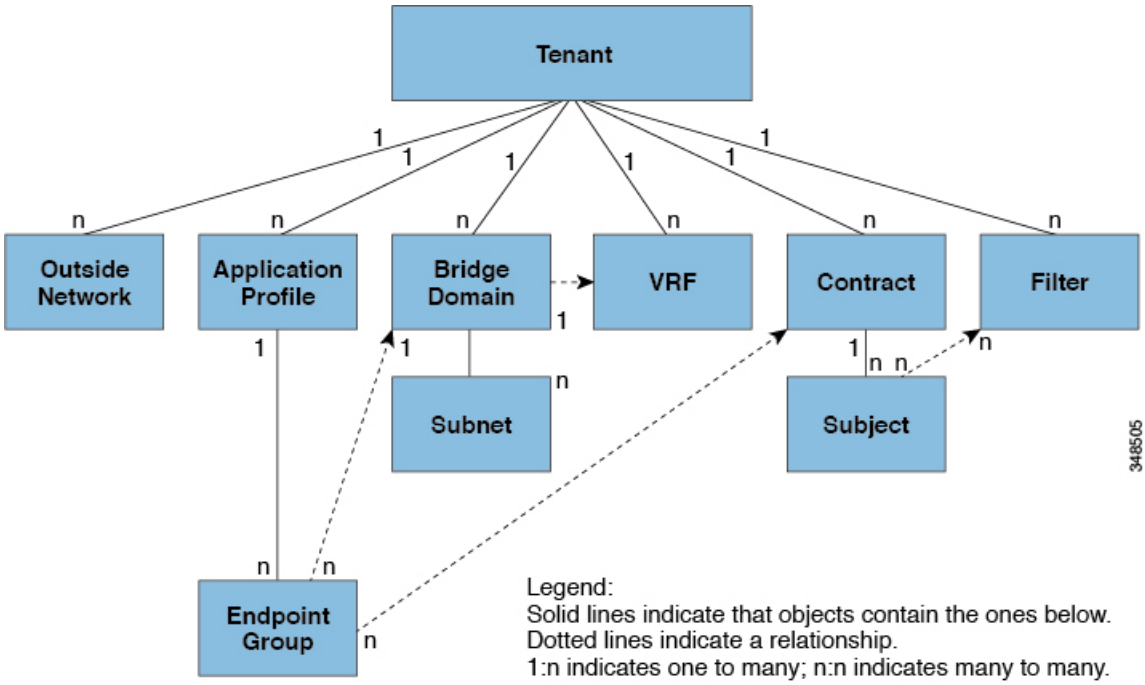
- ファブリック ポリシーは、Network Time Protocol（NTP）のサーバー同期、Intermediate System-to-Intermediate System Protocol（IS-IS）、ボーダーゲートウェイ プロトコル（BGP）のルート リフレクタ、ドメインネームシステム（DNS）などの機能を含む、スイッチ ファブリック ポートの動作を管理します。ファブリック MO には、電源、ファン、シャーシなどのオブジェクトが含まれます。
- 仮想マシン（VM）ドメインは、同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。VM コントローラは、VLAN または Virtual Extensible Local Area Network（VXLAN）のエリアおよびアプリケーション エンドポイント グループ（EPG）を共有できます。APIC はコントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワーク構成を公開します。
- レイヤ 4 ～ レイヤ 7 のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムはダイナミックに応答することができます。ポリシーは、サービス デバイス パッケージとインベントリ管理機能を提供します。
- アクセス、認証、およびアカウンティング（AAA）ポリシーは、Cisco ACI ファブリックのユーザ権限、ロール、およびセキュリティ ドメインを管理します。

階層型ポリシー モデルは、REST API インターフェイスとうまく適合します。呼び出されると、API は MIT 内のオブジェクトで読み取りまたは書き込みを行います。URL は、MIT 内のオブジェクトを識別する識別名に直接マッピングします。MIT 内のデータは、XML または JSON でエンコードされた自己完結型の構造化ツリー テキスト ドキュメントとして説明できます。

テナント

テナント (`fvTenant`) は、アプリケーション ポリシーの論理コンテナで、管理者はドメインベースのアクセス コントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。次の図は、管理情報ツリー (MIT) のテナント部分の概要を示します。

図 *6:* テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントに含まれる主要な要素は、フィルタ、コントラクト、外部ネットワーク、ブリッジ ドメイン、仮想ルーティングおよび転送 (VRF) インスタンス、エンドポイント グループ (EPG) を含むアプリケーション プロファイルです。テナントのエンティティはそのポリシーを継承します。VRF はコンテキストとも呼ばれ、それぞれを複数のブリッジ ドメインに関連付けることができます。

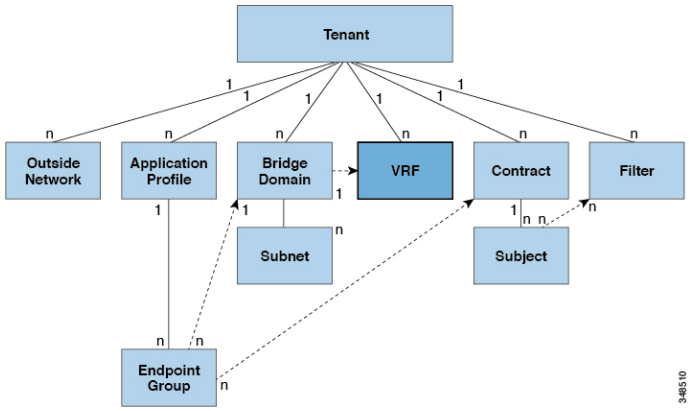
（注） APIC GUI のテナント ナビゲーション パスでは、VRF (コンテキスト) はプライベート ネットワークと呼ばれます。

テナントはアプリケーション ポリシーの論理コンテナです。ファブリックには複数のテナントを含めることができます。レイヤ 4 ～ 7 のサービスを展開する前に、テナントを設定する必要があります。ACI ファブリックは、テナント ネットワークに対して IPv4、IPv6、およびデュアル スタック構成をサポートします。

VRF

仮想ルーティングおよび転送（VRF）オブジェクト（`fvCtx`）またはコンテキストは、テナント ネットワーク（ APIC GUI のプライベート ネットワーク）と呼ばれます。テナントには、複数の VRF を含めることができます。VRF は、一意のレイヤ 3 フォワーディングおよびアプリケーション ポリシー ドメインです。次の図は、管理情報ツリー（MIT）内の VRF の場所とテナントの他のオブジェクトとの関係を示します。

図 *7 : VRF*



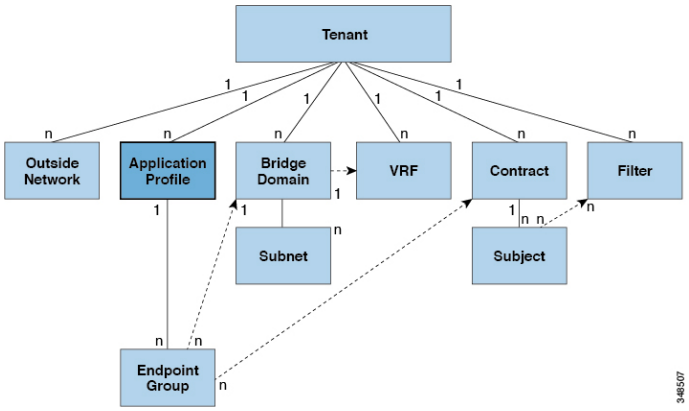
VRF は、レイヤ 3 のアドレス ドメインを定義します。VRF には 1 つ以上のブリッジ ドメインが関連付けられます。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイス クラスタの選択基準ポリシーを提供する論理デバイスの VRF を作成できます。論理デバイスは、コントラクト名、グラフ名、またはグラフ内の関数ノード名に基づいて選択できます。

（注） APIC GUI では、VRF（`fvCtx`）は「コンテキスト」または「プライベートネットワーク」とも呼ばれます。

アプリケーション プロファイル

アプリケーション プロファイル（`fvAp`）は、ポリシー、サービス、およびエンドポイント グループ（EPG）間の関係を定義します。次の図は、管理情報ツリー（MIT）内のアプリケーション プロファイルの場所と、テナント内の他のオブジェクトとの関係を示します。

図 *8:* アプリケーション プロファイル



アプリケーション プロファイルには、1 つ以上の EPG が含まれます。最新のアプリケーションには、複数のコンポーネントが含まれます。たとえば、e-コマース アプリケーションには、Web サーバ、データベース サーバ、ストレージ エリア ネットワーク内にあるデータ、および金融取引を可能にする外部リソースへのアクセスが必要となる場合があります。アプリケーションプロファイルには、アプリケーションの機能の提供に論理的に関連する必要な数の（またはそれ以下の）EPG が含まれます。

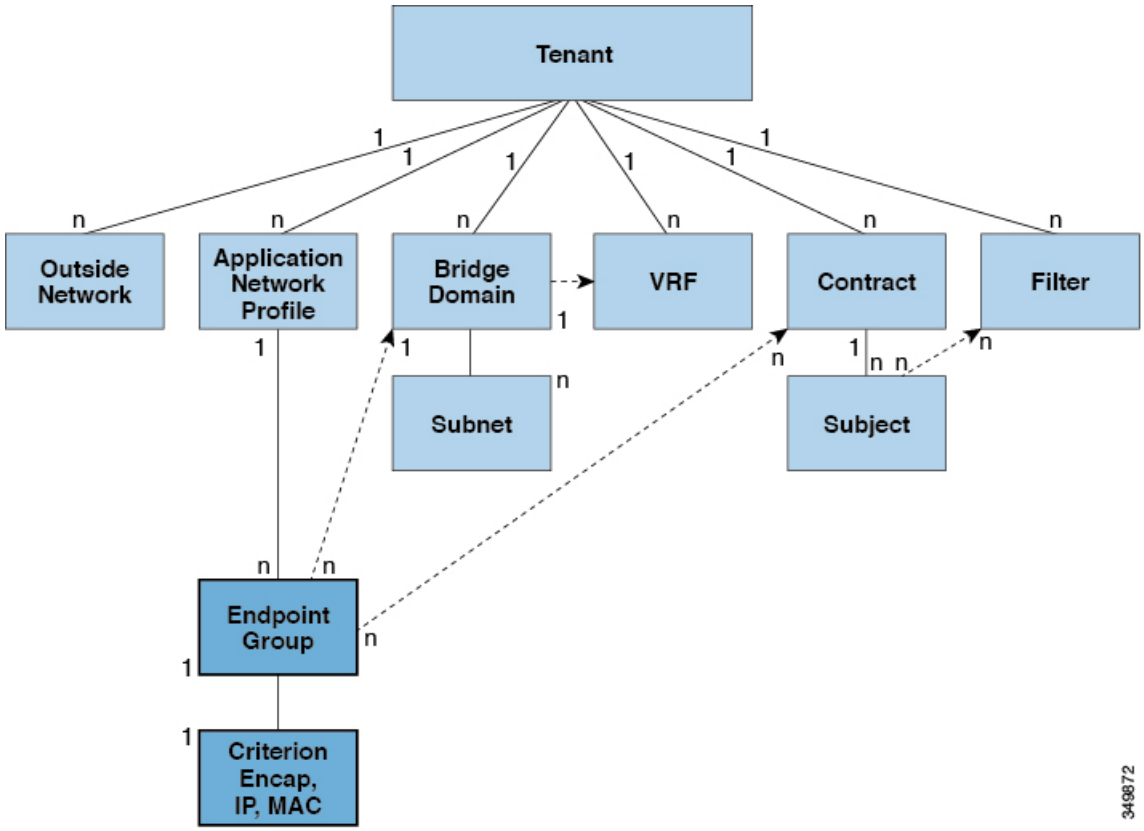
EPG は次のいずれかに従って組織化できます。

- 提供するアプリケーション（DNS サーバや SAP アプリケーションなど）（『*Cisco APIC REST API Configuration Guide*』の「*Tenant Policy Example*」を参照）。
- 提供する機能（インフラストラクチャなど）
- データセンターの構造内の場所（DMZ など）
- ファブリックまたはテナントの管理者が使用することを選択した組織化の原則

エンドポイント グループ

エンドポイント グループ（EPG）は、ポリシー モデルの最も重要なオブジェクトです。次の図は、管理情報ツリー（MIT）内のアプリケーション EPG の場所とテナント内の他のオブジェクトとの関係を示します。

図 *9 :* エンドポイント グループ



EPGは、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントには、アドレス（ID）、ロケーション、属性（バージョンやパッチ レベルなど）があり、物理または仮想にできます。エンドポイントのアドレスを知ることで、他のすべてのID の詳細にアクセスすることもできます。EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ネットワーク接続ストレージ、またはクライアントが含まれます。EPG 内のエンドポイント メンバシップは、ダイナミックまたはスタティックにできます。

ACI ファブリックには、次のタイプの EPG を含めることができます。

- アプリケーション エンドポイント グループ（`fvAEPg`）
- レイヤ 2 外部外側ネットワーク インスタンスのエンドポイント グループ（`l2extInstP`）
- レイヤ 3 外部外側ネットワーク インスタンスのエンドポイント グループ（`l3extInstP`）
- アウトオブバンド（`mgmtOoB`）またはインバンド（`mgmtInB`）アクセス用の管理エンドポイント グループ。

EPGには、セキュリティ、仮想マシンのモビリティ（VMM）、QoS、レイヤ4～レイヤ7サービスなどの共通のポリシー要件を持つエンドポイントが含まれます。エンドポイントは個別に設定および管理されるのではなく、EPG 内に配置され、グループとして管理されます。

ポリシーは EPG に適用されます。個々のエンドポイントに適用されることは絶対にありません。EPG は、APIC において管理者により静的に設定されるか、vCenter または OpenStack などの自動システムによって動的に設定されます。



（注） EPG がスタティック バインディング パスを使用する場合、この EPG に関連付けられるカプセル化 VLAN はスタティック VLAN プールの一部である必要があります。IPv4/IPv6 デュアルスタック設定の場合、IP アドレスのプロパティは `fvStCEp` MO の `fvStIp` 子プロパティに含まれます。IPv4 および IPv6 アドレスをサポートする複数の `fvStIp` を 1 つの `fvStCEp` オブジェクト下に追加できます。ACI を、IPv4 のみのファームウェアから、IPv6 をサポートするバージョンのファームウェアにアップグレードすると、既存の IP プロパティが `fvStIp` MO にコピーされます。

EPG の設定内容にかかわらず、含まれるエンドポイントに EPG ポリシーが適用されます。

ファブリックへの WAN ルータ接続は、スタティック EPG を使用する設定の 1 つの例です。ファブリックへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む `l3extInstP` EPG を管理者が設定します。ファブリックは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通して EPG のエンドポイントについて学習します。エンドポイントを学習すると、ファブリックは、それに基づいて `l3extInstP` EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション（`fvAEPg`）EPG 内でサーバとの TCP セッションを開始すると、`l3extInstP` EPG は、`fvAEPg` EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、そのエンドポイントはもうファブリック内に存在しません。



（注） リーフ スイッチが EPG 下の *static binding (leaf switches)* 用に設定されている場合は、次の制限が適用されます。

- スタティック バインディングをスタティック パスで上書きすることはできません。
- そのスイッチのインターフェイスをルーテッド外部ネットワーク（L3out）設定に使用することはできません。
- そのスイッチのインターフェイスに IP アドレスを割り当てることはできません。

VMware vCenter への仮想マシン管理接続は、ダイナミック EPG を使用する設定の 1 つの例です。ファブリックで仮想マシン管理ドメインが設定されると、vCenter は、必要に応じて仮想マシン エンドポイントを開始、移動、シャットダウンさせることのできる EPG の動的設定をトリガーします。

IP ベース EPG

カプセル化ベースの EPG が一般的に使用されますが、IP ベース EPG は、最長プレフィックス一致（LPM）分類ではサポートできない多数の EPG が必要なネットワークに適しています。IP ベース EPG では、LPM 分類とは異なり、EPG ごとにネットワーク/マスク範囲を割り当てる必要はありません。また、IP ベース EPG ごとに一意のブリッジドメインは必要ありません。IP ベースの EPG の構成手順は、Cisco AVS vCenter 構成で使用される仮想 IP ベースの EPG を構成する手順に似ています。

次に示す IP ベース EPG のガイドラインおよび制限事項に従ってください。

- IP ベース EPG は、APIC 1.1(2x) および ACI スイッチ 11.1(2x) リリース以降、次の Cisco Nexus N9K スイッチでサポートされています。
  - スイッチ名の末尾に「E」が付いているスイッチ（N9K-C9372PX-E など）。
  - スイッチ名の末尾に「EX」が付いているスイッチ（N9K-93108TC-EX など）。

  IP ベース EPG をサポートしていない古いスイッチに展開しようとすると、APIC で障害が発生します。
- IP ベース EPG は、特定の IP アドレスまたはサブネットに対して構成できますが、IP アドレスの範囲には構成できません。
- IP ベース EPG は、次のシナリオではサポートされていません。
  - 静的 EP 構成と組み合わせて使用します。
  - 外部のインフラストラクチャテナント（インフラ）構成はブロックされませんが、この場合はレイヤ 3 学習がないため、有効になりません。
  - レイヤ 2 のみのブリッジドメインでは、ルーティングされたトラフィックがないため、IP ベースの EPG は有効になりません。レイヤ 3 ブリッジドメインでプロキシ ARP が有効になっている場合、エンドポイントが同じサブネットにある場合でも、トラフィックはルーティングされます。したがって、この場合は IP ベース EPG が機能します。
  - 共有サービスと IP ベース EPG の両方に使用されるプレフィックスを持つ構成。

マイクロセグメンテーション

マイクロセグメンテーションでは、仮想マシンの属性、IP アドレス、または MAC アドレスに従って、複数の EPG のエンドポイントが、マイクロセグメント化された EPG に関連付けられます。仮想マシン属性には、VNic ドメイン名、VM 識別子、VM 名、ハイパーバイザ識別子、VMM ドメイン、データセンター、オペレーティングシステム、またはカスタム属性が含まれます。

マイクロセグメンテーションには、次のような利点があります。

- ライン レートを適用するステートレス ホワイト リスト ネットワーク アクセスセキュリティ。
- マイクロセグメントごとの粒度セキュリティ自動化により、ダイナミック レイヤー 4 ～ レイヤー 7 サービスの挿入と連鎖が可能。
- 幅広い仮想スイッチ環境でのハイパーバイザに依存しないマイクロセグメンテーション。
- 問題のある VM を検疫セキュリティ ゾーンに簡単に移動させる ACI ポリシー。
- ベアメタルおよび VM エンドポイントの EPG 内分離と組み合わせると、マイクロセグメンテーションは、アプリケーション階層内でポリシー駆動型の自動化された完全なエンドポイント分離を提供できます。

どの EPG についても、ACI ファブリック入力リーフスイッチは、入力ポートに関連付けられたポリシーに従って、パケットを EPG に分類します。マイクロセグメント化された EPG は、マイクロセグメント化された EPG ポリシーで指定された VM 属性、MAC アドレス、または IP アドレスに基づいて派生した個々の仮想または物理エンドポイントにポリシーを適用します。

EPG 内エンドポイント分離

EPG内エンドポイント分離ポリシーにより、仮想エンドポイントまたは物理エンドポイントが完全に分離されます。分離を適用した状態で稼働している EPG 内のエンドポイント間の通信は許可されません。分離を適用した EGP では、多くのクライアントが共通サービスにアクセスするときに必要な EPG カプセル化の数は低減しますが、相互間の通信は許可されません。

EPG の分離は、すべての Cisco Application Centric Infrastructure（ACI）ネットワーク ドメインに適用されるか、どれにも適用されないかの、どちらかになります。Cisco ACI ファブリックは接続エンドポイントに直接分離を実装しますが、ファブリックに接続されているスイッチはプライマリ VLAN（PVLAN）タグに従って分離規則を認識します。



（注） EPG 内エンドポイント分離を適用して EPG を設定した場合は、次の制限が適用されます。

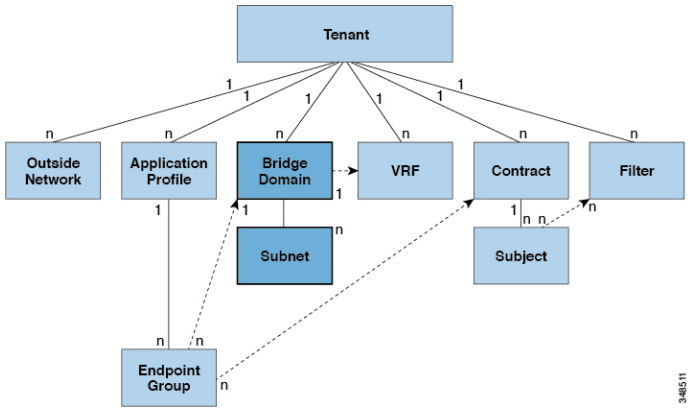
- 分離を適用した EPG 全体のすべてのレイヤ 2 エンドポイント通信がブリッジ ドメイン内にドロップされます。
- 分離を適用した EPG 全体のすべてのレイヤ 3 エンドポイント通信が同じサブネット内にドロップされます。
- トラフィックが、分離が適用されている EPG から分離が適用されていない EPG に流れている場合、QoS CoS の優先順位設定の保持はサポートされません。

BPDU は、EPG 内分離が有効になっている EPG を介して転送されません。したがって、Cisco ACI 上の独立した EPG にマッピングされている VLAN でスパニング ツリーを実行する外部レイヤ 2 ネットワークを接続すると、Cisco ACI は外部ネットワークのスパニング ツリーがレイヤ 2 ループを検出できなくなる可能性があります。この問題を回避するには、これらの VLAN 内の Cisco ACI と外部ネットワーク間に単一の論理リンクのみを設定します。

ブリッジ ドメインとサブネット

ブリッジ ドメイン（fvBD）は、ファブリック内のレイヤ 2 フォワーディングの構造を表します。次の図は、管理情報ツリー（MIT）内のブリッジ ドメインの場所とテナントの他のオブジェクトとの関係を示します。

図 *10* : ブリッジ ドメイン



ブリッジ ドメインは、VRF インスタンス（コンテキストまたはプライベート ネットワークとも呼ばれる）にリンクする必要があります。レイヤ 2 VLAN を除いて、少なくとも 1 つのサブネット（fvSubnet）が関連付けられている必要があります。フラッディングが有効な場合、ブリッジ ドメインは、一意のレイヤ 2 MAC アドレス空間とレイヤ 2 フラッド ドメインを定義します。VRF インスタンスが一意の IP アドレス空間を定義する一方で、そのアドレス空間は複数のサブネットで構成できます。これらのサブネットは、対応する VRF インスタンスを参照する 1 つ以上のブリッジ ドメインで定義されます。

ブリッジ ドメインまたは EPG の下のサブネットのオプションは次のとおりです。

- パブリック（*Public*）：サブネットをルーテッド接続にエクスポートできます。
- プライベート（*Private*）：サブネットはテナント内にのみ適用されます。
- 共有（*Shared*）：共有サービスの一部として、同じテナントまたは他のテナントにわたる複数の VRF インスタンスに対してサブネットの共有やエクスポートを行うことができます。共有サービスの例としては、異なるテナントの別の VRF インスタンスに存在する EPG へのルーテッド接続などがあります。これにより、トラフィックが VRF インスタンス間で双方向に移動することが可能になります。共有サービスを提供する EPG は、その EPG の下で（ブリッジ ドメインの下ではなく）サブネットを設定する必要があり、そのスコープは外部にアドバタイズするように設定し、VRF インスタンス間で共有する必要があります。

（注） 共有サブネットは、通信に含まれるVRFインスタンス全体で一意でなければなりません。EPG 下のサブネットがレイヤ 3 外部ネットワーク共有サービスを提供する場合、このようなサブネットは、Cisco Application Centric Infrastructure（ACI）ファブリック内全体でグローバルに一意である必要があります。

ブリッジ ドメイン パケットの動作は次の方法で制御できます。

パケット タイプ	モード
ARP	**ARP フラッディング**は有効または無効にできます。フラッディングを行わない場合、ARP パケットはユニキャストで送信されます。 （注） `limitIpLearnToSubnets` を `fvBD` で設定すると、ブリッジドメインの構成済みサブネット内または共有サービス プロバイダーである EPG サブネット内にIPアドレスが存在する場合のみ、エンドポイントの学習がブリッジドメインに限定されます。
未知のユニキャスト	**L2 Unknown Unicast** は、**Flood** または **Hardware Proxy** になり得ます。 （注） ブリッジ ドメインが **L2 Unknown Unicast** を持っており、それが **Flood** に設定されている場合、エンドポイントが削除されると、システムはそれを両方のローカル リーフ スイッチから削除します。そして、**Clear Remote MAC Entries** を選択すると、ブリッジドメインが展開されているリモートのリーフスイッチからも削除されます。この機能を使用しない場合、リモートリーフは、タイマーが時間切れになるまで、学習したこのエンドポイントの情報を保持します。 **L2 Unknown Unicast** の設定を変更すると、このブリッジドメインに関連付けられたEPGにアタッチされているデバイスのインターフェイス上で、トラフィックがバウンスします(アップ ダウンします)。

パケット タイプ	モード
未知の IP マルチキャスト	**L3 の不明なマルチキャスト フラッディング** **フラッド（Flood）**：パケットは入力および境界リーフ スイッチ ノードでのみフラッディングされます。N9K-93180YC-EX では、パケットは、ブリッジ ドメインが導入されているすべてのノードでフラッディングされます。 **最適化（Optimized）**：1 リーフあたり 50 のブリッジ ドメインのみサポートされます。この制限は N9K-93180YC-EX には該当しません。
L2 マルチキャスト、ブロードキャスト、ユニキャスト	**マルチ宛先フラッディング**、次のいずれかになり得ます。 • **BD でフラッド（Flood in BD）**：ブリッジ ドメインにフラッドします。 • **カプセル化でフラッド（Flood in Encapsulation）**：カプセル化でフラッドします。 • **ドロップ（Drop）**：パケットをドロップします。

（注） Cisco APIC リリース 3.1(1) 以降では、Cisco Nexus 9000 シリーズ スイッチで (EX と FX で終わる名前を持つものとそれ以降)、次のプロトコルのカプセル化のフラッディングまたはブリッジ ドメインにフラッディングが可能です：OSPF/OSPFv3、BGP、EIGRP、LACP、ISIS、IGMP、PIM、ST-BPDU、ARP/GARP、RARP、および ND。

ブリッジ ドメインは複数のスイッチにまたがることができます。ブリッジ ドメインには複数のサブネットを含めることができますが、サブネットは単一のブリッジ ドメイン内に含まれます。ブリッジ ドメイン（fvBD）の `limitIPLearnToSubnets` プロパティが `yes` に設定されていると、ブリッジ ドメインの設定済みサブネットのいずれかの中に IP アドレスがあるとき、または EPG が共有サービス プロバイダーである場合には EPG サブネット内に IP アドレスがあるときのみ、ブリッジ ドメイン内でエンドポイントの学習が行われます。サブネットは複数の EPG にまたがることができ、1 つ以上の EPG を 1 つのブリッジ ドメインまたはサブネットに関連付けることができます。ハードウェアのプロキシ モードでは、異なるブリッジ ドメインのエンドポイントがレイヤ 3 のルックアップ動作の一部として学習されると、そのエンドポイントに ARP トラフィックが転送されます。

ブリッジ ドメイン オプション

ブリッジ ドメインは、不明なユニキャスト フレームのフラッド モードで、またはこれらのフレームのフラッディングを排除する最適化されたモードで動作するように設定できます。フラッディング モードで使用する場合、レイヤ 2 の不明なユニキャスト トラフィックはブリッジ ドメイン（GIP）のマルチキャスト ツリーでフラッディングされます。最適化されたモードでブリッジ ドメインを動作するようにするには、ハードウェア プロキシに設定する必要があります。この状況では、レイヤ 2 の不明なユニキャスト フレームはスパイン プロキシ エニーキャスト VTEP アドレスに送信されます。

⚠

注意 不明なユニキャスト フラッディング モードから hw プロキシ モードに変更すると、ブリッジ ドメイン内のトラフィックが停止します。

ブリッジ ドメインで IP ルーティングが有効になっている場合、マッピング データベースは、MAC アドレスだけでなく、エンドポイントの IP アドレスを学習します。

レイヤ 3 の設定 ブリッジ ドメイン ()] パネルのタブには次のパラメータを設定するには、管理者が使用できます。

- **ユニキャスト ルーティング** ：この設定が有効になっているサブネット アドレスが設定されている場合は、ファブリックはデフォルト ゲートウェイの機能を提供して、トラフィックをルーティングします。ユニキャストルーティングを有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与された IP アドレスと VTEP の対応関係を学習します。IP学習は、ブリッジドメイン内にサブネットが構成されているかどうかに左右されません。
- **サブネット アドレス** ：このオプションは、ブリッジ ドメインの SVI IP アドレス (デフォルト ゲートウェイ) を設定します。
- **制限のサブネット IP ラーニング** ：このオプションは、ユニキャスト リバース転送パス チェックに似ています。このオプションを選択すると、ファブリックはブリッジ ドメインに設定されている 1 以外のサブネットから IP アドレスを学習されません。

⚠

注意 有効化 **サブネットに制限 IP ラーニング** がブリッジ ドメイン内のトラフィックを停止します。

拡張 L2 専用モード：レガシーモード

Cisco Application Centric Infrastructure（ACI）では、VLAN が異なるリーフ ノードに展開されている限り、任意の目的で同じ VLAN ID を再利用できます。これにより、Cisco ACI ファブリックは、ファブリックとしての VLAN の理論上の最大数、4094 を超えることができます。ただし、これを実現するため、および基盤となる VxLAN 実装の複雑さを隠すために、個々のリーフノードに含めることのできる VLAN の数は少なくなります。このことは、リーフノードあたりの VLAN の密度が必要な場合に問題の原因となる可能性があります。このようなシナリオでは、ブリッジ ドメインで以前はレガシーモードと呼ばれていた、拡張 L2 専用モードを有効

にできます。拡張 L2 専用モードのブリッジドメインでは、リーフノードごとに多数の VLAN を使用できます。ただし、このようなブリッジ ドメインにはいくつかの制限があります。

拡張 L2 専用モードとそれ以外のモードで、リーフ ノードごとにサポートされる VLAN またはブリッジ ドメインの数については、ご使用のリリースの Verified Scalability Guideを参照してください。

拡張 L2 専用モードの制限事項

レガシー モードまたは拡張 L2 専用モードの制限は次のとおりです。

- ブリッジ ドメインには、1 つの EPG と 1 つの VLAN のみを含めることができます。
- ユニキャスト ルーティングはサポートされていません。
- コントラクトはサポートされていません。
- VMM 統合のダイナミック VLAN 割り当てはサポートされていません。
- サービス グラフはサポートされていません。
- QoS ポリシーはサポートされていません。
- ブリッジ ドメインは、スタンドアロン Cisco NX-OS では基本的に VLAN として動作します。

拡張 L2 専用モードの設定

次に、拡張 L2 専用 モードでブリッジ ドメインを設定する際の考慮事項を示します。

- VLAN ID はブリッジドメインで設定されます。
- EPG で設定された VLAN ID は上書きされます。
- 既存のブリッジ ドメインで拡張 L2 専用モードの有効と無効を切り替えると、サービスに影響します。

  VLAN ID が変更前に使用されていたものと異なる場合、Cisco Application Policy Infrastructure Controller（APIC）は自動的にブリッジ ドメインの展開解除と再展開を行います。

  モード変更の前後で同じ VLAN ID が使用された場合、Cisco APIC はブリッジ ドメインの自動的な展開解除と再展開は行いません。手動でブリッジ ドメインを展開解除して再展開する必要があります。これは、 EPG で静的ポート設定を削除して再作成することで実行できます。

- 拡張 L2 専用モードの VLAN ID を変更する場合は、まずモードを無効にしてから、新しい VLAN ID で拡張 L2 専用モードを有効にする必要があります。

ブリッジ ドメインごとの IP 学習の無効化

ブリッジ ドメインの IP データプレーン学習は無効にできます。MAC 学習は引き続きハードウェアで行われますが、IP 学習は ARP/GARP/ND プロセスからのみ行われます。この機能は、

Cisco APIC 3.1 リリースで主にサービス グラフ ポリシーベース リダイレクト（PBR）展開用に導入されましたが、VRF インスタンスごと（Cisco APIC リリース 4.0）ブリッジ ドメインサブネットごと、（Cisco APIC リリース 5.2）、および EPG ごと（Cisco APIC リリース 5.2）に IP データプレーン学習を無効にする機能に置き換えられました。ブリッジ ドメインごとに IP ラーニングを無効にすることは推奨されません。また、PBR で使用する場合を除き、サポートされません。

ブリッジ ドメインごとに IP 学習を無効化するには、次の注意事項と制限事項を参照してください。

- リモート リーフ スイッチで送信元 IP アドレスが S,G 情報を入力するように学習していないため、レイヤ 3 マルチキャストはサポートされていません。
- DL ビットが iVXLAN ヘッダーで設定されているため、MAC アドレスはリモート リーフ スイッチのデータ パスから学習されません。そのため、ブリッジ ドメインが展開されているファブリックで、リモート リーフ スイッチからすべてのリーフ スイッチに、不明なユニキャスト トラフィックがフラッディングされることになります。エンドポイント データプレーン学習が無効になっている場合は、この状況への対策として、プロキシモードでブリッジ ドメインを構成することをお勧めします。
- ARP がフラッド モードであり、GARP ベースの検出を有効にする必要があります。
- IP 学習を無効にすると、対応する VRF インスタンスでレイヤ 3 エンドポイントがフラッシュされません。同じリーフ スイッチを恒久的に指すエンドポイントになる可能性があります。この問題を解決するには、すべてのリーフ スイッチで、 この VRF 内のすべてのリモート IP エンドポイントをフラッシュします。

ブリッジ ドメインの構成を変更して、データプレーン学習を無効にしても、以前にローカルに学習したエンドポイントはフラッシュされません。これにより、既存のトラフィック フロー中断の影響は限られます。Cisco ACI リーフ スイッチが特定の送信元 MAC を持つトラフィックをエンド ポイント保持ポリシーよりも長く見ない場合、MAC が学習したエンドポイントは通常どおりエージングします。

（注） IP データプレーン学習を無効にすると、トラフィック転送の結果としてエンドポイントの IP 情報が更新されることはなくなりますが、Cisco ACI は ARP/ND を使用してエンドポイント IP 情報を更新できます。つまり、ローカルエンドポイントのエージング（設定変更前に学習されたか、設定変更後に学習されたか）は、通常のエージングとは若干異なり、[システム (System)] > [システム設定 (System Settings)] > [エンドポイント制御 (Endpoint Controls)] > [IPエージング (IP Aging)] にも依存します。

IP エージングが無効の場合、すでに学習されたエンドポイント MAC と一致する送信元 MAC からのトラフィックは、エンドポイントテーブルの MAC アドレス情報を更新し、その結果、IP 情報も更新します（これは IP データプレーンの学習が有効になっている場合と同じです）。

IP エージングが有効の場合、Cisco ACI はエンドポイント IP アドレスを個別にエージング アウトします（これは IP データプレーン学習が有効になっている場合と同じです）が、すでに学習したエンドポイントとマッチする既知の送信元 MAC および IP からのトラフィックにより、エンドポイントテーブルの MAC アドレス情報は更新されるのに対し、IP 情報は更新されないという点で、IP データプレーン学習を有効にした構成とは異なります。

接続可能エンティティ プロファイル

ACI ファブリックにより、リーフ ポートを通してベア メタル サーバ、仮想サーバ、ハイパーバイザ、レイヤ 2 スイッチ（たとえば、Cisco UCS ファブリック インターコネクト）、またはレイヤ 3 ルータ（たとえば、Cisco Nexus 7000 シリーズ スイッチ）などのさまざまな外部エンティティに接続する複数の接続ポイントが提供されます。これらの接続ポイントは、リーフ スイッチ上の物理ポート、FEX ポート、ポート チャネル、またはバーチャル ポート チャネル（vPC）にすることができます。

（注） 2 つのリーフ スイッチ間での VPC ドメインを作成するとき、同じスイッチの生成を次のいずれかのどちらのスイッチも必要があります。

- 1: なしで Cisco Nexus N9K スイッチの生成」EX」または「FX」、スイッチ名前末尾にたとえば、N9K 9312TX
- 2: Cisco Nexus N9K スイッチ間での生成」EX」または「FX」スイッチ モデルの名前の末尾にたとえば、N9K-93108TC-EX

スイッチなど、これらの 2 つが互換性のある VPC ピアではありません。代わりに、同じ世代のスイッチを使用します。

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control

Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。カプセル化ブロック（および関連 VLAN）は、リーフ スイッチで再利用可能です。AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

次の AEP の要件と依存関係は、さまざまな設定シナリオ（ネットワーク接続、VMM ドメイン、マルチポッド設定など）でも考慮する必要があります。

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN プールを定義しないと、EPG がプロビジョニングされても VLAN はリーフ ポートでイネーブルになりません。
- リーフ ポートで静的にバインディングしている EPG イベントに基づいて、または VMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからの VM イベントに基づいて、特定の VLAN がリーフ ポート上でプロビジョニングされるかイネーブルになります。
- 添付されているエンティティ プロファイルに関連付けられているすべてのポートに関連付けられているアプリケーション Epg を導入するアプリケーション Epg に直接と関連付けることができますプロファイルのエンティティが添付されています。AEP では、アタッチ可能なエンティティ プロファイルに関連付けられているセレクタの一部であるすべてのインターフェイスで導入されている EPG (infraRsFuncToEpg) との関係が含まれている設定可能な一般的な機能 (infraGeneric) があります。

Virtual Machine Manager（VMM）ドメインは、AEP のインターフェイス ポリシー グループから物理インターフェイス ポリシーを自動的に取得します。

AEP のオーバーライド ポリシーを VMM ドメイン用の別の物理インターフェイス ポリシーを指定するために使用できます。このポリシーは、VM コントローラが中間レイヤ 2 ノードを介してリーフ スイッチに接続され、異なるポリシーがリーフ スイッチおよび VM コントローラの物理ポートで要求される場合に役立ちます。たとえば、リーフ スイッチとレイヤ 2 ノード間で LACP を設定できます。同時に、AEP オーバーライド ポリシーで LACP をディセーブルにすることで、VM コントローラとレイヤ 2 スイッチ間の LACP をディセーブルにできます。

VLAN と EPG

アクセス ポリシーによる VLAN から EPG への自動割り当て

テナント ネットワーク ポリシーがファブリックのアクセス ポリシーと別に設定される一方で、テナント ポリシーの基盤となるアクセス ポリシーが整わないとテナント ポリシーはアクティブ化されません。ファブリック アクセス外向きインターフェイスは、仮想マシン コントローラなどの外部デバイス、ハイパーバイザ、ホスト、ルータ、またはファブリック エクステンダ (FEX) と接続します。アクセス ポリシーにより、管理者はポート チャネルおよび仮想ポート

チャネル、LLDP、CDP、LACP などのプロトコル、モニタリングや診断などの機能を設定することができます。

図 *11* : アクセス ポリシーとエンドポイント グループの関連付け



ポリシー モデルでは、vlan の Epg 緊密に結合されています。トラフィックが流れるようにするには、物理、VMM、L2out、L3out、またはファイバ チャネル ドメイン内に VLAN を持つリーフ ポートに EPG を展開する必要があります。詳細については、ネットワーク ドメイン（178 ページ）を参照してください。

ポリシー モデルでは、EPG に関連付けられているドメイン プロファイルには、VLAN インスタンス プロファイルが含まれています。ドメイン プロファイルには、両方の VLAN インスタンス プロファイル (VLAN プール) および attacheable アクセス エンティティ プロファイル (AEP) アプリケーション Epg に直接と関連付けられているが含まれています。AEP は、すべてのポートの [接続されている、および Vlan の割り当てのタスクを自動化するに関連付けられているアプリケーション Epg を展開します。大規模なデータセンター数千の Vlan の数百のプロビジョニング仮想マシンのアクティブなは簡単に、中に ACI ファブリックは VLAN プールから、VLAN Id を自動的に割り当てることができます。これは、膨大な従来データセンターで Vlan をトランキングと比較して、時間を節約できます。

VLAN の注意事項

EPG トラフィックがフローは、Vlan の設定には次のガイドラインを使用します。

- 複数のドメインは、VLAN プールを共有できますが、1 つのドメインは、1 つの VLAN プールにのみ使用できます。
- 1 つのリーフ スイッチで同じ VLAN のカプセル化を複数の Epg を展開するを参照してください。 ポート単位の VLAN （34 ページ） 。

インターフェイス上のネイティブ 802.1p およびタグ付き EPG

アクセス（802.1p またはタグなし）モードを割り当てるときは、次のガイドラインに従って、タグなしまたは 802.1p パケットを必要とするデバイスが ACI リーフスイッチのアクセス ポートに接続されたときに想定通りに動作するようにします。

これらのガイドラインは、単一のリーフスイッチのポートに展開された EPG に適用されます。EPG が異なるスイッチに展開されている場合、これらの制限は適用されません。

- APIC GUI では、ポートの VLAN を EPG に割り当てるときに、**[トランク（Trunk）]**、**[アクセス（802.1p）（Access（802.1p））]**、または **アクセス（タグなし）（Access（Untagged））]** のいずれかの VLAN モードを割り当てることができます。
- 1 つのポートで許可される 802.1p VLAN またはタグなし VLAN は 1 つだけです。どちらか一方の場合もありますが、両方の場合はありません。

- 第 1 世代スイッチの場合、リーフスイッチのいずれかのポートに展開された EPG がアクセス（タグなし）モードで構成されている場合、EPG によって使用されるすべてのポートは、同じリーフスイッチとその VPC ピア（存在する場合）でタグ付けされていない必要があります。 第 2 世代スイッチ（-EX、-FX、または -FX2 サフィックス付き）では、タグなしポートとタグ付きポートを組み合わせて使用できます。
- **[アクセス（タグなし）（Access（Untagged））]** モードのポートに展開された EPG を使用して、同じポートの **[トランク（Trunk）]** モードで（タグ付き）VLAN 番号を使用して異なる EPG を展開できます。

リーフスイッチ ポートが **[アクセス（802.1p）（Access（802.1p））]** または **[アクセス（タグなし）（Access（Untagged））]** モードとして構成されている単一の EPG に関連付けられている場合、スイッチに応じて、トラフィック処理にいくつかの違いがあります。

第 1 世代スイッチ

- ポートが **アクセス（802.1p）** モードで構成されている場合：
  - 出力時に、アクセス VLAN がポートに展開された唯一の VLAN である場合、トラフィックはタグ付けされません。
  - 出力で、ポートにタグなしの EPG とともに展開された他の（タグ付き）VLAN がある場合、その EPG からのトラフィックはタグ付きゼロです。
  - 出力では、ポートに構成されている 1 つ以上の VLAN タグに関係なく、すべての FEX ポートのトラフィックはタグ付けされていません。
  - ポートは、タグなし、タグ付き、または 802.1p モードの入力トラフィックを受け入れます。
- ポートが **アクセス（タグなし）** モードで構成されている場合：
  - 出力では、EPG からのトラフィックはタグなしです。
  - ポートは、タグなし、タグ付き、または 802.1p の入力トラフィックを受け入れます。

第 2 世代スイッチ

第 2 世代以降のスイッチは、**[アクセス（タグなし）（Access（Untagged））]** モードと **[アクセス（802.1p）（Access（802.1p））]** モードを区別しません。EPG がタグなしまたは 802.1p モードで構成された第 2 世代ポートに展開されている場合：

- 出力では、トラフィックはこれが展開されているノードで常にタグなしです。
- ポートは、タグなし、タグ付き、または 802.1p モードの入力トラフィックを受け入れます。

ポートでの VLAN モードの組み合わせ：3.2(3i) 以前の Cisco APIC リリースを実行する第 1 世代および第 2 世代のハードウェア

1 つの EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	異なるポートの EPG 1 では、次の VLAN モードが許可されます。
トランク	トランクまたは 802.1p
タグなし	タグなし
802.1p	トランクまたは 802.1p

複数の EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	ポート 2 の EPG 1 では、次のモードが許可されます。	ポート 1 の EPG 2 では、次のモードが許可されます。
タグなし	タグなし	トランク
802.1p	トランクまたは 802.1p	トランク
トランク	802.1p またはトランク	トランクまたは 802.1p またはタグなし

ポートでの VLAN モードの組み合わせ：Cisco APIC リリース 3.2(3i) 以降を実行する第 2 世代ハードウェア

1 つの EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	異なるポートの EPG 1 では、次の VLAN モードが許可されます。
トランク	トランク（タグ付き）、タグなし、または 802.1p
タグなし	タグなし、または 802.1p またはトランク（タグ付き）
802.1p	トランク（タグ付き）または 802.1p またはタグなし

複数の EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	ポート 2 の EPG 1 では、次のモードが許可されます。	ポート 1 の EPG 2 では、次のモードが許可されます。
タグなし	タグなし、または 802.1p またはトランク（タグ付き）	トランク（タグ付き）

VLAN モードで、ポート 1 上の EPG 1 の場合：	ポート 2 の EPG 1 では、次のモードが許可されます。	ポート 1 の EPG 2 では、次のモードが許可されます。
802.1p	トランク（タグ付き）または 802.1p またはタグなし	トランク（タグ付き）
トランク	802.1p またはトランク（タグ付き）またはタグなし	トランク（タグ付き）または 802.1p またはタグなし

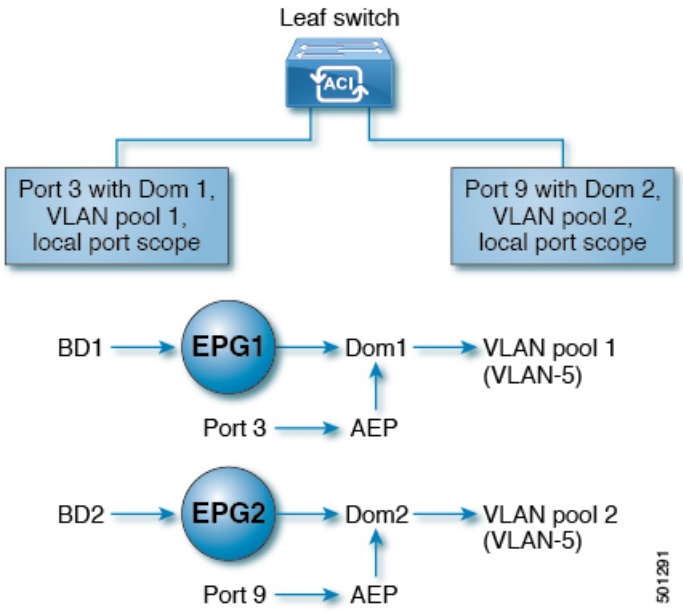
（注） タグなしのネイティブ VLAN でトラフィックを送信する特定の古いネットワーク インターフェイス カード（NIC）は、VLAN 0 としてタグ付けされたリターン トラフィックをドロップします。これは通常、トランク ポートとして構成されたインターフェイスでのみ問題になります。ただし、アクセス ポートのアタッチ可能エンティティ プロファイル（AEP）がインフラ VLAN を伝送するように構成されている場合、アクセス ポートとして構成されていても、トランク ポートとして扱われます。このような状況では、ネットワーク フロー エンジン（NFE）カードを備えたスイッチからネイティブ VLAN で送信されたパケットは VLAN 0 としてタグ付けされ、古いスイッチの NIC はパケットをドロップする可能性があります。この問題に対処するオプションは次のとおりです。

- AEP からインフラ VLAN を削除します。
- ポートで「ポート ローカル スコープ」を構成します。これにより、ポートごとの VLAN 定義が可能になり、NFE を搭載したスイッチがネイティブ VLAN 上でタグなしでパケットを送信できるようになります。

ポート単位の VLAN

v1.1 リリースより前の ACI バージョンでは、特定の VLAN カプセル化はリーフ スイッチ上の単一の EPG だけにマッピングされます。同じリーフ スイッチ上に同じ VLAN カプセル化を持つ第 2 の EPG があると、ACI でエラーが発生します。

v1.1 リリース以降では、次の図と同様、ポート単位の VLAN 設定で、特定のリーフ スイッチ (または FEX) 上に複数の EPG を同じ VLAN カプセル化で展開することができます。



単一のリーフ スイッチ上で、同じカプセル化番号を使用する複数の EPG の展開を有効にするには、次の注意事項に従ってください。

- EPG は、さまざまなブリッジ ドメインに関連付けられている必要があります。
- EPG は、さまざまなポートに展開する必要があります。
- ポートと EPG の両方が、VLAN 番号が含まれている VLAN プールに関連付けられている同じドメインに関連付けられている必要があります。
- ポートは `portLocal` VLAN スコープで設定されている必要があります。

たとえば、上の図の ポート 3 と 9 上に展開されている EPG のポート単位の VLAN で、両方が VLAN-5 を使用していれば、ポート 3 と EPG1 は Dom1 (プール 1) に、ポート 9 と EPG2 は Dom2 (プール 2) に関連付けられます。

ポート 3 からのトラフィックは EPG1 に関連付けられ、ポート 9 からのトラフィックは EPG2 に関連付けられます。

これは、外部レイヤ 3 外部接続用に設定されたポートには適用されません。

EPG に複数の物理ドメインがあり、VLAN プールが重複している場合は、EPG をポートに展開するために使用される AEP に複数のドメインを追加しないでください。これにより、トラフィック転送の問題が回避されます。

EPG に重複する VLAN プールを持つ物理ドメインが 1 つしかない場合、複数のドメインを単一の AEP に関連付けることができます。

入力および出力の両方向で個別の（ポート、VLAN）変換エントリの割り当てが可能なのは、`vlanScope` が `portlocal` に設定されているポートだけです。特定のポートで `vlanScope` が `portGlobal` (デフォルト) に設定されている場合には、EPG で使用される各 VLAN は、特定のリーフ スイッチ上で一意のものである必要があります。

（注） マルチ スパニング ツリー (MST) で設定されているインターフェイス上では、ポート単位の VLAN はサポートされていません。このツリーでは、VLAN ID が 1 つのリーフ スイッチ上で一意であること、そして VLAN の範囲がグローバルであることを必要とするからです。

同じリーフ スイッチで EPG に使用されていた VLAN 番号の再利用

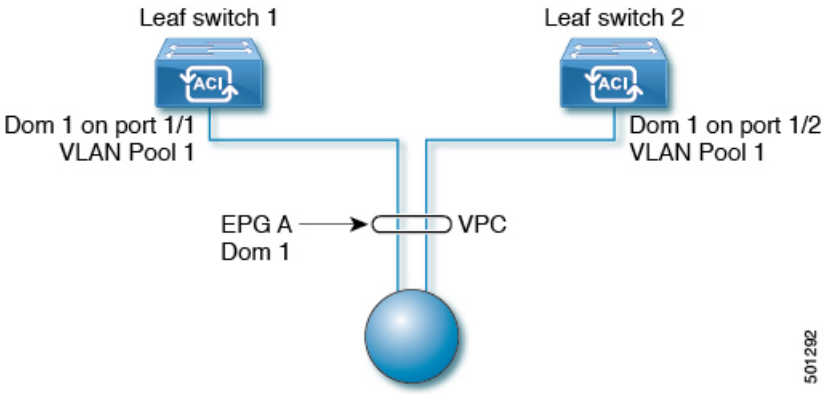
以前に、リーフ スイッチのポートに展開されている EPG 用に VLAN を設定していて、同じ VLAN 番号を同じリーフ スイッチの異なるポートの異なる EPG で再利用する場合には、中断なしでセットアップできるようにするため、次の例に示すようなプロセスに従ってください。

この例では、EPGは以前、9 ～ 100 の範囲の VLAN プールを含むドメインに関連付けられていたポートに展開されていました。ここで、9 ～ 20 からの VLAN カプセル化を使用する EPG を設定したいとします。

1. 異なるポート (たとえば、9 ～ 20 の範囲) で新しい VLAN プールを設定します。
2. ファイアウォールに接続されているリーフ ポートを含む新しい物理的なドメインを設定します。
3. ステップ 1 で設定した VLAN プールに物理的なドメインを関連付けます。
4. リーフ ポートの VLAN の範囲を `portLocal` として設定します。
5. 新しい EPG (この例ではファイアウォールが使用するもの) を、ステップ 2 で作成した物理ドメインに関連付けます。
6. リーフ ポートで EPG を展開します。

vPC に展開された EPG の VLAN ガイドライン

図 *12 : vPC の 2 つのレッグの VLAN*



EPG を vPC に展開する場合は、vPC の 2 つのレッグのリーフ スイッチ ポートに割り当てられた同じドメイン（同じ VLAN プール）に関連付ける必要があります。

この図では、EPG A は、リーフ スイッチ 1 およびリーフ スイッチ 2 のポートに展開されている vPC に展開されています。2 本のリーフ スイッチ ポートおよび EPG は、すべて同じ VLAN プールが含まれている同じドメインに関連付けられています。

カプセル化によるすべてのプロトコルおよびプロキシARPのカプセル化のフラッディングを設定する

Cisco Application Centric Infrastructure（ACI）は、ブリッジ ドメインをレイヤ 2 ブロードキャスト境界として使用します。各ブリッジ ドメインには複数のエンドポイント グループ（EPG）を含めることができ、各 EPG は複数の仮想ドメインまたは物理ドメインにマッピングできます。各 EPG は、ドメインごとに異なる VLAN カプセル化プールを使用することもできます。各 EPG は、ドメインごとに異なる VLAN または VXLAN カプセル化プールを使用することもできます。

通常、ブリッジ ドメイン内に複数の EPG を配置すると、ブロードキャスト フラッディングはブリッジ ドメイン内のすべての EPG にトラフィックを送信します。EPG はエンドポイントをグループ化し、特定の機能を実行するためにトラフィックを管理するために使用されるものなので、ブリッジ ドメイン内のすべての EPG に同じトラフィックを送信することは必ずしも実用的ではありません。

カプセル化でのフラッディングは、ネットワーク内のブリッジ ドメインを統合するのに役立ちます。この機能は、EPGが関連付けられている仮想ドメインまたは物理ドメインのカプセル化に基づいて、ブリッジ ドメイン内のエンドポイントへのブロードキャスト フラッディングを制御できるようにするからです。

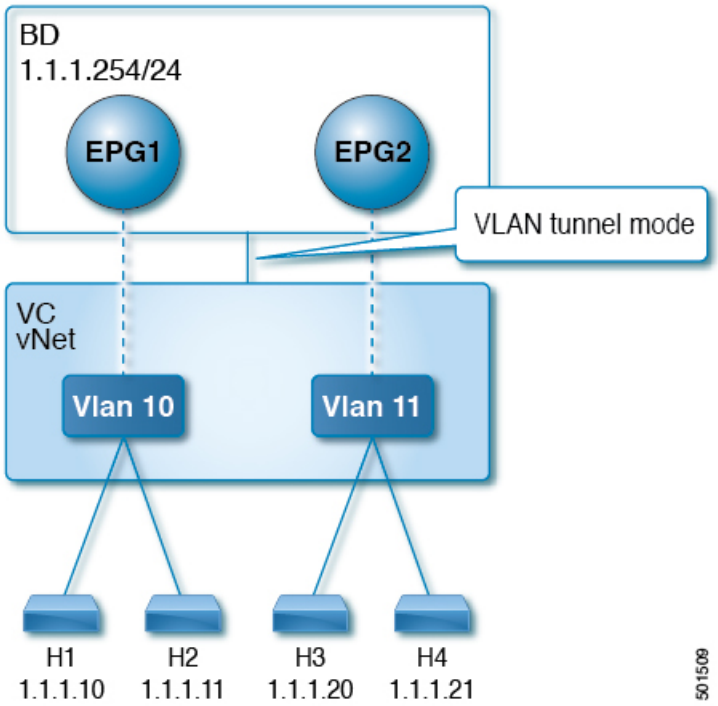
カプセル化でのフラッディングでは、同じブリッジ ドメインにおける異なる EPG のエンドポイント間の通信を許可するために、ブリッジ ドメインにサブネットと IP ルーティングを構成する必要があり、Cisco ACI がプロキシ ARP の役割を果たします。

VLAN カプセル化を使用したカプセル化でのフラッディングの使用例

カプセル化のフラッディングは、外部デバイスがVLANに依存しないMAC学習のためにvNetごとに 1 つの MAC アドレスが維持される仮想接続 トンネル モードを使用している場合によく用いられます。

トンネル モードで複数の VLAN を使用すると、いくつかの課題を導入できます。次の図に示すように、単一のトンネルでCisco ACIを使用する一般的な導入では、1つのブリッジ ドメインの下に複数の EPG があります。この場合、特定のトラフィックがブリッジ ドメイン内（つまりすべての EPG 内）でフラッディングし、MACがあいまいになって転送エラーが発生するリスクがあります。

図 *13 : VLAN*トンネルモードの*Cisco ACI*の課題



このトポロジでは、ブレードスイッチ（この例では仮想接続）に、1つのアップリンクを使用してCisco ACIリーフノードに接続する単一のトンネルネットワークが定義されています。このリンクでは、2 人のユーザの VLAN、VLAN 10 と VLAN 11 が行われます。サーバーのゲートウェイがCisco ACIクラウドの外部にあるため、ブリッジ ドメインはフラッディング モードに設定されます。次のプロセスで ARP 交渉が発生します。

- サーバは、VLAN 10 ネットワーク経由で 1 つの ARP ブロードキャスト要求を送信します。
- ARP パケットは、外部のサーバに向かってトンネル ネットワークを通過し、そのダウンリンクから学習した送信元 MAC アドレスを記録します。
- その後、サーバーはアップリンクからCisco ACIリーフスイッチにパケットを転送します。
- Cisco ACIファブリックは、アクセスポート VLAN 10に着信する ARP ブロードキャスト パケットを確認し、EPG1 にマッピングします。
- ブリッジ ドメインは ARP パケットをフラッディングするように設定されているため、パケットはブリッジ ドメイン内でフラッディングされます。したがって、両方の EPG が同じブリッジ ドメイン内にあるため、これらのポートにフラッディングされます。
- 同じ ARP ブロードキャスト パケットは、同じアップリンクで復帰します。
- ブレードスイッチは、このアップリンクからの元の送信元MACアドレスを認識します。

結果：ブレード スイッチは、単一の MAC 転送テーブル内のダウンリンク ポートとアップリンク ポートの両方から学習した同じMACアドレスを持ち、トラフィックが中断します。

推奨される解決策

カプセル化オプションのフラッディングは、ブリッジドメイン内のフラッディング トラフィックを単一のカプセル化に制限するために使用されます。EPG1/VLAN X and EPG2/VLAN Y が同じブリッジドメインを共有し、カプセル化でのフラッディングが有効になっている時、カプセル化フラッディング トラフィックは他の EPG/VLAN に到達しません。

Cisco Application Policy Infrastructure Controller（APIC）リリース 3.1(1) 以降、Cisco Nexus 9000 シリーズスイッチ（名前の末尾が EX および FX 以降）では、すべてのプロトコルがカプセル化されます。また、VLAN 間のトラフィックのブリッジ ドメインでフラッディングが有効になっている場合、プロキシ ARP は MAC フラップの問題が発生しないようにします。また、すべてのフラッディング（ARP、GARP、および BUM）をカプセル化に制限します。この制限は、有効になっているブリッジ ドメイン下のすべての EPG に適用されます。



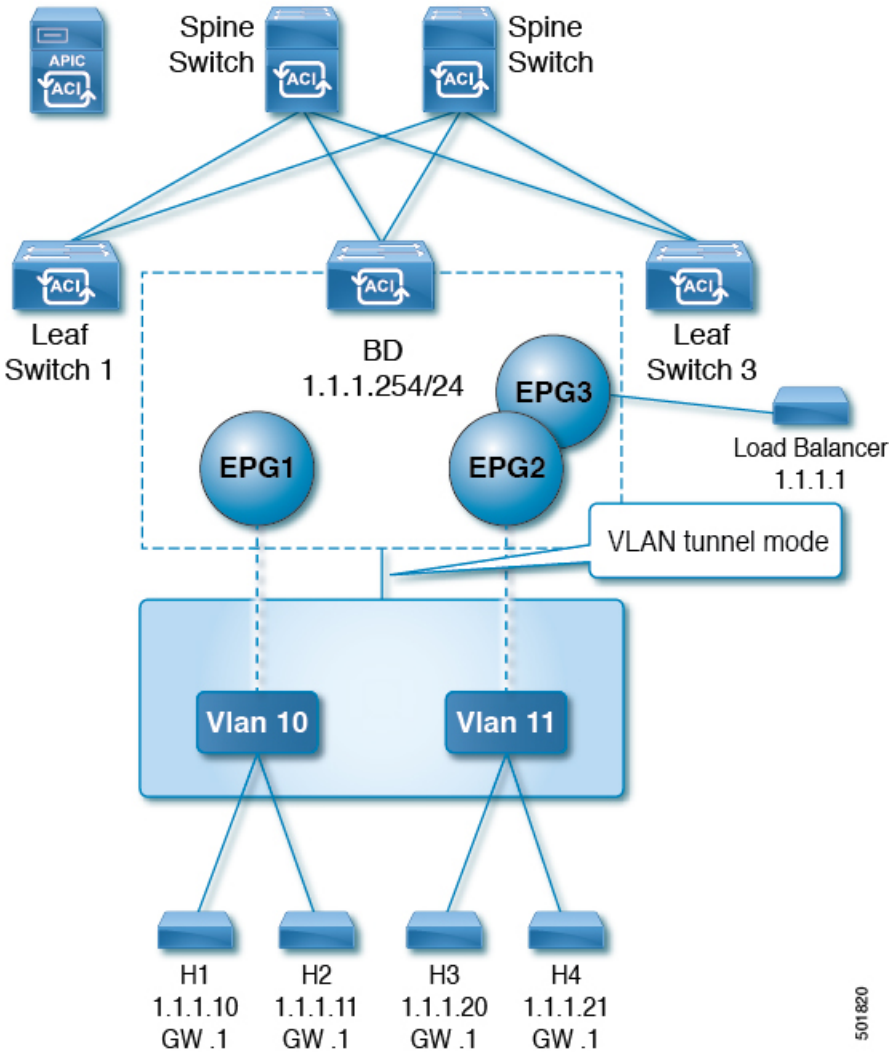
（注） Cisco APIC APIC リリース 3.1 (1) より前のリリースでは、これらの機能はサポートされていません（カプセル内でフラッディングするとき含まれるプロキシ ARP およびすべてのプロトコル）。以前の Cisco APIC リリースまたは以前の世代のスイッチ（名前に EX または FX がない）では、カプセル化でフラッディングを有効にしても機能しません。情報障害は生成されませんが、Cisco APIC はヘルス スコアを 1 減らします。



（注） Cisco APIC リリース 3.2(5) 以降では、VXLAN カプセル化に関連付けられた EPG のカプセル化でフラッディングを設定できます。以前は、VLAN のみが仮想ドメインのカプセル化でのフラッディングでサポートされていました。ブリッジ ドメインまたは EPG を作成または変更するときに、カプセル化でのフラッディングを設定します。

推奨される解決策は、外部スイッチを追加して、1 つのブリッジ ドメインで複数の EPG をサポートすることです。外部のスイッチがある 1 つのブリッジ ドメイン下で複数の EPG を持つこの設計は、次の図に示されています。

図 *14 :* 外部のスイッチがある *1* つのブリッジ ドメイン下で複数の *EPG* を持つ設計



同じブリッジ ドメイン内では、一部の EPG をサービス ノードにすることができ、他の EPG にはカプセル化でのフラッディングを設定できます。ロード バランサは別の EPG に存在します。ロード バランサは EPG からパケットを受信し、その他の EPG に送信します（プロキシ ARP はなく、カプセル内のフラッディングは発生しません）。

マルチ宛先プロトコル トラフィック

EPG/ブリッジ ドメイン レベルのブロードキャスト セグメンテーションは、次のネットワーク制御プロトコルでサポートされます。

- OSPF
- EIGRP
- LACP
- IS-IS

- BGP
- IGMP
- PIM
- STP BPDU（EPG 内フラッディング）
- ARP/GARP（ARP プロキシによって制御）
- ND

カプセル化でのフラッディングの制限事項

すべてのプロトコルのカプセル化でのフラッディングには、次の制限が適用されます。

- カプセルのフラッディングは、ARP ユニキャスト モードでは機能しません。
- このリリースでは、ネイバー送信要求（プロキシ NS/ND）はサポートされていません。
- プロキシアドレス解決プロトコル（ARP）は暗黙的に有効にされるため、ARP トラフィックは異なるカプセル化間の通信のために CPU に送信できます。

  ARP トラフィックを処理するために異なるポートに均等に配信されるようにするには、ポート単位のコントロール プレーン ポリシング（CoPP）を有効にします。
- カプセル化でのフラッディングは、フラッド モードのブリッジ ドメインおよびフラッド モードの ARP でのみサポートされます。ブリッジ ドメイン スパイン プロキシ モードはサポートされていません。
- IPv4 レイヤ 3 マルチキャストはサポートされていません。
- カプセル化でのフラッディングが有効な場合でも、IPv6 NS/NDプロキシはサポートされません。その結果、同じ IPv6 サブネット下にあっても、カプセル化が異なる EPG に存在する 2 つのエンドポイント間の接続は、機能しないことがあります。
- 別の VLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。別の VLAN または VXLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。
- 仮想マシンの IP アドレスが、ファイアウォールの IP アドレスではなく、ゲートウェイの IP アドレスに変更された場合、ファイアウォールはバイパスされるため、ファイアウォールをゲートウェイにする仮想マシン間の通信セットアップは推奨されません。
- 以前のリリースではサポートされていません（以前と現在のリリース間の相互運用もサポートされていません）。
- 古い世代アプリケーション リーフ エンジン（ALE）とアプリケーション スパイン エンジン（ASE）を使用した混合モード トポロジは推奨されません。また、カプセル化でのフラッディングではサポートされません。同時に有効にすると、QoS の優先順位が適用されるのを防ぐことができます。
- 同じマルチサイト ドメインの一部であるCisco ACIファブリック全体に拡張された EPG とブリッジドメインでは、カプセル化でのフラッディングはサポートされません。ただし、

Cisco ACIファブリックでローカルに定義された EPG とブリッジ ドメインでは、カプセル化でのフラッディングは引き続き機能し、完全にサポートされています。Cisco ACIファブリックと、そのファブリックに関連付けられたリモート リーフ スイッチ間でストレッチされる EPG またはブリッジ ドメインにも、同じ考慮事項が適用されます。

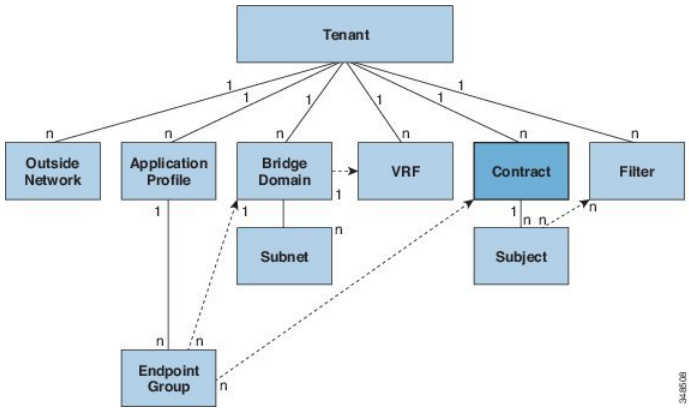
- マイクロセグメンテーションがいずれかの形式で構成されている EPG では、カプセル化でのフラッディングはサポートされません。これには、EPG 内分離、VMM ドメインでの「マイクロセグメンテーションを許可する」、マイクロセグメンテーション EPG、EPG 内コントラクトが含まれます。
- 共通パーベイシブ ゲートウェイでは、カプセル化でのフラッディングはサポートされていません。Cisco APIC Layer 3 Networking Configuration Guide の「Common Pervasive Gateway」の章を参照してください。
- ブリッジ ドメインのすべてのEPGでカプセル化でのフラッディングを設定する場合は、ブリッジ ドメインでもカプセル化でのフラッディングを設定してください。
- IGMP スヌーピングは、カプセル化でのフラッディングではサポートされません。
- Cisco ACIにおいては、カプセル化でのフラッディングのために設定された EPG で受信されるパケットのフラッディングを、（カプセル化ではなく）ブリッジ ドメインで生じさせる条件が存在します。これは、管理者がカプセル化でのフラッディングを EPG で直接設定したか、ブリッジ ドメインで設定したかに関係なく発生します。この転送動作の条件は、入力リーフ ノードに宛先MACアドレスのリモートエンドポイントがあり、出力リーフ ノードに対応するローカル エンドポイントがない場合です。これは、インターフェイスのフラッピング、STP TCNによるエンドポイント フラッシュ、過剰な移動のためにブリッジ ドメインで学習が無効になっているなどの理由で発生する可能性があります。

  4.2(6o) 以降の 4.2(6) リリース、4.2(7m) 以降の 4.2(7) リリース、および 5.2(1g) 以降のリリースでは、この動作が拡張されました。管理者が（EPG ではなく）ブリッジ ドメインでカプセル化のフラッディングを有効にした場合、Cisco ACI は非入力（出力および中継）リーフ ノード上の外部デバイスに面したダウンリンクからのカプセル化で、このようなパケットを送信しません。この新しい動作により、パケットが予期しないカプセル化に漏洩することが防止されます。カプセル化でのフラッディングが EPG レベルでのみ有効になっている場合、非入力リーフ ノードは、カプセル化ではなくブリッジ ドメインでパケットをフラッディングする可能性があります。詳細については、拡張バグ CSCvx83364 を参照してください。
- レイヤ 3 ゲートウェイは Cisco ACI ファブリック内にある必要があります。

コントラクト

EPG に加えて、コントラクト（vzBrCP）はポリシー モデルのキー オブジェクトです。EPG が他の EPG と通信するには、コントラクトのルールに従う必要があります。次の図は、管理情報ツリー（MIT）内のコントラクトの場所とテナントの他のオブジェクトとの関係を示します。

図 *15* : コントラクト



管理者はコントラクトを使用して、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。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。EPG 内の通信に必要なコントラクトはありません。EPG 内の通信は常に暗黙的に許可されています。

また、コントラクト優先グループを構成して、VRF で EPG 間のより高度な通信の制御も可能です。VRF の EPG のほとんどはオープン通信ですが、一部には他の EPG との制限がある場合、コントラクト優先グループとフィルタ付きのコントラクトの組み合わせを構成し、通信を正確に制御できます。

コントラクトは、次のタイプのエンドポイント グループの通信を管理します。

- ACI ファブリック アプリケーション EPG （`fvAEPg`）間、テナント内およびテナント間の両方

（注） 共有サービス モードの場合、コントラクトはテナント間通信に必要です。テナントVRFがポリシーを適用していなくても、コントラクトが VRF 間で静的ルートを指定するために使用されます。

- ACI ファブリック アプリケーション EPG とレイヤ 2 外部外側ネットワークのインスタンス EPG （`l2extInstP`）間
- ACI ファブリック アプリケーション EPG とレイヤ 3 外部外側ネットワークのインスタンス EPG （`l3extInstP`）間
- ACI ファブリック アウトオブバンド（`mgmtOoB`）またはインバンド（`mgmtInB`）管理 EPG 間

コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付された EPG 間の通信を制御します。EPG プロバイダーは、コンシューマ EPG が従う必要のあるコントラクトを公開します。EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。EPG がコントラクトを提供すると、通信が提供されたコントラクトに準拠している限り、その EPG

との通信は他の EPG から開始できます。EPG がコントラクトを使用すると、その EPG のエンドポイントは、コントラクトを指定した EPG のエンドポイントと通信を開始できます。

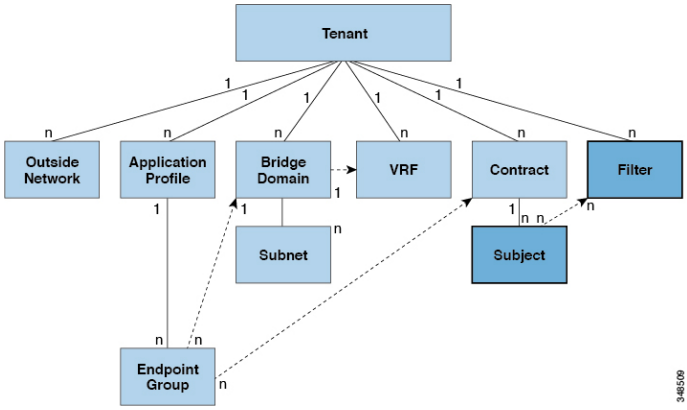
（注） 1 つの EPG で同じコントラクトを指定および使用できます。EPG は複数のコントラクトを同時に指定および使用することもできます。

（注） ユーザーテナントから common テナントにエクスポートされたコントラクトは、他のユーザーテナントで自動的に使用できるようにはなりません。複数のユーザーテナントと common テナント間でコントラクトを共有するには、コントラクトを common テナントで定義するか、目的の各テナントに個別にエクスポートする必要があります。

EPG 通信を制御するラベル、フィルタ、エイリアス、および情報カテゴリ

ラベル、情報カテゴリ、エイリアス、およびフィルタの管理対象オブジェクトにより、さまざまなアプリケーションまたはサービスの提供要件を満たすための EPG とコントラクト間の混合と照合が可能になります。次の図は、管理情報ツリー（MIT）内のアプリケーション サブジェクトおよびフィルタの場所と、テナント内の他のオブジェクトとの関係を示します。

図 *16 :* ラベル、情報カテゴリ、およびフィルタ



コントラクトには、複数の通信ルールを含めることができ、複数の EPG は複数のコントラクトを消費および提供できます。ラベルは、EPG の特定のペア間で通信が行われるときにどのルールが適用されるかを管理します。ポリシーの設計者は、複雑な通信ポリシーを簡潔に表し、アプリケーションの複数のインスタンス間でこれらのポリシーを再利用できます。たとえば、*Cisco Application Centric Infrastructure Fundamentals* の「Contract Scope Examples」の章のサンプルポリシーは、同じコントラクトがラベル、情報カテゴリ、およびフィルタを使用して、HTTP または HTTPS を必要とするさまざまな EPG 間で通信がどのように発生するかを区別する方法を示しています。

ラベル、情報カテゴリ、およびフィルタは次のオプションに従って EPG 通信を定義します。

- ラベルは、プロパティ（名前）を 1 つだけ持つ管理対象オブジェクトです。ラベルにより、互いに通信できるオブジェクトとできないオブジェクトを分類できます。ラベルの一致は最初に行われます。ラベルが一致しない場合、他のコントラクトまたはフィルタ情報は処理されません。ラベルの一致属性は、次の値のいずれかになります。At Least One（デフォルト）、All、None または Exactly One。*Cisco Application Centric Infrastructure Fundamentals* の「Label Matching」の章では、すべてのラベル マッチ タイプとその結果の簡単な例を示しています。

（注） ラベルは、EPG、コントラクト、ブリッジ ドメイン、DHCP リレー ポリシー、および DNS ポリシーなどのさまざまなプロバイダーおよびコンシューマの管理対象オブジェクトに適用できます。ラベルはオブジェクト タイプ間では適用されません。アプリケーション EPG のラベルは、ブリッジドメインのラベルと関連がありません。

ラベルは、互いに通信できる EPG コンシューマと EPG プロバイダーを決定します。ラベルの一致により、コントラクトのどのサブジェクトがそのコントラクトの所定の EPG プロバイダーまたは EPG コンシューマに使用できるかが決定されます。

ラベルには次の 2 つのタイプがあります。

- 情報カテゴリのラベルは EPG に適用されます。サブジェクト ラベルの一致により、EPG はコントラクト内のサブジェクトのサブセットを選択することができます。
- EPG に適用されるプロバイダー/コンシューマ ラベル。プロバイダー/コンシューマのラベルの一致により、コンシューマ EPG はプロバイダー EPG を選択できます。その逆も可能です。

- エイリアスは、オブジェクトに適用できる代替名であり、名前とは異なり、変更できます。
- フィルタは、レイヤ 2 ～ レイヤ 4 フィールド、レイヤ 3 プロトコル タイプ、レイヤ 4 ポートなどの TCP/IP ヘッダー フィールドなどです。関連するコントラクトに従って、EPG プロバイダーは、IN および OUT 両方の方向でプロトコルおよびポートを決定します。コントラクトの情報カテゴリは、コントラクトを提供する側と消費する側の EPG の間に適用されるフィルタ（およびその方向）への関連付けが含まれています。

（注） コントラクト フィルタの一致タイプが すべて（All） の場合、ベスト プラクティスは VRF 非強制モードを使用することです。特定の状況下では、これらのガイドラインに従わないと、コントラクトで VRF の EPG 間のトラフィックが許可されなくなります。

- 情報カテゴリはコントラクトに含まれています。コントラクト内の1つ以上の情報カテゴリがフィルタを使用して、通信できるトラフィックのタイプと発生の仕方を指定します。たとえば、HTTPS メッセージの場合、サブジェクトはその方向と許可される IP アドレスタイプ（たとえば IPv4）、HTTP プロトコル、およびポートを指定するフィルタを指定します。サブジェクトは、フィルタを単方向にするか双方向にするかを決定します。単方向フィルタは 1 方向で使用されます。単方向フィルタは、IN または OUT の通信を定義しますが、両方に対して同じではありません。双方向フィルタは両方に対して同じで、IN および OUT の通信を定義します。

コントラクトまたはコントラクトの件名の例外の設定

Cisco APIC リリース 3.2(1) では、EPG 間のコントラクトが拡張され、コントラクトに参加しているコントラクトプロバイダまたはコンシューマのサブネットを拒否できます。インター EPG コントラクトおよびい内部 EPG コントラクトは、この機能でサポートされます。

プロバイダ EPG の件名を有効にして、件名またがコントラクトの例外で一致基準が設定されているものを除くすべてのコンシューマ EPG との通信が可能になります。たとえば、サブセットを除く、テナントのすべての EPG にサービスを提供するために EPG を有効にする場合、これら EPG を除外できます。これを設定するには、コントラクトまたはそのコントラクトの件名のいずれかで例外を作成します。サブセットがコントラクトの提供または消費のアクセスを拒否します。

ラベル、カウンタ、許可および拒否ログは、コントラクトおよび件名の例外でサポートされています。

コントラクトのすべての件名に例外を適用するには、コントラクトに例外を追加します。コントラクトの単一の件名にのみ例外を適用する場合、件名に例外を追加します。

件名にフィルタを追加する場合、フィルタのアクションを設定できます（フィルタ条件に一致するオブジェクトを許可または拒否する）。また、**[拒否]**フィルタについては、フィルタの優先順位を設定することができます。**[許可]**フィルタは常にデフォルトの優先順位があります。自動拒否の件名-フィルタ関係をマーキングすると、件名に一致している場合、各 EPG のペアに適用されます。コントラクトと件名には、複数の件名-フィルタ関係を含むことができます。これは、フィルタに一致するオブジェクトを許可または拒否するように独自に設定できます。

例外タイプ

コントラクトと件名の例外は次のタイプに基づき、* ワイルドカードなどの正規表現を含むことができます。

例外の条件は、[コンシューマ正規表現] および [プロバイダ正規表現]のフィールドで定義されているように、これらのオブジェクトを除外します。	例	説明
テナント	<vzException consRegex= “common” field= “Tenant” name= “excep03” provRegex= “t1” />	この例では、common テナントを使用して、 EPG が t1 テナントにより提供されるコントラクトを消費しないように除外します。
VRF	<vzException consRegex= “ctx1” field= “Ctx” name= “excep05” provRegex= “ctx1” />	この例では、ctx1 のメンバーが同じ VRF から提供されるサービスを使用しないように除外します。
EPG	<vzException consRegex= “EPgPa.*” field= “EPg” name= “excep03” provRegex= “EPg03” />	この例では、名前が EPGPa から始まる複数の EPG が存在すると仮定し、EPg03 により提供されているコントラクトのコンシューマとしてすべて拒否される必要があります。
Dn	<vzException consRegex= “uni/tn-t36/ap-customer/epg-epg193” field= “Dn” name=“excep04” provRegex= “uni/tn-t36/ap-customer/epg-epg200” />	この例では、epg193 が epg200 により提供されたコントラクトを消費しないように除外します。
タグ	<vzException consRegex= “red” field= “Tag” name= “excep01” provRegex= “green” />	例では、red タグでマークされているオブジェクトが消費することと、green タグでマークされているオブジェクトがコントラクトに参加しないように除外します。

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。

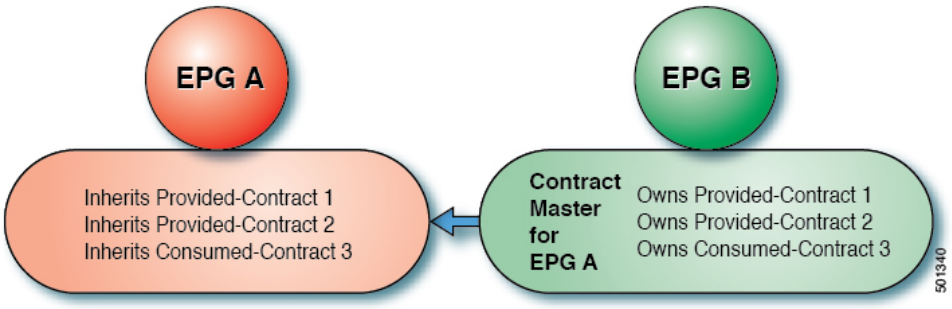
コントラクト継承について

関連する契約を新しい EPG に統合するため、EPG を有効にして同じテナントの別の EPG に直接関連する契約すべて（提供済み/消費済み）を継承できます。コントラクトの継承は、アプリケーション EPG、マイクロセグメント EPG、L2Out EPG、および L3Out EPG に設定できます。

リリース 3.x では、EPG 間の提供済み/消費済みの両方の契約に、契約を継承する設定も可能です。EPG 間契約が、モデル名や後発のモデルの最後に EX または EX が付く、Cisco Nexus 9000 シリーズ スイッチでサポートされています。

EPG を有効にし、APIC GUI、NX-OS スタイル CLI、REST API を使用して、別の EPG に直接関連する契約すべてを継承できます。

図 *17:* コントラクトの継承



上の図で、EPG A は EPG B から（EPG A の契約マスター）提供済みの契約 1 および 2、消費済みの契約 3 を継承するように設定されています。

コントラクト継承を設定する際は、次のガイドラインに従ってください。

- コントラクト継承は、アプリケーション EPG、マイクロセグメント（uSeg）EPG、外部 L2Out EPG、および外部 L3Out EPG 用に設定できます。コントラクト関係は同じタイプの EPG 間で確立する必要があります。
- 関係が確立されると、提供するコントラクトと消費するコントラクトの両方がコントラクト マスターから継承されます。

- コントラクト マスターとコントラクトを継承する EPG は同じテナント内にある必要があります。
- マスター契約への変更は、すべての継承に伝播されます。新しい契約がマスターに追加される場合、継承先にも追加されます。
- EPG は、複数のコントラクト マスターからコントラクトを継承することができます。
- コントラクト継承は単一のレベルでのみサポートされ（連結できない）、コントラクトマスターがコントラクトを継承することはできません。
- コントラクト継承のラベルがサポートされます。EPG A が EPG B からコントラクトを継承するとき、EPG A と EPG B で異なるサブジェクト ラベルが設定されている場合、APIC は EPG B から継承されたコントラクトの EPG B で設定されたラベルを使用します。 APIC は EPG A が直接関与するコントラクトに対し、EPG A の下で設定されたラベルを使用します。
- EPG が契約に直接関連付けられている、または契約を継承しているかどうかに関わらず、TCAM 内のエントリが消費されます。したがって契約スケール ガイドラインが引き続き適用されます。詳細については、お使いのリリースの「検証されたスケーラビリティ ガイド」を参照してください。
- vzAny セキュリティ コントラクトとタブー コントラクはサポートされません。
- Cisco APIC リリース 5.0(1) および 4.2(6) 以降、コントラクトと EPG が同じテナントにある場合、サービス グラフによるコントラクトの継承がサポートされます。

契約の継承設定および継承済みおよびスタンドアロン契約を表示することに関する詳細は、「*Cisco APIC* の基本設定ガイドを参照してください。

契約優先グループについて

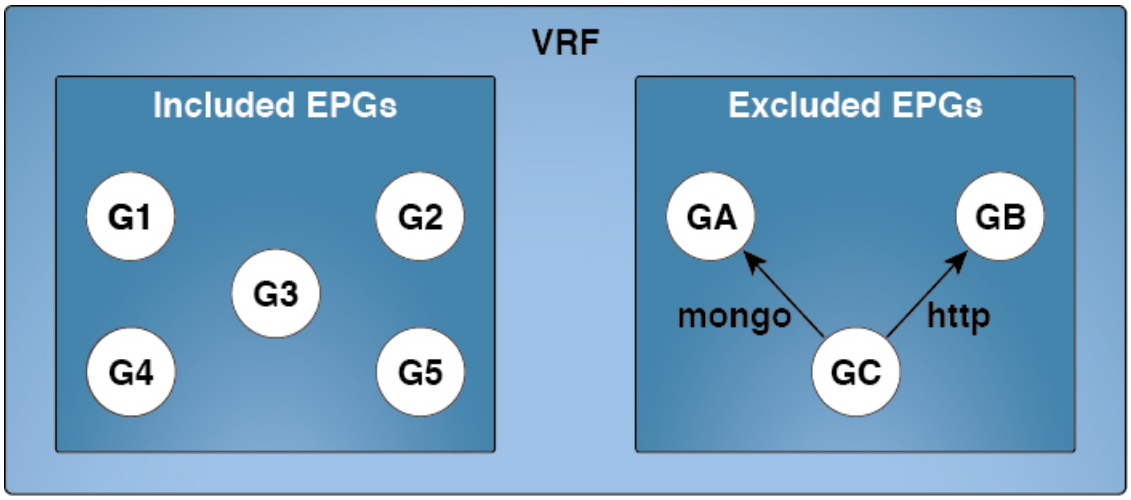
契約優先グループが設定されている VRF で、EPG に利用可能なポリシー適用には 2 種類あります。

- EPG を含む：EPG が契約優先グループのメンバーシップを持っている場合、EPG は契約をせずにお互いに自由に通信できます。これは、source-any-destination-any-permit デフォルト ルールに基づくものです。
- EPG を除外：優先グループのメンバーではない EPG は、相互に通信するために契約が必要です。そうしない場合、デフォルトの source-any-destination-any-deny ルールが適用されます。

契約優先グループ機能では、VRF で EPG 間のより高度な通信の制御が可能です。VRF の EPG のほとんどはオープン通信ですが、一部には他の EPG との制限がある場合、契約優先グループとフィルタ付きの契約の組み合わせを設定し、EPG 内の通信を正確に制御できます。

優先グループから除外されている EPG は、source-any-destination-any-deny デフォルト ルールを上書きする契約がある場合にのみ、他 EPG と通信できます。

図 *18 :* 契約優先グループの概要



Source	Destination	Filter	Action
any	any	implicit	permit
GA	any	implicit	deny
any	GA	implicit	deny
GB	any	implicit	deny
any	GB	implicit	deny
GC	any	implicit	deny
any	GC	implicit	deny

Source	Destination	Filter	Action
GC	GA	mongo	permit
GA	GC	mongo	permit
GC	GB	http	permit
GB	GC	http	permit

サービス グラフ サポート

APIC リリース 4.0(1) 以降では、サービス グラフによって作成された EPG を優先契約グループに含めることができます。優先グループ メンバーシップのタイプ（include または exclude）を定義する新しいポリシー（サービス EPG ポリシー）が使用可能です。設定後は、デバイス選択ポリシーまたはサービス グラフ テンプレートのアプリケーションを通じて適用できます。

また、シャドウ EPG を優先グループに含めるか、優先グループから除外するかも設定できるようになりました。

制限事項

以下の制限が契約優先グループに適用されます。

- L3Out およびアプリケーション EPG が契約優先グループで設定されており、EPG が VPC でのみ展開されているトポロジで、VPC の 1 つのリーフ スイッチのみに L3Out のプレフィックス エントリがあることがわかります。この場合、VPC の他のリーフ スイッチにはエントリがなく、そのためトラフィックをドロップします。

  この問題を回避するには、次のいずれかを行います。

  - VRF の契約グループを無効および再度有効にします。

- L3Out EPG のプレフィックス エントリを削除し再度作成します。

- また、サービス グラフ契約のプロバイダまたはコンシューマ EPG が契約グループに含まれる場合、シャドウ EPG は契約グループから除外できません。シャドウ EPG は契約グループで許可されますが、シャドウ EPG が展開されているノードで契約グループ ポリシーの展開をトリガしません。ノードに契約グループ ポリシーをダウンロードするには、契約グループ内にダミー EPG を展開します。
- CSCvm63145 により、コントラクト優先グループの EPG は共有サービス コントラクトを使用できますが、L3Out EPG をコンシューマとして使用する共有サービス コントラクトのプロバイダになることはできません。

契約のパフォーマンスの最適化

Cisco APIC、リリース 3.2 で始まるより効率的なハードウェア契約データの TCAM ストレージをサポートしている双方向契約を設定できます。最適化を有効になっている、両方向の統計情報を契約は統合します。

TCAM 最適化は、第 2 世代 Cisco Nexus 9000 シリーズのトップオブラック（TOR）スイッチでサポートされます。これは、EX、FX、および FX2 以降のサフィックスが付いたものです（たとえば、N9K-C93180LC-EX または N9K-C93180YC-FX ）。

TCAM 契約の効率的なデータ ストレージを設定するには、次のオプションが有効にします。

- プロバイダとコンシューマの間で両方向に適用されるコントラクトをマークします。
- IP TCP または UDP プロトコルを使用するフィルタの場合は、リバース ポート オプションを有効にします。
- コントラクト サブジェクトを設定する場合は、**[ポリシー圧縮の有効化（Enable Policy Compression）]** ディレクティブを選択します。これにより、`actrl : Rule` 管理対象オブジェクトの`アクション`属性に `no_stats` オプションが追加されます。

制限事項

[ポリシー圧縮の有効化（Enable Policy Compression）]（`no_stats`）オプションを選択すると、ルールごとの統計情報が失われます。ただし、両方の方向の複合ルール統計情報は、ハードウェア統計情報に存在します。

Cisco APIC 3.2(1) にアップグレードした後、`no_stats` オプションをアップグレード前のコントラクト サブジェクト（フィルタまたはフィルタ エントリを含む）に追加するには、コントラクト サブジェクトを削除し、**Enable Policy Compression** ディレクティブで再設定する必要があります。そうしないと、圧縮は行われません。

双方向サブジェクト フィルタを使用するコントラクトごとに、Cisco NX-OS は 2 つのルールを作成します。

- `sPcTag` および `dPcTag` が含まれ、`direction=bi-dir` とマークされているルール。これはハードウェアでプログラミングされます。

- プログラミングされていない direction=uni-dir-ignore でマークされたルール

次の設定とルールは圧縮されません。

- ルールの優先順位を持つ fully_qual
- ルールの反対側 (双 dir および uni dir 無視 マーク) と同一ではないプロパティは、次のように **アクション** を含む **統制** 、 **prio**、**qos** または **markDscp**
- ルール 暗黙的 または implarp フィルタ
- ルール アクションで Deny 、 Redir 、 コピー 、または Deny ログ

次の月クエリ出力は、圧縮のと見なされる、契約の 2 つのルールを示します。

```
apic1# moquery -c actrlRule
Total Objects shown: 2

# actrl.Rule
scopeId            : 2588677
sPcTag             : 16388
dPcTag             : 49156
fltId              : 67
action             : no_stats,permit
actrlCfgFailedBmp  :
actrlCfgFailedTs   : 00:00:00:00.000
actrlCfgState      : 0
childAction        :
ctrctName          :
descr              :
direction          : bi-dir
dn                 : sys/actrl/scope-2588677/rule-2588677-s-16388-d-49156-f-67
id                 : 4112
lcOwn              : implicit
markDscp           : unspecified
modTs              : 2019-04-27T09:01:33.152-07:00
monPolDn           : uni/tn-common/monepg-default
name               :
nameAlias          :
operSt             : enabled
operStQual         :
prio               : fully_qual
qosGrp             : unspecified
rn                 : rule-2588677-s-16388-d-49156-f-67
status             :
type               : tenant


# actrl.Rule
scopeId            : 2588677
sPcTag             : 49156
dPcTag             : 16388
fltId              : 64
action             : no_stats,permit
actrlCfgFailedBmp  :
actrlCfgFailedTs   : 00:00:00:00.000
actrlCfgState      : 0
childAction        :
ctrctName          :
descr              :
direction          : uni-dir-ignore
```

```
dn                  : sys/actrl/scope-2588677/rule-2588677-s-49156-d-16388-f-64
id                  : 4126
lcOwn               : implicit
markDscp            : unspecified
modTs               : 2019-04-27T09:01:33.152-07:00
monPolDn            : uni/tn-common/monepg-default
name                :
nameAlias           :
operSt              : enabled
operStQual          :
prio                : fully_qual
qosGrp              : unspecified
rn                  : rule-2588677-s-49156-d-16388-f-64
status              :
type                : tenant
```

表 *6:* 圧縮マトリクス

リバース フィルタ ポートが有効	TCP または UDP 発信元ポート	TCP または UCP 宛先ポート	圧縮
はい	ポート A	ポート B	はい
○	未指定	ポート B	はい
○	ポート A	未指定	はい
○	未指定	未指定	はい
非対応	ポート A	ポート B	いいえ
非対応	未指定	ポート B	いいえ
非対応	ポート A	未指定	いいえ
非対応	未指定	未指定	はい

vzAny とは

vzAny 管理対象オブジェクトは、各 EPG の個別のコントラクト関係を作成するのではなく、1 つまたは複数のコントラクト（vzBrCP）に仮想ルーティングと転送（VRF）のすべてのエンドポイント グループ（EPG）を関連付ける便利な方法を提供します。

Cisco ACI ファブリックでは、コントラクトのルールにより、EPG は他の EPG としか通信できません。EPG とコントラクトの関係によって、EPG がコントラクトのルールに定義された通信を提供するのか、消費するのか、あるいは提供も消費も行うのかが指定されます。VRF 中のすべての EPG にコントラクトのルールを動的に適用することで、vzAny ではEPG とコントラクトとの関係を構成するプロセスが自動化されます。新しい EPG が VRF に追加されるたびに、vzAny コントラクト ルールが自動的に適用されます。vzAny と EPG の「1 対すべて」の関係は、コンテキスト中のすべての EPG にコントラクトのルールを適用するための最も効率的な方法です。

（注） テナントの APIC GUI では、VRF はプライベートネットワーク（テナント内のネットワーク）またはコンテキストとも呼ばれます。

共有サービスの場合は、コンシューマ（vzAny）側の接続先の pcTag（分類）を適切に導出するために、EPG の下にプロバイダ EPG 共有サブネットを定義する必要があります。コンシューマとプロバイダの両方のサブネットがブリッジ ドメイン下で定義され、共有サービス コンシューマとして機能する vzAny に対して、BD から BD への共有サービス設定から移行する場合は、少なくとも共有フラグを使用してプロバイダ サブネットを EPG に追加する追加の設定手順を実行する必要があります。

（注） 定義済みの BD サブネットの複製として EPG サブネットを追加する場合は、サブネットの両方の定義に同じフラグが定義されていることを確認してください。そうしないと、予期しないファブリック転送の動作が発生する可能性があります。

vzAny を使用するには、**[テナント（Tenants）]**> > **[*tenant-name*]**> > **[ネットワーキング（Networking）]** > > **[VRFs]**> > **[*vrf-name*]**> > **[VRF 向けの EPG 収集（EPG Collection for VRF）]** の順に移動します。

コピー サービスについて

すべてのトラフィックを複製する SPAN とは異なり、 Cisco Application Centric Infrastructure (ACI) のコピー サービス機能は、契約での仕様に従って、エンドポイント グループ間のトラフィックのうちコピーの部分だけを選択的に有効にします。ブロードキャスト、不明なユニキャストとマルチキャスト (BUM)、および契約の対象外であるコントロール プレーン トラフィックは、コピーされません。対照的に、SPAN は、エンドポイント グループ、アクセス ポートまたはアップリンク ポートから発するすべてのトラフィックをコピーします。SPAN とは異なり、コピーサービスは、コピーされたトラフィックにヘッダーを追加しません。コピーサービスのトラフィックは、通常のトラフィックの転送への影響を最小限に抑えるため、スイッチ内で内部的に管理されます。

コピー サービスは、コピーされるトラフィックの宛先としてコピー クラスタを指定する、レイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートの一部として構成されます。コピー サービスはサービス グラフ内の異なるホップにタップすることができます。たとえば、コピー サービスは、コンシューマ エンドポイント グループとファイアウォール プロバイダ エンドポイントの間のトラフィック、またはサーバのロードバランサとファイアウォールの間のトラフィックを選択することができます。コピー クラスタは、テナント間で共有することができます。

コピー サービスを使用するには、以下のタスクを実施する必要があります:

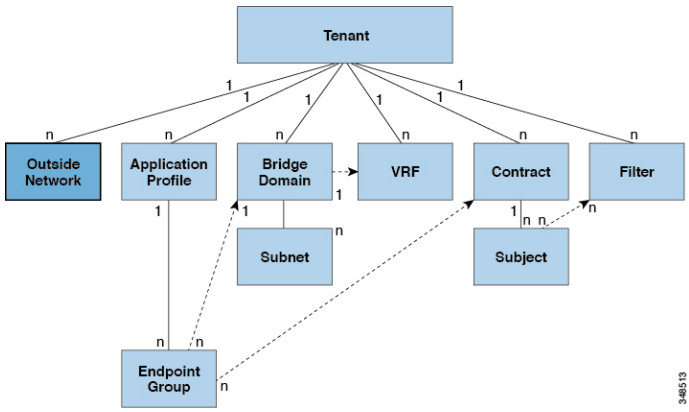
- 送信元と宛先エンドポイント グループを特定します。
- 情報カテゴリ、および契約フィルタで許可されている内容に従って、コピー対象を指定する契約を構成します。

- ターゲット デバイスを特定するレイヤ 4 ～ レイヤ 7 のコピー デバイスを構成し、それらが接続するポートを指定します。
- コピー サービスをレイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートの一部として使用します。
- どのデバイスがサービス グラフからのトラフィックを受信するかを指定する、デバイス選択ポリシーを構成します。デバイス選択ポリシーを構成する際には、契約、サービス グラフ、コピー クラスタ、およびコピー デバイス内のクラスタ論理インターフェイスを指定します。

外部ネットワーク

外部ネットワーク ポリシーは、外部への接続を制御します。テナントには、複数の外部ネットワーク オブジェクトを含めることができます。次の図は、管理情報ツリー（MIT）内の外部ネットワークの場所とテナントの他のオブジェクトとの関係を示します。

図 *19 :* 外部ネットワーク



外部ネットワーク ポリシーは、外部のパブリック/プライベート ネットワークと ACI ファブリック間の通信を制御する関連するレイヤ 2（`l2extOut`）またはレイヤ 3（`l3extOut`）プロパティを指定します。WAN およびエンタープライズ コアに接続するルータや既存のレイヤ 2 スイッチなどの外部デバイスは、リーフスイッチの前面パネルのインターフェイスに接続します。このような接続を提供するリーフスイッチは、境界リーフとして知られています。外部デバイスに接続する境界リーフスイッチ インターフェイスは、ブリッジドまたはルーテッド インターフェイスとして構成できます。ルーテッドインターフェイスの場合、静的またはダイナミック ルーティングを使用できます。境界リーフスイッチは、標準のリーフスイッチのすべての機能を実行することもできます。

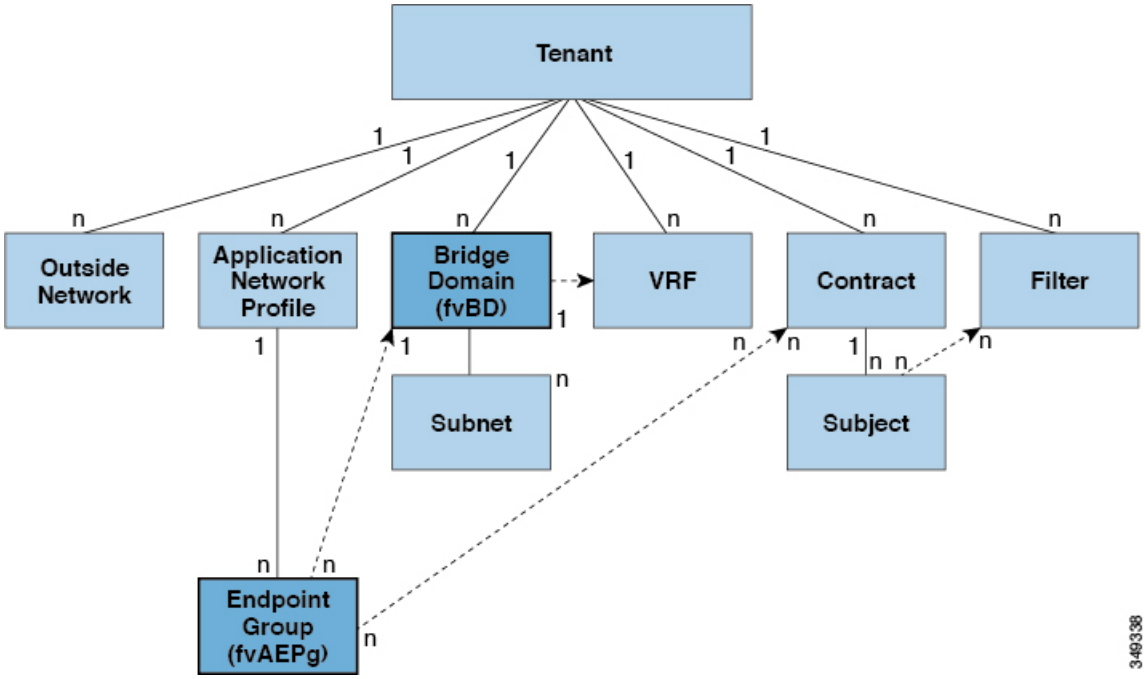
管理対象オブジェクトの関係とポリシー解決

関係管理対象オブジェクトは、抑制（親/子）の関係を共有しない管理対象オブジェクトのインスタンス間の関係を表します。MO の関係は、次の 2 つの方法のいずれかでソース MO とターゲット MO の間に確立されます。

- 明示的な関係（`fvRsPathAtt`）は、ターゲット MO の識別名（DN）に基づいて関係を定義します。
- 名前付きの関係は、ターゲット MO の名前に基づいて関係を定義します。

次の図の点線は、いくつかの一般的な MO の関係を示します。

図 *20 : MO* の関係



たとえば、EPG とブリッジドメイン間の点線は、これら 2 つの MO 間の関係を定義します。この図では、EPG（`fvAEPg`）には、ターゲットのブリッジドメイン MO（`fvBD`）の名前が付いた関係 MO（`fvRsBD`）が含まれます。たとえば、実稼働がブリッジドメイン名（`tnFvBDName=production`）である場合、関係の名前は実稼働（`fvRsBdName=production`）になります。

「命名された関係に基づくポリシー解決では、一致する名前を持つ対象の MO が現在のテナントで見つからない場合、ACI ファブリックが共通テナントで解決を試みます。たとえばユーザーのテナント EPG に、存在しないブリッジドメインを対象とした関係 MO が含まれていた場合、システムは共通テナントでその関係の解決を試行します。名前付き関係が現在のテナントまたは共通のテナントで解決できない場合、ACI ファブリックは、デフォルト ポリシーに解決を試行します。デフォルト ポリシーが現在のテナントに存在する場合、それが使用されま

す。デフォルトポリシーが存在しない場合は、ACIファブリックが共通テナント内のデフォルトポリシーを検索します。ブリッジドメイン、VRF、コントラクト（セキュリティポリシー）の命名済み関係はデフォルト値に解決されません。

デフォルト ポリシー

APIC デフォルト ポリシー値の初期値は、スイッチにロードされる具象モデルから取得されます。ファブリックの管理者は、デフォルト ポリシーを変更できます。



警告 デフォルト ポリシーは、変更または削除できません。デフォルト ポリシーを削除すると、ポリシー解決プロセスが異常終了する可能性があります。

ACIファブリックは、そのコア機能の多くにデフォルトのポリシーを含んでいます。デフォルト ポリシーの例には、次のものがあります。

- ブリッジドメイン（common テナント内）
- レイヤ 2 およびレイヤ 3 プロトコル
- ファブリックの初期化、デバイスの検出、およびケーブル接続の検出
- ストーム制御とフラッディング
- 仮想ポートチャネル
- スイッチバッファ内の学習済みエンドポイントのキャッシングとエージングのためのエンドポイント保持
- ループ検出
- モニタリングと統計情報



（注） デフォルトポリシーを使用する構成を実装する際の混乱を避けるために、デフォルトポリシーに加えられた変更を文書化します。デフォルトポリシーを削除する前に、現在または将来の構成がデフォルトポリシーに依存していないことを確認してください。たとえば、デフォルトのファームウェアの更新ポリシーを削除すると、将来のファームウェアの更新に問題が生じる可能性があります。



（注） デフォルトの VRF またはブリッジ ドメインがユーザー テナントに存在し、VRF またはブリッジ ドメインの関連付けがブリッジ ドメイン/EPG で空の場合、インストゥルメンテーション ポリシーが必要です。

ACI ファブリックをアップグレードした場合、デフォルト値が新しいリリースで変更されても既存のポリシーのデフォルト値が保持されます。ノードが APIC に初めて接続されると、ノードはそれ自体をすべてのデフォルト ポリシーをノードにプッシュする APIC に登録します。デフォルト ポリシーでのすべての変更がノードにプッシュされます。

デフォルト ポリシーは、次の複数の目的に使用されます。

- ファブリックの管理者がモデル内のデフォルト値を上書きできます。
- 管理者が明示ポリシーを提供しない場合、APIC はデフォルト ポリシーを適用します。管理者はデフォルト ポリシーを作成でき、管理者が明示ポリシーを提供しない限り、APIC はそのポリシーを使用します。

たとえば、管理者が行うアクションまたは行わないアクションに応じて、APIC は次を実行します。

- 管理者が選択したポートに対して LLDP ポリシーを指定しないため、APIC はポート セレクタに指定されたポートに対しデフォルトの LLDP インターフェイス ポリシーを適用します。
- 管理者がポート セレクタからポートを削除すると、APIC はそのポートにデフォルト ポリシーを適用します。この例では、管理者がポート 1/15 をポート セレクタから削除すると、そのポートはポート チャネルの一部ではなくなり、APIC はそのポートにすべてのデフォルト ポリシーを適用します。

次のシナリオでは、一般的なポリシー解決の動作について説明します。

- 構成は、デフォルト ポリシーを明示的に参照します。現在のテナントにデフォルト ポリシーが存在する場合は、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。
- 構成は、現在のテナントまたはテナント共通に存在しない名前付きポリシー (デフォルトではない) を参照します。現在のテナントにデフォルト ポリシーがある場合は、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。

（注） これは、テナント内のブリッジドメインまたは VRF（プライベートネットワーク）には適用されません。

- 構成はポリシー名を参照しません。現在のテナントにデフォルト ポリシーが存在する場合、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。

（注） ブリッジドメインと VRF の場合、これは、**common** テナントの接続計測ポリシー（`fvConnInstrPol`）に適切なブリッジドメインまたは VRF フラグが設定されている場合にのみ適用されます。これにより、意図しない EPG がテナント **common** サブネットに展開されるのを防ぎます。

ポリシー モデルは、オブジェクトが自身の下に関係管理対象オブジェクト（MO）を持つことによって別のポリシーを使用していることや、関係 MO が名前によってターゲット ポリシーを参照することを指定します。この関係が、名前による明示的なポリシー参照を行わない場合には、システムは、デフォルトと呼ばれるポリシーの解決を試みます。ブリッジドメイン（BD）と VRF（Ctx）は、このルールの例外です。

エンドポイント グループ（EPG）には、`tnFvBDName` というプロパティを持つ BD（`fvRsBd`）との関係があります。これが設定されていない場合（`tnVfBDName=""` ）、接続計測ポリシー（`fvConnInstrPol`）がこの場合の動作を派生させます。このポリシーは、すべての EPG ケース（VMM、ベアメタル、l2ext、l3ext）に適用されます。計測ポリシーは、`bdctrl` プロパティを使用してデフォルトの BD ポリシーを使用するかどうかを制御し、`ctxCtrl` プロパティを使用してデフォルトの VRF（Ctx）ポリシーを使用するかどうかを制御します。次のオプションは両方で同じです。

- *do not instrument*：リーフスイッチはデフォルト ポリシーを使用しません。
- *Instruments-and-no-route*：ポリシーを計測し、ルーティングを有効にしません。
- *Instruments-and-route*：ポリシーを計測し、ルーティングを有効にします。

トランス テナント EPG 通信

あるテナントの EPG は、共有テナントに含まれるコントラクト インターフェイスを介して他のテナントの EPG を伝達できます。コントラクト インターフェイスは、異なるテナントに含まれる EPG によってコントラクト消費インターフェイスとして使用できる MO です。インターフェイスへの関連付けによって、EPG は共有テナントに含まれるコントラクトへのインターフェイスによって表される情報カテゴリを消費します。テナントは第 3 位で定義された単一のコントラクトに参加できます。より厳しいセキュリティ要件は、テナントが互いに完全に独立したままになるようにテナント、コントラクト、情報カテゴリおよびフィルタの方向を定義することで満たすことができます。

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

- インバンド EPG とアウトオブバンド EPG の間でコントラクトが構成されている場合、次の制限が適用されます。
  - 両方の EPG が同じ VRF（コンテキスト）にある必要があります。
  - フィルタは、着信方向にのみ適用されます。

- レイヤ 2 フィルタはサポートされません。
- QoS は、インバンド レイヤ 4 ～ レイヤ 7 のサービスには適用されません。
  - 管理統計は利用できません。
  - CPU 宛てトラフィックの共有サービスはサポートされません。

- プライベートネットワークを適用しない場合、コントラクトがブリッジ間ドメインのトラフィックに必要です。
- プレフィクスベースの EPG はサポートされません。共有サービスはレイヤ 3 外部外側ネットワークではサポートされません。レイヤ 3 外部外側ネットワークによって提供または消費されるコントラクトは、同じレイヤ 3 VRF を共有する EPG により消費または提供される必要があります。
- 共有サービスは、重複しないサブネットのみでサポートされます。共有サービスのサブネットを構成するときは、次のガイドラインに従ってください。
  - 共有サービスプロバイダーのサブネットは、ブリッジドメイン下ではなく EPG 下で構成します。
  - 同じ VRF を共有する EPG で構成されたサブネットは、統合および重複してはなりません。
  - ある VRF からリークされたサブネットは、切り離されている必要があり、重複してはなりません。
  - 複数のコンシューマー ネットワークから VRF に、またはその逆にアドバタイズされたサブネットは、切り離されている必要があり、重複してはなりません。



（注） 2 人のコンシューマーが誤って同じサブネットに構成されている場合は、両方のサブネットの構成を削除してこの状態からリカバリし、その後サブネットを正しく再構成します。

- プロバイダー VRF で共有サービスを `AnyToProv` で構成しないでください。APIC はこの構成を拒否し、障害が発生します。
- 共有サービスを提供している間は、プロバイダーのプライベートネットワークは非強制モードにできません。

タグ

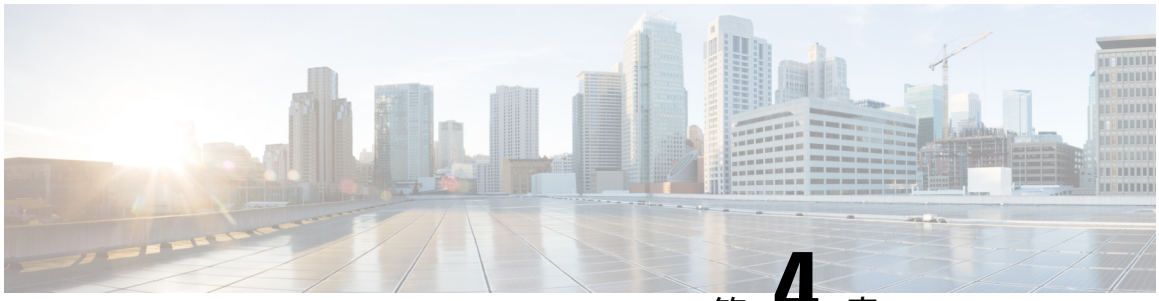
オブジェクト タグにより、API 操作が簡素化されます。API 操作では、識別名（DN）の代わりにタグ名でオブジェクトまたはオブジェクトのグループを参照できます。タグは、タグ付けするアイテムの子オブジェクトです。名前以外に他のプロパティはありません。

オブジェクトのグループに記述名を割り当てる際にタグを使用します。同じタグ名を複数のオブジェクトに割り当てることができます。複数のタグ名を1つのオブジェクトに割り当てることができます。たとえば、すべての Web サーバ EPG へのアクセスを簡単に検索できるようにするには、該当するすべての EPG に Web サーバ タグを割り当てます。ファブリック全体の Web サーバ EPG は、Web サーバ タグを参照することで検索できます。

APIC クォータ管理の構成について

Cisco Application Policy Infrastructure Controller（APIC）リリース 2.3(1) 以降から、テナント管理者が構成できるオブジェクトの数に制限が設けられました。これにより管理者は、特定のテナントの下に、またはテナント全体でグローバルに追加できる管理対象オブジェクトを制限できます。

この機能は、テナントまたはテナントのグループが、リーフごと、またはファブリックごとの ACI の最大数を超えないようにする点で、または利用可能なリソースの大部分を不当に消費して、同じファブリックの他のテナントに影響を及ぼすことがないようにする点で役立ちます。



第 4 章

ファブリック プロビジョニング

この章は、次の内容で構成されています。

- ファブリック プロビジョニング （64 ページ）
- スタートアップ検出と構成 （64 ページ）
- ファブリック インベントリ （66 ページ）
- プロビジョニング （68 ページ）
- 多層アーキテクチャ （68 ページ）
- APIC クラスタの管理 （69 ページ）
- メンテナンス モード （71 ページ）
- ストレッチ ACI ファブリックの設計の概要 （73 ページ）
- ストレッチ ACI ファブリック関連ドキュメント （74 ページ）
- ファブリック ポリシーの概要 （74 ページ）
- ファブリック ポリシーの構成 （75 ページ）
- アクセスポリシーの概要 （76 ページ）
- アクセス ポリシーの構成 （78 ページ）
- Cisco ACI の仮想ポート チャネル （79 ページ）
- ポートチャネルと仮想ポートチャネル アクセス （81 ページ）
- FEX 仮想ポート チャネル （81 ページ）
- ファイバチャネルおよび FCoE （83 ページ）
- 802.1Q トンネル （89 ページ）
- ダイナミック ブレイクアウト ポート （91 ページ）
- ポート プロファイルの設定 （92 ページ）
- ポート プロファイルの設定のまとめ （98 ページ）
- ファブリック ポートの障害検出のためのポート トラッキング ポリシー （105 ページ）
- Epg の Q-で-Q カプセル化のマッピング （106 ページ）
- レイヤ 2 マルチキャスト （107 ページ）
- ファブリック セキュア モード （112 ページ）
- FAST リンク フェールオーバー ポリシーの構成 （112 ページ）
- ポート セキュリティと ACI について （113 ページ）
- ファースト ホップ セキュリティについて （115 ページ）

• MACsec について （116 ページ）
• データ プレーン ポリシング （117 ページ）
• スケジューラ （118 ページ）
• ファームウェア アップグレード （119 ページ）
• **設定ゾーン** （122 ページ）
• 位置情報 （124 ページ）

ファブリック プロビジョニング

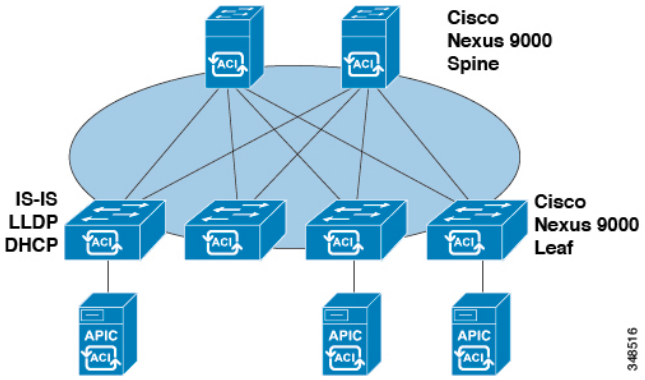
Cisco Application Centric Infrastructure（ACI）の自動化とセルフプロビジョニングにより、従来のスイッチング インフラストラクチャに勝るこれらの操作上のメリットがもたらされます。

- クラスタ化され論理的に一元化されたが物理的に分散されている APIC では、ファブリック全体にポリシー、ブートストラップおよびイメージ管理が提供されます。
- APIC 起動トポロジの自動検出、自動構成、およびインフラストラクチャ アドレッシングでは、次の業界標準のプロトコルが使用されます。Intermediate System-to-Intermediate System（IS-IS）、Link Layer Discovery Protocol（LLDP）、Dynamic Host Configuration Protocol（DHCP）。
- APIC では、シンプルで自動化されたポリシーベースのプロビジョニングとアップグレードのプロセス、および自動イメージ管理が提供されます。
- APIC では、スケーラブルな構成管理が提供されます。ACI のデータセンターは非常に規模が大きい場合があるため、スイッチまたはインターフェイスを個別に構成すると、スクリプトを使用しても十分に拡張しません。APIC ポッド、コントローラ、スイッチ、モジュール、およびインターフェイスセレクタ（すべて、範囲、特定のインスタンス）により、ファブリック全体の対称構成が可能になります。対称構成を適用するには、管理者がインターフェイス構成を単一のポリシー グループに関連付けるスイッチ プロファイルを定義します。その後、個別に構成する必要なく、そのプロファイル内のすべてのインターフェースに迅速に展開されます。

スタートアップ検出と構成

クラスタ化された APIC コントローラでは、ファブリックに DHCP、ブートストラップ構成およびイメージ管理が提供され、自動化されたスタートアップおよびアップグレードが可能になります。次の図は、スタートアップ検出を示します。

図 *21* : スタートアップ検出の構成



Cisco Nexus ACI ファブリック ソフトウェアは ISO イメージとしてバンドルされており、Cisco Integrated Management Controller（CIMC）の KVM インターフェイスを介して Cisco APIC サーバーにインストールできます。Cisco Nexus ACI Software ISO には、Cisco APIC イメージ、リーフ ノードのファームウェア イメージ、スパイン ノードのファームウェア イメージ、デフォルトのファブリック インフラストラクチャ ポリシー、運用に必要なプロトコルが含まれています。

ACI ファブリックのブートストラップ シーケンスは、すべてのスイッチにインストールされている工場出荷時のイメージによってファブリックがブートすると開始されます。ACI ファームウェアと APIC を実行する Cisco Nexus 9000 シリーズ スイッチは、ブート プロセスに予約済みのオーバーレイを使用します。このインフラストラクチャ スペースはスイッチ上でハードコードされています。APICはデフォルトのオーバーレイを通じてリーフに接続できます。または、ローカルで有効な ID を使うことができます。

ACI ファブリックはインフラストラクチャ スペースを使用します。インフラストラクチャ スペースはファブリック内でセキュアに隔離され、ここですべてのトポロジ検出、ファブリック管理、インフラストラクチャ アドレッシングが行われます。ファブリック内の ACI ファブリック管理コミュニケーションは、内部のプライベート IP アドレスを通じてインフラストラクチャ スペース内で行われます。このアドレッシング方式によって、APICはクラスタ内のファブリック ノードおよび他の Cisco APIC コントローラとの通信を行えます。APIC は、Link Layer Discovery Protocol（LLDP）ベースの検出プロセスを使用してクラスタ内の他の Cisco APIC コントローラの IP アドレスとノード情報を検出します。

次に、APIC クラスタ検出プロセスについて説明します。

- Cisco ACI の各 APIC は、内部のプライベート IP アドレスを使用してクラスタ内の ACI ノードおよび他の APIC と通信します。APIC は、LLDP ベースの検出プロセスを通じてクラスタ内の他の APIC コントローラの IP アドレスを検出します。
- APIC は、APIC ID から APIC IP アドレスと APIC の汎用一意識別子（UUID）にマッピングを提供するアプライアンス ベクトル（AV）を維持します。最初に、各 APIC がローカルの IP アドレスで満たされた AV から開始し、他のすべての APIC スロットが不明としてマークされます。

- スイッチの再起動後、リーフのポリシー要素（PE）が APIC からその AV を取得します。スイッチはその後、この AV をすべてのネイバーにアドバタイズし、ローカル AV とネイバーの AV 間の不一致をローカル AV のすべての APIC にレポートします。

このプロセスを使用して、APIC はスイッチを介して ACI の他の APIC コントローラについて学習します。クラスタ内のこれらの新しく検出された APIC コントローラを検証した後、APIC コントローラはローカル AV を更新して、スイッチを新しい AV でプログラミングします。その後、スイッチはこの新しい AV のアドバタイズを開始します。このプロセスは、すべてのスイッチが同一の AV を持ち、すべての APIC コントローラが他のすべての APIC コントローラの IP アドレスを認識するまで継続します。

（注） クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の 1 つ以上の APIC コントローラが正常でない場合は、先に進む前にそのクラスタに変更を加えてその状況を修復してください。また、APIC に追加されたクラスタ コントローラが APIC クラスタ内の他のコントローラと同じファームウェア バージョンを実行しているか確認してください。APIC クラスタを正常に変更するために従う必要があるガイドラインについては、「KB: Cisco ACI APIC クラスタ管理」 の記事を参照してください。

ACI ファブリックは、APIC に直接接続されているリーフノードから順に段階的に起動されます。LLDP およびコントロール プレーン IS-IS コンバージェンスは、このブート プロセスと並行して行われます。ACI ファブリックは LLDP および DHCP ベースのファブリック検出機能を使用して、ファブリック スイッチ ノードの検出、インフラストラクチャの VXLAN トンネル エンドポイント（VTEP）アドレスの割り当て、スイッチへのファームウェアのインストールを自動的に行います。この自動プロセスの前に、Cisco APIC コントローラ上で最小限のブートストラップ構成を行う必要があります。APIC コントローラが接続され、IP アドレスが割り当てられると、Web ブラウザに APIC コントローラのアドレスを入力して APIC GUI にアクセスできます。APIC GUI は HTML5 を実行し、Java をローカルにインストールする必要がなくなります。

ファブリック インベントリ

ポリシーモデルには、すべてのノードおよびインターフェイスを含むファブリックの完全なリアルタイムインベントリが含まれます。このインベントリ機能により、プロビジョニング、トラブルシューティング、監査、およびモニタリングを自動化できます。

Cisco ACI のファブリック スイッチの場合は、ファブリック メンバーシップのノードインベントリに、ノード ID、シリアル番号および名前を識別するポリシーが含まれます。サードパーティのノードは、管理対象外のファブリック ノードとして記録されます。Cisco ACI のスイッチは自動的に検出することができ、またはポリシー情報をインポートできます。ポリシーモデルは、ファブリック メンバー ノードのステータス情報も保持します。

ノードのステータス	条件
不明	ポリシーが存在しません。すべてのノードにはポリシーが必要で、ポリシーがない場合はメンバー ノードのステータスは不明となります。
検出中（Discovering）	ノードが検出され、ホスト トラフィックの応答待ちであることを示す一時的な状態です。
未検出	ノードにはポリシーがありますが、ファブリックで提示されたことはありません。
Unsupported	ノードは Cisco のスイッチですが、サポートされていません。たとえば、ファームウェアのバージョンがACIのファブリックと互換性がありません。
廃止	ノードはポリシーとして検出されましたが、ユーザがこれを無効にしました。ノードを再び有効化することができます。 （注） リーフスイッチを廃止するときにワイプ オプションを指定すると、APIC はリーフスイッチと APIC の両方のリーフスイッチ構成すべての削除を試みます。リーフスイッチに到達できない場合は、APIC のみがクリーニングされます。この場合、ユーザはリーフスイッチをリセットして手動でワイプする必要があります。
非アクティブ	ノードが到達不能です。検出されましたが、現在アクセスできません。たとえば、電源がオフになっているか、ケーブルが切断されている可能性があります。
アクティブ	ノードはファブリックのアクティブ メンバーです。

無効のインターフェイスは、管理者によってブラックリスト化されたものや、APIC が異常を検出するため取り除かれたものである可能性があります。リンク ステート異常の例を次に示します。

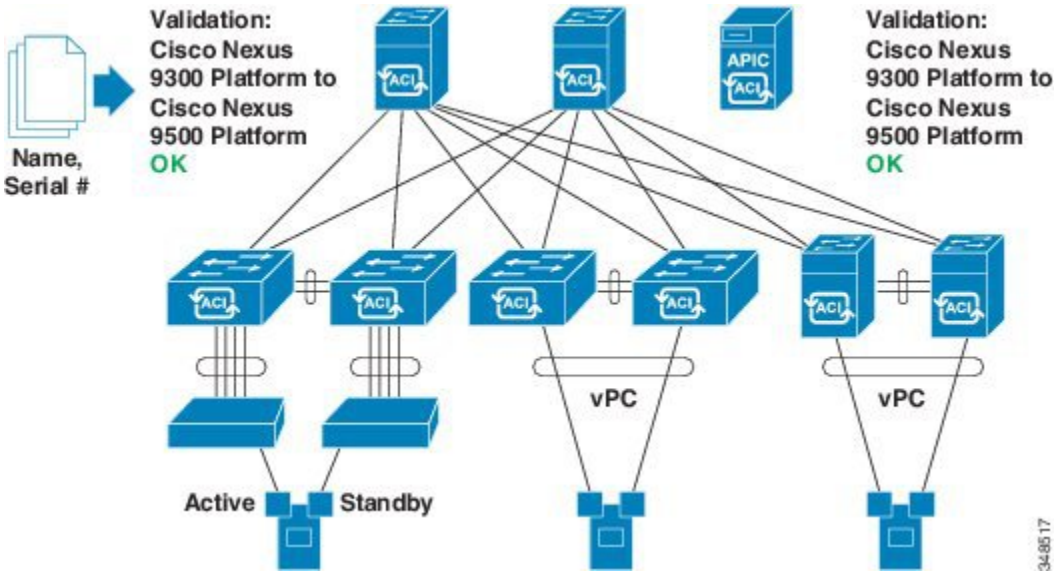
- スパインに接続されているスパイン、リーフに接続されているリーフ、リーフ アクセス ポートに接続されているスパイン、非 ACI ノードに接続されているスパイン、または非 ACI デバイスに接続されているリーフ ファブリック ポートなどの配線の不一致。
- ファブリック名の不一致。ファブリック名は各 ACI ノードに保存されます。工場出荷時のデフォルト状態に戻して再設定されることなくノードが別のファブリックに移動される場合、ファブリック名が保持されます。
- UUID の不一致によって APIC がノードを無効化します。

（注） 管理者が APIC を使用してスパインのすべてのリーフ ノードを無効化する場合、スパインへのアクセスを回復するためにスパインの再起動が必要です。

プロビジョニング

APIC プロビジョニング方式により、適切な接続を通じて ACI ファブリックが自動的に起動します。次の図は、ファブリックのプロビジョニングを示します。

図 *22 :* ファブリック プロビジョニング



Link Layer Discovery Protocol（LLDP）ディスカバリが隣接するすべての接続を動的に学習した後、これらの接続は緩やかなルールに照らし合わせて検証できます。たとえば、「LEAF can connect to only SPINE-L1-*」または「SPINE-L1-* can connect to SPINE-L2-* or LEAF」などと指定できます。ルールの不一致が発生すると、障害が発生し、リーフが別のリーフまたはスパインに接続されたスパインに接続できないため、接続がブロックされます。また、接続に注意が必要であることを示すアラームが作成されます。Cisco ACI ファブリックの管理者は、テキスト ファイルからすべてのファブリック ノードの名前とシリアル番号を APIC にインポートすることができ、または APIC GUI、コマンド ライン インターフェイス（CLI）または API を使用してシリアル番号を自動的に検出し、名前をノードに割り当てることをファブリックに許可できます。APIC は、SNMP 経由で検出可能です。次の asysobjectId があります。

```
ciscoACIController OBJECT IDENTIFIER ::= { ciscoProducts 2238 }
```

多層アーキテクチャ

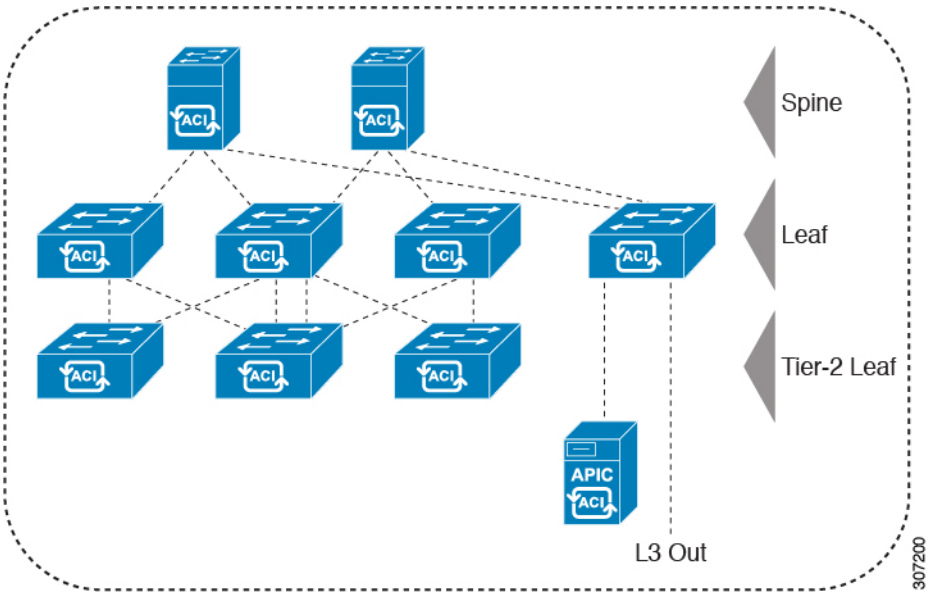
3 階層コア集約アクセス アーキテクチャは、データ センター ネットワーク トポロジで共通です。Cisco APIC リリース 4.1(1) 時点で、コア集約アクセス アーキテクチャに対応するマルチ階層 ACI ファブリック トポロジを作成するため、ラックスペースや配線などコストが高いコンポーネントのアップグレードの必要性を軽減できます。階層 2 リーフ レイヤーを追加することで、このトポロジが可能になります。階層 2 リーフ レイヤーは、ダウンリンク ポート上のホ

ストまたはサーバへの接続、およびアップリンク ポート上のリーフ レイヤー (集約) への接続をサポートします。

マルチ階層トポロジでは、リーフ スイッチには最初にスパイン スイッチへのアップリンク接続と、階層 2 リーフ スイッチへのダウンリンク接続があります。トポロジ全体を ACI ファブリックにするには、階層 2 リーフ ファブリック ポートに接続されているリーフ スイッチ上のすべてのポートが、ファブリック ポートとして設定されている必要があります (まだデフォルトのファブリック ポートを使用していない場合)。APIC が階層 2 リーフ スイッチを検出した後、階層 2 リーフ上のダウンリンク ポートをファブリック ポートに変更し、中間レイヤ リーフ上のアップリンク ポートに接続できます。

次の図は、マルチ階層ファブリック トポロジの例を示します。

図 *23*: マルチ階層ファブリック トポロジ例



上の図のトポロジがリーフ集約レイヤに接続している Cisco APIC および L3Out/EPG を示しており、階層 2 リーフ アクセス レイヤは APIC および L3Out/EPG への接続もサポートしています。

APIC クラスタの管理

クラスタ管理の注意事項

Cisco Application Policy Infrastructure Controller (APIC) クラスタは複数の Cisco APIC コントローラで構成され、Cisco Application Centric Infrastructure（ACI）ファブリックに対する統合されたリアルタイム モニタリング、診断および構成管理機能がオペレータに提供されます。最適なシステム パフォーマンスが得られるように、Cisco APIC クラスタを変更する場合は次のガイドラインに使用してください：

- クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の 1 つ以上の Cisco APIC のヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。また、Cisco APICに追加されたクラスタ コントローラが Cisco APIC クラスタ内の他のコントローラと同じファームウェア バージョンを実行しているか確認してください。
- クラスタ内には少なくとも3つのアクティブなCisco APICがあり、追加のスタンバイ Cisco APIC があることを推奨します。 Cisco APIC クラスタには、3 ～ 7 個のアクティブな Cisco APICを含めることができます。展開に必要なアクティブな Cisco APIC の数を確認するには、『検証済みスケーラビリティ ガイド』を参照してください。
- 現在クラスタにない Cisco APIC からのクラスタ情報は無視します。正確なクラスタ情報ではありません。
- クラスタ スロットにはCisco APIC `ChassisID` を含みます。スロットを設定すると、割り当てられたシャーシ `ID` の Cisco APIC を解放するまでそのスロットは使用できません。
- Cisco APIC ファームウェア アップグレードが進行中の場合は、それが完了し、クラスタが完全に適合するまでクラスタへの他の変更はしないでください。
- Cisco APIC を移動する際は、最初に正常なクラスタがあることを確認します。Cisco APIC クラスタの状態を確認するには、後にシャットダウンするCisco APICを選択します。Cisco APICをシャットダウンした後、Cisco APICに移動し、再接続して、電源を入れます。GUI から、クラスタ内のすべてのコントローラが完全に適合状態に戻すことを確認します。



（注） 一度に 1 つの Cisco APIC のみ移動します。

- 一連のリーフ スイッチに接続されている Cisco APIC を別のリーフ スイッチのセットに移動する場合、またはCisco APICを同じリーフ スイッチ内の別のポートに移動する場合は、まずクラスタが正常であることを確認します。Cisco APICクラスタの状態を確認したら、移動してクラスタからデコミッションする Cisco APIC を選択します。Cisco APIC がデコミッションされたら、 Cisco APIC を移動してコミッションします。
- Cisco APICクラスタを設定する前に、すべてのCisco APICのパフォーマンスが同じファームウェアバージョンを実行していることを確認します。異なるバージョンを実行してCisco APIC のパフォーマンスの最初のクラスタ リングはサポートされていない動作し、クラスタ内の問題が発生する可能性があります。
- 他のオブジェクトとは異なり、ログ レコード オブジェクトは、いずれかの Cisco APIC のデータベースの1つのシャードにのみ保存されます。これらのオブジェクトは、使用停止またはCisco APIC交換すると永久に失われます。
- Cisco APICをデコミッションすると、Cisco APIC に保存されていたすべての障害、イベント、および監査ログ履歴が失われます。すべての Cisco APIC を交換すると、すべてのログ履歴が失われます。Cisco APICを移行する前に、ログ履歴を手動でバックアップすることをお勧めします。

Cold Standby について (Cisco APIC クラスタ用)

Cold Standby 機能 Cisco Application Policy Infrastructure Controller(APIC クラスタ用) を使用すれば、クラスタ内の Cisco APIC をアクティブ/スタンバイモードで運用できます。Cisco APIC クラスタでは、指定されたアクティブ状態の Cisco APIC は負荷を共有し、指定されたスタンバイ状態の Cisco APIC はアクティブなクラスタ内の任意の Cisco APIC の置き換えとして動作することができます。

管理者ユーザーとして、Cisco APIC が初めて起動したときに Cold Standby 機能をセット アップできます。クラスタ内には少なくとも 3 基のアクティブ状態の Cisco APIC があり、1 基以上のスタンバイ状態の Cisco APIC があるようにすることを推奨します。管理者ユーザーとして、アクティブな Cisco APIC をスタンバイ状態の Cisco APIC で置き換えるには、切り替えを開始できます。

メンテナンス モード

メンテナンス モードを使用する際に理解に役立つ用語を紹介します。

- **メンテナンス モード**：デバッグ目的でユーザー トラフィックからスイッチを分離するために使用されます。**ファブリック** インベントリ ファブリック メンバーシップ**にある APIC GUI の** [ファブリック メンバーシップ（Fabric Membership）] > **ページの [メンテナンス（GIR）（Maintenance（GIR））]フィールドを有効にすることで、スイッチを メンテナンス モード**>**にできます**（スイッチを右クリックして**[メンテナンス（GIR）Maintenance（GIR）]** を選択します）。

  スイッチを**メンテナンス モード**にすると、そのスイッチは動作可能な ACI ファブリック インフラストラクチャの一部とは見なされず、通常の APIC 通信は受け入れられません。

メンテナンスモード使用してスイッチを正常に取り出し、そのスイッチをネットワークから分離して、デバッグ操作を実行することができます。スイッチは、最小限のトラフィックの中断だけで、通常の転送パスから取り外されます。

正常に削除、外部のすべてのプロトコルが適切に電源を切るファブリック プロトコル (IS-IS) を除くと、スイッチは、ネットワークから切り離します。メンテナンスモード時に、最大メトリックは IS-IS 内でアドバタイズ、 Cisco Application Centric Infrastructure (Cisco ACI) ファブリックおよびそのため、メンテナンス モードがスパイン スイッチからのトラフィックをひく点されません。さらに、スイッチの前面パネルのすべてのインターフェイスが、スイッチ ファブリック インターフェイスを除いてシャット ダウンされます。デバッグ操作後にスイッチを完全動作（通常）モードに戻すには、スイッチをリコミッショニングさせる必要があります。この操作により、スイッチのステートレス リロードがトリガーされます。

グレースフルの挿入で、スイッチは自動的にデコミッショニング、再起動、およびリコミッショニングされます。リコミッショニングが完了したら、外部のすべてのプロトコルを復元し、IS-IS で最大のメトリックは 10 分後にリセットされます。

次のプロトコルがサポートされています。

- Border Gateway Protocol（BGP）

- Enhanced Interior Gateway Routing Protocol（EIGRP）
- Intermediate System-to-Intermediate System（IS-IS）
- Open Shortest Path First（OSPF）
- リンク集約制御プロトコル（LACP）

プロトコルに依存しないマルチキャスト (PIM) はサポートされていません。

特記事項

- 境界リーフ スイッチに静的ルートがあり、メンテナンス モードがある場合、境界リーフ スイッチからのルートは ACI ファブリックにあるルーティング テーブルから削除されない可能性があり、ルーティングの問題が発生します。

  この問題を回避するには、次のいずれかを実行します。

  - その他の境界リーフ スイッチで同じ管理ディスタンスを持つ同じ静的ルートを設定するか、
  - 静的ルートの次のホップへの到達性を追跡するため IP SLA または BFD を使用します

- イーサネット ポート モジュールでは、インターフェイスを増殖停止、スイッチは、メンテナンス モードでは、通知に関連します。その結果、リモート スイッチを再起動するか、またはこの時間中にファブリック リンクかを調べますは、ファブリック リンクはありません確立した後で、スイッチがリブート手動でない限り (を使用して、 **acidiag タッチ クリーン** コマンド)、廃棄、および recommissioned。
- スイッチがメンテナンス モード中の場合、スイッチの CLI「show」コマンドでは、前面パネル ポートがアップ状態であり、BGP プロトコルがアップ状態かつ実行中であることを示します。インターフェイスは実際にシャットダウンされ、BGP のその他すべての隣接関係がダウンしますが、表示されているアクティブ状態でデバッグが可能です。
- マルチポッド/マルチサイトの場合、ノードをファブリックに戻すときのトラフィックの中断を最小限に抑えるために、 **再配布されるルートの IS-IS メトリックを** 63 未満に設定する必要があります。**再配布されるルートの IS-IS メトリック**を設定するには、**[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポッド ポリシー（Pod Policies）] > [IS-IS ポリシー（IS-IS Policy）]**を選択します 。
- 既存の登場させには、すべてのレイヤ 3 トラフィック迂回がサポートされています。LACP でレイヤ 2 のすべてのトラフィックは、冗長ノードを迂回も。ノードは、メンテナンス モードに入ります、されるとすぐに、ノードで実行されている LACP は、不要になった集約できるようにポート チャネルの一部としてネイバーを通知します。すべてのトラフィックは vPC ピア ノードを迂回します。
- メンテナンス モードでは、次の操作は許可されません。
  - **アップグレード**：ネットワークを新しいバージョンにアップグレードすること
  - **ステートフル リロード**：GIR ノードまたはその接続されたピアの再起動

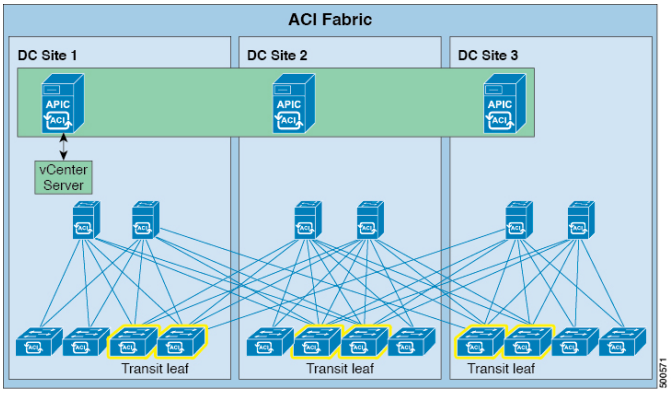
- **ステートレス リロード**：GIR ノードまたはその接続されたピアのクリーン設定または電源再投入による再起動
- **リンク操作**：GIR ノードまたはそのピアノードでのシャットダウン/非シャットダウンまたは光ファイバの OIR（オンラインでの挿入または取り外し）
- **構成変更**：設定変更（クリーン構成、インポート、スナップショット ロールバックなど）
- **ハードウェアの変更**：ハードウェアの変更（FRU または RMA の追加、交換、削除など）

ストレッチ ACI ファブリックの設計の概要

ストレッチ ACI ファブリックは、複数の場所に分散された ACI リーフおよびスパイン スイッチを接続する部分的にメッシュ化された設計です。通常、ACI ファブリックの実装は、フルメッシュ設計がファブリック内の各リーフスイッチを各スパイン スイッチに接続する単一のサイトであり、最高のスループットとコンバージェンスが得られます。マルチサイトのシナリオでは、フルメッシュ接続が不可能であるか、コストがかかりすぎる可能性があります。複数のサイト、建物、または部屋が、十分なファイバ接続ではサービスを提供できない距離にまたがる場合や、サイト全体の各リーフスイッチを各スパイン スイッチに接続するにはコストがかかりすぎる場合があります。

次の図にストレッチ ファブリック トポロジを示します。

図 *24 : ACI* ストレッチ ファブリック トポロジ



ストレッチ ファブリックは単一の ACI ファブリックです。サイトには 1 つの管理ドメインおよび 1 つの可用性ゾーンがあります。管理者は、サイトを 1 つのエンティティとして管理できます。 APIC コントローラ ノードで行われた構成変更は、サイト全体のデバイスに適用されます。ストレッチされた ACI ファブリックは、サイト間でのライブ VM 移行機能を保持します。ACI ストレッチ ファブリックの設計は検証されており、相互接続された最大 3 つのサイトでサポートされています。

ACI ストレッチ ファブリックは、基本的に、さまざまな場所に広がる「ストレッチ ポッド」を表します。ACI マルチポッド アーキテクチャを備えた ACI リリース 2.0(1) 以降、さまざまな場所に分散して ACI ファブリックを展開するための、より堅牢で回復力のある（推奨される）方法が提供されています。詳細については、次のホワイトペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737855.html

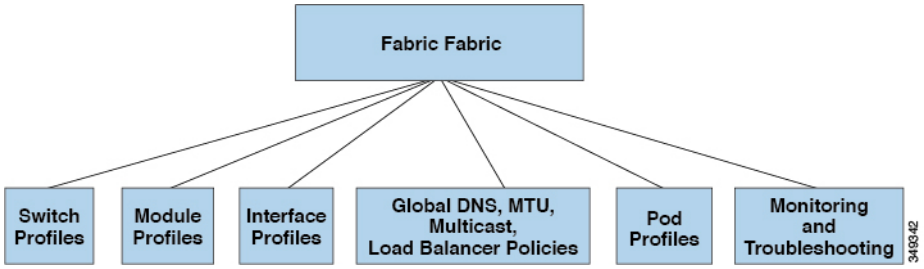
ストレッチ ACI ファブリック関連ドキュメント

KB ストレッチ ACI ファブリック設計の概要 テクニカル ノートは、トラフィック フロー、APIC クラスタの冗長性、および複数のサイトにまたがる ACI ファブリックを実装するための運用上の考慮事項に関する設計ガイドラインを提供します。

ファブリック ポリシーの概要

ファブリック ポリシーは、内部のファブリック インターフェイスの操作を管理し、スパインおよびリーフスイッチを接続するさまざまな機能、プロトコル、およびインターフェイスの構成を可能にします。ファブリックの管理者権限を持つ管理者は、要件に応じて新しいファブリック ポリシーを作成できます。APIC では、管理者はファブリック ポリシーを適用するポッド、スイッチおよびインターフェイスを選択できます。次の図は、ファブリックのポリシーモデルの概要を示します。

図 *25 :* ファブリック ポリシーの概要



ファブリック ポリシーは、次のカテゴリにグループ化されます。

- スイッチ プロファイルは、構成するスイッチとスイッチの構成ポリシーを指定します。
- モジュール プロファイルは、構成するスパイン スイッチ モジュールとスパイン スイッチの構成ポリシーを指定します。
- インターフェイス プロファイルは、構成するファブリック インターフェイスとインターフェイスの構成ポリシーを指定します。
- グローバルポリシーは、DNS、ファブリック MTU のデフォルト、マルチキャスト ツリー、およびファブリック全体で使用するロードバランサの構成を指定します。

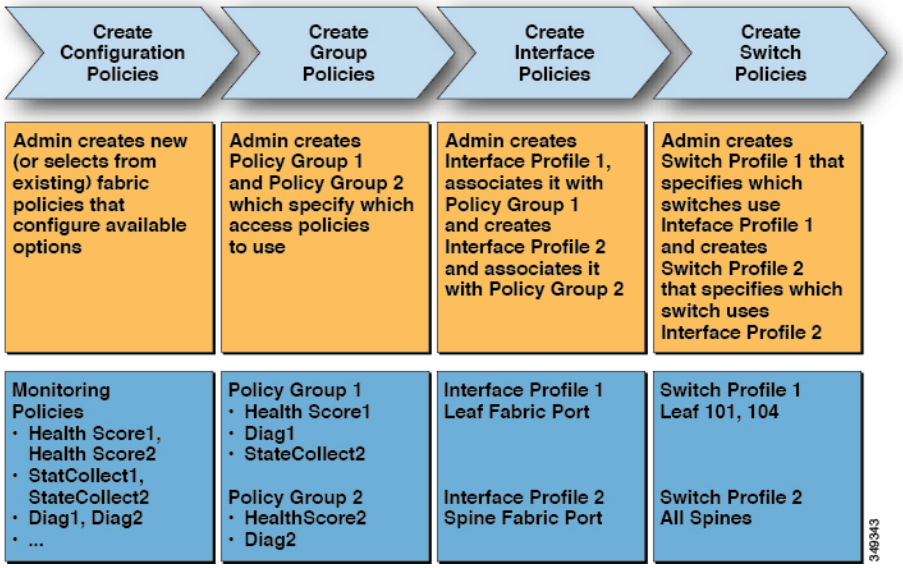
- ポッドプロファイルは、日付と時刻、SNMP、Council of Oracle Protocol（COOP）、IS-IS、および Border Gateway Protocol（BGP）ルート リフレクタ ポリシーを指定します。
- モニタリングおよびトラブルシューティングのポリシーは、モニタする対象、しきい値、障害とログの処理方法、および診断方法を指定します。

ファブリック ポリシーの構成

ファブリック ポリシーは、スパインおよびリーフスイッチに接続するインターフェイスを構成します。ファブリック ポリシーは、モニタリング（統計の収集および統計のエクスポート）、トラブルシューティング（オンデマンド診断と SPAN）、IS-IS、Council of Oracle Protocol（COOP）、SNMP、ボーダーゲートウェイ プロトコル（BGP）のルート リフレクタ、ドメインネームシステム（DNS）、またはNetwork Time Protocol（NTP）などの機能を有効にできます。

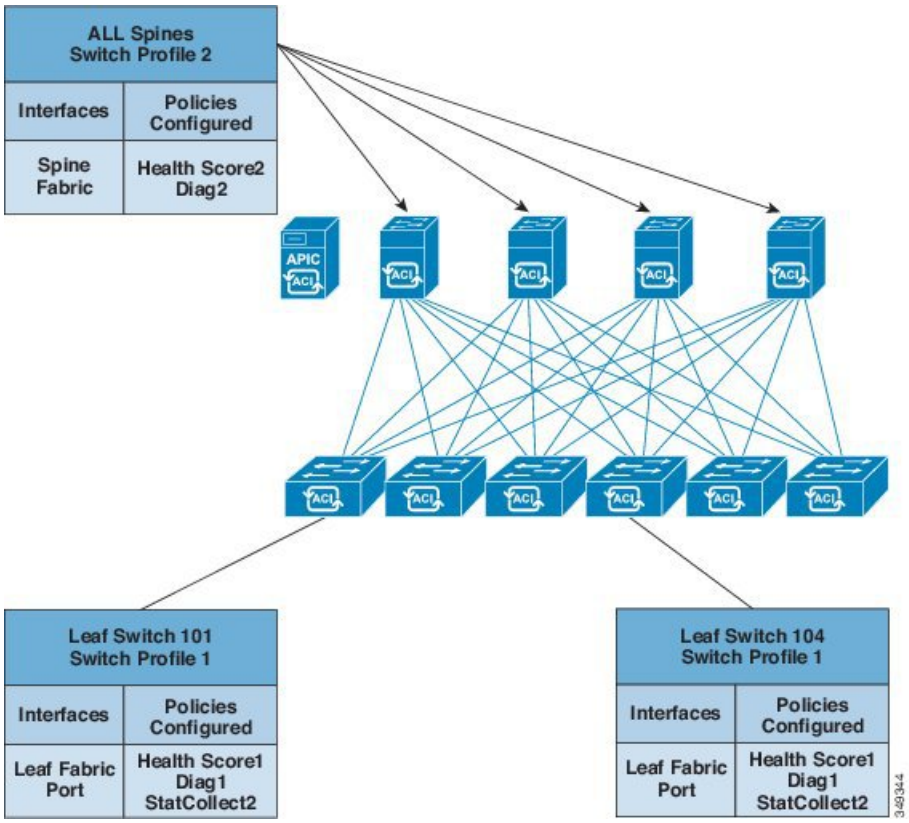
ファブリック全体で構成を適用するには、管理者がポリシーの定義済みグループをスイッチ上のインターフェイスに単一段階で関連付けます。このようにして、ファブリック上の多数のインターフェイスを一度に構成できます。1 個のポートを一度に構成することはスケーラブルではありません。次の図は、ACI ファブリックを構成するプロセスがどのように動作するかを示します。

図 *26 :* ファブリック ポリシーの構成プロセス



次の図は、ACI ファブリックにスイッチ プロファイル 1 およびスイッチ プロファイル 2 を適用した結果を示します。

図 *27:* ファブリック スイッチ ポリシーの適用



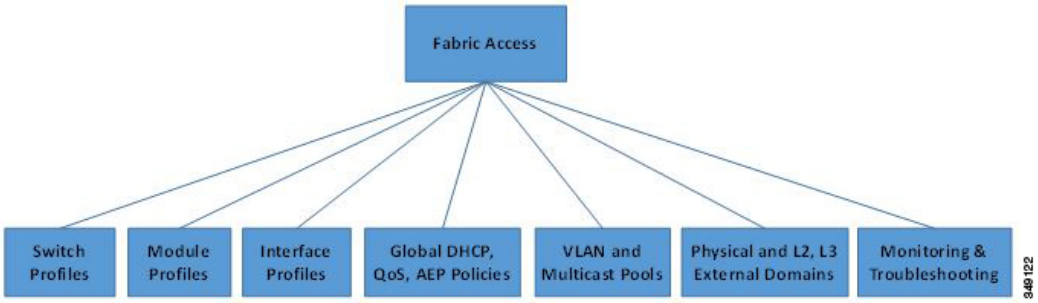
インフラストラクチャと範囲を組み合わせることにより、管理者はスケーラブルな方法でファブリック構成を管理することができます。これらの設定は、REST API、CLI、またはGUIを使用して実行できます。GUI 内の [クイック スタート インターフェイス（Quick Start Interface）] 構成ウィザードでは、そのようなポリシーの実行に必要な基盤となるオブジェクトが自動的に作成されます。

アクセスポリシーの概要

アクセスポリシーは、仮想マシン コントローラおよびハイパーバイザなどのデバイスに接続する外向きインターフェイス、ホスト、ネットワーク接続ストレージ、ルータ、または Fabric Extender（FEX; ファブリックエクステンダ）インターフェイスを構成します。アクセスポリシーにより、ポートチャネルおよび仮想ポートチャネル、Link Layer Discovery Protocol（LLDP）、Cisco Discovery Protocol（CDP）、または Link Aggregation Control Protocol（LACP）などのプロトコル、および統計収集、監視、および診断などの機能の構成が可能になります。

次の図は、アクセスポリシー モデルの概要を示します。

図 *28* : アクセスポリシー モデルの概要



アクセスポリシーは、次のカテゴリにグループ化されます。

- スイッチ プロファイルは、構成するスイッチとスイッチの構成ポリシーを指定します。
- モジュール プロファイルは、構成するリーフスイッチのアクセスカードおよびアクセス モジュールとリーフスイッチの構成ポリシーを指定します。
- インターフェイス プロファイルは、構成するアクセス インターフェイスとインターフェイスの構成ポリシーを指定します。
- グローバル ポリシーにより、ファブリック全体に使用できる DHCP、QoS、および接続可能アクセス エンティティ（AEP）のプロファイル機能の構成が可能になります。AEP プロファイルは、リーフ ポートの大規模セットでハイパーバイザ ポリシーを展開するためのテンプレートを提供し、仮想マシン管理（VMM）のドメインと物理ネットワーク インフラストラクチャを関連付けます。また、レイヤ 2 およびレイヤ 3 の外部ネットワークの接続にも必要となります。
- プールは、VLAN、VXLAN およびマルチキャストアドレス プールを指定します。プールは共有リソースで、VMM などの複数のドメインおよびレイヤ 4 ～ レイヤ 7 のサービスで消費できます。プールは、さまざまなトラフィックのカプセル化 ID を表します（たとえば、VLAN ID、VNID、マルチキャストアドレスなど）。
- 物理および外部ドメイン ポリシーには、次のものが含まれます。
  - 外部ブリッジドメインのレイヤ2ドメインプロファイルには、ファブリックに接続されたブリッジ レイヤ 2 ネットワークが使用するポートおよび VLAN の仕様が含まれます。
  - 外部ルーテッド ドメインのレイヤ 3 ドメイン プロファイルには、ファブリックに接続されたルーテッド レイヤ 3 ネットワークが使用するポートおよび VLAN の仕様が含まれます。
  - 物理ドメイン ポリシーには、テナントまたはエンドポイント グループで使用されるポートや VLAN などの物理インフラストラクチャの仕様が含まれます。
- モニタリングおよびトラブルシューティングのポリシーは、モニタする対象、しきい値、障害とログの処理方法、および診断方法を指定します。

アクセス ポリシーの構成

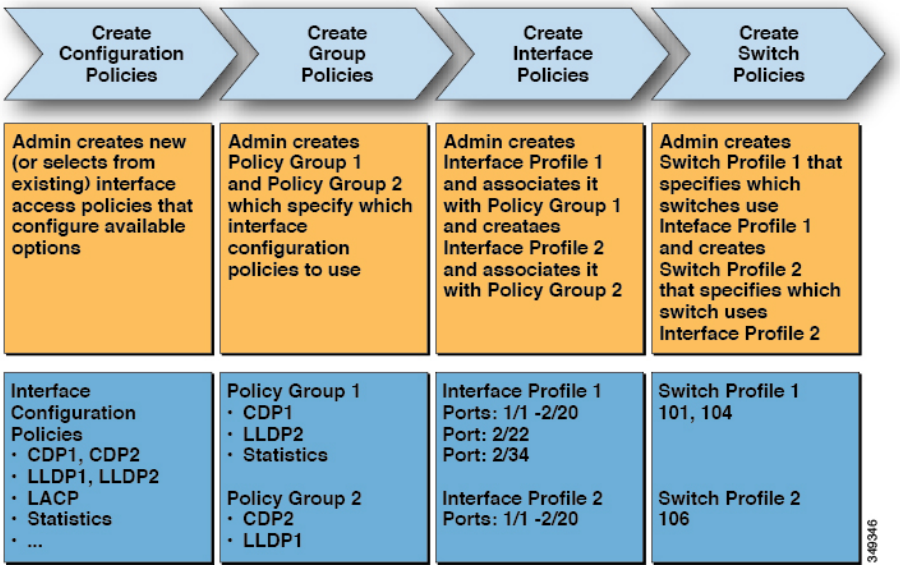
アクセスポリシーは、スパインスイッチに接続していない外向きインターフェイスを構成します。外向きインターフェイスは、仮想マシンコントローラなどの外部デバイス、ハイパーバイザ、ホスト、ルータ、または Fabric Extender（FEX; ファブリックエクステンダ）と接続します。アクセスポリシーにより、管理者はポートチャネルおよび仮想ポートチャネル、LLDP、CDP、LACP などのプロトコル、モニタリングや診断などの機能を設定することができます。

スイッチインターフェイス用のサンプル XML ポリシー、ポートチャネル、仮想ポートチャネル、およびインターフェイスの変更のスピードについては、『*Cisco APIC Rest API* 構成ガイド』に記載されています。

（注） テナントネットワークポリシーがファブリックのアクセスポリシーと別に構成される一方で、依存する基盤となるアクセスポリシーが整わないとテナントポリシーはアクティブ化されません。

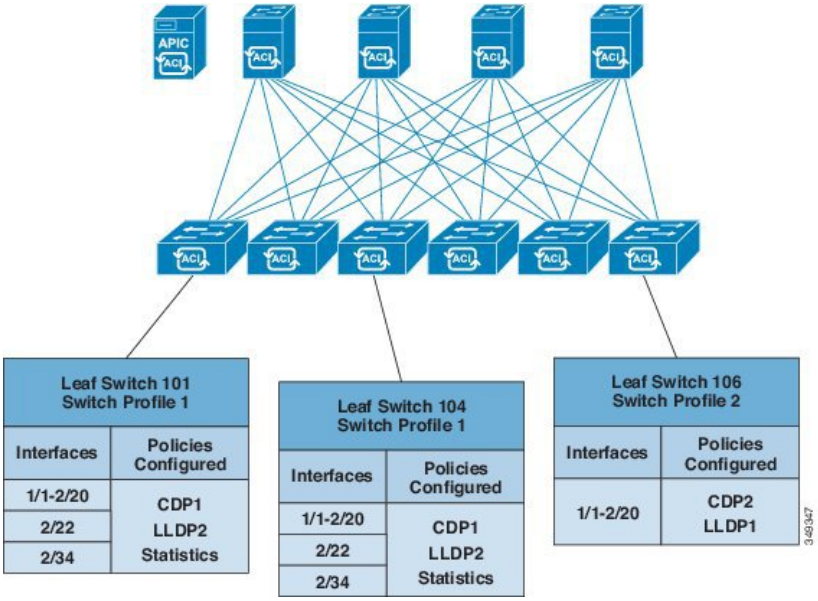
潜在的に多数のスイッチ間で構成を適用するためには、管理者は、単一のポリシーグループのインターフェイス構成を関連付けるスイッチ プロファイルを定義します。このようにして、ファブリック上の多数のインターフェイスを一度に構成できます。スイッチ プロファイルには、複数のスイッチに対する対称構成や一意の特殊用途構成を含めることができます。次の図は、ACI ファブリックへのアクセス構成のプロセスを示します。

図 *29*：アクセスポリシーの構成プロセス



次の図は、ACI ファブリックにスイッチ プロファイル 1 およびスイッチ プロファイル 2 を適用した結果を示します。

図 *30 :* アクセススイッチ ポリシーの適用

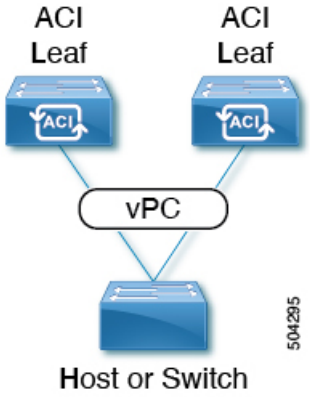


インフラストラクチャと範囲を組み合わせることにより、管理者はスケーラブルな方法でファブリック構成を管理することができます。これらの設定は、REST API、CLI、またはGUIを使用して実行できます。GUI内の[クイック スタート インターフェイス（Quick Start Interface）]、[PC]、[VPC 構成（VPC Configuration）] ウィザードでは、そのようなポリシーの実行に必要な基盤となるオブジェクトが自動的に作成されます。

Cisco ACI の仮想ポート チャネル

仮想ポートチャネル（vPC）によって、2つの異なるCisco Application Centric Infrastructure（ACI）リーフノードに物理的に接続されたリンクを、リンク集約テクノロジーをサポートするネットワークスイッチ、サーバー、他のネットワークデバイスなどから単一のポートチャネル（PC）に見えるようにすることができます。vPC は、vPC のピア スイッチとして指定された 2 台の Cisco ACI リーフ スイッチから構成されます。Of the vPC peers, one is primary and one is secondary. The system formed by the switches is referred to as a vPC domain.

図 *31 : vPC* ドメイン



次の動作は、Cisco ACI vPC 実装に固有です。

- vPC ピア間に専用ピア リンクはありません。代わりに、ファブリック自体がマルチシャーシ トランキング（MCT）として機能します。
- ピア到達可能性プロトコル：Cisco ACI は、Cisco Fabric Services（CFS）の代わりに Zero Message Queue（ZMQ）を使用します。
  - ZMQ は、トランスポートとして TCP を使用するオープンソースの高性能メッセージング ライブラリです。
  - このライブラリは、スイッチ上では libzmq としてパッケージ化されており、vPC ピアと通信する必要がある各アプリケーションにリンクされています。
- ピアの到達可能性は、物理ピア リンクを使用して処理されません。代わりに、ルーティング トリガーを使用してピアの到達可能性を検出します。
  - vPC マネージャは、ピア ルート通知のためにユニキャスト ルーティング情報ベース（URIB）に登録します。
  - IS-IS がピアへのルートを検出すると、URIB は vPC マネージャに通知します。vPC マネージャは、ピアとの ZMQ ソケットを開こうとします。
  - ピア ルートが IS-IS によって取り消されると、URIB は vPC マネージャに再び通知し、vPC マネージャは MCT リンクをダウンします。
- 2 つのリーフ スイッチ間に vPC ドメインを作成する場合は、以下のハードウェア モデルの制限が適用されます。
  - 第 1 世代のスイッチは、第 1 世代の他のスイッチとのみ互換性があります。これらのスイッチ モデルは、スイッチ名の末尾に「EX」、「FX」、「FX2」、「GX」またはそれ以降のサフィックスがないことで識別できます。たとえば、N9K-9312TX という名前などです。
  - 第 2 世代以降のスイッチは、vPC ドメインで混在させることができます。これらのスイッチ モデルは、スイッチ名の末尾に「EX」、「FX」、「FX2」、「GX」またはそ

れ以降のサフィックスが付いていることで識別できます。たとえば、N9K-93108TC-EX や N9K-9348GC-FXP という名前などです。

互換性のある vPC スイッチ ペアの例：

- N9K-C9312TX および N9K-C9312TX
- N9K-C93108TC-EX および N9K-C9348GC-FXP
- N9K-C93180TC-FX and N9K-C93180YC-FX
- N9K-C93180YC-FX および N9K-C93180YC-FX

互換性のない vPC スイッチ ペアの例：

- N9K-C9312TX および N9K-C93108TC-EX
- N9K-C9312TX および N9K-C93180YC-FX

- ポートチャネルおよび仮想ポートチャネルは、LACP の有無にかかわらず構成できます。

  ポートを LACP 付きで構成したのに、ポートがピアから LACP PDU を受信しなかった場合、LACP はポートを中断状態に設定します。これによって、サーバーの中には起動に失敗するものがあります。LACP がポートを論理的 up 状態にすることを必要としているからです。**LACP suspend individual** を無効にして、動作を個々の使用に合わせて調整できます。そのためには、vPC ポリシー グループでポート チャネル ポリシーを作成し、モードを LACP アクティブに設定してから、**Suspend Individual Port** を削除します。これ以後、vPC 内のポートはアクティブなまま、LACP パケットを送信し続けます。

- ARP ネゴシエーションに基づく、仮想ポート チャネル間での適応型ロード バランシング（ALB）は、Cisco ACI ではサポートされていません。

ポートチャネルと仮想ポートチャネル アクセス

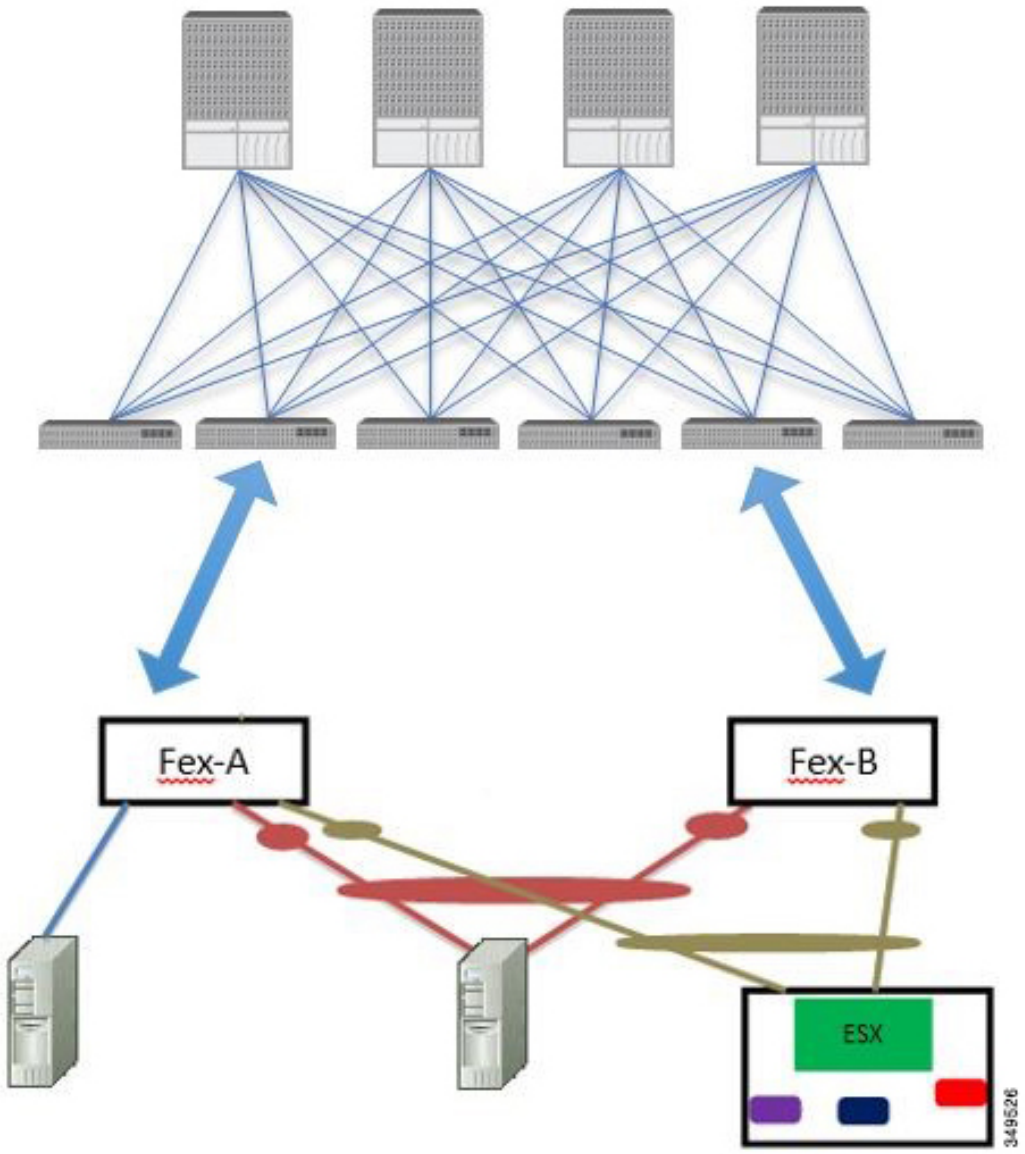
アクセスポリシーにより、管理者はポートチャネルと仮想ポートチャネルを構成できます。スイッチ インターフェイス用のサンプル XML ポリシー、ポートチャネル、仮想ポートチャネル、およびインターフェイスの変更のスピードについては、『*Cisco APIC Rest API* 構成ガイド』に記載されています。

FEX 仮想ポート チャネル

ACI ファブリックは、FEX ストレート vPC とも呼ばれる Cisco Fabric Extender（FEX）サーバ側仮想ポート チャネル（vPC）をサポートします。

（注） 2 つのリーフ スイッチ間に vPC ドメインを作成する場合は、同じ vPC ペアの一部になる 2 つのリーフ スイッチのハードウェアに互換性があることを確認します。詳細については、Cisco ACI の仮想ポート チャネル （79 ページ）を参照してください。

図 *32 :* サポートされる *FEX vPC* トポロジ



サポートされる FEX vPC ポート チャネル トポロジは次のとおりです。

- FEX の背後にある VTEP および非 VTEP の両方のハイパーバイザ。

- ACI ファブリックに接続された 2 つの FEX に接続された仮想スイッチ（AVS や VDS など）（物理 FEX ポートに直接接続された vPC はサポートされません。vP Cはポート チャネルでのみサポートされます）。



（注） GARP を、同じ FEX 上の異なるインターフェイスで IP から MAC バインディングへ変更する際の通知プロトコルとして使用する場合、ブリッジ ドメインは **[ARP フラッディング (ARP Flooding)]** に設定し、**[EP 移動検出モード (EP Mode Detection Mode)]** : **[GARP ベースの検出 (GARP-based Detection)]** を、ブリッジ ドメイン ウィザードの **[L3 構成 (L3 Configuration)]** ページで有効にする必要があります。この回避策は、のみ生成 1 スイッチで必要です。第 2 世代のスイッチで、または以降では、この問題ではありません。

ファイバチャネルおよび FCoE

ファイバチャネルおよびFCoE構成情報については、『*Cisco APIC Layer 2 Networking Configuration Guide*』を参照してください。

Cisco ACI ファブリックでの Fibre Channel over Ethernet トラフィックのサポート

Cisco Application Centric Infrastructure（ACI）では、Cisco ACI ファブリック上の Fibre Channel over Ethernet（FCoE）に対するサポートを設定して、管理することができます。

FCoE は、ファイバ チャネル パケットをイーサネット パケット内にカプセル化するプロトコルです。これにより、ストレージ トラフィックをファイバ チャネル SAN とイーサネット ネットワーク間でシームレスに移動できます。

Cisco ACI ファブリックで FCoE プロトコルのサポートを標準実装することにより、イーサネットベースの Cisco ACI ファブリックに配置されているホストが、ファイバ チャネル ネットワークに配置されている SAN ストレージデバイスと通信できます。ホストは、Cisco ACI リーフスイッチに展開された仮想 F ポートを介して接続しています。SAN ストレージ デバイスとファイバ チャネル ネットワークは、ファイバチャネルフォワーディング（FCF）ブリッジおよび仮想 NP ポートを介して Cisco ACIファブリックに接続されます。このポートは、仮想 F ポートと同じ Cisco ACI リーフスイッチに導入されます。仮想 NP ポートおよび仮想 F ポートも汎用的に仮想ファイバ チャネル (vFC) ポートに呼ばれます。

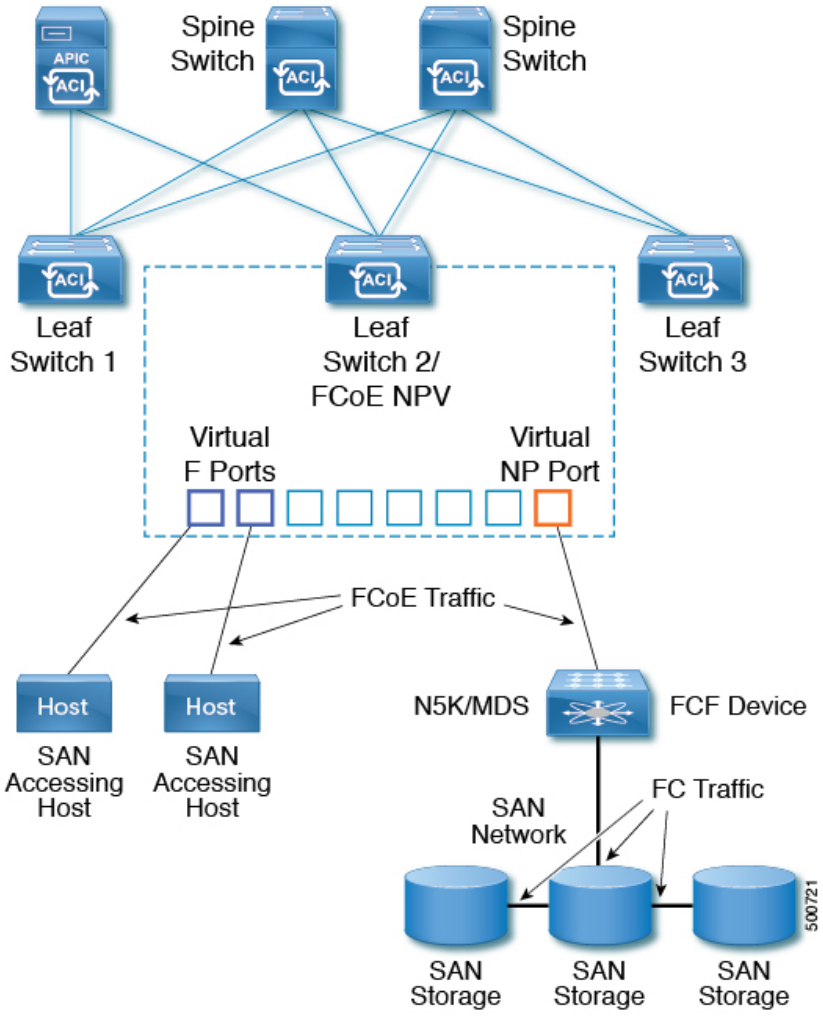


（注） FCoE トポロジにおける Cisco ACI リーフ スイッチの役割は、ローカル接続された SAN ホストとローカル接続された FCF デバイスの間で、 FCoE トラフィックのパスを提供することです。リーフ スイッチでは SAN ホスト間のローカル スイッチングは行われず、FCoE トラフィックはスパイン スイッチに転送されません。

Cisco ACI を介した FCoE トラフィックをサポートするトポロジ

Cisco ACIファブリック経由のFCoEトラフィックをサポートする一般的な設定のトポロジは、次のコンポーネントで構成されます。

図 *33 : Cisco ACI FCoE* トラフィックをサポートするトポロジ



- NPV バックボーンとして機能するようにファイバ チャネル SAN ポリシーを通して設定されている 1 つ以上の Cisco ACI リーフ スイッチ。
- 仮想 F ポートとして機能するように設定された NPV 設定リーフ スイッチ上で選択されたインターフェイス。SAN管理アプリケーションまたはSANを使用しているアプリケーションを実行しているホストとの間を往来する FCoE トラフィックの調整を行います。
- 仮想 NP ポートとして機能するように設定された NPV 設定リーフ スイッチ上で選択されたインターフェイス。ファイバ チャネル転送（FCF）ブリッジとの間を往来する FCoE トラフィックの調整を行います。

FCF ブリッジは、通常 SAN ストレージ デバイスを接続しているファイバ チャネルリンクからファイバ チャネル トラフィックを受信し、ファイバ チャネル パケットを FCoE フレームにカプセル化して、Cisco ACI ファブリック経由で SAN 管理ホストまたは SAN データ消費ホストに送信します。FCoE トラフィックを受信し、ファイバ チャネルに再パッケージしてファイバ チャネル ネットワーク経由で伝送します。



（注） 前掲の Cisco ACI トポロジでは、FCoE トラフィックのサポートには、ホストと仮想 F ポート間の直接接続、および、FCF デバイスと仮想 NP ポート間の直接接続が必要です。

Cisco Application Policy Infrastructure Controller（APIC）サーバーは、Cisco APIC GUI、NX-OS スタイルの CLI、または REST API へのアプリケーション コールを使用して、FCoE トラフィックを設定およびモニタできます。

FCoE の初期化をサポートするトポロジ

FCoE トラフィック フローが説明の通り機能するためには、別の VLAN 接続を設定する必要があります。SAN ホストこの接続を経由して、FCoE 初期化プロトコル（FIP）パケットをブロードキャストし、F ポートとして有効にされているインターフェイスを検出します。

vFC インターフェイス設定ルール

Cisco APIC GUI、NX-OS スタイル CLI、または REST API のいずれを使用して vFC ネットワークと EPG の導入を設定する場合でも、次の一般的なルールがプラットフォーム全体に適用されます。

- F ポート モードは、vFC ポートのデフォルト モードです。NP ポート モードは、インターフェイス ポリシーで具体的に設定する必要があります。
- デフォルトのロード バランシング モードはリーフ スイッチ、またはインターフェイス レベル vFC 設定が src dst ox id。
- ブリッジ ドメインごとに 1 つの VSAN 割り当てがサポートされます。
- VSAN プールおよび VLAN プールの割り当てモードは、常にスタティックである必要があります。
- vFC ポートでは、VLAN にマッピングされている VSAN を含む VSAN ドメイン（ファイバ チャネル ドメインとも呼ばれます）との関連付けが必要です。

ファイバ チャネル接続の概要

Cisco ACI では、N ポート仮想化（NPV）モードを使用したリーフ スイッチでのファイバ チャネル（FC）接続がサポートされています。NPV により、スイッチにおいて、ローカル接続されたホスト ポート（N ポート）からの FC トラフィックをノード プロキシ（NP ポート）アップリンクに集約して、コア スイッチに送ることができます。

スイッチは、NPV を有効にした後は NPV モードになります。NPV モードはスイッチ全体に適用されます。NPV モードのスイッチに接続するエンド デバイスはそれぞれ、この機能を使用するために N ポートとしてログインする必要があります（ループ接続デバイスはサポートされていません）。（NPV モードの）エッジ スイッチから NPV コア スイッチへのすべてのリンクは、（E ポートではなく）NP ポートとして確立されます。このポートは、通常のスイッチ間リンクに使用されます。

（注） FC NPV アプリケーションにおける ACI リーフ スイッチの役割は、ローカル接続された SAN ホストとローカル接続されたコア スイッチ間の FC トラフィックのパスを提供することです。リーフ スイッチでは SAN ホスト間のローカル スイッチングは行われず、FC トラフィックはスパイン スイッチに転送されません。

FC NPV の利点

FC NPV では次の機能を提供します。

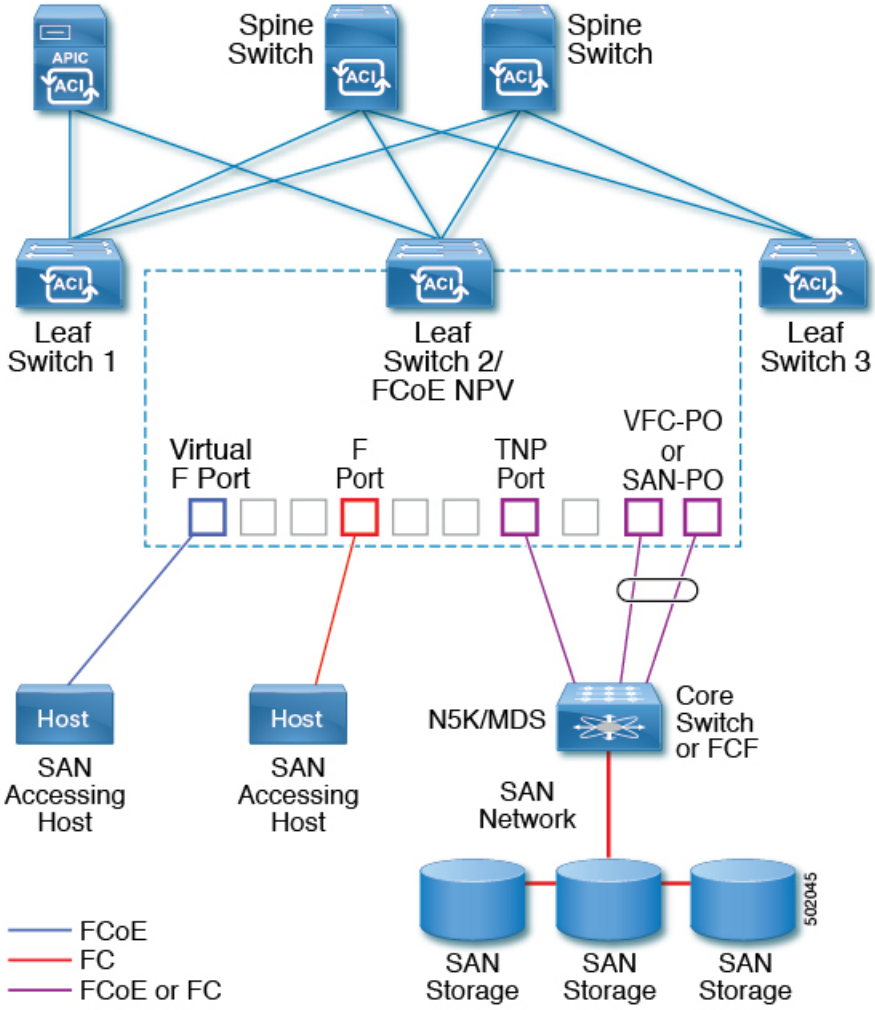
- ファブリックでドメイン ID を追加しなくても、ファブリックに接続するホスト数が増加します。NPV のコア スイッチのドメイン ID は、複数の NPV スイッチ間で共有されます。
- FC ホストと FCoE ホストは、ネイティブの FC インターフェイスを使用して SAN ファブリックに接続します。
- トラフィックの自動マッピングによるロード バランシング。NPV に接続しているサーバを新しく追加した場合に、トラフィックが現在のトラフィック負荷に基づいて、外部のアップリンク間で自動的に分散されます。
- トラフィックの静的マッピング。NPV に接続しているサーバを、外部のアップリンクに静的にマッピングすることができます。

FC NPV モード

ACI の Feature-set fcoe-npv は、最初に FCoE/FC 設定がプッシュされるときに、デフォルトで自動的に有効になります。

FC トポロジ

ACI ファブリック経由の FC トラフィックをサポートするさまざまな設定のトポロジを、次の図に示します。



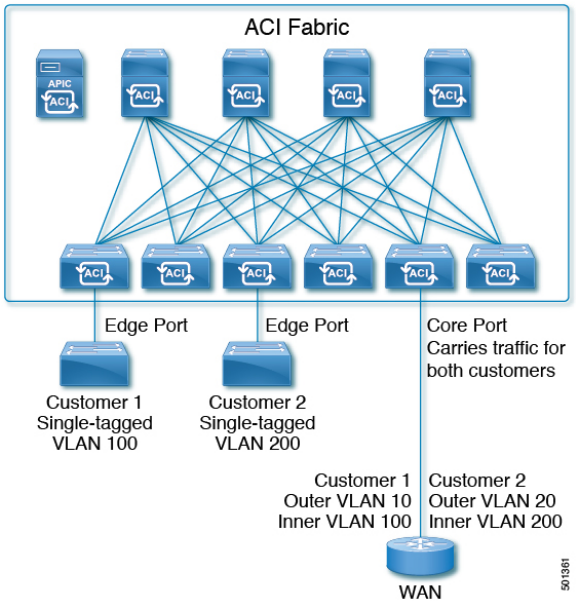
- ACI リーフ スイッチ上のサーバー/ストレージ ホスト インターフェイスは、ネイティブの FC ポートか仮想 FC（FCoE）ポートのどちらかとして機能するように設定できます。
- FC コア スイッチへのアップリンク インターフェイスは、次のいずれかのポート タイプとして設定できます。
  - ネイティブ FC NP ポート
  - SAN-PO NP ポート
- FCF スイッチへのアップリンク インターフェイスは、次のいずれかのポート タイプとして設定できます。
  - 仮想（vFC）NP ポート
  - vFC-PO NP ポート

- N ポート ID 仮想化（NPIV）がサポートされており、デフォルトで有効になっています。そのため、単一のリンクを経由して N ポートに複数の N ポート ID またはファイバ チャネル ID（FCID）を割り当てることが可能です。
- コア スイッチへの NP ポートでは、トランキングを有効にすることができます。トランキングにより、ポートで複数の VSAN をサポートできます。トランク モードが有効になった NP ポートのことを、TNP ポートと呼びます。
- 複数の FC NP ポートを結合してコア スイッチへの SAN ポート チャネル（SAN-PO）とすることができます。トランキングは SAN ポート チャネルでサポートされます。
- FC F ポートでは 4/16/32 Gbps および自動速度設定がサポートされますが、ホスト インターフェイスでは 8Gbps はサポートされません。デフォルトの速度は「auto」です。
- FC NP ポートでは、4/8/16/32 Gbps および自動速度設定がサポートされます。デフォルトの速度は「auto」です。
- Flogi に続く複数の FDISC（ネスト NPIV）は、FC/FCoE ホストと FC/FCoE NP リンクによってサポートされます。
- FEX の背後にある FCoE ホストは、FCoE NP/アップリンクを介してサポートされます。
- APIC 4.1(1) リリース以降、FEX の背後にある FCoE ホストは、ファイバ チャネル NP/アップリンクを介してサポートされます。
- 1 つの FEX の背後にあるすべての FCoE ホストは、複数の vFC および vFC-PO アップリンク間、または単一のファイバ チャネル/SAN ポート チャネル アップリンクを通じてロード バランシングできます。
- SAN ブートは、FEX で FCoE アップリンク経由でサポートされます。
- APIC 4.1(1) リリース以降、SAN ブートは FC/SAN-PO アップリンクでもサポートされます。
- SAN ブートは、FEX を介して接続された FCoE ホストの vPC を介してサポートされます。

802.1Q トンネル

ACI 802.1 q トンネルについて

図 *34 : ACI 802.1 q* トンネル



エッジ（トンネル）ポートで 802.1Q トンネルを設定して、Quality of Service（QoS）の優先順位設定とともに、ファブリックのイーサネット フレームの point-to-multi-point トンネリングを有効にできます。Dot1q トンネルは、タグなし、802.1Q タグ付き、802.1ad 二重タグ付きフレームを、ファブリックでそのまま送信します。各トンネルでは、単一の顧客からのトラフィックを伝送し、単一のブリッジ ドメインに関連付けられています。Cisco Application Centric Infrastructure（ACI）の前面パネル ポートは、Dot1q トンネル の一部とすることができます。レイヤ 2 スイッチングは宛先 MAC（DMAC）に基づいて行われ、通常の MAC ラーニングはトンネルで行われます。エッジ ポート Dot1q トンネル は、スイッチ モデル名の最後に「EX」またはそれ以降のサフィックスが付く、Cisco Nexus 9000 シリーズ スイッチでサポートされます。

同じコア ポートで複数の 802.1Q トンネルを設定することができ、複数の顧客からの二重タグ付きトラフィックを伝送できます。それぞれは、802.1Q トンネルごとに設定されたアクセスのカプセル化で識別されます。802.1Q トンネルでは、MAC アドレス学習を無効にすることもできます。エッジ ポートとコア ポートの両方を、アクセス カプセル化が設定され、MAC アドレス学習が無効にされた 802.1Q トンネルに所属させることができます。エッジ ポートとコア ポートの Dot1q トンネル は、スイッチ モデル名の最後に「FX」またはそれ以降のサフィックスが付く、Cisco Nexus 9000 シリーズ スイッチでサポートされます。

IGMP および MLD パケットは、802.1Q トンネルを介して転送できます。

このドキュメントで使用する用語は、**Cisco Nexus 9000 シリーズ** のドキュメントとは異なっている場合があります。

表 *7: 802.1Q* トンネルの用語

ACI のドキュメント	Cisco Nexus 9000 シリーズのドキュメント
エッジ ポート	トンネル ポート
コア ポート	トランク ポート

次の注意事項および制約事項が適用されます:

- VTP、CDP、LACP、LLDP、およびSTPプロトコルのレイヤ2トンネリングは、次の制限付きでサポートされます。
  - リンク集約制御プロトコル(LACP)トンネリングは、個々のリーフ インターフェイスを使用する、ポイントツーポイントトンネルでのみ、予想通りに機能します。ポートチャネル（PC）または仮想ポートチャネル（vPC）ではサポートされていません。
  - PC または vPC を持つ CDP および LLDP トンネリングは確定的ではありません。これは、トラフィックの宛先として選択するリンクによって異なります。
  - レイヤ 2 プロトコル トンネリングに VTP を使用するには、CDP をトンネル上で有効にする必要があります。
  - レイヤ2プロトコルのトンネリングが有効になっており、Dot1q トンネルのコア ポートにブリッジ ドメインが展開されている場合、STP は 802.1Q トンネル ブリッジ ドメインではサポートされません。
  - Cisco ACI リーフ スイッチは、トンネル ブリッジ ドメインのエンドポイントでフラッシングを行い、ブリッジ ドメインでフラッディングすることにより、STP TCN パケットに反応します。
  - 2 個上のインターフェイスを持つ CDP および LLDP トンネリングが、すべてのインターフェイスでパケットをフラッディングします。
  - エッジ ポートからコア ポートにトンネリングしているレイヤ 2 プロトコル パケットの宛先 MAC アドレスは、01-00-0c-cd-cd-d0 に書き換えられ、コア ポートからエッジ ポートにトンネリングしているレイヤ 2 プロトコル パケットの宛先 MAC アドレスは、プロトコルに対して標準のデフォルト MAC アドレスに書き換えられます。
- PC または vPC が Dot1q Tunnel 内の唯一のインターフェイスであり、削除してから再設定した場合には、PC/VPC の Dot1q トンネル への関連付けを削除して、再設定してください。
- 製品IDにEXが含まれるスイッチに導入された802.1Qトンネルでは、最初の2つのVLANタグの 0x8100 + 0x8100、0x8100 + 0x88a8、0x88a8 + 0x88a8のEthertype の組み合わせはサポートされません。

トンネルが EX と FX またはそれ以降のスイッチの組み合わせに導入されている場合は、この制限が適用されます。

製品 ID に FX 以降が含まれるスイッチにのみトンネルが導入されている場合、この制限は適用されません。

- コア ポートについては、二重タグつきフレームのイーサタイプは、0x8100 の後に 0x8100 が続く必要があります。
- 複数のエッジ ポートおよびコア ポートを（リーフ スイッチ上のものであっても）Dot1q トンネル に含めることができます。
- エッジ ポートは 1 つのトンネルの一部にのみ属することが可能ですが、コア ポートは複数の Dot1q トンネルに属することができます。
- 通常の EPG を 802.1Q で使用されるコア ポートに展開できます。
- L3Outs は、Dot1q トンネルで有効になっているインターフェイスではサポートされていません。
- FEX インターフェイスは Dot1q トンネル のメンバーとしてはサポートされていません。
- ブレークアウト ポートとして設定されているインターフェイスは、802.1 q をサポートしていません。
- インターフェイス レベルの統計情報は Dot1q トンネル のインターフェイスでサポートされていますが、トンネル レベルの統計情報はサポートされていません。
- 802.1Q トンネルは、マルチポッド ファブリック全体でサポートされますが、マルチサイト全体ではサポートされません。

ダイナミック ブレイクアウト ポート

ブレークアウト ポートの設定

ブレークアウト ケーブルは非常に短いリンクに適しており、コスト効率の良いラック内および隣接ラック間を接続する方法を提供します。ブレークアウトでは、40 ギガビット（Gb）ポートを 4 つの独立した論理 10 Gb ポートに分割すること、100Gb ポートを 4 つの独立した論理 25Gb ポートに分割するころ、または 400Gb ポートを 4 つの独立した論理 100Gb ポートに分割することができます。

スイッチのダウンリンク（アクセス側ポートまたはダウンリンク ポートとも呼ばれます）およびファブリック リンクにブレークアウトを設定します。ファブリック リンクは、リーフ スイッチとスパイン スイッチ間の接続、またはマルチティア トポロジのティア 1 リーフ スイッチとティア 2 リーフ スイッチ間の接続を形成します。

ブレークアウト ポートは、次の方法で構成できます。

- ポート プロファイルとセレクタを使用できます。この方法では、リーフ インターフェイス プロファイルでブレークアウト リーフ ポートを構成し、プロファイルとスイッチを関連付け、サブポートを構成します。
- Cisco Application Policy Infrastructure Controller（APIC）6.0(1) リリース以降では、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [インターフェイス構成（Interface Configuration）]**ワークフローを使用できます。
- **[ファブリック（Fabric）] > [インベントリ（Inventory）] >** ***pod*** **>** ***leaf_name*** ワークフローを使用できます。Cisco APIC 6.0(1) リリース以降、インベントリ ビューの構成でもインターフェイスの構成を使用します。

ポート プロファイルの設定

アップリンクおよびダウンリンク変換は、名前の末尾が EX か FX、またはそれ以降の Cisco Nexus 9000 シリーズ スイッチでサポートされます（たとえば、N9K-C9348GC-FXP または N9K-C93240YC-FX2）。変換後のダウンリンクに接続されている FEX もサポートされています。

サポートされているサポート対象の Cisco スイッチについては、『ポート プロファイルの設定のまとめ （98 ページ）』を参照してください。

アップリンク ポートがダウンリンク ポートに変換されると、他のダウンリンク ポートと同じ機能を持つようになります。

制約事項

- FAST リンク フェールオーバー ポリシーとポート プロファイルは、同じポートではサポートされていません。ポート プロファイルが有効になっている場合、FAST リンク フェールオーバーを有効にすることはできません。その逆も同様です。
- サポートされているリーフ スイッチの最後の 2 つのアップリンク ポートは、ダウンリンク ポートに変換することはできません（これらはアップリンク接続用に予約されています）。
- ダイナミック ブレークアウト（100Gbと40Gbの両方）は、N9K-C93180YC-FX スイッチのプロファイルされた QSFP ポートでサポートされます。ブレイクアウトおよびポート プロファイルでは、ポート 49-52 でアップリンクからダウンリンクへの変換が一緒にサポートされています。ブレークアウト（**10g-4x** オプションと **25g-4x** オプションの両方）は、ダウンリンク プロファイル ポートでサポートされます。
- N9K-C9348GC-FXP は FEX をサポートしていません。
- ブレークアウトはダウンリンク ポートでのみサポートされます。他のスイッチに接続されているファブリック ポートではサポートされません。
- Cisco ACI リーフスイッチは、56 を超えるファブリック リンクを持つことはできません。

- スイッチのポート プロファイル構成を変更した後にスイッチをリロードすると、データプレーンを通過するトラフィックが中断されます。
- ポート プロファイルがいずれかの LEM タイプで構成されており、その LEM を交換する場合は、交換する LEM タイプが、取り外した LEM タイプと一致している必要があります。

ガイドライン

アップリンクをダウンリンクに変換したり、ダウンリンクをアップリンクに変換したりする際は、次の注意事項にご注意ください。

サブジェクト	ガイドライン
N9K-X9400-8D のポート プロファイルの注意事項	この LEM には、次の注意事項が適用されます。 • この LEM には 8 つのポートがあり、デフォルトでは 4 つのダウンリンクと 4 つのアップリンクがあります。 • ポート プロファイルの変換は、最初の 6 つのポートでサポートされます。 • この LEM には、ポート グループの依存関係はありません。
N9K-X9400-16W のポート プロファイルの注意事項	この LEM には、次の注意事項が適用されます。 • この LEM には 16 個のポートがあり、デフォルトは 12 個のダウンリンクと 4 個のアップリンクです。 • ポート プロファイルの変換は、最初の 6 つのポートでサポートされます。 • この LEM には、ポート プロファイル変換用の 2 ポートのポート グループ依存関係があります。つまり、ポート 1 ～ 2、3 ～ 4、および 5 ～ 6 にはポート グループの依存関係があります。たとえば、ポート 2 をアップリンクとして変換する場合は、ポート 1 もアップリンクに変換する必要があります。

サブジェクト	ガイドライン
N9K-X9400-22L のポート プロファイルの注意事項	6.1(2) リリースでは、この LEM のサポートが追加されています。以下の注意事項が適用されます。 • この LEM には 22 個のポートがあり、デフォルトでは 14 個のダウンリンクと 8 個のアップリンクがあります。 • ポート プロファイルの変換は、最初の 18 個のポートでサポートされます。 • この LEM には、ポート 9 と 10 を除くポート プロファイル変換用の 4 つのポートのポート グループ依存関係があります。これは、ポート 1 ～ 4、5 ～ 8、11 ～ 14、および 15 ～ 18 がポート グループの一部であることを意味します。たとえば、ポート 2 をアップリンクに変換する場合は、ポート 1 ～ 4 をすべて変換する必要があります。 • ポート 9 および 10 は 2 のポート グループです。ポート 10 をアップリンクとして変換する場合は、ポート 9 もアップリンクにする必要があります。
LEM の不一致	N9K-C9400-SUP-A で、ポート 7 ～ 18 にポート プロファイルが構成された N9K-X9400-22L LEM があり、N9K-X9400-8D や N9K-X9400 などの別の LEM タイプと交換する場合-16W の場合、8D または 16W モジュールはモジュール ステータスを表示します。 **LEM タイプの不一致**。この障害は、ポートプロファイルの変換が一致しないために発生します。8D および 16W モジュールの場合、ポートプロファイルの変換はポート 1 ～ 6 のみです。 8D または 16W LEM を不一致から回復するには、以前の LEM（つまり、N9K-X9400-22L LEM）のすべてのポートに存在するポートプロファイル構成を削除します。ポートプロファイルを構成しないでください。このプロセスの後、クリーン リロードを実行して LEM を回復します。

サブジェクト	ガイドライン
ポート プロファイルを使用したノードのデコミッション	デコミッションされたノードがポートプロファイル機能を展開している場合、ポート変換はノードのデコミッション後も削除されません。 ポートをデフォルト状態に戻すには、デコミッション後に手動で設定を削除する必要があります。これを行うには、スイッチにログオンし、`setup-clean-config.sh` スクリプトを実行して、実行されるまで待ちます。それから、`リロード` コマンドを入力します。 オプションとして、`-k` を `setup-clean-config.sh` スクリプトで指定することができます。ポートプロファイルの設定がリロード後も維持され、追加のリブートが不要になります。 6.0(5) 以降では、オプション `-k` または `--keep-port-profile` を指定せずに `setup-clean-config.sh` スクリプトを実行すると、リロード後もポートプロファイル設定が保持されます。構成を手動で削除するには、 `-d` または `--delete-profiles` を指定して `setup-clean-config.sh`スクリプトを実行します。
最大アップリンク ポートの制限	最大アップリンク ポートの制限に達し、ポート 25 および 27 がアップリンクからダウンリンクへ返還されるとき、Cisco 93180LC EX スイッチのアップリンクに戻ります。 Cisco N9K-93180LC-EX スイッチでは、ポート 25 および 27 がオリジナルのアップリンク ポートです。ポート プロファイルを使用して、ポート 25 および 27 をダウンリンク ポートに変換する場合でも、ポート 29、30、31、および 32 は引き続き 4 つの元のアップリンク ポートとして使用できます。変換可能なポート数のしきい値のため（最大 12 ポート）、8 個以上のダウンリンク ポートをアップリンク ポートに変換できます。たとえば、ポート 1、3、5、7、9、13、15、17 はアップリンク ポートに変換されます。ポート 29、30、31、および 32 は、4 つの元からのアップリンク ポートです（Cisco 93180LC-EX スイッチでの最大アップリンク ポートの制限）。 スイッチがこの状態でポート プロファイル設定がポート 25 および 27 で削除される場合、ポート 25 および 27 はアップリンク ポートへ再度変換されますが、前述したようにスイッチにはすでに 12 個のアップリンク ポートがあります。ポート 25 および 27 をアップリンク ポートとして適用するため、ポート範囲 1、3、5、7、9、13、15、17 からランダムで 2 個のポートがアップリンクへの変換を拒否されます。この状況はユーザにより制御することはできません。 そのため、リーフ ノードをリロードする前にすべての障害を消去し、ポートタイプに関する予期しない問題を回避することが必須です。ポートプロファイルの障害を消去せずにノードをリロードすると、特に制限超過に関する障害の場合、ポートは予想される動作状態になることに注意する必要があります。

ブレークアウト制限

スイッチ	リリース	制限事項
N9K-C93180LC-EX	Cisco APIC 3.1(1) 以降	• 40 Gb と 100 Gb のダイナミック ブレークアウトは、ポート 1 ~ 24 の奇数ポート上でサポートされます。 • 上位ポート（奇数ポート）ブレークアウトされると、下部ポート（偶数ポート）はエラーが無効になります。 • ポート プロファイルおよびブレークアウトは、同じポートでサポートされていません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。
N9K-C9336C-FX2-E	Cisco APIC 5.2(4) 以降	• 40Gb および 100Gb のダイナミック ブレークア ウトは、ポート 1 ー 34 でサポートされます。 • ポート プロファイルは、ブレークアウトが有効になっているポートには適用できません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。 • 34 ポートすべてをブレークアウトポートとして設定できます。 • 34 のポートにブレークアウト設定を適用する場合は、34 のダウンリンク ポートを持つようにポートのポート プロファイルを設定してから、リーフ スイッチをリブートする必要があります。 • 複数のポートのリーフ スイッチにブレークアウト設定を同時に適用する場合、34 ポートのハードウェアがプログラムされるまでに最大 10 分かかります。プログラミングが完了するまで、ポートはダウンしたままになります。新しい設定の場合、クリーン リブート後、またはスイッチの検出中に遅延が発生する可能性があります。

スイッチ	リリース	制限事項
N9K-C9336C-FX2	Cisco APIC 4.2(4) 以降	• 40Gb および 100Gb のダイナミック ブレークア ウトは、ポート 1 ー 34 でサポートされます。 • ポート プロファイルは、ブレークアウトが有効になっているポートには適用できません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。 • 34 ポートすべてをブレークアウトポートとして設定できます。 • 34 のポートにブレークアウト設定を適用する場合は、34 のダウンリンク ポートを持つようにポートのポート プロファイルを設定してから、リーフ スイッチをリブートする必要があります。 • 複数のポートのリーフ スイッチにブレークアウト設定を同時に適用する場合、34 ポートのハードウェアがプログラムされるまでに最大 10 分かかります。プログラミングが完了するまで、ポートはダウンしたままになります。新しい設定の場合、クリーン リブート後、またはスイッチの検出中に遅延が発生する可能性があります。
N9K-C9336C-FX2	Cisco APIC 3.2(1) 以降、ただし 4.2(4) は含まない	• ポート 1 ~ 30 では、40 Gb と 100 Gb のダイナミック ブレークがサポートされています。 • ポート プロファイルおよびブレークアウトは、同じポートでサポートされていません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。 • 最大 20 のポートをブレークアウト ポートとして設定できます。

スイッチ	リリース	制限事項
N9K-C93180YC-FX	Cisco APIC 3.2(1) 以降	• 40 Gb と 100 Gb のダイナミック ブレークは、52、上にあるときにプロファイリング QSFP ポートがポート 49 でサポートされます。ダイナミック ブレークアウトを使用するには、次のステップを実行します。 • ポート 49~52 を前面パネル ポート（ダウンリンク）に変換します。 • 次の方法のいずれかを使用して、ポート プロファイルのリロードを実行します。 • Cisco APIC GUI で、**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[ポッド（Pod）]** > **[リーフ（Leaf）]** に移動し、**[シャーシ（Chassis）]** を右クリックして、**[リロード（Reload）]** を選択します。 • iBash CLI で、**reload** コマンドを入力します。 • プロファイルされたポート 49 - 52 のブレーク アウトを適用します。 • ポート 53 および 54 では、ポート プロファイルまたはブレークアウトをサポートしていません。
N9K-C93240YC-FX2	Cisco APIC 4.0(1) 以降	ブレークアウトは変換後のダウンリンクではサポートされていません。

ポート プロファイルの設定のまとめ

次の表に、アップリンクからダウンリンク、およびダウンリンクからアップリンクへのポート プロファイル変換をサポートするスイッチでサポートされるアップリンクおよびダウンリンクをまとめます。

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9348GC-FXP[1] N9K-C9348GC-FX3	48 x 100 M/1 G BASE-T ダウンリンク 4 x 10/25 Gbps SFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	48 x 100 M/1 G BASE-T ダウンリンク 4 x 10/25 Gbps SFP28 アップリンク 2 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	3.1(1) 6.0(5)
N9K-C93180LC-EX	24 x 40 Gbps QSFP28 ダウンリンク（ポート 1ー24） 2 x 40/100 Gbps QSFP28 アップリンク（ポート 25、27） 4 x 40/100 Gbps QSFP28 アップリンク（ポート 29ー32） または 12 X 100 Gbps QSFP28 ダウンリンク（1ー24 の奇数番号ポート） 2 x 40/100 Gbps QSFP28 アップリンク（ポート 25、27） 4 x 40/100 Gbps QSFP28 アップリンク（ポート 29ー32）	18 X 40 Gbps QSFP28 ダウンリンク（1 ー 24） 6 X 40 Gbps QSFP28 アップリンク（1 ー 24） 2 x 40/100 Gbps QSFP28 アップリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32） または 6 x 100 Gbps QSFP28 ダウンリンク（1 ー 24 の範囲の奇数） 6 x 100 Gbps QSFP28 アップリンク（1 ー 24 の範囲の奇数） 2 x 40/100 Gbps QSFP28 アップリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32）	24 X 40 Gbps QSFP28 ダウンリンク（1 ー 24） 2 x 40/100 Gbps QSFP28 ダウンリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32） または 12 X 100 Gbps QSFP28 ダウンリンク（1 ー 24 の範囲の奇数） 2 x 40/100 Gbps QSFP28 ダウンリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32）	3.1(1)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C93180YC-EX N9K-C93180YC-FX N9K-C93180YC-FX3	48 x 10/25 Gbps ファイバ ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	48 x 10/25 Gbps ファイバ ダウンリンク 4 x 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	3.1(1)
		48 X 10/25 Gbps ファイバ アップリンク 6 x 40/100 Gbps QSFP28 アップリンク		4.0(1) 5.1(3)
N9K-C93108TC-EX[2] N9K-C93108TC-FX[2] N9K-C93108TC-FX3	48 x 10GBASE T ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	48 x 10/25 Gbps ファイバ ダウンリンク 4 x 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	3.1(1) 4.0(1) 5.1(3)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9336C-FX2	30 x 40/100 Gbps QSFP28 ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	18 x 40/100 Gbps QSFP28 ダウンリンク 18 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	3.2(1)
		18 x 40/100 Gbps QSFP28 ダウンリンク 18 x 40/100 Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	3.2(3)
		36 x 40/100-Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.1(1)
N9K-C9336C-FX2-E	30 x 40/100 Gbps QSFP28 ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	36 x 40/100-Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	5.2(4)
N9K-93240YC-FX2	48 x 10/25 Gbps ファイバ ダウンリンク 12 x 40 / 100Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	48 x 10/25 Gbps ファイバ ダウンリンク 10 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.0(1)
		48 X 10/25 Gbps ファイバ アップリンク 12 x 40 / 100Gbps QSFP28 アップリンク		4.1(1)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C93216TC-FX2	96 X 10G BASE-T ダウンリンク 12 x 40 / 100Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	96 X 10G BASE-T ダウンリンク 10 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.1(2)
N9K-C93360YC-FX2	96 X 10/25 Gbps SFP28 ダウンリンク 12 x 40 / 100Gbps QSFP28 アップリンク	44 x 10 / 25Gbps SFP28 ダウンリンク 52 x 10 / 25Gbps SFP28 アップリンク 12 x 40 / 100Gbps QSFP28 アップリンク	96 X 10/25 Gbps SFP28 ダウンリンク 10 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.1(2)
N9K-C93600CD-GX	28 x 40/100 Gbps QSFP28 ダウンリンク（ポート 1～28） 8 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 29～36）	28 X 40/100 Gbps QSFP28 アップリンク 8 x 40/100/400 Gbps QSFP-DD アップリンク	28 X 40/100 Gbps QSFP28 ダウンリンク 6 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	4.2(2)
N9K-C9364C-GX	48 x 40/100 Gbps QSFP28 ダウンリンク（ポート 1～48） 16 x 40/100 Gbps QSFP28 アップリンク（ポート 49～64）	56 x 40/100 Gbps QSFP28 アップリンク	62 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.2(3)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9316D-GX	12 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～12） 4 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 13～16）	16 X 40/100/400 Gbps QSFP-DD アップリンク	14 x 40/100/400 Gbps QSFP-DD ダウンリンク	5.1(4)
N9K-C9332D-GX2B	2 x 1/10 Gbps SFP+ ダウンリンク（ポート 33～34） 24 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～24） 8 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 25～32）	2 X 1/10 Gbps SFP+ ダウンリンク 32 X 40/100/400 Gbps QSFP-DD アップリンク	2 X 1/10 Gbps SFP+ ダウンリンク 30 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	5.2(3)
N9K-C9348D-GX2A	2 x 1/10 Gbps SFP+ ダウンリンク（ポート 49～50） 36 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～36） 12 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 37～48）	2 X 1/10 Gbps SFP+ ダウンリンク 48 x 40/100/400 Gbps QSFP-DD アップリンク	2 X 1/10 Gbps SFP+ ダウンリンク 46 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	5.2(5)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9364D-GX2A	2 x 1/10 Gbps SFP+ ダウンリンク（ポート 65～66） 48 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～48） 16 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 49～64）	2 X 1/10 Gbps SFP+ ダウンリンク 56 X 40/100/400 Gbps QSFP-DD アップリンク	2 X 1/10 Gbps SFP+ ダウンリンク 62 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	5.2(5)
N9K-C9408（N9K-X9400-8D 搭載）[3]	6 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	8 x 40/100/400 Gbps QSFP-DD アップリンク	デフォルトのポート設定と同じ	6.0(2)
N9K-C9408（N9K-X9400-16W 搭載）[3]	12 x 100/200 Gbps QSFP56 ダウンリンク 4 x 100/200 Gbps QSFP56 アップリンク	6 x 100/200 Gbps QSFP56 アップリンク（ポート 1～6） 6 x 100/200 Gbps QSFP56 ダウンリンク（ポート 7～12） 4 x 100/200 Gbps QSFP56 アップリンク（ポート 13～16）	デフォルトのポート設定と同じ	6.0(2)[4]

1 FEX をサポートしていません。

2 アップリンクからダウンリンクへの変換のみがサポートされています。

3 ポート 1～6 のみがポート プロファイルの変換をサポートします。

4 6.0(2) リリースは 200 Gbps をサポートしていません。

ファブリック ポートの障害検出のためのポート トラッキング ポリシー

ファブリック ポートの障害検出は、ポート トラッキング システム設定で有効にすることができます。ポートトラッキングポリシーは、リーフスイッチとスパインスイッチ間のファブリック ポート、およびティア1リーフスイッチとティア2リーフスイッチ間のポートのステータスを監視します。有効なポートトラッキングポリシーがトリガーされると、リーフスイッチは、EPGによって導入されたスイッチ上のすべてのアクセスインターフェイスをダウンさせます。

[ポート トラッキングがトリガーされたときにAPICポートを含める（Include APIC ports when port tracking is triggered）] オプションを有効にした場合、リーフスイッチがすべてのファブリック ポートへの接続を失うと（つまり、ファブリック ポートが0になると）、ポート トラッキングは Cisco Application Policy Infrastructure Controller（APIC）ポートを無効にします。Cisco APIC がファブリックに対してデュアルまたはマルチホームの場合にのみ、この機能を有効にしてください。Cisco APIC ポートを停止すると、デュアルホームの Cisco APIC の場合にセカンダリ ポートに切り替えるのに役立ちます。

（注） ポートトラッキングの設定は、**[システム（System）]**> > **[システム設定（System Settings）]** > >**[ポート トラッキング（Port Tracking）]** で行えます。

ポート トラッキング ポリシーは、ポリシーをトリガーするファブリック ポート接続の数と、指定されたファブリック ポートの数を超えた後にリーフスイッチアクセス ポートをバックアップするための遅延タイマーを指定します。

次の例は、ポート トラッキング ポリシーの動作を示しています。

- ポート トラッキング ポリシーは、ポリシーをトリガーする各リーフ スイッチのアクティブなファブリック ポート接続のしきい値が 2 であると指定しています。
- ポート トラッキング ポリシーは、リーフ スイッチからスパイン スイッチへのアクティブなファブリック ポート接続の数が 2 に低下したときにトリガーされます。
- 各リーフスイッチは、そのファブリック ポート接続を監視し、ポリシーで指定されたしきい値に従ってポート トラッキング ポリシーをトリガーします。
- ファブリック ポート接続が復旧すると、リーフ スイッチは遅延タイマーの設定時間が経過するのを待ってから、アクセスポートを復旧します。これにより、トラフィックがリーフスイッチ アクセス ポートで再開可能になる前に、ファブリックが再コンバージェンスする時間が与えられます。大規模なファブリックでは、遅延タイマーをより長い時間に設定する必要がある場合があります。

（注） このポリシーを構成するときは注意してください。ポートトラッキングをトリガーする、アクティブなスパインポートの数に関するポートトラッキング設定が高すぎる場合、すべてのリーフ スイッチ アクセス ポートがダウンします。

Epg の Q-で-Q カプセル化のマッピング

Cisco Application Policy Infrastructure Controller（APIC）を使用すれば、通常のインターフェイス、PC、または vPC で入力される二重タグ付き VLAN トラフィックを EPG にマッピングできます。この機能が有効で、二重タグ付きトラフィックが EPG のネットワークに入ると、両方のタグがファブリック内で個別に処理され、Cisco Application Centric Infrastructure（ACI）スイッチの出力時に二重タグに復元されます。単一タグおよびタグなしのトラフィックの入力はドロップします。

次の注意事項および制約事項が適用されます。

- この機能は、Cisco Nexus 9300-FX、9300-FX2、および 9300-FX3 プラットフォーム スイッチでサポートされます。
- 外側と内側の両方のタグは、EtherType 0x8100 である必要があります。
- MAC ラーニングとルーティングは、アクセスのカプセル化ではなく、EPG ポート、sclass、および VRF インスタンスに基づいています。
- QoS 優先度設定がサポートされ、入力の外側のタグから派生し、出力の両方のタグに書き換えられます。
- EPG はリーフ スイッチの他のインターフェイスに同時に関連付けることができ、単一タグの VLAN に設定されます。
- サービス グラフは、Q-in-Q カプセル化したインターフェイスにマッピングされているプロバイダとコンシューマ EPG をサポートしています。サービス ノードの入力および出力トラフィックが単一タグのカプセル化フレームにある限り、サービス グラフを挿入することができます。
- vPC ポートが Q-in-Q カプセル化モードに対して有効になっている場合、VLAN 整合性チェックは実行されません。

この機能では、次の機能とオプションがサポートされていません。

- ポート単位の VLAN 機能
- FEX 接続
- Mixed mode

たとえば、Q-in-Q カプセル化モードのインターフェイスでは、通常の VLAN のカプセル化ではなく、二重タグ付きカプセルのみを持つ EPG にバインディングされている静的パスを有します。

- STP と「カプセル化でのフラッディング」オプション
- タグなしおよび 802.1p モード
- マルチポッドと複数サイト
- レガシ ブリッジ ドメイン
- L2Out および L3Out 接続
- VMM の統合
- ポート モードをルーテッドから Q-in-Q カプセル化モードに変更する
- Q-in-Q カプセル化モードのポートでの VLAN 単位の誤配線プロトコル

レイヤ 2 マルチキャスト

Cisco APIC および IGMP スヌーピングについて

IGMP スヌーピングは、Internet Group Management Protocol（IGMP）ネットワーク トラフィックをリスニングするプロセスです。この機能により、ネットワーク スイッチはホストとルータ間の IGMP 対話をリスニングして、必要ないマルチキャスト リンクをフィルタでき、特定のマルチキャスト トラフィックを受け取るポートを制御することができます。

Cisco APIC は、N9000 スタンドアロンなどの従来のスイッチに含まれる完全な IGMP スヌーピング機能をサポートします。

- ブリッジドメインごとのポリシーベースの IGMP スヌーピング構成

  APIC を使用すると、ブリッジドメインごとに IGMP スヌーピングのプロパティを有効化、無効化、またはカスタマイズするポリシーを構成できます。その後、そのポリシーを 1 つまたは複数のブリッジドメインに適用できます。

- 静的ポート グループの導入

  スイッチ ポートが IGMP マルチキャスト トラフィックを受信および処理しているため、IGMP 静的ポートのグループ化によりすでにアプリケーション EPG に静的に割り当てられた事前プロビジョニングは有効です。この事前プロビジョニングは、通常 IGMP スヌーピング スタックがポートを動的に学習するときに発生する参加遅延を防止します。

  静的グループ メンバーシップは、アプリケーション EPG に割り当てられている静的ポート（*static-binding ports* とも呼ばれます）でのみ事前プロビジョニングできます。

- アプリケーション EPG のアクセス グループ構成

「アクセス-グループ」ができるストリームを制御するために使用任意ポート背後に参加します。

実際に所属するするポートの設定を適用できることを確認するには、アプリケーション EPG に静的に割り当てられているインターフェイスでアクセス グループ設定を適用できる EPG。

ルート マップ ベースのアクセス グループのみが許可されます。

（注） **vzAny** を使用して、VRF 内のすべての EPG に対して IGMP スヌーピングなどのプロトコルを有効にすることができます。**vzAny** について詳細は、「vzAny を使用して VRF 内のすべての EPG に通信ルールを自動的に適用する」を参照してください。

vzAny を使用するには、**[テナント（Tenants）]**>**[*tenant-name*]**>**[ネットワーキング（Networking）]**>**[VRFs]**>**[*vrf-name*]**>**[VRF 向けの EPG 収集（EPG Collection for VRF）]** の順に移動します。

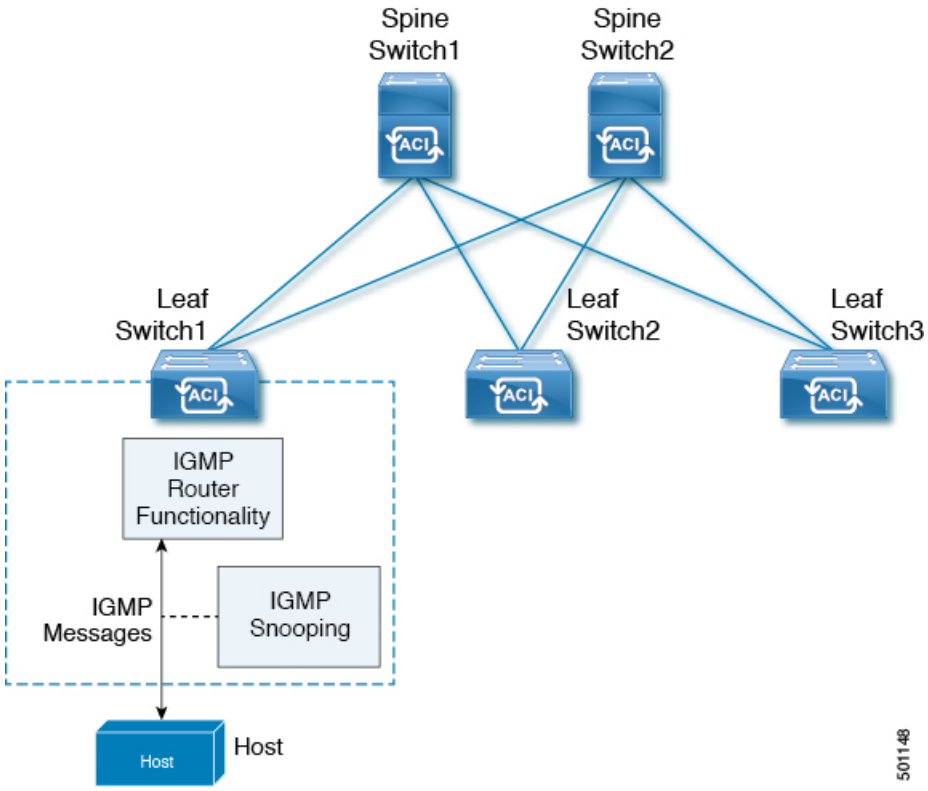
ACI ファブリックに IGMP スヌーピングを実装するには

（注） ブリッジ ドメインで IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、ブリッジ ドメインで不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセスブリッジ ドメイン環境における帯域幅消費量を削減し、ブリッジ ドメイン全体へのフラッディングを回避します。デフォルトでは、IGMP スヌーピングがブリッジ ドメインでイネーブルにされています。

この図は、ホストへの接続を持つ ACI リーフ スイッチに含まれる IGMP ルーティング機能と IGMP スヌーピング機能を示しています。IGMP スヌーピング機能は、IGMP メンバーシップ レポートをスヌーピングし、メッセージを残し、必要な場合にのみIGMPルータ機能に転送します。

図 *35 : IGMP* スヌーピング機能



IGMP スヌーピングは、IGMPv1、IGMPv2、および IGMPv3 コントロール プレーン パケットの処理に関与し、レイヤ 3 コントロール プレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

IGMP スヌーピングには、次の独自機能があります。

- 宛先および送信元の IP アドレスに基づいたマルチキャスト パケットの転送が可能な送信元フィルタリング
- MAC アドレスではなく、IP アドレスに基づいたマルチキャスト転送
- MAC アドレスに基づいた代わりのマルチキャスト転送

ACI ファブリックは、RFC 4541の2.1.1 項「IGMP 転送ルール」に記載されているガイドラインに従って、プロキシ レポーティング モードでのみ IGMP スヌーピングをサポートします。

IGMP □□□□

その結果、ACI ファブリックは送信元 IP アドレス 0.0.0.0 の IGMP レポートを送信します。

（注） IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

リーフ スイッチでは、**show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーブ機能

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリー メッセージがホストに送信されません。APIC は、IGMP 脱退メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP 脱退メッセージが存在しないため、 APIC の IGMP スヌーピング機能は、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトを使用する必要があります。

（注） 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、IGMP スヌーピング機能は、最終メンバーのクエリー インターバル設定を無視します。

APIC IGMP スヌーピング ファンクション キーと IGMPv3

APIC での IGMPv3 スヌーピング ファンクションでは、完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの （S、G） 情報に基づいて、抑制されたフラッディングが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャスト グループにトラフィックを送信する送信元に基づいて、マルチキャスト トラフィックの宛先ポートを制限できます。

デフォルトでは、IGMP スヌーピング機能は、ブリッジ ドメインでは、各 VLAN ポート上のホストを追跡します。この明示的なトラッキング機能は、高速脱退メカニズムをサポートして

います。IGMPv3 ではすべてのホストがメンバーシップ レポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制を有効にしていても、IGMPv1 または IGMPv2 ホストが同じグループをリクエストしなかった場合、IGMP スヌーピング機能はプロキシ レポートを作成します。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートには ブリッジ ドメインのグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、ソフトウェアはメンバーシップ クエリーを送信します。最終メンバーのクエリー インターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合、IGMP スヌーピングはグループ ステートを削除します。

Cisco APIC および IGMP スヌーピング クエリア関数

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast（PIM）がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するように IGMP スヌーピング クエリア機能を設定する必要があります。APIC、IGMP スヌープ ポリシー内で定義マルチキャストのソースとレシーバが含まれているブリッジ ドメインでクエリアがないその他のアクティブなクエリアします。

Cisco ACI はデフォルトで、IGMP スヌーピングが有効になっています。さらに、ブリッジ ドメイン サブネット制御は、「クエリア IP」を選択、リーフ スイッチによって、クエリアとして動作およびクエリ パケット送信を開始します。セグメントは、明示的なマルチキャスト ルータ (PIM が有効になっていません) があるないときに ACI Leaf スイッチでクエリアを有効にする必要があります。ブリッジ ドメインで、クエリアが設定されている、使用される IP アドレス マルチキャストのホストが設定されている同じサブネットからにする必要があります。

（注） クエリアの IP アドレスは、ブロードキャスト IP アドレス、マルチキャスト IP アドレス、または 0（0.0.0.0）にしないでください。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

ファブリック セキュア モード

ファブリック セキュア モードは、ファブリック機器に物理的にアクセスできる関係者が、管理者による手動の承認なしに、スイッチまたは APIC コントローラをファブリックに追加できないようにします。リリース 1.2(1x) 以降、ファームウェアは、ファブリック内のスイッチとコントローラに、有効な Cisco のデジタル署名付き証明書に関連付けられた有効なシリアル番号があることを確認します。この検証は、このリリースへのアップグレード時またはファブリックの初期インストール時に実行されます。この機能のデフォルト設定は permissive モードです。既存のファブリックは、リリース 1.2(1) 以降へのアップグレード後もそのまま実行されます。ファブリック全体のアクセス権を持つ管理者は、strict モードを有効にする必要があります。次の表は、2 つの動作モードをまとめたものです。

Permissive モード（デフォルト）	**Strict モード**
1 つ以上のスイッチに無効な証明書がある場合でも、既存のファブリックが正常に動作できるようにします。	有効な Cisco シリアル番号と SSL 証明書を持つスイッチのみが許可されます。
シリアル番号ベースの認証を強制しません。	シリアル番号認証を強制します。
自動検出されたコントローラとスイッチが、シリアル番号認証を強制せずにファブリックに参加できるようにします。	管理者がコントローラとスイッチを手動で承認してファブリックに参加させる必要があります。

FAST リンク フェールオーバー ポリシーの構成

FAST リンク フェールオーバー ポリシーは、-EX、-FX、および -FX2 サフィックスが付いたスイッチ モデルのアップリンクに適用されます。アップリンク MAC ステータスに基づいてトラフィックを効率的に負荷分散します。この機能により、スイッチはレイヤ 2 またはレイヤ 3 ルックアップを実行し、アップリンク ステータスを考慮して、パケット ハッシュ アルゴリズムに基づいて出力レイヤ 2 インターフェイス（アップリンク）を提供します。この機能により、データ トラフィックのコンバージェンスが 200 ミリ秒未満に短縮されます。

FAST リンク フェールオーバーの構成に関する次の制限事項を参照してください。

- FAST リンク フェールオーバーとポート プロファイルは、同じポートではサポートされていません。ポート プロファイルが有効になっている場合、FAST リンク フェールオーバーを有効にすることはできません。その逆も同様です。
- リモート リーフの構成は、FAST リンク フェールオーバーでは機能しません。この場合、FAST リンク フェールオーバー ポリシーは機能せず、障害は生成されません。
- FAST リンク フェールオーバー ポリシーが有効になっている場合、個々のアップリンクでの SPAN の構成は機能しません。個々のアップリンクで SPAN を有効にしようとしても障

害は生成されませんが、FAST リンク フェールオーバー ポリシーはすべてのアップリンクで一緒に有効にすることも、個々のダウンリンクで有効にすることもできます。



（注） FAST リンク フェールオーバーは、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [ポリシー（Policies）] > [スイッチ（Switch）] > [FAST リンク フェールオーバー（Fast Link Failover）]** の下にあります。

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。

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。

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。

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。

Cisco APIC リリース 6.0(2) 以降、FHS は VMware DVS VMM ドメインでサポートされます。EPG 内に FHS を実装する必要がある場合は、EPG 内分離を有効にします。EPG 内分離が有効

になっていない場合、同じ VMware ESX ポートグループ内のエンドポイントは FHS をバイパスすることがあります。EPG 内分離を有効にしない場合でも、異なるポートグループにあるエンドポイントに対しては、FHS 機能は引き続き有効です。たとえば、FHS は、侵害された VM が異なるポートグループ内の別の VM の ARP テーブルをポイズニングするのを防ぐことができます。

MACsec について

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。

802.1 ae MKA と暗号化はリンク、つまり、リンク (ネットワーク アクセス デバイスと、PC か IP 電話機などのエンドポイント デバイス間のリンク) が直面しているホストのすべてのタイプでサポートされますかにリンクが接続されている他のスイッチまたはルータ。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。ユーザは、送信元と宛先の MAC アドレスの後に最大 50 バイトの暗号化をスキップするオプションもあります。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（EAPOL）プロトコル データ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。3 回のハートビート後（各ハートビートは 2 秒）に参加者から MKPDU を受信しなかった場合、ピアはライブ ピア リストから削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントから最後の MKPDU を受信した後、3 回のハートビートが経過するまで MKA の動作を継続します。

APIC ファブリック MACsec

APIC はまたは責任を負う MACsec キーチェーン ディストリビューションのポッド内のすべてのノードに特定のポートのノードになります。サポートされている MACsec キーチェーンし、apic 内でサポートされている MACsec ポリシー ディストリビューションのとおりです。

- 単一ユーザ提供キーチェーンと 1 ポッドあたりポリシー
- ユーザが提供されるキーチェーンとファブリック インターフェイスごとのユーザが提供されるポリシー
- 自動生成されたキーチェーンおよび 1 ポッドあたりのユーザが提供されるポリシー

ノードは、複数のポリシーは、複数のファブリック リンクの導入を持つことができます。これが発生すると、ファブリック インターフェイスごとキーチェーンおよびポリシーが優先して指

定の影響を受けるインターフェイス。自動生成されたキーチェーンと関連付けられている MACsec ポリシーでは、最も優先度から提供されます。

APIC MACsec では、2 つのセキュリティ モードをサポートしています。MACsec **セキュリティで保護する必要があります** 中に、リンクの暗号化されたトラフィックのみを許可する **セキュリティで保護する必要があります** により、両方のクリアし、リンク上のトラフィックを暗号化します。MACsec を展開する前に **セキュリティで保護する必要があります** モードでのキーチェーンは影響を受けるリンクで展開する必要がありますまたはリンクがダウンします。たとえば、ポートをオンにできますで MACsec **セキュリティで保護する必要があります** モードがピアがしているリンクでのキーチェーンを受信する前にします。MACsec を導入することが推奨されて、この問題に対処する **セキュリティで保護する必要があります** モードとリンクの 1 回すべてにセキュリティ モードを変更 **セキュリティで保護する必要があります** 。

（注） MACsec インターフェイスの設定変更は、パケットのドロップになります。

MACsec ポリシー定義のキーチェーンの定義に固有の設定と機能の機能に関連する設定で構成されています。キーチェーン定義と機能の機能の定義は、別のポリシーに配置されます。MACsec 1 ポッドあたりまたはインターフェイスごとの有効化には、キーチェーン ポリシーおよび MACsec 機能のポリシーを組み合わせることが含まれます。

（注） 内部を使用して生成キーチェーンは、ユーザのキーチェーンを指定する必要はありません。

APIC アクセス MACsec

MACsec はリーフ スイッチ L3out インターフェイスと外部のデバイス間のリンクを保護するために使用します。APIC GUI および CLI のユーザを許可するで、MACsec キーとファブリック L3Out インターフェイスの設定を MacSec をプログラムを提供する物理/pc/vpc インターフェイスごと。ピアの外部デバイスが正しい MacSec 情報を使用してプログラムすることを確認するには、ユーザの責任です。

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）を使用して、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、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。

（注） 出力データ プレーン ポリサーは、スイッチ仮想インターフェイス（SVI）ではサポートされていません。

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、ACI ファブリックのファブリック アクセス（`infraInfra`）部分で構成され、ファブリック管理者が構成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、ACI ファブリックのテナント（`fvTenant`）部分で構成され、テナント管理者が構成できます。

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。

スケジューラ

スケジュールにより、設定のインポート/エクスポートまたはテクニカル サポートの収集などの操作を 1 つ以上の指定した時間帯に発生させることができます。

スケジュールには、一連のタイム ウィンドウ（オカレンス）が含まれます。これらのウィンドウは、1回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。期間や実行するタスクの最大数などのウィンドウで定義されているオプションにより、スケジュール設定されたタスクの実行時期が決定されます。たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、APIC が 1 つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する 1 つ以上のオカレンスが含まれています。オカレンスは次のいずれかになります。

- [One-time] ウィンドウ：一度だけ行うスケジュールを定義します。 これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。
- [Recurring] ウィンドウ：繰り返すスケジュールを定義します。この時間帯は、タスクの最大数に達するまで、または時間帯に指定された日の終わりに達するまで継続します。

スケジュールを構成すると、構成中に次のエクスポートポリシーとファームウェア ポリシーを選択して適用できます。

- テクニカル サポート エクスポートポリシー
- 構成エクスポートポリシー：日次自動バックアップ
- ファームウェアダウンロード

ファームウェア アップグレード

APIC 上のポリシーは、ファームウェア アップグレード プロセスの次の項目を管理します。

- 使用するファームウェアのバージョン。
- シスコから APIC リポジトリへのファームウェア イメージのダウンロード。
- 互換性の適用。
- アップグレードするもの：
  - スイッチ
  - 結果を表示するためのAPIC
  - 互換性カタログ
- アップグレードを実行する時期。
- 障害の処理方法（再試行、一時停止、無視など）。

各ファームウェア イメージには、サポートされるタイプおよびスイッチ モデルを識別する互換性カタログが含まれます。APICは、ファームウェア イメージ、スイッチ タイプ、およびそのファームウェア イメージを使用することを許可されるモデルのカタログを保持しています。デフォルトの設定では、互換性カタログに適合しない場合、ファームウェアの更新が拒否されます。

イメージ管理を実行する APIC には、互換性カタログ、APIC コントローラのファームウェア イメージおよびスイッチイメージのイメージリポジトリがあります。管理者は、イメージ ソース ポリシーを作成することで外部 HTTP サーバまたは SCP サーバから新しいファームウェア イメージを APIC イメージリポジトリにダウンロードできます。

APIC 上のファームウェア グループポリシーは、必要なファームウェア バージョンを定義します。

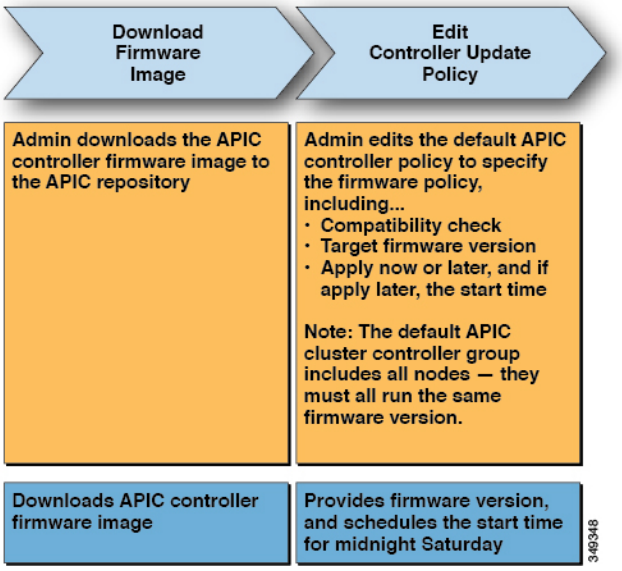
メンテナンス グループポリシーは、ファームウェアをアップグレードする時期、アップグレードするノード、および障害の処理方法を定義します。また、メンテナンス グループポリシーは、同時にアップグレードできるノードのグループを定義して、それらのメンテナンス グループをスケジュールに割り当てます。ノード グループ オプションには、すべてのリーフ ノード、すべてのスパイン ノード、またはファブリックの一部であるノードのセットが含まれます。

APIC コントローラのファームウェア アップグレード ポリシーは、クラスタ内のすべてのノードに常に適用されますが、アップグレードは常に一度に 1 つのノードに実行されます。APIC GUI により、ファームウェア アップグレードに関するリアルタイムのステータス情報が提供されます。

（注） 定期的アップグレードまたは1度だけのアップグレードのスケジュールに過去の日時が設定されている場合、スケジューラはただちにアップグレードをトリガーします。

次の図は、APIC クラスタ ノードのファームウェア アップグレードのプロセスを示します。

図 *36 : APIC* クラスタ コントローラのファームウェア アップグレードのプロセス



APIC は、次のようにこのコントローラのファームウェア アップグレード ポリシーを適用します。

- 管理者が土曜日の午前 0 時にコントローラ アップデート ポリシーを構成したため、 APIC は土曜日の午前 0 時にアップグレードを開始します。
- システムは、既存のファームウェアの互換性を確認し、新しいファームウェア イメージで提供される互換性カタログに従って、新しいバージョンにアップグレードします。
- アップグレードは、クラスタ内のすべてのノードがアップグレードされるまで、一度に 1 個のノードずつ行われます。

（注） APIC はノードの複製クラスタであるため、中断は最小限に抑えるべきです。管理者は、APIC のアップグレードのスケジュールを検討する際にシステムの負荷を認識し、メンテナンス期間中にアップグレードを計画する必要があります。

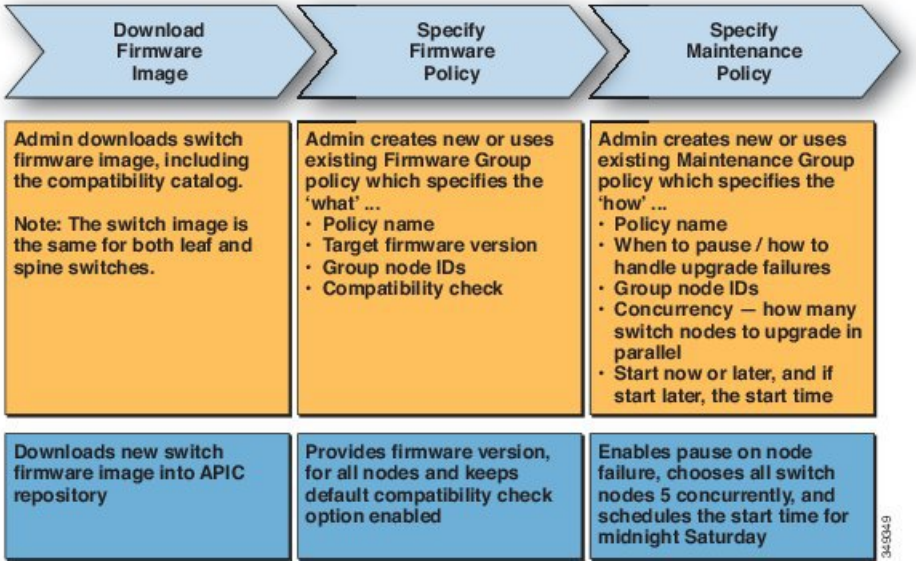
- APIC を含む ACI ファブリックは、アップグレードが進行中でも動作し続けます。

（注） コントローラのアップグレードはランダムに行われます。各APICコントローラはアップグレードに約10分かかります。コントローラのイメージがアップグレードされると、クラスタからドロップし、新しいバージョンで再起動します。その間、クラスタ内の他の APIC コントローラは動作しています。コントローラが再起動すると、クラスタに再び参加します。その後、クラスタが収束し、次のコントローラのイメージのアップグレードを開始します。クラスタがすぐに収束せず、完全な適合状態にならなければ、その後のアップグレードは、クラスタが収束して完全な適合状態になるまで待機状態になります。この期間中、「Waiting for Cluster Convergence」メッセージが表示されます。

- コントローラ ノードのアップグレードが失敗すると、アップグレードが一時停止し、手動による介入が行われるまで待機します。

次の図は、すべての ACI ファブリック スイッチ ノードのファームウェアをアップグレードするプロセスがどのように動作するかを示します。

図 *37 :* スイッチ ファームウェアのアップグレード プロセス



APIC は、次のようにこのスイッチ アップグレード ポリシーを適用します。

- 管理者が土曜日の午前 0 時にコントローラ アップデート ポリシーを構成したため、 APIC は土曜日の午前 0 時にアップグレードを開始します。
- システムは、既存のファームウェアの互換性を確認し、新しいファームウェアイメージで提供される互換性カタログに従って、新しいバージョンにアップグレードします。
- アップグレードは、すべての指定されたノードがアップグレードされるまで、一度に 5 個のノードずつ行われます。

（注） ファームウェアのアップグレードにより、スイッチがリブートします。リブートにより数分間スイッチの操作が中断される場合があります。メンテナンス期間中にファームウェアのアップグレードをスケジュールします。

- スイッチ ノードのアップグレードが失敗すると、アップグレードが一時停止し、手動による介入が行われるまで待機します。

ファームウェア アップグレードを実行するための詳細な手順については、『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』を参照してください。

設定ゾーン

構成ゾーンは、ACI ファブリックをさまざまなゾーンに分割します。これらのゾーンは、異なる時間で構成変更を使用して更新できます。これにより、トラフィックを中断させたり、ファ

ブリックをダウンさせたりする可能性のある、欠陥のあるファブリック全体の構成を展開するリスクを制限できます。管理者は、クリティカルでないゾーンに構成を展開し、それが適切であると判断した後でクリティカルなゾーンに展開することが可能です。

次のポリシーは、構成ゾーンのアクションを指定します。

- infrazone:ZoneP は、システムアップグレード時に自動的に作成されます。削除することも変更することもできません。
- infrazone:Zone には、1 つ以上のポッド グループ（PodGrp）または 1 つ以上のノード グループ（NodeGrp）が含まれます。

（注） PodGrp または NodeGrp のいずれかのみを選択できます。両方は選べません。

ノードは 1 つのゾーン（infrazone:Zone）のみに属することができます。NodeGrp には、名前と展開モードの 2 つのプロパティがあります。展開モードのプロパティは次のとおりです。

- enabled：保留中の更新がすぐに送信されます。
- disabled：新しい更新は延期されます。

（注）
- 無効な構成ゾーンでノードをアップグレード、ダウングレード、コミッション、またはデコミッションしないでください。
- 無効な構成ゾーンでノードのクリーンリロードまたはアップリンク/ダウンリンク ポート変換リロードを実行しないでください。

- triggered：保留中の更新はすぐに送信され、展開モードは変更が triggered 以前の値に自動的にリセットされます。

特定のノードセットでポリシーが作成、変更、または削除されると、ポリシーが展開されている各ノードに更新が送信されます。ポリシー クラスと infrazone の構成に基づいて、次のことが起こります。

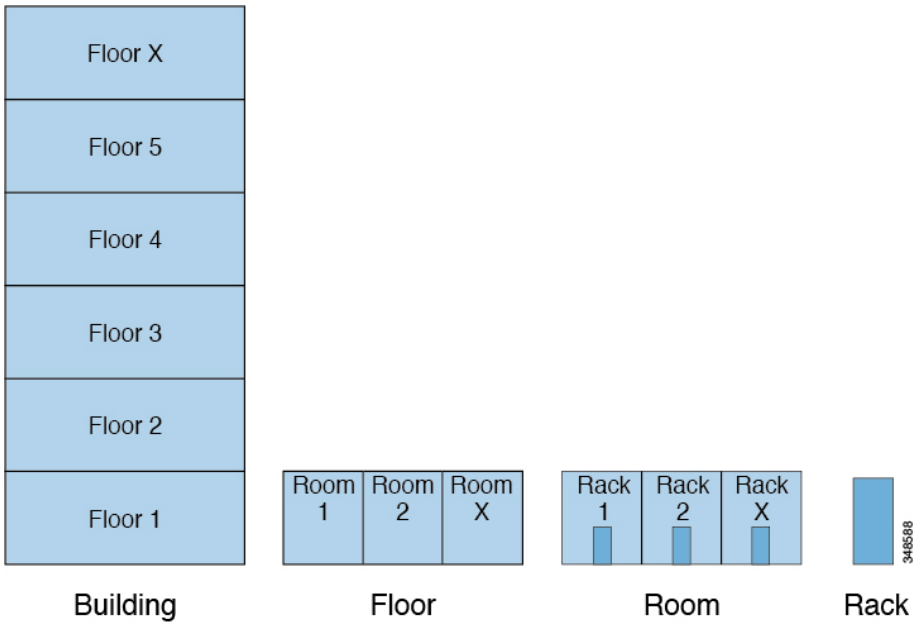
- infrazone 構成に従わないポリシーの場合、APIC はすべてのファブリック ノードに更新をすぐに送信します。
- infrazone 構成に従うポリシーの場合、更新は infrazone 構成に従って進行します。
  - ノードが infrazone:Zone の一部である場合、ゾーンの展開モードが有効に設定されている場合、更新はすぐに送信されます。それ以外の場合、更新は延期されます。

- ノードが infrazone:Zone の一部でない場合、更新はすぐに実行されます。これは、ACI ファブリックのデフォルトの動作です。

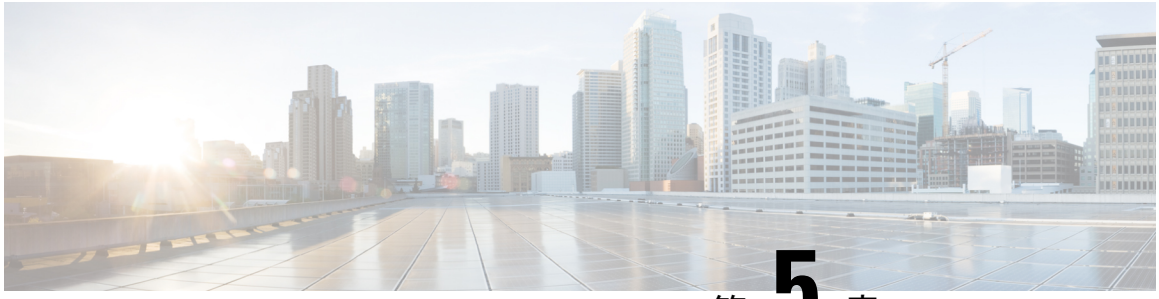
位置情報

管理者は、位置情報ポリシーを使用して、データセンター施設内の ACI ファブリック ノードの物理ロケーションをマッピングします。次の図は、地理位置情報マッピング機能の例を示します。

図 *38 :* 位置情報（*GeoLocation*）



たとえば、単一の部屋でのファブリック展開の場合は、管理者がデフォルトのルーム オブジェクトを使用して、スイッチの物理ロケーションに一致する 1 つ以上のラックを作成します。大規模な展開の場合、管理者は 1 つ以上のサイト オブジェクトを作成できます。各サイトには、1 つ以上の建物を含めることができます。各建物には、1 つ以上のフロアがあります。各フロアには 1 つ以上の部屋があり、各部屋には 1 つ以上のラックがあります。最後に、各ラックは 1 つ以上のスイッチに関連付けることができます。



第 5 章

ACI ファブリック内での転送

この章は、次の内容で構成されています。

- ACI ファブリック内の転送について （125 ページ）
- ACI ファブリックは現代のデータ センター トラフィック フローを最適化する （126 ページ）
- ACI で VXLAN （127 ページ）
- サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID （129 ページ）
- ポリシー ID と適用 （131 ページ）
- 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） （132 ページ）
- マルチキャスト ツリー トポロジ （138 ページ）
- トラフィック ストーム制御について （140 ページ）
- ストーム制御の注意事項と制約事項 （140 ページ）
- ファブリック ロード バランシング （143 ページ）
- エンドポイントの保持 （146 ページ）
- IP エンドポイントの学習動作 （148 ページ）
- プロキシ ARP について （149 ページ）
- ループ検出 （156 ページ）
- 不正なエンドポイントの検出 （159 ページ）
- TCP MSS調整について （160 ページ）

ACI ファブリック内の転送について

ACI ファブリックは、64,000 以上の専用テナント ネットワークをサポートしています。単一のファブリックは、100 万以上の IPv4/IPv6 エンドポイント、64,000 以上のテナント、および 200,000 以上の 10G ポートをサポートできます。ACI ファブリックにより、物理サービスと仮想サービス間を接続する追加のソフトウェアやハードウェア ゲートウェイを必要とすることなくサービス（物理または仮想）がどこでも可能になり、Virtual Extensible Local Area Network（VXLAN）/VLAN/Network Virtualization using Generic Routing Encapsulation（NVGRE）のカプセル化が正規化されます。

ACI ファブリックは、基盤となる転送グラフからエンドポイント ID ポリシーおよび関連するポリシーを分離します。また、最適なレイヤ 3 およびレイヤ 2 フォワーディングを保証する分散レイヤ 3 ゲートウェイが提供されます。ファブリックは、一般的な場所の制約（あらゆる場所の IP アドレス）なしで標準のブリッジングおよびルーティングのセマンティックをサポートし、IP コントロールプレーンの Address Resolution Protocol（ARP）/Gratuitous Address Resolution Protocol（GARP）に関するフラッディング要件を削除します。ファブリック内のすべてのトラフィックは、VXLAN 内にカプセル化されます。

ACI ファブリックは現代のデータ センター トラフィック フローを最適化する

Cisco ACI アーキテクチャは、従来のデータセンター設計から来る制限を解放して、最新のデータセンターで増大する East-West トラフィックの需要に対応します。

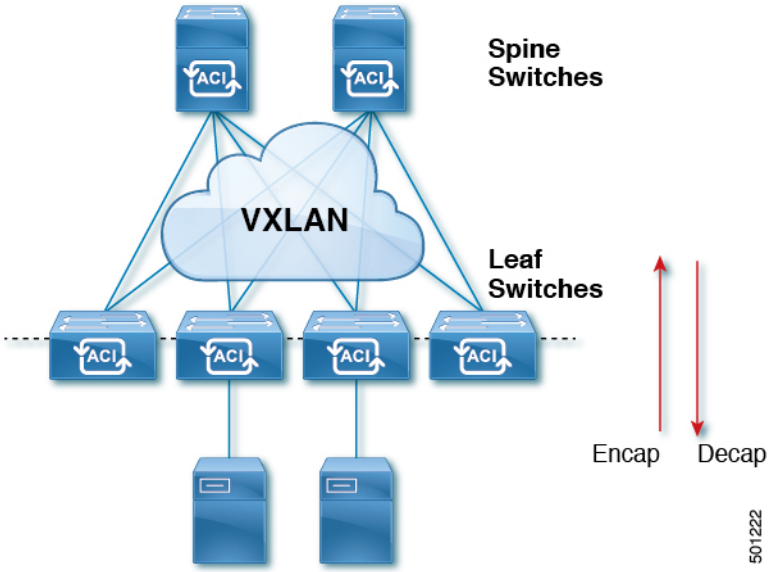
今日のアプリケーション設計は、データセンターのアクセス レイヤを通る、サーバ間の East-West トラフィックを増大させています。このシフトを促進しているアプリケーションには、Hadoop のようなビッグデータの分散処理の設計 、VMware vMotion のようなライブの仮想マシンまたはワークロードの移行、サーバのクラスタ リング、および多層アプリケーションなどが含まれます。

North-South トラフィックは、コア、集約、およびアクセス レイヤ、またはコラプスト コアとアクセス レイヤが重要となる、従来型のデータセンター設計を推進します。クライアントデータはWAN またはインターネットで受信され、サーバの処理を受けた後、データセンターを出ます。このような方式のため、WAN またはインターネットの帯域幅の制限により、デーセンターのハードウェアは過剰設備になりがちです。ただし、スパニング ツリー プロトコルが、ループをブロックするために要求されます。これは、ブロックされたリンクにより利用可能な帯域幅を制限し、トラフィックが準最適なパスを通るように強制する可能性があります。

従来のデータセンター設計においては、、IEEE 802.1Q VLAN がレイヤ 2 境界の論理セグメンテーションまたはまたはブロードキャスト ドメインを提供します。ただし、ネットワーク リンクの VLAN の使用は効率的ではありません。データセンター ネットワークでデバイスの配置要件は柔軟性に欠け、VLAN の最大値である 4094 の VLAN が制限となり得ます。IT 部門とクラウドプロバイダが大規模なマルチテナントデータセンターを構築するようになるにつれ、VLAN の制限は問題となりつつあります。

スパイン リーフ アーキテクチャは、これらの制限に対処します。ACI ファブリックは、外界からは、ブリッジングとルーティングが可能な単一のスイッチに見えます。レイヤ 3 のルーティングをアクセス レイヤに移動すると、最新のアプリケーションが必要としている、レイヤ 2 の到達可能性が制限されます。仮想マシン ワークロード モビリティや一部のクラスタ リングのソフトウェアのようなアプリケーションは、送信元と宛先のサーバ間がレイヤ 2 で隣接していることを必要とします。アクセス レイヤでルーティングを行えば、トランク ダウンされた同じ VLAN の同じアクセス スイッチに接続したサーバだけが、レイヤ 2 で隣接します。ACI では、VXLAN が、基盤となるレイヤ 3 ネットワーク インフラストラクチャからレイヤ 2 のドメインを切り離すことにより、このジレンマを解決します。

図 *39 : ACI* ファブリック



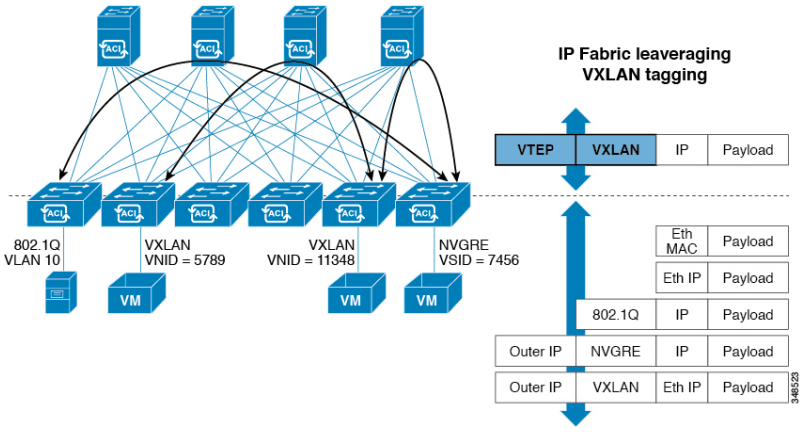
トラフィックがファブリックに入ると、ACIがカプセル化してポリシーを適用し、必要に応じてスパイン スイッチ (最大 2 ホップ) によってファブリックを通過させ、ファブリックを出るときにカプセル化を解除します。ファブリック内では、ACIはエンドポイント間通信でのすべての転送について、Intermediate System-to-Intermediate System プロトコル (IS-IS) および Council of Oracle Protocol (COOP) を使用します。これにより、すべての ACI リンクがアクティブで、ファブリック内での等コストマルチパス (ECMP) 転送と高速再コンバージョンが可能になります。ファブリック内と、ファブリックの外部のルータ内でのソフトウェア定義ネットワーク間のルーティング情報を伝播するために、 ACI はマルチプロトコル Border Gateway Protocol (MP-BGP) を使用します。

ACI で VXLAN

VXLAN は、レイヤ 2 オーバーレイの論理ネットワークを構築するレイヤ 3 のインフラストラクチャ上でレイヤ 2 のセグメントを拡張する業界標準プロトコルです。ACIインフラストラクチャ レイヤ 2 ドメインが隔離ブロードキャストと障害ブリッジ ドメインをオーバーレイ内に存在します。このアプローチは大きすぎる、障害ドメインの作成のリスクなしで大きくなるデータセンター ネットワークを使用できます。

すべてのトラフィック、ACIファブリックはVXLANパケットとして正規化されます。入力でACI VXLANパケットで外部VLAN、VXLAN、およびNVGREパケットをカプセル化します。次の図は、ACIカプセル化の正規化を示します。

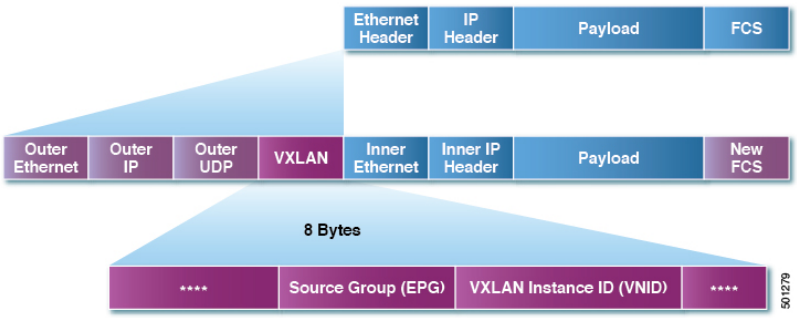
図 *40 : ACI* カプセル化の正規化



ACI ファブリックでの転送は、カプセル化のタイプまたはカプセル化のオーバーレイ ネットワークによって制限または制約されません。ACI ブリッジ ドメインのフォワーディング ポリシーは、必要な場合に標準の VLAN 動作を提供するために定義できます。

ファブリック内のすべてのパケットにACIポリシー属性が含まれているため、ACIは完全に分散された方法でポリシーを一貫して適用できます。ACIにより、アプリケーションポリシーのEPGIDが転送から分離されます。次の図に示すように、ACIVXLANヘッダーは、ファブリック内のアプリケーション ポリシーを特定します。

図 *41 : ACI VXLAN* のパケット形式



ACIVXLAN パケットには、レイヤ 2 の MAC アドレスとレイヤ 3 IP アドレスの送信元と宛先フィールド、ファブリック内の効率的なと拡張性の転送を有効にします。ACIVXLAN パケット ヘッダーの送信元グループ フィールドは、パケットが属するアプリケーション ポリシー エンドポイント グループ (EPG) を特定します。VXLAN インスタンス ID (VNID) は、テナントの仮想ルーティングおよび転送 (VRF) ドメイン ファブリック内で、パケットの転送を有効にします。VXLAN ヘッダーで 24 ビット VNID フィールドでは、同じネットワークで一意レイヤ 2 のセグメントを最大 16 個の拡張アドレス空間を提供します。この拡張アドレス空間は、大規模なマルチテナント データセンターを構築する柔軟性 IT 部門とクラウド プロバイダーを提供します。

VXLANを有効にACIファブリック全体にわたってスケールでの仮想ネットワーク インフラストラクチャのレイヤ 3 のアンダーレイ レイヤ 2 を展開します。アプリケーション エンドポイント ホスト柔軟に配置できます、アンダーレイ インフラストラクチャのレイヤ 3 バウンダリ

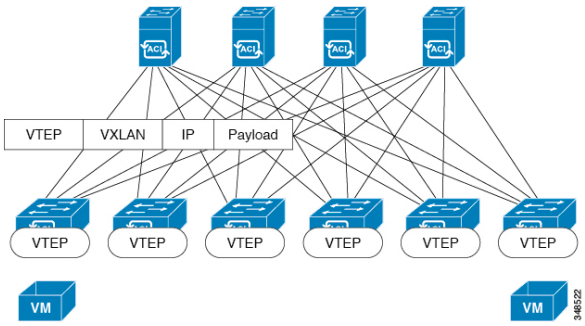
のリスクなしでデータセンター ネットワーク間をオーバーレイ ネットワーク、VXLAN でレイヤ 2 の隣接関係を維持します。

サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID

ACI ファブリックは、ACI ファブリック VXLAN ネットワーク間のルーティングを実行するテナントのデフォルト ゲートウェイ機能を備えています。各テナントに対して、ファブリックはテナントに割り当てられたすべてのリーフ スイッチにまたがる仮想デフォルト ゲートウェイを提供します。これは、エンドポイントに接続された最初のリーフ スイッチの入力インターフェイスで提供されます。各入力インターフェイスはデフォルト ゲートウェイ インターフェイスをサポートします。ファブリック全体のすべての入力インターフェイスは、特定のテナント サブネットに対して同一のルータの IP アドレスと MAC アドレスを共有します。

ACI ファブリックは、エンドポイントのロケータまたは VXLAN トンネル エンドポイント (VTEP) アドレスで定義された場所から、テナント エンドポイント アドレスとその識別子を切り離します。ファブリック内の転送は VTEP 間で行われます。次の図は、ACI で切り離された ID と場所を示します。

図 *42 : ACI* によって切り離された *ID* と場所



VXLAN は VTEP デバイスを使用してテナントのエンド デバイスを VXLAN セグメントにマッピングし、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP 機能には、次の 2 つのインターフェイスがあります。

- ブリッジングを介したローカル エンドポイント通信をサポートするローカル LAN セグメントのスイッチ インターフェイス
- 転送 IP ネットワークへの IP インターフェイス

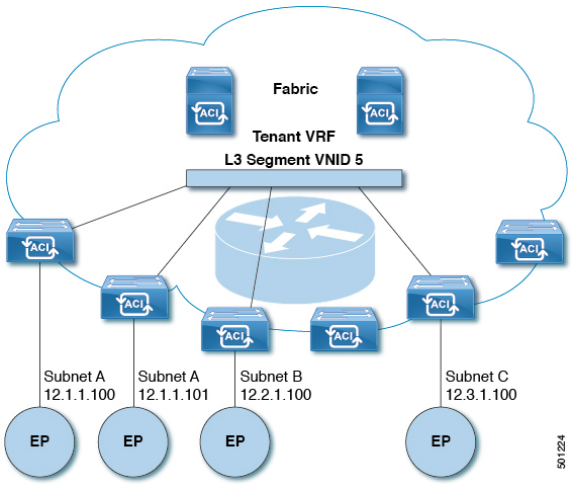
IP インターフェイスには一意の IP アドレスがあります。これは、インフラストラクチャ VLAN として知られる、転送 IP ネットワーク上の VTEP を識別します。VTEP デバイスはこの IP アドレスを使用してイーサネット フレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。また、VTEP デバイスはリモート VTEP で VXLAN セグメントを検出し、IP インターフェイスを介してリモートの MAC Address-to-VTEP マッピングについて学習します。

ACI の VTEP は分散マッピング データベースを使用して、内部テナントの MAC アドレスまたはIP アドレスを特定の場所にマッピングします。VTEP はルックアップの完了後に、宛先リーフ スイッチ上の VTEP を宛先アドレスとして、VXLAN 内でカプセル化された元のデータ パケットを送信します。宛先リーフ スイッチはパケットをカプセル化解除して受信ホストに送信します。このモデルにより、ACI はスパニングツリー プロトコルを使用することなく、フル メッシュでシングル ホップのループフリー トポロジを使用してループを回避します。

VXLAN セグメントは基盤となるネットワーク トポロジに依存しません。逆に、VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。これは送信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてパケットをカプセル化します。

次の図は、テナント内のルーティングがどのように行われるかを示します。

図 *43 : ACI* のサブネット間のテナント トラフィックを転送するレイヤ *3 VNID*



ACI はファブリックの各テナント VRF に単一の L3 VNID を割り当てます。ACI は、L3 VNID に従ってファブリック全体にトラフィックを転送します。出力リーフ スイッチでは、ACI によって L3 VNID からのパケットが出力サブネットの VNID にルーティングされます。

ACI のファブリック デフォルト ゲートウェイに送信されてファブリック入力に到達したトラフィックは、レイヤ 3 VNID にルーティングされます。これにより、テナント内でルーティングされるトラフィックはファブリックで非常に効率的に転送されます。このモデルを使用すると、たとえば同じ物理ホスト上の同じテナントに属し、サブネットが異なる 2 つの VM 間では、トラフィックが (最小パス コストを使用して) 正しい宛先にルーティングされる際に経由する必要があるは入力スイッチ インターフェイスのみです。

ACI ルート リフレクタは、ファブリック内での外部ルートの配布にマルチプロトコル BGP（MP-BGP）を使用します。ファブリック管理者は自律システム (AS) 番号を提供し、ルート リフレクタにするスパイン スイッチを指定します。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定することを推奨します。

IGP プロトコル パケット（EIGRP、OSPFv3）は、インターフェイス MTU サイズに基づいてコンポーネントによって構築されます。 Cisco ACIでは、CPU MTU サイズがインターフェイス MTU サイズよりも小さく、構築されたパケットサイズが CPU MTU より大きい場合、パケットはカーネルによってドロップされます（特に IPv6）。このような制御パケットのドロップを回避するには、コントロールプレーンとインターフェイスの両方で常に同じ MTU 値を設定します。

Cisco ACI、Cisco NX-OS、および Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS および Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

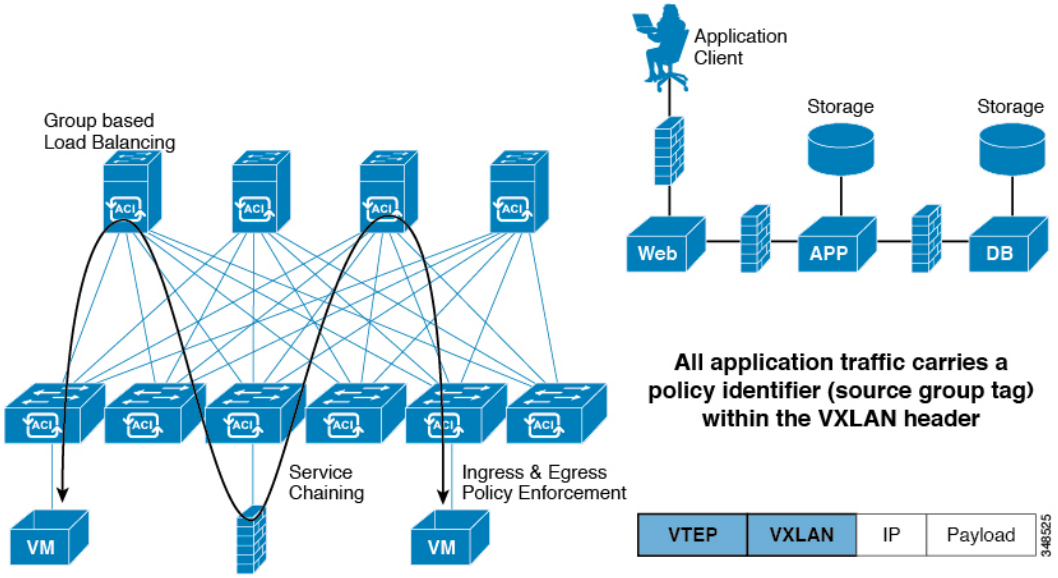
各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で、コマンド、ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1 を使用してください。

ポリシー ID と適用

アプリケーション ポリシーは、VXLAN パケットで送信される個別のタギング属性を使用して転送から分離されます。ポリシー ID は、ACI ファブリック内のすべてのパケットで送信され、完全に分散した形でポリシーの一貫した適用を行うことができます。次の図は、ポリシー ID を示します。

図 *44 :* ポリシー *ID* と適用



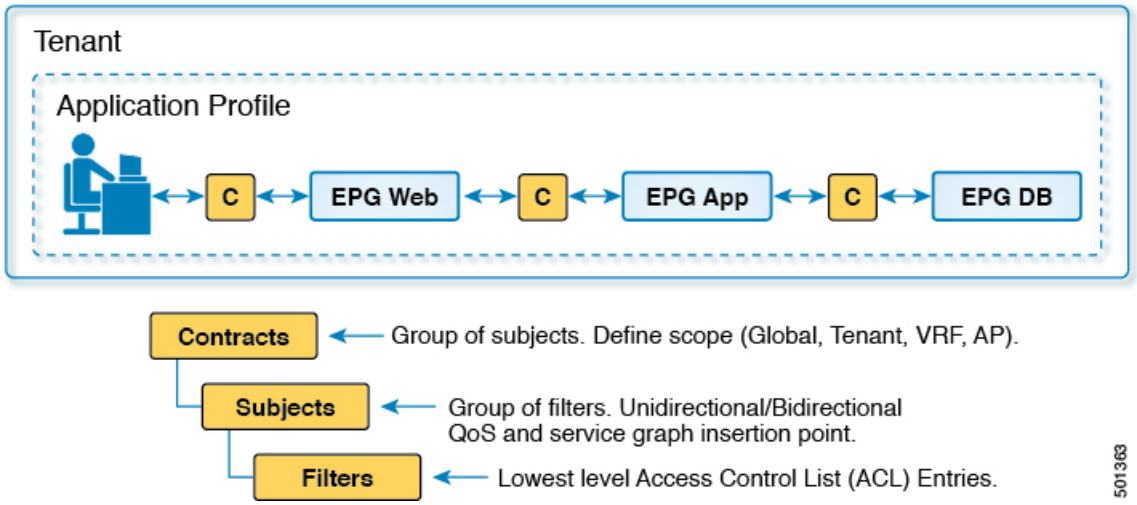
ファブリックおよびアクセスポリシーは、内部のファブリック インターフェイスおよび外部のアクセスインターフェイスの動作を管理します。システムは、デフォルトのファブリックおよびアクセスポリシーを自動的に作成します。ファブリックの管理者（ファブリック全体へのアクセス権がある者）は、要件に応じてデフォルトのポリシーを変更したり、新しいポリシーを作成できます。ファブリックおよびアクセスポリシーにより、さまざまな機能やプロトコルを有効にできます。APICのセレクタにより、ファブリックの管理者は、ポリシーを適用するノードおよびインターフェイスを選択できます。

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 *45* : 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。

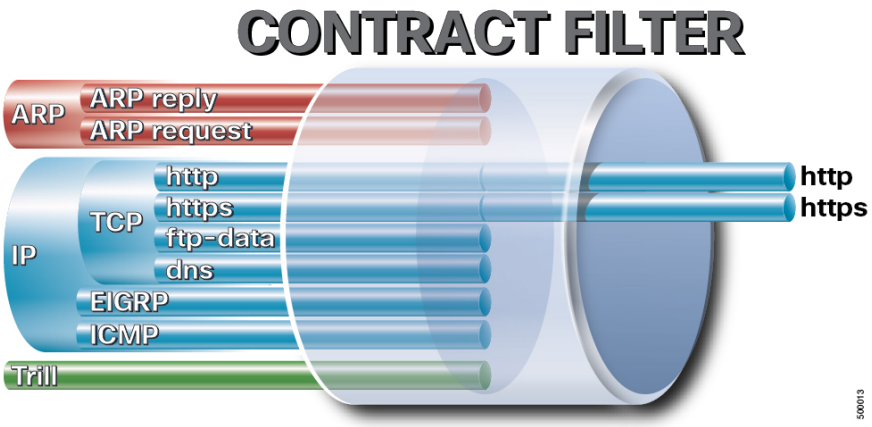
また EPG とコントラクトの関係には方向性があります。EPG はコントラクトを提供または消費できます。コントラクトを提供する EPG は通常、一連のクライアント デバイスにサービスを提供する一連のエンドポイントです。そのサービスによって使用されるプロトコルはコントラクトで定義されます。コントラクトを消費する EPG は通常、そのサービスのクライアントである一連のエンドポイントです。クライアント エンドポイント (コンシューマ) がサーバ エンドポイント(プロバイダー)に接続しようとすると、コントラクトはその接続が許可されるかどうかを確認します。特に指定のない限り、そのコントラクトは、サーバが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

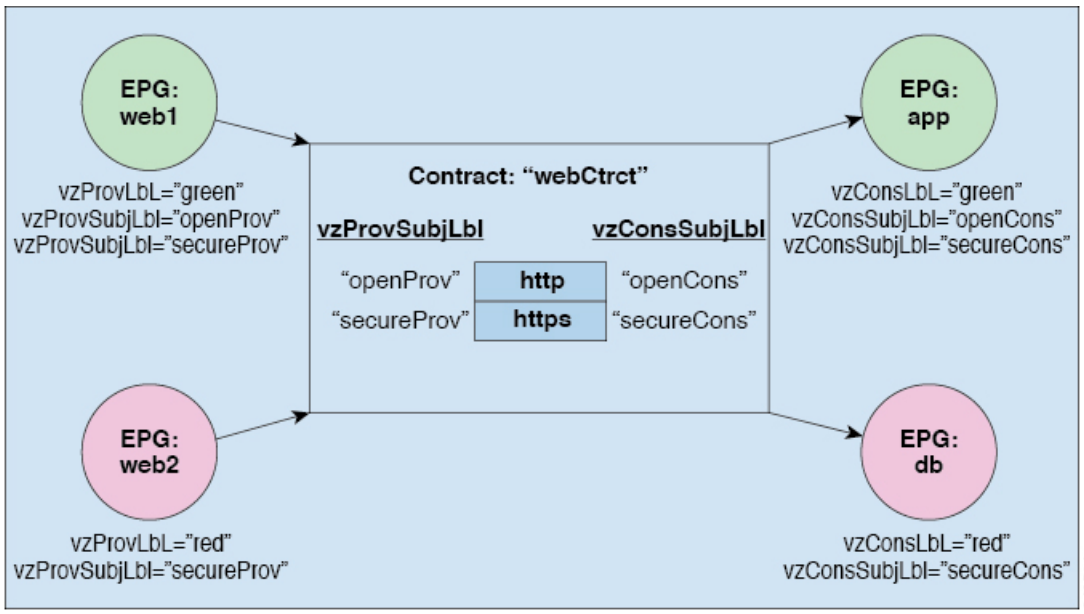
コントラクトは階層的に構築されます。1 つ以上のサブジェクトで構成され、各サブジェクトには 1 つ以上のフィルタが含まれ、各フィルタは 1 つ以上のプロトコルを定義できます。

図 *46* : 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 *47* : *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。

マルチキャスト ツリー トポロジ

ACIファブリックは、アクセス ポートからのユニキャスト、マルチキャスト、およびブロードキャスト トラフィックの転送をサポートします。エンドポイント ホストからのすべてのマルチデスティネーション トラフィックは、ファブリックにマルチキャスト トラフィックとして伝送されます。

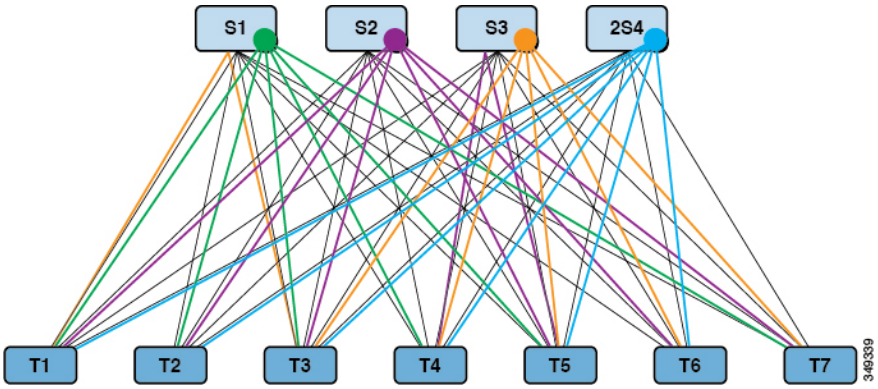
ACI ファブリックは、入力インターフェイスに入るトラフィックを使用可能な中間ステージのスパイン スイッチを介して関連する出力スイッチにルーテッドできる Clos トポロジ（Charles Clos にちなんで名付けられた）に接続されるスパインおよびリーフスイッチで構成されます。リーフスイッチには次の 2 種類のポートがあります。スパイン スイッチに接続するためのファブリック ポートと、サーバー、サービス アプライアンス、ルータ、Fabric Extender（FEX; ファブリックエクステンダ）などを接続するアクセス ポートです。

リーフスイッチ（top-of-rack（ToR; トップオブラック）スイッチとも呼ばれます）は、スパイン スイッチ(「エンド オブ ロウ」または「EoR」スイッチとも呼ばれます）に接続されます。リーフスイッチは互いに接続されず、スパイン スイッチはリーフスイッチのみに接続します。この Clos トポロジでは、すべての下位層のスイッチがフルメッシュ トポロジの最上位層のスイッチにそれぞれ接続されます。スパイン スイッチに不具合があると、ACI ファブリック全体のパフォーマンスだけがわずかに低下します。データ パスは、トラフィック負荷がスパイン スイッチ間で均等に分散されるように選択されます。

ACI ファブリックは、Forwarding Tag（FTAG）ツリーを使用してバランス マルチデスティネーション トラフィックをロードします。すべてのマルチデスティネーション トラフィックは、ファブリック内でカプセル化された IP マルチキャスト トラフィックの形式で転送されます。入力リーフは、FTAG をスパインに転送するときにトラフィックに割り当てます。FTAG は接続先マルチキャストアドレスの一部としてパケットに割り当てられます。ファブリックでは、トラフィックは指定された FTAG ツリーに沿って転送されます。スパインおよび中間リーフスイッチは、FTAG ID に基づいてトラフィックを転送します。転送ツリーは、FTAG ID 1 つにつき 1 つ構築されます。任意の 2 つのノード間で、FTAG 1 つにつきリンク 1 つだけが転送されます。複数の FTAG を使用することで、転送に異なるリンクを使用している各 FTAG でパラレル リンクを使用できます。ファブリック内の FTAG ツリーの数が多いほど、ロード バランシングの効果が大きい可能性があるということになります。ACI ファブリックは、最大 12 個の FTAG をサポートします。

次の図は、4 つの FTAG によるトポロジを示します。ファブリック内のすべてのリーフスイッチは、各 FTAG に直接または中継ノードを介して接続されます。1 つの FTAG が各スパイン ノードに根付いています。

図 *48 :* マルチキャスト ツリー トポロジ



リーフスイッチはスパインへの直接接続性がある場合、直接パスを使用して FTAG ツリーに接続します。直接リンクがない場合、リーフスイッチは上記の図に示すように FTAG ツリーに接

続されている中継ノードを使用します。図には、各スパインが 1 つの FTAG ツリーのルートとして示されていますが、複数の FTAG ツリー ルートを 1 つのノード上に置くことができます。

ACI ファブリック起動検出プロセスの一環として、FTAG ルートはスパイン スイッチに配置されます。APIC は、各スパイン スイッチをスパインがアンカーする FTAG で構成します。ルートの ID と FTAG の数は構成から取得されます。APIC は、使用される FTAG ツリーの数と各ツリーに対するルートを指定します。FTAG ツリーは、ファブリックでトポロジの変更があるたびに再計算されます。

ルートの配置は誘導される構成で、スパイン スイッチの障害などのランタイム イベントで動的に再度ルート付けされることはありません。通常、FTAG 構成は静的です。スパイン スイッチの追加または削除時は、管理者がスパイン スイッチの残りのセットまたは拡張セット間で FTAG を再配布することを決める可能性があるため、FTAG はあるスパインから別のスパインへ再アンカーできます。

トラフィック ストーム制御について

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御ポリシーを使用すると、物理インターフェイス上におけるブロードキャスト、未知のマルチキャスト、または未知のユニキャストのトラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防ぐことができます。

デフォルトでは、ストーム制御は ACI ファブリックでは有効になっていません。ACI ブリッジ ドメイン（BD）レイヤ 2 の未知のユニキャストのフラッディングは BD 内でデフォルトで有効になっていますが、管理者が無効にすることができます。その場合、ストーム制御ポリシーはブロードキャストと未知のマルチキャストのトラフィックにのみ適用されます。レイヤ 2 の未知のユニキャストのフラッディングが BD で有効になっている場合、ストーム制御ポリシーは、ブロードキャストと未知のマルチキャストのトラフィックに加えて、レイヤ 2 の未知のユニキャストのフラッディングに適用されます。

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信するブロードキャスト、マルチキャスト、未知のユニキャストのトラフィックのレベルを 1 秒間隔でモニタできます。この間に、トラフィック レベル（ポートで使用可能な合計帯域幅のパーセンテージ、または特定のポートで許可される 1 秒あたりの最大パケット数として表されます）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。管理者は、ストーム制御しきい値を超えたときにエラーを発生させるようにモニタリング ポリシーを設定できます。

ストーム制御の注意事項と制約事項

以下のガイドラインと制約事項に従って、トラフィック ストーム制御レベルを設定してください。

- 通常、ファブリック管理者は以下のインターフェイスのファブリック アクセス ポリシーでストーム制御を設定します。
  - 標準トランク インターフェイス。
  - 単一リーフ スイッチ上のダイレクト ポート チャネル。
  - バーチャル ポート チャネル（2 つのリーフ スイッチ上のポート チャネル）。
- リリース 4.2(1) 以降では、ストーム制御のしきい値に達した場合に、次の制約事項に従って、SNMP トラップをCisco Application Centric Infrastructure（ACI）からトリガーできるようになりました。
  - ストーム制御に関連するアクションには、ドロップとシャットダウンの 2 つがあります。シャットダウン アクションでは、インターフェイス トラップが発生しますが、ストームがアクティブまたはクリアであることを示すためのストーム制御トラップは、シャットダウンアクションによっては決定されません。したがって、ポリシーでシャットダウンアクションが設定されているストーム制御トラップは無視する必要があります。
  - ストーム制御ポリシーがオンの状態でポートがフラップすると、統計情報の収集時にクリア トラップとアクティブ トラップが一緒に表示されます。通常、クリア トラップとアクティブ トラップは一緒に表示されませんが、この場合は予期される動作です。
- ポート チャネルおよびバーチャル ポート チャネルでは、ストーム制御値（1 秒あたりのパケット数またはパーセンテージ）はポート チャネルのすべての個別メンバーに適用されます。

（注） Cisco Application Policy Infrastructure Controller（APIC）リリース 1.3(1) およびスイッチ リリース 11.3(1) 以降のスイッチ ハードウェアの場合、ポート チャネル設では、集約ポートのトラフィック抑制は設定値の最大 2 倍になることがあります。新しいハードウェア ポートは slice-0 と slice-1 の 2 つのグループに内部的にさらに分割されています。スライス マップを確認するには、`vsh_lc` コマンドの `show platform internal hal l2 port gpd` を使用して、`Sl` カラムで `slice 0` または `slice 1` を探します。ポート チャネル メンバーがスライス 0 とスライス 1 の両方に該当する場合、式は各スライスに基づいて計算されるため、許可されるストーム制御トラフィックが設定値の 2 倍になることがあります。

- 使用可能な帯域幅のパーセンテージで設定する場合、値 100 はトラフィック ストーム制御を行わないことを意味し、値 0.01 はすべてのトラフィックを抑制します。
- ハードウェアの制限およびさまざまなサイズのパケットのカウント方式が原因で、レベルのパーセンテージは概数になります。着信トラフィックを構成するフレームのサイズに応

じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。1 秒あたりのパケット数（PPS）の値は、256 バイトに基づいてパーセンテージに変換されます。

- 最大バーストは、通過するトラフィックがないときに許可されるレートの最大累積です。トラフィックが開始されると、最初の間隔では累積レートまでのすべてのトラフィックが許可されます。後続の間隔では、トラフィックは設定されたレートまでのみ許可されます。サポートされる最大数は 65535 KB です。設定されたレートがこの値を超えると、PPS とパーセンテージの両方についてこの値で制限されます。
- 累積可能な最大バーストは 512 MB です。
- 最適化されたマルチキャスト フラッディング（OMF）モードの出力リーフ スイッチでは、トラフィック ストーム制御は適用されません。
- OMF モードではない出力リーフ スイッチでは、トラフィック ストーム制御が適用されます。
- FEX のリーフ スイッチでは、ホスト側インターフェイスにはトラフィック ストーム制御を使用できません。
- Cisco Nexus C93128TX、C9396PX、C9396TX、C93120TX、C9332PQ、C9372PX、C9372TX、C9372PX-E、C9372TX-E の各スイッチでは、トラフィック ストーム制御のユニキャスト/マルチキャストの差別化がサポートされていません。
- Cisco Nexus C93128TX、C9396PX、C9396TX、C93120TX、C9332PQ、C9372PX、C9372TX、C9372PX-E、C9372TX-E の各スイッチでは、トラフィック ストーム制御の SNMP トラップがサポートされていません。
- Cisco Nexus C93128TX、C9396PX、C9396TX、C93120TX、C9332PQ、C9372PX、C9372TX、C9372PX-E、C9372TX-E の各スイッチでは、トラフィック ストーム制御トラップがサポートされていません。
- ストーム制御アクションは、物理イーサネット インターフェイスおよびポート チャネル インターフェイスでのみサポートされます。

  リリース 4.1(1) 以降では、ストーム制御**シャットダウン**オプションがサポートされています。デフォルトの Soak Instance Count を持つインターフェイスに対して**シャットダウン**アクションが選択されると、しきい値を超えるパケットは 3 秒間ドロップされ、ポートは 3 秒間シャットダウンされます。デフォルトのアクションは、**ドロップ**です。**シャットダウン**アクションを選択すると、ユーザーはソーキング間隔を指定するオプションを使用できます。デフォルトのソーキング間隔は 3 秒です。設定可能な範囲は 3 ～ 10 秒です。
- インターフェイスに設定されたデータ プレーン ポリシング（DPP）ポリサーの値がストーム ポリサーの値よりも低い場合、DPP ポリサーが優先されます。DPPポリサーとストーム ポリサーの間に設定されている低い方の値が、設定されたインターフェイスで適用されます。
- リリース 4.2(6) 以降、ストーム ポリサーは、DHCP、ARP、ND、HSRP、PIM、IGMP、および EIGRP プロトコルに対応する、リーフ スイッチのすべての転送制御トラフィックに強制されます。このことは、ブリッジ ドメインが**BD でのフラッディング**または**カプセル**

化でのフラッディングのどちらに設定されているかには関係しません。この動作の変更は、EX 以降のリーフスイッチにのみ適用されます。

- EX スイッチでは、プロトコルの 1 つに対し、スーパーバイザ ポリサーとストーム ポリサーの両方を設定できます。この場合、サーバーが設定されたスーパーバイザ ポリサー レート（制御プレーン ポリシング、CoPP）よりも高いレートでトラフィックを送信すると、ストーム ポリサーはストーム ポリサー レートとして設定されているよりも多くのトラフィックを許可します。着信トラフィック レートがスーパーバイザ ポリサー レート以下の場合、ストーム ポリサーは設定されたストーム トラフィック レートを正しく許可します。この動作は、設定されたスーパーバイザ ポリサーおよびストーム ポリサーのレートに関係なく適用されます。
- ストーム ポリサーが、指定されたプロトコルのリーフ スイッチで転送されるすべての制御トラフィックに適用されるようになった結果、リーフ スイッチで転送される制御トラフィックがストーム ポリサー ドロップの対象になります。以前のリリースでは、この動作の変更の影響を受けるプロトコルでは、このようなストーム ポリサーのドロップは発生しません。

- トラフィック ストーム制御は、PIM が有効になっているブリッジ ドメインまたは VRF インスタンスのマルチキャスト トラフィックをポリシングできません。
- ストーム コントロール ポリサーがポートチャネル インターフェイスに適用されている場合、許可されるレートが設定されているレートを超えることがあります。ポート チャネルのメンバー リンクが複数のスライスにまたがる場合、許可されるトラフィック レートは、構成されたレートにメンバー リンクがまたがるスライスの数を掛けたものに等しくなります。

  ポートからスライスへのマッピングは、スイッチ モデルによって異なります。

  例として、ストーム ポリサー レートが 10Mbps のメンバー リンク port1、port2、および port3 を持つポートチャネルがあるとします。

  - port1、port2、port3 が slice1 に属している場合、トラフィックは 10Mbps にポリシングされます。
  - port1 と port2 が slice1 に属し、port3 が slice2 に属している場合、トラフィックは 20Mbps にポリシングされます。
  - port1 が slice1 に属し、port2が slice2 に属し、port3 が slice3 に属している場合、トラフィックは 30Mbps にポリシングされます。

ファブリック ロード バランシング

Cisco Application Centric Infrastructure（ACI）ファブリックでは、利用可能なアップリンク リンク間のトラフィックを平衡化するためのロード バランシング オプションがいくつか提供されます。ここでは、リーフからスパインへのスイッチ トラフィックのロード バランシングについて説明します。

スタティック ハッシュ ロードバランシングは、各フローが5タプルのハッシュに基づいてアップリンクに割り当てられるネットワークで使用される従来のロードバランシング機構です。このロードバランシングにより、使用可能なリンクにほぼ均等な流量が分配されます。通常、流量が多いと、流量の均等な分配により帯域幅も均等に分配されます。ただし、いくつかのフローが残りよりも多いと、スタティック ロード バランシングにより完全に最適ではない結果がもたらされる場合があります。

Cisco ACI ファブリック ダイナミック ロードバランシング（DLB）は、輻輳レベルに従ってトラフィック割り当てを調整します。DLB では、使用可能なパス間の輻輳が測定され、輻輳状態が最も少ないパスにフローが配置されるので、データが最適またはほぼ最適に配置されます。

DLB は、フローまたはフローレットの粒度を使用して使用可能なアップリンクにトラフィックを配置するように設定できます。フローレットは、時間の大きなギャップによって適切に区切られるフローからのパケットのバーストです。パケットの2つのバースト間のアイドル間隔が使用可能なパス間の遅延の最大差より大きい場合、2 番目のバースト（またはフローレット）を1つ目とは異なるパスに沿ってパケットのリオーダーなしで送信できます。このアイドル間隔は、フローレット タイマーと呼ばれるタイマーによって測定されます。フローレットにより、パケット リオーダーを引き起こすことなくロードバランシングに対する粒度の高いフローの代替が提供されます。

DLB 動作モードは積極的または保守的です。これらのモードは、フローレット タイマーに使用するタイムアウト値に関係します。アグレッシブ モードのフローレット タイムアウトは比較的小さい値です。この非常に精密なロード バランシングはトラフィックの分配に最適ですが、パケット リオーダーが発生する場合があります。ただし、アプリケーションのパフォーマンスに対する包括的なメリットは、保守的なモードと同等かそれよりも優れています。保守的なモードのフローレット タイムアウトは、パケットが並び替えられないことを保証する大きな値です。新しいフローレットの機会の頻度が少ないので、トレードオフは精度が低いロードバランシングです。DLB は常に最も最適なロード バランシングを提供できるわけではありませんが、スタティック ハッシュ ロード バランシングより劣るということはありません。



（注） すべての Nexus 9000 シリーズ スイッチには DLB のハードウェア サポートがありますが、DLB 機能は、第 2 世代プラットフォーム（EX、FX、および FX2 サフィックスを持つスイッチ）の現在のソフトウェア リリースでは有効になっていません。

Cisco ACI ファブリックは、リンクがオフラインまたはオンラインになったことで使用可能なリンク数が変化すると、トラフィックを調整します。ファブリックは、リンクの新しいセットでトラフィックを再分配します。

スタティックまたはダイナミックのロードバランシングのすべてのモードでは、トラフィックは、Equal Cost Multipath (ECMP) の基準を満たすアップリンクまたはパス上でのみ送信され、これらのパスはルーティングの観点から同等で最もコストがかかりません。

ロードバランシング技術ではありませんが、Dynamic Packet Prioritization（DPP）は、スイッチで DLB と同じメカニズムをいくつか使用します。DPP の設定は DLB 専用です。DPP は、長いフローよりも短いフローを優先します。短いフローは約 15 パケット未満です。短いフローは

長いフローよりも遅延の影響を受けやすいため、DPPはアプリケーション全体のパフォーマンスを向上させることができます。

6.0（1）および6.0（2）リリースでは、イントラリーフ スイッチ トラフィックの場合、カスタム QoS 構成に関係なく、すべての DPP 優先トラフィックが CoS 0 とマークされます。リーフ間スイッチ トラフィックの場合、カスタムQoS構成に関係なく、すべてのDPP優先トラフィックが CoS 3 とマークされます。6.0（3）リリース以降、イントラリーフ スイッチおよびインターリーフ スイッチのトラフィックでは、カスタム QoS 構成に関係なく、すべての DPP 優先トラフィックが CoS 0 とマークされます。

GPRS トンネリング プロトコル（GTP）は、主にワイヤレス ネットワークでデータを配信するために使用されます。Cisco Nexus スイッチは Telcom データセンター内の場所です。パケットがデータセンターの Cisco Nexus 9000 スイッチを介して送信される場合、トラフィックは GTP ヘッダーに基づいてロード バランシングされる必要があります。ファブリックがリンク バンドルを介して外部ルータに接続されている場合、トラフィックはすべてのバンドル メンバー（たとえば、レイヤ 2 ポート チャネル、レイヤ 3 ECMP リンク、レイヤ 3 ポート チャネル、およびポート チャネル上の L3Out）に均等に分散される必要があります。）。GTP トラフィックのロード バランシングは、ファブリック内でも実行されます。

GTP ロード バランシングを実現するために、Cisco Nexus 9000 シリーズ スイッチは 5 タプルのロード バランシング メカニズムを使用します。ロードバランシング メカニズムでは、パケットの送信元 IP、宛先 IP、プロトコル、レイヤ 4 リソース、および宛先ポート（トラフィックが TCP または UDP の場合）フィールドが考慮されます。GTP トラフィックの場合は、これらのフィールドへの一意の値の数が限られていると、トンネルでのトラフィック ロードの均等分散が制限されます。

ロード バランシングにおける GTP トラフィックの極性化を回避するために、GTP ヘッダーのトンネル エンドポイント ID（TEID）が UDP ポート番号の代わりに使用されます。TEID がトンネルごとに異なるため、トラフィックをバンドルの複数のリンク間で均等にロードバランシングすることができます。

GTP ロード バランシングは、GTPU パケットに存在する 32 ビット TEID 値で送信元および宛先ポート情報を上書きします。

GTP トンネルのロード バランシング機能により、次のサポートが追加されます。

- 物理インターフェイスでの IPv4/IPv6 トランスポート ヘッダーによる GTP
- UDP ポート 2152 を使用した GTPU

Cisco ACIファブリックのデフォルト構成では、従来の静的なハッシュが使用されます。スタティックなハッシュ機能により、アップリンク間のトラフィックがリーフ スイッチからスパイン スイッチに分配されます。リンクがダウンまたは起動すると、すべてのリンクのトラフィックが新しいアップリンク数に基づいて再分配されます。

リーフ/スパイン スイッチ ダイナミック ロード バランシング アルゴリズム

次の表に、リーフ/スパイン スイッチ ダイナミック ロード バランシングで使用されるデフォルトの設定不可能なアルゴリズムを示します。

表 *8 : Cisco ACI*リーフ/スパイン スイッチ ダイナミック ロード バランシング

Traffic Type	データ ポイントのハッシュ
リーフ/スパイン IP ユニキャスト	• 送信元 MAC アドレス • 宛先 MAC アドレス • 送信元 IP アドレス • 宛先 IP アドレス • プロトコル タイプ • 送信元レイヤ 4 ポート • 宛先レイヤ 4 ポート • セグメント ID（VXLAN VNID）または VLAN ID
リーフ/スパイン レイヤ 2	• 送信元 MAC アドレス • 宛先 MAC アドレス • セグメント ID（VXLAN VNID）または VLAN ID

エンドポイントの保持

スイッチでキャッシュ エンドポイントの MAC アドレスと IP アドレスを保持することで、パフォーマンスが向上します。スイッチは、アクティブになるときにエンドポイントについて学習します。ローカル エンドポイントはローカル スイッチにあります。リモート エンドポイントは他のスイッチにありますが、ローカルでキャッシュされます。リーフスイッチは、直接（または直接接続されたレイヤ2スイッチまたはファブリックエクステンダを通じて）接続されたエンドポイント、ローカルエンドポイント、およびファブリックの他のリーフスイッチに接続されたエンドポイント（ハードウェアのリモート エンドポイント）に関する場所とポリシーの情報を保存します。スイッチは、ローカル エンドポイントには 32 Kb エントリ キャッシュを、リモート エンドポイントには 64 Kb エントリ キャッシュを使用します。

リーフスイッチで稼働するソフトウェアは、これらのテーブルを能動的に管理します。ローカル的に接続されたエンドポイントでは、ソフトウェアは各エントリの保持タイマーの期限切れ後にエントリをエージング アウトします。エンドポイント エントリは、エンドポイントのアクティビティが終了するとスイッチ キャッシュからプルーニングされ、エンドポイントの場所が他のスイッチに移動するか、またはライフサイクルの状態がオフラインに変わります。ローカル保持タイマーのデフォルト値は15分です。非アクティブのエントリを削除する前に、リーフスイッチはエンドポイントに 3 つの ARP 要求を送信し、実際になくなっているかを確認します。スイッチが ARP 応答を受信しない場合、エントリはプルーニングされます。リモート

で接続されたエンドポイントの場合、スイッチは非アクティブになってから5分後にエントリをエージング アウトします。リモート エンドポイントは、再度アクティブになるとテーブルにすぐに再入力されます。



（注） バージョン 1.3(1g) では、仮想ホストおよびローカル ホストに対してトリガーされるサイレント ホスト トラッキングが追加されています。

エンドポイントが再度キャッシュされるまでリモート リーフスイッチで適用されるポリシー以外にテーブルにリモートエンドポイントがなくても、パフォーマンスのペナルティはありません。

ブリッジドメインのサブネットが *enforced* に構成されている場合、エンドポイント保持ポリシーは次のように動作します。

- ブリッジ ドメインのサブネットに含まれていない IP アドレスを持つ新しいエンドポイントは学習されません。
- デバイスが追跡に応答しない場合、学習済みのエンドポイントはエンドポイント保持キャッシュからエージアウトします。

この実施プロセスは、サブネットがブリッジドメインで定義されているかどうか、またはサブネットが EPG で定義されているかどうかに関係なく、同じように動作します。

エンドポイントの保持タイマー ポリシーは変更できます。静的エンドポイントの MAC および IP アドレスを設定すると、保持タイマーをゼロに設定することで、スイッチ キャッシュに永久的に保存できます。エントリの保持タイマーをゼロに設定することは、それが自動的に削除されないことを意味します。この操作は慎重に行う必要があります。エンドポイントが移動したりポリシーが変化する場合は、 APIC を介してエントリを手動で最新情報に更新する必要があります。保持タイマーがゼロ以外の場合、この情報は APIC の介入なしで各パケットで確認されほぼ瞬時に更新されます。

エンドポイントの保持ポリシーは、プルーニングがどのように行われるかを決定します。ほとんどの場合、デフォルトのポリシーアルゴリズムが使用されます。エンドポイントの保持ポリシーを変更すると、システムパフォーマンスに影響を与える場合があります。何千ものエンドポイントと通信するスイッチの場合、エージング間隔を短くすると、多数のアクティブなエンドポイントをサポートするのに使用可能なキャッシュ ウィンドウの数が増えます。エンドポイントの数が 10,000 を超える場合は、複数のスイッチにエンドポイントを分散させることを推奨します。

デフォルトのエンドポイント保持ポリシーの変更に関しては、次のガイドラインに従ってください。

- リモート バウンス間隔 =（リモート エージ * 2）+ 30 秒
  - 推奨されるデフォルト値：
    - ローカル エイジ = 900 秒
    - リモート エージ = 300 秒

- バウンス エージ = 630 秒

- アップグレードに関する考慮事項：リリース 1.0(1k) より前の ACI バージョンにアップグレードする場合は、テナント共通のエンドポイント保持ポリシー（`epRetPol`）のデフォルト値が次のようになっていることを確認してください: バウンス期間 = 660 秒。

IP エンドポイントの学習動作

ACI ブリッジ ドメインがユニキャスト ルーティングを有効にして構成されている場合、MAC アドレスを学習するだけでなく、MAC アドレスに関連付けられた IP アドレスも学習します。

ACI は MAC アドレスを追跡し、ブリッジ ドメインごとに一意である必要があります。ACI では、エンドポイントは単一の MAC アドレスに基づいていますが、任意の数の IP アドレスをブリッジ ドメインの単一の MAC アドレスに関連付けることができます。ACI は、これらの IP アドレスを MAC アドレスにリンクします。MAC アドレスが、IP アドレスのみを持つエンドポイントを表す場合があります。

したがって、ACIは次のようにローカルエンドポイントを学習して保存する場合があります。

- MACアドレスのみ
- 単一の IP アドレスを持つ MAC アドレス
- 複数の IP アドレスを持つ MAC アドレス

3 番目のケースは、サーバーがプライマリおよびセカンダリ IP アドレスなど、同じ MAC アドレスに複数の IP アドレスを持っている場合に発生します。また、ACI ファブリックがファブリック上のサーバーの MAC アドレスと IP アドレスを学習したが、サーバーの IP アドレスがその後変更された場合にも発生する可能性があります。これが発生すると、ACI は MAC アドレスを保存し、古い IP アドレスと新しい IP アドレスの両方にリンクします。ACI ファブリックがエンドポイントをベース MAC アドレスでフラッシュするまで、古い IP アドレスは削除されません。

ACI でのローカル エンドポイントの移動には、主に 2 つのタイプがあります。

- MAC アドレスが別のインターフェイスに移動する場所
- IP アドレスが別の MAC アドレスに移動する場所

MAC アドレスが別のインターフェイスに移動すると、ブリッジドメインの MAC アドレスにリンクされているすべての IP アドレスも一緒に移動します。ACI ファブリックは、IP アドレスのみが移動した場合（および新しい MAC アドレスを受信した場合）も移動を追跡します。これは、たとえば、仮想サーバーの MAC アドレスが変更され、新しい ESXI サーバー（ポート）に移動された場合に発生する可能性があります。

VRF 内の複数の MAC アドレスに IP アドレスが存在する場合、これは IP フラップが発生したことを示しています（これは、ファブリック転送の決定に悪影響を与える可能性があります）。

これは、レガシー ネットワークの 2 つの個別のインターフェイスでの MAC フラッピング、またはブリッジドメインでの MAC フラップに似ています。

IP フラップが発生する可能性のあるシナリオの 1 つは、サーバーのネットワーク情報カード（NIC）ペアがアクティブ/アクティブに設定されているが、その2つが単一の論理リンク（ポートチャネルや仮想ポートチャネルなど）で接続されていない場合です。このタイプのセットアップにより、単一の IP アドレス（仮想マシンの IP アドレスなど）が、ファブリック内の 2 つの MAC アドレス間を常に移動する可能性があります。

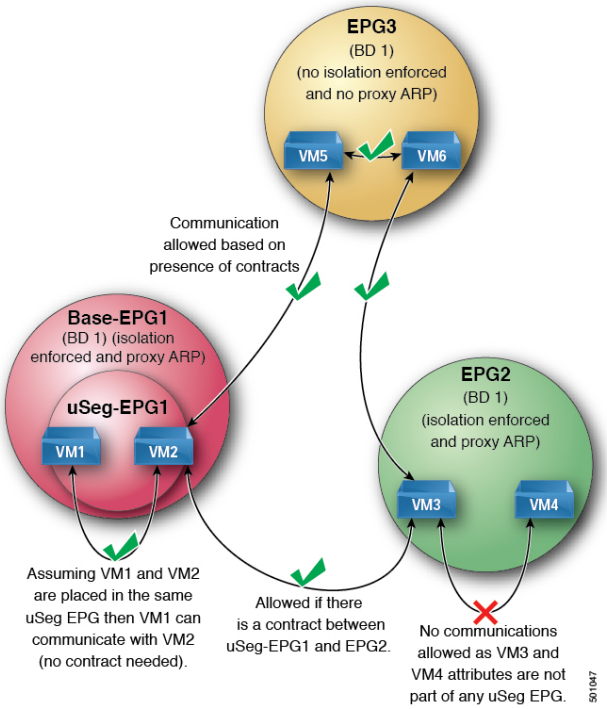
この種の動作に対処するには、NIC ペアを VPC の 2 つのレッグとして構成して、アクティブ/アクティブ セットアップを実現することをお勧めします。サーバー ハードウェアがアクティブ/アクティブ構成（ブレード シャーシなど）をサポートしていない場合、アクティブ/スタンバイ タイプの NIC ペア構成も IP フラッピングの発生を防ぎます。

プロキシ ARP について

Cisco ACI のプロキシ ARP は、ネットワークまたはサブネット内のエンドポイントが、別のエンドポイントの MAC アドレスを知らなくても、そのエンドポイントと通信できるようにします。プロキシ ARP はトラフィックの宛先場所を知っており、代わりに、最終的な宛先として自身の MAC アドレスを提供します。

プロキシ ARP を有効にするには、EPG 内エンドポイント分離を EPG で有効にする必要があります。詳細については、次の図を参照してください。EPG 内エンドポイント分離と Cisco ACI の詳細については、「*Cisco ACI* 仮想化ガイド」を参照してください。

図 *49 :* プロキシ *ARP* および *Cisco APIC*



Cisco ACI ファブリック内のプロキシ ARP は従来のプロキシ ARP とは異なります。通信プロセスの例として、プロキシ ARP が EPG で有効になっているとき、エンドポイント A が ARP 要求をエンドポイント B に送信し、エンドポイント B がファブリック内で学習される場合、エンドポイント A はブリッジ ドメイン（BD）MAC からプロキシ ARP 応答を受信します。エンドポイント A が B、エンドポイントの ARP 要求を送信し、エンドポイント B はすでに ACI ファブリック内で学習しない場合は、ファブリックはプロキシ ARP の BD 内で要求を送信します。エンドポイント B は、ファブリックに戻る要求、このプロキシ ARP に応答します。この時点では、ファブリックはプロキシ ARP エンドポイント A への応答を送信しませんが、エンドポイント B は、ファブリック内で学習します。エンドポイント A は、エンドポイント B に別の ARP 要求を送信する場合、ファブリックはプロキシ ARP 応答から送信 BD mac です。

次の例ではプロキシ ARP 解像度がクライアント VM1 と VM2 間の通信の手順します。

1. VM2 通信を VM1 が必要です。

図 *50 : VM2* 通信を *VM1* が必要です。

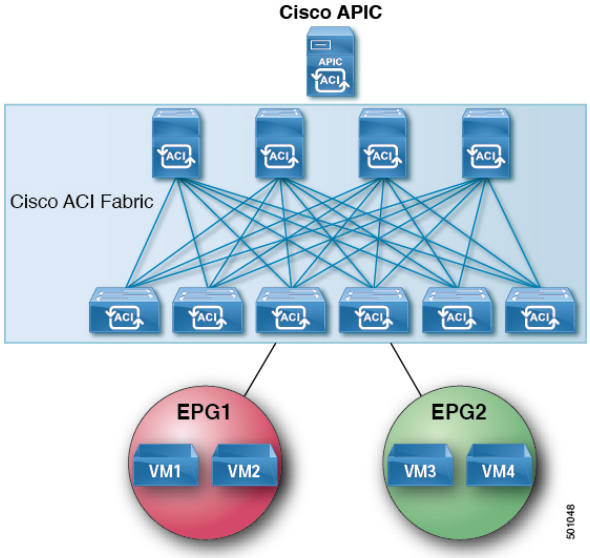


表 *9 : ARP* 表の説明

デバイス	状態
VM1	IP = * MAC = *
ACI ファブリック	IP = * MAC = *
VM2	IP = * MAC = *

2. VM1 は、ブロードキャスト MAC アドレスとともに ARP 要求を VM2 に送信します。

図 *51 : VM1* はブロードキャスト *MAC* アドレスとともに *ARP* 要求を *VM2* に送信します

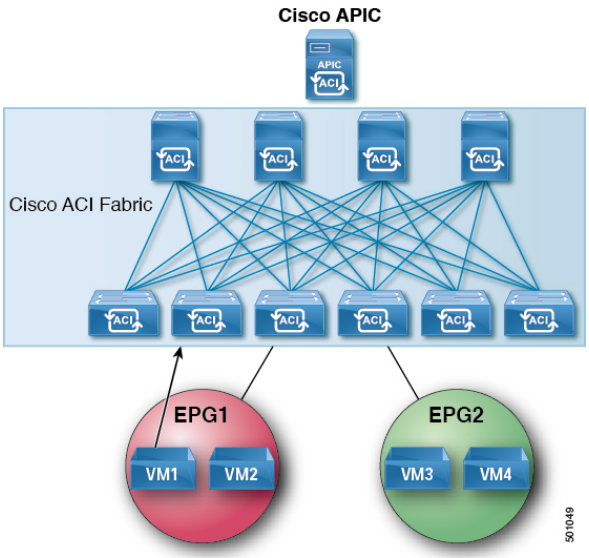


表 *10 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC
VM2	IP = * MAC = *

3. ACI ファブリックは、ブリッジ ドメイン（BD）内のプロキシ ARP 要求をフラッディングします。

図 *52 : ACI* ファブリックは *BD* 内のプロキシ *ARP* 要求をフラッディングします

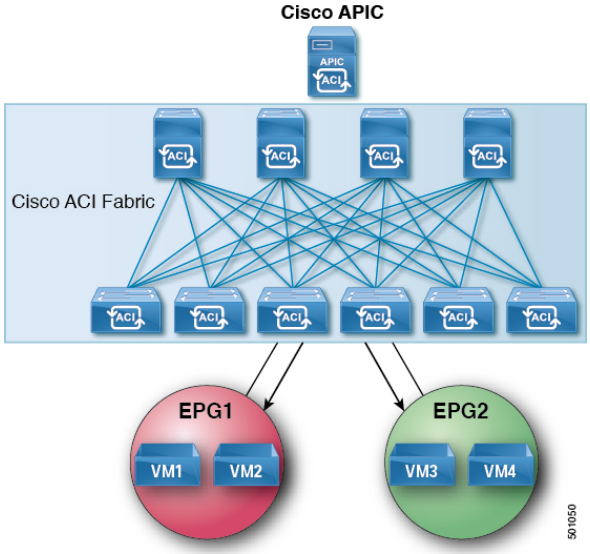


表 *11 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC
VM2	IP = VM1 IP; MAC = BD MAC

4. VM2 は、ARP 応答を ACI ファブリックに送信します。

図 *53 : VM2* は *ARP* 応答を *ACI* ファブリックに送信します

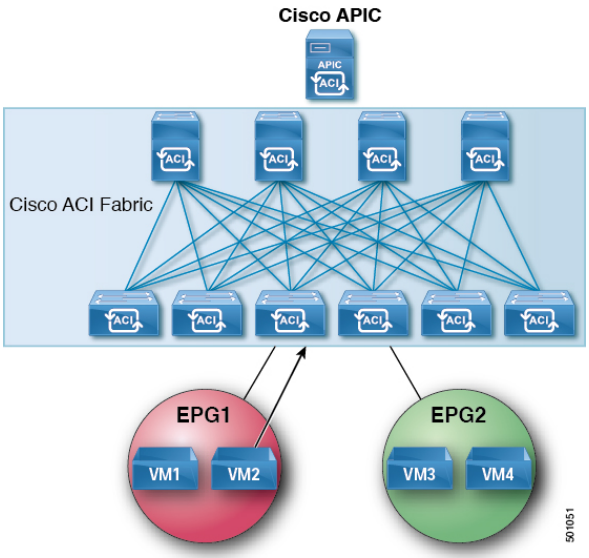


表 *12 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC
VM2	IP = VM1 IP; MAC = BD MAC

5. VM2 が学習されます。

図 *54 : VM2* が学習されます

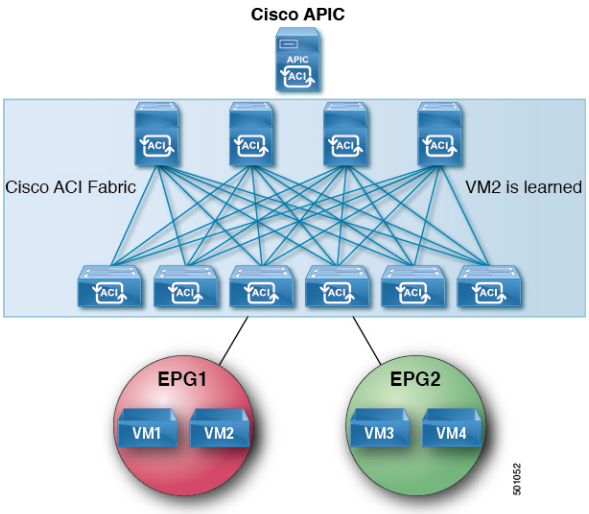


表 *13* : *ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC IP = VM2 IP; MAC = VM2 MAC
VM2	IP = VM1 IP; MAC = BD MAC

6. VM1 は、ブロードキャスト MAC アドレスとともに ARP 要求を VM2 に送信します。

図 *55* : *VM1* はブロードキャスト *MAC* アドレスとともに *ARP* 要求を *VM2* に送信します

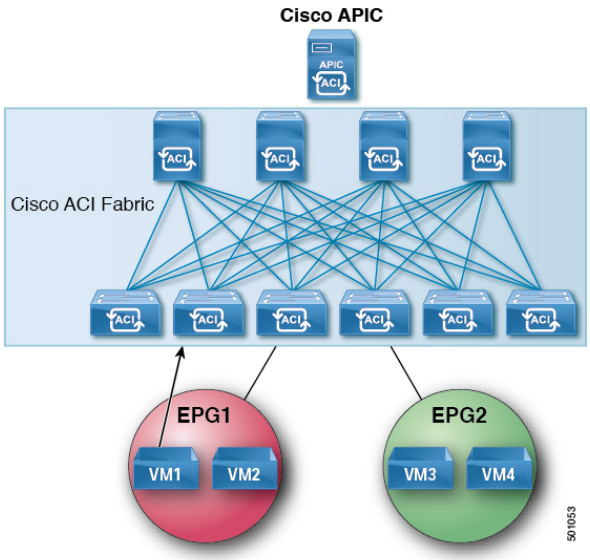


表 *14* : *ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC IP = VM2 IP; MAC = VM2 MAC
VM2	IP = VM1 IP; MAC = BD MAC

7. ACI ファブリックは、プロキシ ARP VM1 への応答を送信します。

図 *56 : ACI* ファブリック *VM1* にプロキシ *ARP* 応答を送信します。

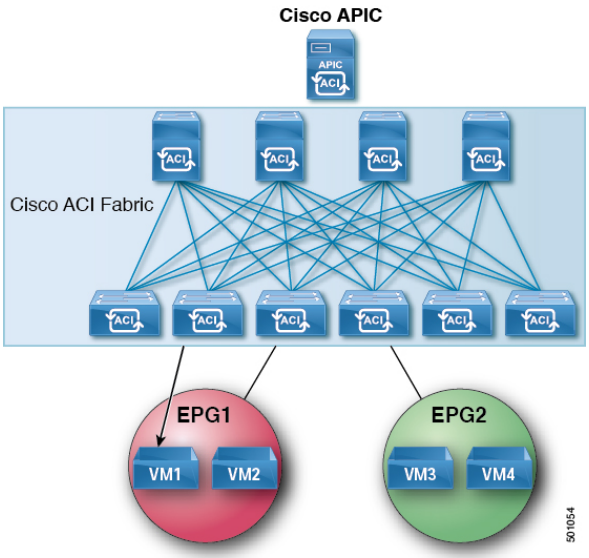


表 *15 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP;MAC = BD MAC
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC IP = VM2 IP; MAC = VM2 MAC
VM2	IP = VM1 IP; MAC = BD MAC

ループ検出

Cisco Application Centric Infrastructure（ACI）ファブリックは、Cisco ACI アクセス ポートに接続されているレイヤ2ネットワーク セグメントのループを検出できるグローバルなデフォルト ループ検出ポリシーを提供します。これらのグローバル ポリシーはデフォルトで無効になっていますが、ポート レベルのポリシーはデフォルトで有効になっています。グローバル ポリシーを有効にすると、個々のポート レベルで無効にされていない限り、すべてのアクセス ポート、仮想ポート、および仮想ポート チャネル（VPC）でポリシーが有効になります。

Cisco ACI ファブリックは、スパニングツリープロトコル（STP）に参加していません。代わりに、ループを検出するために、ミスケーブル プロトコル（MCP）を実装します。MCP は、外部レイヤ 2 ネットワークで実行されている STP と補完的に機能します。

（注） スパニングツリーを実行し、Cisco ACI ファブリックに接続されている外部スイッチからのインターフェイスは、loop_inc ステータスになる可能性があります。外部スイッチからのポートチャネルをフラッピングすると、問題が解決します。外部スイッチでBDPUフィルタを有効にするか、ループガードを無効にすると、問題を回避できます。

ファブリック管理者は、Cisco ACI ファブリックによって開始されたMCPパケットを識別するためにMCPが使用するキーを提供します。管理者は、MCPポリシーがループを識別する方法と、ループに対処する方法（syslog のみ、またはポートを無効にする）を選択できます。

VM の移動などのエンドポイントの移動は正常ですが、頻度が高く、移動の間隔が短い場合は、ループの兆候である可能性があります。個別のグローバルなデフォルトエンドポイント移動ループ検出ポリシーを使用できますが、デフォルトでは無効になっています。管理者は、移動検出ループに対処する方法を選択できます。

また、エラー無効化の回復ポリシーは、管理者が構成できる間隔の後に、検出をループするポートを有効にし、BPDU ポリシーを無効にすることができます。

MCP はネイティブ VLAN モードで実行され、デフォルトでは、送信される MCP BPDU に VLAN タグが付けられません。MCPは、ネイティブVLANで送信されたパケットがファブリックによって受信された場合、ケーブル接続の誤りによるループを検出できますが、EPGVLANの非ネイティブ VLAN にループがある場合は検出されません。リリース 2.0(2) 以降、Cisco Application Policy Infrastructure Controller（APIC）は構成された EPG 内のすべての VLAN で MCP BPDU の送信をサポートしているため、それらの VLAN 内のループが検出されます。新しい MCP 構成モードでは、送信される PDU に各 EPG VLAN ID を持つ 802.1Q ヘッダーを追加することにより、物理ポートが属するすべての EPG VLAN で MCP PDU が送信されるモードで動作するように MCP を構成できます。

3.2(1) リリース以降、Cisco ACI ファブリックは 100 ミリ秒から 300 秒の送信頻度でより高速なループ検出を提供します。

5.2(3) リリース以降では、いずれかのインターフェイスで 256 を超える VLAN を動作させようとすると、フォールト F4268 が生成されます。いずれかのリーフスイッチで 2000 を超える論理ポート（ポート x VLAN）動作させようとすると、フォールト F4269 が生成されます。

（注） VLAN ごとの MCP は、インターフェイスごとに 256 の VLAN でのみ実行されます。256 を超える VLAN がある場合、最初の数値の 256 VLAN が選択されます。

MCP は、Fabrix Extender（FEX）ホスト インターフェイス（HIF）ポートではサポートされていません。

Mis-cabling プロトコルのモード

MCP は 2 つのモードで動作できます。

- 非厳格モード：MCP対応ポートが*UP*の場合、データトラフィックとコントロールプレーン トラフィック（STP、MCP プロトコル パケットなど）が受け入れられます。MCP はリンクのループを監視し、ループが検出されると、リンクはエラー ディセーブルになります。このモードでは、グローバル MCP インスタンス ポリシーに従って、パケットが 2 秒間隔で送信されます。このモードでのループ検出のデフォルト時間は 7 秒です。

- 厳格モード：リリース 5.2(4) 以降、MCP は厳格モードをサポートします。MCP が有効になっているポートが起動するとすぐに、ループをチェックするために MCP パケットが短期間、アグレッシブな間隔で送信されます。これは早期ループ検出フェーズと呼ばれ、データトラフィックを受け入れる前に、リンク（ポートに接続されている）にループがないかどうかがチェックされます。ループが検出されると、ポートはエラーディセーブルになり、シャットダウンされます。ループが検出されない場合、ポートはデータトラフィックの転送を開始します。MCPは、グローバルMCPインスタンス ポリシーに従って、非アグレッシブタイマーを使用してパケットの送信を開始します。

  すでに *UP* 状態のポートで MCP 厳格モードが構成されている場合、MCP はこのポートで早期ループ検出を実行しません。MCP 厳格モード構成のポートをフラップして、すぐに有効にします。

  MCP 厳格モードのイベント シーケンス：

  1. MCP対応ポートが起動すると、初期遅延タイマーが開始されます。リンクレベルの制御パケット（LLDP、CDP、STPなど）のみが受け入れられ、転送されます。この期間中、データトラフィックは受け入れられません。初期遅延タイマーは、外部 L2 ネットワークでSTPがコンバージするための時間です。デフォルト値は0ですが、トポロジと外部ネットワークでのスパニングツリーの構成方法によっては、STP が収束してループを切断するまでの時間を確保するために、初期遅延を 45 ～ 60 秒に設定することもできます（必要な場合）。外部 L2 ネットワークで STP が有効になっていない場合は、初期遅延タイマーを 0 に設定する必要があります。

  2. 猶予期間タイマーは、初期遅延タイマーが期限切れになった後に開始されます。この間ポートは、ループ検出に使用される MCP パケットをアグレッシブに送信します。この間に、早期のループ検出が行われます。ループが検出されると、ポートはエラーディセーブルになります。デフォルト値は3秒です。この期間中、データ トラフィックは受け入れられません。

     猶予タイマー期間中、MCP は次のグローバル MCP インスタンス ポリシー構成を上書きします。

     - ループが検出されると、GUI で **[ポート無効化（Port Disable）]** チェックボックスが選択されていなくても、MCP はポートをエラー ディセーブルにします。
     - MCP の倍率が 1 より大きい値に設定されている場合でも、単一の MCP フレームを受信するとループと見なされます。

  3. 猶予期間タイマーが期限切れになり、ループが検出されなくなると、ポートは転送ステートに移行し、データトラフィックが受け入れられます。MCPパケットは、グローバルな送信頻度構成に従って、非アグレッシブな間隔で送信されます。

MCP 厳格モードのガイドラインおよび制約事項

次のガイドラインおよび制約事項に従って、厳格モード MCP を構成します。

- MCP 厳格モードは FEX ポートではサポートされません。
- MCP 厳格モードは QinQ エッジ ポートではサポートされません。
- ポートで MCP 厳格モードが有効になっている場合、vPC 高速コンバージェンスはサポートされません。 vPC トラフィックは、収束に時間がかかります。
- 厳格モードの MCP 制御パケットは、APIC リリース 5.2(4) より前のバージョンを実行しているリーフスイッチではデコードできません。したがって、厳格ループ検出を機能させるには、MCP に参加するすべてのリーフスイッチに 5.2(4) の最小バージョンが必要です。
- APIC バージョン 5.2(4) より前のリリースにファブリックをダウングレードする前に、MCP 対応ポートで厳格モードを無効にします。厳格モードが無効になっていない場合、厳格ループ検出は以前のバージョンのスイッチでは機能しません。
- リーフスイッチのポートで厳格モードが有効になっている場合、そのポートで特定の VLAN が有効になっていない場合でも、STP BPDU は受け入れられます。リモート側で設定不備があると、外部 L2 スイッチで意図しない STP 状態が発生する可能性があります。
- 厳格モードが有効になっているか、送信頻度が 2 秒未満の場合は、MCP CoPP バーストと CoPP レートを 5000 に設定します。
- 2 つの MCP 厳格対応ポートが同時に 起動 すると、どちらかの側でループが検出されたときに両方のポートがエラー無効になる可能性があります。

不正なエンドポイントの検出

不正なエンドポイントの制御ポリシーについて

不正なエンドポイントは、リーフ スイッチを頻繁に攻撃し、異なるリーフ スイッチ ポートにパケットを繰り返し挿入し、802.1Q タグを変更する（エンドポイントの移動をエミュレートする）ことで、学習されたクラスと EPG ポートを変更します。誤設定により頻繁に IP アドレスと MAC アドレスが変更 (移動する) されることになります。

ファブリックの急速な移動などで、大きなネットワークの不安定状態、高い CPU 使用率、まれなケースでは、大量かつ長期のメッセージおよびトランザクション サービス (MTS) バッファ消費のため、エンドポイント マッパー (EPM) および EPM クライアント (EPMC) がクラッシュすることになります。また、このような頻繁な移動により、EPM および EPMC ログが非常にすばやくロールオーバーされ、無関係なエンドポイントのデバッグを妨害する可能性があります。

不正なエンドポイントの制御機能は脆弱性にすばやく対処します。

- 急速に移動する MAC および IP エンドポイントの特定。

- エンドポイントを一時的に静的にして、エンドポイントを隔離することによって移動を停止します。
- 3.2(6) リリースより前：**不正 EP 検出間隔**のエンドポイントを静的に維持し、不正エンドポイントとの間のトラフィックをドロップします。この時間が経過すると、不正な MAC アドレスまたは IP アドレスが削除されます。
- 3.2(6) リリース以降：**不正な EP 検出間隔**のエンドポイントを静的に維持（この機能はトラフィックをドロップしなくなりました）。この時間が経過すると、不正な MAC アドレスまたは IP アドレスが削除されます。
- ホスト トラッキング パケットを生成して、影響を受ける MAC または IP アドレスをシステムが再学習できるようにします。
- 修正アクションを有効にするための障害の発生。

不正なエンドポイント制御ポリシーはグローバルに設定されており、他のループ防止方法とは異なり、個々のエンドポイント レベルの機能です (IP および MAC アドレス) 。ローカルまたはリモートの移動を区別していません。いかなる種類のインターフェイスの変更も、エンドポイントを隔離する必要があるかどうかを決定する際に移動と見なされます。

不正なエンドポイント制御機能は、デフォルトで無効になっています。

不正/ COOP 例外リストについて

不正/ COOP 例外リストを使用すると、エンドポイントが不正としてマークされる前に、不正エンドポイント制御によるエンドポイント移動の許容度を高くするエンドポイントの MAC アドレスを指定できます。不正/ COOP 例外リストのエンドポイントは、10 分以内に 3000 回以上移動した場合にのみ不正としてマークされます。エンドポイントが不正としてマークされた後、学習を防ぐためにエンドポイントは静的なままになります。不正エンドポイントは 30 秒後に削除されます。

Cisco Application Policy Infrastructure Controller（ APIC）6.0（3）リリース以降では、グローバルな不正/COOP 例外リストを作成できます。このリストは、MAC アドレスが見つかるブリッジ ドメイン上の全ての不正エンドポイント コントロールから MAC アドレスを除外します。そして、L3Outs の 不正 /COOP 例外リストを作成できます。ブリッジ ドメインまたは L3Out のすべての MAC アドレスを除外することもできます。これにより、すべての MAC アドレスに対して例外を作成する場合に例外リストを簡単に作成できます。各アドレスを個別に入力する必要はありません。

TCP MSS調整について

Cisco Application Policy Infrastructure Controller （APIC）6.0(3) リリース以降、伝送制御プロトコル（TCP）最大セグメントサイズ（MSS）調整機能を使用すると、リーフ スイッチによって転送される一時パケットの最大セグメント サイズを構成できます。ファブリック VXLAN トンネルを介して送受信される一時的なパケットのみが調整されます。2 つのデバイスが TCP セッションを確立すると、最初の SYN パケットで MSS をネゴシエートします。この MSS 値は、

パケットのフラグメンテーションやドロップを回避するために、基盤となるネットワークでサポートされている MTU よりも小さくする必要があります。Cisco ACI ファブリックは、9216 バイトのレイヤ 2 MTU サイズをサポートします。Cisco ACI ファブリックに接続されたデバイスは、最大 9104 バイトの MTU をネゴシエートできます。ただし、 Cisco ACI マルチポッド、Cisco ACI マルチサイト、および Cisco ACI ファブリックのリモート リーフ スイッチなどの機能には、サポートされる MTU が Cisco ACI ファブリックでサポートされるものよりも小さい外部ネットワークを介したトラフィック フローが含まれます。

TCP MSS 調整機能を使用すると、TCP SYN/SYN-ACK パケット内の TCP MSS 値を事前定義された値に調整できます。この調整では、TCP SYN/SYN-ACK パケットのみが CPU にパントされます。ユーザーは、IPv4 と IPv6 に個別の MSS 値を指定できます。MSS 調整は、リーフ スイッチごとに 1 秒あたり最大 2000 の TCP 接続に対して実行できます。

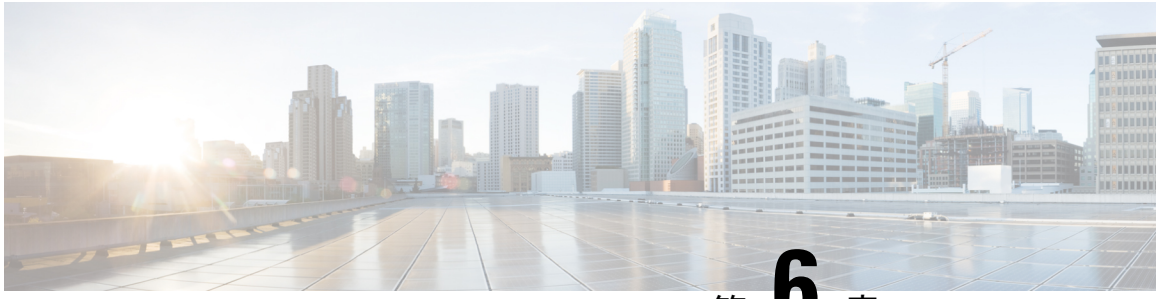
TCP MSS 調整には、さまざまなトポロジに対応するための 4 つのノブがあります。

1. **[無効（Disabled）]**：機能は無効です。
2. **[RL のみ（RL Only）]**：リモート リーフ スイッチとの間で送受信されるトラフィックが調整されます。バックツーバック リンクを使用する 2 つのリモート リーフ スイッチ間のトラフィックは調整されません。
3. **[RL およびマルチサイト（RL and Multi-Site）]**：Cisco ACI マルチサイト 内のサイト間で送信されるトラフィックが、リモート リーフ スイッチ トラフィックに加えて調整されます。
4. **[グローバル（Global）]**：異なる TEP プール内のリーフ スイッチとの間で送受信されるトラフィック。

   例：

   - 異なるリモート リーフ スイッチ TEP プール内のリモート リーフ スイッチとの間で送受信されるトラフィック
   - リモート リーフ スイッチとローカル リーフ スイッチとの間で送受信されるトラフィック
   - Cisco ACI マルチポッド の異なるポッドのリーフ スイッチとの間で送受信されるトラフィック
   - Cisco ACI マルチサイト の異なるサイトのスイッチとの間で送受信されるトラフィック

   同じリモート リーフ スイッチ TEP プール内のリモート リーフ スイッチとの間で送受信されるトラフィックは調整されません。



第 6 章

ネットワーキングと管理接続

この章は、次の内容で構成されています。

- DHCPリレー （163 ページ）
- DNS （166 ページ）
- インバンドおよびアウトオブバンド管理アクセス （166 ページ）
- IPv6 のサポート （170 ページ）
- テナント内のルーティング （175 ページ）
- WAN およびその他の外部ネットワーク （177 ページ）
- テナント ルーテッド マルチキャスト （195 ページ）
- Cisco ACI GOLF （202 ページ）
- マルチポッド （205 ページ）
- エニーキャストサービスについて （209 ページ）
- リモート リーフ スイッチ （210 ページ）
- QoS （222 ページ）
- HSRP （224 ページ）

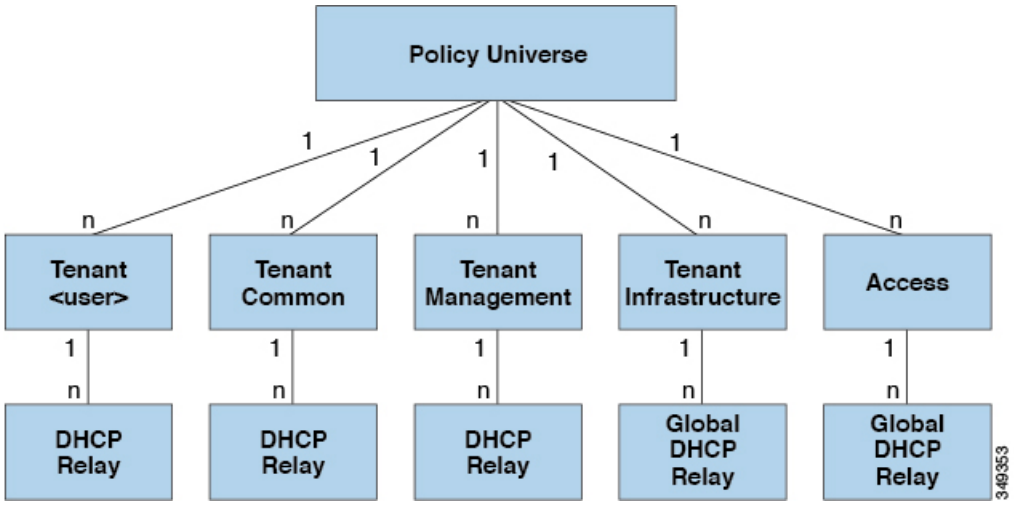
DHCPリレー

ACIのファブリック全体のフラッディングはデフォルトで無効になっている一方で、ブリッジドメイン内のフラッディングはデフォルトで有効になっています。ブリッジドメイン内のフラッディングがデフォルトで無効になっているため、クライアントは同じEPG内のDHCPサーバーに接続できます。ただし、DHCPサーバーがクライアントとは異なるEPGまたは仮想ルーティングおよび転送（VRF）インスタンスにある場合、DHCPリレーが必要です。また、レイヤ2フラッディングが無効の場合、DHCPリレーが必要です。

（注） ACI ファブリックは DHCP リレーとして動作するときに、DHCP オプション 82（DHCP リレーエージェント情報オプション）を、クライアントの代わりに中継する DHCP 要求に挿入します。応答（DHCP オファー）がオプション 82 なしで DHCP サーバから返された場合、その応答はファブリックによってサイレントにドロップされます。ACI が DHCP リレーとして動作するときは、ACI ファブリックに接続されたノードを計算するために IP アドレスを提供している DHCP サーバーはオプション 82 をサポートする必要があります。Windows 2003 および 2008 はオプション 82 をサポートしていませんが、Windows 2012 はサポートしています。

次の図は、DHCP リレー（ユーザ テナント、`common` テナント、`infra` テナント、`mgmt` テナントおよびファブリック アクセス）を含むことができる管理情報ツリー（MIT）内の管理対象オブジェクトを示します。

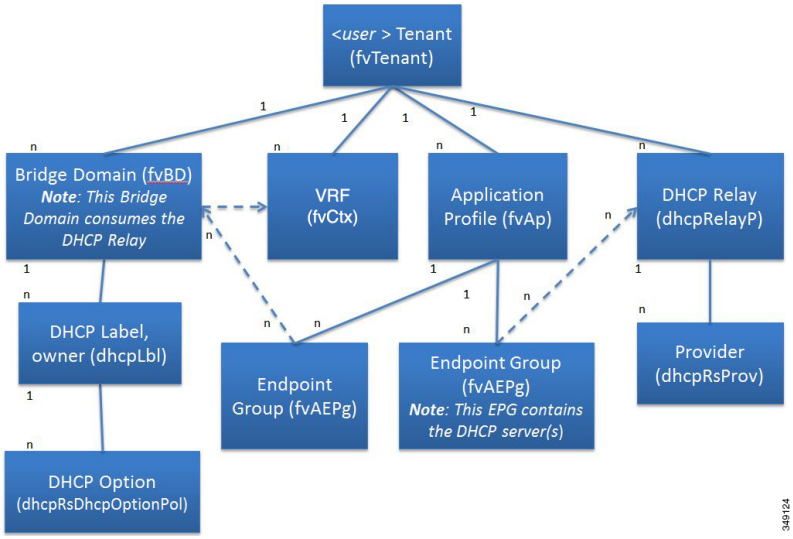
図 *57 : MIT* 内の *DHCP* リレーの場所



（注） DHCP リレーは、ブリッジドメインごとに 1 つのサブネットに制限されます。

次の図は、ユーザ テナント内の DHCP リレー オブジェクトの論理関係を示します。

図 *58* : テナント *DHCP* リレー



DHCP リレー プロファイルには 1 つまたは複数のプロバイダーが含まれます。EPG には 1 つ以上の DHCP サーバが含まれ、EPG と DHCP リレーの関係は DHCP サーバーの IP アドレスを指定します。コンシューマ ブリッジドメインには、プロバイダーの DHCP サーバーをブリッジドメインと関連付ける DHCP ラベルが含まれます。ラベルの一致により、ブリッジ ドメインは DHCP リレーを消費できます。

（注） ブリッジ ドメインの DHCP ラベルは、DHCP リレーの名前と一致する必要があります。

DHCP ラベル オブジェクトは、所有者も指定します。所有者には、テナントまたはアクセス インフラストラクチャを指定できます。所有者がテナントの場合、ACI ファブリックは最初にテナント内で一致する DHCP リレーを検索します。ユーザ テナント内で一致するものが見つからなかった場合、ACI ファブリックは次に共通テナント内を検索します。

DHCP リレーは、次のように Visable モードで動作します。`Visible` ：プロバイダーの IP とサブネットがコンシューマの VRF に漏洩します。DHCP リレーが表示されているときは、コンシューマの VRF に限定されます。

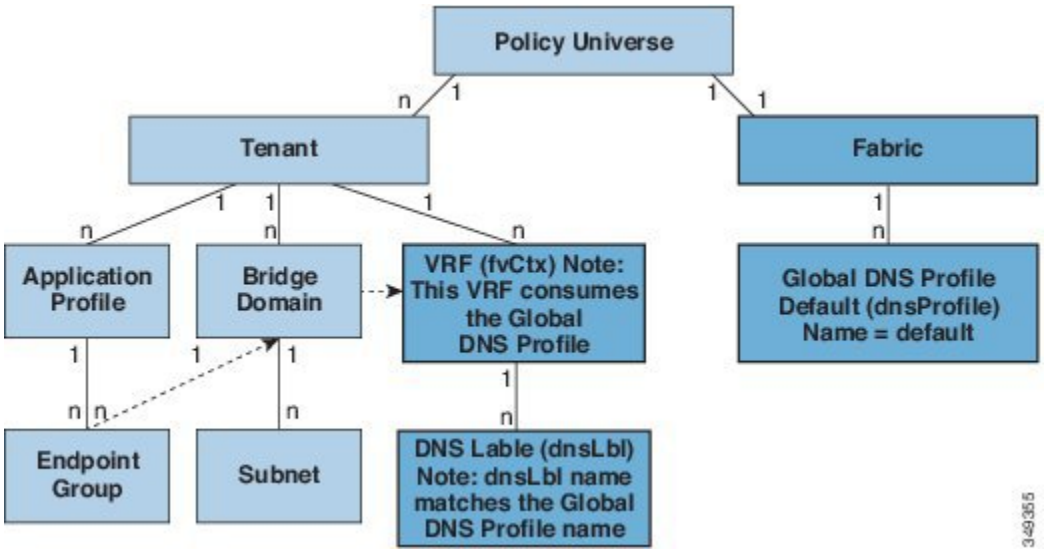
テナントおよびアクセスの DHCP リレーが同じ方法で構成されている一方で、以下の使用例はそれに応じて異なります。

- 共通テナントの DHCP リレーは、どのテナントでも使用できます。
- インフラ テナントの DHCP リレーは、ACI ファブリックのサービスプロバイダーによって他のテナントに選択的に公開されます。
- ファブリック アクセス（`infraInfra`）の DHCP リレーは、どのテナントでも使用でき、DHCP サーバーのより細かい構成が可能になります。この場合、同じブリッジドメイン内の別個の DHCP サーバーをノード プロファイルの各リーフスイッチ用にプロビジョニングすることができます。

DNS

ACI ファブリックの DNS サービスは、ファブリックの管理対象オブジェクトに含まれます。ファブリックのグローバル デフォルト DNS プロファイルには、ファブリック全体でアクセスできます。次の図は、ファブリック内の DNS 管理対象オブジェクトの論理関係を示します。

図 *59 : DNS*



VRF（コンテキスト）には、グローバル デフォルト DNS サービスを使用するために `dnsLBL` オブジェクトを含める必要があります。ラベルの一致により、テナント VRF はグローバル DNS プロバイダーを消費することができます。グローバル DNS プロファイルの名前が「default」なので、VRF ラベル名は「default」になります（`dnsLBL name = default`）。

インバンドおよびアウトオブバンド管理アクセス

管理テナントでは、ファブリック管理機能へのアクセスを構成するための便利な方法が提供されます。APIC を介してファブリック管理機能にアクセスできると同時に、インバンドおよびアウトオブバンドのネットワーク ポリシー経由で直接アクセスすることもできます。

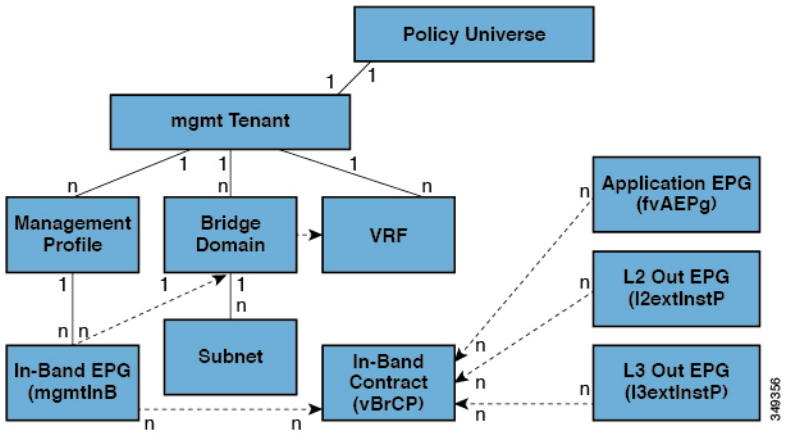
静的および動的管理アクセス

APICは、静的および動的管理アクセスの両方をサポートします。ユーザが少数のリーフスイッチとスパイン スイッチの IP アドレスを管理する単純な展開では、静的なインバンドおよびアウトオブバンド管理接続の構成がより簡単になります。多数の IP アドレスを管理する必要があるリーフスイッチとスパインスイッチが多数ある、より複雑な展開の場合、静的管理アクセスは推奨されません。静的管理アクセスの詳細については、「*Cisco APIC* および静的管理アクセス」を参照してください。

インバンド管理アクセス

次の図は、管理テナントのインバンドファブリック管理アクセスポリシーの概要を示します。

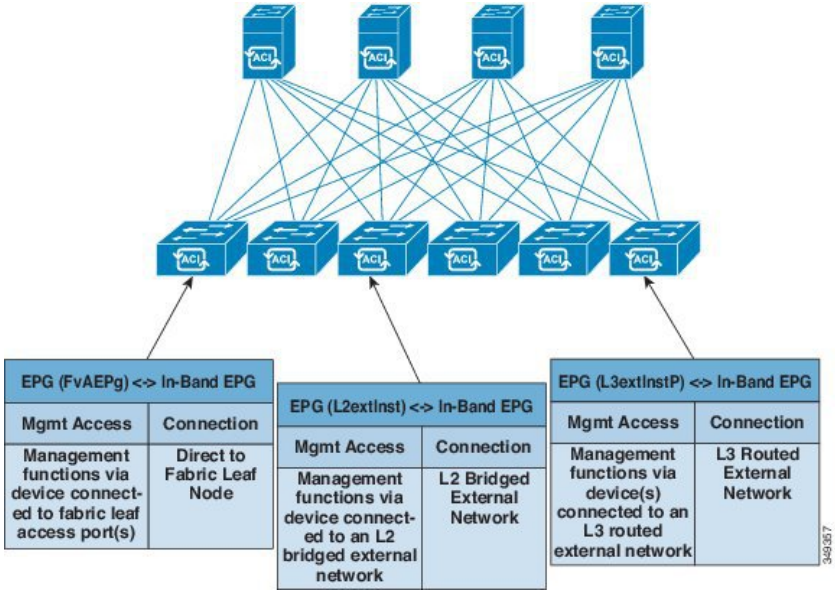
図 *60* : インバンド管理アクセスポリシー



管理プロファイルには、インバンドコントラクト（vzBrCP）を介した管理機能へのアクセスを提供するインバンドEPG MOが含まれます。vzBrCP は、fvAEPg、l2extInstP、および l3extInstP EPG がインバンド EPG を消費することを可能にします。これにより、ローカルで接続されたデバイスや、レイヤ2ブリッジ外部ネットワークおよびレイヤ3ルーテッド外部ネットワーク経由で接続されたデバイスにファブリック管理が提供されます。コンシューマおよびプロバイダー EPG が異なるテナントにある場合は、**common** テナントからブリッジドメインおよびコンテキストを使用できます。認証、アクセス、および監査のロギングはこれらの接続に適用され、インバンド EPG を通して管理機能にアクセスしようとするユーザには適切なアクセス権が必要です。

次の図は、インバンド管理のアクセス シナリオを示します。

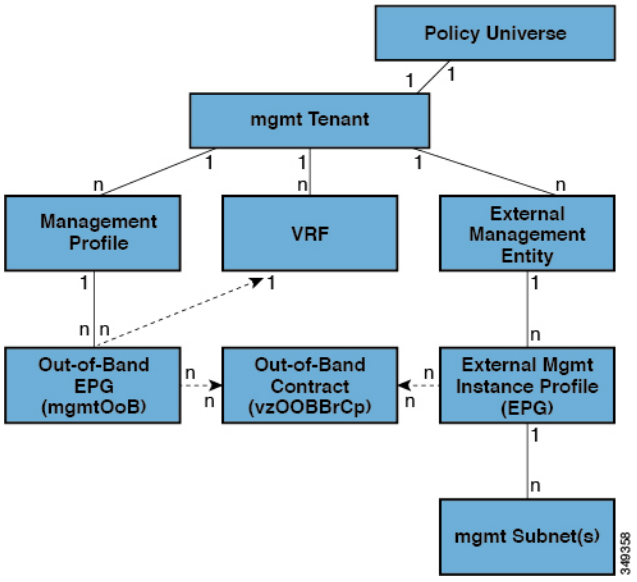
図 *61* : インバンド管理のアクセス シナリオ



アウトオブバンド管理アクセス

次の図は、管理テナントのアウトオブバンドファブリック管理アクセスポリシーの概要を示します。

図 *62* : アウトオブバンド管理アクセスポリシー

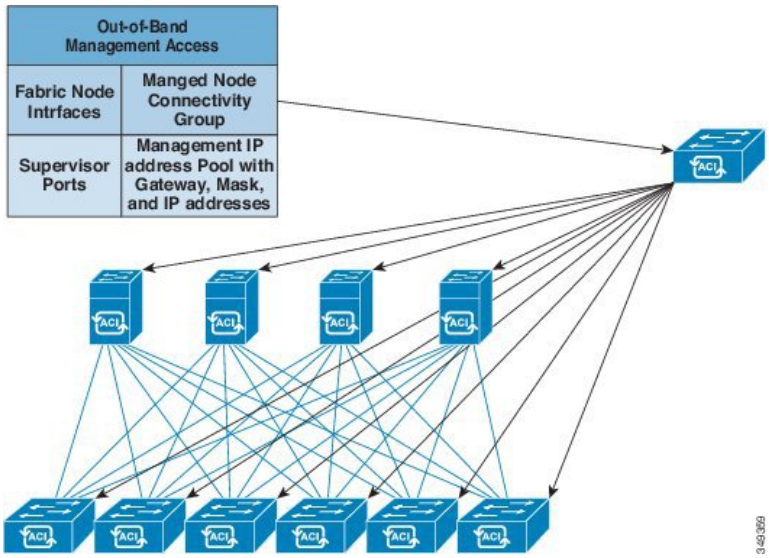


管理プロファイルには、アウトオブバンドコントラクト（`vzOOBBrCP`）を介した管理機能へのアクセスを提供するアウトオブバンド EPG MO が含まれます。`vzOOBBrCP` により、外部管理インスタンス プロファイル（`mgmtExtInstP`）EPG はアウトオブバンド EPG を消費できます。こ

れにより、サービスプロバイダーのプリファレンスに応じて、ローカルまたはリモートで接続されたデバイスにファブリック ノードのスーパーバイザ ポートが公開されます。スーパーバイザ ポートの帯域幅がインバンド ポート未満である間は、インバンド ポートを介したアクセスが利用できない場合、スーパーバイザ ポートが直通窓口を提供できます。認証、アクセス、および監査のロギングはこれらの接続に適用され、アウトオブバンド EPG を通して管理機能にアクセスしようとするユーザには適切なアクセス権が必要です。管理者が外部管理インスタンスプロファイルを構成する場合、アウトオブバンドアクセスを許可するデバイスのサブネット範囲を指定します。この範囲にないデバイスには、アウトオブバンド アクセスがありません。

次の図は、アウトオブバンド管理アクセスを専用スイッチを通じてどのように統合できるかについて示します。

図 *63* : アウトオブバンド アクセスのシナリオ



サービスプロバイダーによってはローカル接続へのアウトオブバンド接続を制限するように選択します。また、外部ネットワークからルーテッドまたはブリッジ接続を有効にすることを選択するサービス プロバイダーも存在します。また、サービス プロバイダーはローカル デバイスのみ、またはローカルおよびリモートデバイス両方に対するインバンドおよびアウトオブバンド管理アクセスの両方を含む一連のポリシーを構成することを選択することもできます。

（注） APIC リリース 1.2(2) 以降では、アウトオブバンド管理ノード EPG でコントラクトが提供されると、アウトオブバンド ノード管理アドレスで構成されるローカル サブネットが、デフォルトの APIC アウトオブバンド コントラクト送信元アドレスになります。以前は、任意のアドレスをデフォルトの APIC アウトオブバンド コントラクト送信元アドレスにすることが可能でした。

IPv6 のサポート

ACI ファブリックは、インバンドおよびアウトオブバンド インターフェイス、テナント アドレッシング、コントラクト、共有サービス、ルーティング、レイヤー 4 ～ レイヤー 7 サービス、およびトラブルシューティングのための次の IPv6 機能をサポートします。

- IPv6 アドレス管理、パーベイシブ ソフトウェア仮想インターフェイス（SVI）ブリッジドメイン サブネット、外部ネットワークの外部インターフェイス アドレス、およびロードバランサや侵入検出などの共有サービスのルート。
- ルータ通知（RA）およびルータ要請（RS）と呼ばれる ICMPv6 メッセージ、および重複アドレス検出（DAD）を使用したネイバー探索
- ステートレス アドレス自動設定（SLAAC）および DHCPv6
- ブリッジドメイン転送。
- トラブルシューティング（トラブルシューティングの章のアトミック カウンター、SPAN、ipping6、および traceroute のトピックを参照してください）。
- IPv4 のみ、IPv6 のみ、または帯域内および帯域外インターフェイスのデュアル スタック構成。

現在の ACI ファブリック IPv6 実装の制限には、次のものがあります。

- マルチキャストリスナー検出（MLD）スヌーピングはサポートされません。
- IPv6 管理の場合、静的アドレスのみが許可されます。動的 IPv6 プールは、IPv6 管理ではサポートされていません。
- IPv6 トンネル インターフェイス（サイト内自動トンネル アドレッシング プロトコル、6to4 など）は、ファブリック内でサポートされていません。ファブリック上で実行される IPv6 トンネル トラフィックは、ファブリックに対して透過的です。

ACI ファブリック インターフェイスは、リンク ローカル、グローバル ユニキャスト、およびマルチキャスト IPv6 アドレスで構成できます。

（注） このマニュアルで提供されている多くの例では 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。

グローバル ユニキャスト アドレスは、パブリック インターネットを介してルーティングできます。ルーティング ドメイン内でグローバルに一意です。リンク ローカル アドレス（LLA）はリンク ローカルの範囲を持ち、リンク（サブネット）上で一意です。LLA をサブネット間でルーティングすることはできません。これらは、ネイバー探索や OSPF などの制御プロトコルによって使用されます。マルチキャストアドレスは、複数のエンドポイントにパケットを配信するために、ネイバー探索などの IPv6 制御プロトコルによって使用されます。これらは構成できません。それらはプロトコル コンポーネントによって自動的に生成されます。

グローバル ユニキャスト アドレス

管理者は、1 つ以上の完全な 128 ビット IPv6 グローバル ユニキャスト アドレスを、圧縮または非圧縮形式でインターフェイスに手動で指定できます。たとえば、管理者は次のいずれかの形式でアドレスを指定できま
す。'2001:0000:0000:0001:0000:0000:0000:0003'、'2001:0:0:1:0:0:0:3'、'2001:0:0:1::3' ACI ファブリックの命名プロパティでは、IPv6アドレスは常に圧縮形式で表されます。上記の例では、相対名は 2001:0:0:1::3 です。管理者は、アドレスに応じて任意のマスク長を選択できます。

管理者は、ACI ファブリック IPv6 グローバル ユニキャスト アドレスを EUI-64 形式で指定することもできます。RFC2373 で指定されているように、拡張一意識別子（EUI）により、ホストは一意の 64 ビット IPv6 インターフェイス識別子（EUI-64）をホスト自体に割り当てることができます。IPv6 EUI-64 形式のアドレスは、128 ビットの IPv6 グローバル ユニキャスト アドレス内にスイッチのMACアドレスを組み込むことによって取得されます。IPv6 のこの機能により、手動構成またはDHCPの必要がなくなります。EUI-64 フォーマットで指定されたブリッジドメインまたはレイヤ 3 インターフェイスの IPv6 アドレスは、次のように形成されます。<IPv6 prefix>::/<mask>/eui64 where the mask is <=64 たとえば、2002::/64/eui64 は管理者が指定したもので、スイッチはアドレスを 2002::222:bdff:fef8:19ff/64 として割り当てます。スイッチは、スイッチの MAC アドレスを使用して EUI-64 アドレスを作成します。形成された IPv6 アドレスは、`ipv6If` オブジェクトの `operAddr` フィールドに含まれています。

（注） EUI-64 形式は、パーベイシブ ブリッジドメインとレイヤ 3 インターフェイス アドレスにのみ使用できます。外部サーバー アドレスや DHCP リレーなど、ファブリック内の他の IP フィールドには使用できません。

ブリッジドメイン サブネットとレイヤ 3 外部インターフェイスの IP アドレスは、/1 から /127 までのマスクを持つIPv6グローバルアドレスにすることができます。ブリッジドメインには、複数の IPv4 および IPv6 サブネットを含めることができます。同じ L3 外部インターフェースで IPv4 および IPv6 アドレスをサポートするには、管理者は複数のインターフェース プロファイルを作成します。EPG または外部 EpP がスイッチに展開されると、同等の bridge domain/L3 インターフェイスに手動で構成されたリンクローカル アドレス、または subnet/address フィールドに IPv6 アドレスが存在すると、スイッチに `ipv6If` インターフェイスが作成されます。

リンクローカル アドレス

1 つのインターフェイスに 1 つのリンクローカル アドレス（LLA）を割り当てることができます。LLA は、管理者が自動生成または構成できます。デフォルトでは、ACI LLA はスイッチによって EUI-64 形式で自動生成されます。管理者は、自動生成された LLA がスイッチで生成されるように、インターフェイスに少なくとも1つのグローバルアドレスを構成する必要があります。自動生成されたアドレスは、`ipv6If` MO の `operllAddr` フィールドに保存されます。パーベイシブSVIの場合、使用されるMACアドレスは、構成されたインターフェイスのMACアドレスと同じです。他の種類のインターフェイスには、スイッチの MAC アドレスが使用されます。管理者は、圧縮または非圧縮形式で、インターフェイス上に完全な 128 ビット IPv6 リンクローカル アドレスを手動で指定するオプションがあります。

（注） スイッチ ハードウェア テーブルは、仮想ルーティングおよび転送（VRF）インスタンスごとに 1 つの LLA に制限されています。

各パーベイシブ ブリッジドメインは、単一の IPv6 LLA を持つことができます。この LLA は、管理者が設定することも、提供されていない場合はスイッチによって自動的に構成することもできます。自動的に構成されると、スイッチは、MAC アドレスが IPv6 アドレスにエンコードされて一意のアドレスを形成する、変更された EUI-64 形式で LLA を形成します。パーベイシブ ブリッジドメインは、すべてのリーフ ノードで 1 つの LLA を使用します。

LLA を設定するには、次のガイドラインに従ってください。

- 外部 SVI および VPC メンバーの場合、LLA はすべてのリーフ ノードに固有です。
- LLA は、インターフェイスのライフサイクルの内いつでも、手動（手動で指定されたゼロ以外のリンクローカル アドレス）または自動（指定されたリンクローカル アドレスを手動でゼロに設定）に変更できます。
- 管理者が指定する LLA は、IPv6 リンクローカル形式（FE80:/10）に準拠する必要があります。
- IPv6 インターフェイス MO（`ipv6If`）は、インターフェイスで最初のグローバル アドレスが作成されたとき、または管理者が LLA を手動で構成したときのいずれか早い方で、スイッチに作成されます。
- 管理者が指定した LLA は、ブリッジドメインの `llAddr` プロパティおよび論理モデルのレイヤ 3 インターフェイス オブジェクトで表されます。
- スイッチによって使用される LLA（`llAddr` から、または `llAddr` がゼロの場合に自動生成されたもの）は、対応する ipv6If オブジェクトの `operLlAddr` プロパティで表されます。
- 重複 LLA などの運用 LLA 関連エラーは、重複アドレス検出プロセス中にスイッチによって検出され、`ipv6If` オブジェクトの `operStQual` フィールドに記録されるか、必要に応じて障害が発生します。
- `llAddr` フィールドとは別に、LLA（FE80:/10）は、APIC の他の IP アドレス フィールド（外部サーバー アドレスやブリッジドメイン サブネットなど）の有効なアドレスにすることはできません。これらのアドレスはルーティングできないためです。

スタティック ルート

ACI IPv6 静的ルートは、構成のアドレスとプレフィックス形式の違いを除いて、IPv4 でサポートされているものと似ています。次のタイプの静的ルートは、通常、IPv6 静的ルート モジュールによって処理されます。

- ローカル ルート：インターフェイスに構成された /128 アドレスは、CPU を指すローカル ルートにつながります。

- 直接ルート：パーベイシブ BD で構成されたアドレスの場合、ポリシー要素は、スパイン上の IPv4 プロキシ トンネルの接続先を指すサブネット ルートをプッシュします。非パーベイシブ レイヤ 3 外部インターフェイスに構成されたアドレスの場合、IPv6 マネージャ モジュールは、CPU を指すサブネット ルートを自動的にプッシュします。
- PE からプッシュされた静的ルート：外部接続に使用されます。このようなルートのネクスト ホップ IPv6 アドレスは、外部ルータの直接接続されたサブネット、または直接接続されたサブネット上の実際のネクスト ホップに解決できる再帰ネクスト ホップに置くことができます。インターフェイス モデルでは、インターフェイスをネクスト ホップとして使用できないことに注意してください（ただし、スイッチではサポートされています）。テナント間で共有サービスを有効にするために使用され、共有サービス静的ルートのネクスト ホップは、ルートが入力リーフスイッチにインストールされているテナント VRF とは異なる、共有サービスの仮想ルーティングおよび転送（VRF）インスタンスにあります。

ネイバー探索

IPv6 ネイバー探索（ND）は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレス プレフィックスの探索、および他のアクティブなネイバー ノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバー アドバタイズメント（NS/NA）およびルータ要求/ルータ アドバタイズメント（RS/RA）パケット タイプは、物理、層3 サブ インターフェイス、および SVI（外部およびパーベイシブ）を含むすべての ACI ファブリックのレイヤ 3 インターフェイスでサポートされます。APIC リリース 3.1(1x) まで、RS/RA パケットはすべてのレイヤ 3 インターフェイスの自動設定のために使用されますが、拡散型 SVI の設定のみ可能です。

APIC リリース 3.1(2x) より、RS/RA パケットは自動設定のため使用され、ルーテッド インターフェイス、レイヤ 3 サブ インターフェイス、SVI（外部および拡散）を含むレイヤ 3 インターフェイスで設定できます。

ACI のブリッジ ドメイン ND は常にフラッド モードで動作します。ユニキャスト モードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイス ポリシー（`nd:IfPol`）は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックス ポリシー（`nd:PfxPol`）コントロール RA メッセージ。
- ND の IPv6 サブネット（fv:Subnet）の設定。
- 外部ネットワークの ND インターフェイス ポリシー。
- 外部ネットワークの設定可能 ND サブネットおよびパーベイシブ ブリッジ ドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
  - 設定可能な静的 Adjacencies：（<vrf、L3Iface < ipv6 address> --> mac address）
  - 動的 Adjacencies：NS/NA パケットの交換経由で学習
- インターフェイス単位
  - ND パケットの制御（NS/NA）
    - ネイバー要求間隔
    - ネイバー要求再試行回数
  - RA パケットの制御
    - RA の抑制
    - RA MTU の抑制
    - RA 間隔、RA 最小間隔、再送信時間
- プレフィックス単位（RA でアドバタイズ）の制御
  - ライフタイム、優先ライフタイム
  - プレフィックス コントロール（自動設定、リンク上）
- ネイバー検索重複アドレスの検出（DAD）

重複アドレス検出

重複アドレス検出（DAD）は、構成中のアドレスを既に使用しているリンク上の他のノードを検出します。DAD は、リンクローカル アドレスとグローバル アドレスの両方に対して実行されます。構成された各アドレスは、次の DAD 状態を維持します。

- NONE：これは、DAD を試みる前にアドレスが最初に作成されたときの状態です。
- VALID：これは、アドレスが重複アドレスとして検出されることなく、アドレスがDADプロセスを正常に通過したことを示す状態です。
- DUP：これは、アドレスがリンク上で重複として見つかったことを表す状態です。

構成されたアドレスは、DAD 状態が VALID の場合にのみ、IPv6 トラフィックの送受信に使用できます。

ステートレス アドレス自動設定（SLAAC）および DHCPv6

次のホスト構成がサポートされています。

- SLAACのみ
- DHCPv6 のみ
- SLAAC と DHCPv6 ステートレスを一緒に使用すると、アドレス構成にのみ SLAAC を使用しますが、DNS 解決やその他の機能には DHCPv6 を使用します。

DHCP リレーでは IPv6 アドレスがサポートされています。DHCPv6 リレーは仮想ルーティングおよび転送（VRF）インスタンス全体に適用します。VLAN および VXLAN を介した DHCP リレーもサポートされています。DHCPv4 は DHCPv6 と連携して動作します。

テナント内のルーティング

アプリケーションセントリック インフラストラクチャ（ACI）のファブリックでは、テナントのデフォルト ゲートウェイ機能が提供され、ファブリックの Virtual Extensible Local Area（VXLAN）ネットワーク間のルーティングが行えます。各テナントについて、APIC でサブネットが作成されるたびに、ファブリックは仮想デフォルト ゲートウェイまたはスイッチ仮想インターフェイス（SVI）を提供します。これは、そのテナント サブネットの接続エンドポイントがあるすべてのスイッチにわたります。各入力インターフェイスはデフォルトのゲートウェイ インターフェイスをサポートし、ファブリック全体のすべての入力インターフェイスは任意のテナント サブネットに対する同一のルータの IP アドレスと MAC アドレスを共有します。

ルート リフレクタの設定

ACI ファブリックのルート リフレクタは、マルチプロトコル BGP（MP-BGP）を使用してファブリック内に外部ルートを配布します。ACI ファブリックでルート リフレクタをイネーブルにするには、ファブリックの管理者がルート リフレクタになるスパイン スイッチを選択して、自律システム（AS）番号を提供する必要があります。冗長性を確保するために、ポッドあたり少なくとも 2 つのスパイン ノードを MP-BGP ルート リフレクタとして設定することを推奨します。

ルート リフレクタが ACI ファブリックで有効になったら、管理者は、レイヤ 3 Out（L3Out）というコンポーネントを使用してリーフ ノードを介して外部ネットワークへの接続を設定できます。L3Out で設定されたリーフ ノードは、境界リーフと呼ばれます。境界リーフは、L3Out で指定されたルーティング プロトコルを介して、接続された外部デバイスとルートを交換します。L3Out 経由でスタティック ルートを設定することもできます。

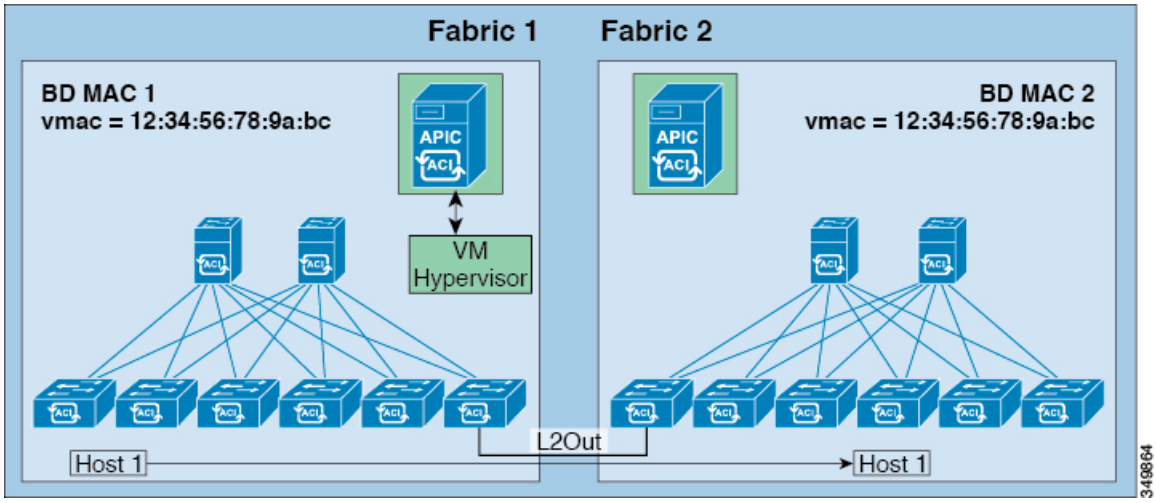
L3Out とスパイン ルート リフレクタの両方が展開されると、境界リーフ ノードは L3Out を介して外部ルートを学習し、それらの外部ルートはスパイン MP-BGP ルート リフレクタを介してファブリック内のすべてのリーフ ノードに配布されます。

リーフでサポートされるルートの最大数については、ご使用のリリースの『Cisco APICの検証済みスケーラビリティ ガイド』を参照してください。

共通パーベイシブ ゲートウェイ

ブリッジ ドメインごとに IPv4 共通ゲートウェイを使用して複数の ACI ファブリックを構成できます。これにより、1 つ以上の仮想マシン（VM）または従来型のホストを、ホストの IP アドレスを保持したまま、ファブリック間で移動できます。ファブリック間の VM ホストの移動は、VM ハイパーバイザによって自動的に行うことができます。ACI ファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACI ファブリック間のレイヤ 2 接続は、ローカル リンクか、ルーテッド WAN リンクにわたるものになります。次の図は、基本的な共通パーベイシブ ゲートウェイ トポロジを示しています。

図 *64 : ACI* マルチファブリック共通パーベイシブ ゲートウェイ



ブリッジドメインごとの一般的なパーベイシブ ゲートウェイの構成要件は次のとおりです。

- 各ファブリックのブリッジドメイン MAC（*mac*）値は一意である必要があります。

（注） デフォルトのブリッジドメイン MAC（*mac*）アドレス値は、すべての ACI ファブリックで同じです。共通のパーベイシブ ゲートウェイでは、管理者がブリッジドメインの MAC（*mac*） 値を各 ACI ファブリックに固有になるように構成する必要があります。

- ブリッジ ドメインの仮想 MAC（*vmac*）アドレスとサブネットの仮想 IP アドレスは、ブリッジドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。

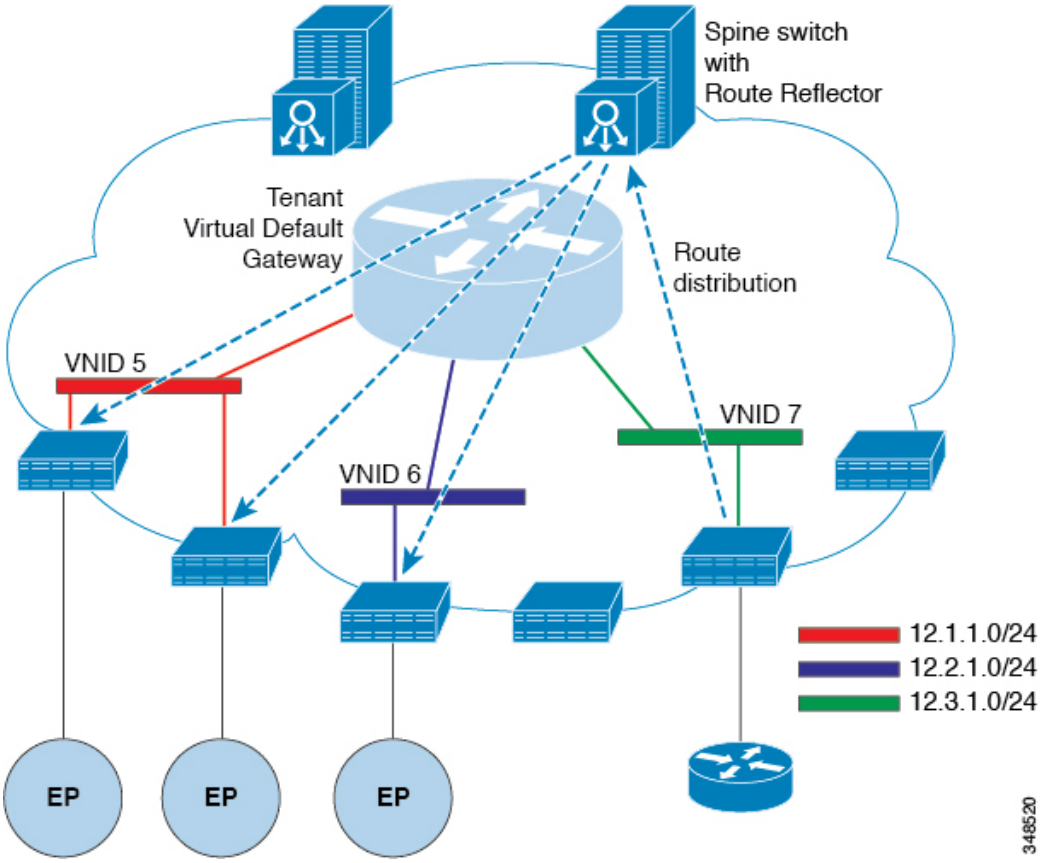
WAN およびその他の外部ネットワーク

WAN およびエンタープライズ コアに接続する外部ルータは、リーフスイッチの前面パネルのインターフェイスに接続します。外部ルータに接続するリーフスイッチインターフェイスは、ブリッジ インターフェイスまたはルーティング ピアとして構成できます。

ルータ ピアリングおよびルート配布

次の図に示すように、ルーティング ピア モデルを使用すると、リーフ スイッチ インターフェイスが外部ルータのルーティング プロトコルとピアリングするように静的に設定されます。

図 *65* : ルータのピアリング



ピアリングによって学習されるルートは、スパインスイッチに送信されます。スパインスイッチはルートリフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフスイッチに配布します。これらのルートは、最長プレフィクス照合(LPM)により集約されたアドレスで、外部ルータが接続されているリモートのリーフスイッチのVTEP IP アドレスが含まれるリーフ スイッチの転送テーブルに配置されます。WAN ルートには転送プロキシはありません。WAN ルートがリーフ スイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。外部ルータがデフォルト ゲートウェイではないため、テナン

トのエンドポイント (EP) からのパケットは ACI ファブリックのデフォルト ゲートウェイに送信されます。

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLANプール、およびカプセル化を設定するドメインポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者がACIファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル（`vmmDomP`）は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル（`physDomP`）は、ベア メタル サーバ接続と管理アクセスに使用します。
- ブリッジド外部ネットワーク ドメイン プロファイル（`l2extDomP`）は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメイン プロファイル（`l3extDomP`）は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。
- ファイバチャネル ドメインプロファイル(`fcDomP`)は、ファイバチャネルの VLAN と VSAN を接続するために使用されます。

ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

（注） EPG ポートと VLAN の設定は、EPG が関連付けられているドメイン インフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメインインフラストラクチャ設定がEPGポートと VLAN の設定に一致していることを確認してください。

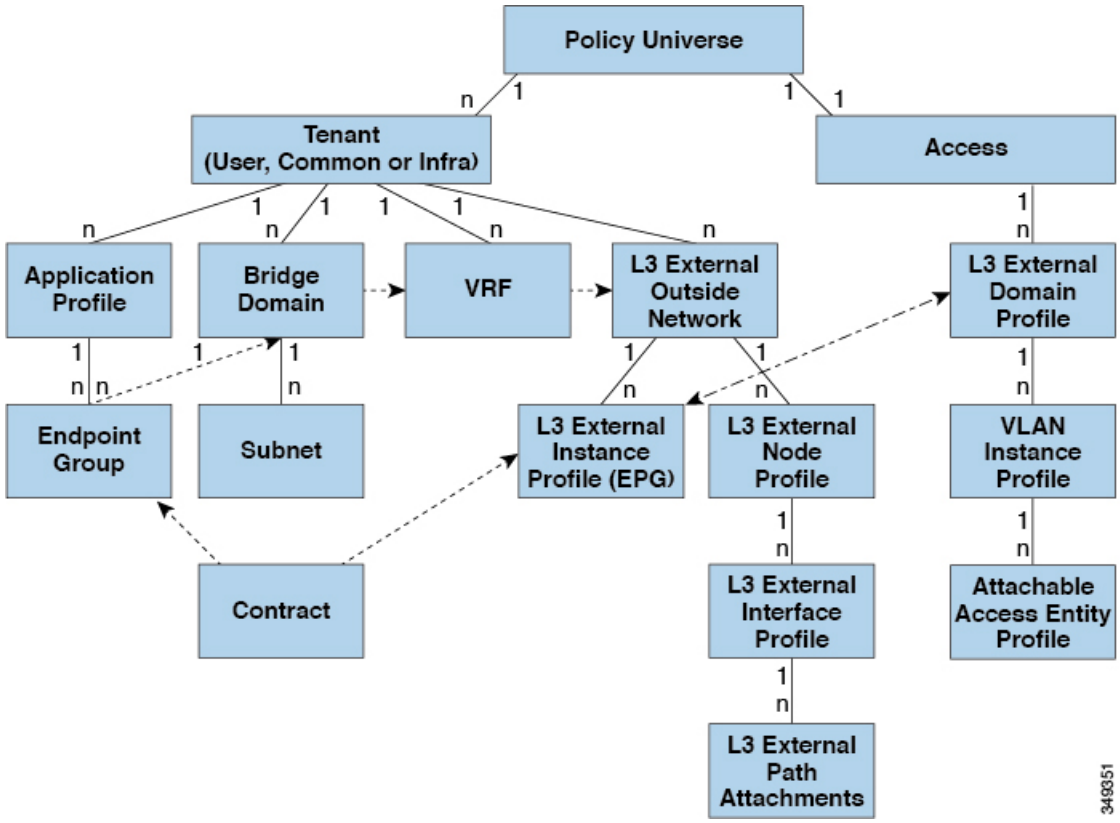
外部ネットワークへのブリッジおよびルーテッド接続

外部ネットワークの管理対象オブジェクトにより、外部ネットワークへのレイヤ2およびレイヤ3のテナント接続が可能になります。GUI、CLI、またはREST APIは、外部ネットワークへのテナント接続を構成するために使用できます。ファブリック内の外部ネットワーク アクセス ポイントを簡単に検索するために、レイヤ2およびレイヤ3の外部リーフ ノードを「ボーダー リーフ ノード」としてタグ付けできます。

外部ネットワークへのブリッジ接続用レイヤ 2 Out

テナント レイヤ2の外部ネットワークへのブリッジ接続は、次の図に示すようにファブリック アクセス（infraInfra）外部ブリッジドメイン（L2extDomP）をレイヤ2外部外側ネットワーク（l2extOut）のレイヤ 2 外部インスタンス プロファイル（l2extInstP）に関連付けることによって有効化されます。

図 *66 :*外部ネットワークへのテナント ブリッジ接続

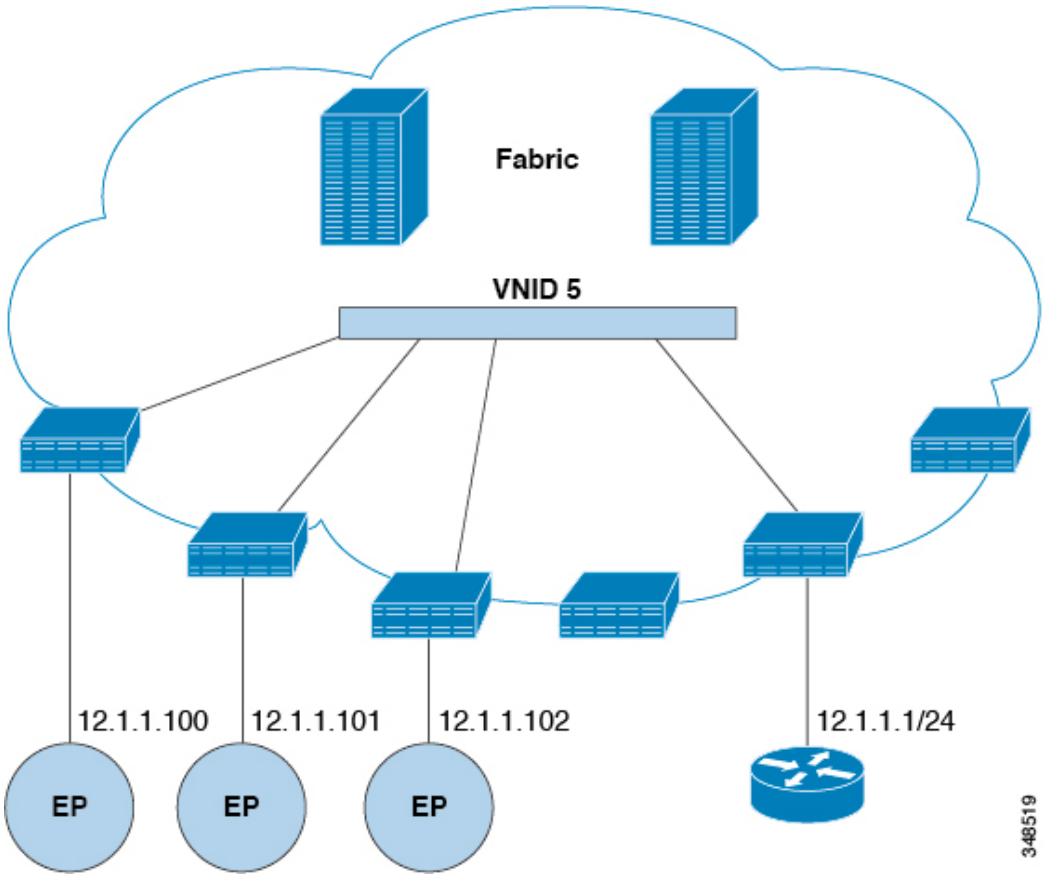


l2extOut には、スイッチ固有の構成およびインターフェイス固有の構成が含まれます。l2extInstP EPG は、コントラクトを通してテナント EPG に外部ネットワークを公開します。たとえば、ネットワーク接続ストレージ デバイスのグループを含むテナント EPG は、レイヤ2外部外側ネットワークに含まれるネットワーク構成に応じてコントラクトを介して l2extInstP EPG と通信できます。リーフスイッチ 1 つにつき構成できる外部ネットワークは 1 つのみです。ただし、外部ネットワーク構成は、ノードを L2 外部ノード プロファイルに関連付けることで複数のノードに容易に再利用できます。同じプロファイルを使用する複数のノードをフェールオーバーやロード バランシングのために設定できます。

外部ルータへのブリッジド インターフェイス

次の図に示すように、リーフ スイッチのインターフェイスがブリッジド インターフェイスとして設定されている場合、テナント VNID のデフォルト ゲートウェイが外部ルータとなります。

図 *67:* ブリッジド外部ルータ

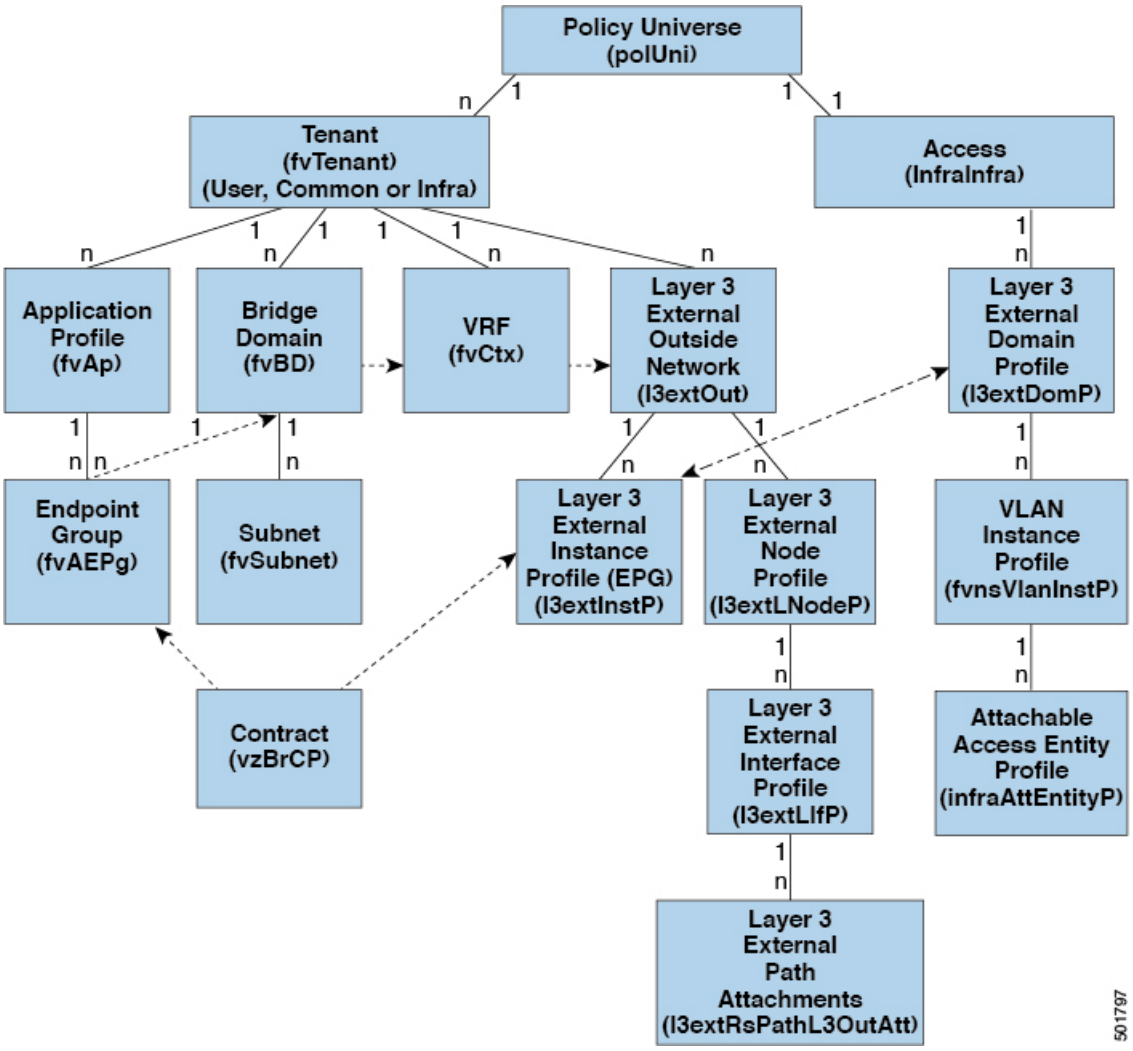


ACI ファブリックは、外部ルータの存在を認識せず、APIC はリーフ スイッチのインターフェイスを EPG に静的に割り当てます。

外部ネットワークへのルーテッド接続のためのレイヤ 3 Out

外部ネットワークへのルーテッド接続は、次の図の階層で示すようにファブリック アクセス（`infraInfra`）外部ルーテッド ドメイン（`l3extDomP`）をレイヤ 3 外部外側ネットワーク（`l3extOut`）のテナント レイヤ 3 外部インスタンス プロファイル（`l3extInstP` または外部 EPG）に関連付けることによって有効になります。

図 *68 :* レイヤ *3* 外部接続のポリシー モデル



レイヤ 3 外部アウトサイドネットワーク（`l3extOut` オブジェクト）には、ルーティング プロトコルのオプション（BGP、OSPF、または EIGRP またはサポートされている組み合わせ）およびスイッチとインターフェイス固有の設定が含まれています。`l3extOut` にルーティング プロトコル（たとえば、関連する仮想ルーティングおよび転送（VRF）およびエリア ID を含む OSPF）が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

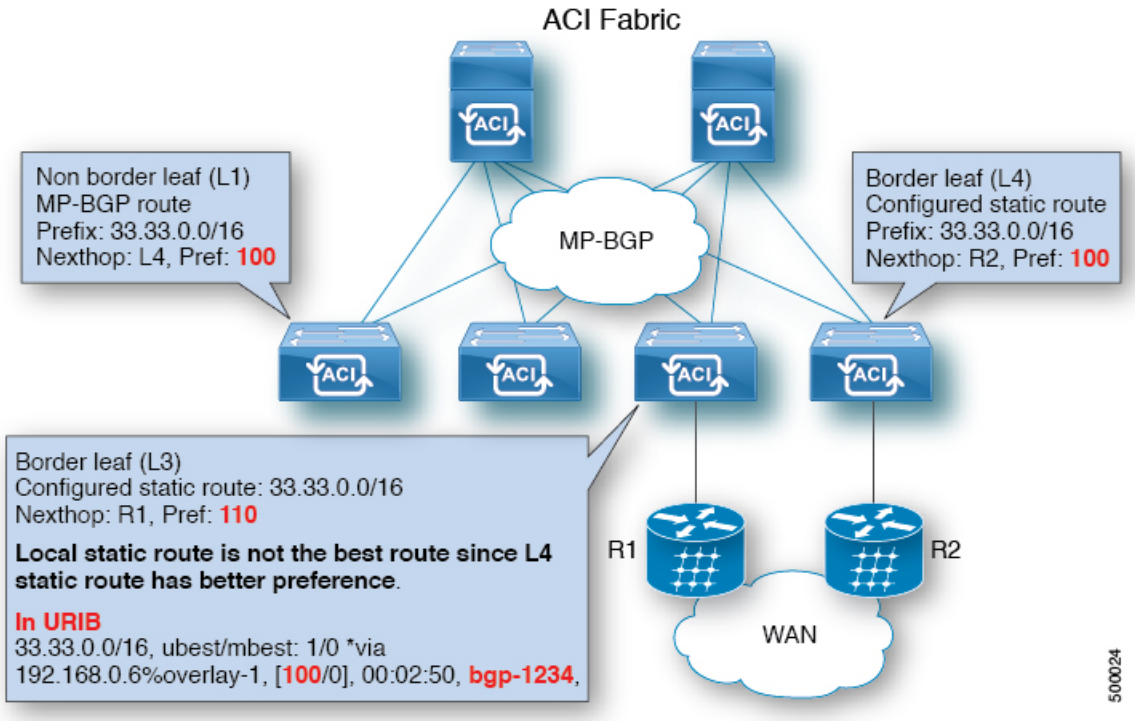
`l3extInstP` EPG は、コントラクトを通してテナント EPG に外部ネットワークを公開します。たとえば、Web サーバのグループを含むテナント EPG は、`l3extOut` に含まれるネットワーク設定に応じてコントラクトを介して `l3extInstP` EPG と通信できます。外部ネットワーク設定は、ノードを L3 外部ノード プロファイルに関連付けることで複数のノードに容易に再利用できます。同じプロファイルを使用する複数のノードをフェールオーバーやロードバランシングのために設定できます。ノードを複数の l3extOuts に追加することで、l3extOuts に関連付けられている VRF がノードでも展開されます。拡張性に関する情報については、現行の「*Verified Scalability Guide for Cisco ACI*」を参照してください。

静的ルート プリファレンス

ACI ファブリック内の静的ルート プリファレンスは、コスト拡張コミュニティを使用して MP-BGP で伝送されます。

次の図は、ACI ファブリックがリーフスイッチ全体で静的ルート プリファレンスを維持し、ルート選択がこのプリファレンスに基づいて行われるようにする方法を示しています。

図 *69 :* 静的ルート プリファレンス



この図は、ローカル静的ルートよりも優先されるリーフスイッチ 4（L4）からリーフスイッチ 3（L3）に到達する MP-BGP ルートを示しています。静的ルートは、管理者によって構成された優先順位でユニキャスト ルーティング情報ベース（URIB）にインストールされます。ACI 非境界リーフスイッチでは、ネクストホップとしてリーフスイッチ 4（L4）を使用して静的ルートがインストールされます。L4 のネクストホップが使用できない場合、L3 スタティック ルートがファブリック内の最適なルートになります。

（注） リーフスイッチの静的ルートが `next hop Null 0` で定義されている場合、MP-BGP はそのルートをファブリック内の他のリーフスイッチにアドバタイズしません。

ルートのインポートとエクスポート、ルート集約、ルート コミュニティの一致

サブネット ルートのエクスポートまたはインポート設定オプションは、次に説明するスコープおよび集約オプションに従って指定できます。

ルーティング対象サブネットについては、以下のスコープ オプションが使用可能です。

- エクスポート ルート制御サブネット：エクスポート ルート方向を制御します。
- インポート ルート制御サブネット：インポート ルート方向を制御します。

（注） インポート ルート コントロールは、BGP と、OSPF が EIGRP ではなく、サポートされています。

- 外部 EPG (セキュリティ インポート サブネット) の外部サブネット: どの外部サブネットが、特定の外部 L3Out EPG（ `l3extInstP` ）の一部として適用されるコントラクトを保持するか指定します。サブネットの `l3extInstP` 外部 EPG として分類、サブネット上の範囲を「インポートセキュリティ」に設定する必要があります。この範囲のサブネットを決定する IP アドレスが関連付けられています、 `l3extInstP` 。これが決定されると、契約は、他のどの Epg でその外部のサブネットが通信を許可を決定します。たとえば、レイヤ 3 外部の外部ネットワーク (`L3extOut`) の ACI スイッチでトラフィックが開始する場合、`l3extInstP` に関連付けられている送信元 IP アドレスを判断するための検索が行われます。このアクションより一般的なサブネット上で複数の特定のサブネットが優先されるようにで最長プレフィックス一致 (ほか) に基づいて行われます。
- 共有ルート制御サブネット — 共有サービス設定においては、この特性が有効になっているサブネットだけが、コンシューマ EPG の Virtual Routing and Forwarding （VRF）にインポートされます。これは VRF 間の共有サービスのルート方向を制御します。
- 共有セキュリティ インポート サブネット：インポート対象サブネットに共有コントラクトを適用します。デフォルトの仕様では、外部 EPG 用外部サブネットが設定されています。

ルート対象サブネットを集約することができます。集約が設定されていない場合は、サブネットが正確に照合されます。たとえば、サブネットが 11.1.0.0/16 の場合、11.1.1.0/24 ルートにはポリシーが適用されず、ルートが 11.1.0.0/16 である場合のみ適用されます。すべてのサブネットを 1 つずつ定義する作業は面倒でエラーが発生しやすいので、それを回避するために、サブネットのセットを 1 つのエクスポート、インポートまたは共有ルート ポリシーに集約することができます。現時点では、0/0 サブネットのみ集約可能です。0/0 に集約を指定すると、次の選択オプションに基づき、すべてのルートがインポート、エクスポートされ、異なる VRF と共有されます:

- 集約エクスポート — VRF (サブネット 0/0) のすべての中継ルートをエクスポートします。
- 集約インポート — 所定の L3 ピア (サブネット 0/0) のすべて着信ルートをインポートします。

（注） BGP、OSPF が EIGRP の集約インポート ルート制御はサポートされます。

- 集約共有ルート — 1 つの VRF で学習されているルートを別の VRF にアドバタイズする必要がある場合、サブネットとの正確な一致、またはサブネットマスクに従った方法で共有できます。集約共有ルートでは、複数のサブネットマスクを使用して、どの特定のルートグループを VRF 間で共有するかを決定できます。たとえば、10.1.0.0/16 と 12.1.0.0/16 を指定してこれらのサブネットを集約することができます。あるいは、0/0 を使用すると、複数の VRF のすべてのサブネット ルートを共有できます。

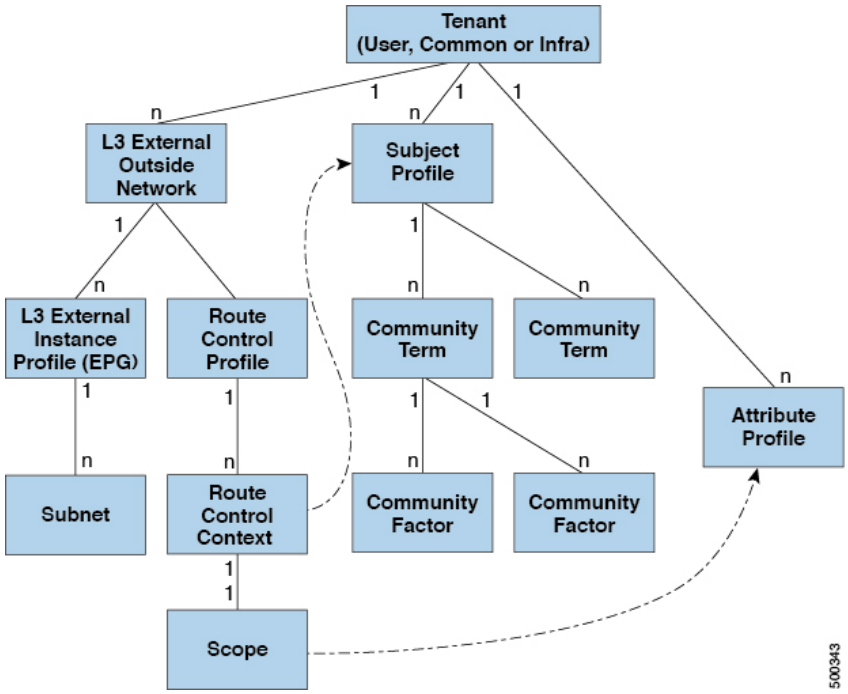
（注） 第 2 世代のスイッチの VRF 機能間で正常にルートが共有されます（N9K-93108TC-EX など、スイッチ モデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K）。第 1 世代のスイッチですが、ルートを保存する物理的な 3 進コンテンツ対応メモリ（TCAM）にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

ルート集約では、多数の具体的なアドレスを 1 つのアドレスに置き換えることで、ルート テーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 は 10.1.0.0/16 に置き換えられます。ルート集約ポリシーにより、ボーダー リーフ スイッチとそのネイバー リーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいは EIGRP のルート集約ポリシーは、ブリッジ ドメインまたは中継サブネットに適用されます。OSPF では、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされます。ファブリック内でのアドバタイズは行われません。上記の例では、ルート集約ポリシーが適用され、EPG が 10.1.0.0/16 サブネットを使用している場合、10.1.0.0/16 の範囲全体がすべての隣接リーフ スイッチと共有されます。

（注） 同じリーフ スイッチで 2 つの `L3extOut` ポリシーに OSPF を設定している場合（1 つはレギュラーで、もう 1 つはバックボーン）には、VRF内の全エリアに集約が適用されるため、一方の `L3extOut` で設定されているルート集約ポリシーが両方の L3extOut ポリシーに適用されます。

次の図に示すように、ルート制御プロファイルは、プレフィックス ベースおよびコミュニティ ベースの一致に基づいて、ルート マップを取得します。

図 *70* : ルート コミュニティ マッチング



ルート制御プロファイル（rtctrtlProfile）は、許可される対象を指定します。ルート制御コンテキストは一致対象を指定し、スコープは設定すべき対象を指定します。サブジェクト プロファイルには、コミュニティ マッチの仕様が含まれます。これは複数の l3extOut で使用できます。サブジェクト プロファイル（SubjP）には、それぞれ 1 つまたは複数のコミュニティ ファクタ（コミュニティ）を含む複数のコミュニティ タームを含めることができます。これにより、次のブール演算を指定することができます。

- 複数コミュニティ ターム間の論理的 OR
- 複数コミュニティ ターム間の論理的 AND

たとえば、北東と呼ばれるコミュニティ タームに、それぞれ多くのルートを含む複数のコミュニティが含まれているとします。また、南東という別のコミュニティ タームにも、さまざまなルートが多数含まれているとします。管理者は、そのどちらかあるいは両方を一致させることを選択できます。コミュニティ ファクタ タイプには、レギュラーまたは拡張を使用できます。拡張タイプのコミュニティ ファクタを使用する際には、仕様間の重複がないよう注意することが必要です。

ルート制御プロファイルのスコープ部分は、属性プロファイル（rtctrlAttrP）を参照して、適用すべき設定-アクション（プリファレンス、ネクスト ホップ、コミュニティなど）を指定します。ルートを l3extOut から学習した場合は、ルートの属性を変更できます。

上の図は、l3extOut に rtctrtlProfile が含まれているケースを示しています。rtctrtlProfile はテナントの下にも配置できます。この例では、l3extOut に、自身をテナント下の rtctrtlProfile と関連付ける相互リーク関係ポリシー（L3extRsInterleakPol）が設定されています。この設定により、再利用、 rtctrtlProfile 複数の l3extOut 接続します。BGP 属性

(BGP は、ファブリック内で使用される) は、それを OSPF からは、ファブリックを学習ルートの追跡することもできます。L3extOut 下で定義された rtctrtlProfile の優先順位は、テナント下で定義されたものよりも高くなります。

rtctrtlProfile には、組み合わせ可能およびグローバルという 2 つのモードがあります。デフォルトの組み合わせ可能モードでは、パーベイシブ サブネット（fvSubnet）および外部サブネット（l3extSubnet）に一致/設定メカニズムを組み合わせてルート マップをレンダリングします。グローバル モードはテナント内のすべてのサブネットに適用され、そのほかのポリシー属性の設定が無効になります。グローバル rtctrtlProfile では、明示的な（0/0）サブネットを定義しなくても、すべての動作が許可されます。グローバル rtctrtlProfile は、コミュニティやネクストホップといった異なるサブネット属性を使用してマッチングが行われる非プレフィックス ベースの一致ルールと一緒に使用されます。1 つのテナント下で複数の rtctrtlProfile ポリシーを設定できます。

rtctrtlProfile ポリシーによって、デフォルト インポートおよびデフォルト エクスポートのルート制御の拡張が可能になります。集約インポートあるいはエクスポートルートを伴う Layer 3 Outside ネットワークには、サポート対象デフォルト エクスポート/デフォルト インポートおよびサポート対象 0/0 集約ポリシーを指定するインポート/エクスポート ポリシーを設定できます。すべてのルート（着信または発信）に rtctrtlProfile ポリシーを適用するには、一致ルールのないグローバル デフォルト rtctrtlProfile を定義します。

（注） 1 つのスイッチ上で複数の l3extOut 接続を設定することは可能ですが、スイッチは 1 つのルートマップしか持つことができないため、スイッチで設定されているすべてのレイヤ 3 外側ネットワークが同じ rtctrtlProfile を使用する必要があります。

プロトコル相互リークと再配布ポリシーは、ACI ファブリック BGP ルートで共有される外部学習ルートを制御します。設定属性はサポートされています。これらのポリシーは L3extOut 単位、ノード単位、VRF 単位でサポートされます。相互リークポリシーは、L3extOut 内のルーティング プロトコルによって学習されたルートに適用されます。現在のところ、相互リークと再配布ポリシーは、OSPF v2 および v3 でサポートされています。ルート制御ポリシー rtctrtlProfile は、相互リーク ポリシーによって消費される場合、グローバルとして定義する必要があります。

共有サービス契約の使用

共有サービスにより、テナントの分離ポリシーとセキュリティポリシーを維持しながら、テナント間の通信が可能になります。外部ネットワークへのルーティング接続は、複数のテナントが使用する共有サービスの例です。

共有サービス契約の構成時は、次のガイドラインに従ってください。

- サブネットをさまざまな Virtual Routing and Forwarding（VRF）インスタンス（コンテキストまたはプライベートネットワークとも呼ばれる）にエクスポートする共有サービスの場合、サブネットはEPGの下で構成する必要があり、範囲は**[外部でアドバタイズ（Advertised Externally）]** および **[VRF 間で共有（Shared Between VRFs）]** に設定する必要があります。

- VRF が適用されていない場合、ブリッジ間ドメイン トラフィックにコントラクトは必要ありません。
- VRF が適用されていない場合でも、共有サービスの VRF 間トラフィックにはコントラクトが必要です。
- プロバイダー EPG の VRF は、共有サービスの提供中に非強制モードにすることはできません。
- 共有サービスは、重複しないサブネットのみでサポートされます。共有サービスのサブネットを構成するときは、次のガイドラインに従ってください。
  - 共有サービスプロバイダーのサブネットは、ブリッジドメイン下ではなく EPG 下で構成します。
  - 同じ VRF を共有する EPG で構成されたサブネットは、統合および重複してはなりません。
  - ある VRF からリークされたサブネットは、切り離されている必要があり、重複してはなりません。
  - 複数のコンシューマー ネットワークから VRF に、またはその逆にリークされたサブネットは、切り離されている必要があり、重複してはなりません。



（注） 2 人のコンシューマーが誤って同じサブネットに構成されている場合は、両方のサブネットの構成を削除してこの状態からリカバリし、その後サブネットを正しく再構成します。

- プロバイダー VRF で共有サービスを `AnyToProv` で構成しないでください。APIC はこの構成を拒否し、障害が発生します。
- インバンド EPG とアウトオブバンド EPG の間でコントラクトが構成されている場合、次の制限が適用されます。
  - 両方の EPG が同じ VRF にある必要があります。
  - Ffilter は、着信方向にのみ適用されます。
  - レイヤ 2 フィルタはサポートされません。
  - QoS は、インバンド レイヤ 4 ～ レイヤ 7 のサービスには適用されません。
  - 管理統計は利用できません。
  - CPU 宛てトラフィックの共有サービスはサポートされません。

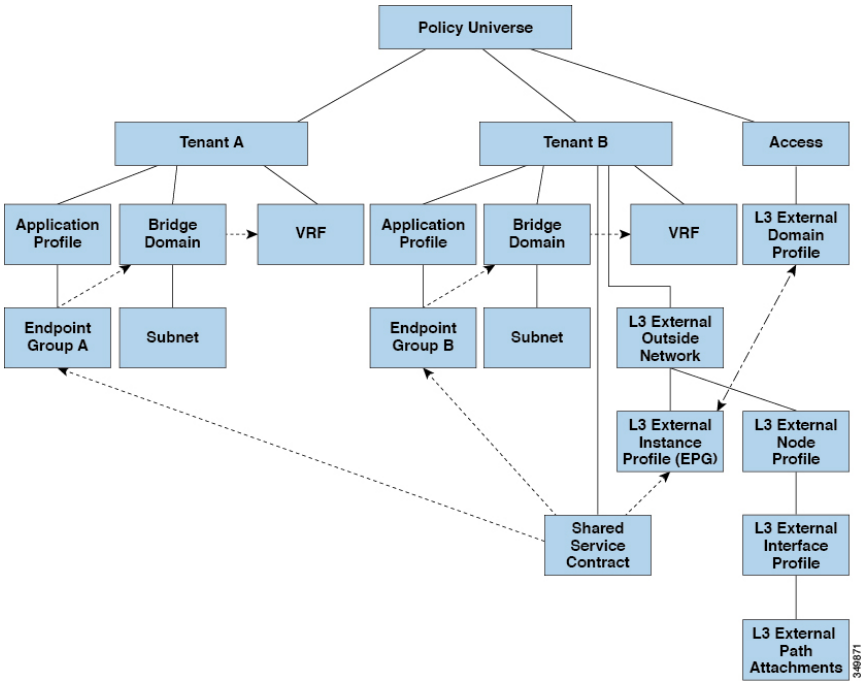
共有レイヤ 3 Out

共有レイヤ 3 アウトサイド（L3Out または `l3extOut`）構成は、外部ネットワークへのルーテッド接続を、VRF インスタンス間またはテナント間の共有サービスとして提供します。L3Out の外部 EPG インスタンス プロファイル（外部 EPG または `l3extInstP`）は、ルーティングの観点とコントラクトの観点の両方から共有できるルートを制御するための構成を提供します。外部 EPG 下のコントラクトは、これらのルートをリークする必要がある VRF インスタンスまたはテナントを決定します。

L3Out は、任意のテナント（*user*、`common`、`infra`、`mgmt`.）の共有サービスとしてプロビジョニングできます。任意のテナントの EPG は、外部 EPG がファブリック内のどこにプロビジョニングされているかには関係なく、共有サービス コントラクトを使用して、外部 EPG に接続できます。これにより、外部ネットワークへのルーテッド接続のプロビジョニングが簡単になります。複数のテナントが、外部ネットワークへのルーテッド接続用に単一の外部 EPG を共有できます。外部 EPG を共有すると、単一の共有外部 EPG を使用する EPG の数には関係なくスイッチ上で使用されるセッションは 1 つのみであるため、より効率的になります。

次の図は、共有外部 EPG 用に構成された主なポリシー モデル オブジェクトを示しています。

図 *71* : 共有 *L3Out* ポリシー モデル



共有 L3Out ネットワーク設定については、以下の注意事項と制限事項に注意してください。

- テナント制限なし：テナント A と B は、任意の種類のテナント（*user*、`common`、`infra`、`mgmt`）です。共有外部 EPG が `common` テナントにある必要はありません。
- EPG の柔軟な配置：上の図の EPG A と EPG B は異なるテナントにあります。EPG A と EPG B で同じブリッジ ドメインと VRF インスタンスを使用することはできますが、それ

は必須ではありません。EPG A と EPG B は異なるブリッジ ドメインおよび異なる VRF インスタンスにありますが、同じ外部 EPG を共有しています。

- サブネットは、*private*、*public*、または *shared* です。L3Out のコンシューマまたはプロバイダ EPG にアドバタイズされるサブネットは、*shared* に設定されている必要があります。L3Out にエクスポートされるサブネットは *public* に設定される必要があります。
- 共有サービス コントラクトは、共有 L3Out ネットワーク サービスを提供する外部 EPG が含まれているテナントからエクスポートされます。共有サービス コントラクトは、共有サービスを使用する EPG が含まれているテナントにインポートされます。
- 共有 L3Out では禁止コントラクトを使用しないでください。この構成はサポートされません。
- 外部 EPG は、共有サービス プロバイダーとしてサポートされますが、非外部 EPG コンシューマと組み合わせる場合に限られます（L3Out EPG が外部 EPG と同じ）。
- トラフィック中断（フラップ）：外部 EPG を、外部サブネット 0.0.0.0/0 を使用して構成し、外部 EPG サブセットのスコープ プロパティを共有ルート制御（*shared-rctrl*）または共有セキュリティ（*shared-security*）に設定すると、VRF インスタンスはグローバル `pcTag` を使用して再配置されます。これにより、その VRF インスタンス内のすべての外部トラフィックが中断されます（VRF インスタンスがグローバル `pcTag` を使用して再配置されるため）。
- 共有レイヤ L3Out のプレフィックスは一意である必要があります。同じ VRF インスタンスの同じプレフィックスを使用した、複数の共有 L3Out 構成は動作しません。VRF インスタンスにアドバタイズする外部サブネット（外部プレフィックス）が一意であることを確認してください（同じ外部サブネットが複数の外部 EPG に属することはできません）。プレフィックス prefix1 を使用した L3Out 構成（たとえば、`L3Out1`）と、同じくプレフィックス prefix1 を使用した 2 番目のレイヤ 3 アウトサイド構成（たとえば、`L3Out2`）を同じ VRF に所属させると、動作しません（導入される pcTag は 1 つのみであるため）。
- L3Out の異なる動作が、同じ VRF インスタンスの同じリーフ スイッチ上に構成される場合があります。考えられるシナリオは次の 2 つです。
  - シナリオ 1 は、SVI インターフェイスおよび 2 つのサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義された L3Out がある場合です。L3Out ネットワーク上の入力トラフィックが、マッチング プレフィックス 10.10.10.0/24 を持っていると、入力トラフィックは外部 EPG pcTag を使用します。L3Out ネットワーク上の入力トラフィックが、マッチング デフォルト プレフィックス 0.0.0.0/0 を持っていると、入力トラフィックは外部ブリッジ pcTag を使用します。
  - シナリオ 2 は、2 つのサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義されたルーテッドまたはルーテッドサブインターフェイスを使用する L3Out がある場合です。L3Out ネットワーク上の入力トラフィックが、マッチング プレフィックス 10.10.10.0/24 を持っていると、入力トラフィックは外部 EPG pcTag を使用します。L3Out ネットワーク上の入力トラフィックが、マッチング デフォルト プレフィックス 0.0.0.0/0 を持っていると、入力トラフィックは VRF インスタンス pcTag を使用します。

- ここまでで説明した動作の結果として、同じ VRF インスタンスおよび同じリーフ スイッチに、SVI インターフェイスを使用する L3Out-A および L3Out-B が構成されている場合、次のユース ケースが考えられます。

  ケース 1 は L3Out-A 用です。この外部ネットワーク EPG には、10.10.10.0/24 および 0.0.0.0/1 という 2 つのサブネットが定義されています。L3Out-A 上の入力トラフィックがマッチング プレフィックス 10.10.10.0/24 を持っている場合、外部 EPG pcTag と contract-A を使用します。このコントラクトは L3Out-Aに関連付けられるものです。L3Out-A の出力トラフィックで特定のマッチが見つからない場合でも、0.0.0.0/1 との最大プレフィックス マッチがあるので、外部ブリッジ ドメイン pcTag と contract-A を使用します。

  ケース 2 は L3Out-B 用です。この外部 EPG では、1 つのサブネット 0.0.0.0/0 が定義されています。L3Out-B上の入力トラフィックが、マッチングプレフィックス10.10.10.0/24（L3Out-A の下で定義されたもの）を持っている場合、L3Out-A および contract-A の EPG pcTag を使用します。このコントラクトは L3Out-A と結びつけられています。L3Out-Bと関連付けられている contract-B は使用しません。

- 許可されないトラフィック：無効な設定で、共有ルート制御（shared-rtctrl）に対する外部サブネットのスコープが、共有セキュリティ（shared-security）に設定されているサブネットのサブセットとして設定されている場合、トラフィックは許可されません。たとえば、以下の設定は許可されません。

  - *shared rtctrl*：10.1.1.0/24, 10.1.2.0/24
  - *shared security*：10.1.0.0/16

  この場合、10.1.1.0/24 および 10.1.2.0/24 の各プレフィックスがドロップ ルールを使用してインストールされているため、宛先 IP 10.1.1.1 を使用して非境界リーフの入力トラフィックはドロップされます。トラフィックは許可されません。そのようなトラフィックは、shared-rtctrl プレフィックスを shared-security プレフィックスとしても使用するように設定を修正することで、有効にすることができます。

- 不注意によるトラフィック フロー：次の設定シナリオを避けることで、不注意によるトラフィック フローを予防します。

  - **ケース 1** 設定の詳細：
    - VRF1 を使用する L3Out ネットワーク構成（例えば L3Out-1）を、provider1 と呼ぶことにします。
    - VRF2 を使用する 2 番目の L3Out ネットワーク構成（例えば L3Out-2）を provider2 と呼ぶことにします。
    - L3Out-1 の VRF1 は、デフォルト ルート、0.0.0.0/0 をインターネットにアドバタイズします。これは *shared-rtctrl* および *shared-security* の両方を有効にします。
    - L3Out-2 の VRF2 は特定のサブネット、192.0.0.0/8 を DNS および NTP にアドバタイズし、*shared-rtctrl* を有効にします。

- L3Out-2 の VRF2 には特定のサブネット、192.1.0.0/16 があります。これは *shared-security* を有効にします。
- **バリエーション A**：EPG トラフィックは複数の VRF インスタンスに向かいます。
  - EPG1 と L3Out-1 の間の通信は *allow_all* コントラクトによって制御されます。
  - EPG1 と L3Out-2 の間の通信は *allow_all* コントラクトによって制御されます。

    結果：EPG1 から L3Out-2 へのトラフィックも 192.2.x.x に向かいます。
- **バリエーション B**：EPG は 2 番目の共有L3Out ネットワーク の *allow_all* コントラクトに従います。
  - EPG1 と L3Out-1 の間の通信は *allow_all* コントラクトによって制御されます。
  - EPG1 と L3Out-2 の間の通信は *allow_icmp* コントラクトによって制御されます。

    結果：EPG1 から L3Out-2、そして 192.2.x.x へのトラフィックは *allow_all* コントラクトに従います。

- **ケース 2** 設定の詳細：
  - 外部 EPG は、1 つの共有プレフィックスと、その他の非共有プレフィックスを持っています。
  - src = non-shared で到達するトラフィックは、EPG に向かうことが許可されます。
    - **バリエーション A**：意図しないトラフィックが EPG を通過します。

      外部 EPG トラフィックは、次のプレフィックスを持つ L3Out を通過します。

      Unordered List bullet 5 192.0.0.0/8 = import-security, shared-rtctrl

      Unordered List bullet 5 192.1.0.0/16 = shared-security

      Unordered List bullet 5 EPG には 1.1.0.0/16 = shared があります。

      結果：192.2.x.x からのトラフィックも EPG に向かいます。
    - **バリエーション B**：意図しないトラフィックが EPG を通過します。共有 L3Out に到達したトラフィックは EPG を通過できます。

      Unordered List -共有 L3Out VRF には、pcTag = prov vrf を持つ EPG と *allow_all* に設定されているコントラクトがあります。

bullet
5
Unicast EPG は <subnet> = shared となっています。
List
bullet
5

結果：レイヤ 3 Out に到達するトラフィックは EPG を通過することができます。

双方向フォワーディング検出

双方向フォワーディング検出（BFD）を使用して、ピアリング ルータの接続をサポートするように設定されたCisco Application Centric Infrastructure（ACI）ファブリック境界リーフ スイッチ間の転送パスのサブセカンド障害検出時間を可能にします。

BFD は、次のような場合に特に役立ちます。

- ルータ同士の間に直接的な接続がない場合に、レイヤ 2 デバイスまたはレイヤ 2 クラウド経由でピアリング ルータが接続されているとき。転送パスに障害があっても、ピア ルータにはそれがわからない可能性があります。プロトコルの制御に利用できるメカニズムは hello タイムアウトだけですが、タイムアウトまでには数十秒、さらには数分の時間がかかる場合があります。BFD では、障害を 1 秒未満で検出することが可能です。
- 信頼できる障害検出に非対応の物理メディア（共有イーサネットなど）経由でピアリング ルータが接続されているとき。この場合も、ルーティング プロトコルは、時間のかかる hello タイマーに頼るしかありません。
- 1 組のルータの間で多くのプロトコルが実行されているとき、各プロトコルは、独自のタイムアウトでリンク障害を検出する独自の hello メカニズムを持っています。BFD は、すべてのプロトコルに均一のタイムアウトを指定し、それによってコンバージェンス時間の一貫性を保ち、予測可能にします。

次に示す BFD の設定のガイドラインおよび制限事項に従ってください。

- Cisco APIC リリース 3.1(1) 以降、リーフおよびスパイン スイッチ間の BFD は IS-IS のファブリック インターフェイスでサポートされています。さらに、スパイン スイッチの BFD 機能は、OSPF ルートとスタティック ルートでサポートされます。
- Cisco APIC リリース 5.2(4) 以降、BFD 機能は、セカンダリ IPv4/IPv6 サブネットを使用して到達可能なスタティック ルートでサポートされています。サブネットに複数のアドレスが設定されている場合、スタティック BFD セッションは L3Out インターフェイスのセカンダリ サブネットから発信できません。共有サブネット アドレス (vPC シナリオに使用) と浮動 L3Out に使用される浮動 IP アドレスは、サブネットの追加アドレスとして許可され、自動的にスキップされ、静的 BFD セッションの発信元には使用されません。

（注） セッションのソースに使用されているセカンダリアドレスを変更するには、同じサブネットに新しいアドレスを追加し、後で以前のアドレスを削除します。

- BFD は -EX および -FX ライン カード（または新しいバージョン）のモジュラ スパイン スイッチでサポートされ、また BFD は Nexus 9364C 非モジュラ スパイン スイッチ（または新しいバージョン）でサポートされます。
- vPC ピア間の BFD はサポートされません。
- Cisco APIC リリース 5.0(1) 以降、BFD マルチホップはリーフ スイッチでサポートされます。BFD マルチホップ セッションが合計に含まれるようになったため、BFD セッションの最大数は変更されません。
- Cisco APIC リリース 5.0(1) 以降、Cisco ACI は C ビット対応 BFD をサポートしています。BFD がコントロール プレーンに依存しているかいないかは、受信する BFD パケットの C ビットによって判別されます。
- ループバック アドレス ピアでの iBGP 上の BFD はサポートされません。
- インターフェイス ポリシーで BFD サブインターフェイス最適化を有効化できます。このフラグを 1 つのサブインターフェイスに立てることにより、その物理インターフェイス上のすべてのサブインターフェイスの最適化が有効になります。
- BGP プレフィクス ピアの BFD はサポートされません。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

ACI IP SLA

多くの企業ではビジネスのほとんどをオンラインで行い、サービスの損失は企業の収益性に影響を及ぼすことがあります。今では、インターネット サービス プロバイダ（ISP）や内部 IT 部門でさえも、定義済みのサービス レベル、サービス レベル契約（SLA）を提供して、お客様に一定の予測可能性を提供しています。

IP SLA トラッキングは、ネットワークの一般的な要件です。IP SLA トラッキングにより、ネットワーク管理者はネットワーク パフォーマンスに関する情報をリアルタイムで収集できます。Cisco ACI IP SLA では、ICMP および TCP プローブを使用して IP アドレスを追跡できます。トラッキング設定はルートテーブルに影響を与える可能性があり、トラッキング結果がネガティブになったときにルートを削除し、結果が再びポジティブになったときにルートをテーブルに戻すことができます。

ACI IP SLA は、次のものに使用できます。

- スタティック ルート：
  - ACI 4.1 の新機能
  - ルート テーブルからのスタティック ルートの自動削除または追加
  - ICMP および TCP プローブを使用してルートを追跡する
- ポリシーベース リダイレクト（PBR）トラッキング：
  - ACI 3.1 以降で使用可能
  - ネクスト ホップの自動削除または追加
  - ICMP プローブと TCP プローブ、または L2Ping を使用した組み合わせを使用して、ネクストホップ IP アドレスを追跡します。
  - ネクストホップの到達可能性に基づいて PBR ノードにトラフィックをリダイレクトする

PBR トラッキングの詳細については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「ポリシーベース リダイレクトの設定」を参照してください。

（注） いずれの機能でも、設定、API の使用、スクリプトの実行など、プローブの結果に基づいてネットワーク アクションを実行できます。

ACI IP SLA でサポートされるトポロジ

次の ACI ファブリック トポロジは IP SLA をサポートします。

- シングル ファブリック：IP SLA トラッキングは、L3out と EPG/BD の両方を介して到達可能な IP アドレスでサポートされます。

- マルチポッド
  - 異なるポッドで単一のオブジェクト トラッキング ポリシーを定義できます。
  - ワークロードは、あるポッドから別のポッドに移動できます。IP SLA ポリシーは引き続きアクセス可能性情報をチェックし、エンドポイントが移動したかどうかを検出します。
  - エンドポイントが別のポッドに移動すると、IP SLA トラッキングも他のポッドに移動されるため、トラッキング情報は IP ネットワークを通過しません。
- リモート リーフ
  - ACI メイン データ センターおよびリモート リーフ スイッチ全体で単一オブジェクト トラッキング ポリシーを定義できます。
  - リモート リーフ スイッチの IP SLA プローブは、IP ネットワークを使用せずに IP アドレスをローカルに追跡します。
  - ワークロードは、1 つのローカル リーフからリモート リーフに移動できます。IP SLA ポリシーは引き続きアクセス可能性情報をチェックし、エンドポイントが移動したかどうかを検出します。
  - IP SLA ポリシーは、エンドポイントの場所に基づいてリモート リーフ スイッチまたは ACI メイン データ センターに移動し、ローカル トラッキングを行うため、トラッキング トラフィックは IP ネットワークを通過しません。

テナント ルーテッド マルチキャスト

Cisco Application Centric Infrastructure （ACI）テナント ルーテッド マルチキャスト（TRM）は、Cisco ACI テナント VRF インスタンスでレイヤ 3 マルチキャスト ルーティングを有効にします。TRM は、同じサブネット内または異なるサブネット内の送信者と受信者の間のマルチキャスト転送をサポートしています。マルチキャストの送信元と受信者は、同じまたは異なるリーフ スイッチに接続することや、L3Out 接続を使用してファブリックの外部に接続することができます。

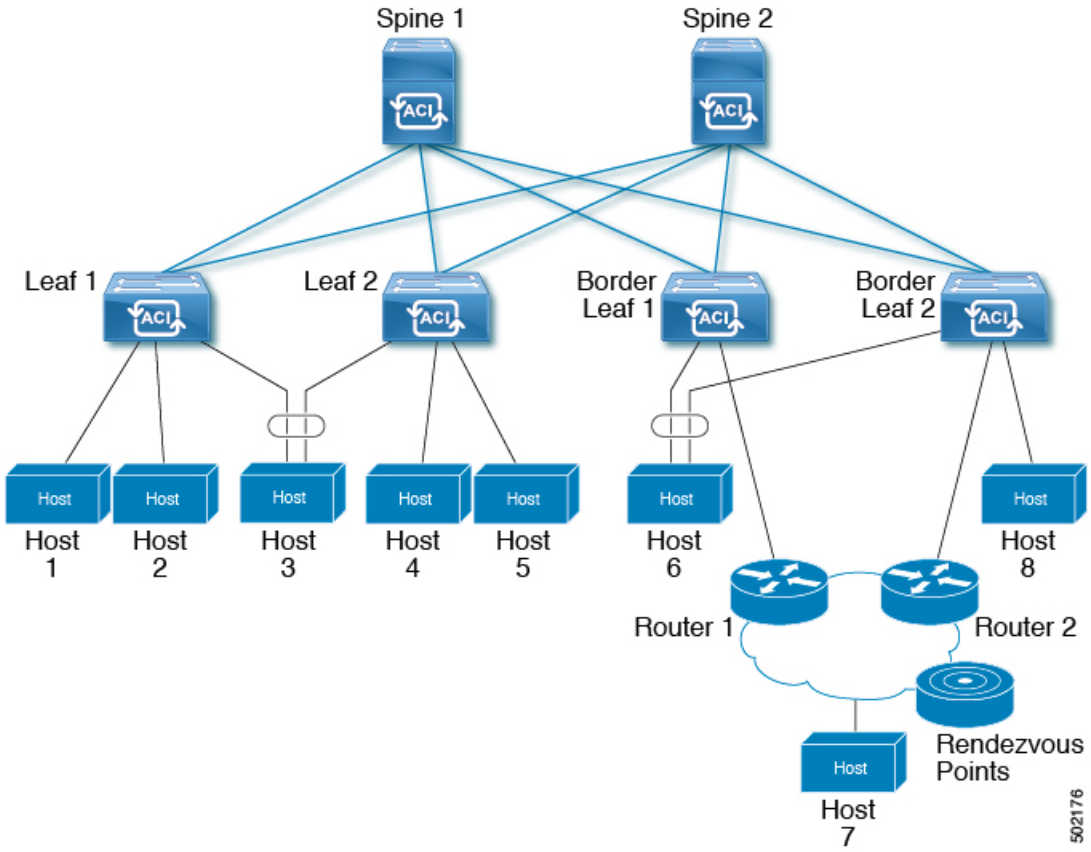
Cisco ACI ファブリックでは、ほとんどのユニキャストと IPv4/IPv6 マルチキャスト ルーティングが同じ境界リーフ スイッチで稼働しており、ユニキャスト ルーティング プロトコル上でマルチキャスト プロトコルが稼働しています。

このアーキテクチャでは、境界リーフ スイッチのみが完全な Protocol Independent Multicast （PIM）または PIM6 プロトコルを実行します。非境界リーフ スイッチは、インターフェイス上でパッシブ モードの PIM/PIM6 を実行します。これらは、その他の PIM/PIM6 ルータとピアリングしません。境界リーフ スイッチは、L3Out を介してそれらの接続された他の PIM/PIM6 ルータとピアリングし、またそれら相互にもピアリングします。

次の図は、IPv4/IPv6 マルチキャスト クラウド内のルータ 1 とルータ 2 に接続する境界リーフ スイッチ 1 と境界リーフ スイッチ 2 を示しています。IPv4/IPv6 マルチキャスト ルーティング

を必要とするファブリック内の各 Virtual Routing and Forwarding（VRF）インスタンスは、それぞれ別に外部マルチキャスト ルータとピアリングします。

図 *72*: マルチキャスト クラウドの概要



ファブリック インターフェイスについて

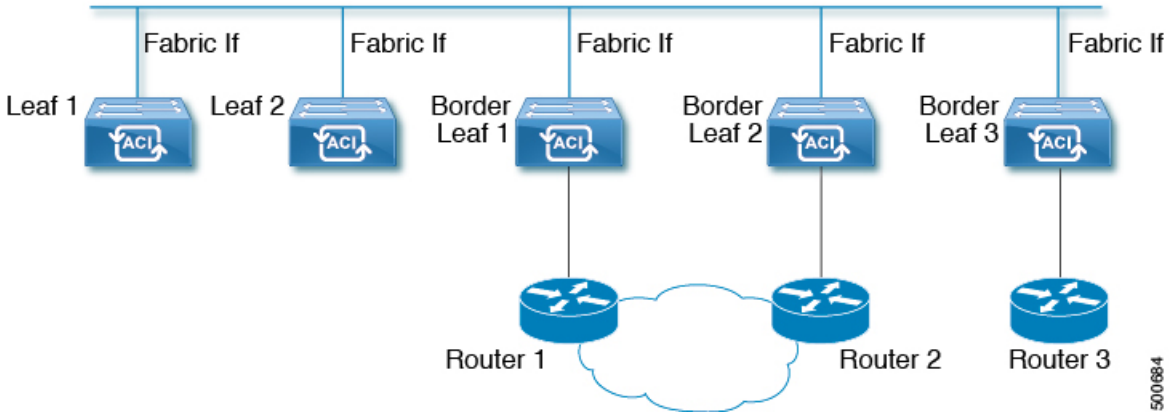
ファブリック インターフェイスはソフトウェア モジュール間の仮想インターフェイスであり、IPv4/IPv6 マルチキャスト ルーティングのファブリックを表します。インターフェイスは、宛先が VRF GIPo（グループ IP 外部アドレス）であるトンネル インターフェイスの形式を取ります。[1]. PIM6 は、PIM4 が使用するものと同じトンネルを共有します。たとえば、境界リーフがグループのトラフィックの転送を担当する指定フォワーダの場合、ファブリック インターフェイスはグループの発信インターフェイス (OIF) となります。ハードウェアのインターフェイスに相当するものはありません。ファブリック インターフェイスの動作状態は、intermediate system-to-intermediate system（IS-IS）によって公開される状態に従ったものとなります。

[1] GIPo（グループ IP 外部アドレス）とは、ファブリック内で転送されたすべてのマルチデスティネーション パケット（ブロードキャスト、未知のユニキャストおよびマルチキャスト）で、VXLAN パケットの外部 IP ヘッダーで使用される宛先マルチキャスト IP アドレスです。

（注） マルチキャスト対応の各 VRF には、ループバック インターフェイスで構成された 1 つ以上の境界リーフ スイッチが必要です。PIM 対応の L3Out のすべてのノードで、一意の IPv4 ループバック アドレスを設定する必要があります。Router-ID ループバックまたは別の一意のループバック アドレスを使用できます。

ユニキャストルーティング用に設定された任意のループバックは再利用できます。このループバック アドレスは、外部ネットワークからルーティングする必要があり、VRF のファブリック MP-BGP (マルチプロトコル境界ゲートウェイ プロトコル) ルートに挿入されます。ファブリック インターフェイスの送信元 IP は、このループバックに、ループバック インターフェイスとして設定されます。次の図は、IPv4/IPv6 マルチキャスト ルーティング用のファブリックを示しています。

図 *73 : IPv4/IPv6* マルチキャスト ルーティング用のファブリック



IPv4/IPv6 テナント ルート マルチキャストの有効化

ファブリックで IPv4 または IPv6 マルチキャスト ルーティングを有効または無効にするプロセスは、次の 3 つのレベルで実行されます。Cisco ACI

- VRF レベル：VRF レベルでマルチキャスト ルーティングを有効にします。
- **L3Out レベル**：VRFインスタンス で構成された 1 つ以上の L3Out に対して PIM/PIM6 を有効にします。
- ブリッジ ドメイン レベル：マルチキャスト ルーティングが必要な 1 つ以上のブリッジ ドメインに対して PIM/PIM6 を有効にします。

トップ レベルでは、IPv4/IPv6 マルチキャスト ルーティングは、任意のマルチキャスト ルーティングが有効なブリッジ ドメインを持つ VRF インスタンスで有効にする必要があります。IPv4/IPv6 マルチキャスト ルーティングが有効な VRF インスタンスでは、IPv4/IPv6 マルチキャスト ルーティングが有効なブリッジ ドメインおよび IPv4/IPv6 マルチキャスト ルーティングが無効なブリッジ ドメインの組み合わせにすることができます。IPv4 / IPv6マルチキャスト ルーティングが無効になっているブリッジドメインは、VRF IPv4 / IPv6マルチキャストパネル

に表示されません。IPv4/IPv6 マルチキャスト ルーティングが有効な L3Out はパネル上でも表示されますが、IPv4/IPv6 マルチキャスト ルーティングが有効なブリッジ ドメインは常に IPv4/IPv6 マルチキャスト ルーティングが有効な VRF インスタンスの一部になります。

Cisco Nexus 93128TX、9396PX、9396TX などのリーフ スイッチでは、IPv4/IPv6 マルチキャスト ルーティングはサポートされていません。すべての IPv4/IPv6 マルチキャスト ルーティングと IPv4/IPv6 マルチキャストが有効な VRF インスタンスは、製品 ID に -EX および -FX という名前を持つスイッチでのみ展開される必要があります。

（注） L3Out ポートとサブインターフェイスがサポートされています。外部 SVI のサポートは、リリースによって異なります。

- リリース 5.2(3) より前のリリースでは、外部 SVI はサポートされていません。
- リリース 5.2(3) 以降では、SVI L3Out のレイヤ 3 マルチキャストがサポートされます。PIM は、物理ポートおよびポート チャネルの SVI L3Out でサポートされますが、vPC ではサポートされません。PIM6 は L3Out SVI ではサポートされません。

レイヤ 3 IPv4/IPv6 マルチキャストの設定のガイドライン、制約事項、および予想される動作

次のガイドラインと制限を確認します。

- IPv4/IPv6 マルチキャストのガイドラインと制約事項 （198 ページ）
- IPv4 マルチキャストのガイドラインと制約事項 （200 ページ）
- IPv6 マルチキャストのガイドラインと制約事項 （201 ページ）

IPv4/IPv6 マルチキャストのガイドラインと制約事項

IPv4 マルチキャストと IPv6 マルチキャストの両方に次の制限が適用されます。

- 第 2 世代リーフスイッチでレイヤ 3 IPv4/IPv6 マルチキャスト機能がサポートされています。第 2 世代スイッチは、製品 ID に -EX、-FX、-FX2、-FX3、-GX、またはそれ以降のサフィックスが付いたスイッチです。
- カスタム QoS ポリシーは、Cisco Application Centric Infrastructure（ACI）ファブリックの外部から送信された（L3Out から受信した）レイヤ 3 マルチキャスト トラフィックではサポートされません。
- ブリッジドメインでの PIMv4/PIM6 およびアドバタイズ ホスト ルートの有効化がサポートされています。
- レイヤ 3 マルチキャストは VRF レベルで有効になり、マルチキャスト プロトコルは VRF インスタンス内で機能します。各 VRF インスタンスでは、マルチキャストを個別に有効化または無効化できます。

- マルチキャストで VRF インスタンスが有効になると、有効になった VRF インスタンスの個別のブリッジドメインと L3Out を有効にしてマルチキャストを構成できます。デフォルトでは、マルチキャストはすべてのブリッジ ドメインと L3Out で無効になっています。
- 双方向 PIMv4/PIM6 は現在サポートされていません。
- マルチキャスト ルータは、パーペイシブ ブリッジ ドメインではサポートされていません。
- サポートされるルートスケールは 2,000 です。マルチキャスト スケール番号は、IPv4 と IPv6 の両方を含む複合スケールです。合計ルート制限は、ルート カウントとして定義されます。各 IPv4 ルートは 1 としてカウントされ、各 IPv6 ルートは 4 としてカウントされます。より多くのマルチキャスト スケールをサポートするノードプロファイルでも、IPv6 ルート スケールは 2,000 のままです。
- PIMv4/PIM6 は、L3Out ルーテッド インターフェイス、レイヤ 3 ポート チャネルを含むルーテッド サブインターフェイス、およびレイヤ 3 ポート チャネル サブインターフェイスでサポートされます。Cisco ACI リリース 5.2(3) 以降、PIMv4 は、物理ポートチャネルおよび直接接続されたポートチャネルの L3Out SVI インターフェイスでサポートされます。PIMv4/PIMv6 はvPC インターフェイスでの L3Out SVI ではサポートされません。
- L3Out で PIMv4/PIM6 を有効にすると、暗黙的な外部ネットワークが設定されます。このアクションの結果、L3Out が導入され、外部ネットワークを定義していない場合でもプロトコルが発生する可能性があります。
- マルチキャスト送信元が孤立ポートとしてリーフA に接続され、リーフB に L3Out があり、リーフA とリーフB が vPC ペアにある場合、マルチキャスト送信元に関連付けられた EPG カプセル化 VLAN はリーフB に展開されます。
- ブリッジ ドメインに接続されている送信元からパケットを受信する入力リーフ スイッチの動作は、レイヤ 3 IPv4 または IPv6 マルチキャスト サポートによって異なります。
  - レイヤ 3 IPv4 マルチキャスト サポートは、IPv4 マルチキャスト ルーティングのために有効になっているブリッジドメインに接続された送信元からのパケットを入力リーフスイッチが受信した場合、その入力リーフスイッチは、ルーテッド VRF インスタンスのコピーのみをファブリックに送信します（ルーテッドは、TTL が 1 ずつ減少し、送信元 MAC がパーベイシブ サブネット MAC で書き換えられることを意味します）。また、出力リーフ スイッチも、関連するすべてのブリッジ ドメイン内の受信者へパケットをルーティングします。そのため、受信者のブリッジドメインが送信元と同じで、リーフ スイッチが送信元とは異なる場合、その受信者は同じブリッジ ドメイン内ですが、ルーティングされたコピーを受け取り続けます。これは、送信元と受信者が同じブリッジ ドメインおよび同じリーフ スイッチ上にあり、このブリッジドメインで PIM が有効になっている場合にも適用されます。

    詳細については、次のリンク ポッドの追加 で、既存のレイヤ 2 設計を活用するマルチポッドをサポートする、レイヤ3マルチキャストに関する詳細情報を参照してください。

  - レイヤ 3 IPv6 マルチキャスト サポートは、IPv6 マルチキャスト ルーティングのために有効になっているブリッジドメインに接続された送信元からのパケットを入力リーフスイッチが受信した場合、その入力リーフスイッチは、ルーテッド VRF インスタ

ンスのコピーのみをファブリックに送信します（ルーテッドは、TTL が 1 ずつ減少し、送信元 MAC がパーベイシブ サブネット MAC で書き換えられることを意味します）。また、出力リーフ スイッチも、受信者へパケットをルーティングします。出力リーフは、パケット内の TTL を 1 だけ減らします。これにより、TTL が 2 回減少します。また、ASM の場合、マルチキャスト グループに有効な RP が設定されている必要があります。

- VRF 間マルチキャスト通信ではフィルタを使用できません。
- **clear ip mroute** コマンドは使用しないでください。このコマンドは内部デバッグに使用され、実稼働ネットワークではサポートされません。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

- マルチキャスト PIM では、グループ範囲が SSM と共有ツリー範囲の間で同じであるか、または重複している場合、SSM が優先されます。

IPv4 マルチキャストのガイドラインと制約事項

IPv4 マルチキャストには、特に次の制限が適用されます。

- Cisco ACI ファブリックの境界リーフスイッチがマルチキャストを実行しており、L3Out でマルチキャストを無効にしているときにユニキャスト到達可能性がある場合、外部ピアが Cisco Nexus 9000 スイッチの場合、トラフィック損失が発生します。これは、トラフィックがファブリックに送信される場合（送信元はファブリックの外部にあり、受信者はファブリックの内部にある場合）、またはファブリックを通過する場合（送信元と受信者がファブリックの外部にあり、ファブリックが送信中の場合）に影響します。
- Any Source Multicast (ASM) と Source-Specific Multicast (SSM) は IPv4 向けにサポートされています。

- VRF インスタンスごとにルートマップで SSM マルチキャストの範囲を最大 4 つ構成できます。
- IGMP スヌーピングは、マルチキャスト ルーティングが有効になっているパーベイシブ ブリッジ ドメインでは無効にできません。
- FEX ではレイヤ 3 マルチキャストはサポートされていません。FEX ポートに接続されているマルチキャストの送信元または受信先がサポートされています。テスト環境で FEX を追加する方法についての詳細は、次の URL の『アプリケーション セントリック インフラストラクチャとファブリック エクステンダの構成』を参照してください：https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/200529-Configure-a-Fabric-Extender-with-Applica.html。FEX ポートに接続されているマルチキャストの送信元または受信先はサポートされていません。

IPv6 マルチキャストのガイドラインと制約事項

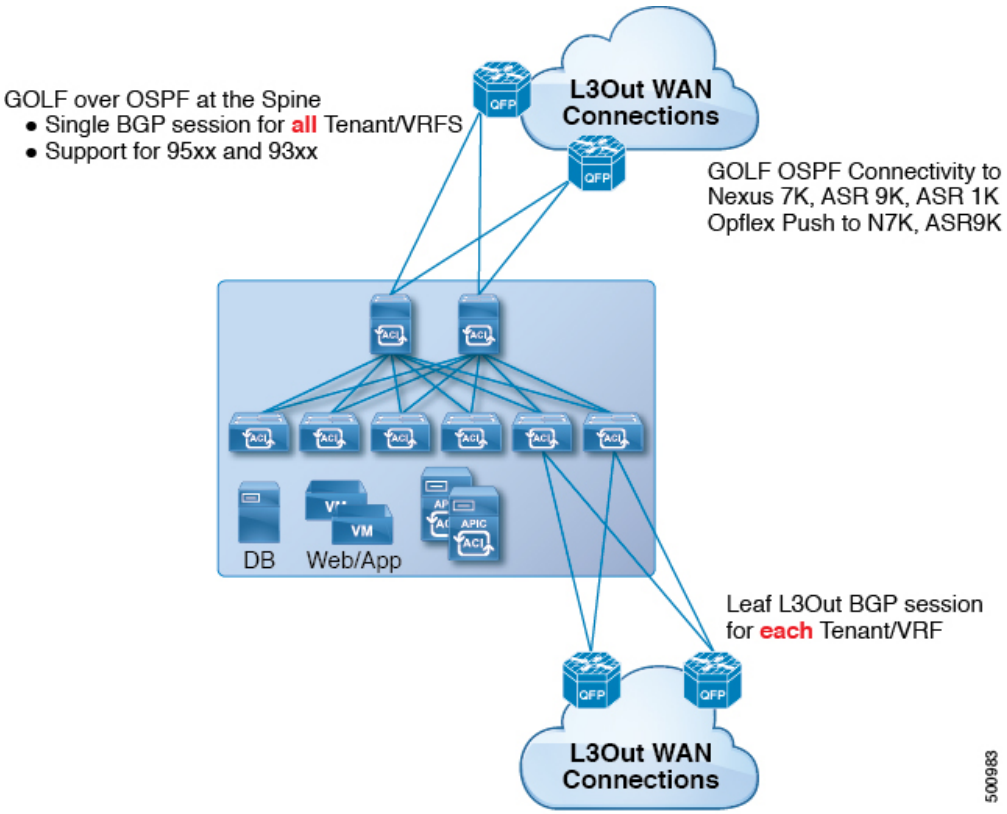
IPv6 マルチキャストには、特に次の制限が適用されます。

- Source Specific Multicast（SSM）はサポートされていますが、RFC 3306-Unicast-Prefix-based IPv6 Multicast Addresses で固定 SSM 範囲が指定されています。したがって、SSM の範囲は IPv6 では変更できません。
- VRF インスタンスごとにルートマップで SSM マルチキャストの範囲を最大 4 つ構成できます。
- Any Source Multicast（ASM）は IPv6 でサポートされます。
- IPv6 の OIF および VRF スケール番号は、IPv4 の場合と同じです。
- スタティック RP 設定のみの PIM6 をサポートしています。Auto-RP および BSR は PIM6 ではサポートされません。
- ファブリック内のレシーバはサポートされません。IPv6 マルチキャストを有効にする場合は、MLD スヌープ ポリシーを無効にする必要があります。MLD スヌーピングと PIM6 を同じ VRF インスタンスで有効にすることはできません。
- 現在、レイヤ 3 マルチキャスト リスナー検出（MLD）は Cisco ACI ではサポートされていません。
- ファブリック ランデブー ポイント（RP）は、IPv6 マルチキャストではサポートされません。
- Cisco Multi-Site Orchestrator のサポートは利用できません。

Cisco ACI GOLF

Cisco ACI GOLF 機能 (ファブリック WAN のレイヤ 3 EVPN サービス機能とも呼ばれる) では、より効率的かつスケーラブルな ACI ファブリック WAN 接続が可能になります。スパイン スイッチに接続されている WAN に OSPF 経由で BGP EVPN プロトコルが使用されます。

図 *74 : Cisco ACI GOLF* のトポロジ



すべてのテナント WAN 接続が、WAN ルータが接続されたスパイン スイッチ上で単一のセッションを使用します。データセンター相互接続ゲートウェイ（DCIG）へのテナント BGP セッションのこの集約では、テナント BGP セッションの数と、それらすべてに必要な設定の量を低減することによって、コントロールプレーンのスケールが向上します。ネットワークは、スパイン ファブリック ポートに設定された レイヤ 3 サブインターフェイスを使用して拡張されます。GOLF を使用した、共有サービスを伴うトランジット ルーティングはサポートされていません。

スパイン スイッチでの GOLF 物理接続のためのレイヤ 3 外部外側ネットワーク (`L3extOut`) は、`infra` テナントの下で指定され、次のものを含みます:

- `LNodeP` (infra テナントの L3Out では、`l3extInstP` は必要ありません)。
- infra テナントの GOLF 用の `L3extOut` のプロバイダ ラベル。
- OSPF プロトコル ポリシー

- BGP プロトコル ポリシー

すべての通常テナントが、上記で定義した物理接続を使用します。通常のテナントで定義した `L3extOut` では、次が必要です:

- サブネットとコントラクトを持つ `l3extInstP` (EPG)。サブネットの範囲を使用して、ルート制御ポリシーとセキュリティ ポリシーのインポートまたはエクスポートを制御します。ブリッジドメインサブネットは外部的にアドバタイズするように設定される必要があり、アプリケーション EPG および GOLF L3Out EPG と同じ VRF に存在する必要があります。
- アプリケーション EPG と GOLF L3Out EPG の間の通信は、(契約優先グループではなく) 明示的な契約によって制御されます。
- `l3extConsLbl` コンシューマ ラベル。これは `infra` テナントの GOLF 用の `L3Out` の同じプロバイダ ラベルと一致している必要があります。ラベルを一致させることにより、他のテナント内のアプリケーション EPG が `LNodeP` 外部 `L3Out` EPG を利用することが可能になります。
- `infra` テナント内のマッチング プロバイダ `L3extOut` の BGP EVPN セッションは、この `L3Out` で定義されたテナント ルートをアドバタイズします。

ルート ターゲット フィルタリング

ルート ターゲット フィルタリングは、BGP ルーティング テーブルに格納されているルートをフィルタリングすることにより、BGP ルーティング テーブルを最適化する方法です。このアクションは、明示的なルート ターゲット ポリシーまたは自動化されたアルゴリズムによって実行できます。

ルート ターゲット ポリシー

ルート ターゲット ポリシーは、VRF 間で共有できる BGP ルートを明示的に定義します。ローカル VRF から別のローカル VRF にエクスポートできるローカル ルートを指定し、外部 VRF からローカル VRF にインポートできるルートを指定します。

APIC 内では、VRF の作成時または構成時にルート ターゲット ポリシーを指定できます。これを L3 Out ポリシーに関連付けて、そのポリシーに関連付けられた BGP ルート共有を定義できます。

自動ルート ターゲット フィルタリング

自動ルート ターゲット フィルタリングは、BGP ルーティング テーブルを最適化して全体的な効率を最大化する自動アルゴリズムを実装し、直接接続された VPN に関連付けられているものを除き、インポートされたすべての BGP ルート ターゲットのストレージをフィルタリングしてメモリを節約します。

VRF が別のポリシー要素（PE）ルータから BGP VPN-IPv4 または VPN-IPv6 ルート ターゲットを受信すると、少なくとも 1 つの VRF がそのルートのルート ターゲットをインポートする場合にのみ、BGP はそのルート ターゲットをローカル ルーティング テーブルに格納します。

ルートのルート ターゲットのいずれかをインポートする VRF がない場合、BGP はルート ターゲットを破棄します。その意図は、BGP が直接接続された VPN のルート ターゲットのみを追跡し、他のすべての VPN-IPv4 または VPN-IPv6 ルート ターゲットを破棄してメモリを節約することです。

新しい VPN がルータに接続されている場合（つまり、VRF のインポート ルート ターゲット リストが変更された場合）、BGP は自動的にルート リフレッシュ メッセージを送信して、以前に破棄したルートを取得します。

DCIG への BGP EVPN タイプ 2 のホスト ルートの配信

APIC ではリリース 2.0(1f) まで、ファブリック コントロール プレーンは EVPN ホスト ルートを直接送信してはいませんでしたが、Data Center Interconnect Gateway（DCIG）にルーティングしている BGP EVPN タイプ 5（IP プレフィックス）形式のパブリック ドメイン（BD）サブネットをアドバタイズしていました。これにより、最適ではないトラフィックの転送となる可能性があります。転送を改善するため APIC リリース 2.1 x では、ファブリック スパインを有効にして、パブリック BD サブネットとともに DCIG に EVPN タイプ 2（MAC-IP）ホスト ルートを使用してホスト ルートをアドバタイズできます。

そのためには、次の手順を実行する必要があります。

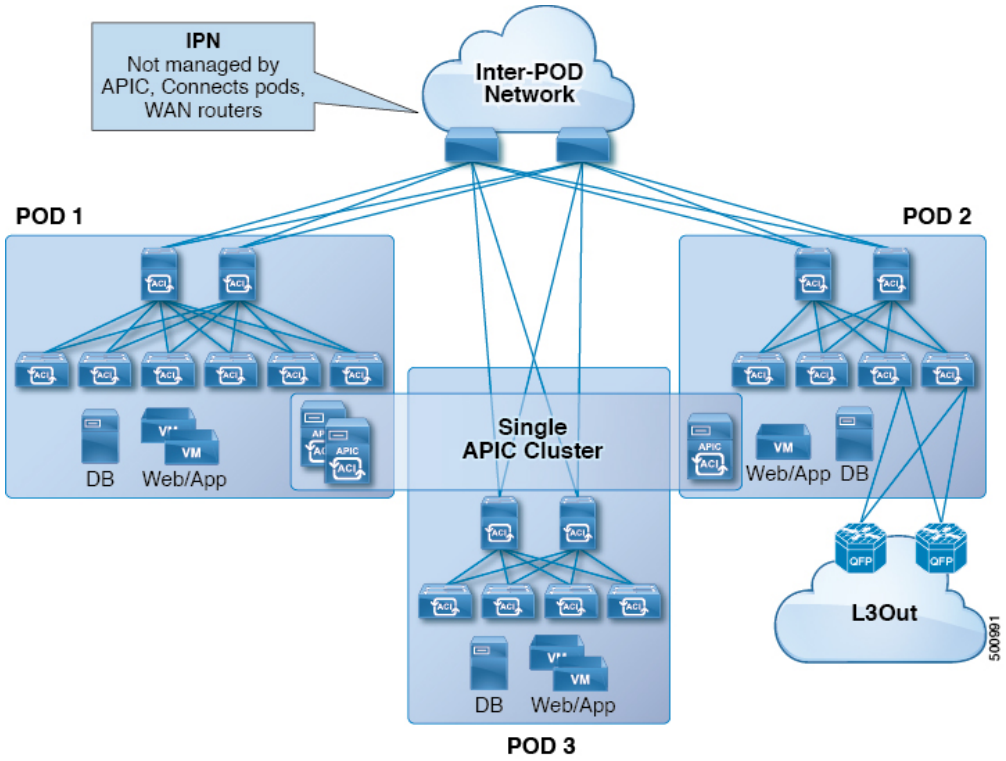
1. BGP アドレス ファミリ コンテキスト ポリシーを設定する際に、ホスト ルート リークを有効にします。
2. GOLF セットアップで BGP EVPN へのホスト ルートをリークする場合：
    1. GOLF が有効になっている場合にホスト ルートを有効にするには、インフラストラクチャ テナント以外に、BPG アドレス ファミリ コンテキスト ポリシーがアプリケーション テナント（アプリケーション テナントはコンシューマ テナントであり、エンドポイントを BGP EVPN にリークします）で設定されている必要があります。
    2. 単一ポッド ファブリックについては、ホスト ルート機能は必要ありません。ホスト ルート機能は、マルチポッド ファブリック セットアップで最適ではない転送を避けるために必要です。ただし、単一ポッド ファブリックがセットアップされる場合、エンドポイントから BGP EVPN にリークするため、ファブリック外部接続ポリシーを設定し ETEP IP アドレスを提供する必要があります。そうしないと、ホスト ルートは、BGP EVPN にはリークされません。
3. VRF のプロパティを設定する場合：
    1. IPv4 および IPv6 の各アドレス ファミリの BGP コンテキストに BGP アドレス ファミリ コンテキスト ポリシーを追加します。
    2. VRF からインポートまたはエクスポート可能なルートを特定する BGP ルート ターゲット プロファイルを設定します。

マルチポッド

マルチポッドは、隔離されたコントロールプレーンプロトコルを持つ複数のポッドで構成された、フォールトトレラントの高いファブリックのプロビジョニングを可能にします。また、マルチポッドでは、さらに柔軟にリーフとスパイン スイッチ間のフル メッシュ配線を行うことができます。たとえば、リーフ スイッチが異なるフロアや異なる建物にまたがって分散している場合、マルチポッドでは、フロアごと、または建物ごとに複数のポッドをプロビジョニングし、スパイン スイッチを通じてポッド間を接続することができます。

マルチポッドは、異なるポッドの ACI スパイン間のコントロール プレーン通信プロトコルとして MP-BGP EVPN を使用します。WAN ルータは、IPN でプロビジョニング可能で、スパイン スイッチに直接接続されるか、境界リーフスイッチに接続されます。マルチポッドはすべてのポッドに単一の APIC クラスタを使用します。そのため、すべてのポッドが単一のファブリックとして機能します。ポッド全体にわたって個々の APIC コントローラが配置されますが、それらはすべて単一の APIC クラスタの一部です。

図 *75*: マルチポッドの概要



コントロールプレーンの分離では、IS-IS と COOP はポッド間で拡張されません。エンドポイントは、ポッド間の IPN 経由で BGP EVPN を使用してポッド間で同期します。各ポッドの 2 つのスパインは、他のポッドのスパインとの BGP EVPN セッションを持つように構成されています。IPN に接続されたスパインは、ポッド内の COOP からエンドポイントとマルチキャスト グループを取得しますが、ポッド間の IPN EVPN セッションを介してそれらをアドバタイズします。受信側では、BGP がそれらを COOP に返し、COOP はポッド内のすべてのスパイン

間でそれらを同期します。WAN ルートは、BGP VPNv4/VPNv6 アドレス ファミリを使用してポッド間で交換されます。EVPN アドレス ファミリを使用して交換されることはありません。

ピアおよびルート リフレクタとしてポッド間で通信するためにスパイン スイッチを設定するには、2 つのモードがあります。

- 自動化
  - 自動モードは、すべてのスパインが相互にピアリングするフルメッシュをサポートしないルート リフレクタ ベースのモードです。管理者は、既存の BGP ルート リフレクタ ポリシーを投稿し、IPN 対応（EVPN）ルート リフレクタを選択する必要があります。すべてのピア/クライアント設定は、APIC によって自動化されます。
  - 管理者には、ファブリックに属していないルート リフレクタ（たとえば、IPN 内）を選択するオプションがありません。
- 手動
  - 管理者は、ルート リフレクタなしですべてのスパインが相互にピアリングするフルメッシュを構成するオプションがあります。
  - 手動モードでは、管理者は既存の BGP ピア ポリシーを投稿する必要があります。

次に示すガイドラインおよび制限事項に従ってください。

- ポッドを ACI ファブリックに追加するときは、コントロールプレーンが収束するのを待ってから、別のポッドを追加します。
- OSPF は、POD 間の到達可能性を提供するために、ACI スパイン スイッチおよび IPN スイッチに展開されます。レイヤ 3 サブインターフェイスは、IPN スイッチに接続するスパイン上に作成されます。OSPF はこれらのレイヤ 3 サブインターフェイスで有効になっており、POD ごとに TEP プレフィックスが OSPF を介してアドバタイズされます。外部スパイン リンクごとに 1 つのサブインターフェイスが作成されます。POD 間の東西トラフィックの量が多いことが予想される場合は、各スパインに多くの外部リンクをプロビジョニングします。現在、ACI スパイン スイッチは各スパインで最大 64 の外部リンクをサポートしており、各サブインターフェイスは OSPF 用に構成できます。スパイン プロキシ TEP アドレスは、すべてのサブインターフェイス上の OSPF でアドバタイズされ、プロキシ TEP アドレスの IPN スイッチで最大 64 ウェイの ECMP につながります。同様に、スパインは OSPF 経由で IPN スイッチから他の POD のプロキシ TEP アドレスを受け取り、スパインはリモート ポッド プロキシ TEP アドレスに対して最大 64 ウェイ ECMP を持つことができます。このようにして、これらすべての外部リンクに分散された POD 間のトラフィックは、必要な帯域幅を提供します。
- スパイン スイッチのすべてのファブリック リンクがダウンすると、OSPF は最大メトリックで TEP ルートをアドバタイズします。これにより、IPN スイッチは ECMP からスパイン スイッチを強制的に削除し、IPN がトラフィックをダウン スパイン スイッチに転送するのを防ぎます。その後、トラフィックは、アップ状態のファブリック リンクを持つ他のスパインによって受信されます。

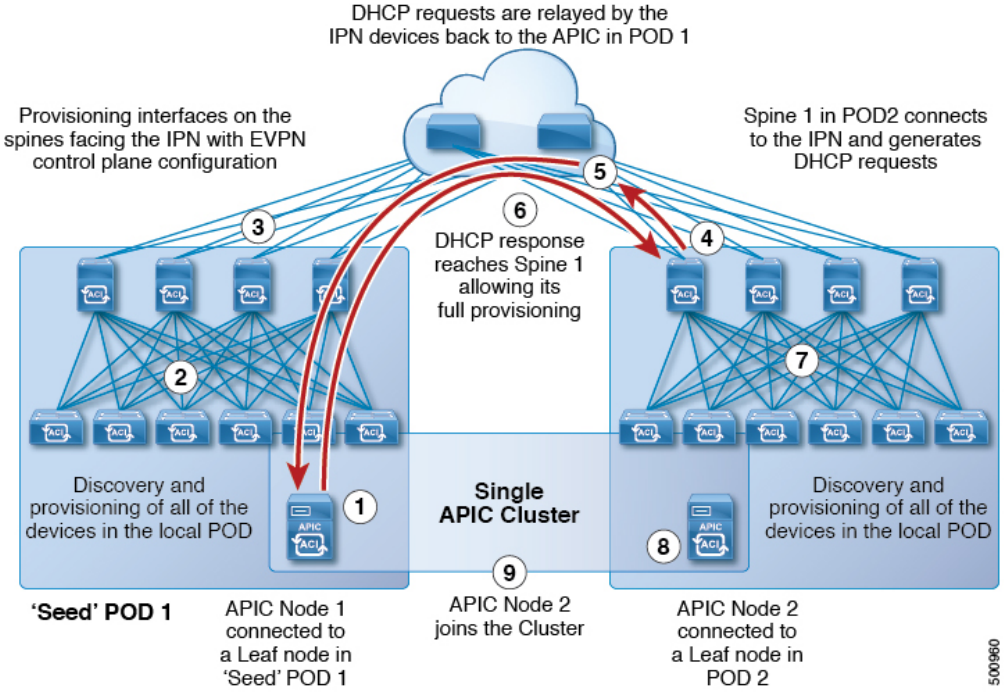
- APIC リリース 2.0(2) までマルチポッドは GOLF でサポートされていません。リリース 2.0(2) では、同じファブリックでの 2 つの機能を、スイッチ名の末尾に「EX」のない Cisco Nexus N9000K スイッチ上でのみサポートしています。たとえば N9K-9312TX です。2.1(1) リリース以降では、2 つの機能を、マルチポッドおよび EVPN トポロジで使用されているすべてのスイッチでともに展開できるようになりました。
- マルチポッド ファブリックで、POD1 のスパインがインフラ テナント L3extOut 1 を使用する場合、他のポッド（POD2、POD3）の TOR は同じインフラ L3extOut（L3extOut 1）をレイヤ 3 EVPN コントロールプレーンの接続には使用できません。他のポッドの WAN 接続のトランジットとして POD を使用することはサポートされていないため、各ポッドは独自のスパイン スイッチとインフラ L3extOut を使用する必要があります。
- ポッド間で交換されるルートを制限するためのフィルタリングは行われません。各ポッドに存在するすべてのエンドポイントおよび WAN ルートは、他のポッドにエクスポートされます。
- ポッド間のインバンド管理は、すべてのスパインのセルフ トンネルによって自動的に構成されます。
- ポッド間でサポートされる最大遅延は 10 ミリ秒 RTT であり、これは、最大 500 マイルの地理的距離に大まかに変換されます。

複数ポッドのプロビジョニング

IPN は APIC では管理されません。これは、次の情報が事前する必要があります。

- すべての POD のスパインに接続されているインターフェイスを構成します。VLAN 4 または VLAN 5 を使用し、 MTU 9150 のおよび正しい IP アドレスが関連付けられています。ポッドの接続のいずれかにリモート リーフスイッチが含まれている場合は、multipod インターフェイス/サブインターフェイスの VLAN 5 を使用します。
- 正しいエリア ID を持つサブインターフェイスで OSPF を有効にします。
- すべての背表紙に接続されている IPN インターフェイスで DHCP リレーを有効にします。
- PIM をイネーブルにします。
- PIM Bidir グループの範囲（デフォルトで 225.0.0.0/8）としてブリッジドメイン GIPO 範囲を追加します。
- PIM として 239.255.255.240/28 を追加 bidir 範囲をグループ化します。
- すべてのスパインに接続された PIM および IGMP をインターフェイスで有効にします。

図 *76 :* マルチポッドのプロビジョニング



マルチポッド検出プロセスは、次のシーケンスに従います。

1. POD1 に接続された APIC1 は、検出プロセスを開始します。

2. APIC1 に直接接続されている POD のスパイン スイッチとリーフスイッチは、単一ポッド ファブリックの検出と同じ方法で検出されます。

3. APIC1 は L3out ポリシーを POD1 のスパインにプッシュします。スパイン L3out ポリシーは、スパイン上の IPN 接続インターフェイスをプロビジョニングし、IPN への IP 接続が確立されます。

4. POD2 スパインは DHCP リクエストを IPN に送信します。

5. IPN は DHCP リクエストを APIC にリレーします。

6. APIC は、スパイン L3Out 構成からのサブインターフェイス IP を使用して DHCP 応答を送信します。DHCP応答を受信すると、スパインはIPNインターフェイスにIPアドレスを構成し、DHCP 応答のリレー アドレスをゲートウェイ アドレスとして使用して APIC への静的ルートを作成し、OSPG を有効にするスパインから L3Out 構成をダウンロードします。 APIC 静的ルートは、インフラ DHCP リレーを構成し、すべてのファブリック ポートとスパイン L3Out ポートに対してDHCP クライアントを有効にします。その後、スパインは通常の起動シーケンスに従って起動します。

7. POD2 の他のすべてのノードは通常どおり起動します。

8. POD2 の APIC コントローラは通常どおり検出されます。

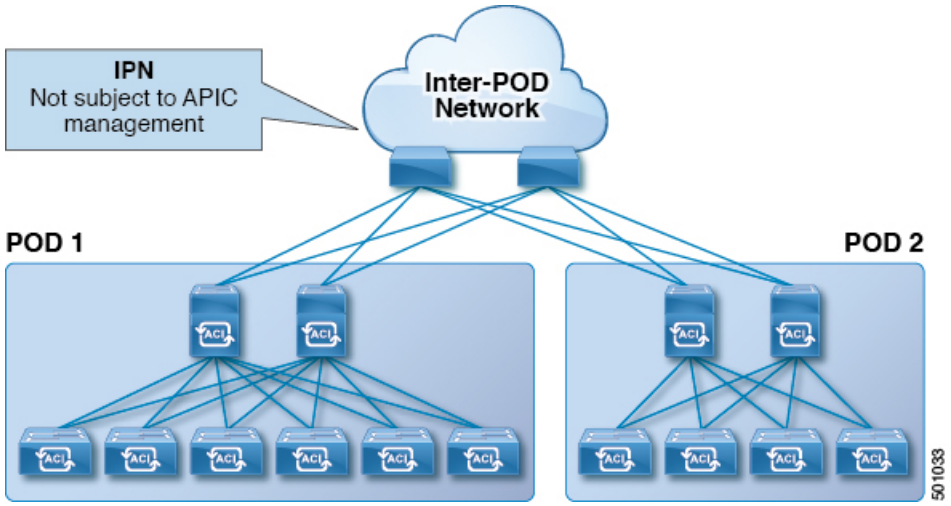
9. POD2 の APIC コントローラが APIC クラスタに加わります。

マルチポッド QoS および DSCP 変換ポリシー

Cisco ACI ファブリック内でトラフィックが送受信される場合、QoS レベルは VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定されます。Cisco APIC の管理下にないデバイスが通過するパケットの CoS 値を変更する可能性があるマルチポッド トポロジでは、Cisco ACI とパケット内の DSCP 値の間のマッピングを作成することにより、QoS レベルの設定を保持できます。

ポッド間の IPN トラフィックで QoS 設定を保持することは検討しないが、ファブリックに入出力するパケットの元の CoS 値を保持したい場合は、入力および出力トラフィックのサービスクラス（CoS）プレゼンテーション （222 ページ） を参照してください。

図 77: マルチポッド トポロジ



この図に示すように、マルチポッド トポロジ内のポッド間のトラフィックは IPN を通過します。IPN には、Cisco APIC の管理下にないデバイスが含まれる場合があります。ネットワークパケットが POD1 のスパインまたはリーフスイッチから送信されると、IPN のデバイスはパケットの 802.1p 値を変更する場合があります。この場合、フレームが POD2 のスパインまたはリーフスイッチに到達すると、POD1 のソースで割り当てられた Cisco ACI QoS レベル値ではなく、IPN デバイスによって割り当てられた 802.1p 値が設定されます。

パケットの適切な QoS レベルを維持し、優先順位の高いパケットが遅延またはドロップされないようにするために、IPN によって接続された複数の POD 間を移動するトラフィックに DSCP 変換ポリシーを使用できます。DSCP 変換ポリシーが有効になっている場合、Cisco APIC は指定したマッピング ルールに従って、QoS レベル値（VXLAN パケットの CoS 値で表される）を DSCP 値に変換します。POD1 から送信されたパケットが POD2 に到達すると、マッピングされた DSCP 値が適切な QoS レベルの元の CoS 値に変換されます。

エニーキャストサービスについて

エニーキャスト サービスは、Cisco ACI ファブリックでサポートされています。一般的な使用例は、マルチポッドファブリックのポッドで Cisco 適応型セキュリティアプライアンス（ASA）

ファイアウォールをサポートすることですが、エニーキャストを使用して、ドメインネームシステム（DNS）サーバーやプリント サービスなどの他のサービスを有効にすることもできます。ASAの使用例では、ファイアウォールがすべてのポッドにインストールされ、エニーキャストが有効になっているため、ファイアウォールをエニーキャスト サービスとして提供できます。ファイアウォールの1つのインスタンスがダウンしても、リクエストは次に利用可能な最も近いインスタンスにルーティングされるため、クライアントには影響しません。各ポッドにASA ファイアウォールをインストールしてから、エニーキャストを有効にして、使用する IP アドレスと MAC アドレスを構成します。

APICは、VRFが展開されている、またはエニーキャストEPGを許可するコントラクトがあるリーフスイッチに、エニーキャスト MAC および IP アドレスの構成を展開します。

最初に、各リーフスイッチはエニーキャスト MAC アドレスと IP アドレスをスパイン スイッチへのプロキシ ルートとしてインストールします。エニーキャスト サービスからの最初のパケットが受信されると、サービスの接続先情報が、サービスがインストールされているリーフスイッチにインストールされます。他のすべてのリーフスイッチは、引き続きスパインプロキシをポイントします。ポッド内のリーフの背後にあるエニーキャスト サービスが学習されると、COOPは、ポッドにローカルなサービスを指すようにスパイン スイッチにエントリをインストールします。

エニーキャスト サービスが 1 つのポッドで実行されている場合、スパインは BGP-EVPN を介してポッドに存在するエニーキャストサービスのルート情報を受け取ります。エニーキャストサービスがすでにローカルに存在する場合、COOPはリモートPodのエニーキャストサービス情報をキャッシュします。リモート ポッドを介したこのルートは、サービスのローカル インスタンスがダウンした場合にのみインストールされます。

リモート リーフ スイッチ

ACI ファブリックのリモート リーフ スイッチについて

ACI ファブリックの展開では、ローカルスパインスイッチまたは APIC が接続されていない Cisco ACI リーフスイッチのリモートデータセンタに、ACI サービスと APIC 管理を拡張できます。

リモート リーフ スイッチがファブリックの既存のポッドに追加されます。メインデータセンターに展開されるすべてのポリシーはリモートスイッチで展開され、ポッドに属するローカルリーフスイッチのように動作します。このトポロジでは、すべてのユニキャストトラフィックはレイヤ 3 上の VXLAN を経由します。レイヤ 2 ブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）メッセージは、WAN を使用するレイヤ 3 マルチキャスト（bidirectional PIM）を使用することなく、 Head End Replication（HER）トンネルを使用して送信されます。スパイン スイッチ プロキシを使用する必要があるすべてのトラフィックは、メイン データセンターに転送されます。

APIC システムは、起動時にリモート リーフ スイッチを検出します。その時点から、ファブリックの一部として APIC で管理できます。

（注）
- すべての inter-VRF トラフィック（リリース 4.0(1) 以前）は、転送される前にスパイン スイッチに移動します。
- リリース 4.1(2) 以前では、リモート リーフを解除する前に、vPC を最初に削除する必要があります。

リリース 4.0(1) でのリモート リーフ スイッチの動作の特性

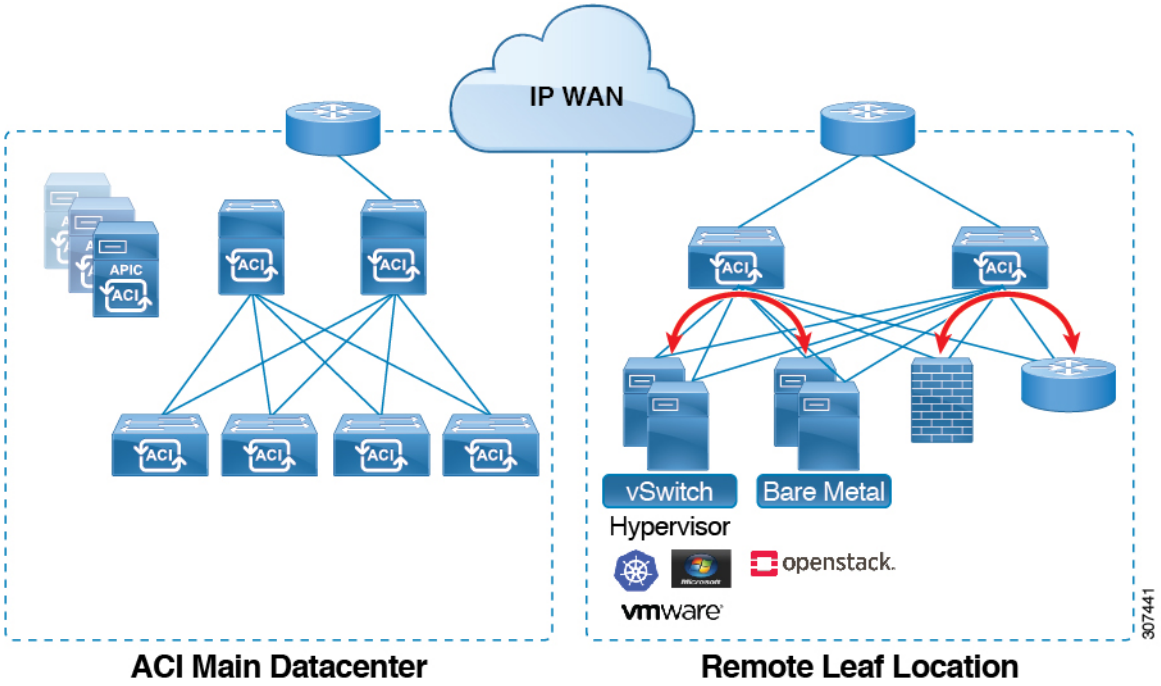
リリース 4.0(1) 以降、リモート リーフ スイッチの動作には次の特徴があります。

- spine-proxy からサービスを切り離すことによって WAN 帯域幅の使用量を削減します。
  - PBR：ローカル PBR デバイスまたは vPC の背後にある PBR デバイスでは、ローカル スイッチングはスパイン プロキシに移動せずに使用されます。ピア リモート リーフ上の孤立ポートの PBR デバイスでは、RL-vPC トンネルを使用します。これは、主要 DC へのスパイン リンクが機能しているか否かを問わず該当します。
  - ERSPAN：ピア接続先 EPG では、RL-vPC トンネルが使用されます。ローカルな孤立ポートまたは vPC ポート上の EPG は、宛先 EPG へのローカル スイッチングを使用します。これは、主要 DC へのスパイン リンクが機能しているか否かを問わず該当します。
  - 共有サービス：パケットはスパイン プロキシ パスを使用しないため WAN 帯域幅の使用量を削減します。
  - Inter-VRF トラフィックは上流に位置するルータ経由で転送され、スパインには配置されません。
  - この機能強化は、リモート リーフ vPC ペアにのみ適用されます。リモート リーフ ペアを介した通信では、スパイン プロキシは引き続き使用されます。
- spine-proxy に到達不能な場合のリモート リーフ ロケーション内の（ToR グリーニング プロセスを通じた）不明な L3 エンドポイントの解像度。

リリース4.1(2) でのリモート リーフ スイッチ動作の特性

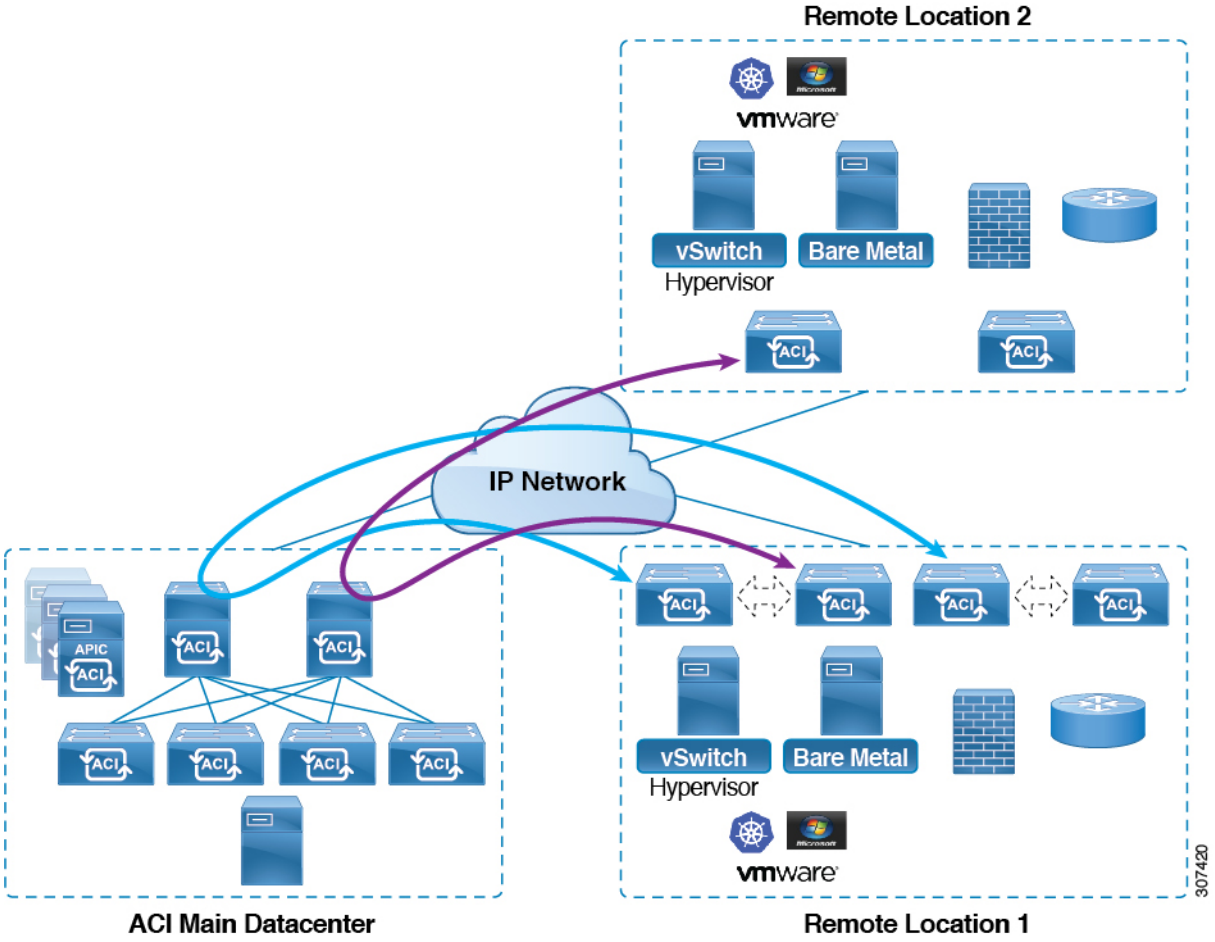
リリース4.1(2) よりも前のリリースでは、次の図に示すように、リモート リーフ ロケーション上のすべてのローカル スイッチング（リモート リーフ vPC ピア内）トラフィックは、物理的または仮想的にエンドポイント間で直接スイッチングされます。

図 *78 : Local Switching Traffic* : リリース *4.1(2)* 以前



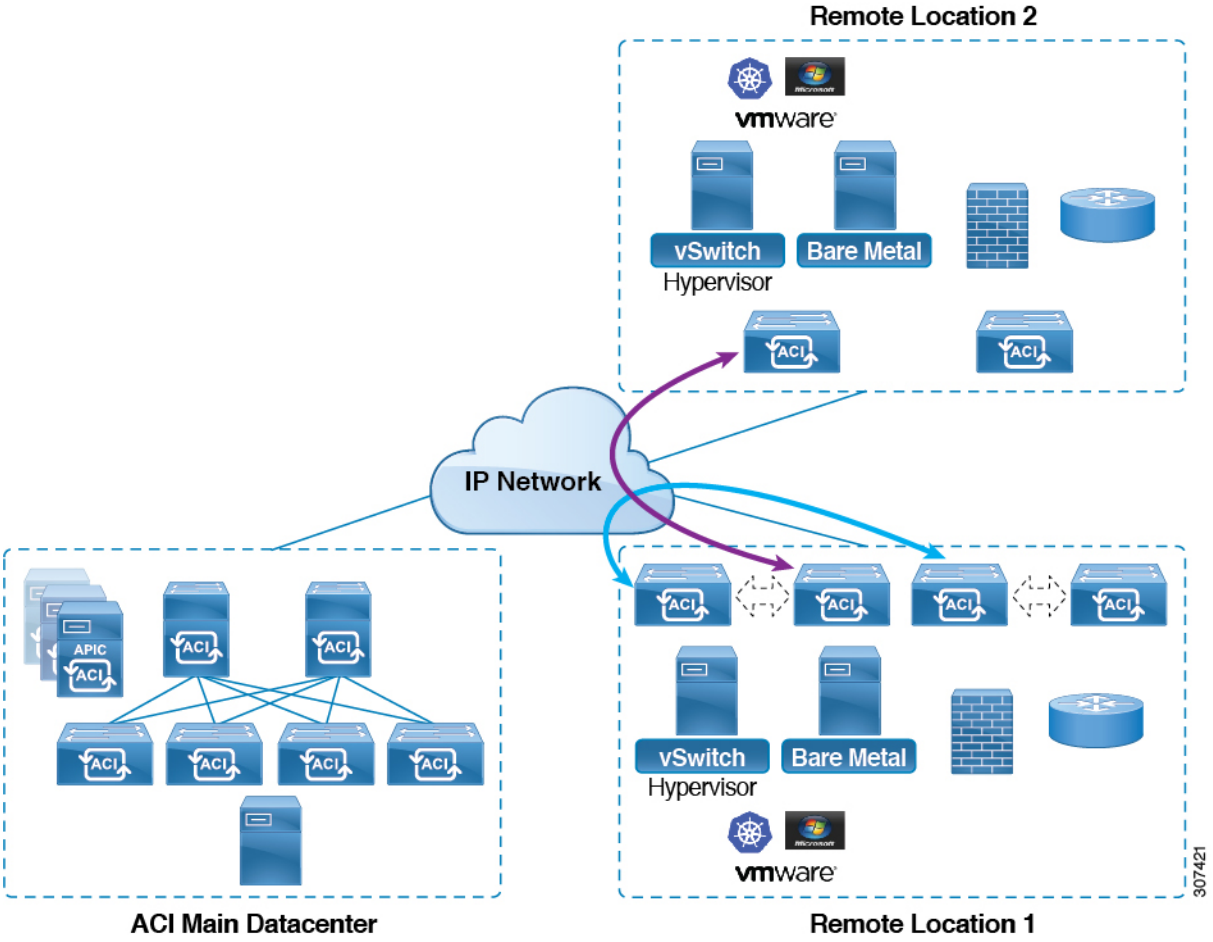
さらに、リリース4.1(2)よりも前では、次の図に示すように、リモートロケーション内またはリモート ロケーション間のリモート リーフ スイッチ vPC ペア間のトラフィックは、ACI メイン データ センター ポッドのスパイン スイッチに転送されます。

図 *79 : Remote Switching Traffic* : リリース *4.1(2)* より以前



リリース 4.1(2) 以降では、異なるリモート ロケーションにあるリモート リーフ スイッチ間の直接トラフィック転送がサポートされるようになりました。この機能は、次の図に示すように、リモート ロケーション間の接続に一定レベルの冗長性と可用性を提供します。

図 *80 : Remote Leaf Switch Behavior* : リリース *4.1(2)*



また、リリース 4.1(2) 以降でも、リモート リーフ スイッチの動作には次の特徴があります。

- リリース 4.1(2) 以降、ダイレクト トラフィック転送では、シングル ポッド設定内でスパイン スイッチに障害が発生すると、次のようになります。
  - ローカル スイッチングは、上記の「ローカル スイッチング トラフィック：リリース 4.1(2) 以前」に示すように、リモート リーフ スイッチ vPC ピア間の既存および新規のエンドポイント トラフィックに対して機能し続けます。
  - リモート ロケーション間のリモート リーフ スイッチ間のトラフィックの場合：
    - リモート リーフ スイッチからスパイン スイッチへのトンネルがダウンするため、新しいエンドポイント トラフィックは失敗します。リモート リーフ スイッチから、新しいエンドポイントの詳細はスパイン スイッチに同期されないため、同じまたは異なる場所にある他のリモート リーフ スイッチ ペアは、COOP から新しいエンドポイント情報をダウンロードできません。
    - 単方向トラフィックの場合、既存のリモートエンドポイントは300秒後にエージングアウトするため、そのポイント以降のトラフィックは失敗します。ポッド内

のリモート リーフ サイト内（リモート リーフ VPC ペア間）の双方向トラフィックは更新され、引き続き機能します。リモート ロケーション（リモート リーフ スイッチ）への双方向トラフィックは、900 秒のタイムアウト後に COOP によってリモートエンドポイントが期限切れになるため、影響を受けることに注意してください。

- 共有サービス（VRF 間）の場合、同じポッド内の 2 つの異なるリモート ロケーションに接続されたリモート リーフ スイッチに属するエンドポイント間の双方向トラフィックは、リモート リーフ スイッチ COOP エンドポイントのエージアウト時間（900秒）後に失敗します。これは、リモートリーフスイッチからスパインへの COOP セッションがこの状況でダウンするためです。ただし、2 つの異なるポッドに接続されたリモート リーフ スイッチに属するエンドポイント間の共有サービス トラフィックは、COOP 高速エージング タイムである 30 秒後に失敗します。
- スパイン スイッチへの BGP セッションがダウンするため、L3Out 間通信は続行できません。

- トラフィックが 1 つのリモート リーフ スイッチから送信され、別のリモート リーフ スイッチ（送信元の vPC ピアではない）に送信されるリモート リーフ直接単方向トラフィックがある場合は、300 秒のリモート エンド ポイント（XR EP）タイムアウトが発生するたびに、ミリ秒単位のトラフィック損失が発生します。
- ACI Multi-Site 設定を使用したリモート リーフ スイッチでは、スパイン スイッチに障害が発生しても、リモート リーフ スイッチから他のポッドおよびリモート ロケーションへのすべてのトラフィックが継続します。これは、この状況ではトラフィックが代替の使用可能なポッドを通過するためです。

リモート リーフ スイッチの IPN での 10 Mbps 帯域幅のサポート

リモート リーフ スイッチからのデータ トラフィックのほとんどがローカルで、ポッド間ネットワーク（IPN）が管理目的でのみ必要な場合があります。このような状況では、100 Mbps の IPN は必要ない場合があります。これらの環境をサポートするために、リリース 4.2(4) 以降、IPN の最小帯域幅として 10 Mbps のサポートが利用可能になりました。

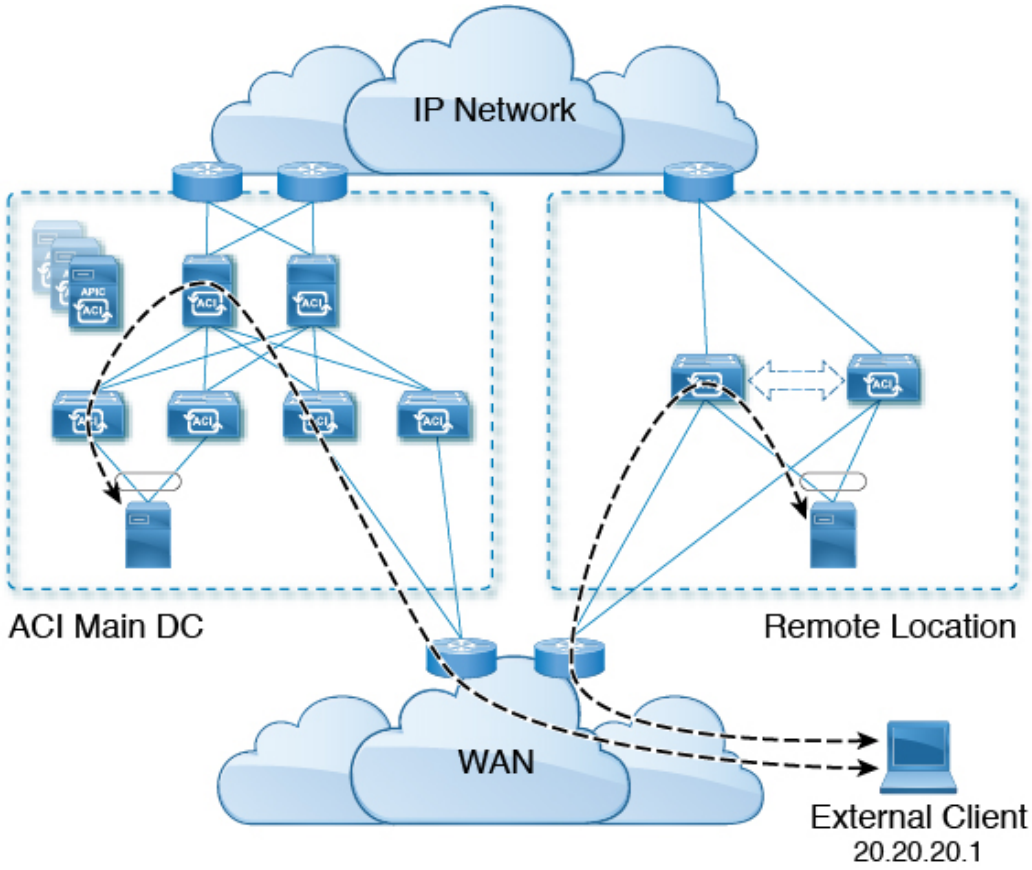
これをサポートするには、次の要件を満たす必要があります。

- IPN パスは、リモート リーフ スイッチ（アップグレードおよびダウングレード、ディスカバリ、COOP、ポリシー プッシュなどの管理機能）の管理にのみ使用されます。
- 「Cisco APIC GUI を使用した DSCP 変換ポリシーの作成」の項に記載されている情報に基づいて、Cisco ACI データセンターとリモート リーフ スイッチ ペア間のコントロールおよび管理プレーン トラフィックに優先順位を付けるために、QoS 設定を使用して IPN を設定します。
- データセンターおよびリモート リーフ スイッチからのすべてのトラフィックは、ローカル L3Out を経由します。Cisco ACI

- EPG またはブリッジ ドメインは、リモート リーフ スイッチと ACI メイン データセンター間で拡張されません。
- アップグレード時間を短縮するには、リモート リーフ スイッチにソフトウェア イメージを事前にダウンロードする必要があります。

次の図に、この機能のグラフィカル表示を示します。

図 *81 :* リモート リーフ スイッチ動作（リリース *4.2(4)*）：*IPN* でのリモート リーフ スイッチの管理

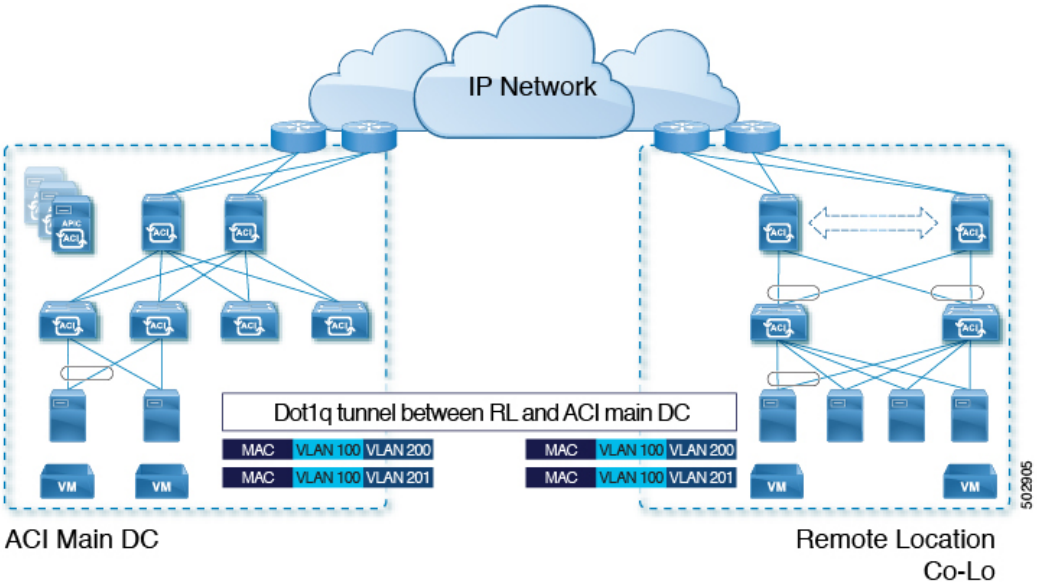


リモート リーフ スイッチでの Dot1q トンネルのサポート

状況によっては、コロケーションプロバイダーが複数のカスタマーをホストしており、各カスタマーがリモート リーフ スイッチ ペアごとに数千の VLAN を使用している場合があります。リリース 4.2(4) 以降では、リモート リーフ スイッチと ACI メイン データセンター間に 802.1Q トンネルを作成するためのサポートを利用できます。これにより、複数の VLAN を単一の 802.1Q トンネルに柔軟にマッピングできるため、EPG の拡張要件が軽減されます。

次の図に、この機能のグラフィカル表示を示します。

図 *82* : リモート リーフ スイッチの動作、リリース *4.2*（*4*）：リモート リーフ スイッチでの *802.1Q* トンネル サポート



Cisco APIC ドキュメンテーションのランディング ページにある『Cisco APIC Layer 2 Networking Configuration Guide』の「802.1Q Tunnels」の章に記載されている手順を使用して、リモート リーフ スイッチと ACI メイン データセンター間にこの 802.1Q トンネルを作成します。
https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

ウィザードを使用するか（使用しない場合も）、REST API または NX-OS スタイル CLI を使用して、APIC GUI のリモート リーフ スイッチを設定できます。

リモート リーフ スイッチの制約事項と制限事項

リモート リーフには、次の注意事項および制約事項が適用されます。

- リモート リーフ ソリューションでは、リモート リーフ スイッチとメイン データ センターのリーフ/スパイン スイッチの /32 トンネル エンド ポイント（TEP）IP アドレスが、要約なしでメイン データ センターとリモート リーフ スイッチ間でアドバタイズされる必要があります。
- リモート リーフ スイッチを同じポッド内の別のサイトに移動し、新しいサイトに元のサイトと同じノード ID がある場合は、仮想ポート チャネル（vPC）を削除して再作成する必要があります。
- Cisco N9K-C9348GC-FXP スイッチでは、ポート 1/53 または 1/54 でのみ最初のリモート リーフスイッチディスカバリを実行できます。その後、リモートリーフスイッチの ISN/IPN へのファブリック アップリンクに他のポートを使用できます。
- 6.0(3) リリース以降、ダイナミック パケットの優先順位付けが有効になっており、CoS 保持ポリシーまたは Cisco ACI マルチポッド ポリシーのいずれかが有効になっている場合、予想される動作は、マウス フロー（低帯域幅フロー）が、 VLAN CoS 優先順位 0 でファ

ブリックから出力されるというものです。このことは、ダイナミック パケットの優先順位付けとともに、CoS 保持機能も有効にするか、Cisco ACI マルチポッド DSCP 変換機能 も有効にしている場合に成り立ちます。ただし、実際の動作は次のとおりです。

- 物理リーフおよびリモート リーフ スイッチでダイナミック パケットの優先順位付け機能を使用して CoS 保持を有効にした場合、マウス フローは VLAN CoS 優先順位 0 でファブリックを出ます。
- 物理リーフ スイッチでダイナミック パケットの優先順位付け機能を使用して Cisco ACI マルチポッド DSCP 変換を有効にした場合、マウス フローは VLAN CoS 優先順位 0 でファブリックを出ます。
- リモート リーフ スイッチでダイナミック パケットの優先順位付け機能を使用して Cisco ACI マルチポッド DSCP 変換を有効にした場合、マウス フローは VLAN CoS 優先順位 3 でファブリックを出ます。

Cisco ACI マルチポッド DSCP 変換を有効にしていても、マウス フローがリモート リーフ スイッチを出るときに、マウス フローの VLAN CoS プライオリティが 3 にならないようにするには、代わりに CoS 保存機能を使用します。

ここでは、リモート リーフ スイッチでサポートされるものとサポートされないものについて説明します。

- Supported Features （218 ページ）
- サポートされない機能 （219 ページ）
- リリース 5.0(1) の変更点 （221 ページ）
- リリース 5.2(3) での変更点 （221 ページ）

Supported Features

Cisco APIC リリース 6.1(1) 以降、ファブリック ポート（アップリンク）は、ルーテッド サブインターフェイスとして、ユーザーテナント L3Out と SR-MPLS インフラ L3Out を伴うように構成できるようになりました。

- リモートリーフファブリックポートでは、ルーテッドサブインターフェイスを伴う L3Out のみが許可されます。
- リモートリーフファブリックポートは、ユーザーテナントの L3Out または SR- MPLS インフラ L3Out としてのみ展開できます。
- アプリケーション EPG にリモートリーフファブリックポートを展開することはできません。ルーテッドサブインターフェイスを伴う L3Out のみが許可されます。
- ハイブリッドポートでは、PTP/同期アクセスポリシーのみがサポートされます。他のアクセスポリシーはサポートされません。
- ハイブリッドポートではファブリック SPAN のみがサポートされます。

- NetFlow は、ユーザーテナント L3Out で構成されたファブリックポートではサポートされません。

Cisco APIC リリース 6.0(4) 以降では、vPC リモート リーフ スイッチ ペア間での L3Out SVI のストレッチがサポートされています。

Cisco APIC リリース 4.2(4) 以降、802.1Q（Dot1q）トンネル機能がサポートされています。

Cisco APIC リリース 4.1(2) 以降、次の機能がサポートされています。

- ACI Multi-Site を使用したリモート リーフ スイッチ
- 同じリモート データ センター内の 2 つのリモート リーフ vPC ペア間またはデータ センター間でのトラフィック転送（これらのリモート リーフ ペアが同じポッドまたは同じマルチポッド ファブリックの一部であるポッドに関連付けられている場合）
- 主要な Cisco ACI データ センター ポッドが 2 つのリモート ロケーションの間の中継である場合、リモート ロケーションでの L3Out の中継（RL `location-1`の L3Out と RL`location-2` の L3Out がそれぞれのプレフィックスをアドバタイズしている）

Cisco APIC リリース 4.0(1) 以降、次の機能がサポートされています。

- Epg の Q-で-Q カプセル化のマッピング
- リモート リーフ スイッチでの PBR トラッキング（システムレベルのグローバル GIPo が有効になっている場合）
- PBR の復元力のあるハッシュ
- Netflow
- MacSec の暗号化
- ウィザードのトラブルシューティング
- アトミック カウンタ

サポートされない機能

このリリースで、サポート対象外の次の機能を除き、ファブリックおよびテナントの完全なポリシーがリモート リーフ スイッチでサポートされています。

- GOLF
- vPod
- フローティング L3Out
- ローカル リーフ スイッチ（ACI 主要データ センター スイッチ）とリモート リーフ スイッチ間の L3out SVI のストレッチ、または 2 つの異なるリモート リーフ スイッチの vPC ペア間のストレッチ
- コピー サービスは、ローカル リーフ スイッチに導入されている場合、および送信元または宛先がリモート リーフ スイッチにある場合はサポートされません。この状況では、ルー

ティング可能な TEP IP アドレスはローカル リーフ スイッチに割り当てられません。詳細については、『APIC ドキュメンテーション ページ』で入手可能な『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Configuring Copy Services」の章の「Copy Services Limitations」を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

- レイヤ 2 (スタティック Epg) を除く接続外部
- VzAny 契約とサービスをコピーします。
- リモートのリーフ スイッチの FCoE 接続
- ブリッジ ドメインまたは Epg のカプセル化をフラッディングします。
- Fast Link Failover ポリシーは、リーフ スイッチとスパイン スイッチ間の ACI ファブリック リンク用であり、リモート リーフ接続には適用されません。リモート リーフ接続のコンバージェンスを高速化するために、Cisco APICリリース 5.2(1) で代替方法が導入されています。
- 遠隔地での管理対象のサービス グラフに接続されたデバイス
- トラフィック ストーム制御
- Cloud Sec 暗号化
- ファーストホップ セキュリティ
- レイヤ 3 マルチキャスト リモート リーフ スイッチ上のルーティング
- メンテナンス モード
- TEP 間アトミック カウンタ

Multi-Site アーキテクチャでリモート リーフ スイッチをサイト間 L3Out 機能と統合する場合、次のシナリオはサポートされません。

- 別々のサイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out 間のトランジット ルーティング
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するローカル サイトに接続されたエンドポイント
- リモート サイトに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント

（注） 異なるデータ センター サイトが同じマルチポッド ファブリックの一部としてポッドとして展開されている場合、上記の制限は適用されません。

リモート リーフ スイッチ機能では、次の導入と設定がサポートされていません。

- 特定のサイト（APIC ドメイン）に関連付けられたリモート リーフ ノードとマルチサイト展開の別のサイトのリーフ ノード部分の間でブリッジドメインを拡張することはサポートされていません（これらのリーフ ノードがローカルまたはリモート）、この制限を強調表示するために障害が APIC に生成されます。これは、Multi-Site Orchestrator（MSO）でストレッチ ブリッジドメインを構成するときに、BUM フラッディングが有効または無効であることとは無関係です。ただし、ブリッジドメインは、同じサイト（APIC ドメイン）に属するリモート リーフ ノードとローカル リーフ ノード間で常に拡張できます（BUM フラッディングを有効または無効にします）。
- リモート リーフスイッチ ロケーションおよび主要データセンター全体でのスパニング ツリープロトコル
- APIC は、リモート リーフスイッチに直接接続されます。
- vPC ドメインでの、リモート リーフスイッチ上の孤立ポート チャネルまたは物理ポート（この制限は、リリース 3.1 以降に適用します）。
- コンシューマ、プロバイダー、およびサービス ノードがすべてリモート リーフスイッチに接続されていて、vPC モードである場合、サービス ノード統合の有無に関わらず、リモート ロケーション内でのローカル トラフィック転送のみサポートされます。
- スパイン スイッチから IPN にアドバタイズされる /32 ループバックは、リモート リーフスイッチに向けて抑制/集約してはなりません。/32 ループバックは、リモート リーフスイッチにアドバタイズする必要があります。

リリース 5.0(1) の変更点

Cisco APIC リリース 5.0(1) 以降では、リモート リーフスイッチに次の変更が適用されています。

- 直接トラフィック転送機能はデフォルトでイネーブルになっており、ディセーブルにできません。
- リモート リーフ スイッチの直接トラフィック転送を使用しない設定はサポートされなくなりました。リモート リーフ スイッチがあり、Cisco リリース 5.0(1) にアップグレードする場合は、「Direct Traffic Forwardingについて」の項に記載されている情報を確認し、その項の手順を使用して直接トラフィック転送をイネーブルにします。APIC

リリース 5.2(3) での変更点

Cisco APIC リリース 5.2(3) 以降では、リモート リーフスイッチに次の変更が適用されています。

- リモート リーフ スイッチとアップストリーム ルータ間のピアへの IPN アンダーレイ プロトコルは、OSPF または BGP のいずれかです。以前のリリースでは、OSPF アンダーレイのみがサポートされています。

QoS

L3Out QoS

L3Out QoS は、外部 EPG レベルで適用されるコントラクトを使用して設定できます。リリース 4.0(1) 以降、L3Out QoS は L3Out インターフェイスで直接設定することもできます。

（注） Cisco APICリリース 4.0(1) 以降を実行している場合は、L3Out に直接適用されるカスタム QoS ポリシーを使用して L3Out の QoS を設定することを推奨します。

パケットは入力 DSCP または CoS 値を使用して分類されるため、カスタム QoS ポリシーを使用して着信トラフィックを Cisco ACIQoS キューに分類できます。カスタム QoS ポリシーには、DSCP/CoS 値をユーザ キューまたは新しい DSCP/CoS 値（マーキングの場合）にマッピングするテーブルが含まれます。特定の DSCP/CoS 値のマッピングがない場合、ユーザ キューは入力 L3Out インターフェイスの QoS 優先度設定によって選択されます（設定されている場合）。

入力および出力トラフィックのサービスクラス（CoS）プレゼンテーション

トラフィックが Cisco ACI ファブリックに入ると、各パケットの優先順位が Cisco ACI QoS レベルにマッピングされます。これらの QoS レベルは、パケットの外部ヘッダーの CoS フィールドと DEI ビットに格納され、元のヘッダーは破棄されます。

入力パケットの元の CoS 値を保持し、パケットがファブリックを離れるときにそれを復元する場合は、このセクションで説明するように、グローバル ファブリック QoS ポリシーを使用して 802.1p サービス クラス（CoS）の保持を有効にすることができます。

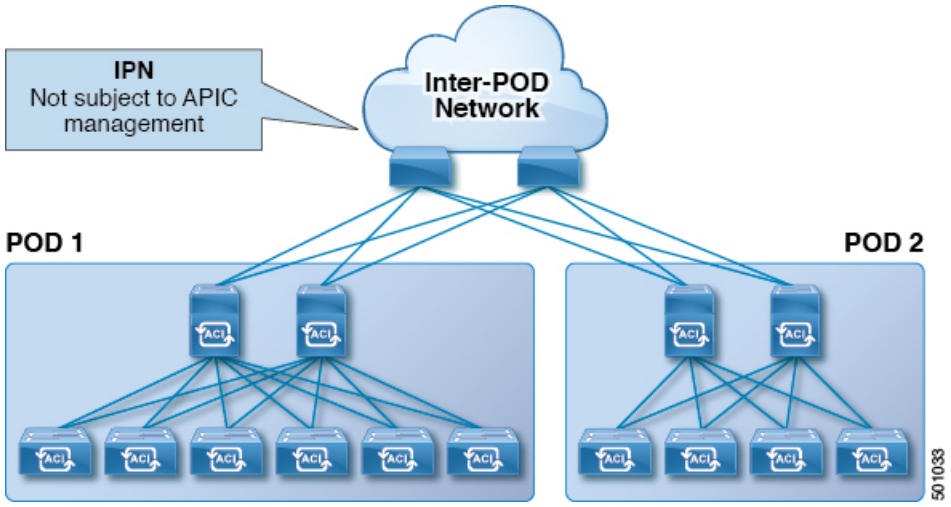
CoS の保持は単一のポッドおよび multipod トポロジでサポートされます。しかしマルチポッド トポロジでは、ユーザが IPN の設定をポッド間で保持することに懸念がない場合にのみ、CoS の保持を使用できます。パケットが IPN を通過するときにパケットの CoS 値を保持するには、マルチポッド QoS および DSCP 変換ポリシー （209 ページ） で説明されているように DSCP 変換ポリシーを使用します。

マルチポッド QoS および DSCP 変換ポリシー

Cisco ACI ファブリック内でトラフィックが送受信される場合、QoS レベルは VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定されます。Cisco APIC の管理下にないデバイスが通過するパケットの CoS 値を変更する可能性があるマルチポッド トポロジでは、Cisco ACI とパケット内の DSCP 値の間のマッピングを作成することにより、QoS レベルの設定を保持できます。

ポッド間の IPN トラフィックで QoS 設定を保持することは検討しないが、ファブリックに入出力するパケットの元の CoS 値を保持したい場合は、入力および出力トラフィックのサービスクラス（CoS）プレゼンテーション （222 ページ） を参照してください。

図 *83*: マルチポッド トポロジ



この図に示すように、マルチポッド トポロジ内のポッド間のトラフィックは IPN を通過します。IPN には、Cisco APIC の管理下にないデバイスが含まれる場合があります。ネットワークパケットが POD1 のスパインまたはリーフスイッチから送信されると、IPN のデバイスはパケットの 802.1p 値を変更する場合があります。この場合、フレームが POD2 のスパインまたはリーフスイッチに到達すると、POD1 のソースで割り当てられた Cisco ACI QoS レベル値ではなく、IPN デバイスによって割り当てられた 802.1p 値が設定されます。

パケットの適切な QoS レベルを維持し、優先順位の高いパケットが遅延またはドロップされないようにするために、IPN によって接続された複数の POD 間を移動するトラフィックに DSCP 変換ポリシーを使用できます。DSCP 変換ポリシーが有効になっている場合、Cisco APIC は指定したマッピング ルールに従って、QoS レベル値（VXLAN パケットの CoS 値で表される）を DSCP 値に変換します。POD1 から送信されたパケットが POD2 に到達すると、マッピングされた DSCP 値が適切な QoS レベルの元の CoS 値に変換されます。

QoS マーキングの入力から出力への変換

Cisco APIC は入力トラフィックの DSCP および CoS 値を、Cisco ACI ファブリック内で使用される QoS レベルに変換できるようにします。変換は、DSCP 値が IP パケットに存在し、CoS 値がイーサネット フレームに存在する場合にのみサポートされます。

たとえば、この機能により、Cisco ACI ファブリックは、IP ヘッダーを持たないレイヤ 2 パケットなど、CoS 値のみに基づいてトラフィックを分類するデバイスのトラフィックを分類できます。

CoS 変換のガイドラインと制約事項

入力および出力トラフィックのサービスクラス（CoS）プレゼンテーション （222 ページ） で説明されているように、グローバル ファブリック CoS 保存ポリシーを有効にする必要があります。

CoS 変換は、外部 L3 インターフェイスではサポートされていません。

CoS 変換は、出力フレームが 802.1Q カプセル化されている場合にのみサポートされます。

次の構成オプションが有効になっている場合、CoS 変換はサポートされません。

- QoS を含むコントラクトが構成されています。
- 発信インターフェイスは FEX 上にあります。
- DSCP ポリシーを使用したマルチポッド QoS が有効になっています。
- ダイナミックパケット優位性が有効化されています。
- EPG 内エンドポイント分離を適用して EPG を構成した場合。
- マイクロセグメンテーションを有効にして EPG が構成されている場合。

HSRP

HSRP について

HSRP はファーストホップ冗長プロトコル（FHRP）であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルト ルータの IP アドレスを指定して設定された、イーサネット ネットワーク上の IP ホストにファーストホップ ルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイ ルータを選択します。ルータ グループでは、アクティブ ルータはパケットをルーティングするルータであり、スタンバイ ルータはアクティブ ルータに障害が発生したときや、プリセット条件に達したときに使用されるルータです。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオー

バーヘッド、セキュリティ上の問題など、さまざまな理由で現実的ではありません。HSRPは、そうしたホストにフェールオーバー サービスを提供します。

HSRP を使用するとき、ホストのデフォルト ルータとして HSRP 仮想 IP アドレスを設定します（実際のルータ IP アドレスの代わりに）。仮想 IP アドレスは、HSRP が動作するルータのグループで共有される IPv4 または IPv6 アドレスです。

ネットワーク セグメントに HSRP を設定する場合は、HSRP グループ用の仮想 MAC アドレスと仮想 IP アドレスを設定します。グループの各 HSRP 対応インターフェイス上で、同じ仮想アドレスを指定します。各インターフェイス上で、実アドレスとして機能する固有の IP アドレスおよび MAC アドレスも設定します。HSRP はこれらのインターフェイスのうちの 1 つをアクティブ ルータにするために選択します。アクティブ ルータは、グループの仮想 MAC アドレス宛てのパケットを受信してルーティングします。

指定されたアクティブ ルータで障害が発生すると、HSRP によって検出されます。その時点で、選択されたスタンバイ ルータが HSRP グループの MAC アドレスおよび IP アドレスの制御を行うことになります。HSRPはこの時点で、新しいスタンバイ ルータの選択も行います。

HSRP ではプライオリティ指示子を使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべてのHSRP設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは100なので、それよりもプライオリティが高いインターフェイスを1つ設定すると、そのインターフェイスがデフォルトのアクティブルータになります。

HSRPが動作するインターフェイスは、マルチキャストユーザデータグラムプロトコル（UDP）ベースの hello メッセージを送受信して、障害を検出し、アクティブおよびスタンバイ ルータを指定します。アクティブ ルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ ルータがアクティブルータになります。アクティブ ルータとスタンバイ ルータ間のパケット フォワーディング機能の移動は、ネットワーク上のすべてのホストに対して完全に透過的です。

1 つのインターフェイス上で複数の HSRP グループを設定できます。仮想ルータは物理的には存在しませんが、相互にバックアップするように設定されたインターフェイスにとって、共通のデフォルト ルータになります。アクティブ ルータの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。代わりに、仮想ルータの IP アドレス（仮想 IP アドレス）をホストのデフォルト ルータとして設定します。アクティブ ルータが設定時間内に hello メッセージを送信できなかった場合は、スタンバイ ルータが引き継いで仮想アドレスに応答し、アクティブ ルータになってアクティブ ルータの役割を引き受けます。ホストの観点からは、仮想ルータは同じままです。

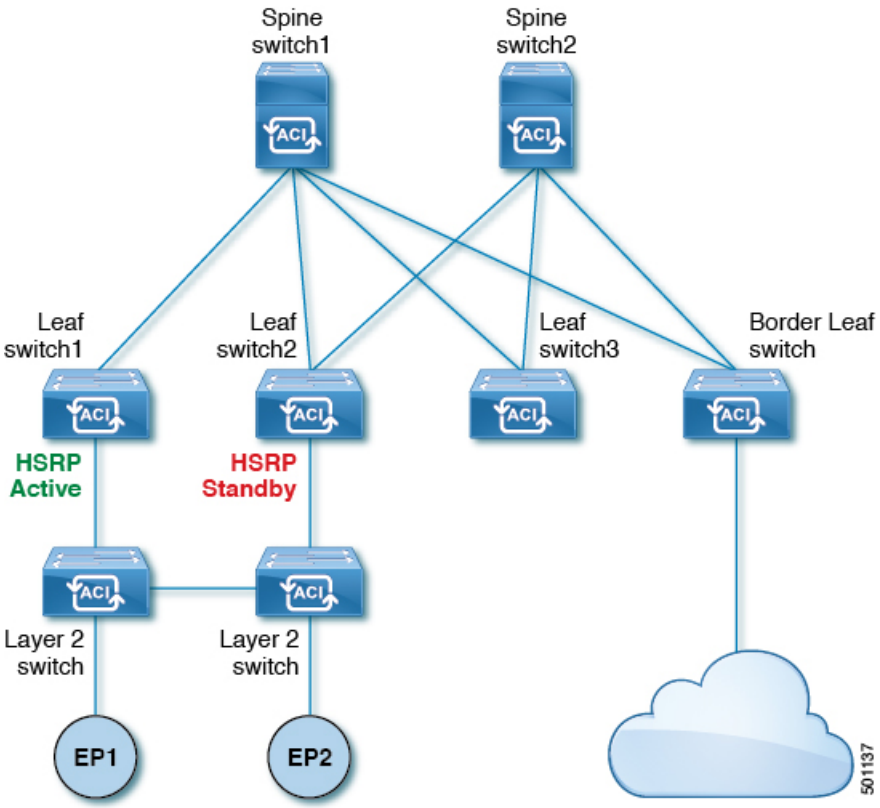
（注） ルーテッド ポートで受信した HSRP 仮想 IP アドレス宛のパケットは、ローカル ルータ上で終端します。そのルータがアクティブ HSRP ルータであるのかスタンバイ HSRP ルータであるのかは関係ありません。このプロセスには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2（VLAN）インターフェイスで受信した HSRP 仮想 IP アドレス宛のパケットは、アクティブ ルータ上で終端します。

Cisco APIC と HSRP について

Cisco ACI の HSRP は、ルーテッドインターフェイスまたはサブインターフェイスでのみサポートされます。したがって HSRP は、レイヤ 3 Out でのみ設定できます。レイヤ 2 接続は、HSRP を実行している ACI リーフ スイッチ間のレイヤ 2 スイッチなどの外部デバイスから提供される必要があります。HSRP は外部レイヤ 2 接続上で Hello メッセージを交換するリーフ スイッチ上で動作するからです。HSRP の hello メッセージは、スパイン スイッチではパス スルーされません。

次に示すのは、Cisco APIC での HSRP の導入のトポロジの例です。

図 *84 : HSRP* の配置トポロジ



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。

- HSRP 状態は、HSRP IPv4 および IPv6 の両方で同じである必要があります。フェールオーバー後に同じ状態になるようにするには、プライオリティとプリエンプションを設定する必要があります。
- 現在、1 個の IPv4 と 1 個の IPv6 グループのみが Cisco ACI の同じサブインターフェイスでサポートされています。デュアル スタックが設定されている場合でも、仮想 MAC は IPv4 および IPv6 HSRP の設定で同じである必要があります。

- HSRP ピアに接続しているネットワークが純粋なレイヤ 2 ネットワークである場合、BFD IPv4 および IPv6 がサポートされています。リーフ スイッチでは、別のルータの MAC アドレスを設定する必要があります。BFD セッションは、リーフ インターフェイスで異なる MAC アドレスを設定する場合にのみアクティブになります。
- ユーザーは、デュアル スタック設定の IPv4 および IPv6 HSRP グループに同じ MAC アドレスを設定する必要があります。
- HSRP VIP はインターフェイス IP と同じサブネット内にある必要があります。
- HSRP 設定のインターフェイス遅延を設定することをお勧めします。
- HSRPは、ルーテッドインターフェイスまたはサブインターフェイスでのみサポートされます。HSRPは、VLANインターフェイスおよびスイッチ済み仮想インターフェイス（SVI）ではサポートされていません。したがって、HSRP の VPC サポートは使用できません。
- HSRP のオブジェクト トラッキングはサポートされていません。
- SNMP の HSRP 管理情報ベース（MIB）はサポートされません。
- HSRP では、複数グループの最適化（MGO） はサポートされていません。
- ICMP IPv4 および IPv6 のリダイレクトはサポートされていません。
- Cold Standby および Non-Stop Forwarding（NSF）は、Cisco ACI 環境で再起動できないためサポートされていません。
- HSRPはリーフ スイッチでのみサポートされているため、拡張ホールドダウン タイマーのサポートはありません。HSRP はスパイン スイッチでサポートされていません。
- APIC 内では、HSRP のバージョン変更はサポートされていません。設定を削除し、新しいバージョンを再設定する必要があります。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一ルータの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。
- ルート セグメンテーションは、HSRP がインターフェイスでアクティブな場合、Cisco Nexus 93128TX、Cisco Nexus 9396PX、および Cisco Nexus 9396TX リーフ スイッチでプログラムされています。したがって、インターフェイスでルート パケットに実施する DMAC=router MAC チェックはありません。この制限は、Cisco Nexus 93180LC EX、Cisco Nexus 93180YC-EX、Cisco Nexus 93108TC EX リーフ スイッチには適用されません。
- HSRP 設定は、基本的な GUI モードではサポートされていません。APIC リリース 3.0 (1) 以降、基本的な GUI モードが廃止されました。
- ファブリックからレイヤ 3 アウト トラフィックは、状態に関係なく HSRP リーフ スイッチ全体で常にロード バランスします。HSRP リーフ スイッチが複数のポッドにわたる場合、ファブリックからアウト トラフィックは同じポッドで常にリーフ スイッチを使用します。

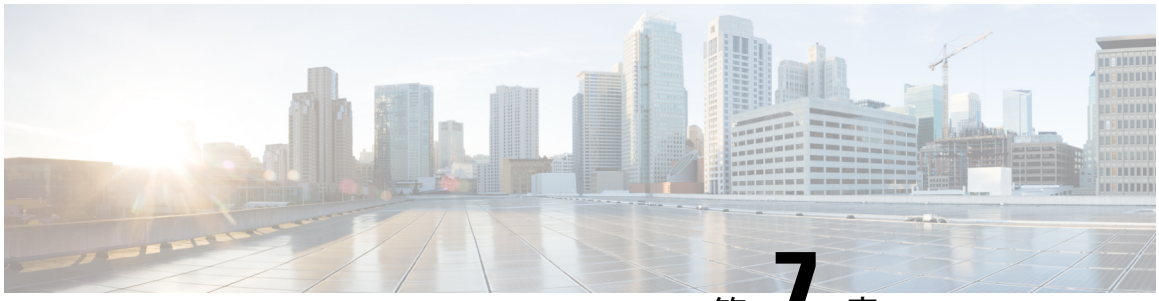
- この制限は、以前の Cisco Nexus 93128TX、Cisco Nexus 9396PX と Cisco Nexus 9396TX スイッチの一部に適用されます。HSRP を使用すると、レイヤ 2 の外部デバイスのフラッピングを防ぐため、ルーテッド インターフェイスまたはルーテッド サブインターフェイスの MAC アドレスを 1 個変更する必要があります。これは、インターフェイス論理プロファイルの下で論理インターフェイスごとに Cisco APIC が同じ MAC アドレス（00:22:BD:F8:19:FF）を割り当てるためです。

HSRP のバージョン

Cisco APICは、デフォルトで HSRP バージョン 1 をサポートします。HSRP バージョン 2 を使用するようにインターフェイスを設定できます。

HSRP バージョン 2 では、HSRP バージョン 1 から次のように拡張されています。

- グループ番号の範囲が拡大されました。HSRP バージョン 1 がサポートするグループ番号は 0 ～ 255 です。HSRP バージョン 2 がサポートするグループ番号は 0 ～ 4095 です。
- IPv4 では、HSRP バージョン 1 で使用する IP マルチキャスト アドレス 224.0.0.2 の代わりに、IPv4 マルチキャスト アドレス 224.0.0.102 または IPv6 マルチキャスト アドレス FF02::66 を使用して hello パケットを送信します。
- IPv4 では 0000.0C9F.F000 ～ 0000.0C9F.FFFF、IPv6 アドレスでは 0005.73A0.0000 ～ 0005.73A0.0FFF の MAC アドレス範囲を使用します。HSRP バージョン 1 で使用する MAC アドレス範囲は、0000.0C07.AC00 ～ 0000.0C07.ACFF です。



第 7 章

ACI トランジット ルーティング、ルート ピアリング、および EIGRP サポート

この章は、次の内容で構成されています。

- ACI 中継ルーティング （229 ページ）
- トランジット ルーティングの使用例 （230 ページ）
- ACI ファブリック ルート ピアリング （234 ページ）
- トランジット ルート制御 （241 ページ）
- デフォルト ポリシー動作 （243 ページ）
- EIGRP プロトコルのサポート （244 ページ）

ACI 中継ルーティング

ACI ファブリックは、中継ルーティングをサポートしています。これにより、境界ルータが他のルーティングドメインとの双方向再配布を実行できます。トランジット再配布をブロックする以前の ACI リリースのスタブ ルーティング ドメインとは異なり、双方向再配布では、あるルーティング ドメインから別のルーティング ドメインにルーティング情報が渡されます。このような再配布により、ACI ファブリックは異なるルーティング ドメイン間で完全な IP 接続を提供できます。これにより、ルーティング ドメイン間のバックアップ パスを有効にして、冗長接続を提供することもできます。

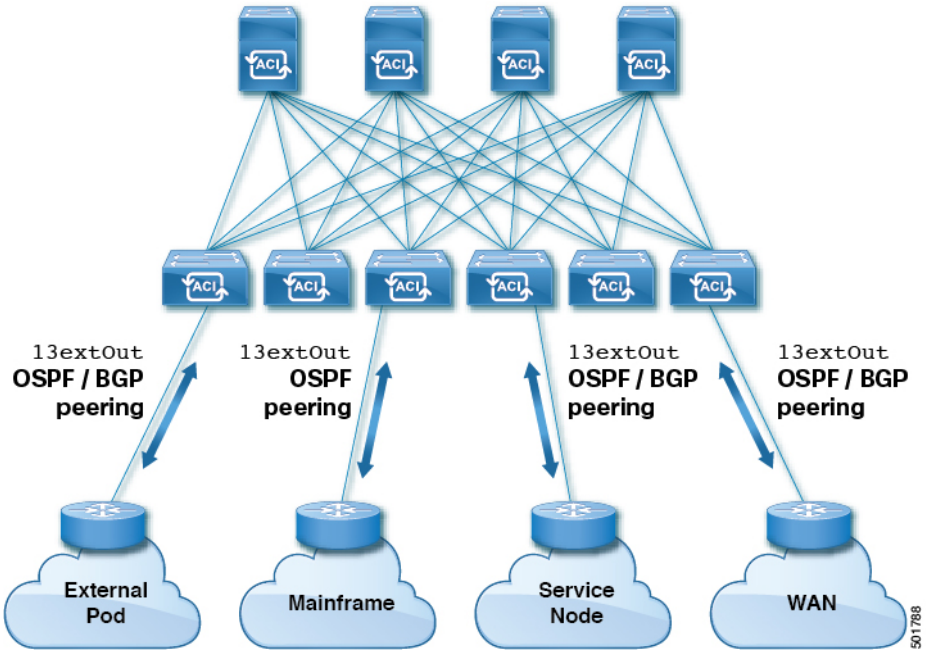
最適でないルーティングや、ルーティング ループのより深刻な問題を回避する中継再配布ポリシーを設計します。通常、トランジット再配布は元のトポロジとリンクステート情報を保持せず、距離ベクトル形式で外部ルートを再配布します（ルートは、リンクステートプロトコルを使用する場合でも、ベクトルプレフィックスおよび関連付けられた距離としてアドバタイズされます）。このような状況では、ルータが意図せずにルーティング ループを形成し、パケットを接続先に配信できないことがあります。

トランジット ルーティングの使用例

レイヤ 3 ドメイン間のトランジット ルーティング

外部ポッド、メインフレーム、サービス ノード、WAN ルータなどの複数のレイヤ 3 ドメインが ACI ファブリックとピアリングして、それらの間のトランジット機能を提供することができます。

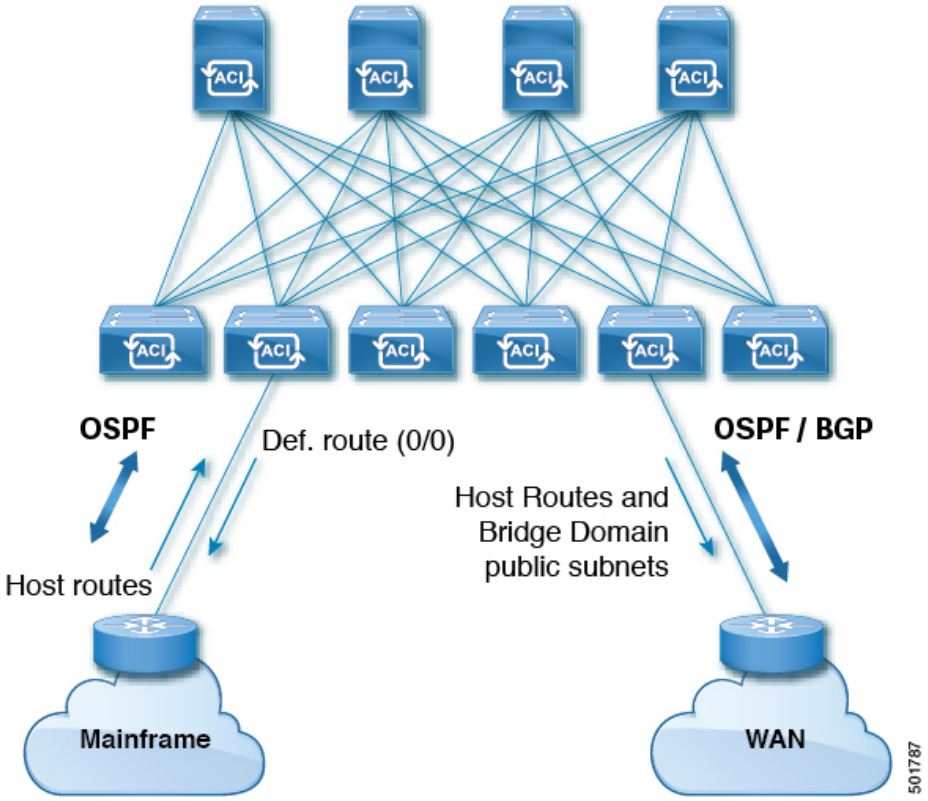
図 *85 :* レイヤ *3* ドメイン間のトランジット ルーティング



ACI ファブリックで中継されるメインフレーム トラフィック

メインフレームは、論理パーティション（LPAR）および仮想 IP アドレッシング（VIPA）の要件に対応する標準 IP ルーティング プロトコルを実行する IP サーバとして機能します。

図 *86 :* メインフレームのトランジット接続

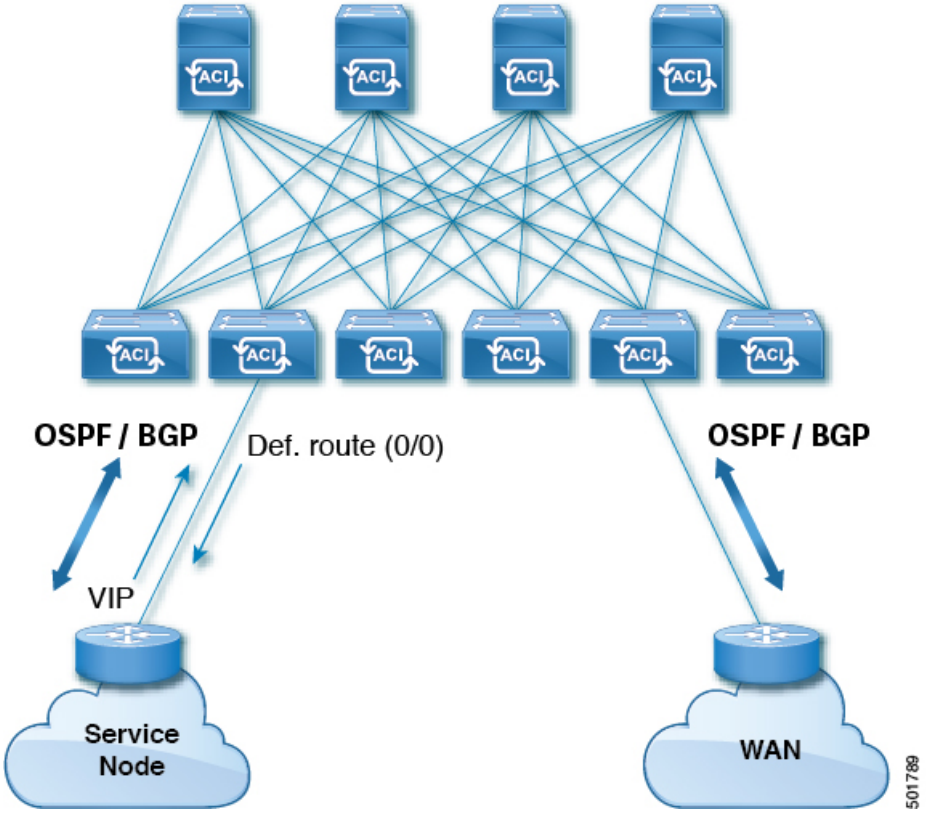


このトポロジにおいて、メインフレームは、ACI ファブリックが WAN ルータを経由して外部と接続するため、およびファブリック内の East-West トラフィックのための中継ドメインとなることを必要とします。これらは、ホストルートをファブリックにプッシュして、ファブリック内、および外部インターフェイスに再配布されるようにします。

サービス ノードのトランジット接続

サービス ノードは ACI ファブリックとピアリングし、外部 WAN インターフェイスに再配布される仮想 IP (VIP) ルートをアドバタイズすることができます。

図 *87:* サービス ノードのトランジット接続

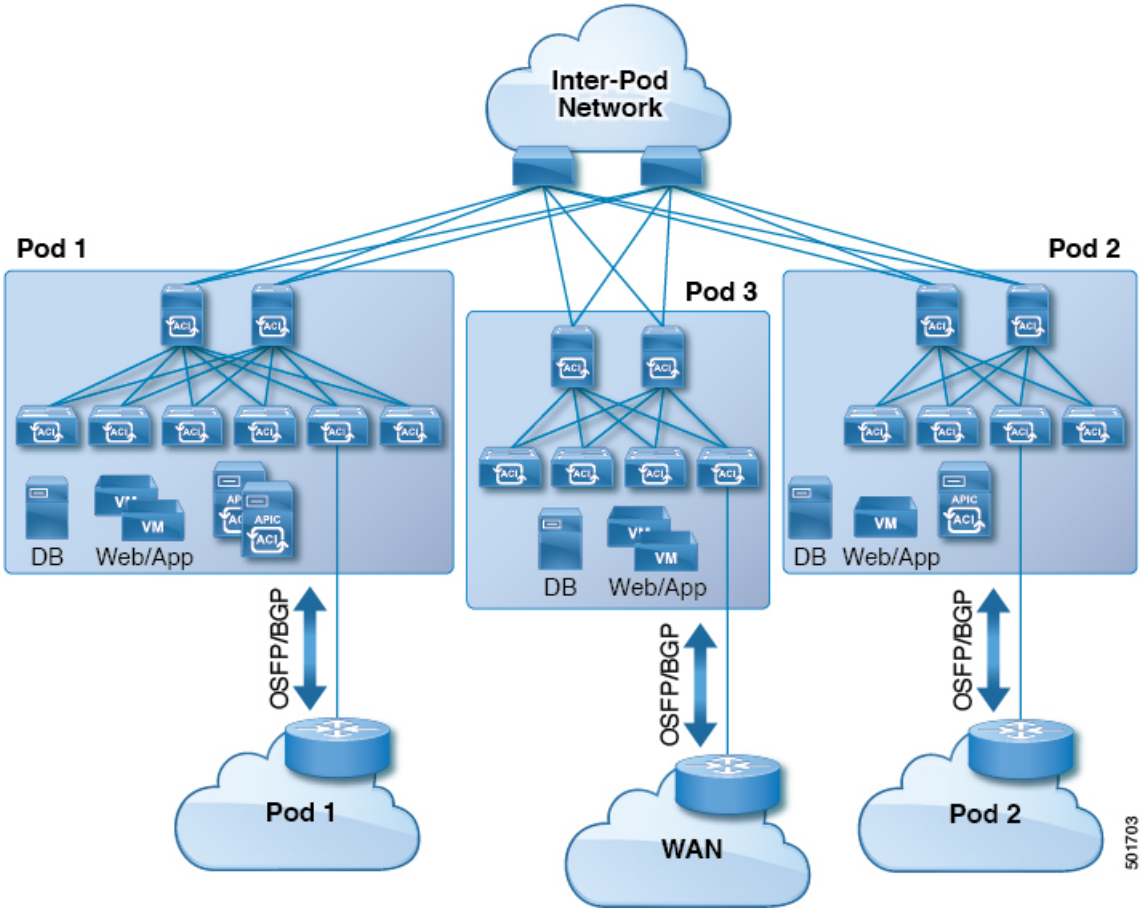


VIP は、特定のサイトやサービスの外部向けの IP アドレスです。VIP は、サービス ノードの背後にある 1 つ以上のサーバまたはノードに関連付けられています。

中継ルーティング設定でのマルチポッド

マルチポッド トポロジでは、ファブリックは、外部接続と複数のポッド間の相互接続の中継として機能します。クラウド プロバイダは、顧客データセンター内に管理対象のリソース ポッドを展開できます。責任分界点は、ファブリックとのピアリングを行っている OSPF または BGP を伴う L3Out にすることができます。

図 *88 :* 中継ルーティング設定における *L3Out* を伴う複数のポッド



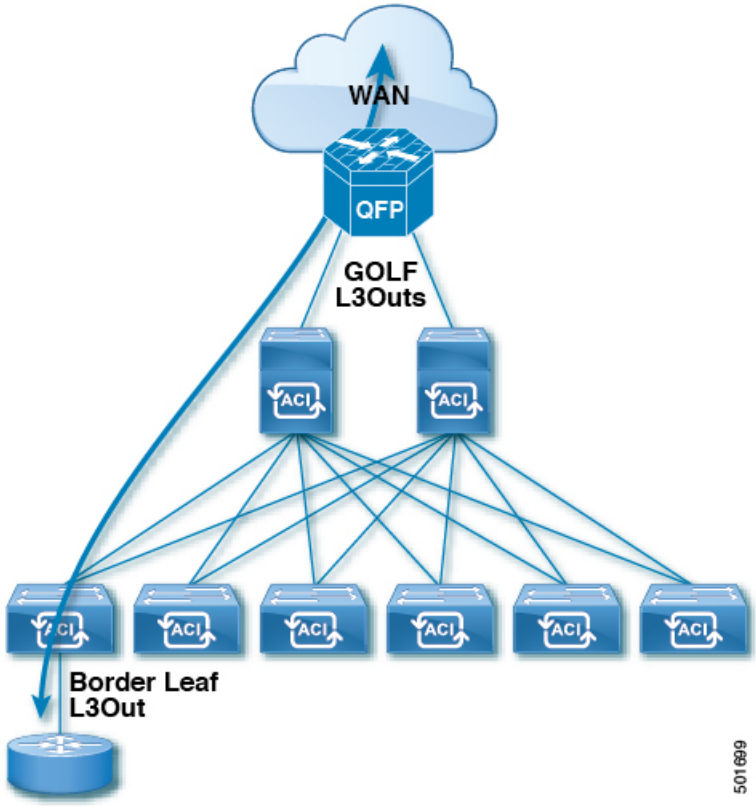
このようなシナリオでは、ポリシーは責任分界点で管理され、ACI ポリシーを設定する必要はありません。

レイヤ4 ～ レイヤ 7 ルート ピアリングはファブリックを中継として使用する特殊な使用例であり、ファブリックは複数ポッドに対する中継 OSPF または BGP ドメインの役目を果たします。ルート ピアリングは、接続されているリーフ ノードとルートを交換できるようにするため、レイヤ4 ～ レイヤ 7 サービス デバイス上で OSPF または BGP ピアリングを有効にするように設定します。ルート ピアリングの一般的な使用例として、SLB VIP が OSPF および iBGP を介して ファブリック外のクライアントにアドバタイズされる、ルート ヘルス インジェクションがあります。このシナリオの詳細については、『*L4-L7 Route Peering with Transit Fabric - Configuration Walkthrough*』を参照してください。

中継ルーティング設定での GOLF

APIC、リリース 2.0 以降では、Cisco ACI は、GOLF L3Out での中継ルーティング (BGP と OSPF) をサポートしています。 たとえば、次の図は、GOLF L3Out と境界リーフ L3Out を伴うファブリックで中継されるトラフィックを示しています。

図 *89 :* 中継ルーティング設定での *GOLF L3Out* と境界リーフ *L3Out*



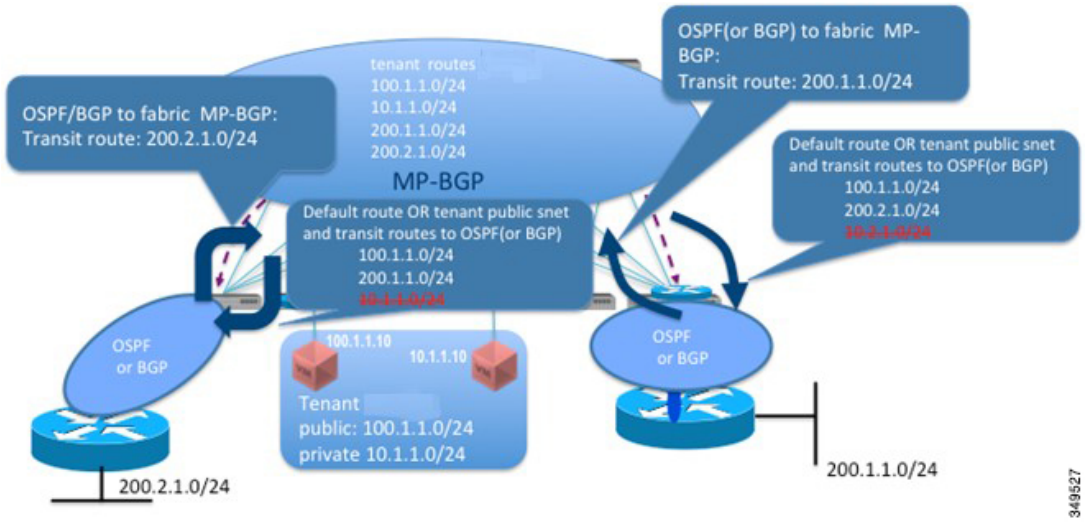
ACI ファブリック ルート ピアリング

ファブリックとのレイヤ3接続およびピアリングは、レイヤ3外部外側ネットワーク（l3extOut）インターフェイスを使用して構成されます。ピアリングプロトコルの構成は、ルートの再配布およびインバウンド/アウトバウンドのフィルタリング ルールとともに、l3extOut に関連付けられます。ACI ファブリックは、外部ピアには巨大なルータとしてではなく、別々のレイヤ 3 ドメイン間のトランジットとして表示されます。1 つの l3extOut のピアリングの考慮事項は、他の l3extOut ポリシーのピアリングの考慮事項に影響を与える必要はありません。ACI ファブリックは、MP-BGP を使用してファブリック内に外部ルートを配布します。

ルートの再配布

外部ピアからのインバウンドルートは、インバウンドフィルタリングルールに従って、MP-BGP を使用して ACI ファブリックに再配布されます。これらは、トランジット ルートまたは WAN 接続の場合の外部ルートである可能性があります。MP-BGP は、テナントが展開されているすべてのリーフ（他の境界リーフを含む）にルートを配布します。

図 *90 :* ルートの再配布



インバウンド ルート フィルタリング ルールは、`l3extOut` インターフェイス上のファブリックに外部ピアによってアドバタイズされたルートのサブセットを選択します。インポート フィルタ ルートマップは、プレフィックス ベースの EPG のプレフィックスを使用して生成されます。インポート フィルタ リストは、ファブリックに配布されるプレフィックスを制限するために MP-BGP にのみ関連付けられます。セット アクションは、ルートマップのインポートに関連付けることもできます。

アウトバウンド方向では、管理者はデフォルトルートまたはトランジットルートとブリッジドメイン パブリック サブネットをアドバタイズするオプションがあります。デフォルトルート アドバタイズメントが有効になっていない場合、アウトバウンド ルート フィルタリングは、管理者によって構成されたルートを選択的にアドバタイズします。

現在、ルートマップは、テナントごとにプレフィックス リストを使用して作成され、外部ルータにアドバタイズされるブリッジドメイン パブリック サブネットを示します。さらに、すべてのトランジットルートを外部ルータにアドバタイズできるように、プレフィックスリストを作成する必要があります。トランジットルートのプレフィックスリストは、管理者によって構成されます。デフォルトの動作では、外部ルータへのすべてのトランジット ルート アドバタイズを拒否します。

トランジット ルートに関連付けられたルートマップには、次のオプションを使用できます。

- *Permit-all*：すべてのトランジット ルートの再配布と外部へのアドバタイズを許可します。
- *Match prefix-list*：トランジット ルートのサブセットのみが再配布され、外部にアドバタイズされます。
- *Match prefix-list* および *set action*：set アクションを通過ルートのサブセットに関連付けて、特定の属性でルートにタグを付けることができます。

ブリッジドメインのパブリック サブネットとトランジット ルート プレフィックスは、異なるプレフィックスリストにすることができますが、異なるシーケンス番号を持つ単一のルートマップに結合されます。トランジット ルートとブリッジドメインのパブリック サブネットは

同じプレフィックスを持つことが想定されていないため、プレフィックス リストの一致は相互に排他的です。

プロトコルによるルート ピアリング

BGP と OSPF を静的ルートと組み合わせる場合、ルート ピアリングをプロトコルごとに構成できます。

OSPF	BGP
接続を有効にして冗長性を提供するために、さまざまなホスト タイプが OSPF を必要とします。これらには、ファブリック内および WAN へのレイヤ 3 中継として ACI を使用するメインフレーム、外部ポッド、およびサービス ノードがあります。このような外部デバイスは、OSPF を実行している非ボーダー リーフを介してファブリックとピアリングします。理想的には、OSPF エリアは、Not-So-Stubby Area（NSSA）または完全スタブエリアとして構成され、デフォルトルートを受信できるようにして、フルエリア ルーティングに参加しないようにします。管理者がルーティング構成を変更したくない既存の展開では、スタブエリア構成は必須ではありません。 2 つのファブリック リーフスイッチは、同じ外部 SVI インターフェイスを共有しない限り、互いに OSPF 隣接関係を確立しません。	外部ポッドとサービス ノードは、ファブリックで BGP ピアリングを使用できます。BGP ピアは `l3extOut` に関連付けられており、`l3extOut` ごとに複数の BGP ピアを構成することができます。BGP ピアには、OSPF、EIGRP、接続されたインターフェイス、静的ルート、またはループバック経由で到達できます。外部ルータとのピアリングには iBGP または eBGP を使用できます。ファブリック内への外部ルートの配付には MP-BGP が使用されるため、外部ルータからの BGP ルート属性は保持されます。 同じ値を持つ推移的および非推移的 BGP 拡張コミュニティの両方に一致する構成はサポートされていません。 APIC はこの構成を拒否します。

OSPF	BGP
OSPF ルート再配布 OSPF 内の default-information originate ポリシーは外部ルータへのデフォルトルートを生成します。メインフレーム、外部ポッド、およびサービス ノードとピアリングする場合は、ポリシーを有効にすることが推奨されています。 default-information originate ポリシーが有効になっていない場合は、OSPF ドメインで redistribute-static および redistribute-BGP を構成して、静的ブリッジドメイン（BD）パブリック サブネットとトランジット ルートをそれぞれアドバタイズします。ルートマップをアウトバウンド フィルタリングの再配布ポリシーに関連付けます。外部 WAN ルータとピアリングする場合は、default-information originate オプションを有効にしないことが推奨されています。インバウンド方向では、OSPF ルートは MP-BGP を使用して ACI ファブリックに再配布されます。	**BGP ルートの再配布** アウトバウンド方向では、デフォルトルートは、default-originate ポリシーによってピアごとに BGP によって生成されます。ローカル ルーティング テーブルにデフォルトルートがない場合でも、デフォルトルートは BGP によってピアに挿入されます。default-originate ポリシーが構成されていない場合、ブリッジドメインのパブリック サブネットに対して静的再配布が有効になります。MP-BGP からの通過ルートは、アドバタイズのために BGP に使用できます。これらのルートは、アウトバウンドフィルタリング ポリシーに従って、条件付きで外部にアドバタイズされます。 インバウンド方向では、アドバタイズされたルートを MP-BGP で使用して、インバウンドフィルタリング ルールに従ってファブリック内で再配布できます。BGP が外部ピアリングに使用されている場合、ルートのすべての BGP 属性はファブリック全体で保持されます。

OSPF	BGP
OSPF ルート フィルタリング 外部ピアから受け入れられるリンクステート アドバタイズメント（LSA）の数を制限するように OSPF を構成して、不正な外部ルータが原因でルート テーブルが過剰に消費されないようにすることができます。 着信ルート フィルタリングは、OSPF を使用したレイヤ 3 外部の外部テナント ネットワークでサポートされています。これは、ファブリックで許可される通過ルートをフィルタリングするために、ルートマップを間接的に使用して適用されます。 アウトバウンド方向では、OSPF ドメイン レベルで redistribute-static および redistribute-BGP を構成します。ブリッジドメインのパブリック サブネットとトランジット ルートをフィルタリングするルートマップを構成します。オプションで、ルートマップの一部のプレフィックスは、ルート タグを追加する set アクションで構成することもできます。エリア間プレフィックスも、アウトバウンドフィルタ リストを使用してフィルタリングされ、OSPF エリアに関連付けられます。	**BGP ルート フィルタリング** BGP のインバウンド ルート フィルタリングは、ピアごとにルートマップを使用して適用されます。ルートマップは、間接的な *peer-af* レベルで構成され、ファブリックで許可される通過ルートをフィルタリングします。 アウトバウンド方向では、静的ルートは *dom-af* レベルで BGP に再配布されます。MP-BGP からのトランジット ルートは、外部 BGP ピアリング セッションで使用できます。ルートマップは、パブリック サブネットと外部の選択されたトランジット ルートのみを許可するように、アウト方向の *peer-af* レベルで構成されます。必要に応じて、選択したプレフィックスのコミュニティ値をアドバタイズする set アクションをルートマップに構成します。 ブリッジドメインのパブリック サブネットとトランジット ルート プレフィックスは、異なるプレフィックス リストにすることができますが、*peer-af* レベルで異なるシーケンス番号を持つ単一のルートマップに結合されます。

OSPF	BGP
OSPF 名ルックアップ、プレフィックス抑制、およびタイプ 7 変換 OSPF は、ルータ ID の名前ルックアップを有効にし、プレフィックスを抑制するように構成できます。 APIC システムは、変換されたタイプ 5 LSA 機能で OSPF 転送アドレス抑制を実行します。これにより、NSSA ABR はタイプ 7 LSA をタイプ 5 LSA に変換します。これを回避するには、Type-7 LSA で指定されているものではなく、0.0.0.0 サブネットを転送アドレスとして使用します。この機能を使用すると、フォワーディング アドレスをバックボーンにアドバタイズしないよう設定されているルータが、転送されたトラフィックを、変換を行う NSSA ASBR に渡すようになります。	**BGP ダイナミック ネイバー サポートとプライベート AS コントロール** 特定のネイバーアドレスを提供する代わりに、アドレスのダイナミック ネイバー範囲を提供できます。 プライベート自律システム（AS）番号の範囲は、64512 ～ 65535 です。それらは、グローバル BGP テーブルにアドバタイズできません。プライベート AS 番号は、ピアごとに AS パスから削除でき、次のオプションに従って eBGP ピアにのみ使用できます。 • `Remove Private AS`：AS パスにプライベート AS 番号のみが含まれる場合は削除します。 • `Remove All`：AS パスにプライベート AS 番号とパブリック AS 番号の両方がある場合は削除します。 • `Replace AS`：プライベート AS をローカル AS 番号に置き換えます。 （注） `remove private AS` が設定されている場合、`Remove all` と `replace AS` のみ設定できます。

BGP ダンプニングは、ボーダー リーフスイッチ（BL）に接続されている外部ルータから受信したフラッピング e-BGP ルートのファブリックへの伝達を最小限に抑えます。外部ルータからの頻繁なフラッピング ルートは、構成した基準に基づいて BL で抑制されます。その後、iBGP ピア（ACI スパイン スイッチ）への再配布が禁止されます。抑制されたルートは、構成された時間が経過すると再利用されます。各フラップは、1000 のペナルティで e-BGP ルートにペナルティを課します。フラップ ペナルティが定義済みの抑制制限しきい値（デフォルトは 2000）に達すると、e-BGP ルートは抑制済みとしてマークされます。抑制したルートは、他の BGP ピアにアドバタイズされません。ペナルティは、半減期の間隔（デフォルトは 15 分）ごとに半分に減分されます。ペナルティが指定された再利用制限（デフォルトは 750）を下回ると、抑制されたルートが再利用されます。抑制されたルートは、指定された最大抑制時間（最大 45 分）だけ抑制されます。

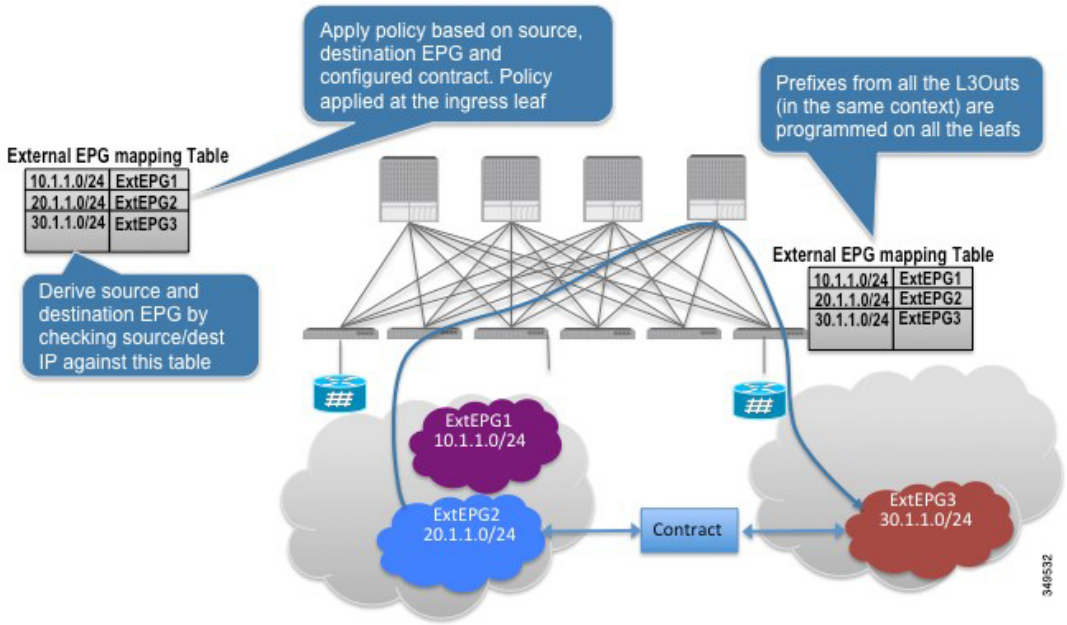
BGP 重み属性を使用してベストパスを選択します。重み (0 ～ 65,535) は、特定のルーターにローカルに割り当てられます。値が伝達されたり、ルート アップデートで伝送されたりすることはありません。デフォルトでは、ルータが送信元となるパスには 32,768 の重みが割り当てられ、他のパスには 0 の重みが割り当てられます。同じ接続先へのルートが複数存在する場合

は、重み値の高いルートが優先されます。BGP ネイバーまたはルートマップの下に重みを設定します。

BGP ピアリングは、通常、ネイバーのループバック アドレスに構成されます。このような場合、ループバックの到達可能性は静的に構成されるか、OSPF を介して（より一般的には）アドバタイズされます。ループバック インターフェイスはパッシブインターフェイスとして構成され、OSPF エリアに追加されます。OSPF に付加される再配布ポリシーはありません。ルート再配布の導入は、BGP を介して行われます。ルート フィルタリングは、BGP または OSPF のいずれかを使用するテナント ネットワークの L3Outs で構成できます。

外部ルートは、それぞれのテナントのボーダー リーフで静的ルートとしてプログラムすることもできます。外部ルートがボーダー リーフで静的ルートとしてプログラムされている場合、ピアリング プロトコルは必要ありません。外部静的ルートは、インポート フィルタリングに従って、MP-BGP を介してファブリック内の他のリーフスイッチに再配布されます。リリース 1.2(1x) 以降、ACI ファブリック内で着信する静的ルート プリファレンスは、コスト拡張コミュニティを使用して MP-BGP で伝送されます。L3Out 接続では、レイヤ 4 からの MP-BGP ルートがローカル静的ルートよりも優先されます。ルートは、管理者によって指定された優先順位でユニキャスト ルーティング情報ベース（URIB）にインストールされます。ACI 非ボーダー リーフスイッチでは、ネクストホップとしてレイヤ 4 を使用してルートがインストールされます。レイヤ 4 のネクストホップが使用できない場合、レイヤ 3 の静的ルートがファブリック内の最適なルートになります。

図 *91 :* トランジットの静的ルート ポリシー モデル



`l3extOut` 接続の場合、IP プレフィックスを基に外部エンドポイントを外部 EPG にマッピングできます。`l3extOut` 接続ごとに、エンドポイントごとに異なるポリシーが必要かどうかに基づいて、1 つ以上の外部 EPG を作成できます。

各外部 EPG は、クラス ID に関連付けられています。外部 EPG の各プレフィックスは、対応するクラス ID を取得するようにハードウェアでプログラムされます。プレフィックスは修飾

された VRF インスタンスのみであり、プレフィックスが展開されている l3extOut インターフェイスによるものではありません。

同じ VRF 内のすべての l3extOut ポリシーからのプレフィックスの結合は、l3extOut ポリシーが展開されているすべてのリーフスイッチでプログラムされます。パケットの送信元および宛先 IP アドレスに対応する送信元および宛先のクラス ID は入力リーフで取得され、ポリシーは構成されたコントラクトに基づいて入力リーフ自体に適用されます。コントラクトで 2 つの L3Out インターフェイス上の 2 つのプレフィックス間のトラフィックが許可されている場合、送信元と宛先 IP アドレス（構成されたプレフィックスに属する）の任意の組み合わせを持つパケットは、L3Out インターフェイス間で許可されます。EPG 間にコントラクトがない場合、トラフィックは入力リーフでドロップされます。

プレフィックスは l3extOut ポリシーが展開されているすべてのリーフスイッチでプログラムされるため、APIC がプレフィックス ベースの EPG に対してサポートするプレフィックスの総数は、ファブリックに対して 1000 に制限されます。

重複するサブネットまたは等しいサブネットは、同じ VRF 内の異なる l3extOut インターフェイスに構成できません。サブネットが重複または等しい必要がある場合は、適切なエクスポート プレフィックスを使用して単一の l3extOut がトランジットに使用されます。

トランジット ルート制御

ルート トランジットは、インポートされるレイヤ 3 アウトサイド ネットワーク L3extOut プロファイル（l3extInstP）を通してトラフィックをインポートするために定義されます。異なるルート トランジットは、エクスポートされる別の l3extInstP を通してトラフィックをエクスポートするために定義されます。

ファブリック内の 1 つまたは複数のノードに複数の l3extOut ポリシーを配置できるので、プロトコルのさまざまな組み合わせがサポートされます。プロトコルの組み合わせはすべて、複数の l3extOut ポリシーを使用して 1 つのノードに配置することも、または複数の l3extOut ポリシーを使用して複数のノードに配置することも可能です。同じファブリック内の異なる l3extOut ポリシーに 3 つ以上のプロトコルを配置することもできます。

エクスポートルートマップは、プレフィックスリストの一致から構成されます。各プレフィックス リストは、VRF 内のブリッジ ドメイン（BD）パブリック サブネット プレフィクスと、外部にアドバタイズする必要のあるエクスポート プレフィクストから構成されます。

ルート制御ポリシーは、l3extOut ポリシーで定義され、l3extOut に関連付けられたプロパティおよび関係によって制御されます。APIC は l3extOut の enforceRtctrl プロパティを使用して、ルート制御方向を適用します。デフォルトでは、エクスポートの制御を適用し、インポートのすべてを許可します。インポートおよびエクスポートされたルート（l3extSubnets）は、l3extInstP で定義されます。すべてのルートのデフォルト スコープはインポートです。これらは、プレフィックス ベースの EPG を形成するルートおよびプレフィックスです。

インポート ルート マップからのすべてのインポート ルートは、BGP および OSPF によってインポートを制御するために使用されます。エクスポート ルート マップからのすべてのエクスポート ルートは OSPF および BGP によってエクスポートを制御するために使用されます。

インポートとエクスポートのルート制御ポリシーは、異なるレベルで定義されます。IPv6 ではすべての IPv4 ポリシー レベルがサポートされます。`l3extInstP` および `l3extSubnet` MO で定義されている追加の関係でインポートを制御します。

デフォルト ルート リークは、`l3extOut` の下の `l3extDefaultRouteLeakP` MO の定義によって有効になります。

OSPF のエリアごと、BGP のピアごとに `l3extDefaultRouteLeakP` は Virtual Routing and Forwarding（VRF）範囲または `L3extOut` 範囲を有することができます。

次の設定ルールは、ルート制御を提供します。

- `rtctrlSetPref`
- `rtctrlSetRtMetric`
- `rtctrlSetRtMetricType`

`rtctrlSetComm` MO の追加構文には以下が含まれています。

- `no-advertise`
- `no-export`
- `no-peer`

BGP

ACI ファブリックは、外部ルータとの BGP ピアリングをサポートします。BGP ピアは `l3extOut` ポリシーに関連付けられており、`l3extOut` ごとに複数の BGP ピアを設定することができます。BGP は、`l3extOut` の下で `bgpExtP` MO を定義することにより `l3extOut` レベルで有効化できます。



（注） `l3extOut` ポリシーにルーティング プロトコル（たとえば、関連する VRF を含む BGP）が含まれる一方で、L3Out インターフェイスのプロファイルには必要な BGP インターフェイス設定の詳細が含まれます。いずれも BGP の有効化に必要です。

BGP ピアには、OSPF、EIGRP、接続されたインターフェイス、スタティック ルート、またはループバック経由で到達できます。外部ルータとのピアリングには iBGP または eBGP を使用できます。ファブリック内への外部ルートの配付には MP-BGP が使用されるため、外部ルータからの BGP ルート属性は保持されます。BGP は `l3extOut` に関連付けられた VRF に Ipv4 や IPv6 アドレス ファミリを有効にすることができます。スイッチ上で有効になるアドレス ファミリは、`bgpPeerP` ポリシーで `l3extOut` のために定義した IP アドレス タイプによって決まります。ポリシーは省略可能です。定義しない場合はデフォルトが使用されます。ポリシーはテナントに対して定義され、名前で参照される VRF によって使用できます。

ピア ポリシーを少なくとも 1 つのピアを定義して、境界リーフ（BL）の各スイッチでプロトコルを有効にする必要があります。ピア ポリシーは 2 つの場所で定義できます。

- `l3extRsPathL3OutAtt` の下：送信元インターフェイスとして物理インターフェイスが使用されます。

- l3extLNodeP の下：送信元インターフェイスとしてループバック インターフェイスが使用されます。

OSPF

接続を有効にして冗長性を提供するために、さまざまなホスト タイプが OSPF を必要とします。これらには、たとえばファブリック内および WAN へのレイヤ 3 中継として ACI ファブリックを使用するサービス ノード、外部ポッド、メインフレーム デバイスなどがあります。このような外部デバイスは、OSPF を実行している非境界リーフ スイッチを介してファブリックとピアリングします。デフォルトルートは受信し、全域ルーティングには参加しないよう、OSPF エリアを NSSA（スタブ）エリアとして設定します。通常は、既存のルーティングの導入によって設定の変更が回避されるため、スタブ エリアの設定は必須ではありません。

l3extOut で ospfExtP 管理対象オブジェクトを設定して、OSPF を有効にします。BL スイッチ上で設定されている OSPF IP アドレス ファミリ バージョンは、OSPF インターフェイス IP アドレスに設定されているアドレス ファミリによって決まります。

（注） l3extOut ポリシーにルーティング プロトコル（たとえば、関連する VRF とエリア ID を含む OSPF）が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

アドレス ファミリごとに設定可能な fvRsCtxToOspfCtxPol 関係を使用して、VRF レベルで OSPF ポリシーを設定します。設定していない場合、デフォルト パラメータが使用されます。

要求されるエリア プロパティ Ipv6 を公開する ospfExtP 管理対象オブジェクトで OSPF を設定します。

デフォルト ポリシー動作

2 つのプレフィックス ベースの EPG 間にコントラクトがない場合、不明な送信元プレフィックスと不明な接続先プレフィックス間のトラフィックはドロップされます。これらのドロップは、未知の送信元プレフィックスと接続先プレフィックスに対して異なるクラス ID を暗黙的にプログラミングすることによって実現されます。クラス ID が異なるため、クラスが等しくないルールの影響を受け、パケットが拒否されます。また、クラス不等ドロップ ルールにより、パケットは既知の送信元および宛先 IP アドレスから不明な送信元および宛先 IP アドレスにドロップされ、その逆も同様です。

このデフォルトの動作の変更により、キャッチオール（0/0）エントリのクラス ID プログラミングが次の例に示すように変更されました。

- 不明な送信元 IP アドレスは EPG1 です。
- 不明な宛先 IP アドレスは EPG2 です。
- 不明なソース IP <—> 不明な接続先 IP => クラス不等ルール => DROP。

- ユーザ構成のデフォルト プレフィックス（0/0）= EPG3 および（10/8）= EPG4。EPG3 と EPG4 間のコントラクトは ALLOW に設定されています。
- プログラム規定：
  - EPG1 <—> EPG4 => class-unequal ルール => DROP
  - EPG4 <—> EPG2 => class-unequal ルール => DROP

EIGRP プロトコルのサポート

EIGRP プロトコルは、Cisco Application Centric Infrastructure（ACI）ファブリック内の他のルーティング プロトコルと同様にモデル化されています。

サポートされる機能

サポートされる機能は次のとおりです。

- IPv4 および IPv6 ルーティング
- 各アドレス ファミリの仮想ルーティングおよび転送（VRF）とインターフェイスの制御
- ノード間の OSPF による再配布
- VRF ごとのデフォルト ルート リーク ポリシー
- パッシブ インターフェイスおよびスプリット ホライズンのサポート
- エクスポートされたルートにタグを設定するためのルート マップ制御
- EIGRP インターフェイス ポリシーの帯域幅および遅延設定オプション
- 認証サポート

サポートされない機能

次の機能はサポートされていません。

- スタブ ルーティング
- BGP 接続に使用される EIGRP
- 同じノード上の複数の EIGRP `L3extOut`
- インターフェイスごとの集約（EIGRP サマリー ポリシーは、L3Out で設定されたすべてのインターフェイスに適用されます）
- インターフェイスごとのインポートおよびエクスポート用配布リスト

EIGRP 機能のカテゴリ

EIGRP の機能は、次のように大きく分類できます。

- プロトコル ポリシー
- L3extOut の設定
- インターフェイス設定
- ルート マップ サポート
- デフォルト ルート サポート
- 中継サポート

EIGRP をサポートしているプライマリ管理対象オブジェクト

次のプライマリ管理対象オブジェクトは、EIGRP サポートを提供します。

- **EIGRP アドレス ファミリ コンテキスト ポリシー** eigrpCtxAfPol：fvTenant（テナント/プロトコル）で設定されているアドレス ファミリ コンテキスト ポリシー
- fvRsCtxToEigrpCtxAfPol：所定のアドレス ファミリ（IPv4 または Ipv6）についての VRF から eigrpCtxAfPol への関係。関係は、アドレス ファミリごとに 1 つのみ存在できます。
- eigrpIfPol：fvTenant で設定される EIGRP インターフェイス ポリシー。
- eigrpExtP：L3extOut 上で EIGRP のフラグを有効にします。
- eigrpIfP：l3extLIfP に接続された EIGRP インターフェイス プロファイル。
- eigrpRsIfPol：EIGRP インターフェイス プロファイルから eigrpIfPol への関係。
- Defrtleak：l3extOut 下のデフォルト ルート リーク ポリシー。

テナントでサポートされる EIGRP プロトコル ポリシー

テナント下では次の EIGRP プロトコル ポリシーがサポートされます。

- **EIGRP インターフェイス ポリシー（eigrpIfPol）**：インターフェイス上の所定のアドレス ファミリに適用される設定が含まれます。インターフェイス ポリシーでは次の設定が可能です。
  - 秒単位の *hello* 間隔
  - 分単位の *hold* 間隔
  - 次のインターフェイス制御フラグのうち 1 つ以上。
    - スプリット ホライズン
    - パッシブ
    - ネクスト ホップ セルフ

- **EIGRP アドレス ファミリ コンテキスト ポリシー（`eigrpCtxAfPol`）**：所定の VRF 内の所定のアドレス ファミリの設定が含まれます。`eigrpCtxAfPol` は、テナント プロトコル ポリシー下で設定され、テナント下の 1 つ以上の VRF に適用できます。`eigrpCtxAfPol` は、VRF-per-address ファミリの関係を通して VRF で有効にできます。所定のアドレス ファミリに関係がない場合、あるいは関係に記述されている `eigrpCtxAfPol` が存在しない場合は、`[共通]` テナント下に作成されたデフォルトの VRF ポリシーがそのアドレス ファミリに使用されます。

  次の設定では、`eigrpCtxAfPol` で許可されます。

  - 内部ルートのアドミニストレーティブ ディスタンス
  - 外部ルートのアドミニストレーティブ ディスタンス
  - 最大許容 ECMP パス数
  - アクティブ タイマー間隔
  - メトリック バージョン（32 ビット/64 ビット メトリック）

L3extOut の構成

EIGRP は、リーフスイッチで構成されたファブリック パブリック サブネット、接続ルート、静的ルート、およびトランジット ルートをアドバタイズするために使用される主要なプロトコルです。

特定のレイヤ 3 外部外側ネットワーク（`l3extOut`）ルーテッド ドメインには、EIGRP の有効化/無効化フラグがあります。

（注） EIGRP に使用されるタグであり、BGP で使用されるファブリック ASN とは異なる自律システム番号。

EIGRP は、同じ `L3extOut` で BGP と OSPF を使用して有効にすることはできません。

以下のEIGRP トランジットのシナリオがサポートされています。

- あるノードの `L3extOut` で実行されている EIGRP と、別のノードの別の `L3extOut` で実行されている OSPF。

（注） 複数の EIGRP `L3extOut` は、同じ Virtual Routing and Forwarding（VRF）の同じノードではサポートされていません。

- EIGRP から静的ルートへのトランジット。

EIGRP インターフェイス プロファイル

インターフェイスで EIGRP を有効にするには、`L3extOut` ->[ノード（Node）] ->[インターフェイス階層（Interface hierarchy）] のインターフェイス プロファイルの下に EIGRP プロファイルを構成する必要があります。EIGRP プロファイルには、テナントで有効になっている EIGRP インターフェイス ポリシーとの関係があります。テナントに関係またはインターフェイス ポリシーがない場合、`common` テナントのデフォルトの EIGRP インターフェイス ポリシーが使用されます。EIGRP は、インターフェイス プロファイルに含まれるすべてのインターフェイスで有効になっています。これには、L3 ポート、サブインターフェイス、ポート上の外部 SVI、ポート チャネル、およびインターフェイス プロファイルに含まれる VPC が含まれます。

ポリシー モデルのルート マップ インフラストラクチャと設定は、すべてのプロトコルで共通です。ルートマップセットアクションは、BGP、OSPF、および EIGRP をカバーするアクションのスーパーセットです。EIGRP プロトコルは、インターリーク/再配布に使用されるルートマップで *set tag* オプションをサポートします。これらのルートマップは、VRF ごとに構成されます。`L3extOut` に IPv4 と IPv6 の両方のインターフェイスがある場合、インターリーク ポリシーは、その VRF の IPv4 と IPv6 の両方のアドレス ファミリに適用されます。

（注） 現時点では、VRF レベルのルートマップはサポートされていますが、インターフェイス ルートマップはサポートされていません。

`L3extOut` のデフォルトのルート リーク ポリシーは、構成に関してプロトコルに依存しません。デフォルトのルート リーク ポリシーで有効になっているプロパティは、個々のプロトコルのスーパーセットです。デフォルト ルート リークでサポートされる構成は次のとおりです。

- *Scope*：VRF は、EIGRP でサポートされる唯一の範囲です。
- **Always**：スイッチは、ルーティング テーブルに存在する場合にのみデフォルトルートをアドバタイズするか、関係なくアドバタイズします。
- *Criteria*：唯一または追加。唯一のオプションを使用すると、デフォルトルートだけが EIGRP によってアドバタイズされます。さらに、パブリック サブネットとトランジット ルートがデフォルトルートとともにアドバタイズされます。

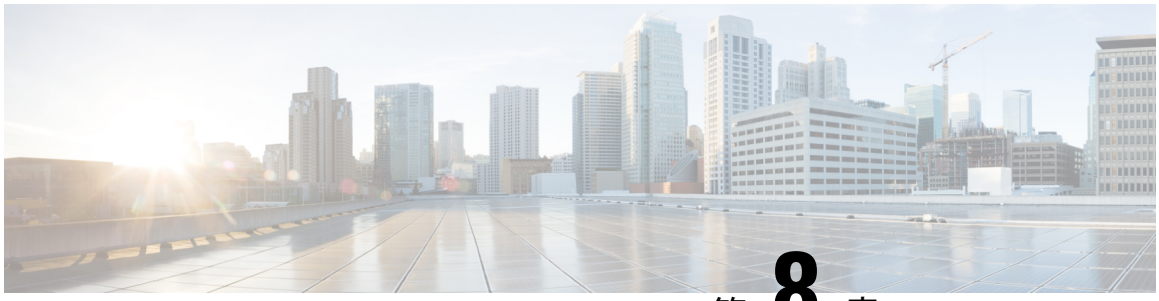
デフォルトルート リーク ポリシーは、アドレス ファミリごとの VRF ごとにドメインで有効になっています。

デフォルトでは、適切なルートマップを使用したプロトコル再配布インターリーク ポリシーが、すべての有効な構成に設定されています。管理者は、同じ VRF 内の 2 つの `L3extOut` 間で特定のルートを送信できるようにするために、*scope=export-route control* を使用して `l3extInstP` サブネットを作成することによって、トランジット ルーティングのみを有効にします。`l3extInstP` サブネットの範囲とは別に、トランジット ケースをカバーするための特別なプロトコル固有の構成はありません。プロトコル固有の範囲とは別に、デフォルトルート リーク ポリシーの他のパラメータは、すべてのプロトコルで共通です。

異なるノード通過シナリオの別の `L3extOut` での OSPF は、EIGRP でサポートされます。

次に示す EIGRP のガイドラインおよび制限事項に従ってください。

- 現時点では、同じリーフスイッチで複数の EIGRP L3Out はサポートされていません。
- すべてのルートは、EIGRP を使用する `L3extOut` にインポートされます。EIGRP が `L3extOut` のプロトコルである場合、インポート サブネット スコープは GUI で無効になっています。



第 8 章

ユーザアクセス、認証およびアカウンティング

この章は、次の内容で構成されています。

- ユーザ アクセス、認可およびアカウンティング （249 ページ）
- マルチテナントのサポート （250 ページ）
- ユーザ アクセス：ロール、権限、セキュリティ ドメイン （250 ページ）
- アカウンティング （252 ページ）
- 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 （254 ページ）
- カスタム RBAC 規則 （254 ページ）
- APIC ローカル ユーザ （255 ページ）
- 外部管理されている認証サーバのユーザ （257 ページ）
- APIC Bash シェルのユーザ ID （263 ページ）
- ログイン ドメイン （263 ページ）
- SAML 認証 （264 ページ）

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。

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、テナントにはセキュリティ 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にはできません。

（注） （R6.1.2まで）セキュリティドメイン内のパスワード強度パラメータは、**[カスタム条件（Custom Conditions）]** を作成するか、または提供されている **[いずれかの 3 つの条件（Any Three Conditions）]** を選択して構成できます。

（注） （R6.1.3以降）セキュリティ ドメイン内のパスワード強度パラメータは、**[Custom Conditions]** を作成するか、小文字、数字、特殊文字を含む **[デフォルトの 3 つの条件（Default Three Conditions）]** を選択することで構成できます。

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
- `Common`：ファブリックの共通オブジェクト/サブツリーへのアクセスを許可
- `Mgmt`：ファブリック管理オブジェクト/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。

アカウンティング

Cisco Application Centric Infrastructure（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によって処理されます。

- `aaaSessionLR` 管理対象オブジェクトは、Cisco Application Policy Infrastructure Controller（APIC）APIC およびスイッチでのユーザー 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。Cisco 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）

（注） 5.3(1) リリース以降、telnet はサポートされていません。

- セッションの時間と長さ
- トークン更新：ユーザー アカウントのログイン イベントは、ユーザー アカウントが Cisco 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 管理対象オブジェクト は、ユーザー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、Cisco 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、古いものから順にレコードが上書きされます。

（注） Cisco 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 管理対象オブジェクトは、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 **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[POD]** > **[履歴（History）]** > **[監査ログ（Audit Log）]** セクションから入手できます。Cisco APIC GUI の **[履歴（History）]** > **[監査ログ（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 と aaaSessionLR 管理対象オブジェクトのクエリ 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。

Cisco 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。

カスタム RBAC 規則

RBAC 規則により、ファブリック全体の管理者は、本来はブロックされるはずのセキュリティ ドメイン間アクセスを許可することができます。RBAC 規則を使用して、別のセキュリティ ドメインにあるため他の方法ではアクセス不可能なサービスを共有したり物理リソースを公開したりできます。RBAC 規則では、ターゲット リソースへの読み取りアクセスのみ許可されます。GUI RBAC 規則ページは、[管理（Admin）] > [AAA] > [セキュリティ管理（Security Management）] の下にあります。RBAC 規則は、リソースが存在する前に作成できます。RBAC 規則、ロール、および権限（およびそれらの依存関係）の説明は、管理情報モデルのリファレンスに記載されています。

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）。

ops 規則は、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。これらは、APIC の他のすべての構成と同様に、admin 権限を使用して行う必要があります。

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 サーバを使用せずに、Cisco Application Policy Infrastructure Controller（APIC）自体でユーザを構成することを選択できます。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、Cisco 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 Application Centric Infrastructure （ACI）では、最大 100 名までの管理者ユーザがサポートされています。

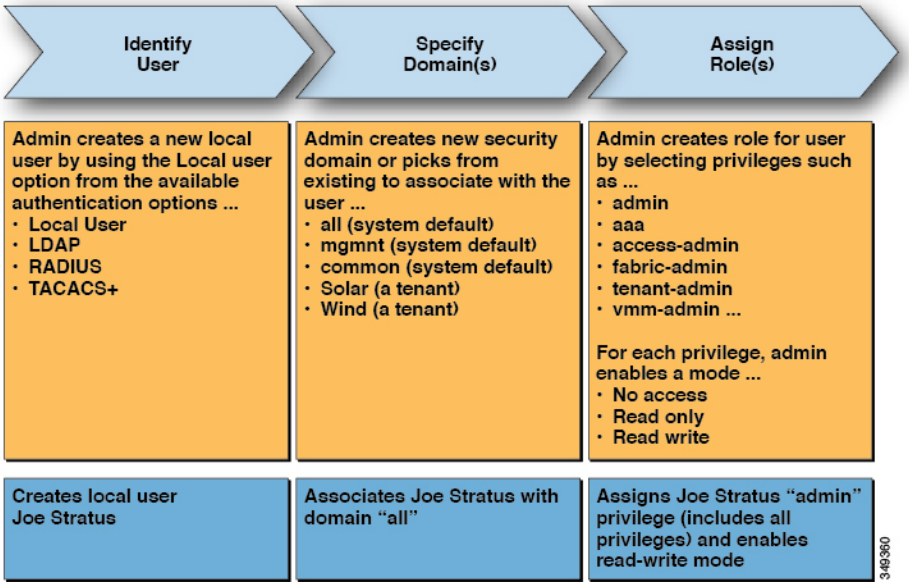
（注） 6.0(2) リリース以降、 Cisco APIC ベース OS が更新され、簡単に推測できるパスワードを検出するためのディクショナリが追加されました。その結果、以前のリリースで強力と見なされたパスワードのうち、現在では強力とは見なされなくなったものがあります。

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 Cisco 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、Cisco APIC に同時にログインできます。

次の図は、Cisco 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 Cisco APIC 認証データベース内の管理ユーザーを設定するプロセスがどのように動作するかを示しています。

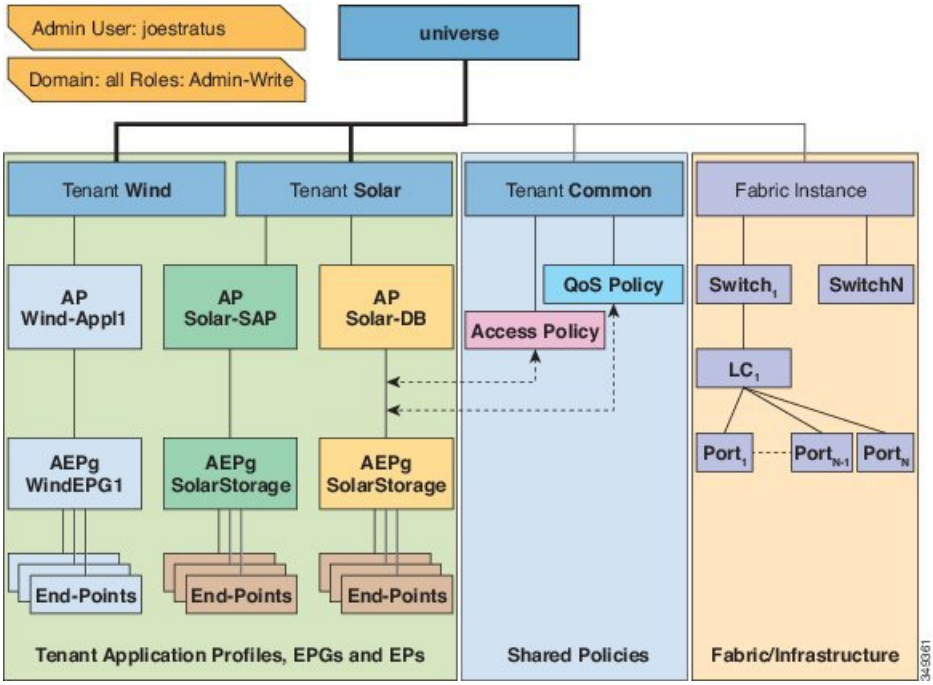
図 *92 : APIC* ローカル ユーザーの構成プロセス



（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 Cisco 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 *93*：「*all*」ドメインへ管理ユーザを設定した結果

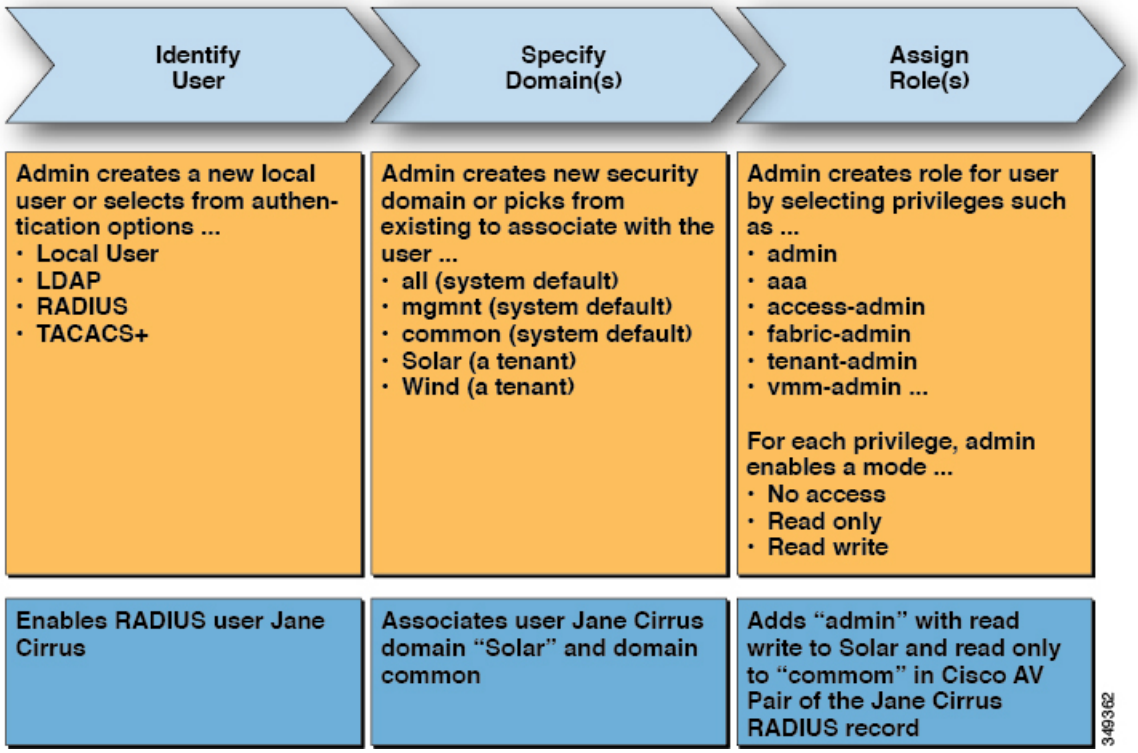


読み取り/書き込み「管理者」権限を持つユーザ Joe Stratus は、ドメイン「all」に割り当てられ、システム全体へのフル アクセス権が与えられます。

外部管理されている認証サーバのユーザ

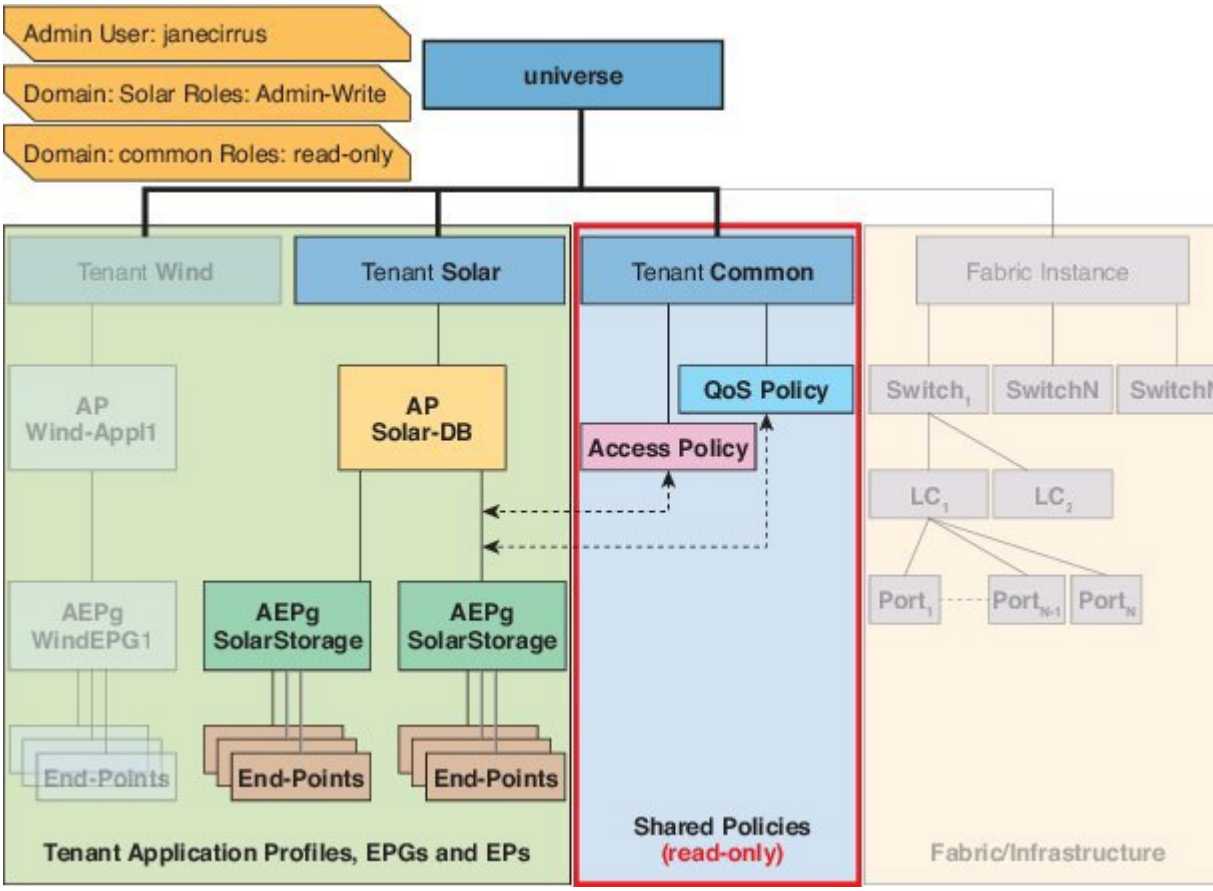
次の図は、テナント Solar へのフル アクセス権がある外部 RADIUS サーバ内の管理ユーザを設定するプロセスがどのように動作するかを示します。

図 *94 :* 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 *95 :* 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。

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 …"
```

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。

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。

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)
```

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。

- APIC とスイッチの両方の REST API、GUI、および CLI で *apic#fallback\\username* 文字列を使用します。
- *apic:fallback\\username* 文字列は、REST API と GUI にのみ使用し、CLI インターフェイスには使用しません。



（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。

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。

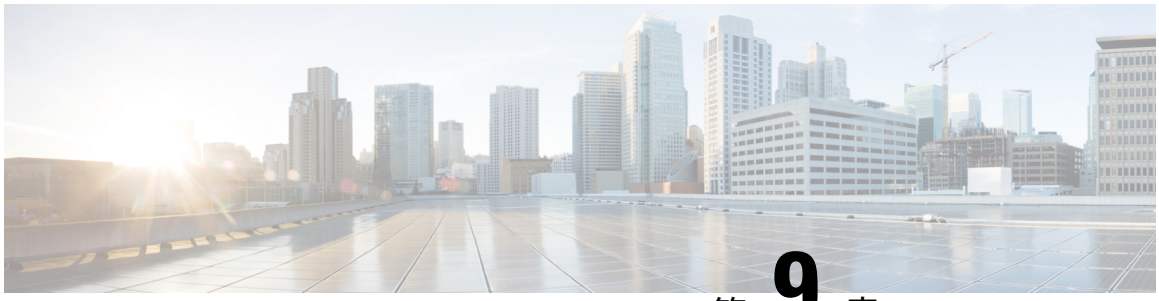
SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

（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。



第 9 章

Virtual Machine Manager のドメイン

この章は、次の内容で構成されています。

- Cisco ACI の VM ネットワーキングによる Virtual Machine Manager のサポート （267 ページ）
- VMM ドメイン ポリシー モデル （269 ページ）
- Virtual Machine Manager ドメインの主要コンポーネント （269 ページ）
- Virtual Machine Manager のドメイン （270 ページ）
- VMM ドメイン VLAN プールの関連付け （271 ページ）
- VMM ドメイン EPG の関連付け （272 ページ）
- トランク ポート グループ （274 ページ）
- EPG ポリシーの解決および展開の緊急度 （275 ページ）
- VMM ドメインを削除するためのガイドライン （277 ページ）

Cisco ACI の VM ネットワーキングによる Virtual Machine Manager のサポート

ACI VM ネットワー キングの利点

Cisco Application Centric Infrastructure（ACI）稼働マシン（VM）ネットワーキングは、複数のベンダーからハイパーバイザをサポートします。ハイパーバイザに対し、高パフォーマンスでスケーラブルな仮想データセンターインフラストラクチャへのプログラム可能で自動化されたアクセスを提供します。

プログラム可能性と自動化は、スケーラブルなデータセンター仮想化インフラストラクチャにおける重要な機能です。Cisco ACI オープン REST API により、ポリシー モデル ベースの Cisco ACI ファブリックとの仮想マシンの統合およびオーケストレーションが可能になります。Cisco ACI VM ネットワーキングでは、複数のベンダーからハイパーバイザにより管理されている仮想および物理ワークロードの両方でのポリシーの一貫した適用を可能にします。

接続可能なエンティティ プロファイルにより、VM のモビリティと、Cisco ACI ファブリック内の任意の場所にワークロードを簡単に配置できます。Cisco Application Policy Infrastructure

Controller（APIC）は、一元化されたトラブルシューティング、アプリケーション ヘルス スコア、および仮想化モニタリングを提供します。Cisco ACI マルチハイパーバイザ VM 自動化により、手動構成と手動エラーが削減または排除されます。これにより、仮想化データセンターが多数の VM を信頼性が高く、コスト効率の優れた方法でサポートすることが可能になります。

サポートされている製品とベンダー

Cisco ACI は、次の製品およびベンダーの virtual machine managers（VMM）をサポートします。

- **Cisco Unified Computing System Manager（UCSM）**

  Cisco UCSM の統合は、Cisco Cisco APIC リリース 4.1(1) 以降でサポートされています。詳細については、『*Cisco ACI 仮想化ガイド、リリース 4.1(1)*』の「Cisco ACI と Cisco UCSM の統合」の章を参照してください。

- **Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod)**

  Cisco ACI vPod は、Cisco APIC リリース 4.0(2) 以降で一般に利用可能です。詳細については、Cisco.com で Cisco ACI vPod のマニュアルを参照してください。

- **Cloud Foundry**

  Cloud Foundry と Cisco ACI との統合は、Cisco APIC リリース 3.1(2) 以降でサポートされています。詳細については、Cisco.com のナレッジ ベース記事「Cisco ACI と Cloud Found 統合」を参照してください。

- **Kubernetes**

  詳細については、Cisco.com の ナレッジ ベースの記事、 『Cisco ACI と Kubernetes の統合』を参照してください。

- **Microsoft System Center Virtual Machine Manager（SCVMM）**

  詳細については、Cisco.com の『*Cisco ACI 仮想化ガイド*』の「Microsoft SCVMM を搭載した Cisco ACI」および「Microsoft Windows Azure Pack を搭載した Cisco ACI」の章を参照してください。

- **OpenShift**

  詳細については、Cisco.com の OpenShift のマニュアルを参照してください。

- **Openstack**

  詳細については、Cisco.com の OpenStack のマニュアルを参照してください。

- **Red Hat 仮想化 (RHV)**

  詳細については、Cisco.com のナレッジ ベースの記事、 『Cisco ACI および Red Hat の統合』を参照してください。

- **VMware 仮想分散スイッチ（VDS）**

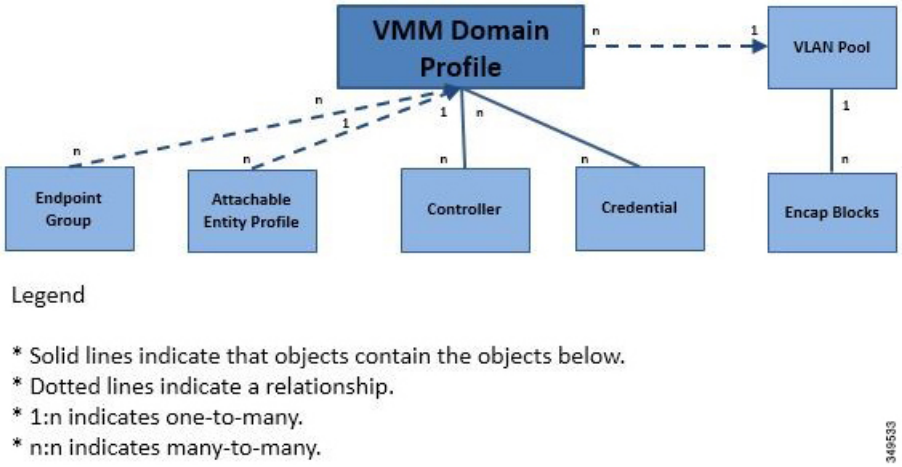
  詳細については、『Cisco ACI 仮想化ガイド』の「Cisco "ACI と VMware VDSの統合」の章を参照してください。

検証済みの相互運用可能な製品の最新のリストについては、『Cisco ACI Virtualization Compatibility Matrix』を参照してください）。

VMM ドメイン ポリシー モデル

VMM ドメイン プロファイル（vmmDomP）は、仮想マシン コントローラが ACI ファブリックに接続できるようにする接続ポリシーを指定します。次の図は、vmmDomP ポリシーの概要を示しています。

図 *96 : VMM* ドメイン ポリシー モデルの概要



Virtual Machine Manager ドメインの主要コンポーネント

ACI ファブリック Virtual Machine Manager（VMM）ドメインにより、管理者は仮想マシン コントローラの接続ポリシーを設定できます。ACI VMM ドメイン ポリシーの基本的なコンポーネントは次のとおりです。

- **Virtual Machine Manager ドメイン プロファイル**：同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。たとえば、VM コントローラは VLAN プールとアプリケーション エンドポイント グループ（EPG）を共有できます。APIC はコントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワーク設定を公開します。VMM ドメイン プロファイルには、次の基本コンポーネントが含まれます。
  - **クレデンシャル**：有効な VM コントローラ ユーザ クレデンシャルを APIC VMM ドメインと関連付けます。
  - **コントローラ**：ポリシーの適用ドメインの一部である VM コントローラへの接続方法を指定します。たとえば、コントローラは VMM ドメインの一部である VMware vCenter への接続を指定します。

（注） 1 つのドメインに VM コントローラの複数のインスタンスを含めることができますが、それらは同じベンダーのものである必要があります（VMware または Microsoft など）。

- **EPG の関連付け**：エンドポイント グループにより、エンドポイント間の接続と可視性が VMM ドメイン ポリシーの範囲内に規制されます。VMM ドメイン EPG は次のように動作します。
  - APIC は、これらの EPG をポート グループとして VM コントローラにプッシュします。
  - 1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。
- **接続可能エンティティ プロファイルの関連付け**：VMM ドメインを物理ネットワーク インフラストラクチャと関連付けます。接続可能エンティティ プロファイル（AEP）は、多数のリーフ スイッチ ポートで VM コントローラ ポリシーを展開するための、ネットワーク インターフェイス テンプレートです。AEP は、使用できるスイッチやポートおよびその設定方法を指定します。
- **VLAN プールの関連付け**：VLAN プールは、VMM ドメインが消費する VLAN カプセル化に使用する VLAN ID または範囲を指定します。

Virtual Machine Manager のドメイン

APIC VMM ドメイン プロファイルは、VMM ドメインを定義するポリシーです。VMM ドメイン ポリシーは APIC で作成され、リーフ スイッチにプッシュされます。

VMM ドメインは以下を提供します。

- 複数の VM コントローラ プラットフォームに対してスケーラブルな耐障害性サポートを可能にする、ACI ファブリックの共通レイヤ
- ACI ファブリック内の複数のテナントに対する VMM サポート

VMM ドメインには、VMware vCenter や Microsoft SCVMM Manager などの VM コントローラと、VM コントローラと対話するための ACI API に必要なクレデンシャルが含まれます。VMM ドメインはドメイン内の VM モビリティを実現できますが、ドメイン間は実現できません。単一の VMM ドメイン コントローラに VM コントローラの複数のインスタンスを含めることはできますが、同じタイプである必要があります。たとえば、1 つの VMM ドメインに、それぞれが複数の VM を実行する複数のコントローラを管理する多くの VMware vCenter を含めることができますが、SCVMM Manager も含めることはできません。VMM ドメインはコントローラ要素（pNIC、vNIC、VM 名など）をインベントリに含め、コントローラにポリシーをプッシュして、ポート グループなどの必要な要素を作成します。ACI VMM ドメインは VM モビリティなどのコントローラ イベントを監視し、状況に応じて応答します。

VMM ドメイン VLAN プールの関連付け

VLAN プールは、トラフィック VLAN ID のブロックを表します。VLAN プールは共有リソースで、VMM ドメインおよびレイヤ 4 ～レイヤ 7 のサービスなど、複数のドメインで使用できます。

各プールには、作成時に定義された割り当てタイプ（静的または動的）があります。割り当てタイプによって、含まれる ID が Cisco APIC で自動割り当てに使用されるか（動的）、管理者によって明示的に設定されるか（静的）が決まります。デフォルトでは、VLAN プールに含まれるすべてのブロックの割り当てタイプはプールと同じですが、ユーザは動的プールに含まれるカプセル化ブロックの割り当てタイプを静的に、また、静的プールに含まれるカプセル化ブロックの割り当てタイプを動的に変更できます。静的割り当てタイプのブロックからのエントリは、動的割り当てから除外されます。

VMM ドメインは、1 つの動的 VLAN プールにのみ関連付けることができます。APIC リリース 6.0(4) 以降、VMware vDS の VMM ドメインは、動的 VLAN プールの代わりに静的 VLAN プールを関連付けることができます。ただし、静的 VLAN プールは、他のタイプの VMM ドメインではサポートされません。デフォルトでは、VMM ドメインに関連付けられた EPG への VLAN ID の割り当ては、Cisco APIC によって動的に行われます。動的割り当てはデフォルトの推奨設定ですが、管理者は代わりにエンドポイント グループ（EPG）に VLAN 識別子を静的に割り当てることができます。この場合、使用する識別子は、VLAN プールの静的割り当てタイプのカプセル化ブロックから選択する必要があります。

物理ワークロードから VM（既存の VLAN プールを使用）に移行する場合は、VMM ドメインが、物理ドメインで使用されているのと同じ VLAN プールを参照するようにすることをお勧めします。レイヤ 4 ～ レイヤ 7 デバイスの場合、デバイスが VMM ドメインを参照している場合、VMM ドメインは動的 VLAN プールを参照する必要があります。

Cisco APIC は、リーフ ポート上の VMM ドメイン VLAN を EPG イベントに基づいてプロビジョニングします（リーフ ポート上の静的バインドまたは VMware vCenter や Microsoft SCVMM などのコントローラからの VM イベントに基づいて）。



（注） 動的 VLAN プールでは、VLAN と EPG の関連付けが解除されると、5 分以内に自動的に EPG に再関連付けされます。

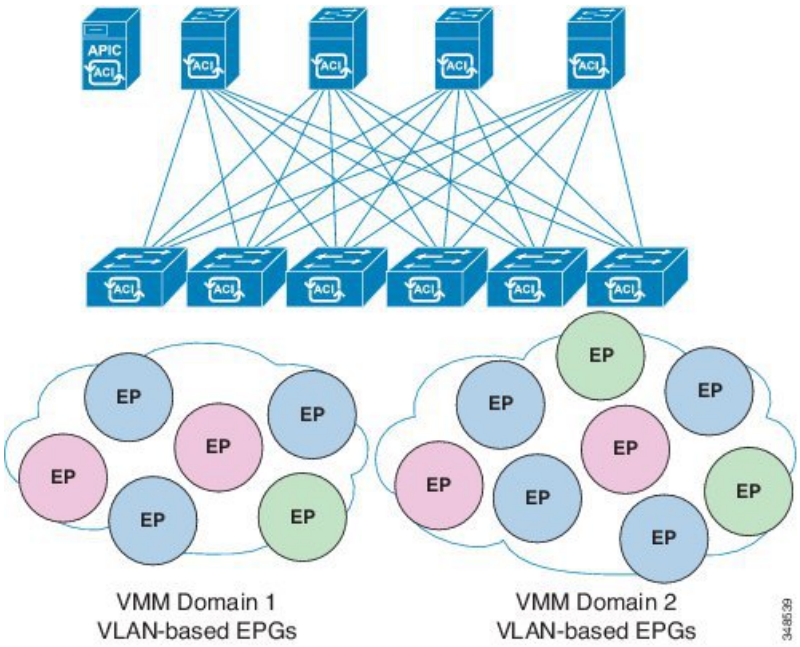


（注） 動的 VLAN 関連付けは構成ロールバックの一部ではありません。つまり、EPG またはテナントが最初に削除され、バックアップから復元された場合、動的 VLAN プールから新しい VLAN が自動的に割り当てられます。

VMM ドメイン EPG の関連付け

Cisco Application Centric Infrastructure（ACI）ファブリックは、テナント アプリケーション プロファイルエンドポイントグループ（EPG）を仮想マシンマネージャ（VMM）ドメインに関連付けます。Cisco ACI では、Microsoft Azure などのオーケストレーション コンポーネントによって自動的に、またはそのような構成を作成する Cisco Application Policy Infrastructure Controller（APIC）管理者によって行われます。1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。

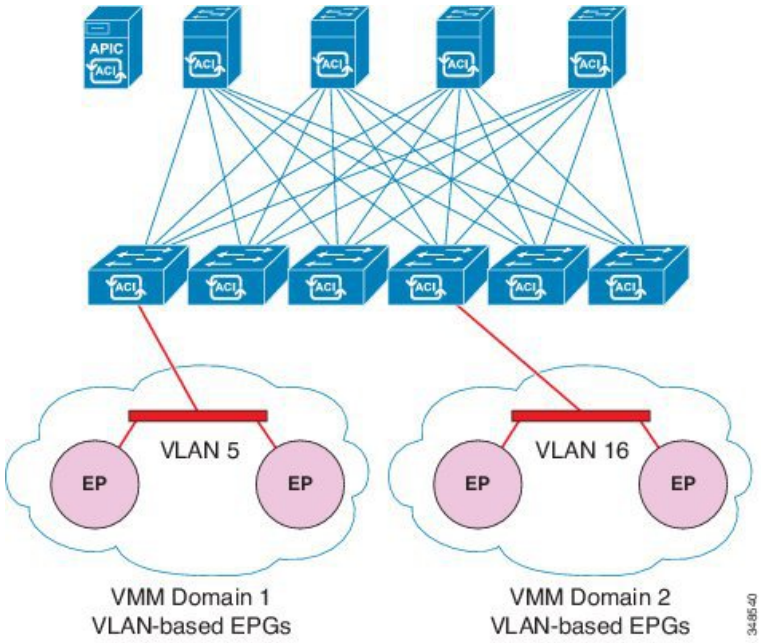
図 *97 : VMM* ドメイン *EPG* の関連付け



前の図では、同じ色のエンド ポイント（EP）が同じ EPG の一部です。たとえば、2 つの異なる VMM ドメインにあるにもかかわらず、すべての緑の EP は同じ EPG にあります。

仮想ネットワークおよび VMM ドメイン EPG の容量情報については、最新の『*Cisco ACI* の検証済みスケーラビリティ ガイド』を参照してください。

図 *98 : VMM* ドメイン *EPG VLAN* の消費



（注） VLAN ID 範囲が重複している複数の VMM ドメインが同じリーフ スイッチに接続されている場合、それらのドメインは同じ VLAN プールを使用する必要があります。同じ VLAN プールを使用すると、 Cisco APIC はドメインと EPG の関連付けごとに異なる VLAN ID を選択できます。そうしないと、 Cisco APIC は、別のドメインと EPG の関連付けのためにスイッチですでに使用されている VLAN ID を選択する可能性があり、これにより VLAN の展開が失敗します。

VLAN ID 範囲が重複する複数の VMM ドメインが同じリーフ スイッチに接続され、それらのドメインが同じ VLAN プールを使用する場合、複数の VMM ドメインを同じ EPG に関連付けることができます。ただし、各ドメインと EPG の関連付けでは、VLAN が同じ EPG 用となり、同じポート上のものとなる可能性があります。それでもそれぞれ異なる VLAN ID を展開します。この方法で VLAN ID を使用することが要件に最適でない場合は、複数の VMM ドメインを使用する代わりに、複数の VMM コントローラで同じ VMM ドメインを使用できます。

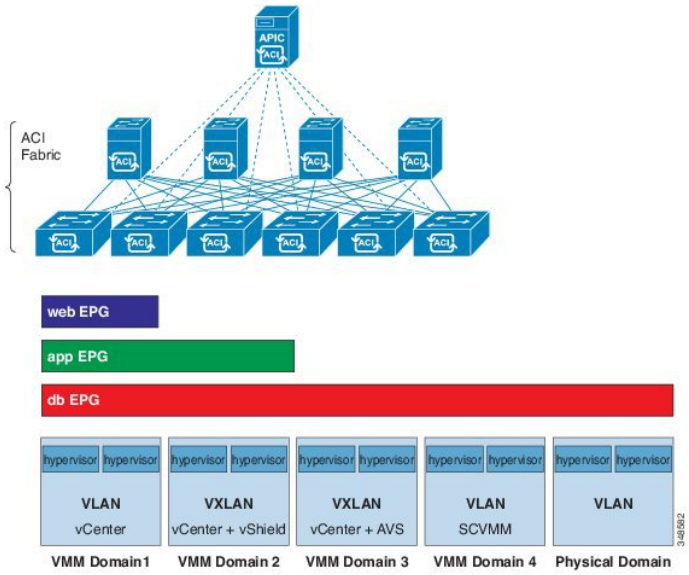
EPG は複数の VMM ドメインを次のように使用できます。

- カプセル化 ID を使用して VMM ドメイン内の EPG が識別されます。Cisco APIC は自動的に ID を管理したり、管理者が静的に選択したりできます。一例は、VLAN、仮想ネットワーク ID（VNID）です。
- EPG は複数の物理ドメイン（baremetal サーバの場合）または仮想ドメインにマッピングできます。各ドメインで異なる VLAN または VNID カプセル化を使用できます。

（注） デフォルトでは、Cisco APIC は EPG の VLAN の割り当てを動的に管理します。VMware DVS 管理者は、EPG に対して特定の VLAN を設定できます。その場合、VLAN は、VMM ドメインに関連付けられているプール内の静的割り当てブロックから選択されます。

アプリケーションは、複数の VMM ドメインに導入できます。

図 *99 :* ファブリック内の複数の *VMM* ドメインと *EPG* の増大



VMM ドメイン内の VM のライブ マイグレーションがサポートされていても、VMM ドメイン間の VM のライブ マイグレーションはサポートされません。

（注） VMM ドメインが関連付けられている EPG にリンクされているブリッジ ドメインで VRF を変更すると、ポート グループが削除され、vCenter に再び追加されます。これにより、EPG が VMM ドメインから展開解除されます。これは想定されている動作です。

トランク ポート グループ

トランク ポート グループを使用して、VMware virtual machine manager (VMM) ドメインのエンドポイント グループ (EPG) のトラフィックを集約します。Cisco Application Policy Infrastructure Controller (APIC) GUI の [テナント (Tenant)] タブで設定されている通常のポート グループとは異なり、[VM ネットワーキング (VM Networking)] タブでトランク ポート グループが設定されます。通常のポート グループは、EPG 名の *T*|*A*|*E* 形式に従います。

同じドメインの EPG の集約は、トランク ポート グループに含まれるカプセル化ブロックとして指定された VLAN の範囲に基づきます。EPG のカプセル化を変更するか、またはトランク

ポート グループのカプセル化ブロックを変更した場合は、EGP を集約する必要があるかどうかを判別するために、集約が再評価されます。

トランク ポート グループは、集約される EPG に割り当てられた VLAN などのネットワーク リソースのリーフ展開を制御します。EPG には、ベース EPG とマイクロセグメント (uSeg) EPG の両方が含まれています。uSeg EPG の場合、トランク ポート グループの VLAN 範囲は、プライマリおよびセカンダリ VLAN の両方を含む必要があります。

EPG ポリシーの解決および展開の緊急度

エンドポイント グループ（EPG）が virtual machine manager（VMM）ドメインに関連付けられるときは常に、管理者は解像度と展開設定を選択して、ポリシーをリーフ スイッチにプッシュするタイミングを指定できます。

解決の緊急性 (Resolution Immediacy)

- 事前プロビジョニング：VM コントローラが仮想スイッチ（例：VMware vSphere 分散スイッチ（VDS））に接続される前でも、ポリシー（例：VLAN、VXLAN バインディング、契約、またはフィルタ）をリーフ スイッチにダウンロードすることを指定します。これにより、スイッチ上の設定が事前プロビジョニングされます。

  「この設定は、ハイパーバイザまたは VM コントローラ用の管理トラフィックに対して、Cisco Application Policy Infrastructure Controller（APIC）VMM ドメインに関連付けられた仮想スイッチ（VMM スイッチ）を使用している状況で役立ちます」

  Cisco Application Centric Infrastructure（ACI）リーフ スイッチで VLAN など VMM ポリシーを展開する場合、Cisco APIC により、VM コントローラおよび Cisco ACI リーフ スイッチを介して両方のハイパーバイザから CDP/LLDP 情報を収集する必要があります。ただし、VM コントローラが同じ VMM ポリシー（VMM スイッチ）を使用してハイパーバイザまたは Cisco APIC と通信することが想定されている場合は、VM コントローラまたはハイパーバイザの管理トラフィックに必要なポリシーがまだ導入されていないため、ハイパーバイザの CDP または LLDP の情報を収集することは絶対にできません。

  事前プロビジョニングを直ちに使用する場合、ポリシーは、CDP/LLDP のネイバーシップには関係なく、Cisco ACI リーフ スイッチにダウンロードされます。VMM スイッチに接続されているハイパーバイザ ホストがない場合でも可能です。

- 即時：EPG ポリシー（契約およびフィルタを含む）が、DVS への ESXi ホスト接続時に関連するリーフ スイッチ ソフトウェアにダウンロードされることを指定します。VM コントローラ/リーフ ノード接続を解決するために LLDP または OpFlex 権限が使用されます。

  VMM スイッチにホストを追加すると、ポリシーがリーフにダウンロードされます。ホストからリーフへの CDP または LLDP のネイバーシップが必要です。

- オンデマンド：ESXi ホストが DVS に接続され、VM がポート グループに配置されるときにのみ、ポリシー（例：VLAN, VXLAN バインディング、契約、またはフィルタ）がリーフ ノードにプッシュされることを指定します。

VMM スイッチにホストが追加されると、ポリシーがリーフにダウンロードされます。VM はポート グループ（EPG）に配置する必要があります。ホストからリーフへの CDP または LLDP のネイバーシップが必要です。

即時とオンデマンドの両方において、ホストおよびリーフが LLDP または CDP のネイバーシップを失うと、ポリシーは削除されます。



（注） OpFlex ベースの VMM ドメインでは、ハイパーバイザの OpFlex エージェントが、EPG への VM/EP 仮想ネットワーク インターフェイス カード（vNIC）の接続をリーフ OpFlex プロセスに報告します。オンデマンド即時解決を使用する場合、次の条件に当てはまる場合、EPG VLAN/VXLAN は**すべて**のリーフ ポート チャネル ポート、仮想ポート チャネル ポート、またはその両方でプログラムされます。

- ハイパーバイザは、直接またはブレードスイッチを介して接続されたポート チャネルまたは仮想ポート チャネルのリーフに接続されます。
- VM またはインスタンス vNIC が EPG に接続されています。
- ハイパーバイザは、EPG または VMM ドメインの一部として接続されます。

Opflex ベースの VMM ドメインは、Microsoft Security Center Virtual Machine Manager（SCVMM）と HyperV、および Cisco Application Virtual Switch（AVS）です。

展開の緊急性

ポリシーがリーフ ソフトウェアにダウンロードされると、展開の緊急度によってポリシーをいつハードウェア ポリシーの Content-Addressable Memory (CAM) にプッシュするかを指定できます。

- 即時：リーフ ソフトウェアにダウンロードされたポリシーがハードウェアのポリシー CAM ですぐにプログラミングされるように指定します。
- オンデマンド：最初のパケットがデータ パス経由で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラミングされるように指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。

（注） オン デマンドの緊急性指定と MAC 固定の VPC の両方を使用する場合、 最初のエンドポイントがリーフごとのEPGを学習するまでは、EPGコントラクトはリーフの三重Content-Addressable Memory (TCAM) にプッシュされません。このような場合、VPC ピア間での TCAM 使用率が不均一になる可能性があります。(通常、コントラクトは両方の両方のピアにプッシュされます)。

VMM ドメインを削除するためのガイドライン

次の手順に従って、VMM ドメインを自動的に削除する APIC リクエストによって関連する VM コントローラ（VMware vCenter または Microsoft SCVMM）がトリガーされ、プロセスが正常に完了すること、および ACI ファブリックに孤立した EPG が残されないことを確認します。

1. VM 管理者は、APIC によって作成されたすべての VM を、ポート グループ（VMware vCenter の場合）または VM ネットワーク（SCVMM の場合）からデタッチする必要があります。

   Cisco AVS の場合、VM 管理者は Cisco AVS に関連付けられている vmk インターフェイスも削除する必要があります。

2. ACI 管理者は、APIC で VMM ドメインを削除します。APIC は、VMware VDS または Cisco AVS または SCVMM 論理スイッチおよび関連するオブジェクトの削除をトリガーします。

（注） VM管理者が仮想スイッチまたは関連オブジェクト（ポートグループまたはVMネットワークなど）を削除することはできません。上記のステップ 2 の完了時に、APIC に仮想スイッチの削除を許可します。VMM ドメインが APIC で削除される前に VM 管理者が VM コントローラから仮想スイッチを削除した場合、EPG は APIC で孤立する可能性があります。

このシーケンスに従わない場合、VM コントローラは APIC VMM ドメインに関連付けられている仮想スイッチを削除します。このシナリオでは、VM 管理者は VM コントローラから VM および vtep アソシエーションを手動で削除してから、以前に APIC VMM ドメインに関連付けられていた仮想スイッチを削除します。



第 10 章

レイヤ 4 ～ レイヤ 7 のサービスの挿入

この章は、次の内容で構成されています。

- レイヤ 4 ～ レイヤ 7 のサービスの挿入 （279 ページ）
- レイヤ 4 ～ レイヤ 7 のポリシー モデル （280 ページ）
- サービス グラフについて （280 ページ）
- ポリシーベースのリダイレクトについて （282 ページ）
- 自動サービス挿入 （285 ページ）
- デバイス パッケージについて （285 ページ）
- デバイス クラスタについて （288 ページ）
- デバイス マネージャとシャーシ マネージャについて （290 ページ）
- 具象デバイスについて （293 ページ）
- 機能ノードについて （294 ページ）
- 機能ノード コネクタについて （294 ページ）
- 端末ノードについて （295 ページ）
- 権限について （295 ページ）
- サービスの自動化と構成管理 （295 ページ）
- サービス リソースのプーリング （296 ページ）

レイヤ 4 ～ レイヤ 7 のサービスの挿入

Cisco Application Policy Infrastructure Controller（APIC）は、ネットワーク サービスを管理します。ポリシーは、サービスを挿入するために使用されます。APIC のサービスを統合することでライフサイクルの自動化フレームワークが確立され、サービスがオンラインまたはオフラインになった場合に、システムが動的に対応できるようになります。ファブリック全体で使用可能な共有サービスは、ファブリックの管理者によって管理されます。単一のテナント向けのサービスは、テナントの管理者によって管理されます。

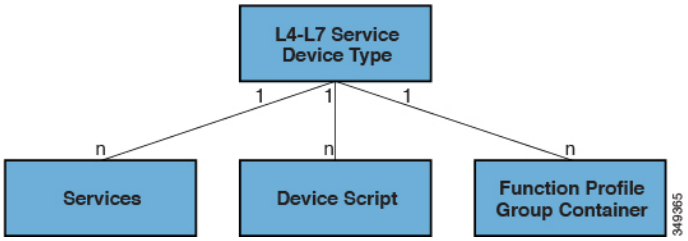
APIC は、ポリシー制御の中心点として機能すると同時に、自動サービス挿入を提供します。APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。また、APIC はアプリケーション要件に従ってサービスを自動的に構成できます。

このアプローチにより、組織はサービス挿入を自動化し、従来のサービス挿入の複雑なすべてのトラフィック誘導技術の管理に伴う課題を排除できます。

レイヤ 4 ～ レイヤ 7 のポリシー モデル

レイヤ 4 ～ レイヤ 7 のサービス デバイス タイプ ポリシーには、パッケージおよびデバイス スクリプトでサポートされるサービスなどの主要な管理対象オブジェクトが含まれます。次の図は、レイヤ 4 ～ レイヤ 7 のサービス デバイス タイプ ポリシー モデルのオブジェクトを示します。

図 *100* : レイヤ *4* ～ レイヤ *7* のポリシー モデル



レイヤ 4 ～ レイヤ 7 のサービス ポリシーには次のものが含まれます。

- **サービス**：SSL オフロードやロードバランシングなどのデバイスによって提供されるすべての機能のメタデータが含まれます。この MO には、コネクタの名前、VLAN や VXLAN などのカプセル化のタイプ、およびインターフェイス ラベルが含まれます。
- **デバイス スクリプト**：名前、パッケージ名、バージョンなどのスクリプト ハンドラの関連属性に関するメタ情報を含むデバイス スクリプト ハンドラを表します。
- **機能プロファイル グループ コンテナ**：サービス デバイス タイプで使用可能な機能を含むオブジェクト。機能プロファイルには、フォルダに編成されたデバイスでサポートされる構成可能なすべてのパラメータが含まれます。

サービス グラフについて

Cisco Application Centric Infrastructure（ACI）はアプリケーションの重要部分としてサービスを見なします。必要なサービスは、Cisco Application Policy Infrastructure Controller（APIC）からの Cisco ACI ファブリックでインスタンス化されたサービス グラフとして処理されます。ユーザは、アプリケーションに対してサービスを定義し、サービス グラフはアプリケーションが必要とする一連のネットワークまたはサービス機能を識別します。

サービス グラフは、次の要素を使ってネットワークを表します。

- 機能ノード：機能ノードは、トランスフォーム（SSL ターミネーション、VPN ゲートウェイ）、フィルタ（ファイアウォール）、または端末（侵入検知システム）など、トラフィックに適用される機能を表します。サービス グラフ内の 1 つの機能は 1 つ以上のパラメータを必要とし、1 つまたは複数のコネクタを持っている場合があります。

- 端末ノード：端末ノードはサービスグラフからの入出力を有効にします。
- コネクタ：コネクタはノードからの入出力を有効にします。
- 接続：接続によって、ネットワーク経由でトラフィックを転送する方法が決定されます。

グラフが Cisco APIC に設定されると、Cisco APIC はサービス グラフに明記されたサービス機能の要件に従って、サービスを自動的に設定します。Cisco APIC はまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定しますが、これによってサービス デバイスでの変更は要求されません。

サービス グラフは、アプリケーションの複数の階層として表され、適切なサービス機能が間に挿入されます。

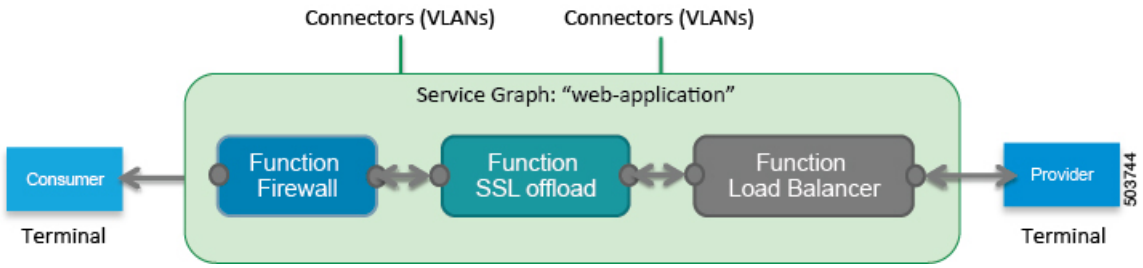
サービス アプライアンス（デバイス）は、グラフ内でサービス機能を実行します。1 つ以上のサービス アプライアンスが、グラフに必要なサービスをレンダリングするために必要になることがあります。1 つ以上のサービス機能が単一のサービス デバイスで実行できます。

サービス グラフおよびサービス機能には、次の特性があります。

- エンドポイント グループで送受信されたトラフィックはポリシーに基づいてフィルタリングでき、トラフィックのサブセットはグラフ内の異なるエッジにリダイレクトできます。
- サービス グラフのエッジには方向性があります。
- タップ（ハードウェア ベースのパケット コピー サービス）は、サービス グラフの異なるポイントに接続できます。
- 論理機能は、ポリシーに基づいて適切な（物理または仮想）デバイスでレンダリングできます。
- サービス グラフでは、エッジの分割と結合がサポートされ、管理者は線形サービス チェーンに制限されません。
- トラフィックは、サービス アプライアンスが発信した後にネットワーク内で再度分類できます。
- 論理サービス機能は、要件に応じて、拡張や縮小が可能で、クラスタ モードまたは 1:1 アクティブ/スタンバイ ハイアベイラビリティ モードで展開できます。

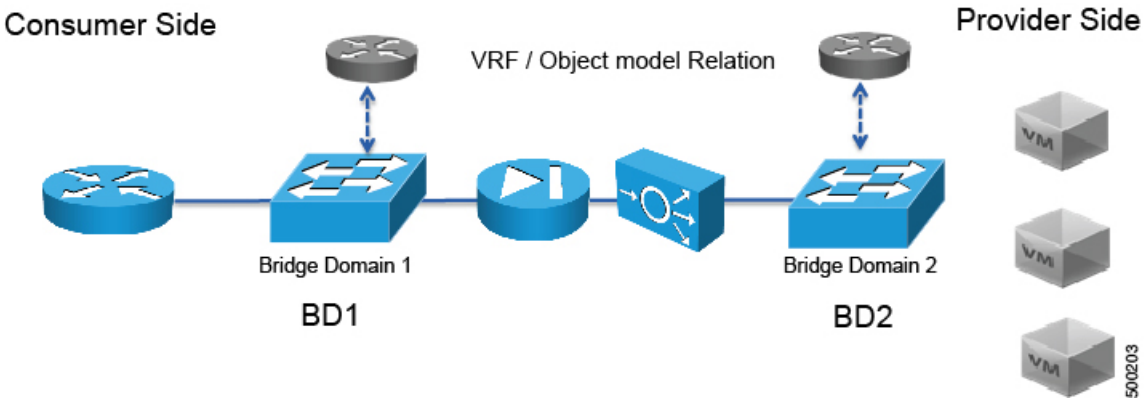
次の図は、サービスグラフの導入の例を示しています:

図 *101* : サービス グラフの展開の例



サービスグラフを展開するには、次の図に示すようにブリッジドメインと VRF インスタンスが必要です。

図 *102*：サービスグラフのブリッジドメインと *VRF* インスタンス



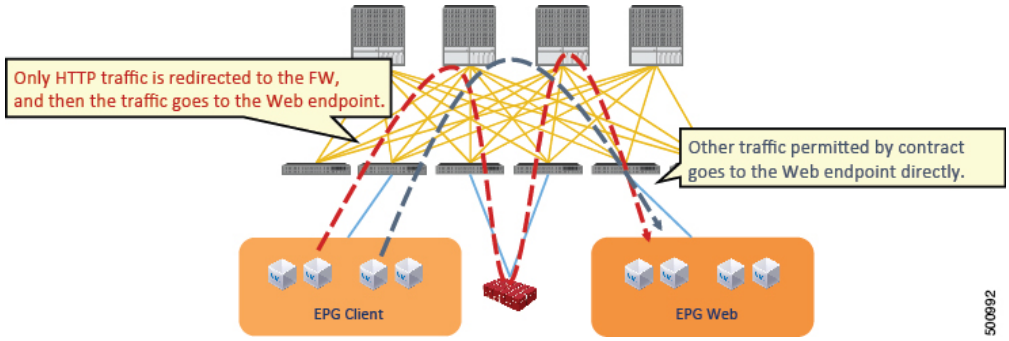
（注） 使用すると、その他のテナント内のエンドポイント グループに関連付けられているサービス グラフの脚の一部があるかどうか、 **グラフ テンプレートの関連のオブジェクトを削除** GUI で、機能、 Cisco APIC 以外のテナントからインポートされた契約は削除されませんサービス グラフが存在します。Cisco APICもサービス グラフよりも異なるテナントにあるエンドポイント グループ契約のクリーニングはありません。手動で異なるテナントではこれらのオブジェクトを削除する必要があります。

ポリシーベースのリダイレクトについて

Cisco Application Centric Infrastructure (ACI) ポリシーベースリダイレクト (PBR) により、ファイアウォールやロードバランサなどのサービスアプライアンスをプロビジョニングできます。一般的な使用例としては、プールしてアプリケーションプロファイルに合わせて調整すること、また容易にスケーリングすることができ、サービス停止の問題が少ないサービスアプライアンスのプロビジョニングがあります。PBR により、プロビジョニングするコンシューマおよびプロバイダー エンドポイント グループをすべて同じ仮想ルーティングおよび転送（VRF）インスタンスに含めることで、サービス アプライアンスの展開をシンプル化できます。PBR の導入は、ルート リダイレクト ポリシーおよびクラスタのリダイレクト ポリシーの設定と、ルーティングとクラスタ リダイレクト ポリシーを使用するサービス グラフ テンプレートの作成から構成されます。サービス グラフ テンプレートを展開した後は、サービス グラフ プロバイダーのエンドポイント グループを利用するためにエンドポイント グループを有効にすることにより、サービス アプライアンスを使用します。これは、vzAny を使用することにより、さらに簡素化し、自動化できます。パフォーマンスの要件が、専用のサービス アプライアンスをプロビジョニングするかどうかを決定するものとなるのに対し、PBR を使用すれば、仮想サービス アプライアンスの展開も容易になります。

次の図は、ファイアウォールへのトラフィックに固有の、リダイレクトの使用例を示しています:

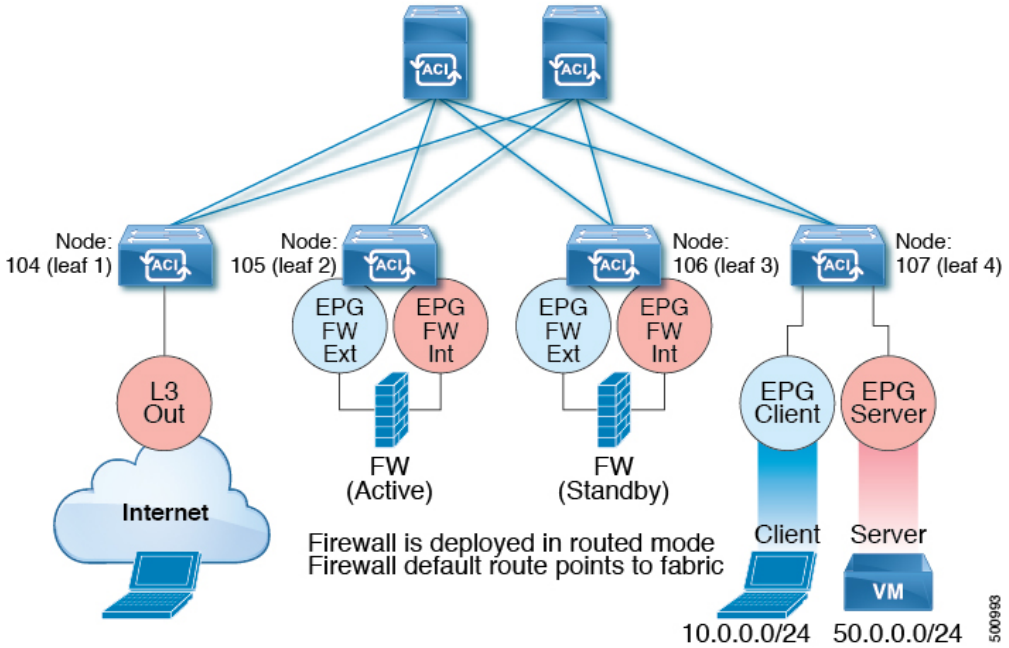
図 *103* : 使用例: ファイアウォール特有のトラフィックのリダイレクト



この使用例では、2つの情報カテゴリを作成する必要があります。最初の情報カテゴリはHTTPトラフィックを許可します。その後このトラフィックはファイアウォールにリダイレクトされます。トラフィックはファイアウォールを通過してから、Webエンドポイントに送られます。2 番目の情報カテゴリはすべてのトラフィックを許可します。これは最初の情報カテゴリではリダイレクトされなかったトラフィックをキャプチャします。トラフィックはそのまま Web エンドポイントに送られます。

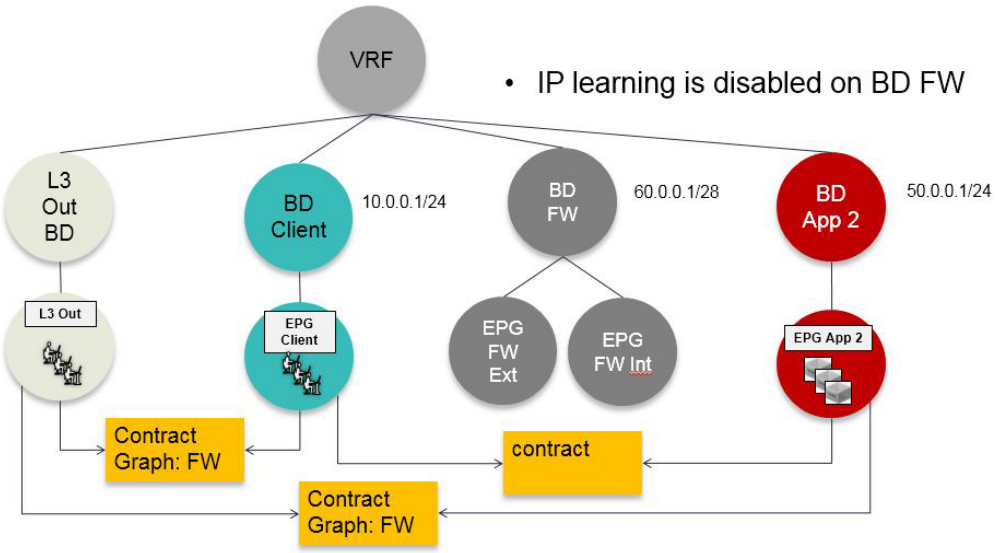
次の図は、ACI PBR 物理トポロジのサンプルを示しています:

図 *104* : サンプルの *ACI PBR* 物理トポロジ



次の図は、ACI PBR 論理トポロジのサンプルを示しています:

図 *105* : サンプルの *ACI PBR* 論理トポロジ



これらの例はシンプルな導入ですが、 ACI PBR は、ファイアウォールやサーバのロード バランサなどのような、複数のサービスのために物理および仮想サービス アプライアンスの両方を混在させたものにスケールアップすることを可能にします。

対称ポリシー ベースのリダイレクトについて

対称ポリシーベースリダイレクト(PBR)構成により、サービスノードのプールをプロビジョニングできるため、ポリシーに基づき、コンシューマーとプロバイダーのエンドポイントグループ間のトラフィックを負荷分散できます。トラフィックは、送信元および宛先 IP 等価コスト マルチパス ルーティング(ECMP)プレフィックス ハッシュに応じて、プール内のサービス ノードの 1 つにリダイレクトされます。

（注） 対称 PBR 構成には、9300-EX 以降のハードウェアが必要です。

対称 PBR REST のサンプルの例を以下に示します。

```
Under fvTenant svcCont

<vnsSvcRedirectPol name="LoadBalancer_pool">
          <vnsRedirectDest name="lb1" ip="1.1.1.1" mac="00:00:11:22:33:44"/>
          <vnsRedirectDest name="lb2" ip="2.2.2.2" mac="00:de:ad:be:ef:01"/>
          <vnsRedirectDest name="lb3" ip="3.3.3.3" mac="00:de:ad:be:ef:02"/>
</vnsSvcRedirectPol>

<vnsLIfCtx name="external">
          <vnsRsSvcRedirectPol tnVnsSvcRedirectPolName="LoadBalancer_pool"/>
          <vnsRsLIfCtxToBD tDn="uni/tn-solar/bd-fwBD">
</vnsLIfCtx>

<vnsAbsNode name="FW" routingMode="redirect">
```

対称 PBR NX-OS スタイルの CLI コマンドの例を次に示します。

テナント スコープの下の次のコマンドは、サービス リダイレクト ポリシーを作成します。

```
apic1(config-tenant)# svcredir-pol fw-external
apic1(svcredir-pol)# redir-dest 2.2.2.2 00:11:22:33:44:56
```

次のコマンドは PBR を有効にします。

```
apic1(config-tenant)# l4l7 graph FWOnly contract default
apic1(config-graph)# service FW svcredir enable
```

次のコマンドは、デバイス選択ポリシー コネクタの下にリダイレクト ポリシーを設定します。

```
apic1(config-service)# connector external
apic1(config-connector)# svcredir-pol tenant solar name fw-external
```

自動サービス挿入

VLANおよび仮想ルーティングおよび転送（VRF）スイッチングは、従来のサービス挿入モデルによってサポートされますが、Application Policy Infrastructure Controller（APIC）はポリシー制御の中心点として機能する一方で、サービス挿入とセキュアソケットレイヤ（SSL）オフロード、サーバ ロード バランシング（SLB）、Web アプリケーション ファイアウォール（WAF）およびファイアウォールなどのネットワーク サービスのプロビジョニングを自動化できます。ネットワーク サービスは通常、Application Delivery Controller（ADC）やファイアウォールなどのサービス アプライアンスによってレンダリングされます。APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。APICは、アプリケーション要件に従ってサービスを自動的に設定することもでき、それにより組織はサービス挿入を自動化し、従来のサービス挿入の複雑な技術の管理に伴う課題を排除できます。

デバイス パッケージについて

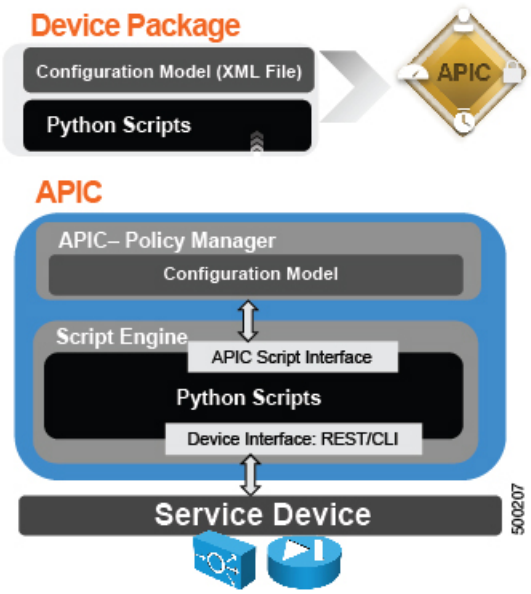
Application Policy Infrastructure Controller（APIC）は、サービス デバイスの設定およびモニタリングにデバイス パッケージを必要とします。Cisco APIC にサービスの機能を追加するには、デバイス パッケージを使用します。デバイス パッケージは、単一クラスのサービス デバイスを管理し、デバイスとその機能に関する情報を Cisco APIC に提供します。デバイス パッケージは次の項目を含む `zip` ファイルです。

デバイス仕様	次を定義する XML ファイル： • デバイス プロパティ： • **[Model]**：デバイスのモデル。 • **[Vendor]**：デバイスのベンダー。 • **[Version]**：デバイスのソフトウェア バージョン。 • ロード バランシング、コンテンツ切り替え、および SSL 終端などの、デバイスによって提供される機能。 • 各機能のインターフェイスおよびネットワーク接続情報。 • デバイス設定パラメータ。 • 各機能の設定パラメータ。
デバイス スクリプト	Cisco APIC とデバイスのやりとりに使用される Python スクリプト。Cisco APIC イベントは、デバイス スクリプトで定義した機能呼び出しにマッピングされます。デバイス パッケージには、複数のデバイス スクリプトを含めることができます。デバイス スクリプトは、REST、SSH、または、同様のメカニズムを使用して、デバイスと連携できます。
機能プロファイル	ベンダーによって指定されたデフォルト値を持つ機能パラメータ。これらのデフォルト値を使用するように機能を設定できます。
デバイス レベル設定パラメータ	デバイスに必要なパラメータを指定するコンフィギュレーション ファイル。この設定は、デバイスを使用している 1 つ以上のグラフで共有できます。

デバイス パッケージを作成できます。または、デバイス ベンダーか Cisco によって提供されるものを使用できます。

次の図では、デバイス パッケージと Cisco APIC の関係について説明します:

図 *106* : デバイス パッケージと、*Cisco APIC*

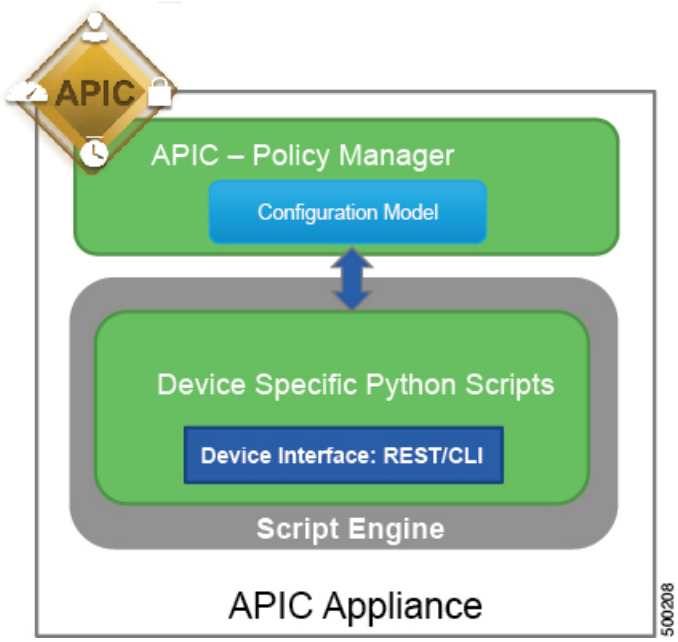


デバイスのスクリプトでの機能は、次のカテゴリに分類されます。

- デバイス/インフラストラクチャ：デバイス レベルの設定とモニタリングを行うため
- サービス イベント：デバイス上でサーバのロード バランサまたはセキュア ソケット レイヤなどの機能を設定するため
- エンドポイント/ネットワーク イベント：エンドポイントとネットワークの接続/接続解除イベントを処理するため

Cisco APIC は、デバイス パッケージで提供されたデバイス構成モデルを使用して、デバイス スクリプトに適切な構成を渡します。デバイス スクリプト ハンドラは、REST または CLI インターフェイスを使用してデバイスと連解します。

図 *107* : デバイス スクリプトがサービス デバイスと連携する方法



デバイス パッケージにより、管理者は次のサービスの管理を自動化することができます。

- デバイスの接続と切断
- エンドポイントの接続と切断
- サービス グラフのレンダリング
- ヘルス モニタリング
- アラーム、通知、ロギング
- カウンタ

デバイス パッケージとデバイス パッケージを作成する方法の詳細については、『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』を参照してください。

デバイス クラスタについて

デバイス クラスタ（別名論理デバイス）は、単一のデバイスとして機能する 1 つ以上の具象デバイスです。デバイス クラスタには、そのデバイス クラスタのインターフェイス情報を説明するクラスタ（論理）インターフェイスがあります。サービス グラフ テンプレートのレンダリング時に、機能ノード コネクタはクラスタ（論理）インターフェイスに関連付けられます。Application Policy Infrastructure Controller（APIC）は、サービス グラフ テンプレートのインスタンス化およびレンダリング時に機能ノード コネクタにネットワーク リソース（VLAN）を割り当て、クラスタ（論理）インターフェイスにネットワーク リソースをプログラミングします。

Cisco APIC では、グラフのインスタンス化時にサービスグラフに対してネットワークリソースのみを割り当てて、ファブリック側のみをプログラミングできます。この動作は、既存のオーケストレータまたはデバイスクラスタ内のデバイスをプログラムする dev-op ツールがすでにある環境では有効です。

Cisco APIC はデバイス クラスタおよびデバイスのトポロジ情報 （論理インターフェイスと具象インターフェイス） を把握する必要があります。この情報により、Cisco APIC はリーフスイッチの適切なポートをプログラミングできます。また、Cisco APIC ではこの情報をトラブルシューティング ウィザードの目的で使用できます。さらに、Cisco APIC はカプセル化の割り当てに使用する `DomP` との関係も把握する必要があります。

デバイス クラスタまたは論理デバイスは、物理デバイスまたは仮想デバイスのいずれかです。デバイス クラスタは、そのクラスタの一部である仮想マシンが、VMM ドメインを使用して Cisco APIC と統合されたハイパーバイザ上に存在する場合、仮想と見なされます。これらの仮想マシンが VMM ドメインの一部ではない場合、仮想マシン インスタンスであっても物理デバイスとして扱われます。

（注） 論理デバイスには、VMware VMM ドメインまたは SCVMM VMM ドメインのみを使用できます。

次の設定が必要です。

- 論理デバイス（`vnsLDevViP`）およびデバイス（`CDev`）の接続情報
- サポートする機能タイプ（go-through、go-to、L1、L2）に関する情報

サービス グラフ テンプレートは、管理者が定義するデバイス選択ポリシー（論理デバイス コンテキストと呼ばれます）に基づく特定のデバイスを使用します。

管理者は、アクティブ/スタンバイ モードで最大2つの具象デバイスをセットアップできます。

デバイス クラスタをセットアップするには、次のタスクを実行する必要があります。

1. ファブリックに具象デバイスを接続します。
2. Cisco APIC を使用してデバイス クラスタを構成します。

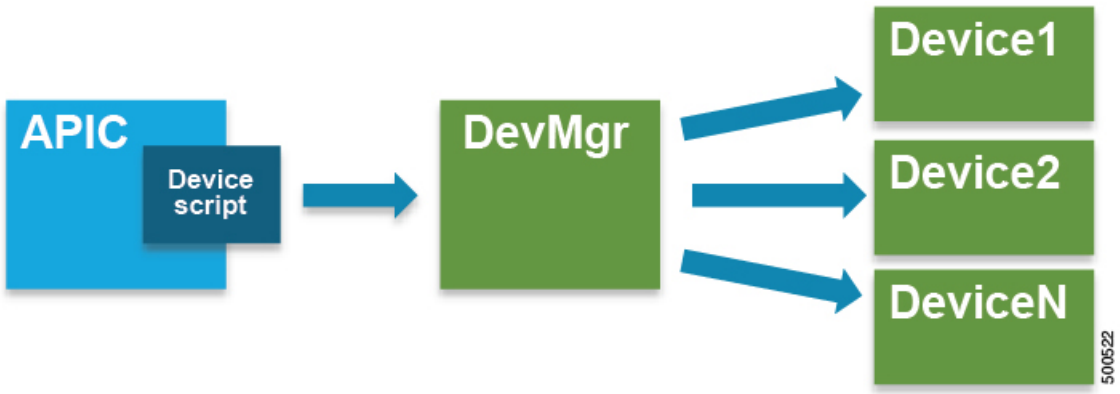
（注） Cisco APIC は、2 つのデバイスのクラスタに IP アドレスが重複して割り当てられているかどうかを検証しません。Cisco APIC は、2 つのデバイスのクラスタが同じ管理 IP アドレスを持っている場合、不適切なデバイスのクラスタをプロビジョニングすることがあります。デバイス クラスタで IP アドレスが重複している場合には、いずれかのデバイスの IP アドレスの設定を削除し、管理 IP アドレスの設定のためにプロビジョニングされた IP アドレスが重複していないことを確認してください。

デバイス マネージャとシャーシ マネージャについて

デバイス マネージャのみで、Cisco Application Centric Infrastructure（ACI）ファブリック内の一連のクラスタを設定できます。管理状態または動作状態はデバイスのネイティブの GUI に表示されます。デバイス マネージャが個々のデバイスの設定を処理するため、Application Policy Infrastructure Controller（APIC）での設定をシンプル化できます。デバイス マネージャにテンプレートを作成してから、APIC のインスタンス固有の値をデバイス マネージャに入力しますが、必要な値はごくわずかです。

次の図に、クラスタ内で複数のデバイスを制御するデバイス マネージャを示します。

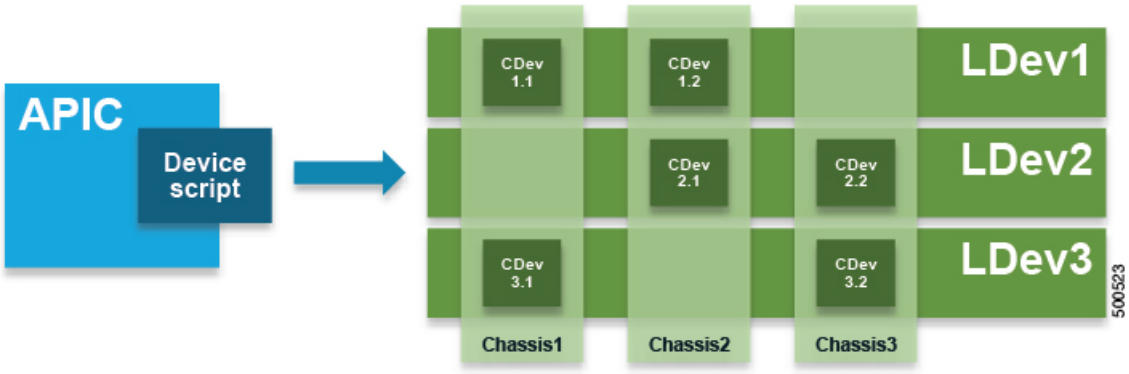
図 *108* : デバイス マネージャでのデバイスの制御



シャーシ マネージャは、処理リソースの物理または仮想「コンテナ」です。シャーシ マネージャは CDev オブジェクトとして表される、いくつかの仮想サービス デバイスをサポートします。シャーシマネージャがネットワーキングを処理し、CDev がプロセスを処理します。シャーシマネージャによって、仮想処理ノードのオンデマンド作成が可能になります。仮想デバイスでは、サービス（特に VLAN）の一部を、仮想マシンではなく、シャーシに適用する必要があります。これを実現するには、シャーシ管理 IP アドレスとクレデンシャルをコールアウトに含める必要があります。

次の図に、処理リソースのコンテナとして機能するシャーシ マネージャを示します。

図 *109* : デバイス マネージャでのデバイスの制御

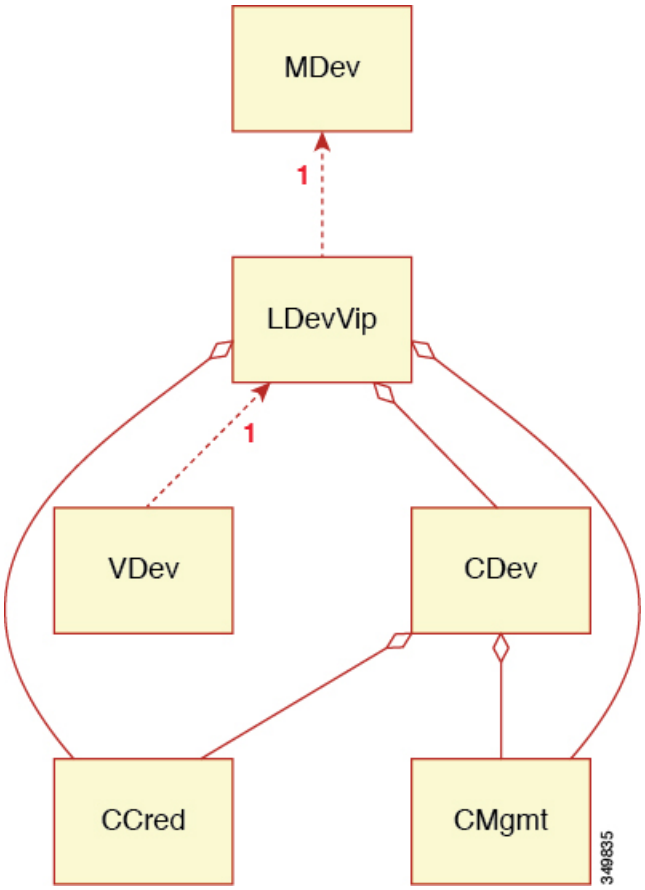


デバイス マネージャまたはシャーシ マネージャを使用せず、サービス デバイスのモデルに次の主要な管理対象オブジェクトを含めます。

- `MDev`：デバイス タイプ（ベンダー、モデル、バージョン）を表します。
- `LDevVIP`：クラスタ、つまりCold Standbyを実現するために同一に設定された一連のデバイスを表します。デバイスにアクセスするための `CMgmt` と `CCred` が含まれます。
- `CDev`：物理または仮想のいずれかのクラスタのメンバーを表します。デバイスにアクセスするための `CMgmt` と `CCred` が含まれます。
- `VDev`：サーバ上の仮想マシンと同様のクラスタのコンテキストを表します。

次の図に、`CMgmt`（管理接続）と `CCred`（クレデンシャル）が含まれた、主要な管理対象オブジェクトのモデルを示します。

図 *110* : デバイス マネージャまたはシャーシ マネージャを含まない管理対象オブジェクト モデル



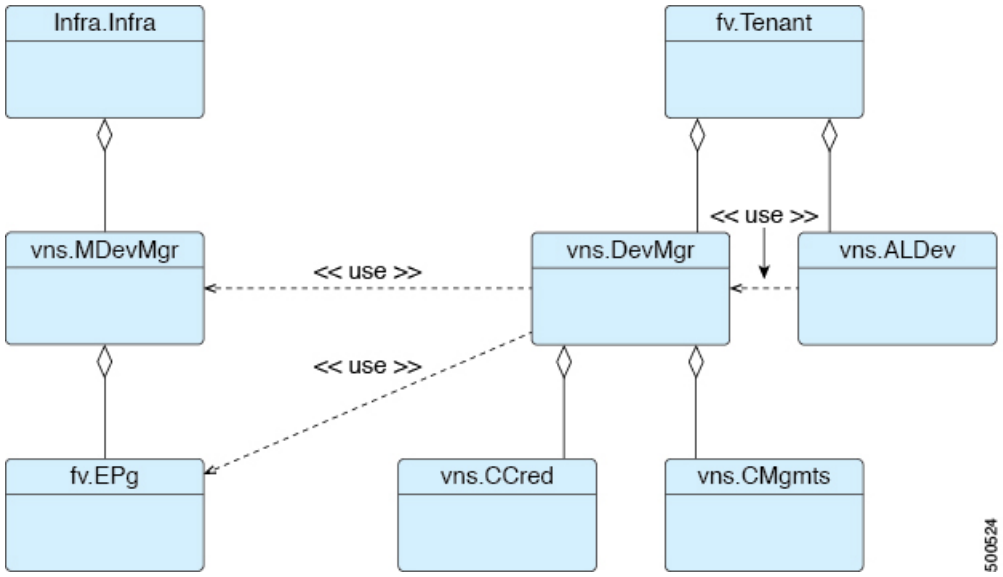
CMgmt（ホスト＋ポート）と CCred（ユーザ名＋パスワード）により、スクリプトでデバイスとクラスタにアクセスできます。

デバイス マネージャとシャーシ マネージャは、集中管理ステーションからのクラスタとデバイスの設定を制御できるようにします。シャーシは並列階層を MDev オブジェクトと ALDev オブジェクトに追加し、特定のシャーシに属しているというタグを CDev オブジェクトに付けることができます。次の管理対象オブジェクトがモデルに追加され、デバイスおよびシャーシマネージャの概念をサポートします。

- MDevMgr：デバイス マネージャのタイプを表します。MDevMgr は、同じベンダーの通常は異なる製品である一連の異なる MDev を管理できます。
- DevMgr：デバイス マネージャを表します。マネージャにアクセスするには、含まれている CMgmt と CCred の管理対象オブジェクトを使用します。各クラスタは 1 つの DevMgr のみと関連付けることができます。
- MChassis：シャーシのタイプを表します。通常、この管理対象デバイスはパッケージに含まれています。
- Chassis：シャーシ インスタンスを表します。これには、CMgmt と CCred[Secret] の管理対象オブジェクトが含まれており、シャーシへの接続を提供します。

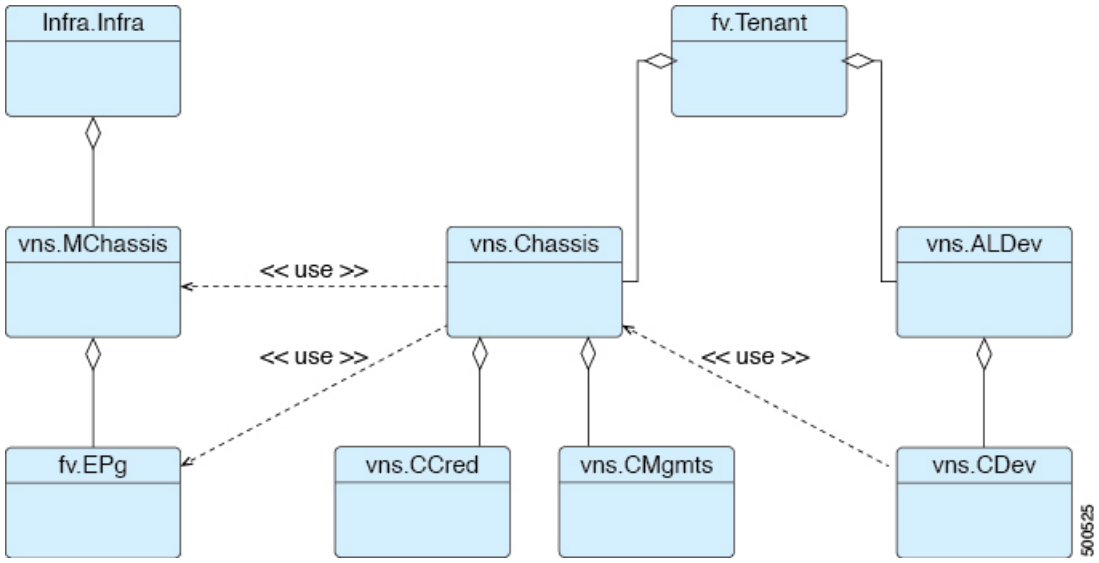
次の図に、デバイス マネージャのオブジェクト モデルを示します。

図 *111* : デバイス マネージャのオブジェクト モデル



次の図に、シャーシ マネージャのオブジェクト モデルを示します。

図 *112* : シャーシ マネージャのオブジェクト モデル



具象デバイスについて

具象デバイスとしては、物理デバイスと仮想デバイスがあり得ます。デバイスが仮想デバイスの場合は、コントローラ（vCenter または SCVMM コントローラ）と仮想マシン名を選択する必要があります。具象デバイスには、具象インターフェイスがあります。具象デバイスが論理

デバイスに追加されると、具象インターフェイスが論理インターフェイスにマッピングされます。サービス グラフ テンプレートのインスタンス化時に、VLAN および VXLAN は、論理インターフェイスとの関連付けに基づいた具象インターフェイス上でプログラミングされます。

機能ノードについて

機能ノードは、単一のサービス機能を表します。機能ノードには、サービス機能のネットワーク要件を表す機能ノード コネクタがあります。

Cisco Application Policy Infrastructure Controller (APIC) は、ネットワークリソースを割り当てて、ファブリック側で VLAN/VXLAN のプログラミングのみを実行します。

次の設定は必要ありません。

- `MFunc` の関係
- サポートされる機能タイプ（go-through、go-to）に関する情報

Cisco APIC は、機能ノードのネットワーク情報（LIF、CIF）を把握する必要があります。この情報は、Cisco APIC がリーフスイッチでネットワークを適切にプログラムするためと、Cisco APIC がこの情報をトラブルシューティング ウィザードの目的で使用するために必要です。

さらに、次の設定が必要です。

- グラフ インスタンス化時に `LDevVip` の選択を可能にする `LDevCtx`
- グラフ インスタンス化時に `LIf` の選択を可能にする `LIfCtx`
- `LIfCtx` 内のブリッジ ドメイン
- `LIfCtx` でのルート ピアリング
- `LIfCtx` 内のサブネット



（注） Cisco ACI マルチサイト 構成の場合、サービスグラフに最大 2 つのノードを展開できます。非 Cisco ACI マルチサイト 構成の場合、サービスグラフに最大 5 つのノードを展開できます。

機能ノード コネクタについて

機能ノード コネクタは、サービス グラフに機能ノードを接続し、グラフのコネクタ サブネットに基づいて適切なブリッジ ドメインと接続と関連付けられます。各コネクタは、VLAN または Virtual Extensible LAN（VXLAN）に関連付けられます。コネクタの両側がエンドポイント グループ（EPG）として扱われ、ホワイトリストがスイッチにダウンロードされ、2 つの機能ノード間の通信がイネーブルになります。

端末ノードについて

端末ノードはサービス グラフとコントラクトを接続します。コントラクトに端末ノードを接続することにより、2台のアプリケーションエンドポイントグループ（EPG）間のトラフィックにサービス グラフを挿入できます。接続されると、コントラクトのコンシューマ EPG とプロバイダー EPG 間のトラフィックはサービス グラフにリダイレクトされます。

権限について

管理者は、（APIC）でロールに権限を付与できます。権限は、ロールが実行できるタスクを決定します。管理者は、管理者のロールに次の権限を付与できます。

特権	説明
nw-svc-connectivity	• 管理 EPG の作成 • 他のオブジェクトに管理接続を作成
nw-svc-policy	• サービス グラフの作成 • アプリケーション EPG およびコントラクトへのサービス グラフのアタッチ • サービス グラフのモニタ
nw-svc-device	• デバイス クラスタの作成 • 具象デバイスの作成 • デバイス コンテキストの作成

（注） インフラストラクチャの管理者だけがデバイス パッケージを APIC にアップロードできます。

サービスの自動化と構成管理

Cisco APIC は、サービス デバイスの構成管理と自動化のポイントとして任意に動作でき、ネットワーク自動化とのサービス デバイスの調整を行うことができます。Cisco APIC は、さまざまなイベントで Python スクリプトを使用してサービス デバイスと連動し、デバイス固有の Python スクリプト機能を呼び出します。

デバイス スクリプトとサービスデバイスでサポートされる機能を定義するデバイスの仕様は、デバイス パッケージとしてまとめられ、Cisco APIC にインストールされます。デバイス スクリプト ハンドラは、デバイス構成モデルに基づいてその REST インターフェイス（推奨）または CLI を使用してデバイスとやりとりします。

サービス リソースのプーリング

Cisco ACI ファブリックは、多数の接続先間で非ステートフル負荷分散を実行できます。この機能により、組織は物理および仮想サービス デバイスをサービス リソース プールにグループ化でき、機能や場所によってさらにグループ化できます。これらのプールは、標準の高可用性メカニズムを使用することで高可用性を提供するか、または障害が発生した場合に、他のメンバーに負荷が再分散された状態で簡易なステートフル サービス エンジンとして使用できます。どちらのオプションでも、等コスト マルチパス（ECMP）、ポートチャネル機能および共有状態を必要とするサービス アプライアンスのクラスタリングの現在の制限をはるかに超える横方向の拡張性が提供されます。

サービス デバイスがファブリックとやりとりする必要がない場合、Cisco ACI はサービス デバイスを使用して簡易バージョンのリソース プーリングを実行できます。また、ファブリックとサービス デバイス間の調整を伴うより高度なプーリングも実行できます。



第 11 章

管理ツール

この章は、次の内容で構成されています。

- 管理ツール （297 ページ）
- 管理 GUI について （297 ページ）
- CLI について （298 ページ）
- ユーザ ログインのメニュー オプション （298 ページ）
- GUI および CLI バナーのカスタマイズ （299 ページ）
- REST API （299 ページ）
- エクスポート/インポートの構成 （309 ページ）
- Puppet を使用したプログラマビリティ （314 ページ）

管理ツール

Cisco Application Centric Infrastructure（ACI）ツールは、ファブリックの管理者、ネットワークエンジニア、および開発者がテナントおよびアプリケーションの開発、構成、デバッグおよび自動展開に役立ちます。

管理 GUI について

次の管理 GUI の機能により、ファブリックおよびそのコンポーネント（リーフとスパイン）にアクセスできます。

- 世界共通の Web 標準（HTML5）に基づく。インストーラまたはプラグインは必要ありません。
- モニタリング（統計、障害、イベント、監査ログ）、操作および構成データへのアクセス。
- シングルサインオン メカニズムによる APIC とスパインおよびリーフスイッチへのアクセス。
- サードパーティが使用できる同じ RESTful API を使用した APIC との通信。

CLI について

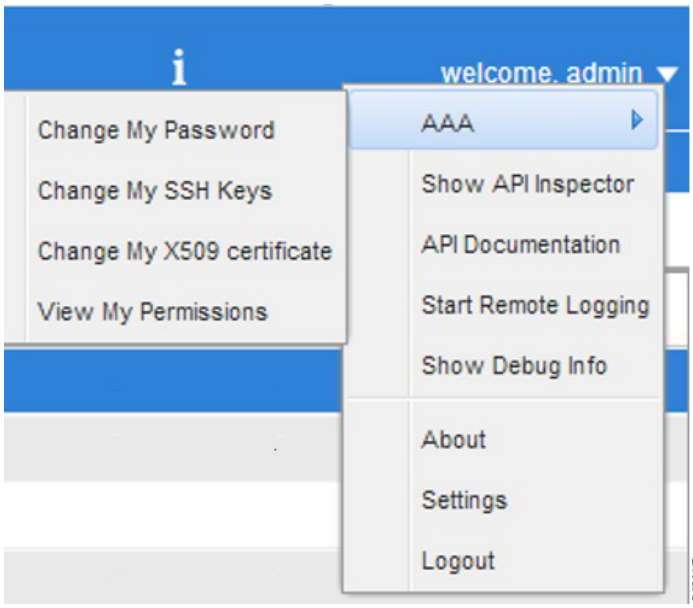
CLI は、APIC、リーフおよびスパイン スイッチへの操作インターフェイスおよび構成インターフェイスを特徴としています。

- Python で初めから実行され、Python インタープリタと CLI 間で切替えることができます。
- 拡張性のプラグイン アーキテクチャ
- 監視、操作、および構成データへの仮想ルーティングおよび転送（VRF）ベースのアクセス
- Python コマンドまたはバッチ スクリプティングによる自動化

ユーザ ログインのメニュー オプション

ユーザ ログインのドロップダウンメニューにより、複数の構成、診断、参照およびプリファレンスのオプションが提供されます。次の図は、このドロップダウンメニューを示します。

図 *113*: ユーザ ログインのメニュー オプション



オプションには次のものが含まれます。

- ユーザ パスワード、SSH キー、X509 証明書を変更、およびログインしたユーザの権限を表示するための AAA オプション。

（注） ACI ファブリックは、すべてのデバイスのシステム クロックが正しいことを保証するために、アクティブな Network Time Protocol（NTP）ポリシーを使用して構成する必要があります。そうでない場合、同期がとれていないノードで証明書が拒否される可能性があります。

- [API インスペクタの表示（Show API Inspector）] では、API インスペクタが開きます。
- [API ドキュメンテーション（API Documentation）] では、管理情報モデルの参照を開きます。
- リモート ロギング
- デバッグ情報
- ソフトウェアの現在のバージョン番号について。
- GUI を使用するためのプリファレンスの設定。
- システムを終了するためのログアウト。

GUI および CLI バナーのカスタマイズ

GUI および CLI バナーは、GUI の [管理（Admin）] > [AAA] > [セキュリティ管理（Security management）] セクションにあります。CLI バナーは、ユーザのログイン認証の前に表示されます。CLI バナーは、コンソールにそのまま出力されるテキスト ベースの文字列です。GUI バナーは、ユーザのログイン認証の前に表示されます。GUI バナーは URL です。URL は、iFrame に配置できるようにする必要があります。URL `x-frame-option` が `deny` または `sameorigin` に設定されている場合、ユーザのログイン認証の前に URL は表示されません。

REST API

REST API について

Application Policy Infrastructure Controller (APIC) REST API は、REST アーキテクチャを使用するプログラム的なインターフェイスです。API は JavaScript オブジェクトの表記（JSON）または拡張マークアップ言語（XML）のドキュメントを含む HTTP（デフォルトでは無効）または HTTPS のメッセージを受け入れ、返します。プログラミング言語を使用して、API メソッドまたは管理対象オブジェクト（MO）の説明を含むメッセージおよび JSON または XML ドキュメントを生成できます。

REST API は、管理情報ツリー（MIT）へのインターフェイスであり、オブジェクト モデルの状態を操作できます。APIC CLI、GUI、および SDK は同じ REST インターフェイスを使用す

るため、情報を表示する場合は常に、REST API を介して読み込まれ、構成変更が行われた場合は REST API を通じて書き込まれます。REST API は、統計、障害、監査イベントなど、他の情報を取得できるインターフェースも提供します。プッシュベースのイベント通知に登録する手段も提供されているので、MIT で変更が発生すると、Web ソケットを介してイベントが送信されます。

API では、HTTP を通じた POST 操作、GET 操作、DELETE 操作など、標準的な REST メソッドがサポートされています。POST メソッドと DELETE メソッドは、同じ入力パラメータで複数回呼び出されても、それ以上の効果を持たないべき等です。GET メソッドはべきゼロで、何らの変更も行うことなく（つまり、読み取り専用操作）ゼロ回または複数回呼び出すことができます。

REST インターフェイスに出入りするペイロードは、XML エンコーディングまたは JSON エンコーディングによりカプセル化できます。XML の場合、エンコーディング操作は簡単です。要素タグはパッケージとクラスの名前で、そのオブジェクトのプロパティはその要素の属性として指定します。含有は、子要素を作成して定義します。

JSON の場合、エンコーディングにはツリーベースの階層を反映する特定のエントリの定義が必要です。ただし、その定義はツリーのすべてのレベルで繰り返されるため、最初に理解していれば実装はかなり簡単です。

- すべてのオブジェクトは JSON ディクショナリとして記述され、キーはパッケージとクラスの名前です。値は、属性と子の 2 つのキーを持つ別のネストされたディクショナリです。
- 属性キーには、オブジェクト上の属性を定義するキー値ペアを記述する、さらにネストされたディクショナリが含まれています。
- 子キーには、すべての子オブジェクトを定義するリストが含まれています。このリストの子オブジェクトは、ここで説明したように定義された、ネストされたオブジェクトを含むディクショナリです。

認証

REST API のユーザー名ベースおよびパスワードベースの認証は、POST 操作の DN ターゲットとして、**aaaLogin**、**aaaLogout**、および **aaaRefresh** などの特殊なリクエストのサブセット、ユニバーサル技術情報識別子（URI）を使用します。ペイロードには、シンプルな XML ペイロードまたは JSON ペイロードが含まれ、これらには **aaaUser** オブジェクトの MO 表現と、ユーザー名とパスワードを定義する属性名および **pwd** が含まれています。たとえば、**<aaaUser name='admin' pwd='password'/>** のようになります。POST 操作の応答には、Set-Cookie ヘッダーと、応答の名前付きトークンの **aaaLogin** オブジェクトの属性の両方として認証トークンが含まれます。この場合の XPath はエンコーディングが XML の場合は **/imdata/aaaLogin/@token** です。REST API の後続の操作では、このトークン値を **APIC-cookie** という名前の cookie としてその後の要求の認証に使用できます。

サブスクリプション

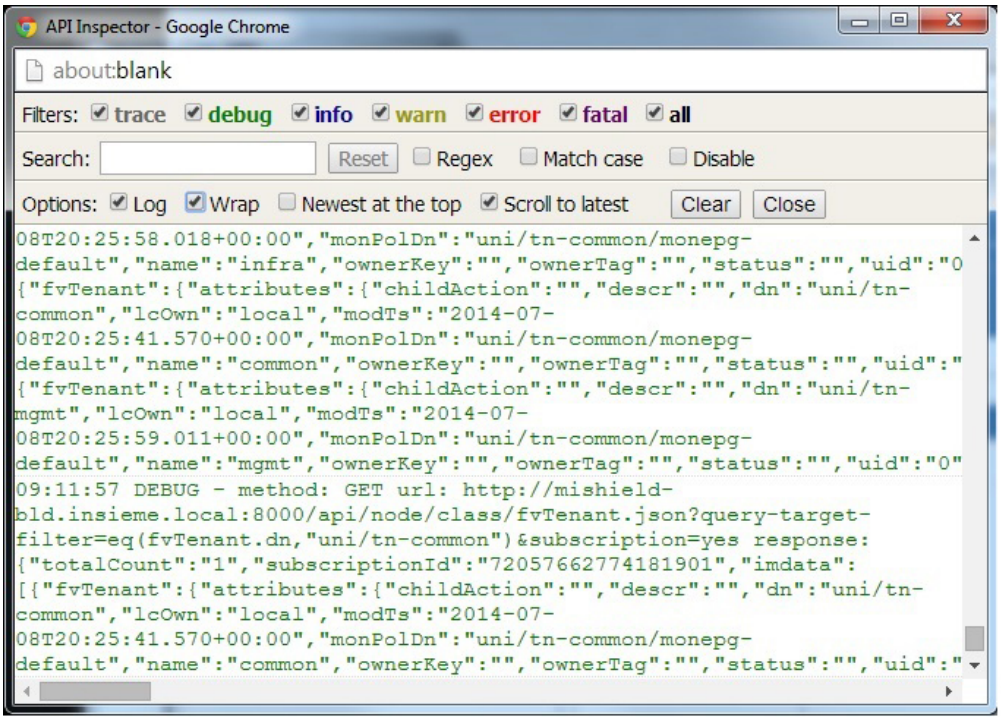
REST API は、アクティブな API セッション中の 1 つ以上の MO へのサブスクリプションをサポートします。ユーザまたはシステムにより開始されたアクションによって、MO が作成、変

更、または削除されると、イベントが生成されます。サブスクライブされたアクティブなクエリ上のデータがイベントにより変更されると、APICはそのサブスクリプションを作成したAPIクライアントに通知を送信します。

API インスペクタ

API インスペクタでは、APIC が GUI インタラクションを実行するために処理する REST API コマンドのリアルタイム表示が提供されます。下の図は、APIインスペクタがGUIの主要テナントのセクションに移動する場合に表示する REST API コマンドを示します。

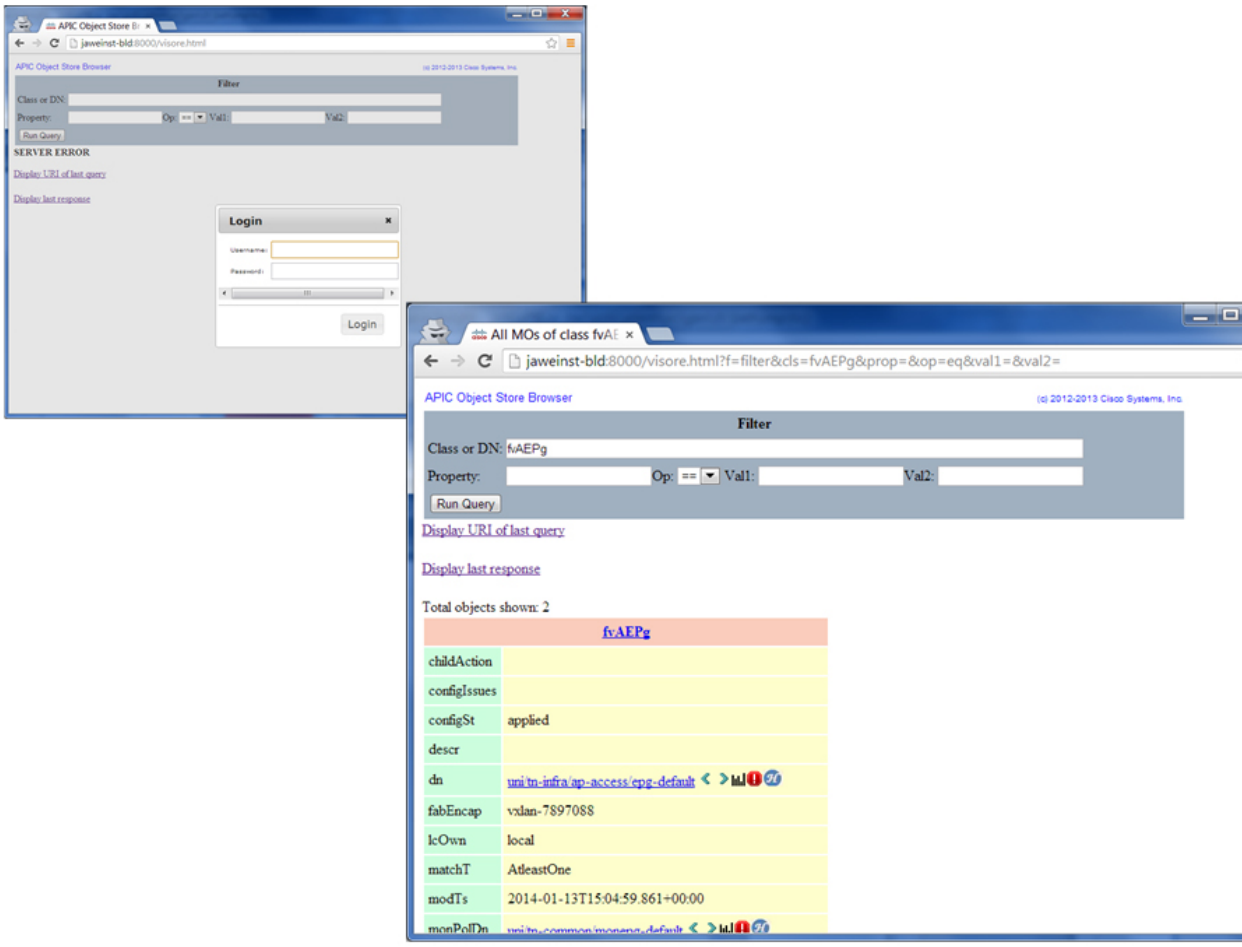
図 *114 : API* インスペクタ



Visore 管理対象オブジェクト ビューア

Visore は、下の図に示すように、読み取り専用の管理情報ツリー（MIT）ブラウザです。これにより、オプションのフィルタを使用して、識別名（DN）とクラスのクエリが可能になります。

図 *115 : Visore MO* ビューア



Visore 管理対象オブジェクト ビューアは次の場所にあります。

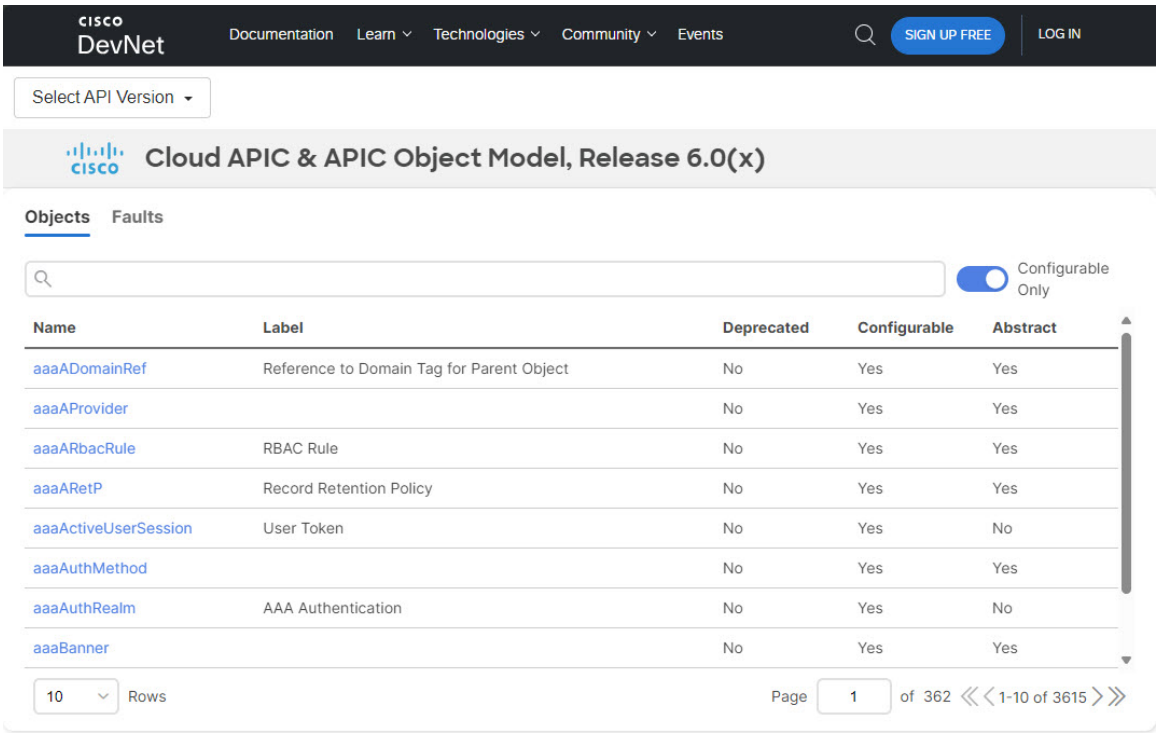
`http(s)://host[:port]/visore.html`

管理情報モデルのリファレンス

管理情報モデル（MIM）には、システム内のすべての管理対象オブジェクトとそのプロパティが含まれます。詳細については、『*Cisco APIC Management Information Model* リファレンス ガイド』を参照してください。

Cisco APIC 6.0 リリースで MIT 内のオブジェクトを検索するために管理者がどのように MIM を使用できるかに関する例については、次の図を参照してください。

図 *116 : Cisco APIC 6.0* リリースの *MIM* リファレンス

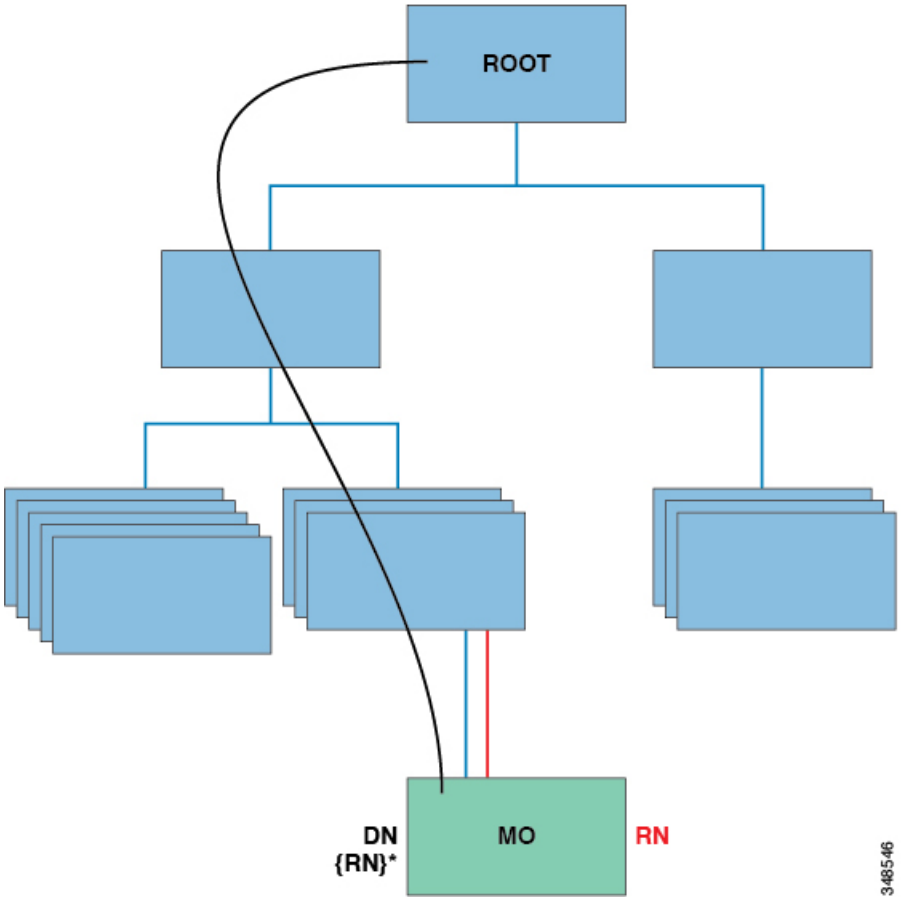


MIT 内のオブジェクトの検索

Cisco ACI は情報モデルベースのアーキテクチャ（管理情報ツリー（MIT））を使用しており、管理プロセスによって制御できるすべての情報がモデルによって説明されます。オブジェクトインスタンスは管理対象オブジェクト（MO）と呼ばれます。

次の図は、任意の MO インスタンスを一意的に表す識別名と、親 MO の下にある MO をローカル的に表す相対名を示します。MIT 内のオブジェクトはすべて、ルート オブジェクトの下に存在します。

図 *117 : MO* の識別名と相対名



システム内のすべての MO は固有の識別名（DN）によって識別されます。このアプローチにより、グローバルにオブジェクトを参照できます。またオブジェクトの識別名のほか、各オブジェクトを相対名（RN）で参照することもできます。相対名は、親オブジェクトに対して相対的にオブジェクトを識別します。指定されたオブジェクトの識別名は、親オブジェクトの識別名に相対名を加えることで取得できます。

DN は、オブジェクトを一意的に識別する一連の相対名です。

```
dn = {rn}/{rn}/{rn}/{rn}
```

dn =”sys/ch/lcslot-1/lc/leafport-1”

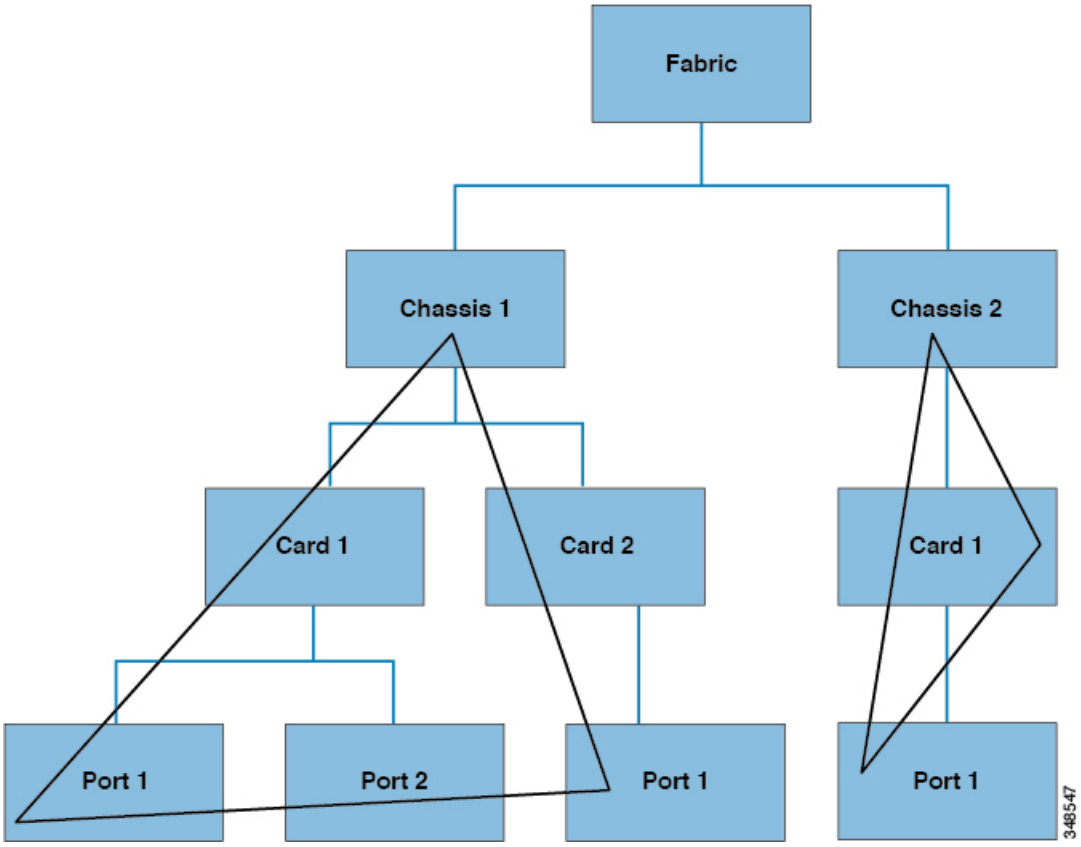
識別名はURLに直接マッピングされます。MIT内におけるオブジェクトの現在位置に応じて、相対名または識別名のいずれかを使用してオブジェクトにアクセスできます。

ツリーは階層型で構成され、属性システムを使用してオブジェクトクラスを識別できるため、さまざまな方法で管理対象オブジェクトの情報を取得するためにツリー内を照会できます。クエリは、識別名を使用してオブジェクト自体に対して実行するか、スイッチシャーシなどのオブジェクトのクラスに対して実行するか、ツリー レベルで実行してオブジェクトのすべてのメンバーを検出できます。

ツリーレベルのクエリ

次の図は、クエリ対象の 2 つのシャーシをツリー レベルで示しています。

図 *118 :* ツリーレベルのクエリ

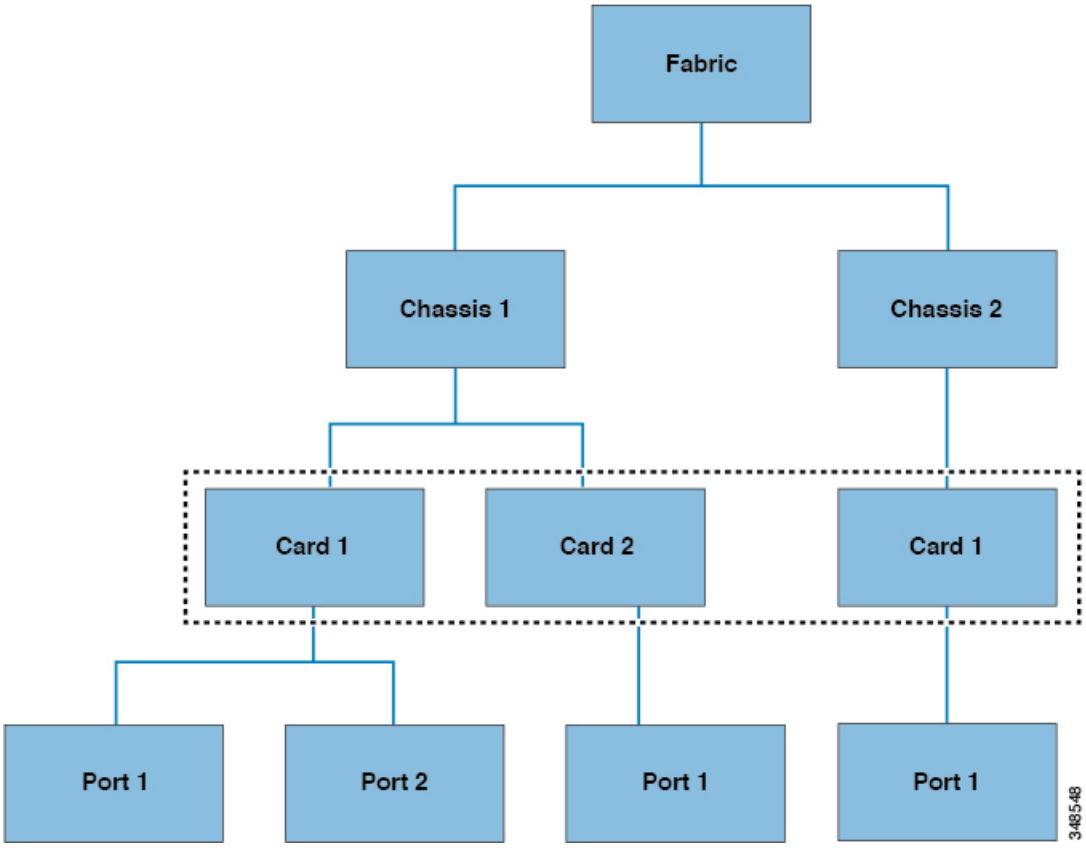


どちらのクエリも、参照されたオブジェクトと、その子オブジェクトを返します。このアプローチは、大規模なシステムのコンポーネントを検出するために役立ちます。この例では、クエリにより指定されたスイッチ シャーシのカードとポートが検出されます。

オブジェクトレベル クエリ

次の図は、2 番目のクエリ タイプ、クラスレベル クエリを示します。

図 *119* : オブジェクトレベル クエリ

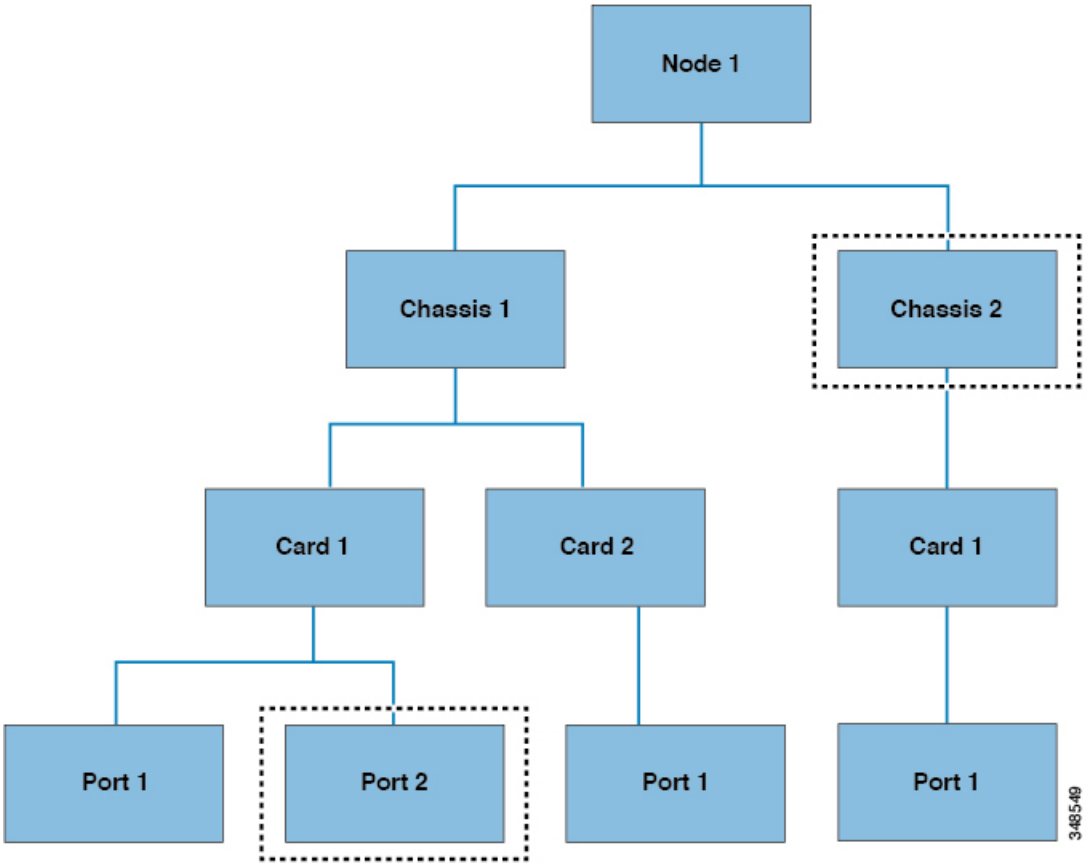


クラスレベル クエリは、任意のクラスのオブジェクトをすべて返します。このアプローチは、MIT で使用できる特定のタイプのオブジェクトをすべて検出する場合に役立ちます。この例で使用しているクラスはカードで、カード タイプのすべてのオブジェクトを返します。

オブジェクトレベル クエリ

3 つ目のクエリ タイプはオブジェクトレベル クエリです。オブジェクトレベル クエリでは、識別名を使用して特定のオブジェクトを返します。次の図は、2 つのオブジェクトレベル クエリを示しており、1 つはノード 1/シャーシ 2、もう 1 つはノード 1/シャーシ 1/カード 1/ポート 2 を照会しています。

図 *120* : オブジェクトレベル クエリ

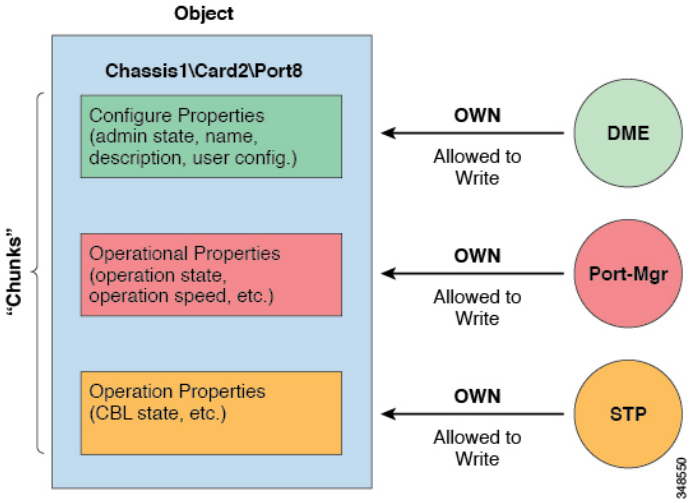


すべての MIT クエリで、管理者はサブツリー全体またはサブツリーの一部を返すよう選択できます。また、システム内のロールベース アクセス コントロール（RBAC）メカニズムによって、返されるオブジェクトが決まります。必ず、ユーザが表示権限を持つオブジェクトのみが返されます。

管理対象オブジェクトのプロパティ

Cisco ACI の管理対象オブジェクトには、管理対象オブジェクトを定義するプロパティが含まれています。管理対象オブジェクトのプロパティはチャンクに分割され、オペレーティング システム内でプロセスによって管理されます。オブジェクトには、複数のプロセスがアクセスする場合があります。これらのプロパティはすべて実行時にまとめてコンパイルされ、単一のオブジェクトとしてユーザに提示されます。次の図は、この関係の例を示します。

図 *121* : 管理対象オブジェクトのプロパティ



オブジェクトの例には、オブジェクト内のプロパティチャンクに書き込むプロセスが3つあります。Cisco APIC（ユーザ）とオブジェクトとの間のインターフェイスとなるデータ管理エンジン（DME）、ポートの構成を処理するポート マネージャ、およびスパニングツリープロトコル（STP）のすべてが、このオブジェクトのチャンクとやり取りします。APICは、実行時にコンパイルされる単一のエンティティとしてオブジェクトをユーザに提示します。

REST インターフェイスによるオブジェクト データへのアクセス

REST は、World Wide Web などの分散型システム用ソフトウェア アーキテクチャの形式で、形式がシンプルであるため、Simple Object Access Protocol（SOAP）や Web サービス記述言語（WSDL）など、その他の設計モデルに代わって採用される機会が増えています。Cisco APIC は REST インターフェイスをサポートしており、Cisco ACI ソリューション全体へのプログラムを通じたアクセスを実現します。

Cisco ACI のオブジェクトベース情報モデルは、REST インターフェイスに非常にうまく適合しています。URL と URI は識別名に直接マッピングされ、MIT 上のオブジェクトを識別でき、MIT 上のデータを XML または JSON 形式でエンコードされた自己完結型の構造化テキスト ツリードキュメントとして記述できます。オブジェクトには、識別名とプロパティを使用して識別される親子関係があり、この関係は一連の作成、読み取り、更新、および削除（CRUD）操作によって読み取りと変更が可能です。

オブジェクトにアクセスするには、明確に定義されたアドレスである REST URL を使用します。Cisco APIC オブジェクト データを取得および操作するには標準の HTTP コマンドを使用します。使用できる URL の形式は次のとおりです。

```
<system>/api/[mo|class]/[dn|class][:method].[xml|json]?{options}
```

URL の前に指定する各構成要素は、次のとおりです。

- `system`：システム識別子、IP アドレスまたは DNS で解決可能なホスト名
- `mo | class`：これが MIT 内の MO かまたはクラスレベルのクエリかどうかの表示

- `class`：照会するオブジェクトのMOクラス（情報モデルでの指定に従う）。クラス名は、`<pkgName><ManagedObjectClassName>` で表されます。
- `dn`：照会するオブジェクトの識別名（MIT 内のオブジェクトの一意の階層名）
- `method`：オブジェクトに対して呼び出すメソッドの指定（オプション）。HTTP POST リクエストにのみ適用されます。
- `xml | json`：エンコード形式
- `options`：クエリ オプション、フィルタ、引数

REST URL で個々のオブジェクトまたはオブジェクト クラスのアドレスを指定してアクセスできる機能により、管理者はオブジェクト ツリー全体、つまりシステム全体にプログラムを通じて完全にアクセスできます。

次に、REST クエリの例を示します。

- テナント solar 下のすべての EPG と障害を検索します。

  `http://192.168.10.1:7580/api/mo/uni/tn-solar.xml?query-target=subtree&target-subtree-class=fvAEPg&rsp-subtree-include=faults`

- フィルタされた EPG クエリ

  `http://192.168.10.1:7580/api/class/fvAEPg.xml?query-target-filter=eq(fvAEPg.fabEncap,%20"vxlan-12780288")`

エクスポート/インポートの構成

すべての APIC ポリシーおよび構成データは、バックアップの作成のためにエクスポートできます。これは、エクスポートポリシーを使用して構成でき、リモート サーバーにスケジュール済みバックアップまたは即時バックアップできます。スケジュール済みバックアップは、定期バックアップ ジョブまたは繰り返しバックアップ ジョブを実行するように構成できます。デフォルトでは、すべてのポリシーおよびテナントがバックアップされますが、管理者は任意に管理情報ツリーの特定のサブツリーのみを指定できます。バックアップは、インポート ポリシーによって APIC にインポートでき、システムを以前の構成に復元できます。

データベースのシェーディング

APIC クラスタは、シャーディングと呼ばれる大規模なデータベース テクノロジを使用します。このテクノロジは、APIC によって生成および処理されるデータ セットに拡張性と信頼性を提供します。APIC 構成のデータは、データベース シャードに類似したシャードと呼ばれる論理的にバインドされたサブセットに分割されます。シャードはデータ管理の単位であり、APIC は次の方法でシャードを管理します。

- 各シャードには 3 つのレプリカがあります。
- シャードは、APIC クラスタを構成するアプライアンス全体に均等に分散されます。

1 つ以上のシャードが各 APIC アプライアンスにあります。シャード データの割り当ては事前に決定されたハッシュ関数に基づいており、静的なシャード レイアウトによってアプライアンスへのシャードの割り当てが決定されます。

設定ファイルの暗号化

リリース 1.1(2) 以降では、AES-256 暗号化を有効にすることにより APIC 設定ファイルのセキュア プロパティを暗号化できます。AES 暗号化はグローバル設定オプションです。すべてのセキュア プロパティは AES 構成設定に従っています。テナント設定などの ACI ファブリック設定のサブセットを AES 暗号化を使用してエクスポートするが、ファブリック設定の残りの部分は暗号化しないということはできません。セキュア プロパティのリストについては、*Cisco Application Centric Infrastructure Fundamentals*の「Appendix K: Secure Properties」を参照してください。

APIC は、16 ～ 32 文字のパスフレーズを使用して AES-256 キーを生成します。APIC GUI には、AES パスフレーズのハッシュが表示されます。このハッシュを使用して、2 つの ACI ファブリックで同じパスフレーズが使用されているかどうかを確認できます。このハッシュをクライアント コンピュータにコピーして、別の ACI ファブリックのパスフレーズ ハッシュと比較できます。これにより、それらのハッシュが同じパスフレーズを使用して生成されたかどうかを確認できます。ハッシュを使用して、元のパスフレーズまたは AES-256 キーを再構築することはできません。

暗号化された設定ファイルを使用する際は、次のガイドラインに従ってください。

- AES 暗号化設定オプションを使用しているファブリックに古い ACI 設定をインポートするための後方互換性がサポートされています。

（注） 逆の互換性はサポートされていません。AES 暗号化が有効になっている ACI ファブリックからエクスポートされた設定を古いバージョンの APIC ソフトウェアにインポートすることはできません。

- ファブリック バックアップ設定のエクスポートを実行するときは、必ず AES 暗号化を有効にします。これにより、ファブリックを復元するときに、設定のすべてのセキュア プロパティが正常にインポートされるようになります。

（注） AES 暗号化を有効にせずにファブリック バックアップ設定がエクスポートされると、どのセキュア プロパティもエクスポートに含まれません。そのような暗号化されていないバックアップにはセキュア プロパティは何も含まれていないため、そのようなファイルをインポートしてシステムを復元すると、ファブリックの管理者およびすべてのユーザがシステムからロックアウトされてしまう可能性があります。

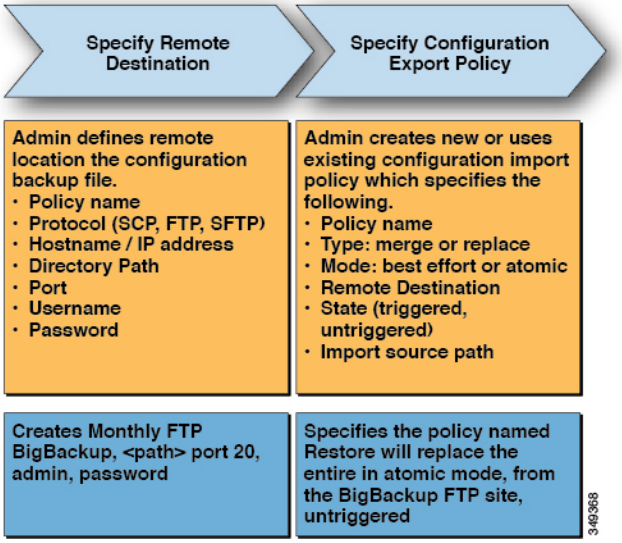
- 暗号化キーを生成する AES パスフレーズは、ACI 管理者やその他のユーザが復元したり読み取ったりすることはできません。AES パスフレーズは保存されません。APIC は AES パスフレーズを使用して AES キーを生成した後、そのパスフレーズを廃棄します。AES キーはエクスポートされません。AES キーは、エクスポートされず、REST API を使用して取得できないため、復元できません。
- 同じ AES-256 パスフレーズは、常に同じ AES-256 キーを生成します。設定のエクスポート ファイルは、同じ AES パスフレーズを使用する他の ACI ファブリックにインポートできます。
- トラブルシューティングを目的として、セキュアプロパティの暗号化データが含まれていない設定ファイルをエクスポートします。設定のエクスポートを実行する前に一時的に暗号化をオフにすると、エクスポートされた設定からすべてのセキュアプロパティ値が削除されます。すべてのセキュアプロパティが削除されたそのような設定ファイルをインポートするには、インポート マージ モードを使用します。インポート置換モードは使用しません。インポート マージ モードを使用すると、ACI ファブリック内の既存セキュア プロパティが保持されます。
- デフォルトで、APICは復号できないフィールドが含まれているファイルの設定のインポートを拒否します。この設定をオフにするときは注意してください。このデフォルト設定がオフになっているときに設定のインポートが適切に実行されないと、ファブリックのAES暗号化設定に一致しない設定ファイルのインポート時にACIファブリックのすべてのパスワードが削除される可能性があります。

（注） このガイドラインに従わないと、ファブリック管理者を含むすべてのユーザがシステムからロックアウトされる可能性があります。

設定のエクスポート

次の図は、エクスポート ポリシーを構成するプロセスがどのように動作するかを示します。

図 *122 :* エクスポートポリシー構成のワークフロー



APIC は、このポリシーを次のように適用します。

- 完全なシステム構成のバックアップは月に一度実行されます。
- バックアップは BigBackup FTP サイトに XML 形式で保存されます。
- ポリシーがトリガーされます（有効になります）。

インポートの構成

管理者は、次の2つのモードのいずれかでインポートを実行するインポートポリシーを作成できます。

- ベストエフォート：インポートできないシャード内のオブジェクトを無視します。

（注） 受信構成のバージョンが既存のシステムと互換性がない場合、互換性のないシャードはインポートされませんが、インポート可能なシャードはインポートされません。

- アトミック：インポート可能なシャードの処理中に、インポートできないオブジェクトを含むシャードを無視します。

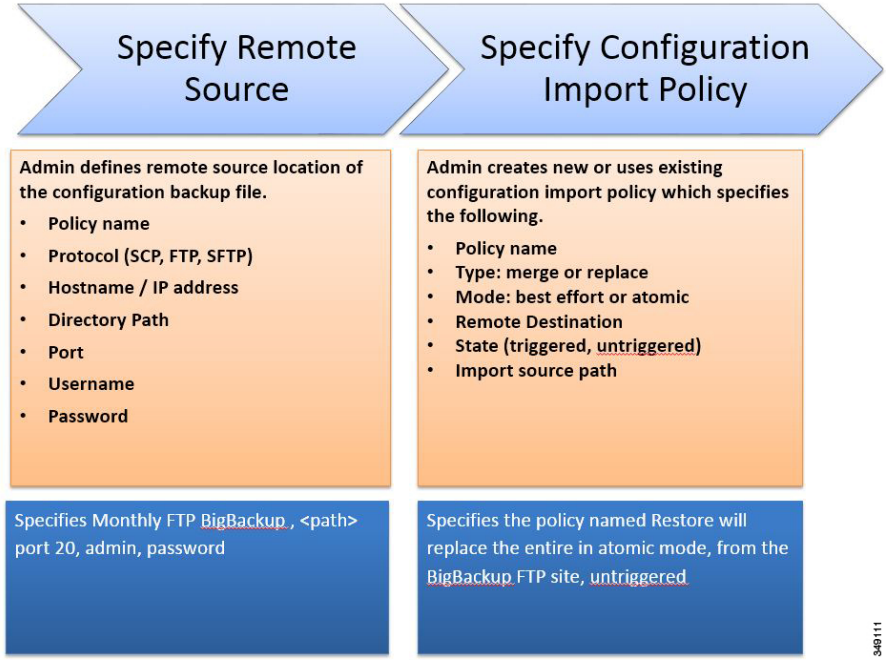
（注） 受信構成のバージョンが既存のシステムと互換性がない場合、インポートは終了します。この場合、代わりにベストエフォートを使用してください。

インポート ポリシーは、次のモードとタイプの組み合わせをサポートします。

- ベストエフォートマージ：インポートされた構成は既存の構成とマージされますが、インポートできないオブジェクトは無視されます。
- アトミック マージ：インポートされた構成は既存の構成とマージされますが、インポートできないオブジェクトを含むシャードは無視されます。
- アトミック置き換え：既存の構成をインポートされた構成データで上書きします。インポートされた構成に存在しない既存の構成のオブジェクトはすべて削除されます。オブジェクトは、既存の構成に子を持つが、インポートされた受信構成に子を持たない既存の構成から削除されます。たとえば、既存の構成に2つのテナント（solar と wind）があり、インポートされたバックアップ構成がテナントの wind が作成される前に保存されている場合、テナントの soar はバックアップから復元されますが、テナントの wind は削除されます。

次の図は、インポート ポリシーを構成するプロセスがどのように動作するかを示します。

図 *123*：インポート ポリシーを構成するワークフロー



APIC はこのポリシーを次のように適用します。

- 毎月のバックアップから完全なシステム構成の復元を実行するためのポリシーが作成されます。
- アトミック置換モードは次のことを行います。
  - 既存の構成を上書きします。
  - インポートされたファイルに存在しない既存の構成オブジェクトを削除します。

- 存在しない子オブジェクトを削除します。

- ポリシーはトリガーされません（使用できますが、アクティブ化されていません）。

テクニカル サポート、統計、コア

管理者は、APIC 内で、コア ファイルとデバッグ データを処理するために、統計情、テクニカル サポートの収集、障害およびイベントをファブリック（APIC およびスイッチ）から外部ホストにエクスポートするようエクスポートポリシーを構成できます。エクスポートは XML、JSON、Web ソケット、SCP、HTTP などのさまざまな形式にできます。エクスポートは登録可能で、定期的またはオンデマンドでストリーミングできます。



（注） 統計のエクスポートポリシーの最大数は、テナントの数とほぼ同じです。各テナントは複数の統計エクスポートポリシーを持つことができ、複数のテナントが同じエクスポートポリシーを共有できますが、ポリシーの合計数はテナントの数とほぼ同数に制限されます。

管理者は、転送プロトコル、圧縮アルゴリズム、転送の頻度などポリシーの詳細を設定できます。ポリシーは、AAA を使用して認証されたユーザによって設定できます。実際の転送のセキュリティ メカニズムは、ユーザ名とパスワードに基づいています。内部的に、ポリシー要素はデータのトリガーを処理します。

Puppet を使用したプログラマビリティ

Puppet について

Puppet は Puppet Labs, Inc. の構成管理ツールです。Puppet はもともと大規模なサーバー管理用に設計されましたが、多くのデータセンター オペレーターは、同じツールを使用してサーバーとネットワークデバイスのプロビジョニングを統合したいと考えています。

次の項目は、Puppet 導入の主要なコンポーネントです。

- **Manifet**：Puppet マニフェストは、管理対象デバイス（ノード）の状態を設定するためのプロパティ定義の集合です。これらのプロパティ状態の確認および設定の詳細は抽象化されているため、マニフェストは複数のオペレーティングシステムまたはプラットフォームで使用できます。

- **Master**：通常、Puppetマスター（サーバー）は個別の専用サーバー上で実行され、複数のノードにサービスを提供します。Puppetマスターは構成マニフェストをコンパイルし、要求に応じてそれらをノードに提供します。

- **Agent または Device**：Puppetエージェントはノードで実行され、定期的に Puppetマスターに接続して構成マニフェストを要求します。エージェントは、受信したマニフェストをノードの現在の状態と調整し、相違点を解決するために必要に応じてノードの状態を更新

します。組み込みの Puppet エージェントを実行できない、または実行したくないノードの場合、Puppet は Puppet デバイスと呼ばれる構造をサポートします。Puppet デバイスは基本的に、ノードの外部にあるプロキシ メカニズムであり、ノードに代わって Puppet マスターからマニフェストを要求します。Puppetデバイスは、受信したマニフェストに必要な更新をノードに適用します。この機能を活用するには、ベンダーは、デバイスを利用する Puppet モジュールとともに、デバイス クラスのベンダー固有の実装を提供する必要があります。ベンダー固有のデバイス クラスは、独自のプロトコルまたは API を使用してリモート ノードを構成します。

Puppet の詳細とドキュメントについては、次の Puppet Web サイトを参照してください。URL：https://puppet.com/

Cisco ciscoacipuppet パペット モジュール

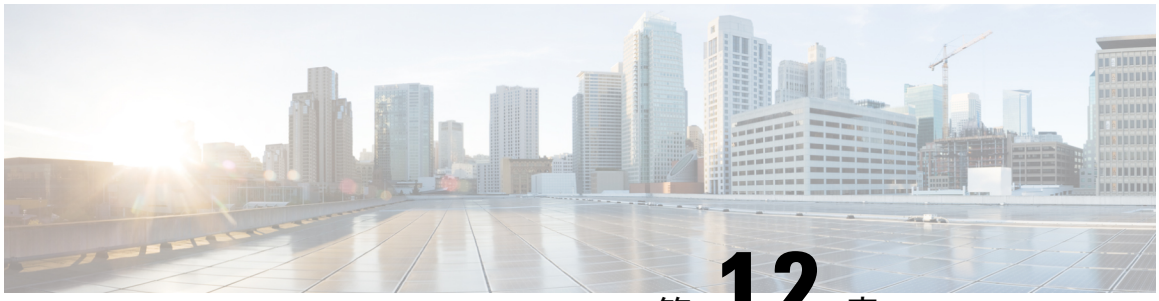
APIC コントローラは、組み込みの Puppet エージェントを実行しません。代わりに、シスコは Puppet モジュール（「ciscoacipuppet」）を提供します。これは、Cisco ACI 固有の Puppet デバイスを使用して、構成管理要求を APIC コントローラにリレーします。ciscoacipuppet モジュールは、受信した Puppet マニフェスト内の変更情報を解釈し、変更要求を APIC REST API メッセージに変換して、ACI ファブリックの構成変更を実装します。

ciscoacipuppet モジュールのインストール、セットアップ、および使用方法の詳細については、次の URL にある GitHub および Puppet Forge のドキュメントを参照してください。

- **GitHub** – https://github.com/cisco/cisco-network-puppet-module
- パペットフォージ – https://forge.puppet.com/puppetlabs/ciscoacipuppet

ACI に関する Puppet ガイドラインと制限事項

- ciscoacipuppet Puppet モジュールを使用してプロビジョニングできるのは、APIC 管理対象オブジェクトのサブセットのみです。サポートのレベルと制限を理解するには、GitHub および Puppet Forge の ciscoacipuppet モジュールのドキュメントを参照してください。



第 12 章

モニタリング

この章は、次の内容で構成されています。

- 障害、エラー、イベント、監査ログ （317 ページ）
- 統計プロパティ、階層、しきい値およびモニタリング （323 ページ）
- 統計データについて （324 ページ）
- モニタリング ポリシーの構成 （325 ページ）
- Tetration Analytics （329 ページ）
- NetFlow （329 ページ）

障害、エラー、イベント、監査ログ

障害、イベント、エラー、システム メッセージについては、Web ベースのアプリケーションである『*Cisco APIC Faults, Events, and System Messages Management Guide*』および『*Cisco APIC Management Information Model Reference*』を参照してください。

APIC は、MO の集合形式で ACI ファブリック システムの管理および操作状態の包括的な現在のランタイム表現を維持します。システムは、これらのプロセスを管理するためにシステムとシステムおよびユーザーが作成するポリシーのランタイム状態に従って、障害、エラー、イベント、および監査ログ データを生成します。

APIC GUI を使用すると、ファブリック スイッチのカスタマイズされた「履歴レコード グループ」を作成できます。これに、カスタマイズされたスイッチ ポリシーを割り当てて、それらのグループのスイッチ用に維持する監査ログ、イベント ログ、正常性ログ、および障害ログのカスタマイズされたサイズと保持期間を指定できます。

APIC GUI を使用すると、このファブリック上のコントローラに対して維持される監査ログ、イベント ログ、正常性ログ、および障害ログのサイズと保持期間を指定するグローバル コントローラ ポリシーをカスタマイズすることもできます。

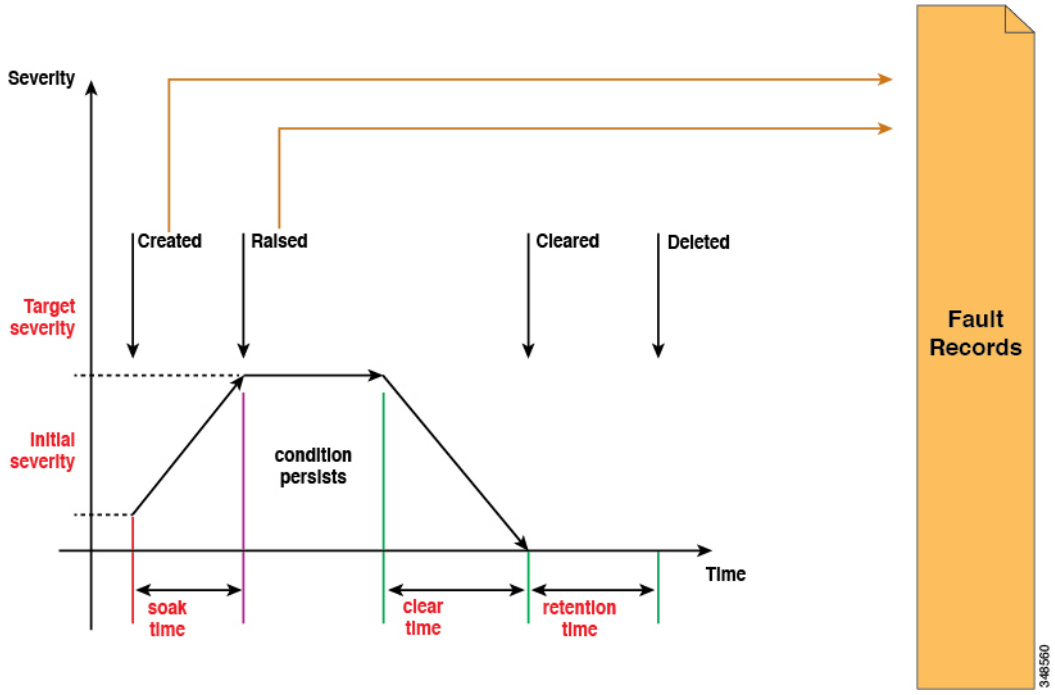
（注） クラスタでは、APIC 1 が正常性統計情報の収集を行います。アップグレード中に APIC 1 が再起動すると、正常性の統計情報が一時的に使用できなくなります。正常性の統計情報は APIC クラスタ内で複製されません。

障害

システムの実行時の状態に基づいて、APICは自動的に異常を検出し、障害を表す障害オブジェクトを作成します。障害オブジェクトには、ユーザが問題を診断してその影響を評価するのに役立ち、解決策を提供するように作られているさまざまなプロパティが含まれます。

たとえば、高いパリティエラー率などポートに関連する問題をシステムが検出すると、障害オブジェクトが自動的に作成され、ポートオブジェクトの子として管理情報ツリー（MIT）内に配置されます。同じ状況が複数回検出される場合、障害オブジェクトの追加インスタンスは作成されません。障害を引き起こした状況が修正された後、障害オブジェクトは障害のライフサイクルポリシーで指定された一定期間保存され、最終的に削除されます。次の図を参照してください。

図 *124 :* 障害のライフサイクル



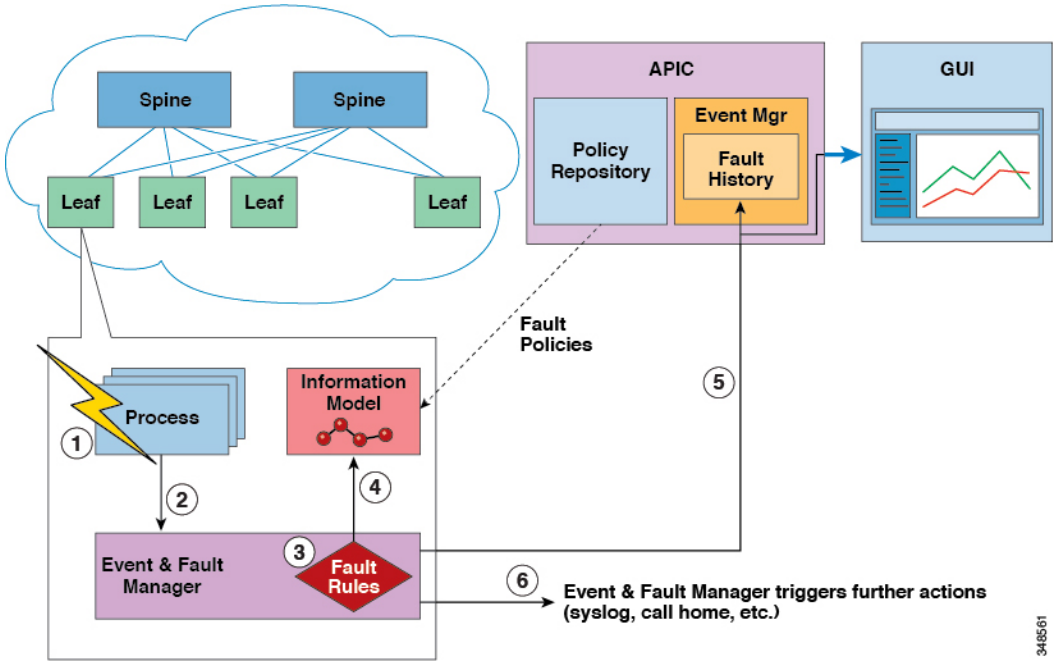
ライフサイクルは問題の現在の状態を表します。サイクルは問題が最初に検出されると、そのソーク時間で開始され、提起された状態へと変わって、問題がまだ存在するとその状態のままになります。状態がクリアされると、「raised-clearing」と呼ばれるステータスに移行します。そのステータスでは、その状態がまだ存在する可能性があると見なされます。次に、「clearing time」に移行し、最終的に「retaining」に移行します。この時点で、問題は解決されたと見なされ、ユーザが最近解決された問題を確認できるようにする目的のために障害オブジェクトは保持されます。

ライフサイクルの移行が発生するたびに、システムは自動的にそれを記録する障害記録オブジェクトを作成します。障害レコードは、作成後は変更されることはなく、レコード数が障害保持ポリシーで指定された最大値を超えた場合にのみ削除されます。

シビラティ（重大度）は、サービスを提供するシステムの機能に対するその状態の影響の概算値です。考えられる値は、Warning（注意）、Minor、Major および Critical です。Warning（注意）に相当するシビラティ（重大度）の障害は、導入されているサービスには現在影響を与えていない潜在的な問題を示します（たとえば、不完全または矛盾した構成など）。Minor および Major の障害は、提供されるサービスが低下する可能性があることを示します。Critical は、大規模な停電がサービスを著しく低下させていたり、同時にサービスが悪化していることを意味します。説明には、追加情報を提供したりトラブルシューティングに役立てるために用意された人間に解読可能な問題の説明が含まれます。

次の図は、障害とイベントに関するレポートを作成するプロセスを示します。

図 *125*：障害およびイベントのレポート/エクスポート



1. プロセスが障害のある状態を検出します。
2. プロセスが Event and Fault Manager に通知します。
3. Event and Fault Manager は障害ルールに従って通知を処理します。
4. Event and Fault Manager は、MIM で障害インスタンスを作成し、障害ポリシーに従ってそのライフ サイクルを管理します。
5. Event and Fault Manager は、APIC および接続されたクライアントに状態遷移を通知します。
6. Event and Fault Manager は、追加のアクションをトリガーします（syslog や call home など）。

ログ レコード オブジェクト

ログ レコード オブジェクトについて

Cisco Application Centric Infrastructure（ACI）ファブリックのイベント（生成された障害、クリアされた障害など）、Cisco Application Policy Infrastructure Controller（APIC）またはスイッチのイベントなど、すべてのイベントがデータベースに記録されるため、ユーザはステータス遷移の履歴、イベントなどをレビューすることが可能です。Cisco APIC ノードおよびスイッチ ノードはどちらも、障害、イベントなどを自ら生成して保存します。ただし、スイッチ ノードからのログ レコードは Cisco APIC にも複製されるため、Cisco APIC ノードおよびスイッチ ノードを含むファブリック全体のログ レコードを Cisco APIC から表示できます。さらに、Cisco APIC データベースは、Cisco APIC をアップグレードした後でも、Cisco APIC ノードおよびスイッチ ノードの両方のログ レコードを保持します。対照的に、スイッチをアップグレードすると、スイッチのログ レコードは失われます。

ログ レコード オブジェクトはシステムによって作成され、ユーザが変更または削除することはできません。ログ レコード オブジェクトのライフサイクルは、保持ポリシーによって制御されます。クラスごとのログ レコード オブジェクトの数が保持ポリシーの最大制限に達すると、最も古いログ レコード オブジェクトがデータベースから削除され、新しいレコード用のスペースが確保されます。

ログ レコード オブジェクトは、次のログ レコード クラスに分類されます。

- **[障害記録（Fault Records）]**：障害記録は、ライフサイクル変更の履歴を示します。障害ルールは、管理対象オブジェクト クラスで定義されます。管理対象オブジェクトに障害がある場合、障害が発生し、管理対象オブジェクトに関連付けられます。障害状態がなくなると、障害はクリアされます。障害が発生またはクリアされるか、ライフサイクル状態が変更されるたびに、FAULT 状態の変化を記録するために障害レコード オブジェクトが作成されます。

- **[イベント レコード（Event Records）]**：Cisco APIC によって管理されるイベントです。各イベント レコードは、スイッチまたは Cisco APIC ノードで発生したイベントを表します。イベント ルールは、管理対象オブジェクト クラスで定義されます。管理対象オブジェクトの状態がイベント ルールに一致すると、イベント（または `eventRecord` オブジェクト）が作成されます。たとえば、スイッチからカードを抜くと、スイッチ イベント マネージャはユーザ操作のイベント通知を生成します。

- **[監査ログ（Audit Logs）]**：監査ログは、管理対象オブジェクトが変更されたときに記録される履歴レコードであり、変更を行ったユーザが含まれます。監査ログには、システムによって内部的に変更された管理対象オブジェクトも記録されます。

- **[セッション ログ（Session logs）]**：セッション ログは、ユーザが Cisco APIC またはスイッチにログインまたはログアウトしたときに記録される履歴レコードであり、クライアントの IP アドレスが含まれています。

- **[正常性レコード（Health Records）]**：正常性レコードは、管理対象オブジェクトの正常性スコア変更の履歴レコードです。管理対象オブジェクトの正常性スコアが 5 ポイント変化するたびに、正常性レコード オブジェクトが作成されます。

ファブリック内の各ログ レコード オブジェクトの最大数は、保持ポリシーによって定義されます。これは、ファブリック全体で数百万になる可能性があります。このような大量のデータをクエリすると、クエリへの応答が遅くなり、最悪の場合、クエリが失敗する可能性があります。これを防止するために、Cisco APIC リリース 5.1(1) 以降、ログ レコード オブジェクトの応答が大幅に高速化されるように、特にリーダープロセスが強化されました。ただし、トレードオフとして、クエリ（ページ）間の並べ替えは保証されません。

クエリ パフォーマンスの向上と新しい制限は、このセクションで説明されているログ レコード オブジェクトのクエリにのみ適用されます。

Cisco APIC リリース 5.2(3) 以降、ログ レコード オブジェクトに対してのみサポートされる新しい API クエリ オプションの `time-range` を使用すると、Cisco APIC はページ間のソートを維持しながら、ログ レコード オブジェクトの API クエリにはるかに高速に応答できます。Cisco APIC GUI はまた、`time-range` オプションを使用することでパフォーマンスとソートを向上します。ログ レコード オブジェクトのクエリの詳細については、『*Cisco APIC REST API* 構成ガイド』リリース *4.2(x)* 以降）を参照してください。

GUI を使用したログ レコード オブジェクトの表示

Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して、Cisco APIC または スイッチのデータベースからログ レコードオブジェクトを表示できます。5.2(3) リリース以降、次のいずれかの方法を使用してログ レコード オブジェクトを表示します。

- ファブリック内のすべての Cisco APIC およびスイッチについて、**[システム（System）]**>> **[履歴（History）]**タブに移動し、**[作業（Work）]** ペインでいずれかのログ レコード タブを選択します。
- 特定のスイッチについては、**[ファブリック（Fabric）]**<>**[インベントリ（Inventory）]**タブに移動します。**[ナビゲーション（Navigation）]** ペインで、**[*pod_id*]**>>**[*leaf_name*]** に移動します。**[作業（Work）]** ペインで、**[履歴（History）]** タブを選択してから、ログ レコード サブタブの 1 つを選択します。

レコードは作成日時の降順で表示されます。**[過去 *x time_measurement* 内の履歴（History within the last x time_measurement）]** の右側にある下矢印をクリックして期間を選択することで、期間に基づいて表示されるログ レコードを絞り込むことができます。**[カスタム（custom）]** 選択により、任意の範囲の日付を指定できます。

1 つ以上のフィルタを作成して、表示されるログ レコードを絞り込むこともできます。**[属性でフィルタ（Filter by attributes）]** フィールドをクリックし、属性を選択し、演算子を選択してから、値を選択または入力します（属性に応じて）。作成するフィルタごとにこのプロセスを繰り返します。

または、レコードのテーブルの値にカーソルを合わせると、値の右側にフィルタアイコン（じょうごで表される）が表示され、アイコンをクリックします。これで、適切なパラメータを持つフィルタが自動的に作成されます。たとえば、障害レコードを表示しているときに障害コード F103824 のフィルタ アイコンをクリックすると、次のパラメータを使用してフィルタが作成されます。`Code == F103824` 自動作成されたフィルタは、`==` 演算子のみをサポートします。

[作業（Work）] ペインの下部にある **[行（Rows）]** ドロップダウン リストを使用して、1 ページに表示するレコードの数を選択します。**[行（Rows）]** の値を大きくすると、GUI の応答時間が遅くなる可能性があります。別のログ レコード クラスをクリックすると、**[行（Rows）]** の値はデフォルトの 10 にリセットされます。

[アクション（Actions）] メニューでは、次のアクションを実行できます。

- **[すべてダウンロード（Download All）]**：選択したクラスのすべてのレコードをローカル システムにダウンロードします。指定した時間範囲とフィルタは無視されます。レコードは XML または JSON ファイルとしてダウンロードできます。

[システム（System）]> > **[履歴（History）]** タブからログ レコード オブジェクトを表示している場合は、行の右端にある 3 つのドットをクリックして、その特定のレコードで追加のアクションを実行できます。 イベント レコードの場合、可能なアクションは次のとおりです。

- **[シビラティ（重大度）の変更（Change Severity）]**：イベントのシビラティ（重大度）を選択するシビラティ（重大度）に変更します。同じイベント コードを持つすべての新しいイベントにも、選択したシビラティ（重大度）が適用されます。同じイベント コードを持つ他のすべての既存のイベントのシビラティ（重大度）は変更されません。
- **[イベントを無視（Ignore Event）]**：イベントは表示されなくなり、同じイベント コードを持つすべての新しいイベントは表示されません。同じイベント コードを持つ他のすべての既存のイベントは引き続き表示されます。
- **[Object Store Browser で開く（Open in Object Store Browser）]**：Object Store Browser の特定のレコードを新しい Web ブラウザ タブで開きます。
- **[名前を付けて保存（Save As）]**：特定のレコードをローカル システムにダウンロードします。レコードは XML または JSON ファイルとしてダウンロードできます。

他のすべてのログ レコード クラスの場合、可能なアクションは次のとおりです。

- **[Object Store Browser で開く（Open in Object Store Browser）]**：Object Store Browser の特定のレコードを新しい Web ブラウザ タブで開きます。
- **[名前を付けて保存（Save As）]**：特定のレコードをローカル システムにダウンロードします。レコードは XML または JSON ファイルとしてダウンロードできます。

Errors

APIC エラー メッセージは通常、APIC GUI および APIC CLI に表示されます。これらのエラー メッセージは、ユーザが実行している処理、あるいはユーザが設定または管理しているオブジェクトに固有のものです。これらのメッセージには次のようなものがあります。

- Informational（情報提供）メッセージ。実行しているアクションのヘルプおよびヒントを提供します。
- 警告メッセージ。ユーザが構成または管理しているオブジェクト（ユーザーアカウントやサービスプロファイルなど）に関連するシステムエラーの情報を提供します。

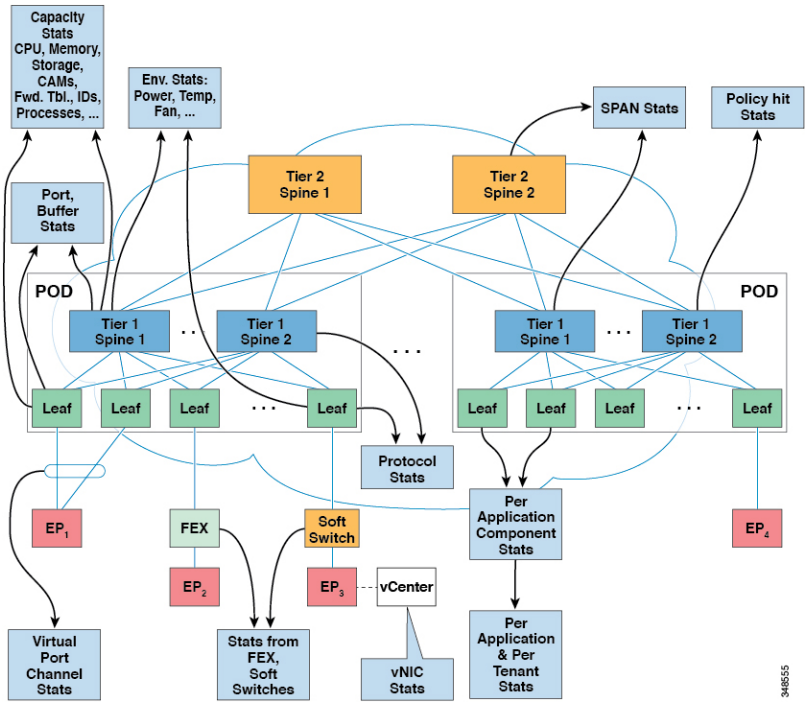
- Finite State Machine（FSM）のステータスメッセージ。FSM 段階のステータスに関する情報を提供します。

多くのエラーメッセージには、1つまたは複数の変数が含まれます。これらの変数を置き換えるために APIC が使用する情報は、メッセージのコンテキストによって決まります。一部のメッセージは、複数のタイプのエラーによって生成される場合があります。

統計プロパティ、階層、しきい値およびモニタリング

統計により、トレンド分析とトラブルシューティングが可能になります。統計収集は、継続的またはオンデマンドの収集用に構成できます。統計により、監視対象オブジェクトのリアルタイム測定が提供されます。統計は、累積カウンタとゲージで収集できます。

図 *126*：統計のさまざまな送信元



ポリシーは、収集する統計の種類、間隔、実行するアクションを定義します。たとえば、入力 VLAN でドロップされたパケットのしきい値が毎秒 1000 を超える場合、ポリシーは EPG 上で 1 つの障害を生成することができます。

統計データは、インターフェイス、VLAN、EPG、アプリケーションプロファイル、ACL ルール、テナント、内部 Cisco Application Policy Infrastructure Controller（APIC）プロセスなどのさまざまな送信元から収集されます。統計は、5 分、15 分、1 時間、1 日、1 週間、1 か月、1 四半期、または1年のサンプリング間隔でデータを蓄積します。短い期間の間隔によって、長い間隔が与えられます。

平均、最小、最大、傾向、変化のペースなど、さまざまな統計プロパティを使用できます。収集/保持時間は構成できます。ポリシーは、統計をシステムの現在の状態から収集するか、履歴的に蓄積するか、またはその両方かを指定できます。たとえば、ポリシーは、履歴統計を 1 時間にわたって 5 分間隔で収集するように指定できます。1 時間は移動ウィンドウです。1 時間が経過すると、次の 5 分間の統計が追加され、一番最初の 5 分間に収集されたデータが放棄されます。



（注） 5 分の粒度サンプル レコードの最大数は 3 サンプル（15 分の統計）に制限されています。他のすべてのサンプル間隔は、1,000 サンプル レコードに制限されています。たとえば、1 時間の粒度統計は 41 日間まで保持できます。統計は、これらの制限を超える期間は保持されません。長期間にわたって統計を収集するには、エクスポートポリシーを作成します。

統計データについて

次のタイプの管理対象オブジェクト（MO）は、オブザーバ モジュールによって収集される統計データに関連付けられています。

- 履歴データ
- 現在のデータ

これらのオブジェクトに対応する MO 名は、HD または CD の 2 文字のプレフィックスで始まります。HD は履歴データを示し、CD は現在のデータを示します。たとえば、「CDl2IngrBytesAg15min」です。MO 名は、データが収集される時間間隔の指標でもあります。たとえば、「CDl2IngrBytesAg15min」は、MO が 15 分間隔に対応することを示します。

CD オブジェクトは現在実行中のデータを保持しており、オブジェクトが保持する値は時間の経過とともに変化します。ただし、指定された時間間隔の最後に、CD オブジェクトで収集されたデータが HD オブジェクトにコピーされ、CD オブジェクトの属性が 0 にリセットされます。たとえば、指定された 15 分間隔の最後に、CDl2IngrBytesAg15min オブジェクトのデータが HDl2IngrBytesAg15min オブジェクトに移動され、CDl2IngrBytesAg15min オブジェクトがリセットされます。

CD...15min オブジェクト データを 15 分以上注意深く観察すると、値が 0 になり、その後 2 回増分され、再び 0 になることがわかります。これは、値が 5 分ごとに更新されるためです。データは HD オブジェクトにロールアップされ、その更新が発生するとすぐに CD オブジェクトがリセットされるため、3 回目の更新（15 分の経過後）は気付かれません。

CD...15min オブジェクトは 5 分ごとに更新され、CD...5min オブジェクトは 10 秒ごとに更新されます。CD...15min オブジェクトは HD...15min オブジェクトとしてロールアップされ、CD...5min オブジェクトは HD...5min オブジェクトとしてロールアップされます。

CD オブジェクトが保持するデータは動的であり、実際には内部データであると見なされる必要があります。HD データ オブジェクトは、さらなる分析目的に使用でき、公開データまたは静的データと見なすことができます。

HD オブジェクトも時間の経過とともにロールアップされます。たとえば、3 つの連続する HD...5min データ オブジェクトは、1 つの HD...15min オブジェクトに寄与します。1 つの HD...5 分オブジェクトがシステムに存在する時間の長さは、統計収集ポリシーによって決定されます。

モニタリング ポリシーの構成

管理者は、次の 4 つの広い範囲でモニタリング ポリシーを作成できます。

- ファブリック全体：ファブリック オブジェクトとアクセス オブジェクトの両方が含まれます。
- アクセス（別名インフラストラクチャ）：アクセス ポート、FEX、VM コントローラなど
- ファブリック：ファブリック ポート、カード、シャーシ、ファンなど
- テナント：EPG、アプリケーション プロファイル、サービスなど

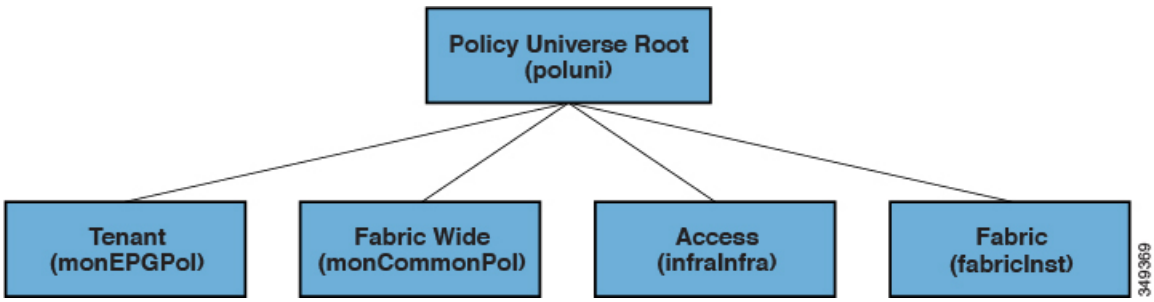
Cisco Application Policy Infrastructure Controller（APIC）には、デフォルトのモニタリング ポリシーの次の 4 つのクラスが含まれます。

- `monCommonPol`（uni/fabric/moncommon）：すべてのファブリック、アクセス、およびテナント階層に適用されます。
- `monFabricPol`（uni/fabric/monfab-default）：ファブリック階層に適用されます。
- `monInfraPol`（uni/infra/monifra-default）：アクセス インフラストラクチャ階層に適用されます。
- `monEPGPol`（uni/tn-common/monepg-default）：テナント階層に適用されます。

モニタリング ポリシーの 4 つのクラスそれぞれにおいて、デフォルト ポリシーは特定のポリシーによって上書きできます。たとえば、Solar テナント（*tn-solar*）に適用されたモニタリング ポリシーは、他のテナントがまだデフォルト ポリシーによってモニタされている一方で、Solar テナントのデフォルト ポリシーを上書きします。

次の図の 4 つのオブジェクトのそれぞれには、モニタリングのターゲットが含まれます。

図 *127*: デフォルト モニタリング ポリシーの *4* つのクラス



インフラ モニタリング ポリシーには monInfra ターゲットが含まれ、ファブリック モニタリング ポリシーには monFab ターゲットが含まれ、テナント モニタリング ポリシーには monEPG ターゲットが含まれます。各ターゲットは、この階層内のオブジェクトの対応するクラスを表します。たとえば、monInfra-default モニタリング ポリシーには、FEX ファブリック対面ポートを表すターゲットがあります。これらの FEX ファブリック対面ポートのモニタリング方法に関するポリシーの詳細はこのターゲットに含まれています。ターゲットに適用できるポリシーのみがそのターゲット下で許可されます。考えられるターゲットすべてがデフォルトで自動作成されるわけではないことに注意してください。管理者は、ターゲットがない場合にポリシー下でターゲットを追加できます。

共通モニタリング ポリシー（monCommonPol ）は、グローバル ファブリック全体の範囲を持ち、Cisco APIC を含むファブリック内のすべてのノードに自動的に展開されます。共通のモニタリング ポリシーの下にある送信元（syslog、callhome、SNMP など）は、すべての障害、イベント、監査、および正常性の発生をキャプチャします。単一の共通モニタリング ポリシーは、ファブリック全体をモニタします。syslog および snmp のシビラティ（重大度）のしきい値、または callhome の緊急度は、ファブリック管理者が適切であると判断した詳細レベルに従って構成できます。

複数のモニタリング ポリシーを使用して、ファブリックの個々の部分を個別にモニタできます。たとえば、グローバル モニタリング ポリシーの下にある送信元は、グローバル ビューを反映します。一部のノードにのみ展開されたカスタム モニタリング ポリシーの下にある別の送信元は、電源を詳しくモニタできます。または、異なるテナントの特定の障害またはイベントの発生は、n.jpgy 特定のオペレーターにリダイレクトできます。

他のモニタリング ポリシーの下にある送信元は、より小さな範囲内で障害、イベント、および監査をキャプチャします。モニタリング ポリシーの直下にある送信元は、範囲内（ファブリックやインフラなど）のすべての発生をキャプチャします。ターゲットの下にある送信元は、そのターゲットに関連するすべての発生をキャプチャします（たとえば、電源の eqpt:Psu）。障害/イベントの重大度の割り当てポリシーの下にある送信元は、その特定の障害またはイベントに一致する発生のみを、障害/イベント コードによって ide.jpgied としてキャプチャします。

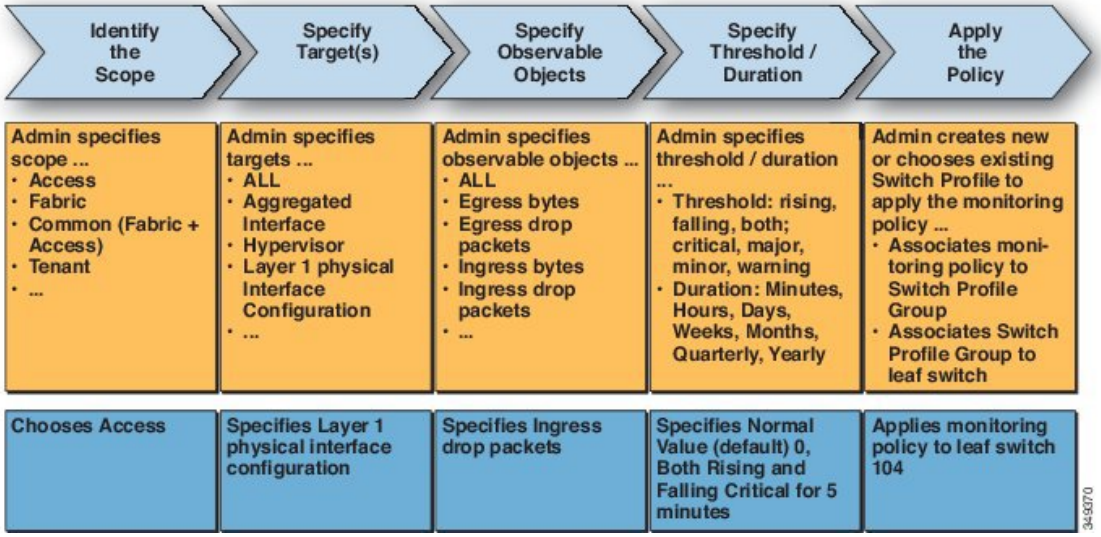
障害/イベント/監査が生成されると、該当するすべての送信元が使用されます。たとえば、次のようなコンフィギュレーションがあるものとします。

- syslog グループ 4 を指す syslog 送信元 4 は、障害 F0123 に対して定義されています。
- ターゲット電源（eqpt:Psu）に対して、syslog グループ 3 を指す syslog 送信元 3 が定義されています。
- syslog グループ 2 を指す syslog 送信元 2 は、範囲インフラ用に定義されています。
- syslog グループ 1 を指す syslog 送信元 1 は、共通の監視ポリシーに定義されています。

範囲インフラ内のクラス eqpt:Psu の MO で障害 F0123 が発生した場合、メッセージのシビラティ（重大度）が各送信元および接続先に定義された最小値以上であると想定して、syslog メッセージが syslog グループ 1 ～ 4 のすべての接続先に送信されます。 この例は syslog 構成を示していますが、callhome および SNMP 構成は同じように動作します。

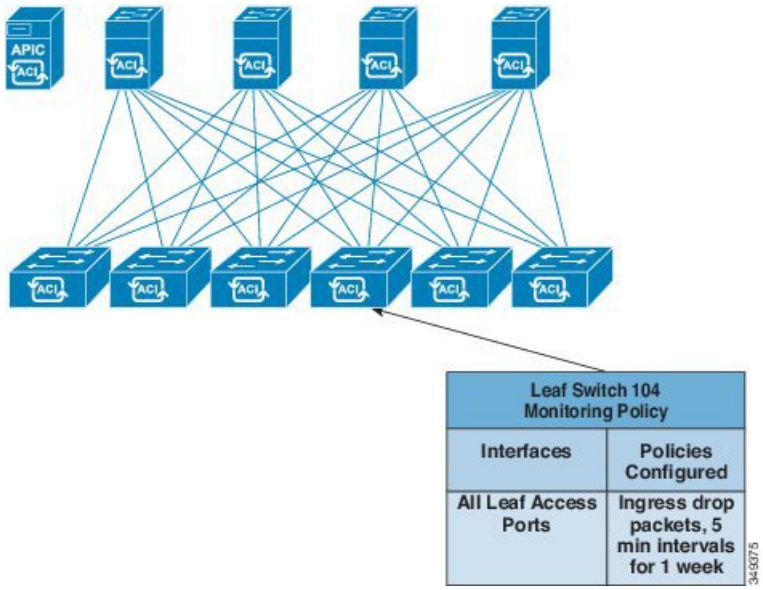
次の図は、統計用のファブリック モニタリング ポリシーを構成するプロセスがどのように動作するかを示します。

図 *128* : アクセス モニタリング ポリシーを構成するワークフロー



Cisco APIC は、次の図に示すように、このモニタリング ポリシーを適用します。

図 *129* : サンプルのアクセス モニタリング ポリシーの結果



モニタリングポリシーは、障害や正常性スコアなどの他のシステム操作に対しても構成できます。この階層へのモニタリング ポリシー マップの構造

ポリシーのモニタリング

- 統計のエクスポート
- 収集ルール
- モニタリング ターゲット

- 統計のエクスポート
- 収集ルール
- 統計情報
  - 収集ルール
  - しきい値ルール
  - 統計のエクスポート

次の図の [統計のエクスポートポリシー（Statistics Export policies）] オプションは、エクスポートする統計のフォーマットと接続先を定義します。出力は、FTP、HTTP、または SCP プロトコルを使用してエクスポートできます。形式は JSON または XML です。ユーザまたは管理者は、出力を圧縮することもできます。エクスポートは、[統計（Statistics）]、[モニタリング ターゲット（Monitoring Targets）] または最上位のモニタリング ポリシー下で定義できます。統計のエクスポートの上位レベルの定義は、定義された下位レベルのポリシーが存在しない限り優先されます。

モニタリング ポリシーは、セレクタまたは関係を使用して、特定の監視可能なオブジェクト（ポート、カード、EPG、テナントなど）または監視可能なオブジェクトのグループに適用されます。モニタリング ポリシーは次を定義します。

- 統計が収集され、履歴に保持されます。
- しきい値超過障害がトリガーされます。
- 統計がエクスポートされます。

収集ルールは、精密に指定されたサンプリング間隔ごとに定義されます。ルールでは、統計の収集をオンまたはオフにする必要があるかどうか、またオンにした場合、履歴保持期間をどうするべきかを構成します。モニタリング ターゲットは、監視可能なオブジェクトに相当します（ポートや EPG など）。収集ルールは、[統計（Statistics）]、[モニタリング ターゲット（Monitoring Targets）] または最上位のモニタリング ポリシー下で定義できます。収集ルールの上位レベルの定義は、定義された下位レベルのポリシーが存在しない限り優先されます。

統計は、統計カウンタのグループに相当します（入力カウンタ、出力カウンタ、またはドロップ カウンタなど）。

しきい値ルールは収集ルール下で定義され、親レベルの収集ルールで定義された、対応するサンプリング間隔に適用されます。

Tetration Analytics

Cisco Tetration Analytics エージェントのインストールについて

Cisco Tetration エージェントのインストールは、RPM Package Manager（RPM）ファイルを Cisco Tetration クラスタからダウンロードし、APIC にアップロードすることによって実行されます。Cisco Tetration クラスタは、Cisco Tetration エージェントの新しいバージョンがアップロードされるたびに、スイッチに通知を送信します。

スイッチへのイメージのインストールに関しては、次の 2 つのシナリオが考えられます。

- Cisco Tetration イメージがスイッチにインストールされていません。スイッチは APIC から通知を受信し、スイッチのコンテナに Cisco Tetration エージェント イメージをダウンロードしてインストールします。
- Cisco Tetration イメージがスイッチにインストールされ、スイッチが APIC から通知を受信します。このスイッチは、APIC バージョンが既にインストールされているエージェント イメージのバージョンよりも高いかどうかを確認します。バージョンが高い場合、スイッチは最新の Cisco Tetration イメージをダウンロードして、スイッチのコンテナにインストールします。

イメージは永続メモリにインストールされます。再起動時に、APIC からコントローラ通知を受信した後、スイッチは APIC で使用可能なイメージに関係なく Cisco Tetration エージェントを開始します。

NetFlow

NetFlow について

NetFlow テクノロジは、ネットワーク トラフィック アカウンティング、従量制のネットワーク課金、ネットワーク プランニング、そしてサービス拒絶に対する監視機能、ネットワーク監視、社外マーケティング、およびサービス プロバイダと企業顧客向け両方のデータ マイニングなど、主要な一連のアプリケーションの計測基盤を効果的にします。Cisco は NetFlow エクスポート データの収集、データ量削減、ポスト プロセッシングを行う一連の NetFlow アプリケーションを提供し、エンド ユーザー アプリケーションが NetFlow データへ簡単にアクセスできるようにします。この機能により、同じレベルを介したトラフィックのモニタリングを実行する、NetFlow がデータ センターを通過するトラフィックのモニタリングを有効にすると、Cisco Application Centric Infrastructure (Cisco ACI) ファブリック。

ハードウェアがレコードからコレクタに直接エクスポートする代わりに、レコードはスーパーバイザ エンジンで処理され、必要な形式で標準の NetFlow コレクタにエクスポートされます。

仮想マシン ネットワークでの NetFlow の構成については、『*Cisco ACI Virtualization Guide*』を参照してください。

NetFlow に関するサポートおよび制限事項

次のリストは、NetFlow で利用可能なサポートとそのサポートの制限に関する情報を提供します。

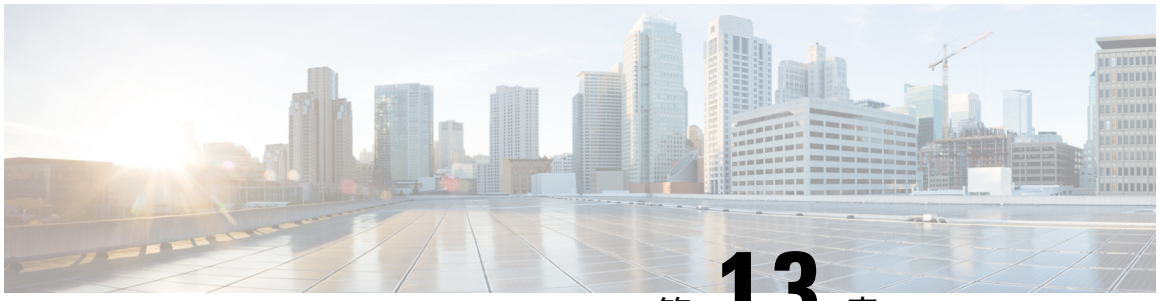
- EX、FX、FX2 以降のスイッチは NetFlow をサポートしています。特定のリリースでサポートされるスイッチ モデルの完全なリストについては、そのリリースの「*Cisco Nexus 9000 ACI* モード スイッチ リリース ノート」を参照してください。
- Cisco Application Policy Infrastructure Controller（APIC）リリース 4.0(1) 以降では、リモート リーフスイッチの NetFlow はサポート対象です。
- Cisco Application Centric Infrastructure（ACI）は NetFlow の入力のみをサポートし、NetFlow の出力はサポート対象外です。ブリッジドメインでは、NetFlow はスパイン スイッチから入ってくるパケットを確実にキャプチャできません。
- スパイン スイッチは NetFlow をサポートしていないため、スパイン スイッチのパケットからテナント レベルの情報をローカルに取得することはできません。
- ハードウェアは、アクティブ/非アクティブ タイマーをサポートしていません。フロー テーブル レコードはテーブルがフラッシュされると集約され、レコードは毎分エクスポートされます。
- すべてのエクスポート間隔で、ソフトウェア キャッシュがフラッシュされ、フローが長期間有効であっても、次の間隔でエクスポートされるレコードには、リセットされたパケット/バイト カウントおよびその他の統計が含まれます。
- フィルタ TCAM には、ブリッジドメインまたはインターフェイスのラベルがありません。NetFlow モニターを 2 つのブリッジドメインに追加すると、NetFlow モニターは IPv4 の場合は 2 つのルール、IPv6 の場合は 8 つのルールを使用します。そのため、スケールは 1K フィルタ TCAM で制限されます。
- ARP/ND は IP パケットとして処理され、それらのターゲット プロトコル アドレスは、プロトコル範囲として 249 から 255 までのいくつかの特別なプロトコル番号とともに IP フィールドに配置されます。NetFlow コレクタは、この処理を理解していない可能性があります。
- ICMP チェックサムはフロー レコードのレイヤ 4 src ポートの一部であるため、ICMP レコードの場合、他の非 TCP/UDP パケットと同様に、これがマスクされていないと多くのフロー エントリが作成されます。
- Cisco ACI-mode スイッチは、2 つのアクティブなエクスポータのみをサポートします。
- スイッチが CPU 生成パケットの VRF インスタンス間ルーティングを実行できないため、リーフスイッチからの NetFlow トラフィックがコレクタに到達できないことがあります。回避策として、NetFlow コレクタに使用される L3Out と同じ VRF インスタンスですでに構成されている EPG の偽の静的パスを作成します。偽のパスにより、トラフィックはコレクタに到達できます。

- 混合モードで NetFlow エクスポータ ポリシーを構成する場合、特定の VRF インスタンスのサブネットを構成できます。フロー テレメトリは、EPG に関連付けられているすべてのテナントを追跡します。サブネットごとに個別のポリシーを構成する必要はありません。

  たとえば、**t1:ctx2** VRF インスタンスのサブネットとして **0.0.0.0/0** を指定すると、フロー テレメトリは、関連付けられている VRF インスタンスに関係なく、すべての IPv4 フローを追跡します。

- NetFlowエクスポータ エンドポイントがブリッジ ドメインの背後にある場合は、ブリッジ ドメインのユニキャスト ルーティング ノブを有効にして、ブリッジ ドメイン サブネットの URIB ルートをインストールする必要があります。ノブが無効になっている場合、パケットはコレクタに転送されず、コレクタ ポリシーに対して operSt が無効になります。

- NetFlow とフロー テレメトリを同時に有効にすることはできません。



第 13 章

トラブルシューティング

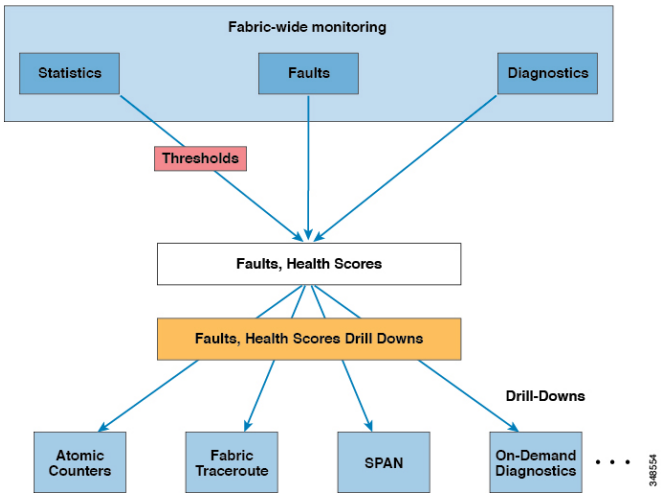
この章は、次の内容で構成されています。

- トラブルシューティング （333 ページ）
- ACL 契約の許可および拒否ログについて （334 ページ）
- ARP、ICMP Ping および Traceroute （335 ページ）
- アトミック カウンタ （336 ページ）
- デジタル オプティカル モニタリング（DOM）について （337 ページ）
- ヘルススコア （338 ページ）
- SPAN の概要 （344 ページ）
- SNMP について （345 ページ）
- Syslog について （345 ページ）
- トラブルシューティング ウィザードについて （346 ページ）
- Cisco Nexus 9000 スイッチの安全な消去について （347 ページ）

トラブルシューティング

ACI ファブリックでは、次の図に示すように広範なトラブルシューティングとモニタリングのツールが提供されます。

図 *130 :* トラブルシューティング



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。

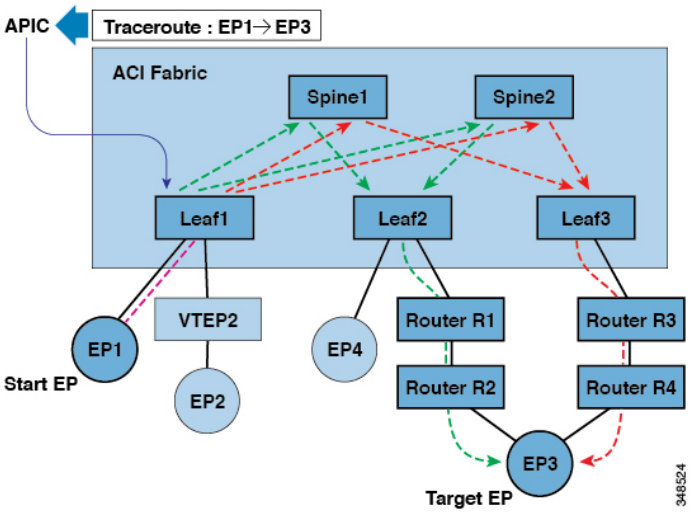
- 入力 TOR で入力ポリシーがインストールされており、出力 TOR で出力ポリシーがインストールされている場合の EPG から EPG へのフロー。
- 境界リーフ TOR で 1 個のポリシーが適用され、非 BL TOR で他のポリシーが適用されている場合の EPG から L3Out へのフロー。

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。

ARP、ICMP Ping および Traceroute

デフォルトゲートウェイ IP アドレスの ARP は入力リーフスイッチでトラップされます。入力リーフスイッチは ARP リクエストを接続先にユニキャストし、接続先は ARP 応答を送信します。

図 *131 : APIC* エンドポイント/エンドポイント トレースルート



テナントのエンドポイントから開始されたトレースルートは、入力リーフスイッチに表示される中間ホップとしてデフォルトゲートウェイを示します。

トレースルート モードには、エンドポイント/エンドポイント、リーフ/リーフ（TEP/TEP）があります。トレースルートはファブリック全体のすべてのパスを検出し、外部エンドポイントの出口を検出します。パスが妨げられているかどうかを発見するのに役立ちます。

トレースルートはIPv6の送信元と宛先アドレスで動作しますが、IPv4アドレスとIPv6アドレスを混在させて送信元IPアドレスと宛先アドレスを構成することはできません。送信元（RsTrEpIpSrc）と接続先（RsTrEpIpDst）の関係は、fvIpタイプの送信元と接続先をサポートします。同じエンドポイントから複数のIPアドレスが学習されることがあります。管理者は、目的の送信元アドレスと宛先アドレスを選択します。

アトミック カウンタ

Cisco APIC リリース 6.1(2) 以降、アトミック カウンタはサポートされなくなりました。

アトミックカウンタは、ファブリック内のドロップと誤ルーティングを検出します。結果の統計により、アプリケーションの接続の問題をすばやくデバッグして分離できます。アトミックカウンタには、アクティブなファブリック ネットワーク タイム プロトコル（NTP）ポリシーが必要です。アトミック カウンタは、IPv6 または IPv4 の送信元アドレスと宛先アドレスに対して機能しますが、異なるアドレス ファミリ間では機能しません。

たとえば、管理者はすべてのリーフ スイッチでアトミック カウンタを有効にして、エンドポイント1からエンドポイント2のパケットをトレースすることができます。送信元と接続先のリーフスイッチ以外のリーフスイッチにゼロ以外のカウンタがある場合、管理者はそれらのリーフスイッチにドリル ダウンできます。

従来の設定では、ベアメタル NIC から特定の IP アドレス（エンドポイント）または任意の IP アドレスへのトラフィックの量をモニタすることはほぼ不可能です。アトミック カウンタでは、データ パスに干渉することなく、管理者がベアメタル エンドポイントから受信されたパケットの数を数えることができます。さらに、アトミックカウンタはエンドポイントまたはアプリケーショングループで送受信されるプロトコルごとのトラフィックをモニタリングできます。

リーフ間（TEP 間）のアトミック カウンタは次を提供できます。

- ドロップ、承認および超過パケットのカウント
- 最後の 30 秒などの短期間のデータ収集、5 分、15 分、またはそれ以上の長期間のデータ収集
- スパイン トラフィックごとの詳細（TEP、リーフ、または VPC の数が 64 未満の場合にのみ使用可能）
- 継続的なモニタリング

（注） リーフ間（TEP間）アトミック カウンタは累積であり、クリアできません。ただし、30 秒のアトミック カウンタは 30 秒間隔でリセットされるため、断続的な問題や再発する問題の分離に使用できます。

テナントのアトミック カウンタは次を提供できます。

- ドロップ、承認および超過パケットを含む、ファブリック全体のトラフィックのアプリケーション固有カウンタ
- モードは次を含みます。
  - Endpoint-to-endpoint アドレス、または Endpoint-to-endpoint IP アドレス。1 つのターゲット エンドポイントに複数の IP アドレスが関連付けられている可能性があることに注意してください。
  - EPG から EPG
  - EPG からエンドポイント
  - EPG から *（任意）
  - エンドポイントから外部 IP アドレス

5.2(3) リリース以降、エンドポイント セキュリティ グループ (ESG) は、これらのモードで EPG の代替として使用できます。

（注） アトミック カウンタの使用は、エンドポイントが異なるテナントまたは同じテナント内の異なる仮想ルート転送（VRF）インスタンス（コンテキストまたはプライベートネットワークとも呼ばれます）にある場合はサポートされません。アトミック カウンタは IPv6 の送信元と接続先で動作しますが、IPv4 アドレスと IPv6 アドレスを混在させて送信元 IP アドレスと宛先 IP アドレスを構成することはできません。

エンドポイントが同じ EPG に属している場合、IPv6 ヘッダーを持つレイヤ 2 ブリッジド トラフィックの、それらのエンドポイント間でのアトミック カウンタ統計は報告されません。

EPG または ESG から L3Out EPG に流れるトラフィックに対してアトミック カウンタが機能するには、すべてのプレフィックスとマッチさせるため、0/0 ではなく 0/1 および 128/1 を使用して L3Out EPG を設定します。

デジタル オプティカル モニタリング（DOM）について

リアルタイムのデジタル オプティカル モニタリング（DOM）データは SFP、SFP+、および XFP から定期的に収集され、警告およびアラームのしきい値テーブル値と比較されます。収集された DOM データは、トランシーバ送信バイアス電流、トランシーバ送信電力、トランシーバ受信電力、およびトランシーバ電源電圧です。

ヘルススコア

ACIファブリックは、ポリシーモデルを使用してデータを正常性スコアに組み入れます。正常性スコアは、システム、インフラストラクチャ、テナント、アプリケーション、またはサービスなどのさまざまなエリアに集約できます。

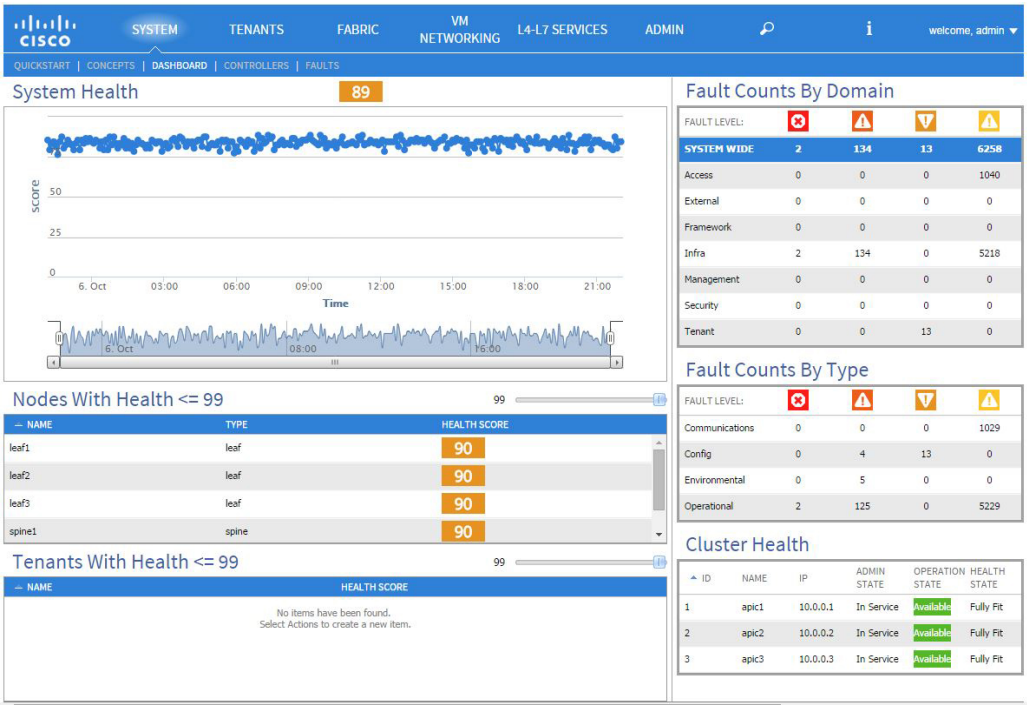
ACI ファブリック ヘルス情報は、システムの次の表示画面で見ることができます。

- System：ポッドの正常性スコア、テナントの正常性スコア、ドメインおよびタイプごとのシステム エラー数、APIC クラスタの正常性の状態など、システム全体の正常性の集約を示します。
- Pod：ポッド（スパインおよびリーフスイッチのグループ）の正常性スコアの集約、ドメインおよびタイプごとのポッド全体のエラー数を示します。
- Tenant：テナント固有のアプリケーションおよびEPGなどのオブジェクトのパフォーマンスデータを含むテナントの正常性スコアの集約、ドメインおよびタイプごとのテナント全体のエラー数を示します。
- Managed Object：管理対象オブジェクト（MO）（独立 MO および関連 MO を含む）の正常性スコア ポリシーを示します。これらのポリシーは、管理者によりカスタマイズできます。

システムおよびポッドの正常性スコア

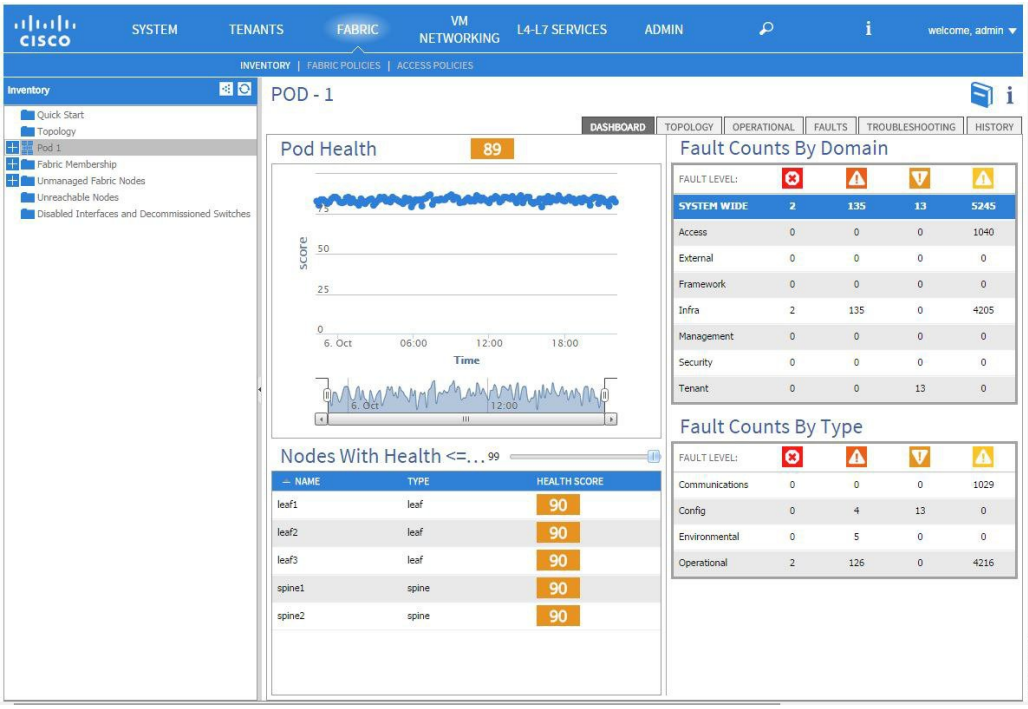
システムとポッドの正常性スコアは、リーフスイッチとスパインスイッチの正常性スコア、およびリーフスイッチで学習されたエンドポイントの数に基づいています。GUI システム ダッシュボードには、ドメイン タイプごとのシステム全体の障害数、およびノードごとのAPICクラスタの管理状態、動作状態、および正常性の状態も表示されます。

図 *132* : システム正常性スコア



ポッドの正常性スコアは、リーフスイッチとスパインスイッチのへ正常性スコア、およびリーフスイッチで学習されたエンドポイントの数に基づいています。GUI ファブリック ポッド ダッシュボード画面には、ドメインおよびタイプごとのポッド全体の障害数も表示されます。

図 *133* : ポッド正常性スコア



システムとポッドの正常性スコアは同じ方法で計算されます。この計算は、リーフ正常性スコアの加重平均を、リーフスイッチの学習済みエンドポイントの総数で割った値に、スパインの数とその正常性スコアから得られるスパイン係数を掛けたものに基づいています。

次の式は、この計算がどのように行われるかを示しています。

図 *134* : システムおよびポッドの正常性スコアの計算

$$Health_{Fabric} = \frac{\sum_{i=1}^{N_{Leaf}} Health_{Leaf_i} \times Weight_{Leaf_i}}{\sum_{i=1}^{N_{Leaf}} Weight_{Leaf_i}} \times \left(1 - \left(1 - \frac{\sum_{i=1}^{N_{Spine}} Health_{Spine_i}}{N_{Spine} \times 100}\right)^{N_{Spine}}\right)$$

304814

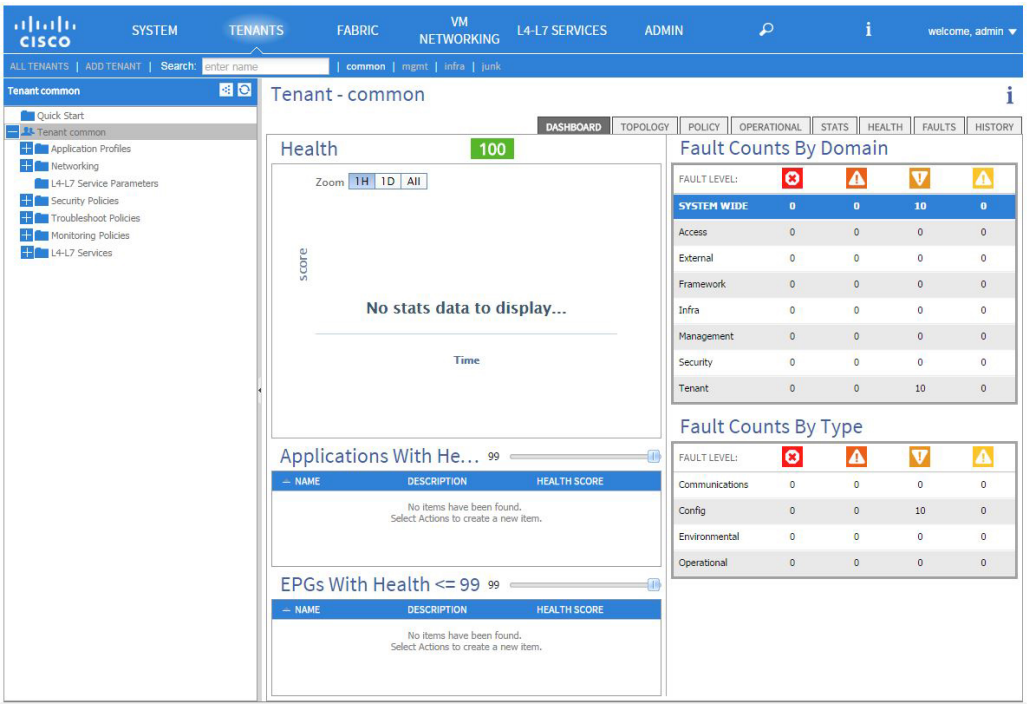
次の凡例は、方程式のコンポーネントを定義します。

- 正常性 $_{Leaf\,i}$ は、リーフスイッチの正常性スコアです。
- 重み $_{Leaf\,i}$ は、リーフスイッチのエンドポイントの数です。
- N $_{Leaf}$は、ファブリック内のリーフスイッチの数です。
- 正常性 $_{Spine\,i}$ は、スパイン スイッチの正常性スコアです。
- N $_{Spine}$ は、ファブリック内のスパイン スイッチの数です。

テナントの正常性スコア

テナントの正常性スコアは、テナントが使用するインフラストラクチャ全体のテナント全体の論理オブジェクトの正常性スコアを集計します。GUI テナント ダッシュボード画面には、ドメインおよびタイプごとのテナント全体の障害数も表示されます。

図 *135* : テナントの正常性スコア

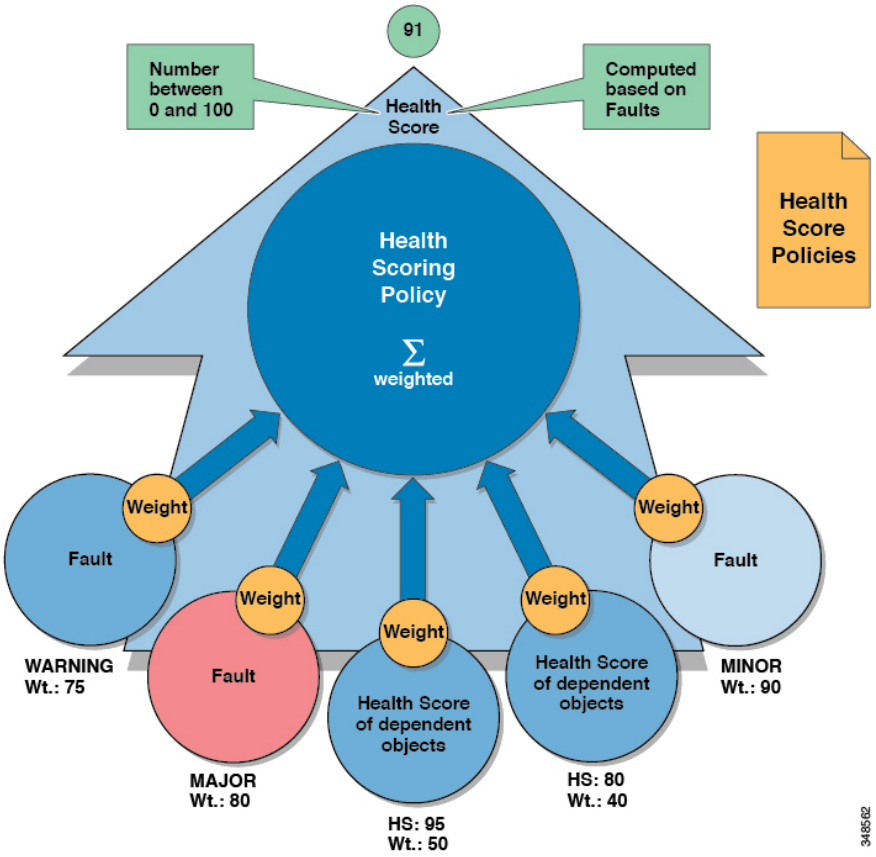


たとえば、EPGは2つのリーフスイッチのポートを使用している可能性があります。各リーフスイッチには、展開された EPG コンポーネントが含まれます。学習されたエンドポイントの数は、重み係数です。各ポートは、学習されたエンドポイントの数が異なる場合があります。したがって、EPG 正常性スコアは、各 EPG コンポーネントの正常性スコアとそのリーフで学習されたエンドポイントの数を合計し、EPGが使用するリーフスイッチ全体で学習されたエンドポイントの総数で割ったものになります。

MO 正常性スコア

各管理対象オブジェクト（MO）は、正常性スコアのカテゴリに属しています。デフォルトでは、MO の正常性スコアのカテゴリは MO のクラス名と同じです。

図 *136 : MO* 正常性スコア



各正常性スコア カテゴリには影響レベルが割り当てられます。正常性スコアの 5 つの影響レベルは、Maximum、High、Medium、Low および None です。たとえば、ファブリック ポートのデフォルトの影響レベルは Maximum で、リーフ ポートのデフォルトの影響レベルは High です。子 MO の特定のカテゴリは、正常性スコアの影響レベル None を割り当てることで、親 MO のヘルス スコアの計算から除外できます。これらのオブジェクト間の影響レベルは、ユーザが構成できます。ただし、デフォルトの影響レベルが None の場合は、管理者はこれを上書きできません。

次の係数は、さまざまな影響レベルです。

Maximum：100% High：80% Medium：50% Low：20% None：0%

カテゴリ正常性スコアは、Lp ノルム式を使用して計算されます。正常性スコア ペナルティは、100 - 正常性スコアと等しくなります。正常性スコア ペナルティは、所定のカテゴリに属し、正常性スコアが計算される MO の子または直接親族である MO のセットの全体的な正常性スコア ペナルティを表します。

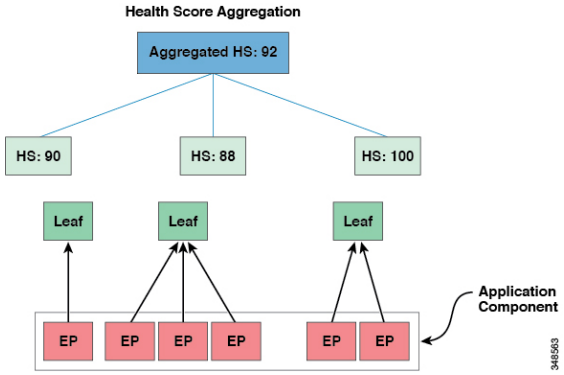
MO クラスの正常性スコアのカテゴリは、ポリシーを使用して変更できます。たとえば、リーフ ポートのデフォルトの正常性スコア カテゴリは `eqpt:LeafP` で、ファブリック ポートのデフォルトの正常性スコア カテゴリは `eqpt:FabP` です。ただし、リーフ ポートとファブリック

ポートの両方を含むポリシーは、ポートと呼ばれる同じカテゴリの一部になるように作成できます。

正常性スコアの集約と影響

アプリケーションコンポーネントの正常性スコアは、次の図に示すように複数のリーフスイッチに分散できます。

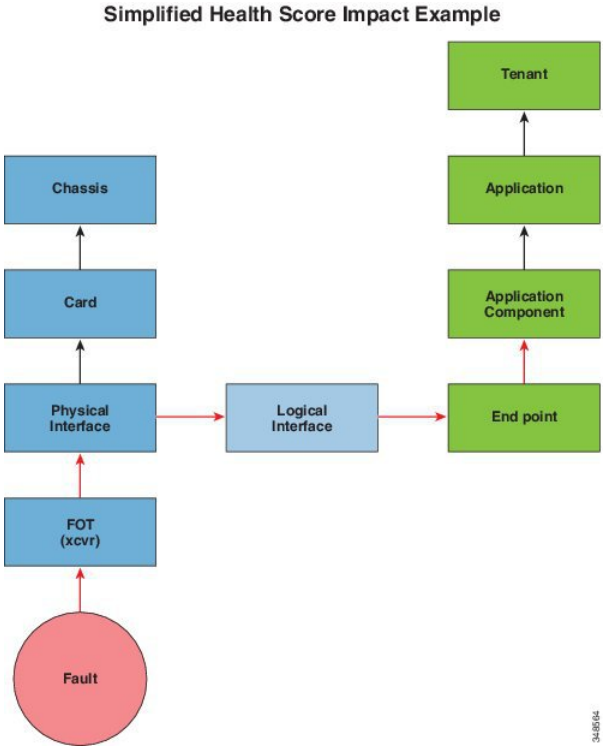
図 *137 :* 正常性スコアの集約



集約された正常性スコアは、APIC で計算されます。

次の図では、ハードウェアの障害が、アプリケーションコンポーネントの正常性スコアに影響します。

図 *138 :* 簡略化した正常性スコアの影響の例



SPAN の概要

スイッチドポートアナライザ（SPAN）ユーティリティを使って、詳細なトラブルシューティングの実行または特定のアプリケーションホストからトラフィックのサンプルを取得し、プロアクティブなモニタリングと分析を行うことができます。

SPANは1つ以上のポート、VLAN、またはエンドポイントグループ（EPG）からのトラフィックをコピーし、ネットワークアナライザによる分析のためにコピーしたトラフィックを1つ以上の送信先に送信します。このプロセスはどの接続デバイスも中断せず、ハードウェア内で実施されるので不要なCPU負荷を防ぎます。

SPANセッションはソースが受信したトラフィック（入力トラフィック）、ソースから送信したトラフィック（出力トラフィック）、またはその両方をモニタリングするように設定できます。デフォルトでは、SPANはすべてのトラフィックをモニタリングしますが、選択したトラフィックだけをモニタリングするようにフィルタを設定できます。

テナントまたはスイッチでSPANを設定できます。スイッチ上で設定する場合、SPANをファブリック ポリシーまたはアクセス ポリシーとして設定できます。

APICは、SPAN（ERSPAN）のカプセル化されたリモート拡張をサポートします。

マルチノード SPAN

APIC トラフィックのモニタリング ポリシーは、各アプリケーション グループのメンバーとそれが接続する場所を追跡するために、適切な場所でポリシーを SPAN することが可能です。いずれかのメンバーが移動した場合、APIC は新しいリーフ スイッチに自動的にポリシーをプッシュします。たとえば、エンドポイントが新しいリーフ スイッチに VMotion すると、SPAN 設定が自動的に調整されます。

その他の情報

SPAN の設定、使用、および制限の詳細については、*Cisco APIC Troubleshooting Guide* を参照してください。

SNMP について

Cisco Application Centric Infrastructure（ACI）は、管理情報ベース（MIB）と通知（トラップ）を含む広範な SNMPv1、v2、および v3 のサポートを提供します。SNMP 標準では、Cisco ACI ファブリックを管理しモニタリングする各 MIB をサポートするサードパーティ製アプリケーションを使用できます。

SNMPv3 はさらに広範なセキュリティ機能を提供します。各 SNMPv3 デバイスで SNMP サービスを有効または無効にするように選択できます。また、各デバイスで SNMP v1 および v2 要求の処理方法を設定できます。

5.1(1) リリース以降、SNMPv3 は Secure Hash Algorithm-2（SHA-2）認証タイプをサポートします。

SNMP の使用方法の詳細については、『*Cisco ACI MIB Quick Reference*』を参照してください。

Syslog について

稼働中、シスコ アプリケーション セントリック インフラストラクチャ（ACI）システムでの障害またはイベントは、コンソール、ローカル ファイル、および別のシステム上のロギング サーバへのシステム ログ（syslog）の送信をトリガーできます。システム ログ メッセージには、通常、障害またはイベントに関する情報のサブセットが含まれます。システム ログ メッセージには、監査ログとセッション ログのエントリを含めることもできます。

（注） APIC およびファブリック ノードが生成できる syslog メッセージのリストについては、https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/syslog/guide/aci_syslog/ACI_SysMsg.html を参照してください。

多くのシステム ログ メッセージは、ユーザが実行している処理、あるいはユーザが設定または管理しているオブジェクトに固有のものです。これらのメッセージには次のようなものがあります。

- 情報メッセージ。実行している処理のヘルプおよびヒントを提供します。
- 警告メッセージ。ユーザが設定または管理しているオブジェクト（ユーザ アカウントやサービス プロファイルなど）に関連するシステム エラーの情報を提供します。

システム ログ メッセージを受信してモニタするためには、syslog 宛先（コンソール、ローカル ファイル、または syslog サーバを実行している 1 つ以上のリモート ホスト）を指定する必要があります。また、コンソールに表示されるか、ファイルまたはホストによってキャプチャされるメッセージのシビラティ（重大度）の最小値を指定できます。syslog メッセージを受信するローカル ファイルは `/var/log/external/messages` です。

Syslog 送信元は、オブジェクト モニタリング ポリシーを適用できる任意のオブジェクトにすることができます。送信されるメッセージのシビラティ（重大度）の最小値、syslog メッセージに含める項目、および syslog の宛先を指定できます。

Syslog の表示形式を NX-OS スタイル形式に変更できます。

これらのシステム メッセージを生成する障害またはイベントの詳細は、『*Cisco APIC Faults, Events, and System Messages Management Guide*』で説明しています。システム ログ メッセージのリストについては『*Cisco ACI System Messages Reference Guide*』を参照してください。

（注） システム ログ メッセージは、必ずしもシステムに問題があることを示しているとは限りません。単に情報を通知するだけのメッセージもありますし、通信回線、内部ハードウェア、またはシステム ソフトウェアに関する問題点の診断に役立つメッセージもあります。

トラブルシューティング ウィザードについて

トラブルシューティング ウィザードを使用すると、ネットワークの動作を理解して可視化できるため、問題が発生した場合にネットワークに関する懸念を緩和できます。たとえば、2 つのエンドポイントで断続的なパケット損失が発生しているが、その理由がわからない場合があります。トラブルシューティング ウィザードを使用すると、問題を評価できるため、この問題のある動作の原因であると思われる各マシンにログオンするのではなく、問題を効果的に解決できます。

このウィザードを使用すると、管理ユーザは、選択した送信元と接続先の特定の時間枠に発生する問題のトラブルシューティングを行うことができます。デバッグを実行する時間枠を定義でき、TAC に送信できるトラブルシューティング レポートを生成できます。

関連トピック

トラブルシューティング ウィザードの開始
トラブルシューティング ウィザードのトポロジについて

Cisco Nexus 9000 スイッチの安全な消去について

Cisco Nexus 9000 スイッチは、永続的なストレージを利用して、システム ソフトウェア イメージ、スイッチ構成、ソフトウェア ログ、および動作履歴を維持します。これらの各エリアには、ネットワーク アーキテクチャや設計の詳細など、ユーザ固有の情報と、潜在的な攻撃者からの目標ベクトルが含まれている可能性があります。安全な消去機能を使用すると、この情報を包括的に消去できます。これは、返品許可（RMA）を使用してスイッチを返品するとき、スイッチをアップグレードまたは交換するとき、または寿命に達したシステムを廃止するときに実行できます。

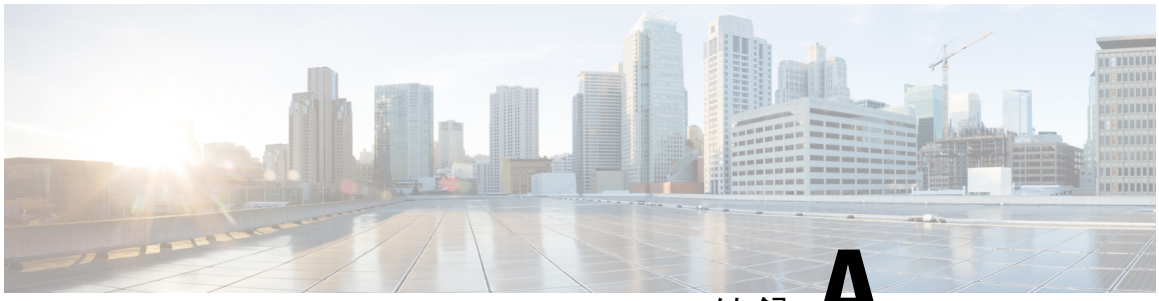
セキュア消去は、Cisco APIC リリース 6.0(x) からサポートされています。ファブリック内のすべてのリーフおよびスパイン スイッチは、APIC リリース 6.0(x) 以降である必要があります。

この機能は、次のストレージ デバイスのユーザ データを消去します。

- SSD
- EMMC
- MTD
- CMOS
- NVRAM



（注） すべてのスイッチ モデルにこれらすべてのストレージ デバイスがあるわけではありません。



付録 A

ラベルの一致

この章は、次の内容で構成されています。

- ラベルの一致 （349 ページ）

ラベルの一致

ラベル マッチングは、どのコンシューマおよびプロバイダーの EPG を通信可能にするかを決定するために使用されます。コントラクトの特定のプロデューサーまたはコンシューマのコントラクト サブジェクトは、コンシューマおよびプロバイダーが通信可能となることを決定します。

一致タイプのアルゴリズムは、次のいずれかの値を持つ matchT 属性によって決定されます。

- すべて
- AtLeastOne（デフォルト）
- [なし（None）]
- AtmostOne

EPG とコントラクトの情報カテゴリの両方のラベルが存在する場合、ラベル マッチングは最初に EPG に対して実行され、次にコントラクト情報カテゴリに対して実行されます。

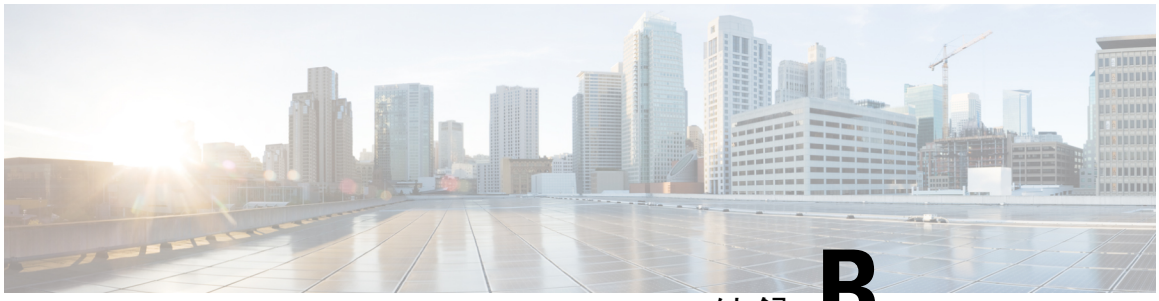
プロバイダー ラベル vzProvLbl とコンシューマ ラベル vzConsLbl の一致を確認する場合、matchT はプロバイダー EPG によって決定されます。

情報カテゴリを含む EPG 内でプロバイダーまたはコンシューマの情報カテゴリ ラベル vzProvSubjLbl および vzConsSubjLbl の一致を確認する場合、matchT は情報カテゴリによって決定されます。

同じ matchT ロジックは、EPG とコントラクトの情報カテゴリ ラベルでも同じです。次の表は、すべての EPG とコントラクトの情報カテゴリ プロバイダーおよびコンシューマの一致タイプとその結果の簡単な例を示します。この表で、[]エントリはラベルがないことを示します（NULL）。

ラベルの一致

matchT	vzProvLbl vzProvSubLbl	vzConsLbl vzConsSubLbl	結果は
すべて	[ ]	[ ]	一致
すべて	LabelX、LabelY	LabelX、LabelY	一致
すべて	LabelX、LabelY	LabelX、LabelZ	No Match
すべて	LabelX、LabelY	LabelX	No Match
すべて	LabelX	LabelX、LabelY	一致
すべて	[ ]	LabelX	No Match
すべて	LabelX	[ ]	No Match
AtLeastOne	LabelX、LabelY	LabelX	一致
AtLeastOne	LabelX、LabelY	LabelZ	No Match
AtLeastOne	LabelX	[ ]	No Match
AtLeastOne	[ ]	LabelX	No Match
AtLeastOne	[ ]	[ ]	一致
[なし（None）]	LabelX	LabelY	一致
[なし（None）]	LabelX	LabelX	No Match
[なし（None）]	LabelX、LabelY	LabelY	No Match
[なし（None）]	LabelX	LabelX、LabelY	No Match
[なし（None）]	[ ]	LabelX	No Match
[なし（None）]	LabelX	[ ]	一致
[なし（None）]	[ ]	[ ]	一致
AtmostOne	LabelX	LabelX	一致
AtmostOne	LabelX、LabelY	LabelX、LabelY	No Match
AtmostOne	LabelX、LabelZ	LabelX、LabelY	一致
AtmostOne	LabelX	LabelY	No Match
AtmostOne	[ ]	LabelX	No Match
AtmostOne	LabelX	[ ]	No Match
AtmostOne	[ ]	[ ]	一致



付録 B

コントラクト範囲の例

この章は、次の内容で構成されています。

• コントラクト範囲の例 （351 ページ）

コントラクト範囲の例

VRF1 に EPG1 と EPG2 があり、VRF2 に EPG3 と EPG4 があるとして、C1 と呼ばれるコントラクトおよび `scope = context` を使用します。

- EPG1 はコントラクト C1 を提供し、EPG2 はコントラクト C1 を消費します。
- EPG3 はコントラクト C1 を提供し、EPG4 はコントラクト C1 を消費します。

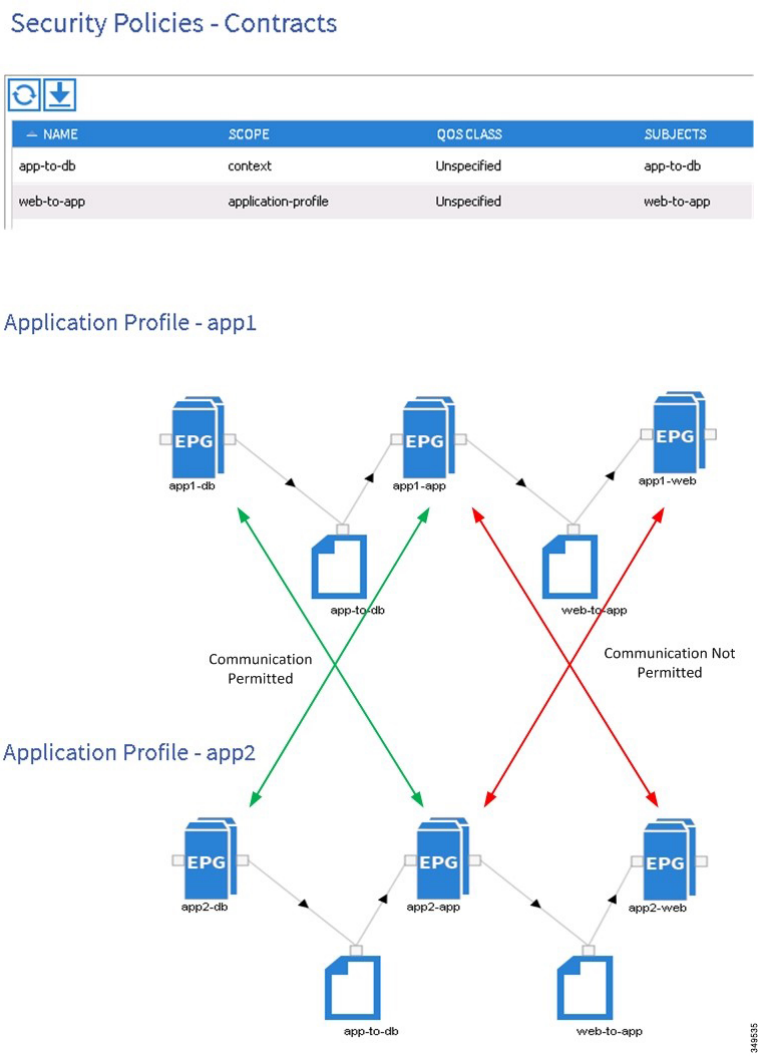
この例では、4 つすべての EPG が同じコントラクトを共有していますが、そのうちの 2 つが 1 つの仮想ルート転送（VRF）インスタンス（コンテキストまたはプライベートネットワークとも呼ばれる）にあり、そのうちの 2 つが他の VRF にあります。コントラクトは EPG1 と EPG2 の間でのみ適用され、EPG3 と EPG4 の間で個別に適用されます。コントラクトは、範囲が何であれ、この場合は VRF に限定されます。

`scope = application profile` の場合も同じです。2 つのアプリケーションプロファイルに EPG があり、`scope = application profile` である場合、コントラクトはアプリケーションプロファイルの EPG に適用されます。

以下に、2 つのコントラクトの APIC GUI スクリーンショットを示します。

コントラクト範囲の例

図 *139 :* セキュリティポリシーのコントラクトの例



1 つのコントラクトは、アプリケーション プロファイルの範囲を持つ Web からアプリへの通信用です。app-to-db コントラクトには、VRF の範囲があります。app1 および app2 アプリケーション プロファイルは、同じ VRF にあります。各アプリケーション プロファイルには EPG が含まれています。

app-to-db コントラクトの範囲は VRF レベルで適用され、両方のアプリケーション プロファイルが同じ VRF に属しているため、app-to-db コントラクトのすべてのコンシューマーはプロバイダー EPG と通信できます。

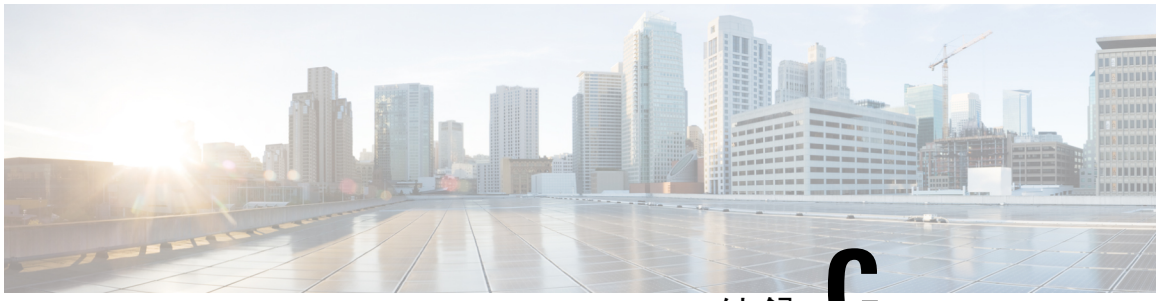
- EPG-app1-db は EPG-app1-app と双方向に通信できます
- EPG-app2-db は EPG-app2-app と双方向に通信できます
- EPG-app1-db は EPG-app2-app と双方向に通信できます
- EPG-app2-db は EPG-app1-app と双方向に通信できます

アプリケーション プロファイルの範囲を持つ Web からアプリへのコントラクトを使用するエンドポイントの次のペアは、コントラクトのプロバイダーとコンシューマーのみがそのアプリケーション プロファイル内で通信できるようにします。

- EPG-app1-app は EPG-app1-web と通信できます
- EPG-app2-app は EPG-app2-web と通信できます

上記とは異なり、アプリおよびデータベースの EPG は、アプリケーション プロファイルの外部で通信できません。

コントラクト範囲の例



付録 C

セキュアプロパティ

この章は、次の内容で構成されています。

- セキュアプロパティ （355 ページ）

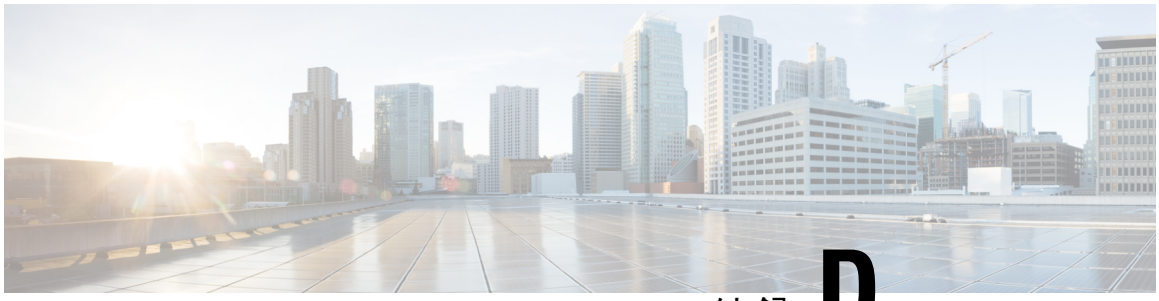
セキュアプロパティ

以下の表は、パスワード フィールド プロパティ タイプを含む管理対象オブジェクトのセキュリティで保護されたプロパティを示しています。

プロパティタイプ	管理対象オブジェクト クラス	プロパティ
[パスワード（Password）] フィールド	*pki:KeyRing*	*key*
	pki:WebTokenData	*hashSecret*
	pki:WebTokenData	*initializationVector*
	pki:WebTokenData	*key*
	pki:CsyncSharedKey	*key*
	pki:CertReq	*pwd*
	mcp:Inst	*key*
	mcp:InstPol	*key*
	sysdebug:BackupBehavior	*pwd*
	stats:Dest	*userPasswd*
	firmware:CcoSource	*password*
	firmware:InternalSource	*password*
	firmware:OSource	*password*
	firmware:Source	*password*
	bgp:PeerDef	*password*
	bgp:Peer	*password*
	bgp:APeerP	*password*
	bgp:PeerP	*password*
	bfd:AuthP	*key*
	comp:UsrAccP	*pwd*
	comp:Ctrlr	*pwd*
	aaa:LdapProvider	*key*
	aaa:LdapProvider	*monitoringPassword*
	aaa:UserData	*pwdHistory*
	aaa:TacacsPlusProvider	*key*
	aaa:TacacsPlusProvidermonitoring	*password*
	aaa:AProvider	*key*

プロパティタイプ	管理対象オブジェクト クラス	プロパティ
	aaa:AProvider	*monitoringPassword*
	aaa:RadiusProvider	*key*
	aaa:RadiusProvider	*monitoringPassword*
	aaa:User	*pwd*
	aaa:ChangePassword	*newPassword*
	aaa:ChangePassword	*oldPassword*
	ospf:AuthP	*key*
	ospf:IfPauth	*Key*
	ospf:AIfPauth	鍵
	ospf:IfDef	*authKey*
	file:RemotePath	*userPasswd*
	file:ARemotePath	*userPasswd*
	vmm:UsrAccP	*pwd*
	snmp:UserSecP	*authKey*
	snmp:UserSecP	*privKey*
	snmp:UserP	*authKey*
	snmp:UserP	*privKey*
	snmp:AUserP	*authKey*
	snmp:AUserP	*privKey*
	vns:VOspfVEncapAsc	*authKey*
	vns:SvcPkgSource	*password*
	vns:SvcPkgSource	*webtoken*
	vns:CCredSecret	*value*

セキュアプロパティ



付録 D

構成ゾーンでサポートされるポリシー

この章は、次の内容で構成されています。

- 構成ゾーンでサポートされるポリシー （359 ページ）

構成ゾーンでサポートされるポリシー

構成ゾーンでは、次のポリシーがサポートされています。

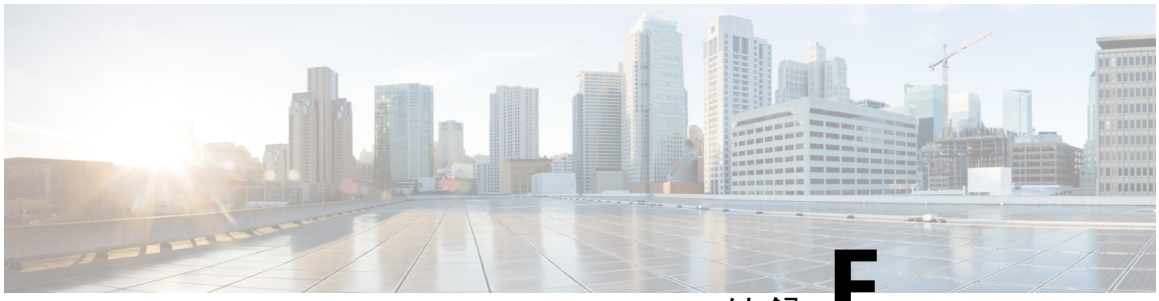
```
analytics:CfgSrv
bgp:InstPol
callhome:Group
callhome:InvP
callhome:QueryGroup
cdp:IfPol
cdp:InstPol
comm:Pol
comp:DomP
coop:Pol
datetime:Pol
dbgexp:CoreP
dbgexp:TechSupP
dhcp:NodeGrp
dhcp:PodGrp
edr:ErrDisRecoverPol
ep:ControlP
ep:LoopProtectP
eqptdiagp:TsOdFabP
eqptdiagp:TsOdLeafP
fabric:AutoGEp
fabric:ExplicitGEp
fabric:FuncP
fabric:HIfPol
fabric:L1IfPol
fabric:L2IfPol
fabric:L2InstPol
fabric:L2PortSecurityPol
fabric:LeCardP
fabric:LeCardPGrp
fabric:LeCardS
fabric:LeNodePGrp
fabric:LePortP
fabric:LePortPGrp
fabric:LFPortS
fabric:NodeControl
```

構成ゾーンでサポートされるポリシー

```
fabric:OLeafS
fabric:OSpineS
fabric:PodPGrp
fabric:PortBlk
fabric:ProtGEp
fabric:ProtPol
fabric:SFPortS
fabric:SpCardP
fabric:SpCardPGrp
fabric:SpCardS
fabric:SpNodePGrp
fabric:SpPortP
fabric:SpPortPGrp
fc:DomP
fc:FabricPol
fc:IfPol
fc:InstPol
file:RemotePath
fvns:McastAddrInstP
fvns:VlanInstP
fvns:VsanInstP
fvns:VxlanInstP
infra:AccBaseGrp
infra:AccBndlGrp
infra:AccBndlPolGrp
infra:AccBndlSubgrp
infra:AccCardP
infra:AccCardPGrp
infra:AccNodePGrp
infra:AccPortGrp
infra:AccPortP
infra:AttEntityP
infra:CardS
infra:ConnFexBlk
infra:ConnFexS
infra:ConnNodeS
infra:DomP
infra:FexBlk
infra:FexBndlGrp
infra:FexGrp
infra:FexP
infra:FuncP
infra:HConnPortS
infra:HPathS
infra:HPortS
infra:LeafS
infra:NodeBlk
infra:NodeGrp
infra:NodeP
infra:OLeafS
infra:OSpineS
infra:PodBlk
infra:PodGrp
infra:PodP
infra:PodS
infra:PolGrp
infra:PortBlk
infra:PortP
infra:PortS
infra:PortTrackPol
infra:Profile
infra:SHPathS
infra:SHPortS
infra:SpAccGrp
```

```
infra:SpAccPortGrp
infra:SpAccPortP
infra:SpineP
infra:SpineS
isis:DomPol
l2ext:DomP
l2:IfPol
l2:InstPol
l2:PortSecurityPol
l3ext:DomP
lacp:IfPol
lacp:LagPol
lldp:IfPol
lldp:InstPol
mcp:IfPol
mcp:InstPol
mgmt:NodeGrp
mgmt:PodGrp
mon:FabricPol
mon:InfraPol
phys:DomP
psu:InstPol
qos:DppPol
snmp:Pol
span:Dest
span:DestGrp
span:SpanProv
span:SrcGrp
span:SrcTargetShadow
span:SrcTargetShadowBD
span:SrcTargetShadowCtx
span:TaskParam
span:VDest
span:VDestGrp
span:VSpanProv
span:VSrcGrp
stormctrl:IfPol
stp:IfPol
stp:InstPol
stp:MstDomPol
stp:MstRegionPol
trig:SchedP
vmm:DomP
vpc:InstPol
vpc:KAPol
```

構成ゾーンでサポートされるポリシー



付録 E

ACI 用語

この章は、次の内容で構成されています。

• ACI 用語 （363 ページ）

ACI 用語

Cisco ACI 用語	業界標準用語（概算）	説明
エイリアス（Alias）	Alias	指定されたオブジェクトの変更可能な名前。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フィールドです。詳細については、「REST API の使用」の「タグとエイリアスの使用」セクションを参照してください。
API インスペクタ	—	Cisco APIC GUI の API インスペクタは、Cisco APIC が GUI インタラクションを実行するために処理する REST API コマンドのリアルタイム表示を提供します。

Cisco ACI 用語	業界標準用語（概算）	説明
アプリケーションセンター	—	Cisco ACI App Center を使用すると、コントローラで実行されるアプリケーションを作成することにより、Cisco APIC の機能を完全に有効にすることができます。Cisco ACI App Center を使用すると、お客様、デベロッパー、およびパートナーは、アプリケーションを構築して、ユースケースを簡素化、拡張、およびより可視化することができます。これらの アプリケーションは、Cisco ACI App Center でホストおよび共有され、Cisco APIC にインストールされます。
Application Policy Infrastructure Controller（APIC）	クラスタ コントローラの概算	複製された同期クラスタ コントローラとして実装される Cisco APIC は、Cisco ACI マルチテナント ファブリックの自動化と管理、ポリシー プログラミング、アプリケーション展開、およびヘルスモニタリングの統合ポイントを提供します。Cisco APIC クラスタの推奨最小サイズは3つのコントローラです。
アプリケーション プロファイル	—	アプリケーション プロファイル（fvAp）は、ポリシー、サービス、およびエンドポイント グループ（EPG）間の関係を定義します。
アトミック カウンタ	アトミック カウンタ	アトミック カウンタは、リーフ間のトラフィックに関する統計を収集できます。アトミック カウンタを使用すると、ファブリック内のドロップとルーティングミスを検出し、アプリケーション接続に関する問題の迅速なデバッグと分離が可能になります。たとえば、管理者はすべてのリーフ スイッチでアトミック カウンタを有効にして、エンドポイント 1 からエンドポイント 2 のパケットをトレースすることができます。送信元と接続先のリーフスイッチ以外のリーフスイッチにゼロ以外のカウンタがある場合、管理者はそれらのリーフスイッチにドリル ダウンできます。

Cisco ACI 用語	業界標準用語（概算）	説明
接続可能エンティティ プロファイル	—	アタッチ可能なアクセス エンティティ プロファイル（AEP）は、同様の要件を持つドメインをグループ化するために使用されます。ドメインを複数のAEPにグループ化してそれらを関連付けることで、ファブリックはドメイン内のさまざまなデバイスが稼働している場所を認識し、Application Policy Infrastructure Controller (APIC)は必要な場所に VLAN とポリシーをプッシュできるようになります。
境界リーフスイッチ	境界リーフスイッチ	境界リーフスイッチは、ファイアウォールやルータ ポートなどの外部ネットワーク デバイスまたはサービスをレイヤ 3 デバイスに接続するリーフです。サーバーなどの他のデバイスも接続できます。
ブリッジドメイン	ブリッジドメイン	ブリッジドメインは、同じフラッディングまたはブロードキャストの特性を共有する論理ポートのセットです。仮想 LAN（VLAN）のように、ブリッジドメインは複数のデバイスにまたがります。
Cisco ACI Optimizer	—	Cisco APIC GUI の Cisco ACI Optimizer 機能は、ネットワークに必要なリーフスイッチの数を決定し、制約に違反することなく各リーフスイッチに各アプリケーションと外部 EPG を展開する方法を提示できる Cisco APIC ツールです。また、現在の設定が必要なものを備えているかどうか、制限を超えているかどうかの判断を支援し、各リーフスイッチに各アプリケーションと外部 EPG を展開する方法を提示します。

ACI 用語

Cisco ACI 用語	業界標準用語（概算）	説明
Cisco Application Virtual Switch（AVS）	—	Cisco AVS は、仮想リーフとして Cisco ACI アーキテクチャと統合され、Cisco APIC によって管理される分散型の仮想スイッチです。さまざまな転送およびカプセル化オプションを提供し、VMware vCenter サーバーによって定義された多くの仮想化ホストおよびデータセンターに拡張します。
構成ゾーン	—	構成ゾーンは、Cisco ACI ファブリックをさまざまなゾーンに分割します。これらのゾーンは、異なる時間で構成変更を使用して更新できます。これにより、トラフィックを中断させたり、ファブリックをダウンさせたりする可能性のある、欠陥のあるファブリック全体の構成を展開するリスクを制限できます。管理者は、クリティカルでないゾーンに構成を展開し、それが適切であると判断した後でクリティカルなゾーンに展開することが可能です。詳細については、構成ゾーン を参照してください。
コンシューマ	—	サービスを利用する EPG。
コンテキストまたは VRF インスタンス	Virtual Route Forwarding（VRF）またはプライベートネットワーク	仮想ルーティングおよび転送インスタンスは、ルーティング テーブルの複数のインスタンスが存在し、同時に機能できるようにするレイヤ 3 アドレス ドメインを定義します。これにより、複数のデバイスを使用しなくてもネットワークパスをセグメント化することで、機能性が向上します。Cisco ACI テナントには、複数の VRF を含めることができます。

Cisco ACI 用語	業界標準用語（概算）	説明
コントラクト	アクセス コントロール リスト（ACL）の概算	ネットワーク内で許可される通信の内容と方法を指定するルール。Cisco ACI では、コントラクトは EPG 間の通信がどのように行われるかを指定します。コントラクト範囲は、アプリケーション プロファイル、テナント、VRF、またはファブリック全体の EPG に制限できます。
識別名（DN）	完全修飾ドメイン名（FQDN）の概算	MO を記述し、MIT でのその場所を特定する一意の名前。
エンドポイント グループ（EPG）	エンドポイント グループ	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構成体。Cisco ACI でエンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントは、アドレス（ID）、ロケーション、属性（バージョンやパッチ レベルなど）を持ち、物理の場合も仮想の場合もあります。エンドポイントの例には、インターネット上のサーバー、仮想マシン、ストレージ、またはクライアントが含まれます。
ファブリック	—	Cisco ACI ファブリックには、リーフ/スパイン Cisco ACI ファブリック モードで実行される Cisco APIC コントローラを搭載した Cisco Nexus 9000 シリーズ スイッチが含まれています。これらのスイッチは、各リーフノードをそれぞれのスパインノードに接続することで、「ファットツリー」ネットワークを形成します。他のすべてのデバイスは、リーフノードに接続されます。Cisco APIC は Cisco ACI ファブリックを管理します。

Cisco ACI 用語	業界標準用語（概算）	説明
フィルタ	アクセス制御リストの概算とファイアウォールの概算	Cisco ACI はホワイトリストモデルを使用します。デフォルトでは、すべての通信がブロックされます。通信には明示的な許可を与える必要があります。Cisco ACI フィルタは、EPG 間のインバウンドまたはアウトバウンド通信を許可するために使用される、レイヤ 3 プロトコル タイプやレイヤ 4 ポートなどの TCP/IP ヘッダー フィールドです。
GOLF	—	Cisco ACI GOLF 機能（ファブリック WAN のレイヤ 3 EVPN サービス機能とも呼ばれる）では、より効率的かつスケーラブルな Cisco ACI ファブリック WAN 接続が可能になります。スパインスイッチに接続されている WAN に OSPF 経由で BGP EVPN プロトコルが使用されます。
L2 出力	ブリッジ接続	ブリッジ接続は、同じネットワークの 2 つ以上のセグメントを接続して、通信できるようにします。Cisco ACI では、L2 Out は、Cisco ACI ファブリックと外部レイヤ 2 ネットワーク（通常はスイッチ）との間のブリッジされた（レイヤ 2）接続です。
L3 Out	ルーテッド接続	ルーティングされたレイヤ 3 接続は、送信元から接続先まで複数のネットワークを移動するためにデータがたどるパスを決定する一連のプロトコルを使用します。Cisco ACI のルーテッド接続は、BGP、OSPF、EIGRP など、選択されたプロトコルに従って IP 転送を実行します。

Cisco ACI 用語	業界標準用語（概算）	説明
ラベル	—	ラベル マッチングは、どのコンシューマおよびプロバイダーの EPG を通信可能にするかを決定するために使用されます。コントラクトの特定のプロデューサーまたはコンシューマのコントラクト サブジェクトは、コンシューマおよびプロバイダーが通信可能となることを決定します。ラベル マッチング アルゴリズムを使用して、この通信を決定します。詳細については、「ACI 基礎ガイド」を参照してください。
管理対象オブジェクト（MO）	月	管理対象のネットワーク リソースの要約文。Cisco ACI での、Cisco ACI ファブリック リソースの要約。
管理情報ツリー（MIT）	マサチューセッツ工科大学（MIT）	システムの管理対象オブジェクト（MO）のすべてを含む階層型管理情報ツリー。Cisco ACI では、MIT に Cisco ACI ファブリックのすべての MO が含まれています。Cisco ACI MIT は、管理情報モデル（MIM）とも呼ばれます。
Cisco ACI でのマイクロセグメンテーション	マイクロセグメンテーション、micro-segmentation	Cisco Application Centric Infrastructure（ACI）によるマイクロセグメンテーションは、さまざまなネットワークベースまたは仮想マシン（VM）ベースの属性に基づいて、エンドポイントをエンドポイント グループ（EPG）と呼ばれる論理セキュリティ ゾーンに自動的に割り当てる機能を提供します。

ACI 用語

Cisco ACI 用語	業界標準用語（概算）	説明
マルチポッド	—	マルチポッドは、隔離されたコントロール プレーン プロトコルを持つ複数のポッドで構成された、障害耐性の高いファブリックのプロビジョニングを可能にします。また、マルチポッドでは、さらに柔軟にリーフとスパイン スイッチ間のフル メッシュ配線を行うことができます。たとえば、リーフ スイッチが異なるフロアや異なる建物にまたがって分散している場合、マルチポッドでは、フロアごと、または建物ごとに複数のポッドをプロビジョニングし、スパイン スイッチを通じてポッド間を接続することができます。マルチポッドは、異なるポッドの Cisco ACI スパイン スイッチ間のコントロール プレーン通信プロトコルとして MP-BGP EVPN を使用します。詳細については、「Multipod ホワイトペーパー」を参照してください。

Cisco ACI 用語	業界標準用語（概算）	説明
ネットワーク ドメイン	—	ファブリック管理者は、ポート、プロトコル、VLAN プール、およびカプセル化を設定するドメイン ポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者が Cisco ACI ファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。次のドメイン タイプを構成できます。 • VMM ドメイン プロファイル（vmmDomP）は、仮想マシンのハイパーバイザ統合のために必要です。 • 物理ドメイン プロファイル（physDomP）は、ベア メタル サーバ接続と管理アクセスに使用します。 • ブリッジ外部ネットワーク ドメイン プロファイル（l2extDomP）は通常、Cisco ACI ファブリックのリーフ スイッチにブリッジされた外部ネットワーク トランク スイッチを接続するために使用されます。 • ルーテッド外部ネットワーク ドメイン プロファイル（l3extDomP）は、Cisco ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。 • ファイバ チャネル ドメイン プロファイル(fcDomP)は、ファイバ チャネルの VLAN と VSAN を接続するために使用されます。

Cisco ACI 用語	業界標準用語（概算）	説明
ポリシー	—	システム挙動の一定の側面を制御するための一般的な仕様を含む名前付きエンティティ。たとえば、レイヤ 3 外部ネットワーク ポリシーにはBGPプロトコルが含まれ、ファブリックを外部レイヤ 3 ネットワークに接続する場合にBGP ルーティング機能をイネーブルにできます。
プロファイル（Profile）	—	ポリシーの 1 つ以上のインスタンスを実行するのに必要な詳細な構成を含む名前付きエンティティ。たとえば、ルーティング ポリシーのスイッチ ノード プロファイルには、BGP ルーティング プロトコルを実装するために必要なすべてのスイッチ固有の詳細な構成が含まれます。
Provider	—	サービスを提供する EPG。
Quota Management	Quota Management	クォータ管理機能を使用すると、管理者は、特定のテナントの下に、またはテナント全体でグローバルに追加できる管理対象オブジェクトを制限できます。クォータ管理を使用すると、テナントまたはテナントのグループが、リーフスイッチごと、またはファブリックごとにCisco ACIの最大数を超えないように制限することができ、または利用可能なリソースの大部分を不当に消費して、同じファブリックの他のテナントに影響を及ぼすことがないように制限をかけることが可能です。 たとえば、ユーザが、障害アクションのあるACIポリシー モデル全体で最大 6 のブリッジドメイン クォータを構成したとします。コードは次のようになります。 `apic1(config)# quota fvBD max 6 scope uni exceed-action fault`

Cisco ACI 用語	業界標準用語（概算）	説明
REST API	REST API	Application Policy Infrastructure Controller（APIC）REST API は、REST アーキテクチャを使用するプログラマチック インターフェイスです。API は JavaScript オブジェクトの表記（JSON）または拡張マークアップ言語（XML）のドキュメントを含むHTTP（デフォルトでは無効）またはHTTPS のメッセージを受け入れ、返します。REST API は、管理情報ツリー（MIT）へのインターフェイスであり、オブジェクト モデルの状態を操作できます。Cisco APIC CLI、GUI、および SDK は同じ REST インターフェイスを使用するため、情報を表示する場合は常に、REST API を介して読み込まれ、構成変更が行われた場合は REST API を通じて書き込まれます。REST API は、統計、障害、監査イベントなど、他の情報を取得できるインターフェースも提供します。プッシュベースのイベント通知に登録する手段も提供されているので、MIT で変更が発生すると、Web ソケットを介してイベントが送信されます。
スキーマ（Schema）	—	Cisco ACI マルチサイト構成で、スキーマはポリシーの定義に使用される単一または複数のテンプレートのコンテナです。
サイト	サイト	Cisco ACI 領域および可用性ゾーンと見なされる Cisco APIC クラスタ ドメイン、または単一のファブリックです。その他のサイトと同じメトロ領域に配置することも、ワールドワイドに配置することもできます。

ACI 用語

Cisco ACI 用語	業界標準用語（概算）	説明
ストレッチ ACI	—	ストレッチ Cisco ACI ファブリックは、複数の場所に分散された Cisco ACI リーフおよびスパイン スイッチを接続する部分的にメッシュ化された設計です。ストレッチ ファブリックは、単一の Cisco ACI ファブリックです。サイトには 1 つの管理ドメインおよび 1 つの可用性ゾーンがあります。管理者は、サイトを 1 つのエンティティとして管理できます。 Cisco APIC コントローラ ノードで行われた構成変更は、サイト全体のデバイスに適用されます。拡張された Cisco ACI ファブリックは、サイト間のライブ VM 移行機能を保持します。複数のサイトに展開する場合、オブジェクト（テナント、VRF、EPG、ブリッジ ドメイン、サブネットまたはコントラクト）を拡張できます。
サブジェクト	アクセス制御リストの概算	Cisco ACI では、コントラクトの情報カテゴリは、どの情報をどのように伝達できるかを指定します。
タグ（Tags）	—	オブジェクト タグにより、API 操作が簡素化されます。API 操作では、識別名（DN）の代わりにタグ名でオブジェクトまたはオブジェクトのグループを参照できます。タグは、タグ付けするアイテムの子オブジェクトです。名前以外に他のプロパティはありません。 詳細については、「REST API の使用」の「タグとエイリアスの使用」セクションを参照してください。
テンプレート	テンプレート	Cisco ACI マルチサイト構成では、テンプレートは、さまざまなサイトにプッシュされるポリシーと構成オブジェクトを保持するフレームワークです。これらのテンプレートは、サイトごとに定義されたスキーマ内にあります。

Cisco ACI 用語	業界標準用語（概算）	説明
テナント	テナント	安全で排他的な仮想コンピューティング環境。Cisco ACI で、テナントはポリシーの観点から分離の単位ですが、プライベートネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。Cisco ACI テナントには、複数のプライベートネットワーク（VRF インスタンス）を含めることができます。
vzAny	—	vzAny管理対象オブジェクトは、各 EPG の個別のコントラクト関係を作成するのではなく、1つまたは複数のコンテキストに仮想ルーティングと転送 (VRF) のすべてのエンドポイント グループ (EPG) を関連付ける便利な方法を提供します。詳細については、「vzAny を使用して VRF 内のすべての EPG に通信ルールを自動的に適用する」を参照してください。

ACI 用語

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。