Cisco APIC 基本設定ガイド、リリース 6.0.x

最終更新：2025 年 7 月 18 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/

© 2022–2024 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 APIC の設定 3

Cisco Application Policy Infrastructure Controller 設定の推薦構成 3

Cisco Application Policy Infrastructure Controller のインターフェイス 4

ユーザー インターフェイスの混在に関する制限 5

コンフィギュレーションの検証 8

第 3 章

初回セットアップ ウィザード 9

初回セットアップ ウィザードについて 9

[Fabric Membership（ファブリック メンバーシップ）] 10

管理 11

vPC ペア 12

BGP 12

DNS 13

NTP 14

プロキシ 14

グローバル設定 15

第 4 章

ユーザ アクセス、認証およびアカウンティング 19

アクセス権のワークフローの依存関係 19

ユーザ アクセス、認可およびアカウンティング 20
マルチテナントのサポート 20
ユーザ アクセス：ロール、権限、セキュリティ ドメイン 20
ログイン ドメイン 22
GUI を使用してローカル ドメインを作成する 23
プロバイダーを作成する 26
ローカル ユーザの設定 31
GUI を使用したローカル ユーザの設定 31
GUI を使用した SSH 公開キー認証の設定 34
リモート ユーザの設定 35
外部認証サーバの AV ペア 35
外部認証サーバの AV ペアの設定 36
TACACS+ アクセス用の APIC の設定 37
RADIUS アクセス用の APIC の設定 38
APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の設定 38
Cisco AVPair を使用した APIC アクセス用の Windows Server 2012 LDAP の設定 40
LDAP アクセス用の APIC の設定 42
Cisco AV ペアが欠落しているか不良であるリモート ユーザのデフォルトの動作の変更 43
署名ベースのトランザクションについて 44
注意事項と制約事項 44
X.509 証明書と秘密キーの生成 45
ローカル ユーザの設定 46
GUI を使用したローカル ユーザの作成とユーザ証明書の追加 46
Python SDK を使用したローカル ユーザの作成 47
秘密キーを使用した署名の計算 48
アカウンティング 51
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 52

第 5 章 管理 53
管理のワークフロー 53

ACI 管理アクセスのワークフロー 53
管理アクセスの追加 55
GUI での管理アクセスの追加 55
IPv4/IPv6 アドレスおよびインバンド ポリシー 56
アウトオブバンド ポリシーの IPv4/IPv6 アドレス 57
既存の IP tables 機能をミラーリングする IPv6 の変更 57
管理アクセスの注意事項および制約事項 58
ウィザードによるインバンドおよびアウトオブバンド管理アクセスの設定 59
Cisco APIC GUI を使用したインバンド管理アクセスの設定 60
Cisco APIC GUI を使用したアウトオブバンド管理アクセスの設定 63
テクニカル サポート、統計情報、およびコア ファイルのエクスポート 65
ファイルのエクスポートについて 65
ファイルのエクスポートに関するガイドラインと制約事項 65
ファイル エクスポート用のリモート ロケーションの作成 66
GUI を使用したオンデマンド テクニカル サポート ファイルの送信 67
概要 67
設定ファイルの暗号化 68
GUI を使用したリモート ロケーションの設定 70
GUI を使用したエクスポート ポリシーの設定 70
GUI を使用したインポート ポリシーの設定 72
GUI を使用した設定ファイルの暗号化 72
コントローラ コンフィギュレーションのバックアップ、復元、およびロールバック 75
設定ファイルのバックアップ、復元、およびロールバックのワークフロー 75
fileRemotePath オブジェクトについて 76
コントローラへの設定のエクスポート 76
コントローラへの設定のインポート 79
スナップショット 81
スナップショット マネージャ ポリシー 82
ロールバック 84
Syslog の使用 86
Syslog について 86

Syslog の宛先および宛先グループの作成 87
Syslog 送信元の作成 89
アトミック カウンタの使用 90
アトミック カウンタについて 90
アトミック カウンタに関する注意事項および制約事項 92
アトミック カウンタの構成 94
SNMP の使用 95
SNMP について 95
Cisco ACI での SNMP アクセスのサポート 95
SNMP トラップ集約機能 96
SNMP の設定 97
GUI による SNMP ポリシーの設定 97
GUI による SNMP トラップ通知先の設定 99
GUI による SNMP トラップ ソースの設定 100
SNMP を使用したシステムのモニタリング 101
SPAN の使用 101
SPAN の概要 101
マルチノード SPAN 102
SPAN の注意事項と制約事項 103
GUI を使用した SPAN の設定 108
Cisco APIC GUI を使用したテナント SPAN セッションの設定 108
APIC GUI を使用した SPAN フィルタ グループの設定 109
APIC GUI を使用したアクセス SPAN ポリシーの設定 111
Cisco APIC GUI を使用したファブリック SPAN ポリシーの設定 112
APIC GUI を使用した外部アクセス用のレイヤ 3 EPG SPAN セッションの設定 113
Cisco APIC GUI を使用したテナント SPAN ポリシーの宛先グループの構成 114
Cisco APIC GUI を使用したアクセス SPAN ポリシーの宛先グループの設定 116
Cisco APIC GUI を使用したファブリック SPAN ポリシーの宛先グループの設定 117
NX-OS スタイルの CLI を使用した SPAN の構成 118
NX-OS スタイルの CLI を使用したアクセス モードでのローカル SPAN の設定 118
NX-OS スタイルの CLI を使用した SPAN フィルタ グループの設定 121

NX-OS スタイルの CLI を使用した SPAN フィルタ グループの関連付け 123
NX-OS スタイルの CLI を使用したアクセス モードでの ERSPAN の設定 124
NX-OS スタイルの CLI を使用したファブリック モードでの ERSPAN の設定 128
NX-OS スタイルの CLI を使用したテナント モードでの ERSPAN の設定 131
NX-OS スタイルの CLI を使用したグローバル SPAN-On-Drop セッションの設定 133
REST API を使用した SPAN の構成 135
REST API を使用した ERSPAN 宛先のファブリック宛先グループの設定 135
REST API を使用したグローバル ドロップ送信元グループの設定 135
REST API を使用した SPAN 宛先としてのリーフ ポートの設定 136
REST API を使用した SPAN アクセス送信元グループの設定 136
REST API を使用した SPAN ファブリック送信元グループの設定 137
REST API を使用した ERSPAN 宛先のアクセス宛先グループの設定 137
トレースルートの使用 138
トレースルートの概要 138
トレースルートの注意事項および制約事項 138
エンドポイント 間での traceroute の実行 139
acidiag コマンド 140

第 6 章 コア ACI ファブリック サービスのプロビジョニング 151
リンク レベル ポリシー 151
電磁場干渉に対する再トレーニング 151
GUI を使用したリンク レベル ポリシーの設定 152
ポート起動遅延 152
リンク レベル ポリシーの制限 152
リンク デバウンス間隔 153
リンク フラップ ポリシー 153
GUI を使用したリンク フラップ ポリシーの設定 154
時刻同期と NTP 154
インバンドの管理 NTP 155
NTP over IPv6 155
GUI を使用した NTP の設定 156

REST API を使用した NTP の設定 157
GUI を使用した NTP の動作の確認 158
NTPサーバ 158
GUI を使用した NTP サーバの有効化 159
GUI を使用した日時形式の設定 161
DHCP リレー ポリシーの設定 162
DHCP リレー ポリシーの注意事項と制約事項 165
GUI を使用した APIC インフラストラクチャに対する DHCP サーバ ポリシーの設定 166
REST API を使用してオプション 79 を設定する 169
NX-OS スタイル CLI を使用した APIC インフラストラクチャの DHCP サーバー ポリシーの設定 170
GUI を使用した APIC インフラストラクチャ用 DHCP サーバ ポリシーの設定 171
DNS サービス ポリシーの設定 172
インバンド DNS サービス ポリシーによる外部宛先の設定 173
デュアル スタック IPv4 および IPv6 DNS サーバ 174
デュアル スタック IPv4 および IPv6 環境 175
DNS プロファイルの IPv4 または IPv6 の優先順位のポリシー 175
GUI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定 176
カスタム証明書の設定 177
カスタム証明書の設定のガイドライン 177
GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定 178
ファブリック全体のシステム設定のプロビジョニング 182
APIC インバンドまたはアウトオブ バンド接続設定 (preferences) の設定 182
クォータ管理ポリシーの設定 183
適用 BD 例外リストの作成 183
BGP ルータ リフレクタ ポリシーとルート リフレクタ ノード エンドポイントの作成 184
ファブリック全体のコントロール プレーンの MTU ポリシーを設定する 185
エンドポイント ループ保護の設定 186
不正エンドポイント制御ポリシー 187
不正なエンドポイントの制御ポリシーについて 187
不正エンドポイント制御ポリシーの制限事項 187

GUI を使用した不正エンドポイント制御ポリシーの設定 188
NX-OS スタイル CLI を使用している不正エンドポイント制御ポリシーの設定 189
不正/ COOP 例外リストについて 190
不正/ COOP 例外リストのガイドラインと制限事項 190
GUI を使用したブリッジ ドメイン作成時の不正/ COOP 例外リストの設定 191
GUI を使用した既存のブリッジ ドメインの不正/ COOP 例外リストの設定 192
GUI を使用した L3Out SVI の不正エンドポイント制御の例外リストの構成 193
GUI を使用したファブリックの不正 エンドポイント制御 の MAC アドレス 例外を構成 194
最大 IP アドレス フロー制御について 194
COOP の設定 195
COOP について 195
GUI を使用した COOP 減衰エンドポイントの表示 197
スイッチ CLI を使用した COOP 減衰エンドポイントの表示 197
GUI を使用した COOP 減衰エンドポイントのクリア 198
スイッチ CLI を使用した COOP 減衰エンドポイントのクリア 198
RESTAPI を使用した COOP エンドポイント ダンプニングの無効化 198
APIC GUI を使用した COOP 認証の設定 199
Cisco NX OS スタイル CLI を使用した COOP 認証の設定 199
REST API を使用した COOP 認証の設定 199
エンドポイント リッスン ポリシー 200
エンドポイント リッスン ポリシーについて 200
GUI を使用したエンドポイント リッスン ポリシーの設定 200
IP エージングの設定 201
リモート エンドポイントの学習を無効にする 201
サブネット チェックのグローバルな適用 202
GIPo の再割り当て 203
ドメインの検証のグローバルな適用 204
OpFlex クライアント認証を有効にする 204
ファブリック ロード バランシング 205
Cisco APIC GUI を使用したロード バランサ ポリシーの作成 207

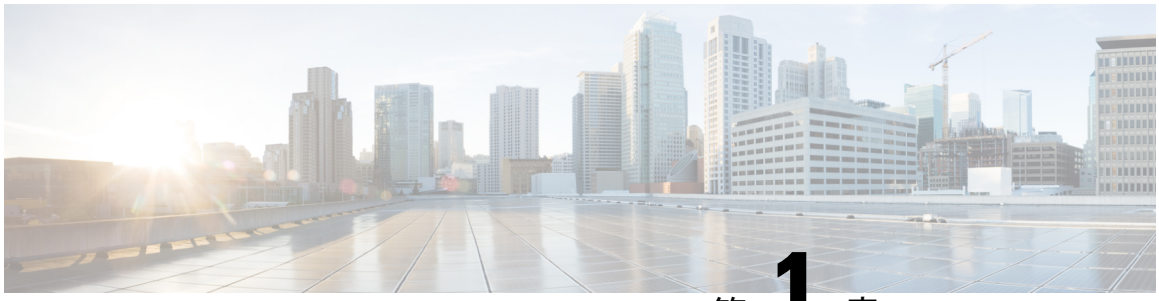
CLI を使用したロード バランサ ポリシーの作成 208
REST API を使用したロード バランサ ポリシーの作成 210
時間精度ポリシーの有効化 210
グローバル システム GIPo ポリシーの有効化 211
ファブリック ポート トラッキング ポリシーの設定 211
グローバル ファブリック アクセス ポリシーのプロビジョニング 212
グローバル接続可能アクセス エンティティ プロファイルの作成 212
QoS クラスのグローバル ポリシーを設定します。 214
グローバル DHCP リレー ポリシーの作成 214
グローバル MCP インスタンス ポリシーの有効化にします。 217
作成エラーには、回復ポリシーが無効になっています 217
ポート単位ポリシー 218
ポート単位ポリシーについて 218
GUI を使用したポート ポリシーごとの設定 218
GUI を使用したポート ポリシーごとの確認 219
GUI を使用した非表示ポリシーの表示 220
GUI を使用した誤配線プロトコル インターフェイス ポリシーの作成（任意） 220

第 7 章 基本ユーザ テナント設定 223
テナント 223
テナント内のルーティング 224
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 225
ルータ ピアリングおよびルート配布 227
外部ルータへのブリッジド インターフェイス 228
ルート リフレクタの設定 229
Layer 3 Out を使用した外部接続の設定 230
GUI を使用した MP-BGP ルート リフレクタの設定 230
ACI ファブリックの MP-BGP ルート リフレクタの設定 231
REST API を使用した MP-BGP ルート リフレクタの設定 231
MP-BGP ルート リフレクタ設定の確認 232
GUI を使用した管理テナントの OSPF L3Out の作成 233

NX-OS CLI を使用したテナントの OSPF 外部ルーテッド ネットワークの作成 235
テナント、VRF、およびブリッジ ドメインの作成 237
テナントの概要 237
テナントの作成 238
VRF およびブリッジ ドメイン 238
GUI を使用したテナント、VRF およびブリッジ ドメインの作成 238
EPG の導入 240
特定のポートへの EPG の静的な導入 240
GUI を使用して特定のノードまたはポートへ EPG を導入する 240
特定のポートに EPG を導入するためのドメイン、接続エンティティ プロファイル、および VLAN の作成 242
GUI を使用して特定のポートに EPG を展開するためのドメインおよび VLAN の作成 242
AEP またはインターフェイス ポリシー グループを使用したアプリケーション EPG の複数のポートへの導入 244
APIC GUI を使用した AEP による複数のインターフェイスへの EPG の導入 244
マイクロセグメント EPG 246
ベア メタルでのネットワークベースの属性によるマイクロセグメンテーションの使用 246
GUI を使用したベアメタル環境でのネットワークベースのマイクロセグメント EPG の設定 246
共有リソースとしての IP アドレスベースのマイクロセグメント EPG 249
GUI を使用した共有リソースとしての IP ベースのマイクロセグメント EPG の設定 249
GUI を使用した共有リソースとしての IP ベースのマイクロセグメント EPG の設定解除 250
アプリケーション プロファイルと契約の導入 251
セキュリティ ポリシーの適用 251
セキュリティ ポリシー仕様を含むコントラクト 252
Three-Tier アプリケーションの展開 255
http 用のフィルタを作成するパラメータ 256
rmi および sql 用のフィルタを作成するパラメータ 256
アプリケーション プロファイル データベースの例 257
GUI を使用したアプリケーション プロファイルの作成 257

GUI を使用した EPG の作成 257
APIC GUI を使用したコントラクトの設定 259
コントラクトとフィルタの注意事項と制約事項 259
GUI を使用したフィルタの作成 259
GUI を使用した契約の作成 260
GUI を使用した契約の消費と提供 260
コントラクト パフォーマンスの最適化 261
契約のパフォーマンスの最適化 261
GUI を使用して TCAM の使用が最適化された契約を設定する 264
契約とサブジェクトの例外 265
コントラクトまたはコントラクトの件名の例外の設定 265
GUI を使用したコントラクトまたはサブジェクトの例外の設定 266
EPG 内契約 267
EPG 内契約 267
EPG 内契約の注意事項と制約事項 268
GUI を使用したアプリケーション EPG への EPG 内契約の追加 269
NX-OS スタイル CLI を使用したアプリケーション EPG への EPG 内契約の追加 271
REST API を使用したアプリケーション EPG への EPG 内契約の追加 272
EPG のコントラクト継承 276
コントラクト継承について 276
GUI を使用した EPG のコントラクト継承の設定 278
GUI を使用したアプリケーション EPG のコントラクト継承の設定 278
GUI を使用した uSeg EPG のコントラクト継承の設定 279
GUI を使用した L2Out EPG のコントラクト継承の設定 279
GUI を使用して外部 L3Out EPG コントラクト継承 280
優先グループ契約 281
契約優先グループについて 281
契約優先グループの注意事項 283
GUI を使用した契約優先グループの設定 283
GUI を使用した L4-L7 サービス EPG ポリシーの作成 284
許可ルールと拒否ルールを含む契約 285

許可ルールおよび拒否ルールを含む契約の概要 285
GUI を使用してACL 契約の許可とロギングの拒否を有効にする 286
NX-OS CLI を使用した ACL 契約許可ロギングの有効化 287
REST API を使用した ACL 契約許可ロギングの有効化 287
GUI を使用した禁止契約拒否ロギングの有効化 288
NX-OS CLI を使用した禁止契約拒否ロギングの有効化 289
REST API を使用した禁止契約拒否ロギングの有効化 290
GUI を使用した ACL 許可および拒否ログの表示 290
REST API を使用した ACL 許可および拒否ログ 291
NX-OS CLI を使用した ACL 許可および拒否ログの表示 292



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。

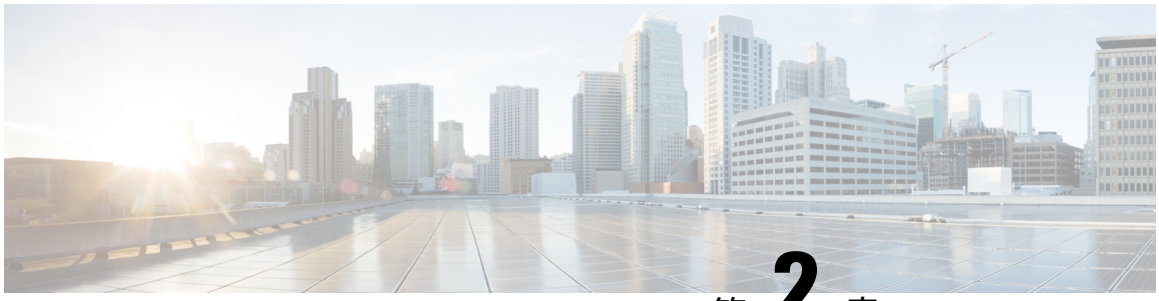
表 *1 : Cisco APIC* リリース *6.1(2)* の新機能および変更された機能に関する情報

特長	説明	参照先
ACI アクセス スパン L3Uut 上の ERSPAN 宛先	SPAN 宛先グループ機能を使用して、ERSPAN トラフィックを L3Out の背後にあるリモート エンドポイントに転送します。	Cisco APIC GUI を使用したテナント SPAN ポリシーの宛先グループの構成 （114 ページ）

新機能および変更された機能に関する情報

表 *2 : Cisco APIC* リリース *6.1(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 APIC OOB 管理サブネット IP アドレスが OOB IP アドレスにアクセスするのを制限します	Cisco APIC アウトオブバンド（OOB）サブネットで厳格なセキュリティを有効にすることで、Cisco APIC へのアクセスを制限できます。以前のリリースでは、ユーザーは、ユーザーの構成に関係なく、ICMP、SSH、HTTP、HTTPS、または TCP 4200 を使用して同じサブネットから OOB IP アドレスを使用して Cisco APIC にアクセスできました。	GUI での管理アクセスの追加（55 ページ）
ネットワーク タイム プロトコルの AES128-CMAC のサポート	Network Time Protocol（NTP）の AES128-CMAC 認証方式を使用できます。	時刻同期と NTP （154 ページ）



第 2 章

Cisco APIC の設定

- Cisco Application Policy Infrastructure Controller 設定の推薦構成 （3 ページ）
- Cisco Application Policy Infrastructure Controller のインターフェイス （4 ページ）
- ユーザー インターフェイスの混在に関する制限 （5 ページ）
- コンフィギュレーションの検証 （8 ページ）

Cisco Application Policy Infrastructure Controller 設定の推薦構成

特定の Cisco Application Policy Infrastructure Controller （APIC）設定を有効にすることをお勧めします。

Enforce Subnet Check

サブネット チェックの適用機能は、Cisco Application Centric Infrastructure（ACI）が IP アドレスをデータ プレーンからエンドポイントとして学習した場合、VRF インスタンス レベルでサブネットのチェックを適用します。サブネット チェックの範囲は VRF インスタンスですが、ファブリック全体での設定ポリシーの下では、この機能をグローバルにのみ有効または無効にすることができます。このオプションを有効にすると、ファブリックはブリッジ ドメインに構成されている 1 つのサブネット以外からは IP アドレスを学習しません。この機能は、このようなシナリオで、ファブリックがエンドポイント情報を学習しないようにします。

サブネットチェックの適用に関するガイドラインと制限事項

1 つの VRF インスタンスだけでこのオプションを有効にすることはできません。オプションを有効にすると、すべての VRF インスタンスで有効になります。

サブネット チェックの適用を有効にする

1. **[システム（System）] > [システム設定（System Settings）] > [ファブリック全体での設定（Fabric Wide Setting）]**
2. **[サブネット チェックの適用（Enforce Subnet Check）]** ボックスをオンにします。

IP エージング ポリシー

IP エージング ポリシーは、エンドポイント上の使用されていない IP アドレスを追跡し、その寿命を管理します。Cisco APIC は、ローカルのエンドポイント エージング間隔の 75% で、IPv4 の場合には ARP リクエスト、IPv6 の場合にはネイバー誘導を送信する、ブリッジ ドメイン用に構成されたエンドポイント保持ポリシーを使用して追跡を実行します。Cisco APIC が IP アドレスから応答を受信しなかった場合、その IP アドレスはエージング アウトします。

IP エージング ポリシーを有効にする

1. **[システム（System）] > [システム設定（System Settings）] > [エンドポイント制御（Endpoint Controls）]** に移動します。
2. **[IP エージング（IP Aging）]** タブをクリックします。
3. **[管理状態（Administrative State）]** で **[有効（Enabled）]** を選択します。

ミスケーブル プロトコル

ミスケーブルプロトコル（MCP）は、リンク層検出プロトコル（LLDP）やスパニング ツリー プロトコル（STP）では検出できない、さまざまな問題（構成ミスなど）によって発生する可能性のあるループを検出します。このオプションは、MCP が EPG 単位でパケットを送信できるようにします。

ミスケーブル プロトコルを有効にする

1. **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] >> [ポリシー（Policies）] > [グローバル（Global）] > [MCP インスタンス ポリシー デフォルト（MCP Instance Policy default）]** に移動します。
2. **[管理状態（Administrative State）]** で **[有効（Enabled）]** を選択します。
3. **[VLAN 単位での MCP PDU を有効にする（Enable MCP PDU per VLAN）]** ボックスをオンにします。

Cisco Application Policy Infrastructure Controller のインターフェイス

次のインターフェイスを使用して、アプリケーション プログラミング インターフェイス（API）を介して Cisco Application Policy Infrastructure Controller（APIC）のすべての機能にアクセスまたは構成できます。

GUI

Cisco APIC GUI は、内部的に REST API メッセージを交換することによって Cisco APIC エンジンと通信する、Cisco APIC へのブラウザベースのグラフィカル インターフェイスです。大規模な構成、展開、および運用には GUI を使用します。GUI を使用すれば、大規模なファブリック構成と展開を自動化するための、インスイッチ プロファイル、インターフェイス プロファ

イル、ポリシー グループ、アクセス エンティティ プロファイル（AEP）などのきめ細かなポリシー制御が可能です。

Cisco APIC GUI の詳細については、『*Cisco APIC Getting Started Guide*』「」および「」を参照して *Cisco APIC* ベーシック コンフィギュレーション ガイドください。

NX-OS スタイルの CLI

NX-OS スタイルのコマンドラインインターフェイス（CLI）は、Cisco APIC の構成、展開、および運用に使用できます。CLI は、EXEC モードをルートとするコマンド モードの階層にまとめられています。グローバル構成モードで始まる構成サブモードのツリーとなっています。使用できるコマンドは実行しているモードによって異なります。

Cisco APIC を構成するために、NX-OS スタイルの CLI と APIC GUI の両方を使用する場合の重要な注意事項については、ユーザー インターフェイスの混在に関する制限 （5 ページ） を参照してください。

REST API

REST API は設定の変更を受け入れ、コントローラの管理機能へのアクセスを提供します。このインターフェイスは、GUI や CLI の重要なコンポーネントであり、自動化ツール、プロビジョニング スクリプト、およびサードパーティのモニタリング ツールや管理ツールへのアクセス ポイントにもなっています。

Cisco 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。任意の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に関する記述を含むメッセージや、JSON または XML ドキュメントを生成できます。

REST API の詳細については、 *Cisco APIC REST API* 設定ガイドを参照してください。

ユーザー インターフェイスの混在に関する制限

Cisco APIC は構成のための複数のユーザー インターフェイス (UI) をサポートしているので、ある UI を使用して構成を作成し、その後別の UI を使用して構成を変更することは可能ですが、予期しない結果になることがあります。たとえば、NX-OS スタイル CLI を使用して実行された構成も、APIC GUI で表示できます。これらを表示できますが、時折 GUI で編集できない可能性があります。同様に、APIC GUI で行われた変更も、NX-OS スタイル CLI で確認はできますが、部分的にしか変更できないことがあります。

インターフェイスごとに設定する場合の NX-OS スタイルの CLI と Cisco APIC GUI の混在による制限

インターフェイスごとに設定する場合、Cisco APIC GUI で実行する設定は、NX-OS スタイルの CLI では部分的にしか機能しない場合があります。

たとえば、GUI の **[テナント（Tenants）] > [tenant-name] > [アプリケーション プロファイル（Application Profiles）] > [application-profile-name] > [アプリケーション EPG（Application EPGs）] > [EPG-name] > [スタティック ポート（Static Ports）] > [PC、VPC、インターフェイス上に静的 EPG を展開（Deploy Static EPG on PC, VPC, or Interface）]** でスイッチ ポートを構成したとします。次に NX-OS スタイルの CLI で **show running-config** コマンドを使用すると、以下のように出力されます。

```
leaf 102
interface ethernet 1/15
switchport trunk allowed vlan 201 tenant t1 application ap1 epg ep1
 exit
 exit
```

NX-OS スタイルの CLI でこれらのコマンドを使用してスタティック ポートを設定すると、次のエラーが発生します。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/15
apic1(config-leaf-if)# switchport trunk allowed vlan 201 tenant t1 application ap1 epg
ep1
No vlan-domain associated to node 102 interface ethernet1/15 encap vlan-201
```

これは、CLI に APIC GUI では実行されない検証があることが原因です。**show running-config** コマンドによって出力されたコマンドが NX-OS CLI で機能するためには、vlan ドメインが事前に構成されている必要があります。設定の順序は GUI に適用されません。

レイヤ 3 外部接続コンフィギュレーション モードのユーザ インターフェイスの混在に関する制限

ここでは、さらに他のユーザーインターフェイスを使用していた場合、NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を構成するための考慮事項を説明します。

APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定する場合、次の 2 つのモードを選択することができます。

- **暗黙モード**：シンプルなモードですが、APIC GUI または REST API と互換性がありません。
- **名前付き（または明示）モード**：APIC GUI および REST API と互換性があります。

いずれの場合も、設定は互換性がない UI では読み取り専用であると考えてください。

レイヤ 3 外部接続構成モードの違い

どちらのモードでも、構成設定は API の l3extOut クラスのインスタンスである内部コンテナ オブジェクト「Layer 3 Outside」（または「L3Out」）内で定義されます。2 つのモード間の主な違いは、このコンテナ オブジェクト インスタンスの命名にあります。

- **暗黙モード**：コンテナの命名は暗黙的であり、CLI コマンドには表示されません。CLI は、これらのオブジェクトを内部的に作成し保持します。
- **名前付きモード**： コンテナの命名を指定します。名前付きモードの CLI コマンドには、追加の l3Out フィールドがあります。名前付き L3Out を正常に構成し、障害を回避するた

めには、ユーザーが外部レイヤ 3 構成用の API オブジェクト モデルを理解する必要があります。

（注） 「名前付きモードを使用したレイヤ3外部接続の構成」セクションの手順を除き、このガイドでは、暗黙モードの手順を説明します。

レイヤ 3 外部接続構成モードの注意事項と制約事項

次の注意事項と制約事項は、レイヤ 3 外部接続構成モードに適用されます。

暗黙モードと名前付きモードの併用

同じ Cisco APIC インスタンスで、両方のモードを一緒に使用してレイヤ 3 外部接続を設定できます。ただし、テナント、VRF インスタンス、およびリーフ スイッチの特定の組み合わせに対するレイヤ 3 外部接続設定は、1 つのモードでのみ実行できます。

レイヤ 3 外部接続用に展開されたテナント VRF インスタンスに 1 つのモードを使用します。

特定のテナント VRF インスタンスの場合、外部 EPG を配置できるポリシー ドメインは、名前付きモードまたは暗黙モードのいずれかになります。推奨する構成方式は、特定のテナント VRF インスタンスがレイヤ3外部接続用に展開されるすべてのノード全体で、その特定のテナント VRF インスタンスの組み合わせに対する 1 つのモードだけを使用することです。モードは、異なるテナントまたは異なる VRF インスタンス全体で異なったものにすることができ、制限は適用されません。

構成は不整合に対して検証される可能性がある

場合によっては、Cisco APIC クラスタへの着信設定で不整合が検証されます。外部から確認できる設定（L3Out を通過するノースバウンド トラフィック）も検証の対象です。構成が無効な状況では、構成が無効であるとのエラー メッセージが表示されます。

外部レイヤ 3 機能でサポートされる構成モード

外部レイヤ 3 機能は、次の例外を除き、両方の構成モードでサポートされます。レイヤ 4 ～ レイヤ 7 サービス アプライアンスを使用したルート ピアリングおよびルート ヘルス インジェクション（RHI）は、指定されたモードでのみサポートされます。ルート ピアリングが関係するテナント VRF インスタンスのすべてのボーダー リーフ スイッチでは、名前付きモードを使用する必要があります。

暗黙モード CLI を使用して作成された L3Out は、GUI では読み取り専用です。

暗黙モード CLI 手順を使用して作成されたレイヤ 3 外部ネットワーク オブジェクト（L3Out とも呼ばれる）は、「_ui_」で始まる名前で識別され、GUI で読み取り専用としてマークされます。

暗黙モード CLI を使用して作成された L3Outs は、REST API を使用して変更された場合、CLI で変更できなくなる可能性がある

CLI は、インターフェイス、プロトコル、ルートマップ、EPG などの機能で、L3Out を分割します。REST API を使用して L3Out の構成を変更すると、この構造が壊れ、CLI を使用して L3Out を変更できなくなる可能性があります。

変更できない L3Out を削除するには、 *Cisco APIC Troubleshooting Guide*の「不要な _ui_ オブジェクトのトラブルシューティング」セクションを参照してください。

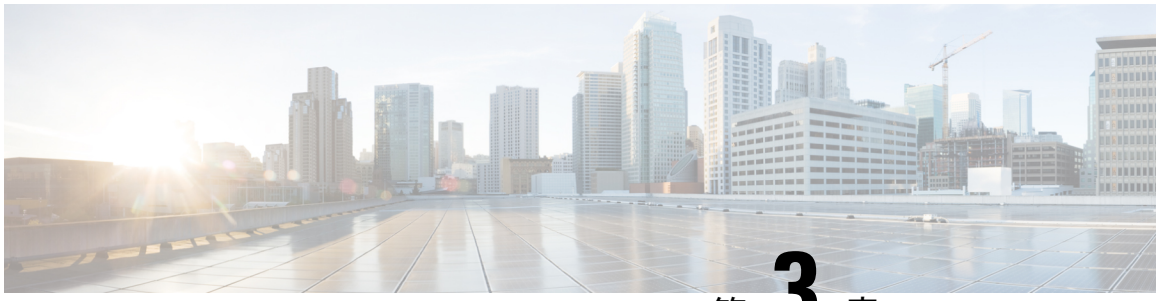
コンフィギュレーションの検証

管理者が Cisco Application Policy Infrastructure Controller（APIC）で構成を入力すると、Cisco APIC はチェックを実行して、構成が有効であるかどうかを確認します。これは検証と呼ばれます。Cisco APIC が構成を受け入れても、その構成が既存の構成と競合する場合、Cisco APIC またはリーフスイッチで障害が発生する可能性があります。構成を受け入れる前に Cisco APIC が実行するチェックの量は、リリースによって異なります。新しいリリースは、非同期的に障害が発生だけではなく、設定が受け入れられる前に、複数のチェックを実行する拡張されています。

これらの検証の目的を減らすか、設定を受け入れると、非同期的に障害を発生させるではなく設定時に、エラーのユーザを知らせるによって設定エラーを排除します。

また、Cisco APIC は、「アトミック」モードではなく「ベスト エフォート」モードで既存の構成をインポートするオプションも提供しています。このオプションは、無効な部分がある場合も、設定を承認する機能を提供します。Cisco APIC は、構成の有効な部分はプッシュし、検証と不整合な部分は無視します。不整合だった部分については、次のコマンドを実行すると、Cisco APIC はエラー メッセージを表示します。

show snapshot jobs *import_job*



第 3 章

初回セットアップ ウィザード

この章は、次の項で構成されています。

• 初回セットアップ ウィザードについて （9 ページ）

初回セットアップ ウィザードについて

初回セットアップ ウィザードを使用して、Cisco APIC の初回セットアップを実行します。

• GUI を使用して Cisco APIC に初めてログインすると、初回セットアップ ウィザードが自動的に表示されます。

• Cisco APIC リリース 4.2(3) 以降では、 GUI ウィンドウの右上隅にある [システムツール（System Tools）] アイコン（Cisco APIC）をクリックし、**[APIC_release_number の新機能（What's New in *APIC_release_number*）]** を選択すると、初期設定ウィザードにアクセスできます。

[APIC へようこそ（Welcome to APIC）] ウィンドウが表示され、この特定のリリースに含まれる新機能に関する情報が示されます。

初回セットアップ ウィザードにアクセスするには、ウィンドウの右下にある **[初回セットアップの開始（Begin First Time Setup）]** または **[初回セットアップの確認（Review First Time Setup）]** をクリックします。**[基本の設定（Let's Configure the Basics）]** ウィンドウが表示され、Cisco APIC の設定に使用できる個々のページへのリンクが示されます。

少なくとも 1 つの BGP ルートリフレクタを含む初期設定が完了すると、**[サマリを続行（Proceed to Summary）]** ボタンが有効になります。設定のサマリータイルを表示するには、このボタンをクリックします。追加のタイルが **[以下がお望みですか（You Might want to ...）]** 見出しの下に表示されます。. これらの追加トピックはオプションですが、推奨されます。

次の項では、このウィンドウから使用できる各初期設定ページの詳細について説明します。

[Fabric Membership（ファブリック メンバーシップ）]

[ファブリック メンバーシップ（Fabric Membership）] ウィンドウを使用して、ACI ファブリックによって検出されたリーフおよびスパイン スイッチを登録します。ボックスに記載されているシリアル番号を使用して、リーフ スイッチとスパイン スイッチをファブリックに手動で追加することもできます。

（注） 少なくとも 2 つのリーフ スイッチと 2 つのスパイン スイッチを登録することを推奨します。初回セットアップ ウィザードを進めるには、少なくとも 1 つのリーフ スイッチと 1 つのスパイン スイッチを登録する必要があります。

[ファブリック メンバーシップ（Fabric Membership）] ウィンドウには、次の 2 つのセクションがあります。

- **検出済み**：このセクションでは、新しく検出されたが未登録のスイッチについて説明します。これらのノードのノード ID は 0 で、IP アドレスはありません。
- **登録済み**：このセクションでは、ACI ファブリックに登録されているすべてのスイッチに関する情報を提供します。

次のいずれかの方法でスイッチを登録できます。

- スイッチが **[検出済み（Discovered）]** セクションに表示されている場合は、そのスイッチの横にある **[登録（Register）]** ボタンをクリックして、**[ファブリック ノード メンバーの作成（Create Fabric Node Member）]** ウィンドウを開きます。この場合、**[ポッド ID（Pod ID）]** フィールドと **[シリアル番号（Serial Number）]** フィールドは **[ファブリック ノード メンバーの作成（Create Fabric Node Member）]** ウィンドウに自動的に入力されます。
- スイッチが **[検出済み（Discovered）]** セクションに表示されない場合は、[アクション（Action）] アイコン（ ）をクリックし、ドロップダウン リストから **[ファブリック ノード メンバーの作成（Create Fabric Node Member）]** を選択します。

[ファブリック ノード メンバーの作成（Create Fabric Node Member）] ウィンドウで、次の情報を入力します。

フィールド	設定
ポッド ID	ノードが存在するポッドを特定します。
シリアル番号（Serial Number）	必須：新しいスイッチのシリアル番号を入力します。

フィールド	設定
ノード ID（Node ID）	必須：100 以上の数字を入力します。最初の 100 ID は、APIC アプライアンス ノードのために予約されています。 （注） リーフ ノードとスパイン ノードには異なる数字をつけることをお勧めします。たとえば、100 の範囲の番号リーフ (例：101、102) と 200 の範囲の番号スパイン (例：201、202)。 （注） ノード ID が割り当てられた後は、更新できません。ノードが **[登録済みノード (Registered Nodes)]** タブ表に追加された後、表の行を右クリックし、**[ノードとラック名の編集 (Edit Node and Rack Name)]** を選択してノードを更新できます。
Switch Name	leaf1 または spine3 などのノード名。
ノードタイプ（Node Type）	割り当てられたノードの役割を選択します。次のオプションがあります。 • **leaf** 必要に応じて、次のボックスのいずれかをオンにします。 • リモート • 仮想 • 階層 2 リーフ • **spine** 必要に応じて、次のボックスをオンにします。 • 仮想 • **unknown**

[ファブリック ノード メンバーの作成（Create Fabric Node Member）] ウィンドウで情報を入力したら、**[送信（Submit）]** をクリックし、**[ファブリック メンバーシップ（Fabric Membership）]** で **[続行（Continue）]** をクリックして、初回セットアップ ウィザードの次のウィンドウに進みます。

管理

[アウトオブバンド管理（Out of Band Management）] ウィンドウを使用して、アウトオブバンド（OOB）ネットワークに接続するリーフ スイッチ、スパイン スイッチ、および APIC ノードの管理インターフェイス IP アドレスを設定します。複数のノードを選択して、IP アドレスの割り当てを開始します。

（注） 初回セットアップ ウィザードは、アウトオブバンド管理用にまだ設定されていないノードの設定に役立ちます。

次のフィールドにゲートウェイのアドレスを入力すると、検出されたノードごとに IP アドレスが自動的に提案されます。

- **IPv4 ゲートウェイ**：アウトオブバンド管理を使用した外部ネットワークへの通信用のIPv4 デフォルト ゲートウェイ アドレス。
- **IPv6 ゲートウェイ**：アウトオブバンド管理を使用した外部ネットワークへの通信用のIPv6 デフォルト ゲートウェイ アドレス。

[属性によるフィルタ（Filter by attributes）] 領域では、検出されたノードを属性でフィルタ処理できます。アウトオブバンド管理用に設定するために選択したノードを変更する場合は、**[編集（Edit）]** をクリックします。

[保存する（Save）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

vPC ペア

[セットアップ - vPC ペア（Setup - vPC Pairs）] ウィンドウは、ファブリック ポリシー ノード エンドポイントを使用してグループのメンバー ノードを明示的に構成するために使用します。

[属性によるフィルタ（Filter by attributes）] 領域で、属性によって vPC ペアをフィルタリングできます。vPC ペアを設定するために選択した vPC ペアを変更する場合は、**[編集（Edit）]** をクリックします。

vPC ペア中央ペインで、**[アクション（Actions）]** ドロップダウン リストを展開し、**[vPC リーフ スイッチ ペアの作成（Create vPC Leaf Switch Pair）]**、**[vPC リーフ スイッチ ペアの削除（Delete vPC Leaf Switch Pair）]**、**[すべてダウンロード（Download All）]**、または **[オブジェクト ストア ブラウザで開く（Open in Object Store Browser）]** を選択します。

[保存する（Save）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

BGP

BGP ウィンドウを使用して、ACI ファブリックのルート リフレクタを設定し、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 ファブリックのルート リフレクタを有効にすると、外部ネットワークへの接続を設定できます。

（注） ルートリフレクタとして設定するスパインスイッチを選択します。初回セットアップウィザードを進めるには、少なくとも1つのルートリフレクタを設定する必要があります。このウィンドウのテーブルにスパインスイッチが表示されない場合は、スイッチが正しいタイプで登録されているか、APIC によって検出されていることを確認します。

[BGP] ウィンドウで、ルート リフレクタとして使用するスパイン スイッチの横にあるボックスをオンにし、**[自律システム番号（Autonomous System Number）]** フィールドにこのスパイン スイッチの ASN を入力します。**[保存して続行（Save and Continue）]** をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

DNS

DNS ウィンドウを使用して、リーフ スイッチ、スパイン スイッチ、および APIC ノードが DNS 名を照会できるように DNS サーバと検索ドメインを設定します。OOB 接続は DNS 通信に使用されます。

（注） 初回セットアップ ウィザードは、**デフォルト**の DNS ポリシーで DNS サーバと DNS ドメインを設定します。

DNS サーバを設定するには、[DNS サーバ（DNS Servers）] 領域で **[+]** をクリックし、次の情報を入力します。

- **アドレス**：プロバイダ アドレスを入力します。
- **希望**：優先するプロバイダとしてこのアドレスが必要な場合は、チェックボックスをオンにします。
- **ステータス**：設定要求のステータスを提供します。

[更新（Update）] をクリックし、必要に応じてこのプロセスを繰り返して追加の DNS サーバを設定します。

検索ドメインを設定するには、[ドメインの検索（Search Domains）] 領域で **[+]** をクリックし、次の情報を入力します。

- **名前**：ドメイン名（cisco.com）を入力します。
- **デフォルト**：チェックボックスをオンにして、このドメインをデフォルトドメインにします。デフォルトとして指定できるドメイン名は 1 つだけです。
- **ステータス**：設定要求のステータスを提供します。

[更新（Update）] をクリックし、必要に応じてこのプロセスを繰り返して追加の検索ドメインを設定します。

[DNS サーバ（DNS Servers）] テーブルまたは [ドメインの検索（Search Domains）] テーブルからエントリを削除するには、削除するエントリを選択し、そのテーブルのゴミ箱アイコンをクリックします。

[保存して続行（Save and Continue）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

NTP

NTP ウィンドウを使用してタイムゾーンを設定し、リーフ スイッチ、スパイン スイッチ、および APIC ノードを有効な時刻源に同期するように NTP サーバを割り当てます。OOB 接続は NTP 通信に使用されます。

（注） 初期セットアップ ウィザードは、**デフォルト**の NTP ポリシーでサーバを設定します。

[表示形式（Display Format）] 領域で、**[local]** をクリックして日付と時刻をローカル タイムゾーン形式で表示するか、**[utc]** をクリックして日付と時刻を UTC タイムゾーン形式で表示します。デフォルトは **[local]** です。

上記で **[local]** を選択した場合は、[タイムゾーン（Time Zone）] 領域で、ドロップダウン矢印をクリックしてドメインのタイムゾーンを選択します。ドロップダウン メニュー領域に入力して、ドロップダウン オプションをフィルタリングすることもできます。デフォルトは **[協定世界時（Coordinated Universal Time）]** です。

NTP サーバを設定するには、[NTP サーバ（NTP Servers）] 領域で **[+]** をクリックし、次の情報を入力します。

- **ホスト名/IPAddress**：NTP サーバのホスト名と IP アドレスを入力します。
- **希望**：複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の **[希望（Preferred）]** チェックボックスをオンにします。
- **ステータス**：設定要求のステータスを提供します。

[更新（Update）] をクリックし、必要に応じてこのプロセスを繰り返して追加の NTP サーバを設定します。

NTP サーバ テーブルからエントリを削除するには、削除するエントリを選択し、そのテーブルのゴミ箱アイコンをクリックします。

[保存して続行（Save and Continue）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

プロキシ

[プロキシ（Proxy）] ウィンドウを使用して、HTTP または HTTPS プロキシ ポリシーを構成します。設定すると、一部の Cisco Cloud Application Policy Infrastructure Controller（APIC）機能、

主に Cisco Intersight 接続などのインターネット アクセスを必要とする機能が、HTTP または HTTPS プロキシを介してトラフィックを送信します。詳細については、*Cisco APIC* システム管理設定ガイドを参照してください。

グローバル設定

[グローバル設定（Global Configurations）] ウィンドウを使用して、特定のエリアを設定します。これは、Cisco Application Centric Infrastructure（ACI）ファブリックの初回セットアップ中のベスト プラクティスとして推奨されます。**[OK]** をクリックします。次の領域を設定する準備ができたら、

- サブネット チェック （15 ページ）
- ドメイン検証 （16 ページ）
- 再配布されたルートの中間システムから中間システム （16 ページ）
- IP エージングの管理状態 （16 ページ）
- 不正なエンドポイントの制御 （16 ページ）
- COOP グループポリシー （17 ページ）

（注） このウィンドウの一部の設定は、[Fabric Wide Setting Policy]ページ（[System] [System Settings] [Fabric-Wide Settings]）で設定できる[Subnet Check]および[Domain Validation]の設定など、初回セットアップ後に設定できます。>>ただし、初回セットアップ後にこれらの設定を行うと、他の既存の設定で問題が発生する可能性があります。たとえば、**[ファブリック全体の設定ポリシー（Fabric Wide Setting Policy）]** ページで **[サブネット チェックの適用（Enforce Subnet Check）]** および **[ドメイン検証の適用（Enforce Domain Validation）]** の設定を有効にすると、インターフェイスまたはEPGにスタティックに割り当てられたポートに適切なポリシーチェーンがない場合、設定済みの L3Out 接続が切断される可能性があります。

サブネット チェック

この機能では、ある VRF で設定されたサブネットの外、つまり他のすべての VRF では、IP アドレス学習が無効になります。

この機能は、Cisco ACI () が IP アドレスをデータ プレーンからエンドポイントとして学習した場合、VRF インスタンス レベルでサブネットのチェックを適用します。このオプションをオンにすると、ファブリックは、ブリッジ ドメインで構成されたもの以外のサブネットからの IPアドレスを学習しなくなります。この機能は、このようなシナリオで、ファブリックがエンドポイント情報を学習しないようにします。

[適用（Enforce）] の横にあるチェックボックスをオンにして、サブネット チェック機能を有効にします。

ドメイン検証

この機能は、スタティック パスが追加されているが、ドメインが EPG に関連付けられていない場合に検証チェックを実行します。

有効な場合、スタティック パスが EPG に追加されているときに検証チェックが実行され、パスが EPG に関連付けられているドメインの一部であるか判断します。このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

[適用（Enforce）] の横のチェックボックスをオンにして、ドメイン検証機能を有効にします。これは強く推奨されています。

再配布されたルートの中間システムから中間システム

これは、IS-IS にすべてインポートされたルートに使用されている IS-IS メトリックです。このオプションで 64（最大）未満のメトリック（63 など）を設定すると、Cisco ACI では新しいスパインでルーティング コンバージェンスが達成されるまで、スイッチは安定したスパインからのルートを優先できます。

[IS-IS メトリック（IS-IS metric）] フィールドに適切な値を入力します。

IP エージングの管理状態

このポリシーを有効にすると、Cisco ACI では各 IP アドレスを個別に追跡し、未使用のアドレスを効率的にエージング アウトできます。それ以外の場合、未使用の IP アドレスは、ベース MAC アドレスが期限切れになるまで学習されたままになります。これはリモート エンドポイントには影響しません。

有効な場合、IP エージング ポリシーは、エンドポイント上の未使用の Ip アドレスをエージングします。この状況では、IP エージング ポリシーは、エンドポイントの IP アドレスを追跡する ARP 要求 (IPv4) とネイバー要請（IPv6）を送信します。応答が指定されていない場合、ポリシーは未使用の IPs アドレスをエージングします。

このフィールドのオプションは次のとおりです。

- **無効**：**デフォルト設定。 Cisco APICでは、IP エージング ポリシーを無視します。**
- **有効**：Cisco APIC は IP エージング ポリシーを監視します。

この機能を有効にすることを強くお勧めします。

不正なエンドポイントの制御

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 タグを変更し（エンドポイントの移動をエミュレート）、その結果、IP アドレスと MAC アドレスが異なる EPG とポートで迅速に学習されます。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。

不正エンドポイント制御機能は、この脆弱性に対処します。このポリシーを有効にすると、Cisco ACI で不正なエンドポイントを検出して削除できます。

このフィールドのオプションは次のとおりです。

- **無効**：デフォルト設定。Cisco APIC は、不正なエンドポイント制御ポリシーを無視します。
- **有効**：Cisco APIC は、不正エンドポイント制御ポリシーを監視します。

この機能を有効にすることを強くお勧めします。

[不正 EP 検出間隔（Rogue EP Detection Interval）]、**[不正 EP 検出倍数係数（Rogue EP Detection Multiplication Factor）]**、**[保持間隔（Hold Interval）]** などの不正エンドポイント制御の追加設定は、**[エンドポイント制御（Endpoint Controls）]** パネルから使用できます。**[エンドポイント制御（Endpoint Controls）]** パネルにアクセスするには、メニューバーで **[システム（System）]** > **[システム設定（System Settings）]** > **[エンドポイント制御（Endpoint Controls）]** をクリックし、**[不正 EP 制御（Rogue EP Control）]** タブをクリックします。

次に、**[エンドポイント制御（Endpoint Controls）]** ウィンドウの **[不正 EP 制御（Rogue EP Control）]** タブのフィールドの有効なデフォルト設定を示します。

- **不正 EP 検出間隔**：有効な値は 0 ー 65535 秒です。デフォルト値は 60 です。
- **不正 EP 検出倍数係数**：有効な値は 2 ー 65535 です。デフォルト値は4です。
- **保持時間**：5.2(1) および 5.2(2) リリースでは、有効な値は 1800 ー 3600 秒です。5.2(3) リリース以降、有効な値は 300 ー 3600 秒です。デフォルト値は 1800 です。

COOP グループポリシー

マッピング情報（ロケーションおよび ID）をスパイン プロキシに伝達するために、Council of Oracles Protocol（COOP）を使用します。リーフ スイッチは、Zero Message Queue（ZMQ）を使用して、エンドポイントアドレス情報をスパイン スイッチ「Oracle」に転送します。スパイン ノードで実行している COOP によって、すべてのスパイン ノードがエンドポイントの一貫したコピーと、マッピング データベースの場所情報を保持していることを確認します。

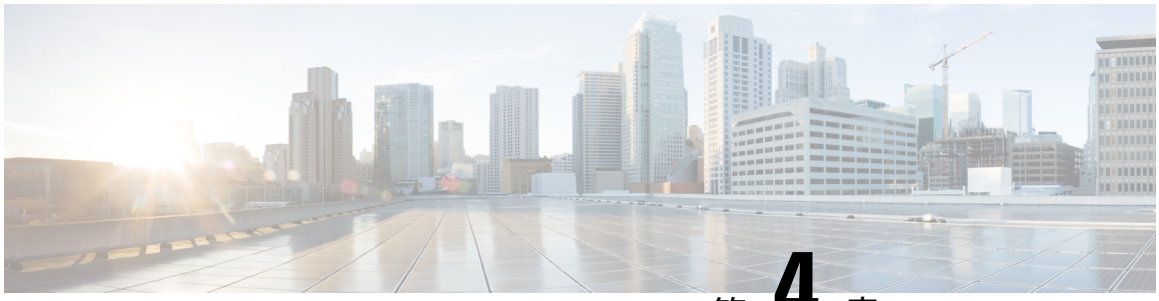
COOP プロトコルは、次の 2 つの ZMQ 認証モードをサポートします。

- **互換性タイプ**：デフォルト設定。COOP は、メッセージ転送のために MD5 認証および非認証 ZMQ 接続の両方を受け入れます。

（注） Cisco APIC は、COOP の MD5 パスワードとして使用されるトークンを管理します。このトークンは、Cisco APIC 1 時間ごとに自動的にローテーションされます。このトークンは表示できません。

- **厳密タイプ**：COOP は MD5 認証 ZMQ 接続のみを許可します。

COOP グループ ポリシーの **[厳密タイプ（Strict Type）]** 設定を強く推奨します。



第 4 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。

- アクセス権のワークフローの依存関係 （19 ページ）
- ユーザ アクセス、認可およびアカウンティング （20 ページ）
- ログイン ドメイン （22 ページ）
- GUI を使用してローカル ドメインを作成する （23 ページ）
- プロバイダーを作成する （26 ページ）
- ローカル ユーザの設定 （31 ページ）
- リモート ユーザの設定 （35 ページ）
- Cisco AVPair を使用した APIC アクセス用の Windows Server 2012 LDAP の設定 （40 ページ）
- LDAP アクセス用の APIC の設定 （42 ページ）
- Cisco AV ペアが欠落しているか不良であるリモート ユーザのデフォルトの動作の変更 （43 ページ）
- 署名ベースのトランザクションについて （44 ページ）
- アカウンティング （51 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 （52 ページ）

アクセス権のワークフローの依存関係

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

接続されたベア メタル サーバを使用するアプリケーション ポリシーを導入するために使用するスイッチ設定ポリシーをセットアップします。

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、**[カスタム条件（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。

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。

GUI を使用してローカル ドメインを作成する

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

始める前に

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

手順

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

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

ステップ 3 作業ペインで、[**ログインドメイン（Login Domains**）] タブを選択します。

ステップ 4 **[アクション（Actions）]** ボタン>**[ログイン ドメインの作成（Create Login Domain）]** をクリックします。

ステップ 5 **[ログイン ドメインの作成（Create Login Domain）]** 画面の **[一般（General）]** ペインで、次を指定します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

プロバイダーを作成する

この手順に従って、認証/承認プロトコルのプロバイダーを作成します。

始める前に

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

手順

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

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

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

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

ステップ 5 表示された **[プロバイダの作成（Create Provider）]** 画面で、**[ホスト名/IP アドレス（Hostname/IP Address）]**、**[説明（Description）]** を入力し、ドロップダウン リストから **[レルム（Realm）]** を選択します。 **レルム** で使用可能な選択肢は次のとおりです。

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

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

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

- RADIUS サーバーのパスワード：確認のためにもう一度パスワードを入力してください。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイント グループを選択します。
- RADIUS のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 1812 です。
- 認証プロトコルのオプションは、**[PAP]**、**[CHAP]**、**[MS-CHAP]** です。このオプションは、**[デフォルト（Default）]** を **[レルム サブタイプ（Realm Subtype）]** として選択した場合にのみ、表示されます。
- RADIUS サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です（レルム サブタイプ：デフォルトの場合）。デフォルトは 30 秒です（レルム サブタイプ：Duo）。

- RADIUS エンドポイントに接続する際の再試行回数。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザ名とパスワードを入力します。

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

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

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

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

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

- LDAP ディレクトリのルート識別名（DN）。
- LDAP ベース DN：APIC がリモートユーザーアカウントを検索する LDAP サーバー内のコンテナ名とパスです。これはパスワードが検証される場所です。フィルタを使用して、APIC が *Cisco AVPair* に使用するために要求している属性を見つけます。
- LDAP サーバーのパスワード。確認のためにもう一度パスワードを入力してください。
- LDAP のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 389 です。
- [**到達可能 EPG の選択（Select Reachability EPG**）] をクリックして、エンドポイントグループを選択します。
- LDAP サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 30 秒です。
- LDAP エンドポイントに接続する際の再試行回数。
- **[有効（Enable）]** チェック ボックスをオンにして、SSL を有効にします。
- SSL 証明書の検証レベル。次のオプションがあります。

- 寛容：DUO LDAP SSL証明書の問題の診断に役立つデバッグノブ。
- 厳密：実稼働環境で使用するレベル。

- LDAP 属性。
- 認証方式。次のオプションがあります。
  - LDAPバインド
  - パスワード比較
- フィルタ タイプフィルタは、検索要求のエントリの識別に使用される条件を定義する、主要なエレメントです。例：（cn=*）。これは、1つ以上の*cn*値を含むエントリを意味します。次のオプションがあります。
  - デフォルト
  - Microsoft Active Directory
  - カスタム（Custom）
- LDAP フィルタこのフィールドは、選択したフィルタ タイプに基づいて自動入力されます（カスタム オプションの [フィルタ タイプ（Filter Type）] を選択した場合を除く）。デフォルトを選択した場合、フィルタは `cn=Suserid` です。 Microsoft Active Directory を選択した場合、フィルタは `sAMAccountName=Suserid` です。
- 定期的なサーバー監視を有効にするには、[**有効（Enabled**）] チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

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

ステップ 9 （オプションの手順で RSA にのみ適用）次を指定します。

- RSA サーバーのパスワード：確認のためにもう一度パスワードを入力してください。
- [**到達可能 EPG の選択（Select Reachability EPG**）] をクリックして、エンドポイントグループを選択します。
- RSA のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 1812 です。
- RSA サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- RSA エンドポイントに接続する際の再試行回数。
- 定期的なサーバー監視を有効にするには、[**有効（Enabled**）] チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

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

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

- **[ID プロバイダ（Identity Provider）]**（IdP）。オプションは、ADFS、OKTA、PING IDENTITY です。
- **[IDP が提供するメタデータ URL（Metadata URL provided by IDP）]**。

  ADFS の場合、**IDP が提供するメタデータ URL** は *https://<FQDN of ADFS>/FederationMetadata/2007-06/FederationMetadata.xml* という形式になります。

  Ping ID については、Ping ID サーバーの構成セクション（SAML アプリケーションの下）メタデータ URL リンクをコピーします。
- SAML ベースのサービスの **[IdP エンティティ ID（IdP Entity ID）]**。
- サービス プロバイダ エンティティ ID である **[SP エンティティ ID（SP Entity ID）]**を入力します。ID はサービス プロバイダから取得できます。形式は次のとおりです。

  `https://apic-id/api/aaaLoginSSO.json?name=domain-name`
- IdP がプライベート CA によって署名されている場合は、**[認証局の選択（Select Certificate Authority）]** をクリックして認証局を選択します。
- GUI リダイレクトバナー。これは URL またはメッセージが可能です。この情報は、認証のためにユーザーが ID プロバイダーのログインページにリダイレクトされる前に表示されます。
- SAML サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- ドロップダウンリストから [署名アルゴリズム（Signature Algorithm）] を選択します。
- **[有効（Enabled）]** チェック ボックスをオンにして、暗号化された SAML アサーション、SAML 応答の署名のアサーション、SAML 認証要求の署名、SAML 応答メッセージの署名のすべてまたは一部を有効にできます。

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

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

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

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

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

ステップ 12 [保存（Save）] をクリックします。

ローカル ユーザの設定

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

GUI を使用したローカル ユーザの設定

始める前に

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

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

手順

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

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

[Work] ペインで、[Local Users] タブを表示していることを確認します。

ステップ 3 **[作業（Work）]**ペインで、タスク アイコンのドロップダウン リストをクリックし、**[ローカル ユーザの作成（Create Local User）]** を選択します。

ステップ 4 **[ステップ 1 > ユーザ ID（STEP 1 > User Identity）]** ダイアログ ボックスで、次の操作を実行します。

a) [Login ID] フィールドで、ID を追加します。

ログイン ID は、次のガイドラインを満たしている必要があります。

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

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

b) [Password] フィールドにパスワードを入力します。

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。

- （R6.1.1 まで）パスワードには、小文字、大文字、数字、記号のうち、3 つ以上の文字タイプが含まれる必要があります。
- （R6.1.2 以降）パスワード強度チェックの条件に応じて、次の要件を満たす必要があります。
  - デフォルト条件が有効の場合：
    - パスワードには、小文字、大文字、数字、記号のうち、3 つ以上の文字タイプが含まれる必要があります。R6.1.3 から、パスワードには小文字、数字、記号の 3 つすべての文字タイプが含まれる必要があります。
  - カスタム条件が有効の場合は、次の条件から 3 つ以上を選択します。
    - パスワードには少なくとも 1 つの大文字を含める必要があります。
    - パスワードには少なくとも 1 つの小文字を含める必要があります。
    - パスワードには少なくとも 1 つの数字を含める必要があります。
    - パスワードには、少なくとも 1 つの記号を含める必要があります。
    - パスワードには同一の文字を 3 回以上連続して含めることはできません。
    - パスワードには、QWERTY キーボード レイアウトから 3 文字以上連続する文字を含めることはできません。
  - 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。

c) [Confirm Password] フィールドで、パスワードを確認します。
d) （任意） 証明書ベースの認証の場合は、**[ユーザ証明書の属性（User Certificate Attribute）]** フィールドに、認証証明書からのユーザ ID を入力します。
e) **[次へ（Next）]** をクリックします。

ステップ 5 **[アカウント ステータス（Account Status）]** コントロールを使用してユーザ アカウントをアクティブまたは非アクティブにできます。また、**[アカウントの有効期限（Account Expires）]** コントロールを使用して有効期限を設定できます。

ステップ 6 **[ステップ 2 > セキュリティ（STEP 2 > Security）]** ダイアログ ボックスの **[セキュリティ ドメイン（Security Domain）]** で、ユーザの機能のセキュリティ ドメインを選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **[ステップ 3 > ロール（STEP 3 > Roles）]** ダイアログ ボックスで、次のアクションを実行します。

a) **[+]** をクリックして、ユーザをドメインに関連付けます。
b) ドロップダウン リストから、ユーザの**ロール名**と**ロール権限タイプ**を選択します。

c) **[更新（Update）]** をクリックします。

読み取り専用または読み取り/書き込み権限を提供できます。

ステップ 8 **[完了（Finish）]** をクリックします。

GUI を使用した SSH 公開キー認証の設定

始める前に

- ターゲット セキュリティ ドメインでローカル ユーザ アカウントを作成します。ターゲット ドメインが `all` である場合、新しいローカル ユーザの作成に使用するログイン アカウントは、`all` にアクセスできるファブリック全体の管理者である必要があります。ターゲット ドメインがテナントである場合、新しいローカル ユーザの作成に使用するログイン アカウントは、ターゲット テナント ドメインに対する完全な読み取り/書き込みアクセス権を持つテナント管理者である必要があります。
- UNIX コマンド **ssh-keygen** を使用して公開キーを生成します。

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

手順

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

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

ユーザーに関する情報を含むウィンドウが右側に表示されます。

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

下方向にスクロールして SSH 認証の詳細を確認します。

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

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

ステップ 5 **[保存（Save）]** をクリックします。

リモート ユーザの設定

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

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

3.1 (1) のリリース以降、**サーバ モニタリング** はRADIUS、TACACS +、LDAP、およびRSA を介して設定され、個別の AAA サーバがアクティブかを判断できます。サーバ モニタリング機能は、サーバがアクティブかどうか確認するためそれぞれのプロトコルのログインを使用します。たとえば、LDAP サーバは ldap1ログインを使用し、Radius サーバはサーバがアクティブか判断するサーバ モニタリング機能を持つ radius のログインを使用します。

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

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

外部認証サーバの AV ペア

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

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

```
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(16003)
```

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

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

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

APIC は、次の正規表現をサポートしています。

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

例：

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

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

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

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

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

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

オープン RADIUS サーバ（/etc/raddb/users）の設定例は次のとおりです。

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

外部認証サーバの AV ペアの設定

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

（注） 6.0(2) リリース以降、telnet はサポートされていません。

手順

外部認証サーバの AV ペアを設定します。

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

例：

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

These are the boost regexes supported by APIC:
uid_regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})(\\(\\d+\\))$");
regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})$");
```

次に、例を示します。

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

TACACS+ アクセス用の APIC の設定

始める前に

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

手順

ステップ 1 APIC で、TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの設定については、プロバイダーを作成する （26 ページ） を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

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

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

手順については、GUI を使用してローカル ドメインを作成する （23 ページ）を参照してください。

次のタスク

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

RADIUS アクセス用の APIC の設定

始める前に

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

手順

ステップ 1 APIC で、RADIUS プロバイダーを作成します。

RADIUS プロバイダーの設定については、プロバイダーを作成する （26 ページ）を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

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

ステップ 2 RADIUS の**ログインドメイン**を作成します。

手順については、GUI を使用してローカル ドメインを作成する （23 ページ）を参照してください。

次のタスク

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

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

始める前に

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

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

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

手順

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

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

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

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

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

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

ステップ 2 ID グループを作成します。

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

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

ステップ 3 ユーザを ID グループにマッピングします。

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

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

ステップ 4 ポリシー要素を作成します。

a) **[Policy Elements]** オプションに移動します。

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

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

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

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

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

ステップ 5 サービス選択ルールを作成します。

a) RADIUS の場合、サービス選択ルールを作成して ID グループをポリシー要素に関連付けるには、**[Access Policies]** > **[Default Device Network Access Identity]** > **[Authorization]** に移動し、ルールの [Name]、[Status]、および [Conditions] を指定し、必要に応じて「Internal Users:UserIdentityGroup in ALL Groups:<identity group name>」を追加します。

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

次のタスク

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

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

始める前に

- 最初に LDAP サーバを設定し、次に Cisco Application Policy Infrastructure Controller（Cisco APIC）を LDAP アクセス用に設定する。

- Microsoft Windows Server 2012 がインストールされ、オンラインになっていること。
- Microsoft Windows Server 2012 サーバ マネージャの ADSI Edit ツールがインストールされていること。ADSI Edit をインストールするには、Windows Server 2012 サーバ マネージャのヘルプに記載されている手順に従ってください。
- `CiscoAVPair` の属性の指定：Common Name = **`CiscoAVPair`**, LDAP Display Name = **`CiscoAVPair`**, Unique X500 Object ID = 1.3.6.1.4.1.9.22.1, Description = **`CiscoAVPair`**, Syntax = **`Case Sensitive String`**。

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

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

手順

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

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

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

b) **[File]** > **[Add/Remove Sanp-in]** > **[Add]** に移動します。

c) [Add Standalonee Snap-in] ダイアログボックスで、[Active Directory Schema] を選択し、[Add] をクリックします。
MMC コンソールが開きます。

d) **[属性]** フォルダを右クリックし、**[属性の作成]** オプションを選択します。
[Create New Attribute] ダイアログボックスが開きます。

e) **[共通名]** に「**`CiscoAVPair`**」、**[LDAP 表示名]** に「**`CiscoAVPair`**」、[Unique X500 Object ID] に「**`1.3.6.1.4.1.9.22.1`**」と入力し、**[構文]** で「**`Case Sensitive String`**」を選択します。

f) [OK] をクリックして、属性を保存します。

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

a) MMC コンソールで、[Classes] フォルダを展開し、[user] クラスを右クリックし、[Properties] を選択します。
[user Properties] ダイアログボックスが開きます。

b) **[属性]** タブをクリックし、**[追加]** をクリックして **[スキーマのオブジェクトを選択する]** ウィンドウを開きます。

c) [Select a schema object:] リストで、「**`CiscoAVPair`**」を選択し、[Apply] をクリックします。

d) MMC コンソールで、[Active Directory Schema] を右クリックし、[Reload the Schema] を選択します。

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

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

a) [ADSI Edit] ダイアログ ボックスで、Cisco APIC にアクセスする必要があるユーザを見つけます。

b) ユーザ名を右クリックし、[Properties] を選択します。
[<user> Properties] ダイアログボックスが開きます。

c) **[属性エディタ]** タブをクリックし、「*CiscoAVPair*」属性を選択し、*[値]* に「**`shell:domains = <domain>/<role>/,<domain>// role`**」と入力します。

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

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

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

次のタスク

Cisco APIC を LDAP アクセス用に設定します。

LDAP アクセス用の APIC の設定

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックがインストールされていて、Application Policy Infrastructure コントローラがオンラインになっており、APIC クラスタが形成されていて正常に動作していること。

- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- APIC 管理エンドポイント グループを使用できること。

手順

ステップ 1 APIC で、LDAP プロバイダーを設定します。

LDAP プロバイダーの設定については、プロバイダーを作成する （26 ページ）を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

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

ステップ 2 LDAP の **ログイン ドメイン** を作成します。

手順については、GUI を使用してローカル ドメインを作成する （23 ページ）を参照してください。

次のタスク

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

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

手順

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

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

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

署名ベースのトランザクションについて

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

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

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

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

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

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

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- ローカル ユーザはサポートされます。リモート AAA ユーザはサポートされません。
- APIC GUI は証明書認証方式をサポートしません。
- WebSocket と eventchannel は X.509 要求では動作しません。

- サードパーティにより署名された証明書はサポートされません。自己署名証明書を使用します。

X.509 証明書と秘密キーの生成

手順

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

例：

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

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

ステップ 2 OpenSSL を使用して証明書のフィールドを表示します。

例：

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

```
                X509v3 Authority Key Identifier:
                  keyid:0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34

                    DirName:/CN=User ABC/O=Cisco Systems/C=US
                    serial:C4:27:6C:4D:69:7C:D2:B6

                X509v3 Basic Constraints:
                    CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        8f:c4:9f:84:06:30:59:0c:d2:8a:09:96:a2:69:3d:cf:ef:79:
        91:ea:cd:ae:80:16:df:16:31:3b:69:89:f7:5a:24:1f:fd:9f:
        d1:d9:b2:02:41:01:b9:e9:8d:da:a8:4c:1e:e5:9b:3e:1d:65:
        84:ff:e8:ad:55:3e:90:a0:a2:fb:3e:3e:ef:c2:11:3d:1b:e6:
        f4:5e:d2:92:e8:24:61:43:59:ec:ea:d2:bb:c9:9a:7a:04:91:
        8e:91:bb:9d:33:d4:28:b5:13:ce:dc:fe:c3:e5:33:97:5d:37:
        cc:5f:ad:af:5a:aa:f4:a3:a8:50:66:7d:f4:fb:78:72:9d:56:
        91:2c
[snip]
```

ローカル ユーザの設定

GUI を使用したローカル ユーザの作成とユーザ証明書の追加

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[AAA]** を選択します。

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

ステップ 3 [Work] ペインで、[Local Users] タブを表示していることを確認します。

デフォルトでは admin ユーザが存在します。

ステップ 4 [Work] ペインで、タスク アイコンのドロップダウン リストをクリックし、[Create Local User] を選択します。

ステップ 5 [Security] ダイアログボックスで、ユーザに必要なセキュリティ ドメインを選択し、[Next] をクリックします。

ステップ 6 [Roles] ダイアログボックスで、ユーザのロールを選択するためのオプション ボタンをクリックし、[Next] をクリックします。

読み取り専用または読み取り/書き込み権限を提供できます。

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

a) [Login ID] フィールドで、ID を追加します。
b) [Password] フィールドにパスワードを入力します。
c) [Confirm Password] フィールドで、パスワードを確認します。
d) （オプション）証明書ベースの認証の場合は、[User Certificate Attribute] フィールドに、認証証明書からのユーザ ID を入力します。

e) [Finish] をクリックします。

ステップ 8 [Navigation] ペインで、作成したユーザの名前をクリックします。[Work] ペインで、[Security Domains] 領域のユーザの横にある [+] 記号を展開します。
ユーザのアクセス権限が表示されます。

ステップ 9 [Work] ペインの [User Certificates] 領域で、ユーザ証明書の [+] 記号をクリックし、[Create X509 Certificate] ダイアログ ボックスで次の操作を実行します。

a) [Name] フィールドに、証明書の名前を入力します。

b) [Data] フィールドに、ユーザ証明書の詳細を入力します。

c) **Submit** をクリックします。

X509 証明書がローカル ユーザ用に作成されます。

Python SDK を使用したローカル ユーザの作成

手順

ローカル ユーザを作成します。

例：

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

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

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

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

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

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

uni = PolUni('') # '' is the Dn string for topRoot
aaaUserEp = AaaUserEp(uni)
aaaUser = AaaUser(aaaUserEp, 'userabc', firstName='Adam',
                  email='userabc@cisco.com')

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

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

秘密キーを使用した署名の計算

始める前に

次の情報が用意されている必要があります。

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

手順

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

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

例：

GET の例：

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

POST の例：

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

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

たとえば、前の手順で示したような取得例を使用します。

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

payload.txt ファイルには、次の情報のみ含める必要があります。

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

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

例：

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

次と同じように出力の最後に **$** 記号があるか確認します。

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

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

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

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

例：

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

生成されたファイルには、複数行に印字された署名があります。

ステップ 5 base64 形式に署名を変換します。

例：

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

ステップ 6 Bash を使用して、署名から改行文字を取り除きます。

例：

```
$ tr -d '\n' < payload_sig.base64
P+OTqK0CeAZjl7+Gute2RlWw8OGgtzE0wsLlx8fIXXl4V79Zl7
Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f7q
IcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=
```

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

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

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

例：

```
APIC-Request-Signature=P+OTqK0CeAZjl7+Gute2RlWw8OGgtzE0wsLlx8f
IXXl4V79Zl7Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f
7qIcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=;
APIC-Certificate-Algorithm=v1.0; APIC-Certificate-Fingerprint=fingerprint;
APIC-Certificate-DN=uni/userext/user-userabc/usercert-userabc.crt
```

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

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

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

例：

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

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

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

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

（注）

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

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。

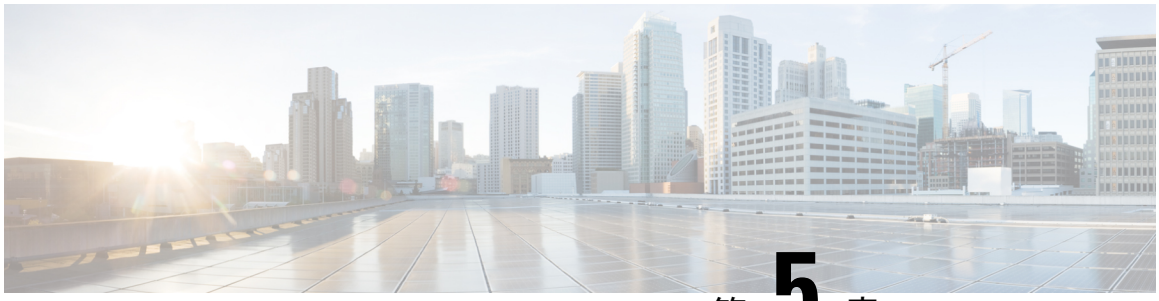
aaaModLR MO と aaaSessionLR 管理対象オブジェクトは、クラスまたは識別名（DN）でクエリできます。クラスのクエリは、ファブリック全体のすべてのログ レコードを提供します。ファブリック全体の aaaModLR レコードはすべて、GUI の **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[POD]** > **[履歴（History）]** > **[監査ログ（Audit Log）]** セクションから入手できます。Cisco APIC GUI の **[履歴（History）]** > **[監査ログ（Audit Log）]** 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。



第 5 章

管理

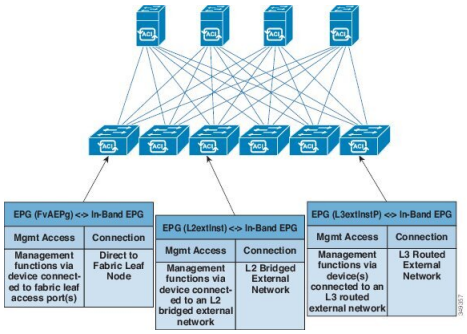
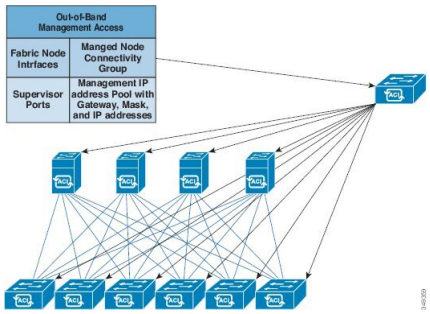
この章は、次の内容で構成されています。

- 管理のワークフロー （53 ページ）
- 管理アクセスの追加 （55 ページ）
- テクニカル サポート、統計情報、およびコア ファイルのエクスポート （65 ページ）
- 概要 （67 ページ）
- コントローラ コンフィギュレーションのバックアップ、復元、およびロールバック （75 ページ）
- Syslog の使用 （86 ページ）
- アトミック カウンタの使用 （90 ページ）
- SNMP の使用 （95 ページ）
- SPAN の使用 （101 ページ）
- トレースルートの使用 （138 ページ）
- acidiag コマンド （140 ページ）

管理のワークフロー

ACI 管理アクセスのワークフロー

このワークフローでは、ACI ファブリック内のスイッチへの管理接続を設定するために必要な手順の概要を示します。

インバンド管理アクセス	アウトオブバンド管理アクセス
	

1. 前提条件

- インフラ セキュリティ ドメインに読み取り/書き込みアクセス権限があることを確認します。
- 必要なインターフェイスを持つターゲット リーフ スイッチが使用できることを確認します。

2. ACI リーフ スイッチのアクセス ポートの設定

次の管理アクセス シナリオのいずれかを選択します。

- **インバンド**管理の場合は、『*APIC Basic Configuration Guide*』のインバンド設定向けに推奨されるトピックに従います。
- **アウトオブバンド**管理の場合は、『*APIC Basic Configuration Guide*』のアウトオブバンド設定向けに推奨されるトピックに従います。

推奨されるトピック

詳細については、『*APIC Basic Configuration Guide*』の以下のトピックを参照してください。

- 拡張 GUI を使用したインバンド管理アクセスの設定
- NX-OS スタイルの CLI を使用したインバンド管理アクセスの設定
- REST API を使用したインバンド管理アクセスの設定
- 拡張 GUI を使用したアウトオブバンド管理アクセスの設定
- NX-OS スタイルの CLI を使用したアウトオブバンド管理アクセスの設定
- REST API を使用したアウトオブバンド管理アクセスの設定

管理アクセスの追加

インバンドの管理テナントで外部管理インスタンスプロファイルを設定しても、ファブリック全体の通信ポリシーで設定されているプロトコルには影響しません。外部管理インスタンスプロファイルで指定されているサブネットおよびコントラクトは、HTTP/HTTPS または SSH/Telnet には影響しません。5.3(1) リリース以降、Telnet はサポートされていません。

GUI での管理アクセスの追加

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

インバンド管理ネットワークでは、Cisco APIC が Cisco Application Centric Infrastructure（ACI）ファブリックを使用してリーフ スイッチや外部と通信でき、外部管理デバイスがファブリック自体を使用して Cisco APIC またはリーフ スイッチおよびスパイン スイッチと通信できます。

アウトオブバンド管理ネットワークの設定は、コントローラ、リーフ スイッチ、およびスパイン スイッチの管理ポートの設定を定義します。

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

Cisco ACI には、管理テナントおよびインバンド VRF インスタンスのブリッジ ドメインのサブネット設定に基づいて、インバンド管理用のルートをプログラムする機能があります。これらのルートは、ブリッジ ドメインからサブネット設定が削除されると削除されます。

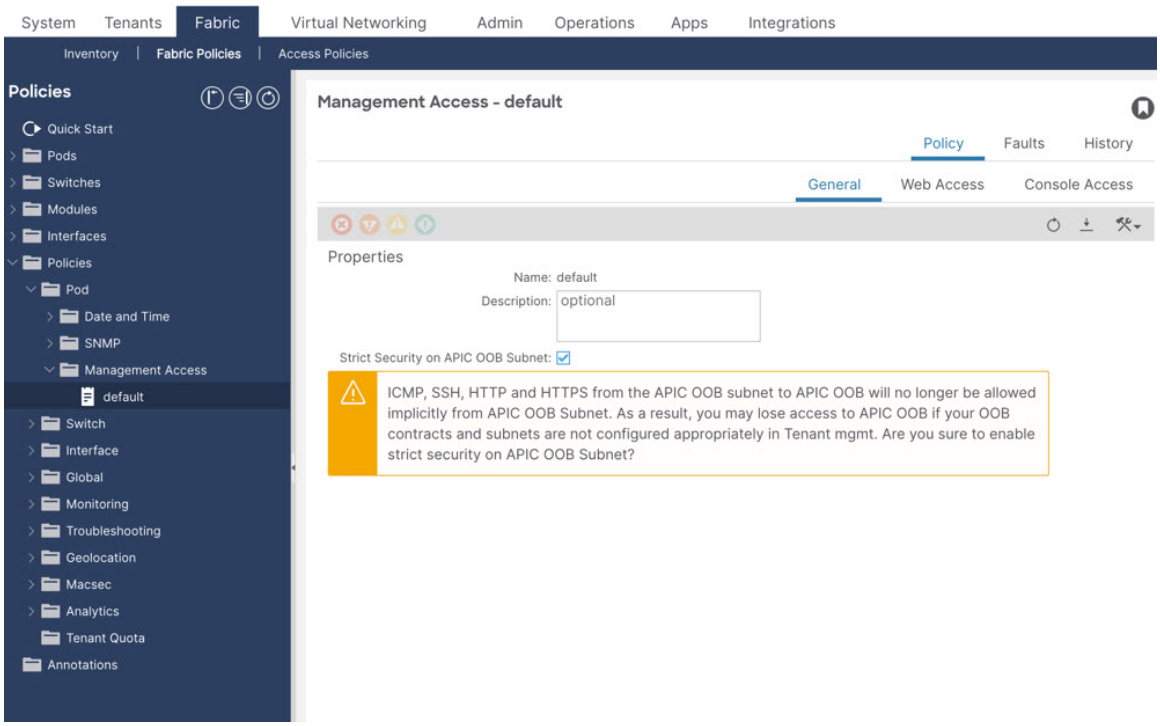
Cisco APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

OOB 管理 IP を使用した APIC へのアクセスは、コントラクトと許可されたサブネットを構成することで制限できます。ただし、APIC OOB サブネットに属する IP アドレスは、コントラクトとサブネットの構成に関係なく、ICMP、SSH、HTTP、HTTPS、および TCP 4200 を使用した APIC OOB へのアクセスが常に許可されます。このセーフガードは、構成ミスによる APIC アクセスの偶発的な損失を防ぐために導入されています。Cisco APIC リリース 6.1(1) 以降では、APIC GUI の **[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[ポリシー（Policies）]** > **[ポッド（Pod）]** > **[管理アクセス（Management Access）]** にあるデフォルトの管理 アクセスを構成する際に **[APIC OOB サブネットでの厳格なセキュリティ（Strict Security on APIC OOB Subnet）]** オプションを有効にすることで、このセーフガードを削除できます。

厳密モードを有効にするとすぐに、[管理アクセス（Management Access）] 画面に警告が表示されます（以下を参照）。厳格モードの有効化に関する同様の警告は、**[外部管理ネットワーク プロファイル（ External Management Network Profile）]** 画面にも表示されます（**[テナント**

（**Tenants**）] > [管理（**mgmt**）] > [ネットワーク インスタンス プロファイル（**External Management Network Instance Profiles**）] の下にあります）。

図 *1:* 厳密セキュリティ モードを有効にした後に表示される警告



IP アドレスによる APIC へのアクセスを許可しないコントラクトとサブネット（外部管理ネットワーク インスタンス プロファイル内）を使用して **[APIC OOB サブネットで厳格なセキュリティ（Strict Security on APIC OOB Subnet）]** を有効にすると、OOB IP アドレスを介した APIC へのアクセスが失われます。APIC OOB サブネットと同じネットワークから APIC にアクセスすることもできません。このような場合は、コンソールにログインし、`acidiag enableoobrecovery` コマンドを使用して、**[APIC OOB サブネットの厳格なセキュリティ（Strict Security on APIC OOB Subnet）]** を無効にします。

（注） ARP 情報をキャッシュする重複する IP アドレスとファイアウォールは、管理ネットワークではサポートされません。これらの条件が存在すると、アップグレード後に Cisco APIC 管理アクセスが完全に失われる可能性があります。

IPv4/IPv6 アドレスおよびインバンド ポリシー

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

アウトオブバンド ポリシーの IPv4/IPv6 アドレス

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

既存の IP tables 機能をミラーリングする IPv6 の変更

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

既存の IP tables

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

IP tables への変更

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

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

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

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

管理アクセスの注意事項および制約事項

- vzAnyは共有サービスのコンシューマとしてサポートされますが、共有サービスのプロバイダとしてはサポートされません。 vzAny 共有サービス コンシューマと vzAny プロバイダはサポートされていません。
- アウトオブバンド管理アクセスを設定する場合、アウトオブバンドコントラクトのロギングオプション（ACL コントラクトおよび許可/拒否ログの有効化と表示）はサポートされません。
- インバンド管理 VRF をリーフ ノードにプッシュするには、リーフ ノードのインバンド管理アドレスを設定する必要があります。
- ゲートウェイ サブネットに [この IP アドレスをプライマリにする（Make this IP address primary）] が選択されていない限り、インバンド管理 VRF のブリッジ ドメイン サブネット IP アドレスをセカンダリ IP アドレスとして割り当てることができます。
- 次のポートはアウトオブバンド コントラクトで拒否できません。
  - プロトコル icmp、レート制限、設定不可
  - tcp dpt：22、レート制限、構成不可
  - tcp dpt：80、デフォルトではリスニング プロセスなし
  - tcp dpt：443、デフォルトの UI/API
  - tcp dpt：4200、Web 経由の SSH アクセス、デフォルトではリッスン プロセスなし

  外部ネットワーク インスタンス プロファイルでサブネットを定義すると、上記のポートリストは、構成された OOB サブネットの送信元に制限されます。

  IPv4 または IPv6 サブネットが外部ネットワーク インスタンス プロファイルで定義されていない場合、対応するアドレス ファミリに対して OOB 契約は有効になりません。

  IPv4 と IPv6 の両方の OOB コントラクトを有効にするには、外部ネットワーク インスタンス プロファイルの下で、少なくとも 1 つの IPv4 サブネットと 1 つの IPv6 サブネットを構成する必要があります。

  リーフ スイッチおよびスパイン スイッチの SNMP の場合、**[ファブリック ポリシー（Fabric Policies）] > [ポッド（Pod）] > [SNMP]** で構成されている**[クライアント エントリ（Client**

Entries）] サブネットは、OOB コントラクトの前に一致します。**[クライアント エントリ（Client Entries）]**の下にサブネットが構成されていない場合は、どの送信元でも SNMP が許可されます。たとえば、UDP **dpt:161** です。

デフォルトでは、リーフ スイッチとスパイン スイッチの管理インターフェイスには IP アドレスが割り当てられていません。ただし、IP アドレスが割り当てられると、帯域外契約で拒否できないポートがいくつかあります。これらは、ACI の組み込み機能に必要です。たとえば、NTP、DHCP、ICMP などです。

外部ネットワーク インスタンス プロファイルで定義されているサブネットは、APIC にのみ適用されます。リーフ スイッチとスパイン スイッチでは、任意の送信元（0.0.0.0/0）が許可されます。

- スパイン スイッチは、インバンド管理 IP アドレスの ARP を解決しません。このため、インバンド管理ネットワーク内のデバイスはスパイン スイッチと通信できません。スパイン スイッチへのアクセスは、レイヤ 3 ネットワーク経由でのみ可能です。
-

ウィザードによるインバンドおよびアウトオブバンド管理アクセスの設定

APIC、リリース 3.1(x) では、管理アクセスの設定を簡略化するためのウィザードが追加されました。このドキュメントに含まれる、管理アクセスを設定する他の方法も引き続き使用できます。

手順

ステップ 1 **In-Band Management Access** を設定するには、次の手順を実行します:

a) メニュー バーで、**Tenants** > **mgmt** をクリックします。
b) **Quick Start** を展開します。
c) **In-Band Management Access** > **Configure In-Band Management Access** > **Start** をクリックします。
d) **Nodes** を管理ネットワークに、**IP addresses** をノードに、通信フィルタを **Connected Devices** に、そして通信フィルタを **Remote Attached Devices** に追加する手順に従います。

ステップ 2 **Out-of-Band Management Access** を設定するには、次の手順を実行します:

a) メニュー バーで、**Tenants** > **mgmt** をクリックします。
b) **Quick Start** を展開します。
c) **Out-of-Band Management Access** > **Configure Out-of-Band Management Access** > **Start** をクリックします。

d) **Nodes** をアウトオブバンド管理ネットワークに、**IP addresses** をノードに、許可されたサブネットを**External Hosts** に追加する手順に従います。そうすると、通信フィルタが **Access** のための通信を決定します。

Cisco APIC GUI を使用したインバンド管理アクセスの設定

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

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[Navigation]**ペインで、**[インターフェイス]** を右クリックし、**[Configure Interface, PC and VPC]** を選択します。

ステップ 3 **[Configure Interface, PC, and VPC]** ダイアログボックスで、Cisco Application Policy Infrastructure Controller (APIC) に接続されるスイッチ ポートを設定し、次の操作を実行します。

a) スイッチ図の横にある大きい **[+]** アイコンをクリックし、新しいプロファイルを作成して VLAN を Cisco APIC 用に設定します。

b) **[Switches]** フィールドのドロップダウン リストから、Cisco APIC を接続するスイッチのチェックボックスをオンにします（leaf1 および leaf2）。

c) [Switch Profile Name] フィールドに、プロファイルの名前（apicConnectedLeaves）を入力します。

d) **[+]** アイコンをクリックして、ポートを設定します。

e) **[Interface Type]** 領域で、**[Individual]** オプション ボタンが選択されていることを確認します。

f) **[インターフェイス（Interfaces）]** フィールドで、Cisco APIC が接続されるポートを入力します。

g) [Interface Selector Name] フィールドに、ポート プロファイルの名前（apicConnectedPorts）を入力します。

h) **[Interface Policy Group]** フィールドで、**[Create One]** オプション ボタンをクリックします。

i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（ベアメタル）を設定します。

j) [Domain] フィールドで、[Create One] オプション ボタンをクリックします。

k) [Domain Name] フィールドに、ドメイン名を入力します（inband）。
l) [VLAN] フィールドで、[Create One] オプション ボタンを選択します。
m) [VLAN Range] フィールドに、VLAN 範囲を入力します。**[Save]** をクリックし、**[Save]** をもう一度クリックします。[送信（Submit）] をクリックします。

ステップ 4 [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。

ステップ 5 [Configure Interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。

a) スイッチ図の横にある大きい [+] アイコンをクリックして、新しいプロファイルを作成して VLAN をサーバ用に設定します。
b) [Switches] フィールドのドロップダウン リストから、サーバが接続されているスイッチのチェックボックスをオンにします（leaf1）。
c) [Switch Profile Name] フィールドに、プロファイルの名前（vmmConnectedLeaves）を入力します。
d) **[+]** アイコンをクリックして、ポートを設定します。
e) **[Interface Type]** 領域で、**[Individual]** オプション ボタンが選択されていることを確認します。
f) [Interfaces] フィールドで、サーバが接続されているポートを入力します（1/40）。
g) **[Interface Selector Name]** フィールドに、ポート プロファイルの名前を入力します。
h) **[Interface Policy Group]** フィールドで、**[Create One]** オプション ボタンをクリックします。
i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（ベアメタル）を設定します。
j) [Domain] フィールドのドロップダウン リストから、[Choose One] オプション ボタンをクリックします。
k) [Physical Domain] ドロップダウン リストから、前に作成したドメインを選択します。
l) [Domain Name] フィールドに、ドメイン名を入力します。
m) [Save] をクリックし、[Save] をもう一度クリックします。

ステップ 6 [Configure Interface, PC, and VPC] ダイアログボックスで、[Submit] をクリックします。

ステップ 7 メニュー バーで、**[テナント（TENANTS）]** > **[管理（mgmt）]** をクリックします。**[ナビゲーション（Navigation）]** ペインで、**[テナント管理（Tenant mgmt）]** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** を展開し、インバンド接続のブリッジ ドメインを設定します。

ステップ 8 インバンド ブリッジ ドメイン（inb）を展開します。[Subnets] を右クリックします。[Create Subnets] をクリックし、次の操作を実行してインバンド ゲートウェイを設定します。

a) [Create Subnet] ダイアログボックスで、[Gateway IP] フィールドに、インバンド管理ゲートウェイ IP アドレスとマスクを入力します。
b) **Submit** をクリックします。

ステップ 9 **[ナビゲーション（Navigation）]** ペインで、**[テナント管理（Tenant mgmt）]** > **[ノード管理 EPG（Node Management EPGs）]** を展開します。[Node Management EPGs] を右クリックし、[Create In-Band Management EPG] を選択します。Cisco APIC と通信するために使用するインバンド EPG の VLAN を設定するには、次の操作を実行します。

a) [Name] フィールドに、インバンド管理 EPG 名を入力します。
b) [Encap] フィールドで、VLAN（vlan-10）を入力します。
c) [Bridge Domain] ドロップダウン フィールドから、ブリッジ ドメインを選択します。**Submit** をクリックします。
d) [Navigation] ペインで、新しく作成したインバンド EPG を選択します。
e) [Provided Contracts] を展開します。[Name] フィールドで、ドロップダウン リストから、デフォルトのコントラクトを選択し、VMM サーバが存在する EPG で消費されるデフォルトのコントラクトを EPG が提供できるようにします。
f) [Update] をクリックし、[Submit] をクリックします。

ステップ 10 **[ナビゲーション（Navigation）]** ペインで、**[ノード管理アドレス（Node Management Addresses）]** を右クリックし、**[ノード管理アドレスの作成（Create Node Management Addresses）]** をクリックし、次の操作を実行してファブリック内の Cisco APIC コントローラに割り当てる IP アドレスを設定します。

a) [Create Node Management Addresses] ダイアログボックスで、[Policy Name] フィールドに、ポリシー名（apicInb）を入力します。
b) [Nodes] フィールドの [Select] 列で、このファブリックの一部となるノードのチェックボックスをオンにします（apic1、apic2、apic3）。
c) [Config] フィールドで、[In-Band Addresses] チェックボックスをオンにします。
d) [Node Range] フィールドに、範囲を入力します。
e) [In-Band IP Addresses] 領域の [In-Band Management EPG] フィールドで、ドロップダウン リストから [default] を選択します。これで、デフォルトのインバンド管理 EPG が関連付けられます。
f) [In-Band IP Addresses] フィールドと [Gateway] フィールドに、必要に応じて IPv4 アドレスまたは IPv6 アドレスを入力します。
g) **Submit** をクリックします。Cisco APIC の IP アドレスが設定されました。

ステップ 11 [Navigation] ペインで、[Node Management Addresses] を右クリックします。[Create Node Management Addresses] をクリックし、次の操作を実行して、ファブリック内のリーフ スイッチおよびスパイン スイッチの IP アドレスを設定します。

a) [Create Node Management Addresses] ダイアログボックスで、[Policy Name] フィールドに、ポリシー名（switchInb）を入力します。
b) [Nodes] フィールドの [Select] 列で、このファブリックの一部となるノードの横のチェックボックスをオンにします（leaf1、leaf2、spine1、spine2）。
c) [Config] フィールドで、[In-Band Addresses] チェックボックスをクリックします。
d) [Node Range] フィールドに、範囲を入力します。
e) [In-Band IP Addresses] 領域の [In-Band Management EPG] フィールドで、ドロップダウン リストから [default] を選択します。デフォルトのインバンド管理 EPG が関連付けられました。
f) [In-Band IP Addresses] フィールドと [Gateway] フィールドに、必要に応じて IPv4 アドレスまたは IPv6 アドレスを入力します。
g) **Submit** をクリックします。[Confirm] ダイアログボックスで、[Yes] をクリックします。リーフおよびスパイン スイッチの IP アドレスが設定されました。

ステップ 12 **[ナビゲーション（Navigation）]**ペインの**[ノード管理アドレス（Node Management Addresses）]**の下で、Cisco APIC のポリシー名（apicInb）をクリックして設定を確認します。[Work] ペインに、さまざまなノードに割り当てられた IP アドレスが表示されます。

ステップ 13 [Navigation] ペインの [Node Management Addresses] 下で、スイッチ ポリシー名（switchInb）をクリックします。[Work] ペインに、スイッチに割り当てられている IP アドレスと使用しているゲートウェイ アドレスが表示されます。

（注）
[システム（System）]>**[システム設定（System Settings）]**>**[APIC接続設定（APIC Connectivity Preferences）]** をクリックして、アウトオブバンド管理アクセスを Cisco APIC サーバのデフォルトの管理接続モードに設定できます。次に、[Connectivity Preferences] ページで [inband] をクリックします。

Cisco APIC GUI を使用したアウトオブバンド管理アクセスの設定

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

リーフ スイッチとスパイン スイッチ、および Cisco APIC のアウトオブバンド管理アクセス アドレスを設定する必要があります。

始める前に

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

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]**>**[管理（mgmt）]** を選択します。[Navigation] ペインで、[Tenant mgmt] を展開します。

ステップ 2 [Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックします。

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

a) [Policy Name] フィールドに、ポリシー名（switchOob）を入力します。

b) [Nodes] フィールドで、適切なリーフおよびスパイン スイッチ（leaf1、leaf2、spine1）の横にあるチェックボックスをオンにします。

c) [Config] フィールドで、[Out of-Band Addresses] のチェックボックスをオンにします。

（注）
[Out-of-Band IP addresses] 領域が表示されます。

d) [Out-of-Band Management EPG] フィールドで、ドロップダウン リストから EPG を選択します（デフォルト）。

e) **アウトオブ バンド ゲートウェイ** フィールドで、外部アウトオブバンド管理ネットワークの IP アドレスとネットワーク マスクを入力します。

f) **[アウトオブバンド IP アドレス]** フィールドに、スイッチに割り当てられる希望の IPv4 または Ipv6 アドレスの範囲を入力します。[Submit] をクリックします。

ノード管理 IP アドレスが設定されます。

ステップ 4 [Navigation] ペインで、[Node Management Addresses] を展開し、作成したポリシーをクリックします。

[Work] ペインに、スイッチに対するアウトオブバンド管理アドレスが表示されます。

ステップ 5 **[Navigation]** ペインで、**[コントラクト（Contracts）]** > **[アウトオブバンド コントラクト（Out-of-Band Contracts）]** を展開します。

ステップ 6 [Out-of-Band Contracts] を右クリックし、[Create Out-of-Band Contract] をクリックします。

ステップ 7 [Create Out-of-Band Contract] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、コントラクトの名前（oob-default）を入力します。

b) [Subjects] を展開します。[Create Contract Subject] ダイアログボックスで、[Name] フィールドに、サブジェクト名（oob-default）を入力します。

c) **[フィルタ]** を展開し、**[名前]** フィールドで、ドロップダウン リストから、フィルタの名前（default）を選択します。[Update] をクリックし、[OK] をクリックします。

d) [Create Out-of-Band Contract] ダイアログボックスで、[Submit] をクリックします。

アウトオブバンド EPG に適用できるアウトオブバンド コントラクトが作成されます。

ステップ 8 **[ナビゲーション（Navigation）]** ペインで、**[ノード管理 EPG（Node Management EPG）]** > **[アウトオブバンド EPG - デフォルト（Out-of-Band EPG - default）]** を展開します。

ステップ 9 [Work] ペインで、[Provided Out-of-Band Contracts] を展開します。

ステップ 10 [OOB Contract] カラムで、ドロップダウンリストから、作成したアウトオブバンドコントラクト（oob-default）を選択します。[Update] をクリックし、[Submit] をクリックします。
コントラクトがノード管理 EPG に関連付けられます。

ステップ 11 **[ナビゲーション（Navigation）]** ペインで、**[外部ネットワーク インスタンス プロファイル（External Network Instance Profile）]** を右クリックし、**[外部管理エンティティ インスタンスの作成（Create External Management Entity Instance）]** をクリックします。

ステップ 12 [Create External Management Entity Instance] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、名前（oob-mgmt-ext）を入力します。

b) [Consumed Out-of-Band Contracts] フィールドを展開します。[Out-of-Band Contract] ドロップダウン リストから、作成したコントラクト（oob-default）を選択します。[Update] をクリックします。

アウトオブバンド管理によって提供された同じコントラクトを選択します。

c) [Subnets] フィールドに、サブネット アドレスを入力します。[Submit] をクリックします。

ここで選択したサブネット アドレスだけがスイッチの管理に使用されます。含まれていないサブネット アドレスはスイッチの管理に使用できません。

ノード管理 EPG は外部 EPG に接続されます。アウトオブバンド管理接続が設定されます。

（注）
[システム（System）]>**[システム設定（System Settings）]**>**[APIC接続設定（APIC Connectivity Preferences）]** をクリックして、アウトオブバンド管理アクセスを Cisco APIC サーバのデフォルトの管理接続モードに設定できます。次に、[Connectivity Preferences] ページで [ooband] をクリックします。

テクニカルサポート、統計情報、およびコア ファイルのエクスポート

ファイルのエクスポートについて

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、統計情報、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 ポリシーを設定できます。エクスポートは XML、JSON、Web ソケット、Secure Copy Protocol (SCP) 、HTTP などのさまざまな形式にできます。ストリーミング、定期的、またはオンデマンドの各形式でエクスポートを登録できます。

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。

ファイルのエクスポートに関するガイドラインと制約事項

- HTTP エクスポートとストリーミング API 形式は、統計情報の場合にのみサポートされます。コアおよびテクニカル サポート データはサポートされていません。
- エクスポートされるファイルの宛先 IP アドレスは、IPv6 アドレスであってはなりません。
- 5 つを超えるノードからのテクニカル サポートを同時にトリガーしないでください。特に Cisco Application Policy Infrastructure Controller（APIC）にエクスポートする場合、または帯域幅とコンピューティング リソースが不十分な外部サーバにエクスポートする場合は、トリガーを実行しないでください。
- ファブリック内のすべてのノードからテクニカル サポートを定期的に収集するには、複数のポリシーを作成する必要があります。各ポリシーは、ノードのサブセットをカバーする必要があり、時間をずらしてトリガーされるようにスケジュールします（少なくとも 30 分離す）。
- Cisco APIC の同じノードに対して複数のテクニカル サポート ポリシーをスケジュールしないでください。同じノードで複数のテクニカル サポート ポリシーのインスタンスを同

時に実行すると、Cisco APIC が大量に消費されたり、 CPU サイクルやその他のリソースが切り替えられたりする可能性があります。

- メンテナンス モードになっているノードについては、オンデマンド テクニカル サポート ポリシーではなく、通常のテクニカル サポート ポリシーを使用することをお勧めします。
- メンテナンス モードのノードに対する進行中のテクニカル サポートのステータスは、Cisco APIC GUI の **[管理（Admin）]** > **[テクニカル サポート（Tech Support）]** > ***[policy_name]*** > **[操作（Operational）]** > **[ステータス（Status）]** セクションでは使用できません。テクニカル サポート ポリシーの **[コントローラへのエクスポート（Export to Controller）]** または **[エクスポート先（Export Destination）]** に基づいて、コントローラ（`/data/techsupport`）または宛先サーバを確認し、テクニカル サポートがキャプチャされていることを確認できます。
- Cisco APIC からのテクニカル サポートの収集は、リーフ スイッチ上のコアがビジー状態の場合にはタイムアウトすることがあります。BGP などのルーティング プロセスや HAL などのプラットフォーム プロセスが CPU を占有すると、コアがビジーになる可能性があります。テクニカル サポートの収集がタイムアウトした場合は、CPU 使用率を調べて、CPU 占有が発生しているかどうかを確認します。そのような場合には、リーフ スイッチのテクニカル サポートを直接収集すれば、タイムアウトの問題を回避できます。

ファイル エクスポート用のリモート ロケーションの作成

この手順では、エクスポートされたファイルを受け取るリモート ホストのホスト情報とファイル転送セッティングを設定します。

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。

ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。

ステップ 4 [Remote Locations] を右クリックし、[Create Remote Path of a File] を選択します。

ステップ 5 [Create Remote Path of a File] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、リモート ロケーションの名前を入力します。

b) [Host Name/IP] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。

c) [Protocol] フィールドで、必要なファイル転送プロトコルのオプション ボタンをクリックします。

d) [Remote Path] フィールドで、リモート ホストでファイルが保存されるパスを入力します。

e) リモート ホストにログインするためのユーザ名とパスワードを入力し、パスワードを確認します。

f) [Management EPG] ドロップダウン リストから管理 EPG を選択します。

g) [Submit] をクリックします。

GUI を使用したオンデマンド テクニカル サポート ファイルの送信

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。

ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。

ステップ 4 **[オンデマンド テクニカル サポート（On-demand Tech Support）]** を右クリックし、**[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）]** を選択します。

[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）] ダイアログ ボックスが表示されます。

ステップ 5 **[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）]** ダイアログ ボックスのフィールドに適切な値を入力します。

（注）
フィールドの説明については、**[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）]** ダイアログ ボックスのヘルプアイコンをクリックします。ヘルプ ファイルが開いてプロパティの説明ページが表示されます。

ステップ 6 **[送信（Submit）]** をクリックし、テクニカル サポート ファイルを送信します。

（注）
オンデマンドのテクニカルサポート ファイルは別の APIC に保存し、ストレージと CPU 条件のバランスを取ることができます。場所を確認するには、**[ナビゲーション（Navigation）]** ペインでオンデマンドのテクニカル サポート ポリシーをクリックし、**[作業（Work）]** ペインで **[操作（OPERATIONAL）]** タブをクリックします。コントローラが [EXPORT LOCATION] フィールドに表示されます。

ステップ 7 ポリシー名を右クリックし、[Collect Tech Support] を選択します。

ステップ 8 [Yes] を選択して、テクニカル サポート情報の収集を開始します。

概要

このトピックでは、次の情報を提供します。

- Cisco APIC の設定のインポートとエクスポートを使用して、設定の状態を最新の既知の良好な状態に回復する方法

- Cisco APIC の設定ファイルのセキュア プロパティを暗号化する方法

ユーザ設定のスケジュール バックアップとオンデマンド バックアップの両方を行うことができます。設定の状態を回復すると（「ロールバック」とも呼ばれます）、以前良好であった既知の状態に戻ることができます。そのためのオプションは、アトミック置換と呼ばれます。設定インポート ポリシー（configImportP）は、アトミック + 置換（importMode=atomic、importType=replace）をサポートします。これらの値に設定すると、インポートされる設定が既存の設定を上書きし、インポートされるファイルに存在しない既存の設定があれば削除されます。定期的に設定のバックアップとエクスポートを行うか、既知の良好な設定のエクスポートを明示的にトリガーすれば、後で以下の CLI、REST API、および GUI 用の手順を使用してこの設定を復元できます。

Cisco APIC を使用した設定状態の回復に関する詳細な概念情報については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

次の項では、設定ファイルのセキュア プロパティの暗号化に関する概念情報を提供します。

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。

GUI を使用したリモート ロケーションの設定

この手順では、APIC GUI を使用してリモート ロケーションを作成する方法について説明します。

手順

ステップ 1 メニュー バーで、[ADMIN] > [Import/Export] の順に選択します。

ステップ 2 ナビゲーション ペインで、[Remote Locations] を右クリックして [Create Remote Location] を選択します。
[Create Remote Location] ダイアログが表示されます。

ステップ 3 [Create Remote Location] ダイアログのフィールドに適切な値を入力します。

（注）
フィールドの説明については、[i]アイコンをクリックするとヘルプ ファイルが表示されます。

ステップ 4 [Create Remote Location] ダイアログのフィールドに値を入力したら、[Submit] をクリックします。
これで、データをバックアップするためのリモート ロケーションが作成されました。

GUI を使用したエクスポート ポリシーの設定

この手順では、Cisco Application Policy Infrastructure Controller（APIC）を使用してエクスポートポリシーを設定する方法について説明します。次の手順を使用して、データのバックアップをトリガーします。

（注） スケジューラ ポリシーで設定されている **[最大同時ノード数（Maximum Concurrent Nodes）]** の値によって、スケジューラ ポリシーで指定された時間に動作する設定エクスポート ポリシーの数が決まります。

たとえば、スケジューラ ポリシーで **[最大同時ノード数（Maximum Concurrent Nodes）]** が **1** に設定され、同じスケジューラ ポリシーを使用する 2 つのエクスポート ポリシーが設定されている場合、1 つのエクスポートポリシーは成功し、もう 1 つは失敗します。ただし、**[最大同時ノード数（Maximum Concurrent Nodes）]** を **2** に設定すると、両方の設定が成功します。

ユーザが読み取り専用権限でログインしている場合でも、[オンデマンド テクニカル サポート（On-Demand Tech Support）] ポリシーまたは [設定のエクスポート（Configuration Export）] ポリシーを右クリックして **[トリガー（Trigger）]** を選択すると、テクニカル サポート データをエクスポートできます。

手順

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[インポート/エクスポート（Import/Export）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシーのインポート（Import Policies）]** を右クリックして、**[設定のインポート ポリシーの作成（Create Configuration Import Policy）]** を選択します。
[Create Configuration Export Policy] ダイアログが表示されます。

ステップ 3 [Create Configuration Export Policy] ダイアログのフィールドに適切な値を入力します。

フィールドの説明については、ヘルプ（[?]）アイコンをクリックするとヘルプ ファイルが表示されます。

ステップ 4 **[設定インポート ポリシーの作成（Create Configuration Import Policy）]** ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

これで、バックアップが作成されました。これは **[設定（Configuration）]** タブで確認できます。バックアップ ファイルが右側の **[設定（Configuration）]** ペインに表示されます。

（注）
Cisco Network Assurance Engine（NAE）を展開して必要な設定を行った場合も、一定間隔でデータを収集するための Cisco APIC のエクスポート ポリシーが Cisco APIC に作成されますCisco NAE エクスポート ポリシーは、アシュアランス コントロール設定に基づく名前で識別できます。Cisco APIC で Cisco NAE エクスポート ポリシーを削除すると、Cisco NAE エクスポート ポリシーが Cisco APIC に再表示されます。Cisco NAE エクスポート ポリシーを削除しないことをお勧めします。

ステップ 5 **[ナビゲーション（Navigation）]** ペインで、**[ポリシーのエクスポート（Export Policies）]** > **[設定（Configuration）]** > ***[policy_name]*** の順に選択します。

ステップ 6 **[作業（Work）]** ペインで、**[操作（Operational）]** > **[ジョブ ステータス（Job Status）]** タブをクリックします。

この画面では、ジョブのエクスポートに関する情報を含むテーブルを表示できます。ジョブのエクスポートをトリガーしなかった場合、テーブルは空になります。**[状態（State）]** カラムは、ジョブのエクスポート ステータスを示します。設定可能な値は次のとおりです。

- `success`：ジョブが成功しました。
- `failed`：ジョブが失敗しました。
- `success-with-warnings`：ジョブは成功しましたが、いくつかの問題がありました。

[詳細（Details）] カラムは、整合性検証が成功したか失敗したかを示します。

バックアップを作成した場合、Cisco APIC は作成されたバックアップファイルの **[操作（Operational）]** ビューに表示されるファイルを作成します。そのデータをインポートする場合は、インポート ポリシーを作成する必要があります。

GUI を使用したインポート ポリシーの設定

この手順では、APIC GUI を使用してインポート ポリシーを設定する方法について説明します。バックアップ データをインポートするには、次の手順に従います。

手順

ステップ 1 メニュー バーで、[ADMIN] > [Import/Export] の順に選択します。

ステップ 2 ナビゲーション ペインで、[Import Policies] を右クリックして [Create Configuration Import Policy] を選択します。
[Create Configuration Import Policy] ダイアログが表示されます。

ステップ 3 [Create Configuration Import Policy] ダイアログのフィールドに適切な値を入力します。

（注）
フィールドの説明については、[i] アイコンをクリックするとヘルプ ファイルが表示されます。[Replace]、[Merge]、[Best Effort]、[Atomic] などのインポート タイプやモードの詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

ステップ 4 [Create Configuration Import Policy] ダイアログのフィールドに値を入力したら、[Submit] をクリックします。

（注）
ファブリックのクリーンリロードを実行し、以前に保存した設定をインポートすると、タイムゾーンはデフォルトで UTC に変更されます。このような状況では、APIC クラスタの設定のインポート後に、タイムゾーンをローカル タイムゾーンにリセットします。

GUI を使用した設定ファイルの暗号化

AES-256 暗号化はグローバル設定オプションです。有効にすると、すべてのセキュア プロパティは AES の構成設定に準拠します。特定の targetDn を持つ設定エクスポートを使用して、ACI ファブリック設定の一部をエクスポートできます。ただし、REST API を使用して、セキュア プロパティと AES 暗号化を含むテナント設定などの ACI ファブリック部分のみをエクスポートすることはできません。REST API 要求時にはセキュア プロパティは含まれません。

この項では、AES-256 暗号化を有効にする方法について説明します。

手順

ステップ 1 メニュー バーで、[ADMIN] > [AAA] を選択します。

ステップ 2 ナビゲーション ペインで、[AES Encryption Passphrase and Keys for Config Export (and Import)] をクリックします。
右側のペインに、[Global AES Encryption Settings for all Configurations Import and Export] ウィンドウが表示されます。

ステップ 3 パスフレーズを作成します（16 ～ 32 文字の長さ）。使用される文字のタイプに制限はありません。

ステップ 4 [Submit] をクリックします。

（注）
パスフレーズを作成して送信すると、バックエンドでキーが生成され、パスフレーズを復元することはできません。したがって、パスフレーズは、キーを自動的に生成した後で削除されるため、誰にも表示されません。バックアップは、パスフレーズを知っている場合にのみ動作します（他のユーザは誰も開くことはできません）。

[Key Configured] フィールドには [yes] と表示されます。[Encrpyted Passphrase] フィールドには暗号化されたハッシュ（実際のパスフレーズではなく、そのハッシュでしかありません）が表示されます。

ステップ 5 パスフレーズを設定および確認したら、[Enable Encryption] の横にあるチェックボックスをオンにして AES 暗号化機能を有効にします（オンにします）。

これで、エクスポートおよびインポート ポリシーの [Global AES Encryption Settings] フィールドはデフォルトで有効になります。

（注）
- インポートおよびエクスポート ポリシーで [Fail Import if secure fields cannot be decrypted] チェックボックスがオンになっていることを確認します（デフォルトではオンになっています）。設定をインポートするときにこのチェックボックスをオフにしないことを強くお勧めします。このチェックボックスをオフにすると、システムがすべてのフィールドをインポートしようとしても、暗号化できないフィールドはブランクまたは欠落となります。その結果、管理者のパスワードがブランクまたは欠落となると、システムからロックアウトされる可能性があります（システムからロックアウトされた場合は、『*Cisco APIC Troubleshooting Guide*』を参照してください）。このチェックボックスをオフにすると、警告メッセージが表示されます。このボックスをオンにすると、ロックアウトを予防するためのセキュリティ チェックが行われ、その設定はインポートされません。
- [Enable Encryption] チェックボックスが選択されていない（オフ）場合は、暗号化が無効になり、エクスポートされるすべての設定（エクスポート）でセキュア フィールド（パスワードや証明書など）が欠落します。このチェックボックスを選択する（オン）と、暗号化が有効になり、すべてのエクスポートでセキュア フィールドが表示されます。
- 暗号化を有効にした後は、新しいインポートまたはエクスポート ポリシーの作成時にパスフレーズを設定することはできません。前に設定したパスフレーズは、このボックス内のすべての設定およびすべてのテナントにわたってグローバルになっています。このタブか

ら設定をエクスポートすると（パスフレーズが設定され、暗号化は有効）、完全なバックアップ ファイルが得られます。暗号化が有効になっていない場合、セキュア プロパティが削除されたバックアップ ファイルが得られます。これらのバックアップ ファイルは、TAC サポート エンジニア向けにエクスポートする場合に役立ちます（たとえば、すべてのセキュア フィールドが欠落しているため）。これは、設定内のすべてのセキュア プロパティに該当します。また、暗号化キーをクリアするクリア オプションもあります。

次の表で、設定インポートの動作と関連する結果のリストに注意してください。

設定インポートの動作シナリオ	結果
以前のリリースからの古い設定	古いリリースの設定のインポートは完全にサポートされ、古い設定に保存されているすべてのセキュア フィールドが正常にインポートされます。
AES 暗号化が設定されていないときの設定インポート	セキュア フィールドがない設定のインポートである場合は、前に説明した動作で正常に行われます。インポートされる設定にセキュア フィールドがある場合は、拒否されます。
AES パスフレーズが一致しないときの設定インポート	セキュア フィールドがない設定のインポートである場合は、前に説明した動作で正常に行われます。インポートされる設定にセキュア フィールドがある場合は、拒否されます。
AES パスフレーズが一致するときの設定インポート	正常にインポートされます。
コピー/ペーストされたフィールドで AES パスフレーズが一致しないときの設定インポート	この特殊なケースは、別のパスフレーズを使用してエクスポートされた他の設定からセキュア フィールドをコピー/ペーストした場合に発生します。最初のパスでインポートされるバックアップ ファイルを解析しているときに、正しく復号できないプロパティがあった場合、インポートはどのシャードもインポートせずに失敗します。したがって、あるシャードですべてのプロパティを復号することができない場合、すべてのシャードが拒否されます。

コントローラコンフィギュレーションのバックアップ、復元、およびロールバック

ここでは、コントローラコンフィギュレーションのバックアップ（スナップショットの作成）、復元、およびロールバックのための一連の機能について説明します。

設定ファイルのバックアップ、復元、およびロールバックのワークフロー

この項では、設定ファイルのバックアップ、復元、およびロールバックのワークフローについて説明します。本書で説明されている機能はすべて同じワークフローパターンに従います。対応するポリシーを設定すると、ジョブをトリガーするために **admintSt** を **triggered** に設定する必要があります。

ジョブがトリガーされると、**configJobCont** タイプのコンテナ オブジェクトで **configJob** タイプのオブジェクト（実行を表す）が作成されます（Naming プロパティの値はポリシー DN に設定されます）。コンテナの**lastJobName**フィールドを使用して、そのポリシーに対してトリガーされた最後のジョブを確認することができます。

（注） 同時に最大 5 つの **configJob** オブジェクトが単一ジョブ コンテナに保持され、それぞれの新規ジョブがトリガーされます。そのために、最も古いジョブは削除されます。

configJob オブジェクトには、次の情報が含まれています。

- 実行時間
- 処理または生成されるファイルの名前
- 以下のステータス：
  - Pending
  - Running
  - 失敗（Failed）
  - Fail-no-data
  - Success
  - Success-with-warnings
- 詳細の文字列（障害メッセージと警告）
- 進捗率 = 100 * lastStepIndex/totalStepCount

- 最後に行われた内容を示す lastStepDescr フィールド

fileRemotePath オブジェクトについて

fileRemotePath オブジェクトは、以下のリモート ロケーションパスのパラメータを保持しています。

- ホスト名または IP
- ポート
- プロトコル：FTP、SCP など
- リモート ディレクトリ（ファイル パスではない）
- ユーザー名
- パスワード

（注） パスワードは、変更するたびに再送信する必要があります。

設定例

以下に設定サンプルを示します。

fabricInst（uni/fabric）の下に、次のように入力します。

```
<fileRemotePath name="path-name" host="host name or ip" protocol="scp"
remotePath="path/to/some/folder" userName="user-name" userpasswd="password" />
```

コントローラへの設定のエクスポート

設定のエクスポートでは、クラスタ内の 32 個のシャードすべてからユーザ設定可能な管理対象オブジェクト（MO）のツリーを抽出して別々のファイルに書き込み、tar gzip に圧縮します。次に、tar gzip を、事前設定されているリモート ロケーション（**fileRemotePath** オブジェクトを指す **configRsRemotePath** を使用して設定）にアップロードするか、またはコントローラ上の**スナップショット**として保存します。

（注） 詳細については、「スナップショット」の項を参照してください。

configExportP ポリシーは次のように設定されます。

- **name**：ポリシー名

- **format**：エクスポートされたアーカイブ内にデータを保存する形式（xml または json）
- **targetDn**：エクスポートする特定のオブジェクトのドメイン名（DN）（空はすべてを意味します）
- **snapshot**：`true` に設定されている場合、ファイルはコントローラ上に保存され、リモートロケーションの設定は不要です。
- **includeSecureFields**：デフォルトで true に設定され、暗号化されたフィールド（パスワードなど）をエクスポートのアーカイブに含めるかどうかを示します。

（注） このスナップショットに関する情報を保持する **configSnapshot** オブジェクトが作成されます（「スナップショット」の項を参照）。

エクスポートのスケジューリング

エクスポートポリシーは、事前設定されたスケジュールに基づいて自動的にエクスポートをトリガーするスケジューラーにリンクできます。これは、ポリシーから **trigSchedP** オブジェクトへの **configRsExportScheduler** 関係によって行われます（後の「設定例」の項を参照）。

（注） スケジューラーはオプションです。ポリシーは、**adminSt** を **triggered** に設定することにより、いつでもトリガーできます。

トラブルシューティング

生成されたアーカイブをリモートロケーションにアップロードできないことを示すエラーメッセージが表示された場合は、接続の問題に関する項を参照してください。

NX-OS スタイルの CLI を使用した設定例

以下に、NX-OS スタイルの CLI を使用した設定例を示します。

```
apic1(config)# snapshot
download  Configuration snapshot download setup mode
export    Configuration export setup mode
import    Configuration import setup mode
rollback  Configuration rollback setup mode
upload    Configuration snapshot upload setup mode
apic1(config)# snapshot export policy-name
apic1(config-export)#
format    Snapshot format: xml or json
no        Negate a command or set its defaults
remote    Set the remote path configuration will get exported to
schedule  Schedule snapshot export
target    Snapshot target

bash      bash shell for unix commands
end       Exit to the exec mode
exit      Exit from current mode
```

```
fabric    show fabric related information
show      Show running system information
where     show the current mode
apic1(config-export)# format xml
apic1(config-export)# no remote path         [If no remote path is specified, the file
is exported locally to a folder in the controller]
apic1(config-export)# target                 [Assigns the target of the export, which
can be fabric, infra, a specific tenant, or none. If no target is specified, all
configuration information is exported.]
WORD  infra, fabric or tenant-x
apic1(config-export)#
apic1# trigger snapshot export policy-name   [Executes the snapshot export task]
apic1# ls /data2                             [If no remote path is specified, the
configuration export file is saved locally to the controller under the folder data2]
ce_Dailybackup.tgz
```

GUI を使用した設定例

以下に、GUI を使用した設定例を示します。

1. メニュー バーで、[Admin] タブをクリックします。
2. **[インポート/エクスポート（IMPORT / EXPORT）]** を選択します。
3. **[ポリシーのエクスポート（Export Policies）]** の下で、**[設定（Configuration）]** を選択します。
4. [Configuration] の下で、ロールバック先の設定をクリックします。たとえば、デフォルトである [defaultOneTime] をクリックできます。
5. **[形式（Format）]** の横で、JSON形式またはXML形式のいずれかに対するボタンを選択します。
6. **[今すぐ開始（Start Now）]** の横で、**[いいえ（No）]** または **[はい（Yes）]** のボタンを選択し、今すぐトリガーするかスケジュールに基づいてトリガーするかを示します最も簡単な方法は、ただちにトリガーすることを選択することです。
7. [Target DN] フィールドに、エクスポートするテナント設定の名前を入力します。
8. 設定をコントローラ自体に保存する場合は、[Snapshot] オプションをオンにします。リモート ロケーションを設定する場合は、このオプションをオフにします。
9. [Scheduler] フィールドでは、オプションで、設定をエクスポートする時間と方法を指示するスケジューラを作成できます。
10. **[暗号化（Encryption）]** フィールドでは、設定ファイルの暗号化を有効または無効にするオプションがあります。
11. 設定が完了したら、[Start Now] をクリックします。
12. **[送信（SUBMIT）]** をクリックして、設定のエクスポートをトリガーします。

REST API を使用した設定例

以下に、REST API を使用した設定例を示します。

```
<configExportP name="policy-name" format="xml" targetDn="/some/dn or empty which means
everything"
snapshot="false" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
<configRsExportScheduler tnTrigSchedPName="some scheduler name" />
</configExportP>
```

（注） リモートロケーションを指定するときに、スナップショットを`True`に設定すると、バックアップはリモート パスを無視し、ファイルをコントローラに保存します。

コントローラへの設定のインポート

設定のインポートでは、指定されている以前にエクスポートされたアーカイブのダウンロード、抽出、解析、分析、および適用を、一度に 1 つのシャードずつ行います（infra、fabric、tn-common、その他すべて、の順）。fileRemotePath設定は、エクスポートの場合と同様に実行されます（configRsRemotePathを使用）。スナップショットのインポートもサポートされます。

configImportP ポリシーは次のように設定されます。

- **name**：ポリシー名
- **fileName**：インポートするアーカイブ ファイルの名前（パス ファイルではない）
- **importMode**
  - ベスト エフォート モード：各 MO は個々に適用され、エラーがあっても無効な MO がスキップされるだけです。

（注） オブジェクトがコントローラに存在しない場合、そのオブジェクトの子は設定されません。ベスト エフォート モードでは、オブジェクトの子を設定しようとします。

  - アトミック モード：設定はシャード全体で適用されます。1 つのエラーがあると、シャード全体が元の状態にロールバックされます。

- **importType**
  - replace：現在のシステム設定は、インポートされる内容またはアーカイブで置換されます（アトミック モードのみをサポート）
  - merge：何も削除されず、アーカイブの内容が既存のシステム設定上に適用されます。
- **snapshot**：true の場合、ファイルはコントローラから取得され、リモート ロケーションの設定は不要です。
- **failOnDecryptErrors**：（デフォルトで true）現在システムに設定されているキーとは異なるキーでアーカイブが暗号化されている場合、ファイルはインポートされません。

トラブルシューティング

以下のシナリオでは、トラブルシューティングが必要な可能性があります。

- 生成されたアーカイブをリモートロケーションからダウンロードできなかった場合は、接続の問題に関する項を参照してください。
- インポートは正常に終了したが警告が表示された場合は、詳細を確認してください。
- ファイルを解析できなかった場合は、以下のシナリオを参照してください。
  - ファイルが有効なXMLまたはJSONファイルでない場合は、エクスポートされたアーカイブから取得したファイルが手動で変更されたかどうかを確認してください。
  - オブジェクトプロパティに未知のプロパティまたはプロパティ値がある場合は、以下の原因が考えられます。
    - プロパティが削除されたか、または未知のプロパティ値が手動で入力された
    - モデル タイプの範囲が変更された（後方互換性がないモデル変更）
    - 名前付けプロパティ リストが変更された
- MO を設定できなかった場合は、以下に注意してください。
  - ベスト エフォート モードでは、エラーをログに記録し、その MO をスキップします
  - アトミック モードでは、エラーをログに記録し、シャードをスキップします

NX-OS スタイルの CLI を使用した設定例

以下に、NX-OS スタイルの CLI を使用した設定例を示します。

```
apic1# configure
apic1(config)# snapshot
 download  Configuration snapshot download setup mode
export    Configuration export setup mode
import    Configuration import setup mode
rollback  Configuration rollback setup mode
upload    Configuration snapshot upload setup mode
apic1(config)# snapshot import
 WORD       Import configuration name
default
rest-user
apic1(config)# snapshot import policy-name
apic1(config-import)#
 action  Snapshot import action merge|replace
file    Snapshot file name
mode    Snapshot import mode atomic|best-effort
no      Negate a command or set its defaults
remote  Set the remote path configuration will get imported from

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
```

```
where   show the current mode
apic1(config-import)# file < from "show snapshot files" >
apic1(config-import)# no remote path
apic1(config-import)#
apic1# trigger snapshot import policy-name       [Executes the snapshot import task]
```

GUI を使用した設定例

以下に、GUI を使用した設定例を示します。

1. メニュー バーで、[ADMIN] タブをクリックします。
2. [IMPORT/EXPORT] を選択します。
3. [Import Policies] の下で、[Configuration] を選択します。
4. [Configuration] の下で、[Create Configuration Import Policy] を選択します。[CREATE CONFIGURATION IMPORT POLICY] ウィンドウが表示されます。
5. [Name] フィールドでは、ファイル名は、バックアップされたファイル名と一致する必要があり、かなり固有の形式です。ファイル名は、バックアップを行った担当者が知っています。
6. 次の 2 つのオプションは、設定の状態の回復に関連しています（「ロールバック」とも呼ばれる）。これらのオプションは、[Input Type] と [Input Mode] です。設定の状態を回復する場合、以前良好であった既知の状態にロールバックします。そのためのオプションは [Atomic Replace] です。
7. 設定をコントローラ自体に保存する場合は、[Snapshot] オプションをオンにします。リモート ロケーションを設定する場合は、このオプションをオフにします。
8. [Import Source] フィールドで、作成済みのリモート ロケーションと同じ値を指定します。
9. [Encryption] フィールドでは、オプションで、設定ファイルの暗号化を

   有効または無効にすることができます。
10. [SUBMIT] をクリックして、設定のインポートをトリガーします。

REST API を使用した設定例

以下に、REST API を使用した設定例を示します。

```
<configImportP name="policy-name" fileName="someexportfile.tgz" importMode="atomic"
importType="replace" snapshot="false" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
</configImportP>
```

スナップショット

スナップショットは設定のバックアップのアーカイブであり、コントローラで管理されているフォルダに保存（および複製）されます。スナップショットを作成するには、**snapshot** プロパティを true に設定してエクスポートを実行します。この場合、リモート パスの設定は不要で

す。スナップショットをユーザに公開するために、**configSnapshot** タイプのオブジェクトが作成されます。

有効になっている場合、繰り返しスナップショットは **[管理（Admin）]** > **[インポート/エクスポート（Import/Export）]** > **[ポリシーのエクスポート（Export Policies）]** > **[設定（Configuration）]** > **[defaultAuto]** に保存できます

configSnapshot オブジェクトは以下を提供します。

- ファイル名
- ファイル サイズ
- 作成日
- 何のスナップショットであるかを示すルート DN（ファブリック、インフラ、特定のテナントなど）
- スナップショットを削除する機能（retire フィールドを true に設定）

スナップショットをインポートするには、最初にインポート ポリシーを作成します。**[管理（Admin）]** > **[インポート/エクスポート（Import / Export）]**に移動し、**[ポリシーのインポート（Import Policies）]** をクリックします。右クリックし、**[設定のインポート ポリシーの作成]** を選択して、インポート ポリシーの属性を設定します。

スナップショット マネージャ ポリシー

configSnapshotManagerP ポリシーを使用すると、リモートで保存したエクスポート アーカイブのスナップショットを作成することができます。ポリシーにリモートパスを付加し、ファイル名（configImportP と同じ）を指定し、モードをダウンロードに設定し、トリガーすることができます。マネージャは、ファイルをダウンロードし、そのファイルを分析してアーカイブが有効であることを確認し、そのファイルをコントローラに保存し、対応する configSnapshot オブジェクトを作成します。

繰り返しスナップショットを作成することもできます。

（注） 有効になっている場合、繰り返しスナップショットは**Admin** > **Import/Export** > **Export Policies** > **Configuration** > **defaultAuto** で保存されます。

スナップショット マネージャを使用すると、リモート ロケーションにスナップショット アーカイブをアップロードすることもできます。この場合、モードをアップロードに設定する必要があります。

トラブルシューティング

トラブルシューティングについては、接続の問題に関する項を参照してください。

NX-OS CLI を使用した、コントローラからリモート パスへのスナップショットのアップロード

```
apic1(config)# snapshot upload policy-name
apic1(config-upload)#
 file    Snapshot file name
no      Negate a command or set its defaults
remote  Set the remote path configuration will get uploaded to

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-upload)# file <file name from "show snapshot files">
apic1(config-upload)# remote path remote-path-name
apic1# trigger snapshot upload policy-name       [Executes the snapshot upload task]
```

NX-OS CLI を使用した、コントローラからリモート パスへのスナップショットのダウンロード

```
apic1(config)# snapshot download policy-name
apic1(config-download)#
 file    Snapshot file name
no      Negate a command or set its defaults
remote  Set the remote path configuration will get downloaded from

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-download)# file < file from remote path>
apic1(config-download)# remote path remote-path-name
apic1# trigger snapshot download policy-name      [Executes the snapshot download task]
```

GUI を使用したスナップショットのアップロードとダウンロード

スナップショット ファイルをリモート ロケーションにアップロードするには、次の手順に従います。

1. [Config Rollbacks] ペインにリストされているスナップショットを右クリックし、[Upload to Remote Location option] を選択します。[Upload snapshot to remote location] ボックスが表示されます。
2. [Submit] をクリックします。

リモート ロケーションからスナップショット ファイルをダウンロードするには、次の手順に従います。

1. 画面の右上にあるインポート アイコンをクリックします。[Import remotely stored export archive to snapshot] ボックスが表示されます。
2. [File Name] フィールドにファイル名を入力します。
3. [Import Source] プルダウンからリモート ロケーションを選択するか、または [Or create a new one] の横にあるボックスをオンにして新しいリモート ロケーションを作成します。
4. [Submit] をクリックします。

REST API を使用したスナップショットのアップロードとダウンロード

```
<configSnapshotManagerP name="policy-name" fileName="someexportfile.tgz"
mode="upload|download" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
</configSnapshotManagerP>
```

ロールバック

configRollbackP ポリシーを使用すると、2 つのスナップショットの間で行われた変更を元に戻して、以前に保存したスナップショットに対する設定変更を効果的にロールバックすることができます。ポリシーがトリガーされると、次のようにオブジェクトが処理されます。

- 削除された MO を再作成します
- 作成された MO を削除します
- 変更された MO を元に戻します

（注）

- ロールバック機能はスナップショットに対してのみ動作します。
- リモート アーカイブは直接的にはサポートされていません。ただし、スナップショット マネージャ ポリシー（configSnapshotMgrP）を使用して、リモートで保存されたエクスポートをスナップショットにすることができます。詳細については、スナップショット マネージャ ポリシー （82 ページ）を参照してください。
- configRollbackP ポリシーでは、リモート パス設定は不要です。リモート パスが指定されている場合は無視されます。

ロールバックのワークフロー

ポリシーの snapshotOneDN フィールドと snapshotTwoDn フィールドには、最初のスナップショット（S1）と次のスナップショット 2（S2）を設定する必要があります。トリガーされると、スナップショットが抽出および分析され、スナップショット間の違いが算出されて適用されます。

MO は次のように処理されます。

- S1 には存在するが S2 には存在しない MO：これらの MO は S2 の前に削除されました。ロールバックではこれらの MO が再作成されます。
- S2 には存在するが S1 には存在しない MO：これらの MO は S1 の後に作成されました。ロールバックでは、次の場合にこれらの MO が削除されます。
  - S2 の取得後に MO が変更されていない。
  - S2 の取得後に作成または変更された MO の子孫がない。

- S1 と S2 の両方に存在するがプロパティ値が異なる MO：S2 の取得後にプロパティが別の値に変更されている場合、プロパティはそのまま残ります。変更されていない場合は、ロールバックによってこれらのプロパティは S1 の値に戻ります。

ロールバック機能では、これらの計算の結果として生成された設定が含まれている diff ファイルも生成されます。この設定の適用は、ロールバック プロセスの最後のステップです。このファイルの内容は、readiff と呼ばれる特殊な REST API を使用して取得できます。
apichost/mqapi2/snapshots.readiff.xml?jobdn=SNAPSHOT_JOB_DN

ロールバックは予測が困難なため、ロールバックによる実際の変更が行われないプレビューモード（preview を true に設定）も利用できます。このモードでは算出と diff ファイルの生成のみが行われ、ロールバックを実際に実行した場合の状況を正確にプレビューできます。

Diff ツール

2 つのスナップショット間の diff 機能を提供する別の特殊な REST API を使用できます。
apichost/mqapi2/snapshots.diff.xml?s1dn=SNAPSHOT_ONE_DN&s2dn=SNAPSHOT_TWO_DN

NX-OS スタイルの CLI を使用した設定例

この例では、NX-OS スタイルの CLI を使用してロールバックを設定および実行する方法を示します。

```
apic1# show snapshot files
File    : ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
Created : 2015-11-21T01:00:21.167+00:00
Root    :
Size    : 22926

File    : ce2_DailyAutoBackup-2015-11-21T09-00-21.tar.gz
Created : 2015-11-21T09:00:24.025+00:00
Root    :
Size    : 23588

apic1# configure
apic1(config)# snapshot rollback myRollbackPolicy
apic1(config-rollback)# first-file ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
apic1(config-rollback)# second-file ce2_DailyAutoBackup-2015-11-21T09-00-21.tar.gz
apic1(config-rollback)# preview
apic1(config-rollback)# end
apic1# trigger snapshot rollback myRollbackPolicy
```

GUI を使用した設定例

この例では、GUI を使用してロールバックを設定および実行する方法を示します。

1. メニュー バーで、[Admin] タブをクリックします。
2. [Admin] タブにある [Config Rollbacks] をクリックします。
3. [Config Rollbacks] リスト（左側のペイン）で最初の設定ファイルを選択します。
4. [Configuration for selected snapshot] ペイン（右側のペイン）で 2 番目の設定ファイルを選択します。

5. [Compare with previous snapshot] ドロップダウン メニュー（右側のペインの下部）をクリックし、リストから 2 番目の設定ファイルを選択します。その後、2 つのスナップショット間の違いを比較できるように diff ファイルが生成されます。

（注） ファイルが生成された後、これらの変更を元に戻すことができます。

REST API を使用した設定例

この例では、REST API を使用してロールバックを設定および実行する方法を示します。

```
<configRollbackP name="policy-name" snapshotOneDn="dn/of/snapshot/one"
snapshotOneDn="dn/of/snapshot/two" preview="false" adminSt="triggered" />
```

Syslog の使用

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。

Syslog の宛先および宛先グループの作成

この手順では、ロギングおよび評価用の syslog データの宛先を設定します。syslog データは、コンソール、ローカル ファイル、または宛先グループ内の 1 つまたは複数の syslog サーバにエクスポートできます。

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[External Data Collectors] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Destinations] を展開します。

ステップ 4 [Syslog] を右クリックし、[Create Syslog Monitoring Destination Group] を選択します。

ステップ 5 [Create Syslog Monitoring Destination Group] ダイアログボックスで、次の操作を実行します。

a) グループおよびプロファイルの [Name] フィールドに、モニタリングの宛先グループおよびプロファイルの名前を入力します。

b) グループおよびプロファイルの [Format] フィールドで、Syslog メッセージの形式を選択します。

デフォルトは [aci]、または RFC 3164 準拠のメッセージ形式ですが、NX-OS スタイル形式に設定することもできます。

c) グループおよびプロファイルの [Admin State] ドロップダウン リストで、[enabled] を選択します。

d) ローカル ファイルへの syslog メッセージの送信を有効にするには、[Local File Destination] の [Admin State] ドロップダウン リストから [enabled] を選択し、[Local File Destination] の [Severity] ドロップダウン リストからシビラティ（重大度）の最小値を選択します。

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。

e) コンソールへの syslog メッセージの送信を有効にするには、[Console Destination] の [Admin State] ドロップダウン リストから [enabled] を選択し、[Console Destination] の [Severity] ドロップダウン リストからシビラティ（重大度）の最小値を選択します。

f) [Next] をクリックします。

g) [Create Remote Destinations] 領域で、[+] をクリックしてリモート宛先を追加します。

注意
指定した DNS サーバがインバンド接続を介して到達可能に設定されている場合、リモート syslog 宛先のホスト名解決に失敗するリスクがあります。この問題を回避するには、IP アドレスを使用して syslog サーバを設定します。ホスト名を使用する場合は、アウトオブバンド インターフェイス経由で DNS サーバに到達できることを確認します。

ステップ 6 [Create Syslog Remote Destination] ダイアログボックスで、次の操作を実行します。

a) [Host] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。

b) （任意） [Name] フィールドに、宛先ホストの名前を入力します。

c) [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

d) （任意） 最小シビラティ（重大度）、**[シビラティ（重大度）（Severity）]**、**[ポート（Port）]** 番号、および syslog **[ファシリティ（Facility）]**を選択します。

[ファシリティ（Facility）]は、メッセージを生成したプロセスを示すためにオプションで使用できる番号で、受信側でのメッセージの処理方法を決定するために使用できます。

e) 5.2（3）以降のリリースでは、**[トランスポート（Transport）]** フィールドで、メッセージに使用するトランスポート プロトコルを選択します。

- リリース 5.2(4) より前のリリースでは、メッセージに使用するトランスポート プロトコルとして **tcp** または **udp** を選択します。
- 5.2(4) リリース以降では、メッセージに使用するトランスポートプロトコルのオプションとして、**ssl** も選択できるようになりました。この機能を使用すると、（クライアントとして機能している）ACI スイッチが、ロギングにセキュアな接続をサポートする（サーバーとして機能している）リモート Syslog サーバーに対してセキュアな暗号化されたアウトバウンド接続を確立できるようになります。認証と暗号化により、この機能では、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

  メッセージに使用するトランスポート プロトコルとして **ssl** を選択した場合は、必要な SSL 証明書もアップロードする必要があることに注意してください。**[認証局の作成（Create Certificate Authority）]** ウィンドウに移動して、必要な SSL 証明書をアップロードできます。

  [管理（Admin）] > **[AAA]** > **[セキュリティ（Security）]** > **[公開キー管理（Public Key Management）]** > **[認証局（Certificate Authorities）]**を選択し、その後**[アクション（Actions）]** > **[認証局の作成（Create Certificate Authority）]**を選択します。

トランスポート プロトコルのデフォルト オプションは **udp** です。

f) [Management EPG] ドロップダウン リストから管理エンドポイント グループを選択します。

g) [OK] をクリックします。

ステップ 7 （任意）リモート宛先グループにリモート宛先を追加するには、もう一度 [+] をクリックし、[Create Syslog Remote Destination] ダイアログボックスの手順を繰り返します。

ステップ 8 **[完了（Finish）]** をクリックします。

Syslog 送信元の作成

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。

始める前に

syslog モニタリング宛先グループを作成します。

手順

ステップ 1 メニュー バーおよびナビゲーション フレームから、関心領域の [Monitoring Policies] メニューに移動します。

テナント、ファブリック、およびアクセスのモニタリング ポリシーを設定できます。

ステップ 2 [Monitoring Policies] を展開し、モニタリング ポリシーを選択して展開します。

[Fabric] > [Fabric Policies] > [Monitoring Policies] > [Common Policy] の下に、基本モニタリング ポリシーがあります。このポリシーは、すべての障害とイベントに適用され、ファブリック内のすべてのノードとコントローラに自動的に導入されます。または、スコープが限定された既存のポリシーを指定することもできます。

ステップ 3 モニタリング ポリシーの下で、[Callhome/SNMP/Syslog] をクリックします。

ステップ 4 [Work] ペインで、[Source Type] ドロップダウン リストから [Syslog] を選択します。

ステップ 5 [Monitoring Object] リストから、モニタ対象の管理対象オブジェクトを選択します。

目的のオブジェクトがリストに表示されない場合は、次の手順に従います。

a) [Monitoring Object] ドロップダウン リストの右側にある [Edit] アイコンをクリックします。
b) [Select Monitoring Package] ドロップダウン リストから、オブジェクト クラス パッケージを選択します。
c) モニタ対象の各オブジェクトのチェックボックスをオンにします。
d) [Submit] をクリックします。

ステップ 6 テナント モニタリング ポリシーでは、[All] ではなく特定のオブジェクトを選択すると、[Scope] 選択が表示されます。

[Scope] フィールドで、オプション ボタンを選択して、このオブジェクトに関して送信するシステム ログ メッセージを指定します。

- [all]：このオブジェクトに関連するすべてのイベントと障害を送信します。
- [specific event]：このオブジェクトに関連する指定されたイベントのみを送信します。[Event] ドロップダウン リストからイベント ポリシーを選択します。
- [specific fault]：このオブジェクトに関連する指定された障害のみを送信します。[Fault] ドロップダウン リストから障害ポリシーを選択します。

ステップ 7 [+] をクリックして syslog 送信元を作成します。

ステップ 8 [Create Syslog Source] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、syslog 送信元の名前を入力します。
b) [Min Severity] ドロップダウン リストから、送信するシステム ログ メッセージのシビラティ（重大度）の最小値を選択します。
c) [Include] フィールドで、送信するメッセージ タイプのチェックボックスをオンにします。
d) [Dest Group] ドロップダウン リストから、システム ログ メッセージの送信先の syslog 宛先グループを選択します。
e) [Submit] をクリックします。

ステップ 9 （任意） syslog 送信元を追加するには、もう一度 [+] をクリックし、[Create Syslog Source] ダイアログボックスの手順を繰り返します。

アトミック カウンタの使用

アトミック カウンタについて

アトミック カウンタは、フロー間のトラフィックに関する統計情報を収集できます。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。送信元と宛先のリーフ 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。

- 送信パケット、受信パケット、ドロップ パケット、および超過パケットのカウント

- 送信パケット：送信数は、送信元 TEP（トンネル エンドポイント）から宛先 TEP に送信されたパケット数を表します。
- 受信パケット：受信数は、宛先 TEP が送信元 TEP から受信したパケット数を表します。
- ドロップパケット：ドロップ数は、伝送中にドロップされたパケット数を表します。この数値は、送信パケット量と受信パケット量の差です。
- 超過パケット：超過数は、伝送中に受信された超過パケット数を表します。この数値は、転送の不一致または間違った場所へのルーティングミスによって予期せず受信されたパケット量です。

- 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。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。

テナントのアトミック カウンタは次を提供できます。

- 送信、受信、ドロップ、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。
  - EPtoEP（エンドポイント間）
  - EPGtoEPG（エンドポイント グループ間）

（注） EPGtoEPG の場合、オプションには ipv4 のみ、ipv6 のみ、ipv4、ipv6 が含まれます。ipv6 オプションがある場合は必ず TCAM エントリを 2 回使用します。これは、スケール数が、純粋な ipv4 ポリシーの場合に予期される数より小さい可能性があることを意味します。

  - EPGtoEP（エンドポイント グループ/エンドポイント間）
  - EPtoAny（エンドポイント ツー エニー）

- AnytoEP（エニー ツー エンドポイント）
- EPGtoIP（エンドポイント グループ/IP 間、外部 IP アドレスの場合にのみ使用）
- EPtoExternalIP（エンドポイント/外部 IP アドレス間）

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。

アトミック カウンタに関する注意事項および制約事項

- 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コンテキスト（VRF）にある場合はサポートされません。
- Cisco APIC リリース 3.1(2m) 以降では、ファブリックのライフタイム内のパスで統計情報が生成されなかった場合、そのパスに対するアトミック カウンタは生成されません。また、**[トラフィック マップ（Traffic Map）]**（**[可視化（Visualization）]** タブにあるもので、**[操作（Operations）]** > **[可視化（Visualization）]**を Cisco APIC GUIで選択する）には、すべてのパスではなく、アクティブなパス、つまりファブリックの寿命のいずれかの時点で、トラフィックがあったパスだけが表示されます。
- IP アドレスが学習されない純粋なレイヤ 2 設定（IP アドレスは 0.0.0.0）では、エンドポイント/EPG 間および EPG/エンドポイント間のアトミック カウンタ ポリシーはサポートされません。この場合、エンドポイント間および EPG 間のポリシーはサポートされます。外部ポリシーは学習された IP アドレスが必要な Virtual Routing and Forwarding（VRF）ベースであり、サポートされます。
- アトミック カウンタの送信元または宛先がエンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）にはアトミック カウンタに必要な子オブジェクト（fv:RsCEpToPathEp）がありません。
- 中継トポロジでは、リーフ スイッチはすべてのスパイン スイッチを使用したフル メッシュにはなく、リーフ間（TEP 間）のカウンタは予期どおりに動作しません。
- リーフ間（TEP 間）アトミック カウンタの場合、トンネル数がハードウェア制限を上回ると、システムはモードをトレール モードからパス モードに変更し、ユーザにはスパインごとのトラフィックは表示されなくなります。
- アトミック カウンタはスパイン プロキシ トラフィックはカウントしません。
- ファブリックに入る前、またはリーフ ポートに転送される前にドロップされたパケット、アトミック カウンタによって無視されます。
- ハイパーバイザで切り替えられるパケット（同じポート グループとホスト）はカウントされません。
- 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 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 アドレスと接続先 IP アドレスを構成することはできません。
- 送信元または宛先として fvCEp を使用して設定されたアトミック カウンタ ポリシーでは、fvCEp 管理対象オブジェクトに存在する MAC アドレスおよび IP アドレスからのトラフィックと、両者へのトラフィックだけがカウントされます。fvCEp の管理対象オブジェクトで IP アドレス フィールドが空の場合、その MAC アドレスとの間で送受信されるすべてのトラフィックが IP アドレスに関係なくカウントされます。Cisco APIC が fvCEp について複数の IP アドレスを学習している場合、前述のように、fvCEp 管理対象オブジェクト自体にある 1 つの IP アドレスのみがカウントされます。特定の IP アドレスとの送受信に関連したアトミック カウンタ ポリシーを設定するには、送信元または宛先として fvIp 管理対象オブジェクトを使用します。
- fvCEp の背後に fvIp が存在する場合は、fvCEp ベースのポリシーではなく fvIP ベースのポリシーを追加する必要があります。
- 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。
- Cisco APIC のトラフィック マップ モードが「trail」に設定されていて、Cisco APIC が F1545 障害を生成した場合、この障害をクリアできる唯一の方法は、トラフィック マップ モードを「path」に設定することです。トラフィック マップ モードを変更するには、**[操作（Operations）]** > **[可視化（Visualization）]** に移動し、**[設定（Settings）]** をクリックし、[モード（Mode）] の**パス**を選択して、**[送信（Submit）]** をクリックします。これにより、入力と出力の両方でポートごとのトンネル統計が得られます。

  トレール モードでは、トンネル論理インターフェイスの最大スケール インデックスに到達する可能性が高くなります。このモードは、より多くのソフトウェアおよびハードウェア リソースを消費します。論理インターフェイスは、ハードウェア内のトンネルに関連付けられている ID です。

  トレイル モードを指定したトンネル エンドポイント（TEP）間に単一のトンネルがある場合は、より多くのハードウェア リソースも消費されます。たとえば、6 つのファブリック ポートと 1 つのトンネルがある場合、ハードウェアは、トンネルの数にファブリック ポートの数を掛けた数に等しいエントリ数を消費します。

  ソフトウェアの場合、割り当てられた論理インターフェイスの数が 2048 を超えると、ハードウェアにエントリを作成できません。その結果、統計情報を取得できません。アトミック カウンタの場合、この問題は減少または超過として表示されることがあります。

  パス モードには、TEP のエントリだけがあります。vPC の場合、2 つのエントリがインストールされます。したがって、上限に達する可能性は低くなります。

アトミック カウンタの構成

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、必要なテナントをクリックします。

ステップ 3 **Navigation** ウィンドウで、テナントを展開し、**Policies** を展開し、それから **Troubleshoot** を展開します。

ステップ 4 **Troubleshoot** の下で、**Atomic Counter Policy** を展開し、トラフィック トポロジを選択します。

エンドポイントの組み合わせ、エンドポイント グループ、外部インターフェイスおよび IP アドレス間のトラフィックを測定できます。

ステップ 5 必要なトポロジを右クリックして、**Add** *topology* **Policy** を選択し、**Add Policy** ダイアログボックスを開きます。

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

a) [Name] フィールドにポリシーの名前を入力します。

b) トラフィックの送信元の識別情報を選択するか、入力します。

必要な識別情報のソース（エンドポイント、エンドポイントのグループ、外部インターフェイス、または IP アドレス）によって異なります。

c) トラフィックの宛先の識別情報を選択するか、入力します。

d) （任意）（任意）[Filters] テーブルで + アイコンをクリックし、カウントするトラフィックのフィルタリングを指定します。

表示される [Create Atomic Counter Filter] ダイアログボックスで、IP プロトコル番号（たとえば TCP=6）によるフィルタリング、および送信元と宛先の IP ポート番号によるフィルタリングを指定できます。

e) [Submit] をクリックし、アトミック カウンタ ポリシーを保存します。

ステップ 7 [Navigation] ペインで、選択したトポロジの下の新しいアトミック カウンタ ポリシーを選択します。

ポリシー設定が [Work] ペインに表示されます。

ステップ 8 [Work] ペインで [Operational] タブをクリックし、[Traffic] サブタブをクリックして、アトミック カウンタの統計情報を表示します。

SNMP の使用

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。

Cisco ACI での SNMP アクセスのサポート

（注） Cisco Application Centric Infrastructure（ACI）でサポートされる MIB の完全なリストについては、 https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html を参照してください。

Cisco ACI での SNMP サポートは次のとおりです。

- SNMP 読み取りクエリー（Get、Next、Bulk、Walk）は、リーフおよびスパイン スイッチと Cisco Application Policy Infrastructure Controller（APIC）によってサポートされます。
- SNMP 書き込みコマンド（Set）は、リーフおよびスパイン スイッチまたは Cisco APIC によってサポートされません。
- SNMP トラップ（v1、v2c、および v3）は、リーフおよびスパイン スイッチと Cisco APIC によってサポートされます。

（注） Cisco ACI は最大 10 個のトラップ レシーバをサポートします。

- SNMPv3 は、リーフおよびスパイン スイッチと Cisco APIC によってサポートされます。
- Cisco APIC IPv6 アドレスを使用した SNMP はサポートされていません。

表 *3 : Cisco APIC* リリースでの *SNMP* サポートの変更

リリース	説明
6.1(2)	APIC の起動中に SNMP デーモンが起動しません。これは、ユーザーが SNMP ポリシーをポッド プロファイル ポリシーにアタッチし、adminSt を「有効」に構成すると開始されます。同様に、ユーザーが adminSt を「無効」に構成するか、ポッド プロファイル ポリシーから SNMP ポリシーを削除すると停止します。この動作は、SNMP トラップデーモンにも適用されます。したがって、SNMP トラップ集約機能は、SNMP ポリシー管理状態に依存します。SNMP トラップ集約を機能させるには、すべての APIC をトラップ転送先として追加します。
1.2(2)	SNMP トラップの宛先として IPv6 サポートを追加。
1.2(1)	Cisco APIC コントローラの SNMP サポートを追加。以前のリリースでは、リーフおよびスパイン スイッチについてのみ SNMP がサポートされています。

SNMP トラップ集約機能

SNMP トラップ集約機能を使用すると、ファブリック ノードからの SNMP トラップを Cisco Application Policy Infrastructure Controller（APIC）によって集約でき、ファブリック ノードから受信した SNMP トラップを APIC によって外部宛先に転送できます。

トラップが個々のファブリック ノードからではなく APIC から送信されることが予想される場合は、この機能を使用します。この機能を有効にすると、APIC は SNMP プロキシとして機能します。

考えられる障害を処理するために、クラスタ内のすべての APIC を SNMP トラップ アグリゲータとして設定することを強く推奨します。SNMP ポリシーでは、複数のトラップの宛先を設定できます。トラップの集約と転送を設定するには、次の手順を実行します。

1. スイッチからトラップを受信するように各 APIC コントローラを設定します。次の設定を使用した GUI による SNMP トラップ通知先の設定 （99 ページ） の手順に従います。
   - **[ホスト名/IP（Host Name / IP）]** フィールドで、APIC の IPv4 または IPv6 アドレスを指定します。
   - **[管理 EPG（Management EPG）]** リストから、アウトオブバンドまたはインバンド管理 EPG を選択します。

   クラスタ内の各 APIC をトラップの宛先として設定するには、この手順を繰り返します。
2. 集約トラップを外部サーバに転送するように APIC を設定します。次の設定を使用した GUI による SNMP ポリシーの設定 （97 ページ） の手順に従います。
   - **[トラップ転送サーバ（Trap Forward Servers）]** テーブルで、外部サーバの **IP アドレス**を追加します。

トラップの集約と転送では、転送されるトラップの送信元 IP アドレスは、実際の送信元ノードではなく、アグリゲータのアドレス（この場合は APIC）になります。実際の送信元を特定するには、OID で検索する必要があります。次の例では、アドレス 10.202.0.1 が APIC IP アドレスで、アドレス 10.202.0.201 が元の送信元リーフ スイッチの IP アドレスです。

```
08:53:10.372378 IP
(tos 0x0, ttl 60, id 59067, offset 0, flags [DF], proto UDP (17), length 300)
    10.202.0.1.45419 > 192.168.254.200.162: [udp sum ok]
    { SNMPv2c C="SNMP-ACI" { V2Trap(252) R=609795065
    .1.3.6.1.2.1.1.3.0=25847714 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.9.9.276.0.1
    .1.3.6.1.2.1.2.2.1.1.436207616=436207616 .1.3.6.1.2.1.2.2.1.7.436207616=2
    .1.3.6.1.2.1.2.2.1.8.436207616=2 .1.3.6.1.2.1.31.1.1.1.1.436207616="eth1/1"
    .1.3.6.1.2.1.2.2.1.3.436207616=6 .1.3.6.1.2.1.2.2.1.2.436207616="eth1/1"
    .1.3.6.1.2.1.31.1.1.1.18.436207616=""
    .1.3.6.1.4.1.9.10.22.1.4.1.1.6="10.202.0.201" } }
```

SNMP トラップ集約機能は、SNMPV2 トラップ集約および転送をサポートする Cisco APIC リリース 3.1(1) で導入されました。Cisco APIC リリース 4.2(6) および 5.1(1)以降では、SNMPv3 トラップの集約および転送がサポートされています。

（注） APIC がデコミッションされた場合、ユーザは廃止された APIC をクリーン再起動する必要があります。SNMP トラップ集約機能はデコミッションされた APIC でアクティブであるため、デコミッションされた APIC がクリーン再起動されない場合、ユーザはトラップ宛先で重複トラップを受信する可能性があります。

SNMP の設定

GUI による SNMP ポリシーの設定

この手順では、Cisco ACI モード スイッチの SNMP ポリシーを構成し、有効にします。

始める前に

SNMP 通信を有効にするには、以下の設定が必要です。

- アウトオブバンド コントラクトを設定して SNMP トラフィックを許可します。SNMP トラフィックは、通常、SNMP 要求に UDP ポート 161 を使用します。
- 「mgmt」テナントで Cisco APIC アウトオブバンド IP アドレスを構成します。Cisco APIC セットアップ中にアウトオブバンドアドレスを構成した場合は、「mgmt」テナントのアドレスを再度設定しないでください。

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Fabric Policies] をクリックします。

ステップ 3 **[Navigation]** ペインで、**[Pod Policies]** を展開します。

ステップ 4 **[Pod Policies]** の下で **[Policies]** を展開します。

ステップ 5 **[SNMP]** を右クリックし、**[Create SNMP Policy]** を選択します。

新しい SNMP ポリシーを作成する代わりに、次の手順で示されるものと同じ方法で **[default]** ポリシー フィールドを編集できます。

ステップ 6 SNMP ポリシーのダイアログボックスで、次の操作を実行します。

a) **[Name]** フィールドに、SNMP ポリシーの名前を入力します。

b) **[Admin State]** フィールドで、**[Enabled]** を選択します。

c) （任意） **[SNMP v3 Users]** テーブルで **[+]** アイコンをクリックし、**名前**を入力して、ユーザの認証データを入力し、**[Update]** をクリックします。

この手順は SNMPv3 アクセスが必要な場合のみ実行します。

d) **[コミュニティ ポリシー（Community Policies）]** テーブルで **[+]** アイコンをクリックし、**[名前（Name）]** を入力して、**[更新（Update）]** をクリックします。

コミュニティポリシー名の最大長は32文字です。名前には、アンダースコア（_）、ハイフン（-）、またはピリオド（。）の文字、数字、および特殊文字のみを使用できます。名前に @ 記号を含めることはできません。

e) **[Trap Forward Servers]** テーブルで、**[+]**アイコンをクリックし、外部サーバの**[IP Address]** を入力し、**[Update]**をクリックします。

ステップ 7 必須: 許可された SNMP 管理ステーションを設定するには、SNMP ポリシーのダイアログボックスで、次の操作を実行します。

a) **[Client Group Policies]** テーブルで **[+]** アイコンをクリックし、**[Create SNMP Client Group Profile]** ダイアログボックスを開きます。

b) **[Name]** フィールドに、SNMP クライアント グループのプロファイル名を入力します。

c) **[Associated Management EPG]** ドロップダウン リストから管理 EPG を選択します。

d) **[Client Entries]** テーブルで **[+]** アイコンをクリックします。

e) **[Name]** フィールドにクライアントの名前を入力し、**[Address]** のフィールドにクライアントの IP アドレスを入力して、**[Update]** をクリックします。

（注）
SNMP 管理ステーションが SNMPv3 を使用して APIC と接続する場合、APIC は SNMP クライアント グループのプロファイルに指定されたクライアント IP アドレスを強制しません。SNMPv3 の場合、管理ステーションが **[Client Entries]** リストに含まれている必要がありますが、SNMPv3 クレデンシャルのみでアクセス可能なため、IP アドレスが一致している必要はありません。

ステップ 8 [OK] をクリックします。

ステップ 9 **[送信（Submit）]** をクリックします。

ステップ 10 **[Pod Policies]** の下で **[Policy Groups]** を展開して、ポリシー グループを選択するか、または **[Policy Groups]** を右クリックし、**[Create POD Policy Group]** を選択します。

新しいポッド ポリシー グループを作成することも、既存のグループを使用することもできます。ポッド ポリシー グループには、SNMP ポリシーに加えて他のポッド ポリシーを含めることができます。

ステップ 11 ポッド ポリシー グループのダイアログボックスで、次の操作を実行します。

a) **[Name]** フィールドに、ポッド ポリシー グループの名前を入力します。

b) **[SNMP Policy]** ドロップダウン リストから、設定した SNMP ポリシーを選択して、**[Submit]** をクリックします。

ステップ 12 **[Pod Policies]** の下で **[Profiles]** を展開し、**[default]** をクリックします。

ステップ 13 **[Work]** ペインで、**[Fabric Policy Group]** ドロップダウン リストから、作成したポッド ポリシー グループを選択します。

ステップ 14 [送信（Submit）] をクリックします。

ステップ 15 **[OK]** をクリックします。

GUI による SNMP トラップ通知先の設定

この手順では、SNMP トラップ通知を受信する SNMP マネージャのホスト情報を設定します。

（注） ACI は最大 10 個のトラップ レシーバをサポートします。10 個より多く設定すると、一部では通知が受信されません。

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[External Data Collectors] をクリックします。

ステップ 3 **[Navigation]** ペインで、**[Monitoring Destinations]** を展開します。

ステップ 4 **[SNMP]** を右クリックし、**[Create SNMP Monitoring Destination Group]** を選択します。

ステップ 5 **[Create SNMP Monitoring Destination Group]** ダイアログボックスで、次の操作を実行します。

a) **[Name]** フィールドに、SNMP 通知先の名前を入力し、**[Next]** をクリックします。

b) **[Create Destinations]** テーブルで **[+]** アイコンをクリックし、**[Create SNMP Trap Destination]** ダイアログボックスを開きます。

c) **[ホスト名/IP（Host Name/IP）]** フィールドに、IPv4 または IPv6 アドレスまたは宛先ホストの完全修飾ドメイン名を入力します。

d) 通知先の**ポート**番号と SNMP **バージョン**を選択します。

e) SNMP v1 または v2c 通知先の場合、**[Security Name]** として設定したコミュニティ名の 1 つを入力し、**[v3 Security Level]** として **[noauth]** を選択します。

SNMP v1 または v2c セキュリティ名の最大長は 32 文字です。名前には、アンダースコア（_）、ハイフン（-）、またはピリオド（。）の文字、数字、および特殊文字のみを使用できます。SNMP v2c の場合、@ 記号も使用できます。

f) SNMP v3 通知先の場合、**[Security Name]** として設定したユーザ名の 1 つを入力し、必要な **[v3 Security Level]** を選択します。

SNMP v3 セキュリティ名の最大長は 32 文字です。名前は大文字または小文字で始まる必要があり、文字、数字、およびアンダースコア（_）、ハイフン（-）、ピリオド（。）、または@記号の特殊文字のみを使用できます。

g) **[Management EPG]** ドロップダウン リストから管理 EPG を選択します。

h) [**OK**] をクリックします。

i) **[完了（Finish）]** をクリックします。

GUI による SNMP トラップ ソースの設定

この手順では、ファブリック内のソース オブジェクトを選択して有効にし、SNMP トラップ通知を生成します。

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Fabric Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Policies] を展開します。

共通ポリシー、**デフォルト** ポリシーで SNMP ソースを作成することも、または新しいモニタリング ポリシーを作成することもできます。

ステップ 4 必要なモニタリング ポリシーを展開し、[Callhome/SNMP/Syslog] を選択します。

[Common Policy] を選択する場合は、[Common Policy] を右クリックして、[Create SNMP Source] を選択し、そのダイアログボックスで次の手順に従ってください。

ステップ 5 [Work] ペインで、[Monitoring Object] ドロップダウン リストから [ALL] を選択します。

ステップ 6 [Source Type] ドロップダウン リストから、[SNMP] を選択します。

ステップ 7 テーブルで + アイコンをクリックし、[Create SNMP Source] ダイアログボックスを開きます。

ステップ 8 [Create SNMP Source] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、SNMP ポリシーの名前を入力します。

b) [Dest Group] ドロップダウン リストから、通知を送信する既存の宛先を選択するか、または [Create SNMP Monitoring Destination Group] を選択して、新しい宛先を作成します。

SNMP の通知先グループを作成する手順は、別項で説明します。

c) [Submit] をクリックします。

SNMP を使用したシステムのモニタリング

個々のホスト（APIC またはその他のホスト）をリモートでモニタし、特定のノードの状態を確認できます。

SNMP を使用してシステムの CPU とメモリの使用状況をチェックし、CPU のスパイクが発生しているかどうかを確認できます。SNMP（ネットワーク管理システム）は、SNMP クライアントを使用して APIC の情報にアクセスし、情報を取得します。

リモートでシステムにアクセスして、情報がネットワーク管理システムのコンテキストに属するものかどうかを確認し、CPU またはメモリの使用量が多すぎないか、またはシステムやパフォーマンスの問題が発生しているかどうかを調べることができます。問題の原因がわかると、システムの正常性をチェックし、メモリまたは CPU の使用量が多すぎないかどうかを確認できます。

詳細については、「*Cisco ACI MIB Quick Reference Manual*」を参照してください。

SPAN の使用

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。

リリース 4.1(1i) 以降、次の機能がサポートされるようになりました。

- 送信元とポートチャネルが同じスイッチ上でローカルである限り、宛先として静的ポートチャネルを使用した、ローカル SPAN に対するサポート。

（注） APIC リリース 4.1(1i) 以降を実行していて、宛先として静的ポート チャネルを設定した後、4.1(1i) より前のリリースにダウングレードすると、これが原因で SPAN セッションが管理者無効状態になります。この機能は、リリース 4.1.(1i) より前には利用できませんでした。機能への影響はありません。

- レイヤ 3 インターフェイス フィルタリングを使用して送信元 SPAN を設定するときに、レイヤ 3 インターフェイスの IP プレフィックスを含める必要がなくなりました。
- 1 つ以上のフィルタ エントリのグループであるフィルタ グループ設定のサポート。フィルタ グループを使用すれば、受信したパケットを SPAN を使用して分析する必要があるかどうかを判断するために使用される一致基準が指定できます。
- ASIC の入力での転送が原因でドロップされたパケットをキャプチャし、事前設定された SPAN 宛先に送信する SPAN-on-drop 機能。SPAN-on-drop 設定には、アクセス ポートを SPAN 送信元として使用するアクセス ドロップ、ファブリック ポートを SPAN 送信元として使用するファブリック ドロップ、およびノード上のすべてのポートを SPAN 送信元として使用するグローバル ドロップの 3 種類があります。SPAN-on-drop は、通常の SPAN を使用し (CLI、GUI、および REST API 経由) とトラブルシューティング SPAN を使用して (CLI および REST API のみを経由) 設定されます。この機能の設定の詳細については、*GUI* を使用した *SPAN* の設定、*NX-OS* スタイル *CLI* を使用した *SPAN* の設定、および *REST API* を使用した *SPAN* の設定を参照してください。

マルチノード SPAN

APIC の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 グループのすべてのメンバーと彼らが接続する場所を追跡するために、適切な範囲にポリシーのスパンを広げることが可能です。メンバーが移動すると、APIC は新しいリーフにポリシーを自動的にプッシュします。たとえば、エンドポイントが新しいリーフ スイッチに VMotion により移動すると、スパンの設定は自動的に調整されます。

ACI ファブリックは、カプセル化リモート SPAN（ERSPAN）形式の次の 2 つの拡張をサポートします。

- アクセスまたはテナント SPAN：VLAN をフィルタとして使用するかどうかにかかわらず、リーフ スイッチのフロント パネル ポートに対して実行されます。リーフ スイッチの Broadcom Trident 2 ASIC は、ERSPAN タイプ 1 形式とはわずかに異なるバージョンをサポートします。上記で参照したドキュメントで定義されている ERSPAN タイプ 1 フォーマットとは、GRE ヘッダーが 4 バイトのみであり、シーケンス フィールドがないという点で異なっています。GREヘッダーは常に次のようにエンコードされます–0x000088be。0x88be は ERSPAN タイプ 2 を示していますが、フィールドの残りの 2 バイトにより、これは 4 バイトの GRE ヘッダーを持つ ERSPAN タイプ 1 パケットとして識別されます。
- ファブリック SPAN：リーフ スイッチの Northstar ASIC により、またはスパイン スイッチの Alpine ASIC により実行されます。これらの ASIC は ERSPAN タイプ 2 および 3 フォー

マットをサポートしていますが、ACI ファブリックは現在、ファブリック SPAN の ERSPAN タイプ 2 のみをサポートしています。これについては、上記のベースライン ドキュメントに記載されています。

ERSPAN ヘッダーの説明については、次の URL にある IETF インターネット ドラフトを参照してください。https://tools.ietf.org/html/draft-foschiano-erspan-00

SPAN の注意事項と制約事項

（注） 多くのガイドラインと制約事項は、スイッチが第 1 世代スイッチか第 2 世代スイッチかによって異なります。スイッチの生成は次のように定義されます。

- 第 1 世代スイッチは、スイッチ名の末尾に「EX」、「FX」、「FX2」などのサフィックスがないことで識別されます（N9K-9312TX など）。
- 第 2 世代スイッチは、スイッチ名の末尾に「EX」、「FX」、「FX2」などのサフィックスが付いています。

- サポートされる SPAN のタイプはさまざまです。
  - 第 1 世代のスイッチの場合、テナントおよびアクセス SPAN は、カプセル化された SPAN（ERSPAN）タイプ I を使用します（Cisco Application Policy Infrastructure Controller（APIC）GUI のバージョン 1 オプション）。
  - 第 2 世代スイッチの場合、テナントおよびアクセス SPAN は、カプセル化された SPAN（ERSPAN）タイプ II（Cisco APIC GUI のバージョン 2 オプション）を使用します。
  - ファブリック SPAN は ERSPAN タイプ II を使用します。
- リリース 5.2(3) 以降、ERSPAN は IPv6 接続先をサポートしています。
- 6.0(3) リリースは、次の SPAN 制限がある Cisco N9K-C9808 スイッチをサポートします。
  - 出力（トランジット（Tx））SPAN はサポートされていません。
  - ドロップ時の SPAN はサポートされていません。
  - 複数のセッションで同じ SPAN 送信元を使用することはできません。
  - SPAN は、最大 343 バイトの MTU をサポートします。
- uSeg EPG または ESG は、SPAN 送信元 EPG として使用できません。これは、SPAN 送信元フィルタが VLAN ID に基づいているためです。したがって、エンドポイントが uSeg EPG または ESG に分類されている場合でも、その VLAN が SPAN 送信元 EPG の VLAN である場合、エンドポイントからのトラフィックはミラーリングされます。
- ERSPAN セッションを構成するときに、SPAN ソースに GOLF VRF インスタンス内のスパイン スイッチからの宛先とインターフェイスが含まれている場合、L3Out プレフィックス

が間違った BGP ネクストホップで GOLF ルータに送信され、GOLF からその L3Out への接続が切断されます。

- SPAN 送信元として l3extLIfP のレイヤ 3 サブインターフェイスを指定することはできません。外部ソースからのトラフィックをモニタリングするためにはポート全体を使用します。
- FEX インターフェイスのローカル SPAN では、FEX インターフェイスは SPAN 送信元としてのみ使用でき、SPAN 宛先としては使用できません。
  - 第 1 世代スイッチでは、レイヤ 3 スイッチド トラフィックに対して Tx SPAN は機能しません。
  - 第 2 世代のスイッチでは、トラフィックがレイヤ 2 またはレイヤ 3 のどちらでスイッチングされているかにかかわらず、Tx SPAN は機能しません。

Rx SPAN に制限はありません。

FEX ファブリック ポートチャネル（NIF）の SPAN の場合、メンバー インターフェイスは第 1 世代リーフ スイッチの SPAN 送信元インターフェイスとしてサポートされます。

（注） 第 2 世代スイッチで FEX ファブリック ポートチャネル（NIF）メンバー インターフェイスを SPAN 送信元インターフェイスとして設定することもできますが、これは Cisco APIC リリース 4.1 より前のリリースではサポートされていません。

ERSPAN ヘッダーについては、IETF の Internet Draft（https://tools.ietf.org/html/draft-foschiano-erspan-00）を参照してください。

- ERSPAN 宛先 IP アドレスは、エンドポイントとしてファブリックで学習する必要があります。

  APIC リリース 6.1(2) 以降、ERSPAN 宛先 IP アドレスは、L3Out（ERSPAN over L3Out）から学習され、到達可能なアドレスにすることもできます。
- SPAN は IPv6 トラフィックをサポートします。
- ポート チャネルまたは vPC の個別ポート メンバーは送信元として設定されます。ポート チャネル、vPC、または vPC コンポーネントを SPAN セッションの送信元として使用します。
- 宛先 EPG が削除されるか使用できない場合、ERSPAN 送信元グループで障害は発生しません。
- SPAN フィルタは、第 2 世代のリーフ スイッチでのみサポートされます。

  アクセス SPAN 送信元は、特定の時点で次のいずれかのフィルタのみをサポートします。
  - EPG
  - 外部ルーティング（L3Out）

- L3Out フィルタを使用してアクセス SPAN 送信元を展開する場合は、L3Out が一致するインターフェイスにも展開されていることを確認します。
  - L3Out がポートに展開されている場合、SPAN 送信元は同じポートに展開する必要があります。
  - L3Out が PC に展開されている場合、SPAN 送信元は同じ PC に展開する必要があります。
  - L3Out が vPC に展開されている場合、SPAN 送信元は同じ vPC に展開する必要があります。
- L3Out ルーテッド インターフェイスおよびルーテッド サブインターフェイスはポートまたは PC に導入できますが、L3Out SVI はポート、PC、または vPC に導入できます。L3Out フィルタを使用する SPAN 送信元は、それに応じて展開する必要があります。
- L3Out フィルタは、ファブリック SPAN またはテナント SPAN セッションではサポートされません。
- EPG ブリッジ ドメインの [L3 設定（L3 Configuration）] タブで正しい L3Out を選択する必要があります。そうしないと、基本的な L3Out のパケット フローが機能しません。
- カプセル化値は、ルーテッドサブインターフェイスおよびSVIには必須ですが、ルーテッドインターフェイスには適用されません。L3Outサブインターフェイスまたは SVI カプセル化値は、EPG カプセル化値とは異なる必要があります。

  SPAN セッション内で EPG フィルタが有効になっている場合、中継、つまり tx 方向のインターフェイスから送信される ARP パケットはスパンされません。
- 次の場合、SPAN フィルタはサポートされません。
  - ファブリック ポート
  - ファブリックおよびテナント SPAN セッション
  - スパイン スイッチ
- 公式にサポートされているよりも多くの L4 ポート範囲を追加しようとしても、L4 ポート範囲フィルタ エントリは追加されません。
- SPAN 送信元グループ レベルまたは個々の SPAN 送信元レベルで、サポートされているフィルタ エントリより多くのエントリを関連付けようとすると、SPAN セッションは起動しません。
- 公式にサポートされているよりも多くのフィルタ エントリを追加または削除すると、削除されたフィルタ エントリは TCAM に残ります。
- アクティブな SPAN セッションの最大数や、SPAN フィルタ制限など、SPAN 関連の制限については、『*Verified Scalability Guide for Cisco ACI*』ドキュメントを参照してください。
- SPAN-on-drop 機能では、次の注意事項と制限事項が適用されます。
  - SPAN-on-drop 機能は、第 2 世代リーフ スイッチでサポートされます。

- SPAN-on-drop 機能は、LUX ブロック内の転送ドロップがあるパケットのみをキャプチャします。これは、入力での転送ドロップ パケットをキャプチャします。SPAN-on-drop 機能は、BMX（バッファ）ドロップおよび RWX（出力）ドロップをキャプチャできません。
- トラブルシューティング CLI を使用して SPAN-on-drop と Cisco APICを有効にして宛先として SPAN セッションを作成する場合、100 MBの データがキャプチャされるとセッションは無効になります。
- モジュラ シャーシでは、SPAN-on-drop 機能はライン カードでドロップされたパケットに対してのみ機能します。ファブリック カードでドロップされたパケットはスパンされません。
- SPAN-on-drop ACL と他の SPAN ACL はマージされません。SPAN-on-drop セッションが ACL ベースの SPAN とともにインターフェイスで設定されている場合、そのインターフェイスでドロップされたパケットは SPAN-on-drop セッションにのみ送信されます。
- SPAN on drop と SPAN ACL を同じセッションで設定することはできません。
- アクセスまたはファブリック ポート ドロップ セッションとグローバル ドロップ セッションが設定されている場合、アクセスまたはファブリック ポート ドロップ セッションがグローバル ドロップ セッションよりも優先されます。
- TCAM でサポートされるフィルタ エントリの数=（M * S1 * 1 + N * S2 * 2）+（S3 * 2）。これは、rx SPAN または tx SPAN に個別に適用されます。現在この式に従うと、tx または rx SPAN でサポートされる最大フィルタ エントリは各方向で 480 です（また、フィルタ グループ アソシエーション（S3 = 0 を意味する）なしで、16 個のポート範囲を含む他の送信元が設定されていない場合））。フィルタ エントリの数が最大許容数を超えると、障害が発生します。フィルタエントリでレイヤ4ポート範囲を指定できることに注意してください。ただし、16個のレイヤ4ポートが単一のフィルタ エントリとしてハードウェアにプログラムされます。

（注）

- M = IPv4 フィルタの数
- S1 = IPv4 フィルタを使用した送信元の数
- N = IPv6 フィルタの数
- S2 = IPv6 フィルタを使用した送信元の数
- S3 =フィルタ グループが関連付けられていない送信元の数

- PC または vPC の LACP ポリシーで MAC ピニングを設定すると、PC メンバー ポートは LACP 個別ポートモードになり、PC は動作しません。したがって、このような PC での SPAN 送信元設定は失敗し、「No operating src / dst」障害が生成されます。MAC ピニング モードが設定されている場合、SPAN は個々のポートでのみ設定できます。

- Cisco Application Centric Infrastructure（ACI）リーフ スイッチで受信されたパケットは、スパンインターフェイスが入力インターフェイスと出力インターフェイスの両方で設定されている場合でも、一度だけスパンされます。
- ルーテッド外部 SPAN 送信元フィルタを使用すると、Tx 方向のユニキャストのみが表示されます。Rx 方向では、ユニキャスト、ブロードキャスト、およびマルチキャストを確認できます。
- L3Out フィルタは、送信マルチキャスト SPAN ではサポートされません。L3Out は、入力 ACL フィルタでは sclass / dclass の組み合わせとして表されるため、ユニキャスト トラフィックのみを照合できます。送信マルチキャスト トラフィックは、ポートおよびポート チャネルでのみスパンできます。
- ポート チャネル インターフェイスを SPAN 宛先として使用できるのは、-EX 以降のスイッチだけです。
- SPAN フィルタ（5 タプル フィルタ）が適用されている場合、同じ送信元インターフェイスで複数の SPAN セッションを設定することはできません。

  リーフ スイッチのローカル SPAN 宛先ポートは、着信トラフィックを予期しません。レイヤ 2 インターフェイス ポリシーを設定し、**VLAN 範囲**プロパティを**グローバル範囲**ではなく**ポート ローカル範囲**に設定することで、スイッチが着信 SPAN 宛先ポート トラフィックをドロップするようにできます。このポリシーを SPAN 宛先ポートに適用します。レイヤ2インターフェイスポリシーを設定するには、GUI で次の場所に移動します。**[ファブリック（Fabric）]**>**[アクセス ポリシー（Access Policies）]**>**[ポリシー（Policies）]**>**[インターフェイス（Interface）]** > **[L2 インターフェイス（L2 Interface）]**

  特定のパケットに SPAN を設定すると、SPAN はそのパケットに対して 1 回だけサポートされます。最初の SSN の Rx の SPAN によってトラフィックが選択された場合、2 番目の SSN の Tx の SPAN によってトラフィックが再度選択されることはありません。したがって、SPAN セッションの入力ポートと出力ポートが単一のスイッチ上にある場合、SPAN セッションのキャプチャは一方向のみです。SPAN セッションは双方向トラフィックを表示できません。
- フィルタ グループに設定された SPAN ACL フィルタは、アクセス インターフェイスから出力されるブロードキャスト、不明ユニキャスト、およびマルチキャスト（BUM）トラフィックをフィルタリングしません。出力方向の SPAN ACL は、ユニキャスト IPv4 または IPv6 トラフィックに対してのみ機能します。

  SPAN 宛先をローカル ポートとして設定する場合、EPG はそのインターフェイスに展開できません。

  リーフ スイッチでは、VRF フィルタを持つ SPAN 送信元は、VRF インスタンスの下のすべての通常のブリッジ ドメインとすべてのレイヤ 3 SVI にマッチします。

  スパイン スイッチでは、VRF を持つ SPAN 送信元は、設定された VRF VNID トラフィックのみにマッチします。また、ブリッジ ドメイン フィルタは、ブリッジ ドメイン VNID トラフィックのみにマッチします。

- 独自の SPAN 拡張フィルタ エントリを作成する場合、拡張フィルタ エントリの管理対象オブジェクトを識別するために、**__UI__AUTO__CONFIG__DEFAULT__EXTENDED__MO** をオブジェクト名として使用することはできません。
- 同じ速度の SPAN 接続先インターフェイスを使用します。SPAN セッションによってモニターされるトラフィックは、接続先ポートがオーバーサブスクライブされていないが、他の SPAN 接続先ポートの 1 つがオーバーサブスクライブされている場合でも、SPAN バッファのドロップが原因でトラフィック損失が発生する可能性があります。SPAN トラフィック レートは、接続先インターフェイスの速度が異なる場合、およびそれらの 1 つがオーバーサブスクライブされている場合、最も遅い SPAN 接続先インターフェイス速度に制限されます。
- 構成されているどの送信元インターフェイスよりも高い SPAN 接続先インターフェイス速度を使用し、マイクロバーストに十分な余裕がある速度を選択します。クラウドスケール ASIC は、SPAN クラスのマイクロバースト モニタリング オプションを提供しません。
- SPAN 宛先グループ機能では、次の注意事項と制限事項が適用されます。
  - [ERSPAN over L3Out]：宛先が Infra L3Out の背後にある場合、サポートされません。
  - [ERSPAN over L3Out]：スパン送信元がスパイン ノードのファブリック ポートである場合、サポートされません。
  - インフラ SR-MPLS L3out を介した ERSPAN はサポートされていません。
  - 宛先がリモート リーフ アップリンク ファブリック ポートのユーザー テナント L3out を介して到達可能な場合、リモート リーフの L3out を介した ERSPAN はサポートされません。

GUI を使用した SPAN の設定

Cisco APIC GUI を使用したテナント SPAN セッションの設定

SPAN は、スイッチまたはテナントで設定できます。このセクションでは、Cisco APIC GUI を使用して、複製された送信元パケットをリモート トラフィック アナライザに転送するようにテナントの SPAN ポリシーを設定する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。フィールドを理解し、有効な値を決定するには、ダイアログ ボックスの右上隅にあるヘルプアイコン（**?**）をクリックしてヘルプ ファイルを表示します。

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでテナントを展開し、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > を展開して、**[SPAN]** を展開します。

[SPAN] に表示される 2 つのノード：**[SPAN 宛先グループ（SPAN Destination Groups）]** と **[SPAN 送信元グループ（SPAN Source Groups）]**。

ステップ 4 **[ナビゲーション（Navigation）]**の下で **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Group）]** を選択します。
[Create SPAN Source Group] ダイアログが表示されます。

ステップ 5 **[SPAN送信元グループの作成（Create SPAN Source Group）]**ダイアログ ボックスの必須フィールドに適切な値を入力します。

ステップ 6 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成]** ダイアログ ボックスを開きます。

ステップ 7 **[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 8 SPAN送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 9 **[リモート場所の作成（Create Remote Location）]**ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 送信先のトラフィック アナライザを使用して、SPAN 送信元 EPGからのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

APIC GUI を使用した SPAN フィルタ グループの設定

手順

ステップ 1 メニュー バーで **[ファブリック（Fabric）]** をクリックし、サブメニュー バーで **[アクセス ポリシー（ Access Policies）]**をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** を展開し、**[SPAN]** を展開します

ステップ 3 **[SPAN]** の下で **[SPAN フィルタ グループ（SPAN Filter Groups）]** を右クリックし、**[SPAN フィルタ グループの作成（Create SPAN Filter Group）]** を選択します。
[フィルタ グループの作成（Create Filter Group）] ダイアログボックスが表示されます。

ステップ 4 SPAN フィルタ グループの名前を入力します。**[フィルタ エントリ（Filter Entries）]** テーブルで、**[+]** をクリックし、次のフィールドに値を入力します。

- **[送信元 IP プレフィックス（Source IP Prefix）]**：*IP* アドレス/マスクの形式で送信元 IP アドレスを入力します。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされていま

す。**0.0.0.0** の値は、このフィールドで**任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。

- **[最初の送信元ポート（First Source Port）]** 最初の送信元レイヤー 4 ポートを入力します。このフィールドは、**[最後の送信元ポート（Last Source Port）]** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[最後の送信元ポート（Last Source Port）]** 最後の送信元レイヤー 4 ポートを入力します。このフィールドは、**[最初の送信元ポート（First Source Port）]** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[宛先 IP プレフィックス（Destination IP Prefix）]** : *IP* アドレス/マスクの形式で宛先 IP アドレスを入力します。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。**0.0.0.0** の値は、このフィールドで**任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。
- **[最初の宛先ポート（First Destination Port）]** : 最初の宛先レイヤー 4 ポートを入力します。このフィールドは、**[最後の宛先ポート（Last Destination Port）]** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[最後の宛先ポート（Last Destination Port）]** : 最後の宛先レイヤー 4 ポートを入力します。このフィールドは、**[最初の宛先ポート（First Destination Port）]** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[IP プロトコル（IP Protocol）]** : IP プロトコルを入力します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[拡張フィルタ エントリ（Extended Filter Entries）]** テーブルで、**[+]** をクリックし、次のフィールドに値を入力します。
  - **[名前（Name）]:** 拡張フィルタ エントリの名前を入力します。
  - **[最初の DSCP（DSCP From）]** : DSCP 値を入力します。このフィールドは、**[最後の DSCP（DSCP To）]** フィールドとともに、DSCP 値をフィルタリングする範囲を指定します。
  - **[最後ののDSCP（DSCP To）]** : DSCP 値を入力します。このフィールドは、**[最初の DSCP（DSCP From）]** フィールドとともに、DSCP 値をフィルタリングする範囲を指定します。
  - **[最初の Dot1P（Dot1P From）]** : Dot1P 値を入力します。このフィールドは、**[最後の Dot1P（Dot1P To）]** フィールドとともに、Dot1P 値をフィルタリングする範囲を指定します。

- **[最後の Dot1P（Dot1P To）]**：Dot1P 値を入力します。このフィールドは、**[最初の Dot1P（Dot1P From）]** フィールドとともに、Dot1P 値をフィルタリングする範囲を指定します。

  送信元ポートと宛先ポートの範囲、または DSCP と Dot1P の範囲の値を指定できます。送信元ポートと宛先ポートの範囲、および DSCP と Dot1P の範囲の両方を指定すると、障害が表示されます。

  DSCP または Dot1P は、出力方向ではサポートされていません。方向として **[両方（Both）]** を選択した場合、DSCP または Dot1P のいずれかが入力方向のみでサポートされ、出力方向ではサポートされません。

- **[TCP フラグ（TCP Flags）]** ドロップダウンリストで、**TCPフラグ**を選択します。

  TCP フラグを設定できるのは、フィルタ グループのドロップダウン リストで **[未指定（Unspecified）]** または **[TCP]** を **[IP プロトコル（IP Protocol）]** として選択した場合だけです。

- **[パケット タイプ（Packet Type）]**：パケット タイプを選択します。**[ルート/スイッチ（Routed/Switched）]**、**[ルート（Routed）]**、または **[スイッチのみ（Switched Only）]** のいずれかを選択します。

ステップ 5 このフォームの各フィールドに適切な値を入力したら、**[更新（Update）]** をクリックし、**[送信（Submit）]** をクリックします。

APIC GUI を使用したアクセス SPAN ポリシーの設定

この手順では、Cisco APIC GUI を使用してアクセス SPAN ポリシーを設定します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

手順

ステップ 1 メニューバーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Groups）]** を選択します。
[Create SPAN Source Group] ダイアログが表示されます。

ステップ 4 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 5 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスを開いて、必須のフィールドに適切な値を入力します。

ステップ 6 [Create SPAN Source] ダイアログ ボックスで、[Add Source Access Paths] を展開して、ソース パスを指定します。

[送信元をパスに関連付ける（Associate Source to Path）] ダイアログ ボックスが表示されます。

ステップ 7 **[送信元をパスに関連付ける（Associate Source to Path）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 8 送信元とパスの関連付けが完了したら、**[OK]** をクリックします。

[SPAN 送信元の作成（Create SPAN Source）] ダイアログ ボックスに戻ります。

ステップ 9 SPAN 送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 10 SPAN 送信元グループの設定が完了したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

Cisco APIC GUI を使用したファブリック SPAN ポリシーの設定

このセクションでは、Cisco APIC GUI を使用してファブリック SPAN ポリシーを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Groups）]** を選択します。
[Create SPAN Source Group] ダイアログが表示されます。

ステップ 4 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 5 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成]** ダイアログ ボックスを開きます。

ステップ 6 **[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 7 完了したら、[OK] をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 8 **[リモート場所の作成（Create Remote Location）]** ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

APIC GUI を使用した外部アクセス用のレイヤ 3 EPG SPAN セッションの設定

この手順は、Cisco APIC GUI を使用して外部アクセス用のレイヤ 3 EPG SPAN ポリシーを設定する方法を示しています。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Groups）]** を選択します。
[Create SPAN Source Group] ダイアログが表示されます。

ステップ 4 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 5 **[フィルタ グループ（Filter Group）]** フィールドで、フィルタ グループを選択または作成します。

詳細については、APIC GUI を使用した SPAN フィルタ グループの設定 （109 ページ）を参照してください。

ステップ 6 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスを開きいて、以下の操作を実行します。

a) 送信元ポリシーの**[名前（Name）]** を入力します。

b) トラフィック フローの **[方向（Direction）]** オプションを選択します。

c) (オプション) **[ドロップ パケットのスパニング（Span Drop Packets）]** チェックボックスをクリックしてチェックマークを付けます。オンにすると、SPAN-on-drop 機能が有効になります。

d) 外部アクセスの場合は、**[外部にルーティング（Routed Outside）]**（**[タイプ（Type）]** フィールド）をクリックします。

（注）
外部アクセスで **[外部にルーティング（Routed Outside）]** を選択した場合、**[名前（Name）]**、**[アドレス（Address）]**、および **[Encap]** フィールドが表示されて、**[L3 Outside]** を設定できるようになります。

e) **[送信元アクセス パスの追加（Add Source Access Paths）]** を展開して、送信元パスを指定します。

[送信元をパスに関連付ける（Associate Source to Path）] ダイアログ ボックスが表示されます。

f) **[送信元をパスに関連付ける（Associate Source to Path）]** ダイアログ ボックスのフィールドに適切な値を入力します。

g) 送信元とパスの関連付けが完了したら、**[OK]** をクリックします。

[SPAN 送信元の作成（Create SPAN Source）] ダイアログ ボックスに戻ります。

h) SPAN 送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 7 SPAN 送信元グループの設定が完了したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

Cisco APIC GUI を使用したテナント SPAN ポリシーの宛先グループの構成

このセクションでは、Cisco APIC GUI を使用して、テナント SPAN ポリシーの宛先グループを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

SPAN宛先グループと送信元を作成すれば、SPAN宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでテナントを展開し、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > を展開して、**[SPAN]** を展開します。

[SPAN] に表示される 2 つのノード：**[SPAN 宛先グループ（SPAN Destination Groups）]** と **[SPAN 送信元グループ（SPAN Source Groups）]**。

ステップ 4 **[SPAN 宛先グループ（SPAN Destination Groups）]** を右クリックして、**[SPAN 宛先グループの作成（Create SPAN Destination Groups）]** を選択します。**[Create SPAN Destination Group]** ダイアログが表示されます。

a) [Name] フィールドに、SPAN 宛先グループの名前を入力します。

b) オプション。**[説明（Description）]** フィールドに、グループの説明を入力します。

c) **[宛先タイプ（Destination Type）]**で、**[アプリケーション EPG（Application EPG ）]** または **[L3Out EPG（L3Out EPG）]**を選択します。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[アプリケーション EPG（Application EPG）]** を指定する場合は、テナント、アプリケーション プロファイル、および宛先 EPG も含める必要があります。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[L3Out EPG]** を 指定する場合は、テナント、L3Out 名、および外部 EPG ネットワークも含める必要があります。

d) 複製されたパケットを受信するリモート サーバの **[宛先 IP（Destination IP）]** を指定します。

e) **[送信元 IP/プレフィックス（Source IP/Prefix）]**：送信元パケットの IP サブネットのベース IP アドレスです。

f) SPAN パケットの **[フロー ID（Flow ID）]** を指定します。指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。

g) **[TTL]** またはホップ制限を指定します。範囲は1ー255 ホップです。ゼロに設定する場合、TTL は指定されません。デフォルトは 64 ホップです。

h) **[MTU]** 値を指定します。範囲は 64 ～ 9216 です。デフォルトは、 1518 です。

i) SPAN 宛先の **[DSCP]** レベルを指定します。

ステップ 5 完了したら、[送信（Submit）] をクリックします。

宛先グループが作成されます。

Cisco APIC GUI を使用したアクセス SPAN ポリシーの宛先グループの設定

このセクションでは、Cisco APIC GUI を使用して、アクセス SPAN ポリシーの宛先グループを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

SPAN宛先グループと送信元を作成すれば、SPAN宛先のトラフィック アナライザを使用して、SPAN送信元からのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

手順

ステップ 1 メニューバーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 宛先グループ（SPAN Destination Groups）]** を右クリックして、**[SPAN 宛先グループの作成（Create SPAN Destination Groups）]** を選択します。**[Create SPAN Destination Group]** ダイアログが表示されます。

a) [Name] フィールドに、SPAN 宛先グループの名前を入力します。

b) オプション。**[説明（Description）]** フィールドに、グループの説明を入力します。

c) **[宛先タイプ（Destination Type）]**で、**[アプリケーション EPG（Application EPG ）]** または **[L3Out EPG（L3Out EPG）]**を選択します。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[アプリケーション EPG（Application EPG）]** を指定する場合は、テナント、アプリケーション プロファイル、および宛先 EPG も含める必要があります。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[L3Out EPG]** を 指定する場合は、テナント、L3Out プロファイル、および外部ネットワークも含める必要があります。

d) 複製されたパケットを受信するリモート サーバの **[宛先 IP（Destination IP）]** を指定します。

e) **[送信元 IP/プレフィックス（Source IP/Prefix）]** : 送信元パケットの IP サブネットのベース IP アドレスです。

f) SPAN パケットの **[フロー ID（Flow ID）]** を指定します。指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。

g) **[TTL]** またはホップ制限を指定します。範囲は1ー255 ホップです。ゼロに設定する場合、TTL は指定されません。デフォルトは 64 ホップです。

h) **[MTU]** 値を指定します。範囲は 64 ～ 9216 です。デフォルトは、 1518 です。

i) SPAN 宛先の **[DSCP]** レベルを指定します。

ステップ 4 完了したら、[送信（Submit）] をクリックします。

宛先グループが作成されます。

Cisco APIC GUI を使用したファブリック SPAN ポリシーの宛先グループの設定

このセクションでは、Cisco APIC GUI を使用して、ファブリック SPAN ポリシーの宛先グループを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

SPAN宛先グループと送信元を作成すれば、SPAN宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

（注） スパン送信元をスパイン ポートとして構成し、L3Outを接続先として選択すると、対応するスパイン ノードで障害が発生し、無効な構成について通知されます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 宛先グループ（SPAN Destination Groups）]** を右クリックして、**[SPAN 宛先グループの作成（Create SPAN Destination Groups）]** を選択します。**[Create SPAN Destination Group]** ダイアログが表示されます。

a) [Name] フィールドに、SPAN 宛先グループの名前を入力します。
b) オプション。**[説明（Description）]** フィールドに、グループの説明を入力します。
c) **[宛先タイプ（Destination Type）]**で、**[アプリケーション EPG（Application EPG ）]** または **[L3Out EPG（L3Out EPG）]**を選択します。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[アプリケーション EPG（Application EPG）]** を指定する場合は、テナント、アプリケーション プロファイル、および宛先 EPG も含める必要があります。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[L3Out EPG]** を 指定する場合は、テナント、L3Out プロファイル、および外部ネットワークも含める必要があります。

d) 複製されたパケットを受信するリモート サーバの **[宛先 IP（Destination IP）]** を指定します。
e) **[送信元 IP/プレフィックス（Source IP/Prefix）]**：送信元パケットの IP サブネットのベース IP アドレスです。
f) SPAN パケットの **[フロー ID（Flow ID）]** を指定します。指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。
g) **[TTL]** またはホップ制限を指定します。範囲は 1 ー 255 ホップです。ゼロに設定する場合、TTL は指定されません。デフォルトは 64 ホップです。
h) **[MTU]** 値を指定します。範囲は 64 ～ 9216 です。デフォルトは、 1518 です。
i) SPAN 宛先の **[DSCP]** レベルを指定します。

ステップ 4 完了したら、[送信（Submit）] をクリックします。

宛先グループが作成されます。

次のタスク

まだ作成していない場合は、ファブリック SPAN ポリシーの送信元を設定します。

NX-OS スタイルの CLI を使用した SPAN の構成

NX-OS スタイルの CLI を使用したアクセス モードでのローカル SPAN の設定

これは、アクセス リーフ ノードにローカルな従来の SPAN 設定です。1 つ以上のアクセス ポートまたはポート チャネルから発信されたトラフィックをモニタリングし、同じリーフ ノードにローカルな宛先ポートに送信できます。

手順

ステップ 1 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor access session** *session-name*

アクセス モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor access session mySession
```

ステップ 3 [**no**] **description** *text*

このアクセス モニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-access)# description "This is my SPAN session"
```

ステップ 4 [**no**] **destination interface ethernet** *slot/port* **leaf** *node-id*

宛先インターフェイスを指定します。宛先インターフェイスを FEX ポートにすることはできません。

例：

```
apic1(config-monitor-access)# destination interface ethernet 1/2 leaf 101
```

ステップ 5 [**no**] **source interface ethernet** {[*fex/*]*slot/port* | *port-range*} **leaf** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-access)# source interface ethernet 1/2 leaf 101
```

ステップ 6 **drop enable**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-access-source)# drop enable
```

ステップ 7 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# direction tx
```

ステップ 8 [**no**] **filter tenant** *tenant-name* **application** *application-name* **epg** *epg-name*

モニタリングするトラフィックのフィルタ処理を行います。フィルタは、送信元ポート範囲ごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
```

ステップ 9 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-access-source)# exit
```

ステップ 10 [**no**] **destination interface port-channel** *port-channel-name-list* **leaf** *node-id*

宛先インターフェイスを指定します。宛先インターフェイスを FEX ポートにすることはできません。

（注）
リリース 4.1(1) 以降、コマンド例に示すように、宛先インターフェイスとしてスタティック ポート チャネルを使用できるようになりました。

例：

```
apic1(config-monitor-access)# destination interface port-channel pc1 leaf 101
```

ステップ 11 [**no**] **source interface port-channel** *port-channel-name-list* **leaf** *node-id* [**fex** *fex-id*]

送信元インターフェイス ポート チャネルを指定します。

（トラフィックの方向とフィルタ設定を入力します。ここには表示されていません）。

例：

```
apic1(config-monitor-access)# source interface port-channel pc5 leaf 101
```

ステップ 12 [**no**] **filter tenant** *tenant-name* **l3out** *L3Out-name* **vlan** *interface-VLAN*

モニタリングするトラフィックのフィルタ処理を行います。フィルタは、送信元ポート範囲ごとに独立して設定できます。

（注）
リリース 4.1(1) 以降、例に示すように、L3Out インターフェイス フィルタリングを設定するときに IP プレフィックスを指定する必要がなくなりました。

例：

```
apic1(config-monitor-access-source)# filter tenant t1 l3out l3out1 vlan 2820
```

ステップ 13 [**no**] **shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-access)# no shut
```

例

この例は、ローカル アクセス モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor access session mySession
apic1(config-monitor-access)# description "This is my SPAN session"
apic1(config-monitor-access)# destination interface ethernet 1/2 leaf 101
apic1(config-monitor-access)# source interface ethernet 1/1 leaf 101
apic1(config-monitor-access)# drop enable
apic1(config-monitor-access-source)# direction tx
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
```

```
apic1(config-monitor-access-source)# exit
apic1(config-monitor-access)# no shut
apic1(config-monitor-access)# show run
# Command: show running-config monitor access session mySession
# Time: Fri Nov 6 23:55:35 2015
  monitor access session mySession
    description "This is my SPAN session"
    destination interface eth 1/2 leaf 101
    source interface eth 1/1 leaf 101
      direction tx
      filter tenant t1 application app1 epg epg
      exit
    exit
```

NX-OS スタイルの CLI を使用した SPAN フィルタ グループの設定

次の手順では、SPAN フィルタ グループとフィルタ エントリを設定する方法について説明します。

手順

ステップ 1 **configure**

グローバル設定モードを開始します。

例：

```
apic1# configure
```

ステップ 2 [**no**] **monitor access filter-group** *filtergroup-name*

アクセス モニタリング フィルタ グループ設定を作成します。

例：

```
apic1(config)# monitor access filter-group filtergroup1
```

ステップ 3 [**no**] **filter srcaddress** *source-address* **dstaddress** *destination-address* **srcport-from** *source-from-port* **srcport-to** *source-to-port* **dstport-from** *destination-from-port* **dstport-to** *destination-to-port* **ipproto** *IP-protocol*

フィルタ グループのフィルタ エントリを設定します。ここで、

- *source-address* は、*IP* アドレス/マスク 形式の送信元 IP アドレスです。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。**0.0.0.0** の値は、このフィールドで **任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。
- *destination-address* は、*IP* アドレス/マスク形式の宛先 IP アドレスです。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。**0.0.0.0** の値は、このフィールドで **任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。

- *source-from-port* は、最初の送信元レイヤ 4 ポートです。このフィールドは、**srcport-to** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *source-to-port* は、最後の送信元レイヤ 4 ポートです。このフィールドは、**srcport-from** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *destination-from-port* は、最初の宛先レイヤ 4 ポートです。このフィールドは、**dstport-to** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *destination-to-port* は、最後の宛先レイヤ 4 ポートです。このフィールドは、**dstport-from** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *IP-protocol* は IP プロトコルです。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。

例：

```
apic1(config-monitor-fltgrp)# filter srcaddress 1.1.1.0/24 dstaddress 0.0.0.0 srcport-from
 0 srcport-to 0 dstport-from 0 dstport-to 0 ipproto 20
```

ステップ 4 **exit**

アクセス モニター フィルタ グループ設定モードに戻ります。

例：

```
apic1(config-monitor-fltgrp)# exit
```

ステップ 5 **exit**

グローバル コンフィギュレーション モードを終了します。

例：

```
apic1(config)# exit
```

例

この例は、SPAN フィルタ グループとフィルタ エントリを設定する方法を示しています。

```
apic1# configure
apic1(config)# monitor access filter-group filtergroup1
apic1(config-monitor-fltgrp)# filter srcaddress 1.1.1.0/24 dstaddress 0.0.0.0 srcport-from
 0 srcport-to 0 dstport-from 0 dstport-to 0 ipproto 20
apic1(config-monitor-fltgrp)# exit
apic1(config)# exit
```

NX-OS スタイルの CLI を使用した SPAN フィルタ グループの関連付け

次の手順では、フィルタ グループを SPAN 送信元グループに関連付ける方法について説明します。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 [**no**] **monitor access session** *session-name*

アクセス モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor access session session1
```

ステップ 3 **filter-group** *filtergroup-name*

フィルタ グループを関連付けます。

例：

```
apic1(config-monitor-access)# filter-group filtergroup1
```

ステップ 4 **no filter-group**

必要に応じて、フィルタ グループの関連付けを解除します。

例：

```
apic1(config-monitor-access)# no filter-group
```

ステップ 5 [**no**] **source interface ethernet** {[*fex/*]*slot/port* | *port-range*} **leaf** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-access)# source interface ethernet 1/9 leaf 101
```

ステップ 6 **filter-group** *filtergroup-name*

フィルタ グループを SPAN 送信元に関連付けます。

例：

```
apic1(config-monitor-access-source)# filter-group filtergroup2
```

ステップ 7 **exit**

アクセス モニター フィルタ グループ設定モードに戻ります。

例：

```
apic1(config-monitor-access-source)# exit
```

ステップ 8 **no filter-group**

必要に応じて、SPAN 送信元からフィルタ グループの関連付けを解除します。

例：

```
apic1(config-monitor-access-source)# no filter-group
```

ステップ 9 **exit**

アクセス モニター フィルタ グループ設定モードに戻ります。

例：

```
apic1(config-monitor-access)# exit
```

ステップ 10 **exit**

グローバル コンフィギュレーション モードを終了します。

例：

```
apic1(config)# exit
```

例

この例は、フィルタ グループを関連付ける方法を示しています。

```
apic1# configure
apic1(config)# monitor access session session1
apic1(config-monitor-access)# filter-group filtergroup1
apic1(config-monitor-access)# source interface ethernet 1/9 leaf 101
apic1(config-monitor-access-source)# filter-group filtergroup2
apic1(config-monitor-access-source)# exit
apic1(config-monitor-access-source)# no filter-group
apic1(config-monitor-access)# exit
apic1(config)# exit
```

NX-OS スタイルの CLI を使用したアクセス モードでの ERSPAN の設定

ACI ファブリックでは、アクセス モードの ERSPAN 設定を使用して、1 つ以上のリーフ ノードのアクセス ポート、ポート チャネル、および vPC から発信されたトラフィックを監視できます。

ERSPAN セッションの場合、宛先は常にエンドポイント グループ (EPG) で、これらはファブリック内のどこにでも展開できます。監視対象のトラフィックは、どこであれ、EPGが移動した場所である宛先に転送されます。

手順

ステップ 1 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor access session** *session-name*

アクセス モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor access session mySession
```

ステップ 3 [**no**] **description** *text*

このモニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-access)# description "This is my access ERSPAN session"
```

ステップ 4 [**no**] **destination tenant** *tenant-name* **application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーションモードを開始します。

例：

```
apic1(config-monitor-access)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
```

ステップ 5 [**no**] **erspan-id** *flow-id*

ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

例：

```
apic1(config-monitor-access-dest)# erspan-id 100
```

ステップ 6 [**no**] **ip dscp** *dscp-code*

ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。指定できる範囲は 0 ～ 64 です。

例：

```
apic1(config-monitor-access-dest)# ip dscp 42
```

ステップ 7 [**no**] **ip ttl** *ttl-value*

ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。

例：

```
apic1(config-monitor-access-dest)# ip ttl 16
```

ステップ 8 [**no**] **mtu** *mtu-value*

ERSPAN セッションの最大伝送単位（MTU）サイズを設定します。指定できる範囲は 64 ～ 9216 バイトです。

例：

```
apic1(config-monitor-access-dest)# mtu 9216
```

ステップ 9 **exit**

モニター アクセス設定モードに戻ります。

例：

```
apic1(config-monitor-access-dest)#
```

ステップ 10 [**no**] **source interface ethernet** {[*fex/*]*slot/port* | *port-range*} **leaf** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-access)# source interface eth 1/2 leaf 101
```

ステップ 11 [**no**] **source interface port-channel** *port-channel-name-list* **leaf** *node-id* [**fex** *fex-id*]

送信元インターフェイスのポートチャネルを指定します。

例：

```
apic1(config-monitor-access)# source interface port-channel pc1 leaf 101
```

ステップ 12 [**no**] **source interface vpc** *vpc-name-list* **leaf** *node-id1 node-id2* [**fex** *fex-id1 fex-id2*]

送信元インターフェイス vPC を指定します。

例：

```
apic1(config-monitor-access)# source interface vpc pc1 leaf 101 102
```

ステップ 13 **drop enable**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-access-source)# drop enable
```

ステップ 14 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# direction tx
```

ステップ 15 [**no**] **filter tenant** *tenant-name* **application** *application-name* **epg** *epg-name*

モニタリングするトラフィックのフィルタ処理を行います。フィルタは、送信元ポート範囲ごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
```

ステップ 16 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-access-source)# exit
```

ステップ 17 **[no] shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-access)# no shut
```

例

この例は、ERSPAN アクセス モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor access session mySession
apic1(config-monitor-access)# description "This is my access ERSPAN session"
apic1(config-monitor-access)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
apic1(config-monitor-access-dest)# erspan-id 100
apic1(config-monitor-access-dest)# ip dscp 42
apic1(config-monitor-access-dest)# ip ttl 16
apic1(config-monitor-access-dest)# mtu 9216
apic1(config-monitor-access-dest)# exit
apic1(config-monitor-access)# source interface eth 1/1 leaf 101
apic1(config-monitor-access-source)# direction tx
apic1(config-monitor-access-source)#drop enable
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
apic1(config-monitor-access-source)# exit
apic1(config-monitor-access)# no shut
apic1(config-monitor-access)# show run
# Command: show running-config monitor access session mySession
# Time: Fri Nov 6 23:55:35 2015
  monitor access session mySession
    description "This is my ERSPAN session"
    source interface eth 1/1 leaf 101
      direction tx
      filter tenant t1 application app1 epg epg1
      exit
    destination tenant t1 application app1 epg epg1 destination-ip 192.0.20.123
source-ip-prefix 10.0.20.1
      ip dscp 42
      ip ttl 16
      erspan-id 9216
```

```
    mtu 9216
    exit
  exit
```

この例は、モニタリング送信元としてポート チャネルを設定する方法を示しています。

```
apic1(config-monitor-access)# source interface port-channel pc3 leaf 105
```

この例は、モニタリング送信元として vPC の 1 つのレッグを設定する方法を示しています。

```
apic1(config-monitor-access)# source interface port-channel vpc3 leaf 105
```

次の例は、FEX 101 からのポートの範囲をモニタリング送信元として設定する方法を示しています。

```
apic1(config-monitor-access)# source interface eth 101/1/1-2 leaf 105
```

NX-OS スタイルの CLI を使用したファブリック モードでの ERSPAN の設定

ACI ファブリックでは、ファブリック モードの ERSPAN 設定を使用して、リーフ ノードまたはスパイン ノードの 1 つ以上のファブリック ポートから発信されたトラフィックをモニタリングできます。ローカル SPAN はファブリック モードではサポートされていません。

ERSPAN セッションの場合、宛先は常にエンドポイント グループ (EPG) で、これらはファブリック内のどこにでも展開できます。監視対象のトラフィックは、どこであれ、EPGが移動した場所である宛先に転送されます。ファブリック モードでは、ファブリック ポートのみが送信元として許可されますが、リーフ スイッチとスパイン スイッチの両方が許可されます。

手順

ステップ 1 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor fabric session** *session-name*

ファブリック モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor fabric session mySession
```

ステップ 3 [**no**] **description** *text*

このモニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-fabric)# description "This is my fabric ERSPAN session"
```

ステップ 4 [**no**] **destination tenant** *tenant-name* **application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーションモードを開始します。

例：

```
apic1(config-monitor-fabric)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
```

ステップ 5 [**no**] **erspan-id** *flow-id*

ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

例：

```
apic1(config-monitor-fabric-dest)# erspan-id 100
```

ステップ 6 [**no**] **ip dscp** *dscp-code*

ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。指定できる範囲は 0 ～ 64 です。

例：

```
apic1(config-monitor-fabric-dest)# ip dscp 42
```

ステップ 7 [**no**] **ip ttl** *ttl-value*

ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。

例：

```
apic1(config-monitor-fabric-dest)# ip ttl 16
```

ステップ 8 [**no**] **mtu** *mtu-value*

ERSPAN セッションの最大伝送単位（MTU）サイズを設定します。指定できる範囲は 64 ～ 9216 バイトです。

例：

```
apic1(config-monitor-fabric-dest)# mtu 9216
```

ステップ 9 **exit**

モニター アクセス設定モードに戻ります。

例：

```
apic1(config-monitor-fabric-dest)#
```

ステップ 10 [**no**] **source interface ethernet** {*slot/port* | *port-range*} **switch** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-fabric)# source interface eth 1/2 switch 101
```

ステップ 11 **drop enable**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-fabric-source)# drop enable
```

ステップ 12 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-fabric-source)# direction tx
```

ステップ 13 [**no**] **filter tenant** *tenant-name* **bd** *bd-name*

ブリッジ ドメインでトラフィックをフィルタリングします。

例：

```
apic1(config-monitor-fabric-source)# filter tenant t1 bd bd1
```

ステップ 14 [**no**] **filter tenant** *tenant-name* **vrf** *vrf-name*

VRF でトラフィックをフィルタリングします。

例：

```
apic1(config-monitor-fabric-source)# filter tenant t1 vrf vrf1
```

ステップ 15 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-fabric-source)# exit
```

ステップ 16 [**no**] **shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-fabric)# no shut
```

例

この例は、ERSPAN ファブリック モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor fabric session mySession
apic1(config-monitor-fabric)# description "This is my fabric ERSPAN session"
apic1(config-monitor-fabric)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
apic1(config-monitor-fabric-dest)# erspan-id 100
apic1(config-monitor-fabric-dest)# ip dscp 42
apic1(config-monitor-fabric-dest)# ip ttl 16
apic1(config-monitor-fabric-dest)# mtu 9216
apic1(config-monitor-fabric-dest)# exit
apic1(config-monitor-fabric)# source interface eth 1/1 switch 101
apic1(config-monitor-fabric-source)# drop enable
apic1(config-monitor-fabric-source)# direction tx
apic1(config-monitor-fabric-source)# filter tenant t1 bd bd1
apic1(config-monitor-fabric-source)# filter tenant t1 vrf vrf1
apic1(config-monitor-fabric-source)# exit
apic1(config-monitor-fabric)# no shut
```

NX-OS スタイルの CLI を使用したテナント モードでの ERSPAN の設定

ACI ファブリックでは、テナント モードの ERSPAN 設定を使用して、テナント内のエンドポイント グループから発信されたトラフィックをモニタリングできます。

テナント モードでは、送信元 EPG から発信されたトラフィックは、同じテナント内の宛先 EPG に送信されます。送信元または宛先の EPG がファブリック内で移動しても、トラフィックのモニタリングには影響しません。

手順

ステップ 1 **configure terminal**

グローバル設定モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor tenant** *tenant-name* **session** *session-name*

テナント モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor tenant session mySession
```

ステップ 3 [**no**] **description** *text*

このアクセス モニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-tenant)# description "This is my tenant ERSPAN session"
```

ステップ 4 [**no**] **destination tenant** *tenant-name* **application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーションモードを開始します。

例：

```
apic1(config-monitor-tenant)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
```

ステップ 5 [**no**] **erspan-id** *flow-id*

ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

例：

```
apic1(config-monitor-tenant-dest)# erspan-id 100
```

ステップ 6 [**no**] **ip dscp** *dscp-code*

ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。指定できる範囲は 0 ～ 64 です。

例：

```
apic1(config-monitor-tenant-dest)# ip dscp 42
```

ステップ 7 [**no**] **ip ttl** *ttl-value*

ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。

例：

```
apic1(config-monitor-tenant-dest)# ip ttl 16
```

ステップ 8 [**no**] **mtu** *mtu-value*

ERSPAN セッションの最大伝送単位（MTU）サイズを設定します。指定できる範囲は 64 ～ 9216 バイトです。

例：

```
apic1(config-monitor-tenant-dest)# mtu 9216
```

ステップ 9 **exit**

モニター アクセス設定モードに戻ります。

例：

```
apic1(config-monitor-tenant-dest)#
```

ステップ 10 [**no**] **source application** *application-name* **epg** *epg-name*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-tenant)# source application app2 epg epg5
```

ステップ 11 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-tenant-source)# direction tx
```

ステップ 12 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-tenant-source)# exit
```

ステップ 13 [**no**] **shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-tenant)# no shut
```

例

この例は、ERSPAN テナント モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor access session mySession
apic1(config-monitor-tenant)# description "This is my tenant ERSPAN session"
apic1(config-monitor-tenant)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
apic1(config-monitor-tenant-dest)# erspan-id 100
apic1(config-monitor-tenant-dest)# ip dscp 42
apic1(config-monitor-tenant-dest)# ip ttl 16
apic1(config-monitor-tenant-dest)# mtu 9216
apic1(config-monitor-tenant-dest)# exit
apic1(config-monitor-tenant)# source application app2 epg epg5
apic1(config-monitor-tenant-source)# direction tx
apic1(config-monitor-tenant-source)# exit
apic1(config-monitor-tenant)# no shut
```

NX-OS スタイルの CLI を使用したグローバル SPAN-On-Drop セッションの設定

このセクションでは、ノード上のすべてのポートを SPAN 送信元とするグローバル ドロップを作成する方法を示します。

手順

ステップ 1 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor fabric session** *session-name*

ファブリック モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor fabric session Spine301-GD-SOD
```

ステップ 3 [**no**] **description** *text*

このモニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-fabric)# description "This is my fabric ERSPAN session"
```

ステップ 4 **source global-drop switch**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-fabric)# source global-drop switch
```

ステップ 5 [**no**] **destination tenant** *tenant-name***application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーション モードを開始します。

例：

```
apic1(config-monitor-fabric-dest)# destination tenant ERSPAN application A1 epg E1
destination-ip 165.10.10.155 source-ip-prefix 22.22.22.22
```

例

次に、SPAN-on-Drop セッションを設定する例を示します。

```
apic1# configure terminal
apic1(config)# monitor fabric session Spine301-GD-SOD
apic1(config-monitor-fabric)# source global-drop switch
apic1(config-monitor-fabric)# destination tenant ERSPAN application A1 epg E1
destination-ip 179.10.10.179 source-ip-prefix 31.31.31.31
```

REST API を使用した SPAN の構成

REST API を使用した ERSPAN 宛先のファブリック宛先グループの設定

このセクションでは、REST API を使用して、ERSPAN 宛先のファブリック宛先グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

ERSPAN 宛先のファブリック宛先グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanDestGrp annotation="" descr="" name="Dest2" nameAlias="" ownerKey="" ownerTag="">
    <spanDest annotation="" descr="" name="Dest2" nameAlias="" ownerKey="" ownerTag="">
    <spanRsDestEpg annotation="" dscp="unspecified" finalIp="0.0.0.0" flowId="1"
ip="179.10.10.179"
     mtu="1518"srcIpPrefix="20.20.20.2" tDn="uni/tn-ERSPAN/ap-A1/epg-E1" ttl="64"
ver="ver2"
     verEnforced="no"/>
    </spanDest>
</spanDestGrp>
```

REST API を使用したグローバル ドロップ送信元グループの設定

このセクションでは、REST API を使用してグローバル ドロップ送信元グループを構成することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

グローバル ドロップ送信元グループを構成します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanSrcGrp adminSt="enabled" annotation="" descr="" name="Spine-402-GD-SOD" nameAlias="">

   <spanSrc annotation="" descr="" dir="both" name="402" nameAlias=""  spanOnDrop="yes">

    <spanRsSrcToNode annotation="" tDn="topology/pod-1/node-402"/>
    </spanSrc><spanSpanLbl annotation="" descr="" name="402-dst-179" nameAlias=""
tag="yellow-green"/>
</spanSrcGrp>
```

REST API を使用した SPAN 宛先としてのリーフ ポートの設定

このセクションでは、REST API を使用してリーフ ポートを SPAN 宛先として設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

リーフ ポートを SPAN 宛先として設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanDestGrp annotation="" descr="" name="Dest4" nameAlias="" ownerKey="" ownerTag="">
    <spanDest annotation="" descr="" name="Dest4" nameAlias="" ownerKey="" ownerTag="">
    <spanRsDestPathEp annotation="" mtu="1518"
tDn="topology/pod-1/paths-301/pathep-[eth1/18]"/>
    </spanDest>
</spanDestGrp>
```

REST API を使用した SPAN アクセス送信元グループの設定

このセクションでは、REST API を使用して SPAN アクセス ソース グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

SPAN アクセス送信元グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanSrcGrp adminSt="enabled" annotation="" descr=""  name="Test-Src2" nameAlias=""
ownerKey=""
 ownerTag="">
    <spanSrc annotation="" descr="" dir="both" name="Src1" nameAlias="" ownerKey=""
ownerTag=""
     spanOnDrop="yes">
    <spanRsSrcToPathEp annotation="" tDn="topology/pod-1/paths-301/pathep-[eth1/1]"/>
    </spanSrc>
   <spanSpanLbl annotation="" descr="" name="Dest1" nameAlias="" ownerKey="" ownerTag=""

     tag="yellow-green"/>
</spanSrcGrp>
```

REST API を使用した SPAN ファブリック送信元グループの設定

このセクションでは、REST API を使用して SPAN ファブリック送信元グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

SPAN ファブリック送信元グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanSrcGrp adminSt="enabled" annotation="" descr="" name="Test-Src2" nameAlias=""
ownerKey=""
 ownerTag="">
    <spanSrc annotation="" descr="" dir="both" name="Src1" nameAlias="" ownerKey=""
     ownerTag="" spanOnDrop="yes">
    <spanRsSrcToPathEp annotation="" tDn="topology/pod-1/paths-301/pathep-[eth1/51]"/>
    </spanSrc>
   <spanSpanLbl annotation="" descr="" name="Dest2" nameAlias="" ownerKey="" ownerTag=""

     tag="yellow-green"/>
</spanSrcGrp>
```

REST API を使用した ERSPAN 宛先のアクセス宛先グループの設定

このセクションでは、REST API を使用して、ERSPAN 宛先のアクセス宛先グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

ERSPAN 宛先のアクセス宛先グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanDestGrp annotation="" descr="" name="Dest4" nameAlias="" ownerKey=""
  ownerTag="">
    <spanDest annotation="" descr="" name="Dest4" nameAlias="" ownerKey=""
     ownerTag="">
    <spanRsDestPathEp annotation="" mtu="1518" tDn="topology/pod-1/paths-301/pathep-
     [eth1/18]"/>
    </spanDest>
</spanDestGrp>
```

トレースルートの使用

トレースルートの概要

トレースルートツールは、パケットが送信先に移動するときに実際に通るルートを検出するために使用されます。tracerouteでは、ホップごとに使用されるパスが識別され、双方向で各ホップにタイムスタンプが付けられます。tracerouteを使用すると、発信元のデバイスと送信先に最も近いデバイスの間のパスに沿ってポート接続をテストできます。送信先に到達できない場合は、パス検出によってパスが障害ポイントまで追跡されます。

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、入力リーフの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。

トレースルートでは、次のようなさまざまなモードがサポートされています。

- エンドポイント間、リーフ間（トンネル エンドポイント、または TEP 間）
- エンドポイントから外部 IP
- 外部 IP からエンドポイント
- 外部 IP 間

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。

トレースルートの注意事項および制約事項

- トレースルートの送信元または宛先がエンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）にはトレースルートに必要な子オブジェクト（fv:RsCEpToPathEp）がありません。
- トレースルートは IPv6 の送信元と宛先で動作しますが、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 アドレスを設定することはできません。
- トレースルート関連の制限については、『*Verified Scalability Guide for Cisco ACI*』ドキュメントを参照してください。
- エンドポイントを新しいMACアドレス（トレースルート ポリシーを設定する際に指定した MAC アドレスと異なる）の ToR スイッチに移動すると、トレースルート ポリシーでそのエンドポイントに「missing-target」と表示されます。この場合は、新しい MAC アドレスを指定して新しいトレースルート ポリシーを設定する必要があります。
- ポリシーベースのリダイレクト機能を含むフローに対してトレースルートを実行する場合、パケットがサービスデバイスからリーフ スイッチに送信されるときに、リーフ スイッチが存続時間（TTL）期限切れメッセージを送信元に伝えるために使用する IP アドレス

は、必ずしもサービス デバイスのブリッジ ドメインのスイッチ仮想インターフェイス（SVI）の IP アドレスにはなりません。この動作は表面的なものであり、トラフィックが予期された経路をたどっていないことを示すものではありません。

エンドポイント 間での traceroute の実行

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション]** ペインでテナントを展開し、**[ポリシー]** > **[トラブルシューティング]** を展開します。

ステップ 4 [Troubleshoot] で次のトレースルート ポリシーのいずれかを右クリックします。

- [Endpoint-to-Endpoint Traceroute Policies] を右クリックして [Create Endpoint-to-Endpoint Traceroute Policy] を選択する
- [Endpoint-to-External-IP Traceroute Policies] を右クリックして [Create Endpoint-to-External-IP Traceroute Policy] を選択する
- [External-IP-to-Endpoint Traceroute Policies] を右クリックして [Create External-IP-to-Endpoint Traceroute Policy] を選択する
- [External-IP-to-External-IP Traceroute Policies] を右クリックして [Create External-IP-to-External-IP Traceroute Policy] を選択する

ステップ 5 ダイアログボックスのフィールドに適切な値を入力し、[Submit] をクリックします。

（注）
フィールドの説明については、ダイアログボックスの右上隅にあるヘルプ アイコン（[?]）をクリックしてください。

ステップ 6 **[Navigation]** ペインまたは **[Traceroute Policies]** テーブルで、traceroute ポリシーをクリックします。

トレースルート ポリシーが [Work] ペインに表示されます。

ステップ 7 [Work] ペインで [Operational] タブをクリックし、[Source Endpoints] タブ、[Results] タブの順にクリックします。

ステップ 8 **[Traceroute Results]** テーブルで、追跡に使用された単数または複数のパスを確認します。

（注）
- 複数のパスが、送信元ノードから宛先ノードへの移動に使用されている場合があります。

- **[Name]** 列など、1 つまたは複数の列の幅を広げると確認しやすくなります。

acidiag コマンド

Cisco APIC でのトラブルシューティング操作では、**acidiag** コマンドを使用します。

⚠

注意 このコマンドは、ACIの日常的な操作を目的としたものではありません。コマンドのすべての形式は、非常に混乱を招く可能性があり、適切に使用しないとネットワークに重大な問題が発生する場合があります。実行する前に、ファブリックへの完全な影響を理解してください。

クラスタ コマンド

```
acidiag

acidiag avread

acidiag fnvread

acidiag fnvreadex
```

構文の説明

オプション	機能
avread	クラスタ内のAPICを表示します。avreadの出力は次のとおりです。 • Cluster of：動作するクラスタのサイズ • out of target：必要なクラスタ サイズ • active=：APICが到達可能かどうかを示します • health=：全体的なAPICの正常性の概要。正常性スコアが低下しているサービスを表示します。 • chassisID=：所定の APIC に対する既知のシャーシ ID。 （注） 現在クラスタにない APIC については、ピア シャーシ ID が正しくない可能性があります。

オプション	機能
bootcurr	次回の起動時に、APIC システムは Linux パーティション内の現在の APIC イメージを起動します。このオプションは、通常は使用されません。
bootother	次回の起動時に、APIC システムは Linux パーティションの以前の APIC イメージを起動します。このオプションは、通常は使用されません。
bond0test	リーフへの APIC 接続の中断テスト。これは、シスコの内部テスト目的でのみ使用されます。それ以外では、ファブリックへの APIC 接続で問題が発生する可能性があります。
fnvread	ファブリックに登録されているスイッチ ノードのアドレスと状態を表示します。
fnvreadex	ファブリックに登録されているスイッチのノードの追加情報を表示します。
linkflap	指定された APIC インターフェイスを停止およびバックアップします。
preservelogs	APIC は現在のログをアーカイブします。通常の再起動中に、これは自動的に発生します。このオプションは、ハード リブートの前に使用できます。
run	使用可能な 2 つのオプションは、iptables-list と lldptool です。iptables-list は、管理テナント コントラクトによって制御される Linux iptables を表示するために使用されます。 lldptool は、APIC によって送受信される lldp 情報を表示するために使用されます。
rvread	データ レイヤの状態を要約します。出力には、各サービスのデータ レイヤの状態の概要が表示されます。シャード ビューには、レプリカが昇順で表示されます。
acidiag rvread *service*	すべてのレプリカのすべてのシャードでのサービスのデータ レイヤの状態を表示します。 （注） 例については、例 （146 ページ） を参照してください。

オプション	機能
acidiag rvread *service shard*	すべてのレプリカの特定のシャードでのサービスのデータ レイヤの状態を表示します。 （注） 例については、例 （146 ページ）を参照してください。
acidiag rvread *service shard replica*	特定のシャードとレプリカでのサービスのデータ レイヤの状態を表示します。 （注） 例については、例 （146 ページ） を参照してください。
validateimage	イメージをファームウェア リポジトリにロードする前に、イメージを検証できます。この関数は、リポジトリに追加されるイメージのプロセスの通常の一部として実行されることに注意してください。
validateenginxconf	APIC で生成された nginx 構成ファイルを検証して、nginx がその構成ファイルで起動できることを確認します。これは、nginx Web サーバーが APIC で実行されていない場合のデバッグでの使用を目的としています。

サービス ID

次の表にリストされているサービス ID は、**man acidiag** コマンドを入力するときにも表示されます。

表 *4:* サービス *ID*

サービス	ID
cliD	1
コントローラ	2
eventmgr	3
extXMLApi	4
ポリシー要素	5
policymgr	6
リーダー	7

サービス	ID
AE	8
topomgr	9
observer	10
dbgr	11
observerelem	12
dbgrelem	13
vmmmgr	14
nxosmock	15
bootmgr	16
appliancedirector	17
adrelay	18 日
ospaagent	19
vleafelem	20
dhcpd	21
scripthandler	22
idmgr	23
ospaelem	24
osh	25
opflexagent	26
opflexelem	27
confelem	28
vtap	29
snmpd	30
opflexp	31
分析	32
policydist	33
plghandler	34
domainmgr	35

サービス	ID
licensemgr	36
なし	37
platformmgr	38
edmgr	39

表 *5:* データの状態

州	ID
コマトーセ	0
NEWLY_BORN	1
不明ファイル	2
DATA_LAYER_DIVERGED	11
DATA_LAYER_DEGRADED_LEADERSHIP	12
DATA_LAYER_ENTIRELY_DIVERGED	111
DATA_LAYER_PARTIALLY_DIVERGED	112
DATA_LAYER_ENTIRELY_DEGRADED_LEADERSHIP	121
DATA_LAYER_PARTIALLY_DEGRADED_LEADERSHIP	122
FULLY_FIT	255

システムのキーワード

```
acidiag [start|stop|restart] [mgmt|xinetd]

acidiag installer  -u imageurl -c

acidiag reboot

acidiag  touch [clean|setup]

acidiag verifyapic
```

構文の説明

オプション	機能
-c	クリーン インストールを指定します
-u	APIC イメージの URL を指定します。
imageurl	APIC イメージを指定します。

オプション	機能
installer	APIC に新しいイメージをインストールします。-cでクリーンインストールを実行します。
mgmt	上のすべてのサービスを指定します。APIC
reboot	APICを再起動します。
restart	APIC でサービスを再起動します。
start	APIC でサービスを開始します。
stop	APIC でサービスを停止します。
touch [clean | setup]	APIC の構成をリセットします。 • **clean** オプションは、APIC ネットワーク構成（ファブリック名、IP アドレス、ログインなど）を保持しますが、すべてのポリシー データを削除します。 • **setup** オプションは、ポリシー データと APIC ネットワーク構成の両方を削除します。
verifyapic	APIC ソフトウェアのバージョンを表示します。
xinetd	sshおよびtelnetデーモンを制御するxinetd（拡張インターネット デーモン）サービスを指定します。5.3(1) リリース以降、telnet はサポートされていません。

診断キーワード

```
acidiag crashsuspecttracker

acidiag dbgtoken

acidiag version
```

構文の説明

オプション	機能
crashsuspecttracker	クラッシュを示すサービスまたはデータのサブセットの状態を追跡します。
dbgtoken	root パスワードの生成に使用するトークンを生成します。これは、必要な場合には、TAC と連携しながら、その指示どおりに使用してください。

オプション	機能
version	APIC ISO ソフトウェアのバージョンを表示します。

例

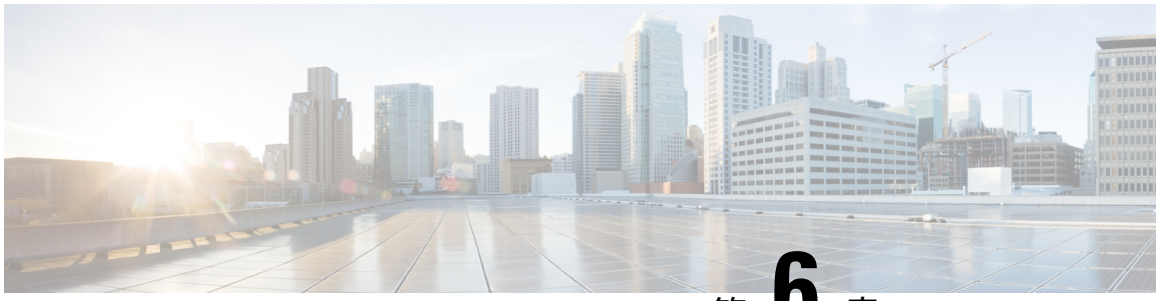
次に、**acidiag** コマンドの使用例を示します。

```
apic1# acidiag version 2.2.1o


apic1# acidiag verifyapic
openssl_check: certificate details
subject= CN=ABC12345678,serialNumber=PID:APIC-SERVER-L1 SN:ABC12345678
issuer= CN=Cisco Manufacturing CA,O=Cisco Systems
notBefore=Sep 28 17:17:42 2016 GMT
notAfter=Sep 28 17:27:42 2026 GMT
openssl_check: passed
ssh_check: passed
all_checks: passed


apic1# acidiag avread
Local appliance ID=1 ADDRESS=10.0.0.1 TEP ADDRESS=10.0.0.0/16 ROUTABLE IP ADDRESS=0.0.0.0
 CHASSIS_ID=1009f750-adab-11e9-a044-8dbd212cd556
Cluster of 7 lm(t):1(2019-08-08T01:02:17.961-07:00) appliances (out of targeted 7
lm(t):7(2019-08-08T03:50:57.240-07:00)) with FABRIC_DOMAIN name=ACI Fabric1 set to
version=apic-4.2(0.235j) lm(t):1(2019-08-17T01:09:16.413-07:00); discoveryMode=PERMISSIVE
 lm(t):0(1969-12-31T17:00:00.007-07:00); drrMode=OFF
lm(t):0(1969-12-31T17:00:00.007-07:00); kafkaMode=OFF
lm(t):0(1969-12-31T17:00:00.007-07:00)
        appliance id=1  address=10.0.0.1 lm(t):1(2019-08-08T01:02:08.544-07:00) tep
address=10.0.0.0/16 lm(t):1(2019-08-08T01:02:08.544-07:00) routable address=0.0.0.0
lm(t):1(zeroTime) oob address=172.23.96.10/21 lm(t):1(2019-08-08T01:02:18.218-07:00)
version=4.2(0.235j) lm(t):1(2019-08-15T15:22:00.158-07:00)
chassisId=1009f750-adab-11e9-a044-8dbd212cd556 lm(t):1(2019-08-15T15:22:00.158-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X7F lm(t):1(2019-08-17T01:13:46.997-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
cntrlSbst=(APPROVED, FCH1748V0SZ) lm(t):1(2019-08-15T15:22:00.158-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):1(2019-08-08T01:02:08.544-07:00) commissioned=YES lm(t):1(zeroTime) registered=YES
 lm(t):1(2019-08-08T01:02:08.544-07:00) standby=NO lm(t):1(2019-08-08T01:02:08.544-07:00)
 DRR=NO lm(t):0(zeroTime) apicX=NO lm(t):1(2019-08-08T01:02:08.544-07:00) virtual=NO
lm(t):1(2019-08-08T01:02:08.544-07:00) active=YES(2019-08-08T01:02:08.544-07:00)
health=(applnc:255 lm(t):1(2019-08-17T01:39:26.296-07:00) svc's)
        appliance id=2  address=10.0.0.2 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):2(2019-07-23T17:51:38.997-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.96.11/21 lm(t):1(2019-08-18T23:14:28.720-07:00)
version=4.2(0.235j) lm(t):2(2019-08-15T15:22:00.300-07:00)
chassisId=694e6a98-adac-11e9-ad79-d1f60e3ee822 lm(t):2(2019-08-15T15:22:00.300-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X2 lm(t):2(2019-08-14T07:55:10.074-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
cntrlSbst=(APPROVED, FCH1748V0MS) lm(t):2(2019-08-15T15:22:00.300-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):2(2019-08-08T01:42:03.670-07:00) commissioned=YES
```

```
lm(t):1(2019-08-08T01:02:17.961-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):2(2019-08-08T01:42:03.670-07:00)
 DRR=NO lm(t):1(2019-08-08T01:02:17.961-07:00) apicX=NO
lm(t):2(2019-08-08T01:42:03.670-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:02:32.983-07:00) health=(applnc:255
lm(t):2(2019-08-17T01:32:51.454-07:00) svc's)
        appliance id=3  address=10.0.0.3 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):3(2019-07-23T19:05:56.405-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.96.12/21 lm(t):1(2019-08-18T23:14:28.721-07:00)
version=4.2(0.235j) lm(t):3(2019-08-15T15:21:59.893-07:00)
chassisId=1f98b916-adb7-11e9-a6f8-abe00a04e8e6 lm(t):3(2019-08-15T15:21:59.893-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X4 lm(t):3(2019-08-14T07:55:22.256-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
cntrlSbst=(APPROVED, FCH1930V1X6) lm(t):3(2019-08-15T15:21:59.893-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):3(2019-08-08T02:15:20.560-07:00) commissioned=YES
lm(t):2(2019-08-08T01:42:15.337-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):3(2019-08-08T02:15:20.560-07:00)
 DRR=NO lm(t):2(2019-08-08T01:42:15.337-07:00) apicX=NO
lm(t):3(2019-08-08T02:15:20.560-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:02:33.182-07:00) health=(applnc:255
lm(t):3(2019-08-15T16:08:46.119-07:00) svc's)
        appliance id=4  address=10.0.0.4 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):4(2019-07-23T17:46:15.545-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.97.231/21 lm(t):1(2019-08-18T23:14:28.717-07:00)
version=4.2(0.235j) lm(t):4(2019-08-15T15:22:00.669-07:00)
chassisId=3a7f38aa-adac-11e9-8869-a9e520cdc042 lm(t):4(2019-08-15T15:22:00.669-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X8 lm(t):4(2019-08-14T07:54:59.490-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
cntrlSbst=(APPROVED, FCH1902V1WW) lm(t):4(2019-08-15T15:22:00.669-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):4(2019-08-08T02:40:09.610-07:00) commissioned=YES
lm(t):3(2019-08-08T02:15:32.613-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):4(2019-08-08T02:40:09.610-07:00)
 DRR=NO lm(t):3(2019-08-08T02:15:32.613-07:00) apicX=NO
lm(t):4(2019-08-08T02:40:09.610-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-15T15:21:59.914-07:00) health=(applnc:255
lm(t):4(2019-08-17T01:39:26.477-07:00) svc's)
        appliance id=5  address=10.0.0.5 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):5(2019-07-23T19:05:11.089-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.97.232/21 lm(t):1(2019-08-18T23:14:28.723-07:00)
version=4.2(0.235j) lm(t):5(2019-08-15T15:22:00.248-07:00)
chassisId=35428666-adb7-11e9-a315-1d7671b518b3 lm(t):5(2019-08-15T15:22:00.248-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X10 lm(t):5(2019-08-14T07:55:19.573-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
cntrlSbst=(APPROVED, FCH1902V1EG) lm(t):5(2019-08-15T15:22:00.248-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):5(2019-08-08T03:03:50.338-07:00) commissioned=YES
lm(t):4(2019-08-08T02:40:15.939-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):5(2019-08-08T03:03:50.338-07:00)
 DRR=NO lm(t):4(2019-08-08T02:40:15.939-07:00) apicX=NO
lm(t):5(2019-08-08T03:03:50.338-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-15T15:21:59.756-07:00) health=(applnc:255
lm(t):5(2019-08-17T01:32:43.730-07:00) svc's)
        appliance id=6  address=10.0.0.6 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
```

```
address=10.0.0.0/16 lm(t):6(2019-07-23T19:39:41.972-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.31.170.230/21 lm(t):1(2019-08-18T23:14:28.727-07:00)
version=4.2(0.235j) lm(t):6(2019-08-15T15:22:00.562-07:00)
chassisId=066c943a-adbc-11e9-bbed-257398025731 lm(t):6(2019-08-15T15:22:00.562-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X20 lm(t):6(2019-08-14T07:55:20.053-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.820-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.821-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.821-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.821-07:00)
cntrlSbst=(APPROVED, WZP22350JFT) lm(t):6(2019-08-15T15:22:00.562-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=9
lm(t):6(2019-08-08T03:28:11.246-07:00) commissioned=YES
lm(t):5(2019-08-08T03:03:57.387-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):6(2019-08-08T03:28:11.246-07:00)
 DRR=NO lm(t):5(2019-08-08T03:03:57.387-07:00) apicX=NO
lm(t):6(2019-08-08T03:28:11.246-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:30:37.663-07:00) health=(applnc:255
lm(t):6(2019-08-15T15:57:05.128-07:00) svc's)
        appliance id=7  address=10.0.0.7 lm(t):7(2019-08-08T03:50:48.149-07:00) tep
address=10.0.0.0/16 lm(t):7(2019-07-24T15:24:19.988-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.31.172.157/21 lm(t):1(2019-08-18T23:14:28.722-07:00)
version=4.2(0.235j) lm(t):7(2019-08-15T15:22:00.539-07:00)
chassisId=859be4ae-ae61-11e9-9840-7d9d67698989 lm(t):7(2019-08-15T15:22:00.539-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X40 lm(t):7(2019-08-14T07:55:23.872-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
cntrlSbst=(APPROVED, FCH2051V116) lm(t):7(2019-08-15T15:22:00.539-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=10
lm(t):7(2019-08-08T03:50:48.149-07:00) commissioned=YES
lm(t):6(2019-08-08T03:28:16.727-07:00) registered=YES
lm(t):6(2019-07-24T15:27:25.518-07:00) standby=NO lm(t):7(2019-08-08T03:50:48.149-07:00)
 DRR=NO lm(t):6(2019-08-08T03:28:16.727-07:00) apicX=NO
lm(t):7(2019-08-08T03:50:48.149-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:30:45.488-07:00) health=(applnc:255
lm(t):7(2019-08-17T01:39:26.549-07:00) svc's)
------------------------------------------------
clusterTime=<diff=2817 common=2019-08-19T15:33:55.929-07:00
local=2019-08-19T15:33:53.112-07:00 pF=<displForm=0 offsSt=0 offsVlu=-25200
lm(t):7(2019-08-08T03:50:55.925-07:00)>>
------------------------------------------------


apic1# acidiag rvread 6 3 1
(6,3,1)  st:6 lm(t):3(2014-10-16T08:48:20.238+00:00) le: reSt:LEADER voGr:0 cuTerm:0x19
 lCoTe:0x18
   lCoIn:0x1800000000001b2a veFiSt:0x31 veFiEn:0x31 lm(t):3(2014-10-16T08:48:20.120+00:00)

    lastUpdt 2014-10-16T09:07:00.214+00:00
------------------------------------------------
clusterTime=<diff=65247252 common=2014-10-16T09:07:01.837+00:00
local=2014-10-15T14:59:34.585+00:00
    pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):3(2014-10-16T04:50:08.714+00:00)>>


apic1# acidiag rvread 6 3
(6,3,1)  st:6 lm(t):3(2014-10-16T08:48:20.238+00:00) le: reSt:LEADER voGr:0 cuTerm:0x19
 lCoTe:0x18
   lCoIn:0x1800000000001b2a veFiSt:0x31 veFiEn:0x31 lm(t):3(2014-10-16T08:48:20.120+00:00)

    lastUpdt 2014-10-16T09:08:30.240+00:00
(6,3,2)  st:6 lm(t):1(2014-10-16T08:47:25.323+00:00) le: reSt:FOLLOWER voGr:0 cuTerm:0x19
 lCoTe:0x18
   lCoIn:0x1800000000001b2a veFiSt:0x49 veFiEn:0x49 lm(t):1(2014-10-16T08:48:20.384+00:00)
```

```
 lp: clSt:2
    lm(t):1(2014-10-16T08:47:03.286+00:00) dbSt:2 lm(t):1(2014-10-16T08:47:02.143+00:00)
 stMmt:1
     lm(t):0(zeroTime) dbCrTs:2014-10-16T08:47:02.143+00:00 lastUpdt
2014-10-16T08:48:20.384+00:00
(6,3,3)  st:6 lm(t):2(2014-10-16T08:47:13.576+00:00) le: reSt:FOLLOWER voGr:0 cuTerm:0x19
 lCoTe:0x18
    lCoIn:0x1800000000001b2a veFiSt:0x43 veFiEn:0x43 lm(t):2(2014-10-16T08:48:20.376+00:00)

     lastUpdt 2014-10-16T09:08:30.240+00:00
---------------------------------------------
clusterTime=<diff=65247251 common=2014-10-16T09:08:30.445+00:00
local=2014-10-15T15:01:03.194+00:00
    pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):3(2014-10-16T04:50:08.714+00:00)>>
```



第 6 章

コア ACI ファブリック サービスのプロビジョニング

この章は、次の内容で構成されています。

- リンク レベル ポリシー （151 ページ）
- リンク フラップ ポリシー （153 ページ）
- 時刻同期と NTP （154 ページ）
- DHCP リレー ポリシーの設定 （162 ページ）
- DNS サービス ポリシーの設定 （172 ページ）
- カスタム証明書の設定 （177 ページ）
- ファブリック全体のシステム設定のプロビジョニング （182 ページ）
- グローバル ファブリック アクセス ポリシーのプロビジョニング （212 ページ）
- ポート単位ポリシー （218 ページ）
- GUI を使用した誤配線プロトコル インターフェイス ポリシーの作成（任意） （220 ページ）

リンク レベル ポリシー

アクセス ポリシーの一種であるリンク レベル ポリシーを設定できます。リンク レベル ポリシーには、自動ネゴシエーション、ポート速度、リンク デバウンスなどの物理層（レイヤ 1）インターフェイス設定が含まれます。

電磁場干渉に対する再トレーニング

5.2(4) 以降のリリースには、電磁干渉（EMI）再トレーニング機能があり、電磁干渉からのリンク上のノイズのフィルタリングを行い、リンク フラップを回避するようにリンクを再トレーニングできます。データセンター環境に大量の EMI ノイズが存在する場合は、EMI 再トレーニングを有効にしてください。

リンク レベル ポリシーを構成するときに、EMI 再トレーニング プロパティの有効化を選択することで、EMI再トレーニングを有効にすることができます。この機能は、銅ケーブルを使用

する Cisco N9K-C93108TC-EX および N9K-C93108TC-FX リーフ スイッチでのみサポートされます。

GUI を使用したリンク レベル ポリシーの設定

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）] > [アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）] > [インターフェイス（Interface）] > [リンク レベル（Link Level）]**を選択します。

ステップ 3 **[リンク レベル（Link Level）]** を右クリックし、**[リンク レベル ポリシー（Create Link Level Policy）]** を選択します。

ステップ 4 **[リンク レベル ポリシーの作成（Create Link Level Policy）]** ダイアログで、必要な設定に応じてフィールドに入力します。

[速度（Speed）]には、デフォルト値である [継承（inherit）] を選択することをお勧めします。この値を使用して、Cisco APIC はスイッチに挿入されたトランシーバに基づいて速度を決定します。

フィールドの詳細については、ツールチップを参照してください。

ステップ 5 [Submit] をクリックします。

ポート起動遅延

リリース 4.2（5）から、リンク レベル ポリシーを構成する場合は、ポートの起動時に判定フィードバック イコライザ（DFE）の調整が遅延する時間をミリ秒単位で指定する **[ポート起動遅延（ミリ秒）（Port bring-up delay (milliseconds)）]** パラメータを設定します。遅延は、一部のサードパーティ製アダプタを使用する場合に、リンクの起動中に CRC エラーを回避するために使用されます。遅延は必要な場合にのみ設定してください。ほとんどの場合、遅延を設定する必要はありません。

（注） ファブリック エクステンダ（FEX）ポートでは、**ポートの起動遅延（ミリ秒）**パラメータは適用されません。

リンク レベル ポリシーの制限

Nexus 9408 ACI モード スイッチの N9K-X9400-22L ライン カード上の 50G-SR-S（短距離）トランシーバと 25G-SR-S トランシーバ間で APIC ファブリックへのリンクを起動することはで

きません。これは、リンクの起動に 25G の速度ポリシーを構成し、この組み合わせが N9K スイッチと暗号化された対称キー（ESK）の間でのみ機能するためです。

いずれかのリンクが APIC に接続されている場合、デフォルト ポリシーがリーフ ポートに適用され、速度ポリシーが削除されます。

この動作は 10G-GLCT トランシーバにも適用されるため、APIC の起動に 10G-GLCT トランシーバを使用することはできません。

リンク デバウンス間隔

リンク レベル ポリシーは、リンク レベルでファブリック インターフェイス（リーフ スイッチ アップリンク ポートおよびスパイン スイッチ ポート）に適用され、リンク ノイズまたは一時的なフラップが発生する可能性がある場合にこのポリシーを使用します。3.2(9f) リリース以降、このポリシーでは、リンクにフラップがある場合のファブリック インターフェイスの待機時間を指定するリンク デバウンス間隔を設定できます。間隔が経過すると、 Cisco Application Centric Infrastructure （ACI）はリンクステータスを再度チェックしてイベントを再確認します。この時点でリンクが正常な場合、インターフェイスはアップ状態のままになります。

Cisco Application Policy Infrastructure Controller （APIC）GUI または **[no] link debounce time<time>** CLI コマンドの **[リンク デバウンス間隔（ミリ秒）（Link debounce interval（msec））]** フィールドを使用して、リンク レベル ポリシーの間隔を設定します。デフォルトのデバウンス間隔は 0 ms です。推奨値は 100 ミリ秒ですが、ファブリックに適した値を選択することを推奨します。

リンク フラップ ポリシー

リンク フラップは、スイッチ上の物理インターフェイスが一定期間にわたって継続的にアップおよびダウンする状況です。原因は通常、不良、サポート対象外、または非標準のケーブルまたは Small Form-Factor Pluggable（SFP）に関連しているか、または他のリンク同期の問題に関連しており、原因は断続的または永続的です。

リンク フラップ ポリシーは、リンク フラッピング エラーのためにスイッチ ポートを無効にするタイミングを指定します。リンク フラップ ポリシーでは、スイッチのポートが指定した時間内にフラップできる最大回数を指定します。ポートが指定された時間内に指定された回数以上フラップした場合、ポートは「error-disable」状態になります。Cisco Application Policy Infrastructure Controller（APIC）を使用してポートで手動フラップを実行し、ポートを無効または有効にするまで、ポートはこの状態のままです。

（注） リンク フラップ ポリシーは、ファブリック エクステンダ（FEX）ホスト インターフェイス（HIF）ポート、および製品 ID に -EX、-FX、-FX2、-GX が指定されていないリーフ スイッチ モデルでは適用されません。

GUI を使用したリンク フラップ ポリシーの設定

次の手順では、GUI を使用してリンク フラップ ポリシーを設定します。これを任意のリーフまたはスパイン ノード インターフェイス ポリシーに接続して、ノードのアクセス ポートにリンク フラップ ポリシーを展開できます。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）] > [アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）] > [インターフェイス（Interface）] > [リンク フラップ（Link Flap）]**を選択します。

ステップ 3 **[リンク フラップ（Link Flap）]** を右クリックし、**[リンク フラップ ポリシーの作成（Create Link Flap Policy）]** を選択します。

ステップ 4 **[リンク レベル ポリシーの作成（Create Link Level Policy）]** ダイアログで、必要な設定に応じてフィールドに入力します。

フィールドの詳細については、ツールチップとオンライン ヘルプを参照してください。

ステップ 5 [Submit] をクリックします。

時刻同期と NTP

シスコ アプリケーション セントリック インフラストラクチャ（ACI）ファブリックにおいて、時刻の同期は、モニタリング、運用、トラブルシューティングなどの多数のタスクが依存している重要な機能です。クロック同期は、トラフィック フローの適切な分析にとって重要であり、複数のファブリック ノード間でデバッグとフォールトのタイム スタンプを関連付けるためにも重要です。

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

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

外部パブリック時刻の使用を決定する際は、時刻源の信頼性について慎重に検討する必要があります。

Cisco APIC リリース 6.1(1) より前は、MD5 および SHA-1 認証方式のみがサポートされていました。Cisco APIC リリース 6.1(1) 以降では、AES128-CMAC 認証方式がサポートされています。MD5 は脆弱で安全ではないと考えられるため、AES128-CMAC が推奨される認証方式です。詳細については、RFC 8573 を参照してください。

（注） FIPS モードが有効になっている場合、AES128-CMAC および SHA-1 認証スキームがサポートされます。

インバンドの管理 NTP

（注） インバンド管理アクセスについては、本書の「管理アクセスの追加」という項を参照してください。

- インバンド管理 NTP：ACI ファブリックをインバンド管理とともに展開する場合は、ACI のインバンド管理ネットワーク内から NTP サーバへの到達可能性を検討します。ACI ファブリック内で使用されるインバンド IP アドレッシングには、ファブリックの外部から到達できません。インバンド管理されているファブリックの外部の NTP サーバを使用するには、その通信を可能にするポリシーを作成します。。

（注） スタンバイ APIC の場合、モニタリングまたは NTP ポリシーがインバンドに適用されている場合に障害が発生します。障害をクリアするには、スタンバイ APIC にもインバンド構成が必要です。

NTP over IPv6

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

GUI を使用した NTP の設定

（注） 使用する DNS サーバがインバンドまたはアウトオブバンド接続で到達可能に設定されている場合、ホスト名ベースの NTP サーバのホスト名解決に失敗するリスクがあります。ホスト名を使用する場合は、DNS プロバイダと接続する DNS サービス ポリシーが設定されていることを確認します。また、DNS プロファイル ポリシーの設定時に選択した管理 EPG のインバンドまたはアウトオブバンド VRF インスタンスに適切な DNS ラベルが設定されていることを確認します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]**を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[ポッド（Pod）]** > **[日付と時刻（Date and Time）]**を選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Date and Time Policy]** の順に選択します。

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

a) 環境内のさまざまな NTP 設定を区別するポリシーの名前を入力します。

b) をクリックして **有効になっている** の **認証状態** フィールドおよび展開、 **NTP クライアントの認証キー** テーブルが表示され、重要な情報を入力します。

c) [+] をクリックすると、新しいキーを作成できます。 **ID**、 **キー**を入力し、[信頼済み（**Trusted**）] 列のチェックボックス（True）を選択し、[認証タイプ（**Authentication Type**）] のアルゴリズムを選択します。ドロップダウンリストで使用可能なオプションは、SHA-1、MD5、AES128-CMAC のアルゴリズムです。

d) **Update** と **Next** をクリックします。

e) [+] 記号をクリックし、使用する NTP サーバ情報（プロバイダー）を指定します。

f) [Create Providers] ダイアログボックスで、次のフィールドを含めて、すべての関連情報を入力します。[Name]、[Description]、[Minimum Polling Intervals]、[Maximum Polling Intervals]。

- 複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の [Preferred] チェックボックスをオンにします。
- ファブリックのすべてのノードがアウトオブバンド管理によって NTP サーバに到達できる場合は、**[管理 EPG（Management EPG）]** ドロップダウン リストで、[アウトオブバンド（Out-of-Band）] を選択します。インバンド管理を導入した場合は、インバンド管理 NTP の詳細を参照してください。[OK] をクリックします。

作成するプロバイダーごとに、この手順を繰り返します。

ステップ 5 [Navigation] ペインで、**[Pod Policies]** > **[Policy Groups]** の順に選択します。

ステップ 6 [Work] ペインで、**[Actions]** > **[Create Pod Policy Group]** の順に選択します。

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

a) ポリシー グループの名前を入力します。

b) **[日付と時刻のポリシー（Date Time Policy）]** フィールドのドロップダウン リストから、前に作成した NTP ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが作成されます。または、デフォルトのポッド ポリシー グループを使用することもできます。

ステップ 8 **[ナビゲーション（Navigation）]** ペインで、**[ポッド ポリシー（Pod Policies）]** > **[プロファイル（Profiles）]**を選択します。

ステップ 9 [Work] ペインで、目的のポッド セレクタ名をダブルクリックします。

ステップ 10 [プロパティ（Properties）] エリアの **[ファブリック ポリシー グループ（Fabric Policy Group）]** ドロップダウン リストから、作成したポッド ポリシー グループを選択します。[Submit] をクリックします。

REST API を使用した NTP の設定

（注） 使用する DNS サーバがインバンドまたはアウトオブバンド接続で到達可能に設定されている場合、ホスト名ベースの NTP サーバのホスト名解決に失敗するリスクがあります。ホスト名を使用する場合は、DNS プロバイダと接続する DNS サービス ポリシーが設定されていることを確認します。また、DNS プロファイル ポリシーの設定時に選択した管理 EPG のインバンドまたはアウトオブバンド VRF インスタンスに適切な DNS ラベルが設定されていることを確認します。

手順

ステップ 1 NTP を設定します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/time-test.xml

<imdata totalCount="1">
    <datetimePol adminSt="enabled" authSt="disabled" descr=""
dn="uni/fabric/time-CiscoNTPPol" name="CiscoNTPPol" ownerKey="" ownerTag="">
        <datetimeNtpProv descr="" keyId="0" maxPoll="6" minPoll="4" name="10.10.10.11"
preferred="yes">
            <datetimeRsNtpProvToEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
        </datetimeNtpProv>
    </datetimePol>
</imdata>
```

ステップ 2 デフォルトの日付と時刻のポリシーをポッド ポリシー グループに追加します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/funcprof/podpgrp-calo1/rsTimePol.xml

POST payload: <imdata totalCount="1">
<fabricRsTimePol tnDatetimePolName="CiscoNTPPol">
</fabricRsTimePol>
</imdata>
```

ステップ 3 ポッド ポリシー グループをデフォルトのポッド プロファイルに追加します。

例：

```
POST url:
https://APIC-IP/api/node/mo/uni/fabric/podprof-default/pods-default-typ-ALL/rspodPGrp.xml

payload: <imdata totalCount="1">
<fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-calo1" status="created">
</fabricRsPodPGrp>
</imdata>
```

GUI を使用した NTP の動作の確認

手順

ステップ 1 メニュー バーで、**[FABRIC]** > **[Fabric Policies]** を選択します。

ステップ 2 [Navigation] ペインで、**[Pod Policies]** > **[Policies]** > **[Date and Time]** > ***[ntp_policy]*** > ***[server_name]*** の順に選択します。

ntp_policy は前に作成したポリシーです。[Host Name] フィールドまたは [IP address] フィールドでは IPv6 アドレスがサポートされます。入力したホスト名に IPv6 アドレスが設定されている場合、IPv6 アドレスが IPv4 アドレスより優先されるように実装する必要があります。

ステップ 3 [Work] ペインで、サーバの詳細を確認します。

NTPサーバ

NTP サーバ機能は、クライアントのスイッチも NTPサーバとして動作して、下流のクライアントに NTP の時間情報を提供できるようにします。NTP サーバを有効にすると、スイッチ上の NTP デーモンは、NTP クライアントからのすべてのユニキャスト (IPv4 または IPv6) リクエストに対し、が時間情報によって応答します。NTP サーバの実装は、NTP RFCv3 に準拠しています。NTP RFC に従い、サーバはクライアントに関連する状態情報は維持しません。

- NTP サーバーは、すべてのテナント VRF とインバンド/アウトオブバンド管理 VRF の IP アドレスを有効にして、NTP クライアントにサービスを提供します。
- NTP サーバーは、両方の管理 VRF またはテナント VRF に着信した NTP 要求に応答し、同じ VRF を使用して応答を返します。

- NTP サーバはIPv4 と IPv6 の両方をポートします。
- スイッチは、IPv4 クライアントとして同期して IPv6 サーバとして動作すること、およびその逆が可能です。
- スイッチは、アウトオブバンド管理またはインバンド管理 VRF を使用して NTP クライアントとして同期でき、管理 VRF またはテナント VRF のいずれかから NTP クライアントにサービスを提供します。
- 追加コントラクトまたは IP テーブルの設定は必要ありません。
- スイッチは上流のサーバと同期すると、サーバとして時間情報をストラタム番号とともに送信します。この番号はシステムのピアのストラタム番号から 1 増えたものになります。
- スイッチ クロックが非統制 (アップストリーム サーバに同期されていない) の場合、サーバはストラタム 16 で時間情報を送信します。クライアントはこのサーバには同期できません。

デフォルトでは、NTP サーバ 機能は無効になっています。これはポリシーの設定によって明示的に有効にする必要があります。

（注） クライアントは、リーフ スイッチのインバンド、アウトオブ バンドの IP アドレスを NTP サーバ IP アドレスとして使用できます。クライアントはまた、自身が一部となっている EPG のブリッジ ドメイン SVI または任意の L3Out IP アドレスを、ファブリック外のクライアントの NTP サーバー IP アドレスとして使用できます。

ファブリックのスイッチは、同じファブリックの他のスイッチに同期するべきではありません。ファブリック スイッチは常に、外部の NTP サーバに同期するべきです。

GUI を使用した NTP サーバの有効化

このセクションでは、APIC GUI で NTP を設定して NTPサーバを有効にする方法について説明します。

手順

ステップ 1 メニュー バーで、**FABRIC** > **Fabric Policies** を選択します。

ステップ 2 **ナビゲーション** ウィンドウで、**Pod Policies** > **Policies** を選択します。

Date and Time オプションが **Navigation** ウィンドウに表示されます。

ステップ 3 **Navigation** ウィンドウで、、**Date and Time** を右クリックして **Create Date and Time Policy** を選択します。

Create Date and Time Policy ダイアログが **Work** ウィンドウに表示されます。

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

a) 環境内のさまざまな NTP 設定を区別するポリシーの名前を入力します。
b) **Server State** オプションで、**enabled** をクリックします。

Server State によって、スイッチを NTP サーバとして動作し、下流のクライアントに NTP 時間情報を提供できるようにします。

（注）
サーバ機能をサポートする場合、サーバは常にピア設定にすることを推奨します。これにより、サーバはクライアントに対し、一貫した時間を提供できるようになります。

Server State を有効にすると、次のことが可能になります:

- NTP サーバは、上流のサーバに同期するスイッチに対し、時刻情報とともにストラタム番号を送信します。この番号はシステムのピアのストラタム番号から 1 つ増えたものになります。
- スイッチのクロックが上流サーバに同期していない場合、サーバは時刻情報とストラタム 16 を送信します。クライアントはこのサーバに同期することはできません。

（注）
サーバ機能をサポートする場合、サーバは常にピア設定にすることを推奨します。ピア設定では、クライアントに対し一貫した時間を提供できます。

c) **Master Mode** オプションで、**enabled** をクリックします。

Master Mode を使用すれば、指定された NTP サーバが、下流のクライアントに対し、設定されたストラタム番号とともに、調整されていないローカルクロック時刻を提供することが可能になります。たとえば、NTP サーバとして動作しているリーフスイッチは、クライアントとして動作しているリーフスイッチに対し、調整されていないローカルクロック時刻を提供できます。

（注）
- **Master Mode** が適用できるのは、サーバのクロックが調整されていない場合のみです。
- デフォルトのマスター モードの **Stratum Value** は 8 です。

d) **Stratum Value** フィールドには、NTP クライアントが同期した時刻を取得するときのストラタム番号を指定します。範囲は 1 ～ 14 です。
e) **Next** をクリックします。
f) [+] 記号をクリックし、使用する NTP サーバ情報（プロバイダー）を指定します。
g) [Create Providers] ダイアログボックスで、次のフィールドを含めて、すべての関連情報を入力します。[Name]、[Description]、[Minimum Polling Intervals]、[Maximum Polling Intervals]。
   - 複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の [Preferred] チェックボックスをオンにします。
   - ファブリックのすべてのノードがアウトオブバンド管理によって NTP サーバに到達できる場合は、[Management EPG] ドロップダウン リストで、[Out-of-Band] を選択しま

す。インバンド管理を導入した場合は、インバンド管理NTPの詳細を参照してください。[OK] をクリックします。

作成するプロバイダーごとに、この手順を繰り返します。

ステップ 5 **Navigation** ウィンドウで、**Pod Policies** を選択し、**Policy Groups** を右クリックします。

Create Pod Policy Group ダイアログが表示されます。

ステップ 6 [Work] ペインで、**[Actions]** > **[Create Pod Policy Group]** の順に選択します。

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

a) ポリシー グループの名前を入力します。

b) [Date Time Policy] フィールドのドロップダウン リストから、前に作成した NTP ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが作成されます。または、デフォルトのポッド ポリシー グループを使用することもできます。

ステップ 8 [Navigation] ペインで、**[Pod Policies]** > **[Profiles]** の順に選択します。

ステップ 9 [Work] ペインで、目的のポッド セレクタ名をダブルクリックします。

ステップ 10 [Properties] 領域の [Fabric Policy Group] ドロップダウン リストから、作成したポッド ポリシー グループを選択します。

ステップ 11 [Submit] をクリックします。

GUI を使用した日時形式の設定

ここでは、Cisco APIC GUI を使用して日時形式を設定する方法を示します。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[システム設定（System Settings）]** を選択します。

ステップ 2 ナビゲーションペインで **[日付と時間（Date and Time）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、次のオプションから選択します。

- **[表示形式（Display Format）]**：**[local]** をクリックして日時を現地時間で表示するか、**[utc]** をクリックして日時を UTC で表示します。デフォルトは **[local]** です。
- **[タイムゾーン（Time Zone）]**：ドロップダウン矢印をクリックして、ドメインのタイムゾーンを選択します。デフォルトは **[協定世界時（Coordinated Universal Time）]** です。

- **[オフセット状態（Offset State）]**：**[有効（enable）]** または **[無効（disable）]** をクリックします。有効にすると、ローカル時刻と基準時刻の差が表示されます。デフォルトは **[有効（enable）]** です。

DHCP リレー ポリシーの設定

DHCP リレー ポリシーは、DHCP クライアントとサーバが異なるサブネット上にある場合に使用できます。

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

オプション 79：DHCPv6 のクライアント リンク層アドレス オプション

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(4) 以降、DHCPv6 オプション 79 を含むように DHCP リレー エージェントとして構成されたブリッジ ドメインを構成できるようになりました。オプション 79 が有効になっている場合、ブリッジ ドメインがリレー エージェントとして設定されているリーフ スイッチには、DHCPv6 リレー パケットのオプション 79 を介してクライアントのリンク層アドレスが含まれます。

オプション 79 を選択すると、DHCP パケットのペイロードにクライアントの MAC アドレス (クライアント リンク層アドレス) が含まれるようになります。オプション 79 には、デバイスの実際のリンク層アドレスが含まれています。リレー メッセージは、クライアントから送信される実際の DHCP パケットのイーサネット送信元 MAC アドレスを使用し、イーサネット ソースを示す 00:01 のプレフィックスを付けてから、これらの 8 バイト（クライアント MAC アドレス）をオプション 79 にコピーします。

DHCPv6 のクライアント リンク層アドレス オプションの詳細については、*RFC 6939* を参照してください。

オプション 79 を使用する利点

デュアルスタック シナリオ（IPv6 と IPv4 をサポート）では、DHCPv4 および DHCPv6 メッセージを同じクライアント インターフェイスに関連付ける必要がある場合、オプション 79 は、RFC 標準に準拠して、DHCPv6 リレー パケットにクライアント MAC アドレスを含めて送信します。

DHCP サーバー設定フィールドについて

（注） 以下は、このセクションで使用されるいくつかの用語の定義です。

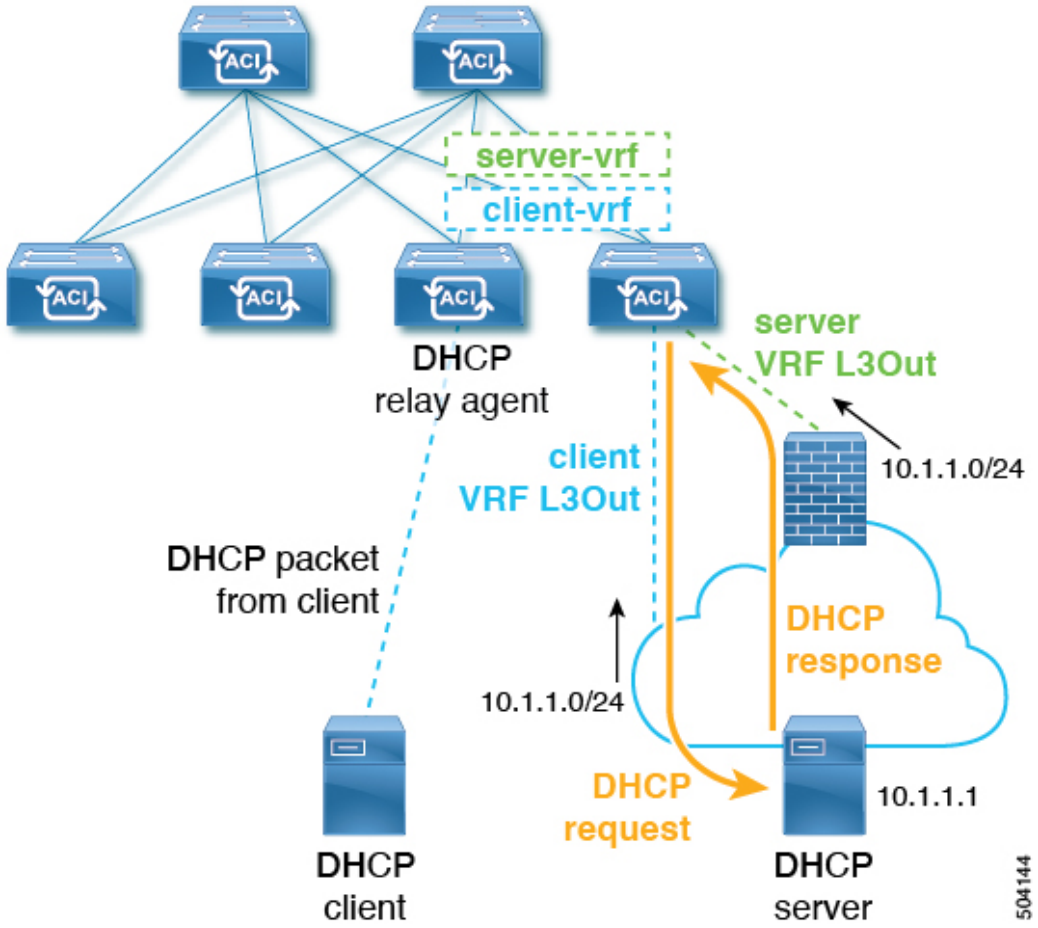
- **クライアント VRF**：DHCP 要求を開始するホストが配置されている VRF。
- **サーバ VRF**：DHCP サーバが配置されている VRF インスタンス、または DHCP サーバに（たとえば L3Out 経由で）到達するためのパスを提供する VRF インスタンス。
- **クライアント EPG**：DHCP 要求を開始するホストが配置されている EPG。
- **サーバ EPG**：DHCP サーバが接続されている EPG（または、DHCP サーバが Cisco ACI ファブリックの外部にある場合は外部 EPG）。

Cisco APICリリース 5.2(4) では、DHCP リレー プロバイダーの設定時の `use-vrf` オプションのサポートが追加されています。この機能は、DHCP プロバイダ EPG（たとえば、DHCP サーバが接続されている EPG）または、DHCP サーバに到達するために使用されるレイヤ 3 外部ネットワークが、DHCP 要求を開始するホストが存在するブリッジ ドメイン（DHCP ポリシーを DHCP リレー ラベルとして参照しているブリッジ ドメイン）とは異なる VRF インスタンスにある場合に使用されます。この機能は、NX-OS で使用可能な DHCP リレー `use-vrf` オプションに相当します。`use-vrf` オプションが DHCP リレー プロバイダに対して有効になっている場合、DHCP クライアントが配置されているリーフ スイッチは、DHCP クライアントの VRF インスタンスの代わりに、構成された DHCP プロバイダ EPG （または、DHCP サーバに到達できるように構成された L3Out）の VRF インスタンスを経由して、DHCP リレーパケットをルーティングします。

リリース 5.2(4) より前の Cisco APIC リリースでは、EPG 内、または DHCP クライアントが存在する VRF インスタンスとは異なる VRF インスタンスの レイヤ 3 外部ネットワークでの DHCP リレー プロバイダ（サーバ）の指定をサポートしています。この VRF 間リレー ポリシーは、VRF 間コントラクトに依存しており、また DHCP サーバへ到達可能な VRF インスタンス（**サーバ VRF** とも呼ばれる）から DHCP クライアントが存在する VRF インスタンス（**クライアント VRF** とも呼ばれる）への DHCP サーバ ネットワークのルート リークにも依存しています。DHCP リレー パケットはクライアント VRF インスタンスからルーティングされ、VRF 間ルート リークを使用して、サーバ VRF インスタンスから DHCP サーバに到達します。一部のシナリオでは、DHCP サーバ ネットワークがクライアント VRF インスタンスからも到達できる場合（たとえば、DHCP サーバ ネットワークにも到達できるクライアント VRF インスタンスにローカル L3Out がある場合）、DHCP リレー パケットがサーバ VRF インスタンスをバイパスすることがあります。DHCP リレー ポリシー プロバイダが、クライアント VRF インスタンスの 1 つとは異なるレイヤ 3 外部ネットワークを使用するように構成されている場合、DHCP リレー パケットのソース IP アドレスは、サーバ VRF インスタンスの L3Out（**プロバイダ L3Out** とも呼ばれる）から選択されます。これらの DHCP リレー パケットが、サーバ VRF インスタンス の L3Out ではなくクライアント VRF インスタンス の L3Out からルーティングされる場合（クライアント VRF インスタンス の L3Out も DHCP サーバへのルートを持っている場合に生じる可能性があります）、DHCP サーバの応答はサーバ VRF インスタンスの L3Out に送り返されます。 DHCP リレー パケットの IP アドレスが、サーバ VRF インスタンスの L3Out の IP アドレスに構成されているためです。これにより、DHCP リレーパケットの非対称転送が発生

し、ファイアウォールなどのステートフル デバイスによってドロップされる可能性があります。

次の図は、このシナリオの例を示しています。



このシナリオ例では、外部 DHCP サーバ ネットワークは、クライアントとサーバの両方の VRF インスタンスを介して、ACI ファブリックで到達可能です。DHCP リレー パケットは、クライアント VRF インスタンスからルーティングされ、クライアント VRF インスタンスの L3Out 経由で送信されます。DHCP リレー パケットの送信元 IP アドレスは、DHCP リレー ポリシーに従って、サーバ VRF インスタンスの L3Out から選択されます。サーバーからの DHCP リレー応答は DHCP サーバー L3Out にルーティングされるため、非対称フローになります。

この問題を解決するため、リリース 5.2(4) 以降では、**[サーバー VRF を使用（Use Server VRF）]** というオプションが、**[DHCP サーバー設定（DHCP Server Preference）]** フィールドで使用できるようになりました。**[サーバ VRF を使用（Use Server VRF）]** オプションを有効にすると、DHCP リレー パケットは常にサーバ VRF インスタンスからルーティングされます。このオプションは、VRF 間コントラクトとルート リークの要件も削除します。

[DHCP サーバ設定（DHCP Server Preference）] フィールドで選択したオプションに基づいて、リーフ スイッチは、DHCP リレー パケットをクライアント VRF インスタンスまたはサーバ VRF インスタンスのどちらからルーティングするかを決定します。

- **[なし（None）]**: これはデフォルトのオプションで、リリース 5.2(4) より前の動作を反映しています。**[なし（None）]**オプションを選択すると、スイッチは常にクライアント VRF インスタンスから DHCP リレー パケットをルーティングします。VRF 間 DHCP リレーに使用する場合、サーバ VRF インスタンス ネットワークをクライアント VRF インスタンスにリークするには、共有サービス コントラクトが必要です。
- **[サーバー VRF を使用（Use Server VRF）]**: このオプションは、リリース 5.2(4) で導入された新しい動作を反映しています。**[サーバ VRF を使用（Use Server VRF）]** オプションを選択すると、スイッチは、DHCP クライアントが存在する EPG と DHCP サーバが存在する EPG（または DHCP サーバが到達可能な L3Out のレイヤー 3 外部）の間にコントラクトがあるかどうかには関わりなく、サーバ VRF インスタンスからの DHCP リレー パケットをルーティングします。

  VRF 間構成の場合、**[DHCP サーバ設定（DHCP Server Preference）]** フィールドで **[サーバ VRF を使用（Use Server VRF）]** オプションを選択すると、ルート ルックアップのため、サーバ サブネット ルートは、クライアント リーフ スイッチのサーバ VRF インスタンス内でプログラムされます。クライアント リーフ スイッチの DHCP プロセスは、それ以後、DHCP リレー パケットをサーバ VRF インスタンス経由で送信します。このため、サーバ VRF インスタンスを、クライアント ブリッジ ドメインが展開されているすべてのリーフ スイッチ上に、少なくとも 1 つの IP アドレスを使用して展開しておく必要があります。

DHCP リレー ポリシーの注意事項と制約事項

- インフラまたは共通テナントで作成された DHCP リレー ポリシーは、ブリッジ ドメインで DHCP リレーを設定するときに他のテナントで使用できません。テナント間 DHCP リレー通信の場合は、グローバル DHCP リレー ポリシーの作成（214 ページ） の説明に従ってグローバル DHCP リレー ポリシーを作成します。
- DHCP リレー IP アドレスは、常にプライマリ SVI IP アドレスに設定されます。
- クライアントとサーバーが L3Out EPG を介して接続されている場合は、DHCP リレーポリシーを使用できません。クライアントまたはサーバーのいずれか（または両方）が通常の（非 L3Out）EPG に存在する必要があります。
- DHCP リレー プロバイダ EPG が L3Out 外部 EPG であり、クライアント ブリッジ ドメインとは異なる VRF インスタンスで構成されている場合、DHCP リレーパケットは、L3Out で構成された各インターフェイスから送信されます。これには、ノードのルータ ID アドレスとすべての L3Out インターフェイス IP アドレスが含まれます。
- L3Out SVI またはフローティング SVI が DHCP リレー エージェントとして構成されている場合、（DHCP リレー ラベル）DHCP サーバ/プロバイダは、L3Out SVI が展開されているのと同じリーフ スイッチに接続しないでください。フローティング SVI の場合、これにはすべてのアンカー スイッチと非アンカー スイッチが含まれます。

GUI を使用した APIC インフラストラクチャに対する DHCP サーバ ポリシーの設定

この手順では、エンドポイント グループ（EPG）の DHCP リレー ポリシーを展開します。

次の注意事項および制約事項を確認します。

- アプリケーション エンドポイント グループで使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインにそれらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。
- シスコ APIC では、プライマリ IP アドレス プールに対してのみ DHCP リレーをサポートしています。
- 次の注意事項と制約事項は、リリース 5.2(4) で導入された **[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールドに適用されます。
  - L3Out 用に DHCP リレーが設定されている場合（たとえば、DHCP サーバーが L3Out の背後にあり、DHCP リレー ポリシーが **[サーバー VRF を使用（Use Server VRF）]** オプションに設定されている場合（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールドにおいて））、EPG/サーバー VRF にインターフェイスがまだ存在しなければ、クライアント ブリッジ ドメインが展開されているリーフ スイッチへ EPG/ブリッジ ドメイン/ブリッジ ドメイン サブネットを展開する必要があります。
  - EPG の背後にある DHCP サーバーに対して、DHCP リレー ポリシーが **[サーバー VRF を使用（Use Server VRF）]** オプションに設定されている場合（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）、IPv4 および IPv6 ルートの両方と、サーバ ブリッジ ドメイン SVI がクライアント リーフ スイッチに作成されます。
  - **[サーバー VRF を使用（Use Server VRF）]** オプションは、サイト間 DHCP トラフィックではサポートされていません。
- オプション 79 には、以下の制限が適用されます。
  - オプション 79 は DHCPv6 でのみサポートされています。
  - オプション 79 はインフラ テナントではサポートされていません。

始める前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenant）]** > *[テナント名（tenant_name）]* を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインの **[テナント（Tenant）]** *[テナント名（tenant_name）]* の下で、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[DHCP]**を展開します。

ステップ 3 [Relay Policies] を右クリックし、[Create DHCP Relay Policy] をクリックします。

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

a) [Name] フィールドに、DHCP リレー プロファイル名（DhcpRelayP）を入力します。

この名前では最大 64 文字までの英数字を使用できます。

b) （任意） [説明（Description）] フィールドに、DHCP リレー ポリシーの説明を入力します。

説明には最大 128 文字までの英数字を使用できます。

c) [Providers] を展開します。

[DHCP プロバイダーの作成（Create DHCP Provider）] ダイアログボックスが表示されます。

d) [Create DHCP Provider] ダイアログボックスの [EPG Type] フィールドで、DHCP サーバがどこで接続されているかによって適切なオプション ボタンをクリックします。

選択する EPG タイプのオプションは、EPG タイプによって異なります。

- EPG タイプとして **[アプリケーション EPG（Application EPG）]** を選択すると、次のオプションが **[アプリケーション EPG（Application EPG）]** 領域に表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。（infra）
  - [Application Profile] フィールドで、ドロップダウン リストから、アプリケーションを選択します。（access）
  - [EPG] フィールドで、ドロップダウン リストから、EPG を選択します。（デフォルト）
- EPG タイプとして **[L2 外部ネットワーク（L2 External Network）]** を選択すると、**[L2 外部ネットワーク領域（L2 External Network）]** に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L2 Out]** フィールドで、ドロップダウン リストから [L2 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。

- EPG タイプとして **[L3 外部ネットワーク（L3 External Network）]** を選択すると、**[L3 外部ネットワーク（L3 External Network）]**領域に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L3 Out]** フィールドで、ドロップダウン リストから [L3 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。
- EPG タイプとして **[DN]** を選択した場合は、ターゲット エンドポイント グループの識別名を入力します。

e) [DHCP サーバ アドレス（DHCP Server Address）] フィールドに、DHCP サーバの IP アドレスを入力します。

f) **[DHCP サーバー プレファレンス（DHCP Server Preference）]**フィールドで、このプロバイダーの管理設定値を選択します。

[DHCP サーバー プレファレンス（DHCP Server Preference）] フィールドは、リリース 5.2(4) 以降で使用できます。リーフ スイッチは、このフィールドの値を基に、クライアント VRF またはサーバー VRF のどちらから DHCP リレー パケットをルーティングするかを決定します。詳細については、DHCP サーバー設定フィールドについて （163 ページ）を参照してください。

- **[なし（None）]** : これはデフォルトのオプションで、リリース 5.2(4) より前の動作を反映しています。**[なし（None）]** オプションを選択すると、スイッチは常にクライアント VRF からの DHCP リレー パケットをルーティングします。VRF 間 DHCP リレーに使用する場合、サーバー VRF ネットワークをクライアント VRF にリークするには、共有サービス コントラクトが必要です。
- **[サーバー VRF を使用（Use Server VRF）]** : このオプションは、リリース 5.2(4) で導入された新しい動作を反映しています。**[サーバー VRF を使用（Use Server VRF）]** オプションを選択すると、スイッチは、DHCP クライアントが存在する EPG と DHCP サーバーが存在する EPG（またはDHCP サーバーが到達可能な L3Out のレイヤー 3 外部）の間にコントラクトがあるかどうかには関わりなく、サーバー VRF からの DHCP リレー パケットをルーティングします。

  VRF 間設定の場合、**[サーバー VRF を使用（Use Server VRF）]** オプション（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）を選択すると、ルート ルックアップのため、サーバー サブネット ルートは、クライアント リーフ スイッチのサーバ - VRF 内でプログラムされます。クライアント リーフ スイッチの DHCP プロセスは、それ以後、DHCP リレー パケットをサーバー VRF 経由で送信します。このため、サーバー VRF は、クライアント ブリッジ ドメインが展開されているすべてのリーフ スイッチに少なくとも 1 つの IP アドレスを使用して展開する必要があります。

g) [OK] をクリックします。

[**DHCP リレー ポリシーの作成（Create DHCP Relay Policy）]** ウィンドウに戻ります。

h) [Submit] をクリックします。

DHCP リレー ポリシーが作成されます。

ステップ 5

ステップ 6 [Navigation] ペインで、**[Networking]** > **[Bridge Domains]** > **[default]** > **[DHCP Relay Labels]** を展開します。

ステップ 7 [DHCP Relay Labels] を右クリックし、[Create DHCP Relay Label] をクリックします。

ステップ 8 [Create DHCP Relay Label] ダイアログボックスで、次の操作を実行します。

a) [Scope] フィールドで、テナントのオプション ボタンをクリックします。
このアクションにより、[Name] フィールドのドロップダウン リストに、以前に作成した DHCP リレー ポリシーが表示されます。

b) [Name] フィールドのドロップダウン リストから、作成済みの DHCP ポリシーの名前（DhcpRelayP）を選択するか、[Create DHCP Relay Policy] を選択して新しいリレー ポリシーを作成します。

c) [DHCP Option Policy] で、既存のオプション ポリシーを選択するか、[Create DHCP Option Policy] を選択して新しいオプション ポリシーを作成します。

オプション 79 を呼び出すには、**ID** として 79 を使用して以前に作成した DHCP オプション ポリシーを選択します。

新しいオプション ポリシーを作成する場合は、**[DHCP オプションポリシー作成（Create DHCP Option Policy）]** ウィンドウの **[オプション（Options）]** ペインで、**ID** として 79 を入力してください。

d) [Submit] をクリックします。

DHCP サーバがブリッジ ドメインに関連付けられます。

ステップ 9 [Navigation] ペインで、**[Networking]** > **[Bridge Domains]** > **[default]** > **[DHCP Relay Labels]** を展開し、作成された DHCP サーバを表示します。

REST API を使用してオプション 79 を設定する

REST API を使用して DHCP オプション ポリシーのオプション 79 を設定するには：

```
POST URL: https://apic-ip-address/api/mo/uni.xml

<dhcpOptionPol dn="uni/tn-dhcp_client/dhcpoptpol-dhcp_option_policy"
name="dhcp_option_policy" status="">
<dhcpOption data="" id="79" name="option_79"/>
</dhcpOptionPol>
```

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

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

始める前に

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

手順

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

例：

エンドポイント グループの DHCP リレー ポリシー

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

例：

レイヤ 3 Outside の DHCP リレー ポリシー

```
ifav28-ifc2(config)# tenant dhcpTn
ifav28-ifc2(config-tenant)# template dhcp relay policy DhcpRelayPol
ifav28-ifc2(config-tenant-template-dhcp-relay)# ip address 11.1.1.11 tenant dhcpTn application ap epg serverEpg
ifav28-ifc2(config-tenant-template-dhcp-relay)# exit
ifav28-ifc2(config-tenant)# exit
ifav28-ifc2(config)# leaf 2001
ifav28-ifc2(config-leaf)# interface ethernet 1/4
ifav28-ifc2(config-leaf-if)# no switchport
ifav28-ifc2(config-leaf-if)# vrf member tenant dhcpTn vrf v1
ifav28-ifc2(config-leaf-if)# dhcp relay policy tenant DhcpRelayPol
ifav28-ifc2(config-leaf-if)# exit
```

GUI を使用した APIC インフラストラクチャ用 DHCP サーバ ポリシーの設定

- このタスクは、vShield ドメイン プロファイルを作成するユーザの前提条件です。
- アプリケーション エンドポイント グループで使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインにそれらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

始める前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順

インフラストラクチャ テナントの DHCP サーバ ポリシーとして APIC を設定します。

（注）
このリレー ポリシーは、接続エンティティ プロファイルの設定を使用した接続されたハイパーバイザであるすべてのリーフ ポートにプッシュされます。接続エンティティ プロファイルによる設定の詳細については、VMM ドメイン プロファイルの作成に関連する例を参照してください。

例：

EPG の DHCP リレー ポリシー

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST https://apic-ip-address/api/mo/uni.xml


  <fvTenant name="infra">

    <dhcpRelayP name="DhcpRelayP"  owner="tenant">
      <dhcpRsProv tDn="uni/tn-infra/ap-access/epg-default" addr="10.0.0.1" />
    </dhcpRelayP>

    <fvBD name="default">
      <dhcpLbl name="DhcpRelayP" owner="tenant"/>
    </fvBD>

  </fvTenant>
</polUni>
```

例：

レイヤ 3 Outside の DHCP リレー ポリシー

（注）
l3extLIfP で適切な名前とオーナーを使用して DHCP リレー ラベルを指定する必要があります。

```
<polUni>
  <fvTenant name="dhcpTn">
    <l3extOut name="Out1" >
      <l3extLNodeP name="NodeP" >
        <l3extLIfP name="Intf1">
           <dhcpLbl name="DhcpRelayPol" owner="tenant" />
       </l3extLIfP>
     </l3extLNodeP>
   </l3extOut>
 </fvTenant>
<polUni>

POST https://apic-ip-address/api/mo/uni.xml
```

例：

DHCP サーバー プリファレンスを [サーバー VRF を使用] オプションに設定する

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST https://apic-ip-address/api/mo/uni.xml

<dhcpRelayP descr="" dn="uni/tn-dhcp_client/relayp-dhcp_relay_pol" status="">
    <dhcpRsProv addr="100.1.1.1/24" pref="use-server-vrf"
tDn="uni/tn-dhcp_server/ap-ap_server/epg-epg_server"/>
</dhcpRelayP>
```

例：

DHCP サーバー プリファレンスを [なし] オプションに設定する

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST https://apic-ip-address/api/mo/uni.xml

<dhcpRelayP descr="" dn="uni/tn-dhcp_client/relayp-dhcp_relay_pol" status="">
    <dhcpRsProv addr="100.1.1.1/24" pref=""
tDn="uni/tn-dhcp_server/ap-ap_server/epg-epg_server"/>
</dhcpRelayP>
```

DNS サービス ポリシーの設定

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

す。ACI ファブリックの DNS ポリシーを設定するには、次のタスクを完了する必要があります。

- 管理 EPG が DNS ポリシー用に設定されていることを確認してください。設定されていない場合、このポリシーはスイッチで有効になりません。

（注） 管理 EPG では、デフォルトの DNS ポリシーのみがサポートされます。

- DNS プロバイダーと DNS ドメインに関する情報が含まれる DNS プロファイル（デフォルト）を作成します。
- DNS プロファイル（デフォルトまたは別の DNS プロファイル）の名前を必要なテナントで DNS ラベルに関連付けます。

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

インバンド DNS サービス ポリシーによる外部宛先の設定

次のように、サービスに対して外部宛先を設定します。

ソース	インバンド管理	アウトオブバンド管理	外部サーバの場所
APIC	IP アドレスまたは完全修飾ドメイン名（FQDN）	IP アドレスまたは FQDN	Anywhere
リーフ スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	Anywhere

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

次に示すのは、外部サーバのリストです。

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

推奨されるガイドラインは次のとおりです。

- 外部サーバは、リーフ アクセス ポートに接続する必要があります。
- 管理ポートの追加の配線を避けるために、リーフ スイッチにはインバンド接続を使用します。
- スパイン スイッチにはアウトオブバンド管理接続を使用します。スパイン スイッチとリーフ スイッチが外部サーバの同じセットに到達できるように、スパイン スイッチのこのアウトオブバンド ネットワークをインバンド管理の仮想ルーティングおよび転送（VRF）機能があるリーフ ポートの 1 つに接続します。
- 外部サーバには IP アドレスを使用します。

デュアル スタック IPv4 および IPv6 DNS サーバ

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

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

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

より一般的な環境では、デュアルスタック IPv4 および IPv6 DNS サーバを使用します。デュアルスタックの場合、IPv4 と IPv6 の両方が /etc/resolv.conf にリストされます。ただし、デュアルスタック環境で、単純に IPv6 DNS サーバをリストに追加すると、DNS 解決の大きな遅延を引き起こす可能性があります。これは、デフォルトで IPv6 プロトコルが優先されるため、IPv4 DNS サーバに接続できないためです (/etc/resolv.conf で最初にリストされている場合) 。この解決法は、IPv4 DNS サーバの前に IPv6 DNS サーバをリストすることです。また、IPv4 と IPv6 両方のルックアップで同一ソケットを使用できるようにするために、「options single-request-reopen」を追加します。

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

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

デュアル スタック IPv4 および IPv6 環境

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

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

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

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

DNS プロファイルの IPv4 または IPv6 の優先順位のポリシー

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

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

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

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

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

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

GUI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定

始める前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順

ステップ 1 メニュー バーで、**[FABRIC]** > **[Fabric Policies]** を選択します。[Navigation] ペインで、**[Global Policies]** > **[DNS Profiles]** を展開し、デフォルトの DNS プロファイルをクリックします。

ステップ 2 [Work] ペインの [Management EPG] フィールドで、ドロップダウン リストから、適切な管理 EPG （デフォルト（Out-of-Band））を選択します。

ステップ 3 [DNS Providers] を展開し、次の操作を実行します。

a) [Address] フィールドに、プロバイダー アドレスを入力します。

b) [Preferred] カラムで、優先するプロバイダーとしてこのアドレスが必要な場合は、チェックボックスをオンにします。

優先するプロバイダーは 1 つだけ指定できます。

c) [Update] をクリックします。

d) （任意）セカンダリ DNS プロバイダーを追加するには、[DNS Providers] を展開し、[Address] フィールドで、プロバイダー アドレスを入力します。[Update] をクリックします。

ステップ 4 [DNS Domains] を展開し、次の操作を実行します。

a) [Name] フィールドに、ドメイン名（cisco.com）を入力します。
b) [Default] カラムで、チェックボックスをオンにしてこのドメインをデフォルト ドメインにします。

デフォルトとして指定できるドメイン名は 1 つだけです。

c) [Update] をクリックします。
d) （任意）セカンダリ DNS ドメインを追加するには、[DNS Domains] を展開します。[Address] フィールドに、セカンダリ ドメイン名を入力します。**Update** をクリックします。

ステップ 5 [Submit] をクリックします。
DNS サーバが設定されます。

ステップ 6 メニュー バーで、**[TENANTS]** > **[mgmt]** をクリックします。

ステップ 7 [Navigation] ペインで、**[Networking]** > **[VRF]** > **[oob]** の順に展開し、[oob] をクリックします。

ステップ 8 [Work] ペインの [Properties] 下で、[DNS labels] フィールドに、適切な DNS ラベル（デフォルト）を入力します。[Submit] をクリックします。
DNS プロファイル ラベルがテナントおよび VRF で設定されました。

カスタム証明書の設定

カスタム証明書の設定のガイドライン

- Cisco Application Policy Infrastructure Controller（APIC）で証明書署名要求（CSR）を生成するために使用される秘密キーのエクスポートはサポートされていません。証明書の CSR を生成するために使用された秘密キーを共有することにより、「Subject Alternative Name（SAN）」フィールドのワイルドカード（「* cisco.com」など）を介して複数のサーバで同じ証明書を使用する場合は、秘密キーを Cisco Application Centric Infrastructure（ACI）ファブリックの外部に配置し、Cisco ACI ファブリックにインポートします。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco APIC は、送信された証明書が設定された CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
  - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。

- Cisco APIC で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
- 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキーリングを削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

- Cisco ACI マルチサイト、VCPlugin、VRA、および SCVMM は、証明書ベースの認証ではサポートされません。
- Cisco APIC クラスタごとに 1つのSSL証明書のみが許可されます。
- 以降のリリースからリリース 4.0(1) にダウングレードする前に、証明書ベースの認証を無効にする必要があります。
- 証明書ベースの認証セッションを終了するには、ログアウトして CAC カードを削除する必要があります。
- Cisco APIC に設定されたカスタム証明書は、リーフ スイッチとスパイン スイッチに展開されます。ファブリック ノードに接続するために使用される URL または DN が **[サブジェクト（Subject）]** または **[サブジェクト代替名（Subject Alternative Name）]** フィールド内にある場合、ファブリック ノードは証明書でカバーされます。
- Cisco APIC GUI は、最大サイズが 4k バイトの証明書を受け入れることができます。
- HTTPS アクセスに使用している自己署名 SSL 証明書の有効期限が切れると、証明書は自動的に更新されます。

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

注意 ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。

ダウンタイムは外部ユーザまたはシステムからの Cisco Application Policy Infrastructure Controller（APIC）APIC クラスタおよびスイッチへのアクセスには影響しますが、Cisco APIC とスイッチの接続には影響しませスイッチで実行されている NGINX プロセスのため、外部接続にも影響が及びますが、ファブリックのデータ プレーンには影響ありません。Cisco APIC、設定、管理、トラブルシューティングなどへのアクセスは影響を受けることになります。Cisco APIC および スイッチで実行されている NGINX Web サーバーは、この操作中に再起動されます。

始める前に

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

手順

ステップ 1 メニュー バーで、**[Admin]** > **[AAA]** の順にクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[セキュリティ（Security）]** を選択します。

ステップ 3 **作業**ペインで、**[認証局（Certificate Authorities）]** > **[アクション（Actions）]** > **[認証局の作成（Create Certificate Authority）]** の順に選択します。

ステップ 4 [**認証局の作成（Create Certificate Authority**）] 画面で、[**Name（名前**）] フィールドに、認証局の名前を入力します。

ステップ 5 （オプション）認証局の [**説明（Description**）] を入力します。

ステップ 6 **[証明書チェーン（Certificate Chain）]** フィールドで、Cisco APIC の証明書署名要求（CSR）に署名する認証局の中間証明書とルート証明書をコピーします。

証明書は、Base64 エンコード X.509 CER（Cisco Emergency Responder）フォーマットである必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 **作業**ペインで、**[キーリング（Key Rings）]** > **[アクション（Actions）]** > **[キーリングの作成（Create Key Ring）]** の順に選択します。

キーリングを使用すると、以下を管理できます。

1. 秘密キー（外部デバイスからインポートされた、またはCisco APIC で内部的に生成されたもの）。
2. 秘密キーによって生成された CSR。
3. CSR を通じて署名された証明書。

ステップ 9 [Create Key Ring] ダイアログボックスで、[Name] フィールドに、名前を入力します。

ステップ 10 （オプション）キーリングの [**説明（Description**）] を入力します。

ステップ 11 [**認証局（Certificate Authority**）] フィールドで、[**認証局の選択（Select Certificate Authority**）] をクリックし、以前に作成した認証局を選択するか、[**認証局の作成（Create Certificate Authority**）] を選択します。

ステップ 12 [**秘密キー（Private Key**）] フィールドで必要なラジオボタンを選択します。

次のオプションがあります。

1. 新しいキーの生成（Generate New Key）
2. 既存キーのインポート（Import Existing Key.）

ステップ 13 秘密キーを入力します。このオプションは、**[秘密キー（Private Key）]**の **[既存キーのインポート（Import Existing Key）]** オプションを選択した場合にのみ表示されます。

ステップ 14 **[秘密キー（Private Key）]** フィールドで **[新しいキーの生成（Generate New Key）]** オプションを選択した場合は、**[キー タイプ（Key Type）]** で必要なラジオ ボタンを選択します。

選択できる基準は、次のとおりです。

1. **[RSA]**（Rivest、Shamir、および Adelman）
2. **[ECC]**（楕円曲線暗号）。 ECDSA（楕円曲線デジタル署名アルゴリズム）とも呼ばれます。

ステップ 15 キーリングで Cisco APIC を使用して CSR を生成する場合は、その内容を **[証明書（Certificate）]** フィールドに追加しないでください。前の手順で Cisco APIC を使用せずに秘密キーおよび CSR を生成していて、CA によって署名された証明書がある場合は、その内容を **[証明書（Certificate）]** フィールドに追加します。

ステップ 16 暗号に必要なキー強度を選択します。このオプションは、**[秘密キー（Secret Key）]**で [新しいキーの生成（Generate New Key）] オプションを選択した場合にのみ表示されます。RSA の場合は **[モジュラス（Modulus）]** ドロップダウン リストで、ECC **[キー タイプ（Key Type）]** の場合は **[ECC カーブ（ECC Curvce）]** ラジオ ボタンで選択します。

a) **[キー タイプ（Key Type）]** で **[RSA]** を選択した場合は、**[モジュラス（Modulus）]** ドロップダウン リストからモジュラス値を選択します。

b) **[キー タイプ（Key Type）]** で **[ECC]** を選択した場合は、**[ECC 曲線（ECC Curve）]** ラジオ ボタンのリストから適切な曲線を選択します。

ステップ 17 [保存（Save）] ([キーリングの作成（Create Key Ring）] 画面) をクリックします。

ステップ 18 **[作業（Work）]**ペインで、**[キーリング（Key Rings）]** > ***[キーリング名]***を選択します（または、必要なキーリングの行をダブルクリックします）。

署名付き証明書と秘密キーを入力していない場合は、**[作業（Work）]** ペインの **[キーリング（Key Rings）]** 領域で、作成されたキーリングの **[管理状態（Admin State）]** に **[開始（Started）]** と表示され、CSR が生成されるのを待ちます。手順 19 に進みます。

署名付き証明書と秘密キーの両方を入力した場合は、**[キーリング（Key Rings）]** 領域に、作成されたキーリングの **[管理状態（Admin State）]** が **[完了（Completed）]** と表示されます。手順 22 に進みます。

（注）
キー リングは削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

展開ボタンをクリックすると、新しい画面に選択したキーリングが表示されます。

ステップ 19 **[証明書要求（Certificate Request）]** ペインで、**[証明書要求の作成（Create Certificate Request）]** をクリックします。

[証明書要求（Certificate Request）] ウィンドウが表示されます。

a) **[サブジェクト（Subject）]** フィールドに、CSR の共通名（[CN]）を入力します。

ワイルドカードを使用して Cisco APIC の完全修飾ドメイン名（FQDN）を入力することもできますが、新しいタイプの証明書では、識別可能な証明書の名前を入力し、**[代替サブジェクト名（Alternate Subject Name）]** フィールド（*[SAN]*フィールド）にすべての Cisco APIC の FQDN を入力することを推奨します（多くの最新のブラウザは、[SAN] フィールドに FQDN が入力されていることを想定しています）。

b) **[代替サブジェクト名（Alternate Subject Name）]** フィールドに、「DNS:apic1.example.com, DNS:apic2.example.com, DNS:apic3.example.com」や「DNS:*example.com」など、すべての Cisco APIC の FQDN を入力します。 。

または、SAN を IP アドレスと一致させる場合は、 Cisco APICの IP アドレスを次の形式で入力します。

```
IP:192.168.2.1
```

このフィールドには、DNS名、IPv4アドレス、またはその両方を組み合わせて使用できます。IPv6 アドレスはサポートされていません。

c) **[地域（Locality）]** フィールドに、組織の市または町を入力します。
d) **[州（State）]** フィールドに、組織が所在する州を入力します。
e) **[国（Country）]** フィールドに、組織の所在地の国を表す 2 文字の ISO コードを入力します。
f) **[組織名（Organization Name）]** を入力し、**[組織単位名（ Organization Unit Name）]** に単位を入力します。
g) 組織の連絡担当者の **[電子メール（Email）]** アドレスを入力します。
h) **[パスワード（Password）]** に入力し、**[パスワードの確認（Confirm Password）]** フィールドにもう一度入力します。
i) [OK] をクリックします。

ステップ 20 [証明書要求の設定（ Certificate Request Settings）] ペインに、上で入力した情報が表示されます（手順 19）。

ステップ 21 **[作業（Work）]**ペインで、**[キーリング（Key Rings）]** > ***[キーリング名]***を選択します（または、必要なキーリングの行をダブルクリックします）。

新しい画面に選択した**キーリング**が表示されます。

（注）
キーリングに示されている認証局によって署名されていない CSR、または MS-DOS 形式の行末を持つ CSR は受け入れられません。エラー メッセージが表示されたら、MS-DOS の行末を削除して解決します。

キーが正常に確認されて、**[作業（Work）]** ペインの **[管理状態（Admin State）]** が **[完了済み（Completed）]** に変わり、HTTP ポリシーで使用できるようになります。

ステップ 22 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]**を選択します。

ステップ 23 [ナビゲーション（Navigation）] ペインで、**[ポリシー（ Policies）]** > **[ポッド（Pod）]** > **[管理アクセス（Management Access）]** > **[デフォルト（default）]** をクリックします。

ステップ 24 [Work] ペインの [Admin Key Ring] ドロップダウン リストで目的のキー リングを選択します。

ステップ 25 （オプション）証明書ベースの認証では、[Client Certificate TP] ドロップダウン リストで、以前に作成したローカル ユーザ ポリシーを選択し、[Client Certificate Authentication state] の [Enabled] をクリックします。

ステップ 26 [Submit] をクリックします。
すべての Web サーバーがリスタートし、証明書がアクティブになり、デフォルト以外のキーリングは HTTPS アクセスに関連付けられます。

次のタスク

証明書の失効日には注意し、期限切れになる前に必要な措置を取ってください。更新された証明書に同じキー ペアを保持するには、CSR を保持します。CSR にはキーリング内の秘密キーとペアになる公開キーが含まれています。証明書が期限切れになる前に、同じ CSR を再送信してください。削除したり、新しいキーリングを作成したりしないでください。キーリングを削除すると、 Cisco APICに保存されている秘密キーが削除されます。

ファブリック全体のシステム設定のプロビジョニング

APICインバンドまたはアウトオブバンド接続設定(preferences)の設定

このトピックでは、APIC サーバ認証サーバまたは ACI ファブリックに外部 SNMP サーバなどのデバイスの管理アクセスのインバンドおよびアウトオブバンド接続の間で切り替える方法について説明します。有効化 **インバンド** ACI ファブリックのリーフ スイッチからの外部デバイスに APIC サーバ間のインバンド管理接続を実行します。有効化 **ooband** ACI ファブリックに外部接続の外部デバイスに APIC サーバ間のアウトオブバンド管理接続を実行します。

始める前に

インバウンドおよびアウトバウンド管理ネットワークを構成します。詳細については、「管理」 (『*Cisco APIC* 基本設定ガイド、リリース *3.x*』) を参照してください。

手順

ステップ 1 メニューバーで、 **System** > **System Settings** の順にクリックします。

ステップ 2 ナビゲーション バーで、をクリックして **APIC 接続設定 (preferences)** 。

ステップ 3 ポリシーを有効にするにはクリックして **インバンド** または **ooband** 。

ステップ 4 [Submit] をクリックします。

クォータ管理ポリシーの設定

Application Policy Infrastructure Controller (APIC) リリース 2.3(1) 移行から、テナント管理者が設定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、テナントを超えてグローバルに追加される管理対象オブジェクトの数を制限できるようになりました。

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。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** をクリックします。

ステップ 2 **Quota** を右クリックして、**Create Quota Configuration** を選択します。

ステップ 3 **Class** フィールドで、クォータによる制限を掛けるオブジェクトのタイプを選択します。

ステップ 4 **Container Dn** フィールドに、クラスを説明する識別名 (DN) を入力します。

ステップ 5 **Exceed Action** フィールドで、**Fail Transaction Action** または **Raise Fault Action** を選択します。

ステップ 6 **Max Number** フィールドで、作成できる管理対象オブジェクトの最大数を入力します。これを超えると、超過アクションが適用されることになります。

ステップ 7 [Submit] をクリックします。

適用 BD 例外リストの作成

このトピックでは、適用対象のブリッジ ドメインには従わない、サブネットのグローバルな例外リストの作成方法について説明します。適用 BD の機能を設定している場合、対象のエンドポイント グループ (EPG) が ping を送信できるのは、関連付けられたブリッジ ドメイン内のサブネット ゲートウェイだけです。

例外 IP アドレスは、すべての VRF のすべての BD ゲートウェイに ping を送信できます。

L3Out 用に設定されたループバック インターフェイスでは、対象のループバック インターフェイスに合わせて設定された IP アドレスへの到達可能性は適用されません。

EBGP ピアとなる IP アドレスが、L3Out インターフェイスのサブネットとは異なるサブネットに存在している場合には、許容例外サブネットにピア サブネットを追加する必要があります。そうしないと、送信元 IP アドレスが L3Out インターフェイスのサブネットとは異なるサブネットに存在するため、eBGP トラフィックがブロックされます。

始める前に

適用対象のブリッジ ドメイン (BD) を作成します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。
ステップ 2 **BD Enforced Exception List** をクリックします。
ステップ 3 **Exception List** の [+] をクリックします。
ステップ 4 任意のサブネット ゲートウェイに ping を送信できるサブネットの IP アドレスとネットワーク マスクを追加します。
ステップ 5 これを繰り返して、適用ブリッジ ドメインの例外となるサブネットを追加します。
ステップ 6 [Submit] をクリックします。

BGP ルータ リフレクタ ポリシーとルート リフレクタ ノード エンドポイントの作成

このトピックでは、ACIファブリック ルート リフレクタを作成する方法について説明します。リフレクタは、ファブリック内で外部ルートを配布するために、マルチ プロトコル BGP (MP-BGP) を使用します。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。ルート リフレクタが ACI ファブリックで有効になれば、管理者は、外部ネットワークへの接続を設定できます。

始める前に

必須項目：

- ACIファブリックに外部ルータを接続するには、ファブリック インフラストラクチャの管理者がボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタとしてスパイン ノードを設定するひつようがあります。
- 冗長性のために、複数のスパインがルータ リフレクタ ノードとして設定されます（1 台のプライマリ リフレクタと 1 台のセカンダリ リフレクタ）。

手順

ステップ 1 BGP ルート リフレクタ ポリシーを作成するには、次の手順を実行します:
a) メニュー バーで、**System** > **System Settings** をックリックします。
b) **BGP Route Reflector** をクリックします。
c) 入力自律システム番号を入力します。
d) **Route Reflector Nodes** で [+] をクリックします。

e) スパイン ルート リフレクタ ノードの ID エンドポイントを入力し、**Submit** をクリックします。

ステップ 2 外部ルート リフレクタ ノードのエンドポイントを作成するには、次の手順に従います:

a) **External Route Reflector Nodes** で [+] をクリックします。
b) 外部ルート リフレクタ ノードのエンドポイントとして機能するスパインを選択します。
c) これがマルチサイトによって管理されるサイトである場合には、インターサイト スパイン ルート リフレクタも指定できます。
d) [Submit] をクリックします。

ファブリック全体のコントロール プレーンの MTU ポリシーを設定する

このトピックでは、ファブリック全体のコントロールプレーン（CP）のMTUポリシーを作成する方法について説明します。これは、ファブリックのノード（スイッチ）から送信されたコントロール プレーン パケットのグローバル MTU サイズを設定します。

マルチポッド トポロジでは、ファブリック外部ポートの MTU 設定は、CP MTU の値セット以上である必要があります。そうしないと、ファブリックの外部ポートがCP MTUパケットをドロップする可能性があります。

（注）
- MTU を IPN から継承する L3Out インターフェイス プロファイルを設定するには 9150 にします。IPN 全体で使用される MTU を 2916 に構成する必要がある場合には、L3Out インターフェイスプロファイル内で明示的に構成する必要があります（**[テナント（Tenants）]**> ***tenant-name*** > **[ネットワーキング（Networking）]** > **[外部ルート ネットワーク（External Routed Networks）]** > **[外のネットワークを作成（Create Routed Outside）]** > **[ノードとインターフェイス プロトコル プロファイル（Nodes and Interface Protocol Profiles）]** > **[ノード プロファイルを作成（Create Node Profile）]** > **[インターフェイス プロファイルを作成（Create Interface Profile）]** で構成します）。
- Cisco APIC は、CP-MTU 設定に関係なく、常に 1496 バイト（TCP MSS 1456）の MTU でファブリック スイッチへの TCP 接続を確立します。リモート ポッドおよびリモート リーフ スイッチの IPN ネットワークは、ファブリック ディスカバリのために少なくとも 1500 バイトの MTU をサポートする必要があります。

IPN または CP MTU を変更する場合、Cisco では CP MTU 値を変更し、次にリモート ポッドのスパイン上のMTU値を変更することをお勧めします。これで、MTUの不一致によりポッド間の接続が失われるリスクが減少します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** をックリックします。
ステップ 2 **Control Plane MTU** をクリックします。
ステップ 3 ファブリック ポートの MTU を入力します。
ステップ 4 [Submit] をクリックします。

エンドポイント ループ保護の設定

エンドポイントのループ保護ポリシーでは、頻繁な MAC の移動を処理することによる、ループ検出の方法を指定します。EP ループ保護を設定するには、次の手順を実行します:

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。
ステップ 2 をクリックして **エンドポイント コントロール** 。
ステップ 3 **Ep Loop Protection** タブをクリックします。
ステップ 4 ポリシーを有効にするには、**Enabled** をクリックします (**Administrative State** フィールドにあります)。
ステップ 5 オプション。ループを検出の間隔を設定します。これはループを検出するための時間を指定します。指定できる範囲は 30〜 300 秒です。デフォルトの設定は 60 秒です。
ステップ 6 ループ検出乗算係数を設定します。これは、ループ検出間隔内で単一の EP がポート間を移動した回数です。範囲は 1 〜 255 です。デフォルトは 4 です。
ステップ 7 ループを検出したときに実行するアクションを選択します。

アクションとしては、次のものがあります:

- **BD Learn Disable**
- **Port Disable**

デフォルトは **Port Disable** です。

ステップ 8 [Submit] をクリックします。

不正エンドポイント制御ポリシー

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。

不正エンドポイント制御ポリシーの制限事項

不正エンドポイント制御ポリシーを使用する際には、次の制限が適用されます:

- 不正エンドポイント制御ポリシーのパラメータを変更しても、既存の不正エンドポイントには影響しません。

- 不正エンドポイントが有効になっていても、ループ検出とブリッジドメイン移動頻度は有効になりません。
- 不正エンドポイント機能を無効にすると、すべての不正エンドポイントがクリアされます。
- エンドポイント マッパー (EPM) の値は、不正エンドポイントのパラメータに制限を課します。この範囲外のパラメータ値を設定すると、Cisco APIC適切でないパラメータごとにエラーが発生します。
- 不正エンドポイント検出のサポートは、リモート リーフ ノードに接続されているエンドポイントではなく、ファブリックに接続されているエンドポイントに限定されます。
- 不正なエンドポイント機能は、Cisco ACI マルチサイト 展開の各サイト内で使用でき、サイト内でエンドポイントを移動させるサーバの設定ミスに役立ちます。不正エンドポイント機能は、エンドポイントがサイト間を移動する可能性があるシナリオ向けには設計されていません。
- Cisco APIC リリース 4.1 にアップグレードする前に、不正エンドポイント制御を無効にする必要があります。

GUI を使用した不正エンドポイント制御ポリシーの設定

Cisco Application Policy Infrastructure Controller（Cisco APIC）GUI を使用して、不正なエンドポイントを検出して削除するようにファブリックの**不正 EP 制御**ポリシーを設定できます。このトピックには、アドホックのリーフスイッチで不正なエンドポイントをクリアする手順も含まれています。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。

ステップ 2 ナビゲーション ウィンドウで、**[エンドポイント制御（Endpoint Controls）]** を選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインで、**[不正な EP 制御（Rogue EP Control）]** タブを選択します。

ステップ 4 **[Administrative State]** を **[Enabled]** に設定します。

ステップ 5 **[不正な EP 検出間隔（Rogue EP Detection Interval）]**、**[不正な EP 検出倍数係数（Rogue EP Detection Multiplication Factor）]**、および **[保持間隔（秒）（Hold Interval (sec)）]** を目的の値に設定します。

- **不正な EP 検出間隔**：不正エンドポイントの検出間隔を設定します。これは、不正エンドポイントを検出する時間を指定します。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。
- **不正な EP 検出倍数係数**：エンドポイントが不正かどうかを判断するための不正エンドポイント検出の乗数を設定します。エンドポイントがこの数よりも多く移動すると、エンド

ポイント検出間隔内で、エンドポイントは不正と宣言されます。有効値は 2 ～ 10 です。デフォルト値は 6 です。

- **保持間隔（秒）**：エンドポイントが不正であると宣言されてからの間隔（秒単位）。学習が防止され、不正なエンドポイントとの間のトラフィックがドロップされます。このインターバルが経過すると、エンドポイントは削除されます。5.2(3) リリースより前では、有効な値は 1800 ー 3600 秒です。5.2(3) リリースより前では、有効な値は 1800 ー 3600 秒です。デフォルト値は 1800 です。

ステップ 6 （任意）リーフスイッチの不正なエンドポイントをクリアするには、次の手順を実行します。

a) Cisco APICメニュー バーで、**[Fabric]** > **[Inventory]** の順にクリックします。
b) ナビゲーションバーで、[Pod] を展開し、不正なエンドポイントをクリアするリーフ スイッチをクリックします。
c) リーフ スイッチ サマリが作業ウィンドウに表示されたら、ナビゲーション バーのリーフ スイッチ名を右クリックし、**[Clear Rogue Endpoints]** を選択します。
d) [はい（Yes）] をクリックします。

NX-OS スタイル CLI を使用している不正エンドポイント制御ポリシーの設定

NX-OS スタイルの CLI を使用して、不正なエンドポイントを検出および削除するように、ファブリックの不正エンドポイント制御ポリシーを設定できます。

手順

ステップ 1 グローバル コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 グローバルな不正エンドポイント制御ポリシーを有効にします。

例：

```
apic1(config)# endpoint rogue-detect enable
```

ステップ 3 ホールド間隔を設定します。

保持間隔は、エンドポイントが不正であると宣言されてからエンドポイントが静的に保たれ、学習が防止され、エンドポイントとの間のトラフィックがドロップされた後の期間（秒）です。このインターバルが経過すると、エンドポイントは削除されます。リリース 5.2(2) 以前では、有効な値は 1800 ～ 3600 秒です。リリース 5.2(3) 以降では、有効な値は 300 ～ 3600 秒です。デフォルト値は 1800 です。

例：

```
apic1(config)# endpoint rogue-detect hold-interval 1800
```

ステップ 4 検出間隔を設定します。

検出間隔は、不正エンドポイント制御がエンドポイントの移動数をカウントしている間の期間（秒）です。この間隔の中のカウントが検出乗算係数で指定された値を超える場合、エンドポイントは不正であると宣言されます。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。

例：

```
apic1(config)# endpoint rogue-detect interval 60
```

ステップ 5 検出倍率を設定します。

エンドポイントが、検出間隔で指定された期間中に検出倍率で指定された値よりも多く移動した場合、エンドポイントは不正であると宣言されます。有効値は 2 ～ 10 です。デフォルト値は 6 です。

例：

```
apic1# endpoint rogue-detect factor 6
```

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。

不正/ COOP 例外リストのガイドラインと制限事項

不正/COOP 例外リストを使用するとき、次の注意事項と制限事項が適用されます。

- MAC アドレス例外リスト機能は、レイヤ 2 ブリッジ ドメイン（IP ルーティングが有効になっていないブリッジドメイン）で動作します。これは、レイヤ3ブリッジドメイン（IP ルーティングが有効になっているブリッジ ドメイン）では、MAC アドレスとともに移動する IP アドレスがあった場合、最初に IP アドレスが放浪しているとしてマークされ、その後 IP アドレスと MAC アドレスの両方が検疫対象とされるためです。
- レイヤ 3 ブリッジ ドメインの場合、放浪エンドポイント制御から除外する特定の IP アドレスについては、サブネットごとのデータプレーン IP アドレス学習を無効にします。

  サブネットごとのデータプレーン IP アドレス学習機能については、*Cisco APIC Layer 3* ネットワーキング設定ガイドを参照してください。

- このリストに追加されている MAC アドレスの種類を完全に理解している必要があります。このリスト内の MAC アドレスが、ファブリック全体または、リーフ スイッチごとでの過剰な移動に寄与しないようにすることは、ユーザーの責任です。
- ブリッジ ドメインごとの例外リストには、ファブリック全体で最大 100 個の MAC アドレスを追加できます。6.0（3）リリース以降では、特定のブリッジ ドメインのすべての MAC アドレスを不正なエンドポイント制御から除外することもできます。
- 6.0（3）リリース以降、ファブリック全体で 100 個の外部 L3Out MAC アドレスを例外リストに追加できます。また、L3Out SVI ブリッジ ドメインのすべての MAC アドレスを不正なエンドポイント制御から除外することもできます。
- 6.0（3）リリース以降、それらの MAC アドレスのエンドポイントの合計数が 6,000 以内であれば、最大 6,000 個の MAC アドレスをグローバル例外リストに追加できます。複数のブリッジ ドメインで検出された同じ MAC アドレスは、合計 6,000 のエンドポイントに対して、同じ数のブリッジ ドメインとしてカウントされます。たとえば、構成された MAC アドレスが 10 のブリッジ ドメインで検出された MAC エンドポイントとして表示される場合、MAC アドレスは 10 のエンドポイントとしてカウントされます。
- リーフ スイッチの例外リストの免除は、放浪エンドポイント制御が有効になっている場合にのみ適用されます。放浪エンドポイント制御が無効になっている場合、MAC アドレス例外リストは、COOP ダンプニングでのみ使用されます。
- 不正/ COOP 例外リストには、ブリッジ ドメインの MAC アドレスのみを含めることができ、VRF インスタンスの IP アドレスは含めることができません。ただし、IP アドレスのみの移動では、IP アドレスが通常の不正エンドポイント制御基準を満たす場合でも、IP アドレスが不正としてマークされる可能性があります。
- データ パストラフィックに基づいて IP アドレスの不正検出およびマーキングをマスクするには、ブリッジ ドメイン サブネット学習無効を使用します。ブリッジ ドメイン サブネット ラーニング無効化は、移動するたびに Cisco ACI が IP アドレスの場所を学習しなくなります。

GUI を使用したブリッジ ドメイン作成時の不正/ COOP 例外リストの設定

次の手順では、ブリッジ ドメインの作成時に不正/ COOP 例外リストを設定します。

始める前に

- ブリッジ ドメインを作成するテナントが必要です。
- 不正エンドポイント制御を有効にする必要があります。不正エンドポイント制御を有効にする手順については、GUI を使用した不正エンドポイント制御ポリシーの設定（188 ページ） を参照してください。

手順

ステップ 1 目的のテナントで、ブリッジ ドメインを作成します。メニューバーで、**[テナント（Tenants）]**> ***[tenant_name]***を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** の順に選択します。

ステップ 3 **Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。

ステップ 4 **[ブリッジ ドメインの作成（Create Bridge Domain）]** ダイアログで、**[ステップ 1（STEP 1）]** の **[メイン（MAIN）]** および **[ステップ 2（STEP 2）]** の **[L3 設定（L3 Configurations）]** に必要なフィールドに入力します。

ステップ 5 **[STEP 3（ステップ 3）]** の **[アドバンスト/トラブルシューティング（Advanced / Troubleshooting）]** で、**[不正/COOP 例外リスト（Rogue / Coop Exception List）]** の **[+]** をクリックし、リストに追加するエンドポイントの MAC アドレスを入力して、**[更新（Update）]** をクリックします。

MAC アドレスの形式は `AA:BB:CC:DD:EE:FF` です。

a) リストに追加するエンドポイントごとにこのステップを繰り返します。

ステップ 6 （オプション）：Cisco Application Policy Infrastructure Controller（APIC）6.0（3）リリース以降、ブリッジドメインからのMACアドレスを無視するために不正エンドポイントコントロール **BD の 不正例外 MAC を有効化** チェック ボックスをチェックします。

ステップ 7 必要に応じて、**[ステップ 3（STEP 3）]** > **[アドバンスト/トラブルシューティング（Advanced/Troubleshooting）]** の残りのフィールドに入力します。

ステップ 8 **[完了（Finish）]** をクリックします。

GUI を使用した既存のブリッジ ドメインの不正/ COOP 例外リストの設定

次の手順では、既存のブリッジ ドメインの不正/ COOP 例外リストを設定します。

始める前に

- ブリッジ ドメインを持つテナントが必要です。
- 不正エンドポイント制御を有効にする必要があります。不正エンドポイント制御を有効にする手順については、GUI を使用した不正エンドポイント制御ポリシーの設定 （188 ページ） を参照してください。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > ***[tenant_name]***を選択します。

ステップ 2 [ナビゲーション（Navigation）] ウィドウで、**[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** > ***[bridge_domain_name]***. を選択します。

ステップ 3 [作業（Work）] ペインで、**[ポリシー（Policy）]** > **[アドバンスト/トラブルシューティング（Advanced/Troubleshooting）]** を選択します。

ステップ 4 **[不正/COOP 例外リスト（Rogue / Coop Exception List）]** で **[+]** をクリックし、リストに追加するエンドポイントの MAC アドレスを入力して、**[更新（Update）]** をクリックします。

MAC アドレスの形式は `AA:BB:CC:DD:EE:FF` です。

a) リストに追加するエンドポイントごとにこのステップを繰り返します。

ステップ 5 （オプション）：Cisco Application Policy Infrastructure Controller（APIC）6.0（3）リリース以降、ブリッジドメインからの MAC アドレスを無視するために不正エンドポイントコントロール **BD の 不正例外 MAC を有効化** チェック ボックスをチェックします。

ステップ 6 [Submit] をクリックします。

GUI を使用した L3Out SVI の不正エンドポイント制御の例外リストの構成

このセクションの手順では、L3Out の選択されたスイッチ仮想インターフェイス（SVI）について、不正なエンドポイント制御機能が無視する MAC アドレスを設定します。

始める前に

- L3Out を持つテナントが必要です。
- 不正エンドポイント制御を有効にする必要があります。不正エンドポイント制御を有効にする手順については、GUI を使用した不正エンドポイント制御ポリシーの設定 （188 ページ） を参照してください。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > ***[tenant_name]***を選択します。

ステップ 2 ナビゲーション ウィンドウで**[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[ロジカル ノード プロファイル（Logical Node Profiles）]** > ***[node_profile_name]*** > **[ロジカル インターフェイス プロファイル（Logical Interface Profiles）]** > ***[interface_profile_name]***を選択します。

ステップ 3 ワーク ペインで、**[ポリシー（Policy）]** > **SVI**を選択します。

ステップ 4 SVI テーブルで、**[+]** をクリックします。

ステップ 5 **[SVIを選択（Select SVI）]** ダイアログ内でいずれかの次のアクションを実行します：

- **[不正除外 MAC グループ（Rogue Exception MAC Group）]** で、既存のグループを選択するか、新しいグループを作成します。

  不正例外 MAC グループは、同じ VLAN カプセル化を持つすべての SVI について、不正エンドポイント制御機能が無視する MAC アドレスを指定します。

- **[不正 EP コントロールからの MAC を全て除外します（Exclude all MACs from Rogue EP Control）]** ボックスをチェックします。

  このオプションを有効にすると、不正エンドポイント制御機能は、同じ VLAN カプセル化を持つすべての SVI のすべての MAC アドレスを無視します。

ステップ 6 目的に応じて、残りのフィールドに入力します。

ステップ 7 [Submit] をクリックします。

GUI を使用したファブリックの不正 エンドポイント制御 の MAC アドレス 例外を構成

6.0（3）リリース以降、ファブリック レベルで、不正なエンドポイント制御が無視する MAC アドレスを設定できます。不正エンドポイント制御は、MAC アドレスが属するブリッジ ドミアンまたは L3Out SVI に関係なく、指定した MAC アドレスを無視します。

始める前に

不正エンドポイント制御を有効にする必要があります。不正エンドポイント制御を有効にする手順については、GUIを使用した不正エンドポイント制御ポリシーの設定（188ページ）を参照してください。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]**を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、 > **[ポリシー（Policies）]** > **[ファブリック ワイルドカード不正例外（Fabric Wildcard Rogue Exception）]**を選択します。

ステップ 3 [ワーク（Work）] ペインの **[ファブリック ワイルドカード不正例外（Fabric Wildcard Rogue Exception）]** テーブルで、**[+]** をクリックします。

a) 無視する不正エンドポイント制御の MAC アドレスを入力し、**[更新（Update）]** をクリックします。

b) 不正なエンドポイント制御で無視する MAC アドレスごとに、この手順を繰り返します。

最大 IP アドレス フロー制御について

3.2(6) リリースでは、最大IPアドレスフロー制御機能が追加されています。これは、エンドポイントの動作不良を識別し、MAC アドレスに関連付けられている学習 IP アドレスの数に基づいて不正としてフラグを立てます。Cisco Application Centric Infrastructure（ACI）ファブリックは、MAC アドレスで最大 4,096 個の IP アドレスをサポートします。リーフ スイッチが MAC アドレスに関連付けられた 4,096 を超える IP アドレスを学習した場合、MAC アドレスとすべての IP アドレスが不正として分類されます。

最大 IP アドレス フロー制御機能がエンドポイントを不正として識別した後、エンドポイントは隔離され、APIC で障害が発生し、このエンドポイントで新しい IP アドレスの学習は行われません。隔離期間は 1 時間です。標準の不正機能が有効になっている場合、隔離期間は標準の不正設定で設定された期間と同じです。

不正なエンドポイント制御ポリシー機能（移動による不正）は有効または無効に設定できますが、最大 IP アドレス フロー制御機能では明示的な設定を有効にする必要はありません。

この機能が導入される前は、設定可能な期間内に設定された回数だけロケーションを移動し続けた場合、ACI ファブリックはエンドポイントを不正と識別していました。この機能を使用すると、ACI ファブリックは、移動の数に基づいて、または MAC アドレスで 4,096 を超える IP アドレスを学習した場合に、エンドポイントを不正として識別できます。

COOP の設定

COOP について

Council of Oracle Protocol（COOP）は、スパイン スイッチ プロキシにマッピング情報（場所と ID）を通信するために使用されます。リーフ スイッチ（「citizen」）は、ゼロ メッセージ キュー（ZMQ）を使用して、エンドポイントアドレス情報をスパイン スイッチ（「oracle」）に転送します。スパイン ノードで実行している COOP によって、すべてのスパイン ノードが一貫性のあるエンドポイントアドレスとロケーション情報のコピーを維持することができ、さらに、ロケーションマッピング データベースに対するエンドポイント ID の分散ハッシュ テーブル（DHT）レポジトリを維持することができます。

COOP エンドポイントのダンプニング

悪意のある動作または誤った動作によって不要なエンドポイント更新が発生すると、COOP プロセスが過負荷になり、有効なエンドポイント更新の処理が妨げられる可能性があります。リーフ スイッチの不正エンドポイント検出機能により、多数の誤った更新がスパイン スイッチに到達するのを防ぐことができます。不正なエンドポイントの検出が不十分な場合、COOP プロセスはエンドポイントのダンプニングを呼び出します。COOP の負荷を軽減するために、スパイン スイッチはすべてのリーフ スイッチに、指定された期間、不正な動作をしているエンドポイントからの更新を無視するように要求します。これが発生すると、エンドポイントのダンプニング状態は「フリーズ」になり、障害が生成されます。

（注） COOP エンドポイント ダンプニングは、Cisco Application Policy Infrastructure Controller（APIC）リリース 4.2(3) で導入され、デフォルトで有効になっています。

検出基準は、次の表に示すように、エンドポイント関連イベントのタイプに基づくペナルティ値の計算に基づきます。

イベント（Event）	ペナルティ値	注
新しい IP アドレスを確認する	0	新しい IP アドレスが学習されます。
追加の IP アドレスを確認する	2	追加の IP アドレスは、既存のエンドポイントの MAC アドレスで学習されます。
IP アドレスの削除	50	リモート エンドポイントの IP アドレスは、IP アドレスが学習されると削除されます。
削除された IP アドレスを確認する	50	IP アドレスが削除された後のリモート エンドポイントの IP アドレスを確認します。
IP アドレスの削除	400	IP アドレスが学習されたら、ローカル エンドポイントの IP アドレスを削除します。
削除された IP アドレスを確認する	400	IP アドレスが削除された後のローカル エンドポイント IP アドレスを確認します。
エンドポイントの移動	200	エンドポイントが別のインターフェイスに移動します。
IP アドレスの移動	200	IP アドレスが別の MAC アドレスに移動する。 このイベントでは、BGP へのルート更新が 2 回発生するため、ペナルティは高くなります。
URIB プログラミング	50	エンドポイントのスパイン スイッチ トンネル インターフェイスのステータス変更（アップ/ダウン）。

ペナルティ値は IP アドレスごとに計算され、5 分ごとに 50% ずつ減少します。たとえば、エンドポイントのペナルティ値が 4000 で、エンドポイントの IP アドレスの数が 2 の場合、IP アドレスあたりのペナルティ値は 4000/2 = 2000 です。IP アドレスあたりのペナルティ値がクリティカルしきい値（4000）を超えると、エンドポイントの状態が **[標準（Normal）]** から **[クリティカル（Critical）]** に変更されます。エンドポイントが 5 分を超えて **[クリティカル（Critical）]** 状態になっている場合、または IP アドレスあたりのペナルティ値がフリーズしきい値（10000）を超えている場合、エンドポイントの状態は**フリーズ**（ダンプニング）になり、エンドポイントの更新は無視されます。IP アドレスあたりのペナルティ値が再利用しきい値（2500）を下回ると、エンドポイントの状態は **Normal**（非ダンプニング）になります。ペナルティ値を 75%（10000 * 0.5 * 0.5 = 2500）減らすには、10 分経過する必要があります。しきい値はユーザが設定することはできません。

COOP 認証

COOP データ パス通信は、セキュアな接続を介した転送を優先します。悪意のあるトラフィック インジェクションから COOP メッセージを保護するために、Cisco APIC およびスイッチは COOP プロトコル認証をサポートしています。

COOP プロトコルは、次の 2 つの ZMQ 認証モードをサポートしています。

- **厳密モード**： COOP では、MD5 認証 ZMQ 接続のみ許可します。
- **互換性モード**：COOP ではメッセージの転送に MD5 認証接続と非認証 ZMQ 接続の両方を許可します。

COOP 認証の詳細については、『*Cisco APIC* セキュリティ設定ガイド』を参照してください。

GUI を使用した COOP 減衰エンドポイントの表示

スパイン ノードのすべての減衰エンドポイントを表示するには、この Cisco Application Policy Infrastructure Controller（APIC）GUI 手順を使用します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）] > [インベントリ（Inventory）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、パッドとスパイン ノードを展開します。

ステップ 3 **[プロトコル（Protocols）] > [COOP]** および **[COOP]** インスタンスを展開します。

ステップ 4 **[エンドポイント データベース（Endpoint Database）]** をクリックして、エンドポイントを表示します。

[減衰状態（Dampened State）] カラムを調べて、減衰したエンドポイントを見つけます。次の状態があります。

- **Normal**：エンドポイントの更新は正常です。
- **Critical**：エンドポイントをフリーズ状態に移行できる十分な更新を受信しました。エンドポイントが 5 分以上 **Critical** 状態のままになると、状態は **Freeze** に変わります。
- **Freeze**：このエンドポイントからの更新は、頻繁に不要な更新が行われているため、現在無視されています。障害が生成されました。

スイッチ CLI を使用した COOP 減衰エンドポイントの表示

スパインまたはリーフ ノードのすべての減衰エンドポイントを表示するには、このスイッチ CLI 手順を使用します。

スパインまたはリーフ スイッチ CLI にログインし、次のコマンドを入力します。

```
show coop internal info repo ep dampening
```

GUI を使用した COOP 減衰エンドポイントのクリア

スパインまたはリーフ ノードのすべての減衰エンドポイントをクリアおよび回復するには、この Cisco Application Policy Infrastructure Controller（APIC）GUI 手順を使用します。この操作は、すべてのスパイン スイッチおよびエンドポイントの送信元リーフ スイッチで実行する必要があります。減衰されたエンドポイントがリーフ スイッチのエンドポイント テーブルにまだある場合、エンドポイントはスパイン スイッチ COOP データベースにパブリッシュされます。そうでない場合、減衰したエンドポイントは、2 分後にスパイン スイッチ COOP データベースから削除されます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）] > [インベントリ（Inventory）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、パッドとスパインまたはリーフ ノードを展開します。

ステップ 3 ノードを右クリックし、**[減衰エンドポイントの消去（Clear Dampened Endpoints）]** を選択します。

ステップ 4 **[はい（Yes）]** をクリックして、アクションを確認します。

スイッチ CLI を使用した COOP 減衰エンドポイントのクリア

スパインまたはリーフ ノードの減衰エンドポイントをクリアして回復するには、次の手順を使用します。この手順では、ダンプニング状態が **Freeze** である単一のエンドポイントを回復します。この操作は、すべてのスパイン スイッチおよびエンドポイントの送信元リーフ スイッチで実行する必要があります。

スパインまたはリーフ スイッチ CLI にログインし、次のコマンドを入力します。

```
clear coop internal info repo ep dampening key <bd> <mac>
```

RESTAPI を使用した COOP エンドポイント ダンプニングの無効化

この手順では、APIC REST API を使用して COOP EP ダンプニングを無効または有効にする方法を示します。

COOP エンドポイントのダンプニングはデフォルトで有効になっていますが、場合によっては無効にする必要があります。たとえば、1つの MAC アドレスに対して多数の IP 更新が予想され、それらの更新を無視するとネットワークが中断される場合があります。

次の API を使用し、`disableEpDampening = "true"` を設定して COOP エンドポイント ダンプニングを無効にします。

```
<!-- api/policymgr/mo/.xml -->

<polUni>
```

```
    <infraInfra>
        <infraSetPol disableEpDampening="true"></infraSetPol>
    </infraInfra>
</polUni>
```

ファブリック内のすべてのノードは COOP エンドポイント ダンプニングを無効にし、ダンプニング状態が「フリーズ」である既存のエンドポイントを回復します。

APIC GUI を使用した COOP 認証の設定

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順に選択します。

ステップ 2 **[ナビゲーション]** ペインで **[COOP グループ]** をクリックします。

ステップ 3 **[作業]** ペインの **[タイプ]** フィールドにある **[ポリシー プロパティ]** 領域で、**[互換性のあるタイプ]** および **[ストリクト タイプ]** オプションから希望のタイプを選択します。

ステップ 4 [Submit] をクリックします。
これにより、COOP 認証ポリシー設定を完了します。

Cisco NX OS スタイル CLI を使用した COOP 認証の設定

手順

ストリクト モード オプションを使用して、COOP 認証ポリシーを設定します。

例：

```
apic1# configure
apic1(config)# coop-fabric
apic1(config-coop-fabric)# authentication type ?
compatible  Compatible type
strict      Strict type
apic101-apic1(config-coop-fabric)# authentication type strict
```

REST API を使用した COOP 認証の設定

手順

COOP 認証ポリシーを設定します。

例では、ストリクト モードが選択されます。

例：

```
https://172.23.53.xx/api/node/mo/uni/fabric/pol-default.xml

<coopPol type="strict">
</coopPol>
```

エンドポイント リッスン ポリシー

エンドポイント リッスン ポリシーについて

エンドポイント リッスン ポリシーを設定して、ポリシーが適用されていない Cisco Application Centric Infrastructure（ACI）のリーフ スイッチに匿名エンドポイントから送信されるタグなしトラフィックを検出できます。デフォルトでは、ポートにポリシーが展開されていない場合、すべてのエンドポイント トラフィックがそのポートでドロップされます。エンドポイント リッスン ポリシーを設定すると、このポリシーは、適用されている既存のポリシーがないすべてのリーフ スイッチ ポートに展開されます。エンドポイント リッスン ポリシーでは、Cisco ACI でこれらのポートに着信するタグなしトラフィックを検出できます。これにより、Cisco ACI で匿名エンドポイントの MAC アドレスまたは IP アドレスがわかります。これにより、Cisco ACI 管理者はこれらのエンドポイントを配置する EPG を決定できます。Cisco Application Policy Infrastructure Controller（APIC）GUI は、検出されたすべての匿名エンドポイントを**グローバル エンド ポイント**設定画面に表示します。

（注） エンドポイント リッスン ポリシーはベータ機能です。この機能が意図したとおりに動作する保証はありません。自己責任で使用してください。

GUI を使用したエンドポイント リッスン ポリシーの設定

この手順では、エンドポイント リッスン ポリシーを設定します。このポリシーは、匿名エンドポイントから、適用されたポリシーがない Cisco Application Centric Infrastructure（ACI）リーフ スイッチに送信されるタグなしトラフィックを検出します。

（注） エンドポイント リッスン ポリシーはベータ機能です。この機能が意図したとおりに動作する保証はありません。自己責任で使用してください。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[システム設定（System Settings）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[グローバル エンドポイント（Global Endpoints）]** を選択します。

ステップ 3 [作業（Work）] ペインで、**[エンドポイント リッスン ポリシー（End Point Listen Policy）]** チェックボックスをオンにします。

ステップ 4 **[エンドポイント リッスン エンキャップ（End Point Listen Encap）]** ドロップダウン リストで、**[VLAN]** を選択します。

ステップ 5 **[エンドポイント リッスン エンキャップ（End Point Listen Encap）]** テキスト フィールドに、VLAN ID を入力します。有効な値は 1 ～ 4094 です。これは予約済みの VLAN カプセル化である必要があり、どの EPG でも使用できません。

ステップ 6 [Submit] をクリックします。

IP エージングの設定

このトピックでは、IP エージング ポリシーを有効にする方法について説明します。有効な場合、IP エージング ポリシーは、エンドポイント上の未使用の Ip 5 します。

管理状態が有効になっているときに、IP エージング ポリシーは、エンドポイントの ip アドレスを追跡する (IPv4) の ARP 要求と (IPv6) のネイバー要請を送信します。応答が指定されていない場合、ポリシーは、未使用の IPs 5 します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。

ステップ 2 をクリックして **エンドポイント コントロール** 。

ステップ 3 **Ip Aging** タブをクリックします。

ステップ 4 ポリシーを有効にするにはクリックして **Enabled** で、 **Administrative State** フィールド。

次のタスク

、、エンドポイント上の ip アドレスを追跡するために使用されるタイマーを指定する必要があるエンド ポイント保持ポリシーを作成します。移動 **テナント** > **テナント名** > > **ポリシー** > **プロトコル** > **エンド ポイント保持** 。

リモート エンドポイントの学習を無効にする

このトピックでは、有効化または IP エンド ポイント ラーニングを無効にする方法について説明します。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

Cisco Nexus 9000 シリーズのスイッチで 93128 を含むファブリックでは、このポリシーを有効にする必要がありますが正常に APIC リリース 2.2(2x) にアップグレードされた以降のすべてのノードが表示された後の N9K M12PQ アップリンク モジュール、TX、9396 PX または 9396 TX がスイッチします。

次の設定の変更のいずれか後に、、手動で以前に学習された IP エンドポイントをフラッシュする必要があります。

- リモート IP エンドポイント ラーニングが無効になっています
- 入力ポリシーの適用、VRF が設定されています。
- VRF に少なくとも 1 つのレイヤ 3 インターフェイスが存在します

以前に学習された IP エンドポイントを手動でフラッシュ、VPC ピアの両方で、次のコマンドを入力します: `vsh-c"システム内部 epm エンドポイントの vrf をクリア<vrf-name>リモート「 </vrf-name>`
。

IP エンドポイントの学習を有効または無効にするには、次の手順を実行します:

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
ステップ 2 **[Fabric Wide Setting]** をクリックします。
ステップ 3 チェック ボックスをクリックして **リモート EP 学習の無効化** 。
ステップ 4 [Submit] をクリックします。

サブネット チェックのグローバルな適用

このトピックでは、サブネットチェックを有効また無効にする方法について説明します。有効にすると、ある VRF で設定されたサブネットの外、つまり他のすべての VRF では、IP 学習が無効になります。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
ステップ 2 **[Fabric Wide Setting]** をクリックします。
ステップ 3 **Enforce Subnet Check** チェック ボックスをオンにします。

ステップ 4 [Submit] をクリックします。

GIPo の再割り当て

このトピックでは、非ストレッチ ブリッジ ドメインの GIPos の再割り当てを有効にして、ストレッチ ブリッジ ドメイン用のスペースを確保する方法について説明します。

Cisco ACI Multi-Site の導入により、GIPo 割り当て方式を変更して次の利点を提供する必要がありました。

1. 同じ GIPo を持つブリッジ ドメインの数を最小限に抑えます。
2. Cisco ACI Multi-Site 拡張ブリッジ ドメインに割り当てられた GIPos は、非拡張ブリッジ ドメインに割り当てられた GIPos と重複しません。

この割り当てを実現するために、Cisco ACI では、ストレッチされたブリッジ ドメインとストレッチされていないブリッジ ドメインの量に基づいてサイズが異なる複数のプールが導入されました。

Cisco ACI の新規インストールの場合、Cisco APIC は ＃1 と ＃2 の両方が実行されることを保証します。2.3(1) よりも前のリリースからの Cisco ACI のアップグレード中は、既存の GIPo が非ストレッチ ブリッジ ドメインにすでに使用されている可能性があるため、ファブリックの中断を避けるために古いスキーマが維持されます。その結果、Cisco ACI は ＃2 が完了したことを保証できません。

Cisco APIC のファブリック全体の設定ポリシーで **[GIPo の再割り当て（Reallocate GIPo）]** ノブを有効にすると、Cisco APIC は GIPos を再割り当てし、新しい割り当て方式を使用します。ノブの有効化は 1 回限りの操作です。その後、GIPos はオーバーラップしません。このノブは、2.3(1) より前のリリースから 3.0(1) 以降のリリースにアップグレードする場合にのみ、Cisco ACI Multi-Site Orchestrator の導入に関連します。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** を選択します。
ステップ 2 [Fabric Wide Setting] をクリックします。
ステップ 3 [Reallocate Gipo] のチェック ボックスをオンにします。
ステップ 4 [Submit] をクリックします。

ドメインの検証のグローバルな適用

このトピックでは、ドメインの検証を適用する方法について説明します。有効な場合、静的なパスを追加すると、EPGに関連付けられたドメインがないかどうか判断するために、検証チェックが実行されます。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 **[Fabric Wide Setting]** をクリックします。

ステップ 3 **Enforce Domain Validation** チェック ボックスをオンにします。

ステップ 4 [Submit] をクリックします。

OpFlex クライアント認証を有効にする

このトピックでは、GOLF および Linux 用の OpFlex クライアント認証を有効にする方法について説明します。

クライアントの ID がネットワークによって保証されない環境で GOLF または Linux Opflex クライアントをデプロイするには、クライアント証明書に基づいてクライアントの ID を動的に検証できます。

（注） 証明書の適用を有効にすると、クライアント認証をサポートしていない GOLF または Linux Opflex クライアントとの接続が無効になります。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 **[Fabric Wide Setting]** をクリックします。

ステップ 3 **OpFlex Client Authentication** のチェック ボックスをクリックして、GOLF および Linux Opflex クライアントのクライアント証明書認証を有効または無効にします。

ステップ 4 [Submit] をクリックします。

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 *6 : 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

Cisco APIC GUI を使用したロード バランサ ポリシーの作成

このトピックでは、デフォルトのロードバランサーポリシーを構成する方法について説明します。

ロード バランシング ポリシー オプションは、利用可能なアップリンク ポート間でトラフィックのバランスをとります。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。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 **[Load Balancer]** をクリックします。

ステップ 3 **[Dynamic Load Balancing Mode]** を選択します。

ダイナミック ロード バランシング (DLB) モードは、輻輳レベルに応じてトラフィックの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、間隔で区切られたフローからのパケットのバーストです。モードは **[Aggressive]**, **[Conservative]**, または **[Off]** (デフォルト)。

ステップ 4 **[オン（On）]** または **[オフ（Off）]**（デフォルト）を選択して、**ダイナミック パケットの優先順位付け**を有効または無効にします。

Dynamic Packet Prioritization (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 です。短いフローは、長いフローより遅延に敏感です。DPP により、アプリケーション全体のパフォーマンスが向上します。

ステップ 5 [Load Balancing Mode] を選択します。モードは、**Link Failure** または **Traditional** (デフォルト) です。

ロードバランサーの管理状態。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。

ステップ 6 [Submit] をクリックします。

CLI を使用したロード バランサ ポリシーの作成

CLI を使用したダイナミック ロード バランサ ポリシーの作成

ダイナミックアグレッシブ と **ダイナミック保守** の 2 つのダイナミック ロード バランサ モードがあります。**ダイナミックアグレッシブ** モードでは、より短い flowlet タイムアウト間隔が有効になり、**ダイナミック保守**モードでは、より長い flowlet タイムアウト間隔が有効になります。これらのコマンドの詳細については、『*Cisco APIC NX-OS* スタイル *CLI* コマンド資料』を参照してください。

このセクションでは、CLI を使用してダイナミック ロード バランサ ポリシーを設定する方法を示します。

手順

ステップ 1 アグレッシブ モードのダイナミック ロード バランシングを有効にするには、次の手順を実行します。

```
apic1# conf t
apic1# (config)# system dynamic-load-balance mode dynamic-aggressive
```

ステップ 2 保守モードのダイナミック ロード バランシングを有効にするには、次の手順を実行します。

```
apic1# conf t
apic1# (config)# system dynamic-load-balance mode dynamic-conservative
```

CLI を使用したダイナミック パケット優先順位付けポリシーの作成

ここでは、CLI を使用してダイナミック パケットの優先順位付けを有効にする方法を示します。このコマンドの詳細については、『*Cisco APIC NX-OS* スタイル *CLI* コマンド資料』を参照してください。

手順

ダイナミック パケット優位性を有効にします。

```
apic1# conf t
apic1# (config)# system dynamic-load-balance mode packet-prioritization
```

CLI を使用した GTP ロード バランサ ポリシーの作成

このセクションでは、CLI を使用して GTP ロード バランサ ポリシーを作成する方法を示します。このコマンドの詳細については、『*Cisco APIC NX-OS* スタイル *CLI* コマンド資料』を参照してください。

手順

ダイナミック パケット優位性を有効にします。

```
apic1# conf t
apic1# (config)# ip load-sharing address source_destination gtpu
```

REST API を使用したロード バランサ ポリシーの作成

このセクションでは、DLB、DPP、および GTP ロード バランサ ポリシーを有効にする方法を示します。使用可能なすべてのプロパティ値のリストについては、『*Cisco APIC* 管理情報モデル資料』を参照してください。

手順

DLB、DPP、およびGTPロードバランサポリシーを有効にするには、次の手順を実行します。

```
https://apic-ip-address/api/mo/uni.xml
<polUni>
<fabricInst>
 <lbpPol name="default" hashGtp="yes" pri="on" dlbMode="aggressive">
 </lbpPol>
</fabricInst>
</polUni>
```

時間精度ポリシーの有効化

このトピックでは、ネットワーク上の分散ノードの時間同期プロトコルである Precision Time Protocol (PTP) を有効にする方法について説明します。そのハードウェアのタイムスタンプ機能は、ネットワーク タイム プロトコル（NTP）などの他の時刻同期プロトコルより高い精度を実現します。

PTPは、システムのリアルタイムPTPクロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスタークロック（階層の最上部にあるクロック）を持つマスター/メンバー同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTPタイミングメッセージを交換することによって実現されます。PTPは、PTPドメインと呼ばれる論理範囲内で動作します。

リリース4.2（5）より前は、PTP機能はCisco ACIファブリック内でのみサポートされていました。リリース4.2（5）以降、PTP機能はCisco ACIファブリックの外部でサポートされるようになりました。Cisco ACIファブリック外部のグランドマスターとクライアントは、Cisco ACIファブリック内のスイッチの前面パネルポートに接続できます。

（注） グランドマスター スイッチのクライアントとして構成されているCisco ACIファブリック内のスイッチに接続できる外部グランドマスター スイッチは1つだけです。現時点では、複数の外部グランド マスター スイッチを単一のクライアント スイッチに接続することはサポートされていません。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** を選択します。

ステップ 2 **Precision Time Protocol** をクリックします。

ステップ 3 **Enabled** または **Disabled** を選択します。

PTP を無効にするように選択した場合は、NTP の時間がファブリックを同期するために使用されます。PTP を有効にすると、サイト全体を同期するためのマスターとしてあるスパインが自動的に選択されます。

ステップ 4 [Submit] をクリックします。

グローバル システム GIPo ポリシーの有効化

このトピックでは、インフラ テナント GIPo をシステム GIPo として使用する方法について説明します。

ACI マルチポッドを導入するには、239.255.255.240 のシステム グローバル IP アウトサイド (GIPo) を、インターポッド ネットワーク (IPN) 上で、PIM BIDIR の範囲として設定する必要があります。この、IPN デバイス上での 239.255.255.240 PIM BIDIR 範囲の設定は、インフラ GIPo をシステム GIPo として使用することによって回避できます。

始める前に

リーフ スイッチおよびスパイン スイッチを含む、ACI ファブリックのすべてのスイッチを、最新の APIC リリースにアップグレードします。

手順

ステップ 1 メニューバーで、 **System** > **System Settings** の順にクリックします。

ステップ 2 **Enabled** または **Disabled** (デフォルト) を、**Use Infra GIPo as System GIPo** で選択します。

ステップ 3 [Submit] をクリックします。

ファブリック ポート トラッキング ポリシーの設定

アップリンク障害検出は、ファブリック アクセス ファブリック ポート トラッキング ポリシーで有効にできます。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 スイッチ間のリンクの状態を監視します。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。ファブリック ポートトラッキングの詳細については、 *Cisco APIC Layer 2 Networking Configuration Guide*を参照してください。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** を選択します。
ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポート トラッキング（Port Tracking）]** を選択します。
ステップ 3 **Port tracking state** を **on** に設定して、ポート トラッキングを有効にします。
ステップ 4 （任意） **[毎日の復元タイマー（Daily restore timer）]** の値を変更します。
ステップ 5 **ポート トラッキング パラメータをトリガーするアクティブなスパイン リンク**の数を設定します。
ステップ 6 [Submit] をクリックします。

グローバル ファブリック アクセス ポリシーのプロビジョニング

グローバル接続可能アクセス エンティティ プロファイルの作成

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。

始める前に

接続されているエンティティ プロファイルに関連付けられるテナント、VRF インスタンス、アプリケーション プロファイルおよび EPG を作成します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** の順にクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 **[接続可能なアクセス エンティティ プロファイル]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成]** を選択します。

ステップ 4 ポリシーの名前を入力します。

ステップ 5 **[ドメイン]** テーブル上の [+] アイコンをクリックします。

ステップ 6 物理ドメイン、以前に作成した物理、レイヤ 2、レイヤ 3、ファイバ チャネル ドメインを入力するか、新規作成します。

ステップ 7 ドメインのカプセル化を入力して、**[更新]** をクリックします。

ステップ 8 **[EPG 展開]** テーブルの [+] アイコンをクリックします。

ステップ 9 テナント、アプリケーション プロファイル、EPG カプセル化（vlan-1 など）、プライマリ カプセル化（プライマリ カプセル化番号）、インターフェイス モードを入力します（トランク、802.1P またはアクセス（タグなし）。

ステップ 10 **Update** をクリックします。

ステップ 11 [Next] をクリックします。

ステップ 12 接続可能なエンティティ プロファイルに関連付けるインターフェイスを選択します。

ステップ 13 **[完了（Finish）]** をクリックします。

QoS クラスのグローバル ポリシーを設定します。

グローバル QoS クラス ポリシーを使用できます。

- CoS を保持する、CoS 値を保証するために、優先度レベル 802.1 P のパケット数を入力し、ACI ファブリックを通過するが保持されます。802.1 P 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。Multipod トポロジは、CoS の保持を使用できますポッド 1 を入力して、ポッド 2 外からの 802.1 P トラフィックの優先順位の QoS の設定を保持したいですが、CoS の保持を行わない/interpod の DSCP 設定のネットワーク (IPN) トラフィックポッド間。CoS を保持するために multipod トラフィックが通信中、IPN の DSCP 設定を使用して、DSCP ポリシー/(で設定されている **テナント** > **インフラ** > > **ポリシー** > **プロトコル** > **DSCP クラス-cos L3 トラフィックのポリシーの変換**)
- 次のように、デフォルトの QoS クラス レベルのプロパティをリセットします **MTU** 、**キュー制限** 、または **スケジューリング アルゴリズム** 。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** の順にクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 **QOS Class** をクリックします。

ステップ 4 CoS 802.1 P の有効化にして、をクリックして、 **保持 COS** チェック ボックス。

ステップ 5 QoS クラスのデフォルト設定を変更するには、それをダブルクリックします。新しい設定を入力し、**Submit** をクリックします。

グローバル DHCP リレー ポリシーの作成

グローバル DHCP リレー ポリシーは、ファブリック全体の異なるテナントのブリッジ ドメインによって参照できる DHCP リレー サーバを識別します。テナント DHCP リレーでは、プロバイダ EPG が common テナントにある場合でも、各テナントで DHCP リレー ポリシーを構成する必要があります。グローバル DHCP リレー ポリシーは、任意のテナントから参照でき、各テナントで DHCP リレー ポリシーを構成する必要がないという点で、テナントの DHCP リレー ポリシーとは異なります。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** の順にクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 **DHCP Relay** を右クリックし、**Create DHCP Relay Policy** を選択します。

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

a) [Name] フィールドに、DHCP リレー プロファイル名（DhcpRelayP）を入力します。

この名前では最大 64 文字までの英数字を使用できます。

b) （任意） [説明（Description）] フィールドに、DHCP リレー ポリシーの説明を入力します。

説明には最大 128 文字までの英数字を使用できます。

c) [Providers] を展開します。

[DHCP プロバイダーの作成（Create DHCP Provider）] ダイアログボックスが表示されます。

d) [Create DHCP Provider] ダイアログボックスの [EPG Type] フィールドで、DHCP サーバがどこで接続されているかによって適切なオプション ボタンをクリックします。

選択する EPG タイプのオプションは、EPG タイプによって異なります。

- EPG タイプとして **[アプリケーション EPG（Application EPG）]** を選択すると、次のオプションが **[アプリケーション EPG（Application EPG）]** 領域に表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。（infra）
  - [Application Profile] フィールドで、ドロップダウン リストから、アプリケーションを選択します。（access）
  - [EPG] フィールドで、ドロップダウン リストから、EPG を選択します。（デフォルト）
- EPG タイプとして **[L2 外部ネットワーク（L2 External Network）]** を選択すると、**[L2 外部ネットワーク領域（L2 External Network）]** に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L2 Out]** フィールドで、ドロップダウン リストから [L2 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。
- EPG タイプとして **[L3 外部ネットワーク（L3 External Network）]** を選択すると、**[L3 外部ネットワーク（L3 External Network）]**領域に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L3 Out]** フィールドで、ドロップダウン リストから [L3 Out] を選択します。

- **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。

- EPG タイプとして **[DN]** を選択した場合は、ターゲット エンドポイント グループの識別名を入力します。

e) [DHCP サーバ アドレス（DHCP Server Address）] フィールドに、DHCP サーバの IP アドレスを入力します。

f) **[DHCP サーバ設定（DHCP Server Preference）]** フィールドで、**[なし（None）]** または **[サーバ VRF を使用（Use Server VRF）]**を選択します。

[DHCP サーバー プレファレンス（DHCP Server Preference）] フィールドは、リリース 5.2(4) 以降で使用できます。リーフ スイッチは、このフィールドの値を基に、クライアント VRF またはサーバー VRF のどちらから DHCP リレー パケットをルーティングするかを決定します。詳細については、DHCP サーバー設定フィールドについて （163 ページ）を参照してください。

- **[なし（None）]** : これはデフォルトのオプションで、リリース 5.2(4) より前の動作を反映しています。**[なし（None）]** オプションを選択すると、スイッチは常にクライアント VRF からの DHCP リレー パケットをルーティングします。VRF 間 DHCP リレーに使用する場合、サーバー VRF ネットワークをクライアント VRF にリークするには、共有サービス コントラクトが必要です。

- **[サーバー VRF を使用（Use Server VRF）]** : このオプションは、リリース 5.2(4) で導入された新しい動作を反映しています。**[サーバー VRF を使用（Use Server VRF）]** オプションを選択すると、スイッチは、DHCP クライアントが存在する EPG と DHCP サーバーが存在する EPG（またはDHCP サーバーが到達可能な L3Out のレイヤー 3 外部）の間にコントラクトがあるかどうかには関わりなく、サーバー VRF からの DHCP リレー パケットをルーティングします。

  VRF 間設定の場合、**[サーバー VRF を使用（Use Server VRF）]** オプション（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）を選択すると、ルート ルックアップのため、サーバー サブネット ルートは、クライアント リーフ スイッチのサーバ - VRF 内でプログラムされます。クライアント リーフ スイッチの DHCP プロセスは、それ以後、DHCP リレー パケットをサーバー VRF 経由で送信します。このため、サーバー VRF は、クライアント ブリッジ ドメインが展開されているすべてのリーフ スイッチに少なくとも 1 つの IP アドレスを使用して展開する必要があります。

g) [OK] をクリックします。

[DHCP リレー ポリシーの作成（Create DHCP Relay Policy）] ウィンドウに戻ります。

h) [Submit] をクリックします。

DHCP リレー ポリシーが作成されます。

グローバル MCP インスタンス ポリシーの有効化にします。

グローバル Mis-Cabling プロトコル (MCP) インスタンス ポリシーを有効にします。現在の実装では、システムで MCP の 1 つだけのインスタンスが実行されます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** の順にクリックします。
ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。
ステップ 3 をクリックして **MCP インスタンス ポリシーのデフォルト** 。
ステップ 4 **Admin State** を **Enabled** に変更します。
ステップ 5 必要に応じて、ファブリックの他のプロパティを設定します。
ステップ 6 [Submit] をクリックします。

次のタスク

作成エラーには、回復ポリシーが無効になっています

エラーディセーブル回復ポリシーは、1つ以上の事前定義されたエラー状態が無効になっていたポートを再度有効にするポリシーを指定します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** の順にクリックします。
ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。
ステップ 3 をクリックして **エラーには、回復ポリシーが無効になっている** .
ステップ 4 回復ポリシーを有効にするイベントをダブルクリックします。
ステップ 5 チェック ボックスをクリックし、をクリックして **更新** 。
ステップ 6 オプション。その他のイベントについて、ステップ 4 と 5 を繰り返します。
ステップ 7 オプション。リセット、 **エラー復旧間隔 (秒) の無効化** 。
ステップ 8 [送信（Submit）] をクリックします。

ポート単位ポリシー

ポート単位ポリシーについて

ポート単位ポリシーは、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してリーフ スイッチのインターフェイスを設定するために使用する暗黙的なポリシーです。ポート単位ポリシーは、標準のポリシーベース モデルと比較して単純化されています。これは、Cisco APIC を使用する方法を学習し続けています。この簡素化のため、既存のポリシーに新しいポートを追加することはできません。代わりに、インターフェイスごとにポリシーの新しいチャンクのみを作成できます。

ポート単位のポリシーペインでは、バックグラウンドで NX-OS CLI を使用して、暗黙的および明示的なオブジェクトを作成します。たとえば、新しいポート チャネルを作成すると、明示的なポート チャネルポリシー グループと暗黙的なオーバーライドが作成されます。明示的なポリシー グループへの変更は、暗黙的なポリシー グループが削除されるまでポートに適用されません。CLI と GUI を組み合わせて使用しないことを推奨します。再利用可能なポリシー設定の高度な使用例に移行する場合は、ポート ポリシー ウィザードを使用して Cisco Application Centric Infrastructure（ACI）ポリシー モデルについて学習し、同じウィザードからポートを設定解除します。

ポート単位のポリシーは、次の GUI の場所からのみ作成できます。

[ファブリック（Fabric）] > **[インベントリ（Inventory）]** > ***[Pod-#]*** > ***[leaf-switch-name]*** > **[インターフェイス タブ（Interface）] タブ**

（注） **[インターフェイス（Interface）]** タブは、作業ペインの **[インターフェイス（Interface）]** タブを参照します。これは、ナビゲーション ペインの **[インターフェイス（Interfaces）]** フォルダではありません。

GUI を使用したポート ポリシーごとの設定

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して、ポート ポリシーごとのポリシーを作成します。

手順

ステップ 1 メニュー バーで、 **[Fabric]** > **[Inventory]** を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***pod-#*** > ***leaf-switch-name*** を選択します。

ステップ 3 [作業（Work）] ペインで、**[インターフェイス（Interface）]** タブを選択します。

ステップ 4 **[モード（Mode）]** ドロップダウン リストで、**[設定（Configuration）]** を選択します。

ステップ 5 インターフェイス番号を 1 つ以上クリックして、それらのインターフェイスを選択します。

[作業（Work）]ペインのタブのすぐ下にあるボタンが、選択したインターフェイスに設定できるコンポーネントでアクティブになります。

ステップ 6 設定するコンポーネントのいずれかのボタンをクリックします。

[作業（Work）] ペインにはそのコンポーネントのプロパティが表示されます。

ステップ 7 コンポーネントのプロパティを必要に応じて設定します。

ステップ 8 **[送信（Submit）]** をクリックします。`

ステップ 9 選択したインターフェイスの追加コンポーネントを設定するか、別のインターフェイスを選択してコンポーネントを設定します。

GUI を使用したポート ポリシーごとの確認

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してポート単位ポリシーを検証する方法について説明します。

始める前に

非表示ポリシーを表示するには、Cisco APIC を設定する必要があります。デフォルトでは、ポート単位のポリシーは Cisco APIC に表示されません。

手順

ステップ 1 メニュー バーで、 **[Fabric]** > **[Inventory]** を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***pod-#*** > ***leaf-switch-name*** を選択します。

ステップ 3 [作業（Work）] ペインで、**[インターフェイス（Interface）]** タブを選択します。

ステップ 4 **[モード（Mode）]** ドロップダウン リストで、**[設定（Configuration）]** を選択します。

ステップ 5 インターフェイス数を選択する場合は、そのインターフェイス名をクリックします。

[作業（Work）]ペインのタブのすぐ下にあるボタンが、選択したインターフェイスに設定できるコンポーネントでアクティブになります。

ステップ 6 プロパティを表示するコンポーネントのいずれかのボタンをクリックします。

[作業（Work）] ペインに、そのコンポーネントのプロパティが表示されます。

ステップ 7 プロパティが正しく設定されていることを確認し、目的の設定に対して正しくない値を変更します。

ステップ 8 変更を加えた場合は、**[送信（Submit）]**をクリックします。アンインストールしない場合は、[キャンセル（Cancel）] をクリックします。

GUI を使用した非表示ポリシーの表示

デフォルトでは、ポート単位のポリシーなどの一部のポリシーは Cisco Application Policy Infrastructure Controller（APIC）に表示されません。これらのポリシーを表示するには、非表示のポリシーを表示するように Cisco APIC を設定する必要があります。

手順

ステップ 1 GUI の右上隅にある **[マイ プロファイルの管理（Manage My Profile）]** > **[設定（Settings）]** を選択します。

[アプリケーション設定（Application Settings）] ダイアログが開きます。

ステップ 2 **[非表示ポリシーの表示（Show Hidden Policies）]** ボックスにチェックを付けます。

ステップ 3 **[OK]** をクリックします。

GUI を使用した誤配線プロトコル インターフェイス ポリシーの作成（任意）

誤配線プロトコル（MCP）は、Link Layer Discovery Protocol（LLDP）、スパニング ツリー プロトコル（STP）が検出できない設定ミスを処理するために設計されました。MCP には、それを使用するレイヤ 2 パケットがあり、MCP はファブリック内のループを形成するポートを無効にします。Cisco Application Centric Infrastructure（ACI）ファブリック リーフ スイッチはスパニング ツリー プロトコル（STP）に参加せず、STP に関してハブとして動作します。MCP パケットが送信された後、ファブリックがパケットが戻ったことを確認し、ループが存在することを認識した場合、ファブリックはそのイベントに基づいてアクションを実行します。これが発生するとエラーとイベントが生成されます。MCP は、グローバルに、およびインターフェイスごとに有効にできます。デフォルトでは、MCP がグローバルに無効にされ、各ポートで有効になっています。MCP が機能するには、インターフェイス単位の設定に関係なく、グローバルに有効にする必要があります。

次の手順では、GUI を使用して MCP インターフェイス ポリシーを作成します。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）]** > **[インターフェイス（Interface）]** > **[MCP インターフェイス（MCP Interface）]** の順に選択します。

ステップ 3 [作業（Work）] ペインで、**[アクション（Actions）]** > **[誤配線プロトコル インターフェイス ポリシーの作成（Create Mis-cabling Protocol Interface Policy）]** の順に選択します。

ステップ 4 [Create Mis-cabling Protocol Interface Policy] ダイアログボックスで、次の操作を実行します。

a) ポリシーの名前を入力します。

b) （任意） ポリシーの説明を入力します。

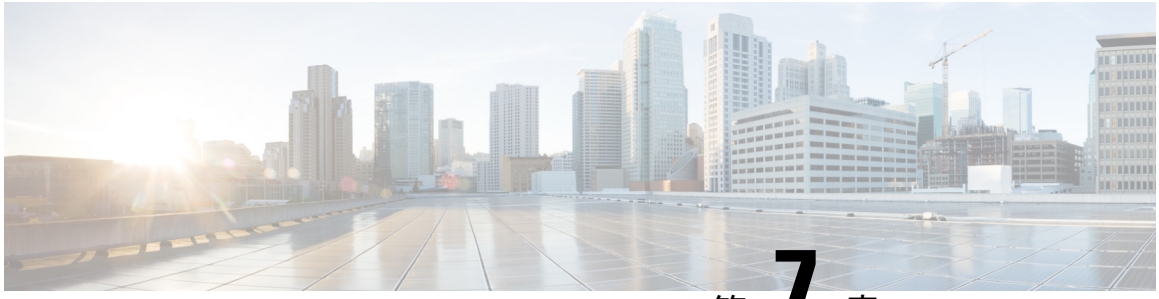
c) **[管理状態（Admin State）]** に対して、ポリシーを有効にするには **[有効（Enable）]** を選択し、ポリシーを無効にするには **[無効（Disable）]** を選択します。

d) MCP の操作モードとして **[精密（Strict）]** または **[非精密（Non-strict）]** を選択します。

[精密（Strict）] を選択すると、次の追加フィールドが表示されます。

- **[初期遅延時間（秒）（Initial Delay Time（sec）]**: 外部レイヤ 2 ネットワークでの STP コンバージェンスの時間。デフォルト値は 0 です（レイヤー 2 ネットワークで STP が無効になっている場合）。STP が有効になっている場合、STP が収束するまでの初期遅延時間の範囲は、スケール/トポロジにもよりますが、45 ～ 60 秒です。
- **[送信頻度（秒、ミリ秒）（Tranmission Frequency（sec, msec）]**: 各レイヤ 2 インターフェイスの猶予期間まで、MCP パケットが送信される頻度を決めるタイマー。デフォルトの値は 500 ミリ秒です。
- 猶予期間 (秒、ミリ秒) : 早期ループ検出が行われる猶予期間の時間。ポートは、ループ検出に使用される MCP パケットを積極的に送信します。デフォルトの猶予期間の値は 3 秒です。

ステップ 5 [Submit] をクリックします。



第 7 章

基本ユーザ テナント設定

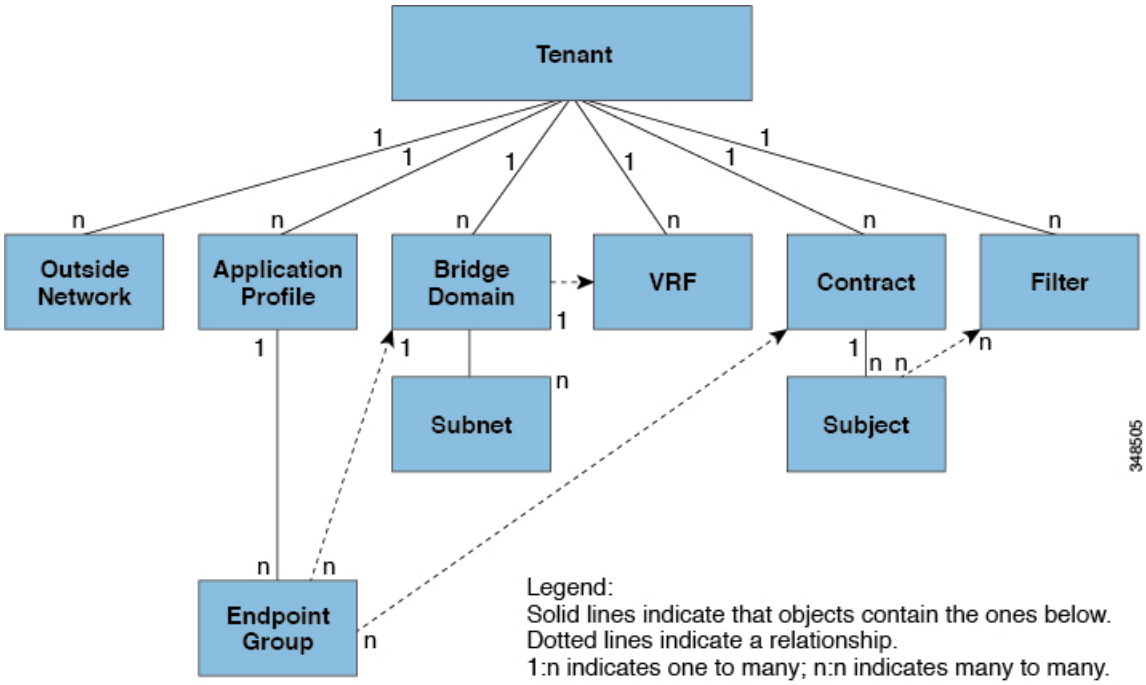
この章は、次の内容で構成されています。

- テナント （223 ページ）
- テナント内のルーティング （224 ページ）
- テナント、VRF、およびブリッジ ドメインの作成 （237 ページ）
- EPG の導入 （240 ページ）
- マイクロセグメント EPG （246 ページ）
- アプリケーション プロファイルと契約の導入 （251 ページ）
- コントラクト パフォーマンスの最適化 （261 ページ）
- 契約とサブジェクトの例外 （265 ページ）
- EPG 内契約 （267 ページ）
- EPG のコントラクト継承 （276 ページ）
- 優先グループ契約 （281 ページ）
- 許可ルールと拒否ルールを含む契約 （285 ページ）

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 *2:* 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。

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

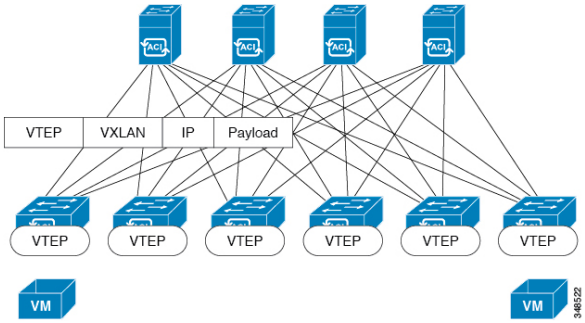
ントがあるすべてのスイッチにわたります。各入力インターフェイスはデフォルトのゲートウェイ インターフェイスをサポートし、ファブリック全体のすべての入力インターフェイスは任意のテナント サブネットに対する同一のルータの IP アドレスと MAC アドレスを共有します。

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3VNID

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 *3 : 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

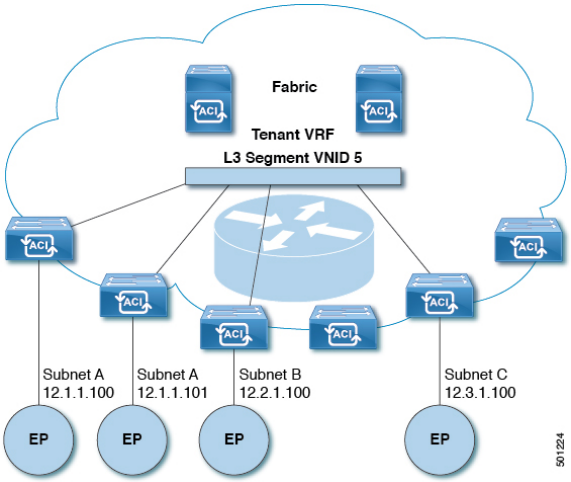
IP インターフェイスには一意の IP アドレスがあります。これは、インフラストラクチャ VLAN として知られる、転送 IP ネットワーク上の VTEP を識別します。VTEP デバイスはこの IP アドレスを使用してイーサネット フレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。また、VTEP デバイスはリモート VTEP で VXLAN セグメントを検出し、IP インターフェイスを介してリモートの MAC Address-to-VTEP マッピングについて学習します。

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 *4: 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。

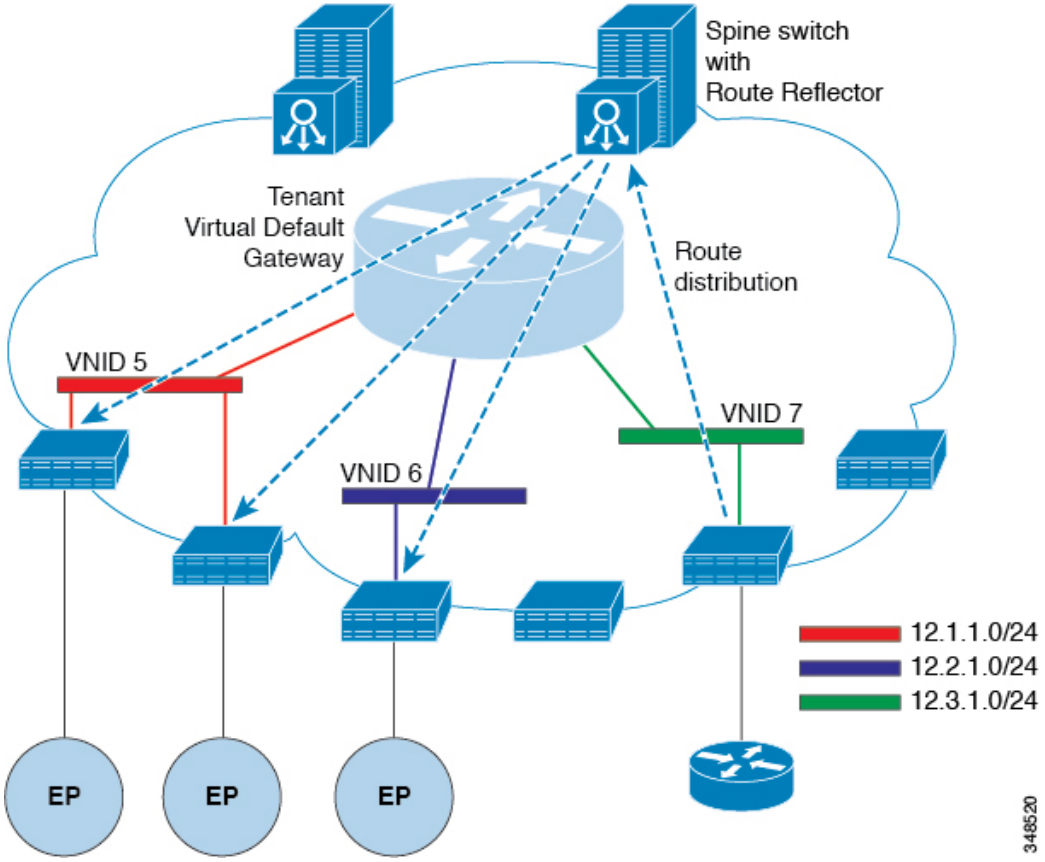
各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

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。

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 *5:* ルータのピアリング

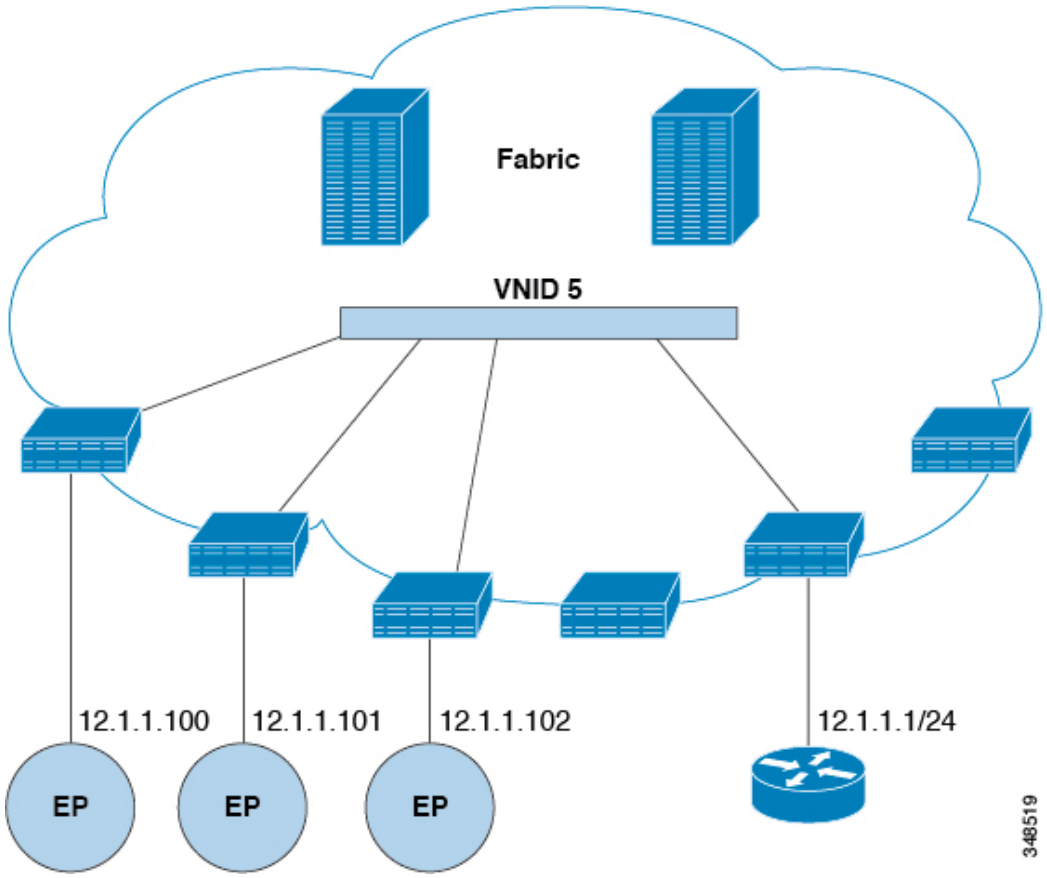


ピアリングによって学習されるルートは、スパイン スイッチに送信されます。スパイン スイッチはルート リフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフ スイッチに配布します。これらのルートは、最長プレフィクス照合 (LPM) により集約されたアドレスで、外部ルータが接続されているリモートのリーフ スイッチの VTEP IP アドレスが含まれるリーフ スイッチの転送テーブルに配置されます。WAN ルートには転送プロキシはありません。WAN ルートがリーフ スイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。外部ルータがデフォルト ゲー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

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 *6 :* 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。

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。

Layer 3 Out を使用した外部接続の設定

この項では、ACI ファブリックが L3Out および MP-BGP ルート リフレクタを介して外部ルーテッド ネットワークに接続するために必要な手順を段階的に説明します。

この例では、Open Shortest Path First（OSPF）を「mgmt」テナント下の L3Out のルーティング プロトコルとして使用します。

GUI を使用した MP-BGP ルート リフレクタの設定

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順に選択します。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、[**BGP ルート リフレクタ**（**BGP Route Reflector**）] を右クリックして、[**ルート リフレクタ ノードの作成**（**Create Route Reflector Node**）] をクリックします。

ステップ 3 **[ルート リフレクタ ノードの作成**（**Create Route Reflector Node**）] ダイアログ ボックスで、[**スパイン ノード**（**Spine Node**）] ドロップダウン リストから、適切なスパイン ノードを選択します。**Submit** をクリックします。

（注）
必要に応じてスパイン ノードを追加するには、上記の手順を繰り返してください。

スパイン スイッチがルート リフレクタ ノードとしてマークされます。

ステップ 4 **BGP Route Reflector** プロパティ エリアの **Autonomous System Number** フィールドで、適切な番号を選択します。**Submit** をクリックします。

（注）
自律システム番号は、Border Gateway Protocol（BGP）がルータに設定されている場合は、リーフが接続されたルータ設定に一致する必要があります。スタティックまたは Open Shortest Path First（OSPF）を使用して学習されたルートを使用している場合は、自律システム番号値を任意の有効な値にできます。

ステップ 5 メニュー バーで、**[ファブリック**（**Fabric**）**]** > **[ファブリック ポリシー**（**Fabric Policies**）**]** > **[ポッド**（**Pods**）**]** > **[ポリシー グループ**（**Policy Groups**）**]** をクリックします。

ステップ 6 **[ナビゲーション**（**Navigation**）] ペインで、[**ポリシー グループ**（**Policy Groups**）] を展開して右クリックし、[**POD ポリシー グループの作成**（**Create POD Policy Group**）] をクリックします。

ステップ 7 **[ポッド ポリシー グループの作成（Create Pod Policy Group）]** ダイアログ ボックスで、**[名前（Name）]** フィールドに、ポッド ポリシー グループの名前を入力します。

ステップ 8 [BGP Route Reflector Policy] ドロップダウン リストで、適切なポリシー（デフォルト）を選択します。[Submit] をクリックします。`
BGP ルート リフレクタのポリシーは、ルート リフレクタのポッド ポリシー グループに関連付けられ、BGP プロセスはリーフ スイッチでイネーブルになります。

ステップ 9 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[プロファイル（Profiles）]** > **[ポッド プロファイル デフォルト（Pod Profile default）]** > **[デフォルト（default）]** を選択します。

ステップ 10 [Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、前に作成されたポッド ポリシーを選択します。[Submit] をクリックします。`
ポッド ポリシー グループが、ファブリック ポリシー グループに適用されました。

ACI ファブリックの MP-BGP ルート リフレクタの設定

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

次に、MP-BGP ルート リフレクタの設定例を示します。

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

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

REST API を使用した MP-BGP ルート リフレクタの設定

手順

ステップ 1 スパイン スイッチをルート リフレクタとしてマークします。

例：

```
POST https://apic-ip-address/api/policymgr/mo/uni/fabric.xml

<bgpInstPol name="default">
  <bgpAsP asn="1" />
  <bgpRRP>
     <bgpRRNodePEp id="<spine_id1>"/>
     <bgpRRNodePEp id="<spine_id2>"/>
  </bgpRRP>
</bgpInstPol>
```

ステップ 2 次のポストを使用してポッド セレクタをセットアップします。

例：

FuncP セットアップの場合：

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricFuncP>
  <fabricPodPGrp name="bgpRRPodGrp”>
    <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default" />
  </fabricPodPGrp>
</fabricFuncP>
```

例：

PodP セットアップの場合：

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricPodP name="default">
  <fabricPodS name="default" type="ALL">
    <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp"/>
  </fabricPodS>
</fabricPodP>
```

MP-BGP ルート リフレクタ設定の確認

手順

ステップ 1 次の操作を実行して、設定を確認します。

a) セキュア シェル（SSH）を使用して、必要に応じて各リーフ スイッチへの管理者としてログインします。

b) show processes | grep bgp コマンドを入力して、状態が S であることを確認します。

状態が NR（実行していない）である場合は、設定が正常に行われませんでした。

ステップ 2 次の操作を実行して、自律システム番号がスパイン スイッチで設定されていることを確認します。

a) SSH を使用して、必要に応じて各スパイン スイッチへの管理者としてログインします。

b) シェル ウィンドウから次のコマンドを実行します。

例：

cd /mit/sys/bgp/inst

例：

grep asn summary

設定した自律システム番号が表示される必要があります。自律システム番号の値が 0 と表示される場合は、設定が正常に行われませんでした。

GUI を使用した管理テナントの OSPF L3Out の作成

- ルータ ID と論理インターフェイス プロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF L3Out を作成するためのものです。テナントの OSPF L3Out を作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、『*Cisco APIC and Transit Routing*』を参照してください。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[mgmt]** の順に選択します。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、**[ネットワーキング**（**Networking**）**]** > **[L3Outs]** を展開します。

ステップ 3 [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] をクリックします。

[**L3Out の作成**（**Create L3Out**）] ウィザードが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウで、次の操作を実行します。

a) [Name] フィールドに、名前（RtdOut）を入力します。
b) [VRF] フィールドのドロップダウン リストから、VRF（inb）を選択します。

（注）
このステップでは、ルーテッド Outside をインバンド VRF に関連付けます。

c) [L3 ドメイン（L3 Domain）] ドロップダウン リストから、適切なドメインを選択します。
d) [OSPF] チェックボックスをオンにします。
e) [OSPF Area ID] フィールドに、エリア ID を入力します。
f) [OSPF Area Control] フィールドで、適切なチェックボックスをオンにします。
g) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
h) [OSPF Area Cost] フィールドで、適切な値を選択します。
i) **[次へ**（**Next**）**]** をクリックします。

[**ノードとインターフェイス**（**Nodes and Interfaces**）] ウィンドウが表示されます。

ステップ 5 [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで、次の操作を実行します。

a) [デフォルトを使用（Use Defaults）] ボックスをオフにします。

これにより、[ノードプロファイル名（Node Profile Name）] フィールドを編集できます。

b) [**ノード プロファイル名**（**Node Profile Name**）] フィールドに、ノード プロファイルの名前を入力します（borderLeaf）。

c) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
d) [Router ID] フィールドに、一意のルータ ID を入力します。
e) ループバック アドレスにルータ ID を使用しない場合は、[ループバック アドレス（Loopback Address）] フィールドで別の IP アドレスを使用するか、空のままにします。

（注）
[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

f) 必要に応じて、このノードの [インターフェイス（Interface）]、[IP アドレス（IP Address）]、[インターフェイス プロファイル名（Interface Profile Name）]、および [MTU] フィールドに適切な情報を入力します。
g) [ノード（Nodes）] フィールドで、[+] アイコンをクリックして、別のノードの 2 番目のフィールド セットを追加します。

（注）
2 つ目のノード ID を追加します。

h) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
i) [Router ID] フィールドに、一意のルータ ID を入力します。
j) ループバック アドレスにルータ ID を使用しない場合は、[ループバック アドレス（Loopback Address）] フィールドで別の IP アドレスを使用するか、空のままにします。

（注）
[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

k) 必要に応じて、このノードの [インターフェイス（Interface）]、[IP アドレス（IP Address）]、[インターフェイス プロファイル名（Interface Profile Name）]、および [MTU] フィールドに適切な情報を入力します。
l) **[次へ（Next）]** をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 6 [プロトコル（Protocols）] ウィンドウの [ポリシー（Policy）] 領域で、[デフォルト（default）] をクリックし、[次（Next）] をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 7 [外部 EPG（External EPG）] ウィンドウで次のアクションを実行します。

a) [Name] フィールドに、外部ネットワークの名前（extMgmt）を入力します。
b) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）]フィールドをオフにします。

[サブネット（Subnets）] 領域が表示されます。

c) [+] をクリックして [サブネットの作成（Create Subnet）] ダイアログ ボックスにアクセスします。
d) [サブネットの作成（Create Subnet）] ダイアログ ボックスで、[IP アドレス（IP address）] フィールドに、サブネットの IP アドレスとマスクを入力します。
e) [Scope] フィールドで、目的のチェックボックスをオンにします。[OK] をクリックします。
f) [外部 EPG（External EPG）] ダイアログ ボックスで、[完了（Finish）]をクリックします。

（注）
[作業（Work）] ペインの [L3Outs] 領域に、[L3Out] アイコン（RtdOut）が表示されます。

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

外部ルーテッド ネットワーク接続の設定には、次のステップがあります。

1. テナントの下に VRF を作成します。
2. 外部ルーテッド ネットワークに接続された境界リーフ スイッチの VRF の L3 ネットワーキング構成を設定します。この設定には、インターフェイス、ルーティング プロトコル (BGP、OSPF、EIGRP) 、プロトコル パラメータ、ルートマップが含まれています。
3. テナントの下に外部 L3 EPG を作成してポリシーを設定し、これらの EPG を境界リーフ スイッチに導入します。ACI ファブリック内で同じポリシーを共有する VRF の外部ルーテッド サブネットが、1 つの「外部 L3 EPG」または 1 つの「プレフィクス EPG」を形成します。

設定は、2 つのモードで実現されます。

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

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

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

手順

ステップ 1 VLAN ドメインを設定します。

例：

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

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

例：

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

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

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24 scope public
apic1(config-tenant-interface)# exit
```

ステップ 4 リーフの VRF を設定します。

例：

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

ステップ 5 OSPF エリアを設定し、ルート マップを追加します。

例：

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

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

例：

（注）

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

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

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

例：

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

ステップ 8 リーフ スイッチの外部 L3 EPG を導入します。

例：

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

テナント、VRF、およびブリッジ ドメインの作成

テナントの概要

- テナントには、承認されたユーザのドメインベースのアクセス コントロールをイネーブルにするポリシーが含まれます。承認されたユーザは、テナント管理やネットワーキング管理などの権限にアクセスできます。
- ユーザは、ドメイン内のポリシーにアクセスしたりポリシーを設定するには読み取り/書き込み権限が必要です。テナント ユーザは、1 つ以上のドメインに特定の権限を持つことができます。
- マルチテナント環境では、リソースがそれぞれ分離されるように、テナントによりグループ ユーザのアクセス権限が提供されます(エンドポイント グループやネットワーキングな

どのため)。これらの権限では、異なるユーザが異なるテナントを管理することもできます。

テナントの作成

テナントには、最初にテナントを作成した後に作成できるフィルタ、契約、ブリッジ ドメイン、およびアプリケーション プロファイルなどのプライマリ要素が含まれます。

VRF およびブリッジ ドメイン

テナントの VRF およびブリッジ ドメインを作成および指定できます。定義されたブリッジ ドメイン要素のサブネットは、対応するレイヤ 3 コンテキストを参照します。

IPv6 ネイバー探索を有効にする方法については、『*Cisco APIC Layer 3 Networking Guide*』の「*IPv6 and Neighbor Discovery*」を参照してください。

GUI を使用したテナント、VRF およびブリッジ ドメインの作成

外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[テナントの追加（Add Tenant）]** を選択します。

ステップ 2 [Create Tenant] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。

b) **[セキュリティ ドメイン（Security Domains）]** セクションで、**[+]** をクリックして、**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスを開きます。

c) **[名前（Name）]** フィールドに、セキュリティ ドメインの名前を入力し、**[送信（Submit）]** をクリックします。

d) **[テナントの作成（Create Tenant）]** ダイアログ ボックスで、作成したセキュリティ ドメインの **[更新（Update）]** をクリックします。

e) 必要に応じて他のフィールドに入力します。

f) [送信（Submit）] をクリックします。

テナント名 > **[ネットワーキング（Networking）]** 画面が表示されます。

ステップ 3 **[作業（Work）]** ペインで、**[VRF]** アイコンをキャンバスにドラッグして **[Create VRF]** ダイアログボックスを開き、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。

b) 必要に応じて他のフィールドに入力します。

c) **[送信（Submit）]** をクリックして VRF インスタンスの設定を完了します。

ステップ 4 **[作業（Work）]** ペインで、VRF インスタンスを囲む円内のキャンバスに **[ブリッジ ドメイン（Brdige Domain）]** アイコンをドラッグして、2 つを接続します。[Create Bridge Domain] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) 必要に応じて他のフィールドに入力します。
c) [次へ（Next）] をクリックします。
d) **[サブネット（Subnets）]** セクションで、**[+]** をクリックして、**[サブネットの作成（Create Subnet）]** ダイアログ ボックスを開きます。
e) **[ゲートウェイ IP**（Gateway IP）] フィールドに、IP アドレスとサブネット マスクを入力します。
f) 必要に応じて他のフィールドに入力します。
g) [OK] をクリックします。
h) **[ブリッジ ドメインの作成（Create Bridge Domain）]** ダイアログ ボックスに戻り、必要に応じて他のフィールドに入力します。
i) [次へ（Next）] をクリックします。
j) 必要に応じてフィールドに入力します。
k) **[OK]** をクリックしてブリッジ ドメインの設定を完了します。

ステップ 5 **[作業（Work）]** ペインで、VRF インスタンスを囲む円内のキャンバスに **[L3]** アイコンをドラッグして、2 つを接続します。[Create Routed Outside] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) **[ノードとインターフェイス プロトコル プロファイル（Nodes And Interfaces Protocol Profiles]** セクションで、**[+]** をクリックして **[ノード プロファイルの作成（Create Node Profile）]** ダイアログ ボックスを開きます。
c) [Name] フィールドに、名前を入力します。
d) **[ノード（Nodes）]** セクションで、**[+]** をクリックして **[ノードの選択（Select Node）]** ダイアログ ボックスを開きます。
e) **[ノード ID（Node ID）]** ドロップダウン リストから、ノードを選択します。
f) [Router ID] フィールドに、ルータ ID を入力します。
g) **[スタティック ルート（Static Routes）]** セクションで、**[+]** をクリックして**[スタティック ルートの作成（Create Static Routes）]** ダイアログ ボックスを開きます。
h) [Prefix] フィールドに、IPv4 アドレスまたは IPv6 アドレスを入力します。
i) **[ネクスト ホップ アドレス（Next Hop Addresses）]** セクションで、**[+]** をクリックして **[ネクスト ホップの作成（Create Next Hop）]** ダイアログ ボックスを開きます。
j) **[ネクスト ホップ アドレス（Next Hop Addresses）]** フィールドを展開し、IPv4 アドレスまたは IPv6 アドレスを入力します。
k) **[設定（Preference）]** フィールドに、数値を入力します。
l) 必要に応じて他のフィールドに入力します。
m) [OK] をクリックします。
n) **[静的ルートの作成（Create Static Route）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
o) [OK] をクリックします。

p) **[ノードの選択（Select Node）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
q) [OK] をクリックします。
r) **[ノード プロファイルの作成（Create Node Profile）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
s) [OK] をクリックします。
t) 必要に応じて **[BGP]**、**[OSPF]**、または **[EIGRP]** チェックボックスをオンにします。
u) 必要に応じて他のフィールドに入力します。
v) [次へ（Next）] をクリックします。
w) 必要に応じてフィールドに入力します。
x) **[OK]** をクリックしてレイヤ 3 の設定を完了します。

レイヤ 3 の設定を確認するには、**[ナビゲーション（Navigation）]** ペインで、**[ネットワーキング（Networking）] > [VRF]**の順に展開します。

EPG の導入

特定のポートへの EPG の静的な導入

このトピックでは、Cisco APIC を使用しているときに特定のポートに EPG を静的に導入する一般的な方法の例を示します。

GUI を使用して特定のノードまたはポートへ EPG を導入する

始める前に

EPG を導入するテナントがすでに作成されていること。

特定のノードまたはノードの特定のポートで、EPG を作成することができます。

手順

ステップ 1 Cisco APIC にログインします。
ステップ 2 **[Tenants[** > ***[tenant]*** を選択します。
ステップ 3 左側のナビゲーション ウィンドウで、 ***tenant***、 **Application Profiles**、および ***application profile*** を展開します。
ステップ 4 **Application EPGs** を右クリックし、**Create Application EPG** を選択します。
ステップ 5 **Create Application EPG STEP 1 > Identity** ダイアログボックスで、次の操作を実行します:
a) **Name** フィールドに、EPG の名前を入力します。
b) **Bridge Domain** ドロップダウンリストから、ブリッジ ドメインを選択します。

c) [Statically Link with Leaves/Paths] チェックボックスをオンにします。

このチェック ボックスを使用して、どのポートに EPG を導入するかを指定できます。

d) [Next] をクリックします。

e) [Path] ドロップダウンリストから、宛先 EPG への静的パスを選択します。

ステップ 6 **Create Application EPG STEP 2 > Leaves/Paths** ダイアログボックスで、**Physical Domain** ドロップダウンリストから物理ドメインを選択します。

ステップ 7 次のいずれかの手順を実行します。

オプション	説明
次のものに EPG を展開する場合、	次を実行します。
ノード	1. **Leaves** エリアを展開します。 2. [Node] ドロップダウン リストから、ノードを選択します。 3. **Encap** フィールドで、適切な VLAN を入力します。 4. (オプション) **Deployment Immediacy** ドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate**を選択します。 5. (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。
ノード上のポート	1. **Paths** エリアを展開します。 2. **Path** ドロップダウンリストから、適切なノードおよびポートを選択します。 3. (オプション) **Deployment Immediacy** フィールドのドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate** を選択します。 4. (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。 5. **Port Encap** フィールドに、導入するセカンダリ VLAN を入力します。 6. (オプション) **Primary Encap** フィールドで、展開するプライマリ VLAN を入力します。

ステップ 8 **Update** をクリックし、**Finish** をクリックします。

ステップ 9 左側のナビゲーション ウィンドウで、作成した EPG を展開します。

ステップ 10 次のいずれかの操作を実行します:

- ノードで EPG を作成した場合は、**Static Leafs** をクリックし、作業ウィンドウで、静的バインド パスの詳細を表示します。

- ノードのポートでEPGを作成した場合は、**Static Ports**をクリックし、作業ウィンドウで、静的バインド パスの詳細を表示します。

特定のポートにEPGを導入するためのドメイン、接続エンティティ プロファイル、および VLAN の作成

このトピックでは、特定のポートに EPG を導入する場合に必須である物理ドメイン、接続エンティティ プロファイル（AEP）、および VLAN を作成する方法の典型的な例を示します。

すべてのエンドポイント グループ（EPG）にドメインが必要です。また、インターフェイス ポリシー グループを接続エンティティ プロファイル（AEP）に関連付ける必要があり、AEP と EPG が同じドメインに存在する必要がある場合は、AEP をドメインに関連付ける必要があります。EPG とドメイン、およびインターフェイス ポリシー グループとドメインの関連付けに基づいて、EPG が使用するポートと VLAN が検証されます。以下のドメイン タイプが EPG に関連付けられます。

- アプリケーション EPG
- レイヤ 3 Outside 外部ネットワーク インスタンス EPG
- レイヤ 2 Outside 外部ネットワーク インスタンス EPG
- アウトオブバンドおよびインバンド アクセスの管理 EPG

APIC は、これらのドメイン タイプのうち 1 つまたは複数に EPG が関連付けられているかどうかを確認します。EPG が関連付けられていない場合、システムは設定を受け入れますが、エラーが発生します。ドメインの関連付けが有効でない場合、導入された設定が正しく機能しない可能性があります。たとえば、VLAN のカプセル化を EPG で使用することが有効でない場合、導入された設定が正しく機能しない可能性があります。

（注） スタティック バインディングを使用しない AEP との EPG アソシエーションは、一方のエンドポイントが同じ EPG の下でタギングをサポートし、もう一方のエンド ポイントが同じ EPG 内で VLAN タギングをサポートしないような AEP の下では、EPG を**トランク**として設定するシナリオで機能させることはできません。EPG で AEPを関連付ける際には、トランク、アクセス（タグ付き）、またはアクセス（タグなし）として設定できます。

GUI を使用して特定のポートに EPG を展開するためのドメインおよび VLAN の作成

始める前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[クイックスタート（Quick Start）]** をクリックします。

ステップ 3 **[作業（Work）]** ペインで、**[インターフェイスの設定（Configure Interfaces）]** をクリックします。

ステップ 4 **[インターフェイスの設定（Configure Interfaces）]** ダイアログで、以下のアクションを実行します。

a) **[ノード タイプ（Node Type）]** で、**[リーフ（Leaf）]** をクリックします。
b) **[ポート タイプ（Port Type）]** で、**[アクセス（Access）]** をクリックします。
c) **[インターフェイス タイプ（Interface Type）]** で、目的のタイプを選択します。
d) **[インターフェイス集約タイプ（Interface Aggregation Type）]** で、**[個別（Individual）]** を選択します。
e) **[ノード（Node）]** で、**[ノードの選択（Select Node）]** をクリックし、目的のノードのボックスにチェックを入れて、**[OK]** をクリックします。複数のノードを選択できます。
f) **[すべてのスイッチのインターフェイス（Interfaces For All Switches）]** で、目的のインターフェイスの範囲を入力します。
g) **[リーフ アクセス ポート ポリシー グループ（Leaf Access Port Policy Group）]** の場合は、**[リーフ アクセス ポート ポリシー グループの選択（Select Leaf Access Port Policy Group）]** をクリックします。
h) **[リーフ アクセス ポート ポリシー グループの選択（Select Leaf Access Port Policy Group）]** ダイアログで、**[リーフ アクセス ポート ポリシー グループの作成（Create Leaf Access Port Policy Group）]** をクリックします。
i) **[リーフ アクセス ポート ポリシー グループの作成（Create Leaf Access Port Policy Group）]** ダイアログの **[リンク レベル ポリシー（Link Level Policy）]** で、**[リンク レベル ポリシーの選択（Select Link Level Policy）]** をクリックします。
j) リンク レベル ポリシーを選択して **[選択（Select）]** を選択するか、**[リンク レベル ポリシーの作成（Create Link Level Policy）]** をクリックし、必要に応じてフィールドに入力して、**[保存（Save）]** をクリックします。
k) [保存（Save）] をクリックします。

ステップ 5 以下のアクションを実行して、ドメインと VLAN プールを作成します。

a) **[ナビゲーション（Navigation）]** ペインで、**[物理ドメインと外部ドメイン（Physical and External Domains）]** を展開します。
b) **[物理ドメイン（Physical Domains）]** を右クリックし、適切な**[物理ドメインの作成（Create Physical Domain）]** を選択します。
c) **[名前（Name）]** に、ドメインの名前を入力します。
d) **[VLAN プール（VLAN Pool）]**で、**[VLAN プールの作成（Create VLAN Pool）]** を選択し、必要に応じてフィールドに入力して、**[送信（Submit）]** をクリックします。

e) 目的に応じて、残りのフィールドに入力します。
f) [送信（Submit）] をクリックします。

ステップ 6 メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 7 **[作業（Work）]** ペインで、目的のテナントをダブルクリックします。

ステップ 8 **[ナビゲーション（Navigation）]** ペインで、**テナント名** > **[アプリケーション プロファイル（Application Profiles）]** > **プロファイル名** > **[アプリケーション EPG（Application EPGs）]** > ***EPG* 名**を展開し、以下の操作を実行します。

a) **[ドメイン（Domains）（VM またはベアメタル）]** を右クリックし、**[物理ドメインの関連付けの追加（Add Physical Domain Association）]** をクリックします。
b) **[物理ドメインの関連付けの追加（Add Physical Domain Association）]** ダイアログで、**[物理ドメインのプロファイル（Physical Domain Profile）]** ドロップダウン リストから、前に作成したドメインを選択します。
c) [Submit] をクリックします。
AEP は、ノード上の特定のポート、およびドメインに関連付けられます。物理ドメインは VLAN プールに関連付けられ、テナントはこの物理ドメインに関連付けられます。

スイッチ プロファイルとインターフェイス プロファイルが作成されます。インターフェイス プロファイルのポート ブロックにポリシー グループが作成されます。AEP が自動的に作成され、ポート ブロックおよびドメインに関連付けられます。ドメインは VLAN プールに関連付けられ、テナントはドメインに関連付けられます。

AEP またはインターフェイス ポリシー グループを使用したアプリケーション EPG の複数のポートへの導入

APIC の拡張 GUI と REST API を使用して、接続エンティティ プロファイルをアプリケーション EPG に直接関連付けることができます。これにより、単一の構成の接続エンティティ プロファイルに関連付けられたすべてのポートに、関連付けられたアプリケーション EPG を導入します。

APIC REST API または NX-OS スタイルの CLI を使用し、インターフェイス ポリシー グループを介して複数のポートにアプリケーション EPG を導入できます。

APIC GUI を使用した AEP による複数のインターフェイスへの EPG の導入

短時間でアプリケーションを接続エンティティ プロファイルに関連付けて、その接続エンティティ プロファイルに関連付けられたすべてのポートに EPG を迅速に導入することができます。

始める前に

- ターゲット アプリケーション EPG が作成されている。

- AEP での EPG 導入に使用する VLAN の範囲が含まれている VLAN プールが作成されている。
- 物理ドメインが作成され、VLAN プールと AEP にリンクされている。
- ターゲットの接続エンティティ プロファイルが作成され、アプリケーション EPG を導入するポートに関連付けられている。

手順

ステップ 1 ターゲットの接続エンティティ プロファイルに移動します。

a) 使用する接続エンティティ プロファイルのページを開きます。**[ファブリック（Fabric）]**>**[アクセス ポリシー（Access Policies）]**>**[ポリシー（Policies）]**>**[グローバル（Global）]**>**[アタッチ可能なアクセス エンティティ プロファイル（Attachable Access Entity Profiles）]** に移動します。

b) ターゲットの接続エンティティ プロファイルをクリックして、[Attachable Access Entity Profile] ウィンドウを開きます。

ステップ 2 [Show Usage] ボタンをクリックして、この接続エンティティ プロファイルに関連付けられたリーフ スイッチとインターフェイスを表示します。

この接続エンティティ プロファイルに関連付けられたアプリケーション EPG が、この接続エンティティ プロファイルに関連付けられたすべてのスイッチ上のすべてのポートに導入されます。

ステップ 3 [Application EPGs] テーブルを使用して、この接続エンティティ プロファイルにターゲット アプリケーション EPG を関連付けます。アプリケーション EPG エントリを追加するには、[+] をクリックします。各エントリに次のフィールドがあります。

フィールド	アクション（Action）
Application EPG	ドロップダウンを使用して、関連付けられたテナント、アプリケーション プロファイル、およびターゲット アプリケーション EPG を選択します。
Encap	ターゲット アプリケーション EPG の通信に使用される VLAN の名前を入力します。
Primary Encap	アプリケーション EPG にプライマリ VLAN が必要な場合は、プライマリ VLAN の名前を入力します。
モード	ドロップダウンを使用して、データを送信するモードを指定します。 • [Trunk]：ホストからのトラフィックに VLAN ID がタグ付けされている場合に選択します。 • [Access]：ホストからのトラフィックに 802.1p タグがタグ付けされている場合に選択します。

フィールド	アクション（**Action**）
	• [Access Untagged] ：ホストからのトラフィックがタグ付けされていない場合に選択します。

ステップ 4 [Submit] をクリックします。
この接続エンティティ プロファイルに関連付けられたアプリケーション EPG が、この接続エンティティ プロファイルに関連付けられたすべてのスイッチ上のすべてのポートに導入されます。

マイクロセグメント EPG

ベア メタルでのネットワークベースの属性によるマイクロセグメンテーションの使用

Cisco APIC を使用して Cisco ACI でのマイクロセグメンテーションを設定し、ネットワークベースの属性、MAC アドレス、または 1 つ以上の IP アドレスを使用した新しい属性ベースの EPG を作成できます。ネットワークベースの属性を使用して Cisco ACI でのマイクロセグメンテーションを設定し、単一のベース EPG または複数の EPG 内で VM または物理エンドポイントを分離できます。

IP ベースの属性の使用

IP ベースのフィルタを使用して、単一のマイクロセグメントで単一 IP アドレス、サブネット、または多様な非連続 IP アドレスを分離できます。ファイアウォールの使用と同様に、セキュリティ ゾーンを作成するための迅速かつ簡単な方法として、IP アドレスに基づいて物理エンドポイントを分離できます。

MAC ベースの属性の使用

MAC ベースのフィルタを使用して、単一 MAC アドレスまたは複数の MAC アドレスを分離できます。不適切なトラフィックをネットワークに送信するサーバがある場合はこの方法を推奨します。MAC ベースのフィルタを使用してマイクロセグメントを作成することで、このサーバを分離できます。

GUI を使用したベアメタル環境でのネットワークベースのマイクロセグメント EPG の設定

Cisco APIC を使用してマイクロセグメンテーションを設定し、異なる複数のベース EPG または同一の EPG に属する物理エンドポイント デバイスを新しい属性ベースの EPG に配置できます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 [Tenants] を選択し、マイクロセグメントを作成するテナントを選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、テナント フォルダ、[Application Profiles] フォルダ、[Profile] フォルダ、および [Application EPGs] フォルダを展開します。

ステップ 4 次のいずれかを実行します。

- 同じベース EPG の物理エンドポイント デバイスを新しい属性ベースの EPG に配置するには、物理エンドポイント デバイスを含むベース EPG をクリックします。
- 異なる複数のベース EPG の物理エンドポイント デバイスを新しい属性ベースの EPG に配置するには、物理エンドポイント デバイスを含むベース EPG の 1 つをクリックします。

ベース EPG のプロパティが作業ウィンドウに表示されます。

ステップ 5 作業ウィンドウで、画面の右上にある [Operational] タブをクリックします。

ステップ 6 [Operational] タブの下の [Client End-Points] タブがアクティブになっていることを確認します。作業ウィンドウに、ベース EPG に属するすべての物理エンドポイントが表示されます。

ステップ 7 新しいマイクロセグメントに配置するエンドポイント デバイス（複数可）の IP アドレスまたは MAC アドレスを書き留めます。

ステップ 8 異なる複数のベース EPG のエンドポイント デバイスを新しい属性ベースの EPG に配置する場合は、各ベース EPG に対してステップ 4 ～ 7 を繰り返します。

ステップ 9 テナントのナビゲーション ウィンドウで、[uSeg EPGs] フォルダを右クリックし、[Create uSeg EPG] を選択します。

ステップ 10 以下の一連の手順を実行し、エンドポイント デバイス グループの 1 つに対して属性ベースの EPG の作成を開始します。

a) [Create uSeg EPG] ダイアログボックスで、[Name] フィールドに名前を入力します。

新しい属性ベースの EPG はマイクロセグメントであることを示す名前を選択することを推奨します。

b) [intra-EPG isolation] フィールドで [enforced] または [unenforced] を選択します。

[enforced] を選択した場合は、ACI によってこの uSeg EPG 内のエンドポイント デバイス間の通信がすべて阻止されます。

c) [Bridge Domain] エリアで、ドロップダウン リストからブリッジ ドメインを選択します。

d) [uSeg Attributes] 領域で、ダイアログボックスの右側にある [+] ドロップダウン リストから [IP Address Filter] または [MAC Address Filter] を選択します。

ステップ 11 フィルタを設定するには、次のいずれかの一連の手順を実行します。

項目	結果
IP ベースの属性	**1.** [Create IP Attribute] ダイアログボックスで、[Name] フィールドに名前を入力します。

項目	結果
	名前については、フィルタ機能を反映したものを選択するよう推奨します。 **2.** [IP Address] フィールドに、適切なサブネット マスクの IP アドレスまたはサブネットを入力します。 **3.** [OK] をクリックします。 **4.** （オプション）ステップ 10 c ～ 11 c を繰り返して、2 番目の IP アドレス フィルタを作成します。 この手順で、マイクロセグメントに不連続の IP アドレスを含めることができます。 **5.** [Create uSeg EPG] ダイアログボックスで、[Submit] をクリックします。
MAC ベースの属性	**1.** [Create MAC Attribute] ダイアログボックスで、[Name] フィールドに名前を入力します。 名前については、フィルタ機能を反映したものを選択するよう推奨します。 **2.** [MAC Address] フィールドに、MAC アドレスを入力します。 **3.** [OK] をクリックします。 **4.** [Create uSeg EPG] ダイアログボックスで、[Submit] をクリックします。

ステップ 12 次の手順を実行して uSeg EPG を物理ドメインに関連付けます。

a) [Navigation] ペインで、uSeg EPG フォルダが開いていることを確認し、作成したマイクロセグメントのコンテナを開きます。
b) [Domains (VMs and Bare-Metals)] フォルダをクリックします。
c) 作業ウィンドウの右側にある [Actions] をクリックし、ドロップダウンリストから [Add Physical Domain Association] を選択します。
d) [Add Physical Domain Association] ダイアログボックスで、[Physical Domain Profile] ドロップダウン リストからプロファイルを選択します。
e) [Deploy Immediacy] エリアで、デフォルトの [On Demand] を受け入れます。
f) [Resolution Immediacy] エリアで、デフォルトの [Immediate] を受け入れます。
g) [Submit] をクリックします。`

ステップ 13 uSeg EPG を適切なリーフ スイッチに関連付けます。

a) ナビゲーション ウィンドウで、uSeg EPG フォルダが開いていることを確認して [Static Leafs] をクリックします。
b) [Static Leafs] ウィンドウで、**[Actions]** > **[Statically Link with Node]** をクリックします
c) [Statically Link With Node] ダイアログで、リーフ ノードとモードを選択します。
d) **Submit** をクリックします。

ステップ 14 作成するその他のネットワーク属性ベースの EPG すべてに対してステップ 9 ～ 13 を繰り返します。

次のタスク

属性ベースの EPG が正しく作成されたことを確認します。

IP ベースまたは MAC ベースの属性を設定する場合は、新しいマイクロセグメントに配置したエンドポイント デバイスでトラフィックが動作していることを確認します。

共有リソースとしての IP アドレスベースのマイクロセグメント EPG

IP アドレスベースのマイクロセグメント EPG を VRF（この EPG が配置されている）の内外からアクセスできるリソースとして設定できます。この場合は、既存の IP アドレスベースのマイクロセグメント EPG にサブネット（ユニキャスト IP アドレスが割り当てられている）を設定し、そのサブネットをこの EPG が属する VRF 以外の VRF にあるデバイスでアドバタイズおよび共有できるようにします。次に、EPG を共有サブネットの IP アドレスに関連付けるオプションを有効にした状態で IP 属性を定義します。

GUI を使用した共有リソースとしての IP ベースのマイクロセグメント EPG の設定

VRF および現在のファブリック外のクライアントがアクセス可能な共有サービスとして、32 ビット マスクの IP アドレスを持つマイクロセグメント EPG を設定できます。

始める前に

設定に関する次の GUI の説明では、サブネット マスクが /32 に設定された IP アドレスベースのマイクロセグメント EPG が事前設定されていることを前提としています。

（注）
- 物理環境で IP アドレス ベースの EPG を設定する手順については、次を参照してください。 ベア メタルでのネットワークベースの属性によるマイクロセグメンテーションの使用 （246 ページ）
- 仮想環境で IP アドレス ベースの EPG を設定する手順については、『*Cisco ACI Virtualization Guide*』の「*Configuring Microsegmentation with Cisco ACI*」を参照してください。

手順

ステップ 1 ターゲットとなる IP アドレスベースの EPG に移動します。

a) APIC GUI で、**[Tenant]** > **[tenant_name]** > **[uSeg EPGs]** > **[uSeg_epg_name]** をクリックして EPG の [Properties] ダイアログを表示します。

ステップ 2 ターゲット EPG では、EPG のサブネット アドレスに一致するように IP 属性を設定します。

a) [Properties] ダイアログで、[uSeg Attributes] テーブルを見つけて [+] をクリックします。プロンプトが表示されたら、**[IP Address Filter]** を選択して **[Create IP Attribute]** ダイアログを表示します。

b) [Name] フィールドに名前を入力します。

c) **[Use FV Subnet]** のチェックボックスをオンにします。

このオプションを有効にすることで、IP 属性値が共有サブネットの IP アドレスに一致することを示します。

d) **[Submit]** をクリックします。

ステップ 3 ターゲット EPG の共有サブネットを作成します。

a) ターゲットとなる IP アドレスベースの uSeg EPG のフォルダを APIC のナビゲーション ウィンドウで開いたまま、**[Subnets]** フォルダを右クリックして **[Create EPG Subnets]** を選択します。

b) **[Default Gateway]** フィールドに、IP アドレスベースのマイクロセグメント EPG の IP アドレスまたはマスクを入力します。

（注）
- いずれの場合もサブネット マスクは /32 である必要があります。
- IP アドレスベースの EPG に関しては、実際にゲートウェイのデフォルト アドレスを入力するのではなく、共有 EPG サブネットの IP アドレスを入力します。

c) **[Treat as a virtual IP address]** を選択します。

d) [Scope] で [Advertised Externally] と [Shared between VRFs] を選択します。

e) [Submit] をクリックします。

GUI を使用した共有リソースとしての IP ベースのマイクロセグメント EPG の設定解除

共有サービスとして設定された IP アドレスベースのマイクロセグメント EPG を設定解除するには、共有サブネットを削除し、さらにそのサブネットを共有リソースとして使用するオプションを無効にする必要があります。

始める前に

共有サービスとして設定された IP アドレスベースのマイクロセグメント EPG を設定解除するには、次の情報を確認しておく必要があります。

- IP アドレスベースのマイクロセグメント EPG の共有サービス アドレスとして設定されているサブネット。
- **Use FV Subnet** オプションが有効な状態で設定されている IP 属性。

手順

ステップ 1 IP アドレスベースのマイクロセグメント EPG からサブネットを削除します。

a) APIC GUI で、**[Tenant]** > **[tenant_name]** > **[Application Profiles]** > **[epg_name]** > **[uSeg EPGs]** > **[uSeg EPGs]** > **[uSeg_epg_name]** をクリックします。

b) ターゲットとなる IP アドレスベースの uSeg EPG のフォルダを APIC のナビゲーション ウィンドウで開いたまま、[Subnets] フォルダをクリックします。

c) **Subnets** ウィンドウで、アドバタイズされて他の VRF と共有されるサブネットを選択し、**Actions** > **Delete** をクリックします。

d) [Yes] をクリックして削除を確定します。

ステップ 2 [Use FV Subnet] オプションを無効にします。

a) ターゲットとなる IP アドレスベースの uSeg EPG のフォルダを APIC のナビゲーション ウィンドウで開いたまま、マイクロセグメント EPG の名前をクリックして EPG の [Properties] ダイアログを表示します。

b) [Properties] ダイアログで、[uSeg Attributes] テーブルから [Use FV Subnet] オプションが有効になっている IP 属性の項目を見つけます。

c) その項目をダブルクリックして **Edit IP Attribute** ダイアログを表示します。

d) [Edit IP Attribute] ダイアログで、[Use FV Subnet] オプションを選択解除します。

e) [IP Address] フィールドに別の IP アドレス属性を指定します。

（注）
このアドレスは、32 ビット マスクのユニキャスト アドレスである必要があります（例：124.124.124.123/32）。

f) [Submit] をクリックします。

アプリケーション プロファイルと契約の導入

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。

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

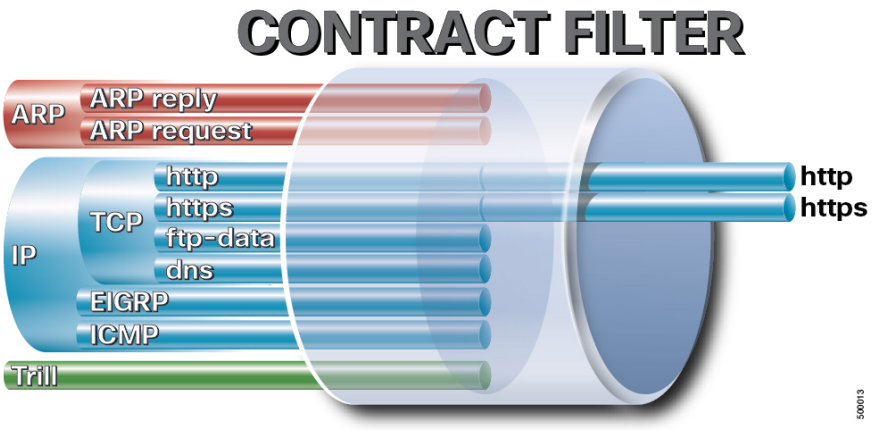
接続を開始することを許可しません。ただし、EPG 間の別のコントラクトが、その方向の接続を簡単に許可する場合があります。

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

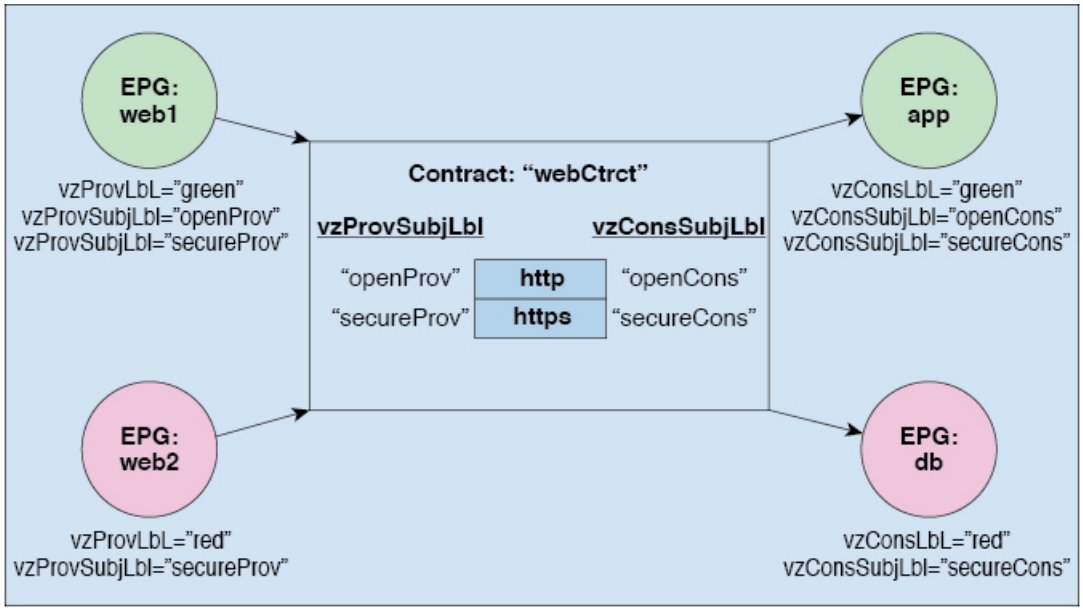
コントラクトは階層的に構築されます。1 つ以上のサブジェクトで構成され、各サブジェクトには 1 つ以上のフィルタが含まれ、各フィルタは 1 つ以上のプロトコルを定義できます。

図 *7:* 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 *8 : 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openConsare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。

Three-Tier アプリケーションの展開

フィルタは、フィルタを含むコントラクトにより許可または拒否されるデータ プロトコルを指定します。コントラクトには、複数のサブジェクトを含めることができます。情報カテゴリは、単方向または双方向フィルタの作成に使用できます。単方向フィルタは、コンシューマからプロバイダー方向（IN）またはプロバイダーからコンシューマ方向（OUT）のどちらかに対して使用されます。双方向フィルタは、両方の方向で使用されます。これは、再帰的ではありません。

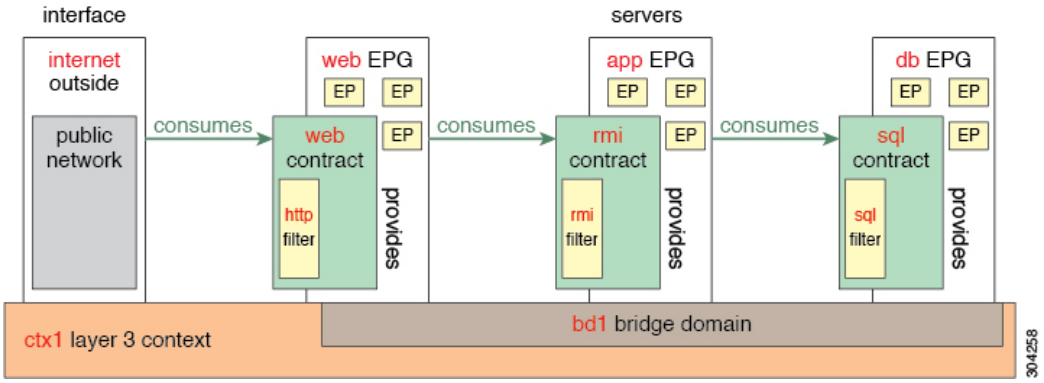
コントラクトは、エンドポイント グループ間 (EPG 間) の通信をイネーブルにするポリシーです。このポリシーは、アプリケーション層間の通信を指定するルールです。コントラクトが EPG に添付されていない場合は、EPG 間通信がデフォルトで無効になります。EPG 内の通信は常に許可されているので、EPG 内の通信には契約は必要ありません。

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

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

Web サーバには HTTP フィルタがあり、アプリケーション サーバには Remote Method Invocation（RMI）フィルタがあり、データベース サーバには Structured Query Language（SQL）フィルタがあります。アプリケーション サーバは、SQL コントラクトを消費してデータベース サーバと通信します。Web サーバは、RMI コントラクトを消費して、アプリケーション サーバと通信します。トラフィックは Web サーバから入り、アプリケーション サーバと通信します。アプリケーション サーバはその後、データベース サーバと通信し、トラフィックは外部に通信することもできます。

図 *9 : Three-Tier* アプリケーションの図



http 用のフィルタを作成するパラメータ

この例での http 用のフィルタを作成するパラメータは次のとおりです。

パラメータ名	http のフィルタ
名前	http
エントリの数	2
エントリ名	Dport-80 Dport-443
Ethertype	IP
プロトコル	tcp tcp
宛先ポート	http https

rmi および sql 用のフィルタを作成するパラメータ

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

パラメータ名	rmi のフィルタ	sql のフィルタ
名前	rmi	sql
エントリの数	1	1
エントリ名	Dport-1099	Dport-1521
Ethertype	IP	IP

パラメータ名	rmi のフィルタ	sql のフィルタ
プロトコル	tcp	tcp
宛先ポート	1099	1521

アプリケーション プロファイル データベースの例

この例のアプリケーション プロファイル データベースは次のとおりです。

EPG	提供されるコントラクト	消費されるコントラクト
web	web	rmi
app	rmi	sql
db	sql	--

GUI を使用したアプリケーション プロファイルの作成

手順

ステップ 1 メニュー バーで、**[TENANTS]** を選択します。**[Navigation]** ペインで、テナントを展開し、**[Application Profiles]** を右クリックし、**[Create Application Profile]** をクリックします。

ステップ 2 **[Create Application Profile]** ダイアログボックスで、**[Name]** フィールドに、アプリケーション プロファイル名 (OnlineStore) を追加します。

GUI を使用した EPG の作成

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

手順

ステップ 1 メニュー バーで、[Tenants]、EPG を作成するテナントの順に選択します。

ステップ 2 ナビゲーション ペインで、テナントのフォルダ、[Application Profiles] フォルダ、アプリケーション プロファイルのフォルダの順に展開します。

ステップ 3 [Application EPG] フォルダを右クリックし、[Create Application EPG] ダイアログボックスで次の操作を実行します。

a) [Name] フィールドに、EPG の名前（db）を追加します。

b) [Bridge Domain] フィールドで、ドロップダウン リストからブリッジ ドメイン（bd1）を選択します。

c) [Associate to VM Domain Profiles] チェックボックスをオンにします。[Next] をクリックします。

d) [STEP 2 > Domains] エリアで、[Associate VM Domain Profiles] を展開し、ドロップダウンリストから対象の VMM ドメインを選択します。

e) [Deployment Immediacy] ドロップダウンリストで、デフォルト値を受け入れるか、いつポリシーが Cisco APIC から物理リーフ スイッチに展開されるかを選択します。

f) [Resolution Immediacy] ドロップダウンリストで、いつポリシーが物理リーフ スイッチから仮想リーフに展開されるかを選択します。

Cisco AVS がある場合には、**Immediate** または **On Demand** を選択します。Cisco ACI Virtual Edge または VMware VDS がある場合には、**Immediate**、 **On Demand**、または **Pre-provision** を選択します。

g) （オプション）[Delimiter] フィールドに、|、~、!、@、^、+、または = のいずれかの記号を入力します。

記号を入力しなかった場合、システムは VMware ポートグループ名のデリミタとしてデフォルトの | を使用します。

h) Cisco ACI Virtual Edge または Cisco AVS を利用している場合は、[Encap Mode] ドロップダウンリストからカプセル化モードを選択します。

次のいずれかのカプセル化モードを選択できます。

- **VXLAN**：これはドメインの VLAN 設定を上書きし、EPG は VXLAN カプセル化を使用します。ただし、ドメインでマルチキャスト プールが設定されていない場合は、EPG に対してエラーが発生します。
- **VLAN**：これはドメインの VXLAN 設定を上書きし、EPG は VLAN カプセル化を使用します。ただし、ドメインで VLAN プールが設定されていない場合は、EPG に対してエラーがトリガーされます。
- **自動**： EPG は、VMM ドメインと同じカプセル化モードを使用します。これはデフォルトの設定です。

i) Cisco ACI Virtual Edge がある場合、**Switching Mode** ドロップダウンリストで、 **native** または **AVE** を選択します。

native を選択した場合、EPGは VMware VDS を通して切り替えられます。**AVE** を選択した場合、EPG はCisco ACI Virtual Edge を通して切り替えられます。デフォルトは**native** す。

j) **Update** をクリックし、**Finish** をクリックします。

ステップ 4 **Create Application Profile** ダイアログボックスで、EPG をさらに 2 つ作成します。同じブリッジ ドメイン、同じデータセンター内に、3 つの EPG を作成します。これらは、db、app、および web です。

APIC GUI を使用したコントラクトの設定

コントラクトとフィルタの注意事項と制約事項

ファブリックが Cisco Nexus 93128TX、93120TX、9396TX、9396PX、9372PX、9372PX-E、9372TX-E などの第 1 世代の Cisco Nexus 9300 リーフ スイッチで構成されている場合、**EtherType** 一致としての **IP** のみがコントラクト フィルタでサポートされます。コントラクト フィルタの **[EtherType]** フィールドで、より詳細なオプション（**IPv4** や **IPv6** など）を照合する機能は、スイッチ名の末尾に -EX、-FX、または -FX2 が指定されたリーフ スイッチ モデルでのみサポートされます。

GUI を使用したフィルタの作成

3 つの個別のフィルタを作成します。この例では、HTTP、RMI、SQL です。このタスクでは、HTTP フィルタを作成する方法を示します。このタスクは、他のフィルタを作成するタスクと同じです。

始める前に

テナント、ネットワーク、およびブリッジ ドメインが作成されていることを確認します。

手順

ステップ 1 メニュー バーで、[テナント] を選択します。

ステップ 2 **Navigation** ウィンドウで、***tenant-name*** > **Contracts** を選択し、**Filters** を選択し、**Create Filter** を選択します。

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

a) [Name] フィールドに、フィルタ名（http）を入力します。
b) **[エントリ（Entries）]** テーブル内で+をクリックして、**[名前（Name）]** フィールドに、名前（Dport-80）を入力します。
c) [EtherType] ドロップダウン リストから、EtherType（IP）を選択します。
d) [IP Protocol] ドロップダウン リストから、プロトコル（tcp）を選択します。
e) [Destination Port/Range] ドロップダウン リストから、[From] フィールドと [To] フィールドで、[http] を選択します。（http）
f) [Update] をクリックし、[Submit] をクリックします。
新しく追加されたフィルタが、[Navigation] ペインと [Work] ペインに表示されます。

（注）
[エントリ（Entries）] テーブルでは、**ARP フラグ**には機能がなく、設定できません。このフィールドは使用しません。

ステップ 4 [Name] フィールドの [Entries] を展開します。同じプロセスを実行して、別のエントリを**宛先**ポートとして HTTPS で追加し、[Update] をクリックします。

この新しいフィルタ ルールが追加されます。

ステップ 5 さらに 2 つのフィルタ（rmi および sql）を作成し、rmi および sql 用のフィルタを作成するパラメータ（256 ページ）に示すパラメータを使用するには、上記手順の同じプロセスを実行します。

GUI を使用した契約の作成

手順

ステップ 1 メニューバーで **Tenants** を選択し、実行するテナント名を選択します。**Navigation** ウィンドウで、***tenant-name*** > **Contracts** を展開します。

ステップ 2 **Standard** > **Create Contract** を右クリックします。

ステップ 3 **Create Contract** ダイアログボックスで、次のタスクを実行します:

a) [Name] フィールドに、契約名（web）を入力します。

b) [Subjects] の横の [+] 記号をクリックし、新しいサブジェクトを追加します。

c) [Create Contract Subject] ダイアログボックスで、[Name] フィールドにサブジェクト名を入力します。（web）

d) （注）
この手順では、契約のサブジェクトで前に作成されたフィルタを関連付けます。

[Filter Chain] 領域で、[Filters] の横の [+] 記号をクリックします。

e) ダイアログボックスで、ドロップダウンメニューから、フィルタ名（http）を選択し、[Update] をクリックします。

ステップ 4 [Create Contract Subject] ダイアログボックスで、[OK] をクリックします。

ステップ 5 この手順と同じステップに従って、rmi と sql 用の契約をさらに 2 つ作成します。rmi 契約の場合は rmi サブジェクトを選択し、sql の場合は sql サブジェクトを選択します。

GUI を使用した契約の消費と提供

EPG 間のポリシー関係を作成するために、前に作成した契約を関連付けることができます。

提供するコントラクトと使用するコントラクトに名前を付けるときは、提供するコントラクトと使用するコントラクトの両方に同じ名前を付けてください。

手順

ステップ 1 （注）
db、app、および web EPG は、アイコンで表示されます。

APIC GUI ウィンドウをクリックして db EPG から app EPG にドラッグします。
[Add Consumed Contract] ダイアログボックスが表示されます。

ステップ 2 [Name] フィールドで、ドロップダウン リストから、**sql** 契約を選択します。[OK] をクリックします。
この手順により、db EPG は sql 契約を提供でき、app EPG は sql 契約を消費することができます。

ステップ 3 APIC GUI 画面 をクリックして、app ePG から web EPG にドラッグします。
[Add Consumed Contract] ダイアログボックスが表示されます。

ステップ 4 [Name] フィールドで、ドロップダウン リストから、**rmi** 契約を選択します。[OK] をクリックします。
この手順により、app EPG は rmi 契約を提供でき、web EPG は rmi 契約を消費することができます。

ステップ 5 web EPG のアイコンをクリックし、[Provided Contracts] 領域の [+] 記号をクリックします。
[Add Provided Contract] ダイアログボックスが表示されます。

ステップ 6 [Name] フィールドで、ドロップダウン リストから、**web** 契約を選択します。[OK] をクリックします。**[送信（Submit）]** をクリックします。
OnlineStore と呼ばれる 3 層アプリケーション プロファイルが作成されました。

ステップ 7 確認するには、[Navigation] ペインで、[Application Profiles] 下の [OnlineStore] に移動してクリックします。
[Work] ペインで、3 つの EPG app、db および web が表示されていることを確認できます。

ステップ 8 [Work] ペインで、**[Operational]** > **[Contracts]** を選択します。
消費/提供される順番で表示された EPG と契約を確認できます。

コントラクト パフォーマンスの最適化

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 *7:*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

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
非対応	ポート A	未指定	いいえ
非対応	未指定	未指定	はい

GUI を使用して TCAM の使用が最適化された契約を設定する

この手順はで、ハーウェア上の TCAM による契約データの保存を最適化する契約を設定する方法について説明します。

始める前に

- テナント、VRF、およびを提供し、契約を消費する Epg を作成します。
- この契約で許可または拒否されるトラフィックを定義する、1 つ以上のフィルタを作成します。

手順

ステップ 1 メニューバーで **Tenants** を選択し、実行するテナント名を選択します。**Navigation** ウィンドウで、*tenant-name* および **Contracts** を展開します。

ステップ 2 **Standard** > **Create Contract** を右クリックします。

ステップ 3 **Create Contract** ダイアログボックスで、次のタスクを実行します:

a) **Name** フィールドに、契約 名を入力します。

b) + アイコン (**Subjects** の隣にあるもの) をクリックして、新しい情報カテゴリを追加します。

c) [Create Contract Subject] ダイアログボックスで、[Name] フィールドにサブジェクト名を入力します。

（注）
この手順では、フィルタを契約の情報カテゴリに関連付けます。

d) TCAM の契約し状況強最適化機能を有効にするには、**Apply Both Directions** および **Reverse Filter Ports** が有効になっていることを確認します。

e) + アイコンをクリックして **Filters** を展開します。

f) ダイアログボックスで、ドロップダウン メニューから、デフォルトのフィルタを指定します。すでに設定したフィルタを選択するか、**Create Filter** で新しいフィルタを作成します。

g) **[指令（Directives）]** フィールドで、**[ポリシー圧縮の有効化（Enable Policy Compression）]** を選択します。

h) **Action** フィールドで、**Permit** または **Deny** を選択します。

（注）
現在のところ、**Deny** アクションはサポートされていません。最適化は **Permit** アクションに対してのみ行われます。

i) （任意） **Priority** フィールドで、優先度レベルを選択します。
j) **Update** をクリックします。

ステップ 4 **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。

ステップ 5 **Create Contract** ダイアログボックスで、**Submit**をクリックします。

契約とサブジェクトの例外

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。

GUI を使用したコントラクトまたはサブジェクトの例外の設定

このタスクでは、EPGのほとんどに対して通信を許可するものの、その一部のアクセスは拒否するコントラクトを設定します。

始める前に

コントラクトを提供し、利用するために、テナント、VRF、アプリケーションプロファイルと EPG を設定します。

手順

ステップ 1 メニュー バーで **[テナント]** > **[すべてテナント]** をクリックします。

ステップ 2 コントラクトを作成しているテナントをダブルクリックします。

ステップ 3 ナビゲーション バーで、**[コントラクト]** を展開し、**[フィルタ]** を右クリックして、**[フィルタの作成]** を選択します。

フィルタでは、コントラクト経由のアクセスを許可または拒否するトラフィックを定義するアクセス制御リスト（ACL）に重要です。許可または拒否できるオブジェクトを定義する複数のフィルタを作成することができます。

ステップ 4 フィルタ名を入力し、許可または拒否するトラフィックを定義する条件を追加して、**[送信]** をクリックします。

ステップ 5 **[コントラクト]** を右クリックし、**[コントラクトの作成]** を選択します。

ステップ 6 コントラクト名を入力し、範囲を設定して、[+] アイコンをクリックし件名を追加します。

ステップ 7 繰り返して別の件名を追加します。

ステップ 8 [Submit] をクリックします。

ステップ 9 コントラクトのすべての件名の例外を追加する手順は、次のとおりです。

a) コントラクトをクリックし、**[コントラクトの例外]** をクリックします。
b) 件名を追加し、許可または拒否するように設定します。
c) [+] アイコンをクリックしてコントラクトを追加します。
d) 例外の名前とタイプを入力します。
e) 正規表現を **[コンシューマ Regex]** および **[プロバイダ Regex]** フィールドに追加し、コントラクトのすべての件名から除外する EPG を定義します。

ステップ 10 コントラクトの 1 つの件名の例外を追加する手順は、次のとおりです。

a) 件名をクリックし、**[件名の例外]** をクリックします。
b) [+] アイコンをクリックしてコントラクトを追加します。
c) 例外の名前とタイプを入力します。
d) 正規表現を **[コンシューマ Regex]** および **[プロバイダ Regex]** に追加し、コントラクトのすべての件名から除外する EPG を定義します。

EPG 内契約

EPG 内契約

EPG 間の通信を制御するには、契約を設定します。Cisco APIC リリース 3.0(1) 以降では、EPG 内の契約を設定できます。

EPG 内契約がない場合、EPG のエンドポイント間の通信は、完全に可能か不可能かになります。通信はデフォルトでは無制限ですが、エンドポイント間の通信を禁止するために、EPG内分離を設定することができます。

ただし、EPG 内契約を使用すれば、同じ EPG のエンドポイント間の通信を制御して、いくつかのトラフィックを許可し、残りの部分を禁止することができます。たとえば、Webトラフィックを許可し、残りの部分をブロックすることが必要な場合があるでしょう。または、すべての ICMP トラフィックと TCP ポート 22 のトラフィックを許可し、他のすべてのトラフィックをブロック中することができます。

EPG 内契約の注意事項と制約事項

EPG 内契約を計画する場合は、次の注意事項と制約事項に従ってください。

- EPG 内契約は、VMware VDS、Open vSwitch (OVS)、およびベアメタル サーバ上のアプリケーション EPG とマイクロセグメント EPG (uSeg) で設定できます。

（注） OVS は、Kubernetes 統合 Cisco Application Centric Infrastructure（ACI）機能で使用できます。Kubernetes では、EPG を作成し、それらに名前空間を割り当てることがことができます。VMware VDS またはベアメタル サーバと同様、Cisco Application Policy Infrastructure Controller（APIC）では、EPG 内ポリシーを EPG に適用することができます。

- EPG 内契約では、リーフ スイッチがプロキシによる Address Resolution Protocol（ARP）をサポートしていることが必要です。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 内契約は、Cisco Application Virtual Switch、Cisco ACI Virtual Edge、および Microsoft ドメインではサポートされていません。EPG内契約を設定してこれらのドメインに適用しようとすると、ポートがブロック状態になる可能性があります。
- サービス グラフでの EPG 内コントラクト：
  - サービス グラフを拒否のアクションを含む EPG 内契約のサブジェクトと関連付けることはできません。
  - サービス グラフで EPG 内契約がサポートされるのは、シングル ノード ワンアーム モードのポリシーベース リダイレクトおよびコピー サービスに限られます。
- Cisco APIC リリース 5.2(1) 以降、EPG 内コントラクトは L3Out EPG でサポートされます。
  - アクションは **[許可（permit）]**、**[拒否（deny）]**、または **[リダイレクト（redirect）]** です。**リダイレクト** アクションには、ポリシーベース リダイレクト（PBR）を使用したサービス グラフが必要です。

- IP アドレスとサブネットが 0.0.0.0/0 または 0 :: 0 の L3Out EPG は、EPG 内コントラクトも EPG 内分離も使用できません。Cisco APIC は、これらの場合に障害を発生させます。ただし、代わりに L3Out EPG の IP アドレスとサブネット 0.0.0.0/1 および 128.0.0.0/1 を使用してすべてのトラフィックを捕捉できます。
- EPG の EPG 内コントラクトとは異なり、L3Out EPG の EPG 内コントラクトには暗黙の拒否ルールが自動的に追加されません。他のトラフィックを拒否するには、EPG内分離を有効にする必要があります。L3Out EPG の EPG 内分離は、VRF インスタンスが強制モードの場合にのみ機能します。
- Cisco ACI では、トラフィックが L3Out 内適用の Cisco ACI 境界リーフ スイッチに到達する方法を制御できません。

GUI を使用したアプリケーション EPG への EPG 内契約の追加

コントラクトを設定した後、EPG内コントラクトとしてEPGにコントラクトを追加できます。この手順は、VMware VDS、OVS、およびベアメタル サーバと同じです。

始める前に

- アプリケーション EPG が設定済みである必要があります。
- このアプリケーション用のフィルタが設定された契約が必要です。「GUIを使用した契約の作成 （260 ページ）」を参照してください。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 EPG のタイプに応じて、次の一連の手順のいずれかを実行します。

EPG 内コントラクトに適用する場合：	結果
アプリケーション EPG	1. 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[アプリケーション プロファイル（application profile）]*** > **[アプリケーション EPG（Application EPGs）]** > ***[epg]*** を展開します。 2. **[コントラクト]** フォルダを右クリックして、**[EPG 内コントラクトの追加]** を選択します。

EPG 内コントラクトに適用する場合：	結果
	3. **[Ext-EPG 内コントラクトの追加（Add Intra Ext-EPG Contract）]** ダイアログ ボックスで **[コントラクト（Contract）]** ドロップダウン リストからコントラクトを選択します。 4. **[送信（Submit）]** をクリックします。`
USeg EPG	1. 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[アプリケーション プロファイル（application profile）]*** > **[uSeg EPGs]** > ***[epg]***を展開します。 2. **[コントラクト]**フォルダを右クリックして、**[EPG 内コントラクトの追加]** を選択します。 3. **[Ext-EPG 内コントラクトの追加（Add Intra Ext-EPG Contract）]** ダイアログ ボックスで **[コントラクト（Contract）]** ドロップダウン リストからコントラクトを選択します。 4. **[送信（Submit）]** をクリックします。`
L3Out EPG	1. [ナビゲーション（Navigation）]ペインで、***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[外部 EPG（External EPGs）]** > ***[ext_epg_name]*** を選択します。 2. [作業（Work）] ペインの **[Ext-EPG 内分離（Intra Ext-EPG Isolation）]** で、**[適用（Enforced）]** を選択します。 3. **[送信（Submit）]** をクリックします。` 4. [作業（Work）] ペインで、**[ポリシー（Policy）]** > **[コントラクト（Contracts）]**タブを選択します。 5. アクション メニューで、**[Ext-EPG 内コントラクトの追加（Add Intra Ext-EPG Contract）]** を選択します。 6. **[Ext-EPG 内コントラクトの追加（Add Intra Ext-EPG Contract）]** ダイアログ ボックスで **[コントラクト（Contract）]** ドロップダウン リストからコントラクトを選択します。 7. **[送信（Submit）]** をクリックします。` 選択した契約が、[作業（Work）] ペインの **[コントラクト タイプ：EPG 内コントラクト（Contract Type：Intra EPG Contract）]** セクションに表示されます。

NX-OS スタイル CLI を使用したアプリケーション EPG への EPG 内契約の追加

契約を設定した後、内通EPG契約として、契約を設定できます。手順はVMware VDS、OVS、およびベアメタル サーバで同じです。

始める前に

- 設定されている、EPG は必須です。
- フィルタを持つ契約を設定している必要があります。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントを作成または選択します。

例：

```
apic1(config)# tenant Tenant-l3out
```

ステップ 3 外部 Layer 3 EPG を作成または選択します。

例：

```
apic1(config-tenant)# external-l3 epg ext-epg
```

ステップ 4 外部 EPG を VRF インスタンスにバインドします。

例：

```
apic1(config-tenant-l3ext-epg)# vrf member vrf1
```

ステップ 5 EPG 内で分離を有効にします。

例：

```
(config-tenant-l3ext-epg)# isolation enforce
```

その後、必要に応じて、コマンドの前に no を付けて EPG 内分離を無効にできます。

例：

```
(config-tenant-l3ext-epg)# no isolation enforce
```

ステップ 6 エンドポイント間の目的のトラフィックを許可する契約を内部 EPG に割り当てます。

例：

```
apic1(config-tenant-l3ext-epg)# contract intra-epg contr-intra
```

REST API を使用したアプリケーション EPG への EPG 内契約の追加

コントラクトを設定した後、EPG内コントラクトとしてEPGにコントラクトを追加できます。この手順は、VMware VDS、OVS、およびベアメタル サーバと同じです。

始める前に

- EPG が設定済みである必要があります。
- フィルタが設定されたコントラクトが必要です。

手順

ステップ 1 次の例のような XML POST 要求を使用してセレクタを設定します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>
  <infraInfra>
    <infraAccPortP name="Ports-1-12" status="deleted"/>

    <!-- VMM VLAN range -->
    <fvnsVlanInstP name="test" allocMode="dynamic">
      <fvnsEncapBlk name="encap" from="vlan-10" to="vlan-100"/>
    </fvnsVlanInstP>

    <!-- Static VLAN range -->
    <fvnsVlanInstP name="test" allocMode="static">
      <fvnsEncapBlk name="default" from="vlan-101" to="vlan-4095"/>
    </fvnsVlanInstP>

    <infraAttEntityP name="test">
      <infraRsDomP tDn="uni/phys-test"/>
      <infraRsDomP tDn="uni/l3dom-test"/>
      <infraRsDomP tDn="uni/vmmp-VMware/dom-test"/>
    </infraAttEntityP>

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

    <!-- Port profile -->
    <infraAccPortP name="test">
      <!-- 12 regular ports -->
      <infraHPortS name="ports1Through12" type="range">
        <infraPortBlk name="default" fromCard="1" toCard="1" fromPort="1" toPort="12"/>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-test"/>
      </infraHPortS>

      <!-- 2 ports in PC -->
      <infraHPortS name="portsForPc1" type="range">
       <infraPortBlk name="default" fromCard="1" toCard="1" fromPort="13" toPort="14"/>
```

```
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-testPc"/>
  </infraHPortS>

  <!-- 2 ports in PC -->
  <infraHPortS name="portsForPc2" type="range">
    <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="15" toPort="16"/>
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-pc"/>
  </infraHPortS>

  <!-- 2 ports in PC for FEX -->
  <infraHPortS name="portsForFex" type="range">
    <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="17" toPort="18"/>
    <infraRsAccBaseGrp tDn="uni/infra/fexprof-default/fexbundle-test" fexId="111"/>
  </infraHPortS>

  <!-- 2 ports in PC for VPC -->
  <infraHPortS name="portsForVpc" type="range">
    <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="19" toPort="20"/>
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-testVpc"/>
  </infraHPortS>
</infraAccPortP>

<!-- FEX profile -->
<infraFexP name="default">
  <infraFexBndlGrp name="default"/>

  <!-- 12 FEX ports -->
  <infraHPortS name="ports1Through12" type="range">
    <infraPortBlk name="default" fromCard="1" toCard="1" fromPort="1" toPort="12"/>
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-test"/>
  </infraHPortS>

  <!-- 3 ports in FEX PC -->
  <infraHPortS name="portsForPc" type="range">
    <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="13" toPort="16"/>
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-testPcOnFex"/>
  </infraHPortS>

  <!-- 3 ports in FEX VPC -->
  <infraHPortS name="portsForVpc" type="range">
    <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="17" toPort="19"/>
    <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-testVpcOnFex"/>
  </infraHPortS>
</infraFexP>

<!-- Functional profile -->
<infraFuncP>
  <!-- Regular port group -->
  <infraAccPortGrp name="test">
    <infraRsAttEntP tDn="uni/infra/attentp-test"/>
  </infraAccPortGrp>

  <!-- PC -->
  <infraAccBndlGrp name="testPc" lagT="link">
    <infraRsLacpPol tnLacpLagPolName="testPc"/>
    <infraRsAttEntP tDn="uni/infra/attentp-test"/>
  </infraAccBndlGrp>

  <!-- VPC -->
  <infraAccBndlGrp name="testVpc" lagT="node">
    <infraRsLacpPol tnLacpLagPolName="testVpc"/>
    <infraRsAttEntP tDn="uni/infra/attentp-test"/>
  </infraAccBndlGrp>
```

```
      <!-- PC on FEX -->
      <infraAccBndlGrp name="testPcOnFex" lagT="link">
        <infraRsLacpPol tnLacpLagPolName="testPcOnFex"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test"/>
      </infraAccBndlGrp>

      <!-- VPC on FEX -->
      <infraAccBndlGrp name="testVpcOnFex" lagT="node">
        <infraRsLacpPol tnLacpLagPolName="testVpcOnFex"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test"/>
      </infraAccBndlGrp>
    </infraFuncP>

    <!-- Link aggregation policies -->
    <lacpLagPol name="testPc" minLinks='1' maxLinks='10'/>
    <lacpLagPol name="testVpc" minLinks='1' maxLinks='10'/>
    <lacpLagPol name="testPcOnFex" minLinks='2' maxLinks='5'/>
    <lacpLagPol name="testVpcOnFex" minLinks='2' maxLinks='10'/>
  </infraInfra>

  <fabricInst>
    <fabricProtPol name="testVpc">
      <fabricExplicitGEp name="testVpc" id="101">
        <fabricNodePEp id="101"/>
        <fabricNodePEp id="102"/>
      </fabricExplicitGEp>
    </fabricProtPol>
  </fabricInst>

  <physDomP name="test">
    <infraRsVlanNs tDn="uni/infra/vlanns-test-static"/>
  </physDomP>

  <l3extDomP name="test">
    <infraRsVlanNs tDn="uni/infra/vlanns-test-static"/>
  </l3extDomP>
</polUni>
```

ステップ 2 次の例のような XML POST 要求を使用してテナントを設定します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>
   <fvTenant name="Tenant-l3out">
      <vzBrCP intent="install" name="contr-intra" scope="context">
         <vzSubj consMatchT="AtleastOne" name="subj" revFltPorts="yes">
            <vzRsSubjFiltAtt action="permit" priorityOverride="default"
              tnVzFilterName="flt-ssh" />
         </vzSubj>
      </vzBrCP>
      <vzBrCP intent="install" name="contr2" scope="context">
         <vzSubj consMatchT="AtleastOne" name="contr2-subj" revFltPorts="yes">
            <vzRsSubjFiltAtt action="permit" priorityOverride="default"
              tnVzFilterName="flt-ftp" />
         </vzSubj>
      </vzBrCP>
      <vzBrCP intent="install" name="contr1" scope="context">
         <vzSubj consMatchT="AtleastOne" name="subj-http" revFltPorts="yes">
            <vzRsSubjFiltAtt action="deny" priorityOverride="default"
              tnVzFilterName="flt-http" />
         </vzSubj>
      </vzBrCP>
      <l3extOut enforceRtctrl="export" mplsEnabled="no" name="l3out1">
```

```
   <l3extRsL3DomAtt tDn="uni/l3dom-test" />
   <l3extRsEctx tnFvCtxName="vrf1" />
   <l3extLNodeP name="l3out1_nodeProfile" tag="yellow-green">
      <l3extRsNodeL3OutAtt rtrId="172.16.0.1" rtrIdLoopBack="yes"
        tDn="topology/pod-1/node-101" />
      <l3extLIfP name="l3out1_interfaceProfile" tag="yellow-green">
         <l3extRsPathL3OutAtt addr="192.168.15.1/24" autostate="disabled"
           encap="unknown" encapScope="local" ifInstT="l3-port" ipv6Dad="enabled"
           isMultiPodDirect="no" llAddr="::" mac="00:22:BD:F8:19:FF"
           mode="regular" mtu="inherit"
           tDn="topology/pod-1/paths-101/pathep-[eth1/10]" />
      </l3extLIfP>
   </l3extLNodeP>

   <!--
     Set pcEnfPref to "enforced" to enable intra-Ext-EPG isolation.
     Set pcEnfPref to "unenforced" to disable intra-Ext-EPG isolation.
   -->
   <l3extInstP floodOnEncap="disabled" matchT="AtleastOne"
     name="l3epg1" pcEnfPref="unenforced" prefGrMemb="exclude">
      <l3extSubnet ip="172.16.0.0/16" scope="import-security" />
      <fvRsCons tnVzBrCPName="contr2" />
      <fvRsIntraEpg tnVzBrCPName="contr-intra" />
   </l3extInstP>
</l3extOut>
<fvCtx bdEnforcedEnable="no" ipDataPlaneLearning="enabled" knwMcastAct="permit"
  name="vrf1" pcEnfDir="egress" pcEnfPref="unenforced" vrfIndex="0">
   <fvRsVrfValidationPol />
   <vzAny matchT="AtleastOne" prefGrMemb="disabled" />
</fvCtx>
<fvBD OptimizeWanBandwidth="no" arpFlood="yes" epClear="no" hostBasedRouting="no"
  intersiteBumTrafficAllow="no" intersiteL2Stretch="no" ipLearning="yes"
  ipv6McastAllow="no" limitIpLearnToSubnets="yes" llAddr="::"
  mac="00:22:BD:F8:19:FF" mcastAllow="no" multiDstPktAct="bd-flood" name="bd-web"
  type="regular" unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood"
  v6unkMcastAct="flood" vmac="not-applicable">
   <fvSubnet ip="192.168.1.254/24" ipDPLearning="enabled" preferred="no"
     scope="private" virtual="no" />
   <fvRsCtx tnFvCtxName="vrf1" />
   <fvRsBdToEpRet resolveAct="resolve" />
</fvBD>
<fvBD OptimizeWanBandwidth="no" arpFlood="yes" epClear="no" hostBasedRouting="no"
  intersiteBumTrafficAllow="no" intersiteL2Stretch="no" ipLearning="yes"
  ipv6McastAllow="no" limitIpLearnToSubnets="yes" llAddr="::"
  mac="00:22:BD:F8:19:FF" mcastAllow="no" multiDstPktAct="bd-flood" name="bd-app"
  type="regular" unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood"
  v6unkMcastAct="flood" vmac="not-applicable">
   <fvSubnet ip="192.168.2.254/24" ipDPLearning="enabled" preferred="no"
     scope="private" virtual="no" />
   <fvRsCtx tnFvCtxName="vrf1" />
   <fvRsBdToEpRet resolveAct="resolve" />
</fvBD>
<vzFilter name="flt-ftp">
   <vzEntry applyToFrag="no" arpOpc="unspecified" dFromPort="ftpData"
     dToPort="ftpData" etherT="ipv4" icmpv4T="unspecified" icmpv6T="unspecified"
     matchDscp="unspecified" name="ftp" prot="tcp" sFromPort="unspecified"
     sToPort="unspecified" stateful="no" />
</vzFilter>
<vzFilter name="flt-ssh">
   <vzEntry applyToFrag="no" arpOpc="unspecified" dFromPort="ssh" dToPort="ssh"
     etherT="ipv4" icmpv4T="unspecified" icmpv6T="unspecified"
     matchDscp="unspecified" name="ssh" prot="tcp" sFromPort="unspecified"
     sToPort="unspecified" stateful="no" />
</vzFilter>
```

```
        <vzFilter name="flt-http">
           <vzEntry applyToFrag="no" arpOpc="unspecified" dFromPort="http" dToPort="http"
             etherT="ipv4" icmpv4T="unspecified" icmpv6T="unspecified"
             matchDscp="unspecified" name="flt1" prot="tcp" sFromPort="unspecified"
             sToPort="unspecified" stateful="no" />
        </vzFilter>
        <fvAp name="ap-app1">
           <fvAEPg floodOnEncap="disabled" hasMcastSource="no" isAttrBasedEPg="no"
             matchT="AtleastOne" name="epg-app" pcEnfPref="unenforced"
             prefGrMemb="exclude" shutdown="no">
              <fvRsProv intent="install" matchT="AtleastOne" tnVzBrCPName="contr2" />
              <fvRsProv intent="install" matchT="AtleastOne" tnVzBrCPName="contr1" />
              <fvRsPathAtt encap="vlan-103" instrImedcy="immediate" mode="native"
                primaryEncap="unknown" tDn="topology/pod-1/paths-101/pathep-[eth1/3]" />
              <fvRsDomAtt bindingType="none" classPref="encap" encap="unknown"
                encapMode="auto" epgCos="Cos0" epgCosPref="disabled" instrImedcy="lazy"
               netflowDir="both" netflowPref="disabled" numPorts="0" portAllocation="none"

                primaryEncap="unknown" primaryEncapInner="unknown" resImedcy="immediate"
                secondaryEncapInner="unknown" switchingMode="native" tDn="uni/phys-test"
                untagged="no" vnetOnly="no" />
              <fvRsBd tnFvBDName="bd-app" />
           </fvAEPg>
           <fvAEPg floodOnEncap="disabled" hasMcastSource="no"
            isAttrBasedEPg="no" matchT="AtleastOne" name="epg-web" pcEnfPref="unenforced"

             prefGrMemb="exclude" shutdown="no">
              <fvRsPathAtt encap="vlan-104" instrImedcy="immediate" mode="native"
                primaryEncap="unknown" tDn="topology/pod-1/paths-101/pathep-[eth1/4]" />
              <fvRsDomAtt bindingType="none" classPref="encap" encap="unknown"
                encapMode="auto" epgCos="Cos0" epgCosPref="disabled" instrImedcy="lazy"
               netflowDir="both" netflowPref="disabled" numPorts="0" portAllocation="none"

                primaryEncap="unknown" primaryEncapInner="unknown" resImedcy="immediate"
                secondaryEncapInner="unknown" switchingMode="native" tDn="uni/phys-test"
                untagged="no" vnetOnly="no" />
              <fvRsCons intent="install" tnVzBrCPName="contr1" />
              <fvRsBd tnFvBDName="bd-web" />
           </fvAEPg>
        </fvAp>
     </fvTenant>
</polUni>
```

EPG のコントラクト継承

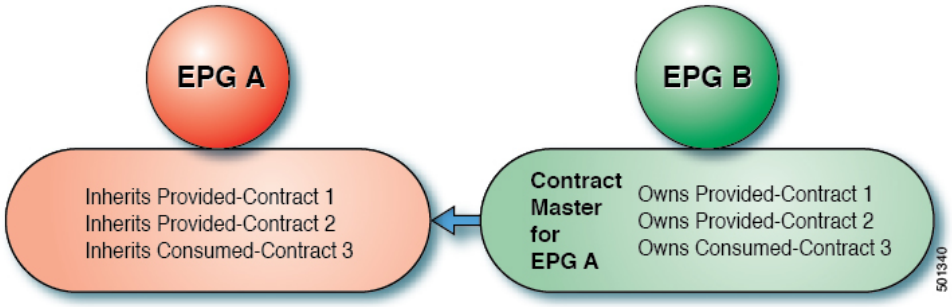
コントラクト継承について

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 *10* : 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。

GUI を使用した EPG のコントラクト継承の設定

GUI を使用したアプリケーション EPG のコントラクト継承の設定

アプリケーション EPG のコントラクト継承を設定するには、APIC の基本または拡張モード GUI で次の手順を使用します。

始める前に

EPG が使用するテナントとアプリケーション プロファイルを設定します。

オプション。コントラクトを継承する EPG が使用するブリッジ ドメインを設定します。

EPG コントラクト マスターとして機能するように、少なくとも 1 つのアプリケーション EPG を設定します。

共有するコントラクトを設定し、コントラクト マスターに関連付けます。

手順

ステップ 1 **[Tenants]** > ***[tenant-name]*** > **[Application Profiles]** に移動して、[AP-name] を展開します。

ステップ 2 [Application EPGs] を右クリックし、[Create Application EPG] を選択します。

ステップ 3 **EPG コントラクト マスター**からコントラクトを継承する EPG の名前を入力します。

ステップ 4 [Bridge Domain] フィールドで、共通/デフォルトのブリッジ ドメインまたは以前に作成したブリッジ ドメインを選択するか、この EPG のブリッジ ドメインを作成します。

ステップ 5 [EPG Contract Master] フィールドで、+ 記号をクリックして事前に設定したアプリケーション プロファイルと EPG を選択し、[Update] をクリックします。

ステップ 6 [Finish] をクリックします。

ステップ 7 EPG に関する情報（コントラクト マスターなど）を表示するには、**[Tenants]** > ***[tenant-name]*** > **[Application Profiles]** > ***[AP-name]*** > **[Application EPGs]** > ***[EPG-name]*** に移動します。**EPG コントラクト マスター**を表示するには、[General] をクリックします。

ステップ 8 継承されるコントラクトに関する情報を表示するには、[EPG-name] を展開して [Contracts] をクリックします。

GUI を使用した uSeg EPG のコントラクト継承の設定

uSeg EPG のコントラクト継承を設定するには、APIC の基本または拡張モード GUI で次の手順を使用します。

始める前に

EPG が使用するテナントとアプリケーション プロファイルを設定します。

オプション。コントラクトを継承する EPG が使用するブリッジ ドメインを設定します。

EPG コントラクト マスターとして機能するように uSeg EPG を設定します。

共有するコントラクトを設定し、コントラクト マスターに関連付けます。

手順

ステップ 1 **[Tenants]** > ***[tenant-name]*** > **[Application Profiles]** に移動して、[AP-name] を展開します。

ステップ 2 [uSeg EPGs] を右クリックし、[Create uSeg EPG] を選択します。

ステップ 3 コントラクト マスターからコントラクトを継承する EPG の名前を入力します。

ステップ 4 [Bridge Domain] フィールドで、共通/デフォルトのブリッジ ドメインまたは以前に作成したブリッジ ドメインを選択するか、この EPG のブリッジ ドメインを作成します。

ステップ 5 [uSeg-EPG-name] をクリックします。[EPG Contract Master] フィールドで、+ 記号をクリックしてアプリケーションプロファイルと EPG（コントラクトマスターとして機能する）を選択し、[Update] をクリックします。

ステップ 6 [Finish] をクリックします。

ステップ 7 契約に関する情報を表示するには、**[Tenants]** > **テナント名** > **[Application Profiles]** > ***AP* 名** > **[uSeg EPGs]** > に移動し、EPG 名を展開して [Contracts] をクリックします。。

GUI を使用した L2Out EPG のコントラクト継承の設定

外部 L2Out EPG のコントラクト継承を設定するには、Cisco Application Policy Infrastructure Controller（APIC）GUI で次の手順を実行します。

始める前に

EPG が使用するテナントとアプリケーション プロファイルを設定します。

Layer 2 Outside（L2Out）と、**L2Out Contract Master** として機能する外部 L2Out EPG（L2extInstP）を設定します。

共有するコントラクトを設定し、コントラクト マスターに関連付けます。

手順

ステップ 1 **[テナント（Tenants）]** > ***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L2Outs]** に移動します。

ステップ 2 [L2Out-name] を展開します。

ステップ 3 **[外部 EPG（External EPGs）]** を右クリックし、**[外部 EPG の作成（Create External EPG）]** を選択します。

ステップ 4 外部ネットワークの名前を入力し、必要に応じてその他の属性を追加します。

ステップ 5 **Submit** をクリックします。

ステップ 6 **外部 EPG（External EPGs）]** を展開します。

ステップ 7 ***external-epg-name*** をクリックします。

ステップ 8 **[外部 EPG（External EPG）]** パネルで、**[L2Out コントラクト マスター（L2Out Contract Masters）]** フィールドの [+] 記号をクリックします。

ステップ 9 この外部 L2Out EPG の L2Out および L2Out コントラクト マスターを選択します。

ステップ 10 [更新（Update）] をクリックします。

ステップ 11 この外部 L2Out EPG によって継承されたコントラクトを表示するには、外部 EPG 名をクリックし、**[コントラクト（Contracts）]** > **[継承コントラクト（Inherited Contracts）]** をクリックします。

GUI を使用して外部 L3Out EPG コントラクト継承

外部 L3Out EPG のコントラクト継承を設定するには、Cisco Application Policy Infrastructure Controller（APIC）GUI で次の手順を使用します。

始める前に

EPG が使用するテナントとアプリケーション プロファイルを設定します。

外部ルーテッド ネットワーク（L3Out）と、**L3Out コントラクト マスター**として機能する外部 L3Out EPG（L3extInstP）を設定します。

共有するコントラクトを設定し、コントラクト マスターに関連付けます。

手順

ステップ 1 外部 L3Out EPG のコントラクト継承を設定するには、**[テナント（Tenants）]** > ***[tenant-name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** に移動します。

ステップ 2 外部 L3Out EPG につながる [L3Out-name] を展開します。

ステップ 3 **[外部 EPG（External EPGs）]** を右クリックし、**[外部 EPG の作成（Create External EPG）]** を選択します。

ステップ 4 外部 EPG の名前を入力し、オプションでサブネットおよびその他の属性を追加します。

ステップ 5 **Submit** をクリックします。

ステップ 6 [Networks] を展開します。

ステップ 7 [network-name] をクリックします。

ステップ 8 **[外部 EPG（External EPG）]** パネルで、**[L3Out コントラクト マスター（L3Out Contract Masters）]** フィールドの [+] 記号をクリックします。

ステップ 9 この外部 L3Out EPG の L3Out コントラクト マスターとして機能する L3Out および外部 EPG を選択します。

ステップ 10 [更新（Update）] をクリックします。

ステップ 11 この外部 L3Out EPG によって継承されたコントラクトを表示するには、外部 EPG 名をクリックし、**[コントラクト（Contracts）]** > **[継承コントラクト（Inherited Contracts）]** をクリックします。

優先グループ契約

契約優先グループについて

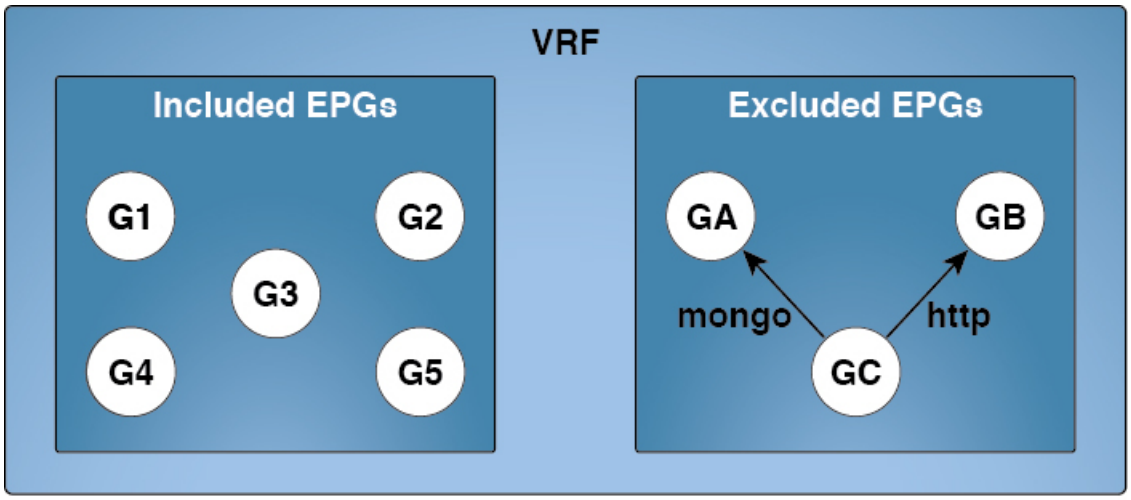
契約優先グループが設定されている VRF で、EPG に利用可能なポリシー適用には 2 種類あります。

- 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 *11* : 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。

契約優先グループの注意事項

契約優先グループを設定する際には、次の注意事項を参照してください:

- （s、g）エントリが境界リーフ スイッチにインストールされている場合、次の条件を満たすと、ファブリックからファブリック外部の送信元に送られたユニキャスト トラフィックでドロップが生じることがあります。
  - 優先グループが L3Out EPG で使用されている
  - 送信元のユニキャスト ルーティング テーブルでデフォルト ルート 0.0.0.0/0 が使用されている

  これは予想された動作です。
- 契約優先グループに含まれる EPG は、外部 EPG (InstP) の 0/0 プレフィックスではサポートされていません。外部 EPG (InstP) からテナント EPG に対し、契約優先グループで使用するために 0/0 プレフィックスが必要な場合には、0/0 を 0/1 と 128/1 に分割することができます。
- 契約優先グループ EPG は、GOLF 機能ではサポートされていません。アプリケーション EPG と GOLF の L3Out EPG との間の通信は、明示的な契約によって制御する必要があります。

GUI を使用した契約優先グループの設定

始める前に

テナントと VRF、および契約優先グループを使用する EPG を作成します。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **テナント名**をクリックします。

ステップ 2 [Navigation] ペインで、テナント、[Networking]、[VRFs] の順に展開します。

ステップ 3 コントラクト優先グループを設定する VRF 名をクリックします。

ステップ 4 **Preferred Group Member** フィールドで、**Enabled** をクリックします。

ステップ 5 **Submit** をクリックします。

ステップ 6 **Navigation** ウィンドウで、**Application Profiles** を展開し、テナント VRF のアプリケーション プロファイルを作成するか、展開します。

ステップ 7 **Application EPGs** を展開し、契約優先グループを使用する EPG をクリックします。

ステップ 8 [Policy] および [General] タブを選択します。

ステップ 9 **Preferred Group Member** フィールドで、**Include** をクリックします。

ステップ 10 **Submit** をクリックします。

次のタスク

この EPG と無制限の通信を行う、他の EPG の優先グループのメンバーシップを有効にします。また、優先グループの EPG とメンバーではないかもしれない他の EPG の間の通信を制御する、適切な契約を設定することもできます。

（注） L4-L7 サービス グラフを介して優先グループ メンバーをサポートする場合は、L4-L7 サービス EPG ポリシーを作成する必要があります。L4-L7 サービス EPG ポリシーの作成に関する詳細については、GUI を使用した L4-L7 サービス EPG ポリシーの作成（284 ページ）を参照してください。

GUI を使用した L4-L7 サービス EPG ポリシーの作成

このタスクでは、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を定義するポリシーを作成します。優先グループ メンバーシップにより、エンドポイントは契約がなくても相互に通信できます。作成したポリシーは、EPG にサービス グラフ テンプレートを適用するときに選択できます。

始める前に

テナントを作成しておく必要があります。

手順

ステップ 1 メニュー バーで、[Tenant] > テナント名を選択します。

ステップ 2 [Navigation] ペインで、[Policies] > [Protocol] > [L4-L7 Service EPG Policy] を選択します。

ステップ 3 [Navigation] ペインで、[L4-L7 Service EPG Policy] を右クリックして [Create L4-L7 Service EPG Policy] を選択します。

[Create L4-L7 Service EPG Policy] ダイアログボックスが表示されます。

ステップ 4 [Name] フィールドにポリシーの一意の名前を入力します。

ステップ 5 オプション。[Description] フィールドにポリシーの説明を入力します。

ステップ 6 [Preferred Group Member] フィールドで、EPG を除外するか優先メンバーとして含めるかを選択します。

ステップ 7 [Submit] をクリックします。`

新しく作成したポリシーが [L4-L7 Service EPG Policy] 作業ウィンドウ リストに表示されます。作業ウィンドウでポリシーを編集するには、ポリシーを含む行をダブルクリックします。

次のタスク

サービス グラフを EPG に適用するときに、サービス グラフ テンプレートで新しい L4-L7 サービス EPG ポリシーを選択できるようになりました。『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「Using the GUI」の章で「Applying a Service Graph Template to Endpoint Groups Using the GUI」を参照してください。

許可ルールと拒否ルールを含む契約

許可ルールおよび拒否ルールを含む契約の概要

Cisco Application Policy Infrastructure Controller（Cisco APIC）リリース 3.2 以降では、許可だけではなく、許可と拒否の両方のアクションを含む契約を設定できます。さまざまな優先順位（デフォルト、高、中、低）の拒否アクションを設定できます。

ルールの競合は次のように解決されます。

- 暗黙の否定には、すべてのルールの中で最も低い優先順位が割り当てられます。
- VzAny 間の契約には暗黙の拒否より高い優先順位が割り当てられます。
- EPG 間の契約のルールは vzAny 間のルールより優先順位が高いため、特定の EPG ペア間の契約は vzAny の契約よりも優先されます。
- 特定の EPG ペア間の契約に含まれるデフォルト優先順位の拒否ルールは、その EPG ペアの許可ルールと優先順位レベルが同じです。同じ優先順位の許可ルールと拒否ルールの両方がトラフィックに一致する場合は、拒否ルールが優先されます。
- vzAny 間の契約に含まれるデフォルト優先順位の拒否ルールは、その vzAny ペアの許可ルールと優先順位レベルが同じです。同じ優先順位の許可ルールと拒否ルールの両方がトラフィックに一致する場合は、拒否ルールが優先されます。
- 優先順位が最も高い拒否ルールは、EPG 間の契約と同じレベルで処理されます。
- 優先順位が中の拒否ルールは、vzAny-EPG 間の契約と同じレベルで処理されます。

- 優先順位が最も低い拒否ルールは、vzAny 間の契約と同じレベルで処理されます。
- EPG 間の契約で拒否の優先順位を下げると、EPG 間の許可ルールの一致が拒否よりも優先されます。

GUI を使用してACL 契約の許可とロギングの拒否を有効にする

次の手順では、GUI を使用してACL 契約の許可とロギングの拒否を有効にする方法を表示します。

（注） 許可ロギングを含むテナントは、EPG が関連する VRF を含むテナントです。これは必ずしもEPG と同じテナントや関連する契約である必要はありません。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[<tenant name>]** の順に選択します。

ステップ 2 [Navigation] ペインで、[Contracts] を展開し、 [Standard] を右クリックして [Create Contract] を選択します。

ステップ 3 [Create Contract] ダイアログボックスで、次の作業を実行します。

a) [Name] フィールドに、契約の名前を入力します。
b) [Scope] フィールドで、そのスコープ（[VRF]、[Tenant]、または [Global]）を選択します
c) オプション。契約に適用するターゲット DSCP または QoS クラスを設定します。
d) [+] アイコンをクリックして、[Subject] を展開します。

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

ステップ 5 件名の名前と詳細な説明を入力します。

ステップ 6 オプション。ターゲット DSCP のドロップダウン リストから、件名に適用する DSCP を選択します。

ステップ 7 契約を両方向でなくコンシューマからプロバイダの方向にのみ適用するのでない限り、[Apply Both Directions] はオンにしたままにしておきます。

ステップ 8 [Apply Both Directions] をチェックしてない場合 [Reverse Filter Ports] をチェックしたままにして、ルールがプロバイダから消費者に適用されるようにレイヤ 4 ソースと宛先ポートを交換します。

ステップ 9 [+] アイコンをクリックして、[Filters] を展開します。

ステップ 10 [Name] ドロップダウン リストで、たとえば、**arp**、**default**、**est**、**icmp** などオプションを選択するか、以前設定したフィルタを選択します。

ステップ 11 [Directives] ドロップダウン リストで、[log] をクリックします。

ステップ 12 （任意） この件名で実行するアクションを [Deny] に変更します（またはアクションをデフォルトの [Permit] のままにします。

Directive：ログ有効化により、この件名のアクションが [Permit] になっている場合、ACL は件名と契約により制御されているフローとパケットを追跡します。この件名のアクションが [Deny] の場合、ACL の拒否ログはフローとパケットを追跡します。

ステップ 13 （任意） 件名の優先順位を設定します。

ステップ 14 [Update] をクリックします。

ステップ 15 [OK] をクリックします。

ステップ 16 **[送信（Submit）]** をクリックします。
ロギングがこの契約に対して有効になります。

NX-OS CLI を使用した ACL 契約許可ロギングの有効化

次の例は、NX-OS CLI を使用して契約許可ロギングを有効にする方法を示しています。

手順

ステップ 1 契約許可ルールにより送信できたパケットまたはフローのロギングを有効にするには、次のコマンドを使用します。

```
configure
tenant <tenantName>
contract <contractName> type <permit>
subject <subject Name>
access-group <access-list> <in/out/both> log
```

例：

次に例を示します。

```
apic1# configure
apic1(config)# tenant BDMode1
apic1(config-tenant)# contract Logicmp type permit
apic1(config-tenant-contract)# subject icmp
apic1(config-tenant-contract-subj)# access-group arp both log
```

ステップ 2 許可ロギングを無効にするには、**no** 形式の access-group コマンドを使用します。たとえば、`no access-group arp both log` コマンドを使用します。

REST API を使用した ACL 契約許可ロギングの有効化

次の例は、REST API を使用して許可および拒否ロギングを有効にする方法を示しています。この例では、ACL の許可を設定し、件名 Permit 設定し、設定されたアクションを拒否するには、契約のロギングを拒否します。

手順

この設定では、次の例のように XML で post を送信します。

例：

```
<vzBrCP dn="uni/tn-Tenant64/brc-C64" name="C64" scope="context">
    <vzSubj consMatchT="AtleastOne" name="HTTPSsbj" provMatchT="AtleastOne"
revFltPorts="yes" rn="subj-HTTPSsbj">
         <vzRsSubjFiltAtt action="permit" directives="log" forceResolve="yes"
priorityOverride="default"
rn="rssubjFiltAtt-PerHTTPS" tDn="uni/tn-Tenant64/flt-PerHTTPS" tRn="flt-PerHTTPS"
tnVzFilterName="PerHTTPS"/>
    </vzSubj>
    <vzSubj consMatchT="AtleastOne" name="httpSbj" provMatchT="AtleastOne"
revFltPorts="yes" rn="subj-httpSbj">
        <vzRsSubjFiltAtt action="deny" directives="log" forceResolve="yes"
priorityOverride="default"
rn="rssubjFiltAtt-httpFilter" tDn="uni/tn-Tenant64/flt-httpFilter" tRn="flt-httpFilter"
 tnVzFilterName="httpFilter"/>
    </vzSubj>
   <vzSubj consMatchT="AtleastOne" name="subj64" provMatchT="AtleastOne" revFltPorts="yes"
 rn="subj-subj64">
        <vzRsSubjFiltAtt action="permit" directives="log" forceResolve="yes"
priorityOverride="default"
rn="rssubjFiltAtt-icmp" tDn="uni/tn-common/flt-icmp" tRn="flt-icmp" tnVzFilterName="icmp"/>

    </vzSubj>
</vzBrCP>
```

GUI を使用した禁止契約拒否ロギングの有効化

次の手順は、GUI を使用して禁止コントラクトの拒否ロギングを有効にする方法を示しています。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[<tenant name>]** の順に選択します。

ステップ 2 [Navigation] ペインで、[Contracts] を展開します。

ステップ 3 [Taboos] を右クリックし、[Create Taboo Contract] を選択します。

ステップ 4 [Create Taboo Contract] ダイアログ ボックスで、次の操作を実行して禁止契約を指定します。

a) [Name] フィールドに、契約の名前を入力します。

b) オプション。[Description] フィールドに、禁止契約の説明を入力します。

c) [+] アイコンをクリックして、[Subject] を展開します。

ステップ 5 [Create Taboo Contract Subject] ダイアログ ボックスで、次の操作を実行します。

a) [Specify Identity of Subject] 領域に、名前と説明（オプション）を入力します。

b) [+] アイコンをクリックして、[Filters] を展開します。
c) [Name] ドロップダウン リストから、**<tenant_name>/arp**、 **<tenant_name>/default**、**<tenant_name>/est**、**<tenant_name>/icmp** などのデフォルト値のいずれかを選択し、以前作成したフィルタか [Create Filter] を選択します。

（注）
[Specify Filter Identity] 領域で [Create Filter] を選択した場合、次の操作を実行して、ACL 拒否ルールの基準を指定します。

1. 名前とオプションの説明を入力します。
2. [Entries] を展開し、ルールの名前を入力して、拒否するトラフィックを定義する条件を選択します。
3. [Directives] ドロップダウンリストで [log] を選択します。
4. [Update] をクリックします。
5. [OK] をクリックします。

ステップ 6 **[送信（Submit）]** をクリックします。
ロギングがこの禁止契約に対して有効になります。

NX-OS CLI を使用した禁止契約拒否ロギングの有効化

次の例は、NX-OS CLI を使用して禁止契約拒否ロギングを有効にする方法を示しています。

手順

ステップ 1 禁止契約拒否ルールのためにドロップされたパケットまたはフローのロギングを有効にするには、次のコマンドを使用します。

```
configure
tenant <tenantName>
contract <contractName> type <deny>
subject <subject Name>
access-group <access-list> <both> log
```

例：

次に例を示します。

```
apic1# configure
apic1(config)# tenant BDMode1
apic1(config-tenant)# contract dropFTP type deny
apic1(config-tenant-contract)# subject dropftp
apic1(config-tenant-contract-subj)# access-group ftp both log
```

ステップ 2 拒否ロギングを無効にするには、**no** 形式の access-group コマンドを使用します。たとえば、`no access-group https both log` コマンドを使用します。

REST API を使用した禁止契約拒否ロギングの有効化

次の例は、REST API を使用して禁止契約拒否ロギングを有効にする方法を示しています。

手順

タブー契約を設定するロギングを拒否する、次の例のように XML で post を送信します。

例：

```
<vzTaboo dn="uni/tn-Tenant64/taboo-TCtrctPrefix" name="TCtrctPrefix" scope="context">
    <vzTSubj name="PrefSubj" rn="tsubj-PrefSubj"">
        <vzRsDenyRule directives="log" forceResolve="yes" rn="rsdenyRule-default"
tCl="vzFilter"
tDn="uni/tn-common/flt-default" tRn="flt-default"/>
    </vzTSubj>
</vzTaboo>
```

GUI を使用した ACL 許可および拒否ログの表示

次の手順は、GUI を使用して、トラフィック フローの ACL 許可および拒否ログを（有効になっていれば）表示する方法を示しています。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[<tenant name>]** の順に選択します。

ステップ 2 [Navigation] ペインで、[Tenant <tenant name>] をクリックします。

ステップ 3 **Tenants <tenant name> [Work]** ペインで、**[Operational]** タブをクリックします。

ステップ 4 [Operational] タブの下で、[Flows] タブをクリックします。
[Flows] タブの下で、いずれかのタブをクリックして、レイヤ 2 許可ログ（[L2 Permit]）、レイヤ 3 許可ログ（[L3 Permit]）、レイヤ 2 拒否ログ（[L2 Drop]）、またはレイヤ 3 拒否ログ（[L3 Drop]）のログ データを表示します。各タブで、トラフィックがフローしていれば、ACL ロギング データを表示できます。データ ポイントは、ログ タイプと ACL ルールに応じて異なります。たとえば、[L3 Permit] ログおよび [L3 Deny] ログには次のデータ ポイントが含まれます。

- VRF
- Alias
- 送信元 IP アドレス

- 宛先 IP アドレス
- プロトコル
- 送信元ポート
- 宛先ポート
- 送信元 MAC アドレス
- 宛先 MAC アドレス
- Node
- 送信元インターフェイス
- VRF Encap
- 送信元 EPG
- 宛先 EPG
- 送信元 PC タグ
- 宛先 PC タグ

（注）
また、[Flows] タブの横の [Packets] タブを使用して、シグニチャ、送信元、および宛先が同じであるパケットのグループ（最大 10 個）の ACL ログにアクセスできます。送信されたりドロップされたりするパケットのタイプを確認できます。

REST API を使用した ACL 許可および拒否ログ

次の例は、REST API を使用して、トラフィック フローのレイヤ 2 拒否ログ データを表示する方法を示しています。次の MO を使用してクエリを送信することができます。

- acllogDropL2Flow
- acllogPermitL2Flow
- acllogDropL3Flow
- acllogPermitL3Flow
- acllogDropL2Pkt
- acllogPermitL2Pkt
- acllogDropL3Pkt
- acllogPermitL3Pkt

始める前に

ACL 契約許可および拒否ログのデータを表示する前に、許可または拒否ロギングを有効にする必要があります。

手順

レイヤ 3 ドロップ ログ データを表示するには、REST API を使用して次のクエリを送信します。

```
GET https://apic-ip-address/api/class/acllogDropL3Flow
```

例：

次の例では、サンプル出力をいくつか示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <acllogPermitL3Flow childAction=""
dn="topology/pod-1/node-101/ndbgs/acllog/tn-common/ctx-inb

/permitl3flow-spctag-333-dpctag-444-sepgname-unknown-depgname-unknown-sip-[100:c000:a00:700:b00:0:f00:0]


-dip-[19.0.2.10]-proto-udp-sport-17459-dport-8721-smac-00:00:15:00:00:28-dmac-00:00:12:00:00:25-sintf-

        [port-channel5]-vrfencap-VXLAN: 2097153" dstEpgName="unknown" dstIp="19.0.2.10"
 dstMacAddr="00:00:12:00:00:25"
        dstPcTag="444" dstPort="8721" lcOwn="local" modTs="never" monPolDn=""
protocol="udp" srcEpgName="unknown"
        srcIntf="port-channel5" srcIp="100:c000:a00:700:b00:0:f00:0"
srcMacAddr="00:00:15:00:00:28" srcPcTag="333"
        srcPort="17459" status="" vrfEncap="VXLAN: 2097153"/>
    <acllogPermitL3Flow childAction=""
dn="topology/pod-1/node-102/ndbgs/acllog/tn-common/ctx-inb

/permitl3flow-spctag-333-dpctag-444-sepgname-unknown-depgname-unknown-sip-[100:c000:a00:700:b00:0:f00:0]-dip-


[19.0.2.10]-proto-udp-sport-17459-dport-8721-smac-00:00:15:00:00:28-dmac-00:00:12:00:00:25-sintf-

        [port-channel5]-vrfencap-VXLAN: 2097153" dstEpgName="unknown" dstIp="19.0.2.10"
 dstMacAddr="00:00:12:00:00:25"
        dstPcTag="444" dstPort="8721" lcOwn="local" modTs="never" monPolDn=""
protocol="udp" srcEpgName="unknown"
        srcIntf="port-channel5" srcIp="100:c000:a00:700:b00:0:f00:0"
srcMacAddr="00:00:15:00:00:28" srcPcTag="333"
        srcPort="17459" status="" vrfEncap="VXLAN: 2097153"/>
</imdata>
```

NX-OS CLI を使用した ACL 許可および拒否ログの表示

次の手順は、NX-OS スタイル CLI **show acllog** コマンドを使用して ACL ログの詳細を表示する方法を示しています。

レイヤ 3 コマンドの構文は、**show acllog {permit | deny} l3 {pkt | flow} tenant <tenant_name> vrf <vrf_name> srcip <source_ip> dstip <destination_ip> srcport <source_port> dstport <destination_port> protocol <protocol> srcintf <source_interface> start-time <startTime> end-time <endTime> detail** です。

レイヤ 2 コマンドの構文は、**show acllog {permit | deny} l2 {flow | pkt} tenant <tenant_name> vrf <VRF_name> srcintf <source_interface> vlan <VLAN_number> detail** です。

（注） **show acllog** コマンドの完全な構文は、第二世代 Cisco Nexus 9000 シリーズ スイッチ（N9K-C93180LC-EX など名前の最後に EX または FX がつく。もしくはそれ以降のシリーズ）および Cisco APIC リリース 3.2 以降でのみ使用できます。第一世代のスイッチ（名前の最後に EX または FX が付かない）または 3.2 以前の Cisco APIC リリースでは、使用可能な構文は上記の通りです。

Cisco APIC 3.2 以降では、追加のキーワードが **detail** keyword:**[dstEpgName <destination_EPG_name>| dstmac <destination_MAC_address> | dstpctag <destination_PCTag> | srcEpgName <source_EPG_name> | srcmac <source_MAC_address> | srcpctag <source_PCTag>]** とともにコマンドの両方のバージョンに追加されます。

手順

ステップ 1 次の例では、**show acllog drop l3 flow tenant common vrf default detail** コマンドを使用して、共通テナントのレイヤ 3 拒否ログに関する詳細情報を表示する方法を示します。

例：

```
apic1# show acllog deny l3 flow tenant common vrf default detail
SrcPcTag  : 49153
DstPcTag  : 32773
SrcEPG    : uni/tn-TSW_Tenant0/ap-tsw0AP0/epg-tsw0ctx0BD0epg6
DstEPG    : uni/tn-TSW_Tenant0/ap-tsw0AP0/epg-tsw0ctx0BD0epg5
SrcIp     : 16.0.2.10
DstIp     : 19.0.2.10
Protocol  : udp
SrcPort   : 17459
DstPort   : 8721
SrcMAC    : 00:00:15:00:00:28
DstMAC    : 00:00:12:00:00:25
Node      : 101
SrcIntf   : port-channel5
VrfEncap  : VXLAN: 2097153
```

この例では第二世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

ステップ 2 次の例では、**show acllog deny l2 flow tenant common vrf tsw0connctx0 detail** コマンドを使用して、共通テナントのレイヤ 3 拒否ログに関する詳細情報を表示する方法を示します。

例：

```
apic1# show acllog deny l2 flow tenant common vrf tsw0connctx0 detail
SrcPcTag DstPcTag   SrcEPG           DstEPG          SrcMAC            DstMAC
Node   SrcIntf   vlan
```

```
--------- --------- ----------------  --------------  --------------------
------------------   -----   ----------  ------
 32773    49153   uni/tn-TSW       uni/tn-TSW  00:00:11:00:00:11  11:00:32:00:00:33
101     port-     2
                  _Tenant0/ap-     _Tenant0/ap-
       channel8
                  tsw0AP0/epg-     tsw0AP0/epg-
                  tsw0ctx0BD0epg5  tsw0ctx0BD0epg6
```

この例では第二世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

ステップ 3 次の例では、**show acllog permit l3 pkt tenant <tenant name> vrf <vrf name> [detail]** コマンドを使用して、送信された一般的な VRF ACL レイヤ 3 許可パケットに関する詳細情報を表示する方法を示しています。

```
apic1# show acllog permit l3 pkt tenant common vrf default detail acllog permit l3 packets
 detail:
srcIp      : 10.2.0.19
dstIp      : 10.2.0.16
protocol   : udp
srcPort    : 13124
dstPort    : 4386
srcIntf    : port-channel5
vrfEncap   : VXLAN: 2097153
pktLen     : 112
srcMacAddr : 00:00:15:00:00:28
dstMacAddr : 00:00:12:00:00:25
timeStamp  : 2015-03-17T21:31:14.383+00:00
```

この例では第一世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

ステップ 4 次の例では、**show acllog permit l2 pkt tenant <tenant name> vrf <vrf name> srcintf <s interface>** コマンドを使用して、インターフェイス ポートチャネル 15 から送信されたデフォルトの VRF レイヤ 2 パケットに関する情報を表示する方法を示しています。

```
apic1# show acllog permit l2 pkt tenant common vrf default srcintf port-channel5

acllog permit L2 Packets
      Node          srcIntf       pktLen     timeStamp
 --------------  --------------  --------  --------------
                 port-channel5      1      2015-03-17T21:
                                           31:14.383+00:00
```

この例では第一世代のスイッチまたは 3.2 以前の Cisco APIC リリースでの出力を示します。

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。